MKWI 2018



Tagungsband

Multikonferenz Wirtschaftsinformatik 2018

Data driven X — Turning Data into Value

Band IV

Paul Drews, Burkhardt Funk, Peter Niemeyer und Lin Xie (Hrsg.)

6. - 9. März 2018, Leuphana Universität Lüneburg

LEUPHANA
UNIVERSITÄT LÜNEBURG

Paul Drews, Burkhardt Funk, Peter Niemeyer und Lin Xie (Hrsg.)

Multikonferenz Wirtschaftsinformatik 2018

Data driven X — Turning Data into Value

Leuphana Universität Lüneburg
6. - 9. März 2018

Band IV

LEUPHANA
UNIVERSITÄT LÜNEBURG

Impressum

Leuphana Universität Lüneburg
Institut für Wirtschaftsinformatik
Universitätsallee 1
21335 Lüneburg

ISBN 978-3-935786-72-0

mkwi2018.leuphana.de

Sponsoren der MKWI 2018













Inhaltsverzeichnis

Sponsoren **V**

Inhaltsverzeichnis **VII**

IT-Sicherheit für Kritische Infrastrukturen: Infrastrukturmanagement, Informationsmanagement und Risikomanagement **1331**

Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes
Clemens Sauerwein, Christian Sillaber, Ruth Breu 1333

Cloud Computing Adoption in Critical Infrastructures - Status Quo and Elements of a Research Agenda
Michael Adelmeyer, Frank Teuteberg 1345

IT-Sicherheit in Kritischen Infrastrukturen – eine Fallstudien-basierte Analyse von Praxisbeispielen
Sebastian Dännart, Thomas Diefenbach, Manfred Hofmeier, Andreas Rieb, Ulrike Lechner 1357

Information Security Awareness – eine konzeptionelle Neubetrachtung
Sebastian Richter, Tobias Straub, Carsten Lucke 1369

Sammlung geleakter Identitätsdaten zur Vorbereitung proaktiver Opfer-Warnung
Timo Malderle, Matthias Wübbeling, Michael Meier 1381

Entwicklung eines Prototypen zur Steigerung der Effizienz im Umgang mit den KRITIS-relevanten ISO/IEC 27K-Normen für die Anspruchsgruppe ISMS-Mitwirkende
Philipp Schütz, René Treibert, Jaroslaw Kopowski 1394

Forschungsprojekt zum digitalen Identitätsdiebstahl (research in progress)
Oliver Vettermann, Fabian Rack, Susan Gonscherowski 1402

Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share
Christian Sillaber, Clemens Sauerwein, Andrea Mussmann, Ruth Breu 1409

IT-Governance in der Integrierten Versorgung – eine risikobezogene Betrachtung
Lena Otto, Hannes Schlieter 1421

Modellierung betrieblicher Informationssysteme 1433

SenSoMod – A modelling language for context-sensitive mobile applications
Julian Dörndorfer, Christian Seel, Daniel Hilpoltsteiner 1435

Role-based Adaptation of Domain Reference Models: Suggestion of a Novel Approach
Hendrik Schön 1447

Enterprise Architecture Management in dynamischen Wertschöpfungsnetzwerken – Empfehlungen zur Interoperabilität
Jens Lachenmaier, Kathrin Pfähler, Hans-Georg Kemper 1454

Aligning Enterprise Knowledge and Data: A Domain-Specific Modeling Method for Social Media Strategies
Anna Widenmaier, Hans-Georg Fill 1466

UnSComT2G – Konzeption eines Tools zur Übertragung normsprachlicher Spezifikationen von Fachkomponenten in UML-Diagramme
Martin Robel 1478

Modelling product-service systems: An empirical analysis of requirements from a process-oriented perspective
Simon Hagen, Thorsten Schoormann, Sven Jannaber, Ralf Knackstedt, Oliver Thomas 1485

Organizational Roles in Capability Management – Experiences from an Industrial Project
Kurt Sandkuhl, Hasan Koç 1497

Towards Explaining the Popularity of the Business Model Canvas: A Dual Coding Approach
Thomas John, Daniel Szopinski 1509

A Multilevel Model of Pharmaceuticals
Monika Kaczmarek-Heß, Michael Heß 1516

OpenLabs als Innovations- und Produktionsstätten für Unternehmen 1529

Enabling decentral collaborative innovation processes - a web based real time collaboration platform
Matthias Joiko, Florian Kohnen, Kevin Lapinski, Houda Moudrik, Florian Paproth, Irawan Nurhas, Jan Pawlowski 1531

Exploring Innovation Practices for B2E Initiatives in the Digital Age
Vanessa Guggisberg, Andrea Back 1543

Smart Services: Kundenzentrierte Kombination von Dienstleistungen für Mobilität, Finanzen und Gesundheit 1551

Kundenzentrierte Mehrwertdienste zur Differenzierung von Automobilherstellern im Markt der Mobilitätsdienstleistungen
Alexander Sandau, Jorge Marx Gómez 1553

Vacuum Cleaning as a Service
Daniel Franzmann, Christoph Mittendorf, Uwe Ostermann 1565

Concepts of Product-Service Configurators for Repurposing used Electric Vehicle Batteries
Markus Monhof 1577

Nutzeranforderungen an mobile Applikationen für NFC-basierte eTickets im ÖPNV
Andreas Kreisel, Denise Rummler, Getraud Schäfer, Ulrike Stopka 1589

Structure for innovations: A use case taxonomy for smart glasses in service processes
Kai Klinker, Lisa Berkemeier, Benedikt Zobel, Hanna Wüller, Veronika Fries, Manuel Wiesche, Hartmut Remmers, Oliver Thomas, Helmut Krcmar 1599

Customer-Centred Intermodal Combination of Mobility Services with Conversational Interfaces
Daniel Braun, Adrian Hernandez-Mendez, Anne Faber, Manfred Langen, Florian Matthes 1611

Crowd Sourcing: Ko-Produktion integrierter multimodaler Mobilitäts- und Versorgungsdienste für Smart Regions - Status Quo, Konzeption und Entwicklungsperspektiven
Ingmar Ickerott, Frank Teuteberg, Maria Carmen Isabel Süßmuth 1623

Social Media Analytics **1635**

Content-Influencer-Fit: Improving Reach and Impact of Content for Influencers in eWOM
Hannes Rothe, Sebastian Wicke 1637

Sorting Out the Lemons – Identifying Product Failures in Online Reviews and their Relationship with Sales
Dominik Gutt 1649

Exploring Sense-Making Activities in Crisis Situations
Milad Mirbabaie, Sina Youn 1656

Strategien und Technologien der Digitalisierung in kleinen und mittleren Unternehmen **1669**

In-store Technologies in the Retail Servicescape
Jan Hendrik Betzing, Anh-Quoc Martin Hoang, Jörg Becker 1671

Sind kleinere und mittlere Unternehmen (KMU) bereits auf die Digitale Transformation vorbereitet?
Can Adam Albayrak, Andreas Gadatsch 1683

Are Local Retailers Conquering the Long Tail? A Web Usage and Association Rule Mining Approach on Local Shopping Platforms
Robin Ahlers, Lars Bollweg, Richard Lackes, André Ruegenberg, Ali Reza Samanpour, Markus Siepermann, Peter Weber 1694

IT-Sicherheit der Digitalisierung in Kleinen und Mittleren Unternehmen: Eine literaturbasierte und empirische Studie von Effekten und Barrieren
Erik Kolek 1706

Toward a Focus Area Maturity Model for Digitalization - A Set Theoretic Development Approach
Katja Bley 1718

Approaching Digitalization with Business Process Management
Florian Imgrund, Marcus Fischer, Christian Janiesch, Axel Winkelmann 1725

ISIS12-Hack: Mitarbeiter sensibilisieren statt informieren
Kristin Weber, Andreas Schütz 1737

Serviceplattformen als Digitalisierungsstrategie – Entwicklung und Anwendung eines Anforderungskatalogs für den Maschinen- und Anlagenbau
Friedemann Kammler, Florian Remark, Oliver Thomas 1749

IT-Sicherheit für Kritische Infrastrukturen: Infrastrukturmanagement, Informationsmanagement und Risikomanagement

Teilkonferenzleitung

Benedikt Buchner
Albrecht Fritsche
Andreas Harner
Dennis-Kenji Kipker
Ulrike Lechner
Kathrin Möslein
Steffi Rudel

Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes

Clemens Sauerwein[1], Christian Sillaber[1], and Ruth Breu[1]

[1] University of Innsbruck, Department of Computer Science, Innsbruck, Austria
{clemens.sauerwein,christian.sillaber,ruth.breu}@uibk.ac.at

Abstract. Cyber threat intelligence is obtained in an unstructured and ad-hoc manner from publicly available cyber security information sources such as security expert blogs or mailing lists. Although these information sources are used by employees as input for critical information security and risk management processes, they often have not received any formal IT department approval or assessment which raises issues in analogy to phenomenon of shadow IT. Little is known about the actual value these cyber security information sources provide and how they complement information security and risk management processes. In this paper, we conduct a structured, in-depth analysis of shadow cyber threat intelligence and investigate how it is used in organizations. Our study revealed that many heterogeneous and overlapping cyber security information sources serve as input for information security and risk management processes and that the obtained shadow threat intelligence is shared internally in a largely unstructured and informal manner.

Keywords: Threat Intelligence Sharing, Shadow IT, Information Security Risk Management

1 Introduction

Recent high profile security incidents have shown that the spectrum of possible attacks steadily increases and that the time frame for organizations to react shrinks constantly [1]. The protection of critical infrastructures, active vulnerability management, a fast internal dissemination of cyber security information and security awareness trainings have become key activities in organizations [2, 3]. To augment well established controls, a trend to systematically exchange cyber security information between organizations and with academia can be observed [4-6].

To aid vulnerability management and to mitigate incidents, security experts, security operatives and risk managers increasingly rely on a variety of information sources to augment their daily activities [7]. A multitude of different sources can be found, ranging from publicly available cyber security information sources (e.g. vulnerability databases) to inter-organizational cyber threat intelligence sharing platforms [8].

Research is mostly focused on how to build cyber threat intelligence sharing platforms and how to best structure the exchange of intelligence [9-13]. In this context, cyber threat intelligence describes any security related artifact that security and risk managers rely on during their information security and risk management processes.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Apart from these cyber threat intelligence sharing platforms, security stakeholders rely to a large extent on publicly available sources. In contrast to cyber threat intelligence sharing platforms, this information is available in unstructured form and mostly used by employees inside the organizational ecosystem without any formal approval or systematic support from the IT department. Hence, the usage of these public available sources resembles in its nature the phenomenon of shadow IT [14, 15]. Accordingly, we introduce the concept of shadow cyber threat intelligence. *Shadow cyber threat intelligence can be defined as cyber threat intelligence obtained from cyber security information sources which are used inside an organization without explicit organizational approval or support.* Previous research showed that shadow IT introduces several risks [14, 16]. Therefore, a comprehensive understanding of the unexplored phenomena of shadow cyber threat intelligence and its implications for research and practice are warranted.

However, to which extent stakeholders utilize shadow cyber threat intelligence remains unclear as no scientific analysis of its use in information security and risk management processes exists and to the best of our knowledge, no empirical research has been conducted yet. To address this gap, we seek to answer the following research questions: (1) *Which shadow cyber threat intelligence sources can be identified in practice?* (2) *What are their characteristics and how is shadow cyber threat intelligence used in information security and risk management processes?*

The goal of our research is therefore to provide a comprehensive analysis of shadow cyber threat intelligence and its use in information security and risk management processes. To achieve this goal, we conducted a case study with 11 experts in the field. We identified 30 (shadow) cyber threat intelligence sources used by security experts to obtain timely and relevant cyber security information and mapped them to organizational information security and risk management processes. We observed that shadow cyber threat intelligence is used as input across all information security and risk management process, except processes related to the security mission (i.e. the most high level security management process). Finally, we discuss its use and how it is distributed to other stakeholders within the organization.

The remainder of this paper is structured as follows: Section 2 discusses related work. Section 3 outlines the underlying research methodology carried out. Section 4 outlines the key findings. Section 5 discusses the results and their implications for research. Section 6 discusses limitations of the research at hand. Finally, Section 7 concludes the paper and provides outlook on future work.

2 Related Work

The phenomena of employees using hardware, software or other solutions inside an organizational ecosystem which have not been formally approved by the IT department and bypassing official solutions has been described in research as shadow IT [17]. In this context, Silic and Back conducted a study to identify the types, usage, values, and risks of shadow IT used in organizations [14]. Several studies have shown that shadow

IT is some sort of insider threat where an employee uses (mostly in good faith) non-approved IT, violating company policies [15, 18].
Since these public cyber security information sources provide an enormous amount of information in a (mostly) unstructured manner, the identification and extraction of valuable cyber threat intelligence is challenging and might even hamper an effective security and risk management process. While researchers primarily focus on the extraction of cyber threat intelligence from social media platforms (e.g. Twitter) [19, 20], limited attention has been paid to other information sources, such as mailing lists, newspapers or security experts' blogs.
Previous research in the field of information security investigated the phenomenon of shadow security, where conscious employees create a more fitting alternative to the policies and mechanisms created by the organization's official information security team [21]. In this context, Kirlappos et. al showed that shadow security should not be treated as problem but as an opportunity to identify gaps in current security policies from which security managers can learn [22]. The research on shadow security focuses on non-compliant behavior to policies and security mechanisms and mostly omits security intelligence artifacts.
To the best of our knowledge, no prior research has been conducted on the nature and use of shadow threat intelligence sources in the context of information security and risk management processes or related areas.

3 Research Methodology

We conducted a case study to investigate the phenomenon of shadow cyber threat intelligence and its use in practice. The case study combines different methodological approaches to improve the resulting quality: (1) We conducted an exploratory survey [23] where the participants were asked to fill out a questionnaire in order to identify shadow cyber threat intelligence sources. They were also asked to identify their use within their organization's processes according to the participants' experience and observations. (2) The participants were asked to associate the identified cyber threat intelligence sources to information security and risk management activities. Finally, (3) we conducted a focus group discussion [23] to discuss the survey results, clarify participants' statements and analyze the participants' mapping of cyber threat intelligence sources to information security and risk management processes. The research was carried out in June 2016 at a neutral premise in a German-speaking country.

3.1 Participants of the Case Study

Table [1] gives an overview of the 11 participants of the case study, their organizational roles, type and size of organization.

Table 1. Overview of study participants

ID	*Organizational Role*	*Type of Org.*	*# of Employees*
1	Head of SOC	Finance	> 1000
2	Security Analyst	Insurance	> 1000
3	CISO	Finance	> 1000
4	Security Analyst	Production	> 1000
5	Security Analyst	Government	> 1000
6	Risk Manager	Finance	> 1000
7	Security Analyst	IT	150 -1000
8	Security Analyst	Production	> 1000
9	Incident Response Team	Finance	> 1000
10	Did not disclose	-	-
11	Did not disclose	-	-

Two of the participants decided to not disclose any information. The majority of participants work directly in their security operations center (e.g. as a security analyst, incident response team member) while only three participants are members of the managerial level (e.g. chief information security officer). Moreover, the composition of branches of industry represents a mixture of finance, production and information technology. While all companies operate globally, one of them is a medium- (150-1000 employees) and eight of them are large-sized organizations with more than 1000 employees each.

3.2 Exploratory Survey

The first part of our case study involved an exploratory survey which was used to identify the most important sources of shadow threat intelligence [23]. A survey was chosen as it is a valuable tool to investigate a technique or process (i.e. use of shadow cyber threat intelligence) in real-world settings [24].

For the exploratory survey, the participants (see Table 1) were asked to answer a questionnaire about the three most relevant (publicly available) cyber threat intelligence sources in use or they consider for use in their organization. In doing so, they had to specify the following for each identified information source: (i) Name of the cyber threat intelligence source, (ii) type of source, (iii) description of provided cyber threat intelligence, (iv) how often they access the information source, (v) how often obtained information had led to actionable events in their respective organization, (vi) how they had had shared information or key findings with colleagues and (vii) with whom from their organization they had shared the obtained information.

3.3 Mapping Session

Based on the questionnaire results, we generated a list of the identified threat intelligence sources and asked the participants in a subsequent mapping study to map

each of them to an information security and risk management process, based on [25]. The process model, as depicted in Figure 1 (center), was used for the mapping session, consisted of the following four sub-processes: (1) Definition of security mission, (2) risk management (including threat analysis and vulnerability analysis), (3) implementation of security architecture, and (4) intuition. The information security and risk management process was displayed on a blackboard during the mapping session and explained to the participants in order to reduce uncertainties. Participants received index cards with the cyber threat intelligence sources identified in the previous session and were asked to pin the index cards to the respective security process where it serves as input.

3.4 Focus Group Discussion

Finally, we conducted a focus group discussion where we discussed the identified cyber threat intelligence sources, their nature, how they are accessed and their mapping to information security and risk management processes. This focus group discussion was held at a neutral premise and lasted roughly two hours. In order to minimize potential limitations, we followed the guidelines described in [26]. The whole focus group discussion was audio recorded. After the workshops, qualitative summaries were produced from the recordings [27] in order to derive findings relevant to our research questions [28].

4 Results

In this section, the key findings from the analysis of the case study are presented.

4.1 Shadow Cyber Threat Intelligence Sources Used in Organizations

Our exploratory survey identified 30 cyber threat intelligence sources. This include 25 shadow cyber threat intelligence sources that are used in practice and 5 formally approved and managed non-shadow sources. This low overall number can be traced back to the fact that we asked the participants to state only the three most important cyber threat intelligence sources they either use or had considered at their organization. The majority of identified shadow cyber threat intelligence sources are mailing lists (34%). 15% are vulnerability databases, 12 % vendor advisories, 6% social media streams, 6% face-to-face meetings, 6% blogs and 6% are other sources (e.g. whitepapers, reports). The remaining 12% are cyber threat intelligence sharing platforms. Study participants stated that these platforms have been officially approved by their respective IT departments and organizations mainly rely on them to obtain indicators of compromise (e.g. malicious IP addresses).
The identified mailing lists mainly focus on cyber security news including news about vulnerabilities, potential exploits, patching information, discussions of cyber security experts on hot topics and indicators of compromise.

The identified vulnerability databases are all using the conventional Common Vulnerabilities and Exposure (CVE) naming schema which standardizes the description of information security vulnerability names and enables the tracing of vulnerabilities over their lifecycle . Moreover, these databases provide CVE dictionaries augmented with additional information, descriptions, corresponding vulnerability severity scores (e.g. Common Vulnerability Scoring System) and search engine functionalities.
Four study participants stated that they visit vendor websites on a regularly basis in order to stay informed about vendor specific advisories. According to them, these advisories contain information about vulnerabilities and patches.
Our study participants frequently rely on social media streams, blogs and face-to-face meetings. In doing so, they exchange and discuss emerging topics in cyber security and share their "cyber war stories" (one respondent).
The focus group discussion showed that there is often no systematic process in place to discuss and access new cyber threat intelligence sources. The needed information is obtained "ad-hoc" through unstructured Google searches or face-to face meetings. In addition, four participants stated that new information sources are found by members of the security operations center, "... if they have time to look for them". Every participant identifies their own information sources without any official approval and coordination with other team members. Consequently, shadow cyber threat intelligence sources remain hidden from other team members and they are used without traces.

4.2 Motivation for the Use of Shadow Threat Intelligence Sources

According to the interviewees, one of the main motivations for using shadow cyber threat intelligence is the timely acquisition of information to stay up-to-date about emerging topics on cyber security. Our case study showed that security experts in organizations primarily focus on the procurement of information regarding new emerging vulnerabilities, indicators of compromise and available patches. In this context, it is noteworthy that the study participants scarcely rely on information regarding threat actors or countermeasures apart from patching.
According to [29], the data quality dimension of timeliness plays an important role for cyber threat intelligence sharing in general as outdated cyber threat intelligence loses its relevance and value quickly. We investigated how frequently shadow cyber threat intelligence sources are accessed within organizations: Almost half of the (shadow) cyber threat intelligence sources are accessed on a daily basis (40%), or instantaneous (20%). 17% of the identified sources are accessed weekly, 7% are monthly, 3% quarterly, 3% are biyearly, 3% yearly and the remaining 7% were not classified.
In order to get a better understanding of how relevant and useful the obtained shadow cyber threat intelligence is, we asked the participants to quantify how often obtained information led to actionable events. In 56% of the self-reported cases, cyber threat intelligence always, in 27% sometimes, and in 7% rarely led to actionable events. Merely in 7% of the cases shadow cyber threat intelligence never led to actions and the remaining 3% were not classified by the interviewees.

4.3 Organizations‘ Internal Distribution of Shadow Cyber Threat Intelligence

After the shadow cyber threat intelligence source is accessed and valuable information is extracted, the next step is to internally disseminate it. It might provide valuable and actionable information to other stakeholders and allows them to put countermeasures in place and prevents that two or more persons within an organization act on overlapping intelligence, which is one of the risks of shadow IT [14].
Our exploratory survey showed that 45% of obtained cyber threat intelligence are distributed via email, 17% via ticket systems, 13% via face-to-face meetings, 11% via forums or chats, 7% via cyber threat intelligence sharing platforms and 7% via security incident event management systems. This result is surprising as it can be expected that a cyber threat intelligence sharing platform would be the first choice to internally distribute cyber threat intelligence. We can conclude that the majority of cyber threat intelligence is distributed over a plethora of unstructured, manual and informal information channels (e.g. face-to-face, forums).
The obtained shadow cyber threat intelligence is mainly shared with cyber security professionals (e.g. security analysts) or the whole security operations team. In 52% of the cases, obtained intelligence is shared with the members of the security operations center, in 11% of the cases with security analysts, in 8% of the cases with the IT service department, in 7% of the cases with the incident response team, in 7% of the cases with the IT forensic department in 2% of the cases with the project management and in 2% of the cases with the IT infrastructure department.

4.4 Shadow Cyber Threat Intelligence as Input for Information Security and Risk Management Processes

After the information is obtained by an organization’s stakeholder, the information serves as input for information security and risk management processes. Shadow cyber threat intelligence sources primarily impact information security risk management processes (60% of the identified sources). In this context, shadow cyber threat intelligence is consulted during vulnerability (30%) and threat analysis (30%) processes in an ad-hoc manner without following any formal process. 27% of the identified sources are used for the implementation of a security architecture (e.g. developing security processes or implementing countermeasures). The remaining 13% of sources are used to support intuitive security management activities. None of the identified cyber security information sources serve as input to the definition of the security mission.

5 Discussion of Results

Figure [1] summarizes the results of our case study. It maps the identified shadow cyber threat intelligence sources to information security and risk management processes and shows how their outputs are internally distributed with responsible stakeholder groups.

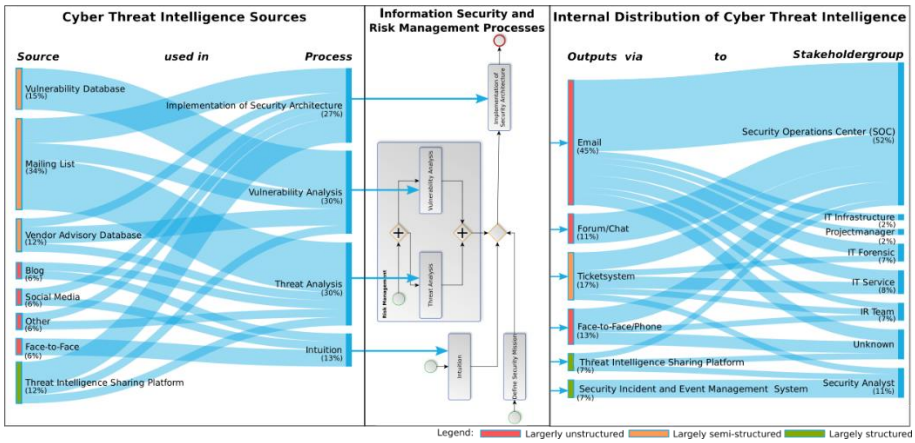


Figure 1. Overview of study results: Mapping of (shadow) cyber threat intelligence sources to information security and risk management processes (based on [25]) and an organization's internal distribution of the outputs

As discussed in Section 4, and depicted in Figure [1], mailing lists (34%), vulnerability databases (15%) and vendor advisories (12%) form the majority of shadow cyber threat intelligence sources accessed in practice. A closer analysis of the types of information obtained from these sources showed that diverse information on different abstraction levels are used. In this context, the heterogeneity of the obtained information ranges from technical indicators of compromise (e.g. hash values, IP addresses, domain names), to informal discussions between security experts about new emerging vulnerabilities or tactics, techniques and procedures carried out by threat actors. Moreover, shadow cyber threat intelligence is distributed over different channels (e.g. social media, mailing lists). Different vocabularies are used, and content is available in a mostly unstructured form.

Consequently, the automatic processing of shadow cyber threat intelligence is infeasible, which increases the complexity of the collection and processing of the obtained information as most steps have to be conducted manually. This leads to the observation that mostly the low hanging fruits, such as IP addresses, hash values of suspicious files, domain names or CVEs are used as input for information security and risk management processes. Moreover, this has been confirmed by the majority of study participants in so far as they stated, that they are mainly interested in indicators of compromise as they don't have the resources, time and software solutions required to analyze more complex cyber threat intelligence.

Our case study showed that shadow cyber threat intelligence serves as input for information security and risk management processes in organizations and represents an additional information source in addition to traditional ones, such as log files or penetration testing results. Moreover, the participants stated that one of the core motivations to rely on shared cyber threat intelligence is the timely acquisition and processing of security related information. Moreover, the case study showed that shadow cyber threat intelligence sources are accessed in 60% of the cases on a daily

(including instantaneous) basis and more than 50% of used sources provided intelligence that lead to actionable events. These facts clarify the value and importance of shadow cyber threat intelligence for organizations.

Our research confirmed that the reliance on shadow threat intelligence can undermine the officially approved information security and risk management process. As a result, intelligence available to decision makers might be incomplete, duplicate already existing information, or faulty which would lead to undesired effects, e.g. information security experts might be fooled and miss potential threats to their information systems. In addition, unapproved shadow cyber threat intelligence sources might become more important than official cyber security information sources in organizations, which might constitute a single point of failure, hidden to senior cyber security stakeholders. As the majority of shadow threat intelligence is obtained and distributed through conventional information channels, as depicted in Figure 1, it is hard to implement controls or take actions to avoid the usage of shadow cyber threat intelligence.

Our research revealed that shadow cyber threat intelligence endangers structured organizational information flows. The majority of study participants mentioned that everybody relies on their own information sources and collects the needed cyber threat intelligence without consulting other employees. Unfortunately, this informal and inconsistent approach might be traced back to a lack of a formal workflow to collect and distribute cyber threat intelligence in organizations. Accordingly, this might lead to wasted resources as the information must be distributed and reconsolidated by other employees. This loss of efficiency is problematic as time plays a crucial role in information security and risk management processes. For example, according to one participant, the earlier an identified threat is communicated to responsible persons within the security operations center, the sooner countermeasures can be implemented. A closer look on how the study participants share the obtained shadow cyber threat intelligence in their organization, showed that they primarily rely on email or face-to-face exchanges. This might lead to information loss and a lack of traceability. The focus group discussion showed that a more formal approach such as using a threat intelligence sharing platform could be a suitable solution to address these problems. However, our investigations showed that only 7% of the organizations participating in our study use a cyber threat intelligence sharing platform to distribute the obtained shadow cyber threat intelligence.

Finally, our case study showed that the majority (57%) of shadow cyber threat intelligence sources serve as input for risk management processes. This is not surprising as processes such as vulnerability analysis or threat analysis primarily focus on the collection of recent information regarding vulnerabilities, threats and threat agents. Moreover, the interviewees stated that the obtained cyber threat intelligence triggers proactive information security and risk management processes. For example, six participants stated that they evaluate if their system is at risk through checking the internal documentation, architecture and log files against the received cyber threat intelligence.

6 Limitations

The research at hand might be limited by certain threats to validity that have to be acknowledged. In order to minimize them, we attempt to triangulate our findings through an exploratory survey followed by a two-stage focus group discussion with information security experts. Limitations that have to be acknowledged and accounted for are: (i) limited generalizability of the results, (ii) selection bias when selecting the participants of the case study (including the exploratory survey, mapping session and focus group discussion), (iii) influences of moderators during focus group discussions, (iv) off-topic discussions, (v) language barriers, (vi) incomplete or biased list of identified shadow cyber threat intelligence sources, (vii) biased mapping of shadow threat intelligence sources to information security and risk management processes and (viii) biased description of shadow cyber threat intelligence sources.
Limitation (i) results from a small sample size of participants and identified (shadow) cyber threat intelligence sources. This was consciously accepted as the focus of the case study was to qualitatively investigate the phenomenon of shadow cyber threat intelligence. Limitations (ii) to (v) primarily result from conducting an exploratory survey and focus group discussion research [30]. They might be counteracted by following the suggestions of Vogt et al. [26]. By following them, (ii) participants of the case study were asked to participate voluntarily at a neutral premise, (iii) moderators tried to keep in the background as much as possible, (iv) moderators refocused the discussion as soon as it got off track and eliminated any uncertainties by answering questions raised, and (v) the exploratory survey and focus group discussions were held in English as a common language. To counteract (vi), the participants were asked to fill out a questionnaire for the three most relevant shadow cyber threat intelligence sources without exchange with other participants. Secondly, to overcome (vii), the participants had to map the identified intelligence sources to information security and risk management processes (based on [25]) on their own without any discussion. Finally, to counteract limitation (vii), the participants had to describe the nature of their identified cyber threat intelligence sources, which served as input to guide the focus group discussion.

7 Conclusion

In this paper, we investigate the phenomenon of shadow cyber threat intelligence, i.e. the unstructured and unapproved use of cyber threat intelligence and its dissemination in organization in a case study with 11 security experts from medium to large-sized organizations. The case study showed that a multitude of different shadow cyber threat intelligence sources are used as input for information security and risk management processes. Moreover, we figured out that the use of shadow cyber threat intelligence might bypass security and risk management review processes or formal approval structures (or at least reduce the amount of information available in tangible form). This goes hand-in-hand with a loss of knowledge as shadow cyber threat intelligence could be lost in email message chains, undocumented face-to-face meetings or social media

messages. During audits or forensic postmortem analysis, attempting to reconstruct whether security and risk management processes have been implemented properly, the hard-to-trace nature of shadow cyber threat intelligence could lead to a skewed or incomplete picture of the process. Future work will focus on empirical research on the phenomenon of shadow cyber threat intelligence, associated risks and how to extract its value in a way compatible with organizational requirements.

References

1. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80, 973-993 (2014)
2. Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: A literature review. International Journal of Information Management 36, 215-225 (2016)
3. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. Mis Quarterly 757-778 (2010)
4. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. Information Management & Computer Security 22, 410-430 (2014)
5. Fransen, F., Smulders, A., Kerkdijk, R.: Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik 132, 106-112 (2015)
6. Skopik, F., Settanni, G., Fiedler, R.: A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security 60, 154-176 (2016)
7. Shackleford, D.: Who's Using Cyberthreat Intelligence and How? SANS Institute. Retrieved February 23, 2016 (2015)
8. Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In: Proccedings of the Wirtschaftsinformatik (WI) (2017)
9. Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1-16. IEEE, (2013)
10. Serrano, O., Dandurand, L., Brown, S.: On the design of a cyber security data sharing system. In: Proceedings of the 1st ACM Workshop on Information Sharing & Collaborative Security, pp. 61-69. ACM, (2014)
11. Brown, S., Gommers, J., Serrano, O.: From cyber security information sharing to threat management. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, pp. 43-49. ACM, (2015)
12. Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C.: Guide to cyber threat information sharing. NIST Special Publication 800, 150 (2016)
13. Kampanakis, P.: Security automation and threat information-sharing options. IEEE Security & Privacy 12, 42-51 (2014)
14. Silic, M., Back, A.: Shadow IT–A view from behind the curtain. Computers & Security 45, 274-283 (2014)

15. György, A.A.B., Cleven, A., Uebernickel, F., Brenner, W.: Exploring the shadows: IT governance approaches to user-driven innovation. In: Proccedings of the European Conference on Information Systems (ECIS) (2012)
16. Strong, D.M., Volkoff, O.: A roadmap for enterprise system implementation. Computer 37, 22-29 (2004)
17. Behrens, S., Sedera, W.: Why do shadow systems exist after an ERP implementation? Lessons from a case study. In: Proceedings of the Pacific Asia Confernece on Information Systems (PACIS) (2004)
18. Warkentin, M., Willison, R.: Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems 18, 101-105 (2009)
19. Cui, B., Moskal, S., Du, H., Yang, S.J.: Who shall we follow in twitter for cyber vulnerability? In: SBP, pp. 394-402. Springer, (2013)
20. Sabottke, C., Suciu, O., Dumitras, T.: Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits. In: USENIX Security Symposium, pp. 1041-1056. (2015)
21. Kirlappos, I., Parkin, S., Sasse, M.A.: Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. In: (Proceedings) Workshop on Usable Security (2014)
22. Kirlappos, I., Parkin, S., Sasse, M.A.: Shadow security as a tool for the learning organization. ACM SIGCAS Computers and Society 45, 29-37 (2015)
23. Babbie, E.R.: Survey research methods. Wadsworth (1973)
24. Pfleeger, S.L.: Experimental design and analysis in software engineering. Annals of Software Engineering 1, 219-253 (1995)
25. Pettigrew, J., Ryan, J.: Making successful security decisions: a qualitative evaluation. IEEE Security & Privacy 10, 60-68 (2012)
26. Vogt, D.S., King, D.W., King, L.A.: Focus groups in psychological assessment: enhancing content validity by consulting members of the target population. Psychological assessment 16, 231 (2004)
27. Mayring, P., Gläser-Zikuda, M.: Die Praxis der Qualitativen Inhaltsanalyse. Beltz Weinheim (2008)
28. Campbell, J.L., Quincy, C., Osserman, J., Pedersen, O.K.: Coding in-depth semistructured interviews: Problems of unitization and intercoder reliability and agreement. Sociological Methods & Research 42, 294-320 (2013)
29. Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Data quality challenges and future research directions in threat intelligence sharing practice. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 65-70. ACM, (2016)
30. Louise Barriball, K., While, A.: Collecting Data using a semi-structured interview: a discussion paper. Journal of advanced nursing 19, 328-335 (1994)

Cloud Computing Adoption in Critical Infrastructures - Status Quo and Elements of a Research Agenda

Michael Adelmeyer[1], and Frank Teuteberg[1]

[1] Osnabrück University, Accounting and Information Systems, Osnabrück, Germany
{michael.adelmeyer,frank.teuteberg}@uni-osnabrueck.de

Abstract. Critical infrastructures, as the backbone of societal life, become increasingly dependent on IT. Thus, in order to ensure security and resilience, they face strict IT legislations and requirements. However, due to efficiency benefits, such as cost savings and increased flexibility, critical infrastructures increasingly adopt innovative IT models like cloud computing. This is despite the fact that migrating processes or systems into a cloud involves major risks for sensitive IT landscapes, since the control over data and security measures is delegated to cloud providers. In order to identify the current status quo of cloud computing in critical infrastructures, we conduct a systematic literature review, an analysis of cloud-based outsourcings of German critical infrastructures and expert interviews. Our findings provide an overview and a research agenda of cloud usage in critical sectors, which are helpful for critical infrastructure and cloud providers alike in order to adopt or manage cloud solutions.

Keywords: Cloud Computing, Critical Infrastructures, IT Security, IT Risks

1 Introduction

Critical infrastructures (CIs) take over a crucial public role, as they provide vital utilities. The German IT Security Law defines CIs as facilities, installations or parts thereof belonging to the sectors of energy, health, water, nutrition, information technology and telecommunications, transport and traffic as well as finance and insurance, which are of great importance for the functioning of the community because their failure or impairment would result in significant supply shortages or threats to public safety. As IT systems are an essential element of reliable service provisioning of CIs [1], CIs face stringent measures and legislations regarding security, privacy and resilience of their IT landscape [2, 3]. Due to the specific risks and requirements, CIs often host their own IT infrastructure or at most share resources with organizations with similar demands [4, 5]. However, due to manifold benefits, such as scalability, flexibility and cost reduction [6], CIs increasingly migrate IT services to cloud environments [2, 4, 7, 8]. Cloud computing is an operational model that provides on-demand access to a shared pool of resources, e.g. applications or hardware [6]. On the one hand, CIs are able to improve their resilience and availability with cloud solutions [8], recover faster in case of a failure [5] or benefit

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

from dynamic resource allocation and thus manage imponderable load peaks [9]. On the other hand, CIs face additional risks when moving IT systems or processes into a cloud [5, 10], such as the loss of control over security and privacy measures, data location, authentication and access control, third-party attacks or interferences, legislative issues or the violation of service level agreements (SLAs) [5]. The risks of deploying services into a cloud are difficult to assess, since cloud environments are opaque and often problematic to monitor [2]. This is especially challenging as CIs and therefore their cloud providers have to meet complex security and resilience requirements and demands of various stakeholders [10, 11]. Although the requirements are strict, existing cloud services fail to take proper account of these issues [2]. The pooling of computing resources in clouds even intensifies structural interdependencies and network risks between CIs and their cloud providers [12].

The IT security requirements of CIs and industrial stakeholders differ substantially and there are major differences even between the individual CI sectors [4]. Further, the risks vary depending on the selected cloud service and deployment model [13]. Existing literature mainly focuses on risks and corresponding standards but lacks an overview of the status quo of cloud usage in CIs. With the increasing adoption of cloud solutions in CIs, there is an urgent need to understand the differences regarding cloud service and deployment models as well as the involved sectors. Based on a systematic literature review, an analysis of outsourcings of German CI providers as well as expert interviews the status quo and a research agenda on cloud adoption in CIs are presented. Thereby, the focus is on systems, processes and functions, cloud service and deployment models, sectors as well as risks arising from cloud usage in CIs. The findings reveal that cloud computing is predominantly adopted in 'non-critical' areas of CIs. However, the use of public cloud or Software as a Service models is increasing. Both cloud providers and CIs need to understand the corresponding challenges, issues and risks in order to successfully adopt and manage cloud solutions. In this context, the research agenda determines future steps for science and practice alike, e.g. regarding risk management.

2 Research Approach

2.1 Literature Analysis

In order to provide an overview of the current state of research regarding the adoption of cloud computing solutions by CI operators, we conducted a systematic literature analysis following the approach of vom Brocke et al. (2009) [14]. The analysis of existing literature is an essential part of scientific work with the objective to elaborate the state of research in a certain field, to reveal possible knowledge gaps and motivate researchers to close these by identifying new research areas and directions. To cover the interdisciplinarity of the topic, we searched the databases AIS electronic library, EBSCOhost, ScienceDirect, SpringerLink, AIS Web of Knowledge and Google Scholar. For the queries, we used the keywords "critical infrastructure*" OR "critical national infrastructure*" OR "critical asset*" OR "critical system*" OR "critic*"

AND “cloud comput*” OR “cloud*” OR “outsourc*” and their German equivalents. We identified relevant publications by inspecting the titles, keywords and abstracts, which resulted in a total of 18 articles. Based on this result set, we conducted a forward and backward search, leading to seven further publications[1]. The majority of the literature found originates from conference proceedings. In order to identify the status quo, the publications were systematically examined using category building. As selection criteria, the different cloud service and deployment models, sector-specifics and risks were chosen. The results of the analysis serve as the basis for the status quo of cloud usage in CIs (cf. section 3) and the research agenda (cf. section 4).

2.2 Practical Analysis

To determine the current status quo in practice, we conducted an analysis of present outsourcings of German CIs to cloud services. In our search for CI providers and given the lack of appropriate public listings, we concentrated on the members of the working group UP KRITIS, a public-private cooperation between CI operators, their unions and governmental authorities. But here again no public list of the UP KRITIS members was available. Therefore, we examined the so-called “logo cloud”[2], in which the logos of the involved organizations can be registered upon request, in order to identify and categorize these CI operators. Since a distinct allocation of the companies to the aforementioned CI sectors of the German IT Security Law was not always possible, “mixed sectors” were defined. In this step, non-CI-providers like unions, governmental authorities and other stakeholders (e.g. cloud providers or certification authorities) were omitted, which led to the identification of 80 CIs[1].

In a next step, the identified CI operators were examined regarding the use of cloud technology. For this purpose, we considered business reports – as far as publicly available – as well as further information on cloud usage of the respective organizations from the internet, mainly from corporate websites. Subsequently, the previously determined sources for the adoption of cloud technologies of CIs were analyzed in detail. In this analysis, the focus was put on the use of cloud service [Infrastructure as a Service (IaaS), Platform as a Service (PaaS) Software as a Service (SaaS)] and deployment models (public, private, hybrid and community). In addition, the respective processes, systems or business functions, which are outsourced to or substituted by cloud technologies, were determined.

2.3 Expert Interviews

The results are further complemented by four expert interviews. Due to the relevance and novelty of an investigated subject, expert interviews can reveal information that is not yet available in scientific literature. The overall approach of the expert interviews can be summarized as follows [15]: on the basis of the literature analysis, a semi-

[1] A full overview of the identified publications, the examined critical infrastructure providers and the corresponding findings can be obtained at http://bit.ly/MKWI2018

[2] http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Logo_Cloud.pdf, *23.11.2017*

structured interview guide was developed containing eight interview questions that target the current use of cloud services, potentials, risks and open issues. After a pretest, the final interviews were conducted and qualitatively analyzed. The experts were employees of a CI and a consulting company (cf. Table 1).

Table 1. Experts Interviewed

ID	*Sector*	*Position/Function*
1	Transport & Traffic	Business Intelligence Architect
2	Transport & Traffic	Project Management
3	Transport & Traffic	Team Lead Application Development
4	Consulting	Senior Consultant, Security Analyst

3 Status Quo of Cloud Usage in Critical Infrastructures

3.1 Overview and Related Work

Although a plenitude of publications addresses cloud usage in specific industry sectors (e.g. finance [16]), only few articles approach the cloud domain from a CI perspective. Of the 25 publications identified the majority dates to the years 2013-2015 (19). A large part of the publications (8) treats security issues and risks related to the adoption of cloud services in critical infrastructures. For example, Younis et al. (2013) and Anastacio et al. (2013) provide an overview of risks and security measures for the deployment of CI components in a cloud [11, 17]. However, these publications often focus on general risks associated with cloud computing. A further major focus lies on regulatory aspects (7). In this context, Adelmeyer et al. (2017) illustrate IT risk management measures regarding the German IT security law [13]. Chochliouros et al. (2015), Paudel et al. (2014), Hudic et al. (2014) and Wagner et al. (2015) highlight various regulatory requirements and standards or guidelines for CIs, such as ISO 27001 [4, 5, 18, 19]. In addition, Wagner et al. (2015) point out that some security aspects are only inadequately addressed by existing standards and guidelines.

First major efforts to overcome the issues of cloud usage in CIs were undertaken by the EU-funded projects "SECCRIT" ("SEcure Cloud computing for CRitical infrastructure IT") with the objective to analyze and evaluate cloud related security risks for CIs [2–5, 8, 10, 20] and "CI2C" ("Critical Infrastructures and Cloud Computing"). Further, the European Network and Information Security Agency (ENISA) published a report that addresses cloud computing from a critical infrastructure information protection perspective with a focus on cloud scenarios and relevant threats [21]. However, the body of knowledge lacks a comprehensive current overview of the field. Thus, we analyzed the identified literature with regard to specifics concerning service and deployment models, functions, CI sectors and risks. Furthermore, as no empirical study on the use of cloud computing services in CIs could be identified, we conducted a practical analysis. At 18 of the 80 investigated CI operators, which approximate 22.5%, we found information on the use of cloud services. In contrast to the predictions of the ENISA, that states that around 80% of all

organizations will be dependent on cloud computing by today [21], the figure is relatively low. However, given the fact that we had to rely on publicly available information only, we assume the actual figure to be higher. In general, little information on the adoption of cloud technology was found in the business and annual reports, so that we had to rely on external sources, such as company websites. It was further found that many CIs simultaneously act as cloud operators and providers. In the following sections, the results of the literature and practical analysis as well as the expert interviews are presented. Table 2 summarizes the aggregated findings of the practical analysis. In total, we identified 23 cloud adoption cases at 18 CIs. However, not for every case we were able to distinctly identify a respective categorization.

Table 2. Aggregated Results of the Practical Analysis

Focus	*Cloud Adoption Cases (Quantity of Occurrence)*							
Systems/ Processes	Sales/ Distribution (7)	Data Center Operations (6)	Finance/ HRM (2)	E-Mail (2)	Software (1)	Unknown/ Others (5)		
Service Models	Software as a Service (13)	Infrastructure as a Service (5)	Platform as a Service (1)	Unknown/ Others (4)				
Deployment Models	Private Cloud (9)	Public Cloud (8)	Community Cloud (1)	Hybrid Cloud (0)	Unknown/ Others (5)			
Sectors	Energy (4)	Finance/ Insurance (4)	Energy/ Water (3)	Transport/ Traffic (3)	Water (2)	Nutri-tion (1)	IT & Telco (1)	

3.2 Systems, Processes and Functions

Regarding the systems, processes and functions of CIs that are outsourced to cloud services, only little information is available in the literature. In most cases, CIs are expected to replace 'non-critical' systems, processes or functions by cloud services [7]. In contrast to 'mission-critical' services, support systems and tertiary services can be provisioned via clouds more easily, especially when considering public cloud environments [22]. This finding coincides with the estimation of expert no. 4 that "the tendency for the adoption of cloud solutions in CIs is rising, but initially concentrates on non-critical areas". Thus, each CI has to individually evaluate every single migration to a cloud with a strong focus on security, availability and integrity [23]. However, with the increasing digitization, formerly isolated systems like Supervisory Control and Data Acquisition (SCADA) or industrial control systems that are widely used in CIs are moving to modern environments like clouds, which expose these systems to cloud-related threats [7, 23, 24]. The practical analysis revealed that sales/distribution (7 cases), including supply chain management, customer service, social media and invoice handling, followed by IT data center operations (6) are the most frequent areas for the adoption of cloud technology in CIs. However, information on outsourced systems, processes and functions is scarce (5 unknown/others), which demands for future research in this area. In summary, the analyses revealed that rather uncritical areas, e.g. sales/distribution, are major adoption areas for cloud technology in CIs.

3.3 Cloud Service Models

Depending on the deployment or service model of a cloud, the corresponding risks vary [13]. Thus, the different service models are associated with individual security requirements and threats [23, 25]. Following Diez and Silva (2011), the majority of CIs use SaaS or IaaS models for 'non-critical' business functions. Further, they state that SaaS offers the least control over the underlying cloud infrastructure, since this is fully delegated to the service provider [7]. As numerous SaaS providers rely on other cloud providers for fundamental resources such as PaaS or IaaS, the latter are seen as critical likewise [21]. The resulting interdependencies between organizations, service providers and users create network risks, as a failure of large cloud service providers would have a cascading effect on other CIs [19]. Thus, particularly IaaS and PaaS providers need to strengthen their resilience and security measures. The quantitative analysis of the service models used in practice revealed that SaaS is used most frequently (13), followed by IaaS (5) and PaaS (1). This distribution resembles the evaluation of the expert interviews. All four respondents indicated the frequent use of SaaS. In this context, especially public cloud SaaS solutions like Salesforce or Microsoft Office 365 (4 cases) are considered. Further, two experts pointed out adoptions of IaaS and one expert indicated a PaaS solution for test environments.

3.4 Cloud Deployment Models

As public clouds are difficult to monitor and control, prone to attacks, lack direct governance and have issues related to multi-tenancy and storage location [7], it is unlikely that CIs outsource core functions or services to public clouds [22]. Since in public and hybrid solutions the data is transferred to third parties, sufficient network and storage security measurements and assurances have to be implemented, to ensure the integrity and confidentiality of data outside of CIs' private IT landscapes [22]. In contrast, private clouds can be used for critical functions and systems that have to stay in-house. Private clouds grant full control over data management and security measures and thus allow for specific fail-safe or cluster mechanisms, which cannot be implemented in public solutions [7, 23, 25]. Further, private clouds can be used as a staged approach to a prospective shift to public environments [7]. However, the economies of scale and the elasticity and flexibility are lower. Since CIs, due to their specific risk exposures and requirements [4, 5], often host their own IT infrastructure or at most share resources with organizations with similar demands, community clouds seem to be an adequate solution [23]. As community clouds limit certain risks, e.g. related to multi-tenancy [7] or the prevention of external dependencies [26], they are suitable in case private clouds are too expensive and public clouds do not meet individual security demands. However, trust in other involved actors and organizations regarding data and environment security measures is crucial in such solutions [7]. Further, the protection of such CI community solutions against cyber-attacks is vital, since they constitute an attractive target for attackers [7, 23].

The investigation of the service and deployment models used in practice revealed that IaaS is most often implemented as a private cloud (4 cases) and SaaS solutions as

public (8) or private clouds (3). Considering all cloud deployments, private clouds were used most frequently (9), followed by public (8) and community clouds (1). Hybrid clouds were not identified. In this context, the cloud of the Deutsche Bahn was categorized as "others", as it is a virtual private cloud based on the open infrastructure of an external service provider that is protected by access restrictions. The experts stated that public clouds are used most frequently in combination with SaaS. Expert no. 4 outlined that it is "often a matter of price, since private clouds are more expensive". According to expert no. 2 there is a "need for combined and distributed architectures that enable the interaction of private and public clouds".

3.5 Sectors

IT environments of CIs are often heterogeneous, since they comprise various kinds of infrastructures and systems. Consequently, CIs have individual security requirements, even between the different sectors [11]. The majority of publications (17) does not provide any information or focus on specific sectors. Instead, only some unrepresentative examples for cloud adoption cases in various sectors are given (e.g. [11, 21]). Driven by the objective to provide more flexible services through the virtualization of their infrastructures, telecommunication operators were among the first to adopt cloud solutions [8, 23]. Also the energy sector is at the forefront of cloud adoption in CIs [11, 21, 25]. Especially in concerns of network simulations, highly flexible computing resources are needed. For example, renewable energy output is less predictable than conventional energy sources and thus demands for a flexible IT infrastructure [23]. Further examples for migrations to cloud computing environments are public sector institutions [7, 17, 21, 23] that use cloud services inter alia to implement e-government services or replace internal IT. The transport sector [2, 8, 21] adapts clouds for centralized service provisioning and traffic management via web-based interfaces. In the financial industry, where IT costs are estimated to represent around 15-20% of the banks' overall administrative expenses [16], the adoption of cloud solutions is promising. However, financial institutions are subject to strict regulations, e.g. regarding risk management and security. Thus, IT capacities for certain services have to be provided in-house in the medium and long term.

The major adopters of cloud solutions were found to be the energy as well as the finance/insurance sector with a total of four cases of application each, followed by energy/water (3), transport/traffic (3), water (2), telecommunications (1) and food (1). The finding that the energy sector is leading in cloud adoption corresponds to the estimation of expert no. 4 as well as the current study on cloud usage in Germany of KPMG [27]. Further, the expert states that the adoption is expanding but still "hampered by individual requirements of some organizations and sectors", e.g. the localization of services. However, as the majority of CIs identified was attributed to energy-related sectors (44) followed by information and telecommunication (14) and finance and insurance (5), the comparability is partially limited. The energy-related sectors consist to a large extent of municipal utilities, which only publish little information. Still, the relation of four out of five identified CIs from the finance/insurance sector that have adopted cloud solutions can be interpreted as high.

3.6 Risks

As outlined before, the risks resulting from a deployment of CI services and functionalities in cloud environments heavily depend on the selected cloud service and deployment model as well as the targeted business systems, processes and functions [13]. For example, in SaaS models, the security requirements and threats focus on the application level, whereas in PaaS and IaaS services virtualization aspects are rather critical [23]. Regarding the deployment models, outsourcing to public, community or hybrid clouds results in a loss of control and a dependency on the respective providers, in contrast to private solutions [18]. Thus, it is outside the scope of this article to provide a comprehensive overview of risks associated with cloud solutions. The latter can be found in control frameworks and standards like the ISO 27000 series or the CSA Cloud Controls Matrix. Further, Paudel et al. (2014) provide a list of security issues related to clouds [19]. The risk focus of CIs is put on IT security, privacy and resilience issues rather than on strategic or financial aspects, especially since CIs underlie stricter requirements [3]. Many risks result from common threats related to network and internet technology, and more rigorous precautions are needed when CI services are exposed in a cloud [22]. For CIs, the security and resilience risks as well as requirements associated to cloud usage are of central importance [2, 8, 18, 23]. For example, Mackay et al. (2015) provide an overview of CI requirements related to cloud usage and emphasize the importance of data security and integrity as well as availability. In this context, a further crucial point is the compliance with the various legal regulations that CIs underlie [22]. Thus, especially cloud-specific risks related to multi-tenancy, virtualization and the pooling of resources need to be evaluated in detail by CIs [8, 21]. At the same time, not all cloud-specific risks have a direct impact on the health, safety, security or economic well-being of citizens, for example a vendor lock-in [21]. Hence, the perspective of CIs on cloud risks differs compared to other enterprises. Another vitally important aspect, that was also expressed in all interviews, concerns the applicable privacy laws and jurisdiction over the data, as the location of data in clouds is often unknown [18].

There are also risks that arise regardless of the specific service model. This is the case with network dependencies and the consequent propagation of risks that result from the interaction of multiple CIs and clouds [7]. Further, cloud environments that run CI services become a more attractive target for attackers [8, 18]. Therefore, CIs need transparency over logical and physical dependencies of CIs and cloud providers [21]. Hence, CIs should conduct a detailed risk assessment and vulnerability analysis, which is followed by an effective risk monitoring and management [18].

4 Research Agenda

The analysis of the status quo of cloud computing in CIs revealed several research gaps, which mainly concern technical (T), jurisdictional (J), organizational (O) and contractual (C) issues. Therefore, Table 3 only illustrates an extract of potential topics for future research. In this context, it is possible to put the research focus on other areas, e.g. solely on technical IT security issues and related risks.

Table 3. Research Agenda for Cloud Usage in Critical Infrastructures

Gap	*No., Research Proposition/Issue [Reference] (Expert) {Practical Analysis}*
T	1. Analysis of interdependency risks of cloud and CI providers [7, 18, 21, 28] (1-4)
	2. Hybrid cloud frameworks and environments for CIs [7, 22, 23, 25] (2) {P}
	3. Secure data transfer to third parties over external networks [19, 22] (1, 2)
	4. Access controls that meet the security requirements of CIs [5, 8, 11, 19, 22, 23] (4)
	5. Deployment of critical business functions in (public) clouds [7, 22, 24] (4) {P}
J	1. Analysis of cloud-related requirements of national CI laws [13, 18, 21, 22] (1, 4)
	2. Legally compliant implementation of CI requirements at the provider [8, 29] (1, 2)
	3. Analysis of privacy issues particularly relevant for CIs [5, 8, 11, 18, 23] (1-4)
	4. Open security standards for cloud migration and deployment in CIs [4, 9, 19] (2)
	5. Legal transparency enforcement regarding data location and security [4, 8, 29] (2)
O	1. Development of flexible cloud risk management solutions for CIs [2, 11, 13, 18]
	2. Investigation of trust relationships between entities [5, 7, 8, 11, 19, 22] (1, 3)
	3. Cloud integration of security incidents reporting to authorities [5, 13, 18, 21] (2, 4)
	4. CI-relevant risk models for individual sectors and cloud deployments [2, 4, 18, 21]
C	1. Investigation of contractual relationships between CIs and cloud service providers, i.e. enhancement of SLAs or smart contract solutions [5, 8, 11, 22, 26, 29] (2, 4)
	2. Continuous assurance of legal security requirements [4, 5, 8, 11, 19, 20, 22] (1, 4)

The literature analysis unveiled that depending on the service and deployment model selected, the respective risks vary [13, 23, 25] (O4). In this context, hybrid cloud solutions combine the benefits of public and private clouds (T2). Although the risks for CI operators cannot completely be eliminated, they can at least be minimized. Thus, there is a need for a flexible risk management that allows for the consideration of individual circumstances and national legislations, especially for large and globally operating CIs (J1, O1). The adoption of cloud solutions by CIs results in a complex and opaque network of various actors and parties. Given the dependencies between cloud services and other actors risk assessments are often difficult [28]. Hence, the understanding of the involved actors, risks and dependencies is vital for sustainable business relationships of CIs and their cloud service providers to address the resulting technical and legal requirements [8] (T1). A further research topic is the area of trust, as trust is a central element in the outsourcing relationship between CIs and cloud providers [5, 8, 11, 19, 22]. This comes especially true when considering large and opaque public cloud services that rely on other cloud providers unknown to the direct contractual partner, i.e. the CI. Thus, there is a need to investigate such three-part trust relations and their impact on outsourcings (O2). In this context, the contractual configuration between the stakeholders in terms of SLAs is of further decisive importance in order to meet the specific demands of CIs [8, 22, 29] (C1). As SLAs are often predefined by cloud providers, the specific requirements of CIs and responsibilities of the parties need to be defined [7, 11, 23, 25]. In addition, there is a need for continuous assurance that the determined agreements are enforced, e.g. by appropriate certification methods [4, 8] (C2). The interplay of the actors with the corresponding research propositions and issues of Table 3 are displayed in Figure 1.

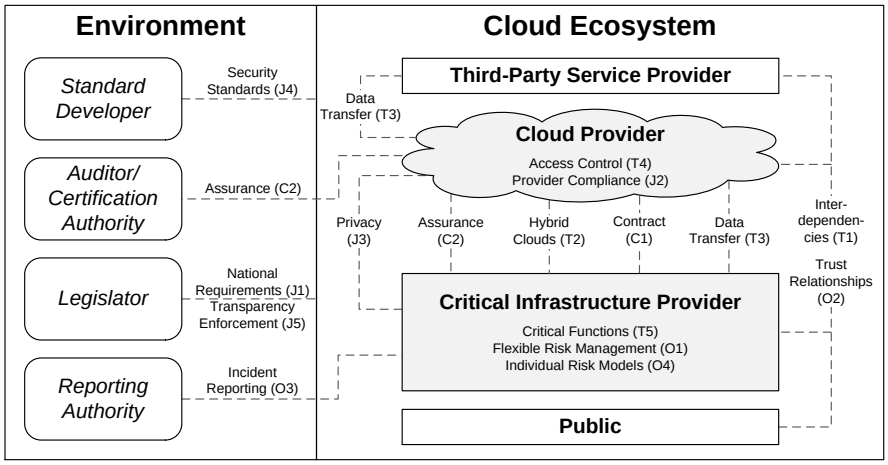


Figure 1. Open Issues and Research Propositions for Cloud Adoption in CIs [30]

5 Conclusion

The analyses revealed that cloud computing is only used in partial areas of critical infrastructures. Risks related to data security lead to a rather restrained attitude of many organizations. Yet, due to the fact that outsourcing into a cloud is advantageous, an increasing number of CIs decide to adopt cloud solutions for 'non-critical' business functions. Thus, future research on cloud solutions for core functions of CIs, such as industrial control systems [24], is necessary. Among the cloud services used by CIs private clouds for basic infrastructure services are considered frequently. Further, the use of services hosted in public clouds expands, especially SaaS. However, regulations and unclear legislations are obstacles for the adoption of cloud solutions by CIs, specifically in sectors with strict requirements for data privacy and security, such as finance or health. Thus, the assurance over actions and security measurements of the cloud provider and a minimization of dependencies are crucial. In summary, it can be stated that despite the increasing demand various aspects have to be considered and clarified, such as risk management issues. In this context, the results of the analysis of the current status quo of cloud computing in CIs are helpful for CIs and cloud providers alike to sustainably decide for or against cloud solutions.

However, the study has to be viewed under the light of some limitations. First, the practical analysis does not reflect the overall ratio of German CIs. Further, as we had to rely on publicly available information, the generalizability of the results is limited. As expert no. 4 stated that the risks associated to the disclosure of internal information on the IT landscape and outsourcings induce CIs to consciously withhold such information, we assume that the actual user numbers are significantly higher. In addition, it was not always clear whether the CIs use a classic IT outsourcing model or a cloud, and in case if, which kinds of cloud services were used particularly. Further, the results of the expert interviews might be biased by the sector affiliation of the respondents. Likewise, further interviews covering all CI sectors are desirable.

Acknowledgements

The authors thank the project members, especially Ms. Anne Christin Münning, Ms. Maria Borgmann, Mr. Niclas Bruhne, Mr. Heiko Halstenberg and Mr. Jonas Brinker for their valuable help and support during the research process. Furthermore, the authors thank Ms. Imhorst as well as the reviewers for their constructive feedback.

References

1. Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2016. (2016)
2. Hecht, T., Smith, P., Schöller, M.: Critical Services in the Cloud: Understanding Security and Resilience Risks. In: 6th International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 131–137. Barcelona, Spain (2014)
3. Bless, R., Hutchison, D., Schöller, M., Smith, P., Tauber, M.: SECCRIT: Secure Cloud Computing for High Assurance Services. ERCIM NEWS. 95, 40–41 (2013)
4. Wagner, C., Hudic, A., Maksuti, S., Tauber, M., Pallas, F.: Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud. In: 3rd International Conference on Future Internet of Things and Cloud. Rome, Italy (2015)
5. Hudic, A., Hecht, T., Tauber, M., Mauthe, A., Santiago Cáceres, E.: Towards Continuous Cloud Service Assurance for Critical Infrastructure IT. In: 2nd International Conference on Future Internet of Things and Cloud, pp. 175–182. Barcelona, Spain (2014)
6. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A.: Cloud Computing - The Business Perspective. Decision Support Systems. 51, 176–189 (2011)
7. Diez, O., Silva, A.: Reliability Issues Related to the Usage of Cloud Computing in Critical Infrastructures. In: Bérenguer, C., Grall, A., Guedes Soares, C. (eds.) Advances in Safety, Reliability and Risk Management: ESREL 2011. Troyes, France (2011)
8. Schöller, M., Bless, R., Pallas, F., Horneber, J., Smith, P.: An Architectural Model for Deploying Critical Infrastructure Services in the Cloud. In: IEEE International Conference on Cloud Computing Technology and Science, pp. 458–465. Bristol, UK (2013)
9. Paudel, S., Tauber, M., Brandic, I.: Security Standards Taxonomy for Cloud Applications in Critical Infrastructure IT. In: 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 645–646. London, UK (2013)
10. Rudolph, M., Schwarz, R., Jung, C.: Security Policy Specification Templates for Critical Infrastructure Services in the Cloud. In: 9th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 61–66. London, UK (2014)
11. Younis, Y.A., Merabti, M., Kifayat, K.: Secure Cloud Computing for Critical Infrastructure: A Survey. Liverpool John Moores University, Technical Report 599-610 (2013)
12. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems. 21, 11–25 (2001)
13. Adelmeyer, M., Petrick, C., Teuteberg, F.: IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes. HMD Praxis der Wirtschaftsinformatik. 54, 111–123 (2017)
14. Brocke, J. vom, Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the Giant: on the Importance of Rigour in Documenting the Literature

Search Process. In: 17th European Conference on Information Systems (ECIS), pp. 2206–2217. Verona, Italy (2009)
15. Gläser, J., Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse. Springer VS Verlag für Sozialwissenschaften, Wiesbaden (2010)
16. Lampe, U., Müller, A., Wenge, O., Schaarschmidt, R.: On the Relevance of Security Risks for Cloud Adoption in the Financial Industry. In: 19th Americas Conference on Information Systems (AMCIS). Chicago, Illinois, USA (2013)
17. Anastacio, M.M.B., Blanco, J.A.R., Villalba, L.J.G, Al-Dahoud, A.: E-Government: Benefits, Risks and a Proposal to Assessment Including Cloud Computing and Critical Infrastructure. In: 6th International Conference on Information Technology (ICIT). Amman, Jordan (2013)
18. Chochliouros, I.P., Spiliopoulou, A.S., Stephanakis, I.M., Arvanitozisis, D.N., Sfakianakis, E., Belesioti, M., Georgiadou, E., Mitsopoulou, N.: Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also Focusing upon the Cloud Perspective. In: 16th International Conference on Engineering Applications of Neural Networks (INNS). Rhodes Island, Greece (2015)
19. Paudel, S., Tauber, M., Wagner, C., Hudic, A., Ng, W.-K.: Categorization of Standards, Guidelines and Tools for Secure System Design for Critical Infrastructure IT in the Cloud. In: 6th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 956–963. Singapore, Singapore (2014)
20. Tauber, M., Wagner, C., Pallas, F.: Sicherheit und rechtliche Herausforderungen in Bezug auf Cloud Computing und Kritische Infrastruktur-IT. e & i Elektrotechnik und Informationstechnik. 131, 33–36 (2014)
21. Dekker, M.A.C.: Critical Cloud Computing. Technical Report, European Network and Information Security Agency (ENISA) (2012)
22. Mackay, M., Baker, T., Al-Yasiri, A.: Security-oriented Cloud Computing Platform for Critical Infrastructures. Computer Law & Security Review. 28, 679–686 (2012)
23. MacDermott, A., Shi, Q., Merabti, M., Kifayat, K.: Hosting Critical Infrastructure Services in the Cloud Environment Considerations. International Journal of Critical Infrastructures. 11, 365–381 (2015)
24. Piggin, R.: Are Industrial Control Systems Ready for the Cloud? International Journal of Critical Infrastructure Protection. 9, 38-40 (2015)
25. MacDermott, A., Shi, Q., Merabti, M., Kifayat, K.: Protecting Critical Infrastructure Services in the Cloud Environment. In: 12th European Conference on Information Warfare and Security (ECIW), pp. 336–343. Jyväskylä, Finland (2013)
26. Niekerk, B. van, Jacobs, P.: Cloud-based Security Mechanisms for Critical Information Infrastructure Protection. In: International Conference on Adaptive Science and Technology (ICAST). Pretoria, South Africa (2013)
27. KPMG: Cloud-Monitor 2017. Technical Report, KPMG, Bitkom (2017)
28. Keller, R.: Analyse von Risikomanagementstrategien in Cloudnetzwerken – Was tun bei verknüpften, voneinander abhängigen Cloud Services? HMD Praxis der Wirtschaftsinformatik. 53, 674–687 (2016)
29. Florian, M., Paudel, S., Tauber, M.: Trustworthy Evidence Gathering Mechanism for Multilayer Cloud Compliance. In: 8th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 529–530. London, UK (2013)
30. Floerecke, S., Lehner, F.: Cloud Computing Ecosystem Model: Refinement and Evaluation. In: 24th European Conference on Information Systems (ECIS). İstanbul, Turkey (2016)

IT-Sicherheit in Kritischen Infrastrukturen – eine Fallstudien-basierte Analyse von Praxisbeispielen

Sebastian Dännart[1], Thomas Diefenbach[1], Manfred Hofmeier[1], Andreas Rieb[1], Ulrike Lechner[1]

[1] Universität der Bundeswehr München, Fakultät für Informatik, 85577 Neubiberg
{Sebastian.Daennart, Thomas.Diefenbach, Manfred.Hofmeier, Andreas.Rieb, Ulrike.Lechner}@unibw.de

Abstract. Die wachsende Bedeutung von IT-Sicherheit in Organisationen aufgrund einer vielfältigen Bedrohungslage ist unbestritten. Dies gilt insbesondere für Kritische Infrastrukturen mit hoher Bedeutung für das staatliche Gemeinwesen. In diesem Beitrag werden Beispiele erfolgreicher Umsetzungen von IT-Sicherheitsprojekten und -konzepten untersucht sowie Gemeinsamkeiten und Unterschiede bei den vorherrschenden kontextualen Rahmenbedingungen analysiert. Sieben Fallstudien wurden im Rahmen des Forschungsprojekts *Vernetzte IT-Sicherheit Kritischer Infrastrukturen* (VeSiKi*)* aus dem durch das BMBF geförderten Förderschwerpunkt *IT-Sicherheit für Kritische Infrastrukturen* (ITS|KRITIS) erhoben. Auf dieser Fallstudienserie aufbauend wurde eine Cross Case-Analyse durchgeführt. Die Ergebnisse zeigen, dass IT-Sicherheitsmaßnahmen nicht isoliert betrachtet werden können, sondern aufgrund der Einbindung in bestehende Geschäftsprozesse auch eine Anpassung organisationaler und personeller Aspekte wesentliche Erfolgsfaktoren sind.

Keywords: Kritische Infrastrukturen, IT-Sicherheit, Cross Case-Analyse

1 Einleitung

IT-Sicherheit Kritischer Infrastrukturen ist ein vergleichsweise neues Themenfeld, das mit Stuxnet, einer IT-Sicherheitsbedrohung für Industrieanlagen, im Jahr 2010 ins Bewusstsein der Öffentlichkeit drang [1]: Eine Schadsoftware konnte über längere Zeit hinweg unbemerkt Steuerungsanlagen und Leittechnik in der Uranaufbereitungsanlage Natanz und dem Kernkraftwerk Buschehr stören. Eine neuere und ebenfalls prominente Schadsoftware ist das Mirai-Botnetz mit dem Distributed Denial of Service-Angriffe organisiert werden und das im Jahr 2016 auch Router in Privathaushalten in Deutschland betraf. Die Blackouts von 2015 und 2016 in der Ukraine werden der Schadsoftware Industroyer zugeschrieben [2]. Verschiedene Versionen von Ransomware haben in den Jahren 2015 und 2016 sowohl Privatpersonen als auch Universitäten, Krankenhäuser und Behörden betroffen [3]. Fake News sowie die Diskussion über Manipulationsmöglichkeiten von demokratischen Wahlen in 2016 und 2017 sind weitere Beispiele für Verwundbarkeiten der Zivilgesellschaft.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Kritische Infrastrukturen (KRITIS) sind „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ [4]. Funktionierende Informations- und Kommunikationsstrukturen sind Voraussetzung und IT-Sicherheit der Lebensnerv für medienbruchfreie Geschäftsprozesse oder Leitbilder der Zukunft wie autonome Fahrzeuge und Data Driven X (http://mkwi2018.leuphana.de).

Um die IT-Sicherheit Kritischer Infrastrukturen zu studieren, wurde eine Fallstudienserie durchgeführt. In diesem Beitrag wird die Fallstudienserie mit Methodik und durchgeführten Fallstudien vorgestellt (Kapitel 2 und 3) sowie eine Cross Case-Analyse (Kapitel 4) präsentiert. Ziel des Beitrags ist es, Erfolgsfaktoren von Projekten der IT-Sicherheit Kritischer Infrastrukturen zu identifizieren und die Implikationen von IT-Sicherheitsverfahren auf den Kontext zu studieren, um so einen Beitrag zum Verständnis der IT-Sicherheit Kritischer Infrastrukturen zu leisten.

2 Methodik

Da die Einführung von IT-Sicherheitsmaßnahmen zumeist einen Eingriff in bestehende Geschäftsprozesse erfordert, stellen komplexe und schwer voneinander abzugrenzende Zusammenhänge und Folgen eine große Herausforderung dar. Fallstudien bieten eine Forschungsstrategie zur Datenerhebung [5], die sich sehr gut dazu eignet, diese komplexen Phänomene in ihrem natürlichen Kontext darzustellen [6]. Dazu werden Methoden der qualitativen Datenanalyse verwendet, um Prozessabläufe und die Dynamik in konkreten Situationen zu verstehen [7].

Um die Forscher bei der einheitlichen Erstellung der Fallstudien zu unterstützen und deren Arbeiten im Anschluss vergleichbar zu machen, orientieren wir uns an der eXperience Methodik [8]. Die eXperience Methodik will authentisches Wissen rund um E-Business und IT-Management vermitteln und stellt dazu ein Raster und Vorgehensmodell sowie begleitende Materialien bereit. Angelehnt an diese Methodik wurden ein Rahmen für Fallstudien zum Thema „IT-Sicherheit Kritischer Infrastrukturen“ und ein Prozess zur Erhebung der notwendigen Daten entwickelt und mit den Projekten im Förderschwerpunkt *IT-Sicherheit für Kritische Infrastrukturen* des Bundesministeriums für Bildung und Forschung im Jahr 2015 verfeinert. Drei Fallstudientemplates bieten dabei einen Leitfaden zur Darstellung unterschiedlicher Arten von IT-Sicherheitsfallstudien:

- **projektbezogene Fallstudien** beziehen sich auf ein IT-Sicherheitsprojekt,
- **produktbezogene Fallstudien**, die die Implementierung oder den Einsatz von speziellen, innovativen IT-Sicherheitstechnologien beschreiben und
- **unternehmensbezogene Fallstudien**, die die gelebte IT-Sicherheit einer Organisation aus verschiedenen Perspektiven erfassen.

Nach zwei ersten Fallstudien im Jahr 2015 wurden weitere Fallstudien im Jahr 2016 und 2017 durchgeführt und verfasst. Dabei erfolgte die Datenerhebung auf Basis von leitfadengestützten Experteninterviews.

Eine Cross Case-Analyse ermöglicht die analysierten Daten zu kategorisieren und Aussagen mehr Aussagekraft zu geben [9]. Nach Mayring [10] wurde dazu eine Kodierung entwickelt und die Fallstudien qualitativ analysiert, sodass Kernaussagen extrahiert werden konnten. Nach einem Review der Codes wurden die Extrakte als Basis für die vorliegende Cross Case-Analyse genutzt. In der Datenanalyse wurden Rephrasierungen und Aussagen von den Autoren der Fallstudien und dem Autorenteam dieses Beitrags reflektiert, um Verfälschungen auszuschließen.

3 Die Fallstudien

Als Partner für die Erstellung der Fallstudien wurden zunächst Verbundprojekte aus dem Förderschwerpunkt ITS|KRITIS gefragt, darüber hinaus aber auch weitere Betreiber Kritischer Infrastrukturen oder KRITIS-relevante Zulieferer eingebunden. Die Fallstudien wurden in den Jahren 2015 bis 2017 entwickelt und stellen den Stand vor Inkrafttreten des IT-Sicherheitsgesetzes (Bundestag-Drucksache 18/4096 und 18/5121) [11] dar. Für diesen Beitrag wurden sieben Fallstudien ausgewählt, die eine große Bandbreite Kritischer Infrastrukturen und IT-Sicherheitsprojekten abdecken. In diesem Kapitel werden die Fallstudien einzeln vorgestellt.

Tabelle 1. Übersicht über die Fallstudien[1]

Nr.	*Organisation*	*Titel*	*Autor(en)*	*Art*
1	***	Fernwartung Kritischer Infrastrukturen	A. Rieb	Produkt
2	***	Ein sicherer Standardprozess für die Digitale Tatortfotografie	S. Lücking, S. Dännart	Projekt
3	kbo	Ausgewogenes Risikomanagement für nachhaltige IT-Sicherheit	T. Kehr, S. Dännart	Projekt
4	PREVENT	IT-Sicherheit für Geschäftsprozesse im Finanzsektor – die Managementlösung PREVENT	S. Rudel, T. Bollen	Projekt
5	SAP SE	Informationssicherheit bei SAP SE: Die längste Human Firewall der Welt	U. Lechner, T. Gurschler, A. Rieb	Unternehmen
6	ugarbe.de software	Informationssicherheit durch IT-gestützte Klassifizierung von Dokumenten und E-Mails	A. Rieb	Produkt
7	***	IT-Sicherheit in der Nahrungsmittelindustrie: Tradition und Hochverfügbarkeit	S. Dännart	Unternehmen

Fallstudie 1: Fernwartung Kritischer Infrastrukturen. Die Fallstudie thematisiert Risiken der Fernwartung industrieller Kontroll- und Steuerungssysteme in Kritischen

[1] Einige Fallstudien sind anonymisiert; Kennzeichnung mit ***

Infrastrukturen und stellt den Ansatz eines Herstellers vor: eine Fernwartungslösung, die es erlaubt, Fernwartungszugänge kontrolliert zu öffnen und abgesicherten Zugang zur Kritischen Infrastruktur zu ermöglichen. Ein Wildwuchs an Fernwartungszugängen oder „geheime“ Zugänge für IT-Mitarbeiter zu Kritischen Infrastrukturen sind klassische IT-Sicherheitsthemen Kritischer Infrastrukturen. Die Lösung in Form von Hard- und Software ermöglicht die Administration von Wartungsobjekten aus der Ferne und kann insbesondere für die Sicherheit existierender Infrastrukturen eingesetzt werden.

Es werden sowohl unternehmensinterne als auch -übergreifende Herausforderungen beschrieben, die für erfolgreiche Implementierungen gelöst werden müssen.

Fallstudie 2: Ein sicherer Standardprozess für die Digitale Tatortfotografie. In dieser Fallstudie wird die Digitalisierung der Tatortfotografie – ein Prozess der Polizeiarbeit – vorgestellt. Beschrieben wird die lückenlose, justiziable Absicherung des gesamten Prozesses von der Beweismittelaufnahme bis zur Verhandlung vor Gericht.

Der digitalisierte Prozess der Tatortfotografie hat durch die neue Systemarchitektur zudem Vorteile in der polizeilichen Arbeit. Die Zulassung aller fototauglichen Geräte erleichtert die tägliche Polizeiarbeit und ermöglicht effiziente Beschaffungsvorgänge, während die Informationssicherheit der Fotos durch eine automatisch erstellte und zentral überwachte Signatur unmittelbar nach Anschließen des Datenträgers gewährleistet wird. Auch finanziell ist das Projekt ein Erfolg: Bereits drei Jahre nach Implementierung waren die Investitionskosten amortisiert.

Der digitale Prozess ist nicht nur moderner sondern auch anwenderfreundlicher als der tradierte analoge Prozess, der das Ausdrucken von Bildern für analoge Akten vorsah. Die Einbindung aller Stakeholder und deren Sensibilisierung für die Anforderungen der Informationssicherheit vom unmittelbaren Beginn des Projekts an waren für die erfolgreiche Umsetzung wichtig.

Fallstudie 3: Ausgewogenes Risikomanagement für nachhaltige IT-Sicherheit. Den Kern der Fallstudie bildet die Reaktion auf Ransomware-Angriffe auf Krankenhäuser Anfang 2016, die Impuls waren, um geplante Maßnahmen beschleunigt umsetzen zu können. Beschrieben werden die ersten Reaktionen, wie die vollständige Trennung vom Internet oder Deaktivierung von aktiven Inhalten sowie die daraus resultierenden Auswirkungen wie fehlende Unterstützung für medizinische Recherchen, Medikamentenbestellungen und die Erstellung von Arztbriefen.

Zentrales Thema der Fallstudie ist der Prozess der Freigabe von IT-Projekten, der alle Stakeholder im Klinikverbund und IT-Sicherheitsexperten miteinbezieht. Die Umsetzung eines nachhaltigen IT-Sicherheitskonzepts ist ein weiteres Thema. Die kbo erweiterten in diesem Prozess ihre Fähigkeiten mit Bedrohungen umzugehen. Organisatorisch wurden ein IT-Sicherheitskomitee, die offene Zusammenarbeit zwischen Mitarbeitern und der IT sowie der Einbezug externer Partner implementiert. Die konsequente Handlungsweise und die Maßnahmen führten dazu, dass gezielte Angriffe auf den Verbund abgewehrt werden konnten.

Fallstudie 4: IT-Sicherheit für Geschäftsprozesse im Finanzsektor – die Managementlösung PREVENT. Die Fallstudie beschreibt am Beispiel der fiktiven FutureBank und des ebenfalls fiktiven Dienstleisters FutureRZ die technische Lösung PREVENT, die das Risikomanagement in Banken unterstützt, indem ein Dashboard zur Verfügung gestellt wird, das die Daten aus einer Vielzahl an Quellen aggregiert und aufbereitet. Es entsteht eine Datenbasis, die die Wechselwirkungen zwischen verschiedenen Ebenen – Geschäfts- und Serviceprozesse, Funktionen, IT-Systeme und Netzwerk – abbilden kann und aus der verschiedene Sichten bedarfsgerecht erzeugt werden.

Dies erlaubt neue einheitliche Risikobewertungen und löst heterogene Risikomanagementlandschaften ab. Nun können von der Managementebene aggregierte Risiken erkannt werden, die über dem als kritisch eingestuften Schwellenwert der Bank liegen und die zuvor als Einzelrisiken nicht im Fokus von Minimierungsmaßnahmen waren. So soll die Entscheidungsfindung für Verantwortliche verbessert werden.

Fallstudie 5: Informationssicherheit bei SAP SE – Die längste Human Firewall der Welt. Die Human Firewall ist eine Kampagne zur Informationssicherheit der SAP SE. Key Visual ist eine Kette von Mitarbeitern von SAP mit verschränkten Armen – ein Symbol dafür, dass die Mitarbeiter keine Bedrohung zu SAP durchlassen. Mitarbeiter absolvieren eine Schulung zur Informationssicherheit und können mit ihrem Foto und einem individuellen Statement Teil der Human Firewall werden.

Die Fallstudie thematisiert Vertrauen in Mitarbeiter und Awareness zur Informationssicherheit: Kunden können das Vertrauen in SAP und seine Produkte und Dienstleistungen verlieren, wenn Mitarbeiter mit Fragestellungen der IT-Sicherheit nicht sensibel umgehen. Die Fallstudie thematisiert die Einbindung dieser Kampagne in verschiedene IT-Sicherheitsmaßnahmen, genau wie Spaß und Unterhaltung durch die einzelnen Elemente, die Messung der Awareness der Mitarbeiter sowie den Erfolg.

Fallstudie 6: Informationssicherheit durch IT-gestützte Klassifizierung von Dokumenten und E-Mails. ClassifyIt von ugarbe.de software ist ein PlugIn für Microsoft Office. Es unterstützt Nutzer bei der Klassifikation von Dokumenten und E-Mails. Die Software kann so konfiguriert werden, dass die Firewall sicherstellt, dass nur Dokumente und E-Mails mit entsprechender Klassifikation eine Organisation verlassen und dass dem Sicherheitsniveau entsprechende Verschlüsselungen gewählt werden.

Die Fallstudie beschreibt, dass ca. 60% bis 75% aller Dokumente in einer Organisation sensitiver Natur und 5% bis 10% sogar „echte kritische Informationen“ sind. ClassifyIt adressiert Risiken, die mit Sorglosigkeit im Umgang mit Informationen oder Weitergabe von Informationen an Unberechtigte einhergehen und letzten Endes einen Vertraulichkeits- oder Integritätsverlust von Daten bedeuten können. Die Software wird über Standard-Softwareverteilungstools in einer Organisation ausgerollt, die Einstellungen und Sicherheitsniveaus können von der Organisation direkt angepasst werden.

Die Fallstudie beschreibt einen wichtigen Erfolgsfaktor: das IT-Sicherheitsprodukt passt sich an die Organisation an – und nicht umgekehrt. So bietet ClassifyIt ein Höchstmaß an Flexibilität, das zudem mit einer hohen Nutzerfreundlichkeit einhergeht.

Fallstudie 7: IT-Sicherheit in der Nahrungsmittelindustrie: Tradition und Hochverfügbarkeit. Ein Nahrungsmittelhersteller steht vor besonderen Herausforderungen der IT-Sicherheit: Die Verarbeitung von sensiblen Rohstoffen wie etwa Milch erfordert eine Hochverfügbarkeit der Produktionsanlagen. Im Beispiel setzt der IT-Verantwortliche eine Strategie um, in der traditionelle organisatorische Maßnahmen um moderne Maßnahmen zur Datensicherung und Prozessautomatisierung ergänzt werden. Den Mitarbeitern in der IT und ihrer Ausbildung kommt dabei eine zentrale Rolle zu.

Themen der Fallstudie sind die IT-Sicherheitsphilosophie und Aspekte der Echtzeitsicherung des SAP-Systems, die VLAN-Kapselung der Produktionsanlagen zur Gewährleistung sicherer Fernwartung und die Integration der Mitarbeiter in IT-Prozesse.

4 Cross Case-Analyse

Die Fallstudien decken unterschiedliche Kritische Infrastrukturen und unterschiedliche IT-Sicherheitsthemen ab. Im Zuge einer übergreifenden Qualitativen Inhaltsanalyse war es das Ziel, in den Fallstudien Muster, Gemeinsamkeiten und Unterschiede zu identifizieren, die Rückschlüsse auf allgemeingültige Zusammenhänge, bewährtes Vorgehen und für den Erfolg relevante Rahmenumstände erlauben.

Die Zieldimension „IT-Sicherheit“ motiviert die ersten vier Codes: Angelehnt an die Themen des Förderschwerpunkts ITS|KRITIS ist es von besonderem Interesse aus der Praxis Erkenntnisse zu den Themenschwerpunkten *Neue Ansätze zur Beurteilung von IT-Sicherheit* sowie *Neue Ansätze zur Verbesserung der IT-Sicherheit* zu erlangen, gerade im Hinblick auf die Notwendigkeit *einfacher und kosteneffizienter* Lösungen für kleine und mittlere Unternehmen. Dies wird durch die Codes *Beurteilung und Messung von IT-Sicherheit*, *Erhöhung der IT-Sicherheit*, *Einfachheit der Maßnahme* und *Kosteneffizienz der Maßnahme* erfasst.

Tabelle 2. Übersicht über ausgewählte Codes der Qualitativen Inhaltsanalyse

Nr.	*Thema*	*Code*
1	Zieldimension „IT-Sicherheit“	Beurteilung und Messung von IT-Sicherheit
2		Erhöhung der IT-Sicherheit
3		Einfachheit der Maßnahme
4		Kosteneffizienz der Maßnahme
5	Kontext	Nebeneffekte
5.1		Wechselwirkungen mit anderen IT-Sicherheitsmaßnahmen
5.2		Einflüsse auf andere Geschäftsprozesse
6		Erfolgsfaktoren für die Implementierung
8		IT-Sicherheitsphilosophie
8.1		Vertrauensfokus in TOM
8.2		Aspekt Organisationskultur

Darüber hinaus interessieren uns auch praktische Aspekte der Implementierung von IT-Sicherheitsmaßnahmen oder -konzepten in einem Unternehmen, sodass neben den bisher genannten Codes – welche sich auf eine Sicherheitsmaßnahme im engeren Sinne

fokussieren – auch auf andere Bereiche des Unternehmens übergreifende Sachverhalte untersucht werden. Dies ist Motivation für die weiteren Codes *Nebeneffekte*, *Erfolgsfaktoren für die Implementierung*, *Treiber und Auslöser*, *IT-Sicherheitsphilosophie* und *Adressierte Risiken*. Ausgewählte Codes sind in Tabelle 2 aufgeführt.

4.1 Ergebnisse Zieldimension „IT-Sicherheit“ (Codes 1 bis 4)

Beurteilung und Messung von IT-Sicherheit (Code 1). Die Aufrechterhaltung der Informationssicherheit einer Organisation erfordert eine kontinuierliche Verbesserung, die wiederum eine fortwährende Messung und Beurteilung notwendig macht [12]. In den Fallstudien werden Methoden der Praxis in Nr. 3, Nr. 4 und Nr. 5 beschrieben. Es ist zu erkennen, dass sowohl qualitative als auch quantitative Daten erhoben werden. So nutzt SAP bspw. Fragebögen, um die Einschätzung der Mitarbeiter hinsichtlich ihrer Awareness zur Informationssicherheit zu erheben.

Zur Überprüfung der Eignung und Wirksamkeit von Maßnahmen beziehen die kbo sowohl interne IT-Experten als auch externe Dienstleister bspw. für Penetrationstests mit ein. Ferner werden bei kbo zur Beurteilung und Messung der IT-Sicherheit Metriken wie die Erkennungsrate von Malware, Anzahl an Incidents u.a. berücksichtigt. Die Ergebnisse solcher Messungen und Einschätzungen können entsprechend der adressierten Zielgruppe aufbereitet werden (z.B. Effektivitätsmessungen, Berichte). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht hier vorrangig das Management und insbesondere das Sicherheitsmanagement als Adressat der Ergebnisse [13], „um seinen Lenkungs- und Steuerungsaufgaben nachkommen zu können“ [12].

Erhöhung der IT-Sicherheit (Code 2). Das BSI empfiehlt im Zuge eines ganzheitlichen Informationssicherheitsansatzes in den IT-Grundschutz Katalogen sowohl präventive Maßnahmen als auch Maßnahmen zur Behebung von Sicherheitsvorfällen [14]. Als Hilfestellung für Betreiber von KRITIS und Nicht-KRITIS ist der Standard 100-4 zu nennen, der das Notfallmanagement adressiert [15]. Ebenso bietet das National Institute of Standards and Technology zu diesem Thema eine Publikation an [16].

In der Analyse der Fallstudien wird ersichtlich, dass die beschriebenen Maßnahmen primär präventive Maßnahmen sind, in Teilen aber auch Maßnahmen des Notfallmanagements berücksichtigen. Exemplarisch ist hier Fallstudie Nr. 7 hervorzuheben: „Die Rechenzentren […] beinhalten jeweils ein komplettes physisches Serversystem für SAP […]. Im Backup-Rechenzentrum läuft parallel ein zweites, baugleiches SAP-System, auf das zur Absicherung mit einem Zeitversatz […], auf Transaktionsebene alle Bewegungen des Systems übertragen werden“. Unter der Notwendigkeit der Hochverfügbarkeit in der Nahrungsmittelverarbeitung ist in dieser Fallstudie Redundanz ein wichtiges Thema.

Das BSI schreibt in [17] von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen, die auch in den Fallstudien wiederzufinden sind. So beschreibt Fallstudie Nr. 5 Maßnahmen, die den Faktor Mensch adressieren. Maß-

nahmen wie die o.a. Redundanz (Nr. 7) oder die Schaffung eines Gremiums zur Bewertung der IT-Bedrohungslage (Nr. 3) fokussieren mehr organisatorische Aspekte, können aber durch personelle und technische Maßnahmen unterstützt werden.

Darüber hinaus beschreiben die Fallstudien Nr. 1, 2 und 6 primär technische Maßnahmen, wie eine Software zur Datenklassifikation, eine Fernwartungslösung oder eine Software zur Absicherung des Standardprozesses für die digitale Tatortfotografie.

IT-Sicherheitsmaßnahmen wirken unterschiedlich auf IT-Risiken. Die Risikobehandlung ist nach Definition der DIN ISO IEC 27000 ein „Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos“ [18] und Organisationen stehen nach BSI-Standard 100-3 [13] verschiedene Möglichkeiten offen, mit Risiken umzugehen. Während die Software ClassifyIt eine ergänzende Schutzmaßnahme darstellt, ist die Nutzung von Thin Clients (Nr. 7) der Risikovermeidung zu zuordnen.

Ein weiterer Punkt, der in der Analyse festgestellt wurde, ist der unterschiedliche Adressatenkreis durch die IT-Sicherheitsmaßnahmen. In Summe adressieren die Maßnahmen in den Fallstudien alle Mitarbeiter, ausgewählte IT-Nutzer, IT-Fachpersonal, die Managementebene oder externe Firmen wie Zulieferer, Hersteller oder Partner.

Einfachheit der Maßnahme (Code 3). Mit diesem Code werden in den Fallstudien jene Textstellen codiert, die Aussagen zur Komplexität, dem eingesetzten bzw. zukünftig zu erwartenden Aufwand und alles weitere hinsichtlich der Einfachheit einer IT-Sicherheitsmaßnahme treffen. So entsteht eine konkrete Vorstellung davon, was eine einfache IT-Sicherheitsmaßnahme in der Praxis für Unternehmen ausmacht. In der Analyse zeigte sich, dass sich eine Einteilung in drei Kategorien anbietet; so waren in den Fallstudien mehrere Erwähnungen im Kontext der Einfachheit hinsichtlich *Nutzerfreundlichkeit*, *Implementierungsaufwand* sowie den für die Maßnahme erforderlichen *Schulungsaufwand* (sowohl für Nutzer als auch für die Administration) vorhanden.

Auffallend ist, dass in allen Fallstudien die Nutzerfreundlichkeit und Einfachheit der Implementierung der betrachteten Maßnahme mehrfach betont wird. Darüber hinaus ist zu erkennen, dass die Integration von neuen IT-Sicherheitsmaßnahmen in bestehende Prozesse – welche weder eine organisationale Anpassung von Geschäftsprozessen oder besondere Maßnahmen von Anwendern erforderten – besonders reibungsarm eingeführt werden konnten (Nr. 1, 2, 5, 6). Auch eine Implementierung in bestehende technische Anlagen und die Einbindung in vorhandene Software sowie leichte und transparente Konfiguration wurden als Merkmale der Einfachheit erwähnt.

Kosteneffizienz der Maßnahme (Code 4). Wie in jeder unternehmerischen Entscheidung spielen ebenso bei IT-Sicherheitsmaßnahmen finanzielle, personelle und zeitliche Ressourcen eine Rolle [1]. Auch wenn das IT-Sicherheitsbudget in den meisten Unternehmen wächst [19], bindet die Erreichung und Erhaltung eines bestimmten Sicherheitsniveaus in allen drei Bereichen Ressourcen. Daher muss das Ziel auch hier eine kostenbewusste Lösung sein. Gordon und Loeb stellen zudem die Verwundbarkeit von Informationen und den möglichen Schaden ins Verhältnis zu den nötigen Ausgaben, stellen jedoch nicht zwingend eine Verbesserung der IT-Sicherheit durch mehr Ausga-

ben in diesem Bereich fest [20]. Für die Kosteneffizienz von Projekten oder Umsetzungen steht zunächst offensichtlich eine schnelle Amortisation der Investitionen im Vordergrund. In der Regel ist es bei IT-Sicherheitsinvestitionen jedoch nicht möglich, eine exakte Kalkulation der Wirtschaftlichkeit für IT-Sicherheitsprojekte durchzuführen, da ihr Ertrag eben nicht unmittelbar messbar ist [21].

Die Fallstudien thematisieren die Kosteneffizienz unterschiedlich. In der Fallstudie zum Standardprozess in der digitalen Tatortfotografie wird Kosteneffizienz durch direkte monetäre Einsparungen erreicht und ist damit sehr gut belegbar (Nr. 2). Typischer ist eine schwierige Bezifferung der Einsparungen, wie im Beispiel der Fallstudie Nr. 1, in der eine gut realisierte Fernwartung Kosten reduziert, was jedoch kaum exakt messbar ist. Eine weitere Möglichkeit Kosteneffizienz zu gewährleisten ist die Reduktion des Schulungsaufwands wie dies bei ugarbe.de software vorgesehen ist (Nr. 6).

Gerade vor dem Hintergrund, dass Unternehmen regelmäßig nur einen Bruchteil des zu erwartenden Schadens investieren [20], fällt auf, dass insgesamt auch in den Unternehmen der untersuchten Beispiele wenig Augenmerk auf das Verhältnis zwischen Kosten und dem zu erwartenden Schaden gelegt wird.

4.2 Kontext (Codes 5, 6 und 8)

Die Implementierung einer Maßnahme zur Förderung der IT-Sicherheit in einem Unternehmen kann nicht isoliert betrachtet werden. Da IT-Sicherheit gerade nicht nur ein AddOn zu bestehenden Abläufen einer Organisation ist, sondern nahezu immer einen Eingriff in bestehende Geschäftsprozesse – technisch oder organisational – bedeutet bzw. erfordert, werden in diesem Abschnitt die Ergebnisse der Analyse der kontextualen Dimensionen der Sicherheitsmaßnahmen in den Fallstudien beschrieben.

Diesbezüglich werden Fallstudien nach Aussagen zu Wechselwirkungen, zur IT-Sicherheitsphilosophie sowie damit zusammenhängenden Erfolgsfaktoren für die Implementierung einer IT-Sicherheitsmaßnahme analysiert. Die Analyse zeigt auf, dass die Betrachtung der organisationalen IT-Sicherheit stets ganzheitlich mit Anpassungen bei Personal und Organisation erfolgen muss – selbst dann, wenn nur eine technische Maßnahme in das Unternehmen eingeführt wird.

Nebeneffekte (Code 5). Das BSI empfiehlt in der Vorgehensweise gemäß IT-Grundschutz die Anwendung von organisatorischen, infrastrukturellen, personellen und technischen Sicherheitsmaßnahmen [17]. Dabei kann es Wechselwirkungen der IT-Sicherheitsmaßnahmen mit anderen IT-Sicherheitsmaßnahmen geben.

In Fallstudie Nr. 6 kann die Software ClassifyIt, die als Microsoft Office PlugIn Anwender in der Klassifikation von Dokumenten unterstützt, durch die Firewall unterstützt werden: die Firewall erlaubt nur das Versenden von Dokumenten, die die Organisationsgrenzen verlassen dürfen. Hier ist ClassifyIt von anderen IT-Sicherheitsmaßnahmen abhängig. Die Fernwartungslösung aus Fallstudie Nr. 1 hingegen ist technisch von anderen IT-Sicherheitsmaßnahmen unabhängig, bedarf neben der technischen Implementierung jedoch Maßnahmen auf organisatorischer und personeller Ebene.

Das BSI beschreibt die Rolle von IT-Sicherheitsmanagement wie folgt: „Die Schaffung von Informationssicherheit ist kein Selbstzweck. […] Informations- und Kommunikationstechnik soll die Ziele einer Institution sinnvoll unterstützen und dient zur Unterstützung von Geschäftsprozessen“ [12]. In der Analyse der Fallstudien konnten verschiedene Geschäftsprozesse erhoben werden, die unmittelbar von den Maßnahmen der IT-Sicherheit beeinflusst werden: Beschaffung, Change Management, Dokumentenmanagement, Informationspolitik (intern), IT-Support, Öffentlichkeitsarbeit, Personalverwaltung, Wartung, Zahlungsverkehr (in alphabetischer Reihenfolge).

Maßnahmen der IT-Sicherheit oder Informationssicherheit hören – genau wie Geschäftsprozesse – nicht an einer Organisationsgrenze auf. Auch die Schnittstellen von Geschäftsprozessen Dritter müssen mitbetrachtet werden.

IT-Sicherheitsphilosophie (Code 8). Das BSI nennt als Faktoren, die bei der Konzeption und Planung von Sicherheitsprozessen berücksichtigt werden sollen, u.a. Umwelteinflüsse in Form von sozialen und kulturellen Rahmenbedingungen [17]. IT-Sicherheit, wenn sie gelebt wird, wird Teil der Organisationskultur und die Maßnahmen können die Kultur mitprägen [22].

Die Human Firewall von SAP (Nr. 5) fördert neben der Awareness das Commitment der Mitarbeiter und fließt in die gelebte Organisationskultur ein. Im Unternehmen aus Fallstudie Nr. 7 dagegen gilt neben Einsatzbereitschaft und langjähriger Beschäftigung das Commitment als wichtiger Erfolgsfaktor für die Umsetzung von IT-Sicherheit.

Die Fallstudie kbo (Nr. 3) thematisiert, dass sich aller Einsatz von IT nach den Bedürfnissen des Patienten und dem Datenschutz zu richten hat, was der IT-Sicherheit ambivalent gegenübersteht. In der Fallstudie Nr. 1 wird auf Kompetenzstreitigkeiten oder Machtverlust als Resultat der IT-Sicherheitsmaßnahmen hingewiesen, während die Fallstudie SAP (Nr. 5) Vertrauen in die Mitarbeiter aber auch Vertrauen der Kunden in SAP als zentralen Bestandteil hervorhebt.

Ein Thema der Unternehmensphilosophie ist der „Faktor Mensch“ – der Mensch als mögliche Fehlerquelle oder Risiko der IT-Sicherheit. In der Balance zwischen dem Vertrauen in den Menschen und der Kontrolle durch Technik gibt es Unterschiede in den Ansätzen. In den Fallstudien zu ClassifyIt von ugarbe.de software, der Human Firewall von SAP und der IT-Sicherheitsstrategie beim Nahrungsmittelproduzenten (Nr. 7) wird der Faktor Mensch thematisiert und als potenzielles Risiko bewertet.

Die Ansätze von Fallstudie Nr. 6 und Nr. 7 adressieren das Risiko durch den Menschen mit technischen Maßnahmen, während SAP (Nr. 5) direkt beim Menschen ansetzt.

In den Fallstudien sind die Zusammenhänge zwischen Organisationskultur, dem Faktor Mensch und IT-Sicherheit vielfältig. Dennoch ist Kultur immer ein Bestandteil des Rahmens, in dem IT-Sicherheit stattfindet.

Erfolgsfaktoren für die Implementierung (Code 6). In den untersuchten Fallstudien ergeben sich Gemeinsamkeiten in Bezug auf Faktoren, die eine erfolgreiche Implementierung begünstigen oder sogar Voraussetzung dafür sind. So ist in vier Fallstudien ein erfolgreiches Einbinden der Management-Ebene ein wichtiger Faktor (Nr. 1, 4, 5, 6).

Daneben wird als weiterer Faktor die Akzeptanz der Maßnahme (Nr. 1, 4, 6, 7), die durch Nutzerfreundlichkeit der Maßnahme gefördert werden kann (Nr. 6), identifiziert.

Insgesamt zeichnet sich ab, dass es wichtig ist, alle entscheidenden Organisationseinheiten einzubeziehen und „an einem Strang zu ziehen". So ist es wichtig, alle involvierten Parteien einzubeziehen (Nr. 1, 3) und eine effektive Zusammenarbeit zu ermöglichen (Nr. 2). Dies steht auch im Einklang mit der Empfehlung des BSI, dass ein Realisierungsplan für die Umsetzung eines Sicherheitskonzepts neben der Bereitstellung von Ressourcen durch das Management auch die Festlegung von Verantwortlichkeiten enthalten sollte [12]. Dabei soll laut BSI auch die Informationssicherheit in die Abläufe und Prozesse der jeweiligen Organisation integriert werden.

5 Zusammenfassung und Diskussion

Wir haben sieben Fallstudien durchgeführt, die entweder Projekte zur Erhöhung der IT-Sicherheit, IT-Sicherheitskonzepte von Unternehmen oder einzelne IT-Sicherheitsmaßnahmen eines Dienstleisters qualitativ untersucht haben.

Bei den betrachteten Unternehmen kamen sowohl technische als auch organisatorische IT-Sicherheitsmaßnahmen zum Einsatz, die teilweise Angriffe von außen, teilweise das mögliche Fehlverhalten eigener Mitarbeiter adressieren.

Um Muster in der Fallstudienserie zu erkennen, haben wir nach Fertigstellung der Fallstudien eine Cross Case-Analyse in Form einer Qualitativen Inhaltsanalyse nach Mayring durchgeführt. Die Auswahl der Codes folgte dabei einerseits der Untersuchung von Aspekten der einzelnen IT-Sicherheitsmaßnahmen, andererseits der Betrachtung kontextueller Dimensionen bei der Implementierung der neuen Maßnahme in den untersuchten Organisationen.

Dieser Artikel leistet einen Beitrag zum Verständnis zu den Gesamtzusammenhängen von erfolgreichen IT-Sicherheitsprojekten und Implementierungen von IT-Sicherheitskonzepten. Die Codes selbst stellen einen Analyserahmen für IT-Sicherheitsprojekte dar und sollen bei der Erstellung zukünftiger Fallstudien im Kontext der IT-Sicherheit von Unternehmen und Kritischen Infrastrukturen Impulse für die Auswahl des Untersuchungsgegenstands und der Entwicklung von Forschungsfragen bieten.

Für die vorliegende Arbeit gelten die methodeninhärenten Limitationen von Fallstudien. Die Generalisierbarkeit der Ergebnisse ist durch Anzahl und Auswahl der Fallstudien eingeschränkt möglich; es bleibt jedoch abzuwarten, inwiefern darauf aufbauende qualitative und auch quantitative Forschung die gefundenen Gemeinsamkeiten und Unterschiede bestätigt oder Grenzen der Ergebnisse aufzeigt.

6 Acknowledgements

Wir bedanken uns bei allen Fallstudienpartnern und Interviewpartnern für die Fallstudien, den weiteren Autoren der Fallstudien T. Bollen, T. Gurschler, T. Kehr, S. Lücking sowie bei unseren Kollegen im Projekt VeSiKi. Den Gutachtern sind wir für die hilfreichen und konstruktiven Kommentare dankbar. Wir bedanken uns beim BMBF für die Förderung des Projekts VeSiKi mit den Fallstudien (FKZ: 16KIS0213).

References

1. Zetter, K.: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers, New York (2014).
2. Strathmann, M.: Malware führte zum Blackout, http://www.zeit.de/digital/internet/2016-01/stromausfall-hacker-ukraine-blackenergy.
3. BSI: Die Lage der IT-Sicherheit in Deutschland 2016. , Bonn (2016).
4. BMI: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), (2009).
5. Yin, R.K.: The Case Study Crisis: Some Answers. Adm. Sci. Q. 26, 58–65 (1981).
6. Wilde, T., Hess, T.: Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung, http://www.wim.bwl.uni-muenchen.de/download/epub/ab_2006_02.pdf, (2006).
7. Eisenhardt, K.M.: Building theories from case study research. Acad. Manag. Rev. 532–550 (1989).
8. Schubert, P., Wölfle, R.: The Experience Methodology For Writing IS Case Studies. Am. Conf. Inf. Syst. 19–30 (2006).
9. Yin, R.K.: Case Study Research - Design and Methods. SAGE Publications Inc., Thousand Oaks, London, New Delhi (2003).
10. Mayring, P.: Qualitative Inhaltsanalyse. Grundlagen und Techniken. Beltz (2008).
11. Bundesgesetzblatt: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31), (2015).
12. BSI: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), (2008).
13. BSI: BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, (2008).
14. BSI: IT-Grundschutz-Kataloge - 15. Ergänzungslieferung, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/GSTOOL/gstool-html_el15_zip.zip.
15. BSI: BSI-Standard 100-4: Notfallmanagement, (2008).
16. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K.: NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery. (2016).
17. BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, http://www.bsi.bund.de/gshb, (2008).
18. DIN: DIN ISO/IEC 27000, (2011).
19. VeSiKi: Monitor IT-Sicherheit Kritischer Infrastrukturen, https://monitor.itskritis.de/monitor1/, (2017).
20. Gordon, L. a., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5, 438–457 (2002).
21. Stöwer, M.: Beispiele für die Wirtschaftlichkeit von Informationssicherheit, (2011).
22. Helisch, M., Pokoyski, D., Beyer, M., Haucke, A., Prantner, K.: Security Awareness - Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Vieweg+Teubner Verlag, Wiesbaden (2009).

Information Security Awareness – eine konzeptionelle Neubetrachtung

Sebastian Richter[1], Tobias Straub[1], Carsten Lucke[2]

[1] DHBW Stuttgart, Zentrum für Wirtschaftsinformatik, Stuttgart, Germany
{sebastian.richter@dhbw-stuttgart.de, tobias.straub@dhbw-stuttgart.de }
[2] TH Mittelhessen, Kompetenzzentrum für Informationstechnologie, Friedberg, Germany
{carsten.lucke@mnd.thm.de}

Abstract. Das Konzept „Information Security Awareness" (ISA) wird zur Betrachtung und Bemessung des menschlichen Sicherheitsbewusstseins herangezogen. Der vorliegende Beitrag illustriert die gegenwärtige Heterogenität der Benutzung des ISA-Konzepts und unternimmt eine konzeptionelle Neubetrachtung. Unsere Definition basiert auf einer Analogie zum aus der Psychologie stammenden Konzept des Situationsbewusstseins (Situation Awareness) und unterscheidet die Dimensionen von ISA vergleichbar dem Informationsmanagement nach Krcmar, um so eine differenzierte Betrachtungsweise zu ermöglichen. Dies fördert den intuitiven Umgang mit dem Begriff und verringert Missverständnisse.

Keywords: Informationssicherheit, Information Security Awareness, Konzeptentwicklung, Mentales Modell

1 Einleitung

Es liegt im vitalen Interesse von Organisationen im öffentlichen und privaten Sektor, Vertraulichkeit, Integrität und Authentizität sowie Verfügbarkeit als die grundlegenden Schutzziele der Informationssicherheit (Information Security, IS) zu gewährleisten [1]. Bei der Umsetzung dieser Anforderungen hat der Faktor Mensch eine wesentliche Rolle, sind es doch häufig Mitarbeiter der eigenen Organisation, die – meist ungewollt, teilweise auch gewollt – eine Kompromittierung der Sicherheit erst ermöglichen [2,3].

Vor allem, um ungewolltes Fehlverhalten bezüglich der Informationssicherheit zu vermeiden, bilden Organisationen ihre Mitarbeiter zunehmend aus, um die Information Security Awareness (ISA) zu erhöhen (vgl. [4-6]). Gleichzeitig formulieren Organisationen Regeln (vgl. [7,8]), um ihren Mitarbeitern Sicherheit im Umgang mit schützenswerten Informationen (*Assets*, sowohl digitalisiert als auch analog) zu geben.

Bei der Analyse des in der Wissenschaft genutzten Konzepts fällt auf, dass die Definition von ISA sehr heterogen und in weiten Teilen einschränkend erfolgt. Oft wird darunter nur das Bewusstsein über Vorhandensein und Inhalt der

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Sicherheitsregeln verstanden (vgl. [9,10]). In dieser Arbeit wird eine neue Sichtweise entwickelt, die es ermöglicht, das Mitarbeiterverhalten bezüglich der Informationssicherheit differenzierter beschreiben zu können. Dazu wird im folgenden Abschnitt zunächst die Bandbreite der Definitionen dargestellt. Der zentrale Beitrag dieser Arbeit ist die in Abschnitt 3 vorgeschlagene Neukonzeption auf Basis des Ansatzes der *Situation Awareness* unter Einbeziehung des Modells des Informationsmanagements nach Krcmar (vgl. [25]). Die Konzeptualisierung wird abgerundet durch eine Betrachtung, aus welcher Analyseperspektive (Individuum, Team, Organisation) ISA untersucht werden kann.

2 Das ISA-Konzept – State-of-the-Art-Analyse

Eine *Leitlinie zur Informationssicherheit* (Information Security Policy, ISP) wird auf strategischer Ebene einer Organisation definiert. Für Mitarbeiter werden verbindliche *Richtlinien* (Information Security Regulations) abgeleitet, die der operativen Umsetzung der Leitlinie dienen [9,11]. Dies ist ein probater und auch aus Gründen der Governance ratsamer Weg, um Mitarbeitern Handlungssicherheit im Umgang mit Assets zu ermöglichen. Zur sprachlichen Vereinfachung ist im Verlauf einheitlich von *Regeln* die Rede, wenn Vorgaben der Leitlinie und der Richtlinien gemeint sind. Bei der Analyse, wann und warum sich Mitarbeiter an die Regeln halten oder nicht, spielt das Konzept ISA eine wichtige Rolle (vgl. [5,7,9]).

2.1 Gängige Definitionen

Nachfolgend wird aufgezeigt, wie das ISA-Konzept in der Wissenschaft definiert ist. Anstelle eines ausführlichen Literature Review (wie ihn etwa [1] bzgl. der möglichen Maßnahmen zur Steigerung und Aufrechterhaltung von ISA durchführt), wird hier anhand ausgewählter Definitionen die Heterogenität bei der Benutzung des ISA-Konzepts illustriert.

Die folgende Definition aus [12] verdeutlicht das in der Literatur vorherrschende Konzeptverständnis exemplarisch.

> *"We thus view security awareness as consisting of three interrelated and inter-dependent parts that are required to be mutually understood and in balance: formal security awareness, cognitive security awareness and behavioral security awareness. […] Security awareness is thus about understanding the information security policies, as well as complying with them."*

ISA im engeren Sinne drückt somit aus, ob und inwieweit Mitarbeiter die Regeln ihrer Organisation kennen und verstehen. Ein hohes Maß an ISA führt – bei entsprechender Motivation und Nutzenerkenntnis – zur Befolgung der Regeln [9,10]. Ein weiteres Beispiel [13] betont den instrumentalen Charakter von ISA sowie die Ausrichtung auf die Einhaltung der Regeln wie folgt:

„Information security awareness is a vital communication tool used by organizations to influence end-users towards compliance with information security policies and controls in the organization.“

Ohne Anspruch auf Vollständigkeit zeigt **Tabelle 1** verschiedene Definitionen für das ISA-Konzept, auf die im Verlauf teilweise eingegangen wird.

Tabelle 1: Einige Beispiele für verschiedene Informations- bzw. informationssystem- und informationstechnologiebezogene Awareness-Begriffe.

Nr.	***Quelle*** / **Definition (D)** / **Verständnis (V)**	***Begriff***
1	*Wilson und Hash 2003 [14]* **D:** „Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.” **V:** Initiales Wissen, dass es IT-Sicherheit gibt und welche Verhaltensmuster für jedermann adäquat sind.	*IT Security Awareness*
2	*Hellquist et al. 2013 [12]* **D:** “Security awareness is thus about understanding the information security policies, as well as complying with them.” **V:** Ziel von Awareness ist, dass sich Mitarbeiter der Verhaltensregeln bewusst sind und sich entsprechend verhalten.	*Security Awareness*
3	*Banerjee et al. 2013 [15]* *Banerjee und Pandey 2010 [16]* **D:** „Security awareness can be defined as the knowledge that members of an organization possess regarding protection of the physical and information assets of that organization.” **V:** Software Security Awareness wird als Konzept selbst nicht definiert, stützt sich jedoch auf eine Definition der Security Awareness ab. Als allgemeinerer Wissensbegriff umfasst es Wissen, wie schützenswerte Güter gesichert werden können.	*Software Security Awareness*
4	*Bulgurcu et al. 2010 [9]* **D:** “Information security awareness is defined as an employee’s general knowledge about information security and his cognizance of the information security policy (ISP) of his organization. General information security awareness and ISP awareness are the key dimensions of ISA. General information security awareness is defined as an employee’s overall knowledge and understanding of potential issues related to information security and their ramifications. Beyond general ISA, organizations have specific expectations of their employees that are reflected in the ISP. ISP awareness is defined as an employee’s knowledge and understanding of the requirements prescribed in the organization’s ISP and the aims of those requirements.” **V:** Unterscheidung zwischen generellem Wissen über IT-Sicherheit und dem Wissen um die in der Organisation geltenden Regeln.	*- Information Security Awareness* *- General Information Security Awareness* *- Information Security Policy Awareness*

Nr.	*Quelle* **Definition (D)** **Verständnis (V)**	*Begriff*
5	*Choi et al. 2008 [17]* **D:** “Managerial Information Security Awareness in the current study particularly focuses on how senior managers regard the significance of information security.” **V:** Begriff beschreibt die wahrgenommene Wichtigkeit von Information Security bei Managern der obersten Führungsebene mit Bezug zur eigenen Aufgabe.	*Managerial Information Security Awareness*
6	*Siponen 2000 [10]* **D:** "The term 'information Security awareness' is used to refer to a state where users in an organization are aware of - ideally committed to - their security mission (often expressed in end-user security guidelines)." **V:** Begriff bezieht sich auf den Idealzustand, dass sich Mitarbeiter nicht nur ihres Sicherheitsauftrags bewusst sind, sondern ihn befolgen.	*Information Security Awareness*
7	*Spears und Barki [18]* **D:** "Thus, organizational awareness refers to different target groups (e.g., end users, IS professionals, senior management, third parties, etc.) that exhibit a consciousness about organizational policies, procedures, or the need to protect sensitive information." **V:** Differenzierte Sichtweise, die verschiedene Nutzergruppen bezüglich der Sensitivität von schützenswerter Information unterscheidet und den Mitgliedern dieser Gruppen unterschiedliche Sichtweisen zuspricht.	*Organizational Awareness*

2.2 Begriffskritik

Bei Betrachtung der Konzeptdefinitionen in Tabelle 1 fällt auf, dass verschiedene Bezeichner für gleiche bzw. ähnliche Konzepte verwendet werden, ohne dass die Gründe hierfür ersichtlich wären. Die sich ergebende Frage angesichts der Begriffsheterogenität ist, ob IT Security Awareness und Information Security Awareness tatsächlich das gleiche Konzept ist.

Um diese Frage zu beantworten, kann man sich über verschiedene Rollen und deren Tätigkeiten dem Konzeptverständnis nähern. Zunächst scheint es ratsam, Endnutzer oder Manager nicht mit detaillierten technischen Vorgaben (z.B. Firewall-Regeln) zu konfrontieren, wie der Bezeichner IT Security Awareness implizieren würde. Ein Manager muss jedoch Bewusstsein bezüglich schützenswerter Informationen, die in seiner Reichweite sind, haben. Hierzu gehören z.B. auch ausgedruckte Unterlagen, die er physisch transportiert, was intuitiv dem Bezeichner Information Security Awareness zuzuordnen wäre. Es liegt also nahe, mit Hilfe von Rollen und deren Umgang mit Technik bzw. Information das Konzept Security Awareness zu durchdenken.

Bei den obigen Definitionen fällt weiter auf, dass der Begriff Awareness – also am ehesten Bewusstheit – sich auf Wissen um Regeln (Nummern 2, 4, 6, 7) oder aber auf ganz allgemeines Wissen bezüglich Informationssicherheit (Nummern 3, 4) bezieht. Somit hat das Konzept im Gegensatz zum allgemein in der Psychologie gebräuchlichen Awarenesskonzept keinen expliziten Umweltbezug. Im Kern meint das Awarenesskonzept, abhängig von der Umweltentwicklung eigene Handlungen

anzupassen. Die mentale Bewusstheit über Vorgänge – sowohl im Inneren des Menschen aber vor allem bezüglich der Wirkung der äußeren Umgebung auf den eigenen Erfahrungskontext sind Gegenstand des Awarenesskonzepts. Der gestalttherapeutische Begriff Awareness meint *"ein 'mehr Dinge in der Umwelt oder an sich selbst Wahrnehmen' [...], in welchem weniger Bewertung und Absichtlichkeit liegt."* [19]. Insofern würde der Begriff Information Security Awareness eher auf einen Zustand hindeuten, in dem Mitarbeiter bei Ihren Handlungen die Gefährdung und den Schutz von Informationen durch ihre Handlungen ständig bewerten und entsprechend handeln. Regularien können hierbei zweifelsohne helfen.

Ein entscheidender Nachteil, wenn sich Awareness nur auf Regularien bezieht, ist, dass das Konzept zu widersprüchlichen Aussagen führen kann. Crossler et al. identifizieren in ihren Untersuchungen zur „Behavioral Information Security" den Bedarf, Innentäter, die mit vollem Bewusstsein und Willen handeln, von Personen, die aus Versehen und Unwissenheit handeln, zu unterscheiden und dazu passende Konzepte zu entwickeln [20]. Interessanterweise würde man bei beiden Verhaltensweisen eine geringe ISA im engeren Sinn konstatieren, was insofern kontraintuitiv ist, als dass ein Mitarbeiter, der Regeln bewusst bricht, diese sehr gut kennt, aber eben Schaden anrichten möchte.

Basierend auf diesen Gedanken erscheint es sinnvoll, das Konzept Information Security Awareness zu überdenken. Dabei werden folgende Anforderungen gestellt:

1. Die Konzeptverwendung sollte der allgemeinen sprachlichen Intuition entsprechen.
2. Der bewusst gewählte Begriff Awareness sollte ebenso wie in der Psychologie, aus dem er entstammt, einen Bezug zur Handlung und zur Umwelt haben.
3. Das Grundkonzept sollte Security Awareness heißen, so dass die Präfixe *IT*, *IS* und *Information* als qualifizierende Bezeichner echte Bedeutung erlangen.
4. Bei der Verwendung des Konzepts sollte Klarheit über die Analyseebene herrschen: Ist das Konzept auf der Ebene des Individuums, auf der Ebene des Teams oder auf der Ebene der Organisation angesiedelt?

3 Das Konzept Security Awareness – eine Neubetrachtung

Ganz intuitiv soll hohe Information Security Awareness eines Mitarbeiters zunächst so verstanden werden, dass er sich bei seinem Handeln darüber bewusst ist, dass – aber auch in welchem Maße – die Informationen, mit denen er umgeht, schützenswert sind und welche Bedrohungen der Informationssicherheit im Rahmen seiner Handlungen bestehen oder erst durch seine Handlungen entstehen und wie er diesen begegnen kann (vgl. hierzu auch [5]).

3.1 Situation Awareness

Um dieses intuitive Verständnis genauer zu modellieren, wird in Analogie das Konzept *Situation Awareness* (Situationsbewusstsein), das mit Hilfe von [21] erklärt wird, genutzt. Einzelpersonen oder Gruppen von Personen erzeugen mentale Repräsentationen ihrer Umgebung, um eigene Handlungen an dieser Repräsentation,

aber vor allem an der Antizipation der kurzfristigen Weiterentwicklung der Umgebung auszurichten [21]. Der Prozess des Aufbaus des mentalen Modells verläuft in den Phasen *Perzeption*, *Verarbeitung* und *Projektion*, bezogen auf die Umwelt und deren jeweilige Veränderung (vgl. [22,23]). Die Phase *Handlung* wird zur Situation Awareness nicht hinzugezählt. Das Modell stellt dar, dass Individuen zyklisch durch sensorische Wahrnehmungen und deren mentaler Verarbeitung das für das eigene Handeln relevante Umweltbild aktualisieren. Bereits in der Ursprungstheorie hat Endsley dieses Modell auf Teams übertragen [21].

Warum eignet sich die Übertragung dieses Modells auf das ISA-Konzept? Bei der Betrachtung von Gefährdungen der Informationssicherheit geht man typischerweise von einer dynamischen Umwelt aus, in der a priori unbekannte Akteure versuchen, auf (Informations-)Ressourcen der Organisation in von ihr nicht intendierter Weise zuzugreifen. Die Dynamik ergibt sich insbesondere dadurch, dass zeitgleich viele legitime Zugriffe geschehen und so eine hohe Änderungsrate im Informationsbestand herrscht. Eingebettet in diese dynamische Umwelt, sollten Mitarbeiter zunächst „aware“ bei eigenen Handlungen sein. Sie sollten Umweltveränderungen, aber auch die durch eigene Handlungen entstehende Veränderung zunächst wahrnehmen, auf dieser Basis verarbeiten, und darauf aufbauend ein Bewusstsein entwickeln, wie die Veränderungen in naher Zukunft wirken (bspw., welche Sicherheitsgefahren aus den Handlungen entstehen, aber auch, ob eigene Handlungen Regularien widersprechen).

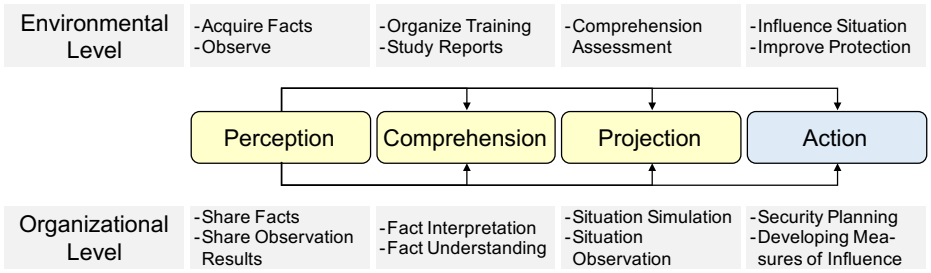


Abbildung 1: ISA basierend auf der Entwicklung von Situation Awareness

Die Abbildung visualisiert die Modellübertragung aus Sicht der Gesamtorganisation (die hier Awareness erlangt):

- *Perzeption* von Veränderung bedeutet, die Umwelt zu beobachten und so relevante Fakten zu sammeln. Dies können neue Angriffsvektoren oder Sicherheitswerkzeuge sein, auf die die Organisation aufmerksam wird. Beobachten bedeutet, dass die Organisation Angriffsversuche detektieren kann, etwa weil einzelne Mitarbeiter Bewusstsein für entsprechende Vektoren haben. Auf Organisationsebene gilt es, gesichtete Fakten und Beobachtungen zu teilen, um die Awareness zu steigern.
- Bei weitergehender Verarbeitung dieser „Reize“ (*Comprehension*) gilt es, bereits verarbeitete und zur Organisation passende organisationsexterne Information bzw. Wissen zu sichern. Dies kann in Form „eingekaufter“ Trainings, aber auch in der gezielten Auswertung von Studien und Erkenntnissen, geschehen. Diese

Verarbeitung ist im Innern zu interpretieren, zu verdichten und ins mentale Bewusstsein aufzunehmen, um künftige Gefährdungen erkennen und adäquat handeln zu können.
- Zum Schutz vor Bedrohungen wird bei der *Projektion* die nahe Zukunft vorhergesagt, insbesondere unter Berücksichtigung aktueller Eintrittswahrscheinlichkeiten. Auf organisationaler Ebene können hierbei „Simulationen" von Bedrohungsszenarien helfen, aber auch die gezielte Überwachung von Situationen, z.B. durch Honeypots. Diese Projektion ermöglicht Handlungen, die letztlich in ein integriertes Sicherheitsmanagement führen.

Bei diesem Modellansatz wird dem Mitarbeiter nicht nur eine passive Rolle der Regeleinhaltung zugewiesen. Vielmehr soll ein tiefergehendes Verständnis der Regeln bezüglich der jeweiligen Rollen der Mitarbeiter entwickelt werden. Handlungssicherheit ist das Ziel.

Der Vorteil des beschriebenen Konzepts liegt darin, Mitarbeiter zu eigenständigem Handeln und zur Eigenverantwortung zu ermutigen. Wie Balozian und Leidner zeigen, empfinden Mitarbeiter negativen Stress, wenn sie Regeln nicht verstehen und diese ihre Arbeit beeinflussen, was oftmals zum Umgehen der Regeln führt [11]. Awareness würde aber bedeuten, dass Mitarbeitern der Nutzen der Regeleinhaltung klar ist und ihre Motivation hierfür steigert. Ein anderes Problem entsteht, wenn die Regeln nicht mehr geeignet sind, neuesten Bedrohungen zu begegnen. Im Rahmen der Systemadministration etwa bedeutet Security Awareness mehr als Regelkenntnis und -einhaltung, weil Administratoren eben selbst die Regeln entwickeln müssen und zwar gemäß ihrer Awareness bezüglich der Bedrohungen der Umwelt. In diesem Kontext werden Mitarbeiter beim Testen der Sicherheit bewusst Regeln brechen, gerade weil ihre Security Awareness so hoch ist. Das vorgeschlagene Konzept bringt den Begriff der Security Awareness in Einklang mit diesen Beispielen und macht ihn intuitiv nutzbar.

3.2 Bildung von Subkategorien

Tabelle 1 macht deutlich, dass bezüglich des Konzepts Security Awareness die Bezeichner IT, IS und Information überraschenderweise weitestgehend synonym verwendet werden. Erachtet man den qualifizierenden Bezeichner als reine Geschmackssache, so wird das Konstrukt unspezifischer und den unterschiedlichen Gefährdungen der Informationen nicht gerecht. Diese können stark variieren, je nachdem, welches Medium zum Transport bzw. zum Speichern der Information betrachtet wird. Die Gefährdung, die z.B. durch einen im PKW verbliebenen Papierausdruck von Geschäftsunterlagen (Information) entsteht, ist eine andere, als wenn durch Vergabe leicht zu erratender Passwörter tausende Datensätze eines Datenbanksystems kopiert werden können (IS) oder aber, wenn durch unerlaubtes Öffnen eines Ports Schadsoftware den Weg ins organisationseigene Netz finden kann (IT). Da zumindest in größeren Organisationen Mitarbeiter bezüglich des Zugriffs und der Konfiguration der IT-Infrastruktur aber auch der Informationen an sich sehr

unterschiedliche Kenntnisse und auch Rechte haben, ist es durchaus sinnvoll, das Konzept Security Awareness klarer zu differenzieren.

Krcmar schlägt für das Informationsmanagement ein Modell gemäß Abb. 2 vor, das verschiedene Managementebenen unterscheidet, bei denen jeweils die gleichen Führungsaufgaben, wozu auch IT-Sicherheit gehört, umzusetzen sind [25]. Die vorgeschlagenen Ebenen sind Informations- und Kommunikationstechnik (IKT), Informationssysteme (IS) und Information.

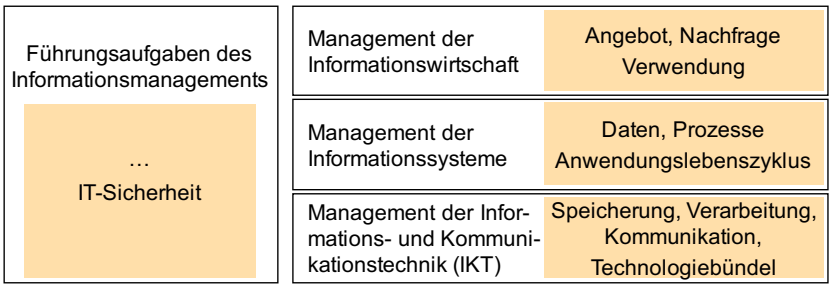


Abbildung 2: Modell des Informationsmanagements nach Krcmar [25]

Es scheint sinnvoll und fruchtbar, diese Unterscheidung für eine Neukonzeption der Security Awareness in folgender Weise zu übernehmen.[1]

- *IT Security Awareness* wird definiert als der (bezüglich der Sicherheitsgefahren) bewusste Umgang mit IT. Hier sind z.B. Konfiguration und Betrieb von Firewalls oder die Nutzung von Antiviren-Software gemeint. Eine ausgeprägte IT Security Awareness ist etwa für Mitarbeiter erforderlich, die IT bereitstellen. Diese Art Awareness ist dagegen weniger für Mitarbeiter nötig, die als Anwender IT nutzen, wenngleich die Übergänge nicht trennscharf sind.
- *IS Security Awareness* wird definiert als der bewusste Umgang mit Informations- und Kommunikationssystemen. Darunter fällt der Umgang mit Passwörtern, die Auswirkungen von Phishing-Mails und anderen Gefahren, die der Organisation durch Anwendung komplexer IS drohen. Diese Art Awareness benötigen zwar alle Mitarbeiter einer Organisation, aber wiederum sehr unterschiedlich. Während auf technischer Ebene Fragen des Identity and Access Managements relevant sind, müssen Benutzer eher den Zugangsschutz oder das Verteilen der Informationen aus sicherheitsrelevanter Sicht durchdringen.
- *Information Security Awareness* schließlich wird definiert als der bewusste Umgang mit Informationen, unabhängig vom Medium.

Besonders beim Erstellen von Schulungen oder -Kampagnen sollte – im Rahmen der Personalisierung der Ausbildung – die Zuordnung der jeweiligen Ebene durchdacht sein und Bewusstsein herrschen, welches Konstrukt wirklich angesprochen wird.

[1] Aufgrund der naheliegenden Bezeichnungen für die drei Ebenen werden diese Präfixe weiter verwendet und die "Überladung" bestehender Begriffe in Kauf genommen. Im Rest des Beitrags werden die nachfolgenden Definitionen verwendet.

IT Security Awareness fokussiert nicht unmittelbar die Gefährdung der Information, sondern die technische Komponente der IT und somit nur indirekt die mittels IT „verwaltete“ Information. IS Security Awareness hat technische und informationale Anteile. Information Security Awareness behält ebenfalls eine technische Komponente, weil die meisten Informationen mittels technischer Medien gespeichert und verbreitet werden.

Es ist möglich, die drei Konzepte definitorisch scharf voneinander abzugrenzen. Es ist aber anzunehmen, dass diese Trennschärfe empirisch nicht gegeben ist, da das Konzept ein mentales ist, das primär anhand der Handlungen eines Individuums beobachtbar wird. Der Mitarbeiter wird dabei in unterschiedlichem Maße alle drei Konzepte benötigen, um das angestrebte Schutzniveau zu erreichen. Jedoch wird die Gewichtung der drei Konzepte je nach Position und Rolle eines Mitarbeiters variieren. So muss ein Administrator über viel IT Security Awareness und u.U. weniger über Information Security Awareness verfügen. Bei einem Manager strategischer Ebene wird es im Allgemeinen umgekehrt sein. Sachbearbeiter werden eher IS Security Awareness benötigen.

3.3 Die Analyseebene des Konstrukts

Bei einem sozialen bzw. organisationalen Konstrukt wie ISA sollte beschrieben werden, auf welcher Ebene der Analyse (Individuum, Team, Organisation) es betrachtet wird [26]. Zunächst ist Awareness ein kognitives, auf der **Ebene des Individuums** angesiedeltes Konstrukt [21]. Wie oben beschrieben, nimmt das Individuum Umweltreize auf und verarbeitet diese, um eigene Reaktionen anzupassen. Bezogen auf Security Awareness ist es das Individuum, das sich der Gefahren bewusst wird und entsprechend handelt. Hierbei ist das Wissen um Bedrohungen und Schutzmaßnahmen zentral. Zusätzlich benötigt das Individuum die Fähigkeit, dieses Wissen in den Anwendungskontext spezifischer Handlungssituationen zu setzen (vgl. Modell der Wissenstreppe [27]), um Wissen über z.B. IT-Sicherheit oder aber Regularien der Organisation anzuwenden. Dazu muss es die Reize der Umwelt (z.B. den Kontext von Gesprächen oder die Konfiguration von IT-Systemen) zyklisch auswerten und so die Umwelt bewerten.

IT, IS und Information Security Awareness können ebenso auf **Teamebene** betrachtet werden. Unter einem Team wird eine Gruppe von Menschen verstanden, die hohe Zielkonvergenz haben und gleichzeitig in einem Setting hoher Interdependenz arbeiten, um bspw. ein Projektziel zu verwirklichen [28]. Es stellt sich z.B. die Frage, ob ein Softwareentwicklungsteam über hohe Security Awareness verfügt. Das Konstrukt bezieht sich dann auf eine Gruppe von Menschen, die einerseits miteinander interagiert und sich beeinflusst und andererseits Sichten, Fähigkeiten und Wissen, bezogen auf das zu lösende Problem, spezialisiert (vgl. [29,30]). Mentale Modelle, die solch ein Team entwickelt, sind Team-Level-Konstrukte (vgl. [22,31]). Das bedeutet, dass dieses Konstrukt auf Teamebene nicht anhand der Individuen betrachtet werden kann (z.B. durch „Summation“ oder „Durchschnittsbildung“ der individuellen Awareness), sondern nur durch Beobachtung und Bewertung des kompletten Teams. Wenn Rollen im Team

spezialisiert sind, wird auch die individuelle Security Awareness spezialisiert sein. Wenn z.B. in einem Softwareentwicklungsteam ein Teammitglied für Datenbankprogrammierung verantwortlich ist, muss dieses Teammitglied vor allem Angriffsvektoren und Gegenmaßnahmen kennen, die sich auf Datenbanken beziehen. Das sind andere Bedrohungen als bei der Entwicklung von User Interfaces. Wichtig ist allerdings die Verbindung und Interdependenz dieser Bedrohungen. Es sollte im Team also gemeinsames Wissen darüber herrschen, dass die Umwelt in spezifischen situativen Entwicklungen unterschiedlichen Einfluss auf die Informationssicherheit bezüglich der Arbeit oder Handlungen von Mitgliedern des Teams nimmt. Weniger wichtig ist, dass jeder im Team weiß, welchen spezifischen Einfluss die Entwicklung bzgl. der Informationssicherheit bei den Partnern im Team hat. Hierfür ist das spezialisierte Wissen im Team nötig. Dennoch sollte das Wissen um die Bedrohung kommuniziert werden, sollte ein Teammitglied bspw. die Auswirkung einer spezifischen Konfiguration nicht bemerkt haben. Da Security Awareness den vorstehenden Ausführungen zufolge also nicht auf der individuellen Ebene erfasst werden kann, ist das generelle Messen des Teamkonstrukts im Grunde nur indirekt (anhand der Beobachtung der Handlungen im Team) und nicht mehr (gut) introspektiv möglich. Fragebogenmethoden sind hier beispielsweise relativ schwer anwendbar.

Awareness kann ebenso auf **Organisationsebene** angesiedelt sein. Hier gelten die Aussagen zur Teamebene weitestgehend analog. Bereits Siponen betrachtet die Organisation als Dimension für Information Security Awareness [32]. Es wird durch dieses Konstrukt das Bewusstsein der gesamten Organisation (manifestiert durch gemeinschaftliche Handlungen) hinsichtlich der Bedrohungen der Umwelt in Bezug auf Informationssicherheit adressiert. Auch hier ist die Frage nach dem Messen des Konstrukts wichtig und nicht einfach zu beantworten.

4 Synthese und Ausblick

Basierend auf der Betrachtung der vorhandenen teils heterogenen und teils ungenauen Definitionen des Konstrukts Information Security Awareness liefert dieser Beitrag eine andere – eher auf das gestalttherapeutische Konstrukt Awareness bezogene – Betrachtung und fügt weitere Dimensionen hinzu.

Das Konstrukt kann auf der Ebene des Individuums, des Teams oder der Organisation analysiert werden, wodurch sich in Relation die Umwelt ergibt, auf die sich Awareness bezieht. Security Awareness selbst beschreibt einen Verarbeitungs- und letztlich Prognoseprozess, der sich aufgrund des vorhandenen Wissens und der Perzeptionen der Umweltveränderungen ergibt. Es hilft, vor allem für Schulungen, Security Awareness in den Unterkategorien IT, IS und Information zu betrachten.

Die Vorteile des Modells liegen in der differenzierten Betrachtungsweise und vor allem darin, dass der neue Konzeptbegriff anschlussfähig zu dem Wissenschaftsgebiet – der Psychologie – wird, dem das Konzept Awareness entstammt.

Ein Nachteil des so definierten Konzepts ist, dass es, wie alle mentalen Modelle, schwer messbar ist [31,33]. Verbreitete, auf Introspektion basierende Fragebogen-

konzepte scheinen hier schwer umsetzbar. Vielmehr kann man Spuren mentaler Modelle am ehesten durch Beobachtung von Handlungen zeigen [22]. Aus diesem Nachteil ergibt sich direkt die Forderung, dass sich das vorgestellte Konzept empirisch bewährt, beides zusammen ist Gegenstand zukünftiger Forschung.

Das Security Awareness-Konzept ist hilfreich für Praktiker, weil es stark an der Handlung der Mitarbeiter orientiert ist und diese erklären hilft. Darüber hinaus können Schulungsmaßnahmen mit Hilfe des Modells besser beschrieben und somit koordiniert werden. Aus wissenschaftlicher Sicht hilft es, einige, mit der bisherigen Konzeptualisierung verbundenen Widersprüche, wie bspw. die vermeintlich niedrige Awareness von Innentätern zu überwinden. Zudem ist das Konzept differenzierter, so dass ebenfalls genauer adressiert werden kann, was Kern der Analyse ist.

Literatur

1. Puhakainen, M.: A design theory for information security awareness. Faculty of Science, University of Oulu, Oulu (2006)
2. Chen, Y., Ramamurthy, K., Wen, K.-W.: Organizations' Information Security Policy Compliance. Stick or Carrot Approach? Journal of Management Information Systems 29, 157–188 (2012)
3. PwC: Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015, www.pwc.com/gsiss2015
4. Puhakainen, M., Siponen, M.T.: Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly 34, 757–778 (2010)
5. Häussinger, F., Kranz, J.: Antecedents of Employees' Information Security Awareness - Review, Synthesis, and Directions for Future Research. In: Proceedings of the Twenty-Fifth European Conference on Information Systems (ECIS) (2017)
6. Karjalainen, M., Siponen, M.: Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. Journal of the Association for Information Systems (JAIS) 12, 518–555 (2011)
7. D'Arcy, J., Hovav, A., Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse. A Deterrence Approach. Information Systems Research 20, 79–98 (2009)
8. Whitman, M.E., Townsend, A.M., Aalberts, R.J.: Information Systems Security and the Need for Policy. In: Dhillon, G. (ed.) Information Security management: Global Challenges in the New Millennium, pp. 10–20. IGI Global, Hershey (2001)
9. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. MIS Quarterly 34, 523–548 (2010)
10. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8, 31–41 (2000)
11. Balozian, P., Leidner, D.: IS Security Menace: When Security Creates Insecurity. In: Proceedings of the 37th International Conference on Information Systems (ICIS) (2016)
12. Hellquist, F., Ibrahim, S., Jatko, R., Andersson, A., Hedström, K.: Getting their Hands Stuck in the Cookie Jar - Students' Security Awareness in 1:1 Laptop Schools. International Journal of Public Information Systems 9, 1–19 (2013)

13. Rastogi, R., von Solms, R.: Information Security Service Branding – beyond information security awareness. SYSTEMICS, CYBERNETICS AND INFORMATICS 10, 54–59 (2012)
14. Wilson, M., Hash, J.: Building an Information Technology Security Awareness and Training Program. NIST - National Institute of Standards and Technology, Gaithersburg (2003)
15. Banerjee, C., Banerjee, A., Murarka, P.D.: An Improvised Software Security Awareness Model. International Journal of Information, Communication and Computing Technology 1, 43–48 (2013)
16. Banerjee, C., Pandey, S.K.: Research on software security awareness: Problems and Prospects. SIGSOFT Software Engineering Notes 35, 1–5 (2010)
17. Choi, N., Kim, D., Goo, J., Whitmore, A.: Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Information Management & Computer Security 16, 484–501 (2008)
18. Spears, J.L., Barki, H.: User Participation in Information Systems Security Risk Management. MIS Quarterly 34, 503–522 (2010)
19. Blankert, S., Doubrawa, E.: Lexikon der Gestalttherapie. Peter Hammer Verlag, Wuppertal (2005)
20. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security 32, 90–101 (2013)
21. Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors 37, 32–64 (1995)
22. Richter, S.: Kommunikation und Performanz in Command & Control Teams. Eine Analyse von World of Warcraft(TM)- und Battlefield 2(TM)-Teams. WiKu, Duisburg, Köln (2014)
23. Richter, S., Lechner, U.: Transactive Memory Systems and Shared Situation Awareness: A World of Warcraft Experiment. In: Proceedings of the International Conference on Organizational Learning, Knowledge and Capabilities (OLKC) (2009)
24. Hänsch, N., Benenson, Z.: Specifying IT Security Awareness. In: 25th International Workshop on Database and Expert Systems Applications (DEXA), pp. 326–330 (2014)
25. Krcmar, H.: Informationsmanagement. Springer Gabler, Berlin, Heidelberg (2015)
26. Suddaby, R.: Editor's Comment: Construct Clarity in Theories of Management and Organization. Academy of Management Review 201035, 346–357 (2010)
27. North, K.: Wissensorientierte Unternehmensführung. Wertschöpfung durch Wissen. Gabler, Wiesbaden (2011)
28. Mathieu, J., Maynard, M.T., Rapp, T., Gilson, L.: Team Effectiveness 1997-2007: A Review of Recent Advancements and a Glimpse Into the Future. Journal of Management 34, 410–476 (2008)
29. Wegner, D.M.: A Computer Network Model of Human Transactive Memory. Social Cognition 13, 319–339 (1995)
30. Wegner, D.M., Erber, R., Raymond, P.: Transactive memory in close relationships. Journal of Personality and Social Psychology 61, 923–929 (1991)
31. Klimoski, R., Mohammed, S.: Team Mental Model. Construct or Metaphor? Journal of Management 20, 403–437 (1994)
32. Siponen, M.T.: Five dimensions of information security awareness. Computers and Society 31, 24–29 (2001)
33. Mohammed, S., Klimoski, R., Rentsch, J.R.: The Measurement of Team Mental Models: We Have No Shared Schema. Organizational Research Methods 3, 123–165 (2000)

Sammlung geleakter Identitätsdaten zur Vorbereitung proaktiver Opfer-Warnung

Timo Malderle[1], Matthias Wübbeling[1,2], Michael Meier[1,2]

1 Universität Bonn, Bonn, Deutschland
{malderle|wuebbeling|mm}@cs.uni-bonn.de
2 Fraunhofer FKIE, Bonn, Deutschland
{vorname.nachname}@fkie.fraunhofer.de

Abstract. Identitätsdiebstahl ist eine häufige Folge digitaler Einbrüche bei Unternehmen und dem anschließenden Entwenden von Mitarbeiter- oder Kundendaten. Kriminelle erbeuten Identitätsdaten, um sie als Sammlungen an potenzielle Betrüger zu verkaufen oder aber sie selber zu benutzen. Die Warnung von Betroffenen nach einem Identitätsdiebstahl ist notwendig. Es gibt bereits verschiedene Dienste, bei denen sich Identitätsinhaber über den Status ihrer verwendeten Identitäten informieren können. Eine proaktive Warnung von potenziellen Opfern solcher Betrüger gibt es bisher jedoch nicht. Damit die Betroffenen zeitnah benachrichtigt werden können, müssen zunächst geleakte und verfügbare Daten vorliegen. Diese Arbeit präsentiert eine Methodik zur Sammlung aktueller Identitätsdatenleaks zur Vorbereitung proaktiver Opfer-Warnung.

Keywords: Identitätsdiebstahl, Identitätsdatenleaks, Cyber-Crime, Identitätsbetrug, proaktive Opfer-Warnung

1 Einleitung

Jeder Internetnutzer verwendet gewöhnlich mehrere Online-Dienste wie Foren, Socialmedia-Plattformen oder Online-Shops [1]. Bei diesen Diensten besitzt er zumeist ein eigenes Benutzerkonto, welches in den meisten Fällen eine E-Mail-Adresse und das gewählte Benutzerpasswort enthält [2]. Das Benutzerkonto stellt eine digitale Identität des Benutzers dar, wobei der Benutzer zum Identitätsinhaber dieser digitalen Identität wird. Jeder Benutzer kann bei unterschiedlichen Diensten verschiedene Identitäten besitzen. Digitale Identitäten sind für Kriminelle von großem Interesse, um sie für betrügerische Aktivitäten zu verwenden. In der Vergangenheit wurden immer wieder großen Mengen digitaler Identitätsdaten illegal kopiert und für jegliche Art von Betrug verwendet. In den meisten Fällen bemerken die betroffenen Identitätsinhaber erst sehr viel später, dass sie Opfer einer Straftat geworden sind. Häufig werden gestohlene Identitäten nicht nur für einen klassischen Betrug missbraucht, sondern verkauft oder für eine breite Masse zugänglich im Internet veröffentlicht. Dadurch wird das Risiko für den Identitätsinhaber deutlich erhöht, weil eine größere Anzahl potenzieller Betrüger Zugang zu den Identitätsdaten erhält. Es existiert nicht nur die Gefahr, dass

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

gestohlene Zugangsdaten für kriminelle Zwecke missbraucht werden, sondern es bestehen zusätzlich datenschutzrechtliche Risiken. Verschiedene digitale Identitäten einer Person könnten unter Umständen miteinander verknüpft werden, um ein umfassendes Profil des einen Benutzers zu erhalten [3].

Deshalb ist es erstrebenswert, den betroffenen Identitätsinhaber über eine Entwendung seiner Identitätsdaten zu informieren, so dass präventive, bzw. reaktive Maßnahmen eingeleitet werden können. Da sich nicht jeder Webdienst neben seiner Haupttätigkeit mit der kontinuierlichen und aufwändigen Analyse von Identitätsdatenleaks und der Benachrichtigung seiner Benutzer beschäftigt und dies aus datenschutzrechtlichen Gründen vermutlich auch nicht darf [4], ist es sinnvoll, einen Dienstleister zu etablieren, der Privatpersonen und Unternehmen über Identitätsdatenleaks mit deren Identitäten informiert.

Für eine solche Benachrichtigung müssen mehrere Verarbeitungsschritte durchlaufen werden. Zunächst müssen gewöhnliche Quellen für Identitätsdatenleaks, sogenannte Datensenken, identifiziert werden. Anschließend werden die verfügbaren Daten aus den Datensenken geladen und ausgewertet, um auf dieser Grundlage gezielte Maßnahmen durchführen und Warnungen gegenüber dem Identitätsinhaber aussprechen zu können.

Die Basis dieser Warnungen bildet die Auswertung der Daten aus der Datensenke und somit das Wissen, welche Identitätsdaten entwendet wurden und öffentlich erreichbar sind. Problematisch hierbei ist, dass nicht alle Datenleaks ohne monetäre Gegenleistung veröffentlicht und herausgegeben werden. Beispielsweise werden manche Datenleaks auf dem Schwarzmarkt verkauft. Denkbar ist aber auch, das Datenleaks gar nicht veröffentlicht, sondern nur im Verborgenen missbraucht werden.

Die vorliegende Ausarbeitung beziffert die Menge frei verfügbarer Identitätsdatenleaks und analysiert den Aufwand, der für die kontinuierliche Beschaffung solcher Daten notwendig ist. Dazu wird eine systematische Herangehensweise gewählt, so dass zunächst existierende Datensenken identifiziert und anschließend die darin enthaltenen Daten beschafft werden. Zusätzlich wird untersucht, wie der beschaffte Datenbestand auch zukünftig aktuelle Daten integrieren und vorhalten kann. Diese Methodik wird zusammenfassend dargestellt.

Die Sammlung und Auswertung von Identitätsdatensätzen ist aktueller Forschungsgegenstand des Forschungsprojektes Effektive Information nach digitalem Identitätsdiebstahl (EIDI), das vom Bundesministerium für Bildung und Forschung gefördert wird. Das nachfolgende Kapitel 2 beschreibt verwandte Arbeiten im Bereich der Aufklärung von Identitätsdatendiebstahl. In Kapitel 3 wird die Sammlung von Datenleaks beschrieben, die anschließend in Kapitel 4 analysiert werden. In Kapitel 5 wird die Aktualität von Datenleaks und Identitätsdaten thematisiert, während Kapitel 6 das Modell der perpetuellen Datensammlung präsentiert. Kapitel 7 fasst die Ergebnisse zusammen und gibt einen Überblick über weitere geplante Arbeiten.

2 Verwandte Arbeiten

Dienste, wie *have i been pwned* [5], *Vigilante.pw* [6], *Hacked-Emails* [7], aggregieren große Datenmengen von Identitätsdatenleaks, damit Personen sich über die Betroffenheit der Datenleaks informieren können. Diese Dienste legen allerdings nicht offen, wie sie vorgehen, um an Sammlungen geleakter Daten zu gelangen.

Ein anderer Dienst, der zum Erhalt von Sammlungen genutzt werden kann und der häufig von Diensten der vorgenannten Art genutzt wird, ist *dumpmon* von Wright [8]. Dumpmon durchsucht Paste-Websites wie *Pastebin* [9] nach bestimmten Mustern, beispielsweise Emailadressen und Passwort-Hashes, um so Einträge (Pastes) mit Identitätsdaten zu erkennen. Anschließend informiert der Twitter-Account des Dienstes über entdeckte Identitätsdaten-Sammlungen. Die genutzte Software ist Open-Source und kann für eigene Projekte verwendet werden. Dieser Ansatz wird im Rahmen des vorliegenden Projekts als Einstieg genutzt, um weitere Arten an Datensenken einzubinden.

Verwandte Arbeiten im Bereich der Opfer-Warnung in Deutschland ist der *Identity-Leak-Checker* des Hasso Plattner Instituts (HPI) [10] und der *BSI Sicherheitstest* des Bundesamts für Sicherheit in der Informationstechnik (BSI) [11]. Beide bieten ähnliche Funktionen wie die bereits erwähnte Website *have i been pwned*. Nach der Angabe einer E-Mail-Adresse werden Informationen über die Existenz dieser E-Mail-Adresse in den verfügbaren Datensammlungen per E-Mail zugesandt. An dieser Stelle lassen sich mehrere Schwächen dieser Dienste aufzeigen. Potenziell betroffene Personen müssen diese Dienste kennen und zusätzlich regelmäßig nutzen. Problematisch ist auch, dass diese Dienste die in ihrem Datenbestand existierenden Identitätsdatenleaks nicht nennen. So kann nicht überprüft werden, ob ein solcher Dienst über aktuelle Datenleaks informieren kann. Eine Erweiterung dieser Dienste mit proaktiver Opfer-Information ist den Autoren nicht bekannt.

3 Die Sammlung von Datenleaks

Zur umfassenden Warnung betroffener Identitätsinhaber müssen ausreichend Daten vorliegen. Um die Handhabbarkeit und Skalierbarkeit der Daten als auch des Systems zu gewährleisten, wird eine Automatisierung angestrebt. Zusätzlich soll in einem gewissen Maße dafür gesorgt werden, dass der Datenbestand aktuell gehalten wird, um bei neuen Bedrohungen schnellstmöglich zu reagieren. Dazu werden zunächst existierende (halb-) öffentlich Datensenken analysiert, um anschließend die darin enthaltenen Daten für weitere Analysen zu sammeln.

3.1 Kategorisierung von Datensenken

Eine große Anzahl digitaler Identitäten werden regelmäßig von kriminellen Angreifern entwendet. In manchen Fällen werden die entwendeten Daten unmittelbar von diesen Angreifern genutzt, um betrügerische Handlungen durchzuführen. Oftmals

werden die Daten jedoch nicht von den Angreifern selbst genutzt, sondern vor der Nutzung durch Datenhehler weitergereicht oder verkauft.

Eine weitere mögliche Verwendung dieser Daten durch Kriminelle ist die Veröffentlichung, um eine Steigerung der eigenen Reputation in (cyber-) kriminellen Kreisen zu erlangen.

Geleakte Daten werden meist über eine sogenannte Datensenke verbreitet. Eine Datensenke ist der Dienst oder Speicherort im Internet, an dem Datenleaks gehandelt oder hinterlegt, beziehungsweise allgemein verfügbar gemacht werden. Datensenken können (halb-) öffentlich oder auf einen bestimmten Personenkreis beschränkt sein. Da diese Definition von einer Datensenke sehr umfassend ist, bedarf es zunächst einer Kategorisierung, um die Eigenschaften der jeweiligen Datensenke besser darstellen zu können. Dazu können Datensenken in die folgenden zwei Kategorien unterteilt werden: Automatisiert auffindbare Datensenken und Datensenken, die manuell identifiziert werden müssen.

Automatisiert auffindbare Datensenken sind beispielsweise einzelne Einträge auf *Paste-Pages* [12], wie *Pastebin* [9], über die sämtliche Arten von Texten mit anderen Personen geteilt werden können. Diese Paste-Pages werden häufig von Kriminellen dazu genutzt, Identitätsdaten aus Datenleaks zu teilen. Dabei kann die URL, die auf den jeweiligen Eintrag einer solchen Paste-Page verweist, als Datensenke bezeichnet werden. Viele dieser Paste-Pages bieten die Möglichkeit, neueste Veröffentlichungen anderer Benutzer einzusehen. Diese Funktion wird genutzt, um durch regelmäßiges Abrufen des Dienstes die relevanten Inhalte mit Identitätsdaten zu erhalten. Dazu werden alle neuesten unbekannten Einträge abgerufen und nach bestimmten Mustern, wie E-Mail-Adressen, durchsucht. Das Softwareprojekt *dumpmon* setzt diesen Ansatz um [8].

Manuell zu identifizierende Datensenken zeichnen sich dadurch aus, dass diese mit deutlich höherem Aufwand aufzufinden sind. Um Zugang zu diesen Datensenken zu erhalten, muss beispielsweise zunächst ein Hackerforum besucht werden. Dazu müssen häufig soziale oder semantische Hürden überwunden werden. Eine soziale Anforderung wäre, dass man von einem existierenden Forums-Mitglied geworben wird oder man in der Szene generell bekannt ist. Eine semantische Hürde könnte das Lösen von Captchas während der Registrierung sein. Diese Form der Identifizierung kann nicht ohne weiteres mit einem automatisierten Ansatz gelöst werden. Ein Grund dafür sind die divergenten Speicherorte, an denen die Datensenken abgelegt werden.

Mögliche weitere Speicherorte sind existierende *File-Hosting-Provider* [12], die anonymes Veröffentlichen von Dateien ermöglichen. Es können auch andere Teile des Internets als das Web verwendet werden, um Datenleaks zu verbreiten. Beispielsweise werden auch *BitTorrent* [12] oder das sogenannte *Usenet* genutzt. Diese Speicherorte können aufgrund ihrer Struktur und Datenmenge nur mit einem noch höheren Aufwand automatisiert ausgewertet werden. Für die Identifizierung solcher Datensenken benötigt es eine URL, die den Speicherort eindeutig beschreibt. Die URLs zu solchen Datensenken werden auf *Leak-Announcement*-Pages [12] weitergegeben. Dabei gilt es verschiedene Arten der Hinweis-Websites zu unterscheiden: Hacker Foren, Leak-Monitoring-Pages und Social Media [12].

Die Inhalte von Leak-Announcement-Pages verweisen per URL auf Speicherorte von Datensenken oder integrieren die Inhalte der Datensammlungen direkt. Leak-Announcement-Pages verwenden dabei verschiedene Sicherungsmechanismen, um die Inhalte zu schützen. Für den Zugriff bedarf es häufig der Registrierung eines Benutzerkontos. Dieser Vorgang ist meist durch Captchas gesichert und benötigt zusätzlich die manuelle Freischaltung durch einen Administrator des Dienstes. Die für die Registrierung genutzten E-Mail- und IP-Adressen können zur Ablehnung der Registrierung führen. Die tatsächlichen Kriterien sind den Autoren nicht bekannt. Nach der Freischaltung kann man je nach Dienst nicht alle Inhalte sofort einsehen. Eventuell wird eine soziale Beteiligung an den Inhalten des Forums gefordert. Beispielsweise müssen dann Beiträge zu Diskussionen oder eigene Datensammlungen veröffentlicht werden. In dem hier beschriebenen Projektkontext wurde eine Freischaltung nur mit gefälschten Dummydaten erreicht. Häufig hat dies allerdings zum zeitnahen Ausschluss aus dem jeweiligen Forum geführt, wobei erneute Versuche auch zum Erfolg führen können.

3.2 Identifizierung der Datensenken

Datensammlungen werden auf unterschiedlichen Wegen und von verschiedenen Kriminellen veröffentlicht. So tauchen Datensammlungen an verschiedenen Orten auf, an denen sie geteilt oder verkauft werden. Eine manuelle Recherche in gängigen Suchmaschinen identifiziert potenzielle Datensenken aus der Kategorie der manuell zu identifizierenden Datensenken. Weiterhin werden geeignete *Leak-Announcement-Pages* ermittelt. Insgesamt führt die Recherche zu einer Liste mit 15 solcher Dienste. Diese Liste wird gern auf berechtigte Anfrage zur Verfügung gestellt.

Gefundene Datensenken wurden in öffentliche, halböffentliche und geschlossene Datensenken eingeteilt. Öffentliche Datensenken sind solche, aus denen Datenleaks ohne die Überwindung technischer oder sozialer Sicherungsmaßnahmen entnommen werden können. Dagegen zeichnen sich halböffentliche Datensenken dadurch aus, dass sie eine zumeist soziale Sicherungsmaßnahme durchsetzen. Bei den gefundenen halböffentlichen Seiten war eine Registrierung notwendig, indem ein Benutzerkonto mit E-Mail-Adresse und Passwort angelegt wird. Weitere Angaben, zum Beispiel Name oder Anschrift, wurden nicht gefordert. Beide Formen erlauben eine (teil-) automatisierte Auswertung, wie in Abschnitt 3.1 dargestellt.

Geschlossene Datensenken sind solche Datensenken, die eine stärkere soziale oder technische Sicherungsmaßnahme umsetzen oder bei denen die Notwendigkeit eines finanziellen Aufwandes besteht. Natürlich wurden keine finanziellen Mittel oder realen personenbezogenen Daten als Tauschwährung aufgewendet. Eine automatisierte Auswertung ist dabei in der Regel nicht möglich.

Für die automatisierte Erfassung von Datenleaks werden folgende Dienste genutzt, von denen Identitätsdaten bezogen werden können: *pastebin.com*[8], *pastie.org*[8], *slexy.org* [8], *micropaste.com*, *siph0n.net*, *pastelink.net*. Dazu wurde das Programm *dumpmon* [8] angepasst und weiterentwickelt. Dieses Werkzeug ruft regelmäßig neueste Inhalte der genannten Dienste ab und speichert diese in einer Datenbank.

4 Analyse der Ergebnisse der gesammelten Daten

In diesem Abschnitt werden die erhaltenen Datensammlungen von den im vorigen Kapitel ermittelten Datensenken analysiert. Bei der manuellen Sammlung wurden insgesamt 520 Leaks aus den zuvor identifizierten Datensenken geladen. Insgesamt befinden sich in diesen Dateien 3.332.370.763 E-Mail-Adressen. Die Anzahl eindeutiger E-Mail-Adressen beträgt jedoch mit 1.563.002.958 etwas weniger als die Hälfte. Verwandte Dienste besitzen vergleichbar viele Daten. Der Dienst *have i been pwned* besitzt 4,72 Milliarden E-Mail-Adressen, wobei E-Mail-Spam-Listen ohne weitere Informationen wie Passwörter mit eingerechnet werden [5]. Der Dienst *Vigilante.pw* besitzt 3,56 Milliarden E-Mail-Adressen [6]. Dieser Vergleich zeigt, dass in diesem Projekt Identitätsdaten in der gleichen Größenordnung identifiziert und im weiteren Verlauf analysiert werden. Die mehrfache Speicherung von E-Mail-Adressen hat zwei Ursachen. Zum einen sind unter den Datenleaks auch sogenannte Combination-Lists, die eine Aggregation und Aufbereitung anderer Datenleaks darstellen. Zum anderen kann eine E-Mail-Adresse als Identitätsteil auch für mehrere Dienste verwendet werden und taucht somit in mehreren unterschiedlichen Datenleaks auf.

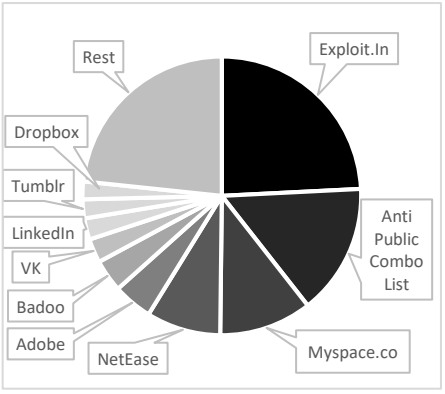


Abbildung 1. Anteile der einzelnen Leaks

In Abbildung 1 sind die Anteile der in der Datenbank enthaltenen E-Mail-Adressen dargestellt. Dabei werden die Top 10 Datenleaks getrennt und alle restlichen Datenleaks zusammengefasst dargestellt. Die Top 10 beinhalten zusammen 76,66 % aller gesammelten E-Mail-Adressen. Allein die drei Größten beinhalten mehr als 50 % der gesamten E-Mail-Adressen.

Bei der weiteren Analyse der einzelnen Datenleaks fallen stark unterschiedliche Formate der enthaltenen Daten auf. Es gibt offenbar kein einheitliches Format, das sich als De-facto-Standard durchgesetzt hat. Vielmehr stellt jeder Angreifer oder Datenhehler die Inhalte der Datensammlung in einem mehr oder weniger eigenen Format dar. Darüber hinaus gibt es Datensammlungen, die innerhalb einer einzigen Datei unterschiedliche Formate verwenden. Diese Tatsache deutet darauf hin, dass Inhalte verschiedener Sammlungen zusammengefasst wurden. Die verschiedenen Formate sind eine mögliche Hürde bei der automatisierten Syntaxanalyse.

Für die automatische Auswertung wird jeder Datensatz in einem Leak in mehrere Bereiche eingeteilt, abhängig von der jeweiligen Zeilenstruktur. Bei einer Analyse der vorhandenen Leaks wurde festgestellt, dass die Datensätze in den geleakten Dateien zumeist eine der folgenden Formen besitzen:

- email:password
- email:hash
- email:hash:cracked-password

- email:user:hash:salt
- userid:username:email:ip:hash:salt
- Gesamte SQL-Tabelle als CSV
- Ein kompletter SQL-Dump

Diese Auflistung zeigt die am häufigsten gefundenen Formate. Anstatt des in der vorherigen Auflistung genutzten Trennzeichens *Doppelpunkt* kann auch ein *Semikolon*, *Komma*, *Tab*, *\r*, *Leerzeichen* oder Ähnliches genutzt werden.

In Tabelle 1 sind die Identitätsdatenleaks mit den meisten E-Mail-Adressen absteigend aufgelistet. Die zweite Spalte der Tabelle zeigt den Dateinamen der Datensammlung. Die dritte Spalte listet die Gesamtsumme der E-Mail-Adressen auf, die in dem jeweiligen Datenleak zu finden sind. Die Spalte *TZ* zeigt das ermittelte Spaltentrennzeichen des Datenleaks und die letzte Spalte der Tabelle zeigt die Anzahl mit dem Spaltentrennzeichen gefundener Spalten. Diese können unterschiedliche Datentypen wie E-Mail-Adressen, Passwörter, Postadressen, Benutzernamen usw. beinhalten.

Tabelle 1. Top 10 der gesammelten Leaks

	Name des Leaks	*Summe E-Mail-Adressen*	*TZ*	*Spalten*
1.	Exploit.In	806581759	:	2
2.	Anti Public Combo List	506952026	:	2
3.	Myspace.com	358801827	:	5
4.	NetEase	287616356	:	2
5.	Adobe	152462193	|	6
6.	Badoo	125352387	[TAB]	8
7.	VK	92735323	:	2
8.	LinkedIn	82208762	:	2
9.	Tumblr	73357032	:	2
10.	Dropbox	68678625	:	2

Nach der Analyse der manuell gesammelten Daten, werden die automatisiert gesammelten Daten ausgewertet. Bei den genutzten Diensten, auf denen automatisiert aufzufindende Datensenken gespeichert werden, gibt es zum Teil die Möglichkeit, über eine API alle zuletzt veröffentlichten Pastes abzurufen. Diese Funktion wird genutzt, um möglichst viele vorhandenen Pastes abzurufen. Da dort alle Arten von Texten geteilt und veröffentlicht werden, muss zunächst eine Auswahl der für dieses Projekt relevanten Texte erfolgen, da die Menge zu speichernder Daten sonst zu umfangreich ist. Die Auswertung und Auswahl relevanter Pastes erfolgt mittels vordefinierter Muster in entsprechenden Suchausdrücken. Konkret muss ein Paste mindestens drei E-Mail-Adressen enthalten, um als relevant zu gelten, da eine geringere Anzahl an E-Mail-Adressen auf eine E-Mail-Kommunikation zwischen zwei Personen hindeutet

und es sich hierbei um keinen Leak handelt. Alternativ zu den E-Mail-Adressen können auch jeweils drei IBAN- oder Kreditkartennummern auftauchen.

Die verwendeten Paste-Sites liefern im arithmetischen Mittel 91 neue Pastes pro Tag mit relevanten Informationen, die entsprechend gespeichert wurden. In dem Zeitraum von April 2017 bis Juli 2017 wurden so insgesamt 8.562.237 E-Mail-Adressen aus den 12.011 gefundenen Pastes importiert. Der größte Anteil, nämlich 85,3 %, der gespeicherten Daten wurde über den Dienst Pastebin, weitere 13,9 % über Slexy verbreitet. Die restlichen 0,8 % teilen sich auf die restlichen Dienste auf. Die meisten identifizierten Datensammlungen werden über Pastebin veröffentlicht. Das liegt vermutlich daran, dass dies der bekannteste Dienst dieser Art ist. Die Struktur der Paste-Inhalte gleicht der, die von *manuell identifizierten Datenleaks* bekannt ist. Allerdings fällt auf, dass Pastes häufig zu Beginn oder Ende des Textes noch kurze Fließtextabschnitt besitzen. In diesen finden sich Hinweise zu den enthaltenen Identitätsdaten, zum Beispiel ob es sich um einen Ausschnitt handelt, der aus einem größeren Datenleak stammt. Der gesamte Datenleak ist dann über eine angegebene URL käuflich zu erwerben. Häufig fehlen aber konkrete Angaben zu den geleakten Daten, weshalb es unbekannt ist, von welchen Diensten diese Zugangsdaten ausgeleitet wurden.

Beim Vergleich der Ergebnisse beider Herangehensweisen zur Sammlung von Identitätsdaten fällt ein deutlicher Unterschied auf. Die manuelle Sammlung ergab 3.332 Millionen E-Mail-Adressen, während die automatisierte Herangehensweise im gleichen Zeitraum nur 8,5 Millionen E-Mail-Adressen hervorgebracht hat.

5 Modell zur Identitätsdatensammlung

Dieser Abschnitt stellt die Methodik aus vorigen Erkenntnissen des Ablaufs zum Sammeln von Identitätsdatenleaks dar.

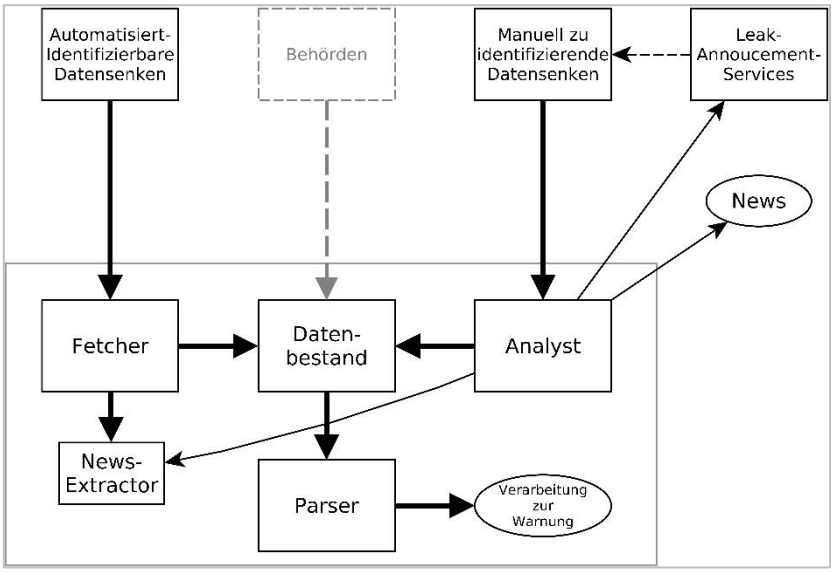


Abbildung 2. Modell zur Sammlung von Identitätsdatenleaks

Abbildung 2 zeigt die prototypischen Bestandteile des Prozesses zur Sammlung von Identitätsdatenleaks. Im oberen Teil der Abbildung sind die Quellen für die Identitätsdatenleaks dargestellt. Im linken Teil sind die *automatisiert identifizierbaren Datensenken* dargestellt, die regelmäßig von einem Softwaremodul mit der Bezeichnung *Fetcher* abgerufen werden. An dieser Stelle werden beispielsweise die letzten 100 Veröffentlichungen von Pastebin abgerufen und auf verwertbare Inhalte untersucht. Werden relevante Inhalte in einer Veröffentlichung gefunden, wird diese Veröffentlichung in der Projektdatenbank mit der Bezeichnug *Datenbestand* gespeichert.

Da *manuell zu identifizierenden Datensenken* nicht automatisiert gesammelt werden können, wird eine Person benötigt, die in dem Prozess als *Analyst* bezeichnet wird. Dieser recherchiert auf den *Leak-Announcement-Pages* relevante Datensammlungen. Werden relevante Inhalte gefunden, so kann der Analyst den Identitätsdatenleak über die gefundene URL aus der Datensenke herunterladen. Problematisch bei diesem Ansatz ist, dass aufgrund der manuellen Verarbeitung, die Daten in dem gepflegten *Datenbestand* nur schwer auf aktuellem Stand zu halten sind. Der *Analyst* muss entweder während der Recherche auf einer *Leak-Announcement-Page* einen neuen Datenleak ermitteln oder mit Hilfe einer externen Quelle über einen neuen Datenleak informiert werden. Dazu kommen beispielsweise Nachrichten-Websites, Blogs oder Twitter-Kanäle in Frage, die in der Abbildung mit *News* gekennzeichnet sind. Sollte

der *Analyst* durch *News* erfahren, dass ein neuer Identitätsdatenleak im Umlauf ist, so kann er gezielt nach diesem auf einer *Leak-Announcement-Page* suchen. Der *News-Extractor* hat die Funktion, automatisiert über neue Identitätsdatenleaks zu informieren. Dazu analysiert er den Fließtext der Pastes von Paste-Pages, falls dieser existiert. In diesem Fließtext wird, wie bereits erwähnt häufig auf weitere Daten des Identitätsdatenleaks verwiesen, da der vorliegende Paste nur eine Art Werbung bzw. Vorschau des gesamten Datenleaks darstellt. Diese Information kann genutzt werden, um den *Analysten* automatisch über neue Identitätsdatenleaks zu informieren.

Eine weitere Bezugsquelle für Identitätsdatenleaks kann auch durch Behörden dargestellt werden. Es ist denkbar, dass öffentliche Institutionen Interesse an der proaktiven Warnung betroffener Identitätsinhaber haben und deswegen Identitätsdatenleaks aus deren Besitz zur Warnung der Betroffenen zur Verfügung stellen.

6 Aktualität der Identitätsdatenleaks

Für die proaktive Warnung betroffener Identitätsinhaber ist es notwendig, die Aktualität eines vorliegenden Datenleaks zu bestimmen. Dabei muss die Aktualität differenziert betrachtet werden. Erstens ist die Aktualität des Datenleaks selbst von Interesse. Diese ist davon abhängig, wann die Daten von dem ursprünglichen legitimen Verwender kopiert wurden. Zweitens interessiert die Aktualität hinsichtlich der Verwendung durch Kriminelle, also Datenhehler oder Identitätsfälscher. Drittens ist die Identität der enthaltenen individuellen Datensätze relevant. Damit ist die Gültigkeit enthaltener Identitätsdaten gemeint, wie beispielsweise der E-Mail-Adresse oder eines Passworts. Die folgenden Abschnitte ermöglichen eine Unterteilung in Leak-Aktualität, Aktivitäts-Aktualität und Datensatz-Aktualität.

6.1 Leak-Aktualität

Die Aktualität des Datenleaks selbst lässt sich in den meisten Fällen nicht exakt datieren. Dies liegt daran, dass eine öffentliche Aufarbeitung von Datenleaks nur in seltenen Fällen stattfindet. Sobald aber eine Zuordnung eines Datenleaks zu einem in der Öffentlichkeit diskutierten Vorfall möglich ist, zum Beispiel Playstation-Network [13] oder Adobe [14], lässt sich über die Berichterstattung oft manuell eine entsprechende Datierung vornehmen. Wenn die enthaltenen Daten auch weiterführende Informationen zu den beschriebenen Accounts beinhalten, lässt sich beispielsweise über das Datum der letzten Benutzer-Anmeldung aller enthaltenen Identitäten eine zeitliche Eingrenzung vornehmen. Dies ist zum Beispiel im Falle des Last.fm-Datenleaks [5] möglich. Die neueste Anmeldung eines Benutzers ist in dem Datenleak auf den 22.03.2012 datiert, vermutlich wurden die Daten in unmittelbarer zeitlicher Nähe dazu entwendet. Somit ist eine näherungsweise Bestimmung der *Leak-Aktualität* möglich.

Die Information über die Aktualität des Datenleaks selbst lässt zunächst keine Rückschlüsse auf die Aktualität der enthaltenen individuellen Datensätze zu. Dafür ist eine weitere Betrachtung dieser notwendig.

6.2 Aktivitäts-Aktualität

Zur Bewertung des individuellen Risikos für Identitätsinhaber ist es notwendig, Informationen über die tatsächliche Nutzung von Identitäten aus einem Datenleak abzuschätzen. Nur, wenn die Daten tatsächlich noch aktiv durch Kriminelle genutzt werden, ist eine Information der betroffenen Identitätsinhaber sinnvoll. Wenn Datensammlungen beispielsweise im Rahmen einer Beschlagnahmung durch Strafverfolgungsbehörden analysiert werden, besteht theoretisch die Möglichkeit, dass die gefundenen Daten noch nicht an weitere Kriminelle weitergereicht wurden. Das Missbrauchspotenzial ist daher unmittelbar abhängig von der Weitergabe der Datensätze eines Datenleaks.

Innerhalb der vorgestellten Arbeiten werden ausschließlich aktiv geteilte Daten für die weitere Analyse verwendet. Es ist daher davon auszugehen, dass die enthaltenen Datensätze zu diesem Zeitpunkt auch für Kriminelle von Interesse sind und von diesen aktiv genutzt werden. Das Datum des Pastes, beziehungsweise des Forum-Beitrags auf dem ein Datenleak beworben wird, lässt sich daher als *Aktivitäts-Aktualität* verwenden.

6.3 Datensatz-Aktualität

Die Nutzbarkeit eines individuellen Datensatzes ergibt sich aus der tatsächlichen Aktualität der enthaltenen Informationen. Dabei wird zwischen *aktiver Nutzbarkeit* und *passiver Nutzbarkeit* unterschieden. Aktive Nutzbarkeit beschreibt die Möglichkeit für einen Identitätsbetrüger unmittelbar die beschriebene Identität missbräuchlich zu verwenden. Dafür sind Informationen über die ursprüngliche Verwendung der beschriebenen Identität sowie aktuelle Account-Informationen wie E-Mail-Adresse und Klartextpasswort notwendig. Es ist somit für den Angreifer möglich, sich bei dem Dienstanbieter anzumelden und den Dienst zu verwenden, was zu weiteren Möglichkeiten für den Identitätsbetrüger führen kann.

Die passive Nutzbarkeit ermöglicht einem Angreifer die Verwendung der enthaltenen Informationen zur mittelbaren Nutzung der dort beschriebenen Identität. Der Angreifer kann die enthaltenen Informationen nutzen, um im Namen des Identitätsinhabers weitere Accounts bei anderen Diensten zu registrieren und zu nutzen. Eine weitere Möglichkeit ist die Nutzung zur Passwort-Wiederherstellung. Häufig ist es dafür nötig, zusätzliche Informationen wie eine Kundennummer, Name und Vorname oder ein Geburtsdatum zu liefern, um ein neues Passwort setzen zu können. Auch die Antworten von zusätzlichen Sicherheitsfragen können grundsätzlich in Datenleaks enthalten sein und zum Account-Zugriff verwendet werden.

Um die Datensatz-Aktualität eines individuellen Datensatzes zu ermitteln, ist es notwendig, die aktive und passive Nutzbarkeit jedes Datensatzes weiter zu untersuchen. Eine Betrachtung der rechtlichen und technischen Möglichkeiten sind leider im

Rahmen dieses Beitrags aus Platzgründen nicht möglich, werden aber im weiteren Verlauf des Projekts intensiv betrachtet.

7 Zusammenfassung

Benutzerkonten und Zugangsdaten repräsentieren dienstspezifische digitale Identitäten der Nutzer von Internetdiensten. Über unterschiedliche Wege, z.B. durch Einbrüche in diensterbringende IT-Systeme, gelangen diese Identitätsdaten in unautorisierte Hände und werden für kriminelle Aktivitäten missbraucht oder von Datenhehlern handelsmäßig vertrieben. Im Zuge dieser Aktivitäten gelangen umfangreiche Sammlungen von Identitätsdaten oft für die breite Masse zugänglich ins Internet. Beispielsweise werden frei zugängliche Internetdienste zur Speicherung oder zum Austausch von Identitätsdaten als Datensenken für Identitätsdatensammlungen verwendet und missbraucht. Typischerweise erhalten betroffene Identitätsinhaber von diesen Vorgängen keinerlei Kenntnis und sind den resultierenden Bedrohungen weitgehend wehrlos ausgesetzt.

Mit der Vision diesen Missstand zu beseitigen systematisiert der vorliegende Beitrag die Abläufe und die beteiligten Dienste als auch Komponenten im Umfeld dieser Aktivitäten und schlägt einen Prozess zur systematischen Sammlung und Auswertung von Identitätsdatensammlungen zum Zweck der proaktiven Information betroffenen Identitätsinhaber vor. Dazu wurden unterschiedliche Arten von Datensenken und mögliche Strategien zur Datenauffindung und -sammlung untersucht sowie Herausforderungen beim Umgang mit variierenden Formaten der Inhalte von Identitätsdaten(-sammlungen) diskutiert. Die konzeptionellen Betrachtungen wurden mit der exemplarischen Analyse der Inhalte bereits aufgefundener Identitätsdatensammlungen untermauert. Gleichzeitig wurden offene Fragen zur Beurteilung der Aktualität von Identitätsdaten und damit der daraus resultierenden Bedrohung thematisiert.

Eine Schwierigkeit bei diesem hochgradig automatisierten Ansatz sind die Datenformate der Sammlungen, da sich diese stark voneinander unterscheiden. Es gibt keinen Standard, der sich für solche Datensätze durchgesetzt hat. Ein weiteres Problem ist, dass ohne weitere Informationen nichts über die Qualität der Daten ausgesagt werden kann, da es keine Anhaltspunkte über die Menge an gefälschten und nicht validen E-Mail-Adressen in den einzelnen Sammlungen gibt.

Zukünftige Arbeiten werden die inhaltliche Analyse der gesammelten Datenleaks thematisieren und die Problematik der Betroffenen-Identifikation adressieren. Dabei stehen anschließend die möglichen Kommunikationswege und das Design der Warnungen im Fokus der weiteren Untersuchungen. Die Autoren danken dem Bundesamt für Bildung und Forschung (BMBF) für die Förderungen des Projekts Effektive Information nach digitalem Identitätsdiebstahl (EIDI) unter dem Förderkennzeichen 16KIS0696K.

Literatur

1. Flo Encio, D., Herley, C.: A Large-Scale Study of Web Password Habits. WWW ’07. 16, 657–666 (2007).
2. Bonneau, J., Van Oorschot, P.C., Herley, C., Stajano, F.: Passwords and the Evolution of Imperfect Authentication. Commun. ACM. 58, 78–87 (2015).
3. Heen, O., Neumann, C.: On the Privacy Impacts of Publicly Leaked Password Databases. In: Polychronakis, M. and Meier, M. (eds.) DIMVA 2017. pp. 347–365. Springer, Cham (2017).
4. ULD - Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein: Kurzpapier Nr. 8 Maßnahmenplan „ DS-GVO “ für Unternehmen. In: DSK. pp. 1–3 (2017).
5. Hunt, T.: have i been pwned?, https://haveibeenpwned.com. (Sichtung: 28.11.17)
6. @vigilante: Vigilante.pw - The Breached Database Directory, https://vigilante.pw/. (Sichtung: 28.11.17)
7. Chia, J.M.: Hacked-Emails, https://hacked-emails.com/. (Sichtung: 28.11.17)
8. Wright, J.: Dumpmon, https://github.com/jordan-wright/dumpmon. (Sichtung: 28.11.17)
9. Pastebin: Pastebin, https://pastebin.com, (2017).
10. Hasso-Plattner-Institut für Digital Engineering gGmbH: HPI Leak Checker, https://sec.hpi.de/leak-checker, (2017). (Sichtung: 28.11.17)
11. Bundesamt für Sicherheit in der Informationstechnik: BSI-Sicherheitstest, https://www.sicherheitstest.bsi.de/. (Sichtung: 28.11.17)
12. Jaeger, D., Graupner, H., Sapegin, A., Cheng, F., Meinel, C.: Gathering and Analyzing Identity Leaks for Security Awareness. In: Mjølsnes, S. (ed.) PASSWORDS 2014. pp. 102–115 (2015).
13. Arthur, C., Stuart, K.: PlayStation Network users fear identity theft after major data leak, https://www.theguardian.com/technology/2011/apr/27/playstation-users-identity-theft-data-leak. (Sichtung: 28.11.17)
14. Hern, A.: Did your Adobe password leak? Now you and 150m others can check, https://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check. (Sichtung: 28.11.17)

Entwicklung eines Prototypen zur Steigerung der Effizienz im Umgang mit den KRITIS-relevanten ISO/IEC 27K-Normen für die Anspruchsgruppe ISMS-Mitwirkende

Philipp Schütz[1], René Treibert[1], Jaroslaw Kopowski[1]

[1] Hochschule Niederrhein University of Applied Sciences, Clavis - Kompetenzzentrum für Informationssicherheit, Mönchengladbach, Deutschland
{philipp.schuetz,rene.treibert}@hs-niederrhein.de {jaroslaw.kopowski}@stud.hn.de

Abstract. Die nationale Gesetzgebung hat mit dem IT-Sicherheitsgesetz für die Betreiber von Kritischen Infrastrukturen einen legislativen Rahmen geschaffen, welcher die gesellschaftlich relevanten informationstechnischen Infrastrukturen härten soll. Die Anforderungen dieses Gesetzes allokieren bei den Betreibern i. d. R. technische und organisatorische Ressourcen. Daher ist für die Betreiber eine effiziente Implementierung der gesetzlich induzierten Anforderungen, welche sich im Wesentlichen durch die Implementierung von Anforderungen aus der Norm ISO/IEC 27001 widerspiegeln, ein Erfolgsfaktor. Der Prototyp, als ein Artefakt des Erkenntnisprozesses aus Begleitforschungen bei KRITIS-Betreibern, soll die Implementierung durch eine Suche-sensitive Zusammenstellung der KRITIS-relevanten Normen effizienzsteigernd begünstigen.

Keywords: KRITIS, ISMS, ISO27k, ISO27k-Prototyp, ISO27k-Werkzeug, IT-Sicherheitsgesetz

1 Einleitung

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (folgend IT-SiG) vom 17. Juli 2015 finden derzeit und zukünftig umfangreiche, u. a. Gesetzgeber induzierte Aktivitäten zur Steigerung der Robustheit sog. 'Kritischer Infrastrukturen' (KRITIS) statt. Um einem Ausfall oder einer Beeinträchtigung entgegenzuwirken, hat das Bundesministerium des Inneren (BMI) eine Strategie zum Schutz Kritischer Infrastrukturen entwickelt.

Aus Sicht der durch quanitative und qualitative Schwellwerte zu determinierenden KRITIS-Betreiber, wie bspw. Energieversorgern, Wasserversorgern und Krankenhäusern, lässt sich der ökonomische Aufwand zur Erfüllung der Anforderungen aus dem IT-SiG im Wesentlichen durch die Aufwände der Implementierung eines ISO/IEC 27001-konformen

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Informationssicherheitsmanagementsystems (ISMS) quantifizieren. Je nach zu betrachtendem KRITIS-Sektor bzw. der zu betrachtenden KRITIS-Betreiber-Domäne werden die Anforderungen aus der ISO/IEC 27001 um domänenspezifische Informationen aus der ISO/IEC 27000-Familie (ISO27k) ergänzt.

2 Problemstellung und Lösungsansatz

Am Beispiel eines Energieversorgungsunternehmens (EVU) im KRITIS-Kontext bedeutet dies, dass ISMS-verantwortliche Akteure zur normgerechten Erfüllung der Anforderungen aus dem IT-SiG mindestens die folgenden Standards der ISO27k berücksichtigen sollten:

- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [1]
- ISO/IEC 27002 IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management [2]
- ISO/IEC 27005 Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement [3]
- ISO/IEC TR 27019 „Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [4]

Dies sind in Summe mehrere hundert Textseiten, welche jeweils miteinander pro Themenstellung und ISMS-Kategorie manuell miteinander zu verknüpfen sind.
Hier setzt die vorliegende Forschung an. Aus dem Erkenntnisgewinn von derzeit stattfindenden, anwendungsnahen Begleitforschungsprojekten bei KRITIS-Betreibern in den Sektoren ’Energie’ und ’Medizinische Versorgung’ lässt sich die Anforderung nach einer, durch Automatisierung gestützten, effizienteren Handhabung der ISO27k ableiten.

3 Konzeptionelles und erste prototypische Implementierung

Dieser Abschnitt skizziert ausgewählte Details zu den durch Begleitforschungen erhobenen Anforderungen der KRITIS-Betreiber. Des Weiteren gibt er erste Einblicke in die strukturelle Realisierung innerhalb der Problemdomäne ISMS-Implementierung, und den Modellierungsdetails, auf der Ebene der Persistenz des Prototypen. Außerdem veranschaulicht er anhand eines praxisüblichen Anwendungsszenarios den derzeitigen Stand der ersten Laufzeitversion des implementierten Prototypen. Subsumierend beansprucht das Bündel der Anforderungen eine effizientere Handhabung der ISO27k, für die Anspruchsgruppe ISMS-Mitwirkende. Dies wird aus der Perspektive des Benutzers durch eine Filter-sensitive ISO27k-Aggregation im Prototypen ermöglicht.

3.1 Prototypengestütztes Anwendungsszenario

Gemäß der Problemstellung aus Abschnitt zwei, verwendet der Benutzer in diesem praxisnahen Szenario den Prototypen um an Informationen aus den Normen zu gelangen. Der Benutzer, er sei ein Mitwirkender bei einem EVU, welcher im Zuge der ISMS-Implementierung die Anforderungen aus dem IT-SiG normenkonform umsetzen möchte. In einer Projektsitzung des EVU wird aus der ISO/IEC 27001 der Prüfbereich (engl. Control) "Änderungssteuerung" thematisiert. Anstatt der manuellen Aggregation der physisch oder digital vorliegenden, jeweils disjunkten, ISO-Normen 27001, 27002 und 27019 (ausgedruckt oder im PDF-Format) verwendet der ISMS-Mitwirkende den Prototypen. Zur Recherche innerhalb der ISO27k hat der Benutzer grundsätzlich drei Suchoptionen (siehe Abb. 1 Anwendungsfälle – ISO27K Recherche), welche jeweils den gleichen Suchraum, bestehend aus der relational-logischen Verknüpfung der ISO-Normen 27001, 27002, 27019 sowie 27799 traversieren.

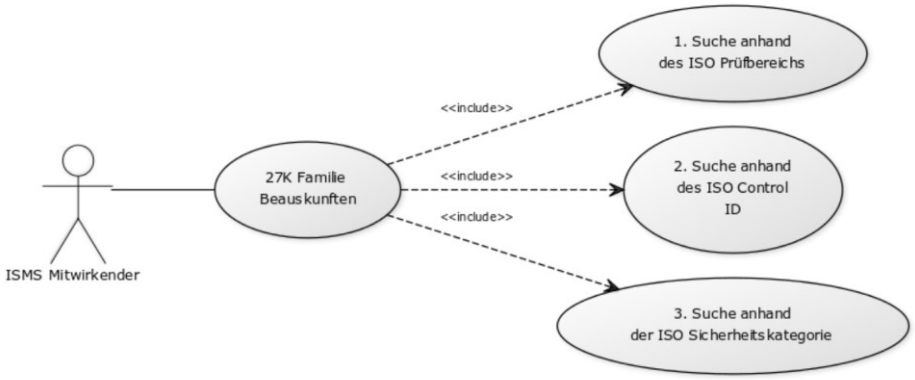


Abbildung 1. Anwendungsfälle – ISO27k Recherche

Anhand der Anwendungsfälle 1. und 2. wird das Anwendungsszenario folgend veranschaulicht.

3.2 Anwendungsfall 1: Suche anhand des ISO-Prüfbereichs

Der Benutzer wählt die ISO-Norm ‚ISO 27001' aus und hinterlegt im Suchfeld den Term „Änderungssteuerung". Die Ergebnismenge lautet: ‚Control-ID: A. 12.2.2 Änderungssteuerung'. Beim Anwählen des Hyperlinks erhält der Benutzer ein fachlich verknüpftes ISO27k-Aggregat der Inhalte, (siehe Abb. 4 Darstellung der aggregierten Ergebnismenge).



Abbildung 2. Anwendungsfall 1 – Suche anhand des ISO-Prüfbereichs

3.3 Anwendungsfall 2: Suche anhand der ISO Control-ID

Alternativ zum Anwendungsfall 1 hinterlegt der Benutzer (siehe Abb. 3 Anwendungsfall 2- Suche anhand der ISO Control-ID) im Suchfeld die Control-ID "12.1.2" zur Änderungssteuerung und wählt wieder die ISO-Norm "ISO 27001" aus. Beim Anwählen der Suche erhält der Benutzer die in der Abbildung 4 äquivalente Darstellung.



Abbildung 3. Anwendungsfall 2- Suche anhand der ISO Control-ID

3.4 Ergebnisdarstellung

Als Resultat der Suche nach der ISO-Control-ID "12.1.2" zur Änderungssteuerung bzw. der Suche nach dem Term "Änderungssteuerung" wird dem Benutzer in diesem Szenario das logisch verknüpfte Aggregat der ISO's 27001, 27002 sowie 27019 dargestellt (siehe dazu Abb. 4 Darstellung der aggregierten Ergebnismenge).

Die durch den Prototypen automatisierte Aggregation der Ergebnismenge aus den ISOs 27001, 27002 und 27019, in diesem Anwendungsfall für den KRITIS-Sektor 'Energie', führt zu erheblichen Effizienzsteigerungen in Form von Zeit, denn ISMS-Mitwirkende können sich innerhalb kürzester Zeit einen Überblick über die Inhalte und Zusammenhänge der ISO27k zusammenstellen.

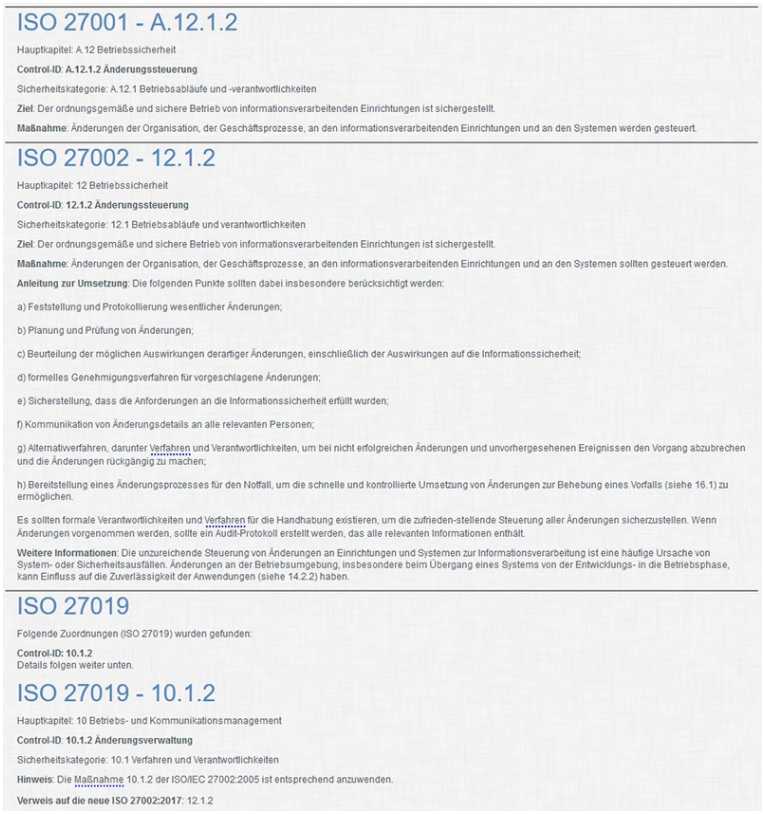


Abbildung 4. Darstellung der aggregierten Ergebnismenge,

Datenquellen [1,2,4]

3.5 Datenmodell in der Persistenz

Die folgende Tabelle 1 gibt eine Übersicht über die bereits im Prototypen implementierten ISO-Normen aus der ISO27k in der jeweiligen Version.

Tabelle 1. Im Prototypen bereits implementierte ISO-Normen der ISO27k

Norm	*Version*	*Thema*	*Internationale Norm*
ISO/IEC 27000	Juli 2011 (DE)	Überblick und Terminologie	ISO/IEC 27000:2009

ISO/IEC 27001	Juni 2017 (DE)	Anforderungen und Maßnahmen	ISO/IEC 27001:2013 einschließlich Cor1:2014 und Cor2:2015
ISO/IEC 27002	Juni 2017 (DE)	Leitfaden Maßnahmen	ISO/IEC 27002:2013 einschließlich Cor1: 2014 und Cor2: 2015
ISO/IEC 27019	März 2015 (DE)	Energieversorger	ISO/IEC TR 27019:2014
ISO/IEC 27799	Dezember 2016 (UK)	Med. Versorgung	ISO/IEC 27799:2016

Im Zuge einer Analyse wurde die ISO27k hinsichtlich ihrer Taxonomie, Verweisen, Erweiterungen sowie fachlichen Inhalten untersucht. Aus diesen Erkenntnissen wurde das relationale Datenmodell in der Abb. 5 des Prototypen iterativ entwickelt. Eine der Besonderheiten war die Implementierung der Zuordnungen der in der ISO/IEC 27019 auf die ISO/IEC 27002:2005 verwiesenen Anforderungen auf die derzeit geltende ISO/IEC 27002:2017 (DE). Im Datenmodell wird eine ISO in ihre Hauptbestandteile disaggregiert. Die ISO/IEC 27019 beispielsweise, dargestellt im Hauptentitätstypen , iso_27019‘, besteht aus den Bestandteilen (Entitätstypen): Hauptkategorie, Sicherheitskategorie, neu hinzugekommener Sicherheitskategorie und Anforderung, welche jeweils eine Erweiterung der ISO 27002 Anforderung oder eine neu hinzugefügte Anforderungen in der ISO/IEC 27019 sein kann. Die Zuordnungen (Mapping) der einzelnen Anforderungen wird im Entitätstypen “Mapping_19” im Datenmodell abgebildet. Diese Strukturwahl in der Modellierung lässt eine flexible Aggregation der Ergebnismenge zu, sowie die Integration weiterer ISO-Normen (siehe auch Abschnitt vier).

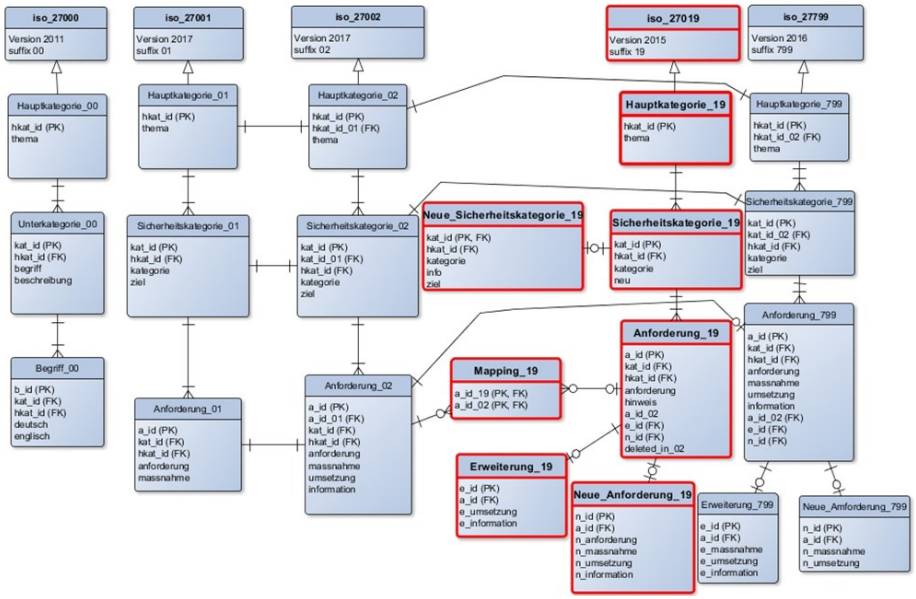


Abbildung 5. Ausschnitt des Datenmodells

3.

In Anlehnung an die normgerechten Aspekte zur Ergonomie der Mensch-System Interaktion [6] wurde am 09.11.2017 eine Erstevaluation mit einer qualifizierten Anspruchsgruppe von 13 Personen anhand des Awendungsszenarios aus den Abschnitten 3.1-3.4 durchgeführt. Die grundsätzliche Gebrauchsttauglichkeit wurde darin, relativ Ausgedrückt, mit 92,31 % bewertet. Ein Hinweis auf eine Optimierung der User Experience als Element der Zufriedenstellung war bspw., dass die Ergebnisdarstellung (siehe Abb. 4) auch hinweisgebender zwischen normativen und nicht-normativen Normen-Bestandteilen unterscheiden sollte. Neben der Gebrauchstauglichkeit wurden weitere Rückmeldungen innerhalb einer offenen Befragung in eine Residualkategorie aufgenommen. Als besonders dienliche, noch zu implementierende Funktionalität wurde eine globale Suche auf die ISO27k, unabhängig und additiv zu den Recherchemöglichkeiten geäußert (als Erweiterung der Anwendungsfälle aus Abb. 1).

4 Konklusion und Ausblick

Der ‚Research-in-Progress' Prototyp, als ein Artefakt der gestaltungsorientierten Wirtschaftsinformatik, gliedert sich in die derzeit zahlreichen Forschungsarbeiten im KRITIS-Komplex ein. Der momentane Fokus liegt auf der Anspruchsgruppe ISMS-Mitwirkende in den KRITIS-Sektoren ‚Energie' und ‚Medizinische Versorgung'. Eine Erweiterung der Funktionalitäten, bspw. zur Verwendung in allen KRITIS-Sektoren steht in Aussicht. Auch die Vergrößerung der Anspruchsgruppen, bspw. für ISMS-

Auditoren ist geplant. Bezogen auf die Phasen im Erkenntnisprozess, finden derzeit weitere Maßnahmen statt, um den Prototypen vertiefender zu evaluieren. Im 2. Quartal 2018 sollen die Funktionalitäten aus diesem Prototypen in einem weiteren, funktional umfangreicheren Prototypen, resultierend aus den Begleitforschungen, portiert werden. Dieser adressiert insbesondere EVU im KRITIS-Komplex und soll die Effizienz der ISMS-Implementierung und des ISMS-Betriebs begünstigen.

Literatur

1. ISO/IEC 27001 (2017) IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
2. ISO/IEC 27002 (2017) IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement
3. ISO/IEC 27005 (2011) IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement
4. ISO/IEC TR 27019 (2015) Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014)
5. ISO/IEC 27799 (2016) Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2016)
6. DIN EN ISO 9241-11 (2016) Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte

Forschungsprojekt zum digitalen Identitätsdiebstahl – Research in Progress –

Susan Gonscherowski[1], Fabian Rack[2], Oliver Vettermann[2]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstraße 98, 24103 Kiel
[2] FIZ Karlsruhe, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen

Abstract. Der Beitrag befasst sich mit den rechtlichen Rahmenbedingungen der Benachrichtigung von Opfern eines Identitätsdiebstahls. Für die Entwicklung eines Frameworks auf dessen Grundlage die Betroffenen proaktiv informiert werden können, sind zunächst die Anforderungen des Datenschutzrechts, Urheberrechts und sich daraus ergebende mögliche Kollisionen verschiedener verfassungsrechtlich geschützter Güter zu klären. Basis des Frameworks ist die Auswertung öffentlich zugänglicher Ansammlungen von Daten - den Datensenken. Diese enthalten personenbezogene Daten, welche für einen Identitätsdiebstahl missbraucht werden können. Denkbar ist jedoch auch, dass dem dadurch einschlägigen Datenschutzrecht das Grundrecht auf Informationsfreiheit gegenüberzustellen und entsprechend abzuwägen ist. Dient der Betrieb einer Datensenke der Sicherung des Lebensunterhalts und wurde die Senke als Bestandteil eines Geschäftsmodells erschaffen, spielen auch die zivilrechtlichen Erwägungen eine Rolle bei der Gestaltung des Frameworks.

Keywords: Digitale Identität, Identitätsdiebstahl, Datenschutz, Datensenken, Haftung

1 Einleitung

Das vorzustellende Projekt beschäftigt sich dem Titel gemäß mit dem Umgang von Opfern des digitalen Identitätsdiebstahls und einer Information ebendieser über den Verlust der Vertraulichkeit ihrer personenbezogenen Daten. Internetnutzer verfügen über diverse Teilidentitäten [1], die für die Nutzung verschiedener Dienste angelegt werden. Die Anmeldung bei diesen Diensten erfolgt häufig mittels E-Mail-Adresse/Benutzername und Passwort. Je nach Dienst sind weitere personenbezogene Daten im Benutzerkonto hinterlegt, z.B. Konto- oder Kreditkartennummer, Adresse, Telefonnummer, Name etc. Da Nutzer häufig dieselbe Authentifikation für mehrere Dienste (Online-Shopping, E-Mail-Postfach, Soziales Netzwerk) verwenden [2], stellt die Veröffentlichung nur weniger Informationen für den Betroffenen bereits ein hohes Risiko dar.

Aber nicht nur die Nutzer selbst, auch Unternehmen legen Teilidentitäten über Nutzer an. Auskunfteien erstellen umfangreiche Profile, die der Berechnung der

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Kreditwürdigkeit eines Kunden dienen. Die hier hinterlegten Informationen, wie Sozialversicherungsnummern, werden z.T. lebenslang vergeben und können nicht geändert werden. Für Angreifer bietet sich hier ein sehr lohnendes Ziel, denn die Daten veralten nicht und können auch als Identitätsnachweis dienen. Jüngstes Beispiel für die Brisanz dieser Problematik ist der Fall Equifax.[3] 44% der US-Amerikaner sind von diesem Datenraub bei der Wirtschaftsauskunftei betroffen und müssen nun damit rechnen, dass ihre Daten in betrügerischer Absicht missbraucht werden. Das Ziel des Projektes ist, eine effektive Nachbetreuung der Opfer zu ermöglichen und zukünftige IT-Sicherheitsvorfälle besser verhindern zu können. Zu diesem Zweck soll im Rahmen rechtlicher Gegebenheiten ein Software-Framework entwickelt werden, welches die Opfer unter Beachtung psychologischer Kenntnisse bzw. Standards in angemessener Weise informiert und Mittel und Wege des Umgangs mit dem digitalen Identitätsdiebstahl aufzeigt oder gar auf letzte Sicherungsmaßnahmen hinweist.
Bei der Untersuchung und Erarbeitung dieser Ziele betreuen die Projektpartner die rechtlichen Aspekte des vorzustellenden Projektes. Insbesondere stellen sich hier schon zu Beginn rechtliche Fragen, die bislang wenig geklärt sind – so zum Beispiel, inwieweit Datensenken und digitale Identitäten nach geltendem Recht geschützt sind und ob wissenschaftliche Untersuchungen diesbezüglich rechtmäßig sind oder sich in einer rechtlichen Grauzone bewegen.

Da das Projekt sich aktuell noch in Arbeit befindet, werden im Sinne eines Research in Progress nur erste Ergebnisse in rechtlicher Hinsicht dargestellt und mögliche, daraus resultierende, Fragen dargelegt. Der Fokus des Beitrags beschränkt sich daher auf die Datensenken und deren Betreiber im rechtlichen Kontext sowie auf rechtliche Beschränkungen bei der Verwertung von Datensenken zu unterschiedlichen Zwecken.

2 Der Begriff der Datensenke

Grundlegend ist zunächst der Begriff der Datensenke. Angelehnt an die Terminologie aus der Geologie, wo eine Senke jeden Ansammlungsort von geologischen Materialien meint, ist sodann auch hier der Ansammlungsort von Daten zu verstehen, wie sie beispielsweise bei Datenendeinrichtungen (kurz DEE) auftreten. [4] Eine derartige Datensammlung ist insbesondere ein Phänomen von Big Data, zeichnet sich also gerade durch willkürliche, ungeordnete „Datenhaufen“ aus. [5] Konkret entspricht eine Datensenke daher jedem Aufzeichnungsmedium, welches die Daten bis zum tatsächlichen Verarbeitungs- oder Verwendungszeitpunkt bereithält. [6] Datensenken sind daher nicht eindimensional, sondern können selbst zu einem späteren Zeitpunkt als Datenquelle verwendet werden. Ob es sich dabei um die Ursprungsquelle handelt, ist dagegen für den Begriff irrelevant.

Kern des geplanten Frameworks sind öffentlich zugängliche Datensenken, die personenbezogene bzw. personenbeziehbare Daten, wie E-Mail-Adressen (mit zugehörigen Passwörtern oder Hashes), Kreditkartennummern, Namen usw. enthalten. Diese Senken sind beispielsweise über Paste Pages, Foren, File Hosting-

Plattformen oder Leak Announcement Pages zu erreichen. Über diese Seiten werden regelmäßig entsprechende Daten veröffentlicht oder getauscht. Theoretisch können die Daten auch käuflich erworben werden. Auf diese Möglichkeit wird jedoch aus ethischen Gründen verzichtet, da fragwürdige Geschäftsmodelle nicht bestätigt werden sollen. Datensenken, die zur Veröffentlichung bestimmte Daten enthalten, wie beispielsweise Online-Telefonbücher, werden ebenfalls nicht berücksichtigt.

3 Verfassungsrechtliche Grundlagen

Dem Verfassungsrecht kommt diesbezüglich eine gewichtige Rolle zu, bildet es doch in der Normenhierarchie die Grundlage für die grundrechtskonforme Auslegung Anwendung von einfachgesetzlichen Vorschriften wie denen des Datenschutzrechts. Zunächst ist daher zu betrachten, inwieweit den Datensenken ein originärer grundrechtlicher Schutz zukommt. Die Frage stellt sich zwar nicht auf der Grundlage, dass Datensenken verfassungsrechtliche Rechtssubjekte sein könnten, da letztere nur natürliche Personen und juristische Personen des Privatrechts im Sinne des Art. 19 III GG sind. Ist die Datensenke allerdings einem oder mehreren Grundrechten zuzuordnen, so könnte derartigen Infrastrukturen im Rahmen von Schutzpflichten ein besonderer Schutz zukommen, welcher vom Gesetzgeber einzurichten ist. Kommt der Gesetzgeber diesem nicht nach, kann sich in Ausnahmefällen auch unmittelbar auf das Verfassungsrecht gestützt werden. [7] Im Rahmen der bisherigen Untersuchung ergab sich eine Zuordnung der Datensenke zur Rundfunk- und Pressefreiheit des Art. 5 I 2 GG, zur aus Art. 13 I GG folgenden Unverletzlichkeit der Geschäftsräume sowie dem IT-Grundrecht als Teilaspekt des allgemeinen Persönlichkeitsrechts gem. Art. 2 I i.V.m. 1 I GG.

Dem Schutz der Rundfunk- und Pressefreiheit aus Art. 5 I 2 GG ist die Datensenke insoweit zuzuordnen, als sie die Aussendung von Informationen an die Allgemeinheit enthält. [8] Die Schutzdimension der Datensenke erschöpft sich also in dem Informationsweg, also seiner Gewährleistung von der erstmaligen Entstehung bis zur Veröffentlichung, und weiteren Verwendung, einschließlich der Betriebs- und Geschäftsräume hinsichtlich des Redaktionsgeheimnisses. [9] Weiterhin erfasst Art. 5 I 2 GG auch den Informantenschutz [10], auf Ebene des Datenschutzes folglich den Status des Whistleblowers. Die Datensenke als Informationsmedium ist daher als (vorübergehender) Träger von Informationen, welche der Allgemeinheit zugänglich gemacht werden sollen, geschützt. Kaum anwendbar erscheinen hingegen die jeweiligen objektiv-rechtlichen Gewährleistungen, wie z.B. das Institut der freien Presse [11] oder die Programmfreiheit des Rundfunkanbieters [12].

Hinsichtlich der Privatheit der Kommunikation innerhalb der Geschäftsräume einschließlich der darin enthaltenen Speichermedien, welche letztlich die Datensenke in physischer Form darstellen, kann auch auf Art. 13 I GG zurückgegriffen werden. Schließlich ist der Schutz derartiger Räumlichkeiten, welche der Allgemeinheit nicht zugänglich sind, durch das Bundesverfassungsgericht anerkannt. [13] Sofern Eingriffe

im Sinne des Art. 13 II-V, VII GG drohen, ist Art. 13 I GG das gegenüber Art. 5 I 2 GG speziellere Grundrecht. [14]

Die Privatheit der Daten selbst und dahingehenden Restriktionen kraft verfassungsrechtlichem Datenschutz entspringen dagegen dem allgemeinen Persönlichkeitsrecht des Art. 2 I i.V.m. 1 I GG, insbes. dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Verwendet der Betreiber zur Absicherung seiner Daten bzw. Systeme entsprechende technische Mittel, z.B. eine Firewall oder andere Cybersecurity-Mittel, entspringt dem eine Indizwirkung: Hinter dem digitalen Schutzwall befinden sich Daten und Systeme, die es zu schützen gilt und dass in den Schutz und die Sicherheit vertraut wird. Gerade dieses Vertrauen in die Informationstechnik schützt die genannte Ausprägung des allgemeinen Persönlichkeitsrechts. [15] Der Gesetzgeber hat diesbezüglich einen weiten Gestaltungsspielraum, begrenzt durch Persönlichkeitsrechte Dritter bzw. den bestehenden Datenschutz. Werden Sicherheitslücken durch staatliche Maßnahmen aufrechterhalten, bestünde darin eine Grundrechtsverletzung.

Der Betreiber kann sich demgemäß auf das IT-Grundrecht aus Art. 2 I i.V.m. 1 I GG und andere dargestellte Grundrechte stützen. Nicht zu vergessen ist weiter, dass in Sonderkonstellationen auch den Betreiber verfassungsrechtliche Schutzpflichten treffen können. Grundsätzlich sind Grundrechte ausschließlich als Abwehrrechte gegen den Staat, die konkrete Ausgestaltung in Privatrechtsverhältnissen als Sache des Gesetzgebers zu verstehen. [16] „Je nach Gewährleistungsinhalt und Fallgestaltung kann die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates vielmehr nahe oder auch gleich kommen.“ [17] Im vorliegenden Falle bedeutet dies, dass – sollte sich die Gewährleistung eines Schutzes digitaler Identitäten und diesbezüglicher Datensenken aus einer verfassungsrechtlichen Schutzpflicht ableiten – auch private Unternehmen, welche den Schutz und damit staatliche Aufgaben übernehmen, unmittelbar grundrechtsgebunden sind. Dies kommt allerdings auf den Einzelfall der Ausgestaltung an.

Die erläuterten Aspekte führen allerdings zu neuen Teilfragen. So könnte zwar aus dem IT-Grundrecht für Datensenken-Betreiber folgen, dass sie zum Eigenschutz die Information ihrer Nutzer übernehmen – sofern es sich nicht um eine staatliche Aufgabe handelt. Letzteren Aspekt, also die mögliche Verpflichtung des Staates kraft Schutzpflicht, gilt es vertieft zu untersuchen. Des Weiteren ist das Verhältnis zwischen möglichen Hinweisgebern und der warnenden/informierenden Institution zu klären.

4 Datenschutzrechtliche Schutzaspekte

Auch wenn der Betrieb einer Datensenke durch das Grundgesetz geschützt ist, so ergeben sich aus den enthaltenen Daten möglicherweise Kollisionen mit anderen Schutzgütern des Grundgesetzes, bspw. mit dem Recht auf informationelle Selbstbestimmung, sofern personenbezogene Daten enthalten sind. In diesen Fällen wird eine Abwägung zwischen den Rechten des Datensenkenbetreibers und den Rechten der Betroffenen erfolgen müssen. Die Risiken für die Rechte und Freiheiten der Betroffenen sind den Interessen des Datensenkenbetreibers gegenüberzustellen. [18] In erster Linie ist der Zweck der Datensenke und damit der Datenverarbeitung zu betrachten. [19] In diesem Zusammenhang ist auch die Rechtmäßigkeit der Datenverarbeitung zu prüfen. Der Betrieb einer öffentlich zugänglichen Datensenke, die personenbezogene Daten enthält, ist nur unter bestimmten Bedingungen möglich. Entweder haben die Betroffenen in die Veröffentlichung eingewilligt (Art. 6 I a DSGVO) oder es gibt eine Rechtsvorschrift, die den Betreiber dazu berechtigt, z.B. eine Verpflichtung zur Veröffentlichung (Art. 6 I c DSGVO) oder ein berechtigtes Interesse des Verantwortlichen oder eines Dritten, gemäß Art. 6 I f DSGVO. [20]

Im Internet finden sich jedoch häufig Datensenken, die diese Anforderungen nicht erfüllen. [21] Derartige Datensenken stellen aufgrund ihrer öffentlich gemachten Inhalte stets eine Verletzung des Datenschutzrechts dar. Art, Umfang, Umstände und Zwecke der Verarbeitung führen zu einem hohen Risiko eines möglichen Missbrauchs, z.B. eines Identitätsdiebstahls. Da die Betroffenen in der Regel nicht über die Veröffentlichung ihrer personenbezogenen Daten informiert sind, werden sie sich des Missbrauchs erst bewusst, wenn sich dieser in Form von beispielsweise Mahnungen oder negativen Kredit-Scorings bemerkbar macht. Bis zu diesem Zeitpunkt können jedoch Jahre vergehen. [22] Die strafrechtliche Verfolgung wird durch diese z.T. sehr langen Zeiträume zwischen Datendiebstahl bzw. Missbrauch und Kenntnis des Betroffenen erschwert oder gar verhindert. Bisher gibt es nur wenige Angebote, die eine Möglichkeit bieten, entsprechende Senken zu durchsuchen und präventiv gegen einen Datenmissbrauch vorzugehen. Zudem verlangt dieses Vorgehen von den Betroffenen ein hohes Maß an Eigeninitiative. [23]

Im Rahmen des Projektes soll ein System entwickelt werden, das öffentliche Datensenken analysiert und die Ergebnisse so auswertet, dass bei einem hohen Risiko die Betroffenen proaktiv benachrichtigt werden. Ein entsprechendes Framework muss jedoch konzeptionell den Ansprüchen des Datenschutzrechts genügen. Für die Operationalisierung der gesetzlichen Vorgaben in konkrete Maßnahmen wird auf das Standard-Datenschutzmodell zurückgegriffen. [24] Dessen Schutzziel-Systematik erlaubt eine umfassende Analyse der durch die Datenverarbeitung bestehenden Risiken. Darüber hinaus sind für jedes Schutzziel bereits generische Maßnahmen formuliert, die weitere Eingriffe durch das Framework in die informationelle Selbstbestimmung der Betroffenen eliminieren oder wenigstens abmildern sollen. Da sich beispielsweise das hohe Risiko für die Rechte und Freiheiten natürlicher

Personen auf die Datenverarbeitung durch das Framework vererbt, ist wahrscheinlich eine Datenschutz-Folgenabschätzung gemäß Art. 35 I DSGVO vorzunehmen. Ziel ist es, den Betroffenen frühzeitig Interventionsmöglichkeiten zu geben Handlungsoptionen aufzuzeigen. Auf diese Weise können sie frühzeitig Gegenmaßnahmen einleiten und auch die straf- und zivilrechtliche Verfolgung würde erheblich vereinfacht.

5 Zivilrechtliche Anforderungen, Haftung der Akteure

Auch das Zivilrecht adressiert einige Fragestellungen an den Umgang mit Datensenken. Flankierend zum datenschutzrechtlichen Umgang mit Identitätsdaten stellt sich die Frage, inwieweit Identitätsdatensammlungen auch immaterialgüterrechtlich geschützt sind. Insbesondere ist hier an das komplexe und kleinteilige Datenbankschutzrecht sui generis zu denken, welches Datenbanken unter Investitionsschutz stellt und Entnahmehandlungen weitgehend verbietet. Die Frage ist deshalb wichtig, weil der Umgang mit Identitätsdatensammlungen in den meisten Fällen Kopien derselben erfordert und diese Kopien unter einem Lizenzvorbehalt stehen könnten. Gerade Akteuren, die Identitätsdatensammlungen untersuchen, ist hier an Rechtssicherheit gelegen. Dasselbe kann angenommen werden für Anbieter von Leak-Checkern, bei denen sich Betroffene aktiv informieren können, ob sie Opfer von Breaches geworden sind. Insgesamt sei als Tendenz vorgegriffen, dass der Datenbankschutz bei Identitätsdatensammlungen nur im Ausnahmefall greift. Sollten Sammlungen dennoch geschützt sein, wird untersucht, ob die genannten Akteure Schranken zu Gunsten der Wissenschaft oder der öffentlichen Sicherheit für sich in Anspruch nehmen können.

Ein weiterer Punkt ist die zivilrechtliche Haftung von Betreibern von Datensenken für das Vorhalten von Datensammlungen: Haften sie selbst auf Unterlassung und auf Auskunft; müssen sie Schadensersatz leisten? Hier sind medienrechtliche Haftungsmaßstäbe einzubeziehen.

6 Fazit

Die Information von Betroffenen eines Identitätsdiebstahls ist nicht nur unter datenschutzrechtlichen Gesichtspunkten zu betrachten. Andere grundrechtlich geschützte Schutzgüter sind in die Entwicklung eines entsprechenden Benachrichtigungssystems ebenso einzubeziehen, wie mögliche zivilrechtliche Haftungsrisiken, die sich aus der Auswertung von Datensenken ergeben können.

Verweise

1. Pfitzmann, Andreas/ Hansen, Marit: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity,

and Identity Management. Über: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (Aufgerufen am 27.11.2017).

2. Siehe Hasso-Plattner-Institut zur Mehrfachnutzung von Passwörtern, über: https://hpi.de/news/jahrgaenge/2016/sicherheitsrisiko-passwort-hpi-studie-zur-mehrfachnutzung-von-passwoertern.html (Aufgerufen am 27.11.2017).
3. Sokolov, Daniel: Hacker-Jackpot – Credit Bureau Equifax gehackt. Über: https://www.heise.de/newsticker/meldung/Hacker-Jackpot-Credit-Bureau-Equifax-gehackt-3824607.html (Zuletzt besucht am 14.11.2017).
4. Zum Begriff der Datenendeinrichtung siehe auch https://web.archive.org/web/20070928000507/http://www.tfh-berlin.de/~siegel/hypermed/netzd/netzd.htm (Aufgerufen am 28.09.2017).
5. So zumindest Hoeren, Thomas: Thesen zum Verhältnis von Big Data und Datenqualität. In: MMR 2016, 8 (8).
6. Microsoft Press - Computer Lexikon, 7. Auflage 2003, Begriff: Datensenke.
7. Klein, Eckart: Grundrechtliche Schutzpflicht des Staates. In: NJW 1989, 1633 (1636).
8. Zum Merkmal Schemmer in: Epping/Hillgruber (Hrsg.), BeckOK GG (Stand: 01.06.2017), Art. 5, Rn. 66 sowie 43; Kühling in: Gersdorf/Paal (Hrsg.) BeckOK InfoMedienR, Art. 5, Rn. 74.
9. Schemmer in: BeckOK GG, Art. 5, Rn. 44.
10. BVerfGE 107, 292 (329 f); 117, 244 (258 f).
11. Hierzu BVerfGE 20, 162 (175); 66, 116 (133).
12. Hierzu Schemmer in: BeckOK GG, Art. 5, Rn. 70 f.
13. Vgl. nur BVerfGE 120 274 (309).
14. Kloepfer, Michael: Verfassungsrecht, Band II, München 2010, § 66, Rn. 11.
15. Vgl. Gersdorf in: BeckOK InfoMedienR, Art. 2, Rn. 28, 29.
16. Zum Charakter der Grundrechte siehe BVerfGE 7, 198 (205).
17. BVerfGE 128, 226 (249).
18. Frenzel in: Paal/Pauly Datenschutz-Grundverordnung, Art. 6 Rn. 30 (BeckOK).
19. Frenzel in: Paal/Pauly Datenschutz-Grundverordnung, Art. 6, Rn. 27 (BeckOK).
20. Albrecht/ Jotzo: Das neue Datenschutzrecht der EU, Baden-Baden 2017, S. 52.
21. Vgl. hierzu exemplarisch für wiederkehrende Datenpannen Eikenberg, Ronald: Hetzner gehackt, Kundendaten kopiert. Über: https://www.heise.de/security/meldung/Hetzner-gehackt-Kundendaten-kopiert-1884180.html (Abgerufen am 28.09.2017)
22. Vgl. Schulzki-Haddouti, Christiane: Bayern: Gemeldete Datenpannen nehmen massiv zu über: https://www.heise.de/newsticker/meldung/Bayern-Gemeldete-Datenpannen-nehmen-massiv-zu-3643086.html (Abgerufen am 06.09.17).
23. Vgl. hierzu den Sicherheitstest des Bundesamtes für Sicherheit in der Informationstechnologie (https://www.sicherheitstest.bsi.de/) oder das Online-Angebot des Hasso-Plattner-Instituts (https://sec.hpi.de/leak-checker/search).
24. Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele V.1.0 – Erprobungsfassung von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern), Über: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V_1_1.pdf (Abgerufen am 14.11.2017).

Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share

Christian Sillaber[1], Clemens Sauerwein[1], Andrea Mussmann[1], and Ruth Breu[1]

[1] Universität Innsbruck, Department of Computer Science, Innsbruck, Austria
{firstname.lastname}@uibk.ac.at

Abstract. An increasing interest in Cyber Threat Intelligence (CTI) sharing platforms can be observed in research and practice. The main purpose of these platforms is to support the automated sharing, evaluation and dissemination of CTI, as well as the creation of inter-organizational sharing communities. Unfortunately, little is known about the added value these platforms provide to organizations as innovation in this area is mostly driven by vendors, and empirical studies are rare. In order to understand how these platforms provide value to organizations, we conducted a case study consisting of an exploratory survey and two focus group discussions with 17 stakeholders currently seeking to implement such a platform. The main goal of our research was to identify stakeholders' key expectations and types of information they are willing to share on a prospective CTI sharing platform. Building on these results, we propose a maturity model for CTI sharing platforms.

Keywords: Cyber Threat Intelligence Sharing, Threat Intelligence Data, Information Sharing, Case Study, Maturity Model

1 Introduction

In the past, organizations used ad-hoc solutions such as email, phone calls, or face-to-face meetings to disseminate cyber security-related information. Recently, a trend to form interconnected communities within and across organizational boundaries to manually and automatically exchange cyber security related information (e.g. Indicators of Compromise) can be observed [1-3]. As a reaction to this trend, software vendors and governmental institutions started to create offerings that facilitate this exchange and appear under the umbrella term *Cyber Threat Intelligence (CTI) Sharing Platforms* [4, 5]. For example, the government of the Netherlands has introduced a national detection, response, and expertise network [6], NATO has initiated the Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) project [7], and the Computer Incident Response Center Luxembourg (CIRCL) has developed the Malware Information Sharing Platform (MISP) [8]. Additionally, several standardization efforts (e.g. STIX, TAXII) to support automated CTI sharing gained traction in recent years [9-11]. Moreover, research and practice have shown that this type of exchange

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

presents a potential countermeasure against today's sophisticated cyberattacks, as not every organization has the resources to develop an adequate security program independently, and organizations can benefit from other organizations' experiences [3, 12, 13].

Today's commercial and non-commercial CTI sharing platforms embody three fundamental concepts to a greater or lesser degree: (a) Facilitate information sharing, (b) enable automation, (c) facilitate the generation, refinement and vetting of data through burden-sharing collaboration or outsourcing [1, 5, 7]. Unfortunately, little is known about the added value these platforms provide as empirical research in this area is almost non-existent and innovation is driven by vendors and technological trends [14]. Moreover, research in recent years has focused on fundamental concepts of CTI sharing platforms [7,15,16] without analyzing the value they provide. As a first step towards closing this gap, we seek to answer the following research question: *What are the capabilities and functionalities of CTI sharing platforms and what is the nature of provided CTI and different levels of maturity?* The goal of our research was therefore to investigate the expectations of stakeholders, especially early adopters, of CTI sharing platforms. Special focus was put on the specific artifacts that are shared and the participants' willingness to share them. Based on these investigations, a maturity model for CTI platforms was derived. This model can be used to measure the maturity and provided value of CTI sharing platforms to stakeholders and organizations.

The case study consisted of a series of focus group discussions and interviews with 17 stakeholders from 17 organizations that are planning to introduce a joint CTI sharing platform. The stakeholders represent 17 globally operating organizations and either directly work in their organization's security operations center or are the organization's chief information officer or chief information security officer.

Our research has shown that stakeholders of CTI sharing platforms expect the platforms to have automated sharing functionalities that facilitate the timely sharing of quantitative and qualitative CTI between participating organizations. Additionally, the platform should offer functionalities to control the information flow and provide trust metrics. In order to provide a comprehensive solution and increase the value of CTI sharing platforms for organizations, stakeholders emphasized the need of integrating external information sources, like vendor specific security advisories or mailing lists. Finally, based on these findings we introduced a model to measure the maturity of CTI sharing. The remainder of this paper is structured as follows. Section 2 provides related work regarding CTI sharing platforms and related studies. Section 3 outlines the underlying research methodology and procedure carried out. Section 4 presents the key findings. Section 5 discusses the results and derives a maturity model to evaluate the maturity level of CTI sharing platforms. Finally, section 6 concludes the paper and provides an outlook on future research.

2 Related work

Dandurand and Serrano were the first who formulated 11 high-level requirements for CTI sharing platforms [7]. Since then, several researchers identified further requirements and challenges for CTI sharing [1, 7, 15, 16]. Moreover, several author

introduced concepts or frameworks for cyber security information sharing [17, 18]. For example, in [17] the authors propose evolving procedures for organizations to advance and improve their cyber security information sharing maturity. However, none of these publications are based on empirical investigations. In addition, several efforts have been made to standardize CTI (e.g. STIX, TAXII, Open IOC) [9, 10, 19]. In 2016, for example, the National Institute of Standards and Technologies (NIST) published an official guide to cyber threat information sharing which is based more or less on these standardization efforts [11]. However, all these contributions introduce high level requirements without taking into consideration the individual stakeholders' expectations and reservations for such platforms.

Only a few empirical studies in the domain of CTI sharing can be identified. In [1], the requirements for a holistic CTI sharing platform based on a study of several market solutions are discussed. In prior work we discuss data quality challenges and future research directions in CTI sharing practice based on focus group interviews with security experts [14]. Murdoch and Leaver provide a case study on the UK government's cyber security information sharing partnerships and arising anonymity and trust issues [20]. Bhatia et al. conducted a survey of 76 security professionals in order to analyze the privacy risk and fears in cyber security data sharing across organizational boundaries [21]. Sauerwein et al. provided a comprehensive analysis and comparison of open and closed source inter-organizational CTI sharing platforms [5].

Maturity models have been proposed by researchers and practitioners across multiple domains to assist organizations with transformations or the introduction of new technologies [22]. By identifying predictable evolutionary stages, maturity models help describe anticipated or desired steps from an initial state of capabilities to a mature state of capabilities of a specific application domain [22, 23].

To the best of our knowledge, no prior empirical research has been conducted that takes into consideration the maturity and value of CTI sharing platforms based on stakeholders' expectations and their willingness to share CTI. Additionally, none of the aforementioned contributions introduces a model to measure the maturity and value of CTI sharing platforms.

3 Research Methodology

We conducted a case study with members of a security expert group developing a national CTI sharing platform in a central European country. The case study consisted of two parts that were conducted during the first half of 2016. At first, we conducted an exploratory survey which formed the basis of our subsequent focus group discussions and interviews. In order to ensure reproducibility, a research protocol was developed which consists of filled out questionnaires, survey results, workshop transcripts, and a list of participants. Following the basic design principles for maturity models, as proposed in [22], we limited the application domain of the maturity model to inter-organizational CTI sharing platforms. As the maturity model was developed in close collaboration with expert matter stakeholders, aforementioned documentation of interviews and discussions serves as documentation of the design process.

3.1 Participants of the Case Study

The case study was conducted with 17 domain experts from industry. Table 1 gives an overview of the participants, their roles, and the types of organization they are belonging to. The majority of participants work in major financial organizations. While all companies operate globally, one of them is small (<150 employees), four of them are medium (150-1000 employees), and 12 of them are large-sized organizations with more than 1000 employees each. Moreover, the composition of participants represents a mixture between employees that work directly in their organization's security operations center (e.g. security analysts) and persons who are members of the managerial level (e.g. chief information security officers). Finally, it is worth mentioning that four participants already use a threat intelligence sharing platform at their organization.

3.2 Explorative Survey

In order to reduce the possibilities of omitting important concepts and artifacts from our case study, we conducted an exploratory survey as a pre-study ([24, 25]). As part of this survey, the participants (see Table 1) were asked to state their expectations and requirements for a CTI sharing platform from the perspective of their role and organization's security operation center's processes. In addition, the participants were asked to specify what type of information and intelligence they are willing to share with other participants of such a platform. To bootstrap the thinking, we provided participants with an initial list of potential information and intelligence artifacts. This list was based on the "data types and elements of interest to members of the security operations team" presented in [11]. The participants were asked to classify the elements of the list based on the Traffic Light Protocol (TLP)[1], where elements can be marked as red (R), amber (A), green (G) or white (W). The color assigned to an information element defines how it may be shared within the CTI sharing platform. For example, information which is marked as red cannot be shared with any party outside of the original group of people the information provider chose to share it with. If an information element is marked as green, it can be shared with all participating organizations. The results of this survey were analyzed and formed the basis for the subsequent focus group discussions.

3.3 Focus Group Discussions

After analyzing the results of the exploratory survey, two focus group discussions [26] were conducted. The participants were the same as in the exploratory survey. The goal of the focus group discussions was to gain deeper insights in the stakeholders' valuation of CTI sharing platforms. Discussion topics were the stakeholders' expectations for such a platform, their willingness to share information, and the classification of information they are willing to share. The two focus group discussions were held in parallel at a neutral premise in 2016 and lasted roughly one and a half hour each. The

[1] 1https://www.us-cert.gov/tlp (Accessed: September 19th, 2017)

aim of these parallel discussions was to limit bias from other participants and get more meaningful results by cross-comparing the results. Before the two discussions started, all 17 participants were instructed by two researchers. Afterwards, two discussion groups were formed randomly, where each group consisted of eight to nine participants and one moderator. Every moderator was a researcher with expert knowledge in the field of CTI sharing platforms. Researchers asked questions during the discussions to clarify participants' statements and to refocus the discussion. Each workshop was recorded and transcribed. After the workshops, qualitative summaries were produced from the recordings [27] in order to derive the findings relevant to the research [28].

Table 1: Overview of the participants of the two focus group discussions.

ID	Organizational Role	Type of Org.	# of Employees	Use TISP
1	Security Analyst	Finance	> 1000	
2	Security Architect	IT	150-1000	X
3	Secuirty Analyst	Finance	> 1000	
4	Security Researcher	Education	< 150	X
5	CERT Member	Production	150-1000	X
6	Security Specialist	Finance	> 1000	
7	Security Task Force	Finance	150-1000	X
8	CSIRT Member	Finance	> 1000	
9	SOC Team Leader	-	< 150	
10	CISO	Insurance	> 1000	
11	CISO	Finance	> 1000	
12	CISO	Finance	> 1000	
13	Security Analyst	Finance	> 1000	
14	MSSP	IT	> 1000	
15	Head of SOC	Finance	> 1000	
16	Security Specialist	Finance	150-1000	
17	Security Consultant	Consulting	> 1000	

4 Study Results

From the analysis of the exploratory survey and focus group discussions, we gained insights into stakeholders' expectations and willingness to share information on a threat intelligence sharing platform. In the following section, we discuss them in detail.

Expectation 1: CTI sharing platforms must reach a critical mass. The interviewees stated that a critical success factor of a CTI sharing platform is the number of participating organizations and contributing branches from industry. In this context, nearly 80% of the interviewees agreed that they expect at least a certain number of participants within a platform which belong to their branch of industry and are located in their country. For example, the majority of study participants belonged to the financial sector and therefore it is not surprising that they primarily expected a certain number of financial institutions in their prospective CTI sharing platform. However, interviewees were not able to quantify the critical number of participants they expect. The remaining 20% of interviewees stated that they expect the participation of large and medium-sized organizations and a good mixture of business, academic and

governmental institutions. While we were not able to obtain quantifiable numbers either, these 20% of interviewees agreed that as many organizations as possible should participate.

Expectation 2: The shared CTI should be more current than conventional information sources and reduce the time to detect threats. All interviewees agreed that they expect the timely supply of actionable information in order to stay up-to-date regarding occurring threats and incidents. They assume that the necessary information can be obtained in real-time, is not outdated and is more current than information from conventional sources like vulnerability or exploit databases. Accordingly, they see great potential to reduce time to detect cyber threats and instantiate countermeasures more timely.

Expectation 3: A CTI sharing platform should offer social media and automated sharing functionalities. Nearly half of the interviewees stated that they expect social media functionalities. For example, they expect features similar to group chats, news streams, dashboards or forums. In this context, two interviewees remarked that a CTI sharing platform should be more a social media platform for information security experts than a data warehouse holding tons of e.g. indicators of compromise. They expect a lively community that shares indicators of compromise for emerging threats enriched with the collective knowledge and experiences of the participating experts. Moreover, five interviewees stated that they expect fast, easy to use and automated sharing capabilities. In this context, two interviewees mentioned that a notification feature regarding new threats or incidents would be desirable.

Expectation 4: CTI sharing platforms should implement functionalities to control what is shared with whom. Using the information from the interviews and the surveys we found that potential users expect control of information exchange and filtering of the received information. The interviewees emphasized that they attach importance on control mechanisms to guarantee the exchange of information with trustworthy participants and capabilities for anonymization or pseudonymization. They want to choose one-to-one or one-to-many information exchange depending on the sensitivity of information. For example, one interviewee stated that he wants to share information regarding a cyber attack with all participants of a platform if his organization is not directly targeted, but keep it confidential if required. In this context, one interviewee made the point that in this case it would be helpful to provide a functionality which enables anonymous sharing of information. Moreover, the interviewees emphasized the need for filtering and subscription functionalities. By using these functionalities, users of a CTI sharing platform can control the information flow and counteract information overload. For example, one participant of the workshops stated that too much information provided by such a platform would result in a lot of additional work to identify information relevant to a company and diminish the value of receiving the right information in time. The interviewees emphasized that functionality to filter for most serious attacks, industry, company size, region or country would be useful. In this context, four interviewees expected that a CTI sharing platform only delivers information which matches with their organization's infrastructure. For example, a company uses only operating system A, then the platform should provide all CTI regarding A and omit information regarding operating system B, which is not used.

Expectation 5: CTI sharing platforms should integrate external information sources. Half of the interviewees stated that they rely on external information sources, such as mailing lists, as part of their daily information security processes. Since they expect that a CTI sharing platform should be an all-encompassing information source to support their processes they emphasized the need of integrating external information sources. Information sources of interest are vulnerability databases, information security mailing list, exploit databases, information security expert blogs, vendor specific security advisories, bug repositories, malware and virus databases. Moreover, one interviewee suggested to establish connections to other CTI sharing platforms and support the information exchange with them. The interviewees reasoned that these external information sources would enrich existing CTI and would provide new security information for a CTI sharing platform.

Expectation 6: Stakeholders expect qualitative as well as quantitative information from a CTI sharing platform. During the workshops, a debate was sparked by the participants' different opinions about the nature of CTI. On the one hand, about 60% of the participants stated that they mainly expect quantitative information or rather technical information from a CTI sharing platform. For example, malicious URLs, malware samples, malicious IP addresses, file hashes, phishing emails or malicious email addresses. On the other hand, nearly 40% of the participants expect qualitative information from a threat intelligence sharing platform. They assume that plain technical information regarding threats can be derived from other information sources while such a platform provides qualitative threat intelligence based on knowledge sharing between organizations. From the interviewees' perspective, qualitative CTI consists of technical information regarding threats enriched with contextual information, and knowledge of other participating organizations. Moreover, qualitative information expands organizational knowledge based on experiences from other organizations, increases the interpret-ability of technical information and provides support for the implementation of proper countermeasures to handle specific threats.

4.1 Stakeholders' willingness to share CTI

The interviewees were asked to classify the information elements according to the respective categories of the Traffic Light Protocol (TLP) [11]: Red, Amber, Green, White and Anonymous. Red and Amber mark limited disclosure and restricted to members of the information exchange. Red is stricter and limits the access to representatives participating in the information exchange which have signed certain rules. Green means that information can be shared with all participating organizations on a CTI sharing platform and White means that the information is intended for public and unrestricted dissemination. Last but not least, Anonymous means that information can be publicly disclosed in an anonymized form. We found that the majority of information sharing elements of interest are marked with Red or Amber which means that stakeholders are willing to share this type of information merely in closed groups where they know each participating organization. During the workshops they argued that the unintentional disclosure of CTI to unknown third party organizations might damage the organization's reputation and put its business at risk. For example, one

interviewee stated that if his organization publicly discloses information about an encountered information leak it might harm the trust relationships with their customers. Another workshop participant added that it might not be beneficial if every competitor on the market is informed about an encountered attack since the competitors can use it to strengthen their market position and harm their competitor. In this context, the interviewees emphasized the need for mechanisms to control with whom the information is shared (c.f. Expectation 4). Moreover, our research showed that the interviewees are willing to share malware samples and artifacts with all participating organizations on a CTI sharing platform. This is understandable as malware samples and artifacts are not necessarily tied to the organization that found it. Few information elements were classified as "White', which means that the information is publicly available to everyone on the platform. This is not surprising since the participants of the study assumed that their prospective CTI sharing platform is closed to organizations within their security expert group. Hence, the platforms do not plan to provide access to third party organizations outside their community. Finally, the interviewees showed willingness to share some information in anonymized form; for example, SMTP headers, emails, captured packets, IP addresses or domain names, or any other information artifact potentially containing personal identifying information. During the workshops, we investigated this phenomenon in detail and the interviewees stated that they are willing to share these elements but they want to avoid traceability. For example, organization A shares the content of an Email of a phishing campaign. Then organization A does not want any other participating organization within the platform to trace it back to them.

5 Discussion

In the following Section we introduce a maturity model based on the results of the explorative survey and the focus group discussions. In addition, we provide a discussion on the limitations of the methodology used to conduct the research.

5.1 Towards a maturity model for CTI sharing platforms

Based on the focus group discussions, and analysis of literature in the field of CTI sharing, we developed a maturity model for CTI sharing platforms. This descriptive maturity model [23] can be used by organizations as a guiding framework to assess the maturity level of their CTI sharing efforts and to move to higher levels of maturity in a systematic and incremental way. Although the maturity model is developed mainly based on data from European financial organization, we believe that it can be used by government agencies or organizations from other domains without major modifications because the core principles and objectives of CTI sharing are the same. The maturity model is depicted in Figure 1. As an organization's CTI sharing effort moves to a higher maturity level, the organization's stakeholders are more engaged and the systems are better connected, thus a greater value for the organization is realized. However, a higher maturity level faces increased complexity and interdependencies which may lead to

greater challenges and risks. Based on the analysis of the CTI sharing platform market presented in [5], we conclude that most CTI sharing platforms cover maturity levels three and four. While we believe that, in principle, an organization should move sequentially through the proposed stages from the lowest to the highest maturity level, a combination of process improvement and adequate tool support will help organizations to "leapfrog" one or more maturity levels at once. By focusing on reaching one maturity level at a time, organizations can effectively build infrastructure, capabilities and knowledge without integrating complex software and joining large sharing communities all at once.

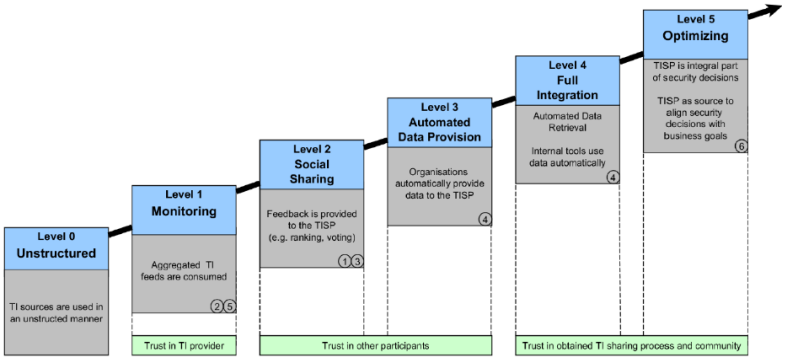


Figure 1: Maturity model for inter-organizational CTI (TI) sharing. (Remark: The numbers in the circles are referencing the respective expectations.)

Level 0: Unstructured Level 0 of the maturity model refers to an initial stage, where no or only some open CTI sources are used in an unstructured and unsystematic manner. A level 0 organization focuses primarily on reactive security and risk management activities and passively consuming information without contributing to the platform. It lacks a centralized, structured approach to collecting and organizing incoming CTI. A typical level 0 organization would have some members of the security and risk team subscribing to mostly technical newsletter, bulletin boards, etc. The utilization of this intelligence largely depends on the personal processes and willingness to share of some individuals.

Level 1: Monitoring: Level 1 represents the first step towards CTI sharing. Organizations at this level have a centralized CTI aggregator that collects incoming information for all team members (c.f. Expectation 5). The interaction is one way, but the organization disseminates the incoming intelligence in a structured way and reacts accordingly. Organizations that have reached this level have an advantage over those that manually collect, filter and process intelligence from conventional information sources and can therefore reduce the time to detect cyber threats (c.f. Expectation 2).

Level 2: Social Sharing: Organizations that have reached level 2 actively participate in an exchange with their peers. Incoming intelligence is disseminated, evaluated and manual feedback is provided through social media functions through e.g. sharing, voting or message based discussions (c.f. Expectation 3) with other participants of the platform. This increased dependency on other participants' feedback requires organizations at this level to trust other participants and the provided data. As

knowledge sharing platforms require a certain number of participants to leverage network effects (c.f. Expectation 1), a full realization of all benefits from level 2 requires a lot of effort.

Level 3: Automated Data Provision: Organizations at level 3 share some of their internal data automatically with the community and directly connect to the CTI sharing platform. For example, manually reported phishing emails or virus alerts are automatically transmitted to and disseminated through the platform. As this requires a high level of trust in the other participants, granular control over what is shared with whom is required. For example, CTI sharing platforms at this level allow organizations to define sharing groups or sharing rules based on e.g. the TLP (c.f. Expectation 4).

Level 4: Full Integration: At level 4, organizations already trust both the data provided by the platform as well as other participants. At this level, organizations integrate some components of their security landscape into the CTI sharing platform to benefit from automation. For example, firewall rules are automatically updated to block suspicions traffic and spam filters automatically include shared rules to detect phishing emails, spam and emails containing viruses. As this requires organizations to select specific subsets of intelligence streams, a granular control over the intelligence flow is required (c.f. Expectation 4).

Level 5: Optimizing: Level 5 indicates that real-time CTI, shared (semi-) automatically, is an integral part of an organization's security and risk management processes. Real-time qualitative and quantitative intelligence is a foundational part of aligning security and risk management decisions with business goals (c.f. Expectation 6). A level 5 organization puts in place an effective governance structure and process to enable continuous improvement and innovation of security and risk management programs. Furthermore, organizations and governmental bodies, and other stakeholders form and nurture a mutually beneficial continuous ecosystem cycle for effective security and risk management through high quality CTI.

5.2 Limitations

Our case study might be limited by certain threats to validity. As described in [29] the application of focus group discussions in empirical research might be limited by certain threats to validity. Limitations that have to be acknowledged and accounted for are a (i) selection bias when selecting the participants for the case study, (ii) influences of moderators during the focus group discussions, (iii) off-topic discussions, (iv) language barriers and (v) an incomplete or biased list of CTI sharing elements stakeholders are willing to share.

In order to counteract limitation (i) to (iv) we followed the suggestions by Vogt et al. [30]. According to them, (i) participants of the case study were asked to participate voluntarily, (ii) moderators tried to keep in the background as much as possible, (iii) moderators refocused the discussion as soon as it got off track, and (iv) the explorative survey and focus group discussions were held in English. To counteract (v), we used the "data types and elements of interest to security operations personnel", presented in [11]. Moreover, the participants had the possibility to extend the list of sharing elements.

6 Conclusion

As organizations adapt to today's cyber threat landscape by leveraging the knowledge and capabilities of multiple organizations to curb advanced cyber threats, the usage of CTI sharing platforms has gained traction to coordinate these efforts. An extensive analysis of stakeholders' expectations and willingness to share through a series of interviews and focus group discussion indicates that different maturity levels of CTI sharing platforms exist. We propose that, by moving from one maturity level to the next level in an orderly manner, organizations can avoid unnecessary risks, build their CTI sharing capabilities systematically, and enable a systematic approach to collecting, analyzing and reacting to CTI. Although we have developed our model with a focused group of expert stakeholders and several interviews, future research needs to validate our model more rigorously using quantitative empirical data. In addition, our model is largely based on these organizations' perspectives and future research can improve the model by incorporating a more holistic community perspective. We acknowledge that there are situations in which the linear progression of our proposed maturity model is not practical and an organization can benefit from skipping one or more levels. We believe that our model will serve as an initial step to engage researchers and practitioners in ongoing conversations to further leverage the promised values of CTI sharing platforms.

Acknowledgements: This work was partially supported by the Austrian Federal Ministry of Science, Research and Economics (BMWFW), FFG Project 855383 SALSA (ICT of the Future).

References

1. S. Brown, J. Gommers, and O. Serrano, "From cyber security information sharing to threat management," in Proceedings of the 2nd ACM WISCS, ACM, 2015, pp. 43–49.
2. F. Fransen, A. Smulders, and R. Kerkdijk, "Cyber security information exchange to gain insight into the effects of cyber threats and incidents," Elektrotechnik und Informationstechnik, vol. 132(2) pp. 106–112, 2015.
3. S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," Information Management & Computer Security, vol. 22, no. 5, pp. 410–430, 2014.
4. F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," Computers & Security, vol. 60, pp. 154–176, 2016.
5. C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives," in 13. Internationale Tagung Wirtschaftsinformatik, WI 2017, St.Gallen, Switzerland.
6. E. V. D. Heuvel and G. K. Baltink, "Coordination and cooperation in cyber network defense: the dutch efforts to prevent and respond," Best Practices in Computer Network Defense: Incident Detection and Response, vol. 35, p. 121, 2014.
7. L. Dandurand and O. S. Serrano, "Towards improved cyber security information sharing," in Cyber Conflict (CyCon), 2013 5th International Conference on. IEEE, 2013, pp. 1–16.
8. C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in Proceedings of the Workshop on Information Sharing and Collaborative Security. ACM, 2016, pp. 49–56.

9. P. Kampanakis, “Security automation and threat information-sharing options,” Security & Privacy, IEEE, vol. 12, no. 5, pp. 42–51, 2014.
10. J. Steinberger, A. Sperotto, M. Golling, and H. Baier, “How to exchange security events? overview and evaluation of formats and protocols,” in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, 2015, pp. 261–269.
11. C. Johnson, L. Bager, D. Waltermire, J. Snyder, and C. Skorupka, “NIST special publication 800-150: Guide to cyber threat information sharing,”, NIST, Tech. Rep., 2016.
12. S. Ernest Chang and C.-S. Lin, “Exploring organizational culture for information security management,” Industrial Management & Data Systems, vol. 107, no. 3, pp. 438–458, 2007.
13. Ponemon, “The value of threat intelligence: A study of North American & United Kingdom companies,” Ponemon Institute LLC, Tech. Rep., 2016.
14. C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, “Data quality challenges and future research directions in threat intelligence sharing practice,” in Proceedings of the 2016 ACM WISCS. ACM, 2016, pp. 65–70.
15. O. Serrano, L. Dandurand, and S. Brown, “On the design of a cyber security data sharing system,” in Proceedings of the 2014 ACM WISCS. ACM, 2014, pp. 61–69.
16. S. Appala, N. Cam-Winget, D. McGrew, and J. Verma, “An actionable threat intelligence system using a publish-subscribe communications model,” in Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. ACM, 2015, pp. 61–70.
17. W. Zhao and G. White, “An evolution roadmap for community cyber security information sharing maturity model,” in Proceedings of the 50th HICCS Conference, 2017.
18. M. A. Alhawamdeh, “Developing a conceptual national information sharing security framework to combat cybercrimes in jordan,” in CCSCloud, 2017 IEEE 4th International Conference on. IEEE, 2017, pp. 344–350.
19. R. A. Martin, “Making security measurable and manageable,” in Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008, pp. 1-9.
20. S. Murdoch and N. Leaver, “Anonymity vs. trust in cyber-security collaboration,” in Proceedings of the 2nd WISCS Workshop. ACM, 2015, pp. 27–29.
21. J. Bhatia, T. D. Breaux, L. Friedberg, H. Hibshi, and D. Smullen, “Privacy risk in cybersecurity data sharing,” in Proceedings of the 2016 WISCS. ACM, 2016, pp. 57–64.
22. J. Pöppelbuß and M. Röglinger, “What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management.” in ECIS, 2011.
23. T. De Bruin, R. Freeze, U. Kaulkarni, and M. Rosemann, “Understanding the main phases of developing a maturity assessment model,” 2005.
24. E. R. Babbie, Survey research methods. Cengage Learning, 1990.
25. S. L. Pfleeger, “Experimental design and analysis in software engineering,” Annals of Software Engineering, vol. 1, no. 1, pp. 219–253, 1995.
26. S. Wilkinson, Qualitative research: Theory, method and practice, Cengage Learning, 2004.
27. P. Mayring and M. Gläser-Zikuda, Die Qualitative Inhaltsanalyse. Beltz Weinheim, 2008.
28. J. L. Campbell, C. Quincy, J. Osserman, and O. K. Pedersen, “Coding in-depth semi structured interviews problems of unitization and intercoder reliability and agreement,” Sociological Methods & Research, 2013.
29. K. Louise Barriball and A. While, “Collecting data using a semi-structured interview: a discussion paper,” Journal of advanced nursing, vol. 19, no. 2, pp. 328–335, 1994.
30. D. S. Vogt, D. W. King, and L. A. King, “Focus groups in psychological assessment: enhancing content validity by consulting members of the target population.” Psychological assessment, vol. 16, no. 3, p. 231, 2004.

IT-Governance in der integrierten Versorgung – eine risikobezogene Betrachtung

Lena Otto[1], Hannes Schlieter[1]

[1] Professur für Wirtschaftsinformatik, insb. Systementwicklung, Technische Universität Dresden, Dresden, Deutschland
{lena.otto, hannes.schlieter}@tu-dresden.de

Abstract. IT-Governance ist in der Industrie wie auch in der Gesundheitswirtschaft inzwischen eine zentrale Aufgabe zur Sicherstellung rechtskonformer und sicherer Prozesse. IT-Governance-Rahmenwerke und die darin vorgeschlagenen Risikomanagementansätze helfen dabei, die Risiken, die mit der Einrichtung und dem Betrieb von IT-Systemen verbunden sind, aktiv in die Managementprozesse einzubeziehen. Jedoch kommt durch die Fokussierung auf das unternehmensinterne Risikomanagement die netzwerkbezogene Betrachtung in bestehenden Governance-Rahmenwerken häufig zu kurz. Im vorliegenden Beitrag wird daher untersucht, inwieweit bestehende Risikomanagementansätze angewendet werden können, um die Verfügbarkeit, Integrität und Vertraulichkeit von Unternehmens- und Patientendaten in Anwendungssystemen der integrierten Versorgung sicherzustellen. Dabei wird deutlich, wie insbesondere der erhöhte Koordinationsbedarf und die rechtliche Autonomie der Netzwerkpartner das Risikomanagement in interorganisationalen Anwendungssysteme beeinflussen. Abschließen werden Schwachstellen in den bestehenden Rahmenwerken aufgezeigt.

Keywords: Integrierte Versorgung, IT-Risikomanagement, IT-Governance-Rahmenwerke, COBIT, ITIL

1 Einleitung

Durch zunehmende Komorbiditäten, Kostendämpfungszwänge und den Anspruch einer durchgehenden Patientenversorgung rücken Modelle der integrierten Versorgung immer stärker in den Fokus. Die relativ geringe Durchdringung des Gesundheitswesens mit integrierten Versorgungsmodellen und kooperativen Versorgungsformen führt dazu, dass sich bisher noch keine Standards für den Aufbau und Betrieb von Netzwerken der integrierten Versorgung durchgesetzt haben. Dies ist v. a. bei der Gestaltung von integrierten Anwendungssystemlandschaften relevant, mithilfe derer große Mengen sensibler Daten übertragen bzw. gemeinsam verarbeitet werden [1]. Für medizinische Versorgungsprozesse wird eine hohe Kompatibilität von Anwendungssystemen benötigt, deren Grundlage verfügbare und integre Daten darstellen [2]. Die hohe Intimität der Patientendaten [3] erfordert zusätzlich die Sicherstellung der Vertraulichkeit. Darüber hinaus können Risiken wie Feuer,

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Cyberangriffe oder Fehlbedienung die Informationssicherheit gefährden [4]. Zur frühzeitigen Vermeidung des Eintritts von Risiken verankert ein Risikomanagement Regeln zur Prävention von und zum Umgang mit solchen Risiken [5]. IT-Governance-Rahmenwerke leiten typischerweise den Aufbau und die Durchführung von Risikomanagement an [6]. Bestehende IT-Governance-Rahmenwerke adressieren jedoch häufig nur den unternehmensinternen Governance-Aspekt [7] und wurden bisher wenig für Netzwerkverbünde, insbesondere in der integrierten Versorgung, untersucht.

Das Ziel des Beitrages ist es, die Anwendung solcher IT-Governance-Rahmenwerke für die Gestaltung von Risikomanagementsystemen in Netzwerkorganisationen zu verbessern. Dafür wird die Möglichkeit des Einsatzes der Rahmenwerke für Anwendungssysteme in Netzwerkorganisationen literaturgestützt evaluiert und Gestaltungsempfehlungen zu deren Nutzung abgeleitet. Damit leistet die vorliegende Arbeit einen Beitrag zum Thema IT-Governance innerhalb der integrierten Versorgung, womit die Wahrung von Verfügbarkeit, Vertraulichkeit und Integrität als wesentliche Schutzziele einhergeht. Folgende Forschungsfrage steht damit im Zentrum der Untersuchung:

- Wie können bestehende IT-Governance-Rahmenwerke für das Management von IT-Risiken in integrierten Versorgungsnetzwerken eingesetzt werden und wo weisen sie ggf. Schwachstellen auf?

Der Beitrag ist wie folgt aufgebaut: Zunächst wird der Stand der Forschung aufgearbeitet. Dazu werden die am weitesten verbreiteten IT-Governance-Rahmenwerke mit Bezug zum Risikomanagement [8,9] (COBIT [10], ITIL [11] und ISO/IEC 27005:2011 [12]) betrachtet sowie die terminologischen Grundlagen gelegt. Weiterhin werden die Charakteristika der integrierten Versorgung aufgezeigt. Im Abschnitt 3 wird auf Basis der zuvor aufgearbeiteten Kriterien ein Evaluationsrahmen aufgebaut, anhand dessen im Abschnitt 4 die Evaluierung hinsichtlich der Ausgestaltung von Risikomanagement untersucht und die Anwendung ausgewählter IT-Governance-Rahmenwerke in der integrierten Versorgung analysiert wird. Die Arbeit schließt mit einer Diskussion der Ergebnisse und präsentiert Gestaltungsempfehlungen für eine bedarfsgerechte Nutzung der IT-Governance-Rahmenwerke.

2 Begriffliche Grundlagen

2.1 IT-Governance und IT-Risikomanagement

Das Ziel von IT-Governance ist es, Geschäftsziele mit Hilfe von IT-Prozessen zu erreichen, indem Werte generiert und Risiken minimiert werden [13,14]. Im engeren Sinn sind nicht alle der ausgewählten Rahmenwerke reine Instrumente der IT-Governance[1], obwohl sie in der Literatur als solche bezeichnet werden [8].

Entsprechend ihres initialen Entwicklungskontextes sind die ausgewählten IT-Governance-Rahmenwerke recht unterschiedlich ausgerichtet. COBIT liefert beispielsweise einen Governance-Ansatz für das gesamte Unternehmen [7]. ITIL hingegen fokussiert auf den Lebenszyklus von IT-Services und stellt dafür Best Practices zur Verfügung [16]. Demgegenüber definiert die ISO 27005 einen generischen Rahmen zur Ausgestaltung von IT-Risikomanagement und adressiert dabei den Aspekt der Informationssicherheit [17].

Risikomanagement dient der präventiven Abschwächung potentieller Risiken und beschreibt die Prozessschritte Definition einer Risikostrategie, Identifikation und Analyse, Bewertung, Steuerung und Überwachung von Risiken [18,5]. Gleichzeitig sind Informationen und deren Schutz ein zentraler Aspekt von Anwendungssystemen, an dem auch die Risikoidentifikation ansetzt. Insbesondere werden Informationssicherheit, und damit Verfügbarkeit, Integrität und Vertraulichkeit [2], als wesentliche Schutzziele benannt. Unterschiedlichste Ereignisse im Unternehmensalltag können eine Gefahr für diese genannten Schutzziele und somit ein unmittelbares Risiko darstellen. So können bspw. Brände die Verfügbarkeit oder Schadsoftware die Integrität bzw. Vertraulichkeit von Daten beeinträchtigen, woraus auch wirtschaftliche und rechtliche Risiken erwachsen können. Wenn von IT-Risiken gesprochen wird, steht der automatisierte Teil des Informationssystems, das sogenannte Anwendungssystem, im Vordergrund. Somit muss ein IT-Risikomanagement auch dessen wesentliche Bestandteile Hardware, System- und Anwendungssoftware beachten [19].

Die zentralen Risikokategorien ergeben sich dabei aus der internen Betrachtungsebene, welche die Risiken durch beteiligte Personen, Prozesse und Systeme adressiert, sowie den externen Risiken, welche die umliegenden Gegebenheiten berücksichtigen [20,4].

2.2 Besonderheiten in der integrierten Versorgung

Der Begriff der integrierten Versorgung ist im Zuge der Hinwendung zu einer kooperativen Versorgungslandschaft entstanden [21]. Er adressiert insbesondere die Spezifika von Netzwerkorganisationen, die Gestaltung unternehmensübergreifender Anwendungssystemlandschaften und die Besonderheiten von Interorganisations-

[1] Der Fokus von ITIL liegt primär auf dem Lebenszyklus-Management von Anwendungssystem-landschaften [15]. In der ISO 2700x Normenfamilie wird ausschließlich Risikomanagement von Informationssicherheit behandelt. Somit adressieren beide Rahmenwerke nur Teildisziplinen der IT-Governance [8].

systemen im Allgemeinen. Unter einem Interorganisationssystem, oder synonym auch interorganisationalen Informationssystem, werden Informationssysteme verstanden, die von mehreren Unternehmen gemeinsam genutzt werden [22]. Informationen werden dabei auch über Unternehmensgrenzen hinweg verarbeitet [23]. Somit ist ein interorganisationales Anwendungssystem der automatisierte Teil eines unternehmensübergreifend genutzten Informationssystems [19]. Die Datenhaltung kann sowohl zentral als auch dezentral (durch Integration der einzelnen Informations-/ Anwendungssysteme) erfolgen.

Aufbau. Im Aufbau ist neben der größeren Anzahl an Komponenten (Hard- und Software) sowie involvierten Administratoren und Benutzern insbesondere die notwendige sichere Verbindung zwischen den einzelnen Anwendungssystemen charakteristisch für interorganisationale Anwendungssysteme [23].

Organisationsform. Auch die veränderte Organisationsform, der Zusammenschluss in einem Unternehmensnetzwerk, bringt spezielle Charakteristika und Herausforderungen mit sich. So zeichnen sich Unternehmensnetzwerke durch komplexe, relativ stabile gegenseitige Beziehungen mit vertraglicher Bindung zwischen rechtlich selbstständigen, wirtschaftlich jedoch abhängigen Teilnehmern aus, denen ein spezieller Zweck zugrunde liegt (und die somit wieder trennbar sind) [24]. Dabei hat das Management keine Weisungsbefugnis [25], wodurch alle Leistungserbringer im Rahmen der Führung eingebunden werden [26]. Damit für alle Teilnehmenden am Netzwerk Vorteile generiert werden, ergeben sich Herausforderungen, die eine sinnvolle Organisation von Unternehmensnetzwerken mit sich bringt. Sie befinden sich in den Spannungsfeldern zwischen Markt und Hierarchie, Wettbewerb und Kooperation, Autonomie und Abhängigkeit, Flexibilität und Spezifität, Vielfalt und Einheit, Vertrauen und Kontrolle, Stabilität und Fragilität, Formalität und Informalität sowie ökonomischem Handeln und Herrschaftssicherung [27]. Jedes Unternehmensnetzwerk positioniert sich in all diesen Spannungsfeldern unterschiedlich. Im Rahmen der integrierten Versorgung in Deutschland sieht diese Positionierung wie folgt aus: Nach §140a SGB V [28] können Verträge der besonderen Versorgung zwischen Krankenkassen und verschiedenen Leistungserbringern geschlossen werden. Die integrierte Versorgung ist somit marktbezogen und die einzelnen Leistungserbringer kooperieren, obwohl sie bei gleicher Versorgungsstufe auch konkurrieren können. Die einzelnen Leistungserbringer agieren sehr autonom, spezifisch und vielfältig, da der Zusammenschluss zum Zwecke der Aufgabentrennung je nach Spezifikation vorgenommen wird. Ähnliches gilt für das Vertrauen, da keine überwachende Kontrollinstanz i.e.S. vorgesehen ist. Die vertragliche Bindung mit der Krankenkasse garantiert einen stabilen Zusammenschluss und hohe Formalität zwischen den Leistungserbringern sowie ökonomisches Handeln.

Interorganisationssysteme. Durch die Informationsverarbeitung über Unternehmensgrenzen hinweg ergeben sich auch bei Interorganisationssystemen Unterschiede im Vergleich zu Informationssystemen innerhalb eines einzelnen Unternehmens. Diese sind zusammengefasst in Tabelle 1 zu finden.

Es bleibt festzuhalten, dass insbesondere die Systeme und Prozesse in der integrierten Versorgung anders ausgestaltet sind als in einer einzelnen Einrichtung. In der Realität der integrierten Versorgung sind die Merkmale vornehmlich wie in Tabelle 1, Spalte 3 ausgeprägt, was Auswirkungen auf die spätere Evaluation hat.

Tabelle 1. Spezifika interorganisationaler Informationssysteme

	Allgemeine Ausprägungsmerkmale	*Typ. Ausprägung in der integrierten Versorgung*
(I)	Austausch / gemeinsame Verwendung von Daten und Anwendungen [29,24]	Lose gekoppelte Anwendungssysteme
(II)	Gefahr heterogener Sicherheitskonzepte [29]	Fokus auf unternehmens-internen Sicherheits-konzepten
(III)	Zentrale / dezentrale Datenhaltung [29,24]	Dezentrale Datenhaltung
(IV)	Kontrollbefugnis bei mehreren Unternehmen [30]	Kontrollbefugnis durch jeweiligen Netzwerkpartner
(V)	Schnittstellenmanagement notwendig (kann bei falscher Ausführung zu System- / Medienbrüchen und Dateninkonsistenzen führen) [29,24]	Keine standardisierten Schnittstellen
(VI)	(einseitige) Abhängigkeitsverhältnisse möglich [29]	Geringe Abhängigkeit
(VII)	Meist standardisierte Systeme [29]	Wenig standardisiert
(VIII)	Zentrale / dezentrale Verfügungsrechte [29]	Sowohl zentral als auch dezentral
(IX)	Hohe Systemsicherheit bzgl. Daten und Transaktionen [29]	
(X)	Flexible Teilnehmerzahl möglich [29]	Flexible Teilnehmerzahl
(XI)	Räumliche Verteilung der Netzwerkbeteiligten [29]	Regionale Verteilung
(XII)	Intensitätsgrad der Zusammenarbeit [24]	Geringe Intensität

3 Ableitung Evaluationsrahmen

Zum Aufbau des Evaluationsrahmens müssen einheitliche Evaluationskriterien definiert werden, anhand derer im weiteren Verlauf der Evaluationsgegenstand (COBIT, ITIL und ISO 27005) geprüft wird. Eine wesentliche Herausforderung des Risikomanagements ist dessen Integration in einen geregelten Unternehmensprozess (siehe Abs. 2.1). Demnach sollte ein IT-Governance-Rahmenwerk Gestaltungsempfehlungen für den IT-Risikomanagementprozess geben. Typischerweise erstrecken sich diese über die Phasen: *Definition einer Risikostrategie* (1), *Identifikation und Analyse* (2), *Bewertung* (3), *Steuerung* (4), *Überwachung* (5) der Risiken (siehe Kategorie: *Abdeckung des gesamten Risikomanagementprozesses*). Weiterhin muss die Berücksichtigung der Schutzziele *Verfügbarkeit, Integrität und Vertraulichkeit* (6) verankert sein. Durch den Betrachtungsfokus auf Anwendungssystemen ist es notwendig, dass in IT-Governance-Rahmenwerken auf die Komponenten *Hard-* (7) und *Software* (8) sowie auf beteiligte *Personen* (9) als möglichen Gegenstand der Untersuchung eingegangen wird.

Weitere zu evaluierende Kriterien sind die genannten *Risikokategorien der Personen-* (10), *Prozess-* (11) und *System-* (12) sowie *externen Risiken* (13) und die *generelle Passfähigkeit aufgrund der Charakteristika* der Rahmenwerke (14).

Anhand der definierten Kriterien werden die drei gewählten Rahmenwerke einem Vergleich bezüglich ihrer Anwendbarkeit auf Risikomanagement intraorganisationaler Anwendungssysteme in Abschnitt 4.1 unterzogen. Nach der prinzipiellen Eignungsfeststellung erfolgt die Prüfung der Übertragbarkeit auf interorganisationale Anwendungssysteme im Kontext der integrierten Versorgung. Zur Feststellung der Übertragbarkeit der Ergebnisse müssen die Charakteristika der integrierten Versorgung einbezogen werden.

4 Evaluation

4.1 Analyse der intraorganisationalen Anwendung

Mit Blick auf die Evaluationskriterien stellt sich COBIT als eines der umfänglichsten IT-Governance-Rahmenwerke dar. COBIT adressiert alle der zuvor aufgestellten Kriterien und gibt detaillierte Erläuterungen zu einzelnen Schritten und Komponenten [7]. Dennoch besteht die Gefahr, dass die Komplexität des Rahmenwerkes dessen Anwendbarkeit negativ beeinflusst [15]. Da bei ITIL der Lebenszyklus von IT-Services und deren Management im Vordergrund stehen, weist ITIL einige Schwachstellen bei der Betrachtung des Risikomanagementprozesses auf [31]. So wird zwar von Risiken im Allgemeinen gesprochen, aber nicht auf konkrete Risikokategorien, wie Prozess- oder Systemrisiken eingegangen. Anders ist es hingegen in der ISO 27005, welche die definierten Evaluationskriterien umfassend berücksichtigt (siehe Tabelle 2).

Tabelle 2. Zusammenfassung der Evaluationsergebnisse bzgl. der Passfähigkeit für das unternehmensinterne IT-Risikomanagement

Kategorie	*COBIT*	*ITIL*	*ISO 27005*
Abdeckung des Risikomanagementprozesses:			
(1) Definition einer Risikostrategie	✓	□	✓
(2) Identifikation und Analyse	✓	✓	✓
(3) Bewertung	✓	✓	✓
(4) Steuerung	✓	✓	✓
(5) Überwachung	✓	□	✓
(6) Fokus auf Verfügbarkeit, Integrität, Vertraulichkeit	✓	✓	✓
Einbeziehung der Komponenten			
(7) Hardware	✓	✓	✓
(8) Software	✓	✓	✓
(9) Personen	✓	✓	✓
Berücksichtigte Risikokategorien:			
(10) Personenrisiken	✓	✓	✓
(11) Prozessrisiken	✓	□	✓
(12) Systemrisiken	✓	□	✓
(13) Externe Risiken	✓	□	✓
(14) Prinzipielle Eigenschaften	x	x	✓

Legende:

Kriterium vollständig erfüllt	Kriterium teilweise erfüllt	Kriterium nicht erfüllt
✓	□	x

Wie dargestellt, unterstützen die untersuchten Rahmenwerke das Risikomanagement unternehmensinterner Anwendungssysteme weitestgehend. Kleinere Abstriche müssen bei ITIL gemacht werden, da hier die Definition einer Risikostrategie sowie der Umgang mit Prozess-, System- und externen Risiken nur wenig berücksichtigt werden.

4.2 Analyse der interorganisationalen Anwendung

Zur Evaluierung der Einsatzfähigkeit der Rahmenwerke für das Risikomanagement innerhalb von Netzwerken der integrierten Versorgung werden nun die in Abschnitt 2.2 erarbeiteten Besonderheiten (I-XII) der integrierten Versorgung mit in die Bewertung einfließen. Ergänzend zu den bestehenden Bewertungskategorien wird dem Evaluierungsrahmen in Tabelle 3 eine weitere Kategorie hinzugefügt. Dies soll eine bessere Differenzierung der Ergebnisse ermöglichen. Wird ein Kriterium mit „-“ bewertet, so adressiert das Rahmenwerk das Kriterium zwar abstrakt, konkretisiert es aber nicht hinsichtlich der Einsetzbarkeit in integrierten Versorgungsnetzwerken.

Obwohl die Prozessschritte des Risikomanagements weiterhin in den Rahmenwerken berücksichtigt werden (siehe Tabelle 2), erfüllen sie dennoch nicht die Ansprüche integrierter Versorgungsnetzwerke. Für jeden der Schritte ist mindestens teilweise eine Konsensbildung zwischen allen Netzwerkteilnehmern erforderlich, da diese trotz rechtlicher Unabhängigkeit wirtschaftlich voneinander abhängig sind. Die

Risikostrategie muss einheitlich definiert werden und Risiken, die durch den Zusammenschluss der einzelnen Beteiligten entstehen, müssen übergreifend identifiziert und analysiert werden. Für eine einheitliche Bewertung, Steuerung und Überwachung sind auch dort gemeinsame Absprachen wichtig, insbesondere da in integrierten Versorgungsnetzwerken geringe Abhängigkeit (VI) und Intensität der Zusammenarbeit (XII) sowie hohe regionale Verteilung der Netzwerkteilnehmer (XI) herrschen. Auf diese Besonderheiten der Unternehmensnetzwerke wird in keinem der Rahmenwerke explizit eingegangen. In COBIT erfolgt eine Berücksichtigung von Anforderungen von Statusgruppen, aber keine ausdrückliche Beachtung von Unternehmensnetzwerken. ITIL erwies sich bereits für intraorganisationale Anwendungssysteme als nur teilweise geeignet. In ISO 27005 existiert ein Verweis, dass es für alle Arten von Unternehmen geeignet ist, ohne dass Besonderheiten von Unternehmensnetzwerken berücksichtigt werden. Anleitungen zur Durchführung der einzelnen Schritte bleiben (v. a. in COBIT und ISO) erhalten, teilweise mit Beispielen. Dennoch werden notwendige integrierte Managementprozesse und Absprachen zwischen mehreren Unternehmen nicht berücksichtigt. Es werden auch keine Lösungen für die Probleme der fehlenden Weisungsbefugnis des Managements, der wenigen Kontrollbefugnis bei (IV) sowie der Abhängigkeit von anderen Unternehmen (insbesondere beim Sicherheitskonzept – VI/II), flexibler Teilnehmerzahl (X) und zusätzlichem Schnittstellenmanagement (V), die Änderungen im Risikomanagement hervorrufen, bereitgestellt. Daher wird die Bewertung verringert (1-5).

Das Kriterium der Verfügbarkeit, Integrität und Vertraulichkeit (6) ist für intra- und interorganisationale Anwendungssysteme gleichermaßen adressiert und damit als erfüllt einzustufen. Aus der integrierten Versorgung erwachsen keine weiteren Aspekte. Herausforderungen sind in der operativen Sicherstellung der Merkmale zu erwarten.

Ein weiterer Aspekt ist die Interoperabilität, die möglichst ohne Risikozuwachs auf allen Ebenen (rechtlich, organisatorisch, semantisch und technisch) sichergestellt werden muss [32]. Obwohl sich intra- und interorganisationale Anwendungssysteme hinsichtlich der Komponenten (Hard- und Softwaresysteme) nicht unterscheiden, erhöht sich bei interorganisationalen die Anzahl involvierter Hard- und Softwaresysteme. Zwischen diesen müssen adäquate Schnittstellen (V) etabliert werden. Insbesondere durch die nur lose gekoppelten Anwendungssysteme (I) sowie die fehlenden standardisierten Schnittstellen und Systeme (VII) innerhalb der integrierten Versorgungsnetzwerke ist dieser Aspekt bedeutend. Zusätzlich erhöht sich auch die Anzahl involvierter Nutzer und Administratoren gegenüber einem einzelnen intraorganisationalen Anwendungssystem. Die Einbeziehung all dieser, teilweise evtl. auch an Schnittstellen eingesetzten, Personen in das Risikomanagement muss sichergestellt werden. Keines der Rahmenwerke gibt explizite Anleitungen für eine dieser Gestaltungsebenen. Im Gegenteil liegt der Fokus auf einzelnen Organisationen und deren ganzheitlicher Betrachtung [7]. Zwar wird für die ISO 27005 deren Anwendbarkeit auf alle Arten von Organisationen festgelegt, eine Berücksichtigung der Charakteristika von Unternehmensnetzwerken fehlt dennoch. Der wesentliche Unterschied liegt in der Unabhängigkeit der einzelnen Netzwerkteilnehmer (VI), die primär ihre eigene Perspektive einnehmen. Eine explizite Berücksichtigung der Netzwerkperspektive und somit der Gesamtsicht muss garantiert werden. Jedoch gibt

es auch dafür keine adäquate Anweisung in einem der Rahmenwerke. Auch hier muss die Bewertung der Kriterien (7-9) entsprechend verringert werden.

Die Risikokategorien und ihre Berücksichtigung in den Rahmenwerken bleiben auch für Unternehmensnetzwerke in der integrierten Versorgung gleich (insbesondere in COBIT und ISO). Die komplexen Beziehungen, regionale Verteilung (XI) wenig intensiv zusammenarbeitender Partner (XII) und die geringe Abhängigkeit (VI) unter den Netzwerkteilnehmer können zu Problemen hinsichtlich notwendiger Absprachen führen. Zusätzlich ergeben sich Änderungen in der Bewertung, insbesondere der Eintrittswahrscheinlichkeit dieser Risikokategorien. Bspw. kann Misstrauen zwischen den einzelnen Netzwerkteilnehmern die Personenrisiken verstärken, während die lose Kopplung der Anwendungssysteme (I) mit nicht standardisierten Schnittstellen (VII) in der integrierten Versorgung eine hohe Gefahr für inkonsistente Daten innerhalb der Prozessrisiken darstellen. Ergänzend dazu sind weitere Absprachen zur einheitlichen Bewertung notwendig. Keines dieser Charakteristika ist in den Rahmenwerken enthalten, was zu entsprechender Verringerung der Kriterienbewertung (10-13) führt.

Unabhängig von der genannten fehlenden Berücksichtigung von Unternehmensnetzwerk-Spezifika ändert sich an der Bewertung der prinzipiellen Eigenschaften (14) nichts. Die gesamte Bewertung ist in Tabelle 3 dargestellt.

Tabelle 3. Übertragbarkeit der Passfähigkeit der Rahmenwerke auf die integrierte Versorgung

Kategorie	*COBIT*	*ITIL*	*ISO 27005*
Abdeckung des Risikomanagementprozesses:			
(1) Definition einer Risikostrategie	–	□	–
(2) Identifikation und Analyse	–	–	–
(3) Bewertung	–	–	–
(4) Steuerung	–	–	–
(5) Überwachung	–	□	–
(6) Fokus auf Verfügbarkeit, Integrität, Vertraulichkeit	✓	✓	✓
Einbeziehung der Komponenten			
(7) Hardware	–	–	–
(8) Software	–	–	–
(9) Personen	–	–	–
Berücksichtigte Risikokategorien:			
(10) Personenrisiken	–	–	–
(11) Prozessrisiken	–	□	–
(12) Systemrisiken	–	□	–
(13) Externe Risiken	–	□	–
(14) Prinzipielle Eigenschaften	x	x	✓

Legende:

Kriterium vollständig erfüllt	Kriterium teilweise erfüllt	Kriterium nicht erfüllt	Kriterium erfüllt, aber ohne Berücksichtigung von Besonderheiten in Unternehmensnetzwerken
✓	□	x	–

Es bleibt festzuhalten, dass von den drei evaluierten Rahmenwerken keines die Kriterien vollumfänglich erfüllt. COBIT und ITIL waren mit Blick auf das intraorganisationale Risikomanagement von Anwendungssysteme bereits nur teilweise oder nicht passfähig. Durch die Besonderheiten der integrierten Versorgung verringert sich die Bewertung und auch die ISO 27005 kann nur teilweise den Anforderungen gerecht werden (insbesondere im Umgang mit spezifischen Schutzzielen).

5 Diskussion und Fazit

Die drei am meisten verwendeten und auf Risikomanagement ausgerichteten Rahmenwerke COBIT, ITIL und ISO 27005 wurden hinsichtlich ihrer Verwendbarkeit für Unternehmensnetzwerke in der integrierten Versorgung untersucht. Es konnte gezeigt werden, dass die Anwendung der evaluierten IT-Governance-Rahmenwerke mit einer Vielzahl von Einschränkungen einhergeht. Insbesondere muss dabei festgestellt werden, dass durch den gewählten Abstraktionsgrad und die mangelnde Explikation des Netzwerkes als Gestaltungsgegenstand die konkrete Anwendung weitestgehend offenbleibt. Nicht erfüllte Anforderungen der Rahmenwerke umfassen insbesondere die Berücksichtigung von Absprachen, fehlende Weisungsbefugnis und Kontrolle (des Managements) sowie die flexible Teilnehmerzahl und zusätzliche Interoperabilität, inkl. Schnittstellenmanagement, die sich aus einem Zusammenschluss im Unternehmensnetzwerk der integrierten Versorgung ergeben. Alle untersuchten Rahmenwerke beschreiben zwar die Schritte des Risikomanagementprozesses und berücksichtigen den Fokus auf Verfügbarkeit, Integrität und Vertraulichkeit sowie alle Arten von Betriebsrisiken allgemein, die Betrachtung der Anwendung in Unternehmensnetzwerken bleibt jedoch aus. In der weiteren Forschung können die gewonnen Ergebnisse in den Gestaltungsprozess für die Entwicklung eines spezifischen, auf die integrierte Versorgung ausgerichteten Risikomanagement-Werkzeugs einfließen. Hierzu sollte ein Ansatz erarbeitet werden, der die Stärken bestehender Rahmenwerke zusammenfasst und um Anforderungen der interorganisationalen Arbeit erweitert. Beispielsweise bietet sich eine Verbindung aus der klaren Struktur der ISO, ergänzt um ausführliche Erläuterungen aus COBIT und praxiserprobte Angaben von ITIL an. Die Generalisierung und Übertragbarkeit der Ergebnisse auf Unternehmensnetzwerke weiterer Branchen und verschiedene Organisations- und Netzwerkgrößen ist zu untersuchen.

Ausgehend von den identifizierten Defiziten ist die Berücksichtigung folgender fünf Anforderungen vorzunehmen, die in den Erstellungsprozess eines domänenspezifischen Rahmenwerkes einfließen können:

- Anf. 1 - **Unternehmensübergreifende Managementprozesse**: Ein expliziter Hinweis auf die erhöhte Notwendigkeit von Absprachen im Rahmen der meisten Schritte des Risikomanagementprozesses
- Anf. 2 - **Übertragung von Verantwortung**: Anleitungen zum Festlegen von Verantwortlichkeiten bzgl. ganzheitlicher Kontrolle aller gemeinsamen Prozesse
- Anf. 3 - **Regeln bei Veränderungen der Beteiligten**: Die Sicherstellung von Verantwortlichkeiten auch bei wechselnden Teilnehmern (bspw. über eine

ausreichende Anzahl festgelegter Stellvertreter oder dem Einführen von Prozessschritten, die bei Austritt von verantwortlichen Personen greifen)
- Anf. 4 - **Interoperabilität**: Ein expliziter Hinweis auf die verschiedenen Ebenen der Interoperabilität und der Notwendigkeit, diese sicherzustellen
- Anf. 5 - **Ganzheitliche Managementprozesse**: Ein expliziter Hinweis auf die Notwendigkeit eines ganzheitlichen Schnittstellenmanagements (evtl. durch Definition von Verantwortlichen).

Zusammenfassend ist zu konstatieren, dass mit der vorliegenden Untersuchung gezeigt werden konnte, welche Einschränkungen mit der Anwendung bestehender IT-Governance-Rahmenwerke in Netzwerken der integrierten Versorgung einhergehen. Mit der finalen Ableitung von Kernanforderungen wurde die Basis für das Zusammenwachsen der IT-Landschaften in der integrierten Versorgung gelegt.

Referenzen

1. Henriksen, E., Burkow, T., Johnsen, E., Vognild, L.: Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. BMC Medical Informatics & Decision Making, 13, 1-13 (2013)
2. Zambon, E., Etalle, S., Wieringa, R.J., Hartel, P.: Model-based qualitative risk assessment for availability of IT infrastructures. Software Systems Modeling 10, 553-580 (2011)
3. Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097) geändert worden ist
4. Wolke, T.: Risikomanagement. De Gruyter Oldebourg, Berlin (2015)
5. Jakolow-Standke, A.: Beschwerde- und Risikomanagement. In: Debatin, J:F:, Ekkernkamp, A., Schulte, B., Tecklenburg, A. (Hrsg.) Krankenhausmanagement : Strategien, Konzepte, Methoden. 2., aktualisierte und erweiterte Auflage. MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin (2013)
6. Helmke, S., Uebel, M.: Leit- und Leistungsbild der IT. In: Helmke, S., Uebel, M. (Hrsg.): Managementorientiertes IT-Controlling und IT-Governance, 15-37, Springer Gabler, Wiesbaden (2016)
7. Gaulke, M.: Praxiswissen COBIT – Grundlagen und praktische Anwendung in der Unternehmens-IT. dpunkt.verlag, Heidelberg (2014)
8. Johannsen, W., Goeken, M.: Referenzmodelle für IT-Governance: Strategische Effektivität und Effizienz mit COBIT, ITIL &Co. dpunkt.verlag, Heidelberg (2007)
9. Häfner, C., Felden, C.: Building a Framework for an Efficient IT Governance. Freiberger Forschungshefte 231, Freiberg (2009)
10. ISACA: COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT (2012)
11. AXELOS: ITIL Service Design. The Stationery Office, London (2013)
12. ISO - International Organization for Standardization: International Standard ISO/IEC 27005:2011(E) – Information technology; Security techniques; Information security risk management (2011)
13. Bienert, P., Wildhaber, B.: IT-Governance: Strategische Führung und Kontrolle von Informationssystemen als Teil der New Corporate Governance. Forte Advisors, Glattzentrum (2007)

14. Rüter, A., Schröder, J., Göldner, A., Niebuhr, J. (Hrsg.): IT-Governance in der Praxis. Springer-Verlag, Berlin, Heidelberg (2010)
15. De Haes, S., Van Grembergen, W., Debreceny, R.S.: COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems 27, 307-324 (2013)
16. Sahibudin, S., Sharifi, M., Ayat, M.: Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. In: Proceedings – 2nd Asia International Conference on Modelling and Simulation, pp. 749-753. IEEE Press, New York (2008)
17. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. Information Management & Computer Security, 22, 410-430 (2014)
18. Cagliano, A.C., Grimaldi, S., Rafele, C.: A systemic methodology for risk management in healthcare sector. Safety Science 49, 695-708 (2011)
19. Ferstl, O.K., Sinz, E.J.: Grundlagen der Wirtschaftsinformatik, Oldenbourg Verlag, München (2013)
20. Bistarelli, S., Fioravanti, F., Peretti, P., Santini, F.: Evaluation of complex security scenarios using defense trees and economic indexes. In: Journal of Experimental & Theoretical Artificial Intelligence 24, 161-192 (2012)
21. Smith, D.L., Bryant, J.H.: Building the Infrastructure for Primary Health Care: An Overview of Vertical and Integrated Approaches. Social Science & Medicine 26, 909-917 (1988)
22. Cash, J.I., Konsynski, B.R.: IS Redraws Competititve Boundaries. Harvard Business Review 2, 134-142 (1985)
23. Johnston, R.H.; Vitale, M.R.: Creating Competitive Advantage With Interorganizational Information Systems. MIS Quarterly 12, 153-165 (1988)
24. Schüppler, D.: Informationsmodelle für überbetriebliche Prozess: Ein Ansatz zur Gestaltung von Interorganisationssystemen. Lang, Frankfurt am Main; Berlin [u.a.] (1998)
25. Bogenstahl, C.: Management von Netzwerken: Eine Analyse der Gestaltung interorganisationaler Leistungsaustauschbeziehungen. Gabler, Wiesbaden (2012)
26. Hildebrandt, H., Stunder, B.H., Wetzel, M., Gröne, O.: Erfolgsfaktoren für Netze und regionale Gesundheitsorganisationen: Organisationsformen, Führung, Patientenorientierung. In: Eble, S., Kurscheid, C. (Hrsg.): Gesundheitsnetzwerke: Strategien, Konzepte, Methoden. MWV, Berlin (2013)
27. Sydow, J.: Strategische Netzwerke: Evolution und Organisation. Gabler, Wiesbaden (1992)
28. Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 4 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214) geändert worden ist
29. Raupp, M.: Informationsmanagement und strategische Unternehmensführung. Lang, Frankfurt am Main; Berlin [u.a.] (2002)
30. Suomi, R.: On the Concept of Inter-organizational Information Systems. Journal of Strategic Information Systems, 2, 93-100 (1992)
31. Vilarinho, S., da Silva, M.M.: Risk Management Model in ITIL. In: Cruz-Cunha, M.M., Varajão, J., Powell, P., Martinho, R. (Hrsg.) ENTERprise Information Systems. CENTERIS 2011. Communications in Computer and Information Science 220, 306-314. Springer, Berlin, Heidelberg (2011)
32. European Commission: ANNEX to the European Interoperability Framework – Implementation Strategy COM(2017) 134 final. Brüssel (2017)

Modellierung betrieblicher Informationssysteme

Teilkonferenzleitung

Peter Fettke
Sven Overhage
Sebastian Schlauderer

SenSoMod – A modeling language for context-aware mobile applications

Julian Dörndorfer[1], Christian Seel[1] and Daniel Hilpoltsteiner[1]

[1] University of Applied Science Landshut, Computer Science, Landshut, Germany
{julian.doerndorfer,seel,daniel.hilpoltsteiner}@haw-landshut.de

Abstract. The success and ubiquity of mobile devices like smartphones and tablets changed the daily work activities of many employees and employers. For example, editing and managing customer data in a mobile version of a customer relationship management (CRM) system can be done anywhere and anytime. In addition, the sensors of the mobile devices make it possible to gather data about the current state of the business process execution and the user's environment. With these data provided by mobile devices and combined with external data from databases or web services, it is possible to recognize the context of a business process. Context recognition allows to adapt the business process by selecting the next process step or providing the necessary data, like the next customer near the current location. However, to use the advantages of context recognition, mobile business processes and applications have to be designed in a context-aware manner.

Keywords Context, Context-Aware Business Processes, Mobile Processes, Domain Specific Modeling Language

1 Introduction

Mobile devices like smartphones or tablets, are increasingly common for professional related activities [1, 2], such as waiters using a smartphone to accept the order from customers and billing the meal with it. With the emerging generation of digital natives, which are increasingly entering the job market, this change from stationary to mobile computer is likely to grow [1]. The widespread use of mobile devices is leading to a change in executing business processes.

Using business processes to standardize important procedures is a standard approach in theory and practice [3–7]. It leads to cost reductions and productivity gains as well as it serves to increase the customer satisfaction or sharpening the competitiveness of a company [8]. The nearly ubiquitous presence of mobile devices can be used to support the execution of business processes. FALK and LEIST [9] find that the use of mobile devices improves the quality and flexibility of business processes, and also saves time and costs during the execution. A second aspect is that mobile devices are providing many sensors or can be additionally equipped via *Bluetooth*, the *universal serial bus* (USB) or other proprietary protocols. Moreover, mobile devices are capable to request

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

additional data from other sources, like databases or web services via their internet connection.

The aggregation and interpretation of sensor data enables detecting and creating the context of the users and supports them during the execution of a business process. According to DEY [10] context is "any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves". Therefore, context recognition can be used to automatically present useful information for the user and moreover pre-select the next possible process steps. Context recognition also improves the efficiency of business processes [11]. To support the design and implementation of supportive mobile context-aware applications, the business process languages also have to consider contextual influences [12]. In addition, the aggregation of context through the sensor data can be complex. For instance, the context parameter *weather* basically consists of the sensor data *humidity*, *wind speed* and *temperature*. Moreover, *weather* can also be a sensor for another context parameter, like *street conditions* in a navigation system. To use the opportunities of context recognition via mobile devices and ease the conduction of mobile context-aware business processes, this paper answers the following research questions.

RQ.1: How can a modeling language for context-aware applications be designed?
RQ.2: Can the language improve the implementation of mobile context-aware applications?

The remainder of this paper is structured as follows: In section 2 a brief overview of the existing literature will be given. Afterwards, the whole modeling approach is presented, which explains the sensor modeling language (SenSoMod) in detail (**RQ.1**). Section 4 shows the evaluation of SenSoMod (**RQ.2**). The paper ends with a conclusion and outlook to further research in context-aware mobile applications.

2 Related Work

Besides DEY context was also defined by others [13–15]. Not only is DEY's definition well known and accepted in the scientific community, but he also declares when an application is context-aware. It is context-aware "if it uses context to provide relevant information and/or services to user, where relevancy depends on the user's task" [16].

Some approaches to make business processes more flexible have been tried. ROSEMANN et al. [17] claim that modeling languages have to be more flexible to model context. Further, they state that an increased attention on flexibility took place in the research area, which leads to a decreasing time-to-market for products [18]. Therefore, the result is a demand for higher process flexibility [19]. In particular, ROSEMANN et al. show the limitation of the actual event-driven process chain (EPC) language and the lack of supporting context modeling. However, they do not present an appropriate way to integrate the identified context in business processes. The extension C-EPC is an approach to make EPC more configurable for decisions at runtime, but it doesn't address context in particular [20]. The approach from LA VARA et al. aims to reveal all

possibilities of a business process and integrate them into one process model. However, this leads to large and complex models. In [21] an approach to identify and apply context in a business process is introduced, but it is more of a theoretical framework to identify context and does not show how a context-aware business process could be designed. In [22] HEINRICH and SCHÖN mention that business processes have to consider "not-static" context events that change the process execution. Moreover, they present an algorithm which supports automated process planning for context-aware processes, but no modeling representation in BPMN. CONFORTI et al. present an approach to manage process risks by sensor evaluation [23]. Furthermore, they show a way to model these risks and when they occur. They only consider sensor data and context evaluation for process risks, but context and its evaluation can be used for more than risk analysis for business processes. DÖRNDORFER and SEEL present in their paper a BPMN extension for business processes, which is able to model context in business processes via a complete modeling technique [24]. They also developed a context-free grammar to state brief context expression for decisions depending on context. Furthermore, two extensions for UML are published by AL-ALSHUHAI and SIEWE. In the first paper, they are extending the class diagram with additional annotations [25]. The second paper [26] expands the activity diagram to mark context-sensitive areas or sequences. Additionally, two paper were found about domain specific languages for mobile applications [27] and for cloud computing [28]. However, both languages aim to ease the transformation of mobile and hybrid applications between different platforms. They do not present a context description language.

All the presented papers do not consider how complex context evaluation is. Furthermore, the implementation of supportive mobile applications is not supported by the modeling languages. Therefore, this paper presents a modeling language that shows how context parameters, which influence business processes, can be extracted from sensor information. Thus, this paper presents in terms of the design sciences paradigm by HEVNER [29] a new artifact.

3 The specification of the domain specific modeling language SenSoMod

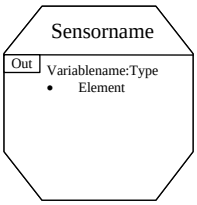
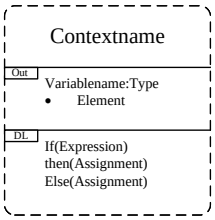
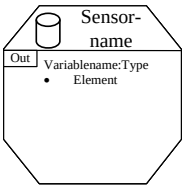
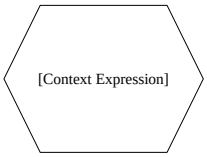
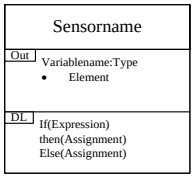
To use the possibilities of mobile devices more efficiently and ease the planning and implementation of supportive context-aware applications, standard business process languages have to consider context. Therefore, we chose the Context4BPMN [24] extension, which allows the design of context-aware business processes. The extension Context4BPMN enables to consider static and non-static context events in BPMN via a context expression, which can be stated through context annotations. It is therefore possible to design context-aware business processes. However, the extension of the BPMN does not specify how context can be evaluated by sensors. For instance, the context *location* has to be measured via GPS, with the values *at home* and *at work*. The difficulty is to state where *home* is and when to switch between these values. To address these questions and to further ease the design and implementation of mobile context-aware applications, which support the execution of context-aware business processes,

the sensor modeling language (SenSoMod) has been developed. It also allows to model context expressions from Context4BPMN and is therefore a possibility to integrate SenSoMod into BPMN.

Notation of the Sensor Modeling Language

Context is measured through sensors. We understand a sensor as any source of information for context. This can be a "usual" physical sensor – like a hygrometer or a temperature sensor –, a database, or an application from which information could be requested. Even a machine in an assembly hall that is accessible through a network connection can be a source of information. Therefore, different types of sensors have to be distinguished. There are atomic sensors which cannot be aggregated from other sensors. Two kinds of atomic sensors exist: *Physical sensors*, which measure physical quantities like temperature or humidity, and *virtual sensors* which are dedicated to non-physical quantities like databases, machines or stock states. Besides the atomic sensor, there is the computed sensor – a sensor relying on other sensors, which could be atomic sensors or other computed sensors. For example, the sensor *weather* could be the combination of the atomic sensors *humidity* and *temperature*. To address the different kind of sensor types we gave each of them a graphical representation (cf. **Table 1**).

Table 1. The notation of the sensor modeling language

Element	Notation	Element	Notation
Physical atomic sensor		Context	
Virtual atomic sensor		Context description	
Computed sensor		Flow	
Multiple Instances	III		

Knowing that the main feature to distinguish modeling constructs is the shape [30] (like the BPMN mainly relies on it [31] because shapes have a significant impact on object recognition [32]), the goal was to design similar objects like the sensor types

alike. Objects which are not similar like sensor and context description were designed in different 2D-shapes. The *physical sensor* is designated to depict physical quantities, whereas the *virtual sensors* are dedicated to non-physical quantities. To differentiate these two atomic sensors, the virtual sensors are marked by a database symbol to the left of the sensor name field. Beneath the name is the output area marked with *Out*. The area is intended to describe the structure of the outgoing objects of the sensor like the type and elements of it. First the name and – separated by a colon – the type of the return object have to be stated. If the object type has specific values – like enums, arrays or lists –, those can be stated in a bullet list. Alternatively, the return values can be specified in the JavaScript Object Notation (JSON) RFC-7159 [33] notation. Next to the two atomic sensors is the *computed sensor*. It can be used to combine different atomic sensors and/or *computed sensors*. Weather, for example, can be aggregated from different types of sensors. *Computed sensors* also have an area for describing outgoing elements. Furthermore, they have a *DL* area dedicated to describing the decision logic for their outgoing objects. This is necessary to express when a certain state from the *Out* area of a sensor will be returned. For example, location *at work* will be returned when the logged-in network name is *companyNetwork*. The accurate description of the decision logic language is presented in **Figure 1**. The *context* notation is the next element in the table. The name of the element has to match with the name of the involved context in the *context description.* Only *context* elements can be connected with a *context description*. Like the sensors, the *context* has the *DL* and *Out* areas. A *context* is based on at least one sensor, whatever type it is. The *context description* is the graphical representation of an expression to describe a contextual influence in a business process. The context expression language is part of the Context4BPMN extension [24]. To connect the different elements and show the sequence stream, the *flow* element has to be used. *Multiple instances* is the last element in the table and is an attribute for any type of sensors. It indicates that a sensor occurs in more than one instance, and is placed to the right of a sensor name. An example, using the introduced elements, is given in **Figure 2**. **Figure 1** depicts the logical decision language which has been developed. The language is a context free grammar in the Extended Backus Naur Form (EBNF) [34] and serves to briefly and precisely express the decision in the *DL* area of the *sensor* and *context* elements. A decision logic consists of a *LogicTerm* and can have a default assignment. The *LogicTerm* itself is built out of an *Expression* and an *Assignment*. If the expression is evaluated as *true*, the variable will be assigned to the designated value. The assigned variable has to exist in the output area of the computed sensor or context.

To shorten some basic definitions, like integer numbers or date, we link with "-->" to standards, like doubles. In order to express the structure of the object returned to a request by a sensor, the "Out" area is provided. First the name and – separated by a colon – the type of the return object have to be stated. Optionally, the values of the type (if existing) could be stated in a bullet list. Alternatively, the return values could be specified in the JSON notation.

An example for a mobile context-aware business process are traveling salesperson in a company's sales department (**Figure 2**). They partly work at the customer side to sell the products from the company as well as in the company to participate in meetings or further training. Moreover, some paper work can also be done at home. Therefore,

the first context parameter is the *location* with the three variables *at the customer*, *at the office* and *at home*.

```
<Decisionlogic>::=  <LogicTerm>  ["else("  <Assignment>  ")"]  |  <LogicTerm>",
   "<LogicTerm> ["else(" <Assignment> ")"]
<LogicTerm>::= "If(" <Expression> ")then(" <Assignment> ")"
<Assignment> ::= <Variable> "=" <Value>
<Expression>::= <Variable> [<MathematicalOperator> <Constant>]
   <Comparison> <Value> | <Expression> <LogicOperator> <Expression>
<Comparison>::= "=" | "!=" | "<=" | ">=" | "<" | ">"
<MathematicalOperator>::= "*" | "/" | "+" | "-"
<LogicOperator>::= "&&" | "||"
<Constant>::= --> "DoubleNumber"
<Interval>::= -->"IntegerNumber" "msec" | "sec" |"min" | "hours" | "days"
<Variable>::= <Character>
<Value>::= <Character>
<Character> = -->"StringIdentifier in UTF-8"
```

Figure 1. EBNF Grammar for the Decision Logic (DL)

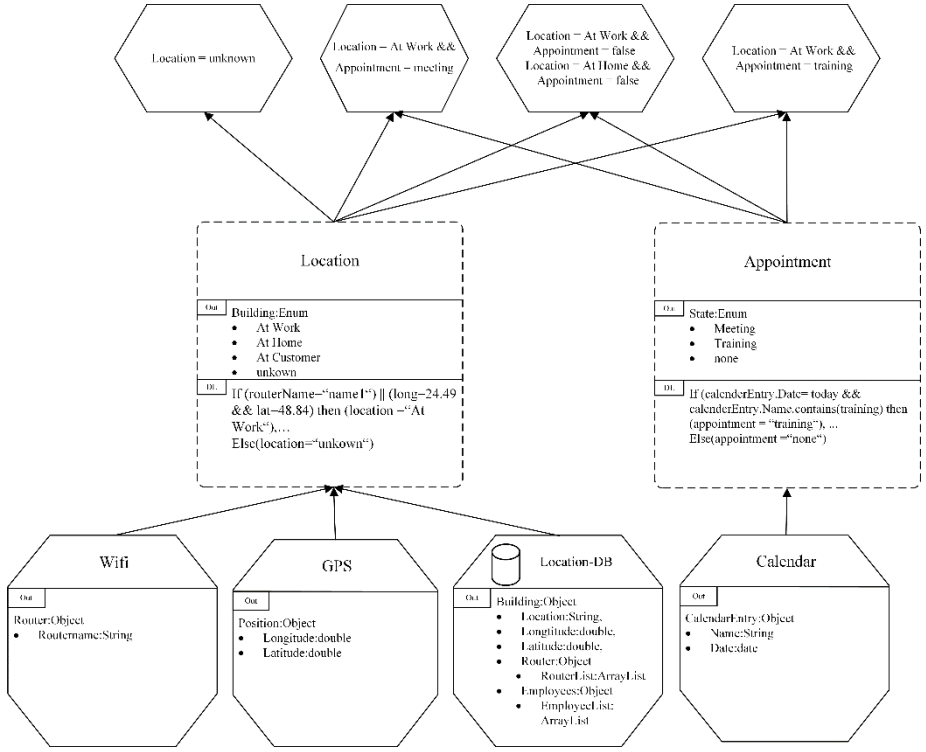


Figure 2. Sensor model for the contexts *location* and *appointment*

The next context parameter is *appointment* with its variables *meeting, training* and *none*. If the context is *location* is *at work* and context *appointment* is *training* the mobile application reminds the user to attend the sales training. Therefore, they are capable to automatically adapt the application to the context of the user. At the bottom line, the sensors are represented. For the context *location*, which is represented in the dotted rectangle above, the physical sensors *Wifi*, *GPS* and the virtual sensor *Location-DB* are needed. The GPS sensor returns an object, consisting of a long- and latitude double to compute the position of the salesperson. In the center of the figure, the context elements are represented. The *DL* areas show when an *appointment* is a *meeting* or *training*, respectively when the *location* is *at work, at home, at the customer* or *unknown*. For example, if the calendar entry is today and the entry description contains the name *training*, the salesperson should be part of the training. At the top of the figure are the context expressions related to the context elements. They are also the connection to the related context-aware business process. This example shows that it is possible to model the context evaluation for mobile context-aware business processes with SenSoMod. It enables to model the aggregation of information from the basic sensor information to the context expressions.

4 Evaluation

The aim of the design science research (DSR) is to create artifacts for a specific purpose that solve a practice oriented problem [29, 35]. One core activity in DSR is the evaluation of the created artifact to prove and justify its usefulness [36]. In the literature of DSR several methods to conduct an evaluation of a developed artifact exist, like mathematical proofs, case studies, surveys, or (lab) experiments, to name just a few [37, 38]. Since the experimental approach is suited for a systematic assessment of an information system artifact's qualities [39], it was chosen as the approach to evaluate the domain specific modeling language SenSoMod.

4.1 Evaluation Design

A classic experiment is conducted by having two groups divided into a so-called *test group* and a *control group*. The *test group* is "exposed to the stimulus (like the new or better design)" [39] whereas the *control group* is not. The reactions of the participants of both groups are compared to each other with the aim to distinguish reality (results of the experiment) from wishful thinking (expected improvement of the artifact). The participants of the experiment should be randomly assigned to either the test or the *control group*. For the data acquisition, one can use for instance a questionnaire, observation, or data transmission instruments (like an eye-tracker). From this data the researchers can derive whether an artifact proved its usefulness or not [39].

The described framework to conduct an experiment in the information system area was used to evaluate SenSoMod. The participants of the two groups had to fulfill the same task: In an office building, there are printers that will report to a smartphone application to change the cartridge when it is empty. If the user is nearby the mobile app

gives a notification. The modeling task of this use case was the information aggregation (printer sensors and smartphone sensors). In the *test group*, the participants had to model this task with SenSoMod, whereas the participants of the *control group* were free to use their preferred modeling language to succeed the task. The task had to fulfill certain criteria like representing a real-world example which is practical and complex enough to rule out trivial models, but at the same time, it had to be manageable for the participants. After the modeling, the *control group* saw a video which explained the language to them and showed how to model the task with SenSoMod. At the end, both groups received a questionnaire to judge the key features of SenSoMod. In addition, the participants in both groups were clocked during the task to observe how the new language can cope with known languages (like UML or BPMN). The aim of the evaluation was to target experienced developers and modelers to implement mobile applications, since this is the target group for the language. In total 15 practitioners took part in the experiment, 10 in the *test group* and 5 in the *control group*. The unbalanced groups are caused by randomly selected practitioners deciding not to attend the experiment after they were chosen.

4.2 Results

After conducting the experiment, the submitted questionnaires were carefully examined by two researchers independently. The results of each group were compared to each other to identify differences. All results from the participators were applicable in terms of consistency and completeness, and remain for further analysis.

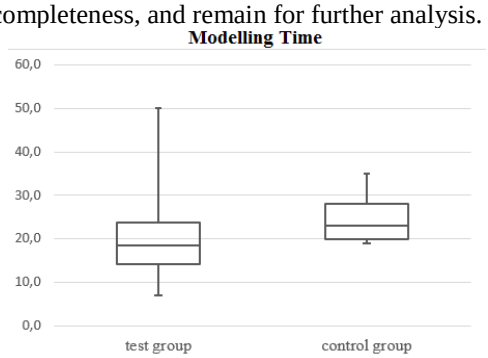


Figure 3. Box plot diagram of the modeling time

The upper limit for the modeling time in the *test group* is 50 minutes (cf. **Figure 3**). However, with Grubbs' [40] formula to determine outliers, this value is a weak outlier. So, if this value can be left out the upper limit would be 35 minutes. The upper limit of the *control group* is also 35 minutes. The average time in the *test group* was 18.1 minutes (with the outlier 21.3 min) with a standard deviation of 7.8 minutes (12.1 min), while in the *control group* it was 25 minutes with a standard deviation of 5.9 minutes. The conclusion of this data is that modeling with SenSoMod does not take longer than with other (preferred) modeling languages, although the *test group* had never seen the language before. It also seems that the *test group* is slightly faster. However, this trend should be investigated further with a bigger group of participants to confirm it. Both

groups had to answer a questionnaire at the end of the experiment. All questions regarding their opinion of SenSoMod were answered on a Likert-scale [41] with 5 answer options ranging between *applies* and *applies not*. The results for every question and group can be seen in **Table 2** and **Table 3**.

Table 2. Answers from the *test* group

	applies	applies rather	neither	applies rather not	applies not
Did you find the modeling language SenSoMod understandable? (All)	10%	70%	0%	20%	0%
Did you find the modeling language SenSoMod understandable? (Experienced modeler)	14%	71%	0%	14%	0%
Were you able to distinguish the individual elements of SenSoMod well from each other?	40%	20%	10%	30%	0%
Do you think that modeling only with SenSoMod can facilitate the implementation of mobile context-sensitive applications? (All)	10%	40%	30%	10%	10%
Do you think that modeling only with SenSoMod can facilitate the implementation of mobile context-sensitive applications? (Experienced developer)	20%	60%	20%	0%	0%
Do you think that a modeling tool for SenSoMod, which enables automatic generation of classes and methods, can facilitate the implementation of mobile context-sensitive applications?	50%	40%	0%	0%	10%
Do you think that SenSoMod makes it easier to collaborate with the business user of the app, by displaying the context aggregation graphically, thus making it easier to explain how the application adapts to the context?	40%	50%	0%	0%	10%

Table 3. Answers from the *control* group

	applies	applies rather	neither	applies rather not	applies not
Did you find the modeling language SenSoMod understandable? (All)	20%	60%	0%	20%	0%
Did you find the modeling language SenSoMod understandable? (Experienced modeler)	25%	50%	0%	25%	0%
Were you able to distinguish the individual elements of SenSoMod well from each other?	20%	60%	0%	20%	0%
Do you think that modeling only with SenSoMod can facilitate the implementation of mobile context-sensitive applications? (All)	40%	20%	20%	20%	0%
Do you think that modeling only with SenSoMod can facilitate the implementation of mobile context-sensitive applications? (Experienced developer)	50%	25%	0%	25%	0%
Do you think that a modeling tool for SenSoMod, which enables automatic generation of classes and methods, can facilitate the implementation of mobile context-sensitive applications?	20%	20%	40%	20%	0%
Do you think that SenSoMod makes it easier to collaborate with the business user of the app, by displaying the context aggregation graphically, thus making it easier to explain how the application adapts to the context?	60%	20%	20%	0%	0%

To get a better understanding how experienced modelers and developers think about SenSoMod, we distinguished between experts and inexperienced participants for two question. Overall the result is positive for SenSoMod. In both groups, SenSoMod was seen as understandable (slightly better within the group of experienced modelers) and can help to create mobile context-aware applications (also slightly better within the group of experienced developers). Only the differentiation between the elements was not clearly supported. The penultimate question targets the next step for the language, to create a tool able to generate classes from the model. Participants of both groups majoritarian stated that this could help to implement context-aware apps. Overall, this experiment showed that SenSoMod can be supportive for implementing apps which

change their behavior based on context information. However, the results of this experiment have to be confirmed in a second round with more participants.

5 Outlook and Further Research

The main contribution of this article is to show how the modeling language for the context evaluation can be used to ease the implementation of supportive mobile context-aware business processes. It provides the possibility for model engineers to plan such processes in a precise, detailed and comprehensive way. It also enables programmers to reuse the decision logic used in the sensor model for the source code of the application. Therefore, it can improve the interaction between modelers and programmers and accelerate the adaption of business processes. To further confirm the positive results of the evaluation a second evaluation should take place with more participants.

There are some tasks for further research in this area: Since mobile context sensitive business processes obviously need to measure context and are supported by an application on smart devices, an automated or semi-automated way to generate code from the business process would be helpful to increase the flow between modeling and implementation phase. The logical context expressions can be used to generate decisions in the application program.

References

1. Prümper, J., Lorenz, C., Hornung, S., Becker, M.: Abschlussbericht der Studie: „Mobiles Arbeiten". spring Messe Management GmbH, Frankfurt am Main (2016)
2. Morabito, V. (ed.): Trends and challenges in digital business innovation. Springer, Cham (2014)
3. Hammer, M., Champy, J.: Reengineering the corporation. A manifesto for business revolution. Harper Business, New York, NY (1993)
4. Becker, J., Kugeler, M., Rosemann, M. (eds.): Process management. A guide for the design of business processes. Springer, Berlin (2011)
5. Vom Brocke, J., Rosemann, M. (eds.): Handbook on Business Process Management 2. Strategic Alignment, Governance, People and Culture. Springer-Verlag Berlin Heidelberg, Berlin, Heidelberg (2010)
6. Scheer, A.-W.: ARIS - Business Process Modeling. Springer, Berlin u.a. (2000)
7. Bichler, M., Frank, U., Avison, D., Malaurent, J., Fettke, P., Hovorka, D., Krämer, J., Schnurr, D., Müller, B., Suhl, L., et al.: Erratum to. Theories in Business and Information Systems Engineering. Bus Inf Syst Eng (2016)
8. Harmon, P., Wolf, C.: The State of Business Process Management 2016 (2016)
9. Falk, T., Leist, S.: Effects of mobile solutions for improving business processes. In: Avital, M., Leimeister, J.M., Schultze, U. (eds.) ECIS 2014 proceedings. 22th European Conference on Information Systems ; Tel Aviv, Israel, June 9-11, 2014. AIS Electronic Library (2014)
10. Dey, A.K.: Understanding and Using Context. Personal and Ubiquitous Computing 5, 4–7 (2001)

11. Heinrich, B., Lewerenz, L.: A Novel Concept for the Usage of Mobile Information Services. In: Linnhoff-Popien, C., Zaddach, M., Grahl, A. (eds.) Marktplätze im Umbruch. Digitale Strategien für Services im mobilen Internet, pp. 319–329. Springer Vieweg, Berlin (2015)
12. Dörndorfer, J., Seel, C.: The impact of mobile devices and applications on business process management. In: Barton, T., Herrmann, F., Meister, V., Müller, C., Seel, C. (eds.) Prozesse, Technologie, Anwendungen, Systeme und Management 2016. Angewandte Forschung in der Wirtschaftsinformatik, pp. 10–19 (2016)
13. Schilit, B., Adams, N., Want, R.: Context-Aware Computing Applications. In: First Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 85–90 (1994)
14. Schmidt, A., Beigl, M., Gellersen, H.-W.: There is more to context than location. Computers & Graphics 23, 893–901 (1999)
15. Weiser, M.: The Computer for the 21st Century. Sci Am 265, 94–104 (1991)
16. Dey, A.K.: Providing Architectural Support for Building Context-aware Applications. Georgia Institute of Technology, Atlanta, GA, USA (2000)
17. Rosemann, M., Recker, J.C., Flender, C.: Contextualisation of business processes. International Journal of Business Process Integration and Management 3 (1), 47–60 (2008)
18. Rosemann, M., Recker, J., Flender, C.: Designing context-aware Business Processes. In: Siau, K., Chiang, R., Hardgrave, B.C. (eds.) Systems analysis and design. People, processes and projects, pp. 51–73. M.E. Sharpe, Armonk, NY u.a (2011)
19. Soffer, P.: On the Notion of Flexibility in Business Processes. In: Proceedings of the CAiSE'05 Workshops, pp. 35–42 (2005)
20. Rosemann, M., van der Aalst, W.M.P.: A configurable reference modelling language. Information Systems 32, 1–23 (2007)
21. Saidani, O., Nurcan, S.: Towards Context Aware Business Process Modelling. In: Workshop on Business Process Modelling, Development, and Support, p. 1. Norway (2007)
22. Heinrich, B., Schön, D.: Automated Planning of Context-aware Process Models. University of Münster, Münster, Germany (2015)
23. Conforti, R., La Rosa, M., Fortino, G., ter Hofstede, A.H.M., Recker, J., Adams, M.: Real-time risk monitoring in business processes. A sensor-based approach. Journal of Systems and Software 86, 2939–2965 (2013)
24. Dörndorfer, J., Seel, C.: A Meta Model Based Extension of BPMN 2.0 for Mobile Context Sensitive Business Processes and Applications. In: Leimeister, J.M., Brenner, W. (eds.) Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI), pp. 301–315. St. Gallen (2017)
25. Al-alshuhai, A., Siewe, F.: An Extension of Class Diagram to Model the Structure of Context-Aware Systems. In: The Sixth International Joint Conference on Advances in Engineering and Technology (AET) (2015)
26. Al-alshuhai, A., Siewe, F.: An Extension of UML Activity Diagram to Model the Behaviour of Context-Aware Systems. In: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), pp. 431–437 (2015)
27. Kramer, D., Clark, T., Oussena, S.: MobDSL. A Domain Specific Language for multiple mobile platform deployment. In: 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications, pp. 1–7. IEEE (2010)

28. Ranabahu, A.H., Maximilien, E.M., Sheth, A.P., Thirunarayan, K.: A domain specific language for enterprise grade cloud-mobile hybrid applications. In: Lopes, C.V. (ed.) Proceedings of the compilation of the co-located workshops on DSM'11, TMC'11, AGERE!'11, AOOPES'11, NEAT'11, & VMIL'11 - SPLASH '11 Workshops, p. 77. ACM Press, New York, New York, USA (2011)
29. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Q 28, 75–105 (2004)
30. Moody, D.: The "Physics" of Notations. Toward a Scientific Basis for Constructing Visual Notations in Software Engineering. IIEEE Trans. Software Eng. 35, 756–779 (2009)
31. Genon, N., Heymans, P., Amyot, D.: Analysing the Cognitive Effectiveness of the BPMN 2.0 Visual Notation. In: Malloy, B., Staab, S., van den Brand, M. (eds.) Software language engineering. Third international conference, SLE 2010, Eindhoven, The Netherlands, October 12 - 13, 2010 ; revised selected papers, 377-369. Springer, Berlin (2011)
32. Biederman, I.: Recognition-by-components. A theory of human image understanding. Psychological Review 94, 115–147 (1987)
33. Internet Engineering Task Force: The JavaScript Object Notation (JSON) Data Interchange Format (2014)
34. Backus, J.W., Wegstein, J.H., van Wijngaarden, A., Woodger, M., Bauer, F.L., Green, J., Katz, C., McCarthy, J., Perlis, A.J., Rutishauser, H., et al.: Report on the algorithmic language ALGOL 60. Commun. ACM 3, 299–314 (1960)
35. March, S.T., Smith, G.F.: Design and natural science research on information technology. Decision Support Systems 15, 251–266 (1995)
36. Peffers, K., Rothenberger, M., Tuunanen, T., Vaezi, R.: Design Science Research Evaluation. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B. et al. (eds.) Design Science Research in Information Systems. Advances in Theory and Practice, 7286, pp. 398–410. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
37. Cleven, A., Gubler, P., Hüner, K.M.: Design alternatives for the evaluation of design science research artifacts. In: Vaishanvi, V., Purao, S. (eds.) Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09, p. 1. ACM Press, New York, New York, USA (2009)
38. Venable, J., Pries-Heje, J., Baskerville, R.: A Comprehensive Framework for Evaluation in Design Science Research. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B. et al. (eds.) Design Science Research in Information Systems. Advances in Theory and Practice, 7286, pp. 423–438. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
39. Mettler, T., Eurich, M., Winter, R.: On the Use of Experiments in Design Science Research. A Proposition of an Evaluation Framework. Communications of the Association for Information Systems 34, 223–240 (2014)
40. Grubbs, F.E.: Procedures for Detecting Outlying Observations in Samples. Technometrics 11, 1–21 (1969)
41. Likert, R.: A Technique for the Measurement of Attitudes. New York, NY (1932)

Role-based Adaptation of Domain Reference Models: Suggestion of a Novel Approach

Hendrik Schön[1]

[1] TU Dresden, Business Informatics, esp. IS in Trade and Industry, Dresden, Germany
hendrik.schoen@tu-dresden.de

Abstract. Reference models capture domain knowledge for reuse and specification through user-defined adaptation. They work as a blueprint for either structure or processes, and the user can apply adaptations to fit specific demands. This research-in-progress paper is about a novel approach that combines reference model adaptation with the concept of roles in order to strictly separate the core elements from user made adaptations. The advantage of using roles as the sole adaptation mechanism is threefold: (a) the structure of the reference model can be combined with behavior of objects, (b) the exclusive use of roles allows broad adaptation without the restriction of other mechanisms (like inheritance) with more expressiveness, and (c) current reference models can continue to be used without modification. Consequently, the roles enriched final application model can be used to describe systems in more detail, and, if available, can be implemented with a role supporting programming language.

Keywords: reference model, enterprise domain model, adaptation, roles

1 Introduction

Reference models are intended to support the derivation of software system construction plans by capturing domain knowledge for reuse and specification through user-defined adaptation [1, 2]. They work as a blueprint for either structure or processes, and the user can apply his adaptations to fit specific demands [3] in order to produce a derived model in a specific context (application model) in a way that allows to easily benefit from further reference model evolution [1, 3]. If continually developed by communities of experts, these reference models promise to capture domain knowledge of highest quality while also being up-to-date. However, insufficient or not uniformly managed possibilities in the reuse process are often the cause of limited reference model exploitation. The paper at hand presents the outline of an approach that is intended to solve this problem for object-oriented models (e.g., structural models). Model adaptation is based on the concept of roles, which is introduced in section 2. Section 3 describes how to adapt business objects via roles, while section 4 outlines the overall approach that strictly separates responsibilities for model evolution (reference model owner) and model adaptation (any model user), thus allowing for convenient model co-evolution.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

2 Roles for Enterprise Modeling and Software Engineering

When building object-oriented (OO) systems, objects, their relationships, and the specialization of objects (mostly implemented as inheritance) are the basic building blocks. Besides those main elements, the concept of roles in conceptual modeling is very intuitive [4–8] but rarely used. Roles can enhance the overall process of system construction as they deliver the possibility of adding structural and behavioral elements to an object, allowing its instances to use this role (and other roles) at some time during their lifetime without changing their identity. Although the relational nature of roles is supported in some modeling languages such as UML via labels at association ends, its behavioral and contextual nature offers untapped potential [9].

We use the concept of roles for enterprise modeling at the conceptual level in a way that supports the transition into system design. We can use roles for finely grained definitions of state and behavior of model elements, allowing us to describe an object with its different aspects. In this context, we define our role concept as follows:

> *A role is a contextual modeling construct with state and behavior that is attached to a (business) object to represent it in the user's context and extend or change its corresponding specifications and interactions. However, a role does not modify identity: When either permanently or temporarily attaching a role instance to an object instance, the object instance's identity remains unchanged.*

This definition correlates with various properties in [6] (e.g., 1, 3, 8, and 14) and rejects or leaves untapped a few others (like 2 and 15). Several authors [6, 8, 10] provide a broad overview of other role definitions. In an enterprise context, the main objects of domain models (objects regarding the domain, means classes not instances) typically need adaptation depending on context or use case. Specifically, in the case of so-called reference models, which aim to capture domain knowledge at a more generic level, adaptation is needed to derive the so-called application models from the reference. Therefore, we suggest roles as an adaptation mechanism of structural domain models. Besides roles, we will make use of some other role-related concepts to fully capture our approach's possibilities, most importantly compartments (objectified contexts, where roles get a further meaning in order to support the contextual nature of roles [6]).

Our main research goal, therefore, is to develop a method on how roles can be used for business object adaptation and to thereby improve the general reference model adaptation process and extend its practical usefulness. We assume that roles in combination with our method overcome common OO-based modeling issues [8] by:

- combining structure and behavior of the model elements (especially objects) in a flexible way, leading to more expressiveness,
- providing a structured and traceable way of business object adaptation without the restrictions of inheritance or other hierarchy-based mechanisms,
- implementing the adaptation without changes to the established (industry standard) reference models, allowing the user to benefit from our approach easily,
- enabling multiple viewpoints and adaptations of single model elements in different ways as well as including one element multiple times within the adaptation.

3 Business Object Adaptation via Roles

We use native role mechanisms as a substitution for traditional OO adaptation mechanisms. By adapting an object via a role, the object itself and its interaction with other model elements is changed. The adaptation of an object is thus achieved by the role providing the corresponding properties that are required as delta concerning the original object [11, 12]. Simply stated, this means that, e.g., a required attribute is added by assigning an appropriate role to the underlying object that contains the new attribute (as a delta). The original object can further be used for other purposes (future adaptations with new roles), is traceably adapted and not invasively modified, and its instances take on the roles but retain their identity.

Therefore, the applied roles should meet the user's adaptation intentions. We outline three different actions that are common in literature and that the user may use to adapt an object: adding (ADD), modifying (MOD), and removing (DEL) (e.g., [11, 13, 14]). Other works mention additional actions like selection [15] or extension [11]. While these are also possible user actions, they usually can be replaced by the other three. The core idea of our method is the result of an adaptation as a delta description compared to the original item, using the possibilities and benefits of the role mechanism to overcome traditional OO issues and to support role-based system design as an initial construction approach with detailed object descriptions [7].

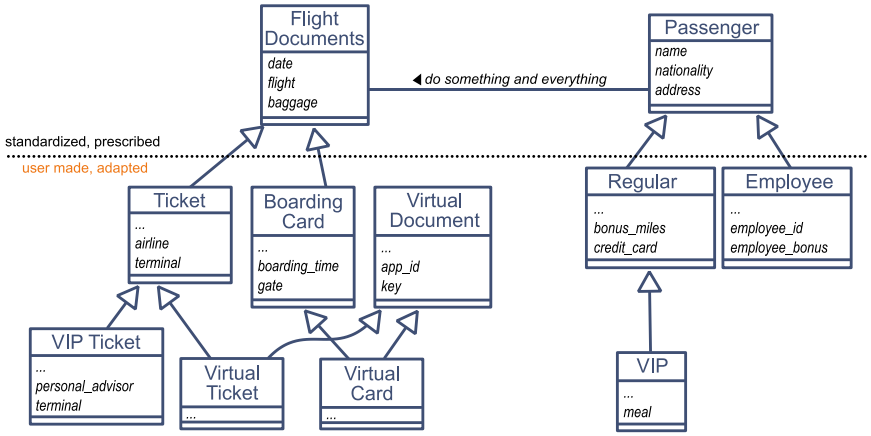


Figure 1. Example of a flight document domain adaptation with object orientation

We further differentiate roles into those that exist only by relationships to other roles ("founded role"), organized within compartments, and those without this restriction ("non-founded"). The latter are used to represent the specifications of an object that only affect the object itself, while the founded roles exist only through a relationship with another object. This allows us to separate the adaptation with regard to specifications or interactions of an object. As an example, we use a sample domain as depicted in figure 1. The adaptation is based on traditional OO mainly using inheritance with known issues (e.g., multiple object identities, lack of flexibility, hierarchy-based

misconceptions). In figure 2 we see the same domain using roles for adaptation. The objects (“ticket” and “passenger”) are represented by non-founded roles and connected through founded roles within a compartment. The non-founded roles, to which the founded roles are attached (a role attached to another role), represent the various types of objects, using founded roles as interfaces to represent the association between the objects. Both business objects are "preserved" as is and their instances keep their identity all the time. The example shows how each role has its own delta, and how the status and behavior can be adapted explicitly. Furthermore, it would now be possible to add more roles. It would also be possible to completely redesign the object at the same time since an object can use any number of roles from any viewpoints, while leaving the original object untapped.

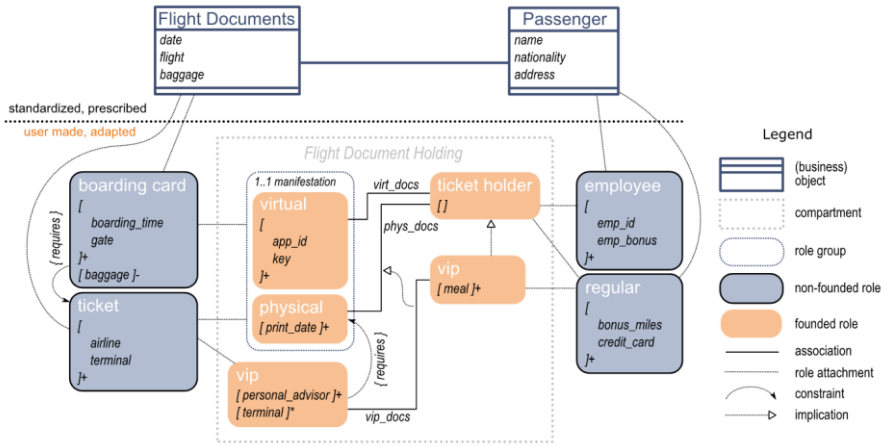


Figure 2. The role-based flight document domain adaptation

Firstly, after a user-defined selection of relevant business objects from the domain model, the selected objects become the origin of our role-based model. They keep those operations and attributes that are initially provided by the reference model. Secondly, we set the characteristics of that object and identify every possible role for it that does not exist only through a relationship. Thirdly, we take care of the founded roles, which exist due to relationships to other objects’ roles. Those roles specify the object within a special context, the compartment. They work as interfaces but do not necessarily have to carry any delta attribute or operation. Nevertheless, they must contain the needed delta for fulfilling the compartment contract. Finally, the founded roles are connected by necessary relationships. Normal associations are therefore drawn between those roles, which should act together, and can be directed or undirected. Their identifier is their main activity or characteristic. Then the constraints are inserted, which allow certain expressions (e.g., exclusion, request, or sequential). Constraints between roles and relationships are allowed, too. Overall, we never change the elements of the original reference model, neither the objects nor the “general” relationships. Within the example in figure 2 we can determine some new features as well: (a) aside of adding things [+],

we could remove [-] or alter items [*]; (b) we can use role groups and multiplicities; (c) roles can be attached to roles; (d) elements can imply each other; and (e) we may use logical, sequential and temporal constraints. In general, many other role features may be applicable to our method [6] to support more possibilities of adaptation.

4 Model Tiers, Evolution, and Adaptation

As claimed in previous sections, the benefits of using roles are advantageous for the case of reference model adaptation and system design. We follow the common approach of the two tiers within the adaptation process (see figure 3).

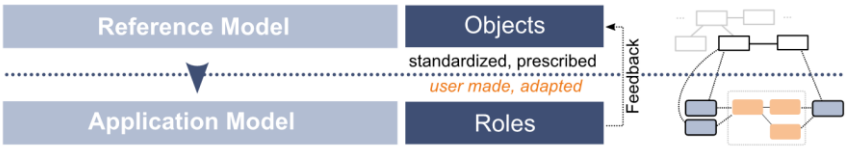


Figure 3. Two tiers (models) of the reference model adaptation process

This two-layered system of models ensures separation of the initial reference model with its template elements (objects and relationships), as well as their user-defined adaptation, as long as we do not invasively change parts of the original reference model. The idea behind a strict separation is twofold: (a) the once adapted application model is fully covered due to non-invasive adaptation processes while an evolution of the underlying reference model occurs, and (b) the user adaptation is handled with the possibility of multi-usage and variant development.

The Reference Model Tier. This first model maps the overall domain knowledge. This layer is fully in hand of the model owner and therefore out of control of the user, as represented by the horizontal dotted line in figure 3. This restriction allows the model owner to be in charge of the reference model's evolution. By strictly separating the adaptation from the reference model and its primary elements, a co-evolution will be possible [16], thus enabling an easier adjustment of any application model towards the new standard reference model, if necessary. The separation in combination with the non-invasive property of our role-based method makes it possible to track and realize (formally expressed) changes to the reference model, as represented in figure 4.

The Application Model Tier. After the user's selection of relevant objects, the construction of the final application model as an adapted version of the original reference model is carried out. The main items within this model are roles, attached to selected objects. In this tier, the user starts to adapt the selected objects as described in the previous section. This again ensures the strict separation.

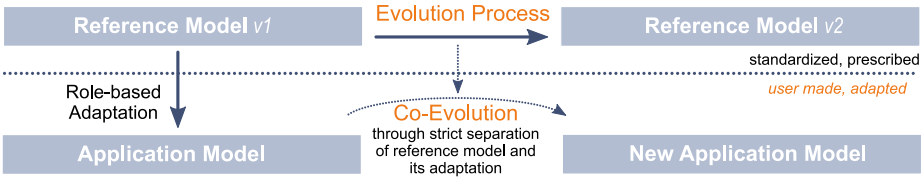


Figure 4. The possibility of co-evolution as a benefit of role-based adaptation

5 Related Work

In research, much literature exists about general or process-oriented reference modeling and adaptation. Less work has been done towards properly defined adaptation mechanisms for structural conceptual models in UML, much less regarding roles (e.g. [4, 5]). For the usage of roles in general, there are several works considering their nature (e.g., [6, 10]) and their applicability (e.g., [7, 9]), which can be used for our approach. In addition, some more specific topics are relevant and relate to ours, e.g., the technical implementation of adaptation [11, 12, 17]. Overall, our research addresses some of the potential topics called for in [1], especially the "modeling languages and methods".

6 Next Steps

The proposed method of role-based reference model adaptation is research in progress. We intend to develop certain artifacts on our design science research roadmap: a well-defined method for our approach for role-based adaptation with necessary sub-artifacts such as a domain specific language (DSL), a meta-model, its formalism, a worked out non-trivial example, and a tool for supporting our adaptation method. Our next step will be to define the foundational basis of role-based adaptation. Based on this, we will try to formalize the adaptation process for two reasons: (a) to check integrity and constraints, and (b) to exploit automation options. We plan to develop tool support, where DSL and formalism are needed. As the last step, we will evaluate our method (e.g., like [18]) by comparing it to traditional adaptation for a real use-case model.

With the help of roles, it will be possible to create rich model variations and adaptations to existing domain models. Further, it will become simpler to react on model evolution. Adaptations can be specified with more precision and thus will maintain and likely increase the model's expressiveness. This approach allows the specific integration of structure and behavior of different views. It also supports transformation towards implementation by fine-grained development details.

7 Acknowledgements

This work is funded by the German Research Foundation (DFG) within the Research Training Group „Role-based Software Infrastructures for continuous-context-sensitive Systems" (GRK 1907).

References

1. Frank, U., Strecker, S., Fettke, P., vom Brocke, J., Becker, J., Sinz, E.: The Research Field "Modeling Business Information Systems." Bus. Inf. Syst. Eng. 6, 39–43 (2014).
2. Thomas, O.: Understanding the Term Reference Model in Information Systems Research: History, Literature Analysis and Explanation. In: Business Process Management Workshops. pp. 484–496. Springer, Berlin, Heidelberg (2005).
3. Fettke, P., Loos, P.: Using Reference Models for Business Engineering - State-of-the-Art and Future Developments. Innov. Inf. Technol. (2006).
4. Steimann, F.: On the representation of roles in object-oriented and conceptual modelling. Data Knowl. Eng. 35, 83–106 (2000).
5. Almeida, J.P.A., Guizzardi, G.: On the foundation for roles in RM-ODP: Contributions from conceptual modelling. In: 2007 Eleventh International IEEE EDOC Conference Workshop. pp. 205–215. IEEE (2007).
6. Kühn, T., Leuthäuser, M., Götz, S.: A Metamodel Family for Role-Based Modeling and Programming Languages. In: Combemale, B., Pearce, D.J., Barais, O., and Vinju, J.J. (eds.) Software Language Engineering. pp. 141–160. Springer, Västerås, Sweden (2014).
7. Riehle, D., Gross, T.: Role Model Based Framework Design and Integration. In: Proceedings of the 13th ACM SIGPLAN Conference on Object-oriented Programming, Systems, Languages, and Applications, OOPLSA. pp. 117–133. ACM, New York, NY, USA (1998).
8. Frank, U.: Delegation: An important concept for the appropriate design of object models. J. Object Oriented Program. 13, 13–17 (2000).
9. Steimann, F.: Role = Interface : A Merger of Concepts. J. Object-Orientated Program. 23–32 (2001).
10. Steimann, F.: A Radical Revision of UML's Role Concept. University of Hannover, Hannover (2000).
11. Schaefer, I., Damiani, F.: Pure delta-oriented programming. In: Proceedings of the 2nd International Workshop on Feature-Oriented Software Development, FOSD. pp. 49–56. ACM Press, Eindhoven, The Netherlands (2010).
12. Jarzabek, S., Ong, W.C., Zhang, H.: Handling variant requirements in domain modeling. J. Syst. Softw. 68, 171–182 (2003).
13. Cazzola, W., Ghoneim, A., Saake, G.: Software Evolution through Dynamic Adaptation of Its OO Design. In: Ryan, M.D. (ed.) Objects, Agents, and Features: International Seminar, Revised and Invited Papers. pp. 67–80. Springer Berlin Heidelberg (2004).
14. Recker, J., Mendling, J., van der Aalst, W., Rosemann, M.: Model-Driven Enterprise Systems Configuration. In: Dubois, E. and Pohl, K. (eds.) Advanced Information Systems Engineering. pp. 369–383. Springer, Luxembourg, Luxembourg (2006).
15. Hofreiter, B., Huemer, C., Kappel, G., Mayrhofer, D., vom Brocke, J.: Inter-organizational Reference Models – May Inter-organizational Systems Profit from Reference Modeling? In: Ardagna, C.A., Damiani, E., Maciaszek, L.A., Missikoff, M., and Parkin, M. (eds.) Business System Management and Engineering: From Open Issues to Applications. pp. 32–47. Springer Berlin Heidelberg (2012).
16. Hebig, R., Khelladi, D.E., Bendraou, R.: Approaches to Co-Evolution of Metamodels and Models: A Survey. IEEE Trans. Softw. Eng. 43, 396–414 (2017).
17. Weber, B., Reichert, M., Rinderle-Ma, S.: Change Patterns and Change Support Features - Enhancing Flexibility in Process-aware Information Systems. Data Knowl Eng. 66, 438–466 (2008).
18. Krogstie, J.: SEQUAL as a Framework for Understanding and Assessing Quality of Models and Modeling Languages. Int. J. Inf. Syst. Model. Des. 3, 24–45 (2012).

Enterprise Architecture Management in dynamischen Wertschöpfungsnetzwerken – Empfehlungen zur Interoperabilität

Jens F. Lachenmaier[1], Kathrin Pfähler[1] und Hans-Georg Kemper[1]

[1] Universität Stuttgart, Lehrstuhl für Wirtschaftsinformatik 1, Stuttgart, Germany
lachenmaier,pfaehler,kemper@wi.uni-stuttgart.de

Abstract. Bestehende Enterprise-Architecture-Management-Ansätze fokussieren in der Regel ein einzelnes Unternehmen oder eine Organisation. In der Praxis finden sich jedoch auf Grund zunehmender Spezialisierung häufig dynamische Wertschöpfungsnetzwerke und zweckgebundene Zusammenschlüsse verschiedener Unternehmen. Damit diese erfolgreich sein können, müssen die Unternehmensarchitekturen der beteiligten Organisationen aufeinander abgestimmt werden. Dies betrifft nicht nur die technische Ebene der Schnittstellen, sondern auch die Geschäftsebene mit Prozessen und Rollen. Im vorliegenden Beitrag werden auf Basis der gesammelten Erfahrung in einem Projekt zur Entwicklung von Referenzarchitekturen für intelligente Verkehrsdienste (IVS) Empfehlungen erarbeitet, wie vorgegangen werden kann, um Unternehmensarchitekturen auf die Zusammenarbeit mit anderen Organisationen vorzubereiten. Dabei wird ein gestaltungsorientierter Forschungsansatz verfolgt, bestehend aus Analyse-, Design und Evaluationsphase. Zentrale Pfeiler des Lösungsansatzes sind Capability-based Planning sowie Modellierung und Tailoring von Architektur-Artefakten.

Keywords: Enterprise Architecture Management, Unternehmensarchitektur, Intelligente Verkehrsdienste, Unternehmensnetzwerke, Capability-based-Planning

1 Einleitung und Ziel des Beitrags

Enterprise Architecture Management (EAM) umfasst die Entwicklung, Umsetzung und Pflege einer Unternehmensarchitektur eines spezifischen Unternehmens bzw. einer Organisation.[1] In großen Unternehmen handelt es sich meist nicht nur um eine, sondern häufig um mehrere Architekturen, die aufeinander abgestimmt werden müssen.[2] The Open Group Architecture Framework (TOGAF) geht an dieser Stelle bereits einen Schritt weiter und definiert eine Organisation über deren gemeinsame Ziele.[3] Ein solches gemeinsames Ziel kann die Erbringung einer gemeinsamen Leistung durch mehrere Unternehmen darstellen, die in einem dynamischen Wertschöpfungsnetzwerk zusammenarbeiten. Damit dieses gemeinsame Ziel erreicht werden kann, müssen die beteiligten Unternehmen eng zusammenarbeiten und auf allen

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Ebenen ihrer Unternehmensarchitekturen interoperabel werden. Das Thema des Beitrags ist demnach die Gestaltung von Unternehmensarchitekturen im Hinblick auf die ganzheitliche Interoperabilität zwischen Organisationen. Ziel ist es, Empfehlungen zu erarbeiten, welche Schwerpunkte dabei gesetzt werden können.

Die Autoren des vorliegenden Beitrags sind an einem Projekt zur Entwicklung von Referenzarchitekturen für intelligente Verkehrsdienste im Auftrag der Bundesanstalt für Straßenwesen beteiligt. Derartige Verkehrsdienste werden in einem Zusammenschluss von mehreren Unternehmen, Behörden und öffentlichen Einrichtungen erbracht. Die Erkenntnisse aus diesem Projekt werden im Rahmen des Beitrags abstrahiert, um Empfehlungen für die Modellierung und Gestaltung von Architekturen ableiten zu können.

2 Forschungsfrage, -methodik und Aufbau des Beitrags

Die Forschungsfrage des vorliegenden Beitrags lautet: „Welche Empfehlungen und Schwerpunkte können im Hinblick auf Interoperabilität mit anderen Organisationen bei der Entwicklung von Unternehmensarchitekturen festgelegt werden?“

Zur Beantwortung der Forschungsfrage orientiert sich der Beitrag an der gestaltungsorientierten Wirtschaftsinformatik, die sich der Design Science zuordnen lässt.[4-6] Anspruchsgruppen sind Unternehmensverbände, die gemeinsame Leistungen entwickeln und anbieten möchten. Das Ergebnis des Beitrags sind Empfehlungen zu Vorgehen, Modellierung und Tailoring in Form eines Leitfadens.

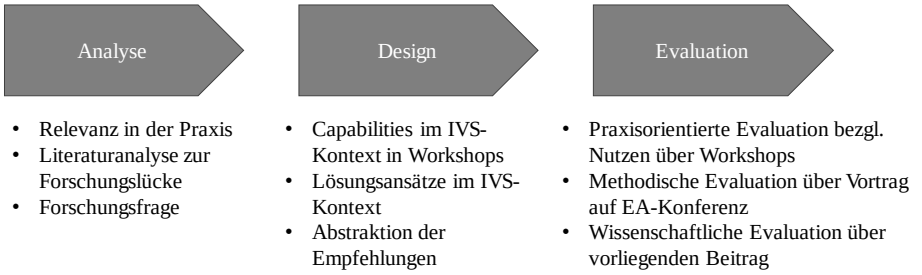


Abb. 1. Durchgeführter Forschungsprozess

Der Forschungsprozess deckt die Phasen Analyse, Design und Evaluation ab (siehe Abb. 1). Im Rahmen der Analysephase wird die Forschungslücke über eine Literaturanalyse nachgewiesen sowie die Forschungsfrage erarbeitet. Die Designphase basiert vor allem auf der Projekterfahrung der Autoren; hier werden in Workshops mit 15 beteiligten Unternehmen, öffentlichen Einrichtungen und Softwareentwicklungs- sowie Beratungshäusern Anforderungen erhoben und mögliche Lösungen diskutiert, was zu den anschließenden Empfehlungen führt. In der Evaluationsphase werden die Ergebnisse aus der Designphase im Rahmen des Forschungsprojekts einem Kreis von 55 Organisationen vorgestellt und hinsichtlich ihres Nutzens überprüft. Ergänzend dazu werden die Empfehlungen bezüglich des Vorgehens auf einer Konferenz Enterprise-

Architekten vorgestellt und intensiv hinsichtlich ihrer Sinnhaftigkeit und der korrekten Anwendung etablierter Methoden diskutiert. Die Evaluation im wissenschaftlichen Bereich und die Diffusion erfolgen durch diesen Beitrag.

Da im Projekt bereits mehrere Organisationen vertreten sind, die Referenzlösungen entwickeln, sind die Empfehlungen bereits abstrahiert, beziehen sich jedoch zunächst auf intelligente Verkehrsdienste. Im Folgenden wird daher nach einer kurzen Erläuterung der Grundlagen auf das Projekt näher eingegangen. In der anschließenden Diskussion wird die Übertragbarkeit der Empfehlungen erörtert und in einem abschließenden Ausblick der weitere Forschungsbedarf dargelegt.

3 Enterprise Architecture Management und Interoperabilität

Grundsätzlich hat EAMt zur Aufgabe, neben der Erstellung, Umsetzung, Pflege und Steuerung der Unternehmensarchitektur den hierfür benötigten strategischen, organisatorischen und konzeptionellen Rahmen sowie erforderliche Methoden, Werkezeuge und Prinzipien bereitzustellen.[1, 7]

TOGAF ist ein hierfür etabliertes Rahmenwerk und dient der Erstellung, Implementierung und Pflege einer Unternehmensarchitektur.[3] Eine Ausrichtung der Unternehmensarchitektur an die Bedarfe und Anliegen der Unternehmen bzw. Organisationen ist von TOGAF vorgesehen. Demnach erfolgt prinzipiell nach Aufnahme der Anliegen der Stakeholder eines Unternehmens die bedarfsgerechte Ausrichtung bzw. der bedarfsgerechte Aufbau einer Unternehmensarchitektur.[8] Damit die Anliegen der Stakeholder bedarfsgerecht abgedeckt werden können, müssen die benötigten Informationen identifiziert und in Form von Modellen oder Matrizen bereitgestellt werden.[9]

Eine klassische Unterteilung der Ausgangsprodukte der durchgeführten Architekturarbeit erfolgt durch TOGAF in Artefakte und Bausteine. Welche Bausteine und Artefakte für eine unternehmensübergreifende Zusammenarbeit relevant sind, wird im vorliegenden Beitrag beschrieben.

Der Ansatz des EAM kann in diesem Kontext genutzt werden, um ganzheitliche Interoperabilität innerhalb dynamischer Wertschöpfungsnetzwerke zu schaffen.[10] Interoperabilität bezeichnet die Fähigkeit, die Interaktion von mehreren Systemen mindestens auf den Ebenen der Prozesse, Daten und technischen Ressourcen sicherstellen zu können.[11] Im Hinblick auf eine Enterprise Interoperabilität bedeutet dies die Gewährleistung von Interaktionen auf rechtlicher (Gesetze und Regeln), organisatorischer (Strategie und Prozesse), semantischer (Informationen) und technischer Ebene (Anwendungen und IT-Infrastruktur), um eine erfolgreiche Zusammenarbeit zwischen verschiedenen Unternehmen zu ermöglichen.[12] Dabei wird darauf geachtet, einen Mehrwert für alle Beteiligten zu generieren. Gerade im öffentlichen Bereich ist Interoperabilität ein erstrebenswertes Ziel, das aktuell in europaweiten Projekten adressiert wird.[13]

4 Literaturanalyse zur Forschungslücke

Eine Literaturanalyse in Anlehnung an [14-16] wird zum Nachweis der Forschungslücke und zur Identifikation verwandter Arbeiten durchgeführt. Durchsucht wurden dazu die Datenbanken Business Source Premier, die AIS Library sowie einschlägige Fachzeitschriften (insbes. Journal of Enterprise Architecture). Ergänzend werden Lehrbücher und den Autoren bekannte Beiträge berücksichtigt. Der verwendete Suchstring (EAM OR „Enterprise Architecture“ OR Unternehmensarchitektur) AND (Kooperation OR cooperation OR Netzwerk OR Konsortium OR Network OR „supply chain“ OR „virtual enterprise“) erbrachte knapp 500 Treffer, die im Anschluss auf Basis der Titel und Abstracts gefiltert wurden. Die verbleibenden, relevanten Ergebnisse sind in der folgenden Tabelle aufgeführt (siehe Tabelle 1).

Tabelle 1. Ergebnisse der Literaturanalyse

Quelle	*Inhalt*	*Bezug zum vorliegenden Beitrag*
[17, 18]	Die Autoren benennen Lücken in der Forschung zu Unternehmensarchitekturen, dazu gehören virtuelle Unternehmen.	Unterstützung der Schließung der Lücke bei virtuellen Unternehmen.
[11]	Der Autor stellt den aktuellen Stand der Praxis im Bereich Interoperabilität vor.	Vorschläge werden teilweise aufgegriffen und erweitert.
[19]	Die Autoren stellen fest, dass sich die EAM-Forschung allgemein vor allem auf die Informationsebene bezieht und dass in der Geschäftsebene noch Forschungsbedarf besteht – insbesondere auch bei Unternehmensnetzwerken. Beispiele dafür sind [20, 21].	Es werden alle Ebenen betrachtet, insbesondere Strategie- und Geschäftsebene.
[22-24]	Erste umfangreiche Lösungen zur EA-Interoperabilität stammen vornehmlich aus dem Bereich der Produktion.	Der vorliegende Beitrag gibt Empfehlungen, auf welche Aspekte besonders geachtet werden sollte und wendet die Konzepte auf Mobilitätsdienste an.

Aus der Literaturanalyse wird ersichtlich, dass es bereits erste Arbeiten im Bereich der unternehmensübergreifenden Architekturgestaltung gibt; die Autoren sehen jedoch in Übereinstimmung mit der Literatur noch Lücken und weiteren Forschungsbedarf. Die vorhandenen Forschungsarbeiten zeigen ebenfalls deutlich die Relevanz des Themas für die Praxis und Forschung auf.

5 Ansätze zur Entwicklung organisationsübergreifender Unternehmensarchitekturen im Kontext intelligenter Verkehrsdienste

5.1 Projektbeschreibung und Beschreibung intelligenter Verkehrsdienste

Die Autoren sind an einem Projekt zur Entwicklung von Referenzarchitekturen für intelligente Verkehrsdienste beteiligt. Das Projekt hat zum Ziel, drei Referenzarchitekturen für die Dienstkategorien „multimodale Reiseplanung“, „individualisierte Reiseinformationen“ und „hoheitsübergreifendes Verkehrsmanagement“ zu entwickeln. Das Projekt begann Ende 2015 und endet Mitte 2018. Vergleichbare Initiativen gab und gibt es auch in anderen Ländern, u.a. Großbritannien und Australien.[25, 26]

Intelligente Verkehrsdienste sind informationsbasierte Services, die schlussendlich Reisende (sowohl Privatpersonen als auch bspw. Logistikunternehmen) bei der Planung ihrer Reise und der Durchführung u.a. durch Baustellen- und Verkehrsdaten unterstützen sollen. Intelligenten Verkehrsdiensten wird dabei ein enormes Potenzial zugesprochen, denn sie sollen langfristig ein effizientes, umweltverträgliches und sicheres Reisen über alle Verkehrsmittel hinweg ermöglichen. [27, 28]

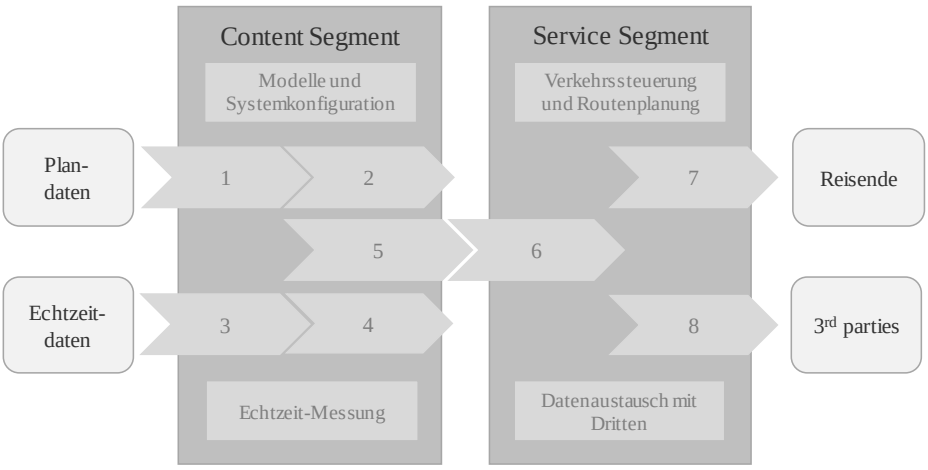


Abb. 2. Typischer Aufbau eines intelligenten Verkehrsdienstes

In der Regel werden intelligente Verkehrsdienste nicht von einem einzelnen Unternehmen erbracht, sondern eine Zusammenarbeit zwischen mehreren Organisationen ist erforderlich. Insbesondere sind neben privatwirtschaftlichen Unternehmen auch Kommunen, Behörden und weitere staatliche bzw. öffentliche Organisationen beteiligt. Grund dafür ist, dass meist die Rohdaten, die unter anderem von Straßenbetreibern oder Kommunen bereitgestellt werden (Content Segment), genutzt werden können, um verschiedene Dienste anzubieten (Service Segment). So

können Baustellendaten einerseits für die Navigation im Fahrzeug (Reisender), andererseits aber auch für eine Anreisesteuerung des Frachtverkehrs zu einer Messe (3rd parties) verwendet werden. Intelligente Verkehrsdienste können weiterhin neben Reisenden auch Behörden unterstützen, z.B. bei der Aufgabe, eine Ausweichroute bei Stau festzulegen. Der Unterschied liegt in der Aufbereitung der Daten und der darauf basierenden Funktionalität des Dienstes. (siehe Abb. 2) Private Unternehmen verfügen meist nicht über Möglichkeiten, ein komplettes Straßennetz zu überwachen oder sind aufgrund der Mengengerüste und dezentralen Planung auf die Weitergabe von Baustelleninformationen durch die jeweils verantwortlichen Behörden angewiesen.

Ergänzend können intelligente Verkehrsdienste auch aufeinander aufbauen. So kann ein Parkplatzassistent auf einem Navigationsdienst basieren, der von diesem die aktuelle Position, die Ankunftszeit und das Ziel der Reise erhält.

5.2 Ausgangssituation und Herausforderungen

Als Grundlage und Vorarbeiten für die Entwicklung der Referenzarchitekturen im Projekt gelten die europäische FRAME-Architektur und die Pyramide der intelligenten Verkehrssysteme (IVS-Pyramide). Die FRAME-Architektur beinhaltet Anforderungen an intelligente Verkehrssysteme und Hinweise zu deren funktionaler Gestaltung.[29] Darauf basierend ist erkannt worden, dass eine rein technisch-funktionale Betrachtung des Themas nicht ausreichend ist. Dies zeigt sich in der IVS-Pyramide. Diese macht deutlich, dass neben den IT-Aspekten auch organisatorische Aspekte bei Entwicklung und Betrieb von intelligenten Verkehrsdiensten zu berücksichtigen sind.[30] Die IVS-Pyramide ist grundsätzlich auf die Architekturebenen verschiedener EAM-Ansätze übertragbar, welche nach den Ebenen der Geschäfts-, Informations- und Technologiearchitektur unterscheiden.[7, 31] Jede an der Erbringung eines intelligenten Verkehrsdienstes beteiligte Organisation hat ihre eigene IVS-Pyramide, d.h. sie hat eigene Ziele, eigene Prozesse und eine eigene, individuelle IT-Infrastruktur. Beispielsweise können an einem multimodalen Reiseplanungsdienst diverse öffentliche Anbieter, wie Busgesellschaften oder Bahn, aber genauso Anbieter aus dem Individualverkehr, wie Navigationsdienstleister, beteiligt sein. Deren eigene, unternehmensbezogenen IVS-Pyramiden müssen angepasst werden, um eine Zusammenarbeit und Interoperabilität mit anderen Organisationen zu ermöglichen; gleichzeitig sollen aber die eigenen Unternehmensziele weiter bestehen bleiben und die Informationssysteme die internen Prozesse und Anforderungen abbilden.

Im Projekt wird mit dem EA-Framework TOGAF gearbeitet, wobei dieses angepasst werden muss, um bspw. neue Elemente wie Verträge mit aufzunehmen oder um die Interoperabilität zwischen den Unternehmen allgemein zu adressieren. Durch die Beteiligung vieler Unternehmen und Organisationen am Projekt soll bereits frühzeitig eine breite Akzeptanz für die Architekturen geschaffen werden und eine schnelle Adaption in der Praxis sichergestellt werden.

5.3 Lösungsansätze im Projekt und abgeleitete Empfehlungen

Grundsätzlich wird im Projekt das Capability-based-Planning angewendet.[32] Dabei werden insbesondere die Geschäftsfähigkeiten betrachtet, welche für die Zusammenarbeit in einem Netzwerk zur Erbringung eines gemeinsamen Services erforderlich sind. Basierend auf den Geschäftsfähigkeiten und den am Betrieb eines intelligenten Verkehrsdienstes erforderlichen Rollen werden dann die relevanten Architekturbausteine ausgewählt (siehe Abb. 3). Diese Auswahl relevanter Architekturbausteine ist verbunden mit der Anpassung des Vorgehensmodells zur Entwicklung einer Unternehmensarchitektur – der Architecture Development Method (ADM). Beides zusammen – also die Auswahl von Bausteinen und die Anpassungen der ADM – wird als Tailoring zusammengefasst.

Konkret wird im Projekt der Fokus auf Interoperabilität gelegt. Dazu werden im Projekt unter Anwendung der Szenariotechnik aus TOGAF in drei eintägigen Workshops der Projektbeteiligten aus den jeweiligen Domänen und einem Workshop des Leitungsgremiums folgende Capabilities zur Interoperabilität herausgearbeitet (Auswahl, siehe Tabelle 2):

Tabelle 2. Capabilities zur Interoperabilität im Projekt

Fähigkeiten	*Erklärung*
Flexible Vertragsschließung	Die Unternehmen müssen in dynamischen Netzwerken in der Lage sein, Vertragspartner und genaue Konditionen zu Datenlieferungen flexibel anzupassen.
Datenakquise und Datenaustausch, ebenso Bewertung und Integration von Daten	Die Fähigkeit, Daten von extern zu beziehen und mit anderen auszutauschen ist zentral und hat Auswirkungen auf alle Ebenen. Die Daten müssen häufig aus mehreren Quellen zusammengeführt werden.
Interoperabilität auf allen Ebenen	Schon auf der Strategieebene müssen sich Unternehmen verständigen und gemeinsame Ziele definieren. Zur Erreichung dieser müssen Informations-systeme interoperabel sein.

Capabilities stellen einen abstrahierten Ansatz zu Planungszwecken dar; die Umsetzung der Capabilities hat die im folgenden beschriebenen Auswirkungen auf die Architekturebenen. Beispielsweise sollte der Datenaustausch durch Verträge abgesichert werden und technische Schnittstellen die zeitnahe und korrekte Übertragung der Daten sicherstellen.

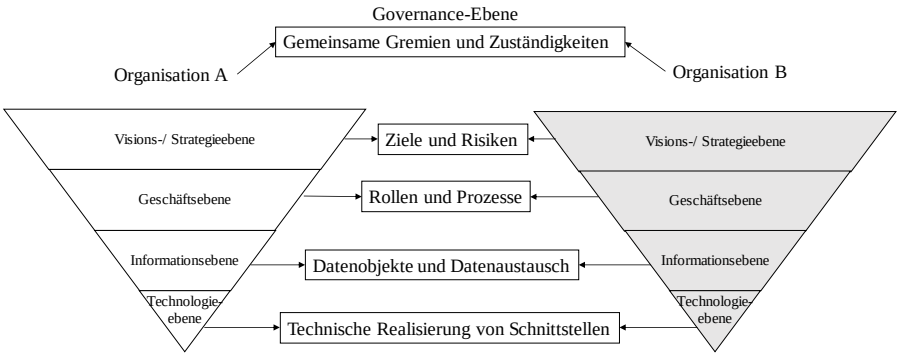


Abb. 3. Empfohlene Schwerpunkte für Interoperabilität

Visions- und Strategieebene: Einzelne Organisationen oder Unternehmen müssen zunächst unternehmensintern in den Wertschöpfungsnetzwerken eine Rolle einnehmen (z.B. die des Serviceproviders oder des Datenveredlers) und entsprechende Fähigkeiten, Ressourcen und Prozesse entwickeln, sofern sie nicht bereits über diese verfügen.

Anschließend müssen sich beteiligte Unternehmen und Organisationen darüber im Klaren sein, welche Ziele sie mit dem intelligenten Verkehrsdienst erreichen wollen und welcher Mehrwert für das einzelne Unternehmen im Verbund durch die Beteiligung entsteht. Gleichzeitig sollten Risiken für das eigene Geschäftsmodell abgewogen werden; so müssen sich beispielsweise Datenanbieter bewusst sein, dass die von ihnen bereitgestellten Daten nicht länger exklusiv der eigenen Organisation zur Verfügung stehen. Im Projektkontext der intelligenten Verkehrsdienste werden hierzu Bezahl- und Verrechnungskonzepte individuell ausgehandelt. Der Mehrwert der Datenbereitstellung wird von den Projektbeteiligten nicht in Frage gestellt, zumal diese staatlich forciert wird. Als Methodik zur Erarbeitung der Ziele wird im Projekt die Szenariotechnik angewendet.

Geschäftsebene: Auf der Geschäftsebene müssen Verträge, bspw. in Form von Service Level Agreements abgeschlossen werden, welche die Zusammenarbeit zwischen den Partnern regeln. Datenlieferungen, deren Häufigkeit und Datenqualität sind ein Thema solcher Verträge, aber auch die finanziellen Modalitäten. In dynamischen Wertschöpfungsnetzwerken sollte die Möglichkeit bestehen, Verträge flexibel abzuschließen. Verträge werden im Projekt als eine besondere Form der Informationsobjekte betrachtet und finden sich auch auf der Informationsebene wieder.

Eine gemeinsame Begriffswelt in Form eines Glossars kann hilfreich sein, Barrieren zwischen den Unternehmen abzubauen. Im Projekt wurde ein gemeinsames Glossar für alle beteiligten Organisationen erarbeitet und abgenommen. Damit besteht die Chance, dass sich die Begriffe etablieren und die kommunikative Leistungsfähigkeit gesteigert wird.

Auf Seiten der Modellierung sollten Prozesse und Geschäftsprozesse modelliert werden, damit allen Beteiligten ihre Rolle und ihre jeweiligen Aufgaben im Prozess verdeutlicht werden. Zusätzlich werden dadurch Verantwortlichkeiten eindeutig definiert. Eine ergänzende Modellierung der Nachrichtenflüsse über UML oder BPMN 2.0 Kollaborationsdiagramme ist empfehlenswert, denn diese kann als Grundlage für die gemeinsame Informationsarchitektur dienen. Vollständige Prozessmodelle mit Teilprozessen, Rollen und benötigten Daten sowie Prozesslandkarten, die den Zusammenhang zwischen den Prozessen darstellen, sind bedeutend, da hierdurch auch Inkompatibilitäten bei bestehenden Abläufen aufgedeckt und Anpassungsbedarfe identifiziert werden können.

Zur Realisierung einer konkreten Capability kann es erforderlich werden, neue Organisationseinheiten zu bilden oder neue Mitarbeiter mit entsprechenden Skills zu beschäftigen. Dies ist ebenfalls der Geschäftsebene zuzuordnen und zeigt nochmals auf, dass die Zusammenarbeit nicht nur die Informationssysteme der Organisationen betrifft, sondern auch organisatorische Konsequenzen haben kann.

Informationsebene: Auf der Informationsebene müssen für die Informationssysteme Schnittstellen zur Datenübertragung erstellt werden. Vor allem aber müssen sich die beteiligten Unternehmen einigen, welche Datenobjekte ausgetauscht werden sollen – hierunter fallen auch die vorher beschriebenen Verträge in dynamischen Wertschöpfungsnetzwerken. Hier ist zunächst eine Betrachtung auf hoher Abstraktionsebene sinnvoll. Dazu gehört die Zuordnung, welche Organisation welche Datenobjekte an wen zu liefern hat. Im Projektkontext sind relevante Datenobjekte unter anderem Baustelleninformationen, Staudaten, Fahrpläne und Positionsangaben. Im nächsten Schritt sollten konkrete Datenmodelle bis zur Attributebene für die einzelnen Datenobjekte definiert werden.

Technische Infrastrukturebene: Für die Ebene der technischen Infrastruktur können auf Grund der Heterogenität der beteiligten Unternehmen und Organisationen wenig Vorgaben auf Ebene der Referenzarchitekturen gemacht werden. Auf Ebene einzelner realer intelligenter Verkehrsdienste sollten hier Absprachen u.a. zu Übertragungsprotokollen getroffen werden, die dann in Form von Architekturprinzipien oder Datenüberlassungserklärungen erfasst und dokumentiert werden können.

Governance: Besondere Bedeutung kommt im Falle dynamischer, unternehmensübergreifender Zusammenschlüsse der Governance zu. So sollte ein Architektur-Governance-Gremium für den einzelnen Dienst und zusätzlich ein hierarchisch höheres Entscheidungsgremium bestehend aus Vertretern der beteiligten Unternehmen etabliert werden. Bei Ausscheiden eines Partners muss die Governance den durchgehenden Betrieb des Dienstes langfristig sicherstellen. Auch technologische Innovationen oder geänderte Rahmenbedingungen (z.B. Gesetze) sollten auf ihren Einfluss auf alle Projektbeteiligten hin geprüft werden, damit diese in einem Konsens gemeinsam umgesetzt werden können. Die gemeinsam abgestimmten Prinzipien

sollten in Architekturprinzipien festgehalten werden und allen Beteiligten zur Verfügung gestellt werden.

Der Bereich Governance wird im Projekt erst zukünftig abschließend adressiert.

5.4 Evaluation im Rahmen des Projekts

Die Ergebnisse aus der Projektarbeit wurden einem Gremium von über 55 Experten aus der Mobilitätsbranche vorgestellt und mit diesen in einem eintägigen Workshop intensiv diskutiert. Dabei wurden einerseits die Anwendung von EAM und TOGAF auf intelligente Verkehrsdienste und anderseits die entstandenen Referenzarchitekturen für dynamische Unternehmensnetzwerke diskutiert und abschließend von den Experten positiv bewertet. Den Beteiligten gefällt besonders der ganzheitliche Ansatz, den TOGAF bietet, der neben der softwaretechnischen und datenzentrierten Lösung auch organisatorische Aspekte und Rahmenbedingungen miteinbezieht. Als Verbesserungsvorschlag wünschen die Experten eine einheitliche und durchgängig konsistente Verwendung von Bausteinen in allen Referenzarchitekturen. Gerade die Zusammenarbeit zwischen verschiedenen Unternehmen wird in der Praxis als Herausforderung angesehen, weswegen Lösungen in diesem Bereich gefragt und relevant sind. Die Ergebnisse des Projekts haben nach Ansicht der Experten in der Praxis das Potential, redundante Arbeiten zu vermeiden, indem die Referenzlösungen zur Orientierung verwendet werden.

Ergänzend wurde das Projekt mit Fokus auf die oben angeführten EAM- und TOGAF-Aspekte auf einer Konferenz der Open Group einer Gruppe von ca. 20 Enterprise-Architekten vorgestellt. Dort ist die Mobilitätsbranche als neue Nutzergruppe von TOGAF wahrgenommen worden und das Feedback zum Vorgehen im Projekt fiel positiv aus. Insbesondere betonten die Architekten den Mehrwert des Capability-based-Planning und stimmten zu, dass TOGAF 9.1 auch für den unternehmensübergreifenden Einsatz geeignet seien, wenn sie entsprechend zugeschnitten werden.

6 Abstraktion, Diskussion und Ausblick

Die Erkenntnisse aus dem Projekt lassen sich aus Sicht der Autoren abstrahieren. Dafür spricht vor allem die Beteiligung vieler Unternehmen und Organisationen am Projekt und die Bearbeitung mehrerer Arten intelligenter Verkehrsdienste. Eine Besonderheit ist sicherlich, dass viele öffentliche Einrichtungen am Projekt beteiligt sind, die nicht immer privatwirtschaftliche Interessen verfolgen, sondern deren Zielsetzung in der Förderung des Gemeinwohls liegt. Eine freizügige Datenbereitstellung ohne Gegenleistungen ist im privatwirtschaftlichen Umfeld weniger zu erwarten.

Der Bereich Sicherheit wird im Projekt und im vorliegenden Beitrag nicht betrachtet und bleibt somit Gegenstand zukünftiger Forschungsarbeiten.

Das laufende Projekt zu intelligenten Verkehrsdiensten wird im Jahr 2018 abgeschlossen. Die Adaption der entwickelten Referenzarchitekturen und der angepassten Vorgehensweise zur Entwicklung von unternehmensübergreifenden

Architekturen in der Praxis beginnt gerade, was zu Anpassungen führen könnte. Weiterer Forschungsbedarf besteht hinsichtlich der Umsetzung interorganisationaler Architekturen und einer darauf basierenden Abschätzung der Wirtschaftlichkeit unter Berücksichtigung der Faktoren einer individuellen, dienstspezifischen Realisierung. Auch die längerfristige Pflege abgestimmter Architekturen ist im Vergleich zur intraorganisatorischen Pflege erschwert.

7 Danksagung

Diesem Bericht liegen Teile der im Auftrag des Bundesministeriums für Verkehr und digitale Infrastruktur, vertreten durch die Bundesanstalt für Straßenwesen, unter FE-Nr. 03.0483/2011/IRB durchgeführten Forschungsarbeit zugrunde. Die Verantwortung für den Inhalt liegt allein beim Autor.

References

1.BITKOM: Enterprise Architecture Management – neue Disziplin für die ganzheitliche Unternehmensentwicklung, Berlin (2011)
2.Fischer, R., Aier, S., Winter, R.: A Federated Approach to Enterprise Architecture Model Maintenance. Enterprise Modelling and Information Systems Architectures 2, 14-22 (2007)
3.The Open Group: TOGAF Version 9.1. The Open Group, U.S. (2011)
4.Hevner, A.R., March, S.T., Park, J.: Design Science in Information Systems Research. MIS Quaterly 28, 75-105 (2004)
5.Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., Sinz, E.J.: Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. Zeitschrift f. betriebswirtschaftl. Forschung 6, 664 - 672 (2010)
6.vom Brocke, J., Buddendick, D.: Reusable Conceptual Models – Requirements Based on the Design Science Research Paradigm. Conference on Design Science Research in Information Systems and Technology 576-604 (2006)
7.Hanschke, I.: Enterprise Architecture Management – einfach und effektiv - Ein praktischer Leitfaden für die Einführung von EAM. Carl Hanser, München (2016)
8.The Open Group: Archimate 3.0.1. The Open Group, Reading (2017)
9.Lankhorst, M.: Enterprise Architecture at Work. Springer, Berlin (2017)
10.Ziemann, J.: Architecture of Interoperable Information Systems. Logos, Berlin (2010)
11.Kosanke, K.: ISO Standards for Interoperability: a Comparison. In: Konstantas, D., Bourrières, J.-P., Léonard, M., Boudjlida, N. (eds.) Interoperability of Enterprise Software and Applications, pp. 55-64. Springer, London (2006)
12.van Pelt, V., Sprenger, M.: ANTILOPE - Adoption and take up of standards and profiles for eHealth Interoperability. Nictiz, Den Haag (2015)
13.Europäische Kommission: European Interoperability Framework, Brüssel (2017)

14.Levy, Y., Ellis, T.J.: A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science 9, 181-212 (2006)
15.vom Brocke, J., Simons, A., Niehaves, B., Reimer, K., Plattfaut, R., Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Seach Process. ECIS Proceedings 2206-2217 (2009)
16.Schryen, G.: Writing Qualitative IS Literature Reviews - Guidelines for Synthesis, Interpretation, and Guidance of Research. Communications of the AIS 37, (2015)
17.Kaisler, S.H., Armour, F., Valivullah, M.: Enterprise Architecting: Critical Problems HICSS Proceedings (2005)
18.Goel, A., Schmidt, H., Gilbert, D.: Formal Models of Virtual Enterprise Architecture: Motivations and Approaches. PACIS Proceedings 1207-1217 (2010)
19.Simon, D., Fischbach, K., Schoder, D.: An Exploration of Enterprise Architecture Research. Communications of the AIS 32, (2013)
20.Cheng, Y.-Y., Lai, H.-H.: Constructing an interoperable, design-centric, service-oriented and knowledge-sharing architecture. International Journal of Computer Integrated Manufacturing 24, 1075-1094 (2011)
21.Janssen, M., Feenstra, R.: Service portfolios for supply chain composition: Creating business network interoperability and agility. International Journal of Computer Integrated Manufacturing 23, 747-757 (2010)
22.Medinia, K., Bourey, J.P.: SCOR-based enterprise architecture methodology. International Journal of Computer Integrated Manufacturing 25, 594–607 (2012)
23.Choi, Y., Kang, D., Chae, H., Kim, K.: An enterprise architecture framework for collaboration of virtual enterprise chains. The International Journal of Advanced Manufacturing Technology 35, 1065-1078 (2008)
24.Chalmeta, R., Pazos, V.: A step-by-step methodology for enterprise interoperability projects. Enterprise Information Systems 9, 436-464 (2015)
25.Venz, J.: National ITS Architecture: Context and Vision. Austroads Ltd., Sydney (2014)
26.Highways Agency, http://www.highways.gov.uk/specialist-information/guidance-and-best-practice/enterprise-architecture/
27.Bundesministerium für Verkehr und digitale Infrastruktur: Roadmap: Digitale Vernetzung im öffentlichen Personenverkehr, Köln (2016)
28.Kommission der Europäischen Gemeinschaften: Aktionsplan zur Einführung intelligenter Verkehrssysteme in Europa Brüssel (2008)
29.Frame Forum: European ITS Framework Architecture (FRAME), Wien (2011)
30.Rittershaus, L., Aicher, P., Albrecht, H., Czogalla, O., Dölger, R., Dubbert, J., Gerres, S., Kroen, A., Ortgiese, M., Roszak, C., Schimandl, F., Schnittger, S., Scholtes, W., Schüler, T.: Hinweise zur Strukturierung einer Rahmenarchitektur für Intelligente Verkehrssysteme (IVS) in Deutschland – Notwendigkeit und Methodik. FGSV, Köln (2012)
31.Dern, G.: Management von IT-Architekturen. Vieweg Teubner, Wiesbaden (2009)
32.Aldea, A., Iacob, M.E., Lankhorst, M., Quartel, D., Wimsatt, B.: Capability-Based Planning - The Link between Strategy and Enterprise Architecture, Reading (2016)

Aligning Enterprise Knowledge and Data: A Domain-Specific Modeling Method for Social Media Strategies

Anna Widenmaier[1], Hans-Georg Fill[2]

[1] University of Vienna, Faculty of Computer Science, Vienna, Austria
anna.widenmaier@googlemail.com
[2] University of Bamberg, Information Systems – System Development and Database Application Group, Bamberg, Germany
hans-georg.fill@uni-bamberg.de

Abstract. For supporting decision makers in their day-to-day operations, enterprise knowledge needs to be combined with data acquired from various IT systems. For this purpose, specifically designed IT-based modeling methods enable this linkage on a conceptual as well as a technical level. In the paper at hand, we describe a domain-specific modeling method that supports the alignment of enterprise knowledge in the form of social media strategies with data acquired from social media platforms. For testing the feasibility of the approach, we implemented the modeling method on the ADOxx meta modeling platform, which was extended with a Java application for linking it to Twitter. Subsequently, we describe a use case for representing and analyzing a social media strategy in a University setting and evaluate the benefits and drawbacks of the approach.

Keywords: *social media strategies, social media strategy modeling method, domain-specific modeling method.*

1 Introduction

The number of social media interactions per second grows steadily. According to InternetLiveStats.com, 797 Instagram photos are uploaded, 7,716 tweets are sent, and 70,355 YouTube videos are viewed per second[1]. The decision makers in businesses that use social media for their purposes, e.g. in marketing or customer interaction, are thus often overwhelmed by these amounts of data. They require structured procedures for the continuous setting of goals concerning social media, for measuring according achievements, and for the adaptation of respective measures. This will be denoted in the following as a *social media strategy*. Such a strategy represents enterprise knowledge made explicit by the decision makers that subsequently needs to be aligned with according data sources [7]. In this way it can be navigated through the different options for addressing social media, setting goals and subsequently measuring the achievement of these goals. In the following we will investigate how this need can be satisfied by reverting to conceptual modeling methods. As a solution, we will present a

[1] See http://www.internetlivestats.com/ (Data from 2017-09-18)

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

domain-specific, i.e. specifically designed, conceptual modeling method for representing social media strategies that is able to directly connect to social media platforms. The remainder of the paper is structured as follows. In Section 2, we outline the characteristics of social media, existing social media strategy approaches and according model-based approaches. In Section 3 the domain-specific modeling method is presented. Section 4 reports about the technical realization of the modeling method and its application to a use case. The approach is discussed in Section 5. The paper is concluded with an outlook in Section 6.

2 Foundations

In this chapter, we discuss required foundations for the design of our approach. These concern social media characteristics, social media strategy approaches and existing strategy modeling approaches.

2.1 Social Media Characteristics

At their core, social media can be described as internet-based applications that are created with Web 2.0 technologies for enabling creative consumers to define value-added content [2, 10].

Web 2.0 is thereby understood as a group of technologies to support consumers rather than organizations in collaboration, communication, content creation, and interoperability [10]. “Creative consumers” are characterized by their intention to create content that is published on social media or websites, and the intention of content creation should be based on personal and not professional reasons. Through the usage of Web 2.0 technologies, a shift from one-to-many to many-to-many is achieved in terms of communication. Several types of content are realized through social media depending on the chosen social media channel, e.g. text, pictures, videos, and networks [2].

From the viewpoint of organizations, it is important to keep track of shared information on social media, especially for the fast reaction on negative comments [13]. Therefore, organizations need to monitor social media channels constantly. In addition, they use social media to engage in a positive manner with consumers [10, 14]. This is today typically realized by using social media management tools that are helpful for natural language processing, data mining, and the identification of public reactions [1]. Popular examples for such tools include swat.io, tweetdeck, or hootsuite[2].

2.2 Social Media Strategy Approaches

Effing & Spill [4] identified a lack of comprehensive, dedicated frameworks for social media strategies and elaborated therefore the “social strategy cone framework”. The research was based on a literature review and included nine case studies. The literature

[2] See the websites: https://swat.io/, https://tweetdeck.twitter.com/, https://hootsuite.com/ (retrieved 2017-09-18)

review revealed seven key elements to consider for social media strategies: target audience, social media channel, goals, resources, policies, monitoring, and content activities. For a successful social media strategy, the authors consider it important to identify the appropriate target audience and consequently the right social media channel. A successful social media presence requires a consistent overall appearance. Therefore, an alignment of business goals, e.g. in terms of customer satisfaction, with social media is essential as well as a clear purpose. The assignment of competent resources is necessary for authentic and valuable communication. To ensure that resources communicate in the name of the organization in a proper manner, policies are required. Furthermore, for managing posts over time, a content activity plan is required. The content activity plan should be used to plan and schedule content that will be posted. Monitoring is inalienable for social media strategies to keep track of the ongoing environment [4].

In another approach, the honeycomb framework by Kietzmann et al. [12] aims to support managers to draw the attention to social media ecology, required engagements, and the audience. The framework defines the seven building blocks: identity, conversation, sharing, presence, relationships, reputation, and groups. It analyzes the functionalities based on the seven building blocks and the linked implications. Therefore, identity is the extent to which users disclose themselves. That implies data privacy controls and additional tools for supporting user self-promotion. Relationships are about the relation from user to user, that requires management of structural and flow properties in a relationship network. The social standing of others and content subsumed under "reputation" comes with monitoring strength, passion, sentiment, and reach of users or organizations. Groups are users coming together as communities and need membership rules and protocols. Conversations cover the extent of user communication and imply the conversations' velocity as well as the risks of starting and joining conversations. The ability to share content requires a content management system and a social graph. Moreover, presence is an important factor on social media platforms. To that end, it is necessary to create and manage the reality, intimacy and immediacy of the context [12].

2.3 Existing Strategy Modeling Approaches

The use of conceptual modeling techniques for the domain of strategic management has been explored in the past from several perspectives. One essential aspect in defining and evaluating strategies is the formulation of goals and the analysis of how goals interact with each other. Recently, a formal approach based on the i* modeling language has been proposed by Horkoff and Yu that permits in-depth analyses of goals including the detection of contradictions or the evaluation of the reachability of goals [8].

In addition to goals, several other aspects of strategic management approaches may be represented using conceptual models. Bock et al. compiled several concepts originating from approaches such as SWOT analyses, the Five Forces framework or balanced scorecards into one meta model and linked it to the MEMO enterprise modeling method [3]. However, the meta model has not yet been implemented as a modeling tool.

With the approach of ADOscore a comprehensive, industrial-scale modeling approach has been proposed. ADOscore is based on Balanced Scorecards developed by Kaplan and Norton and is used to measure the performance of an organization's strategy. The

focus is on the correlation of the financial, internal business process, learning and growth, and customer perspective [11]. ADOscore enables the creation of a flexible controlling system through customizable key performance indicators. The modeling method consists of several modeling types. These are: the Strategy Model, the BSC Map, the Success Factors Model, the Organization Model, the Initiatives Model, the Cause and Effect Model, and the Key Performance Indicator Model. Strategy, vision, guiding principle, slogan and strategic direction are defined in the Strategy Model. Objectives, targets, measures, and initiatives are defined in the Cause and Effect Model. The model type Key Performance Indicator contains the definition of key performance indicators that are used to measure the achievement of strategic goals [15].

3 A Domain-Specific Modeling Method for Social Media Strategies

Although one can partially apply the existing approaches for modeling strategies to the domain of social media strategies, none of them permitted to establish a linkage between the definition of a social media strategy and the data and specific indicators delivered by social media platforms on a technical level. This seems however favorable in order to immediately evaluate the success of the strategy using actual data sources. Based on the foundations in Section 2, we thus decided to create a domain-specific modeling method that would permit such a linkage. In the following, we will describe the procedure used in the modeling method, the underlying meta model and the visual notation for the modeling language. Furthermore, we add algorithms for linking the models with social media platforms.

3.1 Procedure

The procedure of the modeling method for social media strategies builds on the seven key elements identified by Effing & Spil [4] introduced in Section 2.2. The main purpose of the modeling method is to create and analyze social media strategies using actual data. Considering the importance of aligning the social media strategy to an organization's overall business strategy, the definition of the vision and strategy of an organization constitutes the fundament of the modeling method. After vision and strategy are defined, policies and resources are added, followed by the strategy plan definition.

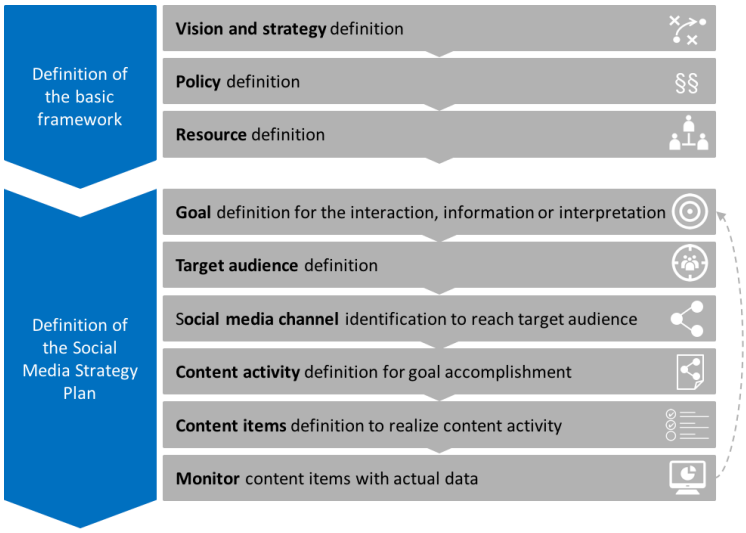


Figure 1. Procedure of the Modeling Method

In the strategy plan, at first the goals for the interaction, information or interpretation are set. This is followed by the definition of the target audience and the social media channel to reach this audience. For goal accomplishment, content activities are elaborated with the according content items that contain the data to be published on a social media platform. For example, this can be posts on a social media platform for a particular topic. Finally, it is important to monitor content items, i.e. the achievement of goals, by retrieving social data. In the case of Twitter for example this would be information on "likes" and "retweets". According to the results of monitoring the strategy plan, actions are identified, e.g. new goals or new content items.

3.2 Meta Model and Visual Notation

For supporting the modeling procedure with a meta model of a domain-specific modeling method, four model types were derived: Vision and Strategy, Policy, Resource, and Strategy Plan (see Figure 2). Each model type consists of at least one class. Every class inherits from the abstract class _StrategyModelElement_ with the attribute description.

In addition to the relations within the model types, e.g. for representing that goals refer to target audience elements and these in turn to content activities, also cross-model references are possible. These are depicted in Figure 2 using the INTERREF connectors. Furthermore, some of the attributes of the elements in the meta model are not to be modified by users but are automatically filled by algorithms (e.g. the Like Count attribute of the Content Item element) as will be described in the next section.

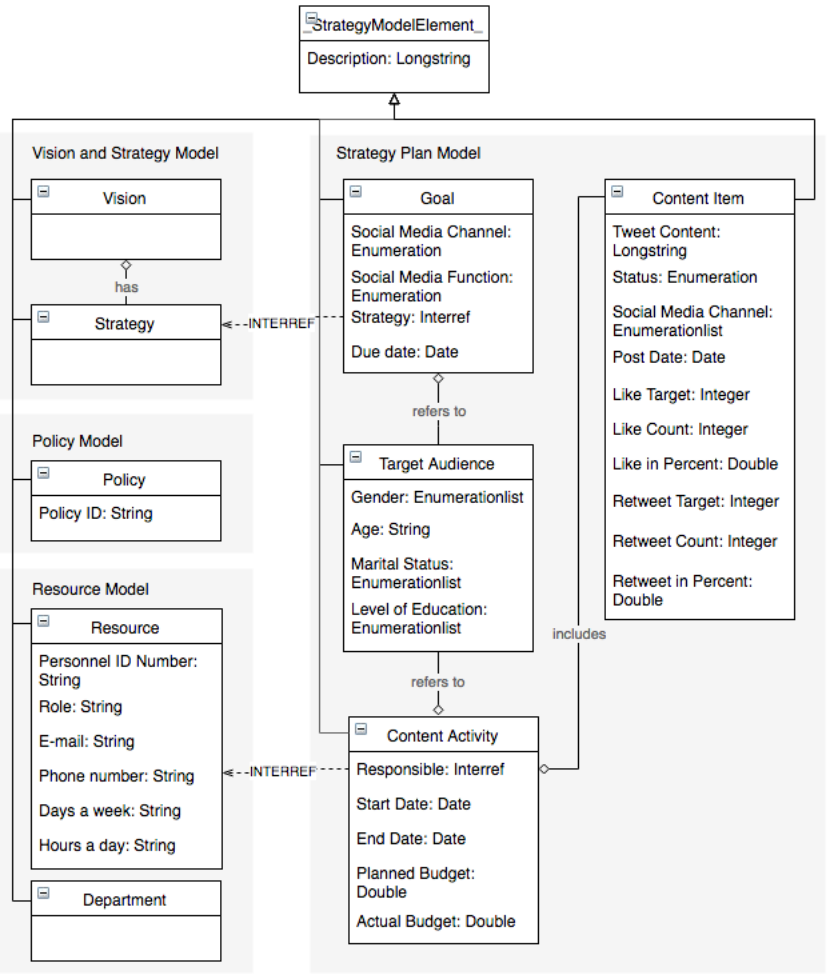
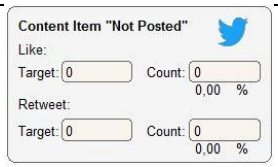
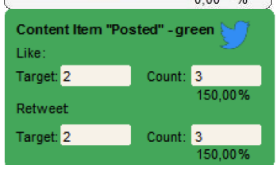
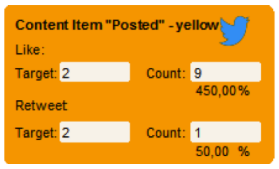
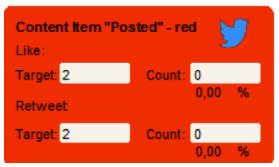


Figure 2. Meta Model for a Domain-Specific Modeling Language for Social Media Strategy Management [16]

The visual notation of the classes and relations in the meta model is shown in Table 1 below. Thereby, a specific color coding is applied to instances of the Content Item class that represents items that are about or were posted on social media. Based on a target value specified by the user for likes and retweets, the color is automatically switched between green, yellow, and red. This indicates – similar to traffic lights – whether the target has been reached, which is assumed if the value in regard to the target is above 88% and the color code is set to green, whether it has not yet been sufficiently reached, which applies if the value in regard to the target is below 33% or, whether it is in a middle stage, i.e. between 33% and 88% - then it is visualized in yellow. It has to be noted that these values are assumptions and may need to be adapted for different scenarios and user preferences.

Table 1. Visual Notation of the Classes and Relations

Class / Relation	*Visual Notation*	*Description*
has		Creates a relation from the Vision element to the Strategy element within the Vision and Strategy Model.
includes		Creates a relation from Content Activity to Content Item within Strategy Plan Model.
refers to		”refers to” is used in the Strategy Plan Model to create a relation between Goal and Target Audience as well as between Target Audience and Content Activity.
Vision		The Vision class is part of the Vision and Strategy model and is used to define the vision of the organization.
Strategy		The Strategy class is part of the Vision and Strategy model and is used to define the strategy to achieve the vision.
Resource		The Resource class is part of the Resource model and is used to define Resources of an organization with information about the role, contact details and availability.
Department		For the assignment of resources to a department the Department class is used within the Resource model.
Policy		The Policy model consists out of the Policy class and is required for the definition of policy elements.
Goal		Within the Strategy Plan model, the goal definition is embedded through the Goal class. It enables to specify the name, description, social media channel, social media function, the INTERREF connector to the Strategy element of the Vision and Strategy Model, and Due date.
Target Audience		The Target Audience is defined in the Strategy Plan model and enables to specify the target group in terms of gender, age, marital status, and level of education.
Content Activity		The Content Activity is used for categorization and content item planning. Next to the definition of a responsible resource with an INTERREF connector to the resource model, the start date, end date, planned budget, and the actual budget could be set.

Class / Relation	*Visual Notation*	*Description*
Content Item (Status: Not Posted)		The Content Item is assigned to the Content Activity and is part of the Strategy Plan model. It holds the actual post content and the social media channel (for now restricted to Twitter). The update of likes and retweets from Twitter is saved in the attributes Like Count and Retweet Count, that are write-protected for users so that they can only be changed by according algorithms. The notation of the Content Item changes based on following attributes: Status, Like in Percent, and Retweet in Percent. The color code depends on the latter two attributes. This notation is displayed with the status "Not Posted".
Content Item (Status: To be Posted)		The Status "To be Posted" is represented with this Content Item notation.
Content Item (Status: Posted; with green color code)		The Status "Posted" is represented with this Content Item notation. If the attributes "Like in Percent" and "Retweet in Percent" are above 88% of the target, the item is represented in green color.
Content Item (Status: Posted; with yellow color code)		The Status "Posted" is represented with this Content Item notation. If the attribute "Like in Percent" is between 33% and 88% of the target or "Retweet in Percent" is between 33% and 88%% of the target, the item is represented in yellow color.
Content Item (Status: Posted; with red color code)		The Status "Posted" is represented with this Content Item notation. If either the attribute "Like in Percent" or "Retweet in Percent" is below 33% of the target, the item is represented in red color.

3.3 Algorithms

The modeling method includes two algorithms for linking the created models with social media platforms. The first algorithm "Update Content Items" refers to Content Item elements that are contained in a strategy plan. If the items have not yet been posted on the respective social media channel, the algorithm automatically posts them using the credentials of a user. Subsequently, for all posted items, the information about likes and retweets (in the case of Twitter) is collected and assigned to the model elements. The

second algorithm “Create Content Items” is used for the analysis of content items that already exist on the social media platform but that have not yet been represented in the model. Based on criteria to be specified by the user, e.g. using time intervals, the algorithm automatically collects content items from a social media platform and adds them to a model. For the next versions of the algorithms it is planned to include further semantic information such as hash tags or particular user names to permit groupings of the elements.

4 Technical Realization and Application to a Use Case

To evaluate the feasibility of the approach, the modeling method has been technically implemented using the ADOxx meta modeling platform [6] and then applied to a use case. In the first iteration, the implementation has been restricted to the use with Twitter as a social media platform. Connectors to other social media platforms such as Facebook, LinkedIn or Instagram are possible and considered for future work. The meta model together with the visual notation was realized in ADOxx. The algorithms were partly realized using the ADOscript language of ADOxx and partly in Java. The latter was used for providing a user interface for entering account data for Twitter and for establishing the connection to the Twitter API using the OAuth protocol. For exchanging data between ADOxx and Twitter it was reverted to the ADOxx XML import and export interfaces. The details of the data exchanges are shown in Figure 3 below.

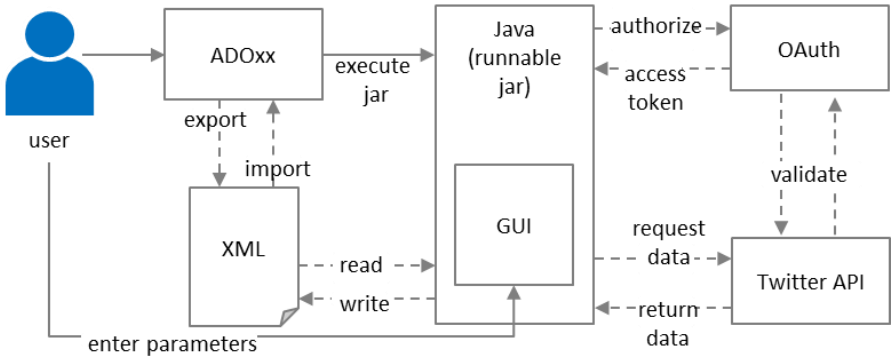


Figure 3. Technical Architecture of the Implementation [16]

A use case of the Research Group Knowledge Engineering at the University of Vienna was considered for the proof of concept to illustrate how the approach could be applied. Therefore it has been focused on Twitter posts in the context of the Next Generation Enterprise Modelling (NEMO) Summer School 2015. The use case application follows a bottom up approach by retrieving first the content items that had already been posted, analyzing them and then developing an according social media strategy. This is beneficial in cases where social media have already been in use but no according strategy had been defined so far.

Figure 4 represents an extract of a possible Strategy Plan model with imported tweets from Twitter about the NEMO Summer School 2015. After we imported all tweets from 23.07.2015 – 31.07.2015 we analyzed the Content Items and identified suitable Content Activities. Target values for likes and retweets were manually identified for each Content Item to assess the success of the items posted so far in regard to the user base (i.e. the followers on Twitter).

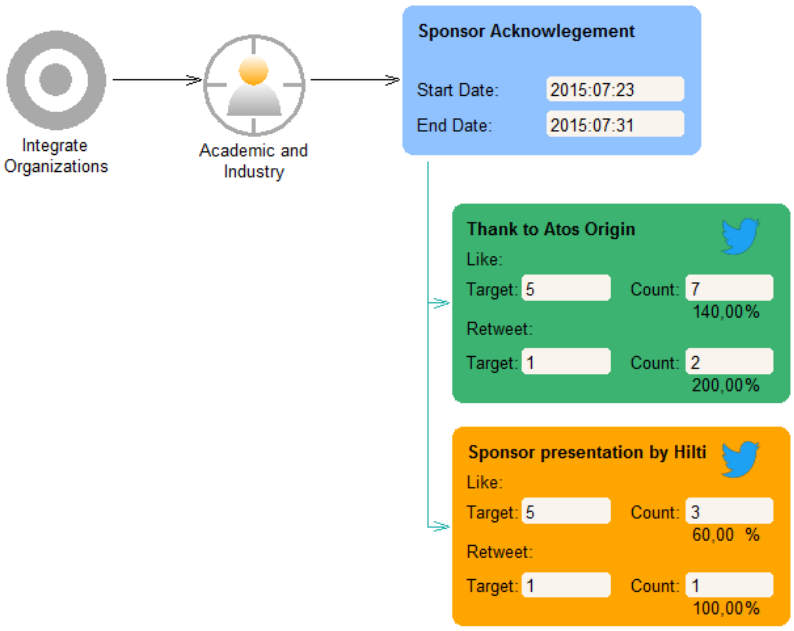


Figure 4. Possible Strategy Plan Model of the Use Case for the NEMO Summer School

The assignment of Content Items to Content Activities enabled in addition to a categorization, an overview of the success of one category and the Content Items. To complete the Strategy Plan model, Goal and Target Audience elements were created. For the assignment of responsible persons to Content Activities and strategies to goals, a Resource model and Vision and Strategy model were created (see Figure 5). A Policy model was also created for usability reasons.

5 Discussion

The domain-specific modeling method enables a structured approach of social media strategy definition with a direct link to social media platforms. In addition, existing social media information can be imported into the Strategy Plan model based on the username and timeframe. Furthermore, post content is visualized through Content Items and categorized by the association of Content Items to Content Activity elements. This is an enhancement in regard to the traditional direct interaction with social media platforms such as Twitter where posts on a common topic are spread over the time line with

no reference, which makes their analysis difficult. Hence, an analysis of success or failure of Content Items and therefore Content Activities is easy to identify based on the provided color code of Content Items. The color code refers to the achieved target likes and target retweets, that are automatically updated with the function Update Content Item.

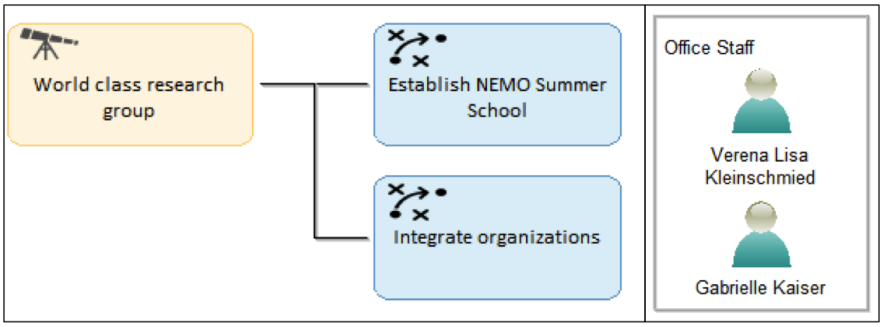


Figure 5. Vision and Strategy Model (left) and Resource model (right) of the Use Case

A weakness of the color code in its current form is that users cannot choose the percent range for green, yellow, and red encodings. Also, the weighting of likes and retweets is equal and not yet customizable by the user. Thus, like and retweet target must be set carefully. A low target could run the risk that the analysis and derived actions are misleading. Furthermore, if the status of a Content Item is accidentally set to "To be Posted" it could result in unintended or double postings. Therefore, an additional definition of clear guidelines and policies is important.

6 Conclusion and Outlook

The objective of this paper was to introduce a domain-specific modeling method for the alignment of enterprise knowledge in the form of social media strategies with data acquired from social media platforms. The modeling method is based on seven key elements for social media strategies identified by Effing & Spil [4] and has been realized on ADOxx together with a Java application for programmatically interacting with Twitter.

Future work will consider the implementation of further social media channels, for instance Instagram, Facebook, and LinkedIn. In addition, the model types Vision and Strategy and Resource will be extended with more advanced existing meta models. For this purpose an approach for the performance management of public health authorities could be considered by Fill et al. [5]. Also, the integration of statistical analysis tools could be of additional value for a more detailed processing of the social media data [7].

References

1. Benthaus, J., M. Risius, and R. Beck (2016). “Social media management strategies for organizational impression management and their effect on public perception.” In: The Journal of Strategic Information Systems 25.2, pp. 127–139.
2. Berthon, P. R., L. F. Pitt, K. Plangger, and D. Shapiro (2012). “Marketing meets Web 2.0, social media, and creative consumers: Implications for international marketing strategy.” In: Business horizons 55.3, pp. 261–271.
3. Bock, A., Frank, U., Bergmann, A., Strecker, S. (2016): Towards Support for Strategic Decision Processes Using Enterprise Models: A Critical Reconstruction of Strategy Analysis Tools, in: Horkoff et al.: PoEM 2016: The Practice of Enterprise Modeling, Springer, pp 41-56.
4. Effing, R. and T. A. M. Spil (2016). “The social strategy cone: Towards a framework for evaluating social media strategies.” In: International journal of information management 36.1, pp. 1–8.
5. Fill, H.-G., A. Eberhart, A. Laslop, I. Reischl, T. Lang, and D. Karagiannis (2011). “An Approach to Support the Performance Management of Public Health Authorities using an IT based Modeling Method.” In: Bernstein, A., Schwabe, G. (2011): Proceedings of the 10th International Conference on Wirtschaftsinformatik WI 2.011, Volume 1, pp. 38–47.
6. Fill, H.-G., and D. Karagiannis, (2013): On the Conceptualisation of Modelling Methods Using the ADOxx Meta Modelling Platform, Enterprise Modelling and Information Systems Architectures - An International Journal, Vol. 8, Issue 1, 4-25.
7. Fill, H.-G. and F. Johannsen (2016). “A knowledge perspective on big data by joining enterprise modeling and data analyses.” In: 49th Hawaii International Conference on Sysetm Sciences (HICSS). IEEE, pp. 4052–4061.
8. Horkoff, J. and Yu, E. (2016): Interactive goal model analysis for early requirements engineering, Requirements Engineering, Vol. 21, Issue 1, pp. 29-61.
9. InternetLiveStats.com. (2017). InternetLiveStats.com. [Online; accessed 13-August-2017]. URL: http://www.internetlivestats.com/one-second/ Effing, R. and T. A. M. Spil (2016). “The social strategy cone: Towards a framework for evaluating social media strategies.” In: International journal of information management 36.1, pp. 1–8.
10. Kaplan, A. M. and M. Haenlein (2010). “Users of the world, unite! The challenges and opportunities of Social Media.” In: Business horizons 53.1, pp. 59–68.
11. Kaplan, R. S. and S. Norton (1996). “The Balanced Scorecard: Measures that Drive Performance.” In: Harvard Business Review 70.1, pp. 71– 79.
12. Kietzmann, J. H., K. Hermkens, I. P. McCarthy, and B. S. Silvestre (2011). “Social media? Get serious! Understanding the functional building blocks of social media.” In: Business horizons 54.3, pp. 241–251.
13. Kimmel, A. J. (2010). Connecting with consumers: Marketing for new marketplace realities. Oxford University Press.
14. Larson, K. and R. Watson (2011). “The value of social media: toward measuring social media strategies.” In: ICIS 2011 Proceedings. 10.
15. Lichka, C., D. Karagiannis, and H. Kühn (2002). “ADOscore R: IT- gestützte Balanced Scorecard.” In: Wisu-das wirtschaftsstudium (7), pp. 915–918.
16. Widenmaier, A. (2017). “Model Based Management of Social Media Strategies.” (Master’s thesis, University of Vienna, Vienna, Austria).

UnSComT2G – Konzeption eines Tools zur Übertragung normsprachlicher Spezifikationen von Fachkomponenten in UML-Diagramme

Martin Robel

University of Bamberg, Chair of Industrial Information Systems, Bamberg, Germany
martin.robel@uni-bamberg.de

Abstract. Die systematische Wiederverwendung spielt eine wichtige Rolle bei der Entwicklung anpassbarer, serviceorientiert ausgerichteter Informationssysteme. Die vollständige Beschreibung wiederverwendbarer Funktionsbausteine bildet die Basis der erfolgreichen Identifikation und Komposition solcher im Lebenszyklus. Mit dem UnSCom-Spezifikationsrahmen (Unified Specification of Components) lässt sich hierbei die fachliche Funktionalität textuell sowie grafisch beschreiben. Im vorliegenden Beitrag wird anhand des entwickelten Tools UnSComT2G gezeigt, wie sich eine textbasierte Spezifikation automatisiert in das entsprechende grafische Format übersetzen lässt. Ziel ist es, den beteiligten Rollen gemäß ihrer Präferenzen die entsprechenden Informationen, sei es für die Entwicklung oder die Komposition von Funktionsbausteinen, bereitzustellen.

Keywords: Komponentenorientierung, Spezifikation, UML, UnSCom.

1 Motivation

Mit der Bereitstellung spezifischer Funktionalität sowohl als Web-Service in der Cloud als auch als herkömmliche Komponente lassen sich komplexe Anwendungssysteme als serviceorientierte Architektur realisieren. Die damit einhergehende höhere Flexibilität durch die systematische Wiederverwendung erlaubt eine schnellere Reaktion auf Marktveränderungen und verspricht vor allem mit Blick auf die Entwicklungskosten und –zeiten Vorteile [1]. Hohe erwartete Wachstumsraten in den nächsten Jahren unterstreichen zudem die herausragende Bedeutung von Cloud-Services [2]. Fraglich bleibt, wie Funktionsbausteine hinreichend detailliert zu beschreiben sind, um eine Auswahl, Komposition oder aber deren Entwicklung zu ermöglichen. Eine Antwort kann ein Spezifikationsrahmen wie der UnSCom-Spezifikationsrahmen (Unified Specification of Components) liefern [3]. Fachkomponenten werden dort als spezielle Funktionsbausteine auf verschiedenen Ebenen sowohl mit textbasierten als auch mit grafischen Notationen umfassend beschrieben. Im Vordergrund des Beitrags steht in diesem Zusammenhang die Beschreibung der fachlichen Funktionalität, welche sich unter Verwendung von normsprachlichen Beschreibungen (Satzbauplänen) textbasiert und grafisch mithilfe von Diagrammen der Unified Modeling Language (UML) [4]

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

spezifizieren lässt. Die Tatsache, dass textbasiertes und grafisches Format über ein gemeinsames Metaschema integriert sind, wirft die Frage auf, inwieweit eine vorliegende textbasierte Spezifikation automatisiert in das ihr entsprechende grafische Äquivalent überführt werden kann. Zur Beantwortung dieser Frage werden im Anschluss an die theoretischen Grundlagen Lösungsansätze und deren konkrete Umsetzung im UnSComT2G-Tool vorgestellt. Die Demonstration eines kleinen Anwendungsfalls sowie die Zusammenfassung und ein Ausblick für weitere Untersuchungen runden den Beitrag ab.

2 Theoretische Grundlagen

In den folgenden Teilabschnitten werden der Begriff Fachkomponente sowie die Inhalte der fachlichen Komponentenspezifikation erläutert.

2.1 Fachkomponenten und Spezifikationsrahmen

Zu den grundlegenden Eigenschaften von Komponenten zählen neben der Wiederverwendbarkeit, Abgeschlossenheit, Vermarktbarkeit sowie Verborgenheit der Realisierung die Einsatzmöglichkeit in zur Entwicklungszeit unvorhersehbarer Kombination mit anderen Komponenten [5].

Definition 1 [Fachkomponente]: „Eine Fachkomponente ist eine Komponente, die eine bestimmte Menge von Diensten einer betrieblichen Anwendungsdomäne anbietet“ [3]. Diese Dienste werden dabei über wohldefinierte Schnittstellen bereitgestellt. Hinsichtlich der vollständigen, widerspruchsfreien und eindeutigen Beschreibung der Außensicht im Rahmen der Spezifikation eignet sich die Verwendung eines Spezifikationsrahmens. Dieser gibt vor, welche Eigenschaften in welcher Form zu beschreiben sind und wie diese schließlich zu einem Gesamtergebnis verbunden werden können [3]. Grundlage des Beitrags bildet der UnSCom-Spezifikationsrahmen, womit sich eine Fachkomponente auf neun Vertragsebenen beschreiben lässt. Die Vollständigkeit der Spezifikation wird durch die Berücksichtigung der unterschiedlichen Abstraktions- und Modellierungssichten sichergestellt [3]. Die relevanten Vertragsebenen zur Beschreibung der angebotenen Dienste aus fachlicher Sicht werden nachfolgend dargestellt.

2.2 Fachliche Komponentenspezifikation

Ziel der Spezifikation auf den fachlichen Ebenen ist die technologieunabhängige Beschreibung der Funktionalität. Die Basis bildet ein Begriffssystem des Anwendungsbereichs, das die bei Informationsverarbeitung verwendeten Informationsobjekte (Dinge), die unterstützten Funktionen (Handlungen) sowie die Prozesse (Abläufe) beinhaltet [3]. Neben einem Lexikon zur Klärung der Begriffe wird zusätzlich eine Aussagensammlung zur Abbildung der Beziehungen zwischen den Begriffen aufgebaut. Konkrete Aussagen werden aus einer Normsprache abgeleitet, mithilfe derer allgemeine Aussagen unter Verwendung der definierten Grammatik

(Syntax) als normsprachliche Beschreibungen zur Verbindung von Begriffen dargestellt werden. Zur Bildung syntaktisch korrekter Aussagen umfasst die Definition der Grammatik verschiedene Wortarten sowie darauf aufbauend Regeln zu deren Bildung in Form von Satzbauplänen. Grafisch werden die Aussagen bezüglich der Informationsobjekte und Funktionen als UML-Klassendiagramm sowie der Prozesse als UML-Aktivitätsdiagramm dargestellt [4]. Die Modellierungskonstrukte der UML-Klassen und UML-Aktivitäten werden in Bezug zur festgelegten Semantik im Metaschema, das die Konsistenz der unterschiedlichen Formate sichergestellt, gezielt ausgewählt und angepasst [3].

3 Konzeption des Tools

Basierend auf den theoretischen Grundlagen wurden zunächst Problembereiche identifiziert, welche dann jeweils durch konkrete Anforderungen an die Lösungsansätze präzisiert wurden. Die Übersetzung in das grafische Format adressiert dabei drei Problembereiche: Automatisierung der Auswertung normsprachlicher Aussagen, Übertragung der Informationen auf UML-Konstrukte (Modell-Repräsentation) sowie Visualisierung des Modells als UML-Diagramm. Nachfolgend werden zunächst die Lösungsansätze für die Problembereiche vorgestellt, um im Anschluss die konkrete Umsetzung im Tool darstellen zu können.

3.1 Ansätze zur Problemlösung

Zur Auswertung der Inhalte von Aussagen wird das Konzept der regulären Ausdrücke genutzt. Die Beschreibung der Muster von Zeichenketten auf Basis einer eigenen Beschreibungssprache stellt dabei die Auswertbarkeit sicher und erlaubt die gezielte Extraktion von relevanten Inhalten. Zur Erzeugung der grafischen Repräsentation als UML-Diagramme wurde das Software-Tool PlantUML verwendet, welches über eine Anwendungsschnittstelle in bestehende Projekte integriert werden kann [6]. Den Input bildet hierbei eine menschenlesbare Textdatei in einem proprietären Format des darzustellenden UML-Modells. Mit den bisher vorgestellten Lösungsansätzen lassen sich die Entwicklungsaufgaben abgrenzen, welche sich insbesondere auf die Übertragung normsprachlicher Konstrukte auf reguläre Ausdrücke sowie die Entwicklung der Modell-Repräsentation beziehen. Aufgrund der umfangreichen Unterstützung regulärer Ausdrücke und der Implementierung von PlantUML als Java-Bibliothek wurde das Projekt mit Java umgesetzt. Das Zusammenspiel der Ansätze in einem durchgängigen Arbeitsablauf wird im Folgenden bei der Vorstellung der Anwendungslogik näher beschrieben.

3.2 Verarbeitungsprozess der Anwendungslogik

Die Architektur der Anwendungslogik orientiert sich an dem zugrunde liegenden Verarbeitungsprozess aus Abb. 1, welcher die einzelnen Verarbeitungsphasen unter

Verwendung der vorgestellten Lösungsansätze verknüpft. Im Folgenden werden die drei Phasen Konfiguration, Verarbeitung und Generierung vorgestellt.

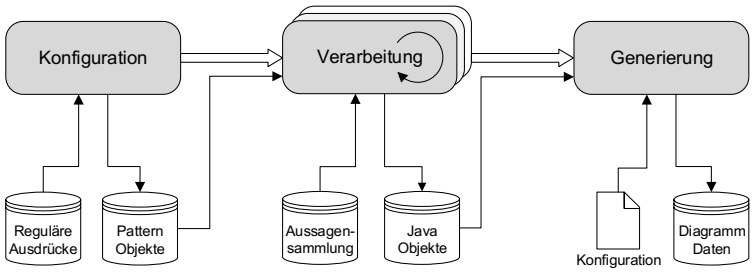


Abbildung 1. Verarbeitungsprozess

Aufgabe der Konfiguration ist die Vorbereitung der Auswertung von Aussagen in der Verarbeitungsphase. Die Ausgangsbasis bildet das Match-State-Objektmodell aus Abb. 2, das die drei abstrakten Schritte bei Verarbeitung regulärer Ausdrücke in einem Verarbeitungsmodell zusammenfasst [7]. Demnach wird der Ausdruck in der Vorbereitung zunächst als Zeichenkette erstellt, kompiliert und mit einer Eingabe-Zeichenkette verbunden, bevor im zweiten Schritt die Prüfung auf Übereinstimmung und im letzten Schritt die Betrachtung und Auswertung des Ergebnisses folgt. Analog zum Verarbeitungsmodell wird in der verwendeten Java-Standardbibliothek das Regex-Objekt in Form eines Pattern-Objekts und das Match-State-Objekt in Form eines Matcher-Objekts abgebildet. Anfragen an das Matcher-Objekt erlauben Auswertungen, mit welchen sich neben der bloßen Rückgabe von Wahrheitswerten auch gezielt Teile der Eingabe-Zeichenkette extrahieren lassen [8]. Im Verarbeitungsprozess aus Abb. 1 wird dabei ersichtlich, dass bei der Konfiguration zunächst die regulären Ausdrücke in vorkompilierte Pattern-Objekte überführt und der nächsten Phase, der Verarbeitung, bereitgestellt werden.

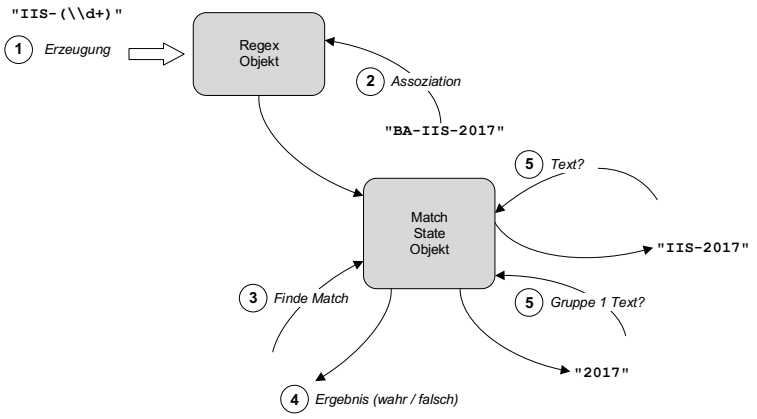


Abbildung 2. Match-State-Objektmodell (in Anlehnung an [7])

In der Verarbeitungsphase erfolgen schließlich alle notwendigen Schritte, um konkrete Aussagen einer Aussagensammlung in eine interne Repräsentationsform des beschriebenen Modells zu transformieren. Die interne Datenstruktur des Modells wird durch konzeptuelle Objekte beschrieben, die aus einem allgemeinen Abbildungsobjekt abgeleitet werden. In einem iterativen Prozess wird die Aussagensammlung sukzessive auf die entsprechenden konzeptuellen Objekte abgebildet und die Datenstruktur fortlaufend aktualisiert. Im Anschluss an die Verarbeitungsphase folgt zuletzt die Phase der Generierung, bei welcher die verarbeiteten Inhalte gemäß der definierten Syntax der PlantUML-Referenz [6] übersetzt und schließlich zur Erzeugung der UML-Diagramme durch PlantUML verwendet werden. Dabei existiert für jede UML-Diagrammart eine separate Generator- sowie Konfigurationsklasse zur Übersetzung in das proprietäre Format. Zur Berechnung der Position der Elemente in Klassendiagrammen nutzt PlantUML zusätzlich die Visualisierungssoftware Graphviz [9]. Die sich hinsichtlich der Prozesssteuerung ergebenden Unterschiede bei der Verarbeitung von Informationsobjekten, Funktionen oder Prozessen sowie der Wahl der benötigten Konfigurationsklasse wurden mithilfe entsprechender Steuerungsklassen berücksichtigt. Diese Steuerungsklassen werden dabei von einer abstrakten Steuerungsklasse als zentrales Element der Prozesssteuerung abgeleitet.

4 Anwendungsfall zur Demonstration

Im Folgenden wird im Rahmen eines stark vereinfachten Anwendungsfalls der Fokus von der abstrakten Darstellung des Verarbeitungsprozesses aus Abschnitt 3.2 auf die Betrachtung der Ergebnisse gelegt. Es wird angenommen, dass die textbasierte Spezifikation einer Buchungskomponente für Elektrofahrzeuge als Aussagensammlung im UnSCom/T-Format auf allen drei Vertragsebenen zur Beschreibung der fachlichen Funktionalität vorliegt. Als Eingabe dient je Vertragsebene eine Textdatei mit den darzustellenden Aussagen. Zur Sicherstellung der korrekten Verarbeitung werden zudem die einzelnen Aussagen während des Einlesens geprüft, ob sie sich syntaktisch einem Satzbauplan zuordnen lassen. Ist dies nicht der Fall, wird dies dem Nutzer angezeigt und eine Hilfestellung geboten, sofern zumindest die Kategorie erkannt wurde.

In Abb. 3 ist jeweils die Aussagensammlung zu Informationsobjekten, Funktionen sowie Prozessen im UnSCom/T-Format sowie das durch das Tool erzeugte Klassen- bzw. Aktivitätsdiagramm im UnSCom/G-Format gegenübergestellt. Bezüglich der Informationsobjekte wird das Objekt Kunde durch die Merkmalsvereinbarung um Attribute ergänzt. Im Kontext der Beziehungsart Inklusion ist die Unterscheidung eines Kunden in Standard- oder Premiumkunde als Spezialisierung beschrieben. Auf der Vertragsebene der Funktionen werden in Form der Aggregation mit den Funktionen Terminfestlegung und Buchungsbestätigung die Bestandteile der Funktion Buchung durchführen spezifiziert. Auf der Prozessebene werden schließlich die genannten Funktionen zu einem Ablauf verknüpft. Zusätzlich verdeutlicht die exklusive Verzweigung die unterschiedlichen Möglichkeiten bei der Fahrzeugauswahl in Abhängigkeit des Kundenstatus.

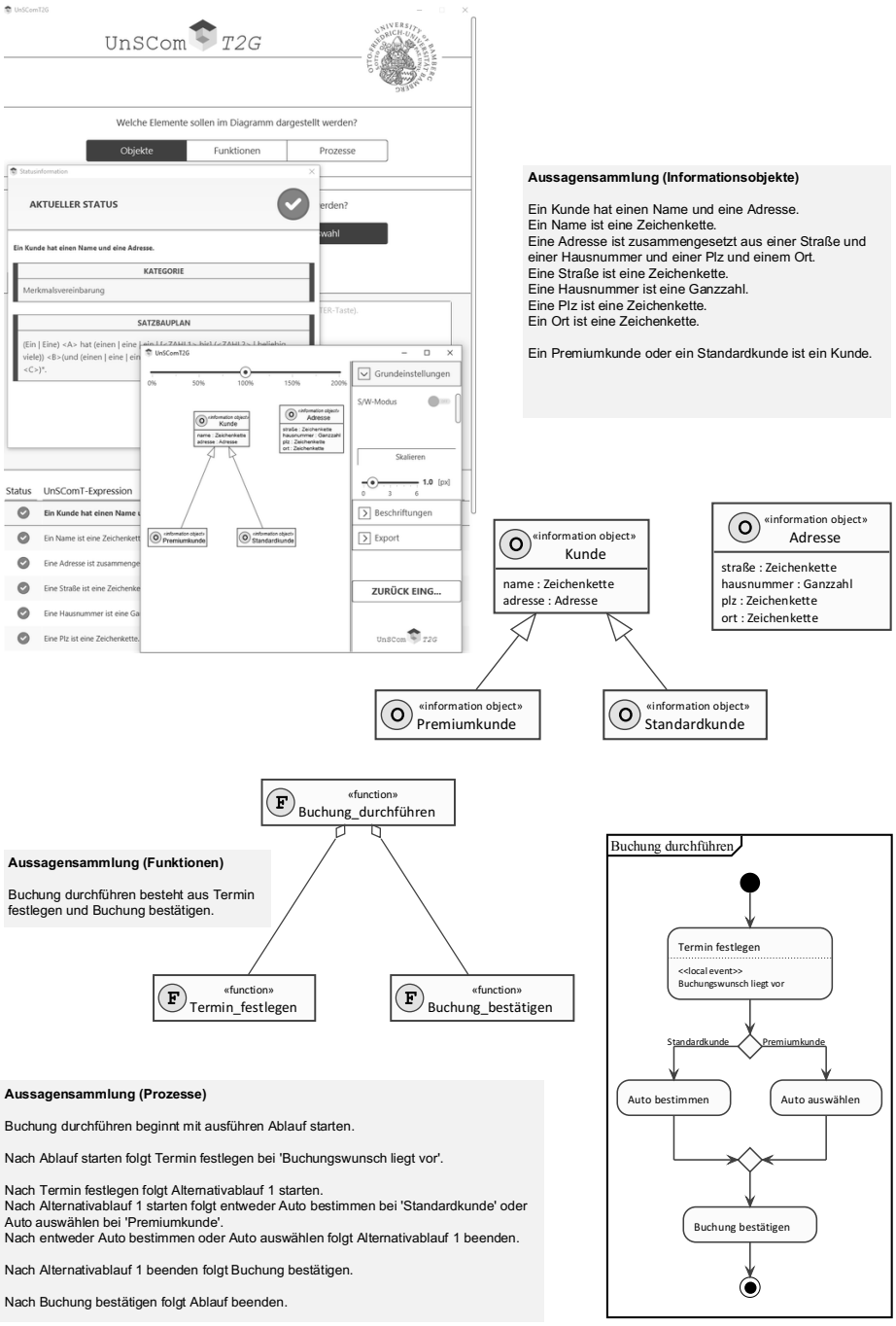


Abbildung 3. Fachliche Spezifikation der Buchungskomponente mit UnSComT2G-Tool

5 Zusammenfassung und Ausblick

Im vorliegenden Beitrag konnte gezeigt werden, wie sich textbasierte, normsprachliche Beschreibungen automatisiert auf Grundlage eines integrierten Metaschemas in das entsprechende grafische Format übersetzen lassen. Ausgehend der theoretischen Grundlagen zur Komponentenspezifikation wurde im zweiten Abschnitt auf Basis der Problembereiche die Umsetzung von Lösungsansätzen zunächst abstrakt beschrieben. Im Anschluss daran wurde das Zusammenspiel verschiedenen Lösungsansätze bei der Spezifikation einer Buchungskomponente demonstriert. Aus Sicht der Praxis entfällt für Marktplatzbetreiber bzw. Verwalter von Komponentenkatalogen die aufwändige, manuelle Übertragung in das grafische Format, zum anderen kann PlantUML sowie das Konzept der regulären Ausdrücke ebenso in anderen Entwicklungskontexten genutzt werden. In der Folge können die verschiedenen Formate umfassend und gemäß den entsprechenden Präferenzen der Verwender genutzt werden. Mit Blick auf die Forschung besteht ein Forschungsbedarf dahingehend, die Wirkung textbasierter und grafischer Notationsformen bei der Komponentenspezifikation auf die unterschiedlichen Adressatenkreise näher zu untersuchen. Besonders interessant erscheint in diesem Zusammenhang die Frage, inwieweit sich in einem möglichen hybriden Ansatz durch die Kombination von Text und Grafik Vorteile hinsichtlich der Verständlichkeit und Nutzbarkeit der Komponentenspezifikation ergeben können. Verbunden mit dem geringen Aufwand bei der Erstellung eines entsprechenden grafischen Formats ebnet das vorliegende Tool durch die automatisierte Übersetzung den Weg zur Untersuchung derartiger Fragestellungen. In Zukunft ließe sich somit anhand der Ergebnisse von Studien das Tool sukzessive in seiner Funktionalität erweitern.

Literatur

1. Sharp, J., Ryan, S.: A Review of Component-Based Software Development. In: 26th International Conference on Information Systems (ICIS). (2005)
2. Gartner Inc., http://www.gartner.com/newsroom/id/3616417 (Accessed: 26.09.2017)
3. Overhage, S.: Vereinheitlichte Spezifikation von Komponenten: Grundlagen, UnSCom Spezifikationsrahmen und Anwendung. Dissertation, Universität Augsburg (2006)
4. Object Management Group, http://www.omg.org/spec/UML/2.5/PDF/ (Accessed: 20.09.2017)
5. Ackermann, J., Brinkop, F., Conrad, S., Fettke, P., Frick, A., Glistau, E., Jaekel, H., Kotlar, O., Loos, P., Mrech, H., Ortner, E., Overhage, S., Raape, U., Sahm, S., Schmietendorf, A., Teschke, T., Turowski, K.: Vereinheitlichte Spezifikation von Fachkomponenten. Technical Report, Gesellschaft für Informatik (GI) (2002)
6. PlantUML, http://plantuml.com/PlantUML_Language_Reference_Guide.pdf (Accessed: 20.09.2017)
7. Friedl, J.E.F.: Mastering Regular Expressions. O'Reilly, Sebastopol (2006)
8. Oracle, https://docs.oracle.com/javase/8/docs/api/java/util/regex/package-summary.html (Accessed: 20.09.2017)
9. Graphviz, http://www.graphviz.org/ (Accessed: 20.09.2017)

Modelling Product-Service Systems: An Empirical Analysis of Requirements From a Process-oriented Perspective

Simon Hagen[1], Thorsten Schoormann[2], Sven Jannaber[1], Ralf Knackstedt[2], and Oliver Thomas[1]

1 University of Osnabrueck, Chair of Information Management and Information Systems
Katharinenstr. 3, 49074 Osnabrueck, Germany
{simon.hagen,sven.jannaber,oliver.thomas}@uni-osnabrueck.de
2 University of Hildesheim, Department of Information Systems and Enterprise Modelling,
Universitätsplatz 1, 31141 Hildesheim, Germany
{thorsten.schoormann,ralf.knackstedt}@uni-hildesheim.de

Abstract. Product-service systems (PSS) offer great opportunities for companies to alter their business model, for example, for being competitive in the digital era. One important contributor for developing PSS is the presence of suitable modelling languages. In order to obtain requirements from the industry regarding process-oriented PSS modelling languages, we conducted 18 interviews with experts from 14 different companies. Based on over eight hours of transcripts, a total of 27 requirements were identified and compared to well-established process-oriented modelling languages (e.g., BPMN, UML and EPC). The findings can act as a framework for developing or adapting modelling languages—method engineering—to fulfil current industry needs.

Keywords: Product-service system, Modelling, Process modelling language

1 Introduction

In an increasingly digitalized world, the concept of product-service systems (PSS) gains importance (e.g., [1]) and classic business models aim at shifting to PSS [2]. However, the transformation from a product to a service-centred value proposition is challenging and is requiring changes in different aspects of a company such as the infrastructure and supporting business processes [3, 4]. From a process-perspective of PSS, for example, workflows of services, products and software have to be unified, coordinated and communicated (also across different companies) in order to allow for offering a solution that best fits individual needs of customers. Moreover, due to the increased complexity, further capabilities are needed for which reason value-adding networks are created [5]. In order to tackle these challenges, developing and modelling PSS becomes a crucial aspect in research and practice (e.g., [3, 6]).

Because modelling techniques can support transformation, the demand in adequate languages is present and has been explored in recent years and decades in the context

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

of PSS [6]. As a result, numerous modelling languages with various purposes are proposed. Due to the variety of such languages and their extensive set of applicability, the selection of appropriate approaches becomes a challenging task. While prior studies on PSS modelling tend to be theoretically, this study aims at empirically gathering requirements from practice that should be addressed by a process modelling technique in PSS. Thus, we formulated the following research question: *Which requirements for process-oriented PSS modelling languages do practitioners currently have?*

Our contribution is a categorized set of requirements that provides guidance for researchers and practitioners in developing process-oriented PSS modelling languages and supporting tools. As a first step, we briefly outline the background related to modelling in PSS (Section 2). Based on our research design (Section 3), we derived five categories and 27 requirements regarding process modelling languages in the context of PSS. To do so, 18 interviews with experts from 14 different companies with more than eight hours of audio recording material were conducted, transcribed and coded. In order to validate our findings and to highlight if current languages support these requirements, we compared the 27 items to six established (BPM) modelling approaches [7] (Section 4). Finally, we discuss the results, provide aspects for further research (Section 5) and conclude with our main findings (Section 6).

2 Process-modelling in Product-service Systems

The integration of (physical) products and services to one marketable bundle of product(s) and service(s), which in combination serve the demands of the user, can be defined as product-service system (e.g., [8, 9]). The share of product or service components is hereby not defined and the system can be offered by a singular firm or a network of companies [10, 11]. The primary goal of a PSS is to provide a solution to the customer that best satisfies his needs in order to generate value for him, and therefore for the offering company. This is accomplished by provisioning the solution through a certain period of time, which leads also to a continuous revenue stream, rather than the onetime sale of a (physical) product. The development of PSS is referred to as product-service systems engineering or service engineering [12].

Since the first appearances of PSS in science and practice, many have thought about intuitive and efficient ways for planning, modelling and developing those systems. In addition, authors also stress the importance of the process dimension of a PSS, since it represents an essential part of the system [4]. Similar to information or process modelling, different approaches were proposed distinctively and in combination (e.g., [6, 13, 14]) – for example, Pezzotta et al. used Business Process Model and Notation (BPMN) combined with Service Blueprinting in their PSS design methodology [15]. However, most of them are developed in a theoretically manner and have not been extensively tested in practice [3], nor are they widely applied in industry. In order to contribute to the outlined deficits, this study focuses on empirical requirements regarding PSS modelling from a process-oriented perspective by analysing common process modelling languages such as BPMN, Unified Modelling Language (UML) and Event driven Process Chain (EPC) [7].

3 Research Design

The data collection was performed by conducting interviews with 18 (domain)experts from 14 different companies, following Meuser and Nagel [15]. In this study, a person is considered an expert due to her/his expertise in a certain domain or industry, however not because of expertise in (process) modelling. The experts selected are from different industries and departments to cover various fields such as software, production and service (Table 1). In order to achieve comparable results, an interview guideline was prepared in advance – based on recommendations by Porst [16]. The questions focus on the representation of PSS in particular, and thus, consist of the following topics: (I) documentation of processes (e.g., which notations? Use of software tools? Experiences with notations? Improvement potential for notations/tools?); (II) use of models (e.g., Where do apply such models?); (III) quality control (e.g., How do you ensure quality of the models?); (IV) responsibilities (e.g., who is in charge for managing models?); (V) data of interviewees (e.g., position in company etc.). For ensuring the applicability of the guideline, it was tested in advance in a pre-test and the interviews were carried out by three different interviewers (IS researchers).

The recorded interviews—a total length of 08:11 hours—were transformed into transcripts and analysed as proposed by Mayring [17]. After paraphrasing important statements, each statement has been generalized to a more generic abstraction level and in two additional steps reduced to the essence of the message. These steps were performed independently by three researchers and merged afterwards to guarantee a common understanding as well as to contribute to the robustness of the results. For categorization, each statement was clustered into a category by the same researchers in an independent manner. Next, in order to find a consensus, the categories were discussed. As a result, five requirement categories were determined (c.f. section 4.1).

Table 1. Overview of experts interviewed

#ID	Expert position	Industry	Length [m:s]
01	Employee	Software (requirements engineering)	10:32
02	CEO	Software (development)	09:17
03	Employee	Software (database management)	13:52
04	Employee	Service (support engineer)	10:54
05	Academic associate	Service	13:28
06	Manager IT	Service (process management, ERP)	11:23
07	Manager „process engineering“	Production (steel industry)	34:03
08	Manager „functional safety“	Production (automotive industry)	7:55
09	Manager „maintenance“	Production (automotive industry)	10:02
10	CEO	Electrical engineering	32:27
11	Manager „service“	Electrical engineering	49:54
12	Deputy CEO	Electrical engineering	23:58
13	CEO	Mobility	25:56
14	Product development	Mobility	49:53
15	Product & company development	Agricultural engineering	57:17
16	Manager „smart services“	Heating, Ventilation & Air Condition industry	40:44
17	Manager „sales“	Heating, Ventilation & Air Condition industry	42:32
18	Manager „market & service“	Agricultural engineering	47:34

4 Results

4.1 Requirements

In total, 27 items were identified as requirements that are titled and described in the following section. Five different categories, namely (1) representation, (2) navigation/ linking, (3) additional information, (4) design/handling, and (5) transformation were derived. Moreover, each of the requirements was assigned with an ID to allow for referencing them in the later sections.

Representation (1). The first category 'representation' (Table 2) deals with aspects that should be illustrated by a modelling language in an explicit way, for example by providing graphical or textual constructs. Due to current changes (e.g., smart factories, smart cities and smart "X"), there is an increasing relevance of data and information. Thus, *information flows (1.4)* to highlight, which actor needs which information at what time (e.g., in a network with various organizations) and *data-objects (1.6)* to consider technology and supporting software should be represented. In addition, *machine/service-related information (1.2), e.g.* availability or downtimes, should be visualized. Experts stated that "machine information" or "electrical circuit diagrams" need to be provided because often an entire process is affected by this.

Another cluster of requirements is dealing with legal aspects, standards and specifications. In global cooperation's, *legal aspects (1.7)* such as employment laws and labour agreements have to be considered, for example, to coordinate which actor may support customer (e.g., 24/7 support). Experts argued that "legal regulations should be represented, for example, in collaboration with locations in the US and Europe […] to spread the service delivery." Besides legal guidelines, internal specifications are relevant such as *safety instructions (1.11*)—which resources (e.g., helmet or safety jacket) are prescribed for certain tasks?—and *time aspects (1.12)*—"visualize deadlines and different timelines" because in a collaboration the execution of certain activities often depend on prior processes and deadlines. In addition, the experts stated that many tasks are carried out because they need to follow *standards, norms or best practices (1.8)*. For example, "models should highlight that machine maintenance is executed following DIN 31051". Accordingly, a modelling language should allow visualizing which steps base on a certain standard, norm or best practice, because it supports the understanding of why a process is done in a specific manner and highlights the quality standards of a company.

Generally, actors, products and tasks are essential for every business process. Thus, a modelling language should allow representing (physical) *products and service objects (1.1)* and provide detailed models such as CAD-diagrams. Experts argued that models should "represent (sub-)products to assign activities to a specific output". Furthermore, different *types of activities (1.9)* are required to allow identifying analogue and digital ones. Experts highlighted this and argued that they "would like to analyse, which steps are executed analogue and which ones digitally." In doing so, *decisions (1.5)* are important for processes because "what happens if a common process has to be done in a divergent way?" or "We would like to see consequences of different process paths". Internal *actors (1.3)* "like users" as well as "employees and their qualifications" need

to be assigned to a model as well as *communication interfaces (1.10)* because various experts argued, “it is a huge challenge to demonstrate, which steps have to be carried out by the customer”. “The customer has to understand that certain tasks require collaboration.” Accordingly, a model should allow for highlighting crucial tasks that need input from another actor such as customers. Especially for co-creation scenarios, this is important.

Table 2. Model representation

Requirement (#)	*Description*
1.1: Products and service objects	Representation of (physical) products and service objects, to show more detailed models such as CAD-diagrams or object lists.
1.2: Machine/service-object information	Integration of information (e.g., availability or downtimes) about resources such as production machines.
1.3: Actors	Representation of actors that are involved in a process or task as well as qualifications that are required to carry out a certain task.
1.4: Information flows	Representation of information flows to show which actor needs which information on what time.
1.5: Decisions	Highlighting decisions (and options), because they play an essential role in coordinating a collaboration
1.6: Data-objects	Representation of data-objects, because of the increasing relevance of information, technology and supporting software systems.
1.7: Legal aspects	Consideration of legal aspects such as employment laws, which especially becomes important in global cooperation’s.
1.8: Standards/Norms	Visualization of steps and elements in a process model that base on a certain standard, norm or best practice.
1.9: Activity types	Representing of different activity types to allow identifying digital and analogue ones.
1.10: Communication interfaces	Highlighting crucial tasks that need input from other actors like customers. Especially for co-creation scenarios, this is important.
1.11: Safety instructions	Visualization of safety instructions related to the entire processes and single tasks to provide guidance for the employees.
1.12: Time aspects	Representation of time aspects to show which activities depend on prior processes and deadlines.

Navigation and linking (2). In order to reduce the complexity of creating a PSS (Table 3) as well as providing guidance in constructing a PSS, the *core phases (2.1*) of a collaborative project should be considered in a process model, for example, to position processes or single tasks to a certain phase. Experts stated that “it must be clear, which tasks belong to the development phase of a service.” Regarding PSS, standardized phases (e.g., conception, implementation and dissolution) can be used such as the DIN PAS 1094. This also refers to the need of following norms (1.8). Correspondingly, a language should allow for representing phases.

Moreover, the structure should contribute to the comprehensibility, which can be supported by aspects such as *hierarchies (2.2)* to allow for integrating different levels

of abstraction or *call of further workflows (2.3)* to refer to further processes and workflows (e.g., by implementing a service-oriented architecture). Experts stated that "it has to be visualized, which use cases and workflows are triggered by a specific process step." In the era of digitalization, internet of things (IoT), smart X and industry 4.0, further types of models become increasingly important for PSSs. The experts argued that particularly software-oriented diagrams (e.g., for components, code and interfaces) are crucial, for example to "represent which steps a customer has to carry out in a software" or "which components are applied to support specific tasks". A language should allow for *embedding different types of diagrams (2.4)*.

Table 3. Model navigation and linking

Requirement (#)	*Description and motivation through expert interviews*
2.1: PSS phases	Representing core phases of PSS construction (e.g., DIN PAS 1094) and allowing for assign objects and tasks to them.
2.2: Hierarchies	Creating hierarchies of processes and provide relationships between different levels of abstraction.
2.3: Further workflows	Presenting references to further processes/workflows (e.g., service-oriented architecture SOA).
2.4: Further diagrams	Embedding of different types of diagrams such as from software engineering (e.g., UML class diagram).

Additional information (3). This category (Table 4) addresses the integration of different quantitative aspects into a process model. As stated before, the integration of data gains increasing relevance for organizations. Consequently, *key performance indicator (KPI) (3.1)* need to be integrated into process models to provide information about the workload of employees, capacity of machines or tools, use of material etc. Many experts argued that indicators like time, costs, capacities of resources, quality etc. are required because they are important for coordinating the actors involved (e.g., to spread support tasks across different locations equality). In addition, data regarding a concrete processes should be *tracked (3.2)* and provided in a model. Various experts stated that information needs to be logged, for example, to "optimize processes that are too slow" or "to follow specified criteria". For the coordination of processes while collaborating with different organizations and locations, *collaboration data (3.3)* such as contact information are needed. Coordinating such networks requires "additional information of the actors involved".

Table 4. Additional model information

Requirement (#)	*Description and motivation through expert interviews*
3.1: KPI	Integration of KPIs related to products and service-objects to provide relevant information (e.g., workload, availability).
3.2: Tracking process data	Continuous tracking of process data to support versioning of process models and their performances.
3.3: Collaboration data	Consideration of collaboration data such as contact information to support the coordination between organizations and locations.

Design and handling (4). This category (Table 5) consists of aspects for the design, handling and construction of a process model and its language. Various experts stated that it is an fundamental issue to "allow the use of existing models on further devices like Smart Glasses" to better integrate them into daily practices of an organization as well as enable creating further formats (e.g., videos and games) based on a model. This requires configuration parameters, for example, related to the responsive design of a process model and the transformability to other formats and *further devices (4.1)*.

Moreover, modelling languages should be *adoptable (4.2)* to fulfil individual needs. For example, experts would like to reduce elements provided by a language to a 'core set' of constructs that are sufficient for a specific situation. Generally, a modelling language should have *limited complexity (4.4)*, for example, regarding the number of elements. Experts claimed for "simplicity", "transparency", and "slimness" of a model (see 4.2). In addition, although different interviewees stated that they "do not focus on rules", numerous of them followed standardized steps related to the construction of a model—mostly by following rules that are provided by a tool. Thus, a modelling language should allow for *standardized construction (4.3)*.

In contrast to the documentation and easy interpretation of a model, experts require the instantiation of a process model. Accordingly, a modelling language should allow for *being executable (4.6)*, for example, in a workflow management system. Furthermore, experts claim for "opportunities that allow for commenting certain model constructs", for example, to point out potential for improvement of a process. Hence, *remarks (4.5)* and comments need to be integrated.

Table 5. Model design and handling

Requirement (#)	*Description and motivation through expert interviews*
4.1: Further devices	Usage and transformability of a model to further devices such as Smart Glasses in order to better integrate them into daily processes.
4.2: Adoption of model constructs	Adaptation of model constructs to fulfil individual needs like reducing an entire set of modelling elements to a 'core set'.
4.3: Construction procedure	Standardized steps and rules for constructing of a certain model in order to provide guidance for the modeller and unity of a model.
4.4: Limited complexity	Limited complexity regarding the application of a modelling language, for example, regarding the number of elements (see 4.2).
4.5: Remarks	Annotation of remarks and comments to a process model in order to visualize, for example, potential or needs for improvement.
4.6: Execution	Instantiation and execution of a process model, for example, to enable the application in 'real scenarios'.

Transformation (5). Finally, the fifth category (Table 6) deals with requirements concerning the transformation of a process model and ways for further use. First, there is a need for *automatic generation (5.1)* of artefacts, for example, "software code should be transformable into models", "a diagram into a SQL-script", or "a model needs to be transformable into a database". Typically, this is discussed with terms such as model

driven architecture" (e.g., [18]). Therefore, *exchange formats* (5.2) of process models are important to allow for exchanging certain data (e.g., [19]).

Table 6. Model transformation

Requirement (#)	*Description and motivation through expert interviews*
5.1: Automatic generate artefacts	Support the transformation and automatic generation of artefacts such as code to model or model to code.
5.2: Exchange models	Support the specification of export and exchange formats in order to allow for transforming data between process models.

4.2 Evaluation

Following the identification of requirements, selected business process modelling notations are assessed regarding their applicability for process modelling in the context of PSS development. The selection of modelling notations adheres to previous work by [20, 21], and thus, encompasses the most prominent and wide-spread notations for process modelling. The notations under consideration are depicted in Table 7. Each notation is evaluated against the defined requirements presented in Section 4.1. The evaluation has been conducted by a team of three researchers with high expertise in the field of business process modelling. Following a two-step procedure, each participant evaluated the notations distinctively first. Afterwards, a workshop took place, in which the initial results have been aligned and finalized. The evaluation is based on available language specifications published by the respective standard development organization. In the EPC case, we have referred to the specification efforts conducted by [22, www.epc-standard.org] and previous consolidation work by for example [23]. The requirements presented in Section 4 are assessed regarding suitable modelling constructs offered by each respective notation that are capable to sufficiently represent each requirement within a model. Accordingly, workaround solutions such as text annotations to overcome specific requirements have not been considered. Fulfilled requirements, marked by an "X", reflect that a particular notation offers modelling constructs that fully support the requirement. A partial fulfilment is marked by an "(X)" and requirements not fulfilled are marked by an "-".

Reviewing the results in Table 7, it becomes apparent that the three dominant notations for business process modelling considered within this assessment, BPMN, EPC and UML Activity Diagram, yield the largest degree of coverage of the requirements extracted from the expert interviews. Especially in terms of process representation and transformation, the aforementioned notations provide a respective set of modelling constructs that suit the needs from practice. Exemplarily, most notations are able to depict a basic information flow as well as provide modelling constructs for resources (e.g., data object and actors). However, the analysis reveals that there are severe shortcomings across all evaluated notations that specifically concern their application within a PSS context. This becomes visible via PSS-related requirements such as the integration of domain-specific procedure models for PSS development within a modelling notation, or the necessity to express legal issues in a

modelled business process, which is of utmost importance for enterprises in the service domain. Even more striking are the shortcomings of traditional notations in the context of data-centric requirements, which have been frequently referred to over the course of the expert interviews, underlining a growing importance of data and data processing across all industry sectors. Here, the assessed notations are not able to handle various forms of data modelling and data integration, exemplarily by incorporating machine and sensor data into modelled processes. Furthermore, requirements summarized in Table 4 indicate that no notation fulfils practical demands concerning additional model information such as quantitative data, which facilitates model analysis or log data that supports model versioning.

Table 7. Validation of requirements
Caption: "X" requirement fulfilled, "(X)" partly fulfilled, "-" not fulfilled

#	Requirement title	BPMN 2.0	UML Activity	EPC	PetriNet	IDEF3	Ansi Flowchart
1.1	Products and service objects	(X)	(X)	(X)	-	X	-
1.2	Machine/service-object information	-	-	-	-	-	-
1.3	Actors	X	X	X	-	-	-
1.4	Information flows	X	X	X	X	X	X
1.5	Decisions	X	X	X	X	X	X
1.6	Data-objects	X	X	X	-	-	X
1.7	Legal aspects	-	-	-	-	-	X
1.8	Standards/Norms	(X)	-	-	-	-	-
1.9	Activity types	X	X	-	-	-	-
1.10	Communication interfaces	X	X	-	-	-	-
1.11	Safety instructions	-	-	-	-	-	-
1.12	Time aspects	X	(X)	-	-	-	(X)
2.1	PSS phases	-	-	-	-	-	-
2.2	Hierarchies	X	X	X	-	-	-
2.3	Further workflows	(X)	(X)	(X)	-	-	(X)
2.4	Further diagrams	-	(X)	(X)	-	-	-
3.1	Key performance indicator (KPI)	-	-	-	-	-	-
3.2	Tracking process data	-	-	-	-	-	-
3.3	Collaboration data	-	-	-	-	-	-
4.1	Further devices	-	-	-	-	-	-
4.2	Adoption of model constructs	-	-	-	-	-	-
4.3	Construction procedure	X	X	(X)	-	-	-
4.4	Limited complexity	(X)		X	-	-	X
4.5	Remarks	X	X	X	-	-	X
4.6	Execution	X	(X)	(X)	X	-	-
5.1	Automatic generate artefacts	X	X	(X)	X	-	-
5.2	Exchange models	X	X	X	X	-	-

5 Discussion and Further Research

Based on the results derived, we—in the following section—discuss different clusters and challenges that should be addressed by further research.

Being compliant with legal aspects and standards. Various aspects from the experts deal with following standards, norms and best practice, considering legal aspects as well as representing them in process models. This cluster can be addressed

by research streams that (a) investigate the applicability of methods from IS research such as process modelling languages to represent legal and contract issues as well as (b) investigate extensions for such languages like BPMN (e.g., [24]). However, currently no well-accepted set of constructs for supporting law and legal aspects exists, thus, further research can deal with (1) method engineering to support the representation of relevant constructs, (2) evaluation to analyse if the suggested extensions are applicable and (3) standardization of the evaluated constructs to allow for developing new software tools that support the construction of them.

Handling the increased relevance of data. Many experts highlighted the utmost importance of data, data structure and data-objects as well as applied software components. These criteria are particularly related to current topics such digitalization of processes, application of new devices or transparency of activities. As a result, data and evolvable information of entire processes, single objects and actors needs to be provided. Due to the importance, different experts ask for the integration of further detail diagrams that allow for presenting these aspects.

Using new devices. One major aspect in the transformation of models is the consideration of new devices for representing process models. Common, real-world scenarios such as maintaining production machines or using big tools to carry out a task hinder the use of process models in a traditional manner (e.g., a digital version on a computer or a printed version). Experts argued that the use of process models on new devices such as Smart Glasses or Smart Watches need to be improved [25]. In doing so, employees are enable to watch models while continuing work. Hence, further research on modelling languages and model formats needs to deal with design issues such as being responsive and being readable on different types of devices.

Modelling language vs. tool-support. Although our interviews aim at identifying requirements for process modelling languages, the implementation of some criteria depends on supporting software-tools. For example, KPIs, the tracking of process data, and the execution of a process model as well as the connection to further diagrams can be improved by software in particular. However, modelling languages can contribute to this by providing specific constructs that allow for visualizing these aspects (e.g., an icon that represents a stored detail diagram). Thus, especially the requirements, which are not fulfilled (c.f. section 4.2), might be supported by tools. In addition, tools enable the transformation of process models to further devices, which can barely enabled by a modelling language itself.

Model complexity vs. execution. Some of the requirements derived are in contrast. Especially criteria related to the reduction of model complexity and criteria related to the transformation and execution of a model. On one hand, experts argued for simplicity and slimness by reducing the set of modelling constructs provided or creating own rules for the application of a modelling language. On the other hand, experts require, such as, an automatic generation of models to software code or automatic transformation into an executable process model (e.g., in form of a workflow). Correspondingly, a modelling language needs to address the challenge between both streams, for example, by providing different level of abstractions or by providing features that operate in the background of a model (e.g., semi-formal, graphical representation layer and formal transformation layer).

6 Conclusion

Due to the importance of business processes in the development and implementation of PSS, the goal of our study was to identify requirements and challenges related to modelling PSS from a process-oriented perspective in an empirical manner. Our contribution is a set of 27 requirements that are based on 18 expert interviews from 14 companies and over eight hours of interview transcripts. Although we derived helpful insights for modelling PSS, our study is not free of limitations. First, our investigation is limited to industry partners and interviewees selected. The participants are from different fields to ensure a broad overview on the integration of service, products, software etc. Nevertheless, further interviewees (e.g., with domain and modelling experienced experts) may provide new aspects. We used an inductive approach that conceptualizes data from empiricism – as a next step, we plan to compare our set of requirements to the literature (deductive approach) to evaluate and revise our initial findings. Second, although our coding follows established guidelines [15, 17], the process is based on own interpretations and decisions. However, to contribute to the reliability, three different researchers coded independently and consolidated the results in a follow-up workshop. Third, in order to initial validate our results, we compared them to common modelling languages. Additionally, the results can be evaluated, for example, with experts to prove the coding and the generic usefulness (e.g., in a Delphi Study or in focus groups). As some of the 'general purpose languages' (e.g., BPMN) already address many aspects, future research can deal with the investigation of domain-specific variants for PSS.

Overall, our work gives orientation as to which requirements and challenges need to be addressed by modelling languages and can be used to redesign existing or develop new languages that support PSS modelling from a process-perspective.

7 Acknowledgments

This research is partly funded by the European Regional Development Fund and the State of Lower Saxony (NBank) in the scope of the research project SmartHybrid—Service Engineering (ID: 6-85003236) and Process Engineering (ID: ZW 6-85003451). We would like to thank them for their support.

References

1. Thomas, O., Nüttgens, M., Fellmann, M.: Smart Service Engineering: Konzepte und Anwendungsszenarien für die digitale Transformation. Springer Fachmedien Wiesbaden, Wiesbaden (2017)
2. Frank, U., Strecker, S., Fettke, P., vom Brocke, J., Becker, J., Sinz, E.: Das Forschungsfeld „Modellierung betrieblicher Informationssysteme". Wirtschaftsinformatik. 56, 49–54 (2014)
3. Vasantha, G., Roy, R., Lelah, A., Brissaud, D.: A review of product–service systems design methodologies. J. Eng. Des. 23, 635–659 (2012)
4. Becker, J., Beverungen, D.F., Knackstedt, R.: The challenge of conceptual modeling for

product–service systems: status-quo and perspectives for reference models and modeling languages. Inf. Syst. E-bus. Manag. 8, 33–66 (2010)
5. Becker, J., Bernhold, T., Knackstedt, R., Matzner, M.: Planung koordinierter Wertschöpfungspartnerschaften. Gabler Verlag (2017)
6. Morelli, N.: Developing new product service systems (PSS): methodologies and operational tools. J. Clean. Prod. 14, 1495–1501 (2006)
7. Harmon, P., Wolf, C.: The State of Business Process Management. A BPTtrends Rep. 1–52 (2016)
8. Mont, O.: Clarifying the concept of product – service system. J. Clean. Prod. 10, 237–245 (2002)
9. Thomas, O., Walter, P., Loos, P.: Design and usage of an engineering methodology for product-service systems. J. Des. Res. 7, 177 (2008)
10. Aurich, J.C., Schweitzer, E., Mannweiler, C.: Integrated design of industrial Product-Service Systems. Manuf. Syst. Technol. New Front. 543–546 (2008).
11. Goedkoop, M.J., Van Halen, C.J.G., Te Riele, H.R.M., Rommens, P.J.M.: Product Service systems , Ecological and Economic Basics. (1999)
12. Cavalieri, S., Pezzotta, G.: Product–Service Systems Engineering: State of the art and research challenges. Comput. Ind. 63, 278–288 (2012)
13. Boucher, X., Medini, K., Fill, H.: Product-Service-System Modeling Method. In: Domain-Specific Conceptual Modeling. pp. 455–482. Springer Int. Pub. (2016)
14. Pezzotta, G., Pirola, F., Pinto, R., Akasaka, F., Shimomura, Y.: A Service Engineering framework to design and assess an integrated product-service. Mechatronics. 31, 169–179 (2015)
15. Meuser, M., Nagel, U.: Das Experteninterview - konzeptionelle Grundlagen und methodische Anlage. In: Pickel, S., Pickel, G., Lauth, H.-J., and Jahn, D. (eds.) Meth. der vgld. Politik- und Sozialwissenschaft. pp. 465–479. VS, Wiesbaden (2009)
16. Porst, R.: Frageformulierung. In: Baur, N. and Blasius, J. (eds.) Handbuch Methoden der empirischen Sozialforschung. pp. 687–699. Springer Fachmedien, Wiesbaden (2014)
17. Mayring, P.: Qualitative Inhaltsanalyse. In: Handbuch Qualitative Forschung in der Psychologie. pp. 601–613. VS Verlag für Sozialwissenschaften, Wiesbaden (2010)
18. Czarnecki, K., Helsen, S.: Feature-based survey of model transformation approaches. IBM Syst. J. 45, 621–645 (2006)
19. Riehle, D.M., Jannaber, S., Karhof, A., Delfmann, P., Thomas, O., Becker, J.: Towards an EPC Standardization – A Literature Review on Exchange Formats for EPC Models. MKWI 2016 Band III. 4, 1167–1178 (2016)
20. Harmon, P., Wolf, C.: Business Process Modeling Survey. A BPTrends Rep. 36 (2011)
21. Recker, J.C., Rosemann, M., Indulska, M., Green, P.: Business process modeling: a comparative analysis. J. Assoc. Inf. Syst. 10, 333–363 (2009)
22. Jannaber, S., Karhof, A., Riehle, D.M., Thomas, O., Delfmann, P.: Invigorating Event-driven Process Chains – Towards an integrated meta model for EPC standardization. AQEMO (2016)
23. Fellmann, M., Bittmann, S., Karhof, A., Stolze, C., Thomas, O.: Do We Need a Standard for EPC Modelling? The State of Syntactic, Semantic and Pragmatic Quality. EMISA (2013)
24. Schoormann, T., Knackstedt, R., Haapio, H.: Modeling and Visualization in Law: Past, Present and Future. In: Internationales Rechtsinformatik Symposium IRIS (2017)
25. Metzger, D., Niemöller, C., Berkemeier, L., Brenning, L., Thomas, O.: Vom Techniker zum Modellierer – Konzeption und Entwicklung eines Smart Glasses Systems zur Laufzeitmodellierung von Dienstleistungsprozessen. In: Smart Service Engineering. pp. 193–213. Springer Fachmedien, Wiesbaden (2017)

Organizational Roles in Capability Management – Experiences from an Industrial Project

Kurt Sandkuhl[1], Hasan Koç[1]

[1] University of Rostock, Institute of Computer Science, Rostock, Germany
{kurt.sandkuhl, hasan.koc}@uni-rostock.de

Abstract. Methods are an important means to provide guidance and support for modelling, systems development, organizational change or problem solving. To engineer new methods is a complex task that usually includes various develop-evaluate cycles. The paper aims to contribute to method engineering by investigating the difference of methods in larger organization and in small and medium-sized enterprises (SME) with a focus on the roles required by a method and how their operationalization differs between larger enterprises and SME. The paper uses a capability management method and an SME case study introducing this method as the basis for presenting experiences.

Keywords: Capability modelling, role distribution, SME, method engineering.

1 Introduction

In many areas of computer sciences and information system engineering, methods are considered as an important means to provide guidance and support for modelling, systems development, organizational change or problem solving (cf. section 2.1). To engineer new methods is a complex task that usually includes various develop-evaluate cycles for different aspects of a method, such as procedures, tools and concepts. In the context of method engineering, the possibility to adapt a method to the situation of method use is considered as very important.

This paper aims to contribute to method engineering by investigating the difference of methods in larger organization and in small and medium-sized enterprises (SME). Our particular focus is on the roles required by a method and how their operationalization differs between larger enterprises and SME. Based on observations from engineering and use of the Capability-driven Development method (CDD) (see section 2.3) and an SME case (see section 4), the paper offers experiences considered relevant for method engineering. Capability management was selected as an application case because the introduction of capability management into an enterprise and establishment of an organization structure is, like for many other management approaches, affecting different parts of the enterprise and requires careful preparation.

The remainder of this paper is structured as follows: Section 2 summarizes the theoretical background for our work. Section 3 briefly presents the research method. Section 4 details the industrial case study and section 5 contains the case analysis and

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

observations. Section 6 discusses the case study results. Section 7 summarizes the work and reflects on future activities.

2 Background

2.1 Method Engineering

The field of method engineering focuses on knowledge how to systematically construct, deploy and maintain "methods". In general, methods are supposed to provide guidance for problem solving or for performing complex tasks in a way which is adaptive to the actual situation the method is applied in 13. Methods build on perspectives, values, principles, and concepts, which are expressed in the method's elements and express the underlying theories and rationality. Different conceptualizations of the term "method" and related terms have been proposed. If there is a close link between procedure, notation, and concepts, the term method component is used 16. The concept of method component is similar to the concept method chunk 12 and the notion of method fragment 14. Methods often consist of an integrated set components, which also could be referred to as methodology 15.

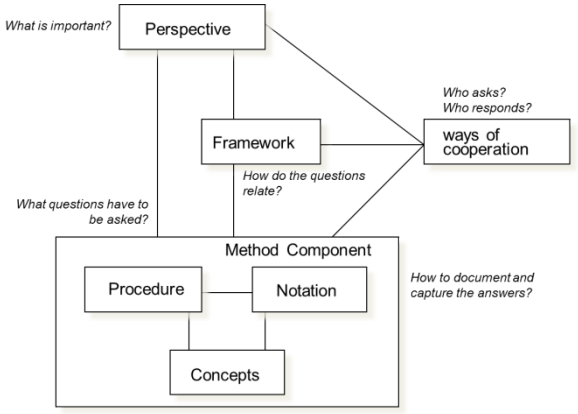


Figure 1. Method components according to Goldkuhl et al. 16

In this paper, we will use the method conceptualization proposed by Goldkuhl et al. 16. According to this conceptualization, comprehensive method descriptions ought to include perspective, framework, cooperation principles and method components. Figure 1 illustrates how these elements are related:

- Method components consist of concepts, procedure and notation. Concepts specify what aspects of reality are relevant and should be captured in a model. The procedure describes how to identify the concepts, incl. prerequisites and resources. The notation specifies how the result of the procedure has to be documented.
- Framework describes the relationships between the individual method components, i.e. sequence and conditions for the use of method components.

- Forms of cooperation: many modeling tasks require a range of specialist skills or cooperation between different roles. These necessary skills and roles must be described, along with the division of responsibilities and the form of cooperation.
- Perspective defines the aims and purpose of the method.

Goldkuhl et al. emphasize that methods should not be considered as rigid frame to be performed in always the same way, but methods and their components have to be adaptable for the situation at hand. Thus, the method conceptualization is not only suitable for traditional software modelling methods but has also been successfully applied for defining methods in other domains (see, e.g. [20]). The method conceptualization clearly shows the importance of defined roles in methods and supports our view that roles have to be subject of research in method implementation.

2.2 Capability Management

Different areas of business information systems use the term "capability". Although in literature there seems to be an agreement about the characteristics of the capability, but there is no generally accepted definition of the term. The definitions mainly put the focus on "combination of resources" 3, "capacity to execute an activity" 2, "perform better than competitors" 5 and "possessed ability 7".

Capabilities must be enablers of competitive advantage and should help companies to continuously deliver a specific business value in dynamically changing circumstances 6. They can be perceived from different organizational levels and thus are utilized for different purposes. According to 17 performance of an enterprise is the best, when the enterprise maps its capabilities to IT applications. Capabilities as such are directly related to business processes that are affected from the changes in context, such as, regulations, customer preferences and system performance. Companies need to anticipate these changes and respond to them 4. Adaptations to changes in context can be realized promptly if the required variations of processes have been anticipated, defined in advance and can be instantiated.

In this paper, capability is defined as the ability and capacity that enable an enterprise to achieve a business goal in a certain context 8. Ability refers to the level of available competence of a subject or enterprise to accomplish a goal; capacity means availability of resources, e.g. money, time, personnel, tools. This definition utilizes the notion of context, thus stresses the need to take variations of the standard processes into consideration. To summarize, capabilities are considered as specific business services delivered to the enterprises in an application context to reach a business goal. In order to facilitate capability management, we propose business service design explicitly considering delivery context.

2.3 Capability Design and Delivery for Capability Management

Capability management has been a topic of the EU-project "Capability-as-a-Service in Digital Enterprises (CaaS)" 10. CaaS investigated capability management in the context of enterprises and their business services. CaaS developed the Capability-

driven Development (CDD) approach. Business services are IT-based services which digital enterprises provide for their customers. Business services usually serve specified business goals, they are specified in a model-based way and include service level definitions. In order to ease adaptation of business services to changes in customer processes or other legal environments, CDD approach explicitly defines (a) the potential delivery context of a business service (i.e. all contexts in which the business service potentially has to be delivered), (b) the potential variants of the business service for the delivery context and (c) what aspect of the delivery context would require what kind of variation or adaptation of the business service.

Table 1: CDD-related stakeholders and roles

Role Group	*Role*	*Tasks*
Core CDD	Capability analyst	Analyses capabilities and operating context, to predict evolution of the context and to use these predictions by providing new services or improving existing services
	Method engineer	Person who has knowledge about CDD methodology and can tailor it for certain needs
	CDD provider	Provides and maintains the CDD methodology
Business stakeholders involved in CDD	Business service manager	Responsible for management strategies for changes in business and to identify opportunities for capitalizing on these changes
	Business analyst	A person who analyses the business models and proposes and guides changes in the business models
	Solution engineer	Configures and carries out business solution implementation, such as by using IT system support.
	Business service operator	Aims to follow best practices for achieving the delivery of services to the customers
	Solution architect	Works closely with solution engineer to ensure proper implementation. Solution architect is the link between the needs of the business and the solution engineer
Other stakeholders	Capability provider	Responsible of providing capabilities to the customer
	Customer (client)	The end user who benefits from the capabilities
	Capability worker	Works directly with the actions needed to deliver the capability
	Capability feedback provider	Provides capability feedback received from customers, capability workers and from other roles within the business

The potential delivery context basically consists of a set of parameters or variables, the context elements, which characterize differences in delivery. The combination of all context elements and their possible ranges define the context set, i.e. the problem

space to cover. The potential variants of the business service, which form the solution space, are represented by process variants. Since in many delivery contexts it will be impractical to capture all possible variants, we propose to define patterns for the most frequent variants caused by context elements and to combine and instantiate patterns to create actual solutions. If no suitable pattern is available, the conventional solution engineering process has to be used. The connection between context elements, patterns and business services has to be captured as transformation or mapping rules. These rules are defined during design time and interpreted during runtime.

The above simplified summary of our approach has been further elaborated by defining meta-model and method components, by developing a tool environment and by performing feasibility studies. Details are available in 9. The CDD methodology consists of several components with the following focus:

- Capability Design Process. Contains an overview on how to design, evaluate and develop capabilities by using process models, goal models and other model types.
- Enterprise Modelling. The component contains method components that guide the creation of enterprise models that are used as input for capability design.
- Context modelling. Describes the method components needed for analysing the capability context, and the variations needed to deal with variations.
- Reuse of Capability Design. This component contains guidelines for the elicitation and documentation of patterns for capability design.
- Run-time Delivery Adjustment. Describes the components needed to adjust a capability at runtime.

During methodology development, required roles and stakeholders were identified, which are summarized in Table 1 11. These roles and stakeholders are part of the descriptions of the method components, i.e. each CDD method component clearly defines the tasks and activities for each of the roles involved, but not all roles are involved in all method components. The roles shown in Table 1 reflect what ideally should be implemented in an organization using CDD with all method components. Experience from CaaS shows that this can be seen as set-up for larger organisations.

3 Research Method

Our research work started from a research question, which is based on the motivation presented in Section 1: *When introducing a new method into an organization, how does the operationalization of roles differ between large organizations and SME?*

The research method used for working on this research question is a descriptive case study. We decided to perform a case study in order to gather information pertinent for the subject area. Qualitative case study is an approach to research that facilitates exploration of a phenomenon within its context using a variety of data sources. This ensures that the subject under consideration is not explored from only one perspective, but rather from a variety of perspectives, which allows for multiple facets of the phenomenon to be revealed and understood. Yin differentiates various kinds of case studies 1: explanatory, exploratory and descriptive. The case study

presented in this paper has to be considered as descriptive, as it is used to describe the phenomenon of method implementation and the real-life context in which it occurs.

The case study focuses on capability management and the introduction of the CDD methodology for this purpose. CDD was developed using a method engineering approach which aims at the most preferable and, thus, somehow "ideal" role distribution as part of the cooperation principles (see section 2.3). Possible constraints regarding resource availability or organizational limitations, which are more likely to appear in SME than in larger organizations, were not taken into consideration. Furthermore, CDD was validated in several industrial cases which for larger organizations confirmed feasibility and utility of the role distribution. In this context, we decided to focus the case study on a medium-sized enterprise with the intention to compare this case study enterprise with the "ideal" CDD set-up which proved suitable for large organizations. The guiding questions for this investigation were:

- Q1: Which organizational roles were involved when introducing CDD into the organization?
- Q2: What were the activities or tasks performed by these roles?
- Q3: How do the roles identified in the use case relate to the roles included in the CDD approach?
- Q4: What conclusions can be derived from the comparison for CDD?

It should be noted that - from a perspective of the method engineering process of CDD - the case study can be seen as an additional validation step of CDD in the context of an SME. The result of this validation step might lead to a new cycle in CDD method design if the case study results should indicate the need and possibility of method (component) variants specifically adapted for SME needs.

4 Industrial Case

SIV group from Rostock (Germany) operates in the utilities sector and offers different kinds of services to their clients. SIV.AG (SIV) is the independent software vendor (ISV) of the ERP platform kVASy® while SIV Utility Services GmbH (US) acts as a business service provider (BSP) for kVASy®. The target group for these services is medium-sized utility providers and other market roles of the energy sector in Germany, Bulgaria, Macedonia and several other European countries (cf. Figure 2).

The BSP offers business process outsourcing (BPO) services, i.e. performing a complete business process for clients outside of the organization. The BSP as such provides services (e.g. billing, message clearing, and accounting) for the clients running kVASy®. Integrated with the business process environment, the "native" kVASy® services providing business logic for the energy sector are implemented using a database-centric approach. In particular, the BSP deals with intercompany business processes between partners in the utility market that requires exchange of messages about energy consumption or customer master data. The exchanged messages have to be both syntactically and semantically correct before being processed further. In case of a faulty message, the BSP might act as a clearing centre

involving the manual interaction of a human agent (knowledge worker). The decision whether to route a case to BSP depends on the case context, such as the policies between the BSP and the client, the available resources on both sides and the number of transactions to be cleared. Different roles participate to the BSP related activities, which are documented in the next section.

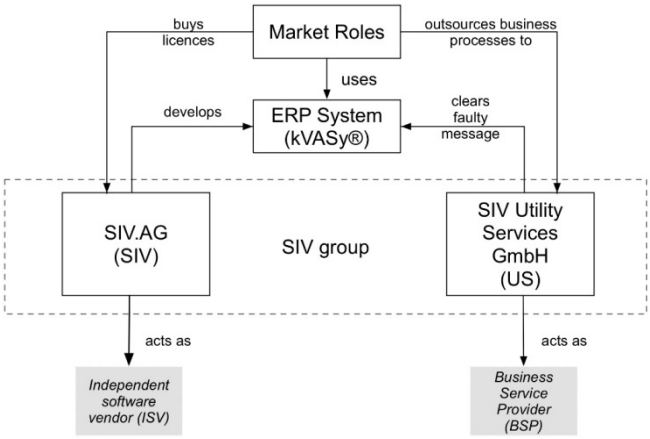


Figure 2: The business model of SIV group 19

5 Case Analysis and Observations

In order to find information for Q1 (roles involved when introducing CDD into the organization) and Q2 (activities and tasks performed by those roles), we analysed documents related to capability design in the case study company, which included material about business services and development processes related to capabilities. The documents were created between May 2014 and February 2016. They included

- hand-written notes from project meetings taken by project members,
- documents produced by bachelor and master students involved in the project, e.g. a report from a study project on instructions for clearing tasks, assignment work or thesis documents,
- deliverables from the CaaS project and internal working documents.

The analysis showed that only a few documents included explicit information about roles. More often, names of persons and their tasks were documented; sometimes the position was noted down, which often is identical to the corresponding role but also can include several roles. Since all documents are related to the same use case and period it was possible to deduct missing information (e.g. the name of a person having a certain role) from other material. As a result, Table 2 was created. Due to the fact that two different subsidiaries of SIV group are involved in the use case (SIV as software provider and SIV Utility Services (US) as BPO service provider; cf. Figure 2) and as the CaaS project created new roles in the organization, the table also includes a column “context” shows in which context the role exists.

Table 2: Identified roles in SIV case

Person	*Context*	*Role*	*Tasks*
JK	SIV group	Enterprise Architect	Development and maintenance of enterprise architecture as basis for business/IT alignment
UC	SIV group	Software product manager Strategy board member	Strategic / operational management of software product's business value and required technical features. Management of business / service strategy on enterprise level incl. target setting
TD	SIV	IT-architect	Definition of method and technology standards for all software products; evaluation of new technology developments and their impacts
FT	SIV	Systems engineer	Configuration and adaptation of software product for requirements from US or clients
HP	SIV	Platform operator	Maintenance and operation of the technical platform for software products and BPO services
TB, JS	US	BPO service manager Key Account Manager	Strategic and operational management of BPO product's business value and required customer features. Contractual agreements with client, service level agreements, client care
MA	US	Business analyst	Analysis of clients' business requirements and implementation in BPO service
TR	US	BPO knowledge worker	Perform all action to deliver the actual BPO service to the client
JK, UC	CaaS	Capability Analyst	Analysis of information about capabilities and operating context
JK	SIV	Solution Engineer	Development of adjustment algorithms; spec. of interaction between solutions components

The next step in our work was to compare the identified roles in the SIV case with the roles defined in the CDD methodology (Q3) to derive conclusions for the CDD roles and stakeholders (Q4). The comparison had to include the following aspects:

- CDD-related roles that are clearly visible in SIV case, although they might have different names.
- CDD-related roles not visible at all in the use case. For such roles, we need to investigate potential reasons of their absence and implications for CDD.
- Roles visible in the use case but not defined in CDD. Such roles could be candidates for including them in CDD.

For comparing the CDD-related roles with the situation at SIV group, we started from the CDD roles and stakeholders (cf. **Table 1**) and identified which roles performed the tasks associated to the CDD-roles within SIV. The result of this comparison is shown in Table 3. The results of this comparison show most of the roles defined in CDD correspond to the roles in SIV group. Existence of these roles is an indicator for the method engineers that they are sufficiently well-defined, useful

for organizational practice and should be kept further. The two CDD-roles, *business service operator* and *capability worker* were identified in the organization with different names. We argue that the change in those roles not only relate to the industrial practices, but also addresses the paradigm shift in the company by introducing CDD (e.g. application of patterns as best practices for business service operator or context-aware clearing processes provided to the capability worker). In that regard, one new role, *capability analyst* has to be established in the organization.

Table 3: Comparison of CDD-related and SIV stakeholder roles

CDD Role	*Corresponding role in SIV*	*Comparison / Comments*
Capability analyst	Capab.. analyst (SIV group)	Role was newly established at SIV group in the CaaS project
Method engineer	n/a	Method engineers for SIV group were the CaaS partner universities. Thus, this role was not required in SIV
CDD provider	n/a	The CaaS project provided and maintained the CDD methodology. Thus, this role was not required in SIV
Business service manager	Software product manager (SIV) BPO service manager (US)	As the business service forming the core of the capability and the software product being the basis for the business service are tightly intertwined, both SIV and US have to be involved with established roles when it comes to management strategies for business changes
Business analyst	Business analyst (US)	The business analyst at US has a wider area of responsibility than defined in CDD. The role includes business models and capability configuration
Solution engineer	Systems engineer Solution engineer (SIV)	Responsibility at SIV is divided in responsibility for the software product and responsibility for the capability operation
Business service operator	BPO knowledge worker (US)	Same task, but different name of the role
Solution architect	Enterprise architect (SIV group)	The enterprise architect has a wider responsibility than the solution architect, but the work includes the link between the needs of the business and the solution
Capability provider	Key Account Manager (US)	From an organizational view, the key account manager is responsible of providing capabilities to the customer.
Customer (client)	US and the clients of US	In SIV there are two customers: (1) US as an internal customer using the results of CaaS, (2) the clients of US using business services and capabilities provided by US
Capability worker	BPO knowledge worker (US)	Same task, but different name of the role
Capability feedback provider	Not established	Many roles provide feedback: software product manager, BPO service manager, business service operator, solution architect, BPO knowledge worker

Two roles defined in CDD, *method engineer* and *CDD provider*, were not established in the organization, as the CaaS project partners supported SIV group and the other industrial project partners in performing the tasks of the respective roles. Furthermore, the tasks of the *capability feedback provider* did not correspond to a single role in SIV group, it is rather performed by more than one stakeholder.

We observed that two roles from SIV could not be mapped to the role list from CDD: platform operator and IT-architect (cf. Table 2). The activities of those roles overlap to a certain extent with the role of a *solution engineer* in CDD. However, the platform operators and IT-architects operate on a wider basis, i.e. define solutions for all software products and services rather than on the capabilities, as defined in CDD.

6 Discussion

CDD defines stakeholders and roles responsible for developing, maintaining and adapting capabilities. In order to investigate their operationalization in an SME, we compared CDD roles with the stakeholders at SIV group, an enterprise from utility industry. We draw different observations and conclusions from this comparison:

- The vast majority of the roles and stakeholders defined in CDD are visible in the use case. The roles are involved in the components of the CDD methodology, such as capability modelling, context modelling, adjustment implementation or business service configuration as anticipated.
- The "feedback provider" role in the SIV use case is distributed on several roles or stakeholders. It seems that collecting, evaluating and implementing feedback should rather be considered as a process involving several roles than as a task of a single role. The established method components of CDD methodology actually already include feedback processes. Thus, the role "feedback provider" should be removed from the CDD role definition.
- The naming of some business related roles at SIV/US is different from what was defined in CDD. This was expected as many industries experience different naming of roles across organizations. Thus, this does not imply that name changes in CDD are required.
- CDD includes a more fine-granular differentiation between roles and their tasks than SIV or US. Some SIV roles basically aggregate the tasks and responsibilities of more than one CDD role (e.g. solution engineer). This observation could be attributed to the rather small number of persons involved in the use case as compared to a large organisation with a rather big or a special CDD organisation unit. In a CDD unit, all defined roles probably would be needed.
- Two roles from SIV are not part of the role and stakeholder list from CDD: platform operator and IT-architect. The role description of a solution engineer in CDD should be extended with additional tasks performed by those two stakeholder roles.

As an overall conclusion, the CDD role and stakeholder model confirmed to be complete and suitable.

7 Summary and Future Work

The introduction of new methods or approaches into an organization often does not only affect the organizational processes but also the organizational structures that are usually reflected in roles, positions and organizational units. This paper investigated the effects of the CDD introduction (if any) on organizational roles and addressed the research question how does the operationalization of roles differ between large organizations and SME? For this, we analysed whether the role and stakeholder definitions described as part of CDD are applicable and adequate in practical use or if changes are required. For the future, the following activities should be considered

- SIV group needs to investigate whether the role of a method engineer should be established within the organisation. Establishing this role is advisable because there might be the need to make situational adaptations of the CDD methodology, e.g. if a new capability development and design activity is started. Furthermore, the method engineer could have the responsibility to spread method knowledge to business analyst in the organization and maintain the method knowledge. From a competence perspective, installation of this role would not require extensive training or other knowledge transfer activities from the CaaS partners to SIV group since the CaaS team at SIV group already has most of the required knowledge.
- As soon as more experience with CDD use in SMEs exists, it should be discussed whether an SME version of the CDD role and stakeholder description can be developed, which would basically have to include fewer roles by aggregating some of the current ones. The experiences from SIV/US could be a blueprint for this.
- Some of the CDD-related activities with many roles and stakeholders involved could benefit from more information about the kind of involvement in the activity. Currently, the methodology explicitly defines who does what, but do not include roles who should be informed about results of activities or supporting roles which might be relevant. More concrete, this kind of information could be proved by adding RACI-like charts to the method components. One example of a RACI chart has been included in CDD methodology's Context Modelling component 18.

Acknowledgments. This work has been performed as part of the EU-FP7 funded project no: 611351 CaaS – Capability as a Service in Digital Enterprises.

References

1. Yin, R. K.: Case Study Research: Design and Methods, Third Edition, Applied Social Research Methods Series, Vol 5; Sage Publications, Inc, 2002; 3rd edition.
2. Jiang Y, Zhao J An empirical research of the forming process of Firm inter-organizational e-business capability: Based on the supply chain processes. In: 2010 2nd International Conference on Information Science and Engineering (ICISE), pp 2603–2606
3. Antunes G, Barateiro J, Becker C et al. Modeling Contextual Concerns in Enterprise Architecture. In: 2011 15th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW), pp 3–10

4. Eriksson T (2013) Processes, antecedents and outcomes of dynamic capabilities. Scandinavian Journal of Management(0): -. doi: 10.1016/j.scaman.2013.05.001
5. Boonpattarakan A (2012) Model of Thai Small and Medium Sized Enterprises' Organizational Capabilities: Review and Verification. jmr 4(3). doi: 10.5296/jmr.v4i3.1557
6. Stirna J, Grabis J, Henkel M., Zdravkovic J. (2012) Capability Driven Development – An Approach to Support Evolving Organizations. In: Sandkuhl et al. (eds) The Practice of Enterprise Modeling, LNBIP vol 134. Springer Berlin Heidelberg, Berlin, Heidelberg.
7. Brézillon P, Cavalcanti M (1998) Modeling and Using Context. Knowl. Eng. Rev. 13(2): 185–194. doi: 10.1017/S0269888998004044
8. S. Bērziša, G. Bravos, T. Gonzalez Cardona, U. Czubayko, S. España, J. Grabis, M. Henkel, L. Jokste, J. Kampars, H. Koc, J. Kuhr, C. Llorca, P. Loucopoulos, R. Juanes Pascual, K. Sandkuhl, H. Simic, J. Stirna, J. Zdravkovic (2014), Deliverable 1.4: Requirements specification for CDD, CaaS – Capability as a Service for Digital Enterprises, FP7 project no 611351, Riga Technical University, Latvia.
9. Sandkuhl, K.; Koc, H. and J. Stirna (2014) Context-aware Business Services: Technological Support for Business and IT-Alignment. Proc. 5th International Workshop on Business and IT Alignment at BIS 2014, May 2014, Larnaca, Cyprus. LNBIP Springer.
10. Bērziša, S.; Bravos, G.; Gonzalez Cardona, T.; Czubayko, U.; España, S.; Grabis, J.; Henkel, M.; Jokste, L.; Kampars, J.; Koç, H.; Kuhr, J.-C.; Llorca, C. Loucopoulos, P.; Juanes Pascual, R.; Pastor, O.; Sandkuhl, K.; Simic, H.; Stirna, J.; Zdravkovic, J. (2015) Capability Driven Development: An Approach to Designing Digital Enterprises. Business and Information Systems Engineering (BISE). February 2015, DOI 10.1007/s12599-014-0362-0.
11. Berziša S, España S, Grabis J et al. (2015) Deliverable 5.2: The Initial Version of Capability Driven Development Methodology: CaaS - Capability as a Service in digital enterprises, Collaborative Project Number 611351
12. Ralyté J., Backlund P., Kühn H., Jeusfeld M. A. (2006) Method Chunks for Interoperability. ER 2006, LNCS 4215, pp. 339 – 353, 2006, Springer-Verlag Berlin Heidelberg.
13. Mirbel I., Ralyté J. (2006) Situational method engineering: combining assembly-based and roadmap-driven approaches, Requirements Eng. 11: 58–78.
14. Brinkkemper S. (1995) Method engineering: engineering of information systems development methods and tools, Information and Software Technology, 1995 37.
15. Avison, D. E. & Fitzgerald, G. (1995) Information Systems Development: Methodologies, Techniques and Tools. Berkshire, England: McGraw Hill.
16. Goldkuhl, G.; Lind, M. and U. Seigerroth (1998) Method integration: the need for a learning Perspective. . IEE Proceedings, Software (Special issue on Information System Methodologies), Vol. 145, Nr 4.
17. Chen J, Tsou H (2012) Performance effects of 5IT6 capability, service process innovation, and the mediating role of customer service. Journal of Engineering and Technology Management 29(1): 71–94. doi: 10.1016/j.jengtecman.2011.09.007
18. Grabis J, Henkel M, Kampars J et al. (2016) Deliverable 5.3: The Final Version of Capability Driven Development Methodology: CaaS - Capability as a Service in digital enterprises, Collaborative Project Number 611351
19. Sandkuhl K, Kuhr J-C, Koç H et al. (2015) Capability Management im Geschäftsprozess-Outsourcing. Controlling 27(12): 693–702. doi: 10.15358/0935-0381-2015-12-693
20. Seigerroth, U. (2015). The Diversity of Enterprise Modeling: A Taxonomy for Enterprise Modeling Actions. *Complex Systems Informatics and Modeling Quarterly*, (04), 12-31.

Towards Explaining the Popularity of the Business Model Canvas: A Dual Coding Approach

Thomas John[1] and Daniel Szopinski[1]

[1] Paderborn University, Business Administration and Economics, Paderborn, Germany
{thomas.john,daniel.szopinski}@wiwi.uni-paderborn.de

Abstract. The Business Model Canvas (or Canvas) has achieved tremendous popularity in research and practice. However, despite its popularity, we know virtually nothing about what makes the Canvas more effective than competing approaches. Therefore, we develop a design theory that explores how the Canvas' visual template affects the behavioral intention to use it. Drawing on dual coding theory and the technology acceptance model, we predict that the visual template of the Canvas facilitates learning the components that the Canvas defines to describe a business model. Facilitated learning, in turn, increases perceived ease of use, and thereby the intention to use the Canvas. An online experiment yields preliminary evidence in favor of our prediction.

Keywords: Business model, modeling language, business model canvas.

1 Introduction

A business model describes a firm's mechanisms for value creation, value delivery, and value capture, and there is widespread agreement on the importance of business models for firm success. Consequently, the interest in business models in recent years has increased tremendously in research as well as practice [1].

Despite the great interest in business models, one major criticism has repeatedly been raised: That the applicability of the business model concept is limited because of the concept's ill-defined and fuzzy nature (e.g., [1]). As an answer to this criticism, more formalized approaches have been proposed, which visualize the core logic and elements of a business model (e.g., the *Business Model Canvas* [2] or *e3-value* [3]). These *business model modeling languages* (BMML; for a review, see [4]) are claimed to facilitate tasks such as understanding, communicating (e.g., [2]), and innovating a business model (e.g., [5]), and they are seen as a promising future field for information systems (IS) research [6].

Despite the relevance of BMMLs, there is a striking imbalance between the potential these languages seem to carry and our limited state of knowledge concerning how such languages should be designed. As an indication of their potential, at least one of the existing BMMLs, the *Business Model Canvas* (or, simply, *Canvas*, [2]) has had tremendous impact on research and practice [5, 7]. However, despite the prevalent use of the Canvas, at a theoretical level we know virtually nothing about

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

what makes the Canvas potentially more effective than competing approaches. That is, we have little to no *justificatory knowledge* [8] that could illuminate (1) how (and whether) the design of the Canvas makes it more effective than competing approaches, (2) that could aid in designing other tools for business model development, or (3) that could constitute the foundation for improving the Canvas or other tools or languages even further. Therefore, in this research-in-progress, we seek to explore theoretical factors for the popularity of the Canvas – because a better understanding of what makes the most popular BMML successful holds the promise to reveal valuable insights for BMMLs in general.

We scope our research in two ways: First, we focus on the early phase of using the Canvas, that is, when users *"see"* the Canvas for the first time and form initial beliefs concerning their intention to use it. This early phase is crucial because the beliefs that users form in that phase act as anchors for later beliefs and resulting usage intentions [9]. Second, we focus on the visual notation of the Canvas (i.e., its visual template). This focus rests on the assumption that the visual template is crucial for the Canvas' usefulness – a notion that is consistent with the results of a survey among 1,500 Canvas users. We thus investigate the following research question: *In the early phase of using the Canvas, what characteristics (if any) inherent in its visual template contribute to a continued intention to use the Canvas?*

To answer this question, we engage in what Kuechler and Vaishnavi refer to as *"reflective, inductive, after fact theory development"* [8], that is, we explore the theoretical underpinnings of an artifact that already exists – and that to some extent has already proven useful. We present the resulting *design-relevant explanatory/predictive theory* [8], which describes what characteristics of the Canvas' visual template increase user acceptance, and through what theoretical mechanisms these characteristics become effective. We thereby contribute to a better understanding of the factors that render the Canvas useful (and popular) and provide design-relevant knowledge that can facilitate designing visual notations for BMMLs.

2 Related Literature

Business Model Modeling Languages. Numerous BMMLs have been developed, which, however, greatly differ and to some extent contradict each other with regards to how they understand and represent a business model (for a review, see [4]). As noted, the Canvas is by far the most widely used of these languages and therefore a better understanding of the factors that make the Canvas potentially useful would contribute to advancing the field of BMMLs in general.

Similar to the major share of available definitions, the Canvas operationalizes business models by defining so-called *components*. While the Canvas prescribes nine components to describe a business model, at least 34 different component-based definitions have been proposed, which each comprise between three and 20 components [10]. What sets these approaches apart from the Canvas is that they do not suggest a specific visual notation for representing business model components, but rather imply using the components in a checklist-like fashion (see Figure 1).

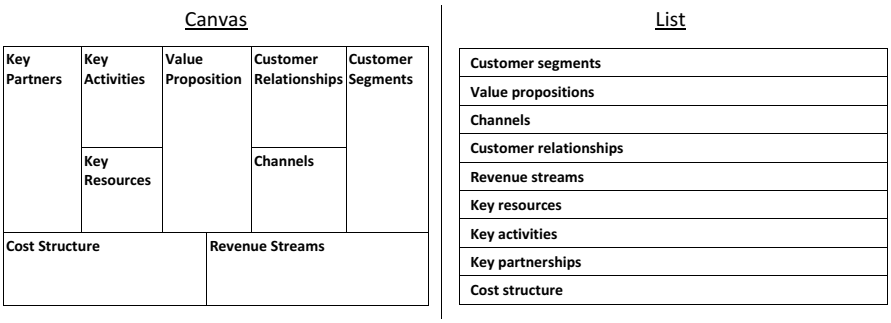


Figure 1. Business Model Canvas (left) and an alternative, list-like representation (right)

So far, there is hardly any research that tries to uncover the reasons for the Canvas' popularity, with the exception of one study that sought to evaluate the Canvas' utility for idea generation: The authors of that study hypothesized that employing the Canvas would increase users' creativity compared to the *PowerPoint* control condition [11]. However, they found that "*the results are significant, but in the opposite direction of our predictions. Subjects who use the interactive template [Canvas] perceive themselves as significantly less creative"* [11]. Consequently, it is largely unclear what characteristics of the Canvas (if any) contribute to its usefulness and popularity.

Dual Coding Theory. Dual coding theory (DCT, [12]) posits that information that is represented textually as well as visually is better and more easily learned than information that is represented as text only [12]. The reason is that humans have two different systems for learning information: a verbal system that processes verbal information (e.g., words) and a nonverbal system that processes nonverbal information (e.g., images). DCT proposes that connections between information items in the verbal and nonverbal systems allow inferring information from either of the systems. Therefore, the chance to recall specific information is higher when that information has been stored in both systems rather than only one. The validity of DCT has been demonstrated in a great variety of contexts [12]. However, DCT has not yet been applied to modeling languages for business models.

Technology Acceptance Model. Substantial research has investigated what factors determine user acceptance. In particular, the technology acceptance model (TAM, [13]) has received wide recognition. TAM posits that the *behavioral intention to use* a system determines actual system usage. The behavioral intention to use a system, in turn, is determined by *perceived usefulness (PU)* and *perceived ease of use (PEOU)*, see Figure 2. TAM has been validated in a wide variety of contexts (for a review, see [14]), but has not yet been applied for investigating user acceptance for visual creativity tools, let alone tools in the business model domain.

3 Research Model and Hypotheses

For exploring how the visual template of the Canvas affects users' intention to use the Canvas, we combine the insights from dual coding theory and TAM (see Figure 2).

We structure our research model through an extension of TAM [9], which states that technology acceptance is determined in two stages: first, through *anchors*, that is, beliefs concerning PEOU that a user forms *when first being exposed* to a specific technology (loosely following the rationale of *"you never get a second chance to make a first impression"*), and second, through *adjustments*, that is, beliefs that a user forms *while actually using* a technology. We theorize that the beliefs concerning PEOU that users form upon initial exposure to the Canvas (*"first impression"*) act as anchors for later beliefs (i.e., the beliefs that concern the intention to continuously use the Canvas). As the initial exposure to the Canvas involves *learning* what components the Canvas actually consists of, we explore how different representations of the Canvas' components affect the beliefs that users form while learning the components.

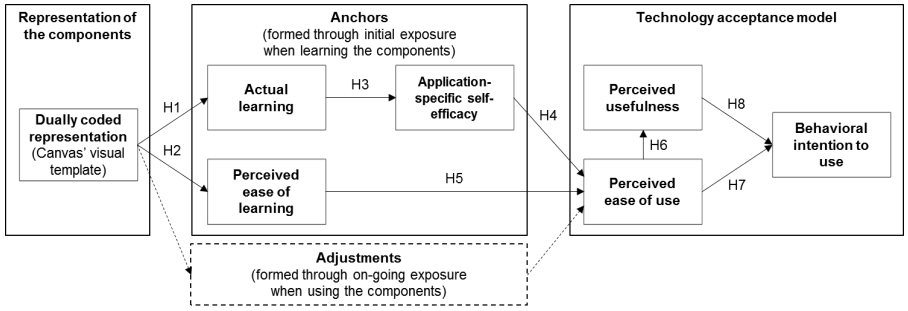


Figure 2. Research Model (the distinction between anchors/adjustments is adopted from [9])

Dually coded representations and learning. There are two ways in which the learning phase of the Canvas can affect the usage phase: through the amount of actual learning and through the perceived ease of learning (PEOL). Actual learning refers to the amount of declarative knowledge that, in objective terms, is built up concerning the components (i.e., knowing the components of the Canvas). PEOL refers to the subjective ease of building up that knowledge. This notion of PEOL is similar to the argument made by Maes and Poels [15], who employ perceived ease of understanding to refer to the ease of inferring information from a conceptual model.

According to DCT, learning is facilitated when information is represented in a way that allows processing the information not only through the verbal but also through the nonverbal system. The Canvas' visual template, in contrast to a list-like representation (see Fig. 1), arranges the components in a two-dimensional space. Hence, the components are not only presented one after the other (as in a list), rather, the two-dimensional layout allows perceiving the components also as an image. Such a dually coded representation allows processing the information on the components not only in the verbal but also the nonverbal system. Therefore, we hypothesize:

H1 The Canvas' visual template has a positive effect on actual learning, compared to a list-like representation.

H2 The Canvas' visual template has a positive effect on perceived ease of learning, compared to a list-like representation.

Learning, self-efficacy, and perceived ease of use. Self-efficacy is the *"judgment of how well one can execute courses of action required to deal with prospective situations"* [16]. In the TAM context, self-efficacy has been investigated at two levels of generality: (general) computer self-efficacy, which captures the general confidence that a user has for using computer applications (e.g., [17]), and application-specific self-efficacy, which refers to a user's confidence in using specific types of applications [18]. In our context this implies that application-specific self-efficacy refers to the judgment of how well one can use the Canvas' components.

An individual's prior accomplishments are one of the major sources of self-efficacy [19]. When learning a new tool, the level of developed declarative knowledge (i.e., actual learning) is an accomplishment that is made prior to using the tool. Accordingly, research has found a positive relationship between declarative knowledge (i.e., actual learning) and self-efficacy [20], and hence:

H3 Actual learning has a positive effect on application-specific self-efficacy.

Self-efficacy affects PEOU, because users anchor their ease of use perceptions relative to the perceived levels of self-efficacy [17]. That is, users with a higher judgment of their proficiency to use a system, that is, with higher self-efficacy, tend to perceive a system to be easier to use. This has been shown to be the case for both types of self-efficacy – generic and application-specific [18], and hence:

H4 Application-specific self-efficacy has a positive effect on perceived ease of use.

PEOL refers to the PEOU that is experienced by a user in the early phase of using a system (i.e., learning the system). Research has shown that the PEOU that one experiences in early usage phases acts as an anchor that affects subsequent perceptions of ease of use. Put differently, with increasing usage experience, PEOU is adjusted towards the actual usability of a system (in the case of an IS). Nonetheless, initial PEOU affects the ease of use that is perceived in later usage phases [9], hence:

H5 Perceived ease of learning has a positive effect on perceived ease of use.

Ease of use, usefulness, and behavioral intention to use. TAM states that the behavioral intention to use is a determinant of actual use, and that perceived usefulness and PEOU jointly determine the behavioral intention to use. Moreover, all else equal, users consider systems more useful when they can use them with lesser effort. Hence, PEOU also affects perceived usefulness. As noted, these relationships have received empirical support through a wide range of studies but, for sake of completeness, we restate them here:

H6 Perceived ease of use has a positive effect on perceived usefulness.

H7 Perceived ease of use has a positive effect on behavioral intention to use.

H8 Perceived usefulness has a positive effect on behavioral intention to use.

4 Preliminary Study

As a first step towards validating our research model, we investigated how the Canvas' visual template affects learning the components (H1 and H2). For that purpose we conducted an online experiment for which we recruited 140 participants from the crowdsourcing platform Crowdflower.com. (For space reasons, in this

research-in-progress we only briefly report on this study. A detailed description of the sample, design, measures etc. is available upon request.) We randomly assigned the participants to one of two conditions: the Canvas' visual template or a list-like representation (see Figure 1). The experiment involved three steps: (1) reading the instructions, (2) learning the nine components of a business model (i.e., trying to memorize their names), and (3) recalling the components as well as answering a questionnaire. We measured actual learning through the number of components recalled correctly and measured PEOL through the scale from [15]. We used regression analysis to test the effect of the Canvas' visual template on actual learning (H1). We found that the representation of components significantly predicted actual learning ($\beta = 1.47$, $p = 0.02$), implying that using the Canvas' visual template increased actual learning by 1.47 words. For testing the effect of the Canvas' visual template on PEOL (H2), we conducted an independent t-test. PEOL for participants given a Canvas ($M = 4.12$, $SE = 0.29$) was higher than for those given a list ($M = 3.53$, $SE = 0.26$), $t(71) = -1.54$, $p = 0.13$. Though not significant, the result suggests a positive effect of the Canvas, and in conclusion, the experiment yields preliminary evidence in support of our predictions.

5 Discussion and Conclusion

The Business Model Canvas is the by far most popular modeling language for business models [4, 7]. However, it is unclear what characteristics (if any) inherent in the Canvas' design contribute to the Canvas' usefulness. This is unfortunate because better understanding the Canvas' success holds the promise to reveal valuable insights for research on modeling languages for business models. Towards resolving this issue, we develop a design-relevant explanatory/predictive theory [8] that captures one specific theoretical mechanism for *why* the visual template of the Canvas has benefits. In so doing, drawing on Kuechler and Vaishnavi [8], we assume that understanding *why* a certain design works is of paramount importance for extending and improving that design. In our next steps, we will test our full research model through laboratory experiments and thereby also extend our research from the anchor to the adjustment part of our research model, that is, explore how the Canvas affects user beliefs also when actually using it (e.g., for communicating or generating business model ideas). With the results of the current and our planned studies, we hope to lay the ground for a more theory-informed design of modeling languages for business models and of software-based tools for business model development.

6 Acknowledgements

This work was partially supported by the German Research Foundation (DFG) within the Collaborative Research Center "On-The-Fly Computing" (CRC 901).

References

1. Massa, L., Tucci, C., Afuah, A.: A critical assessment of business model research. Academy of Management Annals 11, 73-104 (2017)
2. Osterwalder, A., Pigneur, Y.: Business model generation: A handbook for visionaries, game changers, and challengers. Wiley, Hoboken, NJ (2010)
3. Gordijn, J., Akkermans, H.: Value-based requirements engineering: Exploring innovative e-commerce ideas. Requirements Engineering 8, 114–134 (2003)
4. John, T., Kundisch, D., Szopinski, D.: Visual languages for modeling business models: A critical review and future research directions. In: Proceedings of the 38th International Conference on Information Systems, Seoul, Korea (2017)
5. Chesbrough, H.: Business model innovation: Opportunities and barriers. Long Range Planning 43, 354–363 (2010)
6. Veit, D., Clemons, E., Benlian, A., Buxmann, P., Hess, T., Kundisch, D., Leimeister, J.M., Loos, P., Spann, M.: Business models: An information systems research agenda. Business & Information Systems Engineering 6, 45–53 (2014)
7. Strategyzer: The Business Model Canvas: Why and how organizations around the world adopt it (2015)
8. Kuechler, W., Vaishnavi, V.: A framework for theory development in design science research: Multiple perspectives. Journal of the Association for Information Systems 13, 395–423 (2012)
9. Venkatesh, V.: Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. Information Systems Research 11, 342–365 (2000)
10. Krumeich, J., Burkhart, T., Werth, D., Loos, P.: Towards a component-based description of business models: A state-of-the-art analysis (2012)
11. Eppler, M., Hoffmann, F., Bresciani, S.: New business models through collaborative idea generation. International Journal of Innovation Management 15, 1323–1341 (2011)
12. Paivio, A.: Dual coding theory: Retrospect and current status. Canadian Journal of Psychology 45, 255–287 (1991)
13. Davis, F.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly 13, 319–340 (1989)
14. Venkatesh, V., Bala, H.: Technology acceptance model 3 and a research agenda on interventions. Decision Sciences 39, 273–315 (2008)
15. Maes, A., Poels, G.: Evaluating quality of conceptual modelling scripts based on user perceptions. Data & Knowledge Engineering 63, 701–724 (2007)
16. Bandura, A.: Self-efficacy mechanism in human agency. American Psychologist 37, 122–147 (1982)
17. Venkatesh, V., Davis, F.: A model of the antecedents of perceived ease of use: Development and test. Decision Sciences 27, 451–481 (1996)
18. Mun, Y., Hwang, Y.: Predicting the use of web-based information systems: Self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. International journal of human-computer studies 59, 431–449 (2003)
19. Bandura, A.: Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review 84, 191–215 (1977)
20. Martocchio, J., Hertenstein, E.: Learning orientation and goal orientation context: Relationships with cognitive and affective learning outcomes. Human Resource Development Quarterly 14, 413–434 (2003)

A Multilevel Model of Pharmaceuticals

Monika Kaczmarek-Heß[1] and Michael Heß[2]

[1] University of Duisburg-Essen, Essen, Germany
monika.kaczmarek@uni-due.de
[2] Dusseldorf University Hospital, Dusseldorf, Germany
michael.hess@med.uni-duesseldorf.de

Abstract. Pharmaceuticals, i.e., medical drugs, are of pivotal importance in medical care delivery: they are part of hospital processes starting from clinical pathways, through financial accounting, to, e.g., inventory management. Therefore, it seems reasonable to account for medical drugs and integrate them into models of hospitals' processes. As pharmaceuticals, among others, exhibit multiple classification levels and there is a need to treat types as instances, in this paper we apply a relatively new language paradigm and design a multilevel model of medical drugs. We evaluate the proposed model threefold: against requirements, by prototypical application and with the help of domain experts.

Keywords: multilevel modeling, pharmaceutical, FMML^x

1 Introduction

Health-care organizations in general, and hospitals in particular, perceive investing in information technology (IT) as an opportunity to improve the quality of care delivery and reduce costs [1-3]. A pre-requisite for efficient and effective IT application is having a deep understanding of hospital and its processes [4]. Therefore, various researchers proposed the application of domain-specific modeling languages (DSMLs) to support sense-making of a hospital [5-7], with the aim to provide foundations for implementation of hospital information systems (HISs) [4]. However, up till now the focus has been mainly assigned to modeling the flow of clinical pathways, i.e., hospitals' medical processes [5] and not on the involved resources. As pharmaceuticals are of pivotal importance in medical care delivery, it seems however reasonable to account for and integrate them into models of hospitals' processes.

Modeling of pharmaceuticals is nonetheless quite challenging [8]. Firstly, a pharmaceutical product itself is quite complex: it has a rich set of features [9-11], comes in multiple hierarchies (Fig. 1) [9,10], and its characteristics may differ between countries (e.g., reimbursement schema) [9]. Secondly, various processes consider it at different classification levels, e.g., inventory management on the level of packs with serial numbers, drug dispensing on the level of branded product, and drug prescription on the level of type of product, its dosage and pack-size [9].

Although various attempts have been undertaken to model pharmaceuticals and capture their characteristics, e.g., as ontologies [11] or via schemes [12], none of the

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

existing initiatives, to the best of our knowledge, models pharmaceutical products in their entirety and accounts for their variability in a way that would satisfy information needs of all hospital stakeholders. Therefore, in this paper we focus on modeling of pharmaceuticals in the realm of hospital modeling [5] and tackle the question how a pharmaceutical product should be modeled in order to provide relevant information depending on the underlying modeling purpose resp. modelled process.

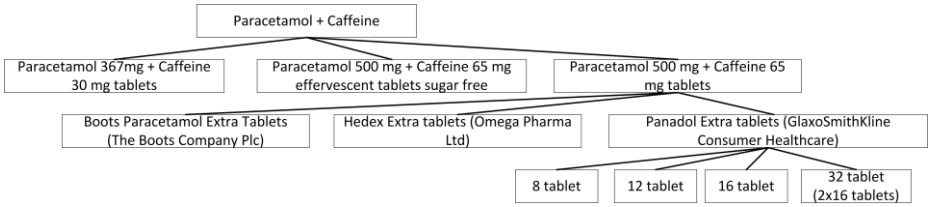


Figure 1. Exemplary hierarchy of pharmaceuticals, NHS database [12]

We follow a design-oriented research path and model pharmaceuticals in collaboration with domain experts. To reach our goal, first, we investigate the concept of pharmaceutical and relevant hospital processes. Then, we identify the main goals that the modeling language should meet. Considering the identified requirements, among others, a need to support numerous classification levels, treat types as instances and equip modeling elements with behavior, we apply a multilevel modeling approach [13]. We evaluate the proposed model threefold: against the requirements, by prototypical implementation, and with the help of domain experts.

The paper is structured as follows. First, the main concepts connected with pharmaceuticals are explained and the main processes using information on pharmaceuticals are mentioned. Then, the goals and resulting requirements towards the approach used to model pharmaceuticals are discussed and a multilevel model of pharmaceuticals is proposed. The paper concludes with final remarks.

2 Pharmaceuticals – Basic Terminology

The European Union (EU) defines pharmaceuticals as "medicinal products", i.e., "(a) any substance or combination of substances presented as having properties for treating or preventing disease in human beings; or (b) any substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis" [14, p. 36]. A pharmaceutical is thus a drug that is used in medicine as a diagnostic, preventive, or therapeutic product [9,10]. Each drug consists of some active moieties/active ingredients (i.e., substances causing a biological effect in living organisms [10]), which can be differentiated into active pharmaceutical ingredients (i.e., ingredients which can serve for prevention, relief, healing or detection of diseases [10, p. 3]) and toxins (i.e., ingredients causing harmful effects) [9].

A medicinal product encompasses at least one active ingredient (e.g., prednisolone) and additional, inactive ingredients (i.e., excipients, e.g., flavors). Each substance has some potency/dosage strength (i.e., "a measure for the dosage respectively concentration, which is required to reach a certain effect: the higher the potency, the lower the necessary dosage" [10, p. 3]). Each drug can be characterized by some therapeutic effect, possible side-effects, and drug-drug-interactions [11].

A medicinal product comes in different dosage forms (e.g., tablets, capsules, syrups). The pharmaceutical's dosage form is chosen based on the route of administration (i.e., the way it is absorbed into the body, e.g., non-invase per oral (through mouth), topical (through skin), or inhalation), respectively defines it [9].

Finally, drugs with the same active ingredients come not only with different potencies, routes of administration and dosage forms, but also with different branded/trade names and in different packs, whose sizes and forms are regulated by corresponding, often country-specific, norms and rules [1,9]. Indeed, there are differences between various countries regarding packs allowed (e.g., blister packs for solid drugs) taking into account, e.g., their character, classification and therapeutic effect or allowed sizes. For instance, for drugs with a short duration of use, packs will be usually designed to provide one course of medicine, for drugs with a longer period of use, packs will be for 28/30-days supply [9,10].

Taking into account the availability of many traded products, the notion of pharmaceutical equivalence has been coined for the products that contain the same active ingredient(s), are of the same dosage form and route of administration and are identical in strength/concentration. However, the products may differ in characteristics such as producer, shape, excipients (e.g., flavors) etc. [9].

The differences between various countries do not relate only to the forms and sizes of packs, but significant differences may be spotted when it comes to, among others, regulation and prescribing practices affecting drug information requirements, drug management and administration [1]. Different countries not only permit the use of different medicinal ingredients, but also have different legal classifications of some drugs, available/allowed ranges of forms/strengths, or different licensed indications.

In addition to that, drug names are quite often different for the same drug in different countries. Indeed, the national naming schemes are quite often country-specific. That is, they refer to ingredients used in the particular country with names intended to be meaningful to its citizens. This lack of standardization hampers the analysis and gathering of information. Therefore, to foster comparability and data exchange on pharmaceuticals, but also to identify drugs that are based on the same active moiety, but have, e.g., country-specific names, the World Health Organization (WHO) introduced in the 1950ies the concept of International Nonproprietary Names (INN) [15]. INNs provide unique names allowing to uniquely identify medical substances. This not only facilitates flow of scientific information and communication among health professionals, but INNs are also used, e.g., by national drug registration authorities and by health assurance bodies defining reimbursement schemes [16].

Being unique and widely recognizable, INNs also serve to classify pharmaceuticals based on the active moiety they contain. In addition, medicinal products are classified taking into account (1) active moieties and the affected organ or system, using the

international Anatomical Therapeutic Chemical Classification System (ATC system) [17], (2) the mode of action, i.e., the way the pharmaceutical works, its therapeutic effect, or the part of the biological system it affects, or (3) the level of control of the drug availability (on prescription, in pharmacies, and over-the-counter [9]).

Motivated by the lack of standardisation in describing drugs, in addition to the standard terminology and classifications mentioned above, numerous (drug) vocabularies have been proposed, which form the foundation of information content in electronic health records, e.g., SNOMED-CT (http://www.snomed.org/) or compatible with it the National Health Service (NHS) Dictionary of Medicine and Devices (dm+d) [12]. NHS dm+d captures the variability of drugs by using four key components [12]: *Virtual Medicinal Product* (virtual therapeutic moiety including the form and strength, e.g., Prednisolone 20mg tablets), *Virtual Medicinal Product Pack* (a generic title for a generic or proprietary product pack), *Actual Medicinal Product* (an actual product linked to the name of a particular supplier), and finally *Actual Medicinal Product Pack* (an actual product linked to the supplier and pack size).

3 Selected Hospital Processes Using Pharmaceutical Data

Pharmaceuticals (or information on those) are used in numerous hospital processes.

Clinical pathways (CPs): a CP is based on a defined clinical guideline and aims to manage institution-specific medical care of "a well-defined group of patients during a well-defined period of time" [19, p. 562] that contributes to improving the quality of care processes, reducing risks, increasing the efficiency of the resource usage, and increasing the patient satisfaction [19,20]. CPs come with different abstraction levels and use the information on drugs as follows. On the level of institution-independent clinical guidelines we deal with a specific class of drugs with some therapeutic effect and/or some active moiety. On the level of some CP, we may either use a specific class of drugs or point to a specific brand of a drug (possibly also with information on the manufacturer, depending on the innovativeness of a product). On the level of patient-specific CP, we point to some specific branded drug with a specific pack size (however, not to a specific pack with some serial number).

Prescription of drugs: the process in which a health-care professional prescribes a drug based on a given indication. Prescribers, depending on the country-specific rules, can opt for the prescription of active substances or brand-name products. A prescribed pharmaceutical has the following properties [4]: brand name or generic name, manufacturer (optional), national/regional drug code(s), active substance(s) denomination(s) (e.g., INN), form, unit dosage, packaging, type of container, number of units. If applicable, additional information, e.g., on the reimbursement level is captured.

Dispense of drugs: the process in which a health-care professional (usually a pharmacist) takes in the prescription and validates it against pharmaceutical knowledge and regulations. If the outcome of the validation is positive, the pharmacist decides on the specific drug, and makes it available to the patient. A record is kept of the dispensed drug (brand, type, form, quantity, etc.). In many cases

the dispenser is entitled to make changes to the prescription (e.g., change the brand of the drug, cf. discussed pharmaceutical equivalence), or reject the prescription. Differences here can exist among different health-care systems.

Administration of drugs: the process in which the medication is actually administered to the patient. The following information is kept, e.g., in the (electronic) health record: specific branded product name, batch number and expiration date, time of administration as well as quantity administered, cf. [4].

Inventory management: the process within which the actual products are being stored (in specific conditions), inventoried, and ordered based on predefined stock levels. Different usage analysis and predictions are used in order to identify the optimal stock size and level, as the lack of availability of a drug may have severe consequences to patients' clinical outcome [4]. Therefore, information on available pack sizes, delivery time, as well as recording dispensed items is required. In hospitals, inventory management applies to both point of care and pharmacy [4].

Decision support: it encompasses such activities as manually or electronically checking for drug interactions, drug allergies/intolerances, correct dosage taking into account patient's age and lab results, duplication of active ingredients in different drugs, identification of equivalent products [4]. In addition, an access is provided to information on therapeutic recommendations, drug contraindications and known side-effects [4,18,21,22].

Epidemiology studies and reporting: Health-care stakeholders are obliged (quite often by law) to conduct various types of reporting, e.g., use of drug categories and the achieved health outcome, adverse drug reaction, usage data (e.g., antibiotics utilization patterns [23]). This reporting is performed on the level of active moiety with its dosage strength and dosage form (e.g., Ibuprofen, 200 mg, capsule), i.e., usually no branded trade name or proprietary names are provided. It may require integrated patient and pharmaceutical data, e.g., number of patients on some active moiety with/without dosage strength and form.

4 Modeling of Pharmaceuticals

Goals and Requirements: The modeling of pharmaceuticals should first and foremost foster availability of information on drugs within relevant (models of) hospital processes, with the aim to: (1) raise the transparency of medical drugs, their characteristics, applications and adverse interactions, (2) raise patient-safety by minimizing the possibility of clinical errors [24], (3) meet regulatory requirements (e.g., reporting), (4) increase the efficiency and effectiveness of relevant processes (e.g., reuse data among different processes: updating medication plan, computerized physician order entry, discharge letters) and (5) contribute to an optimal drug therapy [24]. Based on the conducted literature analysis, analysis of hospital processes and conversations with domain experts, the following requirements have been identified.

R1: *Accounting for different hierarchy levels*. **Rationale**: The processes require information on drugs on different levels of abstraction, e.g., while dispensing is recorded on the level of some specific drug, the inventory goes down to some specific

packs with serial numbers. Thus, the approach should provide information on drugs spanning different levels, e.g., generic types, branded products, specific instances.

R2: *Semantically rich description*. **Rationale**: Discussed processes require rich information on drugs (e.g., starting from a therapeutic effect to reimbursement schema), therefore the approach should allow to create semantically rich models that would provide the desired information.

R3: *Support for both modelling productivity and language reusability*. **Rationale**: On the one hand, the modeling approach should foster reusability by providing rather generic concepts accounting for product-independent aspects common to all drugs in order to be applicable in a wide range of scenarios. However, on the other hand, it should foster the productivity of modeling by providing a set of semantically rich concepts already in the language specification.

R4: *Support for finding the optimal drug therapy*. **Rationale**: The modeling approach should contribute to reducing clinical errors and to optimal drug therapy. Therefore, it should support practitioners by, e.g., making them aware of unsafe measurement of drugs, prescribed overdoses, potential drugs interactions. Therefore, the relevant information (domain-specific constraints) should be incorporated already in the language specification and used while applying the language.

R5: *Support for calculations and reporting*. **Rationale**: To support the discussed processes, a modeling approach should support processing of information defined within the models/language, e.g., identifying overdoses and contra-indications, as well as calculating usage patterns and other statistics for the needs of internal and external epidemiological reporting. It follows that the modeling approach, on the one hand, should account for the required information, e.g., on the adverse reactions (cf. R4). On the other hand, it should provide relevant operations that would perform required computations on different levels of abstraction (cf. R1).

R6: *Integration with external data sources*. **Rationale**: As, e.g., new ingredients are invented, new branded drugs offered, or the stock-level in the hospital pharmacy changes dynamically, the created models should be dynamic in the sense that it should be possible to link language or model elements to external data sources/operational-level systems, e.g., drug databases, and include relevant abstractions within models. This is to ensure that the models are up-to-date and can indeed support the decision making process (cf. R4).

Discussion: Due to the space limitations, the evaluation of existing approaches to represent pharmaceuticals cannot be presented here in details. Instead two main conclusions from the conducted evaluation are mentioned: not only the desired scope of the representation is not supported, but also the existing approaches neither offer the required expressiveness nor the desired mechanisms. We argue that whereas the scope is the matter of goals pursued by an approach, there is a need to investigate the application of alternative language architecture to fulfill other requirements.

In the conventional meta modeling, one describes domain concepts and their relations using a meta model (M_2), which is then instantiated on the type level (M_1). The conventional modeling comes with a couple of rules, e.g., (1) a type/instance dichotomy, implying, among others, that types cannot have a state; (2) a strict separation between different levels (i.e. between language specification, i.e., M_2, and

language application, i.e., M_1); and (3) no possibility to account on M_2 for information applicable on M_0 [13]. However, to address the identified requirements we need a language architecture that deviates from those rules. Firstly, drugs exist in a remarkable variety of types, each of them possessing a variety of type-specific attributes and further hierarchies (cf. Fig. 1) and the refinement relation between different hierarchy levels is partly specialization and partly instantiation (e.g., on the one hand Prednisolone 500 mg orally is an instance of Prednisolone, on the other hand, it is its specialization, which comes with an additional set of attributes). If we follow the traditional modeling paradigm, we need to decide which of those we want to account for. Considering the identified requirements and with the aim to avoid conceptual redundancy and support modeling productivity, we would be interested in making this hierarchy part of a language specification (M_2) and thus, decide for the specialization relation. Thus, we would model a meta type *Pharmaceutical* and specialize it in, e.g., *PrednisoloneProduct* which in turn may be specialized into specific products *PrednisoloneOrally*. However, by deciding to represent the refinement relations as specializations, we would be dealing with a so called level mismatch problem [27] as various hierarchy levels are mapped onto exactly the same model level (i.e., M_2). Although it is certainly *technically* possible to overload the level, by relying on specialization, this would constitute a *workaround inducing an accidental complexity of created models*, cf. [27]. Next, we would want to incorporate information (e.g., on therapeutic effect) already in the language specification, however, we would not be able to do that as meta types cannot have a state (e.g., we cannot assign values to their attributes). In addition, we would like to link concepts defined as part of language specification with concepts being part of language application (e.g., state that *Prednisolone* (M_2) is produced by some specific company (M_1)). This however is also not possible as the only relation allowed between levels is the instantiation relation. Further, as we want to support both productivity and reusability, we also want to be able to define on higher levels (e.g., M_2) what we know would be relevant on lower levels only (e.g., defining that a pharmaceutical has some expiration date known on the instance level only) and in this way increase the concepts' reusability. This requires however support for deferred instantiation (i.e., allowing to define on each level of abstraction what is relevant for our purposes and deferring its instantiation to some not directly proceeding level), which is not supported by traditional approaches. Finally, R4-R6 expect us to link models to external data sources and provide support for analyses and reporting. Fulfilling those requirements would require an integrated programming and modeling environment, i.e., a common representation of model and code. However, as the mainstream object-oriented programming languages feature only one classification level, therefore types and/or meta types are represented as objects by overloading the M_0 level of a programming language. Thus a common representation of code and model is not possible and model-code synchronization is needed [13,25].

Considering the above discussion, although modeling of drugs using traditional two-level modeling is *technically* possible, it would not allow us to deliver a satisfactory solution, i.e., a solution without workarounds, model redundancy and accidental complexity. Therefore, the alternative paradigm is considered.

5 Multilevel Model of Pharmaceuticals

Multilevel modeling covers any approach to modeling that aims to provide systematic support for representing multiple classification levels within a single body of model content [26]. A few multilevel modeling approaches have been proposed, among them, potency-based multilevel modeling/deep instantiation [27], multilevel object (m-object) [28] as well as the Flexible Meta-Modeling and Execution Language (FMML^x) [13]. As FMML^x exhibits distinctive features compared to other approaches [13,29] and as the only one offers a common representation of model and code [13], it becomes our language of choice for modeling pharmaceuticals.

A detailed description of FMML^x can be found in [13]. FMML^x is based on the extension of XCore [30], which is the meta model of an executable meta modeling facility (XMF) [31]. XCore allows for an arbitrary number of classification levels. This is accomplished through a recursive and reflexive language architecture [30]. In XCore a meta class Class inherits from Object. At the same time, objects (instances of Object) are instantiated from Class. As a result, every (meta) class is an object and may have a state [25]. The recursive language architecture allows also for a common representation of code and model. Thus, model elements are classes that allow for the definition of attributes and operations, but at the same time, as they are also objects, we can assign values and execute operations [13]. The definition of attributes, operations and relations has been equipped with intrinsicness [13] (i.e., the deferred instantiation mechanism). It is represented by an integer value that indicates the level on which a given attribute, relation or operation is to be instantiated (cf. the white number in the black box next to the definition of the element in question, Fig. 2). If no intrinsic level is indicated, the element is to be instantiated one level below the current one. FMML^x is supported by the meta modeling and programming environment XModeler [13]. Being a programming environment, XModeler offers mechanisms to, e.g., obtain information from other sources as well as trigger some actions.

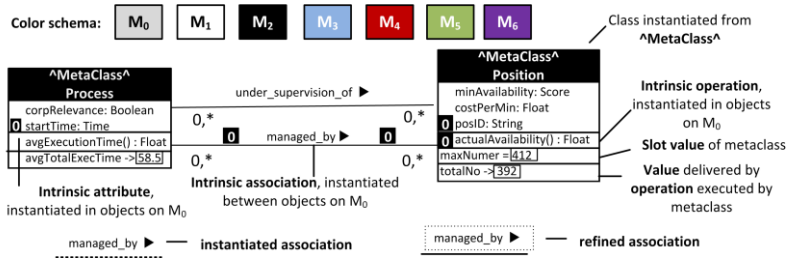


Figure 2. FMMLx – Concrete Syntax based on [13]

Multilevel model: Figure 3 presents an excerpt from the multilevel model of pharmaceutical products. Due to space limitations only selected concepts and selected properties are shown and discussed. On the highest level of abstraction, we define a class Pharmaceutical (M_7). Already at this level, we define everything we know, e.g., that it has a batch number, some expiration date, some producer, some dosage and pack size; although most of those aspects will be known only on the lower levels of

classification (cf. assigned intrinsicness). Here, we take advantage of various auxiliary classes (e.g., RouteOfAdministration, DosageStrength). On M_6, we assign the active pharmaceutical ingredient (M_0) to the product, by instantiating the level-crossing relation has_active_ingredient. Among others, the basic dosage strength, route of administration and dosage form are considered on M_5, M_4 and M_3, respectively.

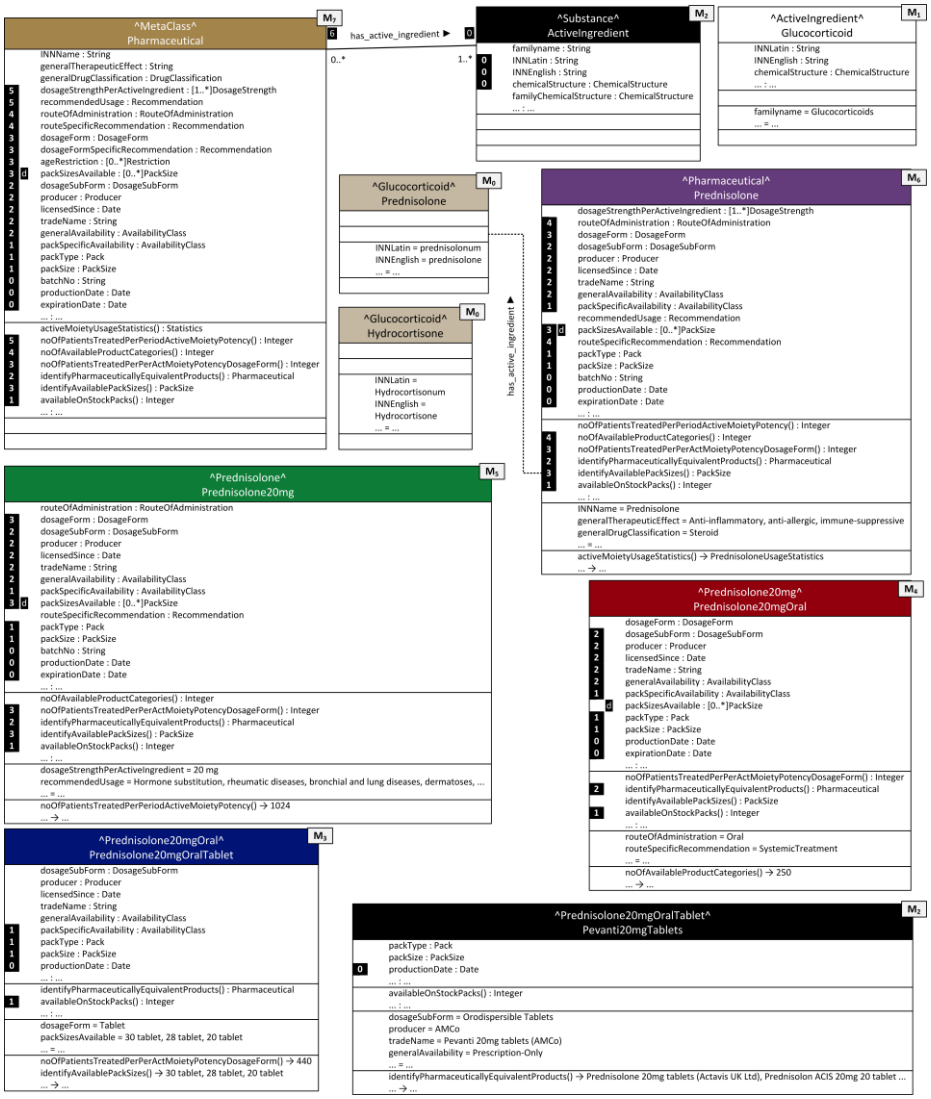


Figure 3. Excerpt from the multilevel model of pharmaceuticals

On each level we benefit from the relaxed type/instance dichotomy and thus, we state relevant information on, e.g., the recommended application specific to the active ingredient or therapeutic effect of some specific dosage strength. The products offered

by different producers are situated at M_2. There we also define additional inactive ingredients as well as subtypes of a dosage form (e.g., chewable tablets). In addition, by using XOCL [30] we define relevant operations, e.g., for the needs of reporting or inventory management (cf., identifyPharmaceuticallyEquivalentProducts()), which may be executed (e.g., noOfAvailableProductCategories=250 on M_4).

Evaluation: We have conducted a threefold evaluation: against the identified requirements, by prototypical application in the XModeler tool (cf. Fig. 4) and with the help of domain experts. Regarding the latter, domain experts working in the pharmacy as well as responsible for HIS conducted the sanity check of the requirements as well as of the proposed multilevel model. When it comes to the requirements, it may be clearly seen that the application of the selected language and the supporting tool opened new possibilities for modeling of drugs. The expressiveness of the approach used allows to (1) account for the specificity of pharmaceuticals without a need to overload layers and apply workarounds, as well as (2) define mechanisms that provide support for desired functions (e.g., reporting).

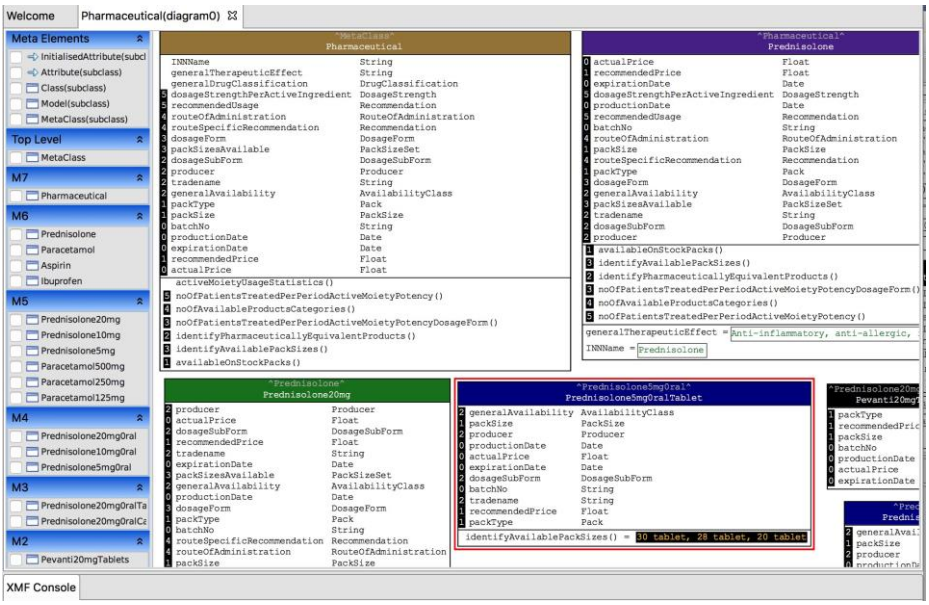


Figure 4. XModeler Screenshot

By allowing defining multiple classification levels, FMML^x makes it possible to define and use concepts that correspond directly with the desired level of details. Thus, we have a possibility to account for the fact that pharmaceutical products span multiple levels of classification, with instances, brands/traded types and generic products being part of the domain of inquiry and related to each other. At each classification level we have the possibility to express relevant information, making the model semantically rich and also facilitating its reuse. At the same time, we have the possibility to freely choose the level we want to deal with within various

processes and thus, information needs of different stakeholders may be satisfied and different views on pharmaceutical products are accounted for. A common representation of model and code allows avoiding the model-code synchronization problem, and treating classes as objects allows defining relevant operations. In addition, thanks to the integrated modeling and programming solution the required epidemiology information can be retrieved. Once the model will be integrated with the electronic CP and electronic health record, one can execute further operations supporting required reporting, e.g., regarding no. of patients treated with Prednisolone (M_6), Prednisolone orally (M_4), Prednisolone oral tablet (M_3), or information on the observed adverse reactions may be automatically tracked. It also becomes possible to link the model elements with external data sources (e.g., drug databases).

6 Conclusions and Outlook on Future Research

In this paper based on the literature study as well as interactions with domain experts, we have proposed a multilevel model of pharmaceuticals. We have designed the model using the integrated modeling and programming approach FMML^x, which allowed designing models that express the objects of consideration directly without the need for overloading. Nevertheless, we consider the proposed multilevel model as the first step only, as a few aspects connected with the pharmaceutical domain are accounted for in a rather superficial manner. This applies to, e.g., accounting mainly for EU-specific rules and regulations, superficial definitions of supporting concepts, e.g., dosage instruction. Regarding the latter, although we have accounted for it as a textual description, e.g., “Take two tablets three times a day”, it seems reasonable to consider a more structured representation that would allow calculating a dose or quantity and thus, improving the patient safety by standardizing the way that dosage instructions are communicated. All of the above aspects are part of our future work.

References

1. Albach, H.H., ed.: Boundaryless hospital: rethink and redefine health care management. Springer (2016)
2. Mettler, T., Fitterer, R., Rohner, P., Winter, R.: Does a hospital’s IT architecture fit with its strategy? Health Systems 3 (2014) 29–42
3. Köbler, F., Fähling, J., Krcmar, H., Leimeister, J.M.: IT-Governance und IT-Entscheidertypen in deutschen Krankenhäusern. WI 52(6) (2010) 353–365
4. Winter, A., Haux, R., Ammenwerth, E., Brigl, B., Hellrung, N., Jahn, F.: Health Information Systems. Architectures and Strategies. 2 edn. Springer, London (2011)
5. Heß, M., Kaczmarek, M., Frank, U., Podleska, L., Taeger, G.: A DSML for Clinical Pathways in the Realm of Multi-Perspective Hospital Modelling. In Becker, J., vom Brocke, J., de Marco, M., eds.: ECIS 2015, Münster (2015) Paper 77.
6. Peleg, M.: Computer-interpretable clinical guidelines: A methodological review. Journal of Biomedical Informatics 46(4) (2013) 744–763
7. Yao, W., Kumar, A.: Conflexflow: Integrating flexible clinical pathways in to clinical decision support systems using context and rules. DSS 55(2) (2013) 499–515

8. Gasmelseid, T.M. In: Improving Pharmaceutical Care through the Use of Intelligent Pharmacoinformatics. IGI Global (2017) 167–188
9. Griffin, J., O'Grady, J.: The textbook of pharmaceutical medicine. 7th ed. Wiley (2013)
10. Mutschler, E., Geisslinger, G., K., K.H., Menzel, S., Ruth, P.: Mutschler Arzneimitelwirkungen. Lehrbuch der Pharmakologie, der klinischen Pharmakologie und Toxikologie. 10 edn. Wissenschaftliche Verlagsgesellschaft, Stuttgart (2013)
11. Herrero-Zazo, M., Segura-Bedmar, I., Martnez, P.: Conceptual models of drug-drug interactions: A summary of recent efforts. KBS 114 (2016) 99 – 107
12. NHS: NHS dictionary of medicines and devices (dm+d). Data model (2015)
13. Frank, U.: Multilevel modeling - toward a new paradigm of conceptual modeling and information systems design. BISE 6(6) (2014) 319–337
14. European Parliament: Directive 2004/27/ec of the European parliament and of the council of 31 March 2004. http://eur-lex.europa.eu/, Access: 2017-07-05.
15. WHO: Guidance on INN. http://www.who.int/ (2017) Access: 2017-07-05.
16. WHO: INN working document 05.167/3. http://www.who.int/ (2006) Access: 2017-07-05.
17. WHO: ATC: structure and principles. http://www.whocc.no/ (2017) Access: 2017-07-05.
18. Agrawal, A.: Medication errors: prevention using information technology systems. BJCP 67(6) (2009) 681–686
19. de Bleser, L., Depreitere, R., Waele, K.d., Vanhaecht, K., Vlayen, J., Sermeus, W.: Defining pathways. Journal of Nursing Management 14(7) (2006) 553–563
20. Schippits, M.G., Schippits, K.M.: Clinical pathways leading healthcare reform: transformational strategies for oncology and beyond. J Med Person 11(2) (2013) 62–68
21. Siska, M.H., Tribble, D.A.: Opportunities and challenges related to technology in supporting optimal pharmacy practice models in hospitals and health systems. American Journal of Health-System Pharmacy 68(12) (2011) 1116–1126
22. Phansalkar, S., Desai, A.A., Bell, D., Yoshida, E., Doole, J., Czochanski, M., Middleton, B., Bates, D.W.: High-priority drug-drug interactions for use in electronic health records. JAMIA 19(5) (2012) 735–743
23. Davey, P., Marwick, C.A., Scott, C.L., Charani, E., McNeil, K., Brown, E., Gould, I.M., Ramsay, C.R., Michie, S.: Interventions to improve antibiotic prescribing practices for hospital inpatients. Cochrane review (2017)
24. Iannone, R., Lambiase, A., Miranda, S., Riemma, S., Sarno, D.: Modelling hospital materials management processes. IJEBM 5 (2013) 15
25. Frank, U.: Designing models and systems to support IT management: A case for multilevel modeling. In Atkinson, C. et al. eds.: MULTI@MoDELS, ceur-ws.org (2016) 3–24
26. Atkinson, C., Kühne, T.: The essence of multilevel metamodeling. In: Proc. of the 4th Int. Conf. on UML, Modeling Languages, Concepts, and Tools, Springer (2001) 19–33
27. Atkinson, C., Kühne, T.: Reducing accidental complexity in domain models. SOSYM 7(3) (2008) 345–359
28. Neumayr, B., Grün, K., Schrefl, M.: Multi-level domain modeling with m-objects and m-relationships. In: Proc. 6th APCCM, Australia, Austr. Computer Society (2009) 107–116
29. de Lara, J., Guerra, E., Cuadrado, J.S.: When and how to use multilevel modelling. ACM TOSEM 24(2) (December 2014) 12:1–12:46
30. Clark, T., Sammut, P., Willans, J.: Applied metamodelling: a foundation for language driven development. Ceteva, Sheffield (2008)
31. Clark, T., Willams, J.: Software language engineering with XMF and XModeler. In Mernik, M., ed.: Formal and practical aspects of domain-specific languages: recent developments. IGI Global (2013) 311–340

OpenLabs als Innovations- und Produktionsstätten für Unternehmen

Teilkonferenzleitung

Edzard Weber

Enabling decentral collaborative innovation processes - a web based real time collaboration platform

Matthias Joiko[1], Florian Kohnen[1], Kevin Lapinski[1], Houda Moudrik[1], Irawan Nurhas[2], Florian Paproth[1] and Jan M. Pawlowski[2]

[1] Hochschule Ruhr West, Institute of Computer Science, Bottrop, Germany
{matthias.joiko,florian.kohnen,kevin.lapinski,houda.moudrik,
florian.paproth}@stud.hs-ruhrwest.de
[2] Hochschule Ruhr West, Institute of Computer Science, Bottrop, Germany
{irawan.nurhas,jan.pawlowski}@hs-ruhrwest.de

Abstract. The main goal of this paper is to define a collaborative innovation process as well as a supporting tool. It is motivated through the increasing competition on global markets and the resultant propagation of decentralized projects with a high demand of innovative collaboration in global contexts. It bases on a project accomplished by the author group. A detailed literature review and the action design research methodology of the project led to an enhanced process model for decentral collaborative innovation processes and a basic realization of a browser based real time tool to enable these processes. The initial evaluation in a practical distributed setting has shown that the created tool is a useful way to support collaborative innovation processes.

Keywords: innovation process model, innovation, collaboration, decentral cooperation, collaboration platform, OERauthors

1 Introduction

Today's companies must cope with rapid technological dynamics and the growing competition on global markets. To master the upcoming challenges steady innovation of processes and products is mandatory. Enabling steady innovations makes it necessary to implement collaborative innovation process models [1, 2]. These process models must be well designed to make the most out of the advantages of collaborative working under consideration of the risks of decentral projects. Well-engineered innovation process models are available [2–4]. What misses in the established models is the consideration of decentral collaborative real time working groups in distributed / global contexts. This paper works out the core processes of established innovation process models to refine them and achieve adaption to these scenarios. For instance, consideration of globalization and localization regarding cultural differences is fundamental.

Decentral collaboration depends on tools which enable communication and interaction between the collaboration group members in real time [5]. Previous research comes to the result, that the market offers a variety of tools which support collaboration, partially

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

also in real time, but not even one provides a simple, holistic approach especially for innovation processes. Also, no fitting tool is available as open source software.
The main purpose of this paper is to outline a collaborative innovation process which is enhanced by web based software. The process model, based on an action design research method, is based on established innovation process models [6, 7] to provide structured stages from idea creation to market release. Finally, the paper provides a platform prototype tool based on latest know-how about collaborative innovation processes in a holistic approach.

2 State of the art

In the following section, we analyze innovation process models as well as existing web based tools which can support collaborative processes.

1.1 Overview of Innovation Process Models

In general, an innovation process is defined as systematic realization of existing and newly created product ideas [8]. The realization covers all steps from idea creation, prototyping up to the final market release. An innovation process aims for timely realization of a product idea to a market stable and releasable product, but is dependent to available capabilities of an organization [9]. This kind of systematic procedure requires special attention on flexibility to be able to react on late or rushed modifications. Several models have been used for the past decades as a reference, such as Schumpeter's or Roger's innovation models [10–12]. Those innovation process models have evolved in recent decades from simple linear and sequential models to increasingly complex models embodying a diverse range of inter and intra stakeholder and process interaction. Our starting point is the first and second-generation models, explaining innovation as either being pulled by market needs, or pushed by technology and science [12]. An obvious disadvantage of their linear process is the distortion of the real innovation process and its formalization and it is impossible to transmit high-quality communication between the components of the innovation process [13]. A further model is a coupling model that recognizes the influence of technological capabilities and market needs within the framework of the innovating firm. However, most of the innovation process models in literature involve a pattern of the following steps or stages: (a) idea generation and identification, (b) concept development, (c) concept evaluation and selection, (d) development, and (e) implementation. Furthermore, all Innovation process model can either be a market pull or technology push, or even a combination [13].

1.2 Collaborative Innovation Process

Collaborative innovation processes are innovation processes, that are geographically distributed and can be realized over frontiers. Innovative new products are developed with shared resources like knowledge or industrial capabilities. Collaborative

innovation requires a more complex coordination and needs a structured way to communicate. A successful innovation process supports real-time collaboration and communication by multidisciplinary teams across different countries and time zones. In order to create an efficient collaborative innovation process, an innovation workflow, with supporting software tools and artefacts, has to be defined.

Pallot et al [14] identified barriers and specifically difficulties to gain trust between collaboration partners but shows that most realized collaborations lead to faster technological process. Collaborative Innovation is based on many success factors, amongst them:

- Strong focus on modelling the value needs of the different stakeholders
- Real Time communication, which stakeholders can directly and openly exchange ideas and information.
- Use of purposive inflows and outflows of knowledge to accelerate internal innovation and expand the markets for external use of innovation
- More collaborative, and more engaging with a wider variety of participants.
- Users are expected to share their knowledge freely within the community because as users they benefit directly from innovation
- Users are a powerful source of innovation in the initial stages of a new product
- Use of internal / external ideas as well as internal / external paths to market

A Collaborative Innovation model is needed incorporating those aspects. The innovation pyramid by Zeidner & Woods [15] meets these criteria because it opens the innovation cycle to a variety of actors and taps into innovation resources across borders, overcomes cultural restrictions.

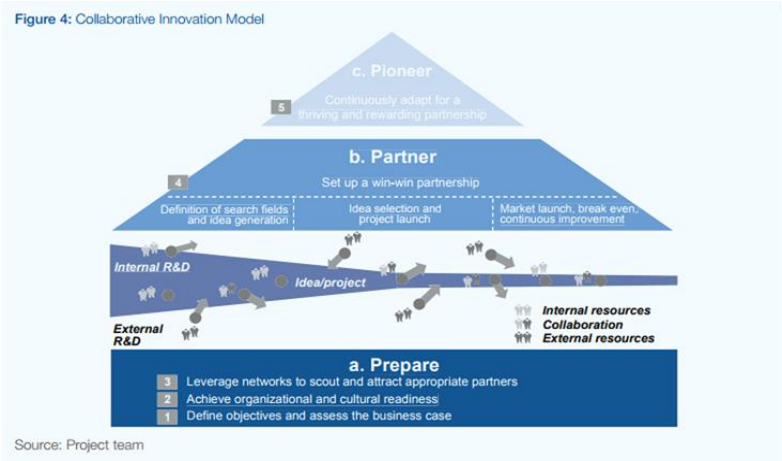


Figure 1 - Collaborative Innovation Pyramid [14]

The preparation layer in this Pyramid lays the critically-important and often overlooked foundation for collaboration, and involves defining objectives and connecting with the right potential partners [16]. Furthermore, the partnering layer focuses on negotiating and tailoring the projects with partners to ensure that the benefits, risks and governance

aspects are adequately defined. Finally, the pioneer layer ensures that partnerships adapt and thrive for the mutual and sustained benefit of all parties as they are executed and as the context changes. Due to the fit of detail, we choose this model as a base for our extended process model, described in detail in section 4.

2 Methodology and used tools

The underlying approach of the project is Action Design Research [17]. The stages implemented in this project are the definition of the leading scientific interrogation, developing and evaluation, reflection and formalization of lessons learned. To achieve an appropriate answer to the central question the project follows practice-inspired research to gain a theory-ingrained artefact. The developing and evaluation step ensures the technological progress and the ongoing sharpening of the final good by considering expert suggestions in weekly meetings. The reflection stage of the action depends on the input parameters of the two stages described above as the team must reflect the developing process and the evaluation feedback in relation to the central research question. Thus, ADR methodology allows a combination of creating, intervening and evaluating during a focused research process [17]. This leads to early and fast alpha versions and continuous improvements without losing sight of the big picture. To enable these processes for the design of the enhanced decentral collaboration process model and the development of the final web based software application the team uses mainly two tools: Git to support versioning and general administration of the developed source code and Signavio to collaboratively design processes [18, 19, 20].

3 Innovation Process Model

Based on the concepts shown above, we refined an innovation process incorporating a focus on networking and collaboration. The innovation environment changes through networking and collaboration from simple linear models to more complex integrated collaboration models. In this new networked paradigm, it's possible to combine linear and coupling processes depending on the requirements. -To build our collaborative innovation process model, three connected level of abstraction were created. The first level of the process model is a value chain diagram. It provides a quick overview of the phases in the innovation management process. The figure below shows these phases of the developed innovation process by using a collapsed process that contains a sub-process und can be linked to the next element of another diagram.

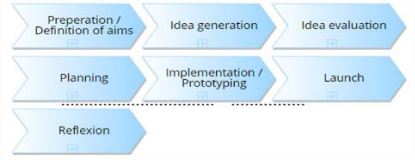


Figure 3: Collaborative Innovation Process Model - Value chain

The first step ‘Preparation’ in our process is to identify problems, needs and expectations for the project. And as a result, new ideas are created during idea generation stage. However, inspiration for a new idea can originate from an improvement of an existing idea, or something from scratch. Once the relevant ideas and references are provided, their accuracies will be verified, evaluated and the potentials will be measured by evaluating benefits and problems in “Idea evaluation” stage. The planning step will start once the ideas and information have been collated and verified. After that, in prototyping stage begins initial prototype. At this stage, the initial model based on the ideas provided will be created and will be shared with the different stakeholders for comment and review. After completion of all iterative versions of product, a second meeting would be scheduled with Client and Partner to review the 3D model and the last product. At least the Marketing and reflection stage are the stage which include production, market launch and penetration in national or international level.
To create the second level of our innovative process model we use Value Chain Diagrams. The following figure shows an example, the idea generation stage.

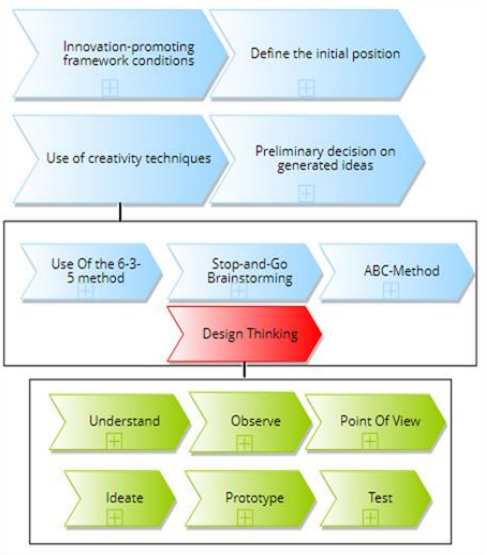


Figure 4: Idea generation stage - Value chain

This figure gives a short insight on the different stages of successful ideation and idea generation techniques. For example, the idea generation techniques identified are briefly introduced as follows:

- Design Thinking [21]
- 6-3-5 Method [22]
- ABC-Method [23]
- Stop-and-Go Brainstorming [24]

In the third level of our integrated innovative process, we modeled detailed, event-driven process chains. The following figure shows an example of the developed process chain diagrams. It describes the collaborative prototyping process within the "Implementation/Prototyping" stage of the top-level value chain.

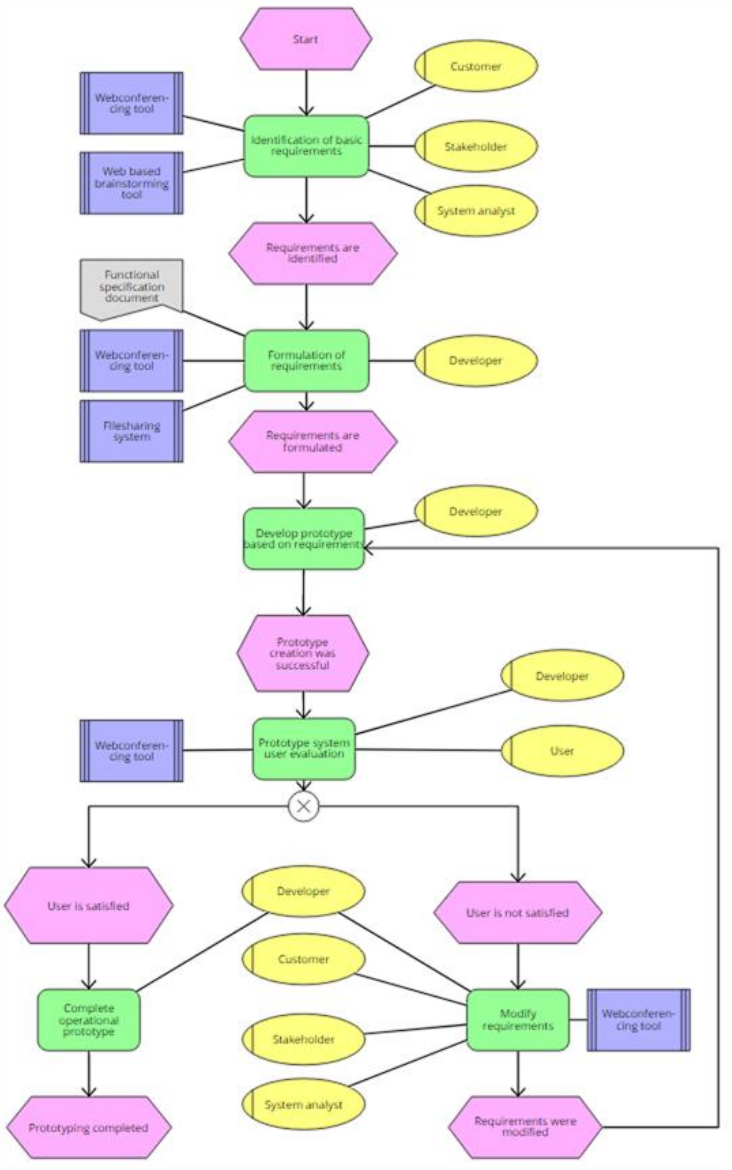


Figure 5: Collaborative Prototyping - EPC Model

In addition, it should be said that there are several ways of approaching collaboration innovation processes. In our case, we had to integrate the different Stakeholders in each step of our process. Ideas are realized in cooperation with customers, users and partners either via virtual networks or real meetings. Also communication and sharing knowledge in different steps are specific for the Collaborative Innovation Process. As a summary, the model can be used as a reference for future innovation processes in different settings.

4 Collaborative Innovation Support Tool

The basic idea of our tool is that it should support a range of core processes defined by the innovation process model described above. Furthermore, it should be a system platform independent browser based solution. The tool is based on a previous research on open innovation [25]. The work provided requirements and recommendations for global authoring platforms under consideration of various barriers as "lack of technical skills, different types of devices and systems as well as the cultural differences in cross-border collaboration' [25]. It also provided a web based platform implementation, which is the foundation of the development described in the following paragraphs of this chapter. The platform is characterized by real time synchronized presentations, where members of the collaboration teams can create, edit and delete slides. Slides can contain text, images and survey elements.
To enhance the platform focusing on collaborative innovation, we decided to implement a new type of presentation slides including "sticky notes". As this raises the complexity of the presentation structure significantly, we had to implement an enhanced, more intuitive site navigation. This navigation includes the usage of linked block titles and predefined jumping points. As the common understanding of "sticky notes" includes, the notes must be enabled for free and direct positioning within the borders of the containing slide including overlapping. Obviously, we implemented highlighting notes with color and linking notes among each other with simple lines, like the advantages of a physical, offline whiteboard also provide. To integrate single sticky notes into the site navigation it is possible to link notes, so you can jump to them wherever a reference link to it appears. Vice versa it is also possible to link presentation block titles within a note. Also, external hyperlinks and further common attachments can be applied to the sticky notes. The sticky note approach is a very good foundation to enable a lot of core process chains described by the collaborative innovation process model. For this purpose, we decided to provide five sticky note background design templates as built-in feature of the platform. Specially to accelerate the idea creation, evaluation and reflection stages, templates for design thinking methods, free sticky walls as well as SWOT analysis are available. Also, we provide general Kanban and Scum templates to enable these project management methods.

The following figures show an example of usage for the tool based on a real collaborative innovation project, initiated by the HRW FabLab [26]. The project aimed at creating a sensor-based dog harness allowing to analyze dogs' emotions including hardware as well as an app for monitoring. The project was realized involving different

stakeholders distributed across the globe. The first figure shows exemplary how the SWOT template of the sticky note platform feature can be used to evaluate the "remote dog harness" idea. It also shows how the sticky note linking mechanism works.

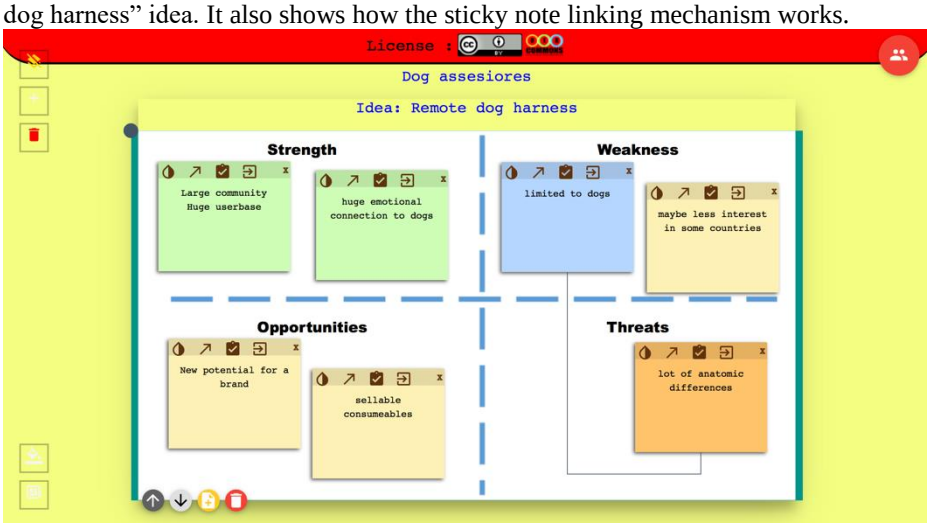


Figure 6 – Platform screenshot – Idea evaluation SWOT

The second figure shows one of the possibilities to manage upcoming tasks while the implementation phase. A Kanban board is used in this example. It illustrates a highlighted sticky note and how transitional task stages can be shown on the board.

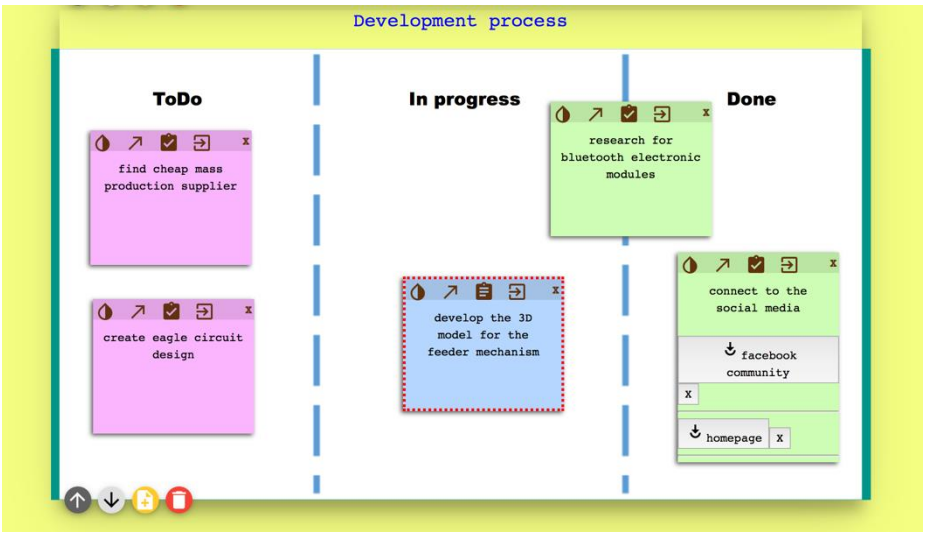


Figure 7 – Platform screenshot – Manage tasks

The part of the software which implements the sticky notes and the templates uses the Node.js ® event driven JavaScript runtime built and Webstrates, which is a research prototype for collaborative editing websites and client synchronisation through HTML DOM manipulations [27, 28]. Sticky note linking is implemented on basis of the jsplumb toolkit [29]. As a matter of course, internationalization and localization (i18n and l10n) software engineering methods are implemented in every developed software part during this research project [30].
The sample case involved different users which were coordinated by the initiating stakeholder. All phases were realized collaboratively utilizing the tool as the main collaboration and feedback support.

5 Proof of concept

This chapter contains two steps to proof the developed concept and tool on top of observing experiences in the initial phase as described in the last chapter. We use a scenario-based evaluation as a first step. The second step was realized by conducting a live tool test and survey with a focus group of researchers and practitioners.

5.1 Scenario

To proof the developed concept, we consider a scenario in which a German company works cooperative with a national park in Finland. Together they try to generate and evaluate new ideas for a touristic attraction in the national park. Due to the distributed workplaces, the employees work collaborative via the online platform OERauthors [30]. In the beginning all members get access to the project, stored on the online platform with a shared unique Project-URL. After connecting to it with a browser, the user can start and his following interactions are sent immediately to all members. Since the whole project is localized, any user can decide which system language he wants to work with. The project manager opens a brainstorm-template in which all ideas can be written down on virtual sticky notes. Any member can create, modify and delete notes. Since the number of sticky notes can vary, there are different types of templates to select. An overview- and a detailed perspective, which can handle more notes without becoming confusing. Helping to categorize the generated ideas in the brainstorming process, it is possible to set different background colors for single notes. After a sufficient number of ideas has been gathered during brainstorming, these need to be evaluated with help of the next template including a SWOT analysis. The ideas to be assessed are written down on notes again and positioned in the corresponding quadrant of the SWOT-template. To discuss various decisions, the members communicate over an integrated chat function. To set the focus of discussion they can highlight sticky notes.
The next step in the innovation process deals with the planning phase, which is also supported by templates. The project manager has the choice between Kanban or Scrum. Just to illustrate the status of all necessary to-do’s he chooses the Scrum-template and creates the topic notes. To make the document scalable, the Project manager links notes to templates which describe the subject in more detail. With help of the implemented

navigation, the members can jump to various templates directly. Media files like videos and pdf-documents are stored on additional cloud server but the links to open them are also saved in notes placed on the template.
This short scenario has been used to show that both templates and tools are useful to support different phases of the innovation process and can be realized in distributed settings.

5.2 **Survey**

To validate the concept and tool in detail, we made a live test of the developed tool with a group of four experts from science and practice. Subsequently we conducted a system usability scale based survey with the expert group [31]. Additionally, the survey contained interview questions with the possibility to add free text comments. Based on the survey, the system received the score on the average system usability scale of 83,75. Additional free text comments showed positive feedback and a high system quality. The gathered results lead to the conclusion that the developed tool enables the acquired collaborative innovation process model in an intuitive way. Not a single free text comment contained a doubt, question or discredit regarding the developed concept. Most of the comments were suggestions for further general user interface features. These perceptions are the focus of the outlook chapter, which follows at the end of this paper.

6 Conclusion & Outlook

The project summarized in this paper was motivated through the increasing competition on global markets and the resultant propagation of decentralized projects with a high demand of decentral innovative collaboration in global contexts. A detailed literature review and the action design research methodology iterations led to progressive reshaping of the developed concept and tool until they achieved the predefined goals.
This paper consolidates core processes of enhanced collaborative innovation process models with state of the art web based software engineering, as it contains a new innovation process model and an enhanced software tool for the integration of the processes into an open authoring platform.
As mentioned in proof of concept, the conducted survey and especially the free text comments brought new perceptions for the future development of the open authoring platform the project was based on and for the tool developed during the project. For instance, a sample of the survey incites to combine the sticky note specific controls with the navigation control elements of the platform in one single control bar. Also, the navigation control design could be more like a classical table of contents in future versions of the platform. Further improvement could be achieved by implementing several sharing functionalities as export to .PDF documents or the possibility to share created projects directly on social media. To promote these features, larger and more scalable sticky note templates could be implemented in future also.

In summary it can be said, that this research project brings a new approach of decentral collaborative innovation and an intuitive web based tool, which both can be very useful in various future projects.

References

1. Kuhlmann, A. M., Sauter, W.: Allgemeine Betriebswirtschaftslehre. https://www.teialehrbuch.de/Kostenlose-Kurse/Allgemeine-Betriebswirtschaftslehre/index.html (Accessed: 24.08.2017)
2. Disselkamp, M.: Innovationsmanagement: Instrumente und Methoden zur Umsetzung im Unternehmen. Springer-Verlag.Wiesbaden (2015)
3. Du Preez, N. D., Louw, L., Essmann, H. (2006). An innovation process model for improving innovation capability. Journal of high technology management research, 2006, 1-24.
4. S. A. Cosmin-Mihai Nacu: A MODEL OF TECHNOLOGICAL INNOVATION PROCESS, "Gheorghe Asachi" Technical University of Iasi, Romani (2015)
5. Forrester Consulting: Building The Future Of Collaboration: A commissioned study conducted by Forrester Consulting on behalf of Adobe Systems, Inc. (2009)
6. Cooper, R. J.: Top oder Flop in der Produktentwicklung: Erfolgsstrategien: Von der Idee zum Launch, Weinheim (2002)
7. Trommsdorff, V.: Fallstudien zum Innovationsmarketing, München (1995)
8. Stieger, U.: Ideengenerierung und -bewertung als Basis für erfolgreiche Produktinnovationen : Umsetzungsmöglichkeiten dargestellt am Beispiel einer KMU (2008)
9. Kahn, K.B.: The PDMA handbook of new product development. Hoboken, NJ: John Wiley & Sons, Inc. (2012)
10. Rogers, E. M.: Diffusion of innovations (1962)
11. Lexis, W. (1913). J. Schumpeter, Theorie der wirtschaftlichen Entwicklung. Jahrbücher für Nationalökonomie und Statistik, 101(1), 84-91.
12. Rothwell, R.: "Towards the fifth-generation innovation process." International marketing review 11.1 (1994): 7-31.
13. Alekseevna, M. A.: Evolution of the Innovation Process Models (2014)
14. Pallot, M., Bergmann, U., Kühnle, H., Pawar, K. S., & Riedel, J. C. : Collaborative Working Environments: Distance Factors Affecting Collaboration., Institute for Ergonomics, Manufacturing systems and Automation (2008)
15. Zeidner, L., Wood, R.: The Collaborative Innovation (CI) Process (2000. https://triz-journal.com/collaborative-innovation-ci-process/) (Accessed: 24.08.2017)
16. World Economic Forum: Collaborative Innovation Transforming Business, Driving Growth: Regional Agenda (2015. http://www3.weforum.org/docs/WEF_Collaborative_Innovation_report_2015.pdf)
17. Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R.: Action design research (2011)
18. Signavio GmbH: Signavio (2012. https://www.signavio.com/) (Accessed: 24.08.2017)
19. Junio C. Hamano, Shawn O. Pearce, and Linus Torvalds: Bring GitHub to work: Securely develop your company's software on GitHub, whether you work for a small startup or a large enterprise.
20. M. La Rosa et al.: Managing Process Model Complexity Via Abstract Syntax Modifications 4. (2011. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6011689)
21. Dorst, K.: The core of 'design thinking' and its application (2011. http://www.sciencedirect.com/science/article/pii/S0142694X11000603) (Accessed: 21.09.2017)

22. Rohrbach, B.: Kreativ nach Regeln – Methode 635, eine neue Technik zum Lösen von Problemen. Absatzwirtschaft 12. Heft 19. S. 73-76 (1969)
23. Atelier für Ideen AG: ABC Methode. http://www.ideenfindung.de/ABC-Methode-Kreativit%C3%A4tstechnik-Brainstorming-Ideenfindung.html (Accessed: 21.09.2017)
24. Bean, E., & Markham, M. H. : A Mini-Guide for Teaching Critical Thinking (2008. http://www.au.af.mil/au/awc/awcgate/eaker/teaching_critical_thinking.pdf (Accessed: 21.09.2017)
25. Nurhas, I., Pawlowski, J. M., Jansen, M.: OERauthors: Requirements for Collaborative OER Authoring Tools in Global Settings, ResearchGate (2016. https://www.researchgate.net/publication/307854627) (Accessed: 24.08.2017)
26. Paproth, F.: Remote Dog Command - final presentation (2017, http://archive.fabacademy.org/archives/2017/fablabbottrophrw/students/66/final_summary.html) (Accessed: 25.11.2017)
27. Klokmose, C. N., Eagan, J. R., Baader, S., Mackay, W., Beaudouin-Lafon, M.: Webstrates: Shareable Dynamic Media (2015. http://www.klokmose.net/clemens/wp-content/uploads/2015/08/webstrates.pdf) (Accessed: 24.08.2017)
28. Node.js Foundation: Node.js (2017. https://nodejs.org/en/ (Accessed: 24.08.2017)
29. jsPlumb Pty Ltd.: jsplumb - Build Connectivity Fast. (2017. https://jsplumbtoolkit.com/ (Accessed: 24.08.2017)
30. Ishida,R., Miller, S. K.: Lokalisierung vs. Internationalisierung (2005. https://www.w3.org/International/questions/qa-i18n (Accessed: 24.08.2017)
31. Rauer, M.: Quantitative Usablility-Analysen mit der System Usability Scale (SUS) (2011. https://blog.seibert-media.net/blog/2011/04/11/usablility-analysen-system-usability-scale-sus/ (Accessed: 24.08.2017)

Exploring Innovation Practices for B2E Initiatives in the Digital Age

Vanessa Guggisberg[1], Andrea Back[1]

[1] University of St. Gallen, Institute of Information Management, St. Gallen, Switzerland
{vanessa.guggisberg,andrea.back}@unisg.ch

Abstract. Digital innovation outcomes are calling traditional project settings and respective processes into question, influenced by software engineering, start-up thinking and design perspective. The challenge incumbent firms face today is how to speed up time to market for digital innovation outcomes due to the rapid speed of technology evolvement. Therefore, we aim at deepening the understanding of how successful digital innovation projects are structured in terms of six dimensions (subject, object, tools, rules, community, division of labor). To do so, we draw on activity theory to analyze nine projects of incumbent firms in the business-to-employee context regarding their way of organizing innovation work in the digital age. Based on our qualitative case analysis, we provide a set of requirements within the six dimensions based on activity theory that are needed to reshape the structure of innovation projects with a digital outcome in incumbent firms.

Keywords: digital innovation management, processes, business-to-employee, agile innovation, activity theory

1 Introduction

Over the past 20 years, incumbent firms have established structured processes and clear innovation paths for physical products and services alike. At the same time these structures are now being challenged by digital product and service innovation as incumbent firms embed digital technologies [1–3] and start to break away from traditional innovation handling [3, 4]. It is not surprising that managers show an extensive interest in tools and means how to handle the portfolio of new products and services with a digital layer, to relate to the new digital environment and how organizational properties support innovation work itself [5].

To tackle these interests, the research stream of digital innovation evolved. Digital innovation as a concept focuses on the change in products, services or business processes as an outcome from the use of digital technology itself [6]. Management of digital innovation is further conceptualized as "practices, processes, and principles that underlie the effective orchestration of digital innovation" [6]. Previous research within digital innovation looked at the nature and structure of new products and services and respective value creation as well as innovation communities, multiple actors and

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

diverse objectives or capabilities, and lastly asked for new approaches of innovation work (e.g. [7–9]).

One key challenge of managing digital innovation addressed by research is understanding the attributes of its process [3]. However, understanding the attributes and respective interdependencies of a digital innovation process is a complex endeavor. In this regard, the rapid pace of digital innovation processes of incumbent firms is defined as particularly challenging when embedding technological components into existing products or adding digital service modules [5]. The combination of physical and digital components is accelerated by various trends such as the digitization of information compiled from outside and inside firms as well as the increased pervasiveness and processing power of (mobile) devices [10].

The challenge that arises when introducing digital components can be traced back to intrinsic differences of practices between traditional and software-focused products [11]. The greater the digital layer of an innovation outcome (e.g. product, service, customer experience), the more software alike thinking is included in its process. [12] describes these competing logics as the "dual regimes of digital innovation". Even though, research has started to classify key challenges and transformational needs in terms of how digital innovation leads to successful outcomes in the past years, practice shows only now increasing interest in identifying requirements to tackle the rapid speed in which digital technology is evolving. Finally, the challenge incumbent firms face today is how to speed up time to market for digital innovation outcomes [6, 13].

Therefore, more research is needed towards identifying requirements in various dimensions to adapt the structure of innovation projects and consequently reduce the time to market of innovation outcomes in the digital age. To do so, we are analyzing nine projects of incumbent firms in the business-to-employee (B2E) context in regard to the way how they are organizing innovation work. Digital B2E initiatives are specifically interesting, since they are resided at the cornerstone of process innovation and new service design and are therefore facing not only external but also internal customers. It is reasoned that "similar to the reengineering wave in the 1990s, a shift can now be observed within the business process modelling discipline from an automation logic to an innovation logic" [14, 15]. Furthermore, this research combines organizational innovation management with digital outcomes [1, 2, 10].

We are particularly interested in understanding how patterns within various dimensions influenced by software engineering, start-up logics and design perspectives reshape the structure of innovation projects with a digital outcome in incumbent firms. We build our work on the activity theory [16] to understand how the six dimensions of an activity system (subject, object, tools, rules, community, division of labor) influence the way incumbent firms structure digital innovation initiatives in the B2E context. Our work employs activity theory to develop a more complete picture on the organizational set-up and corresponding activities during innovation projects. Activity theory fosters the view on a comprehensive activity system in terms of how digital innovation is structured in incumbent firms rather than focusing on individual artefacts. It further includes the environmental context, such as community or situational elements [17].

In the following sections, we will present the theoretical background and develop our propositions. Furthermore, we will describe the approach and context chosen to

empirically test our propositions, and show how we will report on our findings. The paper concludes with a short discussion on the preliminary results, implications and limitations of our research-in-progress.

2 Theoretical Background

2.1 Competing Logics for Digital Innovation

Conceptualizations of digital innovation have evolved over the past ten years. While in the beginning, it was referred to the act of embedding of digital technology into traditional products [13], five years later it was described as "products or services that are either embodied in information and communication technologies or enabled by them" [18]. In line with this, [6] relate to the use of digital technology during the innovation process or as the outcome of innovation. However, literature indicates two competing logics of digital innovation: the product innovation literature and IT innovation literature regime [12]. "Technological progression is not seen as a phenomenon deriving from linear development processes, hierarchical organizations, and vertical industry structures. Instead, IT innovation research underlines that digital technology destroys many barriers favoring incumbent innovation" [12]. As a result, IT innovation fosters a distributed activity that involves whole networks and ecosystems rather than taking place in firm-centric dimensions [3, 19]. In their work, [12] propose a competing logic framework for understanding digital technology in product innovation management. We take this as a starting point to further elaborate on the tensions in the six dimensions of activity theory where the two innovation regimes inevitably meet when innovating digital products and services alike.

2.2 Business-to-Employee Initiatives

In the 1990s, a first generation of IT applications, later mobile applications, were used to digitize internal content as well as to innovate business processes [5]. More recently, besides the adoption of new solutions, the consumerization of IT has played a major role in enabling mobile solutions in the business context [20]. This has led to the second generation of mobile business solutions that focused on incremental improvements in business features. In this regard, technology adoption was a critical key aspect in order to generate business value from the application [21]. For this article, we focus on the latest generation of B2E initiatives, which are considered as "authentically mobile" and therefore at the intersection of business process redesign and new service development [22]. Examples here are smart glasses for distribution purposes or increased data collection combined with algorithms for data quality or product maintenance. Furthermore, digital B2E initiatives are resided at the cornerstone of business process innovation and new service design and are therefore facing not only external but also internal customers. Consequently, digital technologies can create novel business processes or substantially improve existing ones but should be always linked to market offerings [14].

2.3 Activity Theory and its Application to our Research-in-Progress

Activity theory as a meta-theory aims at understanding the object-oriented and tool-mediated interactions between humans [23]. The research paradigm is often used by multidisciplinary research communities in the field of work place practices (e.g [24, 25]) and human-computer interaction (HCI) (e.g. [26, 27]). Furthermore, it has been recently applied in a study on the transformation of tasks influenced by information systems [28]. Historically, there are three generations of activity theory. In particular, Engeström's third generation is widely used in current research endeavors and adopted within this research. As depicted in Figure 1, the activity theory offers six dimensions (subject, object, tools, rules, community, division of labor).

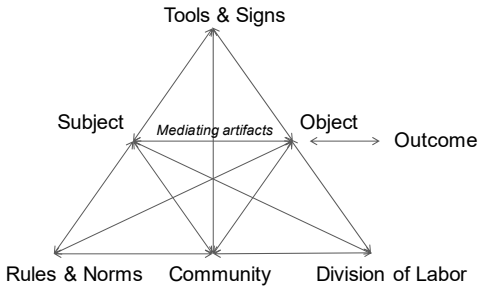


Figure 1: Basic structure of an activity system adapted from [16]

The socio-technical nature of innovation networks is emphasized when shaping the behavior, because it is highly influenced by the cultural context and the technology itself [18]. Applied to this research, activity theory allows us to gain deeper insight in how different dimensions relate and influence each other within an innovation project as a system itself.

3 Methodology

Following our objective, this research endeavor is exploratory in nature. More specifically, because we are interested in understanding how patterns within various dimensions influenced by software engineering, start-up logics and design perspectives reshape the structure of digital innovation projects in incumbent firms in order to speed up time to market. As such, we aim at being "broad-ranging, purposive, systematic, and prearranged undertaking designed to maximize the discovery of generalizations leading to description and understanding of the area of research" [29]. Therefore, we carefully selected nine incumbent organizations in Germany, Austria and Switzerland offering B2E initiatives that met the criteria of [22] for the third generation of mobile business solutions focusing on process redesign, as referred to in Section 2.2. Our data collection comprises three or more interviews per case and end at the point of theoretical saturation. In addition, we consider further sources of evidence, i.e., public and company internal data that is provided by the interviewees. To ensure taking into consideration multiple perspectives from each case company, our interview set-up

included three different user groups within each incumbent firm: 1. Innovation manager, responsible for structure and process, 2. Senior manager responsible for taking decisions regarding resources (financial and personnel), 3. Project owner for an ongoing B2E project. An activity theoretical lens is used to guide both, the data collection and analysis. We are following the guideline to iteratively and continuously collect and analyze data [30]. As such, this research-in-progress represents an intermediate stage of analysis, while data collection is still ongoing (June-October 2017, 22/31 interviews are conducted the remaining ones scheduled). Our structured approach is as follows: We collect the data on audio files, transcribe and upload the transcripts to Atlas.ti. Then, on a first level, the data is coded according to the six dimensions, on a second level, requirements are identified and provided with a specific code. Interviews are coded in a horizontal order based on the user groups introduced earlier.

4 Preliminary Results

Table 1 shows a short description of the dimensions used in the activity theory according to [16], how we apply these in our research and first interview results, e.g. the major effect of location-based influence (such as an innovation lab) or the organizational structure of the project team and team members' roles.

Table 1. Application of the dimensions of activity theory to our research

Dimension	*Description and Application of the Dimension*
Subject (Sub)	The subject is referring to a group of people (the project team), tool-mediated towards reaching the objective. Subjects are led by the project owners within the nine use cases.
Object (Obj)	As object, we refer to the objective of the activity. In our research, this is the digital technology for the outcome (B2E processes and new service offering).
Tools (Too)	In this research, tools are artifacts, methods and instruments such as a specific location (e.g innovation labs), methods from software development (e.g. Scrum, Agile Manifesto), design orientation (e.g. Design Thinking), Lean Start-up thinking (e.g. iterations with learn-build-measure cycles).
Rules and Norms (Rul)	External rules or internal governance are shaping how projects are set-up. Regarding digital innovation, this can refer to the decision-making and approval process on resources, degree of freedom for project teams and structure and content related mechanisms.
Community (Com)	The social context, in which the project is embedded and refers to internal/external partners, its structure and collaboration mechanisms.
Division of Labor (DoL)	This refers to the team structure, roles and responsibilities in digital innovation projects (team roles such as project owner, developer, user experience designer, business analyst, scrum master etc), initial team setting, its development over time and dependencies on related departments within the organization.

5 Conclusion

The objective of this research-in-progress is to understand how time to market of B2E initiatives in digital innovation can be reduced. Digital B2E initiatives are resided at the cornerstone of business process innovation and new service design and therefore create novel business processes or substantially improve existing ones when introducing new service offerings. As a result, we provide a set of requirements within six dimensions based on activity theory that are needed to reshape the structure of innovation projects with a digital outcome in incumbent firms. So far, little research has examined this complex setting of digital innovation projects with an increasing digital layer as outcome that is driven more and more by software development, design and lean start-up logics. We build upon the competing logic framework for understanding digital technology in product innovation management proposed by [12] and analyze the requirements that are needed to adapt the structure of innovation projects and consequently reduce the time to market in the digital age. With our research, we aim at investigating these patterns through activity theory within an exploratory multiple case study setting, which should provide insights regarding the state of the art of digital innovation within the B2E realm of incumbent firms. The long-term aim of this research endeavor is to build a next generation innovation reference model based on the requirements conducted within this setting.

References

1. Tilson, D., Lyytinen, K., Sørensen, C.: Digital infrastructures: The Missing 15 Research Agenda. Inf. Syst. Res. 21, 748–759 (2010).
2. Tiwana, A., Konsynski, B., Bush, A.A.: Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. Inf. Syst. Res. 21, 675–687 (2010).
3. Yoo, Y., Henfridsson, O., Lyytinen, K.: The new organizing logic of digital innovation: An agenda for information systems research. Inf. Syst. Res. 21, 724–735 (2010).
4. Svahn, F., Mathiassen, L., Lindgren, R.: Embracing Digital Innovation in Incumbent Firms: How Volvo Cars Managed Competing Concerns. MIS Quarterly. Spec. Issue IT Innov. 41, 239–254 (2017).
5. Nylén, D., Holmström, J.: Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation. Bus. Horiz. 58, 57–67 (2015).
6. Nambisan, S., Lyytinen, K., Majchrzak, A., Song, M.: Digital Innovation Management: Reinventing Innovation Management Research in a Digital World. MIS Quarterly. Spec. Issue IT Innov. 41, 223–238 (2017).
7. Boudreau, K., Lakhani, K.: Using the Crowd as an Innovation Partner. Harv. Bus. Rev. April, 61–69 (2013).
8. Hui, G.: How the internet of things changes business models. Harv. Bus. Rev. July, 1–6 (2014).
9. Iansiti, M., Lakhani, K.: Sensors, and Data Are Revolutionizing Business. Harv. Bus. Rev. November, (2014).
10. Yoo, Y., Boland, R.J., Lyytinen, K., Majchrzak, A.: Organizing for Innovation in the Digitized World. Organ. Sci. 23, 1398–1408 (2012).

11. Brooks, F.P.J.: No Silver Bullet-Essence and Accidents of Software Engineering. Proc. IFIP Tenth World Comput. Conf. 1069–1076 (1986).
12. Svahn, F., Henfridsson, O.: The Dual Regimes of Digital Innovation Management. Proc. Annu. Hawaii Int. Conf. Syst. Sci. 3347–3356 (2012).
13. Henfridsson, O., Lindgren, R.: User Involvement in Developing Mobile and Temporarily Interconnected Systems. Inf. Syst. J. 20, 119–135 (2010).
14. Looy, A. Van: A Quantitative Study of the Link Between Business Process Management and Digital Innovation. In: International Conference on Business Process Management. pp. 177–192 (2017).
15. Schmiedel, T., Brocke, J.: Business Process Management: Potentials and Challenges of Driving Innovation. In: BPM - Driving Innovation in a Digital World. pp. 3–15. Springer International Publishing, Cham (2015).
16. Engeström, Y.: Expansive Learning at Work: Toward an Activity Theoretical Reconceptualization. J. Educ. Work. 14, 133–156 (2001).
17. Alter, S.: 18 Reasons Why IT-Reliant Work Systems Should Replace "the IT Artifact" As the Core Subject Matter of the IS Field. Commun. Assoc. Inf. Syst. 12, 366–395 (2003).
18. Lyytinen, K., Yoo, Y., Boland, R.J.: Digital Product Innovation Within Four Classes of Innovation Networks. Inf. Syst. J. 47–75 (2015).
19. Tuomi, I.: Networks of Innovation: Change and Meaning in the Age of the Internet. Oxford Univ. Press. 0–390 (2002).
20. Berghaus, S., Back, A.: Adoption of Mobile Business Solutions and its Impact on Organizational Stakeholders. BLED 2014 Proc. 415–427 (2014).
21. Stieglitz, S., Brockmann, T.: Increasing Organizational Performance by Transforming into a Mobile Enterprise. MIS Q. 11, 189–204 (2012).
22. Guggisberg, V.: Vom Mobile Worker zum Augmented Worker. Handb. E-Learning. 8, 93–106 (2017).
23. Kuutti, K.: Activity Theory, Transformation of Work, and Information Systems Design. In: Engeström, Y., Miettinen, R., and Punamäki, R. (eds.) Perspectives on activity theory. pp. 360–376. Cambridge University Press, New York (1999).
24. Engeström, Y.: Expansive Learning at Work: Toward an activity theoretical reconceptualization. J. Educ. Work. 14, 133–156 (2017).
25. Engeström, Y., Kerosuo, H.: From Workplace Learning to Inter-Organizational Learning and back: The Contribution of Activity Theory. J. Work. Learn. 19, 336–342 (2007).
26. Kaptelinin, V., Nardi, B., Macaulay, C.: Methods & Tools: The Activity Checklist: a Tool for Representing the "Space" of Context. Interactions. 6, 27–39 (1999).
27. Nardi, B.A.: Context and Consciousness: Activity Theory and Human-Computer Interaction. MIT Press, Cambridge (1996).
28. Allen, D.K., Brown, A., Karanasios, S., Norman, A.: How Should Technology-Mediated Organizational Change be Explained? A Comparison of the Contributions of Critical Realism and Activity Theory. MIS Q. 37, 835–854 (2013).
29. Stebbins, R.A.: Exploratory Research in the Social Sciences. Sage University Papers Series on Qualitative Research Methods, London (2001).
30. Klein, H.H.K., Myers, M.: A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Q. 23, 67–93 (1999).

Smart Services: Kundenzentrierte Kombination von Dienstleistungen für Mobilität, Finanzen und Gesundheit

Teilkonferenzleitung

Rainer Alt
Jan Fabian Ehmke
Heidi Krömker
Tobias Wienken

Kundenzentrierte Mehrwertdienste zur Differenzierung von Automobilherstellern im Markt der Mobilitätsdienstleistungen

Alexander Sandau[1], Jorge Marx Gómez[1]

[1] Wirtschaftsinformatik, Department für Informatik, Carl von Ossietzky Universität Oldenburg, Oldenburg, Deutschland
{alexander.sandau,jorge.marx.gomez}@uni-oldenburg.de

Abstract. Der Automobilsektor ist beeinflusst durch eine Vielzahl an Herausforderungen, wie Kosten- und Margendruck, abnehmender Pkw-Besitz, Digitalisierung und erheblichen Investitionen in neue Technologien für Elektrofahrzeuge und automatisiertes Fahren und sich verändernde Wertschöpfungsketten. Der Wandel von klassischen Herstellern zu Anbietern von Mobilitätsdienstleistungen ist ein Ansatz, um neue Wertschöpfungsketten aufzubauen und diese Herausforderungen zu bewältigen. Doch durch den Einsatz von Mobilitätsdienstleistungen stellt sich die Frage: "Wie sich die Automobilhersteller in Zukunft differenzieren, wenn das Fahrzeug per se nicht im Vordergrund steht?". Da die Konsumenten von Mobilitätsdiensten auf Basis automatisierter Fahrzeuge weniger Wert auf die Fahrdynamik oder das Design des Exterieurs legen, stellen die Möglichkeiten der Innenraumgestaltung und der damit verbundenen Mehrwertdienste eine zentrale Abgrenzung dar. Die Fahrzeit kann für verschiedene Aktivitäten genutzt werden. Dabei müssen die im Fahrzeug verfügbaren kundenorientierten Mehrwertdienste im Vertrieb der Mobilitätsdienstleistungen berücksichtigt werden. Dafür sind intelligente Flottenmanagementsysteme erforderlich, die die Fähigkeit besitzen, auf Ereignisse von automatisierten Fahrzeugen zu reagieren und Mehrwertdienste für die Konsumenten anzubieten. Dieser Beitrag führt einen agentenbasierten Ansatz zur Vermarktung von Mehrwertdiensten in Flottenmanagementsystemen ein.

Keywords: Flottenmanagement, Nutzerzentrierte Mehrwertdienste, Cyber-Physische-Systeme, Mobilitätsdienste, Hybride Leistungsbündel

1 Einleitung

Die heutige individuelle Mobilität der deutschen Bevölkerung basiert zu 84,5 % auf dem privaten Pkw und liegt somit über dem europäischen Durchschnitt von 81 % [1]. Doch die individuelle Mobilität steht am Beginn einer neuen Evolutionsstufe. Automatisiertes Fahren gilt als einer der entscheidenden Trends in der Automobilindustrie für die nächsten Jahrzehnte. Das selbstfahrende Fahrzeug wird nicht nur die gesamte Branche und die Art der Fortbewegung beeinflussen, sondern unsere Lebenswelt nachhaltig verändern. Insbesondere der Einsatz moderner

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Informations- und Kommunikationstechnologien führt zu neuen Geschäftsmodellen, die die Attraktivität alternativer Lösungen, wie Vehicle-On-Demand Diensten fördern und zu einer abnehmenden Pkw-Besitzquote führen können [2].

Schon heute ist die Vermarktung von Automobilen zu einer zentralen Herausforderung mit vielen neuen Wettbewerbern und stetig abnehmender Neuwagenverkäufe geworden. Neue Absatz- und Vermarktungsstrategien erfordern ein Umdenken der Automobilhersteller [3]. Dies manifestiert sich bereits durch das verstärkte Interesse der Hersteller im Bereich von Sharing-Diensten und Finanzdienstleistungen (z. B. Carsharing und Leasingverträge). Es ist mittelfristig davon auszugehen, dass Mobilitätsdienstleistungen ca. 20 % des Profitpotenzials im Mobilitätsmarkt bilden [4]. Dies führt jedoch zu einem erhöhten Margendruck in der Automobilherstellung, der den Wertschöpfungsanteil der Autoproduktion bzw. dem Verkauf von aktuell 85 % auf ca. 50 % reduzieren wird. Letztlich müssen die Hersteller einen Wandel von klassischen Automobilherstellern zu Anbietern von Mobilität vollführen, um neue Wertschöpfungspotentiale zu erschließen (vgl. [5]). Dies stellt die Automobilhersteller vor erhebliche Herausforderungen [6]. Um sich im stärker werdenden internationalen Wettbewerb weiter zu differenzieren und langfristig erfolgreich bleiben zu können, müssen Unternehmen der Automobilindustrie, und dabei vor allem die OEMs, ihr klassisches Geschäftsmodell weiterentwickeln [7]. Dabei stehen die mit dem automatisierten Fahren einhergehenden Möglichkeiten und Herausforderungen im Fokus [8]. Erste Analysen zum allgemeinen Marktpotenzial durch den Verkauf von automatisierten Fahrzeugen sowie zusätzlicher Geschäftsmodelle im Umfeld dieser Technologie wurden bereits in verschiedenen Studien durchgeführt. Insbesondere bei der Vermarktung von Mobilitätsdiensten stellt sich die Frage: "Wie können sich Automobilhersteller in Zukunft differenzieren, wenn das Fahrzeug per se nicht im Vordergrund steht?". Durch die Nutzung von Mobilität als Dienstleistung tritt die Servicequalität in den Vordergrund. Daher ist davon auszugehen, dass die Konsumenten von Mobilitätsdiensten auf Basis automatisierten Fahrens weniger Wert auf die Fahrdynamik oder das Design des Exterieurs legen, sondern die Möglichkeiten der Innenraumarchitektur und der damit verbundenen Mehrwertdienste kann eine zentrale Abgrenzung darstellen. In Zukunft kann innerhalb dieser Mobilitätsdienstleistung die frei werdende Fahrzeit für andere Tätigkeiten genutzt werden, z. B. für Arbeits- oder Freizeitaktivitäten. Dies bietet ein großes Wertschöpfungspotenzial für die Automobilhersteller, in denen sich die Hersteller als Mobilitätsanbieter mit unterschiedlichen Mehrwertdiensten auszeichnen und abgrenzen. Sobald automatisierte Fahrzeuge die Marktreife erreicht haben, planen viele Hersteller, Flotten von Robo-Taxis (vgl. Roboconomy) zu betreiben. Die entstehenden, auf den Kunden zugeschnittene Mobilitätsdienste, werden bestehende Angebote, wie stationsbasiertes Car-Sharing in der heutigen Form verdrängen.

In den letzten 10 bis 20 Jahren hat die Nutzung von Dienstleistungen sowie hybriden Leistungsbündeln stark an Bedeutung gewonnen. Früher waren physische Produkte und Dienstleistungen häufig getrennte Angebote, heutzutage verschwimmen die Grenzen zunehmend [8]. Insbesondere jüngere Nutzer sind mit einem neuen Produktverständnis aufgewachsen und sensibilisiert für weitere Leistungen nach dem Erwerb eines physischen Produkts situationsbedingt bzw. kontinuierlich zu zahlen (z. B. Video-on-

Demand). Die nachträglich erworbenen Leistungen nehmen dabei einen wesentlichen Teil der Wertschöpfung ein und bestimmen maßgeblich die Kundenzufriedenheit [10].

Bereits heute ermöglichen moderne Softwaresysteme, dass Steuergeräte hochtechnische Aufgaben übernehmen und z. B. den Fahrzeugzustand überwachen oder das Einparken übernehmen. Einige Hersteller haben experimentiert, ob derartige Assistenzfunktion im Rahmen von Zusatzangeboten an die Kunden vermarktet werden können. Dies zeigt, dass bereits eine Sensibilisierung der Hersteller für neue Dienstangebote besteht und innovative digitale Mehrwertdienste im Bereich Mobility-as-a-Service immer Stärker in den Fokus rücken [11]. Dabei wird ein zentrales Verkaufsargument die durch das automatisierte Fahren gewonnene Zeit werden und in den Fokus des Wettbewerbs rücken – die „Freizeit" gilt mitunter als „das zukünftige Kapital für attraktive Dienstleistungen" [12].

Eine Studie der Beratungsunternehmen Strategy& und PwC zeigt, dass die Automobilhersteller den Entwicklungsfokus auf automatisierte, vernetzte und elektrisch angetriebene Fahrzeuge gelegt haben [4]. Die Studie geht davon aus, dass bis 2030 das Segment der neuen Mobilitätsdienste einem exponentiellen Wachstum unterliegt und ein Marktvolumen von 2 Mrd. Euro erreichen wird. Außerdem wird prognostiziert, dass der Anteil der automatisiert zurückgelegten Personenkilometer in der EU zu diesem Zeitraum bereits 42 % beträgt. Jedoch wird der straßenbasierte Personentransport im gleichen Zeitraum um 23 % zunehmen und zu mehr Verkehr führen. Gleichzeitig sinken die Mobilitätskosten für einen Haushalt im Durchschnitt um 10 %. Jedoch verfügen nur 16 % der Privathaushalte über ein automatisiertes Fahrzeug. Durch den Einsatz automatisierter Fahrzeugflotten werden insgesamt ein Viertel weniger Fahrzeuge auf den Straßen unterwegs sein, jedoch mit einer deutlich höheren täglichen Laufleistung.

Das nächste Kapitel beschreibt die Einschränkungen aktueller Flottenmanagementsysteme und stellt die Akzeptanz sowie die Zahlungsbereitschaft von Mehrwertdiensten dar. Kapitel 3 stellt ein agentenbasiertes Flottenmanagementsystem zur Vermarktung von Mehrwertdienste in Mobilitätsdienstleistungen vor. Kapitel 4 schließt mit einem kurzen Fazit.

2 Einschränkung aktueller Flottenmanagementsysteme

Die zukünftige Rolle der Automobilhersteller in der „Roboconomy" kann verschiedene Ausprägungen annehmen: die Rolle als Infrastruktur-Betreiber mit einem eigenen Endkundendienst, eine Vermittlerrolle zwischen den Mobilitätsanbietern und den Endkunden oder die Beschränkung auf die heutige Kernkompetenz der Fahrzeugentwicklung und der Integrationsleistung eines Zulieferernetzwerks. Jedoch bieten die Erweiterung um Funktionen bzw. die Verbesserung der Fahrzeuge mit digitalen Technologien, die Reduktion von Herstellungs- oder Wartungskosten und die Steigerung des Customer Lifetime Values erhebliche neue Marktpotenziale. Langfristig ist es von besonderer Relevanz, als erfolgreicher Marktteilnehmer, sich über die einzelnen Kategorien hinwegzusetzen und sich zu einem übergeordneten Hub für Dienste und E-Commerce zu entwickeln [13].

In diesem Zusammenhang sind die Konzepte ConnectedCar [13] und Vehicle Cloud zu nennen, die die Verschmelzung der klassischen Automotive- und der IKT-Branche beschreiben, die weit über klassische Assistenz- und Fahrzeugsysteme hinausgeht. Die Entwicklung konzentriert sich dabei nicht nur auf wertschöpfende Mehrwertdienste oder Vorteile für den Fahrer, ein großer (sekundärer) Markt auf Basis der generierten Daten stellt neue Verwertungsmöglichkeiten für Big Data und Business Intelligence Anwendungen in der Automobilindustrie dar [14]. Die systematische Auswertung und Übermittlung der Daten eröffnet neue Potenziale für Wertschöpfung und Innovation. Diese reichen von der Erstellung detaillierter Kunden- und Fahrprofile, Tracking und Monitoring, Vernetzung der Fahrzeuge mit Behörden und Institutionen der öffentlichen Hand (Mautgebühren, Straßenverkehrsbehörden, etc.), Kommunikation mit der Infrastruktur (Ampeln und Schilder), die Möglichkeit der Interaktionen zwischen Fahrzeugen (Unfall- und Stauvermeidung) bis zur Etablierung intelligenter Verkehrssysteme (ITS) [15], [16].

Jedoch sind gegenwärtige (Flottenmanagement-)Systeme nicht in der Lage, die Vernetzung mit den beschriebenen Dienstleistern und Institutionen zu ermöglichen, um diesen entstehenden Markt für eine weitere Vermarktung zu erschließen. Außerdem ist es nicht möglich, die Personalisierung von individuellen Fahrzeugpräferenzen von Kunden abzubilden und in geteilten Mobilitätsdiensten zur Verfügung zu stellen. Die Kontrolle der bevorzugten Innenraumtemperatur, das Einstellen der Sitzposition oder der Lautstärke von Multimediadiensten wie Navigation und Radio sind weitere Beispiele für personalisierbare digitale Kundenpräferenzen. Um den Komfortanforderungen des Kunden in Zukunft gerecht zu werden, ist es notwendig, dass ein Kunde von den verschiedenen Fahrzeugen einer Flotte erkannt und das Interieur mit den entsprechen Funktionen angepasst wird. Damit geteilte Mobilitätsdienste das Komfortniveau eines privaten Pkw erreichen und als gleichberichtigte Alternative wahrgenommen werden, müssen Sitz- und Rückspiegeleinstellungen, die Regulierung des Klimasystems oder weitere Komfortfunktionen, wie die Beleuchtung, abhängig von den im System definierten Daten und Wünschen des Kunden, automatisch erfolgen. Wie zuvor erläutert, ist das Marktpotential sehr vielversprechend, wenn diese Dienstleistungen (aktuelle Komfortfunktionen) und zukünftige Mehrwertdienste in Form von Dienstleistungspaketen angeboten werden. Es gibt bereits eine Vielzahl an Konzeptstudien von automatisierten Fahrzeugen die Mehrwertdienste rudimentär integrieren, jedoch sind entsprechende Flottenmanagementsysteme, die Mobilität und Mehrwertdienste als Gesamtangebot vermarkten kaum erforscht. Zu diesem Zeitpunkt ist ein Informationssystem erforderlich, das über entsprechende Schnittstellen bestehende und zukünftige Technologien für wertschöpfende Dienste adressiert und individuell an die Endkunden vermarkten kann.

2.1 Aktuelle Konzepte für Mehrwertdienste

Es existiert kaum Literatur über spezifische Mehrwertdienste in automatisierten Fahrzeugen und deren integrierte Wertschöpfungen. Hauptsächlich existieren Konzept- und Designstudien von Herstellern und Zulieferern der Automobilindustrie [17]. Die

Hersteller erkennen jedoch zunehmend, dass die für den Fahrer durch die Automatisierung der Fahraufgaben gewonnene Zeit zu einer wichtigen Ressource für das Anbieten neuer Mehrwertdienste werden wird. Dabei können zukünftige Dienste noch weit darüber hinausgehen, was für heutige Fahrzeuge denkbar erscheint. Die Automobilindustrie zeigt bereits heute in Visionen und Konzeptfahrzeugen innovative Interieurkonzepte für automatisierte Fahrzeuge, die einen erheblichen Spielraum für (Neben-)Tätigkeiten beim Fahren gewähren. In diesem Zusammenhang sind die Komfortfunktionen von Lastkraftwagen zu nennen, die bereits eine Vielzahl an Technologien vereint.

Vargo et al. haben gezeigt, dass Servicesysteme die Werteschöpfung durch die Integration von speziellen Leistungen der Beteiligten fördern, jedoch eine Abhängigkeit zwischen diesen implizieren. Vor allem betont der Servicesystemansatz die zentrale Rolle der Kunden als letzte Instanz der Dienstleistungsbewertung [18], [19]. Zufriedene Kunden zu schaffen ist die wichtigste Methode für Unternehmen, um einen Wettbewerbsvorteil zu erlangen. Um jedoch Kunden qualitativ hochwertige Dienstleistungen anbieten zu können, muss der Anbieter die Erwartungen des Kunden verstehen [20], [21].

Das Fraunhofer IAO und Horvath&Partners untersuchten die möglichen Nebentätigkeiten beim automatisierten Fahren [10]. Diese wurden in sechs Kategorien unterteilt: Kommunikation, Produktivität, Grundbedürfnisse, Wohlfühlen, Information und Unterhaltung. Jede Kategorie wurde in 3-4 Unterkategorien unterteilt. Die Kategorie Kommunikation wird in Soziale-Medien, professionelle Kommunikation und Privatkommunikation unterteilt. Produktivität unterteilt sich in Arbeit, Bildung, Organisation und Konsum bzw. Online-Shopping. Grundbedürfnisse umfasst Aktivitäten wie Reinigen, Nahrungsaufnahme, Schlafen und Bekleidung wechseln. Wohlfühlen unterteilt sind in Wellness und Körperpflege, Gesundheit sowie Fitness. Die Kategorie Information unterteilt sich in Umgebungs-/Routeninformation, Produktinformationen und Surfen im Internet. Die letzte Kategorie Unterhaltung unterteilt sich in Spiele, künstlerische Tätigkeiten und passive Unterhaltung (z. B. Video-on-Demand). Durch die fortschreitende Technisierung und Digitalisierung des Fahrzeuges sowie des Innenraums können weitere innovative Dienste entstehen die Auswirkungen auf die Nutzung des Fahrzeugs haben. In diesem Kontext können z. B. Stadtrundfahrten vermarktet werden, die der Nutzer selbstständig und individuell zusammenstellt. Ein zu Grunde liegender digitaler Dienst übernimmt die Funktion des Reiseführers und steuert die Rundfahrt.

Zukünftig führt die zur Verfügung stehende Aufenthaltszeit im Fahrzeug zu einer deutlich stärkeren Wahrnehmung des Fahrzeugs als Lebensraum. Bereits heute haben Fahrer schon eine höhere Affinität, auch fahrfremde Tätigkeiten im Auto auszuführen. Die Kommunikation nimmt dabei einen hohen Stellenwert ein, außerdem zeigt die starke Verbreitung von Geschäftsmodellen auf der Basis von Drive-through- oder Drive-in-Kundenschnittstellen (insbesondere in den USA) die Affinität. Eingeschränkt kann bereits heute eine tendenziell höhere Zahlungsbereitschaft für Mehrwertdienste im Auto erklärt werden [10].

Die Erkenntnis, dass Menschen bereit sind, für mehr frei verfügbare Zeit einen nicht unerheblichen Betrag auszugeben, verdeutlicht die Bedeutung von freizeitschaffenden

Technologien für die Menschen und weist für die Fahrzeughersteller eine hohe strategische Relevanz im Wettbewerb um die Kunden auf [10].

2.2 Akzeptanz nutzerbezogener Mehrwertdienste

Die Studie "The Value of Time" [10] fokussiert nutzerbezogene Dienstleistungspotenziale, die durch automatisiertes Fahren ermöglicht werden. In diesem Zusammenhang wurde eine Nutzerumfrage mit 1500 Probanden aus Deutschland, Japan und den USA durchgeführt (je Land 500). Aufgrund der Vielfalt an denkbaren Beschäftigungen und Zeithorizonten wurden sechs Bedürfnisse und 21 Service-Gruppen für Mehrwertdienste formuliert und die Umfrage in zwei Szenarien „das hochautomatisierte Fahrzeug" (hands off und feet off) und „die fahrerlose Kapsel" (hands off, feet off und brain off) untergliedert [10].

Die Studie ergab, dass bei 75 % der Befragten eine Zahlungsbereitschaft für Mehrwertdienste beim automatisierten Fahren vorliegt. Dabei stehen Dienstleistungen, die die Durchführung von (Neben-)Tätigkeiten ermöglichen im Vordergrund und können somit zusammen mit dem Mobilitätsdienst vermarktet werden. Bei der Untersuchung der Dienstleistungen ist die Zahlungsbereitschaft in den Kategorien Kommunikation, Produktivität und Grundbedürfnisse am höchsten. Dabei müssen die Dienste und deren Preisgestaltung in den spezifischen Regionen untersucht und individuell angepasst werden, um die Kundenbedürfnisse bestmöglich adressieren zu können. Insgesamt liegt die durchschnittliche monatliche Zahlungsbereitschaft für alle Bedürfnisgruppen bei ca. 150 € bis 190 € pro Monat. Die Nutzer möchten in der Regel wertschöpfende Tätigkeiten, die bisher nicht im Fahrzeug ausgeführt werden können, in das Fahrzeug verlagern. Für diese Tätigkeiten haben die Nutzer eine höhere Zahlungsbereitschaft als für nicht verpflichtende, unterhaltende Tätigkeiten.

Die Studie zeigt, dass bereits bei kurzen Reisezeiten eine Zahlungsbereitschaft für Mehrwertdienste vorliegt und somit unterschiedliche Nutzungsprofile angeboten werden können. Weiterhin ergab die Studie, dass das Fahrzeugsegment keinen Einfluss auf die Zahlungsbereitschaft hat. Das heißt, die Dienste und Preise können über die gesamte Fahrzeugpalette angeboten werden, solange das Fahrzeug die technischen Anforderungen erfüllt (z. B. Display im Innenraum).

Insgesamt ist die Aufpreisbereitschaft für automatisierte Fahrzeuge über alle Fahrzeugsegmente signifikant [22]. Aus diesem Grund sollten insbesondere die volumenstarken Klein- und Mittelklassefahrzeuge adressiert werden. Der bedeutendste Mehrwert wird in der freiwerdenden Zeit gesehen, die die Erfüllung von Tätigkeiten im Fahrzeug erlaubt, die sonst außerhalb stattfinden würden. Jedoch unterscheiden sich diese stark nach Land, Alter, Einkommen und Fahrzeugsegment.

Die Nutzung von Mehrwertdiensten im Fahrzeug steht somit in direktem Zusammenhang mit der Zeit, die der Endkunde im Fahrzeug verbringt. Der Konsum von Mehrwertdiensten die einen längeren Zeitraum in Anspruch nehmen (z. B. Videostreaming) korrelieren stark mit der Fahrtdauer des Nutzers. Aktivitäten, die kurze Zeiträume beanspruchen und jederzeit unterbrochen werden können (z. B. Beantworten einer E-Mail), haben eine höhere Akzeptanz auf Kurzstrecken. Es ist davon auszugehen, dass die Fahrzeit einen maßgeblichen Einfluss auf den Konsum von

Mehrwertdiensten hat. Weiterführend kann die potenzielle Gesamtnutzungsdauer einen erheblichen Einfluss auf die monatliche Zahlungsbereitschaft und den Konsum von Mehrwertdiensten haben. Außerdem ist die Art und Charakteristik der zu tätigenden Fahrten ein entscheidender Faktor hinsichtlich der Nachfrage nach Zusatzdiensten [10]. Gleichwohl erlauben die Dienste auch vollkommen neue Geschäftsmodelle auf Basis automatisierter Fahrzeuge. Fahrer, die gewöhnlich zusammenhängende, lange Zeiträume oder monotone Fahrtabschnitte absolvieren (z. B. Pendeln auf der Autobahn), werden eher den Bedarf nach Ablenkung und Beschäftigungen verspüren als Fahrer, die vermehrt kurze oder abwechslungsreiche Fahrstrecken zu bewältigen haben.

Der insgesamt hohe Bereitschaftsgrad von 75 % lässt auf eine große Akzeptanz unter den Konsumenten schließen. Dies zeigt deutlich die zukünftige Relevanz und das Potenzial von Geschäftsmodellen auf Basis von Mehrwertdiensten im Fahrzeug [10].

3 Konzept des Flottenmanagementsystems

Wie bereits erläutert, werden bis 2030 ca. 33 % aller Neufahrzeuge für geteilte Mobilitätsdienste eingesetzt werden. Dies wird einen massiven Umbruch für den Automobilsektor zur Folge haben. Insbesondere Mobilitätsdienstleistungen auf Basis automatisierter Fahrzeuge führen dazu, dass Fahrzeuge zukünftig wesentlich intensiver genutzt werden [4], [13]. Durch den schnellen Wertverlust der Fahrzeuge verlieren Geschäftszweige, wie der Gebrauchtwagenhandel an Relevanz und die Hersteller werden stärker in das Service-Geschäft (z. B. Wartung und Instandhaltung) der Flottenfahrzeuge eingebunden sein.

Das Flottenmanagement wird durch die Zunahme an bedarfsorientierten Mobilitätsdiensten an Bedeutung gewinnen und sich zu einem wichtigen Geschäftszweig entwickeln, der durch regional unterschiedliche Verkehrsregulierungen und Infrastruktur beeinflusst wird. Globale Marktführer oder die starke Dominanz eines einzelnen Mobilitätsmodells wird es angesichts der vielseitigen Mobilitätsbedürfnisse nicht geben. Mittelfristig kann die starke Nachfrage nach automatisierten Fahrzeugflotten zu einer Verzahnung und parallelen Wettbewerbssituation von E-Commerce- und Logistikunternehmen sowie Flottenbetreibern führen.

Erste Forschungsbeiträge untersuchen das dynamische Flottenmanagement [23] in denen Fahrzeuge als Agenten modelliert werden und autonom auf Ereignisse reagieren können. Diese Arbeiten zeigen jedoch, dass der traditionelle Top-Down Ansatz zur Steuerung von Flotten zu einem Engpass in den skizzierten offenen und dynamischen Umgebungen wird, in denen Skalierbarkeit, Proaktivität und Autonomie Schlüsselfaktoren werden [23]. Der vorliegende Beitrag führt ein erstes Konzept für ein Flottenmanagementsystem (IS-Artefakt) ein, dass auf Basis verschiedener Schnittstellen Mehrwertdienste in das Flottenmanagement einführt. Eine Herausforderung besteht in der geeigneten Auswahl spezifischer Dienste, da mehrere Dienstleister identische Leistungen anbieten können. In Kombination mit

verschiedenen Mobilitätsoptionen können eine Vielzahl an personalisierten Angeboten erstellt werden.

3.1 Agentenbasiertes Flottenmanagement

Bei der Entwicklung von automatisierten Fahrzeugen sind effiziente und kostengünstige Assistenzsysteme notwendig, um den Mehrwert dieser Produkte zu erhöhen. Jedoch müssen die Fahrzeuge von sich aus alle notwendigen Fahrbedingungen wie ausreichenden Kraftstoffzustand oder den verkehrssicheren Fahrzeugzustand gewährleisten. Für diese Aufgaben müssen die Fahrzeuge die Fähigkeit haben, sich selbständig zu überwachen und mit technischen und menschlichen Akteuren zu kommunizieren. Der Passagier eines vollautomatisierten Fahrzeugs, insbesondere im Vehicle-on-Demand-Geschäft, kann den Betriebszustand des Fahrzeugs nicht bewerten. Derartige operative Aufgaben müssen zentral durch ein Flottenmanagementsystem gesteuert und überwacht werden. Deshalb erfordern automatisierte Fahrzeuge intelligente Dienste und Systeme, die diesen Anforderungen gerecht werden können und den Fahrgästen die Möglichkeit bieten, andere Aktivitäten zu verfolgen. Agenten sind auf Grund der Flexibilität, Wiederverwendbarkeit und Autonomie geeignet, auf Ereignisse zu reagieren, wie z. B. einen niedrigen Kraftstoffzustand oder Verkehrsprobleme [23]. Demzufolge müssen neue Flottenmanagementsysteme in der Lage sein, Aufgaben an automatisierte Fahrzeuge zuzuweisen um z. B. die kostengünstigste Tankstelle/Ladestation in Bezug auf die aktuelle Aufgabe zu ermitteln oder einen Servicetermin in einer Werkstatt unter vorgegebenen Parametern auszuhandeln.

Diese beiden Beispiele zeigen die Nachfrage nach intelligenten Systemen, die in der Lage sind, unabhängig und autonom zu agieren. Als möglicher Ansatz ist das dargestellte System (Abbildung 1) in der Lage, derartige Aufgaben auszuführen. Als Basis werden konventionelle Geschäftsprozesse genutzt (z. B. Wartungsprozess) und um Anforderungen (digitale Terminvergabe) bzw. Fähigkeiten von automatisierten Fahrzeugen (Datentransfer an Werkstatt) erweitert. Anschließend werden diese als Vorlage in das Flottenmanagementsystem überführt.

Die resultierenden Geschäftsprozesse werden als Template für spezifische Workflows genutzt, die entsprechend des Dienstleisters angepasst und im System durchgeführt werden müssen. Für jede Aufgabe kann ein oder mehrere Agenten (mit angeschlossenen Services von externen Dienstleistern) verwendet werden. Je nach Geschäftsprozess und den integrierten Daten aus dem Fahrzeug und des Kunden kann der Workflow verarbeitet und optimiert werden. Abschließend wird das hybride Leistungsbündel (HLB) entsprechend eines Kennzahlensystems bewertet. Dabei ist es auch möglich, einen Workflow auf eine Gruppe von Fahrzeugen anzuwenden, um z. B. die Verteilung einer Flotte in einem bestimmten Gebiet für die Bereitstellung intelligenter Mobilitätsdienste zu steuern.

3.2 Architektur des Flottenmanagementsystems

Das Flottenmanagementsystem basiert auf zwei verschiedenen Diensteverzeichnissen, das agentenbasierte Service-Verzeichnis und das Fahrzeugverzeichnis. Das agentenbasierte Service-Verzeichnis dient als Grundlage für die Umsetzung der Workflows und bildet den Zugang zu externen digitalen Diensten (auch von weiteren Dienstleistern). Das Verzeichnis fungiert somit als technische Schnittstelle zu externen Service-Lieferanten. Das Verzeichnis basiert auf dem Ruby-on-Rails Agentenframework Huginn, dass eine Wiederverwendbarkeit einzelner Funktionalitäten erlaubt. Außerdem können neue Workflows ohne großen Aufwand in dem Framework zusammengesetzt und integriert werden. Innerhalb des Service-Verzeichnisses werden die digitalen Dienste in drei verschiedenen Kategorien unterschieden, Mobilitätsdienstleistungen, Mehrwertdienste und operative Dienste zur Unterstützung des Betriebs des Flottenmanagementsystems. Mobilitätsdienstleistungen umfassen Routing-Dienstleistungen für Haus-zu-Haus-Mobilität, multimodale Mobilität, Pooling-Dienste oder räumliche Allokationsdienste. Weitere mögliche Mobilitätsdienste sind die Überwachung und Abrechnung von Fahrten oder Vorhersage-Algorithmen. Mehrwertdienste umfassen die zweite Kategorie von Dienstleistungen, die z. B. maßgeschneiderte Versicherungsdienstleistungen, Concierge-Service (bereits in Premium-Fahrzeuge vorhanden) oder sogar Video/Music-on-Demand-Dienstleistungen abbilden. Die dritte Kategorie umfasst interne Systemdienste, in diesem Fall die Bewertung von hybriden Leistungsbündel auf Basis eines Kennzahlensystems und die Endkundenschnittstelle. Dabei erfolgt die Kundenkommunikation über etablierte Schnittstellen wie Reiseinformationssysteme oder mobile Applikationen.

Das Fahrzeugverzeichnis bildet die automatisierten Fahrzeuge ab und stellt die fahrzeugbezogenen Daten und Kennzahlen sowie den Service-Endpunkte (Kommunikationsschnittstelle) der Fahrzeuge zur Verfügung. Auf Basis der bekannten Attribute der Fahrzeuge können neue innovative Dienstleistungen etabliert werden. Beispielsweise können fahrzeugindividuelle Routingalgorithmen entwickelt werden, die die CO_2-Emissionen eines Fahrzeugs reduzieren.

In diesem Sinne sollen automatisierte Fahrzeuge als physikalische Ressourcen im System repräsentiert werden, die ihren Zustand in Echtzeit verändern indem diese die Fahrzeugdaten an das System übermitteln. Basierend auf diesen kontinuierlichen Datenströmen sollen mobilitätsbezogene Angebote erstellt, bewertet und an Endverbraucher kommuniziert werden. Dabei enthalten Angebote ein oder mehrere Service-Bündel. Außerdem können verschiedene Angebote an den Endkunden kommuniziert werden (z. B. durch unterschiedliche Routing- und Video/Music-on-Demand Anbieter), die unterschiedliche Preis- und Mobilitätsmerkmale aufweisen.
Da zurzeit keine automatisierten Fahrzeuge mit entsprechender Technologie bzw. Schnittstelle zur Verfügung stehen, ist eine prototypische Implementierung mit Herausforderungen verbunden. Ein Großteil des Systems kann bereits umgesetzt werden, da das Flottenmanagementsystem die Integration der verschiedenen Service-Endpunkte wie Routing-, Versicherungs- oder Zusatzdienste wie Video-on-Demand über cloudbasierte APIs ermöglicht.

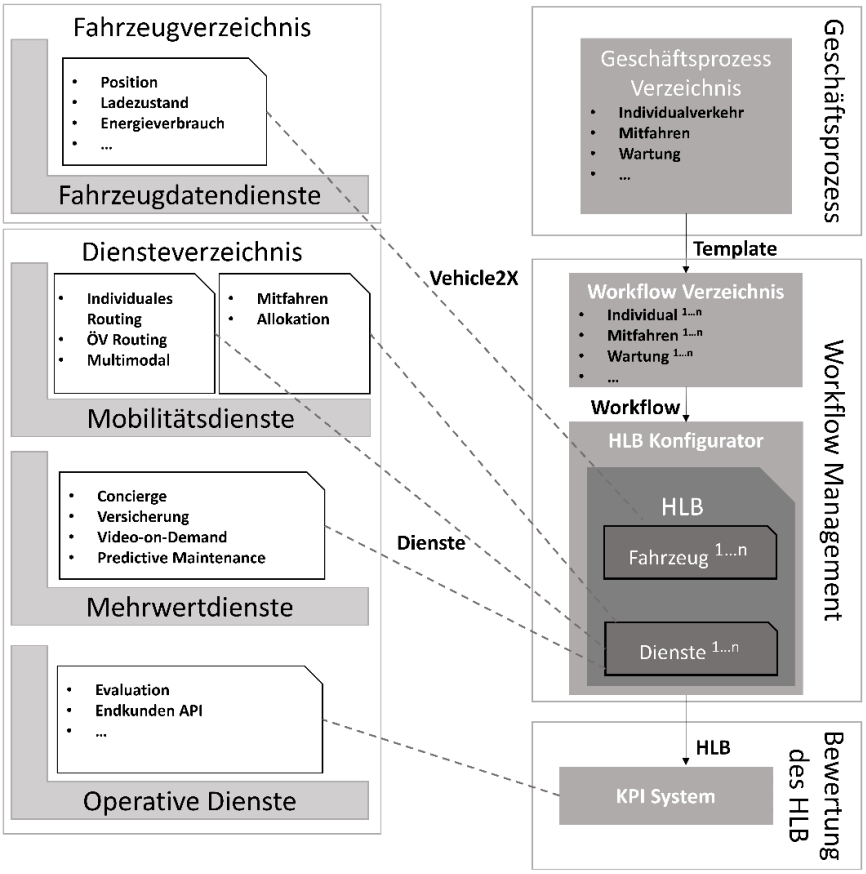


Abbildung 1: Nutzerzentrierte Wertschöpfung durch agentenbasierte Flottenmanagementsysteme

Die Anbindung der Fahrzeuge stellt sich als größte Herausforderung dar, da zurzeit keine standardisierten Schnittstellen zur Kommunikation mit den fahrzeuginternen Systemen vorliegen. Jedoch bieten einzelne Hersteller einen Entwicklerzugang an, um entsprechende In-car Apps zu implementieren, die als Kommunikationsendpunkt dienen können (vgl. GM Developer Network). Das Flottenmanagementsystem ist als mandantenfähige Cloud-Lösung auf Basis von Odoo konzipiert. Dies ermöglicht auch Kommunen und Verkehrsplaner über Schnittstellen Steuerungsmechanismen einzubinden um z. B. ein effizienteres Verkehrsmanagement durchzuführen. Letztlich müssen die Automobilhersteller eine zentrale und sichere Kommunikationsschnittstelle zur Verfügung stellen, um Mobilitätsaufgaben an das Fahrzeug übermitteln zu können und die integrierten Technologien für Mehrwertdienste zur Verfügung zu stellen. Außerdem muss das Flottenmanagementsystem eine Endkunden-API für die Buchung von Mobilitäts- und Mehrwertdiensten bereitstellen (z. B. als White-label app).

Abbildung 1 zeigt das Flottenmanagementsystem mit den verschiedenen Diensteverzeichnissen (links) und deren Integration in den Erstellungsprozess von hybriden Leistungsbündeln auf der Grundlage vordefinierter Geschäftsprozessvorlagen und individuell abgeleiteter Workflows (rechts).

4 Fazit

Der Automobilsektor steht unter Kosten- und Margendruck, abnehmenden Fahrzeugbesitz und hohe Investitionen in neue Technologien für Elektrofahrzeuge und automatisiertes Fahren. Der Wandel der Automobilhersteller zu Anbietern von Mobilitätsdienstleistungen ist ein möglicher Ansatz, um die Herausforderungen zu bewältigen und neue Wertschöpfungsketten aufzubauen. Die entstehenden Innovationen im Bereich des automatisierten Fahrens ermöglichen es, neue Dienstleistungen und Geschäftsmodelle im Fahrzeug anzubieten. Es ist jedoch weitgehend unklar, wie die Mobilitäts- und Mehrwertdienste integriert vermarktet werden können. Dieser Beitrag liefert einen Ansatz, wie auf Basis von hybriden Leistungsbündeln Mobilitäts- und Mehrwertdienste als Bündel an Kunden vermarktet werden können. Jedoch ist es zum aktuellen Zeitpunkt sehr komplex zu bewerten, welche Korrelationen zwischen Personengruppen und relevanten Mehrwertdiensten vorliegen und welche Dienste zukünftig nachgefragt werden.

Des Weiteren ist die Einführung von automatisierten Fahrzeugen stark von der politischen und ethischen Diskussion abhängig. Gleichzeitig gehen die Automobilhersteller ein hohes Risiko ein, da die viele technischen Herausforderungen in der Entwicklung bis zu einer Markteinführung zu bewältigen sind. Insgesamt muss jedoch eine zunehmende Verkehrsbelastung durch Leerfahrten möglichst vermieden werden, um die Chance des Paradigmenwechsels für ein nachhaltigeres und gerechteres Mobilitätssystem zu nutzen.

Anerkennung

Dieser Beitrag ist Teil des Forschungsprojektes "NEMo - Nachhaltige Erfüllung von Mobilitätsbedürfnissen im ländlichen Raum". Das Projekt wird vom Ministerium für Wissenschaft und Kultur Niedersachsen und der Volkswagen-Stiftung durch das Förderprogramm "Niedersächsisches Vorab" (Fördernummer VWZN3122) gefördert.

References

1. European Commission: Statistical Pocketbook - EU Transport in Figures, Luxembourg: Publications Office of the European Union (2016)
2. Canzler, W; Knie, A (2016): Digitale Mobilitätsrevolution - Vom Ende des Verkehrs, wie wir ihn kannten. Oekom verlag, München (2016)
3. Wehinger, S., Cords, S.: Transformation von Geschäftsmodellen in der Automobilindustrie am Beispiel von „Automatischem Fahren“. In: Proff, H.: Entscheidungen beim Übergang in

die Elektromobilität, DOI 10.1007/978-+3-658-09577-2_10, Springer Fachmedien Wiesbaden (2015)
4. Strategy&; PricewaterhouseCoopers: Digital Auto Report, September (2017)
5. Wagner vom Berg, B., Marx Gómez, J., and Sandau, A.: ICT-platform to transform car dealerships to regional providers of sustainable mobility services, Interdisciplinary Journal of Information, Knowledge, and Management (2017)
6. RAND: Autonomous Vehicle Technology - A Guide for Policymakers. (2014)
7. Becker, D., et al.: KPMG - Global Automotive Executive Survey 2016. (2016)
8. Schroers, M. A., Steuwer, S.: Autonomous Driving - Political, Legal, Social, and Sustainability Dimensions. In: Maurer, M., et al.: Autonomes Fahren, S. 151–173 (2015)
9. Pekkola, S., Ukko, J.: "Exploring added value through the service process: a comparative multiple case study", Benchmarking: An International Journal, Vol. 23 Issue: 5, pp.1249-1263 (2016), https://doi.org/10.1108/BIJ-11-2014-0102
10. Fraunhofer IAO, Horváth&Partners: The Value of Time. Nutzerbezogene Service-Potenziale durch autonomes Fahren. Stuttgart, April (2016)
11. MaaS-Alliance: The MaaS Alliance. Building an open market in seamless, demand-based travel. http://maas-alliance.eu. (2017)
12. Abraham, B., Runge, W.: Autonomes Fahren - Nur ein trojanisches Pferd der digitalen Unternehmen? In: ATZ elektronik 01/2016 (2016)
13. PricewaterhouseCoopers: Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles. (2016)
14. McKinsey&Company: Monetizing car data - New service business opportunities to create new customer benefits, Advanced Industries, September (2016)
15. Löw, M., Rothmann, L.: Privatsphäre in smarten Interaktionsräumen? Von intelligenten Städten und der Hoff nung auf die gute Gesellschaft. In: HMD - Praxis der Wirtschaftsinformatik 52, S. 610–623 (2015)
16. Fluegge, B.: Smart Mobility. 1. Wiesbaden: Springer Vieweg (2016)
17. Elbanhawi, M., Simic, M., Jazar, R.: In the Passenger Seat: Investigating Ride Comfort Measures in Autonomous Cars. Hg. v. RMIT University. RMIT University. Melbourne, Australia. (2015)
18. Carrillat, F.A., Jaramillo, F. and Mulki, J.P. (2007), "The validity of the SERQUAL and SERVPERF scales: a meta-analytic view of 17 years of research across five continents", International Journal of Service Industry Management, Vol. 18 No. 5, pp. 472-490.
19. Vargo, S.L. and Lusch, R.F. (2008), "Service-dominant logic: continuing the evolution", Journal of the Academy of Marketing Science, Vol. 36 No. 1, pp. 1-10.
20. Kim, H.-W. and Kim, Y.-G. (2001), "Rationalizing the customer service process", Business Process Management Journal, Vol. 7 No. 2, pp. 139-156.
21. Fließ, S. and Kleinaltenkamp, M. (2004), "Blueprinting the service company – managing service processes efficiently", Journal of Business Research, Vol. 57 No. 4, pp. 392-404.
22. Frost & Sullivan: Strategic Analysis of the European and North American Market for Automated Driving, S. 35–36. (2014)
23. Billhardt, H., Fernández, A., Lemus, L., Lujak, M., Osman, N., Ossowski, S., Sierra, C.: Dynamic Coordination in Fleet Management Systems: Toward Smart Cyber Fleets. In. IEEE Intelligent Systems (Volume: 29, Issue: 3, May-June 2014)

Vacuum Cleaning as a Service

Daniel Franzmann[1], Christoph Mittendorf[1], Uwe Ostermann[1]

[1] Goethe University Frankfurt, Information Systems Engineering, Frankfurt, Germany
{franzmann,mittendorf,ostermann}@wiwi.uni-frankfurt.de

Abstract. Smart technologies, such as autonomous robotic vacuum cleaners recently gained broader attention and change incumbent private work routines. In this research paper, we take the consumers' perspective and evaluate why consumers would intend or deter the use of vacuum cleaners. We investigate the positive influence of motivational drivers, such as trust, personal innovativeness, and hedonic values, as well as negative factors, such as perceived risk and perceived privacy violation. In this regard, we develop a research model that explains the consumers' intention to use an autonomous robotic vacuum cleaner. We use survey data (N = 223) and structural equation modeling for our analyses. Our results outline that trust and perceived risk, as well as other explicit motivational factors influence the consumers' intention to use robotic vacuum cleaners. Consequently, academic and practical implications are discussed.

Keywords: Robotic Vacuum Cleaner, Consumer, Intention to use.

1 Introduction

Autonomous robotic vacuum cleaners, commonly known as RVCs [1], are becoming extremely popular these days. These highly smart robots use artificial intelligence in order to replace the human operator for repetitive tasks respectively vacuum cleaning and can be understood as an example of a digital innovation [2]. Especially high-end models offer an appealing blend of cleaning power and smart home functionality. In this regard, researchers already investigate and test the actual performance of these devices in the laboratory to see whether they could navigate around obstacles, have adequate suction, move in an agile and efficient manner, and clean sufficiently [1, 3]. Although many of the current RVCs already do an impressive job on all those tasks, consumers are still skeptical regarding their intention to use RVCs in their private home.

In this study, we suggest a research model which examines the effect of trust, perceived risk, perceived convenience, hedonic value, personal innovativeness, perceived privacy violation, performance expectancy, social influence, and price value on the consumers' intention to use RVCs. In this regard, we draw on existing literature, such as Venkatesh et al. (2012), to identify potential drivers regarding the engagement in new technologies; thus we want to answer the following research question: *What are the main drivers of the consumers' intention to use RVC devices?*

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

With our study, we contribute to the field of business informatics and information systems by complementing the adoption-theory in the context of smart technologies. In other words, by incorporating the aforementioned drivers in this study, we shed light on distinct antecedents of consumers' intentions towards intention to use RVCs as an example for smart services devices [5, 6].

The remainder of our study is structured as follows: In Section 2, we present the constructs under study and state our research hypotheses as well as the research model. In Section 3, we present our measurement model and perform structural equation modeling. Section 4, concludes our paper by outlining theoretical and practical implications of our findings.

2 Literature Review and Hypotheses Development

2.1 Autonomous Robotic Vacuum Cleaners

A large variety of different RVCs already exists. Whereas some of them are more advanced than others, they basically follow the same principle and often share an almost identical feature set. In this case "autonomous", does not simply mean that the robot has a battery, good computational power, and certain behavioral rules, but operates without any human instructions [7]. Generally, RVCs have a cleaning module and a separated fan as well as an internal hose that connects both modules. Further, the RVC has a microprocessor that performs navigation and control functions based on 'AI' or 'chaos mode'. (1) The AI mode usually represents an active evaluation of the cleaning surroundings. In those cases, the RVC generally uses its data sensors and cameras to scan the cleaning field and calculate the most efficient cleaning routes, whereas (2) chaos mode generally indicates that the RVC randomly decides which routes to take based on predefined algorithms. Since the technology is still at early stage, researchers and analysts argue that it is only a matter of time until RVCs will be the main cleaning force in our homes [8].

2.2 RVC Adoption Factors

Research in business informatics and information systems recognizes **trust** as a core predictor of technology usage and an important notion for understanding consumers' perceptions of new technologies [9]. Trust is a complex concept [10, 11] that has induced IS research from different perspectives in many disciplinary fields, such as sociology [12, 13], psychology [14], philosophy [15, 16], and economics [17]. Independent of the field, researchers state that trust is multi-faceted, context-sensitive, and has several peculiarities [18, 19]. However, there is no agreement on an explicit definition of trust in the setting of new technologies. Recently, scholars started rethinking how the advancement of IT has affected concepts like trust. Researchers agree that the need for trust surges with the growing dependency on further entities, such as new IT, due to greater transaction complexity and uncertainties [12, 20]. Before consumers can use those new technologies they have to overcome the perceptions of

risk and uncertainty. In line with literature, we comprehend trust as the readiness to be exposed to the actions and consequences that new information technologies impose to their users. Therefore, we hypothesize: **H1a:** Increased degrees of trust in RVCs will increase the consumers' intention to use RVCs. **H1b:** Increased degrees of trust in RVCs will decrease the consumers' perceived risk of RVCs.

Sitkin and Pablo (1992) define **perceived risk** as follows: negative outcome expectations, negative outcome uncertainty, and negative outcome potential are incorporated into one broad risk concept. Our definition of perceived risk is further in line with other risk literature, especially with the definition by Nicolaou and McKnight (2006): the level to which one believes uncertainty is prevalent about whether desirable outcomes will occur. Thus, our research paper defines perceived risk as negative outcomes that might arise by using RVCs as a tool for automated cleaning – malfunctioning and poor cleaning performance. Perceived risk in general is an important barrier for potential consumers who consider using new IT [23, 24]. Prior research fortified us to explore the implications of trust and perceived risk on the consumers' intention to use RVCs [25]. In this regard, we hypothesize: **H2:** Increased degrees of perceived risk of RVCs will decrease the consumers' intention to use RVCs.

Technology adoption is influenced by **personal innovativeness**. This driver stems from the diffusion of innovations research and describes individuals who adopt an innovation at an early stage [26]. In 1998, Agarwal and Prasad were the first who specified and used this personality attribute to the domain of IT and defined it as the willingness to try and experiment with any new technology [27]. While the first RVCs were already commercially available in the early 2000s, many households still have not adopted this technology and use traditional vacuum cleaners [28]. IRobot estimates that around 20% of all households use RVCs – however, this number is steadily increasing [8]. We argue that people who are highly innovative towards IT are more likely to purchase and use RVCs. **H3:** Increased degrees of personal innovativeness in IT will increase the consumers' intention to use RVCs.

Hedonic value describes how enjoyable or entertaining a technology is [4]. Holbrook and Hirschman (1985) were among the first who differentiated between hedonic and utilitarian products. IS literature has adapted their definition and focuses further on this differentiation. Moreover, Venkatesh et al. (2012) incorporated hedonic motivation into the extension of the unified theory of acceptance and use of technology (UTAUT2). UTAUT2 was especially developed to explain use intentions and use behavior of consumers. As RVCs are IT-gadgets designed for the consumer market, we hypothesize: **H4:** Increased degrees of hedonic values in RVCs will increase the consumers' intention to use RVCs.

The driver **social influence** is defined as the extent to which a consumer perceives that important others believe he or she should be using RVCs [4]. In other words, the concept of social influence describes the pressure to behave in a way that is endorsed by a social group [30]. According to IS research social influence is an important antecedent for behavioral intention and use [4, 31]. Therefore, we hypothesize: **H5:** Increased degrees of social influence will increase the consumers' intention to use RVCs.

The cost of an IT device plays an important role in the decision process behind a purchase and future use [4]. Compared to normal vacuum cleaners RVCs are far more costly. The **price value** depends on the RVCs' features, such as smart AI modes, speed and suction power, or remote access via smartphone app. Consumers have to form a tradeoff between the benefits and the monetary cost [32]. Therefore, a high value relative to the price will increase the use intention. We hypothesize: **H6:** Increased degrees of price value will increase the consumers' intention to use RVCs.

Performance expectancy is a key driver of IT-adoption. Prior the initial purchase and use of IT, consumers have already formed a specific expectancy of the product and its expected performance [4, 33]. While performance expectancy was originally used in the work context, we apply it to the "job" or "service" of vacuum cleaning a house or flat. In other words, if people believe that the use of an autonomous vacuum robot will save time or increase the quality of their vacuum cleaning, they are more likely to purchase and use one. Therefore, we hypothesize: **H7:** Increased degrees of performance expectancy will increase the consumers' intention to use autonomous RVCs.

In the future, RVCs could replace most of the cleaning duties at homes as well as at workplaces. This could benefit elderly people, people suffering from allergies, and reduce the overall cleaning effort. Consequently, RVCs can help to simplify cleaning tasks. In this regard, we hypothesize for **perceived convenience**: **H8:** Increased degrees of perceived convenience will increase the consumers' intention to use autonomous RVCs.

Similar to trust, the **perceived privacy violation** is a common factor in the adoption of new and cloud-based IT. RVCs use several sensors and cameras to scan the environment, their cleaning path, and their general surroundings in order to optimize the cleaning procedure [34]. Most of the cleaners use cloud storage to store and process information and to make it available through smart services, such as smartphone apps or smart assistances like Google Home or Amazon Alexa. This imposes a potential privacy risk and consumers may be afraid that their personal data (e.g., the floor plan of the flat) might be available to the manufacturer of the cleaning device or even be shared publicly [35, 36]. Therefore, we hypothesize: **H9:** Increased degrees of perceived privacy violation in RVCs will decrease the consumers' intention to use RVCs.

Last, after the development of our hypotheses based on the conducted literature review, we outline our research model. Figure 1 gives an overview of all drivers, hypotheses, and relationships used in the given study.

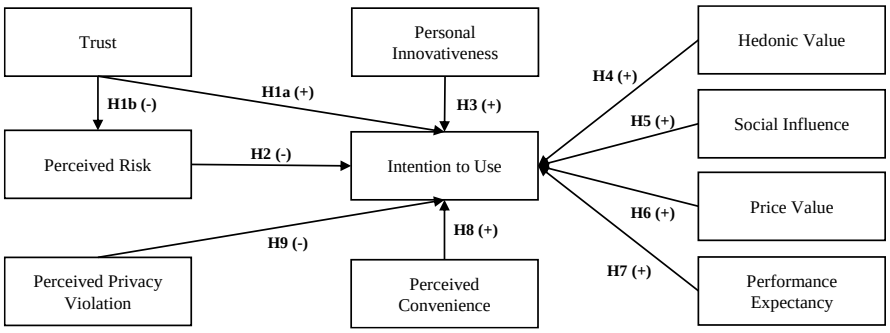


Figure 1. Research model

3 Methodology

3.1 Measurement Development and Data Collection

We designed an online survey to evaluate the potential consumers' intention to use RVCs. In order to assess the personal attitudes and beliefs of consumers, we decided to conduct a survey as a first research step and provides a good foundation for future research. For example, extended research could use methods like laboratory and field experiments to measure the behavioral traits [37]. The questionnaire used in the study contained 47 questions and covered ten constructs. Further, we included income, profession, marital status, age, education, and gender as controls [37], as all these variables could theoretically bias the consumers' intention towards the engagement of new technologies [38].

Table 1. Participants characteristics (N = 223)

	Count	*%*		*Count*	*%*
Age			**Marital status**		
16 to 20 years	14	6.28%	Single	119	53.36%
21 to 25 years	41	18.39%	Married	91	40.81%
26 to 30 years	47	21.08%	Separated	4	1.79%
31 to 35 years	37	16.59%	Divorced	9	4.04%
36 to 40 years	14	6.28%			
41 to 45 years	24	10.76%	**Profession**		
46 to 50 years	20	8.97%	Student	30	13.45%
51 to 55 years	12	5.38%	Employed for wages	94	42.15%
56 to 60 years	13	5.83%	Self-employed	58	26.01%
61 to 65 years	1	0.45%	Out of work	37	16.59%
			Retired	4	1.79%
Income in USD					
less than $20,000	50	22.4%	**Education**		
$20,000 - $29,999	28	12.6%	Less than high school	1	0.45%

$30,000 - $39,999	22	9.9%	High school graduate	82	36.77%
$40,000 - $49,999	45	20.2%	Associate degree	34	15.25%
$50,000 - $59,999	25	11.2%	Bachelor's degree	78	34.98%
$60,000 - $69,999	13	5.8%	Master's degree	23	10.31%
$70,000 - $79,999	16	7.2%	Doctorate degree	5	2.24%
$80,000 - $89,999	4	1.8%			
$90,000 - $99,999	7	3.1%	**Gender**		
above $100,000	13	5.8%	Male	78	34.98%
			Female	145	65.02%

In our survey, we employed a standardized 7-point Likert scale response format – going from strongly disagree (1) to strongly agree (7). Table 5 in the Appendix holds a summary of the items, including the constructs, the loadings, the corresponding item codes, and the references. Our study was conducted in late 2017 and we used clickworker a crowd sourcing platform similar to Amazon Mturk as a platform to target potential consumers of RVCs [39]. By the due date, 223 native English speakers from the US, UK, and Canada completed the survey – see Table 1.

3.2 Measurement Model

First, we evaluated the factor structure of the dataset (N = 223) to evaluate the reliability of the measurement model. In particular, we assessed the validity and reliability of ten constructs by following the recommendations made by Hair et al. (2014) and Straub et al. (2004) to judge for internal consistency. To this end, our tests showed satisfactory reliability for all our constructs, as the calculated Cronbach's Alpha, rho_A, and Composite Reliability score all above the threshold of 0.70 [42]. Table 2 shows the reliability indices for our ten constructs.

Table 2. Descriptive statistics and reliability index

Construct	*Cronbach's Alpha*	*rho_A*	*Composite Reliability*
Hedonic value	0.931	0.948	0.956
Intention to use	0.958	0.959	0.968
Perceived risk	0.918	0.944	0.934
Perceived privacy violation	0.981	0.985	0.985
Perceived convenience	0.936	0.944	0.951
Performance expectancy	0.955	0.960	0.971
Personal innovativeness	0.905	0.910	0.941
Price value	0.919	0.989	0.936
Social influence	0.976	0.977	0.984
Trust	0.931	0.933	0.946

Further, we valued construct validity by measuring convergent validity and discriminant validity [43]. Convergent validity can be understood as the degree to which the measures for an item perform as if they are measuring the principal theoretical construct because they share variance [44]. So, convergent validity can be

considered satisfactory when the Average Variance Extracted (AVE) is higher than 0.50 for all constructs [42]. Finally, discriminant validity can be understood as the degree to which measures of different latent variables are exclusive [43]. To this end, discriminant validity can be considered acceptable when the square roots of the AVE values are higher than the correlations among the research constructs [42]. Moreover, the variance explained by every construct should be higher than the measurement error variance, which is the case.

Table 3. Convergent and discriminant validity coefficients

	AVE	*H*	*Int*	*PC*	*PPV*	*PR*	*PE*	*PI*	*PV*	*SI*	*T*
H	0.88	**0.94**									
Int	0.86	0.64	**0.93**								
PC	0.80	0.61	0.77	**0.89**							
PPV	0.93	-0.16	-0.18	-0.25	**0.96**						
PR	0.70	-0.21	-0.42	-0.45	0.54	**0.84**					
PE	0.92	0.52	0.75	0.74	-0.18	-0.35	**0.96**				
PI	0.84	0.36	0.43	0.33	0.00	-0.08	0.34	**0.92**			
PV	0.75	0.45	0.42	0.34	0.03	-0.07	0.42	0.32	**0.86**		
SI	0.95	0.45	0.55	0.41	0.04	-0.08	0.47	0.4	0.51	**0.98**	
T	0.74	0.47	0.65	0.61	-0.19	-0.41	0.53	0.41	0.43	0.4	**0.86**

Note: AVE = Average Variance Extracted. Diagonal elements of the last ten columns represent the square root of the AVE. Off diagonal elements are the correlations among latent constructs.
H = Hedonic values, Int = Intention to use, PC = Perceived convenience, PPV = Perceived privacy violation, PR = Perceived risk PE = Performance expectancy, PI = Personal innovativeness, PV = Price value, SI = Social influence, T = Trust

The results of our analyses indicate that there is strong evidence of construct validity in the collected dataset. Table 3 shows that discriminant validity seems not to be an issue in our data. Lastly, we evaluated a potential common method bias in SPSS. In particular, we used the Harman's single factor test to verify that no single component explains more than 50% of the total variance (the test scored with: 36.63%). Based on this analysis, we find that the common method bias is unlikely a potential concern in our data.

3.3 Structural Model Assessment

Our main goal of this study was to identify the drivers and the impediments of the consumers' intention to use RVCs. Hence, after we confirmed the adequate factor structure of our dataset, we conducted PLS-SEM to analyze both the measurement and structural relationships demonstrated in our research model [45, 46]. Our analyses show that the data collected through our survey adequately fits our research model. The selected items share only little residual variance and indicate unidimensionality of the SEM approach. Table 4 and Figure 2 show the results of the SEM approach. The explanatory power of our research model was evaluated by exploring the significance levels of the corresponding path coefficients. The results show support for seven out of ten hypotheses.

Table 4. Results of path coefficients

Hypothesis	*Path*	*Path Coefficient*	*Sample Mean*	*T Statistics*	*p-value*
H1a	T → Int	0.168	0.170	2.995	**0.003****
H1b	T → PR	-0.411	-0.418	5.493	**0.000*****
H2	PR → Int	-0.125	-0.124	2.477	**0.013***
H3	PI → Int	0.211	0.066	1.252	0.211
H4	H → Int	0.172	0.173	3.210	**0.001****
H5	SI → Int	0.160	0.159	3.511	**0.000*****
H6	PV → Int	-0.034	-0.034	0.760	0.447
H7	PE → Int	0.289	0.286	4.076	**0.000*****
H8	PC → Int	0.220	0.220	2.539	**0.011***
H9	PPV → Int	0.058	0.059	1.187	0.235

Note: * significant at a .05 level, ** significant at a .01 level, *** significant at a .001 level

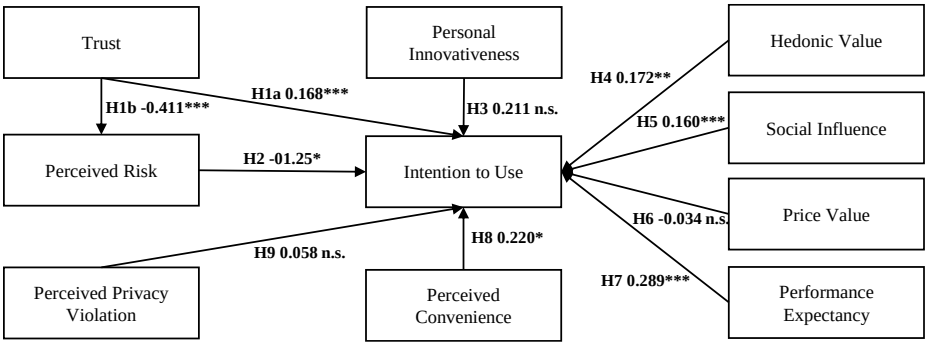


Figure 2. PLS analysis with standardized path coefficients

4 Discussion, Conclusion, and Implications

The objective of this study was to investigate the consumer motives behind the purchase and use of RVCs. To the best of our knowledge, our study is the first that focuses on the consumers' intention to use RVCs instead of (or as an addition to) a normal vacuum cleaner. Our research model is based on existing literature and our measurement instruments were adapted for the specific use case. We conducted a web-based survey with a total of 223 participants. Our PLS-SEM analysis shows that seven of our ten hypotheses were supported.

As hypothesized and in line with the literature, trust has a significant positive effect on the intention to use and a significant negative effect on perceived risk. Further, higher perceived risk leads to a decrease in the intention to use. Hedonic value, social influence, performance expectancy, and perceived convenience have a positive effect on the intention to use a RVC.

However, three of our hypotheses were not supported as determined by the PLS-SEM analysis. Perceived privacy violation had no significant effect on intention to use.

This might be due to two reasons: (1) people might not be aware of the fact that RVCs scan their surroundings and (2) people might perceive the upload to the manufacturer cloud not as a violation of their privacy. Further, personal innovativeness did not have a significant effect on the intention to use. A reason for this might be the fact that RVCs are a digital and enhanced version of normal vacuum cleaners and therefore, are not perceived as something completely new. People might perceive them more in terms of an upgrade instead of a new technology. The third construct that did not have a significant effect on intention to use was price value. One possible explanation might be that people do not know much about the actual price value of RVCs. Therefore, they are not able to distinguish between the features and the benefits.

The study at hand holds theoretical and practical contributions. First, we contribute to the theoretical topic of adoption. The developed research model helps to identify important drivers behind the use of RVCs. Second, RVC-companies can use that knowledge to further enhance their products and increase their market shares. However, there are several limitations. As we conducted an online survey, there is a lack of generalizability, further all our respondents came from western countries, consequently cultural differences could pose a potential issue. For further research, we recommend a focus on cultural differences and evaluate the hedonic value of RVCs through experiments or choice-based conjoint analyses.

References

1. Doh, N.L., Kim, C., Chung, W.K.: A Practical Path Planner for the Robotic Vacuum Cleaner in Rectilinear Environments. In: IEEE Transactions on Consumer Electronics A. pp. 519–527 (2007).
2. Yoo, Y., Henfridsson, O., Lyytinen, K.: The new organizing logic of digital innovation: An agenda for information systems research. Inf. Syst. Res. 21, 724–735 (2010).
3. Bai, Y., Hsueh, M.: Using an Adaptive Iterative Learning Algorithm for Planning of the Path of an Autonomous Robotic Vacuum Cleaner. In: IEEE Global Conference on Consumer Electronics 2012. pp. 406–410 (2012).
4. Venkatesh, V., Thong, J., Xu, X.: Consumer Acceptance and Use of Information Technology: Extending The Unified Theory of Acceptance and Use of Technology. MIS Q. 36, 157–178 (2012).
5. Norton, J.A., Bass, F.M.: A Diffusion Theory Model of Adoption and Substitution for Successive Generations of High-Technology. Manage. Sci. 33, 1069–1086 (1987).
6. Straub, E.T.: Understanding Technology Adoption: Theory and Future Directions for Informal Learning. Rev. Educ. Res. 79, 625–649 (2009).
7. Ulrich, I.R., Mondada, F., Nicoud, J.: Autonomous vacuum cleaner. Rob. Auton. Syst. 1–16 (1997).
8. Trend, R.: 20% of All Vacuums are Robots.
9. Li, X., Hess, T.J., Valacich, J.S.: Why do we trust new technology? A study of initial trust formation with organizational information systems. J. Strateg. Inf. Syst. 17, 39–71 (2008).
10. Shapiro, S.P.: The Social Control of Impersonal Trust. Am. J. Sociol. 93, 623–658 (1987).
11. McKnight, D.H., Chervany, N.L.: What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. Int. J. Electron. Commer. 6, 35–59 (2001).

12. Luhmann, N.: Trust and Power. John Wiley & Sons (1979).
13. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: A cross-discipline view of trust. Acad. Manag. Rev. 23, 393–404 (1998).
14. Geyskens, I., Steenkamp, J.-B.E.M., Scheer, L.K., Kumar, N.: The effects of trust and interdependence on relationship commitment. Int. J. Res. Mark. 13, 303–317 (1996).
15. Porter, T.: Trust in numbers. The pursuit of objectivity in science and public life. (1996).
16. Hosmer, L.T.: Trust: The Connecting Link between Organizational Theory and Philosophical Ethics. Acad. Manag. Rev. 20, 379–403 (1995).
17. Fehr, E.: On the Economics and Biology of Trust. J. Eur. Econ. Assoc. 7, 235–266 (2009).
18. Gefen, D., Straub, D.W.: Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. Omega. 32, 407–424 (2004).
19. McKnight, D.H., Cummings, L.L., Chervany, N.L.: Initial Trust formation in new organizational relationships. Acad. Manag. Rev. 23, 473–490 (1998).
20. Pavlou, P.A., Gefen, D.: Building Effective Online Marketplaces with Institution-Based Trust. Inf. Syst. Res. 15, 37–59 (2004).
21. Sitkin, S.B., Pablo, A.L.: Reconceptualizing the Determinants of Risk Behavior. Acad. Manag. Rev. 17, 9–38 (1992).
22. Nicolaou, A.I., McKnight, D.H.: Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. Inf. Syst. Res. 17, 332–351 (2006).
23. Jarvenpaa, S.L., Tractinsky, N., Saarinen, L.: Consumer trust in an internet store: a cross culture validation. J. Comput. Mediat. Commun. 5, 1–35 (1999).
24. Pavlou, P.A.: Integrating Trust in Electronic Commerce with the Technology Acceptance Model: Model Development and Validation. In: AMCIS 2001. pp. 816–822 (2001).
25. Mittendorf, C., Franzmann, D., Ostermann, U.: Why Would Customers Engage in Drone Deliveries? In: AMCIS 2017 Proceedings. pp. 1–10 (2017).
26. Rogers, E.M.: Diffusion of innovations. (1995).
27. Agarwal, R., Prasad, J.: A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology. Inf. Syst. Res. 9, 204–215 (1998).
28. BBC: Robot cleaner hits the shops.
29. Holbrook, M.B., Hirschman, E.C.: The experiential aspects of consumption: Consumer fantasies, feelings, and fun. J. Consum. Res. 9, 132–140 (1982).
30. Fishbein, M., Ajzen, I.: Belief, attitude, intention and behavior: an introduction to theory and research. Penn State University Press (1975).
31. Slade, E.L., Williams, M.D., Dwivedi, Y.: Extending UTAUT2 To Explore Consumer Adoption Of Mobile Payments. UK Acad. Inf. Syst. Conf. Proc. 23 (2013).
32. Dodds, W.B., Monroe, K.B., Grewal, D.: Effects of Price , Brand , and Store Information on Buyers â€™ Product Evaluations. J. Mark. Res. 28, 307–319 (1991).
33. Tan, D., Bai, J.: Analysis of the Factor Affected Chinese Audience Choice Behavior between Traditional TV and Network Video in PLS-SEM. Mod. Econ. 833–845 (2015).
34. Luo, C.L.C., Yang, S.X.: A real-time cooperative sweeping strategy for multiple cleaning robots. Proc. IEEE Internatinal Symp. Intell. Control. 660–665 (2002).
35. Aleisa, N., Renaud, K.: Privacy of the Internet of Things: A Systematic Literature Review. Proc. 50th Hawaii Int. Conf. Syst. Sci. 5947–5956 (2017).
36. Telegraph: Robot vacuum cleaner plans to share maps of people's homes.
37. Fang, Y., Qureshi, I., Sus, H., Mccole, P., Ramsey, E., Lim, K.H.: Trust, Satisfaction, and Online Repurchase Intention: The Moderating Role of Perceived Effectiveness of E-Commerce Institutional Mechanisms. MIS Q. 38, 407–427 (2014).
38. Kim, D.J., Ferrin, D.L., Rao, H.R.: A trust-based consumer decision-making model in

electronic commerce: The role of trust, perceived risk, and their antecedents. Decis. Support Syst. 44, 544–564 (2008).
39. Buhrmester, M., Kwang, T., Gosling, S.D.: Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? Perspect. Psychol. Sci. 6, 3–5 (2011).
40. Hair, J.F., Black, W.C.., Babin, B.J., Anderson, R.E.: Multivariate Data Analysis. (2014).
41. Straub, D., Boudreau, M.-C., Gefen, D.: Validation Guidelines for Is Positivist Research. Commun. Assoc. Inf. Syst. 13, 380–427 (2004).
42. Fornell, C., Larcker, D.F.: Evaluation of structural equation models with unobservable variables and measurement error: Algebra and statistics. A Second Gener. Multivar. Anal. 2, 382–388 (1982).
43. O'Leary-Kelly, S.W., J. Vokurka, R.: The empirical assessment of construct validity. J. Oper. Manag. 16, 387–405 (1998).
44. McKnight, D.H., Choudhury, V., Kacmar, C.: The impact of initial consumer trust on intentions to transact with a web site: A trust building model. J. Strateg. Inf. Syst. 11, 297–323 (2002).
45. Gefen, D., Rigdon, E.E., Straub, D.W.: An Update and Extension to SEM Guidelines for Administrative and Social Science Research. MIS Q. 35, iii–xiv (2011).
46. Lowry, P.B., Gaskin, J.: Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. IEEE Trans. Prof. Commun. 57, 123–146 (2014).
47. Zaleskiewicz, T.: Beyond risk seeking and risk aversion: personality and the dual nature of economic risk taking. Eur. J. Pers. 15, 105–122 (2001).

Appendix

Table 5. Overview of items after the content validity assessment

Construct	*Code*	*Item*	*Loading*	*Reference*
Perceived convenience	PC1	I feel that robotic vacuum cleaner are convenient.	0.913	Items adapted and modified from Mittendorf et al. (2017)
	PC2	Robotic vacuum cleaner involve little trouble or effort.	0.835	
	PC3	I believe robotic vacuum cleaner are convenient and suitable to use.	0.924	
	PC4	I feel that using robotic vacuum cleaner reduce effort.	0.888	
	PC5	I believe robotic vacuum cleaner are comfortable to use.	0.900	
Hedonic values	H1	Using robotic vacuum cleaner is fun.	0.952	Items adapted from Venkatesh et al. (2012)
	H2	Using robotic vacuum cleaner is enjoyable.	0.960	
	H3	Using robotic vacuum cleaner is very entertaining.	0.898	
Intention to use	Int1	I am very likely to use robotic vacuum cleaner in the future.	0.882	Items adapted and modified from Davis et al. (1989), Gefen et al. (2003), Pavlou (2001)
	Int2	I would use robotic vacuum cleaner in general.	0.937	
	Int3	I would not hesitate to use robotic vacuum cleaner in my home.	0.935	
	Int4	Given the chance, I would use robotic vacuum cleaner.	0.932	
	Int5	Given the opportunity, I intend to use robotic vacuum cleaner as a form of cleaning.	0.942	

Performance expectancy	PE1	Robotic vacuum cleaner would be useful in my daily life.	0.948	Items adapted from Venkatesh et al. (2012)
	PE2	Using robotic vacuum cleaner would help me to accomplish things more quickly.	0.960	
	PE3	Using robotic vacuum cleaner would increase my productivity.	0.965	
Personal innovativeness	PI1	If I heard about a new information technology, I would look for ways to experiment with it.	0.924	Items adapted from Agarwal and Prasad (1998)
	PI2	Among my peers, I am usually the first to try out new information technologies.	0.899	
	PI3	I like to experiment with new information technologies.	0.929	
Perceived privacy violation	PPV1	I have concerns that private data might be leaked when using robotic vacuum cleaner.	0.963	Items adapted from Pavlou and Gefen (2004), Zaleskiewicz (2001)
	PPV2	I have concerns that private data will be revealed to others when using robotic vacuum cleaner.	0.968	
	PPV3	I am afraid that private data will be stored without my knowledge when using robotic vacuum cleaner.	0.960	
	PPV4	I am afraid that private information will be stored insecurely when using robotic vacuum cleaner.	0.967	
	PPV5	I feel that my privacy could be violated when using robotic vacuum cleaner.	0.959	
Perceived risk	PR1	There is a considerable risk involved in using robotic vacuum cleaner.	0.790	Items adapted and modified from Pavlou and Gefen (2004), Zaleskiewicz (2001)
	PR2	There is a high potential for problems involved in using robotic vacuum cleaner.	0.848	
	PR3	A decision to use robotic vacuum cleaner as a cleaning device risky.	0.899	
	PR4	It is likely that a robotic vacuum cleaner, as a cleaning device, will fail to meet my expectations.	0.720	
	PR5	Using robotic vacuum cleaner is unsafe.	0.881	
	PR6	I think it is risky to use a robotic vacuum cleaner as a cleaning device.	0.884	
Price value	PV1	I think robotic vacuum cleaner are not costly.	0.815	Items adapted from Venkatesh, et al. (2012)
	PV2	I believe robotic vacuum cleaner are cheap.	0.765	
	PV3	Robotic vacuum cleaner are reasonably priced.	0.903	
	PV4	Robotic vacuum cleaner are a good value for the money.	0.909	
	PV5	At the current price, robotic vacuum cleaner provide a good value.	0.917	
Social influence	SI1	People who are important to me think that I should use robotic vacuum cleaner.	0.974	Items adapted from Venkatesh, et al. (2012)
	SI2	People who influence my behavior think that I should use robotic vacuum cleaner.	0.976	

Concepts of Product-Service Configurators for Repurposing used Electric Vehicle Batteries

Markus Monhof[1]

[1] Westfälische Wilhelms-Universität Münster, European Research Center for Information Systems (ERCIS), Münster, Germany
markus.monhof@ercis.uni-muenster.de

Abstract. The configuration of Product-Services Systems (PSSs) can be a complex task because of a large number of possibilities and dependencies that have to be considered. PSS configurators as a class of information systems can be used to support this task. To inform the design of a PSS configurator for the domain of repurposing used Electric Vehicle Batteries, a structured literature review on existing configurators is performed to identify underlying concepts and functionality. The results are discussed regarding their applicability in the specific domain of repurposing used EVBs. Additionally, the results are used to triangulate design choices made in the development of a first prototype.

Keywords: Product-service system, configurator, electric vehicle battery, repurposing, second-life

1 Introduction

Electric mobility is seen as one step towards reducing (locale) greenhouse gas emissions and therefore as a way to decelerate climate change and towards environmental sustainability [1]. However, in most countries, the diffusion of electric vehicles is still struggling. One of the reasons is the high initial costs when purchasing an electric vehicle. A significant share of these expenses is caused by the Electric Vehicle Battery (EVB) that is one of the reasons why electric cars are significantly more expensive than comparable conventional vehicles [2, 3].

The EVB is the component that stores and provides the energy necessary to propel the electric engine(s) of an electric vehicle. However, the currently used lithium-ion technology is suffering from degradation effects. In particular, the EVB's capacity (i.e., the amount of energy that can be stored) and power decreases over time and use. For the driver of an electric vehicle, this is notable in the range that can be driven without recharging and the loss of the capability to quickly charge the battery. Currently, it is assumed that an EVB should be removed from the car when the capacity has dropped to about 70%-80% of the original capacity [4, 5]. This is supposed to be reached after about eight years or 120.000 km driven [2].

In the EU the car and battery manufacturers are legally required to take back the used batteries. Therefore, with rising electric car sales the manufacturers will soon have to

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

handle a large amount of old EVBs. Since the recycling of such large lithium-ion batteries is expensive [6] at the moment, it will be economically beneficial for the manufacturers to further use these batteries in different less demanding applications, the so-called *second-life applications* (SLAs).

Previous research has shown that used EVBs can be repurposed for various SLAs and marketed as part of product-service systems (PSSs) [2]. PSSs consist of a physical component and additional services and are suitable to provide customers with fitting offers for their individual needs [7]. In the case of repurposing of used EVBs, a PSS consists of one or more used batteries with additional services that can be required to settle certain drawbacks of the used battery (e.g., higher perceived risk of failure, classification as dangerous goods, unknown quality) or provide additional value to the customer.

Since every used battery has a different condition because of the degradation, their future performances will largely differ so that not every battery can be repurposed for every application [8]. Therefore, possible SLAs have to be determined for each used EVB individually [8]. Additionally, the SLAs have different technical requirements on the battery and additional (electrical) components that are needed for a safe operation [9]. Furthermore, the customers might have additional needs that should be addressed. Therefore, PSSs have to be configured for each customer specific application scenario individually.

Configuring PSSs that satisfy specific customer needs can be challenging. The configuration of PSSs is the process of selecting products and services, which solves an individual customer problem, from a set of predefined modules [10]. Because of a high number of possibilities and dependencies between product and service components this task is hardly possible to do manually. This calls for information systems (IS) to support this task. Since the whole domain of repurposing used EVBs is new, currently no specific PSS configurators for repurposing used EVBs exist. We set out to develop such a configurator as a component of a decision support system in a larger design science research project. We already presented a first prototype in [11]. However, its design is mainly informed by domain knowledge, and evaluation is still missing and challenging because practical application lies much into the further. Therefore, we strive to use knowledge on PSS configurators as a triangulation and to improve the design. To achieve this, in this article, we set out to identify the concepts and functionalities that underlie current configurators for PSS. Furthermore, we are interested in how these can be adapted for configurators for PSS consisting of used EVBs and additional services.

The following research questions are addressed in this paper:

1. *Which are the underlying concepts of existing configurators for PSS?*
2. *How should these concepts be adapted for the domain of repurposing used EVBs?*

To answer the research questions, we provide a systematic literature review of current configurators for PSSs. Based on this, we discuss the results for PSS configurators in the domain of repurposing used EVBs. Furthermore, we use the results to triangulate design decisions made when developing the first prototype.

The remainder of this article is structured as follows. In Section 2 we provide an overview of the research background regarding the repurposing of used EVBs and Product-Service Systems. Afterwards, we present the used methodology, followed by the results of the literature analysis in Section 4. In Section 5 the identified principles are discussed for the domain of repurposing used EVBs. Section 6 concludes the paper and suggests some opportunities for further research.

2 Research Background

2.1 Product-Service Systems

A Product-Service System is the combination of physical products and additional services that are marketed together as an integrated solution that fulfills the needs of individual customers [12]. Some authors, esp. in earlier publications on PSSs, additionally highlight the aspect of environmental gains that have to be achieved through PSSs (e.g., [7]), but this aspect is not present in all definitions (e.g., [12]).

PSSs can be classified into different types that are distinguished by the level of integration of services. Tukker [13] identifies eight types of PSS in the three categories product-oriented, use-oriented, and result-oriented PSS. While the product-oriented PSSs focus on selling a product with additional services that increase the value for the customer, in use-oriented PSS the products remains the property of the provider and only the access to the products is offered. This includes the leasing or renting of products to one customer as well as pooling in which several customers use the same product simultaneously. The result-oriented types include payment per service unit (e.g., per hour) as well as the functional result (e.g., savings on the energy bill) [13]. Since the product remains the property of the seller in use- and results-oriented PSSs, the seller is responsible for the correct function and takes the risk of malfunction.

For the offering of PSSs, it is necessary to design them. Typically, such designs are modular and have to be configured for the specific customer needs [14, 15]. Configurators (also called configuration systems) are ISs that support during the configuration process.

2.2 Repurposing used Electric Vehicle Batteries

Electric vehicle batteries (EVBs) are one of the main components of electric vehicles, like electric passenger cars. They are needed to store and provide the necessary energy to propel the vehicle. Since the current lithium-ion battery technology suffers from degradation within time and use, the performance of batteries decreases. Currently, it is assumed that an EVB should be removed from the vehicle when its capacity has dropped to around 70%-80% of the original capacity [4, 5]. However, since the automotive use is very demanding, even the degraded batteries are still good enough to be repurposed and further used in less demanding applications [16, 17], such as buffer storage for renewable energy or grid stabilization [18, 19]. Because of the high prices for EVBs, marketing for SLAs can be beneficial by bringing in additional revenues

[20]. Furthermore, there are savings in recycling costs, since currently it is expensive to recycle large lithium-ion battery packs [6], but is supposed to drop in the future because of economies of scale. Additionally, currently, very few companies are even able to handle higher amounts of large battery packs. The demand for batteries will also increase because of the rising share of renewable energy (i.e., wind and solar energy) that cannot be leveled as combustion based energy sources (i.e., coal or gas). So, batteries can be used to store energy when there is an overproduction of renewables that can then be used when the demand is higher than the production [21]. One other effect of this transformation towards renewable energy is the increase in the number of energy generators. Larger power plants are replaced by smaller, decentralized ones thus far as that private households with photovoltaic panels feed energy into the grid. This upcoming decentralization of supply needs for additional storage for stabilization [21].

While the technical feasibility of different SLAs is intensively under research ([9, 22]), the economic perspective is mostly reduced to calculations if certain applications are economically feasible (e.g., [23–25]). There is nearly no research on markets for used EVBs or their marketing. Consequently, research on IS support is still scarce.

Previous research from our research group shows that used EVBs can be offered as PSSs consisting of one or more used EVBs and additional services. PSSs are a way to reduce the customer's risk of acquiring used EVBs that arises from the fact that the potential customer is not able to assess the quality of the offered used EVBs and estimate their future degradation [2]. Furthermore, PSSs can improve the value for the customer by including services that are required for a safe start-up and operation as well as additional services that improve the customer experience. Additionally, PSSs can improve the cost-efficiency for the customers [2].

The solutions offered to a customer have to satisfy certain dependencies. First, there are dependencies between the components of the PSS (i.e., services and products). For example, a particular type of used battery might require a specific service. Second, there are dependencies to the specific SLA scenario of a customer. For example, a battery that is repurposed for the usage in a private household has to be complemented by different services and electrical components than a larger storage that is run by a company with battery experts. However, the specific dependencies are unknown and are likely to change with developments in the technology.

The repurposing of used EVBs will likely be done by specialized companies that receive the EVBs from the manufacturers and configure the PSSs for the customers [26]. On a high level the decision process consists of the following steps: Identify technically feasible batteries for given customer requirements, configure different PSSs that solve the customer problem, and offer them to the customers [11].

3 Research Method

In this study, a systematic literature review on configuration systems for PSS is conducted in line with Webster & Watson [27] and vom Brocke et al. [28]. First, a keyword search in three databases was performed. The review is exploratory to identify concepts and functionalities of current PSS configurators. Therefore, we queried

scientific databases using a search string[1] that combines the different objects of investigation (i.e., PSS, product, and service) with various terms for configuration systems. Additionally, the term "knowledge-based configuration," which is mainly used in the context of artificial intelligence, was included. The databases and corresponding hits of the search that was performed in 08/2017 are shown in Table 1.

Table 1. Database query configuration and results

Database	*Configuration*	*Hits*	*Cleaned*	*Relevant*
Scopus	Article title, Abstract, Keywords	9	7	0
AISeL	All Fields	125	18	4
Google Scholar	No patents, no citations	204	15	9

The raw results were cleaned by first removing invalid entries (e.g., complete proceedings) and screened regarding their relevance based on the title and abstract. Additionally, articles from non-peer reviewed outlets were deleted. In a second step, the full texts of the remaining papers were read regarding whether they deal with configuration systems for PSS or service bundles. Since some configurators were described in more than one article, in the end, 13 articles were considered relevant for this study and nine configuration systems for service bundles and product-service systems were identified. Table 2 provides an overview of the identified configurators, referring articles, and whether they are supposed to be used for configuring PSSs or service bundles. In some of the articles, the term PSS is not explicitly used but describe the same construct [10, 15, 29].

Table 2. Overview of configurators and corresponding articles

ID	*Sources*	*Type*
C1	[10, 15, 29]	PSS
C2	[30, 31]	Service bundles
C3	[32, 33]	PSS
C4	[34]	Service bundles
C5	[35]	PSS
C6	[36]	PSS
C7	[37]	PSS
C8	[38]	PSS
C9	[39]	PSS

Afterwards, the results of the literature analysis are discussed regarding their suitability in the targeted domain.

[1] (("service bundle" OR "product service system" OR "hybrid product" OR "product" OR "service") AND ("configurator" OR "configuration system" OR "choice navigator") OR "knowledge-based configuration")

4 Product-Service System Configurators

In the analyzed literature, several concepts and functionalities of configurators can be identified (Table 3). All configurators have a knowledge base that contains information on whether a configuration is valid or not. Typically, this knowledge base is represented as one or more ontologies [30–33, 36, 39] (C2-C4, C6, C9) or using a specific modeling language or meta-model [29, 38] (C1, C8). For the other two, the structure of the knowledge base is not described in the analyzed articles.

In these knowledge bases, different types of dependencies are considered to describe valid configurations and are represented as configuration rules [29, 35]. The dependencies differ in the elements between which the dependencies occur and the type. For example, a certain product component might require the inclusion of a specific type of services Basic dependency types are "require" and "incompatible" [33]. For example, the inclusion of a certain product in the PSS might require or prohibit the inclusion of the particular type of service. Most configuration systems additionally allow the definition of other relationships between the different elements to enable more detailed configuration rules (C1-C4, C6, C9), such as "enhancing," "substitutes," or "supporting." For the others, it is unknown how the dependencies are modeled.

One concept in which the configurators differ is the targeted type of user. Most common is a technical or sales representatives of the vendor that configure PSSs for a specific customer (C1, C4, C7) or the customer can itself be the user of the system (C1, C5, C7, C8). Depending on the targeted group of users, the user interface and the amount of decision support that has to be offered differs. Especially in a complex domain, the customers will not have the necessary knowledge to configure a solution on their own if the support provided by the system is low [15]. Therefore, configurators include several functionalities that aid the user in the configuration task. Most commonly is the validation of configurations using the knowledge base (C1-C6, C9).

Some of the configurators additionally can identify valid solutions for customer preferences (C1-C4, C9). A prerequisite for this is that the customer can state its preferences, that the preferences are represented in the system, and that a matching between the preferences and the PSS elements can be made. To allow automatic configuration, the preferences have to be related to the PSS elements All configurators use explicitly stated relations between preferences and outcomes that can be realized by either product or service components (C1, C2, C3, C4, C9).

To provide further assistance, configurators can include recommender systems that recommend services or outcomes that are likely to be needed by the customer. For example, one configurator includes a collaborative filtering recommender (C1) [10]. Such recommender systems can be based on data gathered from previously sold PSSs or data acquired during the use in a SLA. Even if no recommender system is included in the configurator, a feedback mechanism for such data is reasonable to improve the PSS offerings (C6, C8) [35, 38].

For the vendor of PSSs, it is important to determine how much a certain PSS will cost and which price can be asked for. Therefore, some of the configurators include functions to propose prices (C1, C4, C5, C6) and to provide the possibility to calculate

the costs for the vendor (C1). Different pricing schemes, such as path auctions [34] or willingness-to-pay and competitor price analyses [10], are used.

Apart from the configuration task itself, it can be reasonable to provide the customer with different variants of configured PSSs. Therefore, some configurators include the functionality to oppose and contrast different variants. C1 provides the possibility to generate total cost of ownership calculations for various PSSs [15]. An additional feature incorporated by one configurator (C8) is collaborative work that allows the involvement of different actors in the design and configuration of PSSs [38].

Overall, while there are few advanced configurators (C1, C4), some are only rudimentary implemented in generic rule engines to demonstrate ontologies on which the configurators are based on (C3, C6, C9). The configurators C5 and C7 are described on an abstract level so that some conclusions cannot be made regarding all concepts.

It is noticeable that even though some configurators are especially for PSSs, none of them explicitly incorporates the distinction between the different types of PSS.

Table 3. Concepts of PSS Configurator design

Concept	*Form*	*Configurator(s)*
Knowledge-representation		
	Ontology	C2 – C7, C9
	Meta-model	C1, C8
Dependencies		
	Between services and products	C1, C9
	Between products	C1, C2, C5, C9
	Between services	C2, C3, C4, C6
Targeted User		
	Vendor	C1, C4, C7
	Customer	C1, C5, C7, C8
Functionality		
	Validation of configuration	C1-C6, C9
	Matching needs	C1-C4, C6, C9
	Recommendation of services	C1
	Feedback mechanism	C1, C5, C8
	Costing	C1
	Pricing	C1, C4 – C6
	Comparison of variants	C1
	Collaborative work	C8

5 Principles for PSS Configuration Systems for Repurposing EVBs

Various challenges arise for configuring individual PSSs consisting of used EVBs and additional services. First, a technically suitable battery has to be found satisfying some of the customer's requirements. Additionally, services have to be identified which

either are mandatory or provide additional value for the customer.Also, the PSS can contain additional hardware (e.g., for monitoring) that is not required for the operation but can be used for optimization or to enable different revenue streams [40].

In the literature, various dependencies were identified. Dependencies can occur between the different elements of a PSS (i.e., products and services). However, in the domain of repurposing used EVBs additional dependencies between the PSS elements and the SLA scenario exist. For example, if a single used EVB is installed as buffer storage in a house with photovoltaic panels there are other additional product components needed than for application in a larger energy storage in that many used EVBs are connected. Therefore, the knowledge base has to account for this specific type of dependencies.

In current configurators two ways of knowledge representation are used, ontologies and specific meta-models. Potentially both can be utilized in the domain of repurposing used EVBs. There is a lot of different dependencies inside and outside the PSS that because of the newness of the domain cannot be specified exactly. Therefore, the representation has to be flexible regarding additional constraints.

Because of the complexity of the used good, a customer is likely missing knowledge to configure the solution on its own. Therefore, a technical sales representative of the vendor should configure the solution in cooperation with the customer or by itself based on the preferences articulated by the customer [15]. When the whole domain of repurposing used EVBs becomes more mature, and the products are standardized an e-commerce like setting might become feasible in that the customers can configure their solutions by themselves. For both settings, validation of configurations regarding the dependencies is a functionality that is inevitable for strong support in the configuration task and should be incorporated in configurators for used EVBs.

Automated matching between needs and requirements of the customer and the SLA scenario would bring additional support. However, this requires formalization of those needs and an assignment between needs and the PSS elements have to be formulated. Because of the newness of the domain, such a formalization currently does not exist. Furthermore, because of the complexity of the domain, the customer might not even be aware of its particular needs. Until this additional knowledge is present, the configuration has to be done by sales representatives. Another possibility is the incorporation of recommender systems as present in one configurator. In particular, a collaborative filtering approach that recommends services based on PSSs that previously were successfully sold to similar customers is proposed. This concept can be extended towards similar SLA scenarios and similar used EVBs [11]. Using this approach the person who configures the PSS gets recommendations regarding services that are likely to be successfully sold. This approach works around the problem of not having formalized knowledge about the relationship between specific needs and PSS elements. Such a recommender system also can be used to generate different variants that can be offered to the customer [11].

To train such a recommender system, a feedback mechanism is needed as proposed in three of the identified configurators. In this particular case data about previously sold PSS have to be stored. Apart from that feedback mechanisms are reasonable since the whole domain of repurposing used EVBs is still new and only little is known about

successful SLA scenarios. While there are currently many research projects regarding the technical feasibility and battery degradation in different SLAs, there is not much on successful sales. With an evolving market, it will become beneficial for the vendors to track the usage of the battery and services to improve the product and service offering.

Determining costs and pricing of services is not easy because of the process and co-creation characteristics. In the domain of repurposing used EVBs, the services most likely will be provided by different service providers. Therefore, the aspect of costing could be transferred to the providers. That would require an interface to retrieve specific costs. Pricing is necessary only to allow profitable PSS. Therefore, such a functionality should also be present for repurposing used EVBs.

There are likely different possible PSSs that solve a specific customer's problem [14]. The customers should be able to choose between offers with different value propositions and costs. Therefore, it should be possible for the customer to oppose different variants. E.g., this could be operationalized using a web-based interface (C1).

Collaborative work is another functionality that is incorporated in one of the configurators. Different persons can design and configure PSSs simultaneously [38]. For repurposing used EVBs that will be required since several decisions makers might be involved in the decision process [11]. The selection of a suitable battery might be performed by a different person than the configuration of the PSS. Additionally, since a large amount of used EVBs will be available in the future, many PSSs will have to be configured, and therefore it is necessary to balance the task between different persons.

One concept that is not present in current configurators is the type of PSS. No configurator explicitly consider use- or result-oriented PSSs. Different types of PSSs should be explicitly supported by the configurator since the type has an influence on the functionality (e.g., pricing) and has to be represented by additional constraints in the knowledge base. For used EVBs this would be beneficial since use- and result-oriented PSSs are a way to reduce the risks for the customer and stimulate sales [2]. Battery aging is highly complex the estimation of future degradation is challenging, and profound knowledge of the batteries and their usage history are necessary [8]. For potential buyers of used batteries, it is not possible to identify the quality of the offered product. Furthermore, there is asymmetric information since the seller typically has more information on the quality. According to Principal-Agent Theory, this can lead to adverse selection. To solve this, the seller has to signal the battery's quality or risks market failure as demonstrated in the Lemon Market Theory [8]. One possibility to solve this issue is to transfer the danger of a "bad" battery to the seller. E.g., by providing warranties in a product-oriented PSS or offering use- and result-based PSSs.

The identified concepts and functionalities correspond with the principles identified from domain knowledge for the development of our first prototype [11]. Some of the concepts offer possibilities to extend the solution by incorporating new functionality. Specifically, the system should be adopted for use- and result-oriented PSSs to provide additional possibilities to solve the problem of potential adverse selection. Furthermore, an automatic matching of customer preferences and outcomes could be added. This requires certain information in the knowledge base that is not yet available but would enable customers to configure PSSs themselves. Pricing currently is only implemented rudimentary using a cost-based approach that uses costs for services.

6 Conclusion and Outlook

Product-Service Systems consisting of the used battery and additional services are a possibility to account for asymmetric information, reduce risks for the customer, and provide customers with individual solutions. The configuration of PSS can be complex. Therefore IS are needed to assist the vendor of such PSSs. To inform the design of such an IS, we first performed a structured literature review of existing systems. The results were discussed in a second step for their reasonability for configurators for repurposing used EVBs. Most of the identified concepts and functionalities can be adapted for this domain. However, due to missing knowledge about the future of the technology and specific services that will be required, some are not applicable right now.

In our design science research project the results will be used to refine and extend the design of the existing prototype in a next iteration. For other researchers, the results provide an overview of current research on PSS configurators and their concepts and functionality. Practitioners can use the results as a starting point for their design.

Limitations of the research are only considering existing configurators and methods for PSS development and configuration were neglected. Another limitation and opportunity for further research is that literature on product configurators and knowledge-based configuration is not systematically included in this study. While those two areas mainly deal with support in configuring product alternatives to enable mass-customization strategies, there are several similarities regarding the goals and concepts. Since product configuration is more researched than service or PSS configuration, it can be worth it to analyze which aspects and solutions in this area can be transferred.

7 Acknowledgement

This paper was written within the research project “EOL-IS,” which was funded by the German Federal Ministry for Education and Research (BMBF) (funding label: 02K12A042). We thank the Projektträger Karlsruhe (PTKA) for their support.

References

1. Dijk, M., Orsato, R.J., Kemp, R.: The emergence of an electric mobility trajectory. Energy Policy. 52, 135–145 (2013).
2. Bräuer, S.: They Not Only Live Once – Towards Product-Service Systems for Repurposed Electric Vehicle Batteries. In: Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI) 2016. pp. 1299–1310 (2016).
3. Foster, M., Isely, P., Standridge, C.R., Hasan, M.M.: Feasibility assessment of remanufacturing, repurposing, and recycling of end of vehicle application lithium-ion batteries. J. Ind. Eng. Manag. 7, 698–715 (2014).
4. Saxena, S., Le Floch, C., MacDonald, J., Moura, S.: Quantifying EV battery end-of-life through analysis of travel needs with vehicle powertrain models. J. Power Sources. 282, 265–276 (2015).

5. Keeli, A., Sharma, R.K.: Optimal use of second life battery for peak load management and improving the life of the battery. In: Proceedings of the 2012 IEEE International Electric Vehicle Conference. pp. 1–6 (2012).
6. Richa, K., Babbitt, C.W., Gaustad, G.: Eco-Efficiency Analysis of a Lithium-Ion Battery Waste Hierarchy Inspired by Circular Economy. J. Ind. Ecol. 21, 715–730 (2017).
7. Mont, O..: Clarifying the concept of product–service system. J. Clean. Prod. 10, 237–245 (2002).
8. Beverungen, D., Klör, B., Bräuer, S., Monhof, M.: Will They Die Another Day? A Decision Support Perspective on Reusing Electric Vehicle Batteries. In: Proceedings of the 23rd European Conference on Information Systems (ECIS 2015) (2015).
9. Ahmadi, L., Young, S., Fowler, M., Fraser, R., Achachlouei, M.: A cascaded life cycle: reuse of electric vehicle lithium-ion battery packs in energy storage systems. Int. J. Life Cycle Assess. 1–14 (2015).
10. Becker, J., Beverungen, D., Knackstedt, R., Müller, O.: Pricing of Value Bundles: A Multi-Perspective Decision Support Approach. Enterp. Model. Inf. Syst. Archit. 6, 54–69 (2011).
11. Klör, B., Monhof, M., Beverungen, D., Bräuer, S.: Recommendation and Configuration of Value-Added Services for Repurposing Electric Vehicle Batteries: A Vertical Software Prototype. In: Proceedings of the 19th IEEE Conference on Business Informatics (2017).
12. Baines, T., Lightfoot, H., Peppard, J., Johnson, M., Tiwari, A., Shehab, E., Swink, M.: Towards an operations strategy for product- centric servitization. Int. J. Oper. Prod. Manag. 29, 494–519 (2009).
13. Tukker, A.: Eight types of product–service system: eight ways to sustainability? Experiences from SusProNet. Bus. Strateg. Environ. 13, 246–260 (2004).
14. Shen, J., Erkoyuncu, J.A., Roy, R., Wu, B.: A framework for cost evaluation in product service system configuration. Int. J. Prod. Res. 55, 6120–6144 (2017).
15. Becker, J., Beverungen, D., Knackstedt, R., Müller, O.: Model-Based Decision Support for the Customer-Specific Configuration of Value Bundles. Enterp. Model. Inf. Syst. Archit. 4, 26--38 (2009).
16. Casals, L.C., García, B.A.: Assessing Electric Vehicles Battery Second Life Remanufacture and Management. J. Green Eng. 6, 77–98 (2016).
17. Burke, A.: Performance, Charging, and Second-use Considerations for Lithium Batteries for Plug-in Electric Vehicles. Research Report UCD-ITS-RR-09-17. Institute of Transportation Studies, University of California, Davis, CA, USA (2009).
18. Knowles, M.J., Morris, A.: Impact of Second Life Electric Vehicle Batteries on the Viability of Renewable Energy Sources. Br. J. Appl. Sci. Technol. 4, 152–167 (2014).
19. Schuster, S.F.: Reuse of Automotive Lithium-Ion Batteries : An Assessment from the Cell Aging Perspective, (2016).
20. Elkind, E.N.: Reuse and Repower: How to Save Money and Clean the Grid with Second-Life Electric Vehicle Batteries. Technical Report, UCLA School of Law, LA, CA, USA (2014).
21. Lund, H., Andersen, A.N., Østergaard, P.A., Mathiesen, B.V., Connolly, D.: From electricity smart grids to smart energy systems - A market operation based approach and understanding. Energy. 42, 96–102 (2012).
22. Gohla-Neudecker, B., Bowler, M., Mohr, S.: Battery 2nd life: Leveraging the sustainability potential of EVs and renewable energy grid integration. In: Proceedings of the 2015 International Conference on Clean Electrical Power (ICCEP). pp. 311–318 (2015).

23. Heymans, C., Walker, S.B., Young, S.B., Fowler, M.: Economic analysis of second use electric vehicle batteries for residential energy storage and load-levelling. Energy Policy. 71, 22–30 (2014).
24. Kantor, I., Rowlands, I.H., Parker, P., Lazowski, B.: Economic feasibility of residential electricity storage systems in Ontario, Canada considering two policy scenarios. Energy Build. 86, 222–232 (2015).
25. Assunção, A., Moura, P.S., de Almeida, A.T.: Technical and economic assessment of the secondary use of repurposed electric vehicle batteries in the residential sector to support solar energy. Appl. Energy. 181, 120–131 (2016).
26. Klör, B., Beverungen, D., Bräuer, S., Plenter, F., Monhof, M.: A Market for Trading Used Electric Vehicle Batteries - Theoretical Foundations and Informations Systems. In: Proceedings of the 23rd European Conference on Information Systems (ECIS 2015) (2015).
27. Webster, J., Watson, R.T.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. Manag. Inf. Syst. Q. 26, (2002).
28. Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. Commun. Assoc. Inf. Syst. 37, 205–224 (2015).
29. Becker, J., Beverungen, D.F., Knackstedt, R., Mueller, O.: Modeling, Customer-Specific Configuration and Calculation of Bundles. AMCIS 2008 Proc. (2008).
30. De Kinderen, S., Gordjin, J.: E3-Service - A Model-Based Approach for Generating Needs-Driven E-Service Bundles in a Networked Enterprise. In: ECIS 2008 Proceedings (2008).
31. Razo-Zapata, I.S., Gordijn, J., de Leenheer, P., Wieringa, R.: e 3 service: A Critical Reflection and Future Research. Bus. Inf. Syst. Eng. 57, 51–59 (2015).
32. Shen, J., Wang, L., Sun, Y.: Configuration of product extension services in servitisation using an ontology-based approach. Int. J. Prod. Res. 50, 6469–6488 (2012).
33. Shen, J., Wu, B.: Service Configuration Knowledge Representation and Reasoning Based on a Hybrid Approach. In: Proceedings of the 2013 International Conference on Service Sciences (ICSS). pp. 224–229 (2013).
34. Blau, B., Michalk, W., Neumann, D., Weinhardt, C.: Provisioning of Service Mashup Topologies. ECIS 2008 Proc. (2008).
35. Smirnov, A., Shilov, N., Oroszi, A., Sinko, M., Krebs, T.: Application-Driven Product-Service System Configuration: Customer-Centered Strategy. In: Proceedings of the 5th International Conference on Serviceology for Services. pp. 26–37 (2017).
36. Dong, M., Yang, D., Su, L.: Ontology-based service product configuration system modeling and development. Expert Syst. Appl. 38, 11770–11786 (2011).
37. Meier, H., Massberg, W.: Life cycle-based service design for innovative business models. CIRP Ann. - Manuf. Technol. 53, 393–396 (2004).
38. Matsas, M., Pintzos, G., Kapnia, A., Mourtzis, D.: An Integrated Collaborative Platform for managing Product-service Across their Life Cycle. Procedia CIRP. 59, 220–226 (2017).
39. Wang, P.P., Ming, X.G., Wu, Z.Y., Zheng, M.K., Xu, Z.T.: Research on industrial product–service configuration driven by value demands based on ontology modeling. Comput. Ind. 65, 247–257 (2014).
40. Beverungen, D., Bräuer, S., Plenter, F., Klör, B., Monhof, M.: Ensembles of Context and Form for Repurposing Electric Vehicle Batteries: An Exploratory Study. Comput. Sci. - Res. Dev. (2017).

Nutzeranforderungen an mobile Applikationen für NFC-basierte eTickets im ÖPNV

Andreas Kreisel, Denise Rummler, Gertraud Schäfer und Ulrike Stopka

Institut für Wirtschaft und Verkehr, Technische Universität Dresden, Germany
{andreas.kreisel, denise.rummler, gertraud.schaefer,
ulrike.stopka}@tu-dresden.de

Zusammenfassung. Im Rahmen des OPTIMOS-Projekts wird ein offenes und für die praktische Anwendung einsatzbares IT-basiertes Ecosystem entwickelt. Ein wesentlicher Teil dieses Systems ist das eTicketing auf Basis der NFC-Technologie unter Nutzung elektronischer Identitäten. Bei der Entwicklung einer Applikation für die Anwendung des Systems liegt der Fokus auf der nutzerzentrierten Gestaltung. Diese Arbeit fasst die Ergebnisse der ersten Nutzerstudien zusammen.

Schlüsselwörter: Mobilitätsapplikation, Nutzeranforderungen, Öffentlicher Verkehr, Usability

1 Motivation

Das Smartphone dient als Türöffner in eine digitale Welt mit vielfältigen Einsatzmöglichkeiten, wodurch unser Alltag mehr und mehr von digitalen Anwendungen und Diensten durchdrungen wird. Smartphones bieten eine einfache und für die Nutzer jederzeit verfügbare Möglichkeit, in Echtzeit wichtige Informationen abzurufen und Aktionen zu tätigen. Im Öffentlichen Personennahverkehr (ÖPNV) nutzen Kunden ihre Smartphones zur Verbindungsauskunft, zum Routing und zum Ticketkauf. Laut einer Erhebung von SPLENDID RESEARCH im Frühjahr 2017 nutzen rund 66 % der befragten Personen im Abdeckungsgebiet der zehn größten deutschen Verkehrsverbünde ihr Smartphone für die Fahrplanauskunft. Ca. 23 % der Befragten erwarben mit ihrem Smartphone bereits Tickets innerhalb ihres Nahverkehrsbereichs [9]. Im Frühjahr 2017 testete die STIFTUNG WARENTEST fünf der gängigen deutschlandweiten Mobilitätsapps [10]. Bei der Bewertung der Bedienbarkeit gab es einige Mängel. So werden z. B. bei einigen Applikationen nur wenige Alternativen zu Fahrtrouten angezeigt. Bei anderen fehlt die Informationen zum Fahrpreis komplett. Als großer Mangel ist anzusehen, dass elektronische Tickets in keiner der Apps gekauft werden können. Lediglich eine App bietet dies über eine Weiterleitung zu Partnerseiten an [11].

Gleichwohl bleibt ungeklärt, welche konkreten Anforderungen Nutzer an eine solche Applikationen haben. In einem Teilbereich des Projekts OPTIMOS wurden diese Nutzeranforderungen genauer untersucht. Die Ergebnisse werden in diesem Artikel vorgestellt und eingeordnet.

2 Projekt OPTIMOS

Das Projekt „Open, Practical Infrastructures for Mobile Services“ (OPTIMOS) möchte mit Hilfe der Near Field Communication (NFC)-Technologie eine Verbindung zwischen dem nationalen ÖPNV und der mobilen Kommunikation herstellen. Das Ziel ist die Entwicklung und prototypische Umsetzung eines offenen, praxistauglichen Ecosystems.

Die NFC-Technologie bietet in Kombination mit einem in die Mobilfunkarchitektur integrierten Secure Element die Möglichkeit, die insbesondere von den deutschen ÖPNV-Unternehmen geforderten hohen Sicherheits- und Datenschutzstandards zu erfüllen. Die vergleichsweise geringe Übertragungsreichweite und das Einbinden des Secure Elemets in die Sicherheitsarchitektur verhindern Missbrauch. Darüber hinaus ist das Auslesen der Fahrscheindaten, bspw. durch Kontrolleure, auch bei ausgeschalteten Smartphone möglich. Zudem besteht die Möglichkeit, dass übertragbare Tickets zwischen verschiedenen NFC-fähigen Geräten und Smartcards kopier- und fälschungssicher übergeben werden können. Diese Funktionalitäten bieten ÖPNV-Unternehmen die Möglichkeit, insbesondere Zeitfahrkarten mit ihren individuellen Eigenschaften elektronisch nachzubilden und online zu verkaufen.

Das Projektteam arbeitet eng mit internationalen Standardisierungsgremien, wie bspw. dem European Committee for Standardization (CEN), der GSM Association (GSMA) und dem NFC-Forum, zusammen. Dadurch soll eine hohe Akzeptanz bei Nutzern bzw. Fahrgästen, Transportunternehmen, Mobilfunknetzbetreiber und Endgeräteherstellern erreicht werden. Dieses interdisziplinäre Projekt mit Partnern aus der IT-Sicherheit, Mobilfunk- und Nahverkehrsbranche wird durch das Bundesministerium für Wirtschaft und Energie gefördert.

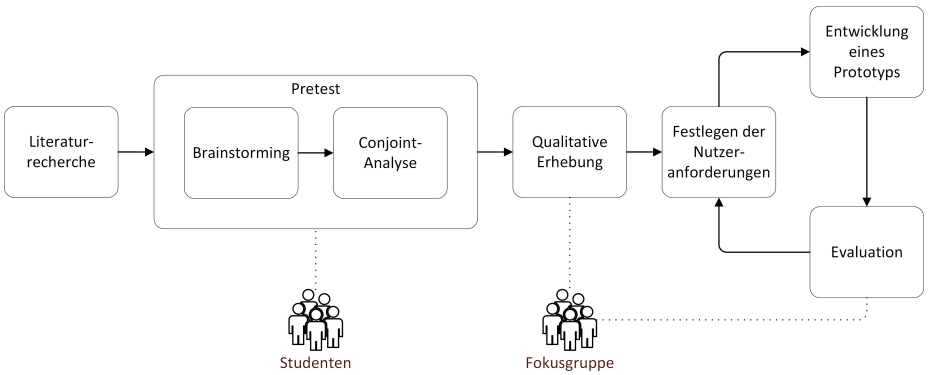


Abb. 1. Ablaufplan zur Entwicklung eines Konzeptes für die Evaluation der Nutzeranforderungen und -akzeptanz

Die Technische Universität Dresden übernimmt im Projekt OPTIMOS die wissenschaftliche Begleitforschung. Sie soll gewährleisten, dass in die Entwicklung der interaktiven Applikation möglichst viele Nutzeranforderung einfließen und die Prototypen regelmäßig evaluiert werden. Um dieses Ziel zu erreichen, wurde ein Konzept entwickelt, das stark an die Vorgaben der DIN EN ISO 9241-210 angelehnt ist [2]. Abbildung1skizziert grob das Vorgehen.

Nach einer ausführlichen Literaturrecherche zu bereits bekannten Nutzeranforderungen an ähnliche Systeme wurde eine explorative Vorstudie durchgeführt. Diese bestand aus einem ungestützten Brainstorming zu Nutzeranforderungen an mobile Applikationen im ÖPNV mit einer Gruppe von ca. 30 zufällig ausgewählten Studierenden. Bei der Auswertung wurde deutlich, dass die Probanden nur auf bereits bekannte und benutzte Funktionen eingingen. Um die Bedeutung und Wichtigkeit einzelner Merkmale zu bestimmen, wurde mit den Probanden anschließend eine Conjoint-Analyse durchgeführt[1].

Die Ergebnisse der Vorstudie bilden die Basis für die anschließende qualitative Erhebung. Sie zeigten aber auch, dass die gewählten Methoden eher zu einer Validierung bereits bekannter Erfahrungen passen und nur bedingt zur Ermittlung von Nutzeranforderungen an noch zu entwickelnde Applikationen geeignet sind. Gerade aber letztere müssen identifiziert werden, um den Zielen des OPTIMOS-Projekts gerecht zu werden.

3 Qualitative Erhebung von Nutzeranforderungen

Mit dem Ziel der Ermittlung möglichst unverfälschter Anforderungen der Testnutzer an mobile Applikationen und unter Berücksichtigung der Ergebnisse des Pretests wurden verschiedene qualitative Erhebungsinstrumente kombiniert. Diese sind in Abbildung2dargestellt.

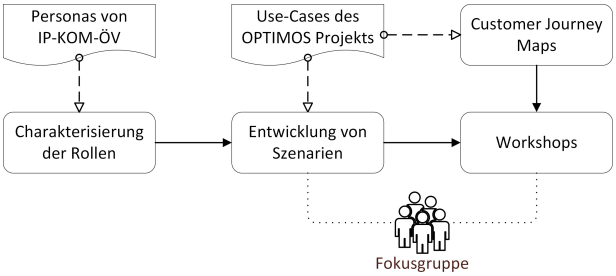


Abb. 2. Schematische Vorgehensweise bei der qualitativen Erhebung der Nutzeranforderungen

[1] Eine ausführliche Darstellung der Ergebnisse der Literaturrecherche, des Brainstormings und der Conjoint-Analyse kann aus SCHÄFER et. al. entnommen werden [6].

3.1 Konzeption und Ablauf

Personas. Zur Beschreibung typischer Vertreter einer Zielgruppe werden *Personas* verwendet. Bei *Personas* handelt es sich um „archetypische Nutzer, deren Bedürfnisse möglichst anschaulich und realitätsnah bestimmt werden“ [7]. Sie spiegeln keine durchschnittliche Person wider, sondern stellen vielmehr spezifische Anwender mit speziellen Wünschen und Zielen dar [8].

Das Projekt IP-KOM-ÖV entwickelte im Jahr 2012 *Personas* mit ÖPNV-Profil[2] mit den Aspekten „Ortskenntnis“, „ÖPNV Systemkenntnis“, „Einschränkungen bei der Nutzung“, „Verfügbarkeit von Alternativen“ und „Ticketverfügbarkeit“. Sie basieren auf den Wünschen und Eigenschaften unterschiedlicher Fahrgasttypen in Kombination mit statistischen Analysen, Experteninterviews und Fokusgruppen [3,6].

Für die Erhebung der Nutzeranforderungen an die OPTIMOS-Applikation wurden fünf Personas modifiziert. Die Eigenschaften „Ortskenntnis“, „ÖPNV Systemkenntnis“ und „Ticketverfügbarkeit“ wurden übernommen und um den Aspekt „Tarifkenntnis“ ergänzt.

Szenarien. *Szenarien* beschreiben, wie „Nutzer mit einem bestehenden System oder einem geplanten System interagieren“ [8]. Ausgehend von den Use-Cases des OPTIMOS-Projekts wurden für die einzelnen Personas *Szenarien* zu den Themen „Registrierung und Ticketerwerb“ und „Ticket- und Kontoverwaltung“ entworfen. Sie sollen den Probanden dabei helfen, sich in die fiktive Person (Persona) und eine spezielle Situation hineinversetzen zu können [1].

Customer Journey Maps. Aus den Use-Cases wurden zudem *Customer Journey Maps* abgeleitet. Diese sind ein Instrument der klassischen Marktforschung und ermöglichen es, Probanden anschaulich durch einen Anwendungsfall zu führen und die Nutzererfahrungen und -erwartungen an verschiedenen Punkten zu beobachten bzw. abzufragen [4].

In Kombination mit Personas und Szenarien können nun verschiedene Situationen aus mehreren Blickwinkeln betrachtet und so die Erwartungen verschiedener Nutzergruppen erhoben werden.

Workshop. Im Frühjahr 2017 wurden *Workshops* in Berlin mit sechs Teilnehmern und in Düsseldorf mit acht Teilnehmern durchgeführt. Zu dem Zeitpunkt waren alle Probanden bereits mehr als sechs Monate lang Testnutzer beim Projekt OPTIMOS. Dadurch konnten sie im Feldtest schon erste Erfahrungen mit dem NFC-basierten eTicketing sammeln.

[2] Beispielsweise gibt es die *Alltagsnutzerin Martina Grundler*, die drei Kinder hat und täglich den ÖPNV für ihre Erledigungen nutzt oder den *Schulpendler Kevin Schubert*, der täglich mit dem Bus zur Schule fährt [3].

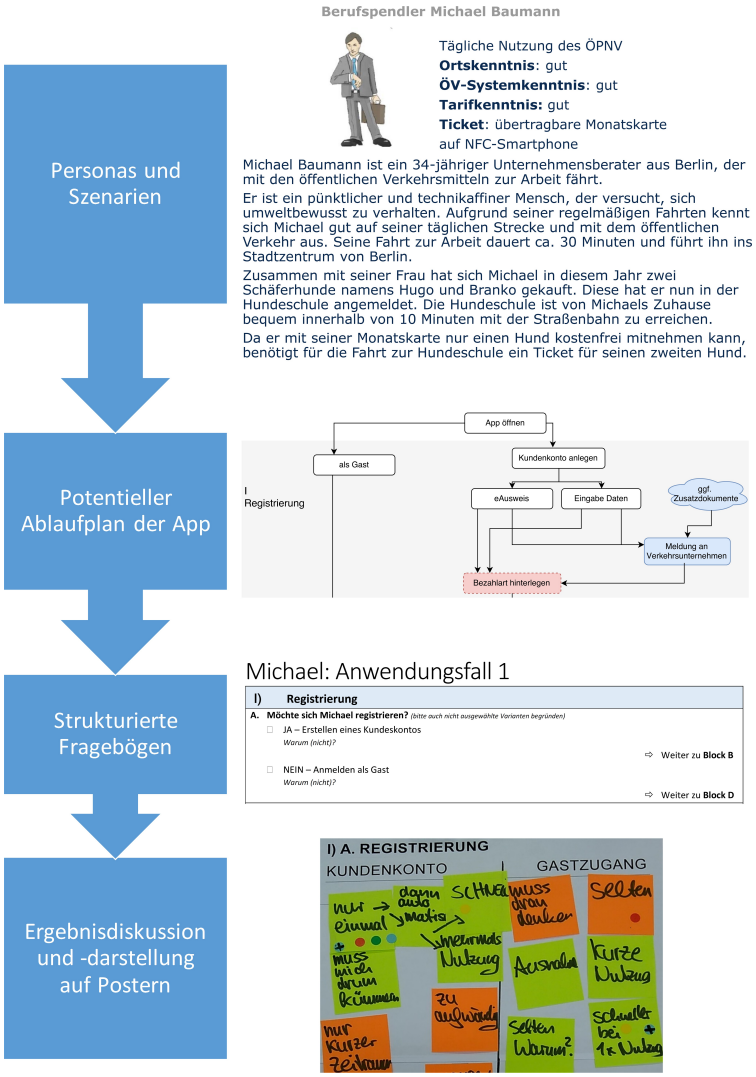


Abb. 3. Ablauf der Workshops in Berlin und Düsseldorf [3,5]

Zu Beginn der *Workshops* wurde jedem Probanden eine Persona samt individuellen Szenario zugelost (siehe Abbildung3oben). Anschließend durchlief jeder Teilnehmer selbstständig die Customer Journey Map aus Sicht seiner Rolle und beantwortete den zugehörigen strukturierten Fragebogen. In ihm wurden an den verschiedenen Punkten zur generellen Nutzung einer App bzw. bei Wahloptionen innerhalb der Menüführung Erfahrungen und Erwartungen, aber auch Unsicherheiten und Ängste abgefragt. In der nachfolgenden Gruppendiskussion wurden die Probanden gebeten, ihre Entscheidungen und Begründungen mit anderen Workshopteilnehmern zu teilen und zu diskutieren. Währenddessen haben die Moderatoren die Argumente zusammengetragen und auf Postern visualisiert (siehe Abbildung3unten). Am Ende des *Workshops* wurde jeder Proband gebeten, die für ihn wichtigsten Argumente mit Moderationspunkten zu kennzeichnen.

3.2 Auswertung und Ergebnisse

Allgemeine Anforderungen. Während der Diskussionen wurden zu verschiedenen Themen bestimmte Argumente mehrmals genannt. Dazu zählen insbesondere Anforderungen an die Usability. Demnach soll eine Applikation einfach, schnell, unkompliziert und vor allem intuitiv sein. Zudem wurde mehrfach der Wunsch geäußert, die Applikation individuell gemäß den eigenen Vorlieben anpassen zu können. Um bessere Auskünfte zu erhalten, sollte eine standortbasierte Routenwahl und -führung möglich sein. Und es wurde gefordert, dass die zur Verfügung gestellten Daten und Informationen strengen Datenschutzregeln unterliegen, um Missbrauch zu verhindern.

Registrierung. Personas, die die Applikation nur selten benutzen, wie bspw. Geschäftsreisende, Touristen oder Gelegenheitsnutzer, möchten sich bei einer spontanen und wahrscheinlich einmaligen Nutzung nicht registrieren, um ein Ticket zu erwerben. Daher soll die Anmeldung mit einem Gastaccount möglich sein. Und es wurde mehrfach der Wunsch nach einem deutschlandweit anwendbaren ÖPNV-Konto geäußert.

Vielfahrer sehen die Vorteile einer Registrierung und die damit verbundenen Komfortfunktionen, wie der schnellerer Kauf eines Tickets, die Ticketverwaltung oder das Hinterlegen von Zahlungsinformationen. Einige Probanden möchten zudem einen Alias anlegen, um dadurch möglichst anonym die Dienste nutzen zu können. Für die Gewährleistung der Sicherheit des Kundenkontos wird ein mehrstufiger Registrierungsprozess gewünscht, z. B. durch ein elektronisches Bestätigungsverfahren. Die Möglichkeit der Hinterlegung der Zahlungsdaten wurde von vielen Nutzern als Komfortgewinn betrachtet, da so die lange IBAN nicht erneut eingetippt werden muss.

Dateneingabe. Für die Sicherstellung der Validität von personengebundenen ÖPNV-Tickets ist zu gewährleisten, dass elektronische Identitäten über die App abgefragt werden können. Die NFC-Technologie lässt eine gesicherte Übertragung der elektronischen Identität des Personalausweises auf ein NFC-fähiges Smartphone zu. Dadurch ist es möglich,



Abb. 4. Genannte Argumente zur Eingabe der Daten beim Workshop in Düsseldorf (links) und Berlin (rechts). Die Anzahl der aufgeklebten Punkte zeigen die Wichtigkeit der Argumente.

bereits während der Registrierung die persönlichen Daten vom elektronischen Personalausweis zu übernehmen. Für diese Variante entschieden sich nur wenige Probanden, obwohl diese Art der Registrierung als schnell, einfach und praktisch angesehen wurde. Häufig wurden Bequemlichkeit[3], Bedenken bezüglich des Datenschutzes oder die mangelnde Verbreitung genannt. Die meisten Probanden haben in ihren Rollen die manuelle Eingabe ihrer Daten vorgezogen. Dies stelle sicher, das nur die Daten übernommen werden, die der Nutzer bewusst eingibt. Gleichzeitig empfanden es einige Probanden als anstrengend und lästig, viele Daten auf den kleinen Displays einzugeben (siehe auch Abbildung4).

Log-in. Die Mehrheit der Personas sprach sich dafür aus, dass ein Teil der Funktionen der Applikation ohne Log-in funktioniert (bspw. die Verbindungsauskunft). Andere Funktionen, wie beispielsweise der Ticketkauf, sollten nur nach einem Log-in möglich sein. Für kleine Zahlungsbeträge soll auf Wunsch des Nutzers auch ein Kauf ohne Log-in ermöglicht werden.

[3] Das Bereithalten der Chipkarte und die Eingabe der PIN wurden als wenig praktikabel bewertet.

Bei der Art des Log-ins bevorzugt der Großteil der Personas die Eingabe von Benutzername und Passwort. Ebenfalls wird das Angebot des Log-in mittels Touch-ID begrüßt. Hingegen wird die Nutzung des elektronischen Personalausweises als zu umständlich empfunden und damit eher abgelehnt.

Für den Abschluss eines Kaufs wünschen sich die registrierten Nutzer eine weitere Kontrollfrage, bspw. eine PIN oder die Verifizierung mittels Touch-ID. Falls der Kunde die Zahlungsdaten bereits hinterlegt hat, sollen diese automatisch vorgeschlagen werden.

Ticketwahl. Die Wahl und der Kauf eines Tickets sollen so schnell, nachvollziehbar und unkompliziert möglich sein (siehe Abbildung5). Grundvoraussetzung ist aber, dass die technischen Systeme dabei zuverlässig funktionieren. Die Nutzer erwarten darüber hinaus einen Vorschlag, welche Ticketart für die gewählte Strecke am geeignetsten ist. Gleichzeitig wird jedoch auch erwartet, dass die Applikation eine manuelle Ticketwahl zulässt. Falls bereits gültige Tickets im System hinterlegt sind, soll dieses automatisch erkennen können, welches zusätzliche Ticket für die gewählte Strecke benötigt wird.

Während beider Workshops gab es Diskussionen über die Entwertung der Tickets. Wird ein Ticket für eine unmittelbar bevorstehende Fahrt erworben, soll dieses sofort entwertet werden. In dem Fall wird ein zusätzlicher Entwertungsvorgang als störend empfunden. Wird jedoch ein Ticket für eine spätere Nutzung im Vorfeld gekauft und in der Applikation gespeichert, ist auch eine Entwertung zum späteren Zeitpunkt zu ermöglichen. Die meisten Nutzer konnten sich mit dem Gedanken der zeitlich versetzten späteren Ticketentwertung

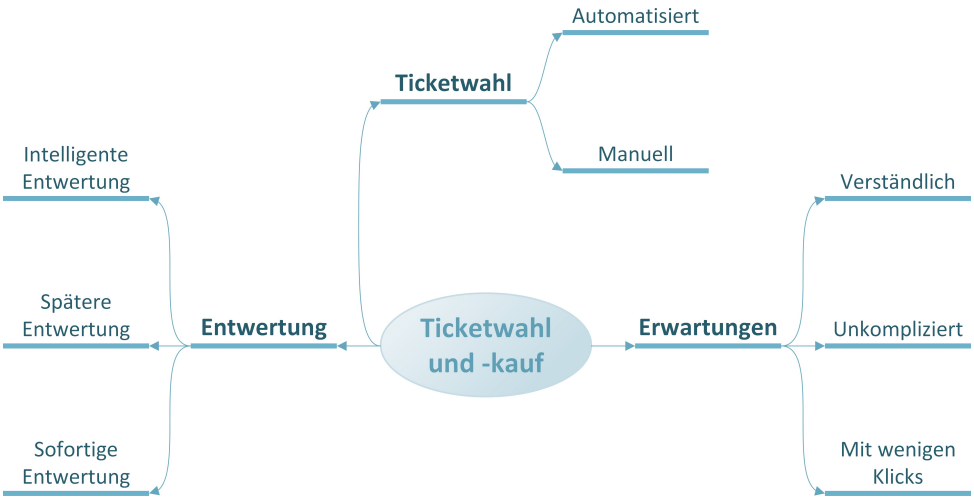


Abb. 5. Diskussionsthemen bei Ticketwahl und -kauf

Tabelle 1. Aufstellung der genannten Argumente zu verschiedenen Bezahlarten (vgl. [5])

Bezahlart	Positiv	Negativ
Lastschrift	EC-Karte weit verbreitet	Nur für registrierte Kunden sinnvoll und nur in Deutschland verfügbar
Kreditkarte	Universal nutzbar (sowohl für Gäste als auch für registrierte Nutzer)	Nummer sehr lang und schwer lesbar
eWallet	Einfach, gewohnt und schnell	Unsicherheit, ob sich Technologie behauptet
Finanzdienstleister	Schnell, sicher und als Prepaid-Konto nutzbar	
Mobilfunkrechnung	Zahlungsdaten bereits hinterlegt	Nicht möglich für ausländische Touristen
Prepaid	Anonym	

anfreunden. Einige Teilnehmer forderten zudem eine intelligente Entwertung, indem die Applikation automatisch erkennt, wenn ein Fahrgast ein entsprechendes Fahrzeug betritt und in dem Moment das Ticket entwertet wird.

Bezahlart. Im letzten Schritt wurden die Nutzer zu ihrer bevorzugten Bezahlart befragt. Eine Aufstellung zu den genannten Vor- und Nachteilen kann Tabelle 1 entnommen werden. Bei der anschließenden Bewertung der Bezahlsysteme mit Moderationspunkten stuften die Probanden das Bezahlen mittels eines Finanzdienstleisters am höchsten ein. Nichtsdestotrotz empfahlen sie, möglichst viele Varianten in der Applikation anzubieten, um jedem Nutzer gerecht zu werden und Nutzungshemmnisse abzubauen.

4 Fazit und Ausblick

Nachdem die ersten Nutzeranforderungen gesammelt und aggregiert worden sind, wird der iterative Entwicklungszyklus der Applikation gestartet werden (siehe Abbildung 1 rechts). Dazu soll im nächsten Schritt ein Prototyp entwickelt werden, der auf diesen Vorgaben basiert. Anschließend wird dieser von den Probanden getestet und im Rahmen einer wissenschaftlichen Begleitforschung evaluiert.

Literatur

1. Brenner, W., und Uebernickel, F.: Design Thinking. Frankfurter Allgemeine Buch (2015)
2. DIN EN ISO 9241-210:2010, Ergonomie der Mensch-System-Interaktion - Teil 210: Prozess zur Gestaltung gebrauchstauglicher interaktiver Systeme

3. Internet Protokoll basierte Kommunikationsdienste im öffentlichen Verkehr: das Begleitheft für den Entwicklungsprozess; Personas, Szenarios und Anwendungsfälle aus AK2 und AK3 des Projektes IP-KOM-ÖV, (2012).https://www.db-thueringen.de/receive/dbt_mods_00019848 (besucht am 28. 11.2017)
4. Nenonen, S., Rasila, H., Junnonen, J.-M., und Kärnä, S.: Customer Journey – a method to investigate user experience. In: Proceedings of the Euro FM Conference Manchester, S. 54–63 (2008)
5. Rummler, D.: Analyse von Nutzeranforderungen an mobile Applikationen für NFC-basierte E-Tickets im ÖPNV. Technische Universität Dresden (2017).
6. Schäfer, G., Kreisel, A., Rummler, D., und Stopka, U.: Development of a Concept for Evaluation User Acceptance and Requirements for NFC Based E-ticketing in Public Transport. In: International Conference on Human-Computer Interaction, S. 522–533 (2017)
7. Semler, J.: App-Design. Rheinwerk Verlag GmbH (2016)
8. Spies, M.: Branded Interactions. Schmidt Hermann Verlag (2012)
9. SPLENDID RESEARCH: Nutzen Sie Ihr Smartphone, um sich über Verbindungen in Ihrer Region zu informieren bzw. Tickets von Ihrem Verkehrsverbund zu kaufen?, hrsg. von Statista. (2017). https://de.statista.com/statistik/daten/studie/713742/umfrage/nutzung-des-smartphones-fuer-informationen-ticket-erwerb-im-oepnv-in-deutschland/(besucht am 27. 11.2017)
10. Stiftung Warentest: Routenplaner: Apps vs. Maps - wer kann mehr?, (2017).https://www.test.de/Routenplaner-Apps-vs-Maps-wer-kann-mehr-5129397-0/(besucht am 29. 09.2017)
11. Weimer, M.: Wenn für Berlin-Hannover ein Taxi für 429 Euro vorgeschlagen wird, (2017).https://www.welt.de/wirtschaft/webwelt/article161798371/Wenn-fuer-Berlin-Hannover-ein-Taxi-fuer-429-Euro-vorgeschlagen-wird.html(besucht am 29. 09. 2017)

Structure for innovations: A use case taxonomy for smart glasses in service processes

Kai Klinker[1], Lisa Berkemeier[2], Benedikt Zobel[2], Hanna Wüller[2], Veronika Huck-Fries[1], Manuel Wiesche[1], Hartmut Remmers[2], Oliver Thomas[2] and Helmut Krcmar[1]

[1] Technical University of Munich, Chair for Information Systems, Munich, Germany
{kai.klinker,veronika.fries,manuel.wiesche, krcmar}@in.tum.de
[2] Osnabrück University, Information Science, Osnabrück, Germany
{lisa.berkemeier,benedikt.zobel,hanna.wueller,remmers,oliver.thomas}@uni-osnabrueck.de

Abstract. The evolution of smart glasses and AR technology holds potential for support of mobile service processes. Yet, little research has focused on systematic identification of potential use cases. In this article, we present a use case taxonomy derived from multiple case studies employing literature search, ethnographies, interviews and focus groups from the domains of nursing, maintenance and logistics. Building upon the identified use cases we propose a framework of task-technology fit for smart glasses. The taxonomy in combination with the framework will allow researchers and practitioners to identify smart glass use cases that are of inter-domain relevance. Moreover, our artefacts enable a structured approach for identification and assessment of potential smart glass use cases without in-depth knowledge of the technology.

Keywords: Smart Glasses, Taxonomy, Service, Health Care, Maintenance, Logistics

1 Introduction

Industrialized countries are experiencing a shift from production to services. 50% of jobs in Brazil, Russia, Japan, and Germany, as well as 75% of the labor force in the United States and the United Kingdom are currently within the service sector [1, 2]. ICTs can facilitate service innovation by playing a dual role, as both an operand (enabler) and an operant (initiator or actor) resource [3]. ICTs are used in combination with other resources (such as skills and knowledge) to leverage information use across different contexts and to create new opportunities for service exchange and for innovation [4]. Several factors complicate digitization efforts of service processes. For many use cases, hands-free interaction with Information Systems is necessary [5]. Reasons for this can be, that both hands are needed for work, hands are dirty or aseptic procedures need to be performed [6]. Thus, many mobile ICTs such as smartphones and smart watches cannot be used in many tasks [7]. As a result,

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

workaround behaviors can often be observed [8, 9]. Furthermore, service processes are often mobile and require mobile networks [10].

The ongoing technological development of smart glasses such as Vuzix, Google Glass or Augmented Reality devices such as Microsoft HoloLens are a promising new direction for the digitization of flexible service processes [11]. Especially in situations where employees perform information-intensive activities, while having to work hands-free, smart glasses can show context-sensitive information in the user's field of view and thereby support employees in their daily work routine [12]. The main potentials for ICT applications to support service processes are expected improvements of performance, process quality, employee satisfaction and IT-enabled collaboration [13, 14]. One of the main problems for current research on smart glasses is to identify use cases for the emerging technology [15]. Prior research has focused on HCI and device-centered perspectives. The question is: "*Which field service tasks can be supported by innovative mobile technology such as wearable devices*" [15].

To address this research void, we have conducted multiple case studies in order to collect use cases for smart glasses in the domains of logistics, nursing and maintenance. Building upon prior research on task-technology fit of mobile devices and the use cases we identified, we propose a task-technology fit framework for smart glasses.

2 Related Work

The use of smart glasses has been investigated in the research fields of Augmented Reality (AR) and Wearable Computing. Augmented Reality focuses on changing the user's perception of the real world by adding information [16].

Table 1. Existing Research Topics for smart glasses

Research Area	*Topic*
Industry	Assembly [17]
	Maintenance & manufacturing [18]
	Technical customer service [19]
Health care	Hands-free photo and video documentation [20]
	Surgery [21]
	Diagnostics support [13]
	Displaying body structures [22]
	Education [23]
Logistics	Pick by vision [24]
	Hardware selection [25]
	Privacy [26]
	Usability [27]

Although this can be achieved through haptics, sound and odor, the majority of research has focused on adding virtual elements to the user's view [28]. In order to classify as an Augmented Reality application three criteria need to be met: The application needs to combine real and virtual, be interactive in real time and

registered in 3D [29]. It is possible to implement AR-applications with Head-Mounted Displays, spatial displays like televisions of projectors and Hand-held devices such as tablets and smartphones [28].
Wearable computing focuses on devices that can be worn by the user. Typical devices are smart glasses, smart watches or clothes with integrated IT-devices [30]. Smart glasses integrate information in the user's field of view without an overlay of information and thereby caused limitations in the visual field [31].

The majority of existing research about smart glasses in both areas has been focused on building and evaluating prototypical applications for use cases in health care and industry [32]. Table 1 presents smart glass topics that have been researched within both domains and cites literature containing representative examples. Especially tasks with intensive information needs, that further require both hands in service delivery benefit from smart glasses-based information systems [33]. Therefore, the implementation of these systems are discussed in the fields of logistics, maintenance and health care.

3 Methodological Procedure

To investigate in which service processes smart glasses can bring benefit we carried out multiple case studies using the case study research design defined by Yin [34]. Two cases from logistics (LG), four cases within nursing (NU) and two cases from the maintenance (MT) domain were evaluated. The domain of nursing fits well to existing research from the health care field, while logistics and maintenance are typical industrial application fields. Each case relies on several sources of evidence, from which data was extracted over the last two years. Table 2 shows an overview of the project partners that were involved in our research.

As we followed a multiple method design, different methods have been applied during the inquiry to increase the breadth and range of our findings. On the strength of the specific characteristics of the different cases, we applied diverging methods for the individual problem components. Thereby four different research methods have been used with the aim of the finding's expansion [35].

Table 2. Companies involved in the Case Study

Domain	*Project Partners*	*Size*
NU	Hospitals	1 large
		1 medium
	Nursing homes	1 small
		1 medium
		2 large
MT	Machine manufacturer	1 medium
	Airport	1 large
LG	Logistics companies	1 small
		1 large

Conducting the multiple case study design, a use case was defined when an activity profited by gaining better access to information or a simpler process was achievable by the use of a smart glass application. In this section, we will briefly explain all employed methods. Starting point and supporting method during our research was a (i) literature review to find links between our findings and existing research. (ii) Shadowing served to identify potential use cases by observing workflows and every day activities. The survey was documented in the form of field notes and process models. To gain further insights on the requirements and needs of the domain experts we conducted (iii) expert interviews. We combined these interviews with evaluations of smart glass applications we were currently working on, to give the interview partners an impression of what smart glasses are capable. After the interview partners had tested one of the applications, we asked them (1) for what else they would like to use such a smart glass in their daily work routine, (2) which processes of their work were the most time consuming or difficult and (3) at what point in their daily work they would like to access information. Furthermore, we held (iv) workshops with focus groups to enable a thematic exploration of research objects from a practical perspective. We formulated a use case if it was supported by at least two independent sources from the spectrum of data sources mentioned above.

4 Taxonomy of use cases for smart glasses in service processes

In total, we found 76 use cases by applying the methodology described above. Through inductive grouping of the use cases by function and process group, we identified 11 categories of use cases, which are listed in Table 3. The inductive grouping was conducted in a group session by the authors. Use cases were printed on paper cards and rearranged into different clusters until groups emerged. In the following, we briefly describe each category in more detail and provide representative examples. A list of all use cases can be found in the Appendix.

Table 3. Taxonomy of use cases for smart glasses applications

Application Area	*Description*
Communication	Helps to get or send information to the operation location
Documentation	Provides the possibility to document processes on the fly
Process guidance	Provides guiding information
Education	Use smart glasses to teach employees
Alerts	Attracts user attention for urgent information or warning
Data Visualization	Shows helpful augmented information in-situ
Automatic Control	Reduces error rates in error-prone processes
Inventory management & automatic ordering	Automatically keep track of objects and resources to enable optimize consumption, usage and re-ordering
Resource allocation	Manage limited capacities, e.g. time, staff
Text Handling	Helps users generate or interpret written language
Navigation	Providing routes and action sequences

4.1 Description of application areas

Communication
A typical example for a communication use case can be found in maintenance. Machine manufacturers sell their machines to customers around the globe. When a machine breaks down, the entire assembly line needs to be stopped and the machine has to be repaired. Currently, maintenance technicians try to resolve problems over the phone or have to send a maintenance technician oversea. The situation could be solved more efficiently, if a worker at the assembly line could use a smart glass application with a live streaming feature. The maintenance technician can thereby see the machine over his PC and give instructions via voice or adding virtual arrows into the live stream.

Documentation
Documentation is a vital part of many processes within logistics, maintenance and health care. In many cases, documentation is needed to fulfill legal requirements.
For instance, chronic wounds of patients need to be documented on a regular basis. In the health care facilities we visited, health care professionals were not satisfied with the current process. It is time-consuming and the documentation is not perceived as accurate. A smart glass application could reduce the time required for documentation and improve its quality. Health care workers could wear smart glasses during the wound care management and fill out the wound protocol via voice commands or hand gestures without breaking the aseptic chain.

Process Guidance
In all three domains, we encountered processes, in which practitioners needed information in-situ for accurate process execution. Maintenance technicians need to know the sequence of maintenance steps and how to perform them. Health care professionals need to make sure they administer the right dosage of the right medication to patients. In logistics, small parts often need to be picked from shelves and placed in boxes, which are then send to the customer.

Education
A well-trained work force is crucial for workplace safety and efficient process execution. Teaching takes up significant time and effort within organizations. With smart glasses, it is possible to design standardized lectures that new employees can work through in the real world environment. For example, in the maintenance domain technicians often need to learn how to maintain machines they do not already know. Augmented Reality smart glasses are very adequate to support such teaching processes, because they can display step-by-step tutorials or show spatial information about hidden parts while the user has both hands free to interact with the machine.

Alerts
Process-related dangers may occur in the daily routine of the workforce. If not taken into account, these dangers may damage the worker or the goods treated. Safety alerts in wearable devices such as smart glasses can be used to remind workers of process-related dangers such as treating a patient with an infectious disease or handling hazardous goods with forklifts in warehouses.

Data Visualization

Stored data, which describes properties of goods treated, may support the working process. E.g. in maintenance displaying names of machine parts can support communication. When treating patients, it can be helpful to know biographic details, medication, diagnoses, written advice from colleagues or food preferences while talking to the patient. In logistics the loading process can be visualized to optimize the load mass. Smart glasses can provide such information in an unobtrusive manner.

Automatic Control

Automatic control of goods can be relevant to all domains in which goods have to be ordered. This is true for maintenance, healthcare and logistics. In logistics centers, incoming freight needs to be checked for damages and completeness. This can be automated by taking a picture of each parcel and scanning its barcode while being able to continue working hands-free.

Inventory Management & Automatic Ordering

Every domain with an inventory may use an inventory management and automatic ordering process if goods have to be replaced regularly. During maintenance, parts of machines often need to be replaced while maintenance workers hands are smeared with oil. Smart glasses could automate this process by simply scanning the product code of the defective part and sending an ordering request.

Resource Allocation

Limited resources like time, space, human capacity and goods are allocated through smart glasses, as the user captures distribution problems, gets informed about available capacities, or retrieves new tasks to compensate an inequitable distribution. For instance, a nurse can get the location of their colleagues displayed. This information can be used if the nurse needs help for a specific task. It may be of special relevance in case of an emergency.

Text Handling

Since many nurses, maintenance and logistics workers work in foreign countries in which other languages than their native language are spoken, smart glass applications capable of translating written text into their first language would be helpful. Moreover, such an application could be helpful for processing shippings and machine parts from other countries or translating Latin medication and body nomenclature.

Navigation

In all three domains, workers often need to navigate from one workplace to another. The optimal route can thereby depend on differing variables. For instance, nursing pathways in health care facilities can be complex. During work, nurses have to consider what needs to be brought to the patient's room, what has to be carried away and in which order patients should be visited. Medication and hygiene essentials like towels have to be present in the patient's room at the right time. However, these objects may be stored in different locations. A smart glass can calculate the shortest way and provide the result as a proposal to the nurse.

4.2 Towards a framework for evaluating fit of process and smart glass technology

Having identified use cases for smart glasses in logistics, maintenance and nursing, we looked for common characteristics, that make them viable for support via smart glasses. We especially looked for differentiating characteristics to existing ICT like

smartphones, PCs and smart watches. Figure 1 displays our framework. Smart glass use cases are only feasible when **timely access** to information is required. If timely access to information is necessary to execute a potential use case, **mobility** requirements can make support via PC infeasible. These characteristics have already been proposed by Liang et al. for mobile technology in general [36] and therefore should also apply to smart glass use cases.

Figure 1. Framework for task-technology fit of smart glasses

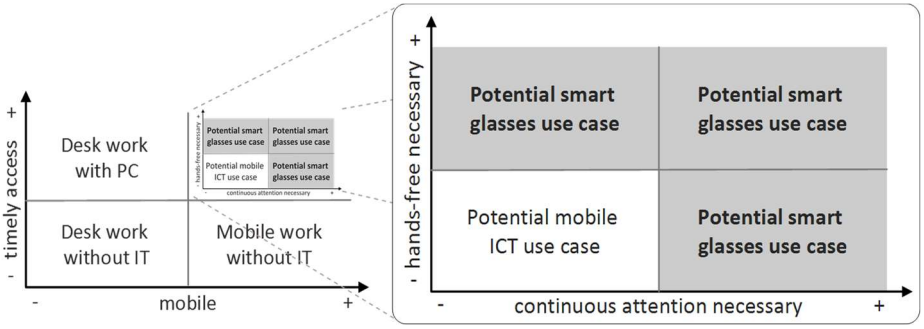


Table 4. Questions for task-technology fit evaluation

Question	*No*	*Yes*
Are both hands necessary for execution of the process?	--	++
Do the activities require timely information access?	--	++
Do the activities demand high mobility?	--	++
Is continuous attention needed?	--	++
Can in- and outputs be depicted visually and/or auditory?	-	+
Is a simple visualization possible?	-	+
Is network-connectivity possible throughout the site?	-	+
Is the amount of information needed also displayable?	-	+
Are speech-commands possible?	-	+
Is content already digitally available?	-	+
Can GPS and localization improve the process?	**o**	+
Can video-communication support the process?	**o**	+
Is the social environment open towards new technology?	-	**o**
Can technology-harmful external factors (e.g. dust) be eliminated?	-	**o**

-- prohibitive - obstructive **o** neutral + favorable ++ required

By comparing the smart glass use cases listed in the Appendix, we found that the following characteristics can help to differentiate smart glass use cases from mobile digitization use cases in general.

Digitization via smartphones and wearable devices like smart watches becomes infeasible when **continuous attention** is required or **hands-free** interaction constraints exist. For instance, it is not advisable to interact with a smartphone while operating a forklift, because the user's attention is diverted through technology interaction. On the other hand, use of smart glasses would be possible in such cases because, similar to navigation systems in cars, information is augmented in to the

field of view, which allows users to keep their focus on the task at hand. Hands-free interaction constraints occur whenever a person cannot use either of his hands to interact with an ICT. Examples of such constraints are to hold an object with both hands or to perform an aseptic procedure. Smart glasses can be used under such circumstances, because applications can be designed to support interaction by voice commands.

Furthermore, we propose additional criteria for task-technology fit building upon our experiences from developing several smart glass applications with project partners. Table 4 presents the criteria as a set of questions. Using this question set, the functional scope can be further explored.

5 Conclusion

Smart glasses are an emerging technology with many potential use cases in the service sector. Their main potential lies in providing mobile information access while being able to use both hands. In this research, we have proposed a cross-domain classification framework for use cases. The framework can be used by domain experts and researchers for identification of digitization potentials in existing services and implementation of assistive systems. Our research contributes to the fields of Augmented Reality, Wearable Computing and Service Science by providing a cross-domain classification taxonomy for smart glass applications and a framework for assessing task-technology fit. Practitioners and researchers can use these artefacts to identify use cases that are of practical relevance to several domains. Our taxonomy provides a structured approach for digitization efforts of service processes. Practitioners from different service domains can identify use cases in their domain by looking at the categories and individual examples of our taxonomy. Starting from there, they can find similar digitization potentials in their domain without needing prior knowledge about smart glasses.

Once potential processes have been identified, our task-technology fit framework for smart glasses can help to assess the viability of smart glass support for a given task. Future research should empirically investigate, whether our frameworks can help practitioners identify service tasks that can be supported by smart glasses. Furthermore, throughout our research we noticed, that in all three domains data security is of central importance. Services in industry and health care often work with highly sensitive data that needs to be kept confidential. This is a complicated task, since most of the use cases we have listed imply use of cameras and networking technology. Sometimes even with external partners, such as machine suppliers or doctors. The recent advances of smart glasses technology holds promising potentials for improving service processes by providing ubiquitous access to information while working hands free.

However, the advances in smart glass technology also raise long-term impact questions. Future generations of these devices will probably have built-in cameras that are constantly recording, using computer algorithms for tracking humans and displays that only show information to its user. Diffusion of such technology into the

consumer market will likely have an impact on our daily lives. Future research on privacy and ethical requirements for this pervasive technology is needed. This research may be part of a technology assessment, which allows addressing technological change as well as changes in morality. Furthermore, participative design of use cases is of high importance for being able to develop technology needs-driven. Thus, application of the framework shall imply inclusion of potential users into the discussion.

6 Acknowledgement

This research study is based on the projects ARinFLEX (grant number 02K14A080) and GLASSHOUSE (grant number 02K14A090), funded by the German Federal Ministry of Education and Research (BMBF) within the Program "Innovations for Tomorrow's Production, Services and Work" and managed by the Project Management Agency Karlsruhe (PTKA).

7 Appendix

Table 5. Complete List of use cases from the domains of nursing (NU), logistics (LG) and maintenance (MT)

Use Case	Explanation	Domain(s)
	Communication Use Cases	
Streaming	Hold videoconferences from the user's perspective	NU, LG
Internal Support	*Receive process guidance from internal experts*	NU, LG
External support	*Receive process guidance from external experts*	NU, LG
Teleassistance	*Show live-stream of machine for far distance maintenance*	MT
Client communitation	*Real-time video-documentation from a user's perspective*	NU, LG
Remote Support	*Get help instructions in emergency situations*	NU
Patient Hand-off	*Display recent patient-specific information*	NU
Fire-resistant sealing	*Show modifications for external certification*	MT
	Documentation Use Cases	
Swich infusion needle	*Reminds the nurse and documents replacement process*	NU
Digitize patient data	*Support documentation while performing health care*	NU
Patient admission	*Provide step-by-step guidance for patient admission*	NU
Measure blood sugar	*Automatically transmit data to electronic health record*	NU
Document damages	*Document damages via camera and transmit to record*	NU, LG, MT
Process execution	*Document processes from the user's perspective*	NU, LG, MT
Monitor processes	*Track processes and monitor KPIs*	LG, MT
	Process Guidance Use Cases	
Display plans	*Show inspection plans (e.g. in multiple languages)*	LG
Display and control package	*Support of picking-process*	LG
Drug management	*Support of drug management with a result control and an overview about drugs and relevant information*	NU
Patient discharge	*Support discharge of patients via checlists*	NU
Checklists	*Support standardized processes via checklists*	NU
Step-by-step guidiance	*Provide guidance for processes or emergencies*	NU
Machine maintenance	*Instructions can be displayed and visualized*	MT
Control cabinet maintenance	*Provide step-by-step guidance*	MT
Fire detector maintenance	*Documentation of fire detector maintenance during maintenance.*	MT
Display instructions	*Instructions to deal with goods can be displayed*	NU, LG, MT
	Education Use Cases	
Support of new employees	*Onbording of new employees can be supported by step-by-step guides*	LG, NU, MT
Integration into the facility	*support integration of newcomers by placing information at locations in facilities*	NU
Transfer perspective	*Allows others to view your actions from the viewer's perspective.*	NU, MT
Use Case	**Explanation**	**Domain(s)**
	Communication Use Cases	

Machine training	*View instructions and the machines at the same time.*	MT
	Alert Use Cases	
Warnings	*Context sensitive acoustic, visual or haptic warnings and safety instructions*	LG, NU
Reminder	*Proactive or controlled notification of crucial events*	NU
	Data Visualization Use Cases	
Visualizations	*Capture information and visualize it in meetings with patients and relatives*	NU
Show optimal load	*Show parcel loading order to optimize space usage*	LG
Vital signs	*Show recently measured vital signs of patients*	NU
Show progress	*Film motions of patients and show it to them afterwards*	NU
Visualize body parts	*Improve health care treatment by visualizing body parts*	NU
Manage nutrition	*Document nutrition consumption and incompatibilities*	NU
Stacking information	*Show how to optimally stack objects*	LG
Object information	*Show additional information about the object*	LG
Show machine configuration	*Help maintenance technicians customize the maintenance to the machine at hand*	MT
Show wiring plans	*Display hands-free visualization of wiring plans next to the machine*	MT
Show patient data	*Show patient data in the patient's room*	NU
Measure objects	*Measure and document the length or size of objects*	LG
Support simulations	*Simulate real world situations for training*	NU
	Automatic Control Use Cases	
Recognize and input errors	*Input-based recognition and feedback to the user in case of errors or mistakes*	LG
Automatic monitoring	*Camera-based recognition and feedback to the user in case of errors or mistakes*	LG
Automatic monitoring for picking	*Camera- or sensor-based checking of picking, e.g. whether workers use the correct compartments*	LG
Automatic checking of promotional displays	*Camera-based checking of the assembly of promotional displays according to the specifications*	LG
Object monitoring	*Camera-based checking of damages or integrity of different objects*	LG
Automatic monitoring of dangerous goods	*Camera-based checking of the goods-handling with dangerous or hazardous goods*	LG
Checking of medication compartments	*Support examining personnel through a display of the correct compilation of medication.*	NU
Predictive Maintenance	*Data visualization on predictive actions in maintenance*	MT
	Inventory Management & Automatic Ordering Use Cases	
Automatic reordering	*The smart glass tracks consumption and re-orders material*	HC
Order parts	*Display availability of machine parts during maintenance*	MT
Material overview	*Display location and amount of existing material*	NU, LG, MT
	Resource Allocation Use Cases	
Monitoring	*Capture and analyze workflow data*	LG
Reward System	*Gamification approaches to reward efficiency*	LG
Workforce distribution	*Prioritization of tasks and workforce based on process metrics*	LG, NU, MT
Monitor workload	*Capture data and prioritize tasks and assistance based on individual performance*	LG
Use of space	*Allocate storage locations efficiently*	LG
	Text Handling Use Cases	
Translation of text	*Camera-based recognition of text followed by a translation*	HC, LG, MT
Speech-to-Text	*Enabling technology for speech-based documentation*	HC, LG, MT
	Navigation Use Cases	
Navigation instructions	*Guide employees by displaying navigation information.*	LG
Real time maps	*The smart glass displays the map with real time traffic information.*	LG
Optimize pathways	*Optimized pathways for nurses could be provided.*	NU
Find place of action	*Employees could be navigated to their workplace.*	MT

References

1. Han, S., Kuruzovich, J., Ravichandran, T.: Service Expansion of Product Firms in the Information Technology Industry: An Empirical Study. J. Manag. Inf. Syst. 29, 127–158 (2013).
2. Wang, Q., Voss, C., Zhao, X., Wang, Z.: Modes of service innovation: a typology. Ind. Manag. Data Syst. 115, 1358–1382 (2015).
3. Lusch, R.F., Nambisan, S.: Service Innovation: a Service-Dominant Logic Perspective. MIS Q. 39, 155–175 (2015).
4. Barrett, M., Davidson, E., Prabhu, J., Vargo, S.L.: Service Innovation in the Digital Age: Key Contributions and Future Directions. MIS Q. 39, 135–154 (2015).
5. Afkari, H., Eivazi, S., Bednarik, R., Mäkelä, S.: The potentials for hands-free

interaction in micro-neurosurgery. Proc. Nord. 2014 8th Nord. Conf. Human-Computer Interact. Fun, Fast, Found. 401–410 (2014).
6. Mewes, A., Hensen, B., Wacker, F., Hansen, C.: Touchless interaction with software in interventional radiology and surgery: a systematic literature review. Int. J. Comput. Assist. Radiol. Surg. 12, 291–305 (2017).
7. Fries, V., Pflügler, C., Wiesche, M., Krcmar, H.: The hateful six – factors hindering adoption at small and medium sized enterprises. Twenty-second Am. Conf. Inf. Syst. (2016).
8. Röder, N., Wiesche, M., Schermann, M., Krcmar, H.: Why Managers Tolerate Workarounds – The Role of Information Systems. (2014).
9. Röder, N., Wiesche, M., Schermann, M.: A situational perspective on workarounds in IT-enabled business processes: A multiple case study.
10. Krcmar, H., Räß, G., Wiesche, M., Pflügler, C., Schreieck, M.: Digitalisierung im Handwerk. (2017).
11. Böhm, K., Esser, R.: Virtual Reality: The Next Big Thing? Zukunft der Consum. Technol. - 2016. Bitkom Res, 43–55 (2016).
12. Huck-Fries, V., Wiegand, F., Klinker, K., Wiesche, M., Krcmar, H.: Datenbrillen in der Wartung : Evaluation verschiedener Eingabemodalitäten bei Servicetechnikern. In: Informatik 2017. Lecture Notes in Informatics (LNI), Chemnitz (2017).
13. Mitrasinovic, S., Camacho, E., Trivedi, N., Logan, J., Campbell, C., Zilinyi, R., Lieber, B., Bruce, E., Taylor, B., Martineau, D., Dumont, E.L.P., Appelboom, G., Connolly, E.S.: Clinical and surgical applications of smart glasses. Technol. Heal. Care. 23, 381–401 (2015).
14. Schreieck, M., Wiesche, M., Krcmar, H.: Governing nonprofit platform ecosystems–an information platform for refugees. Inf. Technol. Dev. 23, 618–643 (2017).
15. Herterich, M.M., Peters, C., Uebernickel, F., Brenner, W., Neff, A. a: Mobile Work Support for Field Service : A Literature Review and Directions for Future Research. Int. Tagung Wirtschaftsinformatik. S. 134-148 (2015).
16. Klinker, K., Fries, V., Wiesche, M., Krcmar, H.: CatCare : Designing a serious game to foster hand hygiene compliance in health care facilities. In: Twelfth international conference on Design Science Research in Information Systems and Technology. pp. 20–28 (2017).
17. Khuong, B.M., Kiyokawa, K., Miller, A., La Viola, J.J., Mashita, T., Takemura, H.: The effectiveness of an AR-based context-aware assembly support system in object assembly. Proc. - IEEE Virtual Real. 57–62 (2014).
18. Nee, A.Y.C., Ong, S.K., Chryssolouris, G., Mourtzis, D.: Augmented reality applications in design and manufacturing. CIRP Ann. - Manuf. Technol. (2012).
19. Niemöller, C., Metzger, D., Thomas, O.: Design and Evaluation of a Smart-Glasses-based Service Support System. 13. Int. Conf. Wirtschaftsinformatik. (2017).
20. Jeroudi, O.M., Christakopoulos, G., Christopoulos, G., Kotsia, A., Kypreos, M.A., Rangan, B. V., Banerjee, S., Brilakis, E.S.: Accuracy of remote electrocardiogram interpretation with the use of google glass technology. Am. J. Cardiol. 115, (2015).
21. Chen, X., Xu, L., Wang, Y., Wang, H., Wang, F., Zeng, X., Wang, Q., Egger, J.: Development of a surgical navigation system based on augmented reality using an optical see-through head-mounted display. J. Biomed. Inform. 55, 124–131 (2015).

22. Ruminski, J., Smiatacz, M., Bujnowski, A., Andrushevich, A., Biallas, M., Kistler, R.: Interactions with recognized patients using smart glasses. Proc. - 2015 8th Int. Conf. Hum. Syst. Interact. HSI 2015. 187–194 (2015).
23. Rolland, J., Davis, L., Hamza-Lup, F., Daly, J., Ha, Y., Martin, G., Norfleet, J., Thumann, R., Imielinska, C.: Development of a training tool for endotracheal intubation: distributed augmented reality. Stud Heal. Technol Inf. 94, 288–294 (2003).
24. Reif, R., Günthner, W.A., Schwerdtfeger, B., Klinker, G.: Pick-by-Vision comes on age. In: Proceedings of the 6th International Conference on Computer Graphics, Virtual Reality, Visualisation and Interaction in Africa - AFRIGRAPH '09. p. 23. , New York, NY, USA (2009).
25. Büyüközkan, G., Güler, M., Uztürk, D.: Selection of Wearable Glasses in the Logistics Sector. (2016).
26. Berkemeier, L., McGuire, M.-R., Steinmann, S., Niemöller, C., Thomas, O.: Datenschutzrechtliche Anforderungen an Smart Glasses-basierende Informationssysteme in der Logistik. In: Eibl, M. and Gaedke, M. (eds.) Informatik 2017. pp. 1037–1048. Lecture Notes in Informatics (LNI), Chemnitz (2017).
27. Zobel, B., Berkemeier, L., Werning, S., Thomas, O.: Augmented Reality am Arbeitsplatz der Zukunft: Ein Usability-Framework für Smart Glasses. Inform. 2016. 1727–1740 (2016).
28. Krevelen, D.W.F. van, Poelman, R.: A Survey of Augmented Reality Technologies, Applications and Limittions. Int. J. Virtual Real. 9, 1–20 (2010).
29. Azuma, R.: A survey of augmented reality. Presence Teleoperators Virtual Environ. 6, 355–385 (1997).
30. Lukowicz, P., Kirstein, T., Tröster, G.: Wearable systems for health care applications. Methods Inf. Med. 43, 232–238 (2004).
31. Niemöller, C., Metzger, D., Fellmann, M., Özcan, D., Thomas, O.: Shaping the Future of Mobile Service Support Systems – Ex-Ante Evaluation of Smart Glasses in Technical Customer Service Processes. In: Informatik, Lecture Notes in Informatics (LNI 259) (2016).
32. Chatterjee, A., Aceves, A., Dungca, R., Flores, H., Giddens, K.: Classification of wearable computing: A survey of electronic assistive technology and future design. 2016 Second Int. Conf. Res. Comput. Intell. Commun. Networks. 22–27 (2016).
33. Metzger, D., Niemöller, C., Berkemeier, L., Brenning, L., Thomas, O.: Vom Techniker zum Modellierer - Konzeption und Entwicklung eines Smart Glasses Systems zur Laufzeitmodellierung von Dienstleistungsprozessen. In: Thomas, O., Nüttgens, M., and Fellmann, M. (eds.) Smart Service Engineering (Proceedings of Dienstleistungsmodellierung). pp. 193–213. Springer Gabler, Wiesbaden (2016).
34. Yin, R.K.: Case study research: design and methods. Eval. Res. Educ. 24, 221–222 (2011).
35. Greene, J.C., Caracelli, V.J., Graham, W.F.: Toward a Conceptual Framework for Mixed-Method Evaluation Designs. Educ. Eval. Policy Anal. 11, 255–274 (1989).
36. Liang, T., Huang, C., Yeh, Y., Lin, B.: Adoption of mobile technology in business: a fit-viability model. Ind. Manag. Data Syst. 107, 1154–1169 (2007).

Customer-Centred Intermodal Combination of Mobility Services with Conversational Interfaces

Daniel Braun[1], Adrian Hernandez-Mendez[1], Anne Faber[1], Manfred Langen[2], Florian Matthes[1]

[1] Technical University of Munich, Department of Informatics, Munich, Germany
{daniel.braun,adrian.hernandez,anne.faber,matthes}@tum.de

[2] Siemens AG, Corporate Technology, Munich, Germany
manfred.langen@siemens.com

Abstract. The way we consume mobility is drastically changing. Mobility is no longer only provided by traditional public transport and goods we own, like cars and bicycles, but also by service providers which offer mobility as a service, like car sharing companies. This new mobility ecosystem enables more flexibility, but also introduces additional complexity, especially for intermodal travel, i.e. reaching one's destination by using multiple means of transportation. In this paper, we present an approach to combine mobility services in a customer-centred way, which enables intermodal journey planning through an intuitive natural language interface. In contrast to other approaches, our architecture does not rely on the cooperation of mobility service providers, which has proven to be one of the main obstacles towards an integrated solution of multiple mobility services in the past.

Keywords: mobility, conversational interfaces, modelling

1 Introduction

With the growth of the sharing economy, mobility is transforming from something provided by owned goods, like cars and bicycles, and traditional public transport, to a service that can be consumed on demand. This development leads to a new flexibility which encourages so called intermodal mobility, i.e. the combination of multiple means of transportation during one journey. Renting a bike to get to the train station, taking a train to another city and renting a car at the destination is just one example, how a combination of multiple means of transportation can look like. Depending on the preferences of the user, different combinations could provide different benefits, like being cheaper or faster.

However, finding the most suitable combination of means of transport can be a very time consuming and tedious task. Currently, customers have to check multiple proprietary apps or websites and calculate transfer times and connections manually. In this paper, we present an approach to combine mobility services in a customer-centred, easy to use fashion in order to facilitate intermodal mobility.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

This approach benefits from another major business trend called API economy. A growing number of mobility companies, including traditional players from the public transport industry, as well as new players, which are part of the sharing economy, offer APIs to retrieve the information which is necessary to plan a journey. However, since there is no common standard for representing this data, these APIs have different formats and are not compatible with each other.

By introducing an additional abstraction layer, we want to create a system which is able to combine different existing mobility service APIs and is easily adaptable to new service providers. In order to make this combined information accessible and easily consumable for users, we developed a conversational interface which enables user to communicate with our system in the most natural way, using natural language. Moreover, we developed a platform which is able to store, process and share contextual information, like user profiles, which can be used to provide information tailored to the needs of the user.

2 Methodology

This work follows a design science research approach [7,8]. This approach was particularly suitable for our research, since one of the main parts of our work is a research prototype. The artefacts we have designed are the aforementioned prototype, a conversational interface for intermodal mobility, a meta-model for mobility services, and a reference architecture, which is a more generalized abstraction of the architecture of our prototype. According to Hevner's three-cycle view of design science [7,9], our research contributes in the following ways to each of the cycles:

- **Relevance Cycle**: The changing mobility ecosystem and the changed demands of customers regarding mobility (i.e. the increasing desire for flexibility and the decreasing desire to own mobility providing goods such as cars) establish a need for the intermodal connection of mobility services. Existing solution approaches, as we show in Section 3, have not been adopted in practice. Therefore, there is still a need for an applicable solution to this problem. Insights gathered from the prototypical implementation are used to assess the utility and viability of our approach.
- **Design Cycle**: The design artefact is the prototypical implementation, based on the architecture described in Section 4. In its current stage, the system can already connect to different mobility services, but we plan to add support for more services in the future, to test the scalability of the routing algorithm with regard to the number of mobility services. The designed artefact is evaluated as part of the relevance cycle by conducting a prototypical field test and including expert feedback which might stimulate further developments.
- **Rigor Cycle**: We have studied and evaluated the existing literature and artefacts in the domain of conversational interfaces, and service-oriented architectures. We draw on the current state of the art in system design approaches for conversational interfaces. In addition to the prototype, as design artefact, we contribute to the

knowledge space by designing a reference architecture and describing benefits and limitations of our approach.

3 Related Work

There have been multiple proposals, how mobility services could be connected to enable intermodal mobility. Beutel et al. [3] for example suggested a mobility broker architecture which introduces an independent mobility broker operator, which receives data from mobility service providers, combines them and offers a unified API to providers of webportals and mobile apps.

In contrast to our approach, Beutel et al. assume that mobility service providers will cooperate with the mobility broker and adapt der APIs according to the needs of the mobility broker. However, given the development we saw in the past, we do not think this is a realistic scenario in the near future. With a growing number of competitors, mobility service providers tend to be more closed up, rather than open and a cooperation of a significant number of service providers to use one unique interface seems at the moment unlikely.

The platform architecture proposed by Masuch et al. [10] makes the same assumption, that mobility service providers will actively adapt their services to fit the needs of a platform provider. However, in addition to the architecture of Beutel et al., the architecture from Masuch et al. contains a central storage for user information, a component which is also included in our architecture.

It is also worth mentioning that both, Beutel et al. and Masuch et al., only describe a high-level architecture, while we have also implemented a prototype based on the architecture we developed, in order to gather insights about the suitability of the approach.

From a commercial perspective, the most prominent example for a platform enabling intermodal journey planning is Google Maps. With its market power, Google was able to establish a format called General Transit Feed Specification (GTFS) [2], in which public transport companies have to provide their information in order to be included in Google Maps. However, GTFS only support street- and rail-based public transport. Hence, Google Maps is not able to include car and bike sharing in their journey planning or even a combination of trains and flights.

On a more general level, the TUM-LLCM project [5] researches open mobility platforms and their ecosystem, with a focus on the topics governance, architecture and core services, use cases, and geospatial-temporal analytics.

While there is also a huge amount of literature about chatbots and conversational interfaces, from past and present, there is only a few publications when it comes to conversational interfaces within the domain of transport and mobility. An early example of such a system is TRIPS (The Rochester Interactive Planning System) from Allen et al. [1]. TRIPS helps emergency services to plan the transport of patients to a hospital. The conversational interface takes the site of the accident and the hospital to which the patient should be transported as input and suggests which mode of transportation (e.g. helicopter or ambulance) is appropriate. Compared to the NLP

technologies available nowadays, Allen et al. were very limited and had to rely on a purely rule-based system.

4 Architecture

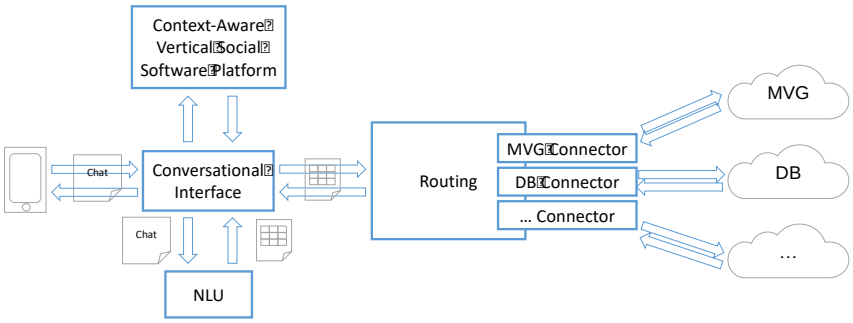


Figure 1. Architecture

The architecture we propose is shown in Figure 1. It contains five main elements. The Conversational Interface, which is described in more detail in Section 5, handles all interaction with the user. Incoming requests (i.e. chat messages) from the users are processed here and outgoing information is transformed from data to text within this element. For the processing of incoming messages, an external NLU component is used, which is connected to the conversational interface through a REST API. This component is also described in more detail in Section 5.

Once the incoming messages are processed and transformed from text to structured data, this data is used to generate search queries. Before these search queries are sent to the routing component, they are enhanced by information stored in the Context-Aware Vertical Social Software Platform, which is based on the architecture described by Hernandez-Mendez et al. [6]. This platform can for example be used to replace phrases like “home” or “work” in queries like “How can I get home from the main station?” or to incorporate user preferences (e.g. prefer trains over planes because of aviatophobia).

The enhanced query is subsequently sent to the routing component. In the simplest case, the routing component, described in Section 7, just chooses the appropriate mobility service. If the user is for example looking for a bus in Berlin, the routing component will connect to the BVG (Berliner Verkehrsbetriebe) API, if the user is looking for a bus in Munich, it will connect to the MVG (Münchner Verkehrsgesellschaft) API. In more complex cases, the routing algorithm will choose multiple mobility service providers to allow intermodal traveling.

In order to be able to query APIs from different mobility service providers and connect their results, the routing module needs the fifth element of our architecture, the different mobility service connectors. These connectors can be easily plugged into the routing component and are based on the meta-model for mobility services we describe in Section 6.

5 Conversational Interface

Natural language is one of the most intuitive ways for humans to interact with their environment. The recent hype regarding chatbots and conversational interfaces in both, industry and science, was fuelled not only by advances in machine learning and natural language processing, but also by the emergence of centralized messenger platforms. Messenger apps like Telegram or Facebook Messenger start to become the one-stop shop for users to interact with a range of different services, making individual apps for specific services obsolete.

Therefore, we decided to make our system available through a conversational interface which allows users to interact with the system from their favourite messenger. The user could for example ask “How can I get from Platz der Republik in Berlin to Marienplatz in Munich?” or set his preferences by writing “I live in Hamburg”. The design of our conversational interface follows the architecture described by Braun et al. [4], shown in Figure 2. We will give a more detailed view on our implementation of the architecture in this section.

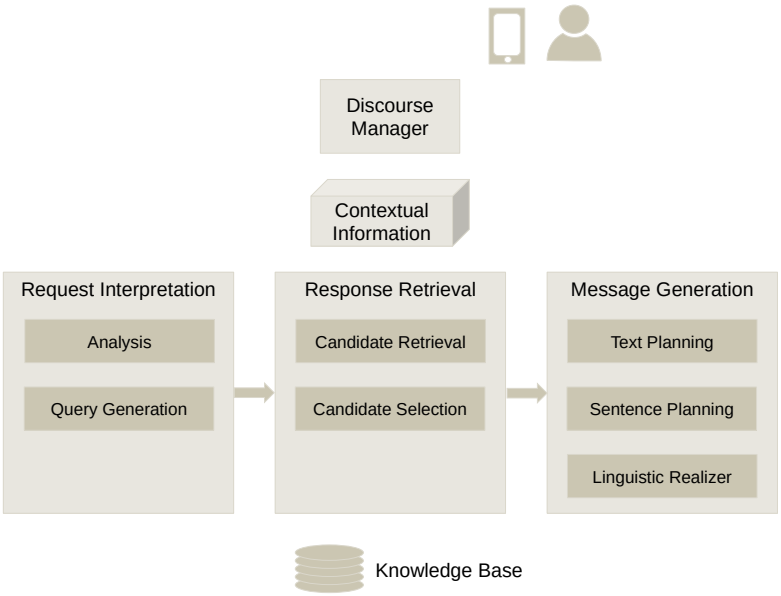


Figure 2. General Architecture for Chatbots by Braun et al. [4]

5.1 Discourse Manager

The Discourse Manager keeps track of the current state of the conversation, which includes the history, possible next steps, and missing information. In order to do routing, for example, we need a start and an end point for the trip. If a user just enters a destination ("I want to travel to Hamburg"), the conversational interface should detect the missing information and react accordingly, e.g. by sending a message like "From where do you want to travel?". If the user now responses for example "From Cologne", the conversational interface has to know that this is the start point for a trip to the destination Hamburg. This is what the Discourse Manager does. In the prototype we developed, we use Rasa Core[1], an open source discourse manager which is currently in closed beta.

The logic handled by the Discourse Manager can best be visualised by a tree structure. Figure 3 shows a simplified version of the subtree which is used if the user asks for a departure time. The only mandatory information that is needed to search for departure times is the place (e.g. "When can I leave from Sendlinger Tor?"). Therefore, the system has to ask for the place, if it is not given as part of the first message. However, the user might also decide to ask for something different when asked for the place. In this case, the current state (or memory) of the conversation tree is erased and the system jumps back to the top of the root node of the conversation tree. Other information, like a vehicle number ("When does ICE 123 depart from Berlin Hauptbahnhof?"), are optional.

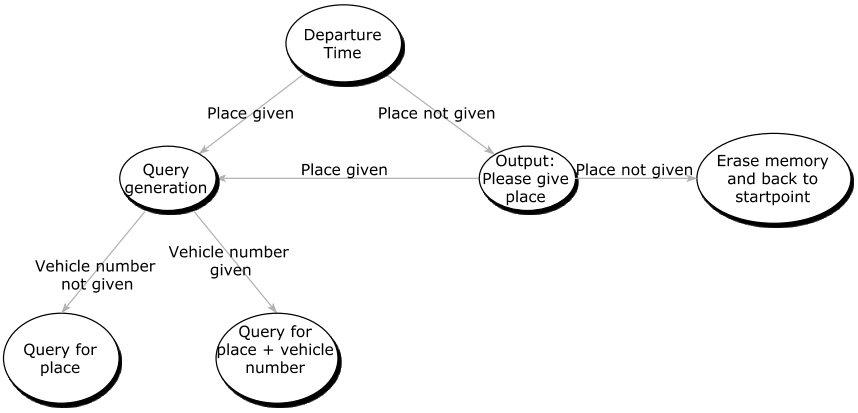


Figure 3. Simplified version of the representation of the subtree for the intent "Departure Time" in the Discourse Manager

5.2 Request Interpretation

In order to analyse incoming requests, we use so called Natural Language Understanding (NLU). Braun et al. [4] evaluated four different NLU services:

[1] https://rasa.ai/products/rasa-core/

Microsoft LUIS, IBM Watson Conversation, API.ai, and Rasa NLU. In their evaluation, Microsoft LUIS performed best, followed by Rasa NLU. Since Rasa NLU was the only tested NLU service which is open source and can be hosted on premise, we decided to use it for our prototype.

We trained the NLU service with two main intents: “Find Connection”, for finding a connection between two places and “Departure Time” for getting the departure time of public transport at a certain station. Moreover, we trained five entities: “Location Start”, “Location Destination”, “Mode of Transportation”, which allows the user to search for a certain mode of transportation, like a train, “Line”, which allows the user to search for a certain line, like U6 or ICE 1234, and “Criterion” which can be used to specify preferences for the routing algorithm, like “fastest”, “cheapest” and so on.

Additionally, we trained some auxiliary intents, like “Set Preferences” or “Greeting” and “Farewell”, which are used to make the interaction with the conversational interface more natural. However, it is important to underline that we do not try to mimic human behaviour and our prototype is built to be a conversational interface, not a chatbot.

For training, we used a corpus with 206 utterances, collected from a mobility chatbot for Telegram and manually annotated by the authors. Overall, the corpus consists of 706 labels, 206 intents and 500 entities.

After an incoming message is processed, the NLU services returns a JSON object containing the extracted information, which could look like this:


```
{
    "text": "Can you find a connection from Berlin to Munich?",
    "intent": "FindConnection",
    "entities": [
      {
        "entity": "Location Start",
        "start": 6,
        "stop": 6,
        "text": "Berlin"
      },
      {
        "entity": "Location Destination",
        "start": 8,
        "stop": 8,
        "text": "Munich"
      }
    ]
}
```


Afterwards, this structured information and our mobility service model, which is described in Section 6, is used to create a query for the routing algorithm, which is described in Section 7.

5.3 Message Generation

Our prototype uses a template-based approach for the generation of response messages, instead of a full NLG pipeline, as suggested by Braun et al. [4]. The data which is used as input for the message generation is returned by the routing algorithm. In order to offer some text variation, multiple templates have been created for each possible response.

An example responses for the intent "Find Connection" is: *"First, take the bus N40 from Haderner Stern to Karlsplatz (Stachus) at 13:08. You will arrive at 13:28. Then, walk from Karlsplatz (Stachus). You will arrive at 13:38. Your journey will take 30 minutes."* An Example response for the intent "Departure Time" is: *"Bus 197 departs at 00:36 from Quiddestraße to Innenring Neuperlach."*

Whenever a user connects to the conversational interface for the first time, a welcome message is send including example questions which can be asked, in order to help the user to get an idea how he can interact with the conversational interface.

6 Meta-Model for Mobility Services

In order to build a system which does not rely on the assumption that mobility service providers will cooperate and provide a certain, unified, API format, we did need to find an abstraction which allows us to subsume the majority of the existing mobility services and their APIs. This abstraction needs to provide sufficient information for intermodal routing but at the same time, it can only rely on information that is provided by almost all mobility service APIs.

In order to find such an abstraction, we analysed multiple APIs, public and private, from different mobility service providers, including Deutsche Bahn, Lufthansa, Drive Now, and MVG. Based on the inspection of these APIs, we developed the three-layered model for mobility services shown in Figure 4.

The first layer of the meta-model, called *MobilityService*, contains all information that is mandatory for every mobility service, this includes the name of the service, the means of transportation offered by the service (e.g. subways, buses, cars, etc.), and its level of operation, which can be either regional, national, or international. In Section 7, we will explain why this information is necessary. We can also check for every mobility service, whether a specific place is reachable with the service or not, and we can ask for a connection from a start point to an end point, which is used by our routing mechanism, described in Section 7.

In the second layer, we differentiate between public transport services and individual transport services like car and bike sharing. For public transport services, there is a function which enables the system to find stations next to a given place and to get a list of departures at a certain station. For the individual transport services, we can find the vehicle closest to a given place. On the third layer, we have concrete models, derived from the above-mentioned layer, for a specific service. Since we do not rely on the cooperation of mobility service providers, an individual model has to be created for every mobility service and has to be maintained in case the API changes. However,

once this model exists, the mobility service can be immediately plugged into the system and will be included in the routing process without any additional changes.

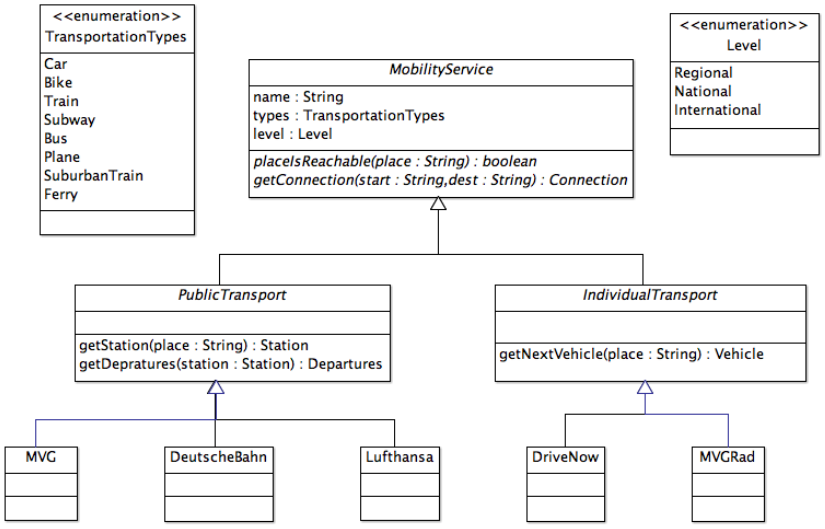


Figure 4. Mobility Service Model

7 Routing

Compared to other approaches, which we introduced in Section 3, our system does not rely on the cooperation of mobility service providers. One drawback of this approach is the fact that we have only very restricted access to information. This specifically limits us with regard to the routing, which is necessary to connect different modes of transportation and enable intermodal mobility.

Since most mobility services offer their own routing algorithm through their API, they do not offer all the information which would be necessary to do the routing manually. Therefore, we have to rely on these routing algorithms and connect them, rather than creating our own routing algorithm based on geospatial data. While this might result in some routes not being found, it enables us to integrate as much services as possible, without relying on the cooperation of their operators.

The main challenge for our routing process is therefore the shift of modes of transportation. If a user, for example, wants to travel from Platz der Republik in Berlin to Marienplatz in Munich, she first has to walk from Platz der Republik to the subway Station “Bundestag” and take the U55 from there to Hauptbahnhof, then take e.g. ICE 1513 from Berlin to Munich and in Munich S1 from Hauptbahnhof to Marienplatz. In this section, we describe, how our routing process solves this problem.

First, we calculate the distance between the start location and the end location. We do this by using the Google Maps API to geocode the extracted addresses (e.g. street names) to coordinates of latitude and longitude. Afterwards, we can use the Haversine

formula, to calculate the distance between the two locations. If the distance is less than 50 km, the trip is classified as "regional". Based on this classification, the system decides which mobility service providers should be checked. For a travel within Berlin, for example, we do not want to check flight or long distance train connections. Therefore, we only check mobility service providers which are also labelled as regional and operate in this region. In Berlin, this could be for example BVG or Car2Go.

A trip from Berlin to Munich, on the other hand, will be labelled as national. Therefore, the system would for example check Deutsche Bahn first. The Deutsche Bahn API will return a route from Berlin Hauptbahnhof to Munich Hauptbahnhof. Afterwards, the system will recursively try to find a route from Platz der Repbulik to Berlin Hauptbahnhof and from Munich Hauptbahnhof to Marienplatz, until a direct connection is found.

One additional challenge of this approach is the fact that most mobility service APIs "greedily" try to deliver an answer for every input. The Münchner Verkehrsgesellschaft (MVG), for example, obviously does not offer any connections to Berlin, however, if the API gets Berlin and Marienplatz as input, it will return a route from "Berlinerstraße" (Berlin street) in Munich to Marienplatz. Therefore, we cannot only rely on the results from the APIs, to check if a place is really reachable with a given service.

We tested different approaches how to deal with this issue, e.g. by calculation how different the returned result (e.g. "Berlinerstraße") is from the actual input (e.g. "Berlin") with linguistic metrics like the the Levenshtein distance. However, we achieved the best results with the same method we also use for the routing itself: we geocode the input and the returned result and calculate the spatial distance between both points with the Haversine formula. If it is more than one kilometre, we assume that the returned place is not identical with the input.

8 Advantages and Limitations

As we have stressed before, one of the key points of our approach is the fact that we do not rely on the cooperation of mobility service providers. While we think, this is a major advantage, it is also the cause for most of the limitations of our approach.

It is an advantage, because in the past, many approaches failed, because mobility service providers could not agree on one data format or were not willing to cooperate with each other at all. Even Google, despite its market power, could only include a limited number of services. And all services included are almost exclusively from the "old" public transport industry. Car sharing services or similar offers are not included. One reason for this might be the fact that traditional public transport providers almost never directly compete with each other in one area, at least in Germany. In Munich, there is MVG, in Berlin, there is BVG, but no competing alternatives. On longer distances, there is a competition between trains and planes, however, Google Maps does not offer intermodal journey planning including flights.

The main disadvantage of our approach is the fact that connectors have to be maintained for all services. While the initial creation is relatively easy, partially thanks to the provided meta-model, every time a service provider changes its API, the

connector has to be adapted, which can lead to an interruption of service, until the connector is updated.

We hope that in the future, mobility service providers will be more willing to cooperate with each other and open standards will emerge for mobility service APIs. While this would make our routing module with the connectors obsolete, the rest of our architecture would still be valid. Moreover, we believe that our meta-model for mobility services and the insights we gained during its design could be a blueprint for the development of an open standard.

From a computational perspective, our approach has another advantage, because most of the routing is outsourced to the servers of mobility service providers. Our system only has to do the routing between different modes of transportation, which is usually a very short distance.

Another main advantage of our architecture is the usage of a conversational interface, which allows a very intuitive interaction with the system. This approach also eradicates the need of downloading and installing an additional app, which makes it more likely to be adopted by users. Additionally, it makes the system very easily incorporable with the popular becoming voice assistants like Apple's Siri or Amazon's Alexa.

9 Conclusion

In this paper, we have presented a customer-centred approach to the intermodal combination of mobility services, using conversational interfaces. Following a design science approach, we have analysed changes in the mobility ecosystem and existing approaches to the intermodal combination of mobility services. We designed a reference architecture, which, in contrast to the existing approaches, does not rely on the cooperation of mobility service providers. Based on this architecture, we have implemented a research prototype combining our findings with the latest research on conversational interfaces, natural language understanding, and context-aware social software. In the discussion of our results, we identified advantages and limitations of the approach.

In the future, we would like to expand our prototype to support additional mobility services. So far, our main focus was on the architecture and the meta-model for mobility services. In the future, an additional focus could be set on the interface, e.g. by comparing our conversational interface to a more classical, form-like interface.

References

1. Allen, J. F., Byron, D. K., Dzikovska, M., Ferguson, G., Galescu, L., & Stent, A.: Toward conversational human-computer interaction. AI magazine, 22(4), 27 (2001)
2. Antrim, A., Barbeau, S.J.: The many uses of GTFS data–opening the door to transit and multimodal applications. Location-Aware Information Systems Laboratory at the University of South Florida (2013)

3. Beutel, M. C., Gökay, S., Kluth, W., Krempels, K. H., Samsel, C., & Terwelp, C.: Product oriented integration of heterogeneous mobility services. In Intelligent Transportation Systems (ITSC), 2014 IEEE 17th International Conference on, pp. 1529-1534. IEEE (2014)
4. Braun, D., Hernandez Mendez, A., Matthes, F., Langen, M.: Evaluating Natural Language Understanding Services for Conversational Question Answering Systems. Proceedings of the 18th Annual SIGdial Meeting on Discourse and Dialogue, Saarbrücken, Germany (2017)
5. Faber, A., Matthes, F., Michel, F.: Digital Mobility Platforms and Ecosystems. Technical Report, Technische Universität München (2016)
6. Hernandez-Mendez, A., Braun, D., Matthes, F., Langen, M.: Towards a Context-Aware Vertical Social Software Ecosystem. Proceedings of the 19 IEEE Conference on Business Informatics (CBI). Thessaloniki, Greece (2017)
7. Hevner, A.R.: A Three Cycle View of Design Science Research, Scand. J. Inf. Syst., vol. 19, no. 2, pp. 87–92 (2007)
8. Hevner, A.R., Chatterjee S.: Design Research in Information Systems: Theory and Practice, vol. 22. Boston, MA: Springer US (2010)
9. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Q 28:75–105 (2004)
10. Masuch, N., Lützenberger, M., & Keiser, J: An open extensible platform for intermodal mobility assistance. Procedia Computer Science, 19, 396-403 (2013)

Crowd Sourcing: Ko-Produktion integrierter multimodaler Mobilitäts- und Versorgungsdienste für Smart Regions − Status Quo, Konzeption und Entwicklungsperspektiven

Ingmar Ickerott[1], Frank Teuteberg[2], Maria Carmen Isabel Süßmuth[1]

[1] Hochschule Osnabrück, Betriebswirtschaftslehre, insbesondere Logistikmanagement, Lingen, Deutschland
{i.ickerott | m.suessmuth}@hs-osnabrueck.de
[2] Universität Osnabrück, Fachgebiet Unternehmensrechnung und Wirtschaftsinformatik, Osnabrück, Deutschland
frank.teuteberg@uni-osnabrueck.de

Abstract. Die Vernetzung der Mobilitäts- und Versorgungskonzepte für Kernstädte und deren Umland kann mit Crowd Sourcing-Plattformen unterstützt werden. Der vorliegende Beitrag gibt einen Überblick über den Stand der Forschung und stellt die Anforderungen an eine Crowd Sourcing-Plattform zur Ko-Produktion integrierter multimodaler Mobilitäts- und Versorgungsdienste dar. Hierzu werden die Ergebnisse einer Anforderungsanalyse auf der Basis von 11 Workshops und 4 Experteninterviews im Zeitraum von Mai 2014 bis Sept. 2017 mit 60 Partnern vorgestellt. Der Beitrag veranschaulicht zudem ein Konzept für die Ko-Produktion integrierter multimodaler Mobilitäts- und Versorgungsdienste. Aus den Ergebnissen wird schließlich eine Forschungsagenda abgeleitet. Die konsolidierten Anforderungen können als Grundlage für die Erstellung von Pflichtenheften für Crowd Sourcing-Plattformen genutzt werden.

Keywords: Ko-Produktion, Crowd Sourcing, Partizipationsplattform, Mobilitäts- und Versorgungsdienste, Smart Regions

1 Einleitung und Motivation

Die Bedürfnisse der Menschen in den Kernbereichen einer Stadt decken sich in wesentlichen Bereichen mit denen der Menschen im Umland. Bürger möchten sich sowohl in einer Stadt als auch im Umland einer Stadt barrierefrei, komfortabel und ohne Angst zwischen Orten des Lebens und der Arbeit bewegen können. Sie möchten auf Angebote treffen, die sie interessieren und ihr geistiges, soziales, kreatives und wirtschaftliches Leben fördern und bereichern.

Neue technologiegestützte Formen der Bürgerbeteiligung im Sinne einer Sharing Economy/Shareable City sowie im Sinne von Crowd Sourcing (z.B. Crowd Funding, Crowd Sensing oder Crowd Logistics) erschließen hierbei bisher ungenutzte Potenziale

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

zur aktiven Entwicklung eines städtischen oder suburbanen Raums [1]. Neuere Definitionen verstehen Crowd Sourcing als eine interaktive Form der Leistungserbringung, die kollaborativ oder wettbewerbsorientiert organisiert ist. Unter Einsatz von modernen Informations- und Kommunikations (IuK)-Technologien trägt eine große Anzahl extrinsisch oder intrinsisch motivierter Akteure unterschiedlichen Wissensstands der Leistungserbringung bei [2].

Kernstädte und deren Umland stehen in einer durch Crowd Sourcing-Initiativen geprägten Shareable City in einem direkten Wechselverhältnis mit unmittelbarer Verbindung zu zentralen Dienstleistungen für Mobilität und Versorgung. Die Voraussetzungen zur Sicherung der Lebens-, Arbeits- und Aufenthaltsqualität gestalten sich jedoch in Kernstädten und in Umlandgemeinden unterschiedlich. Aus diesem Grund unterscheiden sich die Lösungsansätze für Städte als "Smart Cities" signifikant von Lösungen für die weitergefasste Kernstadt inkl. der Umlandgemeinden („Smart Regions“), denn Wertschöpfungssysteme, Mobilitätsformen und Versorgungs- und Logistikstrukturen müssen den unterschiedlichen räumlichen Anforderungen gerecht werden. Dienstleister für Mobilität, Versorgung und Logistik stehen dabei vor der Herausforderung, Dienstleistungsverknüpfungen für das Zusammenspiel dieser Regionen zu entwickeln. Die Angebote in weniger dicht besiedelten Umlandgemeinden einer Stadt sind insbesondere für öffentliche Verkehrsbetriebe und Logistikdienstleister isoliert gesehen häufig relativ wenig rentabel. Auf der Basis integrierender IuK-Technologien kann das zivilgesellschaftliche Engagement der Bürger sowie das Kooperationsverhalten von Mobilitäts-, Versorgungs- und Logistik-Dienstleistern jedoch erschlossen bzw. gestärkt werden. Neu zu entwickelnden Modelle zur Ko-Produktion von integrierten multimodalen Mobilitäts- und Versorgungsdiensten können das Zusammenwirken der Menschen in Smart Regions stärken und somit die Lebensqualität der Bürger unabhängig von ihrem Lebensmittelpunkt verbessern.

2 Ein Fallszenario zur Veranschaulichung

Zur Erläuterung des Zusammenspiels der Akteure im Rahmen der bedarfsorientierten Ko-Produktion integrierter multimodaler Mobilitäts- und Versorgungsdienste dient folgendes Szenario, das einen Teil der geplanten Umsetzung sowie die Einbindung der Akteure verdeutlicht. Die kursiv geschriebenen Kürzel in Klammern kennzeichnen die Anforderungen, die sich daraus an eine Crowd Sourcing-Plattform ableiten lassen und in den Tabellen 1 und 2 dargestellt sind:

Familie Hase ist vor zwei Jahren mit den beiden Kindern Niko (8 Jahre) und Tanja (12 Jahre) in ein Zweifamilienhaus im Landkreis Osnabrück, ca. 30 km vom Zentrum entfernt, gezogen. Die niedrigeren Grundstückpreise haben die Hases zu diesem Schritt bewogen. Herr Hase (42 Jahre) arbeitet als Administrator bei einem IT-Dienstleistungsunternehmen und pendelt täglich mit dem Auto zu einem attraktiven Bürokomplex in der Osnabrücker Innenstadt. Niko besucht eine nahegelegene Grundschule und Tanja fährt täglich mit dem Bus zu einem Fach-Gymnasium Wirtschaft in ca. 5 km Entfernung. Frau Hase (41 Jahre) ist als gelernte Kauffrau im Einzelhandel im direkten Umfeld tätig. Nach einer Informationsveranstaltung in der

neuen Nachbarschaft haben sich die Hases spontan bereit erklärt, gemeinsam mit ihren Nachbarn an einem Pilotprojekt zur Verbesserung der Mobilität und Versorgung teilzunehmen, das kostenfrei genutzt werden kann *(A1)*. Die Sensordaten ihrer Handys werden zu diesem Zweck in einer sicheren Datenumgebung erfasst *(D9, D14)*. Auf dieser Basis können sich die Hases mit Hilfe einer neuen App nun besser untereinander, innerhalb ihrer Nachbarschaft und darüber hinaus (je nach Offenheit) mit weiteren Bürgern und diversen Dienstleistern bei der Organisation von Versorgung und Mobilität koordinieren und gegenseitig unterstützen *(B2, B3, D5)*. Herr Hase fährt nun immer öfter gemeinsam mit einem Nachbarn mit dem E-Bike bis zu einer nahegelegenen Mobilitätsstation mit sicheren Parkmöglichkeiten, um von dort aus mit dem E-Bus in die Innenstadt zu fahren *(D2)*. Hierdurch sammelt er besonders viele Ökopunkte für die Quartiers-Community-Webseite *(A4)*. Die Anbieter von Mobilitäts- und Logistik-Dienstleistungen können auf Basis der gewonnenen Daten Beförderungs- und Belieferungsprozesse untereinander arbeitsteilig gestalten *(D3)*. Eine E-Commerce-Lieferung für Familie Hase wird von einem Logistikdienstleister an den Betreiber des öffentlichen Personennahverkehrs (ÖPNV) übergeben, der das Paket an der Mobilitätsstation in ein Paketfach zwischenlagert. Tanja Hase wird noch während ihrer Heimfahrt von der Schule per Smartphone mit Near Field Communication (NFC) und einem Location Based Service im Bus auf die Mitnahme des Paketes hingewiesen *(D6)*. Der im Rahmen dieser arbeitsteiligen Belieferung eingesparte Betrag wird von dem Logistikdienstleister zur Hälfte an den ÖPNV-Anbieter und Familie Hase weitergereicht *(A2)*. Alternativ kann Frau Hase sich das Paket in ein Paketfach in ihrer Wohnung, auf das nur sie und der Zusteller per RFID-Chip Zugriff haben, oder in den Kofferraum von ihrem Auto, das der Zusteller mit einer Smartphone-App öffnen kann, zustellen lassen. Frau Hase hat mit ihrer Nachbarin Frau Igel (82) jetzt vereinbart, dass Frau Igel einen automatischen Hinweis erhält, wenn Frau Hase sich in einem Supermarkt oder bei ihrem Lieblingsbäcker aufhält, um die Mitnahme von kleineren Einkäufen zu vereinbaren. Die App hierfür hat vor kurzem ein engagierter Entwickler auf der Plattform eingestellt, der selbst eine hilfebedürftige Großmutter hat *(D15, D16)*. Die Stadtverwaltung und der ÖPNV-Anbieter nutzen die Daten der Plattform derweil, um die Investitionen zur Entwicklung von Mobilitätszentren zu bündeln und Feedback zu Handlungsoptionen einzusammeln *(C2, C3)*. Für die Hases genügt ein Knopfdruck in ihrer neuen App und binnen 5 Minuten kommt ein Auto (lokaler Chauffeur aus der Nachbarschaft oder professioneller Dienstleister) vorbeigefahren. Die Ermittlung der Position der Hases erfolgt per GPS. Die Bezahlung erfolgt alternativ über Ökopunkte (virtuelle Währung) oder bargeldlos. Die Steuerung der App erfolgt sprachgesteuert. Es reicht, den Namen des Ziels zu sprechen (z.B. Stadtkino) *(D10)*. Die App ermittelt gemäß Profil der einzelnen Familienmitglieder der Hases den besten integrierten multimodalen Mobilitätsmix aus ÖPNV, Carsharing und Bikesharing. Die Hases können sich die Fahrtkosten mit den Menschen teilen, die zeitgleich in die gleiche Richtung fahren. Nutzer kommen somit mit der günstigsten und attraktivsten Alternative von A nach B, es gibt weniger Verkehr und schädliche Emissionen *(E2)*.

3 Verwandte Arbeiten und Status Quo

3.1 Stand der Wissenschaft

Die Entwicklung innovativer IuK-Technologien für die Stadt der Zukunft adressiert das Deutsche Forschungszentrum für Künstliche Intelligenz in Kaiserslautern mit dem „SmartCity Living Lab“. Einzelne Lösungen wurden bereits entwickelt wie z.B. die App „parKLight“, die alle Parkhäuser in der Umgebung mit vorhandenen Kapazitäten anzeigt, zusätzliche (Erinnerungs-)funktionen (z.B. Ablauf der Parkzeit) hat oder die Buchung von Parktickets ermöglicht. Im Projekt „RADAR“ werden digital vorhandene Inhalte mit Geodaten über sogenannte Augmented Reality Browser vernetzt. Im EffizienzCluster Logistik Ruhr werden im Leitthema „Urbane Versorgung“ Logistiklösungen für die Stadt adressiert. Innovative Warenübergangssysteme auf der letzten Meile sowie die Bündelung verschiedener Warenströme sind die dabei primär adressierten Innovationen. Im Projekt „Smart Urban Services“ vom Fraunhofer-Institut für Arbeitswirtschaft und Organisation in Stuttgart soll eine integrierte Plattform entwickelt werden, die unterschiedlichen Akteuren Zugriff auf Daten zur Entwicklung innovativer Dienste in Bereichen wie Gesundheit, Handel und Umwelt ermöglichen soll. Anknüpfungspunkte gibt es auch zu den Smart Data Projekten „Smart Data for Mobility“ (Plattform für Datenmanagement zur Planungsoptimierung von Mobilitätsdiensten) sowie „ExCell“ (Verkehrslagedaten für KMU-Mobilitätsdienstleistungen).

3.2 Stand der Praxis

Crowdcity, Small Size Smart City und Smart Citizen sind interaktive Plattformen zur Förderung von innovativen Ideen im Bereich „Smarter Cities“, indem die „Crowd“ (Meinungsführer, Stadtplaner, Bloggers etc.) miteinander in den Dialog treten sollen. Im Projekt „The Copenhagen Wheel“ wird ein E-Bike entwickelt, das als mobiler Sensor in der Stadt Kopenhagen fungiert und Sensordaten zu Luftverschmutzung, Wetter, Streckenqualität oder Verkehrsaufkommen in Realzeit ermittelt. Im Rahmen des Projekts „CityLog“ wurde mit der mobilen BentoBox eine Lösung für neue innerstädtische Logistikprozesse prototypisch realisiert. DHL, DPD, GLS, Amazon und Hermes erproben in diversen Pilotprojekten Paketkasten-Konzepte für Mietshäuser sowie private Kurierdienste. DHL, Audi und Amazon führen ein Pilotprojekt durch, bei dem Autos der Kunden als Lieferadresse von Paketsendungen genutzt werden. Eine Smartphone-App entriegelt die Fahrzeuge und informiert die Fahrer über die Paketzustellung. Plattformen zum Zusammenbringen von Angebot und Nachfrage von Privatpersonen zur Beförderung von Gütern wie z.B. Roadie dienen als Marktplätze für private Zustelldienste zwischen Einzelhandelsgeschäften, Lagern, Abholstationen von Paketdienstleistern und Wohnorten der Nachfrager. Im Projekt „Lautern macht mobil“ werden in den Einzelprojekten eBus 2.0, EmoCycling und KoPeMi Mobilitätsangebote für die Stadt der Zukunft entwickelt. Bürger können z.B. CarSharing-Standorte vorschlagen und bewerten. Im Rahmen von Horizont 2020 wurden mit

GROWSMARTER, TRIANGULUM sowie REMOURBAN drei „Leuchtturm-projekte“ ausgewählt, die andere Städte zur Übernahme von erprobten Smart City Lösungen ermutigen.

3.3 Stand der Technik

Im Bereich Crowd Sensing sind in Smartphones und anderen mobilen Geräten integrierte Sensoren (z.B. Barometer, Spektrometer, GPS, Gyroskop), Bluetooth Sensing sowie iBeacons erste Wahl. Zudem steht eine Vielzahl an Apps wie z.B. Sensor Box, Sensor Readout (beide Android) oder Sensor Monitor (iOS) zur Verfügung, um Sensordaten anzuzeigen. Die Nutzung von Crowd Sensing Data bietet dabei einen Mehrwert für Bürger, Stadtverwaltung und Wirtschaft, da sie auf Basis unterschiedlicher Sensordaten in Ko-Produktion z.B. neue Smart City Apps bzw. Services entwickeln können. Nicht zuletzt aufgrund der in den letzten Jahren rasant gesunkenen Kosten für Sensoren ist in Kooperation mit Bürgern so eine Reihe von Diensten realisierbar, wie z.B. gezielte Einblendung von Informationen an Mobilitätsknoten (z.B. Haltestellen) oder die Lenkung von Besucherströmen.

4 Forschungsmethode

Um die wissenschaftliche Wissensbasis und Kenntnisse aus der Anwendungsdomäne zu integrieren, folgt die Entwicklung des hier vorgestellten Crowd Sourcing-Konzeptes dem Design Science Ansatz nach Hevner et al. [3]. Im Rahmen eines iterativen Weiterentwicklungs- und Bewertungsprozesses werden die Schritte Anforderungs-analyse, Konzeption, Implementierung und Evaluation in mehreren Runden durchgeführt. Aktuell befindet sich das Vorhaben mit der Anforderungsanalyse und Konzeption im ersten Schritt. Das Vorhaben ist in das Forschungsprojekt Dorfgemeinschaft 2.0 [4] eingebettet, das im Zeitraum von Nov. 2015 bis Okt. 2020 als eines von bundesweit fünf Verbundvorhaben im Innovationswettbewerb „InnovaKomm“ mit ca. 5 Mio. EUR durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert wird. Beteiligt sind 11 Verbundpartner, mehr als 40 assoziierte Partner aus der kommunalen Selbstverwaltung und der sozialen und privaten Wirtschaft und Bürger aus der Region.

Bisher wurden die Methoden der Literaturanalyse [5] und der qualitativen Querschnittsanalyse in Form von 11 Workshops und 4 unstrukturierten Experteninterviews in Anlehnung an [6-7] im Zeitraum von Mai 2014 bis Sept. 2017 mit insgesamt über 60 Personen angewendet. Dabei handelte es sich um potenzielle Stakeholder einer Crowd Sourcing-Plattform bestehend aus Bürgern, App-Entwicklern, politischen Entscheidungsträgern und Dienstleistern aus den Bereichen Mobilität und Versorgung. Eine erste Evaluationsanalyse wurde durch Aggregation, Konzeptualisierung und Schlussfolgerung [8] erreicht. Zur Wahrung des Design Science Prinzips wird der Leitfaden zur Durchführung des Design Science Ansatzes [8] im Rahmen der Entwicklung des Versorgungskonzeptes gewahrt.

5 Ergebnisse

5.1 Anforderungsdefinition

Anforderungen an eine Crowd Sourcing-Plattform wurden aus Workshops und Experteninterviews mit Bürgern, App-Entwicklern, politischen Entscheidungsträgern und Dienstleistern aus den Bereichen Mobilität und Versorgung erhoben. Die Akteure bestanden sowohl aus Kooperations- und assoziierten Partnern des Forschungsprojekts „Dorfgemeinschaft 2.0“ als auch aus Teilnehmern, die in keinem Zusammenhang zum Forschungsprojekt standen und sich durch ihre Expertise in der Thematik auszeichneten. Die Anforderungen wurden in den Workshops von den Teilnehmern handschriftlich dokumentiert und verbal erläutert, was von den Forschern protokolliert wurde. In den Experteninterviews wurden die Anforderungen mit einem Diktiergerät aufgezeichnet und anschließend wörtlich transkribiert. Widersprüchliche Anforderungen der verschiedenen Akteure wurden nicht aufgenommen. Die ermittelten Anforderungen wurden hinsichtlich der sechs Merkmale, die eine Smart City definieren [9], klassifiziert.

Es wurden vier Anforderungen an eine Crowd-Sourcing-Plattform zur Stärkung des Merkmals *Smart Economy* erhoben. Diese Anforderungen geben den Anbietern und Nachfragern Anreize zur Nutzung der Dienste. Zur Stärkung des Merkmals *Smart People* wurden vier Anforderungen ermittelt, die Anbieter und Nachfrager dazu befähigen, die Crowd Sourcing-Plattform zu nutzen und die Eigenschaften anderer Akteure zu beurteilen. Die drei ermittelten Anforderungen zur Stärkung des Merkmals *Smart Governance* unterstützen Politik und Verwaltung. Auf das Merkmal *Smart Mobility* beziehen sich 16 Anforderungen, die mobilitäts- und informationstechnische Aspekte umfassen. Die zwei identifizierten Anforderungen zum Merkmal *Smart Environment* unterstützen die Einhaltung ökologischer Ziele. Bei den zwei erhobenen Anforderungen zum Merkmal *Smart Living* handelt es sich um Merkmale, die den Zusammenhalt in einer Gemeinschaft stärken.

Die in den Tabellen 1 und 2 genannten Zuordnungen der Anforderungen zur Forschungsmethode und zum Akteur kennzeichnen, dass eine Anforderung überwiegend durch die angegebene Forschungsmethode (d.h. Experteninterviews, Literaturanalyse oder Workshops) erhoben und im Fall von Experteninterviews oder Workshops überwiegend durch die angegebenen Akteure (d.h. Bürger, App-Entwickler, politische Entscheidungsträger oder Dienstleister aus Mobilität und Versorgung) geäußert wurde. Dennoch können die Anforderungen auch mit einer anderen der durchgeführten Forschungsmethoden erhoben oder von einem anderen der beteiligten Akteure geäußert worden sein.

Tabelle 1. Anforderungen an eine Crowd Sourcing-Plattform

Anforderung	*F*	*A*
1. Smart Economy		
A1: Kostenfreier Zugang	W	P
A2: Bereitstellung eines monetären Bezahlungssystems	W	E
A3: Funktion zur kostenoptimierten Planung auf der Basis von Crowd Sensing und Ko-Produktion zwischen Kernstädten und Umland	E	E
A4: Einsatz von gamification-basierten Ansätzen beim Anbieten und Erfüllen von Diensten	W	E
2. Smart People		
B1: Informationsportal mit textbasierten und videobasierten Trainings und Anleitungen über die Vorgehensweise zur Ausführung von Diensten [10]	L	
B2: Funktion zum Anlegen von Nutzerprofilen, die Fähigkeiten, demographische Charakteristika und Dienstehistorien umfassen [10]	L	
B3: Funktion zur Beschränkung der Gruppe von Crowd Sourcees aufgrund der Fähigkeiten, demographischen Charakteristika oder Dienstehistorien [10]	L	
B4: Funktion zur Gewährleistung von formellen und informellen Regeln, um einem Fehlverhalten der Crowd vorzubeugen [10]	L	
3. Smart Governance		
C1: Informationsportal mit regulatorischen Anforderungen wie ethischen Standards und Datenschutz [10]	W	B
C2: Funktion zur Visualisierung von (Rebound-)Effekten	E	P
C3: Funktion zur anonymisierten oder personifizierten Abgabe von Aussagen der Akteure	W	P
4. Smart Mobility		
D1: Ausbau der digitalen Infrastruktur	E	E
D2: Integration bestehender Einzellösungen aus den Bereichen Mobilität, Versorgung und Logistik zu integrierten multimodalen Wertschöpfungsketten im Sinne von Plug & Play	W	D
D3: Funktion zur Aufteilung von Aufgaben in feingliedrige Unteraufgaben [10]	L	
D4: Funktion zur Definition von Lösungsvorschlägen [10]	L	
D5: Funktion zur Abfrage und Buchung der angebotenen Mobilitäts- und Versorgungsdienste	W	B
D6: Funktion zur synchronen und asynchronen Kommunikation mit Akteuren	W	E
D7: Funktion zum Suchen und Abrufen von (un-)strukturierten Daten	E	E
D8: Plausibilitätsüberprüfung bei Dateneingabe	W	D
D9: Nutzung von Sensordaten von Smartphones und anderen Visibility Devices	W	E
D10: Funktion zur Tastatur- und Sprachsteuerung	W	B
D11: Nutzung von akteursspezifischer Terminologie	W	B
D12: Datenbank mit Qualitätsmetriken von Dienstleistungen	E	E
D13: Interoperabilität verschiedener Domänen	E	E
D14: Einhaltung des Datenschutzes und der Datensicherheit	E	E
D15: Nutzerorientierte Gestaltung	E	E
D16: Barrierefreiheit	W	B

Tabelle 2. Anforderungen an eine Crowd Sourcing-Plattform (Fortsetzung)

Anforderung	*F*	*A*
5. Smart Environment		
E1: Funktion zur Quantifizierung und Visualisierung von Synergien, Zielkonflikten und (Rebound-)Effekten	E	P
E2: Funktion zur ressourcenoptimierten Planung auf der Basis von Crowd Sensing und Ko-Produktion zwischen Kernstädten und Umland	W	P
6. Smart Living		
F1: Funktion zur Abstimmung zur gleichberechtigten Entscheidung der Akteursgruppen	W	P
F2: Funktion für Diskussionen zwischen Crowd Sourcern und Sourcees [10]	L	

Anm.: F = Forschungsmethode, E = Experteninterviews, L = Literaturanalyse, W = Workshops; A = Akteur, B = Bürger, E = App-Entwickler, P = politische Entscheidungsträger, D = Dienstleister aus Mobilität und Versorgung.

5.2 Ziele

Die Ziele, die mit der Crowd Sourcing-Plattform verfolgt werden, wurden über die Workshops mit den beteiligten Akteuren aus Wissenschaft (Forschungsziele), Praxis (Implementierungsziele) sowie Bürgern und Gemeinden (Anwendungsziele) erhoben. Die Forschungsziele umfassten die Entwicklung eines Integrationskonzepts und Geschäftsmodells für die bedarfsorientierte Ko-Produktion von Mobilitäts- und Versorgungsdienstleistungen in Smart Regions. Als Entwicklungsziele wurden die Entwicklung Crowd-basierter Dienstleistungen und einer offenen zentralen Informations- und Partizipationsplattform zur Vorstellung, Bewertung, Lenkung und Koordination einzelner Mobilitäts- und Versorgungsdienste (Crowd Testing, Crowd Funding) im Sinnes eines Service Marketplace herausgearbeitet. Anwendungsziele beinhalteten das Angebot und die Evaluation von ko-produzierten Mobilitäts- und Versorgungsdiensten u.a. zum Schaffen eines attraktiven Lebens- und Arbeitsumfeldes und zur Förderung der Auslastung von umweltfreundlichen Verkehren sowie die Sicherstellung, dass individuelle Entscheidungen und Bedürfnisse der Bürger z.B. durch Bündelung und Anreizmodelle zu nachhaltigen Mobilitäts- und Versorgungsdiensten führen.

5.3 Architektur

Mit der Crowd Sourcing-Plattform kann die gesamte Wertschöpfungskette von Mobilitäts- und Versorgungsdiensten in der Kernstadt inkl. den Umlandgemeinden durch integrierte multimodale Dienste geschlossen werden (vgl. Abbildung 1).

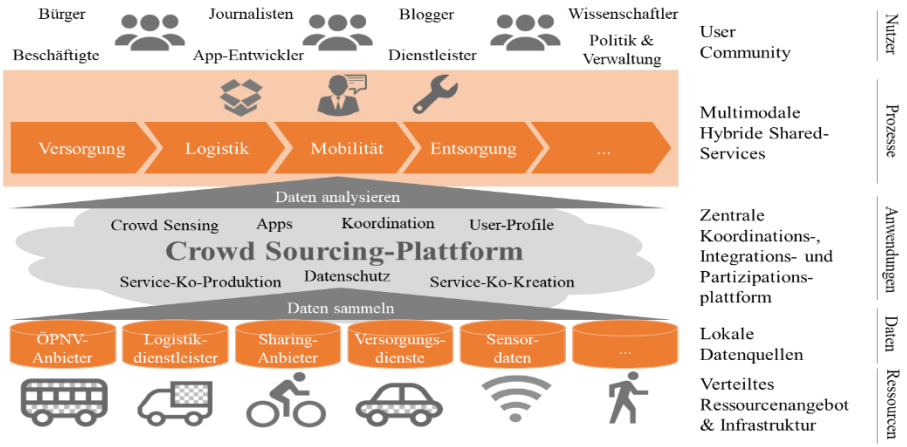


Abbildung 1. Architektur der Crowd Sourcing-Plattform

Dafür werden die Daten aus verschiedenen heterogenen Datenquellen und Anwendungen für stationäre und mobile Mobilitäts- und Versorgungsdienste in der Crowd Sourcing-Plattform gesammelt. Die Ansteuerung und Kopplung der Dienste sowie das Crowd Sensing erfolgen über die integrierte IT-Struktur, die alle Dienste auf der Crowd Sourcing-Plattform zu einer Wertschöpfungskette verbindet. Als offene zentrale Informations- und Partizipationsplattform im Sinne eines Service Marketplace werden die vormals verteilten Einzellösungen in eine Gesamtlösung integriert. Hauptnutzer der Dienste sind Bürger als Privatpersonen sowie auch Beschäftige aus Kernstadt und dem Umland, die selbstbestimmt daran teilhaben können. App-Entwickler können sich kollaborativ an der Weiterentwicklung der Plattform beteiligen und damit Teil der Community werden. Die Bekanntheit der Plattform kann durch Journalisten und Blogger erhöht werden. Mitarbeiter aus Politik und Verwaltung können Rückschlüsse aus den Nutzungszahlen und Bewertungen für notwendige infrastrukturelle Maßnahmen ziehen. Aus der Analyse des Verhaltens des Gesamtsystems und der Einzelkomponenten der Plattform können Wissenschaftler weiteren Forschungsbedarf zur Verbesserung der Smart Sourcing-Plattform ableiten. Die in der Tabelle 1 dargestellten Anforderungen an den Datenschutz können mit Kenntnis der Nutzer der Crowd Sourcing-Plattform spezifiziert werden.

6 Herausforderungen und Forschungsagenda

Es sind v.a. die Bedarfe, Erwünschtheit und Akzeptanz verschiedener Maßnahmen ebenso wie sozioökonomische Ressourcen der Akteure differenziert zu analysieren. Den Akteuren insbesondere die Vorteile aus der Nutzung einer Crowd Sourcing-Plattform aufzuzeigen, wurde als Ergebnisse der Workshops erkannt, da dies als Hauptreiber für die Akzeptanz einer Lösung gesehen wird [11]. Auf dieser Grundlage lassen sich Implementierungs- und Realisierungschancen z.B. soziotechnischer Arrangements beurteilen. Theoretisch orientieren sich die Aufbauarbeiten am Belief-

Action-Outcome (BAO-)Modell [12]. Das Hauptaugenmerk richtet sich dabei auf Einstellungen und Erwartungen (Beliefs) insbesondere bezüglich der Mensch-Technik-Interaktion. Modellhaft dient es zur Entwicklung, Umsetzung und Evaluation von Maßnahmen (Actions) sowie Anreizsystemen für die Verbesserung der Versorgung im Umland von Kernstädten. Ferner dient das BAO-Rahmenwerk der nutzerspezifischen Entwicklung und Anwendung von Methoden zur Messung von Auswirkungen (Outcomes) eingeleiteter Transformationsprozesse. Grundlage bildet eine Analyse der Rahmenbedingungen (Status Quo und Versorgungstrends) mittels standardisierter sowie teilstandardisierter Erhebungen in Kombination mit verfügbaren Statistiken und Registern der Ämter. Die Umsetzung stützt sich ferner auf Ergebnisse von Anforderungsanalysen in Form qualitativer Erhebungen, die in die Erarbeitung von Geschäftsmodellen und in die Konstruktion einer technischen Systemarchitektur einfließen. Dadurch kann eine nutzerbasierte Anwendung ermöglicht werden.

Aktuelle Forschungsfragen, die sich aus der Analyse der Literatur sowie der durchgeführten Workshops und Experteninterviews ergeben, sind:

- Wie lassen sich neue Sharing- und Value-in-Use-Konzepte, Gamification-, Design-Thinking-Ansätze, Open-Innovation und Beteiligungsformen im Sinne von Crowd Sourcing- bzw. Funding-Modellen dafür nutzen, dass Bürger als aktive Prosumer und Ko-Produzenten einen maßgebenden Einfluss auf die Gestaltung ihres unmittelbaren Aktionsraumes in Smart Regions nehmen?
- Welche nachhaltigen Konzepte und Lösungen der Ko-Kreation und Ko-Produktion von hybriden Leistungsbündeln können zur Bündelung logistischer und nicht-logistischer Dienstleistungen z.B. vom Handel, Kurier-, Express- und Paketdiensten, ÖPNV und Handwerk im Hinblick auf die soziodemografischen Herausforderungen in Smart Regions erfolgreich eingesetzt werden?
- Welche Methoden für partizipative Modellierung, Social Forecasting, Empowerment, Lenkung und Anreizsysteme müssen für Crowd Sensing/Ko-Produktion/Crowd Sourcing zur Verfügung gestellt werden?
- Welche Werkzeuge benötigen die Akteursgruppen zur gleichberechtigten Entwicklung von ko-produzierten Mobilitäts- und Versorgungsdiensten?
- Wie kann sichergestellt werden, dass die durch die Crowd Sourcing-Plattform zur Verfügung gestellten Sensordaten und entwickelten Apps/Services über die erforderliche Qualität verfügen sowie nachhaltig sind?
- Welche Chancen und Risiken erzeugen Crowd Sensing Ansätze, AutoID-, Big-Data-, NFC- oder Internet of Things-Anwendungen im Zusammenhang mit den zu entwickelnden hybriden Diensten?
- Welchen Einfluss haben die zu entwickelnden Services bei der Gestaltung eines sachgerechten Gleichgewichts von wirtschaftlich, zivilgesellschaftlich und öffentlich erbrachten Dienstleistungen?

Bei den technischen Entwicklungen wird eine iterative Vorgehensweise gemäß Design Science Ansatz [3] präferiert, um der Schnelllebigkeit des Forschungsgebiets während der 5-jährigen Projektlaufzeit gerecht zu werden. Exemplarische Herausforderungen und Problemaspekte sind als Forschungsagenda bis zum Jahr 2020 dargestellt (vgl. Abbildung 2).

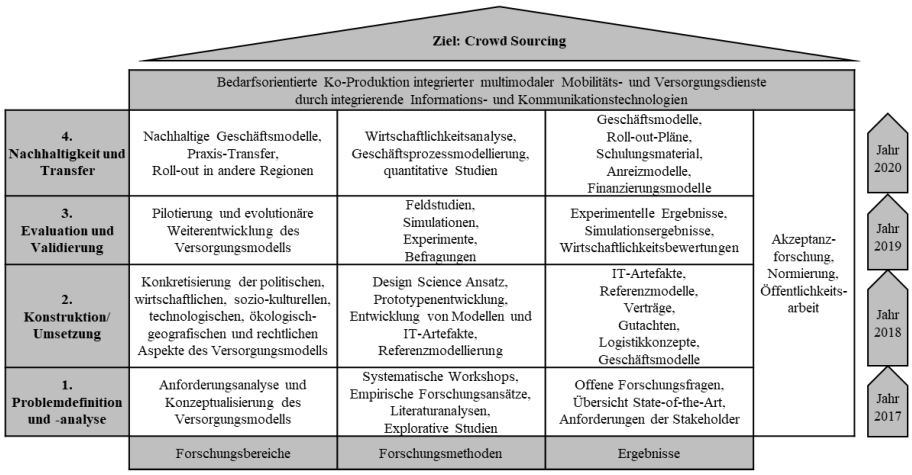


Abbildung 2. Herausforderungen und Problemaspekte (Forschungsagenda bis zum Jahr 2020)

Zur Erreichung des Ziels der Implementierung und nachhaltigen Nutzung einer Crowd Sourcing-Plattform werden verschiedene Schritte durchlaufen. Für die (1.) Problemdefinition und -analyse können zur Anforderungsanalyse und Konzeptualisierung des Versorgungsmodells z.B. systematische Workshops durchgeführt werden, um Anforderungen der Stakeholder zu ermitteln. Zur (2.) Konstruktion/Umsetzung für die Konkretisierung der Aspekte des Versorgungsmodells können z.B. Prototypen entwickelt werden, um erste IT-Artefakte zu gewinnen. Für die (3.) Evaluation und Validierung zur Pilotierung und evolutionären Weiterentwicklung des Versorgungsmodells eignen sich z.B. Feldstudien mit Prototypen. Zur Sicherstellung von (4.) Nachhaltigkeit und Transfer können z.B. Wirtschaftlichkeitsanalysen für die Entwicklung von Geschäftsmodellen eingesetzt werden. Die fortlaufende Akzeptanzforschung, entwicklungsbegleitende Normung durch den Einbezug des Deutschen Instituts für Normung e.V. (DIN) und Öffentlichkeitsarbeit sind unterstützende Maßnahmen für den Einsatz einer Crowd Sourcing-Plattform in Smart Regions.

7 Zusammenfassung und Ausblick

Bisher liegen eher technisch motivierte Einzellösungen vor, die v.a. Lösungen für Kernstädte bieten, wie in Abschnitt 3 verdeutlich wurde. Eine gesamte Abdeckung integrierter multimodaler Mobilitäts- und Versorgungsdienstketten, die in Ko-Produktion von mehreren Akteursgruppen entwickelt und über eine Plattform vernetzt sind, ist noch nicht verfügbar. Ansätze in Wissenschaft, Praxis und Technik fokussieren v.a. Lösungen für Smart Cities. Gerade im Umland von Kernstädten stellen die geringere Einwohnerdichte und die nicht in ausreichendem Umfang vorhandenen Infrastrukturen für zentrale Lebensbereiche wie Mobilität, Versorgung und Logistik eine große Herausforderung dar [13]. Die Erfüllung des Verfassungsgebots nach

Raumordnungsgesetz (ROG) § 1 Abs. 2, gleichwertige Lebensverhältnisse in allen Teilräumen zu gewährleisten, bedarf daher zusätzlicher Anstrengungen in Forschung und Praxis. Smart City-Ansätze können unter Beachtung der integrierenden Crowd Sourcing-Plattform und der spezifischen regionalen Anforderungen auf Smart Regions übertragen werden, was insbesondere für das Umland Vorteile bietet.

8 Danksagung

Dieser Beitrag ist im Rahmen des Projekts „Dorfgemeinschaft 2.0 – Das Alter im ländlichen Raum hat Zukunft (Dorf 2.0)“ entstanden. Das Projekt wird vom Bundesministerium für Bildung und Forschung gefördert (Förderkennzeichen: 16SV7452 und 16SV7453).

Literaturverzeichnis

1. Sikorska, O., Grizelj, F.: Sharing Economy – Sharable City – Smartes Leben. HMD Praxis der Wirtschaftsinformatik 52(4), 502–522 (2015)
2. Martin, N., Lessmann, S., Voß, S.: Crowdsourcing: Systematisierung praktischer Ausprägungen und verwandter Konzepte. In: Bichler, M., Hess, T., Krcmar, H., Lecher, U., Matthes, F., Picot, A., Speitkamp, B., Wolf, P. (eds.) MKWI 2008, pp. 1251–1263. GITO, Berlin (2008)
3. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly 28(1), 75–105 (2004)
4. Dorfgemeinschaft 2.0, http://www.dorfgemeinschaft20.de/ (Abgerufen: 30.08.2017)
5. Fettke, P.: State-of-the-Art des State-of-the-Art. Eine Untersuchung der Forschungsmethode „Review“ innerhalb der Wirtschaftsinformatik. Wirtschaftsinformatik 48, 257–266 (2006)
6. Myers, M.D.: Qualitative Research in Business & Management. SAGE Publications. London (2009)
7. Otto B., Österle H.: Relevance through Consortium Research? Findings from an Expert Interview Study. In: Winter, R., Zhao, J.L., Aier, S. (eds.) Global Perspectives on Design Science Research. DESRIST 2010. LNCS, vol. 6105, pp. 16–30. Springer, Berlin (2010)
8. March, S.T., Smith, G.F.: Design and natural science research on information technology. Decision Support Systems 15(4), 251–266 (1995)
9. Giffinger, R., Haindlmaier, G., Kramar, H.: The role of rankings in growing city competition, Urban Research & Practice 3(3), 299–312 (2010)
10. Leimeister, J.M., Zogaj, S., Durward, D., Blohm, I.: https://www.boeckler.de/pdf/p_study_hbs_324.pdf (Zugegriffen: 29.09.2017)
11. Ermakova, T., Fabian, B., Zarnekow, R.: Acceptance of Health Clouds - A Privacy Calculus Perspective. In: Avital, M., Leimeister, J.M., Schultze, U. (eds.) 22nd European Conference on Information Systems. pp. 1–13, Association for Information Systems, Atlanta (2014)
12. Melville, N.: Information Systems Innovation for Environmental Sustainability. MIS Quarterly 34(1), 1–21 (2010)
13. Bundesministerium für Ernährung und Landwirtschaft: Ländliche Regionen verstehen: Fakten und Hintergründe zum Leben und Arbeiten in ländlichen Regionen. BMEL, Berlin (2016)

Social Media Analytics

Teilkonferenzleitung

Jan Fabian Ehmke
Stefan Stieglitz

Content-Influencer-Fit: Improving Reach and Impact of Content for Influencers in eWOM

Hannes Rothe[1] and Sebastian Wicke[1]

[1] Freie Universität Berlin, Department of Information Systems, Berlin, Germany
hannes.rothe@fu-berlin.de
sebastian.wicke@yahoo.de

Abstract. Marketers who integrate influencers into their advertising strategy seek to improve information reach and information impact of their content. At the same time, influencers are overloaded with information. This design research study proposes a content-influencer-fit model to improve the effectiveness of influencer identification and management. Based on a systematic literature review, interview and usage data from an influencer-marketing platform, this study proposes an attribute framework for marketer-generated content at first. By integrating this framework into a predictive content-influencer-fit model it integrates the discussion on influencer and content characteristics. Finally, the model is able to select influencers on their likelihood to perceive marketer-generated content relevant, which is the basis for content-based recommendation.

Keywords: Influencer marketing, Electronic word-of-mouth, Content-based recommendation systems, Design science research

1 Introduction

Web technologies changed the way consumers attain information about new products and services. They use web pages, video portals, or social networks for information and evaluation purposes [1]. Subsequently, literature on word-of-mouth marketing [2–4] extended its view to inquire the effect of such technologies upon more than face-to-face personal contacts and personal social networks. Even more, the significance of electronic word-of-mouth (eWOM) for consumer behavior rises as traditional marketer-generated content loses ground [5, 6]. Consumers tend to give more trust to information if it is not directly associated to the originator of a product or service [5]. Subsequently, such companies integrate influencers into their advertising strategies.

Influencers regularly have a high reach in specific target groups and promise to leverage on consumer's behavior [7–9]. They may fill the gap of perceived trust in product or service information. Particular examples are web journalists or bloggers [10], twitter users with large follower bases [11], or YouTube channel owners [12]. Marketers provide influencers with targeted information and offers to propagate their products or services to their final target group [13]. For this purpose, they prepare special messages for the intermediate with product information, possible modes of

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

applications, and information on the marketer itself [14]. However, influencers are mostly overloaded with marketer-generated content [15]. Concerning the importance of influencer marketing strategies, we therefore inquire the question: *How can marketers systematically improve the final reach and impact of their content in influencer marketing?*

In this design research study [16, 17], we follow the methodology as proposed by Peffers et al. [18] to create a prescriptive model. We propose a content-influencer-fit model to support marketers in choosing suitable influencers for marketer-generated content. Finally, we shed light on the individual attributes of such content.

2 Targeting Marketer-Generated Content for Influencers

2.1 The role of Influencers in Electronic Word-of-Mouth

Word-of-mouth describes the positive and negative informal communication between consumers about characteristics of a business and/or its goods and services [19]. Electronic word-of-mouth, in comparison, entails the utilization of electronic means of communication for this purpose [20]. Due to the nature of the regular web technologies involved, eWOM is not limited to synchronous one-to-one, but also entails asynchronous one-to-many, or even many-to-many types of communication [20, 21]. The latter type of communication is especially highlighted in current marketing literature. It goes hand in hand with the term "viral marketing" [14, 22], which "departs from traditional advertising in its reliance on consumer word of mouth instead of mass media as the message conveyance vehicle"[12]. Such viral advertising of products and services may be originated by a marketer, but is carried further as "unpaid peer-to-peer communication of provocative content"[23].

Of particular importance are "individuals who were [more] likely to influence other persons in their immediate environment"[24] and who take an intermediating role on the indirect lines of communication between marketers and consumers. They play a key role in initiating or accelerating eWOM communication [7–9, 25–27]. Such influencers – also referred to as opinion leaders or market mavens – not only know how web technologies are applied to information search and propagation for products and services, other web users also have trust in their opinion on both activities [28]. They engage heavily with their environment as they gain many messages and tend to reply or forward these more often [29].

For influencer marketing it is important to understand the motivation of such individuals and their behavior in eWOM [8, 30]. For this purpose, it is also relevant to understand their position on the communication paths in a (social) network [31], as well as the characteristics of message and content [12, 22] sent to them and by them. Typically, influencer marketing consists of two phases: influencer identification and influencer targeting [5]. In the following, we will concentrate on the latter [32].

2.2 Design Parameters for Content Relevance in Influencer Targeting

In most cases, marketers get in touch with influencers via direct messages, such as e-mails or personal contact, to inform them about a product and its specifications. After a further publication, i.e. in forms of an article, a blog post, video or podcast, the message disseminates and gains *information reach*. As consumers receive it, it may trigger an intended effect, such as a buying, lending, renting or informing behavior, which leads to an *information impact* [32–34].

For successful influencer marketing, information reach and information impact need to be considered. However, just raising the amount of messages to influencers does not seem to be effective. Influencers are limited in their resources and time and need to decide quickly on messages for referral [15]. They evaluate the relevance of a message and its content [35], and decide either on its referral or against it. Such messages need to carry useful information for the individual influencer and its target group. Hence, its content has to be close to their needs and interests while be current at the same time [36, 37]. For this reason, we propose our first design parameter, which seeks to incorporate historical data on influencer behavior on marketer-generated content.

Design parameter 1 (DP1): The model predicts the relevance of marketer-generated content for individual influencers (content-influencer-fit)

If a sender of a message is trustworthy in the eye of a recipient, its messages are considered more relevant [38]. At the same time, a lack of trustworthiness reduces the likelihood of message referral [39]. Hence, if influencers get messages by a marketer they as not relevant, this may trigger negative effects on subsequent messages [29, 40]. To raise information reach and impact while at the same time limit negative effects of low reactions from influencers on marketer-generated content, we formulate our second design parameter as follows:

Design parameter 2 (DP1): The model recommends sending content to a selection of influencers with a sufficient content-influencer-fit.

In alignment with both design parameters, we will create a predictive model to assess content-influencer-fit prior to sending marketer-generated content.

3 Content-Influencer-Fit Model

3.1 Method

In the following, we describe our development of a content-influencer-fit model, which fulfills both design parameters and finally seeks to raise information reach and impact in influencer marketing. As we focus on marketer-generated messages, we concentrate on a content-based predictive model [41]. Our design research study follows an iterative and prototypical development, testing, and learning process [42] to create a prescriptive and abstract model [43]. For this purpose, we apply the procedural model proposed by Peffers et al. [18]. The prior sections already outlined (1) problem and context as well the (2) design parameters of the model. To test our assumptions, we inquired six

influencer-marketing platforms on their capacity to fulfill DP1 and DP2 and interviewed two platform owners.

In the following, we outline the (3) development of the artifact, which followed two steps. At first, we iteratively created an (3a) attribute framework for describing marketer-generated content. For this purpose, we systematically reviewed literature on influencer marketing [44]. Afterwards, we applied the attribute framework to real marketer-generated content to (3b) predict influencer behavior and assess the importance of particular attributes of content on influencer behavior. While several predictive models for classification are potentially useful in this scenario, we focused on probabilistic techniques to assess the likelihood of content relevance for influencers. We chose to test two classification models, a Naive Bayes Classifier and a logistic regression model [45, 46], and after first iterations on the data, finally decided for the latter. Following an iterative design research procedure, our (4) evaluation entails artificial and naturalistic methods of artifact evaluation [47] as we abductively design a prescriptive model and test it on real-world data. Figure 1 summarizes our approach.

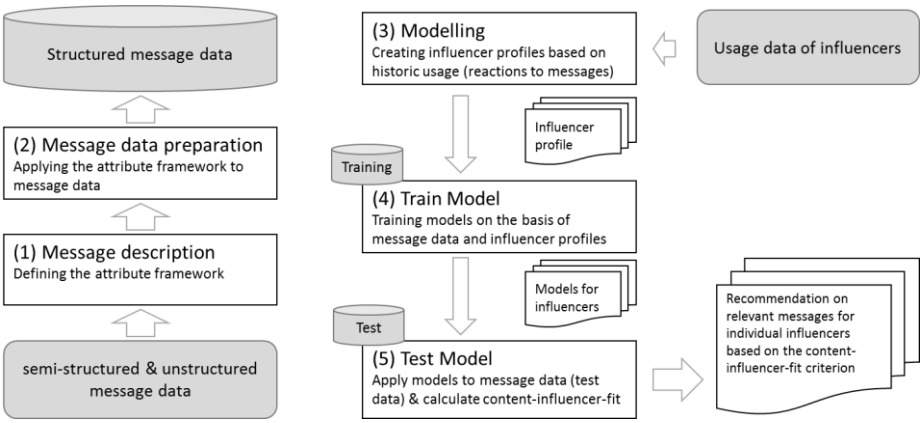


Figure 1 Procedure for designing a content-based recommendation system [45] we followed as part of the design phase in design science research methodology [18]

3.2 Attribute Framework for Marketer-Generated Content

A systematic literature review [44] on attributes, conceptualizations, or categorizations of content for influencers or consumers in eWOM revealed 56 publications. We queried focal libraries (Science Direct, EBSCO Business Source Premier, Web of Science and Scopus) concerning eWOM, message, and attributes (including synonyms). A backward- and forward search led to additional 14 articles. Most publications (>87%) have been published since 2011.

To assess the suitability of content for influencers, marketers need to consider both, its attributes as well as preferences of individual influencers [48–50]. However, only two publications explicitly focus on the relationship between particular content attributes and their effects on influencer's publication and referral behavior [29, 36]. In sum, we found 37 attributes from the literature review and sorted them into four

categories. We discern between the **(a) formal quality**, **(b) informativity**, **(c) emotionality**, and **(d) other attributes** of a message. We coded the messages according to the attribute framework. After applying the result of our systematic literature review to five percent of the data, we added three additional attributes inductively (see table 1) from the interviews and from the additional meta-information provided by our case data. The following section presents the data set we used to train and test the model.

3.3 Data

We applied data from a local influencer-marketing platform "MoreImpact" (anonymized). Marketers use the platform to send messages to registered influencers from YouTube, Instagram, and Facebook. MoreImpact presents marketer-generated content as an offer for referral on its platform. Influencers react to these by explicitly signaling their interest. We applied data from messages to YouTube-influencers to limit a potential bias from diverging behavior between influencers on different networks. All influencers on MoreImpact have at least 1000 subscribers. We attained data on 415 messages from January 2015 to June 2016. The dataset also includes text, image, and metadata. We applied usage data from reactions of 674 active influencers on 4019 events in that timespan to the model. Each event represents an influencer who either reacted or not reacted to a message provided by MoreImpact. However, besides from 28 individuals most influencers lack a minimal activity needed for proper classification [46] per influencer. Minimal activity has been set to 15 positive reactions, which account for five percent of the overall positively coded messages.

Most of the attributes were human coded. However, we also automated coding of some attributes. Readibility was coded by applying the Flesch-Reading-Ease-Metric [52], supported by the web service Fleschindex.de. The length of a message was calculated by the number of characters in each string. "Language negativity and positivity" as well as "Degree of positivity of language" were coded by performing a sentiment analysis on the messages [22, 71]. After considering cross-correlations (correlations between attributes > 0.5) and after applying a variance-filter on binary attributes (variance < 0.1), the model contained 27 attributes.

The target variable for the predictive classification model reflects the reaction of an influencer to an offer provided by marketer-generated content on a binary scale. For this purpose, we controlled for the registration date of the influencer on MoreImpact in comparison to when messages were provided.

Table 1 Attribute framework for marketer-generated content (attributes applied to the models are marked with *)

Attributes on Formal Quality	**Informativity Attributes**
Error-free text [38] *	Experiential product characteristics [56]
Sufficient media quality [51] *	Application domain [57, 58]
Media comprehensibility [inductive] *	Branch [59] *
Readability [52] *	Market stage [60] *
Product comprehensibility [53] *	Luxury product [61]
Comprehensibility of marketer aim [inductive] *	Niche product [62] *
Time of content placement [54]	Stage of development [63]
Image placement [39] *	Product availability [4]
Video placement [39] *	Distribution channels [64] *
Link placement [55]	Price information [65, 66] *
Length [48] *	Specific advertising campaign [49] *
	Product utility explanation [65, 66] *
	List of (product) specifications [63, 64] *
	Comparison with other products [67] *
	Information on market performance [68]
	Application for target group exemplified [67]*
	Independent studies and tests [65, 66]
Emotionality Attributes	**Other Attributes**
Language negativity / positivity [22] *	Incentives [27, 49]*
Degree of positivity of language [22]	Amount of product specific information [65] *
Exemplification through (personal) storytelling [37] *	*Pre-specified video content type ("Review","Haul", "Mention", "Favorite", "Tutorial" , "Lookbook") [inductive]* *
Interactivity with recipient [6] *	
Explicit call to action for influencer [49, 69] *	
Humor [59, 69]	
Message originality [22]	
Product originality [22, 70]*	

3.4 Iterative Design of the Content-Influencer-Fit Model

We designed the models in five steps. For each iteration, we sampled the data into 20 percent training data and 80 percent test data using a stratified sampling method in relation to the target variable [41]. In a first step, we performed a pre-test on a

subsample of five highly active influencers (830 positive and negative reactions). We applied two predictive modelling techniques, a naive Bayes classifier and logistic regression. On our data set, both techniques are fundamentally able to predict the reaction probability of an influencer to marketer-generated content with the coded attributes (see table 1). This probability represents the *content-influencer-fit*.

Subsequently, these techniques assess the individual relevance of a message for an influencer as demanded by DP1. However, DP2 calls for a minimal quality of recommendation. For this reason, we evaluated both techniques on their prediction quality measuring accuracy and the F-measure for individual models of influencers [72]. Accuracy describes the ratio of correct classifications to all classifications. The F-measure, in comparison is a weighted harmonic mean between recall and precision of the model. While the accuracy of naive Bayes is about ten percent higher than logistic regression (0.77 to 0.84), the F-Measure is overall 33 percent higher (0.17 to 0.23). It can largely be explained by a relatively higher recall of logistic regression (0.25 to 0.12) in comparison to an only mildly lower precision (0.21 to 0.29) on average. As accuracy remains relatively high, we considered reducing false negatives in this case as more important than false positives. Subsequently, we moved on with a logistic regression technique and predicted the outcome for the 28 influencers who showed a minimum reaction to 15 marketer-generated messages.

Table 2 A 5x5 excerpt from the content-influencer-fit matrix

Influencer ID	**Message ID 517**	**Message ID 509**	**Message ID 506**	**Message ID 494**	**Message ID 427**
3870	0	0.000001	0	0	**0.998379**
292	0.013985	0.231794	0.01477	0.956613	0.734248
2918	0	0	0	0	**1**
3166	**1**	0	**0.992319**	**0.981688**	0
1188	0	0.000504	**0.999985**	0	0

DP2 demands a minimal content-influencer-fit as a threshold to contact influencers. To find an optimal threshold value, we chose to optimize the receiver operating characteristic (ROC) curve of the model to raise its precision, and contribute to a higher F-measure. In an iterative optimization process, we tested various threshold values and finally derived a minimal content-influencer-fit of 0.97. In comparison to the initial threshold of 0.5, we were able to raise precision by 0.11. Table 2 gives an overview on the results of the predictive analysis as presented in an excerpt of the content-influencer-fit matrix.

3.5 Evaluation

Design science research asks for a rigorous design process and a relevant artifact [17]. With regards to the latter, studies need to give proof to the artifact's usefulness [16]. For this purpose, the artifact needs to solve a relevant problem and fulfill the derived

design parameters [18]. A systematic literature based problem definition and iterative design already represents first steps of a formative, ex-ante evaluation [47, 73, 74]. An inquiry into current influencer marketing platforms on the market together with two interviews with platform owners support our problem definition and design principles as part of the ex ante evaluation. One platform owner subsumed, that "such a function would be a real gain for our platform to create more value and provide additional service to our linked companies and influencers". The other complemented this by saying: "no other providers has such a function at the moment, even though the importance of such a solution is by all means decisive." Throughout the iterative design process of the attribute framework and the predictive model, we performed ex post summative and naturalistic evaluations, as we evaluated the model performance on real world data [47, 75]. The chosen metrics are sufficient for classification-based artifacts [17].

The results of this study are nonetheless also limited. The data focused on YouTube as one advertising platform for influencers. Regarding an inductive addition of attributes which refer to pre-defined video content types (i.e., haul, tutorial, lookbook etc.), we assume, other mediums will add further attributes or characteristics. While we created clear definitions for human coding of the attributes, the framework needs further testing, especially with regards to subjective codes, such as "originality" or "availability of a product". Classifying 335 marketer-generated messages for 28 influencers on average leads to 9,380 classification decisions overall. Even while this is sufficient to test a predictive model with 27 attributes, additional influencers would add a larger variety of individual preferences into the training and test data set.

4 Summary and Contribution

Improving information reach and information impact of marketer-generated content is of decisive relevance for influencer marketing platforms and marketers, alike. However, current solutions for marketers to contact influencers mirror this only partially. Based on two design perimeters, this study proposes three important contributions. First, we present an attribute framework for marketer-generated content. Publications in the field of eWOM tend to reflect only particular attributes and rarely focus on specific target groups such as influencers [29, 36].

Second, we adopt the framework to design a predictive content-influencer-fit model. We integrate the separated discussions on influencer characteristics and attitude [3, 76] on one side, and content characteristics on the other [48].

Third, we find that influencers largely differ in their relevance criteria of marketer-generated content, which may be caused by the variety of underlying motivations to share the content [30]. However, a few patterns emerge, as some attributes tend to raise the content-influencer-fit for many influencers. Concerning the formal quality of marketer-generated content, readability of a message and a comprehensive use of additional media raises the likelihood that an influencer reacts positively mostly in all cases. From an informativity perspective, explaining the utility of a product or service as well as exemplifying the application for a specific target group shows mostly positive effects. Finally, we find that if marketers require a certain type of publication from the

influencer, such as a “Mention” or “Tutorial”, it may raise the likelihood of a positive reaction. At the same time, other types, such as a lookbook, unanimously reduces it. Further behavioral research might inquire these patterns more deeply to propose recommendations for fitting the content to particular influencers.

The content-influencer-fit model, however, considers individual relevance criteria; a subsequent recommendation of influencers for given marketer-generated content is able to reduce the amount of irrelevant content and lowers the information overload.

Bibliography

1. Smith, A.N., Fischer, E., Yongjian, C.: How does brand-related user-generated content differ across YouTube, Facebook, and Twitter? J. Interact. Mark. 26, 102–113 (2012).
2. Arndt, J.: Role of product-related conversations in the diffusion of a new product. J. Mark. Res. 291–295 (1967).
3. Wiedmann, K.-P., Hennigs, N., Langner, S.: Categorizing the Potential and Value of WOM-Referrals: Towards a Comprehensive Typology of Social Influencers. Mark. Theory Appl. 22 (2007).
4. Berger, J., Schwartz, E.M.: What drives immediate and ongoing word of mouth? J. Mark. Res. 48, 869–880 (2011).
5. Brown, D., Hayes, N.: Influencer marketing: Who really influences your customers? Routledge (2008).
6. Alboqami, H., Al-Karaghouli, W., Baeshen, Y., Erkan, I., Evans, C., Ghoneim, A.: Electronic word of mouth in social media: the common characteristics of retweeted and favourited marketer-generated content posted on Twitter. Int. J. Internet Mark. Advert. 9, 338–358 (2015).
7. Chen, Y.-R.R., Fu, J.S.: How to be heard on microblogs? Nonprofit organizations’ follower networks and post features for information diffusion in China. Information, Commun. Soc. 19, 978–993 (2016).
8. Palka, W., Pousttchi, K., Wiedemann, D.G.: Mobile word-of-mouth–A grounded theory of mobile viral marketing. J. Inf. Technol. 24, 172–185 (2009).
9. Wang, Y., Li, Y.: Proactive Engagement of Opinion Leaders and Organization Advocates on Social Networking Sites. Int. J. Strateg. Commun. 10, 115–132 (2016).
10. Uzunoğlu, E., Kip, S.M.: Brand communication through digital influencers: Leveraging blogger engagement. Int. J. Inf. Manage. 34, 592–602 (2014).
11. Bakshy, E., Hofman, J., Mason, W., Watts, D.: Everyone’s an influencer: quantifying influence on twitter. Proc. fourth ACM Int. Conf. Web search data Min. SE - WSDM ’11. 65–74 (2011).
12. Liu-Thompkins, Y., Rogerson, M.: Rising to Stardom: An Empirical Investigation of the Diffusion of User-generated Content. J. Interact. Mark. 26, 71–82 (2012).
13. Matthews, K.: The Definitive Guide to Influencer Targeting, (2014).
14. Deng, C., Lu, Y., Ravichandran, T., He, X.: What Makes Video Ads Viral: Quantifying the Impact of Marketer-and User-Generated Content. In: Twenty-second American Conference on Information Systems. , San Diego, USA (2016).
15. Harrigan, N., Achananuparp, P., Lim, E.-P.: Influentials, novelty, and social contagion: The viral power of average friends, close communities, and old news. Soc. Networks. 34, 470–480 (2012).
16. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. Manag. Inf. Syst. Q. 37, 337–355 (2013).

17. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in Information Systems research. MIS Q. 28, 75–105 (2004).
18. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. J. Manag. Inf. Syst. 24, 45–77 (2007).
19. Westbrook, R.A.: Product/consumption-based affective responses and postpurchase processes. J. Mark. Res. 258–270 (1987).
20. Berger, J., Iyengar, R.: Communication channels and word of mouth: How the medium shapes the message. J. Consum. Res. 40, 567–579 (2013).
21. Moore, M.G.: Editorial: Three types of interaction. (1989).
22. Berger, J., Milkman, K.L.: What makes online content viral? J. Mark. Res. 49, 192–205 (2012).
23. Porter, L., Golan, G.J.: From subservient chickens to brawny men: A comparison of viral advertising to television advertising. J. Interact. Advert. 6, 30–38 (2006).
24. Katz, E., Lazarsfeld, P.F.: Personal Influence, The part played by people in the flow of mass communications. Transaction Publishers (1966).
25. Clement, M., Proppe, D., Sambeth, F.: Der Einfluss von Meinungsführern auf den Erfolg von hedonischen Produkten. Zeitschrift für Betriebswirtschaft. 76, 797–824 (2006).
26. Dobele, A., Lindgreen, A., Beverland, M., Vanhamme, J., Van Wijk, R.: Why pass on viral messages? Because they connect emotionally. Bus. Horiz. 50, 291–304 (2007).
27. Dasari, S., Anandakrishnan, B.: Viral marketing of retail products: A study on the influence of attributes of web portals and incentives offered on user registrations. IUP J. Mark. Manag. 9, 99 (2010).
28. Belch, M.A., Krentler, K.A., Willis-Flurry, L.A.: Teen internet mavens: influence in family decision making. J. Bus. Res. 58, 569–575 (2005).
29. Phelps, J.E., Lewis, R., Mobilio, L., Perry, D., Raman, N.: Viral marketing or electronic word-of-mouth advertising: Examining consumer responses and motivations to pass along email. J. Advert. Res. 44, 333–348 (2004).
30. Walsh, G., Gwinner, K.P., Swanson, S.R.: What makes mavens tick? Exploring the motives of market mavens' initiation of information diffusion. J. Consum. Mark. 21, 109–122 (2004).
31. Watts, D.J., Dodds, P.S.: Influentials, networks, and public opinion formation. J. Consum. Res. 34, 441–458 (2007).
32. Brown, D., Fiorella, S.: Influence marketing: How to create, manage, and measure brand influencers in social media marketing. Que Publishing (2013).
33. Lindenmann, W.K.: An'effectiveness yardstick'to measure public relations suc. Public Relations Q. 38, 7 (1993).
34. Francalanci, C., Hussain, A.: Discovering social influencers with network visualization: evidence from the tourism domain. Inf. Technol. Tour. 16, 103–125 (2016).
35. O'Reilly, K., MacMillan, A., Mumuni, A.G., Lancendorfer, K.M.: Extending our understanding of eWOM impact: The role of source credibility and message relevance. J. Internet Commer. 15, 77–96 (2016).
36. Bobkowski, P.S.: Sharing the news: Effects of informational utility and opinion leadership on online news sharing. Journal. Mass Commun. Q. 92, 320–345 (2015).
37. Kim, H.S.: Attractability and virality: The role of message features and social influence in health news diffusion. University of Pennsylvania (2014).
38. Huang, C.-C., Lin, T.-C., Lin, K.-J.: Factors affecting pass-along email intentions (PAEIs): Integrating the social capital and social cognition theories. Electron. Commer. Res. Appl. 8, 160–169 (2009).

39. Liu, Z., Liu, L., Li, H.: Determinants of information retweeting in microblogging. Internet Res. 22, 443–466 (2012).
40. Miquel-Romero, M.-J., Adame-Sánchez, C.: Viral marketing through e-mail: the link company-consumer. Manag. Decis. 51, 1970–1982 (2013).
41. Basu, C., Hirsh, H., Cohen, W.: Recommendation as classification: Using social and content-based information in recommendation. In: Aaai/iaai. pp. 714–720 (1998).
42. Hevner, A.R.: A Three Cycle View of Design Science Research. Scand. J. Inf. Syst. 19, Article 2 (2007).
43. Barquet, A.P., Wessel, L., Rothe, H.: Knowledge Accumulation in Design-Oriented Research. In: International Conference on Design Science Research in Information Systems. pp. 398–413. Springer (2017).
44. vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. Commun. Assoc. Inf. Syst. 37, 205–224 (2015).
45. Lops, P., De Gemmis, M., Semeraro, G.: Content-based recommender systems: State of the art and trends. In: Recommender systems handbook. pp. 73–105. Springer (2011).
46. Ng, A.Y., Jordan, M.I.: On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes. In: Advances in neural information processing systems. pp. 841–848 (2002).
47. Venable, J., Pries-Heje, J., Baskerville, R.: FEDS: a framework for evaluation in design science research. Eur. J. Inf. Syst. 25, 77–89 (2016).
48. Chen, Y.-L., Tang, K., Wu, C.-C., Jheng, R.-Y.: Predicting the influence of users' posted information for eWOM advertising in social networks. Electron. Commer. Res. Appl. 13, 431–439 (2014).
49. Son, I., Kim, Y., Lee, D.: The Role of Message Content and Source User Identity in Information Diffusion on Online Social Networks. Asia Pacific J. Inf. Syst. 25, 239–264 (2015).
50. Petrescu, M.: Viral advertising: Conceptual and empirical examination of antecedents, context and its influence on purchase intentions. Florida Atlantic University (2012).
51. Fang, Y.H., Li, C.Y.: Electronic word-of-mouth on social networking sites: Cue validity and cue utilization perspectives. Hum. Syst. Manag. 35, 35–50 (2016).
52. Heimbach, I., Schiller, B., Strufe, T., Hinz, O.: Content Virality on Online Social Networks: Empirical Evidence from Twitter, Facebook, and Google+ on German News Websites. In: Proceedings of the 26th ACM Conference on Hypertext & Social Media. pp. 39–47. ACM (2015).
53. Tam, D.D., Khuong, M.N.: The Effects of Guerilla Marketing on Gen Y's Purchase Intention--A Study in Ho Chi Minh City, Vietnam. Int. J. Trade, Econ. Financ. 6, 191 (2015).
54. Shen, C., Kuo, C.-J.: Learning in massive open online courses: Evidence from social media mining. Comput. Human Behav. 51, 568–577 (2015).
55. Sabate, F., Berbegal-Mirabent, J., Cañabate, A., Lebherz, P.R.: Factors influencing popularity of branded content in Facebook fan pages. Eur. Manag. J. 32, 1001–1011 (2014).
56. Lin, T.M.Y., Lu, K.-Y., Wu, J.-J.: The effects of visual information in eWOM communication. J. Res. Interact. Mark. 6, 7–26 (2012).
57. Chen, K., Kim, J., Lin, J.: The effects of affective and cognitive elaborations from Facebook posts on consumer attitude formation. J. Consum. Behav. 14, 208–218 (2015).
58. Schulze, C., Schöler, L., Skiera, B.: Not all fun and games: Viral marketing for utilitarian products. J. Mark. 78, 1–19 (2014).
59. Golan, G.J., Zaidner, L.: Creative Strategies in Viral Advertising: An Application of Taylor's Six-Segment Message Strategy Wheel. J. Comput. Commun. 13, 959–972 (2008).

60. Swani, K., Brown, B.P., Milne, G.R.: Should tweets differ for B2B and B2C? An analysis of Fortune 500 companies' Twitter communications. Ind. Mark. Manag. 43, 873–881 (2014).
61. Daugherty, T., Hoffman, E.: eWOM and the importance of capturing consumer attention within social media. J. Mark. Commun. 20, 82–102 (2014).
62. Meiseberg, B.: The Effectiveness of E-tailers' Communication Practices in Stimulating Sales of Niche versus Popular Products. J. Retail. 92, 319–332 (2016).
63. Kim, H.-J., Son, I.-S., Lee, D.-W.: The viral effect of online social network on new products promotion: Investigating information diffusion on twitter. J. Intell. Inf. Syst. 18, 107–130 (2012).
64. Nguyen, C., Romaniuk, J.: Pass it on: A framework for classifying the content of word of mouth. Australas. Mark. J. 22, 117–124 (2014).
65. Resnik, A., Stern, B.L.: An analysis of information content in television advertising. J. Mark. 50–53 (1977).
66. Abernethy, A.M., Franke, G.R.: The information content of advertising: A meta-analysis. J. Advert. 25, 1–17 (1996).
67. Weathers, D., Swain, S.D., Grover, V.: Can online product reviews be more helpful? Examining characteristics of information content by product type. Decis. Support Syst. 79, 12–23 (2015).
68. Nguyen, T., Shi, W.: Improving resource efficiency in data centers using reputation-based resource selection. Sustain. Comput. Informatics Syst. 2, 138–150 (2012).
69. Hsieh, J.K., Hsieh, Y.C., Tang, Y.C.: Exploring the disseminating behaviors of eWOM marketing: Persuasion in online video. Electron. Commer. Res. 12, 201–224 (2012).
70. Moldovan, S., Goldenberg, J., Chattopadhyay, A.: The different roles of product originality and usefulness in generating word-of-mouth. Int. J. Res. Mark. 28, 109–119 (2011).
71. Waltinger, U.: An empirical study on machine learning-based sentiment classification using polarity clues. In: International Conference on Web Information Systems and Technologies. pp. 202–214. Springer (2010).
72. Provost, F., Fawcett, T.: Data Science for Business: What you need to know about data mining and data-analytic thinking. " O'Reilly Media, Inc." (2013).
73. Venable, J., Pries-Heje, J., Baskerville, R.: A Comprehensive Framework for Evaluation in Design Science Research. In: Peffers, K., Rothenberger, M., and Kuechler, B. (eds.) Design Science Research in Information Systems. Advances in Theory and Practice SE - 31. pp. 423–438. Springer Berlin Heidelberg (2012).
74. Pries-Heje, J., Baskerville, R., Venable, J.R.: Strategies for design science research evaluation. In: ECIS 2008 Proceedings. , Galway (Ireland) (2008).
75. Sonnenberg, C., vom Brocke, J.: Evaluation patterns for design science research artefacts. In: Practical Aspects of Design Science. pp. 71–83. Springer (2012).
76. Heidemann, J., Klier, M., Probst, F.: Identifying key users in online social networks: A pagerank based approach. (2010).

Sorting Out the Lemons – Identifying Product Failures in Online Reviews and their Relationship with Sales

Dominik Gutt[1]

[1] Paderborn University, Business Administration and Economics, Paderborn, Germany
{dominik.gutt}@uni-paderborn.com

Abstract. It is well-established that both average online ratings and the number of ratings positively impact product sales. Yet, the economic implications of the information contained in the online review texts are not that well understood. In this study, we contribute to the understanding of online review texts and their economic implications by conducting and validating an unsupervised machine learning algorithm, the latent dirichlet allocation, to identify online reviews that mention product failures. We show that the textual information on product failures are associated with lower product sales. Our results help online review system designers identifying these reviews and to make them easily accessible to potential customers to support their purchasing decisions. Academics can build on our results by applying our validated topic identification strategy and by linking reviews mentioning product failure to a range of different outcomes.

Keywords: Latent dirichlet allocation, text mining, online reviews

1 Introduction

User-generated social media, in particular online reviews, are a key success factor for businesses because they help erode the information asymmetry between sellers and buyers prior to purchase. Unsurprisingly, the positive economic impact of several metrics of online ratings, such as the average online rating score of a business [1] or the sheer number of online reviews [2, 3], is increasingly well understood. However, online reviews do not only consist of a rating score, commonly on a scale from 1 to 5, but usually also comprise a review text written by the reviewer. Currently, little is known about the economic impact of online review texts. Yet, review text can contain highly valuable information to the customer that probably play a role in her purchasing decisions.

Reviews that contain information about product failures (e.g., malfunctioning of electronic devices) are of particular interest for a number of reasons. For instance, (i) because they might affect economic success negatively [4], (ii) because firms can use them to improve their own product [5], or (iii) because they the assist future customers in making a purchase decision [6]. However, while customers can easily compare the average rating and the number of reviews of a seller or a business, review texts are much more difficult and time-consuming to assess, analyze, and compare. Thus, this

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

study attempts to narrow the research gap on impacts of online review texts on economic outcomes by proposing and validating a machine learning approach to identify online reviews that contain information on product failures. In particular, we would like to answer the following two research questions: 1. *Can we automatically identify online reviews that focus on product failure?* 2. *What is the relationship between online reviews that focus on product failure and economic success?*

To answer these two questions, first, this research in progress applies an unsupervised machine learning approach – the latent dirichlet allocation (LDA, [7]) – to automatically identify the online reviews that mention product failure (*failure reviews*) in a large data set of online reviews for digital cameras from amazon.com. Second, we validate the identification of the failure reviews that resulted from our LDA using manual coders. Third, we conduct regression analyses to examine the association between product failures and sales performance of digital cameras. Our preliminary results indicate that the automatic identification approach is well capable of reliably capturing the failure reviews in our dataset and that failure reviews are, as expected, negatively associated with sales performance. To the best of our knowledge, we are the first to automatically identify and manually validate mentions of product failures in online reviews, as well as quantifying the relationship of these reviews with sales. Based on our results, online rating websites could use this approach to identify and tag failure reviews so website visitors can easily identify these reviews to make better purchasing decisions. This identification can help sellers filtering out failure reviews from all the reviews they receive to either respond to these reviews or further improve their product.

2 Related Literature

A large body of literature has delivered empirical evidence collated from across different industries supporting the claim that there is a positive effect of numerical online ratings. These include the effect of average ratings [1, 2, 8], and the number of ratings [2, 3] on online and offline sales of, for example, movies [9], books [2], and restaurants [1].

A nascent stream of research investigated possible ways to leverage the information contained in online review texts. Studies have demonstrated that the textual information in online reviews can be used to predict the pricing power of products [10] or that review texts can be used for the inference and surveillance of market structure [11]. There are two studies pursing a similar goal to our study, but they differ substantially with regards to the applied methodology and the aim of their research. One study leverages human coders to build a logistic regression framework to detect defects in cars and consumer electronics [12]. Another study identifies potentially dangerous toys from online reviews by using a catchword list obtained through a sampling approach [13]. Our study contributes to both of these streams by proposing and validating a quick, automated machine learning approach to identify one specific topic in online reviews, namely product failures, and by relating this topic to economic outcomes.

3 Topic Modelling and Empirical Analysis

We obtained a data set from amazon.com containing 29,332 single online reviews of 1,146 digital cameras [14] that were collected in July 2014 and contain all reviews from May 1996 until the time of collection. We chose digital cameras for our analysis because they can exhibit product failure in a straightforward way but also comprise substantial share of experience attributes that can be described in the reviews (e.g., usability, picture quality, etc.) Based on the online reviews, we computed the average ratings (AVG_RATING), the number of ratings (NUM_REVIEWS), and the variance of ratings (VARIANCE), as depicted in Table 1.

Table 1. Descriptive Statistics

Variable	N	Mean	Std. Dev.	Min	Max
SALES_RANK	1,128	10,930.72	10,086.21	12	155,504
NUM_FAILS	494	2.014	1.887	1	21
PRICE (in US Dollar)	1,051	141.71	169.489	0.01	899
AVG_RATING	1,146	4.067	0.491	1	5
NUM_REVIEWS	1,146	25.595	33.774	5	280
VARIANCE	1,146	1.210	0.683	0	3.551

3.1 Identification of Product Failure Reviews

To identify failure reviews in our large data set of online reviews, we employ probabilistic topic modeling based on LDA. LDA is a widely-used unsupervised machine learning method that can identify topics in large collections of documents, in our case online reviews, with written text. The essential idea behind LDA, according to Blei et. al [7], is that the authors compose documents *D* by first deciding about a discrete distribution of topics *T* to write about, relying on words *W* from a discrete distribution of words that are typical for the chosen topic. Put differently, a document is defined by a probability distribution over a fixed set of topics and each topic is defined by a probability distribution over a limited set of words [15]. For each topic of the fixed set of topics, the LDA assigns a probability between 0 and 1 to each document, indicating how likely it is that this particular document belongs to a certain topic.

The LDA approach has several advantages over alternative identification approaches. First, this approach can handle large amounts of documents in very short time. Prior literature, e.g., in the field of marketing, has traditionally relied on manual coders to identify topics in online reviews [16]. This approach is very time consuming, costly, and difficult to replicate. Our approach circumvents these limitations. Second, it seems plausible that our underlying data suits the LDA assumption that there is a fixed set of topics underlying the documents. Accordingly, recent studies have highlighted the suitability of LDA to analyze online reviews [15].

Before running the LDA using the web service minemytext.com, we applied standard measures of data pre-processing as suggested in the literature [15]. In particular, we applied stemming, 316 standard stop words (to remove uninformative

words), and we set the n-gram to 1. As the LDA relies on a fixed number of topics that has to be determined by the researcher before running the analysis, the results obtained can depend on the number of topics chosen. As suggested in the literature [15], we tried several different specifications with different numbers of topics (between 15 and 80 topics) and evaluated the quality of the results by reading samples of the reviews marked as failure reviews and comparing the mean rating of the failure reviews with the remaining ones. The LDA that yielded the best results after visual inspection comprises 40 topics, which is within the range of 10 and 50 topics usually proposed in the literature [15].

Within the LDA specification of 40 topics, there was exactly one topic capturing the failure reviews, which we identified by reading the most frequently occurring words. These are camera (7.19%), len(se) (3.02%), problem (2.77%), repair (2.3%), replace (1.35%), fix (1.3%), and defect (0.51%). As each review has a probability between 0 and 1 for each topic, we identified failure reviews as those reviews that had the highest probability, amongst all possible topics, for the above mentioned topic (*failure topic*). In total, our LDA analysis identifies 650 failure reviews within the entire data set of 29,332. As expected, the mean rating of the failure reviews (2.13) is substantially lower than the mean rating of the reviews excluding failure reviews (4.24). As depicted in Figure 1, the shape of the non-failure review distribution resembles the classical J-shape of online reviews [17] whereas the distribution of the failure reviews resembles a perfect inverted J-shape. Therefore, failure reviews are associated with substantially lower rating scores than non-failure reviews. However, there are also some, but not many, 4 and 5 star ratings, which might occur if product failures happened after a longer period of consumption that satisfied the customer.

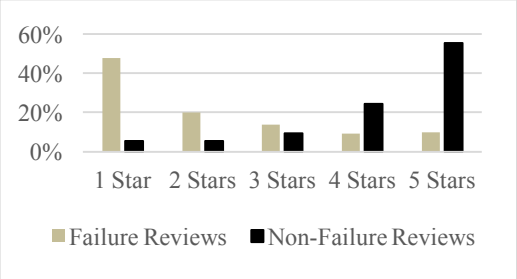


Figure 1. Distribution of Failure and Non-Failure Reviews

3.2 Validation and Estimation Results

In a next step, we validate the results of our topic modeling LDA approach to rule out concerns that our algorithm fails to capture some failure reviews or mistakenly classifies reviews as failure reviews that do not mention any product failure at all. A prime way to do this is by human manual coding and calculate the interrater reliability between the human coding results and the LDA results. We relied on such manual human coding conducted independently by two student assistants. The assistants were asked to read a sample of reviews (without any other information such as the rating or

the brand) and determine review-by-review whether the reviews mentioned product failures or not. Because the entire data contains too many reviews to be handled by humans, we took a random sample of our data comprising 300 reviews (following [18]). Parametric and non-parametric tests of variables such as SALES_RANK, AVG_RATING, and PRICE do not show statistically significant differences between the entire data set and the random sample, thus, we conclude that the random sample is representative of the whole sample. The results of the agreement between the LDA and the human coders are depicted in Table 2.

Table 2. Interrater Agreement between LDA and Human Coders

	%-Agreement	N	Krippendorff's Alpha	Cohen's Kappa
LDA & C 1	97.99%	300	0.740	0.740
LDA & C 2	98.33%	300	0.806	0.806
LDA & C1 & C2	99.00%	300	0.808	0.875

At first glance, one can see that the agreement between the LDA and coder 1 (C1) and coder 2 (C2) is very high in percent (between 97.99% and 99%). This is reconfirmed based on Krippendorff's Alpha and Cohen's Kappa, two conservative standard indices for evaluating interrater agreement [18]. Levels of 0.7 for K's Alpha and C's Kappa are sufficient to conclude interrater agreement and levels above 0.8 indicate large interrater agreement [18]. Based on the results of interrater agreement between the human coders and the LDA, we conclude that our automatic topic modelling approach has reliably captured almost all failure reviews contained in our data set. This also reassuring with regard to our choice of the number of topics (40) and the data pre-processing steps, as these choices have obviously enabled a very robust identification of failure. Finally, we would like to assess the association between the number of failure reviews on a product level and the economic performance of a camera, measured by the sales rank. Like Chevalier and Mayzlin [2], we use the Schnapp - Allwine methodology (LN_SALES_RANK=9.61 – 0.78*ln(SALES_RANK) to translate the sales rank into the natural log of the sales rank for which higher values indicate higher sales.

Table 3. Linear Regression Results

Model	(1)	(2)
Variable	LN_SALES_RANK	LN_SALES_RANK
NUM_FAILS	**-0.0553****	**-0.0601*****
	(0.028)	**(0.0209)**
Control Variables	✓	✓
Brand Fixed Effects	✓	-
Constant	-8.088***	-7.155***
	(0.434)	(0.29)
Observations	460	1,037
R^2	0.398	0.247

Note: Robust standard errors are in parentheses. *p < 0.1; ** p < 0.05; *** p < 0.01.

We conducted a stand linear regression with LN_SALES_RANK as dependent variable controlling the variables shown in Table 1. We computed the variable NUM_FAILS as the sum of failure reviews for each digital camera. We also enriched our data set with information on the camera brand (from synccentric.com) to leverage brand-level fixed effects that control for unobservable time-constant heterogeneity between camera manufacturers (e.g., Fuji, Sony, etc). Because we could not obtain brand information for all cameras, we present also results from regression models without brand-level fixed-effects. The results displayed in Table 3 suggest that there is a significant negative relationship between the number of failure reviews a product has and its sales rank. Based on the coefficient of NUM_FAILS, each failure review is associated with approximately a 5.5% lower (model (1)), respectively 6% lower (model (2)), sales rank.

4 Conclusion

While the positive economic effects of several metrics of online ratings, such as the average rating or the number of ratings, are well-studied, much less attention has been paid to the economic impact of online review texts. This study tries to narrow this gap by proposing and validating a machine learning approach to identify online reviews mentioning product failure and by demonstrating, in turn, that these reviews are negatively associated with the sales of the respective product. Our results show that automated machine learning algorithms based on the LDA approach are capable of reliable identifying failure reviews. Moreover, we can characterize the nature of failure reviews in more detail: (i) they exhibit an inverted J-shape and (ii) they are negatively associated with product sales, after controlling for different metrics of online ratings and digital camera brands. Our results come with implications for practitioners and for future research. Review system designers can use our approach to identify failure reviews and mark them in online review systems, so customers can more easily identify these reviews to make better purchasing decisions. Product designers can filter out failure reviews to learn from the customer feedback and improve their product. Second, researchers can use our identification strategy in order to investigate different consequences of product failures. Additionally, our approach is neither confined to a certain set of products and could also be applied to digital goods such as apps, nor is it limited to identifying failure topics, as it could also be used to identify other topics. Researchers for instance could also investigate failure reviews of apps as antecedents of updates as well as the economic consequences of app updates.

5 Acknowledgements

This work was partially supported by the German Research Foundation (DFG) within the Collaborative Research Centre “On-The-Fly Computing” (SFB 901). I thank Robin Wulfes for excellent student assistance.

References

1. Anderson, M., Magruder, J.: Learning from the Crowd. Regression Discontinuity Estimates of the Effects of an Online Review Database. The Economic Journal 122, 957–989 (2012)
2. Chevalier, J.A., Mayzlin, D.: The Effect of Word of Mouth on Sales. Online Book Reviews. Journal of Marketing Research 43, 345–354 (2006)
3. Duan, W., Gu, B., Whinston, A.B.: Do online reviews matter? — An empirical investigation of panel data. Decision Support Systems 45, 1007–1016 (2008)
4. Herrmann, P., Kundisch, D., Zimmermann, S., Nault, B.: How do Different Sources of the Variance of Consumer Ratings Matter? Proceedings of the International Conference on Information Systems (ICIS) (2015)
5. Dellarocas, C.: The Digitization of Word of Mouth. Promise and Challenges of Online Feedback Mechanisms. Management Science 49, 1407–1424 (2003)
6. Chen, Y., Xie, J.: Online consumer review. Word-of-mouth as a new element of marketing communication mix. Management Science 54, 477–491 (2008)
7. Blei, D.M.: Probabilistic Topic Models. Commun. ACM 55, 77–84 (2012)
8. Luca, M.: Reviews, Reputation, and Revenue. The Case of Yelp.Com, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1928601
9. Chintagunta, P.K., Gopinath, S., Venkataraman, S.: The Effects of Online User Reviews on Movie Box Office Performance. Accounting for Sequential Rollout and Aggregation Across Local Markets. Marketing Science 29, 944–957 (2010)
10. Archak, N., Ghose, A., Ipeirotis, P.G.: Deriving the Pricing Power of Product Features by Mining Consumer Reviews. Management Science 57, 1485–1509 (2011)
11. Netzer, O., Feldman, R., Goldenberg, J., Fresko, M.: Mine Your Own Business. Market-Structure Surveillance Through Text Mining. Marketing Science 31, 521–543 (2012)
12. Abrahams, A.S., Fan, W., Wang, G.A., Zhang, Z.J., Jiao, J.: An Integrated Text Analytic Framework for Product Defect Discovery. Prod Oper Manag 24, 975–990 (2015)
13. Winkler, M., Abrahams, A.S., Gruss, R., Ehsani, J.P.: Toy Safety Surveillance From Online Reviews. Decision Support Systems 90, 23–32 (2016)
14. McAuley, J., Targett, C., Shi, Q., van den Hengel, A.: Image-Based Recommendations on Styles and Substitutes. In: Proceedings of the 38th ACM SIGIR Conference on Research and Development in Information Retrieval, 43–52 (2015)
15. Debortoli, S., Junglas, I., Müller, O., Vom Brocke, J.: Text Mining For Information Systems Researchers. An Annotated Topic Modeling Tutorial. Communications of the Association for Information Systems Paper 7 (2016)
16. Sridhar, S., Srinivasan, R.: Social Influence Effects in Online Product Ratings. Journal of Marketing 76, 70–88 (2012)
17. Hu, N., Pavlou, P.A., Zhang, J.: On Self-Selection in Online Product Reviews. MIS Quarterly 41, 449–471 (2017)
18. Lombard, M., Snyder-Duch, J., Campanella Bracken, C.: Content Analysis in Mass Communication: Assessment and Reporting of Intercoder Reliability. Human Communication Research 28, 587–604 (2002)

Exploring Sense-Making Activities in Crisis Situations

Milad Mirbabaie[1], Sina Youn[1]

[1] University of Duisburg-Essen, Department of Computer Science and Applied Cognitive Science, Duisburg, Germany
{milad.mirbabaie,sina.youn}@uni-due.de

Abstract. This article seeks to explore public crisis response behaviour under the premise of sense-making and assesses what enables officials to drive sense-making on Twitter. As little is known about how sense-making takes place and influences communication behaviour, we focus on sense-making activities of the crowd and analyse the behaviour of emergency agencies. We collected the communication on Twitter concerning two human-induced crises that took place in Germany in 2016: 1) A shooting in Munich, and 2) A terrorist attack in Berlin. Qualitative and quantitative analyses of tweet types and content were conducted to determine sense-making. Our findings indicate that emergency services play a crucial role within sense-making at an early stage of the crisis and lead to suggestions of how to effectively communicate in social media. Furthermore, findings suggest that people perform different sense-making activities at different stages of the crisis, leading to a model of sense-making activities.

Keywords: Social Media Analytics, Sense-Making, Twitter, Crisis Communication, Emergency Management

1 Introduction

Examination of social media communication is exceedingly promising as the pervasiveness of social media platforms, such as Twitter, Facebook, and Instagram, enable scholars to adopt new perspectives on traditional theories and concepts of psychology [1]. They are characterised by "*a technical ease of use that facilitates production, exchange and consumption of user-generated content among social media users*" [2]. In recent years, social media use has become a crucial part not only in people's daily lives but also during crises [3]. Here, [4] revealed that users are even more active during crises in comparison to non-crisis situations, resulting in higher number of messages and higher dissemination of information.

By its definition, a crisis is a threatening, oftentimes unexpected, event that is marked by high levels of uncertainty and potential harm [5, 6]. Here, people are confronted with a sudden loss of meaning, which generates anxiety [7, 8] that, in turn, forces people to define the situation at hand [8, 9]. As a result, people perform sense-making, a process first introduced by [10] and [8], that can be defined as the process, in which people make sense of what is happening and generate their own understanding and interpretation of an ambiguous situation [11, 12].

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Sense-making can be described as an ongoing process that is initiated by a cognitive gap like an ambiguous condition, in which people selectively perceive cues that they interpret based on self-perception, past experiences and the desire to make things seem rational [8]. Moreover, sense-making is primarily a social and communicative process in which the sense-maker actively interacts with others to learn about their views to compare and adjust or rationalise one's own interpretation [8]. This results in an individual interpretation of the situation for the sense-maker and a shared meaning of all participating individuals when sense-making is performed on a collective level [13–16]. This individual and collective understanding reduces ambiguity [7] and helps the sense-maker(s) to cope with the situation [16, 17] and limit the crisis' harm [6]. As crisis situations result in a strong need for communication and information, people actively turn to others, both online and offline [18, 19]. As a result, social media have emerged as a key tool for crisis communication used by all types of social units throughout different kinds of crises [3]. Here, especially Twitter proved to be highly responsive to all types of crises [20, 21].

However, recent studies do not provide a holistic picture of sense-making because little is known about when and how it takes place. Scholars revealed that social media crisis communication is predominantly characterised by collaborative information seeking, sourcing and sharing during crisis situations [22, 23]. Here, researchers identified that a key mechanism for information distribution on Twitter [15] is the retweet function, which lets people share original or commented messages of others within a user's follower network [24]. In crisis communication, shared content usually addresses the general implications of a crisis [25] and information related to evacuations and closures, whereabouts of others as well as help, health care and recover efforts [3]. These pieces of information heighten situational awareness [25], a cognitive state of understanding what is happening and comprehending the big picture during crisis situations [26]. In line with [8], who states that people must notice things first in order to make sense of them, and [11] who introduced two sequential sub-concepts of a sense-making where the first include includes actions like information seeking and sharing, dissemination of situationally relevant information that heightens situational awareness can be interpreted as the 'beginning' of sense-making in social media crisis communication [11, 15]. Moreover, "*the emergence of new lines of strong and coherent themes*" [23] marks the 'end' of sense-making and includes the adoption of cohesive symbols or unified slogans like specific hashtags [11, 23]. However, little is known about what happens in between these stages.

The remainder of this work is structured as follows: In chapter 2, the work is embedded in the context of previous research regarding sense-making. The subsequent chapter 3 specifies the research design by describing the chosen cases and giving an overview on data collection and analyses. The results are presented in chapter 4 and discussed in chapter 5. The work finishes with a conclusion and an outlook.

2 Background

In their work, [7] attempted to open the 'black box' of sense-making and introduced four major communication activities of sense-making, which offers a promising

research basis to turn the process of sense-making into an observable behaviour: The authors postulate that the sense-maker continuously singles out specific cues (noticing), puts them into a frame of reference to understand the situation at hand (interpreting), decides what to do next and act accordingly (enacting), and turns to others to take into account their reactions and interpretations (interacting). The authors derived these communication activities from retrospective interviews that addressed general sense-making situations. However, they did not test their validity reversely using data from real-life crisis communication. In order to address the current knowledge gap and gain further insight of how sense-making influences crisis communication behaviours, we derive the following research question:

RQ: *How is crisis communication on Twitter shaped (sense-making activities) by the general public and the emergency services?*

Besides private persons, who use social media for sense-making purposes, celebrities, media [15], and emergency services are especially central to crisis communication [26, 27]. Because they engage highly in crisis management efforts, including the enhancement of public's health and security as well as the prevention of a crisis' escalation, social media accounts of emergency services usually publish relevant crisis information and advice or guidance [28, 29]. Yet, even more than a decade after the introduction of Facebook and Twitter, social media still embody a difficult communication environment for formal crisis practitioners as "*a central […] may not be the scarcity of information but the glut*" [3] since various publishers contend for people's attention. However, research revealed opportunities for them to cut through and overcome information overload effectively. Here, the retweet mechanism seems to be key to a message's visibility and reach: Findings revealed a tweet within a higher retweet count has an increased potential audience [27, 30]. Emerging research suggests that not only the content itself, but the way it is presented wields a certain influence on its recipient [31, 32]. Following these arguments, it seems plausible that accounts presenting emergency services should publish content in a way that maximises its likelihood to be retweeted. Here, [29] revealed that style factor and sentence function affect retweetability as a clear and specific sentence style is a predictor of retweet count. Even though the crucial role of retweetability is apparent und emphasised by literature within the field of crisis communication and management, research on how emergency services can increase their reach and support public sense-making is still in its infancy. Given the significance of emergency services for crisis management and the sense-making process, this is a knowledge gap which directly affects their efficiency and lead to the risk of making crisis communication decisions based on intuition or inaccurate information [4]. In 2016, [31] proposed the interactive crisis communication (ICC) model, which incorporates 'response form', meaning the attributes dialogic, consistent, precise and timely as well as the emotional valence it discloses. The author based the theoretical model on a literature review including frameworks of traditional crisis communication strategies and social media crisis management, yet did neither specify the influence these variables wield nor reversely validated the assumption with a sample of concrete crisis communication. Following the argument of [29, 32], however, it seems plausible that they might influence a message's retweetability. As such, to contribute to the current body of knowledge, it appears promising to test the

relationships posited in the ICC in the context of retweet count and further include the variables of [29].

3 Research Design

3.1 Case Description

Shooting in Munich: On 22 July 2016 at 5:52pm CET, a man opened gunfire at a restaurant close to the Olympia shopping mall (OEZ) in Munich, Germany. About 40 minutes later, the official account of Munich's police department (@polizeimuenchen) published a Tweet about a "major police operation at the mall". The hours following the shooting were characterised by high levels of uncertainty and anxiety: The police repeatedly called the situation 'ambiguous', publishing statements of uncertainty about the number of and whereabouts of the perpetrator. Additionally, several resistant rumours spread quickly, including another gunfire at Karlsplatz/Stachus in the city centre and that there were at least three perpetrators and the use of long guns, which all turned out to be false. Investigations revealed that the gunman was an 18-year-old man.

Terrorist attack in Berlin: On Monday, 19 December 2016, 12 people were killed and more than 50 others injured when a 40 tonnes truck was deliberately driven into a Christmas market at Breitscheidplatz in Berlin, Germany at 8:02pm CET [33]. At 8.41pm the official account of Berlin's police department (@polizeiberlin) published a 'breaking' tweet about the incident. In the hours following the incident, it was ambiguous whether the incident was an accident or a terrorist attack and many speculations circulated. Around 10pm CET, the message of a suspect's arrest hit Twitter and the police subsequently sent an all-clear signal for the crisis location. On 21 December, it was announced that investigators suspect a man, a failed asylum seeker [34], which resulted in the launch of an official Europe-wide manhunt. On 23 December, four days after the attack, he was killed in a shootout with the police near Milan, Italy. The terrorist group of Daesh claimed responsibility for the attack [34].

3.2 Data Collection

To evaluate sense-making activities by the public and crisis management by officials, we investigate the communication about the two cases on Twitter, since it is the platform of major research interest in the field of crisis communication based on the following arguments: 1) It has emerged as an important communication and management platform in all crisis categories and for all types of social units, especially by emergency services, as it facilitates quick information dissemination [4, 27]. 2) Twitter response to emerging issues is fast and offers the monitoring of an independent public conversation [28]. 3) Here, the number of participating users and tweets is usually high, leading to a big data sample [35]. 4) Data acquisition is easy as the platform provides an API which enables data gathering at scale on specific issues [35].

After the crises occurred, we started the data tracking within a few hours later. As the 'search API' offers the opportunity to track data up to 1 week in the past, we could ensure to collect the data in time. For the tracking, we used a self-developed Java tool, which makes use of the library Twitter4J and connects to the Twitter API. We identified

in each case the most often used keywords related to the extreme events and the accounts from local law enforcement**. Munich** (Time period: 22-07-16, 5:00:00pm to until 23-07-2016, 11:59:59pm CET) **Keywords:** München (Munich), Prayformunich, Oez (abbreviation crisis location), Prayforgermany, Polizeimünchen (local police account). **Berlin** (Time period: 19-12-2016 at 7:00:00pm CET until 23-12-2016 at 12.59:59pm CET) **Keywords:** Terrorist attack in Berlin, Berlin, Breitscheidplatz (public open space), Gedächtniskirche (Memorial church), Anschlag (attack), Polizeiberlin (local police account), Polizeiberlin_E (local police account). We collected the communication and saved it into a My-SQL-Database. We considered in both cases German tweets, as the incidents occurred both in Germany

3.3 Data Analysis

The dataset was segmented in intervals and subsequently, variables related to sense-making activities, namely tweet types and published content, were examined within each interval. In order to analyse Twitter crisis communication behaviour by the public over time, a complex time-series analysis was conducted. The data for each case was divided into 76 (Munich), respectively 360 (Berlin), 15-min intervals, in each of specific the communication behaviour was examined. This allowed us to have a dynamic perspective on the communication [24, 36]. Following the argument of [22, 37], that tweets types suggest communication behaviour, they serve as a first indicator, of how sense-making influences actual communication behaviour. Based on [24], who state that sense-making involves both one-to-one- as well as one-to-many-communication, all tweet types are included within the given study. Here, [7] sense-making communication activities are linked to Twitter's tweet types: Noticing is an internal, attentional process which includes perceptual actions based on cue extraction [7]. There is strong evidence that retweeting influences the noticing process of others as stimuli are noticed through an individual's own efforts as well as through the individual's observation of other people's communication [8] and retweeted messages are considerably more visible [27, 30]. Moreover, following the arguments of [7, 8, 38] that sense-making is an ongoing process, it is anticipated that noticing is performed continuously. As people are constantly noticing and selected cues are inevitably interpreted [8], the same is true for the sense-making activity of interpreting, which is also an internal process. In addition to that, it seems plausible to assume that the outcome of interpreting, meaning achieved sense or interpretations [11, 23], is likely be communicated through original tweets, as they contain opinions [22, 37]. This, in turn, resembles the sense-making activity of enacting, as it is performed when individuals take actions within and to influence their environment. Yet, enacting is not limited to original tweets as information sharing, the main intent behind retweets [22, 37], can also be interpreted as an enactment. As such, for this sense-making activity both retweets and original tweets are considered and further, more unambiguously indicators of communication behaviour are derived from the published content. To get insight into the published content, the ten most frequently used words within each interval were determined. All words within one tweet were extracted and converted into lower-case characters using regular expression. Furthermore, the tweets within the

datasets that included users are arranged in descending order based on their retweet count. This method is used to get additional qualitative information about the published content that gained the highest reach and thus also had a potential influence on the sense-making process by the public.

In the given study, SentiStrength was used for the sentiment analyses. The tool uses a lexical approach based on a list of sentiment-related terms and rules for negations, booster words and misspellings, as well as for ways to express sentiments like exaggerated punctuation or emoticons [39]. Sentiments are reported on a dual scale, which means that a positive sentiment score, ranging from 1 (neutral) to 5 (strongly positive), and a negative score, between -1 (neutral) to -5 (strongly negative), are reported [39]. The sentiments are then used to calculate the polarity for each tweet with the following formula: *polarity = positive sentiment strength + negative sentiment strength*. Therefore, polarity, which is also referred to as 'valence' and is set as an independent variable in the given study, has a score which is negative, positive or neutral [40]. A tweet's emotionality is calculated with the following formula: *emotionality = positive sentiment strength + |negative sentiment strength|* and used as another sentiment-related independent variable.

4 Findings

4.1 Sense-making activities by the Public

The dataset for the gunfire in Munich consists of 411,024 tweets ranging from 74 to 22,831 tweets within each interval (M = 5408.21, SD = 6720.99), out of which 324,042 (78.8%) are retweets, while 73,209 (17.8%) are original tweets and 13,773 (3.4%) are replies or comments, to which 126,467 unique users contributed.

The dataset for the terrorist attack in Berlin contains 475,430 tweets, ranging from 66 to 19,662 tweets within each interval (M = 1320.64, SD = 2293.74). Here, 140,784 unique users contributed to 334,262 (70.3%) retweets, 117,097 (24.6%) original tweets and 24,071 (5.1%) replies or comments. Here, the early hours of the crisis incorporate large amounts of tweets and engagement of a high number of users.

Analysis of the ten most frequently used words within each interval of the Munich dataset revealed that, as soon the as crisis was triggered, major unambiguously crisis-related words, such as 'schüsse' ('shots'), 'einkaufszentrum' ('mall') and 'tote' (casualties) were published on a large scale. Here, the count of 'schüsse' increased from 68 to 1,213 within 45 minutes. Up from 6:30pm until the end of the observed period, the string 'polizeimuenchen' appeared within the most frequently used words, consistently occupying a rank between 1 to 3 in all intervals. Between 8:00pm and 11:30pm, the strings 'offenetuer' and 'offenetür' (both 'open door') occurred within serial intervals. 'Entwarnung' (‚all-clear signal'), along with the words 'täter' ('perpetrator) and 'gefunden' ('found'), ranked high between 1:15am and 1:30am and, 1:30am und 1:45am respectively. Between 2:15am and 3:45am, first details about the perpetrator, namely his nationality and age were used extensively. The words 'dank' ('thanks'), 'hilfsbereitschaft' ('helpfulness') were predominantly published between 3:45am and 4:15am, while 'trauern' ('mourn') was frequently published between

5:15am and 8:00am. Within the last hours of the observed period, in particular between 9:00am and 11:15am, the word 'terror' entered list of the ten most frequently used words and in the very last interval, the words 'amok' and 'is' were used extensively.

The examination of the most frequently used words revealed that, in both cases, words related to the crisis event hit Twitter on a large scale immediately after it was triggered. Here, early contributions were related to the crisis' location and trigger while later, words referring to the crisis' scope and aftermath are published extensively in both crises. Both datasets were characterised by the occurrences of strings that do not refer to factual information or personal names. Within the public communication about the crisis in Munich, the string 'offenetür' ('open door') constantly appeared on high ranks in serial intervals between 8:00pm and 11:30pm on July 22. Moreover, two strings that started in the evening on December 20 and remained on high ranks for several hours were 'muslimegegenterror' ('Muslims against terror') and 'ichbinberlin' ('I am Berlin'). A major difference between the public crisis communication is that, even though both were human-induced, strings referring to the name of the perpetrator were absent within the Munich dataset, even though his nationality and age were published, while the word 'anis' and 'amri' were constantly used within the Berlin dataset up from 10:45am on December 21.

4.2 Sense-making activities by the Emergency Service

In the dataset of the gunfire in Munich, the account '@PolizeiMuenchen' published 36 tweets related to the crisis, which were, in total, retweeted 101,681 times (M = 2,824.47; SD = 3,490.11). The sentiment polarity ranges from -4 to 2 (M = 0.167; SD = 1.344), while the sentiment emotionality ranges from 2 to 6 (M = 3.056; SD = 1.079). Figure 1 gives an overview, showing that the retweet count varied significantly but was considerably higher early in the crisis.

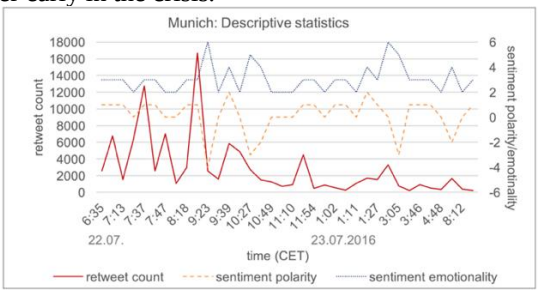


Figure 1. Retweet count, sentiment polarity and emotionality for police tweets (Munich).

In the dataset from the terrorist attack in Berlin, it is noteworthy that the account '@polizeiberlin' published 7 tweets related to the crisis, which were, in sum, retweeted 65,011 times (M = 866.81; SD = 1,684.47), while the account '@PolizeiBerlin_E' published 68 tweets with a consolidated retweet count of 51,984 (M = 741.79; SD = 1,450.59). On a collective level, the sentiment polarity ranges from -3 to 3 (M = -0.134; SD = 1.147), while the sentiment emotionality ranges from 2 to 7 (M = 3.093; SD = 1.073). Also for the police accounts in Berlin were retweeted on a large scale within the early hours (Figure 2).

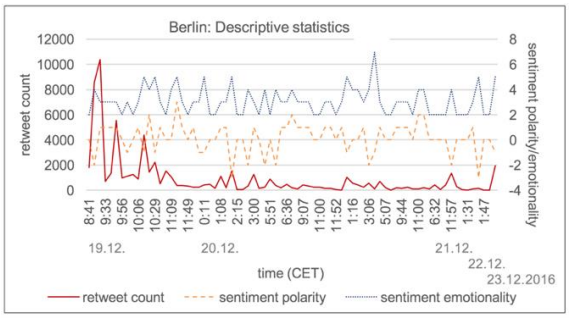


Figure 2. Retweet count, sentiment polarity and emotionality for police tweets (Berlin).

5 Discussion

Once sense-making is initiated by a sudden loss of meaning, people continuously perform the sense-making activity of noticing. Furthermore, as soon as they perceive cues, people start interpreting them and try to make sense of the ambiguous situation at hand. As noticing is an ongoing process, it affects interpreting, which becomes also on ongoing process. Our results indicate that enacting and interacting take place on a temporal level. Subsequently, informed users did not want to passively wait for things to happen but take actions within their environment in the form of retweeting selected tweets. As noticing and interpreting are internal processes, it was not possible to determine a specific communication behaviour performed by the sense-maker during these activities. Yet, as it is anticipated that these communication actions further influence other's noticing and interpreting processes, their impacts are outlined. According to [7, 8], individuals take actions to influence their environment within the sense-making activity of enacting to generate new information, better understand their cognitive processes and update perceptions. Our Analysis revealed that people did so by publishing original tweets and sharing retweets related to specific topics at particular periods of time. Within the Munich dataset, early intervals of heightened retweet use further contained the string 'offenetür', which refers to offer shelter for people seeking safety. This practice was used extensively in social media communication during the attacks in Paris in November 2015. Our examination revealed that the same mechanism was used between two and six hours following the crisis' trigger in Munich. A look into the top retweets revealed that in particular verified users who did not offer refuge themselves, drew the attention towards this mechanism, got high retweet counts. Following the argument of [7, 8], it seems plausible that, after people perceived cues and stimuli through various channels and interactions, they asked themselves what to do next. Results indicate that people then performed actions in the form of retweets as they feel others should know about the information they shared as they might find it useful. Thus, people enacted within their environment as information amplifiers and thereby increased the visibility of specific tweets because they shared them with their own network. It stands to reason that people enacted overwhelmingly on situationally relevant information at the very beginning of a crisis, as it contributes to situational awareness, which in turn, supports people to make sense of a situation and to reduce

uncertainty [3, 25]. Building upon [9], the expression of sympathy (and solidarity) can the interpreted as people's tendency to verbalise their thoughts and emotions to reduce anxiety and establish a sense of connection. This leads to the assumption that people enacted within their environment not only by sharing situationally relevant information but by actively spreading messages that express sympathy and builds a community spirit between remotely connected individuals in order to cope with the situation at hand [3, 24]. Even though neither [7] nor [8] specified actions linked to enactment but broadly defined that they "*bring events and structures into existence and set them into motion*" [12], latest literature suggests that only sharing situationally relevant information and achieved sense are crucial to the sense-making process [15]. As people deliberately decide to retweet messages expressing sympathy, however, we suggest that the sense-making activity of enacting is not only limited to information seeking and sharing, but serves to fulfil socio-psychological needs by publishing emotional content.

Our findings from both cases indicate that observed police accounts played a crucial role within social media crisis communication. Particularly in the Munich dataset, in which the local police account occupied the first ten ranks within the list of top retweets, yet also Berlin's police accounts dominated that list even though not taking up all ten ranks. In both cases, the tweets with the highest retweet count were published during the first hours following the crisis' trigger. Our analyses revealed that published tweets predominantly contained, partially actionable, key emergency information (e.g. advice to keep away from the crisis location) as well as requests for cooperation (e.g. that people should not publish photos). Following the argument of [8, 15] the local police account further played a crucial role within the process of sense-making and had the power to initiate it by the perception of information. The fact that the local police accounts published most of their tweets (60% in Munich and 80% in Berlin), in the early hours of the crisis, which were retweeted very often, leads to the assumption that the local police strongly engaged in crisis management efforts to limit a crisis' harm.

Our content analysis revealed that messages characterised by guidance and/or requests were predominantly stated imperatively. The police told exactly what to do, in order to maximise people's health and safety, while simultaneously supporting 'offline actions' of various related emergency service, e.g. rescue efforts by the fire brigade as well as investigations by the police, with imperative sentences, such as commands, requests or instructions. Update information and expressions of emotion, were written in declarative or exclamatory sentences. Thus, it can be assumed that imperative tweets most likely gain high retweet counts as they contain unambiguous information about what people should (not) do, in order to stay safe and support emergency services' crisis management efforts/work.

6 Conclusion and Further Research

Even though both [8] and [7] state that sense-making is an ongoing and interrelated process, results strongly suggest that collective crisis communication is shaped by specific and temporary communication activities (see Figure 3), thus supporting a sequential assumption also postulated by [11]. In line with [7, 8], however, it can be assumed that people are constantly noticing and interpreting. But, in line with [11], our

findings lead to the conclusion that people perform communication activities in a sequential order: First they enact and subsequently they interact. In this context, it is noteworthy that [7], defined five sub-concepts of interacting, although neither their work nor the one of [8] specified actions related to the sense-making activity of enacting, respectively the sense-making property of enactment. We therefore propose, based on our findings, three sub-concepts of enacting of the public, in particular 'informing', 'sympathising' and 'sense-giving', which take place consecutively: Within the crisis stage, in particular the critical period of the crisis, people enact within their social environment by, first, sharing situationally relevant and key emergency information, while subsequently taking actions within their network by actively sharing expressions of sympathy. By doing so, people influence the noticing process of their social environment, especially their direct followers on Twitter through enactment. As such, enacting and noticing can be interpreted as a reciprocal process within sense-making in social media. At a later stage of the crisis/critical period, as well as during the early post-crisis stage, people enact through the disclosure of personal interpretations of the situation or by forwarding other's that reflect their own opinion, possibly to influence others' sense-making process. This suggests that sense-making and sense-giving are inevitably connected. Moreover, simultaneously with this act of sense-giving, people interact on a more personal level and use mechanics of two-way communication to update, inquire, triangulate, verify, and reflect synchronously.

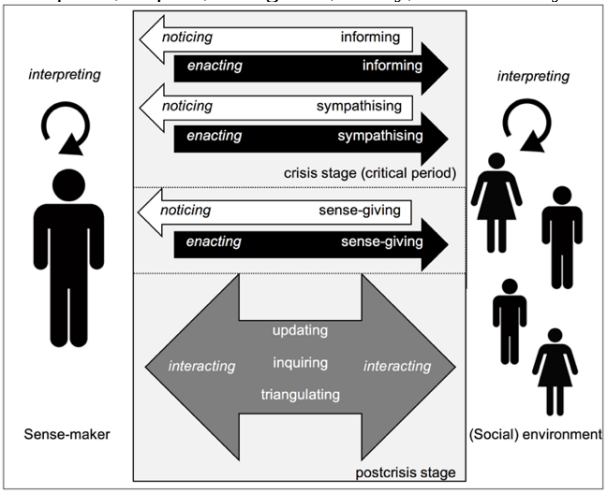


Figure 3. Sense-making activities (adapted and extended from [7]).

Our findings suggest that emergency/rescue services, such as public health and national security agencies on federal, state, and local levels have a 'louder voice' than media outlets or even celebrities, and thus are able to effectively cut through chaotic Twitter communication and distribute situationally relevant information. This underlines the importance for practitioners to actively take part in social media crisis communication. Furthermore, findings lead to clear suggestions of how to effectively incorporate new technologies into crisis management to execute life safety services and support the public in sense-making activities: Emergency services should a) diffuse situationally relevant information within the first hours of the crisis and b) provide an

authoritative source of information to effectively cut through, reach target audience and support people in understanding the situation at hand.
In further research, one could examine other crises and different senders, e.g. natural crises and messages sent from the fire brigade or organisational crises and the involved organisation. Additionally, in order to further contribute to the sense-making research, future studies could differentiate sense-making activities and related communication behaviour and/or published content between the affected and unaffected public. Distinction between these actors could be based on coordinates.

References

1. Kleinberg, J.: The convergence of social and technological networks. Commun. ACM. 51, 66 (2008).
2. Neubaum, G., Rösner, L., Rosenthal-Von Der Pütten, A.M., Krämer, N.C.: Psychosocial functions of social media usage in a disaster situation. Comput. Human Behav. 34, 28–38 (2014).
3. Lachlan, K.A., Spence, P.R., Edwards, A., Reno, K.M., Edwards, C.: If you are quick enough, i will think about it. Comput. Human Behav. 33, 377–380 (2014).
4. Fraustino, J.D., Liu, B., Yan, J.: Social Media Use during Disasters: A Review of the Knowledge Base and Gaps. (2012).
5. Hermann, C.F.: Some Consequences of Crisis Which Limit the Viability of Organizations. Adm. Sci. Q. 8, 61 (1963).
6. Reynolds, B., Seeger, M.W.: Crisis and Emergency Risk Communication as an Integrative Model. J. Health Commun. 10, 43–55 (2005).
7. Muhren, W.J., Van Den Eede, G., Van De Walle, B.: Making sense of media synchronicity in humanitarian crises. IEEE Trans. Prof. Commun. 52, 377–397 (2009).
8. Weick, K.E.: The Nature of Sensemaking. Sensemaking Organ. 1–62 (1995).
9. Dervin, B.: On studying information seeking methodologically: The implications of connecting metatheory to method. Inf. Process. {&} Manag. 35, 727–750 (1999).
10. Dervin, B.: An overview of sense-making research: Concepts, methods, and results to date. In: International Communication Association Annual Meeting. pp. 1–14 (1983).
11. Turner, R.H., Killian, L.M.: Collective Behavior. Prentice Hall College Div; 3 Sub edition (1987).
12. Weick, K.E.: Enacted Sensemaking in Crisis Situations. J. Manag. Stud. 25, 305–317 (1988).
13. Oh, O., Eom, C., Rao, H.R.: Collective sense-making through the twitter service during the 2011 egypt revolution. Thirty Third International Conference on Information Systems, Orlando (2012).
14. Stieglitz, S., Bunker, D., Mirbabaie, M., Ehnis, C.: Sense-Making in Social Media During Extreme Events. J. Contingencies Cris. Manag. 1–17 (2017).
15. Stieglitz, S., Mirbabaie, M., Schwenner, L., Marx, J., Lehr, J., Brünker, F.: Sensemaking and Communication Roles in Social Media Crisis Communication. In: Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen. pp. 1333–1347 (2017).
16. Mirbabaie, M., Zapatka, E.: Sensemaking in Social Media Crisis Communication - A Case Study on the Brussels Bombings in 2016. In: Proceedings of the 25th ECIS. pp. 2169–2186 (2017).
17. Shklovski, I., Palen, L., Sutton, J.: Finding community through information and communication technology in disaster response. Proc. 2008 ACM Conf. CSCW. ACM. 127–136 (2008).
18. Lin, X., Lachlan, K.A., Spence, P.R.: Exploring extreme events on social media: A comparison of user reposting/retweeting behaviors on Twitter and Weibo. Comput. Human Behav. 1–6 (2016).
19. Perez-Lugo, M.: Media Uses in Disaster Situations: A New Focus on the Impact Phase. Sociol. Inq. 74,

210–225 (2004).
20. Mirbabaie, M., Ehnis, C., Stieglitz, S., Bunker, D.: Communication roles in public events – A case study on Twitter communication. In: Information Systems and Global Assemblages. (Re)Configuring Actors, Artefacts, Organizations. pp. 207–218 (2014).
21. Ehnis, C., Mirbabaie, M., Bunker, D., Stieglitz, S.: The role of social media network participants in extreme events. 25th Aust. Conf. Inf. Syst. (2014).
22. Bruns, A., Stieglitz, S.: Quantitative Approaches to Comparing Communication Patterns on Twitter. J. Technol. Hum. Serv. 30, 160–185 (2012).
23. Oh, O., Eom, C., Rao, H.R.: Research Note—Role of Social Media in Social Change: An Analysis of Collective Sense Making During the 2011 Egypt Revolution. Inf. Syst. Res. 26, 210–223 (2015).
24. Heverin, T., Zach, L.: Use of microblogging for collective sense-making during violent crises: A study of three campus shootings. J. Am. Soc. Inf. Sci. Technol. 63, 34–47 (2012).
25. Toriumi, F., Sakaki, T., Shinoda, K., Kazama, K., Kurihara, S., Noda, I.: Information sharing on Twitter during the 2011 catastrophic earthquake. Proceedings of the 22nd international conference on World Wide Web companion. pp. 1025–1028. Geneva (2013).
26. Vieweg, S., Hughes, A.L., Starbird, K., Palen, L.: Microblogging during two natural hazards events: what twitter may contribute to situational awareness. CHI 2010 Cris. Informatics. 1079–1088 (2010).
27. Bruns, A., Burgess, J.: Crisis Communication in Natural Disasters: The Queensland Floods and Christchurch Earthquakes. Twitter and Society. pp. 373–384. Peter Lang, New York (2014).
28. Olteanu, A., Vieweg, S., Castillo, C.: What to Expect When the Unexpected Happens: Social Media Communications Across Crises. Proc. 18th ACM - CSCW '15. 994–1009 (2015).
29. Sutton, J., Spiro, E.S., Johnson, B., Fitzhugh, S., Gibson, B., Butts, C.T.: Warning tweets: serial transmission of messages during the warning phase of a disaster event. Information, Commun. Soc. 17, 765–787 (2014).
30. Bruns, A., Burgess, J.E., Crawford, K., Shaw, F.: #qldfloods and@QPSMedia: Crisis Communication on Twitter in the 2011 South East Queensland Floods. (2012).
31. Cheng, Y.: How Social Media Is Changing Crisis Communication Strategies: Evidence from the Updated Literature. J. Contingencies Cris. Manag. (2016).
32. Stieglitz, S., Dang-Xuan, L.: Emotions and Information Diffusion in Social Media—Sentiment of Microblogs and Sharing Behavior. J. Manag. Inf. Syst. 29, 217–248 (2013).
33. Morgenpost, B.: Protokoll des Lastwagen-Anschlags in Berlin, https://interaktiv.morgenpost.de/breitscheidplatz, last access: 2017-06-01
34. Zeit: Der Anschlag auf den Weihnachtsmarkt, http://www.zeit.de/gesellschaft/zeitgeschehen/2016-12/berlin-weihnachtsmarkt-kurfuerstendamm-gedaechtniskirche-attentat, last access: 2017-06-01
35. Stieglitz, S., Bruns, A., Krüger, N.: Enterprise-Related Crisis Communication on Twitter. Proc. der 12. Int. Tagung Wirtschaftsinformatik (WI 2015). 917–932 (2015).
36. Yin, R.K.: Case Study Research: Design and Methods. SAGE Publications, Beverly Hills, CA (2009).
37. Bruns, A., Stieglitz, S.: Towards more systematic Twitter analysis : metrics for tweeting activities. Int. J. Soc. Res. Methodol. 16, 91–108 (2013).
38. Muhren, W., Van Den Eede, G., Van de Walle, B.: Sensemaking as a Methodology for ISCRAM Research: Information Processing in an Ongoing Crisis. Proc. 5th Int. ISCRAM Conf. 315–323 (2008).
39. Thelwall, M.: The Heart and Soul of the Web? Sentiment Strength Detection in the Social Web with SentiStrength. In: Holyst, J.A. (ed.) Cyberemotions. pp. 119–134. Springer, Switzerland (2013).
40. Thelwall, M., Buckley, K.: Topic-based sentiment analysis for the social web: The role of mood and issue-related words. J. Am. Soc. Inf. Sci. Technol. 64, 1608–1617 (2013).

Strategien und Technologien der Digitalisierung in kleinen und mittleren Unternehmen

Teilkonferenzleitung

Axel Hahn
Egon Müller
Christoph Wunck

In-store Technologies in the Retail Servicescape

Jan H. Betzing[1], Anh-Quoc Martin Hoang[1], and Jörg Becker[1]

[1] University of Muenster, ERCIS, Münster, Germany
{jan.betzing,martin.hoang,jorg.becker}@ercis.uni-muenster.de

Abstract. Brick-and-mortar retailers start to integrate digital in-store technologies into the physical servicescape to leverage individual shopping experiences for their customers and competitive advantage for them. This research provides a starting point for brick-and-mortar retailers, who lack guidance on how these technologies support their business strategies. We review the literature regarding the digital capabilities provided by customer-facing in-store technologies and identify their relations and contributions to the archetypal business strategies individualization and cost-optimization. We thereby extend the shopper-focused decision calculus by a technological view that relates the capabilities of in-store technologies, impacts on customers, and impacts on the retailers' business strategies.
Keywords: In-store Technology, Retailer-Consumer Interface, Brick-and-Mortar Retail, Business Strategy

1 Introduction

The digital era and the advent of omnichannel retailing transform consumers' shopping behavior in favor of digital channels and raise their expectations towards the digital profile of brick-and-mortar retailers [1–5]. Retailers react by integrating digital in-store technologies into the physical servicescape to leverage both the benefits of e-commerce such as multimedia product presentations, recommendations, and reviews and the benefits of the physical store such as personal service, touch and feel of the merchandise, and instant availability [5]. However, especially small and medium-sized retailers—without a large IT organization—that want to integrate these technologies into their business model can easily get lost by the variety of technologies to choose from and may lack a starting point for their assessments [2]. In consequence, they often select technologies without examining the potential contributions to their strategies [6].

Much research exists on the digitization of retail [e.g., 1, 5], the creation of digital shopping experiences [e.g., 3, 7], organizational changes related to in-store technology [e.g., 8], their acceptance by customers [e.g., 9], and the technologies itself [e.g., 2]. To date, there is—to the best of our knowledge—no attempt to provide retailers with a structured overview of the digital capabilities provided by contemporary customer-facing in-store technologies from a strategical point of view [6].

Consequently, our research goals are (1) to identify the digital capabilities that contemporary customer-facing in-store technologies provide to the retailer and (2) to identify their relations and contributions to the archetypal business strategies

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

individualization and *cost-optimization*. These strategies build upon the theoretical lens of the shopper-focused decision calculus [6].

The remainder of this paper unfolds as follows: Section 2 gives the research background and strategic key concepts our analysis builds upon. Section 3 provides the applied research method. Section 4 presents the identified capabilities and shows their association to the key concepts. Section 5 links our findings to the shopper-focused decision calculus theory. Section 6 discusses our results and concludes this paper.

2 Research Background

The introduction of digital technologies in retailing is not a new phenomenon, dating back to the 1960s [1]. While previous advances such as Enterprise Resource Planning (ERP) mainly improved operational processes invisible to the customer, the nature of current developments is different. Self-service terminals, in-store assistants, and mobile payment are just a few examples that are directly visible to the customers. We define in-store technologies in retail as bundles of hard- and software that change or enhance the interface between retailers and customers within the physical retail setting. These technologies augment the servicescape by new customer touchpoints that facilitate technology-enhanced person-to-person, person-to-machine, and even machine-to-machine encounters [10]. Willems et al. remind us that "technology in retailing is and should remain a means to an end rather than an end in se" [2, p. 2]. Consequently, we take a retailer's perspective on the technologies' influence on his or her profit equitation. Primarily, the expected total benefits of ownership (TBO) must outweigh the total cost of ownership (TCO). The TBO depends on manifold internal (e.g., integration in the servicescape, organizational change) and external factors (e.g., customer acceptance, competition, obsolesce) and cannot be quantified in full. From a strategical point of view, benefits manifest in competitive advantage resulting from cost-optimization or differentiation through individualization [11]. The former aims at efficient operations whereas the latter aims at effective operations, which can be achieved by meeting customers' individual needs better than the competition, which in turn, positively affects revenue. The shopper-focused decision calculus theory argues in a similar vein [6]. Retail technology has the potential to decrease the retailers' costs and/or increase their revenue by extracting a consumer surplus, increasing the sales volume, attracting new customers or strengthening the retailer's bargaining power to suppliers [6]. The authors primarily focus on the customers' reactions to selected in-store technologies and treat the influences of retail technology to business strategy as a black box. This work contributes to the shopper-focused decision calculus by shedding light on this black box.

Since innovation cycles in customer-facing technology are fast, reviewing contemporary in-store technologies only reflects a snapshot in time. Therefore, we use generalized digital capabilities as abstract proxies for these technologies and show instances for clarity. In the context of our work, digital capabilities denote sets of features or services provided by an in-store technology and should not be confused with organizational capabilities in the sense of intangible assets known from the resource-

based view. Digital capabilities can be used to classify future technologies and help to identify their merits. Against this background, our analysis of the capabilities and their relations focuses on the following two archetypal strategies:

1. *individualization* subsumes all contributions of in-store technologies to fulfilling the individual customer's needs effectively. Individualization revolves around establishing and maintaining a relation to the customer with the aim of increasing both the individual customer's basket size, and the overall number of customers. Further, differentiation through individualization aims at lowering the customer's opportunity cost, which manifests by either lowering the shopping effort or raising the shopping convenience.
2. *cost-optimization* subsumes all contributions of in-store technologies to fulfilling the retail operations efficiently. The primary goal of cost-optimization is to keep a certain service quality but decrease the retailer's cost through automation or offloading tasks to customers.

3 Research Method

The analysis performed in this work is based on the approaches for systematic literature reviews proposed by vom Brocke et al. [12] and Webster and Watson [13]. Following Cooper [14], we define the scope and goal of the review in identifying the digital capabilities that contemporary in-store technologies provide, and outlining their relations and contributions to the presented strategies. We focus on theoretical designs and practical applications of in-store technology w.r.t. the retailer-consumer interface. A search [13] across relevant journals and conference papers in information systems, computer science, marketing, and business administration was conducted on Scopus on 2017-06-18. Using Willems et al.'s inventory of customer-oriented retail technologies [2], we exploratively derived and refined our search query for various technologies and research streams related to in-store technology (cf. Figure 1).

```
TITLE-ABS-KEY ( ( "retail*" OR "sale*" ) AND ( "technolog*" ) AND ( "digital sign*" OR "assisted
selling" OR "biometric*" OR "convenience" OR "interactive" OR "personal" OR "shelf allocation" OR
"shelf manag*" OR "customer behavior*" OR "consumer behavior*" OR "recommend*" OR "pervasive" OR
"customer preference*" OR "consumer preference*" OR "advert*" OR "customer loyal*" OR "consumer
loyal*" OR "customer retention" OR "consumer retention" OR "automati*" OR "self-service" OR "co-
creation" OR "prosumption" OR "value co-creation" OR "purchase behavior*" ) ) AND DOCTYPE ( ar OR
cp ) AND PUBYEAR > 2008 AND ( LIMIT-TO ( SUBJAREA , "COMP " ) OR LIMIT-TO ( SUBJAREA , "ENGI " )
OR LIMIT-TO ( SUBJAREA , "BUSI " ) OR LIMIT-TO ( SUBJAREA , "SOCI " ) OR LIMIT-TO ( SUBJAREA ,
"DECI " ) OR LIMIT-TO ( SUBJAREA , "MULT " ) )
```

Figure 1. Literature search query

Due to the speed of technological innovation, we limit the literature search to the last eight years. The initial search yielded 2,147 results, whose relevance was evaluated analyzing their titles and abstracts [12]. Based on the initial screening, 81 relevant publications were analyzed in detail. A one-level backward and forward search lead to 14 additional publications. The final literature sample consists of 95 publications.

Although this selection must be seen as representative excerpt, the abstract nature of the digital capabilities allows for a comprehensive view.

4 Digital Capabilities of In-store Technology

We conducted an exploratory analysis of the 95 identified documents[1]. Figure 2 provides an overview of the derived digital capabilities, grouped by their main strategic impact. Five capabilities each primarily account for individualization and cost optimization strategies. We additionally identified three capabilities related to the elicitation of the customer's context. The capabilities are not mutually exclusive, i.e., one technology can support multiple capabilities, and one capability can both support the individualization and cost optimization strategies. In the same way, the capabilities can be combined, with one enhancing the operations of the other. We detail out our findings in the following:

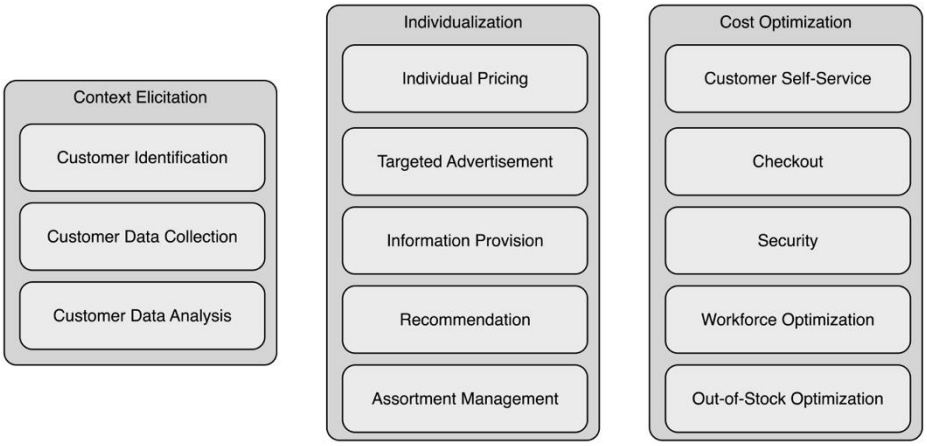


Figure 2. Digital capabilities provided by in-store technologies

Digital information on the customers and their shopping behaviors provide the foundation for most capabilities. Context elicitation, on the one hand, allows to approach the customer individually, and on the other hand to optimize overall store operations. Identification and data collection take place as soon as the customer enters the vicinity of the retailer [15]. Sensor- and vision-based technologies such as cameras, smart devices, wireless communication, and robots can be individually combined to personally identify the customer or at least individual traits, and his or her in-store shopping activities [16– 26]. Customers that already have a relation to the retailer can actively identify themselves at self-service terminals or the point of sale (PoS) using barcodes, QR-codes, loyalty cards, and NFC-equipped smart devices [20, 24].

[1] A concept matrix [13] that relates the literature to the digital capabilities presented in Figure 2 is available online at `https://goo.gl/yYufZU`.

Cameras with biometric face recognition capabilities that monitor the shop floor can identify inter alia the customer's gender, age, height, face, emotion, gestures, speech, and sentiment [21–23]. They also provide a feedback channel for digital customer touch points such as digital signage by monitoring the customer's interaction with the channel.

Sensor-equipped robots directly interact with the customers and adapt to their behavior w.r.t. the customer's reactions [17]. Interconnected robots can act cooperatively, e.g., outdoor robots interacting with pedestrians can inform in-store robots about potential customers entering the shop [18]. Manifold options exist to capture the customer's location and movement patterns using satellite navigation, Bluetooth-based beacons, WiFi, and cameras [18, 19, 25, 27]. RFID-tags (radio-frequency identification) can be attached to products [24], loyalty cards [20], and shopping carts [26], to track customers and their shopping baskets, purchases, and interaction with digital product information and the products itself [21, 28]. Vision-based systems identify, how long customers look at a product, if the product is picked up and bought or if it is placed back again [16, 29].

Customer data analysis generates insights from the collected information. Common approaches apply predictive analytics, data mining, and artificial intelligence to reason upon customer behavior [30–33]. Central insights on the individual customer level are the prediction of purchase behavior, i.e., the customer's willingness to pay and purchase probabilities for products [30, 32, 34] as well as the customer's preferences [35]. Aggregated information on movement patterns, hot spots, item popularity, interaction with digital touchpoints, and PoS data enable continuous improvement of the service delivery [36]. Both individual and aggregated insights set the foundation for the individualization and cost optimization capabilities.

Retailers having knowledge on the customer's willingness to pay and purchase probabilities can provide the customer with individual pricing, i.e., setting product prices that provide a good trade-off between maximizing the purchase probability and the extraction of customer surplus [11]. Individual prices are presented using digital signage, electronic shelf labels, self-service terminals, and mobile apps [24, 37]. Coupons, exclusive discounts, and individual product-service bundles are common means to achieve individual pricing [25]. Like how gas stations vary their prices over the day, retailers can exploit different price sensitivities over the day and automatically adjust their prices using electronic shelf labels [6].

Individual prices can be combined with targeted advertisement and product recommendations to create a tailored shopping experience [3, 7]. Digital signage, digital shopping carts, and self-service terminals that employ viewer analytics adapt to the current audience to display those advertisements to the customer that best fit his or her preferences and maximize purchase probability [38, 39]. Interaction can be initialized, once the customer directs his or her attention to the advertisement [40]. Forms of interaction include personalized messages, changing the display content following the picked-up item [21], sharing discounts [41], and downloading display content to a smart device [42]. Mobile shopping companion apps present current promotions, provide individual offers, create shopping lists, and manage the customer's loyalty status [25, 27]. Location-based push messages are a means to draw the

customer's attention, e.g., informing the customer of promotions when standing close to the product in question [43]. Digital shopping carts allow changing their display content in accordance with the items in the cart [44], e.g., to recommend products that fit the current selection or to display additional information regarding the selected items.

The latter refers to the information provision capability, where retailers provide research-supporting shopping aids [45]. Extending the customer's information base increases the customer's convenience and its product research efficiency [11, 15]. Smart devices, digital signage, digital shopping carts, self-service terminals, and robots can give further product-related information (e.g., the number of stock left, product presentations, manuals, the origin of ingredients, the terms of warranty, and customer reviews) [17, 43, 46]. Product recommendations in the form of alternatives and complementary merchandise to the current product [47] can be presented in the same way to assist the customer in evaluating alternatives [15]. Applications of augmented reality such as smart mirrors, and virtual reality such as car simulators, allow trying products virtually [48, 49]. Smart mirrors can also suggest accessories matching the tried garments and recommend relevant products [48]. As with all instances of personalization, information on the customer's current and historical contexts must be considered [45].

Retailers leverage customer insights such as shopping paths, item view counts, and sales data to improve their offerings [47]. Assortment management is tasked with optimizing the range of offered goods and their placement. The goal is to maximize the product return on investment (ROI) w.r.t. shelf space allocation [33]. Popular items are placed along frequent shopping paths and complemented by related high-margin products to stimulate additional sales [28, 50].

In-store technologies are a means to introduce new services or replace the manual labor of existing services by automation [8, 45]. Information provision and recommendation capabilities are mainly aimed at increasing revenue, while the following instances of automating manual labor at the retailer-consumer interface are aimed at decreasing cost. Electronic shelf labels, for example, replace manual labeling [24]. They further help reducing potential spoilage and excess inventory by automatically adjusting prices w.r.t. nearing expiry dates [6].

Customer self-service using in-store terminals [39], smart devices [27, 43], and robotic service encounters [17, 18] replaces person-to-person encounters and lets the customer perform tasks of the retailer [10]. Self-service terminals and mobile apps are research-supporting aids, which improve the customer's knowledge such as the location of the product [45]. In-store navigation and way-finding is a crucial function of self-service because not finding merchandise is a primary reason for customers leaving the store [51]. Stationary touchpoints provide maps and directions [36, 39, 40], whereas mobile touchpoints directly navigate customers to the item in question [17, 46].

Self-checkout terminals already shift the checkout task to the customer. The consistent procedural nature of the checkout process holds further cost saving potentials from automation [52] by speeding up the payment transaction and scanning of items. Contactless payment using NFC-enabled cards or smart devices fastens the process over cash or card-based transactions that involve entering a PIN or signing [53].

Attaching RFID-tags to the items enables faster scanning of products compared to conventional methods such as barcodes [54, 55].

RFID-tags also double as an anti-theft security feature, rendering older electronic article surveillance tags obsolete [54]. Security also benefits from the customer identification, data collection, and customer analysis capabilities, which can aid security staff in identifying suspiciously behaving customers [56]. The current generation of cameras and RFID-tags fulfills multiple purposes such as customer and stock tracking [54, 57] as well as providing security features, rendering old systems obsolete, and thus abolishing the cost of maintaining multiple systems.

Aggregated information on in-store customer behavior also aids in workforce optimization [23]. Predictive analytics on the expected customer frequency are used to schedule employees more efficiently and to prevent queues to accumulate by constantly calculating the optimal number of registers [23, 52]. Like identifying suspicious behavior, video analysis supports staff in identifying customers in need of assistance [17]. Staff can interact with customers in technology-enhanced service encounters, in which employees use smart devices such as tablets, watches, and glasses to get information on the customer and the respective products [10].

Lastly, video- and sensor-based stock detection in the shelves enable live stock-level tracking and improved inventory management [48, 57, 58]. Staff can be notified in case of nearing or existing out-of-stock situations. Thiesse and Buckel show that the cost of RFID-based replenishment is offset by the performance benefits over periodic manual checks of the shelves [57]. Preventing out-of-stock situations mitigates lost sales and reduces customer dissatisfaction over unavailable merchandise [51].

5 Digital Capabilities in the Shopper-focused Decision Calculus

The shopper-focused decision calculus guides retailers regarding potential impacts of retail technology on shoppers and the retailer's profits [6]. Drawing from equity theory, the authors empirically assess the customers' perceptions and reactions to retail technology on retail patronage and word-of-mouth as mediators of technology adoption [6, p. 15]. However, the potential contributions of contemporary in-store technologies to the archetypal business strategies remain a black box. We presented digital capabilities of contemporary in-store technologies and now incorporate them into an enhanced form of the shopper-oriented decision calculus (see Figure 3).

In-store technology capabilities are divided into enabling and executing capabilities, whereas the former elicit the customer's context either atomic on the individual customer level or aggregated on the store level. The latter is enabled and informed by the gained insights and execute the customer-facing services. In-store technologies themselves can be classified as context-aware if they can recognize and capture different situations using vision- or sensor-based technologies. Shopping-support systems influence the customer's shopping process directly by interacting with the customer (e.g., recommender systems, shopping assistants) or indirectly by altering the store environment (e.g., digital signage, assortment management). In-store technologies

can combine both enabling and executing capabilities and can be both context-aware and shopping-support systems.

The customer's perceptions mediate the potential influences of the capabilities on the archetypal strategies individualization and cost optimization. Following Inman and Nikolova's argumentation [6, p. 17,24], the acceptance of new technologies has an immediate impact on the retailer's profits. When customers, for example, do not adopt self-service terminals, their TCO are not offset by the realized TBO. Mediate effects are visible from customers altering their retail patronage. Good recommendations, for example, might lead customers to favor the service of the particular store over other stores, whereas negative experiences with in-store technologies might lead customers to choose a competitor in future. Similarly, customer word-of-mouth communication on their good and bad experiences moderates the impact of in-store technologies on the retailer's profit.

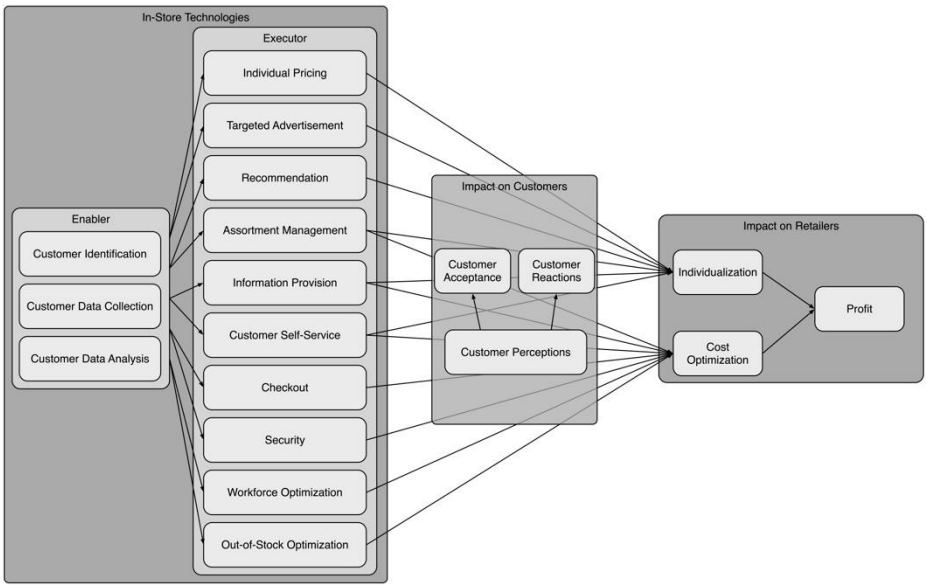


Figure 3. Augmented decision calculus

Individual pricing, targeted advertisements, and recommendations are essential capabilities for providing individual shopping experiences [7]. Research-supporting shopping aids [45] for information provision and customer self-service can both increase revenue through individualization and decrease cost by automating manual labor. Assortment management in a similar fashion increases revenue by optimizing the range and placement of offered goods, might improve customer satisfaction over better assortment, and decreases cost from excess inventory. Checkout, security, workforce optimization, and out-of-stock optimization are central capabilities to decrease cost by automating manual labor and by alleviating losses due to human mistakes, spoilage, theft, or employees being unproductive.

6 Discussion and Conclusion

We identified digital capabilities of in-store technologies and related them to the retailer's profit equitation. Our results serve as a starting point for retailers that want to adopt in- store technologies. The augmented decision calculus can become part of the sophisticated retailer's toolbox along other strategical lenses such as technology acceptance, investment management, and customer experience management.

Our results support the general assessment of new technologies but do not remove the need for a thorough evaluation of internal and external factors influencing the ROI. Retailers have to consider among other things the influence on different customer segments, organizational change [8], competitors, the sustainability of competitive advantage [11], and legal implications of context-aware technologies [43]. Moreover, the relevance and applicability of the individual technologies and capabilities depend among other things on the type of goods sold as well as the retailer's IT maturity and investment budget. Furthermore, the calculus does not consider the influence of an existing IT infrastructure on investment decisions and their profit implications. Future research can apply an integrative lens on the retailer's enterprise architecture regarding the integration, combination, and recombination of existing technologies to fulfill the capabilities. Since we abstract from particular instances of technology, we refrain from comparing the benefits and risks of individual technologies and do not attempt to rank or quantify their potential profit impacts. The digital capabilities are exploratively derived from contemporary literature on in-store technologies. We do not claim completeness of capabilities and ask other researchers to contribute and further extend our results. Moreover, is necessary to evaluate the augmented decision calculus in future research. We imagine conducting two-sided case studies, which validate the derived capabilities and hopefully provide support for their impact on the profit equitation. These results should be contrasted to surveyed customer perceptions, reactions, and measured adoption.

The speed of innovation urges especially small and medium-sized retailers, who are threatened by e-commerce, to continually assess new in-store technologies regarding their potential impact on profit and fit into their overall technological landscape. The presented set of digital capabilities supports retailers in understanding and classifying new technologies w.r.t. their contributions to the profit equitation. By incorporating the capabilities into the decision calculus, we provide retailers with a comprehensive tool for strategic thinking. Lastly, this research provides a comprehensive overview of contemporary in-store technologies for brick-and-mortar retail, which informs our overarching research project to design and evaluate technology-enabled service systems for co-creating digital customer experiences in brick-and-mortar retail.

Acknowledgments

This paper was developed in the research project *smartmarket*^{2}, which is funded by the German Federal Ministry of Education and Research (BMBF), promotion sign 02K15A074. We thank the Project Management Agency Karlsruhe (PTKA).

References

1. J. Hagberg, M. Sundstrom, and N. Egels-Zanden: The Digitalization of Retailing: an Exploratory Framework. Int. J. Retail Distrib. Manag. 44(6), 336–368 (2016)
2. K. Willems, A. Smolders, M. Brengman, et al.: The path-to-purchase is paved with digital opportunities: An inventory of shopper-oriented retail technologies. Technol. Forecast. Soc. Change 124, 228–242 (2017)
3. J. H. Betzing, D. Beverungen, J. Becker, et al.: Interactive Digital Customer Experience in High Street Retailing. HMD Praxis der Wirtschaftsinformatik 54(5), 659–671 (2017)
4. L. Bollweg, R. Lackes, M. Siepermann, et al.: Digitalization of Local Owner Operated Retail Outlets: The Role of the Perception of Competition and Customer Expectations. In: PACIS 2016 Proceedings. Paper 348. Chiayi, Taiwan (2016)
5. E. Brynjolfsson, Y. J. Hu, and M. S. Rahman: Competing in the Age of Omnichannel Retailing. MIT Sloan Manag. Rev. 54(4), 23–29 (2013)
6. J. J. Inman and H. Nikolova: Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns. J. Retail. 93(1), 7–28 (2017)
7. K. N. Lemon and P. C. Verhoef: Understanding Customer Experience and the Customer Journey. J. Mark. 80(6), 69–96 (2016)
8. E. Pantano and H. Timmermans: What is Smart for Retailing? Procedia Environ. Sci. 22, 101–107 (2014)
9. S. K. Roy, M. S. Balaji, S. Sadeque, et al.: Constituents and consequences of smart customer experience in retailing. Technol. Forecast. Soc. Change 124, 257–270 (2017)
10. R. J. Glushko: Seven Contexts for Service System Design. In: P. P. Maglio, C. A. Kieliszewski, and J. C. Spohrer (eds.) Handb. Serv. Sci., pp. 219–249. Springer (2010)
11. M. E. Porter: The Competitive Advantage: Creating and Sustaining Superior Performance. Free Press (1998)
12. J. Vom Brocke, A. Simons, B. Niehaves, et al.: Reconstructing the Giant: on the Importance of Rigour in Documenting the Literature Search Process. In: 17th Eur. Conf. Inf. Syst. pp. 2206–2217. ECIS '09, Verona, Italy (2009)
13. J. Webster and R. T. Watson: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Q. 26(2), 13–23 (2002)
14. H. M. Cooper: Organizing knowledge syntheses: A taxonomy of literature reviews. Knowl. Soc. 1(1), 104–126 (1988)
15. W. D. Hoyer, D. J. MacInnis, and R. Pieters: Consumer behavior. Cengage Learning, 6 edn. (2012)
16. E. Frontoni, P. Raspa, A. Mancini, et al.: Customers' Activity Recognition in Intelligent Retail Environments. In: Int. Conf. Image Anal. Process. pp. 509–516. Springer (2013)
17. F. Bertacchini, E. Bilotta, and P. Pantano: Shopping with a robotic companion. Comput. Human Behav. 77, 382–395 (2017)
18. K. Kamei, T. Ikeda, M. Shiomi, et al.: Cooperative customer navigation between robots outside and inside a retail shop—an implementation on the ubiquitous market platform. Ann. Telecommun. 67(7-8), 329–340 (2012)
19. A. Mancini, E. Frontoni, P. Zingaretti, et al.: Smart Vision System for Shelf Analysis in Intelligent Retail Environments. In: ASME/IEEE Int. Conf. Mechatron. Embed. Syst. Appl. Portland, OR, USA (2013)
20. T. H. S. Chu, F. C. P. Hui, and H. C. B. Chan: Smart Shopping System Using Social Vectors and RFID. In: Int. Multiconference Eng. Comput. Sci. vol. 1, pp. 239–244, IMECS '13, Hong Kong (2013)

21. H. Hwangbo, Y. S. Kim, and K. J. Cha: Use of the Smart Store for Persuasive Marketing and Immersive Customer Experiences: A Case Study of Korean Apparel Enterprise. Mob. Inf. Syst. (2017)
22. R. Ravnik, F. Solina, and V. Zabkar: Modelling In-Store Consumer Behaviour Using Machine Learning and Digital Signage Audience Measurement Data. In: Int. Work. Video Anal. Audience Meas. Retail Digit. Signage. pp. 123–133, VAAM 2014, Stockholm, Sweden (2014)
23. T.-W. Lee, Y.-L. Chiu, Y.-S. Wu, et al.: An intelligent image-based customer analysis service. In: 16th Asia-Pacific Netw. Oper. Manag. Symp., pp. 1–4. APNOMS ’14, Hsinchu, Taiwan (2014)
24. W. Zhou, Y.-J. Tu, and S. Piramuthu: RFID-enabled item-level retail pricing. Decis. Support Syst. 48(1), 169–179 (2009)
25. Kam-Yiu Lam, J. K. Ng, and Jian-Tao Wang: A Business Model for Personalized Promotion Systems on Using WLAN Localization and NFC Techniques. In: 27th Int. Conf. Adv. Inf. Netw. Appl. Work. pp. 1129–1134. WAINA ’13, Barcelona, Spain (2013)
26. A. Karmouche and Y. Salih-Alj: Aisle-level scanning for pervasive RFID-based shopping applications. In: Int. Conf. Comput. Syst. Ind. Informatics, pp. 1–4. ICCSII ’12, Sharjah, United Arab Emirates (2012)
27. R. Pierdicca, D. Liciotti, M. Contigiani, et al.: Low cost embedded system for increasing retail environment intelligence. In: Int. Conf. Multimed. Expo Work. pp. 1–6. ICMEW ’15 Turin, Italy (2015)
28. S.-H. Huang, C.-Y. Tsai, and C.-C. Lo: A multi-data mining approach for shelf space optimization. In: 11th Int. Conf. E-bus. pp. 89–95. ICE-B ’14, Vienna, Austria (2014)
29. J. Liu, Y. Gu, and S. Kamijo: Customer behavior classification using surveillance camera for marketing. Multimed. Tools Appl. 76(5), 6595–6622 (2017)
30. P. Yan and D. D. Zeng: In-store Shopping Activity Modeling based on Decision-theoretic Dynamic Bayesian Networks. In: 19th Work. Inf. Technol. Syst. pp. 55–60. WITS ’09, Phoenix, AZ, USA (2009)
31. Y. Zuo and K. Yada: Using statistical learning theory for purchase behavior prediction via direct observation of in-store behavior. In: 2nd Asia-Pacific World Congr. Comput. Sci. Eng. pp. 1–6. APWC on CSE ’15, Nadi, Fiji (2015)
32. K. Kamei, K. Shinozawa, T. Ikeda, et al.: Recommendation from robots in a real-world retail shop. In: Int. Conf. Multimodal Interfaces. ICMI-MLMI ’10, Beijing, China (2010)
33. H.-B. Li, W. Wang, H.-W. Ding, et al.: Mining paths and transactions data to improve allocating commodity shelves in supermarket. In: Int. Conf. Serv. Oper. Logist. Informatics. pp. 102–106. SOLI ’12, Suzhou, China (2012)
34. T. Nakahara and K. Yada: Evaluation of the Shopping Path to Distinguish Customers Using a RFID Dataset. Int. J. Organ. Collect. Intell. 2(4), 1–14 (2011)
35. A. Ogino, T. Kobayashi, Y. Iida, et al.: Smart Store Understanding Consumer’s Preference through Behavior Logs. In: Int. Conf. Int. Des. Glob. Dev. pp. 385–392, IDGD 2011, Orlando, FL, USA (2011)
36. K. Mankodiya, R. Martins, J. Francis, et al.: Interactive Shopping Experience through Immersive Store Environments. In: Int. Conf. Des. User Exp. Usability. pp. 372–382, DUXU 2013, Las Vegas, NV, USA (2013)
37. S. Longo, E. Kovacs, J. Franke, et al.: Enriching shopping experiences with pervasive displays and smart things. In: Proc. 2013 ACM Conf. Pervasive ubiquitous Comput. Adjun. Publ. pp. 991–998. UbiComp ’13, Zürich, Switzerland (2013)

38. P. Tian, A. V. Sanjay, K. Chiranjeevi, et al.: Intelligent advertising framework for digital signage. In: 18th ACM SIGKDD Int. Conf. Knowl. Discov. data Min. pp. 1532–1535. KDD ’12, Beijing, China (2012)
39. C.-C. Chen: RFID-based intelligent shopping environment: a comprehensive evaluation framework with neural computing approach. Neural Comput. Appl. 25(7-8), 1685–1697 (2014)
40. J. S. Kim: A Study of Contact Frequency and Consumer Preference for Digital Signage Advertisement. In: Green and Smart Technology with Sensor Applications, pp. 181–187. Springer, Berlin, Heidelberg (2012)
41. A. Kaasinen and Y.-I. Yoon: Mobile advertising model in N-Screen environment for CSCW. In: 7th Int. Conf. Comput. Converg. Technol. pp. 140–143, ICCCT ’12, Seoul, Korea (2012)
42. J. S. Lee and K. Yoon: The application of digital signage system using smart device. In: 16th Int. Conf. Adv. Commun. Technol. pp. 675–677. ICACT ’14, Pyeongchang, Korea (2014)
43. M. Bourimi, G. Mau, S. Steinmann, et al.: A Privacy-Respecting Indoor Localization Approach for Identifying Shopper Paths by Using End-Users Mobile Devices. In: Eighth Int. Conf. Inf. Technol. New Gener. pp. 139–144. ITNG ’11, Las Vegas, NV, USA (2011)
44. T. R. Sheltami and E. M. Shakshuki: An efficient RFID solution to expedite services. In: 7th Int. Conf. Adv. Mob. Comput. Multimed. pp. 255–259, Kuala Lumpur, Malaysia (2009)
45. C.-c. Angela Chang and M. Kukar-Kinney: The effects of shopping aid usage on consumer purchase decision and decision satisfaction. Asia Pacific J. Mark. Logist. 23(5), 745–754 (2011)
46. M. Strohbach and M. Martin: Toward a Platform for Pervasive Display Applications in Retail Environments. IEEE Pervasive Comput. 10(2), 19–27 (2011)
47. F. E. Walter, S. Battiston, M. Yildirim, et al.: Moving recommender systems from on-line commerce to retail stores. Inf. Syst. E-bus. Manag. 10(3), 367–393 (2012)
48. J. Melià-Seguí, R. Pous, A. Carreras, et al.: Enhancing the shopping experience through RFID in an actual retail store. In: ACM Conf. Pervasive Ubiquitous Comput. Adjun. Publ. pp. 1029–1036. UbiComp ’13, Zürich, Switzerland (2013)
49. B. Begole, T. Matsumoto, W. Zhang, et al.: Designed to Fit: Challenges of Interaction Design for Clothes Fitting Room Technologies. In: Int. Conf. Human-Computer Interact. pp. 448–457. HCI ’09, San Diego, CA, USA (2009)
50. M. A. Syaekhoni, C. Lee, and Y. S. Kwon: Analyzing customer behavior from shopping path data using operation edit distance. Appl. Intell. pp. 1–21 (2016)
51. M. Stone: The death of personal service: Why retailers make consumers responsible for their own customer experience. J. Database Mark. Cust. Strateg. Manag. 18(4), 233–239 (2011)
52. P. Kumar: The competitive impact of service process improvement: Examining customers’ waiting experiences in retail markets. J. Retail. 81(3), 171–180 (2005)
53. M. Cocosila and H. Trabelsi: An integrated value-risk investigation of contactless mobile payments adoption. Electron. Commer. Res. Appl. 20, 159–170 (2016)
54. M. Hauser, C. Flath, D. Zügner, et al.: Pushing the limits of RFID: Empowering RFID-based Electronic Article Surveillance with Data Analytics Techniques. In: ICIS 2015 Proc. (2015)
55. M. Grabia: Assessment of effectiveness of the use of RFID technology in selected processes at DIY retail store. In: IEEE Int. Conf. RFID Technol. Appl. 134–140, Tokyo, Japan (2015)
56. Y.-k. Wu, H.-C. Wang, L.-C. Chang, et al.: Customer’s Flow Analysis in Physical Retail Store. Procedia Manuf. 3, 3506–3513 (2015)
57. F. Thiesse and T. Buckel: A comparison of RFID-based shelf replenishment policies in retail stores under suboptimal read rates. Int. J. Prod. Econ. 159, 126–136 (2015)
58. E. Frontoni, A. Mancini, P. Zingaretti, et al.: Information Management for Intelligent Retail Environment: The Shelf Detector System. Information 5(2), 255–271 (2014)

Sind kleinere und mittlere Unternehmen (KMU) bereits auf die Digitale Transformation vorbereitet?

Can Adam Albayrak[1] und Andreas Gadatsch[2]

[1] Hochschule Harz, 38855 Wernigerode, Deutschland
calbayrak@hs-harz.de
[2] Hochschule Bonn-Rhein-Sieg, 53757 Sankt Augustin, Deutschland
Andreas.Gadatsch@h-brs.de

Abstract. Eine von den Autoren durchgeführte Untersuchung konnte deutliche Indizien dafür ausmachen, dass viele kleinere und mittlere Unternehmen (KMU) aktuell noch keine ausreichende Reife zur Digitalen Transformation haben. Zur Lösung des Problems wird vorgeschlagen, ein agiles IT-Management-Konzept zu entwickeln, um den IT-Bereich dynamisch und ohne formalen Ballast des klassischen IT-Managements zu steuern.

Keywords: KMU, Digitalisierung, Umfrage, IT-Strategie, Digitalisierungsstrategie, Agilität, IT-Management

1 Digitalisierung bei KMU

Digitale Transformation oder *Digitalisierung* bezeichnet meist eine Veränderung in den Nutzungsmöglichkeiten moderner Informations- und Kommunikationstechnik und deren Anwendungen im wirtschaftlichen und gesellschaftlichen Kontext. Während Großunternehmen häufig weniger Probleme haben, ihre Prozesse zu digitalisieren, kennen kleinere und mittlere Unternehmen (KMU) oftmals nicht die Möglichkeiten der Digitalisierung, verfügen nicht über das notwendige Know-how und die personellen Möglichkeiten oder scheuen die hohen Investitionen die damit einhergehen. Leyh und Bley [10] zeigen beispielsweise mit ihrer Befragung von kleineren und mittleren Unternehmen, dass „noch erheblicher Handlungsbedarf besteht, um die Potenziale moderner Informations- und Kommunikationstechnik […] angemessen zu erschließen, da hier teilweise noch große Hemmnisse auf Seiten der Unternehmen gesehen werden“. Die Autoren dieses Beitrages stellen nun die Hypothese auf, dass viele kleinere und mittlere Unternehmen keine ausreichende Digitalisierungsstrategie haben und auch nicht wissen, wie sie zu einer solchen Strategie kommen. Dazu befragten die Autoren Unternehmen sowohl in Interviews mit der Unternehmensleitung als auch durch eine schriftliche Umfrage.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

1.1 Bedeutung der KMU

Studien über KMU unterscheiden meist zwischen zwei KMU-Begriffen: den des Statistischen Bundesamtes Deutschland bzw. der Europäischen Union und den des *Institut für Mittelstandsforschung* (IfM). Gemäß der Definition des IfM erfüllen KMU folgende zwei Bedingungen: (1) Die Zahl der Beschäftigten ist kleiner als 500 und (2) der Jahresumsatz beträgt maximal 50 Mio. Euro [7]. Für mittlere Unternehmen liegt der Schwellenwert beim IfM bei weniger als 500 Beschäftigten und nicht niedriger als in anderen Definitionen, „um die deutsche Besonderheit" herauszustellen [13,14]. Das Statistische Bundesamt Deutschland bzw. die Europäische Union ziehen diese Grenze bereits bei 250 Mitarbeitern.

Zieht man die Grenze bei 250 Mitarbeitern, so zählen laut Statischem Bundesamt in Wiesbaden rund 99,3% zu den KMU. In diesen Unternehmen arbeiten 61% der Beschäftigten. Nach Angaben des schweizerischen Bundesamtes für Statistik stellen KMU in der Schweiz sogar fast den Regelfall dar, denn 99,7% der Unternehmen zählen dort zu den KMU. Rund 75% der Arbeitnehmer arbeiten in der Schweiz in KMU.

Die Führung von KMU folgt meist anderen Regeln als die in Großunternehmen, weshalb sich auch Art und Weise von IT-Management und IT-Governance bei KMU und bei großen Unternehmen signifikant voneinander unterscheiden. IT-Management ist ein in der Praxis gerne verwendeter unscharfer Begriff, der in einer weiten Fassung die Gesamtheit aller Maßnahmen zur Bereitstellung einer adäquaten Informationsversorgung umfasst. Das *IT Governance Institute* definiert als Hauptziel von IT-Governance, die Anforderungen an die IT sowie die strategische Bedeutung von IT zu verstehen, um den optimalen Betrieb der Unternehmensziele sicherzustellen. Darüber hinaus sollen Strategien für die zukünftige Erweiterung des Geschäftsbetriebes geschaffen werden [8]. Die seit 2008 existierende ISO/IEC 38500 unterscheidet die Begriffe *IT-Management* und *IT-Governance* wie folgt: IT-Governance umfasst die Vorgabe von strategischen Zielen und Regeln an die IT-Führungskräfte, um die Zielerreichung bei Einsatz von IT zu überwachen und zu steuern. Das IT-Management hingegen ist das aus Prozessen und Kontrollen bestehende System, das zur Erreichung der strategischen Ziele erforderlich ist.

In vielen KMU existiert gerade im IT-Bereich aufgrund der dünnen Personaldecke keine ausgeprägte Arbeitsteilung. Etwas überspitzt formuliert, muss jeder Mitarbeiter alle Aufgaben übernehmen können. IT-Leistungen werden oftmals unternehmens-intern erbracht, die Wartung der Arbeitsplatzsysteme oder der Betrieb des Rechenzentrums wird selten an externe IT-Leistungserbringer vergeben [1]. Ein weiteres in KMU anzutreffendes Modell ist die Auslagerung operativer IT-Aufgaben an vorwiegend lokale IT-Dienstleister, die selbst häufig zu den kleineren Unternehmen gerechnet werden können. Lediglich bei größeren KMU und Großunternehmen wird die IT-Leistungserbringung oft durch professionelle externe Dienstleister, also durch IT-Outsourcing, wahrgenommen. Bei diesen Unternehmen koordiniert der Chief Information Officer (CIO) die Leistungserbringung oder führt

aktiv den IT-Nachfragebereich, dessen Aufgabe es unter anderem ist, IT-bezogenen Anforderungen aus den Fachabteilungen aufzunehmen, zu konsolidieren und als Auftraggeber beim IT-Leistungserbringer zu vergeben, um ein IT-Gesamtpaket zur Unterstützung der Geschäftsprozesse zur Verfügung zu stellen. Fachabteilungen des Unternehmens beauftragen also über den CIO den IT-Lieferbereich mit zuvor abgestimmten IT-Leistungen.

1.2 Zentrale Fragen

Die Hypothese der Autoren dieses Beitrages lautete, dass KMU aktuell noch keine ausreichende Reife zur Digitalen Transformation haben, da diese Unternehmen überwiegend keine IT-Strategie besitzen und auch nicht wissen, wie man überhaupt zu einer IT-Strategie gelangt. Im Rahmen von Forschungsaktivitäten wurde daher untersucht, ob KMU bereits die Reife zur Digitalen Transformation haben, indem entsprechende Unternehmen befragt wurden, ob sie eine Strategie zur Digitalisierung haben und ob sie Methoden haben, solche Strategien überhaupt zu entwickeln. Im Abschnitt 2 beschreiben die Autoren die Methodik, die im Abschnitt 3 angewendet wurde. Abschnitt 4 versucht, die Ergebnisse zusammenzufassen. Der Beitrag schließt mit einem Vorschlag zur möglichen Lösung des Problems.

2 Methodisches Vorgehen

Zur Überprüfung der Hypothese der Autoren, wurden im Jahr 2016 insgesamt fünfzehn Unternehmen befragt, davon fünf in zwei- bis dreistündigen Interviewterminen, die übrigen durch eine schriftliche Befragung.

2.1 Interviews

Die als strukturierte Interviews mit den Unternehmensleitungen der KMU durchgeführten Befragungen wurden zuvor hinsichtlich Umfang und Dauer angekündigt, um die Voraussetzung eines tieferen Einblicks in die Unternehmen zu schaffen. Durch Vier-Augen-Gespräche zwischen jeweils einem der Autoren und einem Vertreter der Unternehmensleitung war es möglich, zu untersuchen, ob mit dem Begriff IT-Strategie und Digitalisierung dieselben Objekte gemeint waren. Zuvor wurde zudem durch persönliche Nachfrage bei den Entscheidungsträgern sichergestellt, dass die jeweiligen Interviewpartner tatsächlich für die Entwicklung von Strategien im Allgemeinen und IT- bzw. Digitalisierungsstrategien im Besonderen, zuständig und verantwortlich waren. Zudem wurden nur Unternehmen befragt, die auch eine bestimmte IT-Affinität haben, da nur bei diesen Unternehmen überhaupt eine gewisse Sensibilität für das Thema erwartet werden konnte. Um Sprachbarrieren auszuschließen wurden in den Interviews ausschließlich Unternehmen in Deutschland befragt. Geplante Interviews, die nicht den obigen Qualitätsmerkmalen entsprachen, wurden verworfen, so dass letztendlich fünf Interviewtermine berücksichtigt werden konnten. Nach einer Einleitung zum Thema wurden im Interviewtermin im Wesentlichen die Fragen aus Tabelle 1 gestellt:

Tabelle 1. Fragenkatalog der strukturierten Interviews

	Fragen im strukturierten Interview
1	Haben Sie eine IT-Strategie bzw. eine Digitalisierungsstrategie für Ihr Unternehmen? Ist diese schriftlich fixiert? Wie groß ist der Umfang?
2	Welches sind die wesentlichen Punkte der IT-Strategie/ Digitalisierungsstrategie? Welches sind die Ziele? Welche strategischen Projekte dienen der Zielerreichung? Gibt es strategische Richtlinien? Werden Prozessmodelle wie ITIL für das IT-Service-Management oder Modelle für die Durchführung von IT-Projekten bzw. Digitalisierungsprojekten eingesetzt?
3	Auf welche Art und Weise wurde die IT-Strategie/Digitalisierungs-strategie erstellt?
4	Mit wem im Unternehmen wurde die IT-Strategie/Digitalisierungs-strategie abgestimmt? Wie ist Position der IT im Unternehmen?
5	Mussten bestimmte Vorgaben der Unternehmensleitung bei der Erstellung der IT-Strategie/Digitalisierungsstrategie (wie Budget, bestimmte Kennzahlen, Compliance-Anforderungen etc.) berücksichtigt werden?
6	Wie ist die IT organisiert? Wie ist das Verhältnis der Fach-abteilungen zur IT? Wer macht was in der IT (Organigramm? Standorte? Outsourcing? etc.)?
7	Wer sind die (internen oder externen) Kunden der IT?
8	Wer sind die Lieferanten der IT? Wird der Markt von einzelnen Lieferanten dominiert? Wie wichtig sind Sie dem Lieferanten als Kunde? Wie „eng“ sind die Verträge mit den Lieferanten?
9	Was sind die Hauptrisiken in der IT aus strategischer Sicht?
10	Statistische Angaben über das Unternehmen

2.2 Schriftliche Umfrage

Um die obige Hypothese zu untermauern wurde ergänzend eine schriftliche Umfrage bei weiteren KMU durchgeführt. Zuvor wurde auch hier sichergestellt, dass die oben beschriebenen Rahmenbedingungen auch hier zutrafen. Diejenigen Umfrage-ergebnisse, die nicht den Merkmalen entsprachen, wurden verworfen, so dass hier

letztlich zehn Umfrageergebnisse berücksichtigt werden konnten. Den Befragten wurden online die Fragen aus Tabelle 2 gestellt:

Tabelle 2. Fragenkatalog der schriftlichen Befragung

	Fragenkatalog zur Onlinebefragung
1	Haben Sie eine IT-Strategie/Digitalisierungsstrategie für Ihr Unternehmen? Welches sind die wesentlichen Punkte der IT-Strategie?
2	Mussten bestimmte Vorgaben (Budget, bestimmte Kennzahlen, Gesetze) bei der Erstellung der IT-Strategie/Digitalisierungsstrategie berücksichtigt werden? Ist die IT-Strategie/Digitalisierungsstrategie schriftlich fixiert? Wie umfangreich ist die schriftliche Fixierung der IT-Strategie/Digitalisierungsstrategie?
3	Was sind die IT-Hauptrisiken aus strategischer Sicht in Ihrem Unternehmen?
4	Statistische Angaben: Mitarbeiter (umgerechnet in Vollzeitstellen) im Unternehmen? Wie viele Mitarbeiterinnen und Mitarbeiter (umgerechnet in Vollzeitstellen) sind davon für die IT zuständig?

3 Ergebnisse der Befragung

Die Antworten der insgesamt fünfzehn zufällig ausgewählten Unternehmen stellen aus erkenntnistheoretischer Sicht zwar noch keinen hinreichenden Beweis für die zu überprüfende Hypothese dar, können aber als deutliche Indizien für einen Trend bei KMU gewertet werden. Gerade bei den vergleichsweise umfangreichen Interviewterminen konnten die Autoren zahlreiche Zwischentöne heraushören, die auf die Existenz oder Nichtexistenz bestimmter Punkte hinwiesen. Oftmals konnten Antworten nicht quantitativ ausgedrückt werden, so dass bei der Auswertung „interpretierend und kritisch“ [12] vorgegangen wurde. Wir geben die Ergebnisse der Interviews und der schriftlichen Umfrage zusammenfassend an. In den Interviews wurden ausschließlich die Geschäftsführer bzw. Vorstände befragt, in der schriftlichen Befragung auch andere Entscheidungsträger.

3.1 Statistische Angaben

Abbildung 1 zeigt die Anzahl der Mitarbeiter, die in den befragten Unternehmen beschäftigt sind. Im arithmetischen Mittel haben die Unternehmen 120 Mitarbeiter zum Zeitpunkt der Befragung (Medianwert: 60 Mitarbeiter).

Der Anteil der beschäftigten Mitarbeiter, die ausschließlich für IT zuständig sind, bewegt sich (umgerechnet auf Vollzeitkräfte) absolut zwischen 0 und 12 Mitarbeiter und im arithmetischen Mittel bei 3,2% aller Mitarbeiter des jeweiligen Unternehmens.

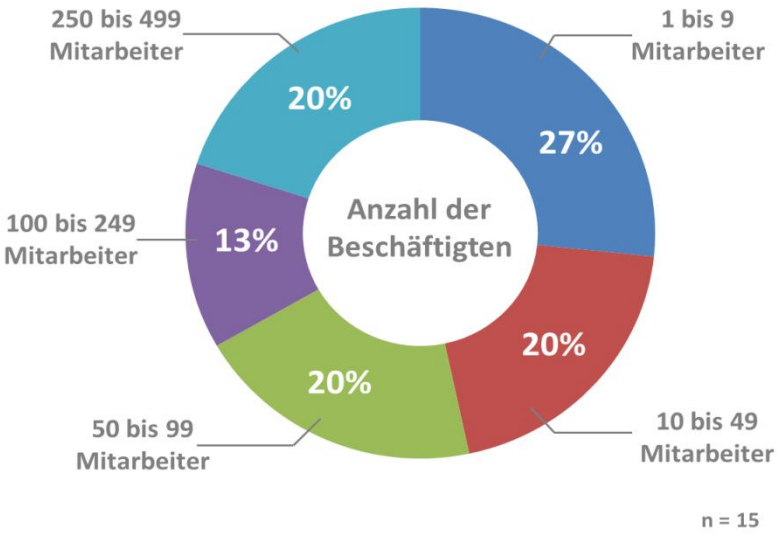


Abbildung 2. Anzahl der Beschäftigten in den befragten Unternehmen

3.2 Zentrale Ergebnisse

Die Umfrage ergab folgende Sachverhalte, die hinsichtlich Existenz, Umfang, Inhalte und Methoden zur Entwicklung kurz zusammengefasst werden:

- **IT- oder Digitalisierungsstrategie:** 6 der 15 befragten Unternehmen gaben an, dass sie eine IT- oder Digitalisierungsstrategie haben, also 40% der Unternehmen haben eine solche Strategie, 60% haben (noch) keine.
- **Umfang der Strategie:** Von den 6 Unternehmen, die eine IT- oder Digitalisierungsstrategie haben, gaben 5 Unternehmen an, dass diese schriftlich fixiert sei. Der Umfang beträgt allerdings nur zwischen einer und 15 Seiten (7 Seiten im arithmetischen Mittel). Details konnten von den Autoren eingesehen werden, allerdings ließen die Einblicke in die Beschreibungen keine Aussage darüber aus, ob die Strategie eine ausreichende Qualität zur Unterstützung der Geschäftsziele aufweist.
- **Eckpunkte der IT-Strategie/Digitalisierungsstrategie:** Von den 6 Unternehmen, die eine IT- oder Digitalisierungsstrategie haben, wurden die in Tabelle 3 aufgelisteten Antworten gegeben.

Tabelle 3. Eckpunkte der IT- oder Digitalisierungsstrategie

Anteil Nennungen	Eckpunkte der Strategie der befragten Unternehmen
50%	Reduzierung der Fertigungstiefe der IT /IT-Services aus der Cloud
33%	Ausbau mobiler Arbeitsplätze
33%	Integration der Prozesse der Kunden
33%	hohe Sicherheit der IT
17%	hohe Datenqualität, Digitalisierung, Wachstum, so wenig IT wie möglich, Flexibilisierung der IT

- **Vorgaben, die eingehalten werden mussten:** Von den 6 Unternehmen, die eine IT- oder Digitalisierungsstrategie haben, mussten laut Aussagen der Unternehmen folgende Vorgaben eingehalten werden:
  - ISO/IEC 27001 für das Sicherheitsmanagement
  - Einhaltung der Prämisse „Die IT dient dem Business, nicht umgekehrt"
  - Jede IT-Anwendung muss sich rechnen oder die Einhaltung von Gesetzen unterstützen
  - Unterstützung der Wachstumsstrategie des Unternehmens
- **Hauptrisiken der IT:** Alle 15 befragten Unternehmen konnten etwas zu den IT-Risiken sagen. Die Antworten werden in Tabelle 4 konsolidiert dargestellt:

Tabelle 4. Risiken der IT

Anteil der Unternehmen	Bezeichnung der Risiken der befragten Unternehmen
100%	IT-Sicherheit, Sicherheit der Daten
47%	Ausfall der IT
20%	Digitalisierung schreitet zu langsam fort
7%	hohe Komplexität der IT, Ausfall der IT-Mitarbeiter, Imageschädigung bei Bekanntwerden von Sicherheitslücken

- **Methoden zur Entwicklung einer IT- oder Digitalisierungsstrategie:** Von den 5 Unternehmen, die im Rahmen von Interviews befragt wurden, konnte zudem ermittelt werden, wie überhaupt die Entwicklung dieser Strategien im jeweiligen Unternehmen erfolgt. Zusammenfassend wurden folgende Methoden verwendet:
  - Workshop zur Entwicklung einer Unternehmensstrategie und Teilstrategien für IT und Digitalisierung (mit erster und zweiter Führungsebene)

– Betrachtung der Anforderungen und Evaluation möglicher Softwareprodukte, die den Anforderungen genügen.

3.3 Bewertung der Ergebnisse

Aus Autorensicht konnten durch die Umfrage deutliche Indizien dafür ausgemachen werden, dass die befragten Unternehmen noch keine ausreichende Reife zur Digitalen Transformation haben. Die Gründe dafür sind sehr vielschichtig. Es existieren zwar zahlreiche Methoden (z. B. Strategiesteuerung mit der Balanced Scorecard, Rahmenwerke wie COBIT und ITIL oder Reifegradmodelle wie CMMI) zur Organisation und Führung des IT-Bereiches, doch richten sie sich in der Regel eher an Großunternehmen, kaum jedoch an KMU.

KMU können Rahmenwerke (wie beispielsweise ITIL oder COBIT) oftmals nicht nutzen, da der zusätzliche administrative Aufwand für diese Unternehmen zu hoch erscheint. Dies ist ein entscheidender Wettbewerbsnachteil, da die Aufgaben und Themen im IT-Bereich für KMU und große Unternehmen sehr ähnlich sind. Klassisches IT-Management ist sehr stark methodengeprägt und geht von einer starken Aufgabenteilung aus. IT-Spezialisten und Mitarbeiter der Fachbereiche arbeiten nach formalisierten Plänen, um Software zu entwickeln, auszuwählen, einzuführen und zu betreiben. Vielfach haben solche Projekte lange Laufzeiten und am Ende nicht den gewünschten Erfolg.

4 Fazit und eine mögliche Lösung für die Misere

Kleine und mittlere Unternehmen sind häufig ganz anders organisiert als Großunternehmen und zögern, Veränderungen im IT-Bereich vorzunehmen. Wenn es Veränderungen gibt, dann erstrecken sie sich oftmals auf den rein technischen Bereich. Es konnte beobachtet werden [11], dass die Entscheider in KMU zudem oft Ad-hoc-Investitionen in IT vornehmen, um auf Markttrends zu reagieren oder weil sie dem Rat von IT-Anbietern folgen. Eine IT-Strategie ist in KMU zudem deutlich seltener vorhanden als bei großen Unternehmen [6]. In letzter Zeit wurden auch Fälle bekannt, bei denen KMU jüngere Unternehmen aufkaufen, die Digitalisierungsprojekte parallel zur eigenen IT vorantreiben („Fast IT“). Die eigene IT ist dann nur noch für die Kernapplikationen und deren Produktion verantwortlich („Slow IT“). Dies ist im Prinzip die „kleine“ Version der Aufgabentrennung nach dem Modell des Chief Digital Officers, der für die schnelllebigen digitalen Anwendungen und neuen Geschäftsmodelle in größeren Betrieben verantwortlich ist (vgl. beispielsweise [16]). Oftmals sind in KMU selbst Kennzahlen, die für eine aktive Führung der IT unabdingbar sind, wie beispielsweise die Gesamthöhe der IT-Kosten oder die Kosten für den IT-Betrieb nicht bekannt [1].

Häufig wird aus Sicht der Unternehmen immer wieder angeführt (vgl. [4] und [5]), dass

- eine feste Strategie die Flexibilität im Unternehmen stark einschränkt,
- die Planung mit viel Bürokratie verbunden ist
- und die Ressourcen zur strategischen Planung besser für andere Unternehmens-aktivitäten wie Vertrieb, Produktion oder Forschung und Entwicklung genutzt werden sollten.

5 Agilität als Lösung

Ein aktueller Trend, der durch Fachzeitschriften des IT-Managements und Gespräche mit IT-Experten bestätigt wird, ist das Konzept der Agilität. Vom lateinischen *agilis* abstammend, heißt agil *schnell und gewandt* aber auch *beweglich*. So positiv das Wort agil auch besetzt ist, so oft kommt es in Unternehmen zu Polarisierungen, wenn es um Agilität geht [9, S. 5-6]. Auf dieser Grundlage wurden zahlreiche Konzepte entwickelt. Beispielsweise listet [15] mehr als 30 verschiedene agile Vorgehensmodelle auf, die als *Agiles Projektmanagement* verstanden werden können.

Agile Methoden setzen vor allem auf Flexibilität und weniger auf starre Regeln und aufwendige Dokumentation. Die Produktqualität und Verfügbarkeit sind wichtiger, als Dokumente und Prozeduren. Allen Ansätzen ist gemeinsam, dass Sie auf dem Agilen Manifest basieren, das 2001 veröffentlicht wurde [2]. Das Agile Manifest hat im Bereich der Softwareentwicklung mittlerweile eine nicht mehr wegzudenkende Position erreicht. Hier wurden von renommierten Softwareexperten für die damalige Zeit revolutionär-innovative Grundsätze festgehalten, welche die Flexibilität der Softwareentwicklung extrem steigern sollen und deren Geist ganz im Gegensatz zu bisherigen starren Konzepten der Softwareentwicklung stehen (Auszug):

- Höchste Priorität ist es, Kunden durch frühe Auslieferung wertvoller Software zufrieden zu stellen.
- Anforderungsänderungen sind selbst spät in der Entwicklung willkommen.
- Agile Prozesse nutzen Veränderungen zum Wettbewerbsvorteil des Kunden.
- funktionierende Software wird regelmäßig innerhalb weniger Wochen oder Monate ausgeliefert.
- Fachexperten und Entwickler arbeiten während des Projektes täglich zusammen.
- Einfachheit ist essenziell.
- Die besten Entwürfe entstehen durch selbstorganisierte Teams.
- in regelmäßigen Abständen optimiert das Team seine Arbeitsweise.

Leider wurde das agile Konzept bislang kaum außerhalb der Softwareentwicklung zu einem „Agilen IT-Management-Konzept“ weiterentwickelt. Lediglich Bente et al. schlagen für das Management der IT-Architektur, also für einen engen Teilbereich des IT-Managements, ein agiles Vorgehen vor [3]. Nach wie vor dominiert im IT-Management sequentielles Arbeiten, d. h. (1) Ableitung einer IT-Strategie und damit

auch Digitalisierungsstrategie aus der Unternehmensstrategie, (2) Erstellung eines IT-Konzeptes auf Basis eines Fachkonzeptes zur Digitalisierung, (3) Implementierung der im IT-Konzept beschriebenen Lösung und (4) Betrieb, Weiterentwicklung und Wartung der Lösung.

Die Autoren sind der Meinung, dass die Prinzipien der Agilität aus dem Bereich der Software-Entwicklung dazu genutzt werden können, um für KMU eine *Agile IT-Management-Methode* zu entwickeln, mit der der IT-Bereich dynamisch ohne formalen Ballast des klassischen IT-Managements gesteuert werden kann. Eine Möglichkeit hierzu wäre die Nutzung und ggf. Gründung von KMU-spezifischen Interessensverbänden und Forschungskooperationen insbesondere mit anwendungsnah arbeitenden Universitäten und Fachhochschulen. Hierbei sind zahlreiche Fragen zu klären:

- Welche Voraussetzungen muss ein Unternehmen mitbringen, um sog. agile Methoden einsetzen zu können?
- Für welche Einsatzfelder ist agil der richtige Ansatz?
- Welche Vorteile und Nachteile müssen in Kauf genommen werden?

Schließlich könnte somit eine leichtgewichtige Methode für die Erstellung einer IT- oder Digitalisierungsstrategie entwickelt werden, die für KMU geeignet erscheint.

Literatur

1. Albayrak, C. A.; Gadatsch, A.: IT-Governance-Modell für kleinere und mittlere Unternehmen. HMD Praxis der Wirtschaftsinformatik, Heft 285 (IT im Mittelstand), S. 82-94 (2012)
2. Beck, K. et al.: Manifesto for Agile Software Development. http://agilemanifesto.org/ (Abruf am 09.09.2017)
3. Bente, S.; Bombosch, U.; Langade, S.: Collaborative Enterprise Architecture: Enriching EA with Lean, Agile, and Enterprise 2.0 practices, Morgan Kaufmann (2012)
4. Esser, W.M., Höfner, K., Kirsch, W. und Wieselhuber, N.: Der Stand der strategischen Unternehmensführung in der Bundesrepublik Deutschland und West-Berlin. In: W. Trux, G. Müller-Stewens und W. Kirsch (Hrsg.) Das Management strategischer Programme, Bd. 2, München, Kirsch, S.495-568 (1985)
5. Füglistaller, U., Frey, U. und Halter, F.: Strategisches Management für KMU - Eine praxisorientierte Anleitung, St. Gallen: KMU HSG (2003)
6. Gadatsch, A.; Kütz, M. und Juszczak, J.: Ergebnisse der 4. Umfrage zum Stand des IT-Controlling im deutschsprachigen Raum, Schriftenreihe des Fachbereiches Wirtschaftswissenschaften Sankt Augustin der Hochschule Bonn-Rhein-Sieg, Bd. 33, S. 8 (2013)
7. Günterberg, B.; Wolter H.-J.: Unternehmensgrößenstatistik 2001/2002 – Daten und Fakten. In: Institut für Mittelstandsforschung Bonn (Hrsg.): IfM-Materialien Nr. 157, Bonn. S. 13-14 (2003)
8. IT Governance Institute: IT Governance für Geschäftsführer und Vorstände, 2. Auflage, 2003, S. 8, http://www.isaca.org/German/Documents/Board-Briefing-on-IT-Governance-German.pdf (Abruf am 25.07.2017)

9. Kaltenecker, S.: Selbstorganisierte Unternehmen. Management und Coaching in der agilen Welt. 1. Auflage. Heidelberg: dpunkt.verlag (2017)
10. Leyh, C.; Bley, K.: Digitalisierung. Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. In: HMD 53 (1), S. 29-41 (2016)
11. Le Néal, C.: IT strategic planning for SMEs. Chartered Professional Accountants Canada, (2010)
12. Orlikowski, Wanda J. und Baroudi, Jack J.: Studying Information Technology in Organizations: Research Approaches and Assumptions. In: Information Systems Research (2:1), S. 1-28 (1991)
13. o. V.: KMU-Definition des IfM Bonn http://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (Abruf am 17.07.2017)
14. o. V.: Satzung der Stiftung des „Institut für Mittelstandsforschung“ in der Fassung vom 10. Juni 2005 http://www.ifm-bonn.org/fileadmin/data/redaktion/ueber_uns/dokumente /Satzung-IfM-Bonn.pdf, (Abruf am 24.07.2017)
15. o.V.: Liste mit agilen Projektmanagementmethoden, openPM e.V., https://www.openpm. info/display/openPM/Agiles+PM (Abruf am 09.09.2017)
16. Singh A.; Barthel P. und Hess, T.: Der CDO als Komplement zum CIO, in WUM, 01/2017, S. 38-47 (2017)

Are Local Retailers Conquering the Long Tail? A Web Usage and Association Rule Mining Approach on Local Shopping Platforms

Robin Ahlers[1], Lars Bollweg[1], Richard Lackes[2], André Ruegenberg[1], Ali Reza Samanpour[1], Markus Siepermann[2] and Peter Weber[1]

[1] Fachhochschule Südwestfalen, Wirtschaftsinformatik, Soest, Germany
ahlers.robin@fh-swf.de
bollweg.lars@fh-swf.de
ruegenberg.andre@fh-swf.de
samanpour.ali-reza@fh-swf.de
weber.peter@fh-swf.de
[2] TU Dortmund, Wirtschaftsinformatik, Dortmund, Germany
richard.lackes@tu-dortmund.de
markus.siepermann@tu-dortmund.de

Abstract. Competitors and customers put Local Owner Operated Retail Outlets (LOOROs) under digitalization pressure. Local Shopping Platforms (LSP) seem to be a promising approach for LOOROs to tackle the digitalization challenge and to overcome their physical and locational disadvantages compared to e-commerce players. However, little is known about the actual performance of LSPs and the (shopping) behavior of the LSP visitors. In this study, we therefore assess the web usage data of five German LSPs. Our findings show that LSPs provide a digital sales and service channel to LOOROs that extends their local catchment area and facilitates their online visibility and accessibility. However, LSPs so far miss the opportunity to create an inter-organizational shopping environment. LSP visitors do not browse across product offers of various vendors, but they mostly follow a single product search strategy and ignore the intended local marketplace structure of the platforms.

Keywords: Local Shopping Platforms, LOOROs, Local Retail, Web Usage Mining, Association Rule Mining

1 Introduction

In an overall positively developing market environment Local Owner Operated Retail Outlets (LOOROs) face an intense business and market transformation [1]. Several independent studies predict a decline in revenue for German LOOROs of 30% within the next four years [2] and even 50% within the next ten years [3]. In particular, the digitalization of sales channels is challenging the traditional hit-driven business models of the small stationery retailers. For decades, a hit-driven approach was a natural consequence of their limited shelf space, preventing them from carrying everything for everybody [4]. According to Anderson (2008), traditional stationery

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

retailers face two main disadvantages in comparison to online retailers: 1) Physically limited shelf and sales space forces them to focus on a strictly limited range of products and to exclude any (long tail) niche products from their shops. 2) Regional if not only local catchment areas and regulated opening hours limit the demand for their goods and services [5]. In today's age of the internet and e-commerce, digital distribution channels like esp. online shops and e-marketplaces challenge such traditional business models, as physical, regional and time limitations do not exist in online retail [5]. In his widely acknowledged book "Long Tail", Anderson (2008) summarizes the disruptive development in retail as follows: *"Our culture and economy are increasingly shifting away from a focus on a relatively small number of hits (mainstream products and markets) at the head of the demand curve, and moving toward a huge number of niches in the tail. In an era without the constraints of physical shelf space and other bottlenecks of distribution, narrowly targeted goods and services can be as economically attractive as mainstream fare*." [4]

However, LOOROs have options. Currently, Local Shopping Platforms (LSP), which act as intermediaries between LOOROs and their customers, are spreading in German cities [6]. The advent of LSPs has many ties to the long tradition of e-marketplaces, which, as inter-organizational information system, allow buyers and sellers to 1) exchange and negotiate prices and product characteristics and 2) to complete transactions [7]. The same is true for LSPs, but these added a very interesting twist to their business models. Striving for the critical mass of buyers, sellers and transactions, almost all well-known and successful e-marketplaces operate on a national if not international scale and address all types of customers, serving any sort of B2B, B2C or C2C transaction. In contrast, LSPs put forward locational self-restrictions and made them a fundamental part of their business models and marketing strategies. Either they allow only local retailers to operate on their platform, and/or they serve only local customers. LSPs harness the resulting local structure as a source of unique selling propositions, like e.g. delivery time advantages or service offers based on the direct neighborhood of the local shops (as decentralized storages) and the local customers [8].

LSPs are without question a promising option for LOOROs as they can help to overcome many of the e-commerce entry barriers (e.g. financial constraints, lack of knowledge, lack of infrastructure, etc.) [9]. Besides being a marketplace, they also act as digital service providers for LOOROs, releasing them from the burden of building up their own digital infrastructure and hiring expensive knowledgeable e-commerce experts. Furthermore, LSPs enable cooperation among competitors and thus facilitate synergy effects and cost savings for online activities [10].

On the other hand, joining an LSP can go along with problematic side effects, as LOOROs then become part of the self-reinforcing spiral of ubiquitous online price competition [11]. Further, LSPs charge LOOROs subscription and transaction fees, also drawing from their margins. Finally, it remains unclear, whether local people will accept the limited local e-marketplaces, when global competitors like ebay and Amazon with their unlimited customer base and their broad product and service range are just one click away [12].

Against this background, we aim to answer the following research questions:
RQ1: Do local shopping platforms in fact help LOOROs to overcome physical and locational disadvantages compared to e-commerce players?
RQ2: Do the origins and preferences of LSP visitors offer insights into potential "Long Tail" opportunities for LOOROs?
To answer the raised questions, we will use Web Usage Mining and Association Rule Analysis. We search for frequent usage patterns geared to Long Tail opportunities (e.g. expansion of the catchment area, the opening hours and/or demand for digital shelf extensions) within the web usage data of five local shopping platforms under the roof of one LSP provider in Germany. Each of the platforms is operating separately in one city and its surrounding region. Together, the platforms serve an installed basis of 238 LOOROs.
The remainder of this paper is structured as follows: In section 2, we discuss the methodological background. In section 3, we conduct the Web Usage and Association Rule Mining procedures and present the according results. In section 4, we discuss our findings to answer the research questions, highlight limitations and derive future research opportunities.

2 Methodology

2.1 Web Usage Mining

Web usage mining is the application of statistics and data mining techniques to discover usage patterns from web usage data like web logs and web tracking reports [13]. The goal of Web Usage Mining is to capture, model, and analyze the behavioral patterns and profiles of users interacting with a website [14]. The Web Usage Mining process consists of three phases, namely data preprocessing, pattern discovery and pattern analysis [15]. In the preprocessing stage, the web usage data needs to be cleansed from irrelevant and unreasonable items. In the pattern discovery stage, statistical, database, and machine learning operations are performed to obtain hidden patterns reflecting the behavior of users. In the final pattern analysis, the discovered patterns and statistics are further processed, filtered and used as input for a variety of data-mining algorithms [13].

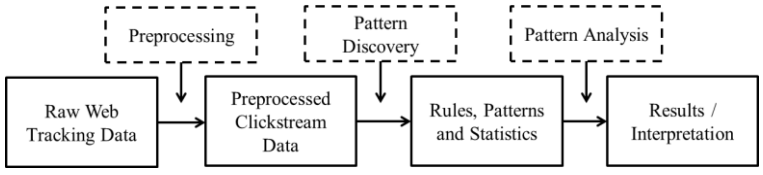


Figure 1. Research Procedure based on Nagi et al. (2011)

2.2 Association Rule Mining

Association Rule Mining on web usage data aims at finding "frequent item" sets, as groups of items (e.g. products or web pages) commonly accessed or purchased together [16]. Such item sets can be one-dimensional (e.g. only products) or multi-dimensional (e.g. products and time stamps) [17]. An association rule expresses an association between an antecedent and a consequent (sets of) item(s) in a shared interaction (e.g. page views in one session) [18]. The association rule r is an expression of $X \rightarrow Y$ (σr , αr), with X and Y as item sets, σ as support ($X \cup Y$), representing the share of interactions in which X and Y occur together, and α as confidence, representing the conditional probability that Y occurs in an interaction that already includes X [18]. An association rule is sound if the response within the target item group (confidence) is much better than the average response for the whole dataset. This is assessed using the metric lift, as the ratio of the response in the target item group and the average response of the whole data set. A lift of <1 or 1 implies that the probability of the occurrence of the antecedent and the consequent are independent of each other and that no rule exists. If lift is >1, the actual value indicates the degree to which a dependency exists, and thus how useful a derived rule would be for predicting the consequent in future data sets [17]. The Apriori algorithm is a well-known algorithm for finding association rules [18]. We used the version implemented by Borgelt (2002).

3 Analysis

3.1 Dataset

To answer the raised research questions, we analyzed the 1) web usage data and the 2) product databases of five LSPs managed by a German local shopping platform provider:

1) The available web usage data, retrieved from Google Analytics, consists of a custom session ID (int), the users' country and city (derived by Google from the IP addresses of the users (string)), the URL of the visited website (string) and the date, hour and minute of the visited webpage (string). The specification of the data is available as part of the Google Analytics Reporting API v4 reference [19].

2) The product data consists of the product name (string), the product URL (string), the product category (string), the vendor name (string), and the vendor category (string). Table 1 shows examples of the retrieved product and vendors categories.

We conducted the data preprocessing, the pattern discovery, and the analysis of the web usage data using the KNIME analytics platform (www.knime.com).

Table 1. Overview Top 8 Product and Vendor Categories

Top 8 Product Categories		Product Views	Top 8 Vendor Categories		Product Views
1.	Local Food & Beverage	9416	1.	Grocery Store	10238
2.	Home & Garden	7326	2.	Jewelry Store	6551
3.	Fashion	6996	3.	Book Store	6395
4.	Media & Books	5214	4.	Hobby Shop	5067
5.	Gifts	2927	5.	Furniture Store	3655
6.	Toys	2783	6.	Office Equipment Store	1708
7.	Sports Equipment	1954	7.	Liquor Store	1310
8.	Art	1860	8.	Pharmacy	1211

3.2 Data Preprocessing

For our analysis, we needed to transform and aggregate the web usage data on different levels of abstraction. In web usage mining, the most basic level of abstraction is a page view [15]. Regarding the website visitor, the most basic level of behavioral abstraction is a session, as a sequence of interactions (page views) by a single user in a given time (usually during a single visit) [15]. We examined frequent usage patterns and preferences on the following levels of abstraction: 1) page views 2) user sessions, and 3) location and time.

First, we cleansed the web usage data from entries not necessary/relevant for the mining process [13]. The initial data set included 487,906 unique page views. We removed all backend related page views (admin or login pages) to eliminate as many page views generated by vendors as possible. Further, we excluded all incomplete page view entries, for example in case of missing locational data, leading to 433,771 remaining datasets. These included 100,681 views of the global homepage, 56,555 views of global content pages (like the imprint, terms and conditions, jobs, etc.), 210,755 views of local product category pages, and 69,760 views of product pages.

In a second step, we preprocessed the sample of product page views for a location and time related analysis. As the time stamp for each interaction and the origin of the visitor were part of the data, only the platform location needed to be added as a reference for distance calculations. The online platform architecture uses one global homepage and local entry pages (as city names) for each local shopping platform on different domain levels. This way, we were able to derive the locational dependency of each page view directly from the URL structure.

In a third step, we joined the two tables (web usage data + product database) using the URL as a unique key available in both tables.

Table 2. Preprocessed Data Structure

Google Analytics						Products Database		
Session ID	Visitor Country	Visitor City	URL	Date / Time	Platform City	Product Category	Vendor Name	Vendor Category

3.3 Pattern Discovery

1) Location & Distance Categories: To identify locational usage patterns and preferences of LSP visitors, we developed a location & distance based categorization. Research on buying power and catchment areas of local shops usually sorts visitors into four different groups based on the distances between the location of the visitors and the location of the platform [20]: 1) Local Catchment Area: visits from within a fifteen kilometer radius around the location of the visited platform; 2) Distant Catchment Area: visits from outside the 15 km radius, but from within a 50 km radius around the visited platform; 3) Online Shopping Distance: visits from outside the 50 km radius of the platform, but from within Germany; 4) Foreign Country Distance: all visits from outside Germany. To implement these categories, we extracted the longitude and latitude of the cities using the Google Geocoding API [21]. With these coordinates at hand we then calculated the distances between each platform and its visitors, applying the Haversine formula. The Haversine formula, which is gaining growing attention in navigational contexts, calculates great-circle distances between two points (d) on a sphere (r), based on their longitude (λ) and latitude (Φ) coordinates [22].

$$d = 2r \arcsin\left(\sqrt{\sin^2\left(\frac{\phi_2 - \phi_1}{2}\right) + \cos(\phi_1)\cos(\phi_2)\sin^2\left(\frac{\lambda_2 - \lambda_1}{2}\right)}\right)$$

Figure.2 Havesine Formular

Table 3 provides an overview of our findings. More than 60% of all LSP visitors accessed the platform from a location more than 50 km away, what we consider as online shopping distance. Only 15% of the users accessed the platform from within the city itself. The results indicate that the self-restriction of LSPs to serve only local customers is contradicting the actually visitor structure and needs revision [6, 8].

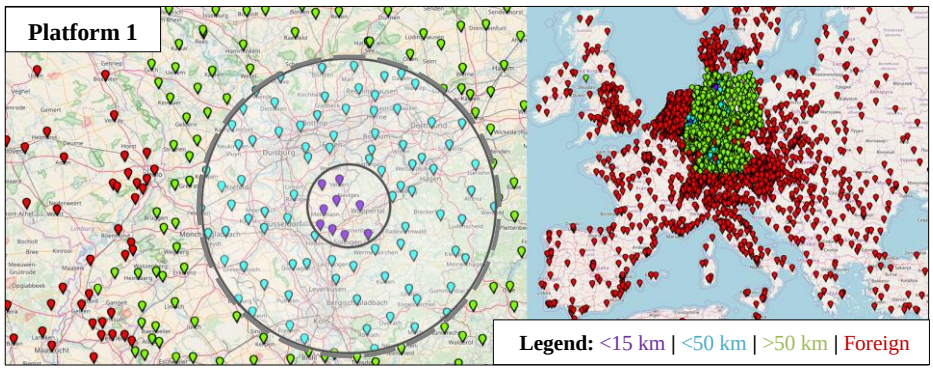


Figure 3. Distance Categories and Visitor Origins

Table 3. Overview Distance Categories / Product views

Location	Total	%	P1	%	P2	%	P3	%	P4	%	P5	%
Local	10263	14.7	7379	16.0	1391	12.6	364	7.0	606	12.3	523	21.6
Distant	8725	12.5	6963	15.1	805	7.3	720	13.9	194	3.9	43	1.8
Online	42170	60.5	26148	56.7	7444	67.2	3437	66.5	3533	71.5	1608	66.4
Foreign	8602	12.3	5653	12.3	1442	13.0	650	12.6	610	12.3	247	10.2

2) Time Categories: Also regarding time, we developed a categorization for platform visits, which we derived from the regular opening hours of local shops. As there are no standard opening hours in Germany, we defined the categories considering the development of the opening hour regulations. Traditionally, since 1956, German retailers had core opening hours between 10 am and 6 pm. A first extension allowed them to open their doors from 6am to 6pm. From on 1989, retailers were allowed to keep their stores open until 8 pm. Since 2006, opening hours are subject to state law and most federal states extended the timeframe to 10 pm or even midnight [23, 24]. Accordingly, we differentiate the following access time categories for platform visits: 1) Early opening hours, covering the time between 6am and 10am; 2) Traditional opening hours, covering the time between 10am and 6pm; 3) Late opening hours, covering the time between 6pm and 10pm; 4) Night / Closing time, covering the time between 22pm and 6am (when stationary retail stores are closed).

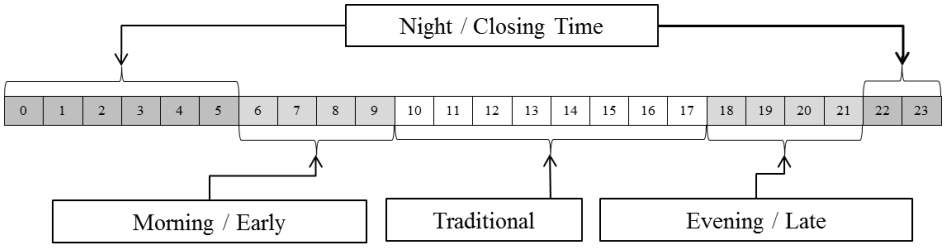


Figure 4. Time Categories

Applying these categories, the data reveals that the majority of users (49%) visited the platforms during traditional opening hours. At night (8%) and during early morning hours (11%), only few visits were recorded, while 32% of the visitors accessed the platform in the evening (see table 4).

Table 4. Overview Time Categories – Product views

Time	Total	%	P1	%	P2	%	P3	%	P4	%	P5	%
Early	8813	11.,3	5655	11.09	1572	12.5	694	11.7	576	10.5	316	11.9
Traditional	37842	48.7	24523	48.08	6337	50.4	3001	50.4	2592	47.1	1389	52.4
Late	24498	31.5	16407	32.17	3729	29.7	1791	30.1	1841	33.5	730	27.5
Night	6532	8.4	4420	8.67	936	7.4	466	7.8	492	8.9	218	8.2

To prepare the data for pattern discovery, we assigned each unique entry for page path (as a representation of a product page), distance, time, vendor and product category a numerical value. Table 5 shows the resulting data structure.

Table 5. Final Data Structure

Session ID	Visitor Country	Visitor City	URL	Date/ Time	Platform City	Product Category	Vendor Category	Distance Category	Time Category

3.4 Pattern Analysis

1) Session dependent Analysis: To identify Long Tail opportunities for LOOROs based on frequently viewed product sets within one session, we conducted a Market Basket Analysis using the Apriori algorithm [16]. Surprisingly, the algorithm was not able to detect any frequently viewed item sets, even when applying a very low threshold of 1% support and 5% confidence. We therefore looked at the session characteristics and found that the average visitor does not visit more than one product page, also indicated by a very low average session length of only 1.2 page views. Furthermore, we found a high number of direct bounces (84%) (see table 6).

Table 6. Session Length Overview

Single page session:	291.964	84.1%
Session 2 to 5 page views	53.145	15.3%
Session 6 to 10 page views	1.760	0.5%
Sessions > 10	296	0.1%

The average length of sessions including a product view was only 3 (page views), including only one product page view. This clearly shows that LSP visitors do not look around, but instead follow a very focused search strategy and usage pattern. Furthermore, the very short session length indicates a low transaction rate for the platforms, as the shortest path to complete a transaction requires six page views. Only 0.6% of the sessions reach this length and could thus carry a transaction (see table 6).

2) Distance and Time dependent Product Views: For further investigation of the Long Tail opportunities (extension of the catchment area, opening hours and/or demand for digital shelf extensions), we analyzed location and time preferences of LSP visitors, using a multi-dimensional association analysis [16]. To make sure that the rules that we discovered (using the Apriori algorithm) only represent frequent and important usage patterns, we defined high thresholds as filters: >25% for category support (support based on the distance categories), >15% for confidence, and >1 for lift [17]. Only rules above these thresholds will be part of the following discussion.
Regarding the impact of distance and time on product category views, we identified seven rules, revealing Long Tail potential mainly for Fashion and Home & Garden products. Rules 1, 2, 3 and 6 show that regardless their location, users especially visit Fashion product pages during traditional opening hours (e.g. “Local Customers + Traditional Shopping Time → Fashion Products”). The high lift (8.6) of rule 3 stresses the importance of this pattern. Further, rules 5 and 7 point at preferences of both, users visiting the platforms from online shopping distance in the evening hours and users visiting the platforms from outside the country during traditional opening hours, for Home & Garden product pages. Rule 4 indicates another interesting

behavioral pattern, as it shows that local food and beverages are of special interest for LSP visitors from outside the local catchment area and during traditional shopping times.

Table 7. Association Rules – Distance / Time to Product Category

	Antecedent		Consequent				
No.	**Distance**	**Time**	**Product Category**	**Support %**	**Category Support %**	**Confidence %**	**Lift**
1.	Local	Traditional	Fashion	7.07	48.1	15.2	1.107
2.	Dist. Catchment	Traditional	Fashion	5.19	41.5	16.6	1.209
3.	Online Shopping	Traditional	Fashion	26.3	43.5	11.9	8.627
4.	Online Shopping	Traditional	Local Food	26.3	43.5	20.4	1.101
5.	Online Shopping	Late	Home & Garden	17.8	29.4	16.7	1.160
6.	Foreign Country	Traditional	Fashion	5.84	47.4	16.2	1.174
7.	Foreign Country	Traditional	Home & Garden	5.84	47.4	18	1.250

(Category Support >25%, Confidence >15%, Lift >1)

Regarding the impact of distance and time on the users' vendor preferences, we identified six rules. Rules 1 and 2 point at a book store and jewelry store focus of users, who are accessing the platform from within a local range and during traditional opening hours. As stated in rule 3, users from the Distant Catchment Area tend to look at Jewelry Stores. Further, rules 4, 5 and 6 (rule 6 with a high lift of 8.9) indicate that during traditional shopping times, visitors from online shopping distances or from outside the country mainly look at Electronic Stores.

Table 8. Association Rules – Distance / Time to Product Category

	Antecedent		Consequent				
No.	**Distance**	**Time**	**Vendor Category**	**Support %**	**Category Support %**	**Confidence %**	**Lift**
1.	Local	Traditional	Book Store	7.07	48.1	17.5	1.390
2.	Local	Traditional	Jewelry Store	7.07	48.1	15.6	1.210
3.	Distant Catchment	Traditional	Jewelry Store	5.19	41.5	17.2	1.335
4.	Online Shopping	Traditional	Electronics Store	26.3	43.5	22.2	1.103
5.	Online Shopping	Late	Electronics Store	17.8	29.4	22.6	1.120
6.	Foreign Country	Traditional	Electronics Store	5.84	47.4	18	8.929

(Category Support >25%, Confidence >15%, Lift > 1)

4 Discussion & Conclusion

Applying Web Usage and Association Rule Mining, we analyzed the web usage data of five local shopping platforms in Germany. Regarding our first research question, *"Do local shopping platforms in fact help LOOROs to overcome physical and locational disadvantages compared to e-commerce players?*, our findings show that LSPs do help LOOROs to tackle locational limitations, but do not help them so far to overcome physical limitations (regarding shelf and sales space).

Concerning the limited catchment area of LOOROs, the platforms attract visitors and potential customers from outside the local and the distant catchment area (60% from

online shopping distance, 12% from foreign countries) and thus help LOOROs to extend their market reach. Surprisingly, local visitors (15%) and visitors from within a radius of 50km (13%) account for only a small portion of LSP user traffic. Further, LSPs extend the opening hours of LOOROs into the late evening (32% visitors between 6 pm and 10 pm), but the platforms mainly attract visitors during traditional opening hours so far (49% visitors between 10 am and 6 pm).
Concerning the physical limitations of LOOROs, LSPs at this point do not attract their visitors to browse around on their platforms, to look at various offers of the local vendors, and to discover unknown niche products from the tail of the demand curve. Based on the examination of the session characteristics, our findings indicate a focused search and usage behavior of the visitors. If LSP visitors view a product page at all (average session length 1.2 page views), they mostly look at only one single product. Apparently, users so far access LSPs mainly for shopping preparation, contributing to the "Research Online – Purchase Offline (ROPO) Effect" (also known as webrooming / showrooming) [25]. Accordingly, so far LSPs miss the opportunity to establish an inter-organizational marketplace with digital shelf extensions for local online shopping (local commerce), and instead only act as information hubs with regards to product availability and opening hours.

As to our second research question, *"Do the origins and preferences of LSP visitors offer insights into potential "Long Tail" opportunities for LOOROs?*, the web usage data revealed several interesting demand patterns, indicating Long Tail opportunities for the expansion of the catchment area and opening hours, but also pointing at demand for digital shelf extensions (see table 7 and 8). For example, we found products of Electronic Stores to be mainly visited by users from online distance or even foreign countries (see table 8). Regarding time, the majority of the demand patterns relate to traditional opening hours. Only two of the discovered rules cover the late evening. In conclusion, at this point especially retailers dealing with "Fashion" and "Home & Garden" products seem to benefit from the Long Tail effects of LSPs (e.g. demand from outside the local and distant catchment area and outside traditional opening hours) and thus could learn from the discovered demand patterns. Additionally, they also could benefit from digital shelf extensions provided by LSPs, as Fashion products are characterized by a huge variety in terms of colors, sizes and cuts, and Home & Garden products (like garden furniture) are often bulky, so that locational limitations are of particular relevance for the according retailers and delivery is of special importance for the customers [4].

Practical Implications: Our findings provide valuable insights for both, the owners of LOOROs and the providers of LSPs :
LOOROs: 1) LOOROs can harness LSPs as information and service hubs, improving their online visibility and allowing potential customers to check e.g. on the availability of products. 2) LOOROs should familiarize themselves with the opportunities of the Long Tail and they should analyze the revealed demand patterns to develop targeted LSP sales strategies [4]. 3) Furthermore, as shopping frequencies in high streets are declining [26], the high numbers of online visitors during

traditional opening hours points at the opportunity for LOOROs to establish a live online touch point with their customers [5].
LSPs: 1) Considering the origins of the platform visitors, a self-restriction to serve only local customers seems questionable. Nearly 85% of the users visited the platform from outside the local area and virtual geo fences would thus simply cut down the demand side of the platforms. 2) So far, LSPs fail to keep visitors on their sites. Improved landing page design and the use of recommendation services could help to extend the average session length and duration of visits, leading to a more attractive local online marketplace environment.

Limitations and Future Research: 1) Web usage data captures behavioral patterns and profiles of users along with their clickstream data. However, it offers no insights into the users' perception of the quality of a website and the attractiveness of its products and services. Thus, for deeper insights, transaction data needs to be taken into account. 2) Further, as long as LSPs fail to attract visitors to browse around on the LSPs, association rule (Market Basket) analysis depending on clickstream behavior can only offer very limited insights.
Considering our findings and the limitations of the research approach, we suggest the following areas of future research: 1) Research is needed, that aims at a better understanding of the search behavior of LSPs visitors, as it is so far unknown, why they leave the platforms so quickly. 2) A possible answer could be that they are preparing online for later offline transactions, as suggested by the "ROPO effect". Of course, LSPs like to put forward this argument in their marketing messages, but so far there is no quantifiable proof of the ROPO effect, as it is very challenging to measure customer journeys across different channels (online / offline) and different devices [27]. Thus, approaches need to be found that can help measure and proof the ROPO effect.

References

1. Bollweg, L.M., Lackes, R., Siepermann, M., Weber, P.: Mind the Gap! Are Local Retailers Misinterpreting Customer Expectations Regarding Digital Services? IADIS International Journal on WWW/Internet 13, 17–29 (2015)
2. Dierig, C.: Deutschlands Innenstädte Drohen zu Veröden, /Deutschlands-Innenstaedte-drohen-zu-veroeden.html (Accessed: 31.08.2017)
3. Siemssen, S.: Oliver Wyman Retail Journal German, http://www.oliverwyman.de/content/dam/oliverwyman/europe/ germany/de/ insights/publications /2017/Feb_2017/2017_Oliver_Wyman_Retail_Journal_German.pdf (Accessed: 31.08.2017)
4. Anderson, C.: Long tail, the, revised and updated edition: Why the future of business is selling less of more. Hyperion (2008)
5. Pantano, E., Viassone, M.: Demand Pull and Technology Push Perspective in Technology-Based Innovations for the Points of Sale: The Retailers Evaluation. Journal of Retailing and Consumer Services, Vol. 21, No. 1:43-47 (2014)

6. Bach, C.: Atalanda und buy local wollen mehr locale Online-Marktplätze aufbauen. Location Insider, http://locationinsider.de/atalanda-und-buy-local-wollen-mehr-lokale-online-marktplaetze-aufbauen/ (Accessed 17.09.2017)
7. Standing, S., Standing, C., Love, P.E.D.: A Review of Research on E-marketplaces 1997–2008. Decision Support Systems 49, 41–51 (2010)
8. Reimann, E.: David gegen Goliath: Wie der lokale Handel gegen Amazon kämpft. Heise online, http://www.heise.de/newsticker/meldung/David-gegen-Goliath-Wie-der-lokale-Handelgegen-Amazon-kaempft-2552842.html (Accessed: 17.09.2017)
9. Sandberg, K. W., Håkansson, F.: Barriers to adapt ecommerce by rural microenterprises in sweden: A case study. International Journal of Knowledge and Research in Management and E-Commerce 4(1), 1-7 (2014)
10. Huber, B., Sweeney E., Smyth, A.: Purchasing consortia and electronic markets. Electronic Markets 14.4, 284-294 (2004)
11. Alt, R., Klein, S.: Twenty Years of Electronic Markets Research-Looking Backwards Towards the Future. Electronic Markets 21, 41–51 (2011)
12. Verhoef, P.C., Kannan, P.K., Inman, J.J.: From Multi-Channel Retailing to Omni-Channel Retailing. Journal of Retailing 91, 174–181 (2015)
13. Nagi, M., ElSheikh, A., Sleiman, I., Peng, P., Rifaie, M., Kianmehr, K., Alhajj, R.: Association rules mining based approach for web usage mining. IEEE International Conference on Information Reuse and Integration, 166-171 (2011)
14. Kumar, B. S., Rukmani, K. V.: Implementation of web usage mining using APRIORI and FP growth algorithms. International Journal of Advanced networking and Applications, 1(06), 400-404 (2010)
15. Chen, Y., et al.: Market basket analysis in a multiple store environment. Decision support systems 40.2, 339-354 (2005)
16. Raorane, A.A., Kulkarni, R.V., Jitkar, B.D.: Association rule–extracting knowledge using market basket analysis. Research Journal of Recent Sciences 1(2), 19-27 (2012)
17. Borgelt, C.: Frequent item set mining. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 2(6), 437-456 (2012)
18. Borgelt, C., Kruse, R.: Induction of association rules: Apriori implementation. Compstat, 395-400 (2002)
19. Google: Dimensions & Metrics Explorer, https://developers.google.com/analytics/devguides/reporting/core/dimsmets (Accessed: 20.09.2017)
20. Wieland, T.: Innenstadtentwicklung und Strukturwandel im Einzelhandel. Ergebnisse einer Angebots-und Nachfragestudie zum Einzelhandel im niedersächsischen Mittelzentrum Holzminden unter besonderer Berücksichtigung der Innenstadt. Göttingen (2011)
21. Google: Entwickler Leitfaden GeoCoder API, https://developers.google.com/maps/documentation/geocoding/intro?hl=de (Accessed: 17.09.2017)
22. Van Brummelen, G.R.: Heavenly Mathematics: The Forgotten Art of Spherical Trigonometry. Princeton University Press (2013)
23. Fischer, I.: Verlängerung der Ladenöffnungszeiten. Statistisches Bundesamt (2003)
24. Hilf, E., Jacobsen, H.: Deregulierung der Öffnungszeiten und Flexibilisierung der Beschäftigung im Einzelhandel. Arbeit, 9(3), 204-216 (2000)
25. Nesar, S., Bin Sabir, L.: Evaluation of Customer Preferences on Showrooming and Webrooming:. Al-Barkaat Journal of Finance & Management 8.1, 50-67 (2016)
26. IFH Köln: Vitale Innenstädte 2016, https://www.ifhshop.de/studien/handel-allgemein/208/vitale-innenstaedte-2016 (Accessed: 17.09.2017)

IT-Sicherheit der Digitalisierung in Kleinen und Mittleren Unternehmen: Eine literaturbasierte und empirische Studie von Effekten und Barrieren

Erik Kolek[1]

[1] Universität Hildesheim, ISUM, Hildesheim, Germany
{erik_kolek}@gmx.de

Abstract. Die für kleine und mittlere Unternehmen (KMU) geeigneten IT-Sicherheitsaspekte wurden festgelegt, welche für die Digitalisierung in KMU wichtig sind. Hierzu wurde eine literaturbasierte Hypothesenbildung angewandt, welche IT-Sicherheitsaspekte für KMU wie Effekte und Barrieren hervorgebracht hat. Darauf aufbauend wurden die Hypothesen über die für KMU geeigneten IT-Sicherheitseffekte sowie -barrieren einer quantitativen Studie von KMU in Deutschland unterzogen. Diese empirische Hypothesenevaluation hat darüber Aufschluss gegeben, dass die literaturbasierten IT-Sicherheitsaspekte auch größtenteils für die Praxis der Digitalisierung in KMU in Deutschland als wichtig eingestuft werden können und daher mehr Beachtung erfahren sollten.

Keywords: IT-Sicherheit, Digitalisierung, Kleine und Mittlere Unternehmen.

1 Einführung

Die Nutzung von Informationstechnologie (IT) unabhängig von der Unternehmensgröße und Branche ist zu einem der wichtigsten Aspekte im Geschäftsumfeld von Unternehmen geworden. Vor allem kleine und mittlere Unternehmen (KMU) investieren einen entscheidenden Teil ihrer (finanziellen) Ressourcen in die IT, um ihre Fähigkeit im weltweiten Wettbewerb auszubauen. Zunehmend werden immer mehr Informationen gebildet und über eine große Anzahl von miteinander verknüpften Netzwerken übertragen. Gleichzeitig haben die Internetkriminalität und IT-Sicherheitsbedrohungen deutlich zugenommen, bspw. Schadsoftware, Spam und Phishing [1-2].

Diese Bedrohungen können zu hohen Verlusten für KMU führen und deren Wachstumschancen beeinträchtigen. Zudem bewirken Bedrohungen Kosten aufgrund von Geschäftsprozessausfällen, Schäden am Unternehmensansehen und Ausgaben, die zum Schutz der genutzten IT vor Angriffen und Missbrauch benötigt werden [2-4].

IT-Sicherheitsbedrohungen sind gekennzeichnet durch eine hohe Komplexität, da diese eine bedeutende Anzahl von Aspekten umfassen, die gemeinsam in Beziehung stehen können. Aufgrund der steigenden IT-Abhängigkeit ist die IT-Sicherheit in KMU von hohem Interesse, um entsprechenden Bedrohungen entgegen wirken zu können [2].

Da IT-Sicherheit in KMU für alle Beteiligten eine wichtige Angelegenheit darstellt, verlangt die Bekämpfung und Vorbeugung von IT-Sicherheitsbedrohungen eine

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

effektive Kooperation zum Aufbau und zur Erhaltung von IT-Sicherheit der Digitalisierung in KMU. Eine Herausforderung bei dieser Kooperation in KMU besteht daraus, dass jeder Beteiligte, wie Funktionen und Mitarbeitende, eine andere Meinung und einen anderen Ansatz vertritt, wie IT-Sicherheitsfragen beantwortet und wie potenzielle IT-Sicherheitsbedrohungen gehandhabt werden sollen. KMU verfügen über eine unterschiedliche – meist limitierte – finanzielle und personelle Ressourcenkapazität, die für die Kooperation zur Bekämpfung und Vorbeugung von IT-Sicherheitsbedrohungen zur Verfügung steht [2].

Die limitiert zur Verfügung stehende Ressourcenkapazität von KMU hinterlassen eine Lücke im Bereich der IT-Sicherheit der Digitalisierung und damit in Netzwerken von Unternehmen. Mittels des Zugangs zu wichtigen Informationssystemen werden KMU effektiver Bestandteil von Unternehmensnetzwerken, sodass in Anbetracht der potenziellen Möglichkeiten von IT-Sicherheitsbedrohungen, KMU als schwächstes Glied im Unternehmensnetzwerk auftreten können. Wie in jedem Netzwerk ist das schwächste Glied ein attraktiver Einstiegspunkt, um die in Unternehmen vorhandene IT anzugreifen. Jedes Netzwerk ist nur so sicher wie seine angreifbarste Schnittstelle, sodass für ein abgesichertes Unternehmensnetzwerk eine spezielle Aufmerksamkeit auf die IT-Sicherheit der Digitalisierung von KMU bestehen muss [2].

Vor diesem Hintergrund der fortschreitenden Digitalisierung in KMU liegt die Motivation dieser Forschungsarbeit darin, diejenigen IT-Sicherheitsaspekte zu erkennen und zu beschreiben, die für die IT-Sicherheit der Digitalisierung in KMU in Deutschland von besonderer Bedeutung sind. Die zugrundeliegende Forschungsfrage lautet daher: *Welche Aspekte hinsichtlich der IT-Sicherheit mit Wichtigkeit für KMU in Deutschland bestehen und wie lassen sich diese Aspekte inhaltlich beschreiben*?

2 Verwandte Arbeiten

Ein großer Anteil der KMU verfügt über unzureichendes IT-Personal mit genügend Wissen über die IT-Sicherheit und nicht über die Zeit und das erforderliche IT-Budget, um nötige IT-Infrastrukturen für eine Digitalisierung in KMU abzusichern [5].

Eine empirische Studie hat vor diesem Hintergrund einen Analyseschwerpunkt auf die Eignung von IT-Sicherheitsmanagement-Standards für KMU gelegt. In der Analyse waren KMU in Frankreich mit weniger als 250 Mitarbeitenden vertreten, da diese eine niedrige Akzeptanz gegenüber IT-Sicherheit innehatten. Weniger als 20% der KMU haben ein betriebliches IT-Sicherheitsmanagement oder einen Notfallplan fixiert. Dies stellt im Vergleich zu Großunternehmen einen offensichtlichen Schwachpunkt dar. In KMU bestehen eindeutige Unterschiede zwischen den tatsächlich eingeführten IT-Sicherheitsmaßnahmen und den tatsächlich vorhandenen IT-Sicherheitslücken. KMU konzentrieren sich auf IT-Sicherheitsmaßnahmen zur Vermeidung der mit niedriger Eintrittswahrscheinlichkeit existierenden Bedrohungen, anstatt häufiger auftretender und kostspieligerer Bedrohungen vorzubeugen [6].

In einer zweiten Studie wurde die Akzeptanz von IT-Sicherheitsstandards in KMU in Deutschland betrachtet. Die Forscher untersuchten deren Eignung hinsichtlich der Unternehmensgröße und diskutierten verschiedene Herausforderungen bei deren

Einführung. Der Untersuchungsgegenstand wurde begrenzt, sodass nur KMU betrachtet wurden, die mehr als 40 Mitarbeitende beschäftigten und einen Umsatz von mehr als 2 Millionen Euro pro Jahr erzielten. Da im Bereich der IT-Sicherheit der Digitalisierung viele Standards und andere Rahmenbedingungen in KMU als in Großunternehmen existieren, wurden die folgenden Rahmenwerke ausgewählt: ISO 27000-Reihe, Standard of Good Practice (SoGP), Control Objectives for Information and Related Technology (COBIT) und IT Infrastructure Library (ITIL). Die Forscher nahmen an, dass Studien hinsichtlich der Eignung von IT-Sicherheitsstandards für KMU bisher kaum im Fokus standen, da diese in KMU weitestgehend unbekannt sind. Zu diesem Phänomen gäbe es diverse Diskussionen vom Mangel an Interesse über zu wenig Akzeptanz bis hin zur geringen Eignung von IT-Sicherheitsstandards für KMU. Nichtsdestotrotz kommen die Forscher zu der Schlussfolgerung, dass im Umgang mit der IT-Sicherheit der Digitalisierung und den damit verbundenen betrieblichen Informationssystemen die Besonderheiten von KMU mehr Beachtung erfordern [7].

3 Literaturbasierte Hypothesenbildung

3.1 Für KMU entwickelte IT-Sicherheitseffekte

Die in der letzten Zeit sich rasant und schnell wandelnde wirtschaftliche Entwicklung im IT-Bereich hat auch KMU vor neuen Herausforderungen gestellt. Zu diesen neuen Herausforderungen zählen die Digitalisierung der gesamten KMU und die dazugehörigen Geschäftsprozesse. Vor allem die Umstrukturierung existierender Geschäftsmodelle, die Automatisierung einzelner oder aller Geschäftsprozesse und die weltweite digitale Vernetzung werden mit der Digitalisierung in Zusammenhang gebracht. Diese Veränderungen führen zu einer Umwandlung aller Geschäftsprozesse, die auch alle KMU beachten müssen, um ihre Wettbewerbsfähigkeit zu erhalten. Solchen Veränderungen waren lange Zeit nur große Unternehmen ausgesetzt – insbesondere im Zusammenhang mit aktuellen Themen wie Big Data, Cloud Computing oder Industrie 4.0, die in der Vergangenheit eingestuft wurden von KMU als nicht wichtig, zu kostspielig und zu kompliziert [8].

Diese digitalen Veränderungen haben zur Folge, dass KMU genauso wie die Großkonzerne allen Arten digitaler Wirtschaftskriminalität ausgesetzt sind, bspw. in Form von Datendiebstahl, Sabotage, Malware, Konkurrenzausspähung usw. Deshalb sind KMU mit schwieriger werdenden Herausforderungen konfrontiert, um relevante Informationen und ihr erworbenes Know-how vor unbefugten Dritten zu schützen und angemessene Vorkehrungen betreffs der IT-Sicherheit ihrer Digitalisierung zu treffen. Das hat zur Folge, das neben den Vorteilen der Digitalisierung insbesondere die ökonomische Bedeutung der IT-Sicherheit für KMU eine größere Rolle einnimmt und die IT-Sicherheit durch ein gutes Zusammenwirken zwischen der IT-Governance, IT-Compliance und dem IT-Risikomanagement unterstützt und gestärkt werden kann [9].

Neben der in Abstimmung mit der IT zu erreichenden Unternehmensziele sind für Unternehmen zudem gesetzliche Vorgaben bezüglich der IT-Compliance zu beachten. Inhalte dieser gesetzlichen Vorgaben sind z. B. der Datenschutz, die Ausfallsicherheit

der IT-Infrastruktur als auch die Erfüllung gesetzlicher Archivierungs- und Dokumentationspflichten. Eine etablierte IT-Compliance-Kultur ist insbesondere in KMU seltener als in Großunternehmen vorzufinden [10].

Zur Vollständigkeit gehört neben der Erreichung von Unternehmenszielen und der Einhaltung gesetzlicher Vorgaben auch ein angemessener Schutz vor Risiken zur IT-Sicherheit eines Unternehmens. Anti-Viren- und Firewall-Software bilden dabei eine solide Grundlage, genügen aber nicht annährend. Der effektivste Weg für einen umfassenden Schutz ist es ein Verständnis über die Auswirkungen der Risiken auf das Geschäftsmodell des Unternehmens zu erzeugen. Zudem sollten die Risiken in Geschäftsplanungen bedacht werden und falls möglich, sollten Investitionen in die Beseitigung oder zumindest Reduzierung der Chance des Auftretens der Risiken ausgeführt werden, um potenzielle Schäden zu verringern, die sie verursachen würden [11].

Die vorangegangenen Literaturbefunde zur Wirtschaftlichkeit, IT-Governance, IT-Compliance und zum IT-Risikomanagement wurden zu vier Hypothesen hinsichtlich der IT-Sicherheitseffekte für KMU zusammengefasst (siehe Tabelle 1).

Tabelle 1. Hypothesen hinsichtlich der IT-Sicherheitseffekte

Hypothesen H1 bis H4
H1. Die ökonomische Bedeutung der IT-Sicherheit hat für kleine und mittlere Unternehmen (KMU) deutlich zugenommen.
H2. IT-Governance (Organisation und Strategie der IT) ist ein wichtiger Aspekt zum Schutz der Vermögenswerte eines kleinen und mittleren Unternehmens.
H3. Die Einhaltung der gesetzlichen und unternehmensinternen Regelungen aus der IT-Compliance ist für KMU eine große Herausforderung im Bereich der IT-Infrastruktur.
H4. Das IT-Risikomanagement unterstützt bei der Identifizierung und Verringerung von Risiken in KMU.

3.2 Für KMU entwickelte IT-Sicherheitsbarrieren

Ein nicht vorhandenes Vertrauen zwischen der Geschäftsführung und IT und das limitierte Know-how des IT-Personals hinsichtlich der Digitalisierung in KMU sind auf eine ungenügende IT-Strategie zurückzuführen, die bei vielen KMU nur aus technologischen Maßnahmen (Virenschutz, Firewalls, Backups) besteht. Verantwortlich dafür ist der für KMU größere Stellenwert technologischer Maßnahmen anstatt der in der IT-Strategie ebenfalls einzubindenden organisatorischen Maßnahmen. Diese falsche Denkweise basiert auf einem Bewusstseins-/Awareness-Defizit der KMU und hat zur Folge, dass IT-Sicherheitsvorkehrungen mittels Schwachstellen- und Sicherheitsuntersuchungen vereinzelt oder gar nicht realisiert werden. Diese zielgerichteten Untersuchungen sind von entscheidender Bedeutung, um die Werte für KMU in ein passendes ökonomisches Verhältnis zu den IT-Sicherheitsinvestitionen zu stellen. Eine systematisierte Prozedur zur Untersuchung potenzieller Sicherheitslücken und deren Beseitigung durch organisatorische Maßnahmen gemäß der IT-Strategie stellen ein grundsolides Gerüst her, um die IT-Sicherheit im Unternehmen zu stärken [9]. Um eine planungsgemäße Umsetzung der IT-Strategie zu garantieren, sind IT-

Richtlinien erforderlich, die z. B. den Datenschutz, Rechenzentrumsbetrieb, die Informationssicherheit als auch das Aussuchen von individuell entwickelter und beschaffter computergestützter Informationssysteme beinhalten [12].

In IT-Richtlinien sind alle Geschäftsanweisungen bezüglich der Entwicklung und Nutzung von Anwendungen und IT-Systemen dokumentiert, die für alle Beteiligte in KMU gelten. IT-Richtlinien orientieren sich an den Anforderungen der in KMU genutzten IT-Applikationen und den darin modellbasiert beschriebenen Geschäftsprozessen. Die Beurteilung der Bedeutung der genutzten IT-Applikationen ist bei KMU dadurch beschränkt, dass die Entscheidungsfindung oft nur von einem Menschen, dem Geschäftsführer, vorgenommen wird. Eine richtliniengemäße Beurteilung der Bedeutung genutzter IT-Applikationen wird nur erreicht, wenn die betroffenen Abteilungen eingebunden werden, da nur diese die Wichtigkeit für das Unternehmen bewerten können. Demzufolge kann eine KMU-weite gültige IT-Richtlinie nur erstellt werden, wenn die Geschäftsführung in Kooperation mit ihren Abteilungen kooperiert und für alle Beschäftigten einzuhaltende IT-Sicherheitsmaßnahmen fixiert [12].

Um ein geplantes IT-Sicherheitsniveau mit den damit verknüpften IT-Richtlinien für die internen IT-Infrastrukturen in KMU zu erreichen, muss ferner eine Untersuchung potenzieller Schadens- und Angriffsszenarien mit einem IT-Sicherheitskonzept realisiert werden. Unzureichende IT-Sicherheitsmaßnahmen führen zu einer fehlerbehafteten IT-Infrastruktur mit verminderter Leistungsfähigkeit, Schäden am Ansehen und zu negativen ökonomischen Folgen. Um möglichst ein effektives IT-Sicherheitskonzept zu erstellen, sollte zuerst die IT-Struktur untersucht werden. Hierzu erfolgen eine Ist-Zustand-Bewertung und die Festlegung der Anwendungen und IT-Systeme, die das IT-Sicherheitskonzept betreffen [13-15].

Eine große Anzahl der KMU, im Gegensatz zu Großunternehmen, stehen vor beträchtlichen Barrieren bezüglich einer erfolgreichen Implementierung von IT-Rahmenwerken, vor allem wegen des Know-how-Mangels und den stark limitierten (finanziellen und personellen) Ressourcen. Die in KMU limitierte IT-Mitarbeiteranzahl führt oft dazu, dass die mit der Implementierung von IT-Rahmenwerken ordnungsgemäßen Aufgaben und Regeln nicht vollständig umgesetzt und eingeführt werden. Die limitierten Kapazitäten haben zur Folge, dass KMU zu vielen schwierigen Prozessen gegenüberstehen, welche für die IT-Rahmenwerkimplementierung ausgeführt werden müssen. Demnach bringen KMU (aktuellen) IT-Rahmenwerken wenig Akzeptanz entgegen und stellen sich nicht den Anforderungen. Um diesen Zustand zu optimieren, ist die Anpassung bzw. Verkleinerung existierender IT-Rahmenwerke oder die Entwicklung eines flexiblen, ökonomischen, und einfach zu nutzenden IT-Rahmenwerks notwendig, das speziell den Anforderungen von KMU entspricht [16].

Mitarbeitende neigen dazu viele Fehler zu machen, indem sie z. B. Passwörter vergessen, ihren Arbeitsplatz verlassen und dabei ihren Rechner anlassen oder Daten einfach nicht auf den neuesten Stand bringen. Solche Fehler gehören zur Arbeitsrealität in unserer heutigen IT-basierten Informationsgesellschaft und stellen auch in vielen KMU eine Barriere dar, die auf ein unzureichendes IT-Bewusstsein (IT-Awareness) zurückzuführen ist. Demnach ist nicht nur die Erkennung von technologischen Schwächen sondern zudem die Identifizierung von Sicherheitsstörungen durch den menschlichen Faktor entscheidend, um die IT-Systeme in KMU abzusichern. Dabei

wird das IT-Bewusstsein nicht nur durch die Bildung und Fortbildung von Mitarbeitenden in der Nutzung der IT erhöht, viel mehr zählt zudem eine Anpassung im Verhalten der Mitarbeitenden dazu, um einen wirkungsvollen Stimulus für die Sicherheit von sensiblen Unternehmensinformationen zu erzeugen. Dagegen weist das IT-Bewusstsein der Mitarbeitenden in KMU viel weniger an Wichtigkeit auf als Investitionen in Hard- und Software, um die IT-Sicherheit auszubauen. Die Gründe dafür sind z. B. Fahrlässigkeit, ein niedriges Verständnis und fehlende Compliance- oder Audit-Vorschriften hinsichtlich des IT-Bewusstseins. Der Ausgangspunkt des niedrigen Interesses für das IT-Bewusstsein liegt vor allem im mangelnden Verständnis der KMU für die potenziellen Risiken und deren potenziellen Auswirkungen [17-18].

Die vorgestellten Literaturbefunde zur IT-Strategie, IT-Richtlinie, IT-Awareness, zum IT-Sicherheitskonzept und IT-Rahmenwerk wurden zu fünf Hypothesen hinsichtlich von IT-Sicherheitsbarrieren für KMU zusammengefasst (siehe Tabelle 2).

Tabelle 2. Hypothesen hinsichtlich der IT-Sicherheitsbarrieren

Hypothesen H5 bis H9
H5. Eine unzureichende IT-Strategie macht den Geschäftsbetrieb eines KMUs verwundbar.
H6. Die IT-Richtlinie wird von der Geschäftsführung in KMU erstellt.
H7. Ein mangelndes IT-Sicherheitskonzept in KMU ist auf eine unvollständige IT-Richtlinie zurückzuführen.
H8. KMU benötigen ein IT-Rahmenwerk, das ihren speziellen Bedürfnissen entspricht.
H9. Die fehlende Förderung des IT-Bewusstseins (IT-Awareness) von Mitarbeitenden führt zur fehlerhaften Anwendung der IT-Richtlinien in KMU.

4 Methodische Vorgehensweise in der quantitativen Studie

Bei der Vorbereitung einer empirischen quantitativen Studie sind methodische Vorgehensweisen ein zentraler Bestandteil für eine wissenschaftliche Durchführung. Dafür wurden folgende Bestandteile einer empirischen quantitativen Studie beachtet: Hypothesenbildung, Fragebogendesign, Studiendurchführung, Datenanalyse und Datenpräsentation. Neben der Hypothesenbildung (siehe Abschnitt 3) ist die Ausgestaltung des Fragebogendesigns ein weiterer wichtiger Bestandteil in der Datenerhebung, um möglichst zahlreiche Teilnehmende gewinnen zu können. Zur Gestaltung des Fragebogens stehen viele Online-Umfragewerkzeuge zur Verfügung. Ausgewählt wurde letztendlich LimeSurvey. Dieses Umfragewerkzeug verfügt über ein Vorlagensystem, das eine benutzerdefinierte Anpassung des Layouts und Designs gestattet. Damit konnte die Studie öffentlich – durch eine vorherige Authentifizierung von Benutzern (Security-Token) – zugänglich gemacht werden. Der Beginn und die Dauer der Studie konnten nach der Ausformulierung der Frageblöcke mit den untergeordneten Fragen (Hypothesen H1-H9) individuell festgelegt werden. Nach dem Abschluss einer empirischen quantitativen Studie, kann die Analyse der erhobenen Daten erfolgen [19].

Das Fragebogendesign wurde nach erfolgreicher Validierung der Verständlichkeit mit Managern aus KMU ausgiebig getestet in LimeSurvey bezüglich der Filterfragen

(Bedingungen). Nach Beseitigung aller Unklarheiten und Fehler in LimeSurvey ging die Studie online und wurde im November 2016 durchgeführt. Die Studie wurde mit Hilfe eines motivierenden Einladungstexts samt Link zur Online-Umfrage in diversen sozialen und beruflichen Netzwerken veröffentlicht. Der Schwerpunkt lag dabei auf Gruppen, die sich z. B. mit Themen auseinandersetzten wie IT, IT-Sicherheit, IT-Rahmenwerken und KMU. Um eine denkbare Mehrfachteilnahme auszuschließen, musste sich jeder Teilnehmende für die Studie registrieren. Nach Ablauf der Frist haben sich 88 potenzielle Teilnehmende für die Studie zur IT-Sicherheit der Digitalisierung in KMU registriert. 76 Manager und Mitarbeitende haben erfolgreich teilgenommen.

Zur Datenanalyse wurde das Microsoft Excel Software-Add-In XLSTAT genutzt. Zuerst erfolgte eine Datenbereinigung unter Beachtung folgender Ausschlusskriterien: Entfernung aller leeren und unvollständigen Datensätze und aller Datensätze mit Bezug zu einem anderen Land außer Deutschland, Entfernung aller Nicht-KMU-Datensätze (bis 499 Beschäftigte UND bis 50 Millionen Euro Umsatz, KMU-Definition des IfM Bonn [20]). Von den ursprünglich 76 Teilnehmenden sind nach der Datenbereinigung 46 Teilnehmende aus KMU in Deutschland übrig geblieben. In dieser explorativen quantitativen Datenanalyse werden für die Datenpräsentation Boxplots genutzt, um die Zustimmung bzw. Ablehnung hinsichtlich einzelner Hypothesen bildlich aufzuzeigen.

Von den insgesamt 46 verbleibenden Befragten kam etwa die Hälfte der Teilnehmer aus Niedersachsen (50,00%) gefolgt von Nordrhein-Westfalen (19,57%) und Hamburg (8,70%). Die verbleibenden Bundesländer waren vereinzelt oder nicht vertreten. Daher kann von keiner statistischen Signifikanz der Datenanalyse für KMU in Deutschland gesprochen werden. Für Niedersachsen können die Daten jedoch als signifikant gelten. Hinsichtlich der Branchen, in denen die KMU positioniert waren, arbeitete ein Großteil der hierin Beschäftigten in der Beratungsbranche (34,78%) und einer anderen Branche (65,22%) als jene, die in der Studie abgefragt wurden. Bei der Frage nach der beruflichen Stellung antworteten die meisten Befragten oberste Managementebene (36,96%) und mittlere Managementebene (26,09%). Der Rest verteilte sich mit 17,39% auf die unterste Managementebene und den Mitarbeitenden, denn 19,56% hatten keine Managementfunktion. Aufgrund der Verteilung der Antworten bezüglich der Branche und des Berufsstatus ist es nicht erstaunlich, dass die meisten Befragten ihren Aufgabenbereich in der Geschäftsführung (30,43%) und im Kundenmanagement (26,09%) hatten. Andere Befragte waren im IT-Management (8,70%), Marketing und Vertrieb (8,70%), in der Revision (8,70%), im Finanzmanagement und Controlling (4,35%) oder in einem sonstigen Aufgabenbereich (13,03%) tätig.

5 Empirische Hypothesenevaluation

5.1 Für KMU in Deutschland wichtige IT-Sicherheitseffekte

Aufgrund der genutzten Likert-Skala (7 = stimme voll und ganz zu; 4 = neutral; 1 = stimme überhaupt nicht zu) ist bei allen vier Hypothesen hinsichtlich der IT-Sicherheitseffekte für KMU in Deutschland eine deutliche Tendenz zur Zustimmung gegeben (siehe Abbildung 1 und ergänzend die Tabellen 1 und 3).

Tabelle 3. Deskriptive Statistiken bezogen auf die Boxplots der IT-Sicherheitseffekte

Statistik	*Ökonomische Bedeutung für KMU*	*IT-Governance*	*IT-Compliance*	*IT-Risiko-management*
Minimum	2,000	3,000	2,000	3,000
1. Quartil	5,000	5,000	5,000	5,000
Median	6,000	6,000	6,000	6,000
3. Quartil	7,000	7,000	7,000	6,750
Maximum	7,000	7,000	7,000	7,000
Mittelwert	5,913	5,696	5,739	5,783
Varianz	1,459	1,328	1,664	1,018

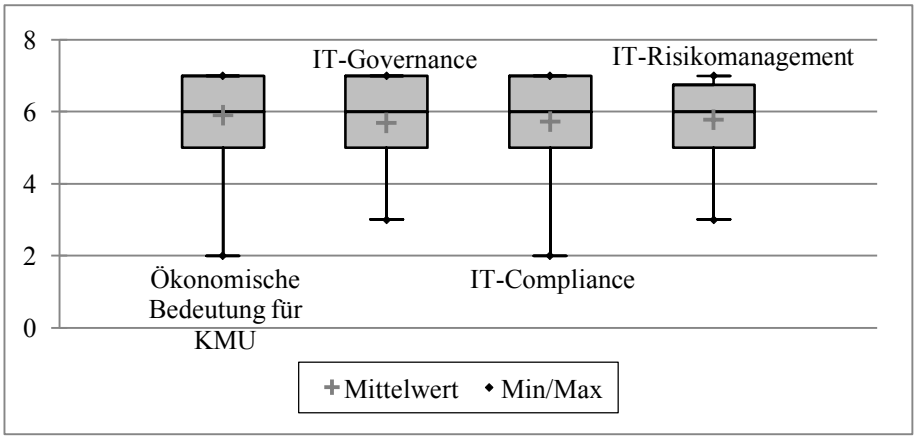


Abbildung 1. Boxplots der IT-Sicherheitseffekte

Der Hypothese H1 wird eindeutig zugestimmt. Die ökonomische Bedeutung der IT-Sicherheit scheint für kleine und mittlere Unternehmen (KMU) in Deutschland deutlich zugenommen zu haben. *Der Hypothese H2 wird eindeutig zugestimmt*. Die IT-Governance inklusive der Organisation und Strategie der IT wird als ein wichtiger Aspekt zum Schutz der Vermögenswerte eines kleinen und mittleren Unternehmens in Deutschland wahrgenommen. *Der Hypothese H3 wird eindeutig zugestimmt*. Die Einhaltung der gesetzlichen und unternehmensinternen Regelungen aus der IT-Compliance erscheint für kleine und mittlere Unternehmen in Deutschland eine große Herausforderung im Bereich der IT-Infrastruktur zu sein. *Der Hypothese H4 wird eindeutig zugestimmt*. Das IT-Risikomanagement unterstützt bei der Identifizierung und Verringerung von Risiken in kleinen und mittleren Unternehmens in Deutschland.

5.2 Für KMU in Deutschland wichtige IT-Sicherheitsbarrieren

Aufgrund der genutzten Likert-Skala ist bei allen fünf Hypothesen hinsichtlich der IT-Sicherheitsbarrieren für KMU in Deutschland eine unterschiedliche Tendenz zur Zustimmung gegeben (siehe Abbildung 2 und ergänzend die Tabellen 2 und 4).

Tabelle 4. Deskriptive Statistiken bezogen auf die Boxplots der IT-Sicherheitsbarrieren

Statistik	*IT-Strategie*	*IT-Richtlinie*	*IT-Sicherheits-konzept*	*IT-Rahmenwerk*	*IT-Bewusstsein*
Minimum	1,000	1,000	1,000	2,000	2,000
1. Quartil	5,000	3,000	4,000	5,000	5,000
Median	5,000	4,500	5,000	6,000	6,000
3. Quartil	6,000	6,000	5,000	7,000	7,000
Maximum	7,000	7,000	7,000	7,000	7,000
Mittelwert	5,261	4,087	4,435	5,848	5,826
Varianz	2,064	3,592	2,251	1,465	1,791

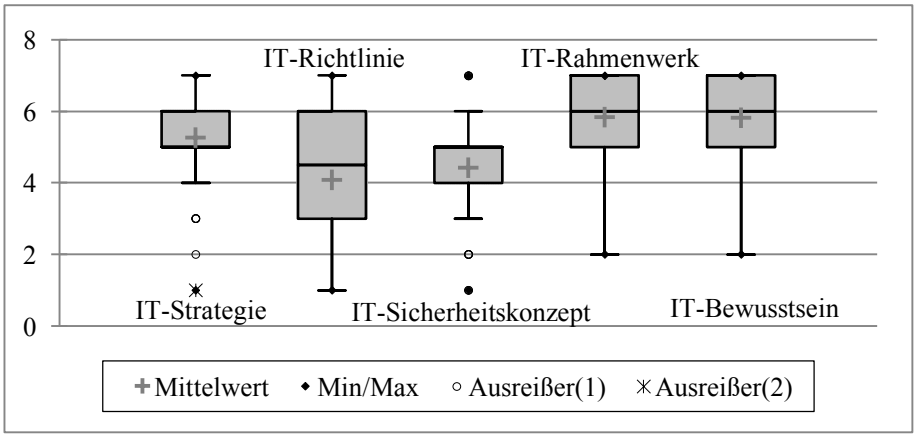


Abbildung 2. Boxplots der IT-Sicherheitsbarrieren

Der Hypothese H5 wird noch zugestimmt, obwohl Ausreißer in den Daten bestehen. Eine unzureichende IT-Strategie kann den Geschäftsbetrieb eines kleinen und mittleren Unternehmens in Deutschland verwundbar machen. *Der Hypothese H6 wird nicht eindeutig zugestimmt*. Die IT-Richtlinie kann von der Geschäftsführung in kleinen und mittleren Unternehmens in Deutschland erstellt werden, jedoch auch von anderen Funktionen und Instanzen. *Der Hypothese H7 wird nicht eindeutig zugestimmt und es bestehen Ausreißer in den Daten*. Ein mangelndes IT-Sicherheitskonzept in kleinen und mittleren Unternehmen in Deutschland kann auf eine unvollständige IT-Richtlinie zurückzuführen sein, jedoch können auch andere wichtige Ursachen vermutet werden. *Der Hypothese H8 wird eindeutig zugestimmt*. Kleine und mittlere Unternehmen in Deutschland benötigen ein (angepasstes oder zu entwickelndes) IT-Rahmenwerk, das ihren speziellen Bedürfnissen entspricht. *Der Hypothese H9 wird eindeutig zugestimmt*. Die fehlende Förderung des IT-Bewusstseins (IT-Awareness) von Mitarbeitenden führt zur fehlerhaften Anwendung der IT-Richtlinien in kleinen und mittleren Unternehmen in Deutschland. Es kann daher angenommen werden, dass in KMU in Deutschland keine gezielte Förderung des IT-Bewusstseins stattfindet und entsprechende IT-Richtlinien falsch angewandt werden.

6 Diskussion der IT-Sicherheit der Digitalisierung in KMU

Aus der empirischen Hypothesenevaluation (siehe Abschnitt 5) kann die Schlussfolgerung gezogen werden, dass KMU in Deutschland der IT-Sicherheit der Digitalisierung eine hohe ökonomische Bedeutung zuordnen und sich nicht vor Veränderungen durch die Digitalisierung hinter Großunternehmen verbergen. Zudem ist den Studienteilnehmenden klar, dass der Stellenwert einer gut implementierten IT-Governance und ein ordnungsgemäßes IT-Risikomanagement wichtige Bestandteile sind, um die eigenen angestrebten Ziele der IT-Sicherheit der Digitalisierung zu erreichen und Vermögenswerte vor digitaler Wirtschaftskriminalität abzusichern.

Die Studienteilnehmenden stimmen zu, dass Schwierigkeiten bestehen, interne Regelungen und gesetzliche Vorgaben ordnungsgemäß umzusetzen. Gründe dafür könnten hinsichtlich der gesetzlichen Vorgaben die kaum abschreckenden gesetzlichen Sanktionierungen in Verbindung mit dem niedrigen Verständnis der Geschäftsführung, große Investitionen im Gebiet der IT-Sicherheit der Digitalisierung durchzuführen, sein. Allgemein besteht ein Schwerpunkt auf den Kosten anstelle einer langfristigen Kostenverringerung aufgrund sicherer und stabiler Geschäftsprozesse, um negative geschäftliche und gesellschaftliche Reaktionen (bspw. durch sensiblen Datenverlust) aufgrund einer ungenügenden IT-Sicherheit im KMU zu verhindern. Folglich sind vom mangelnden Verständnis der Geschäftsführer zudem interne Regelungen involviert, die durch die Geschäftsführung vorgelebt werden sollten, um die Förderung der IT-Sicherheit der Digitalisierung zu bewerkstelligen.

Die Hypothesenevaluation gibt Aufschluss darüber, dass KMU in Deutschland den Standpunkt vertreten, dass ihre IT-Strategie zur Stabilität ihres Geschäftsbetriebs beitragen kann. Insbesondere sollten sich KMU in Deutschland hinsichtlich einer ordnungsgemäßen IT-Strategie mit ihren limitierten Ressourcen den zu sehr einseitigen technologischen Schwerpunkt (bspw. Virenschutz) verringern und zusätzlich verstärkt die organisatorischen Infrastrukturen involvieren. Zudem sollte die organisatorische Planung, Koordination und Kontrolle dazu beitragen, mit intelligenten Entscheidungen (bspw. Schwachstellenanalysen) und gezielten Investitionen (bspw. IT-Schulungen) das nötige Know-how und Vertrauen aufzubauen, um kontinuierlich die IT-Sicherheit der Digitalisierung zu stärken. Hinsichtlich der Erstellung von IT-Richtlinien bestand keine klare Zustimmung, da nur mit geringer Tendenz dahingehend zugestimmt wurde, dass IT-Richtlinien lediglich von der Geschäftsführung erstellt werden. Diese Tendenz kann sowohl positiv als auch negativ interpretiert werden. Auf der einen Seite wurde aufgezeigt, dass nicht alle KMU in Deutschland sich darüber bewusst sind, dass IT-Richtlinien auch durch zusätzliche Instanzen erstellt werden können, wohingegen höchstwahrscheinlich andere Studienteilnehmende es aus der Praxis nicht anders kennen oder nicht die erforderlichen Ressourcen aufbringen können, um IT-Richtlinien mit weiteren Instanzen auszuarbeiten. Daher sollten – ohne Abweichungen – alle KMU in Deutschland die Strategie verfolgen, bei der Ausgestaltung der IT-Richtlinien die betroffenen Abteilungen zu involvieren, da sich IT-Richtlinien z. B. an den Anforderungen der genutzten Applikationen und IT-Systemen sowie den damit verknüpften Geschäftsprozessen orientieren. Nur durch eine effektive Kooperation der einzelnen Fachbereiche auf Basis ihres Wissens, die im Geschäftsalltag sich mit den

Applikationen, IT-Systemen und Geschäftsprozessen auseinandersetzen, können IT-Richtlinien erstellt werden, welche die IT-Sicherheit der Digitalisierung gewährleisten.

Ein vergleichbares Bild entstand beim IT-Sicherheitskonzept, da auch bei dieser Hypothese nur mit geringer Tendenz zugestimmt wurde, dass ein mangelndes IT-Sicherheitskonzept auf eine unvollständige IT-Richtlinie zurückzuführen sei. Hier baut sich ebenso, wie bei den IT-Richtlinien, die Ansicht auf, dass die limitierten Ressourcen einen hohen Einfluss auf dieses nicht eindeutige Ergebnis haben könnten. Insbesondere wird durch das limitiert vorhandene Know-how die Beurteilung von Gefahrenbereichen aufgrund von Schwächen im IT-Betrieb oft unterbewertet und kann daher zu fehlerbehafteten IT-Sicherheitskonzepten und damit verbundenen IT-Sicherheitsmaßnahmen führen. Limitiertes Know-how im eigentlichen Sinne, dass lediglich eine Instanz entscheidungsbefugt ist, wie das IT-Sicherheitskonzept aufgebaut werden soll, ohne die Kooperation mit den betroffenen Fachbereichen zu suchen, die eine bessere Perspektive auf das haben, das diese im Geschäftsalltag bewältigen. Insbesondere die Fachbereiche sind dazu befähigt aus vielfältigen Kontexten betreffs ihres geschäftlichen Handelns auf Gefahren oder Schwächen aufmerksam zu werden, die für außenstehende Instanzen (bspw. Geschäftsführung) vorab nicht offenkundig sind. Speziell das IT-Sicherheitskonzept ist stark mit der IT-Richtlinie verknüpft, da mit IT-Richtlinien Bereiche, Anwendungen, Systeme und Prozesse fixiert werden, die für den Geschäftsbetrieb von großer Bedeutung sind. Folglich kann ein mangelndes IT-Sicherheitskonzept in KMU in Deutschland durchaus auf eine unvollständige IT-Richtlinie zurückzuführen sein.

Hinsichtlich der IT-Rahmenwerke wurde die Hypothese bestätigt, da ein Großteil der KMU in Deutschland das Bedürfnis nach einem für sie angepassten oder entwickelten IT-Rahmenwerk verspürt. Dies ist insbesondere zurückzuführen auf große Schwierigkeiten mit bereits etablierten IT-Rahmenwerken, wie bspw. der ISO 2700x, die mit ihrer extremen Anzahl an Anforderungen in keinem Verhältnis zu der Kapazität eines KMU stehen. Daher haben KMU in Deutschland nicht die nötige Akzeptanz, diese Schwierigkeiten zu meistern, sodass erleichternde Bedingungen erforderlich werden mit für KMU flexibleren, ökonomischeren und einfacheren IT-Rahmenwerken.

Auch bezüglich des IT-Bewusstseins entstand der Eindruck, dass für KMU in Deutschland mit der IT-Strategie, IT-Richtlinie, dem IT-Sicherheitskonzept und IT-Rahmenwerk nur eine erste Grundlage entsteht, wenn das IT-Bewusstsein in KMU nicht ordnungsgemäß gefördert wird. Entsprechendes IT-Bewusstsein umfasst nicht nur eine Förderung der Mitarbeitenden sondern bestenfalls eine Verhaltensanpassung, sodass jeder Mitarbeitende auf unvorhergesehene Situationen richtig reagieren kann. IT-Bewusstsein sollte deutlich weiter oben in der Geschäftsführung ansetzen, hier wird das IT-Bewusstsein für das ganze KMU vorgelebt. Insbesondere sollte die Geschäftsführung ein Verständnis entwickeln für potenzielle Risiken und potenzielle Folgen und darf die limitierten Ressourcen (bspw. IT-Budget und Zeitaufwand) nicht als Vorwand nutzen, die IT-Sicherheit der Digitalisierung zu vernachlässigen.

Referenzen

1. Householder, A., Houle, K., Dougherty, C.: Computer attack trends challenge Internet security. IEEE Computer 35(4), 5–7 (2002)

2. Tawileh, A., Hilton, J., McIntosh, S.: Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. In: Pohlmann, N., Reimer, H., Schneider, W. (Hrsg.) ISSE/SECURE 2007 Securing Electronic Business Processes. S. 331–339. Friedr. Vieweg & Sohn Verlag, GWV Fachverlage GmbH, Wiesbaden (2007)
3. Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 69–104 (2002)
4. Ashish, G., Curits, J., Halper, H.: Quantifying the financial impact of IT security breaches. Information Management & Computer Security 11(2), 74–83 (2003)
5. Groner, R., Brune, P.: Towards an Empirical Examination of IT Security Infrastructures in SME, Secure IT Systems 7617, 73–88 (2012)
6. Barlette, Y., Fomin, V.V.: Exploring the suitability of IS security management standards for SMEs. In: Hawaii International Conference on System Sciences (HICSS), pp. 1-10. Waikoloa, Big Island, Hawaii (2008)
7. Kluge, D., Sambasivam, S.: Formal Information Security Standards in German Medium Enterprises. Proc CONISAR 1, 1–12 (2008)
8. Leyh, C., Bley, K.: Digitalisierung: Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. HMD Praxis der Wirtschaftsinformatik 53, 29–41 (2016)
9. Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr, http://www.smwa.sachsen.de/download/it-sicherheit_sachsen_endbericht.pdf (Aufgerufen: 09.09.2017)
10. Schäfer, G., Strolz, G., Hertweck, D.: IT-Compliance im Mittelstand. HMD Praxis der Wirtschaftsinformatik 45(5), 69–77 (2014)
11. Rees, J.: Information security for small and medium-sized business. Computer Fraud & Security, 18–19 (2010)
12. Bartelt, J., Rieger, B.: IT-Sicherheit im Mittelstand. In: Fahrenschon, G., et al. (Hrsg.) Mittelstand – Motor und Zukunft der deutschen Wirtschaft. S. 557–569. Springer Fachmedien, Wiesbaden (2015)
13. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/it-grundschutz_profil_klein.pdf?__blob=publicationFile (Aufgerufen: 09.09.2017)
14. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/studie_ueberblick-standards.pdf?__blob=publicationFile&v=1 (Aufgerufen: 09.09.2017)
15. Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf;jsessionid=170B98EEDC9C3517E5079802636EE736.1_cid351?__blob=publicationFile&v=2 (Aufgerufen: 09.09.2017)
16. Ayat, M., Masrom, M., Sahibuddin, S., Sharifi, M.: Issues in Implementing IT Governance in Small and Medium Enterprises. In: International Conference on Intelligent Systems, Modelling and Simulation, S. 197–201. (2011)
17. Williams, P.: What Does Security Culture Look Like For Small Organizations? In: Security Research Institute Conferences, pp. 48-54. Edith Cowan University (2009)
18. Goucher, W.: Do SMEs have the right attitude to security?. Computer Fraud & Security, 1–3 (2011)
19. Lederer, B.: Quantitative Erhebungsmethoden. In: Hug, T., Poscheschnik, G. (Hrsg.) Empirisch Forschen. S. 100-132. UVK Verlagsgesellschaft, Konstanz (2010)
20. Institut für Mittelstandsforschung Bonn, http://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (Aufgerufen: 09.09.2017)

Toward a Focus Area Maturity Model for Digitalization - A Set Theoretic Development Approach

Katja Bley[1]

[1] TU Dresden, Business Informatics, esp. IS in Trade and Industry, Dresden, Germany
Katja.bley@tu-dresden.de

Abstract. When it comes to evolving processes or domains, staged or continuous maturity models have long been mighty tools used to reach or determine a certain organizational development level. The process of digitalization is an interesting domain in which to apply these models, since it combines a high degree of complexity with practical relevance. However, our research proposes that a classic fixed-level maturity model is not appropriate for depicting digitalization to its full extent for small and medium sized enterprises (SMEs). Our goal is to develop a Focus Area Maturity Model, which would allow the representation of interdependencies between individual development stages in different areas of the company. We use Qualitative Comparative Analysis, a methodology rooted in the social sciences, to develop this model. The resulting model should enable SMEs to determine their own digital maturity and guide them, if necessary and desired, to achieve a higher digital penetration.

Keywords: Focus Area Maturity Model, Digitalization, QCA, Maturity Model

1 Introduction

Over the last few decades, a plethora of maturity models (MM) has arisen. These models have turned out to be valuable instruments - in theoretical science as well as in applied practice - for defining and evaluating processes or other organizational capabilities that evolve over time. Their appearance and their development have been a widely discussed topic ever since.

Different research purposes and scopes called for different models; nevertheless, in terms of overall structure, five-staged MMs dominate. An advantage of such models is their predefined composition, which helps researchers subdivide an evolving process into stages or continuous levels. Due to many existing approaches and guidelines on how to build a maturity model (see sec. 2.2), it is possible to straightforwardly create a new model. However, this advantage can also be considered detrimental. Researchers and practitioners tend to build and use these models too hastily; respective models are quickly developed based on a specific research domain, which needs to be structured and lacks an evolvement process that can be chronologically sorted. As a result, a multitude of staged maturity models exist, each based on relevant literature for the construction process, however, the model becomes vulnerable to a subjective error of the researcher,

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

as he or she assumes the topic to be mapped completely by using a certain kind of MM. Although these models are mighty tools to assess a relative position with respect to a domain, the trend is to copy and adapt given model structures without considering their overall fit regarding the context.

A strong need exists for defining, categorizing, and evaluating upcoming phenomena, especially when it comes to complex and dynamic research fields such as digitalization or the industrial internet and their impact on enterprises. Thus, a broad variety of new models has been developed in theoretical science as well as applied practice (see sec. 3). However, their validity depends on the definition of the scope each model is applied to. This is the aspect our research focuses on. According to our understanding, it is not possible to reproduce the full extent of digitalization for enterprises - especially for SMEs - by means of a staged or continuous MM, since these models often assume a stringent development process along these stages. Even though this assumption might hold for some of the larger enterprises undergoing well-coordinated digital transformation programs, it is usually inept for SMEs. The primary goals of a holistic digitalization for SMEs remain cost reduction, an increase in operational efficiency, a clearly defined role in its related ecosystem, and a consolidation of market position; consequently, we consider digitalization as a multidimensional phenomenon, which needs to be captured by applying a multi-layered MM. Thus, we aim to develop a Focus Area Maturity Model (FAMM) for SMEs, a model with several functional domains that can be used not only to represent development stages, but also to display dependencies between individual characteristics. In order to meet the requirements of a transparent and rigorous research process, we use a mix of methods to identify relevant factors for digitalization. In addition to a broad literature review and expert interviews, the application of the set theoretic approach Qualitative Comparative Analysis (QCA) will be one of the main instruments to identify the manifold characteristics and complex dependencies which earmark digitalization in enterprises.

The paper is structured as follows. First, we describe different types of MMs, as well as their developments and their points of criticism. Second, we consider digitalization, its definition, and several kinds of MMs which focus on this and related topics. Third, we introduce the research method QCA and focus on the development of a FAMM for our research purpose. The paper concludes with a summary in section five.

2 Maturity Models in Research and Practice

2.1 Purpose and Structure

The main purpose of an MM is the structured, systematic elaboration of best practices and processes that are mostly related to the functioning and structure of an organization. A model is divided into different levels, which are then used as benchmarks for the maturity of a company. Perspectives differ on what the highest level of maturity is. In the *life cycle perspective* on maturity models, the process of growth is divided into several stages, and only by reaching the last level can perfect maturity be attained (staged MM). In the *potential performance perspective*, the maturity of each level is considered

separately, and it is individually decided whether reaching a higher level in the model is desired (continuous MM) [1]. The most well-known MM in both perspectives is the CMMI, which belongs to the area of software development; however, there are other MMs in other domains, such as project management or business process management. The structure of the MM is similar in each case: principal requirements are defined for processes/functions/domains; these requirements are placed on different levels of maturity; and, depending on which requirements are fulfilled, a certain degree of maturity is awarded.

In addition to these classic models, so-called focus area maturity models (FAMMs) feature a more diversified structure of a maturity matrix (Tab. 1). This model type was developed by [2] and initially used in the context of software testing. Later on, [3] enhanced the original model for a broader use in IS, but with a special focus on functional domains.

Table 1. Focus Area Maturity Model [3, 4]

	$MatLev_1$	$MatLev_2$	$MatLev_3$	$MatLev_4$	$MatLev_5$	...	$MatLev_n$
FA_1	A_1		B_1	C_1			
FA_2			A_2	B_2			C_2
FA_3		A_3	B_3		C_3		F_3
...			…				
FA_n	A_n	B_n	…				N_n

FAMMs examine the maturity of an investigated domain using different Focus Areas (FAs). These are in turn subdivided into maturity levels (MatLev). Within the FAs, so-called Capabilities (A_1-N_n) represent conditions that must be fulfilled in order to reach the level of maturity denoted in the respective table column. When considering the columns, it becomes clear that in order to reach $MatLev_3$ (for example), the conditions of FA_1 must reach B_1, the conditions of FA_2 must reach A_2, the conditions of FA_3 must reach B_3, and so on. By applying this subdivision of FAs and MatLevs, it is possible to depict the capabilities' dependencies even across FAs. To measure the characteristics, the relevant capabilities must be assessed. With this model, it is possible to reach a different level for every FA, which results in not one but several MatLevs in the end. It provides a better representation of the minute granularity of digitalization and its effects in SMEs.

2.2 Development and Criticism

As mentioned above, a variety of guidelines exists for the development of MMs, as the topic is widely discussed in science. For instance, [5] described a six-step generic phase model, based on the findings of the Business Process Maturity Model (BPMM) and Knowledge Management Capability Assessment (KMCA). The phases to be followed by the researcher are scope, design, populate, test, deploy, and maintain. A different procedure model is postulated by [6]. They created an eight-phase development approach, focusing on: problem definition, comparison of existing maturity models, determination of the development strategy, iterative maturity model development, conception of transfer

and evaluation, implementation of transfer media, evaluation, and rejection of maturity model. [7] also set up general design principles (principles of form and function) in order to meet the requirements for useful maturity models. They criticize the lack of empirical foundation, which often leads to a simple copy of model structures without considering a conceptual grounding based in literature. [8] further criticize a lack of validation when selecting variables or appropriate dimensions, as well as a missing operationalization of maturity measurements. Moreover, they criticize that a linear course of maturation must be a prerequisite for the creation and application of an MM. The concept of equifinality (which postulates that an outcome can be achieved by more than one path) is barely considered in the area of MM development.

3 Maturity Models with a Focus on Digitalization

When it comes to technical opportunities of digitizing data by using computing technology, the past few decades have been characterized by radical changes. Digital convergence enables information exchange decoupled from devices, networks, and physical interfaces [9]. Companies and organizations are forced to cope with a growing amount of information and data, and need to accept that their original manner of economizing, as it was known for decades, has now changed. Formerly stand-alone IT infrastructure has to be enhanced to a digital infrastructure, a "collection of technological and human components, networks, systems, and processes that contribute to the functioning of an information system [entailing] both social and technical elements" [10 p. 908]. In our understanding, digitalization not only describes a process but also defines a conceptual approach towards a phenomenon that is continuously changing and not meant to be completed. It should be seen as a dynamic socio-technical process that considers both business and technological complexity in a simultaneous, continuous way [11].

Several MMs already focused on this and related topics. For instance, "SIMMI 4.0" is a staged MM that was developed to classify a company-wide application system landscape in the context of Industry 4.0 [12]. The model has four dimensions (vertical, horizontal, digital product development, and cross-sectional technology criteria) and five stages (basic, cross-departmental, horizontal and vertical, full digitalization, and optimized full digitalization). While the authors based their model and its development on the recommendation of [6], documenting the empirical validation well, the aspect of equifinality is still not part of the fixed-level MM. Another MM focusing on the topic of digitalization, the CMMI-based "DREAMY" (digital assessment readiness MM) [13], is subject to the same criticism. It focuses on manufacturing companies and consists of five levels: design and engineering, production management, quality management, maintenance management, and logistics management. However, its development is not described in detail. Thus, any empirical foundation of the model, if it exists, is not made explicit to the reader. A similar MM approach can be found in [14]. Although the authors consider different stages of maturity, the level's characteristics are still detached from each other, therefore it is not obvious to the reader if and when which path dependencies are considered.

When it comes to practitioner contributions, mostly management consultancies approach the field of digitalization by using MMs. Ernst & Young developed an IT-digitalization compass for insurance companies, which consists of four stages [15]. KPMG developed a maturity model that assigns companies to defined clusters and reflects the current digitalization status of their accounting systems [16]. PwC published a report considering an MM to assess the maturation of digital controlling for companies [17]. Summarizing the existing maturity models, we can state that many exist which are similar in their appearance and application; however, none of them follows an equifinalitive approach to digitalization, or focuses on SME in general.

4 Development of a FAMM for Digitalization

4.1 QCA as a Method for Constructing a FAMM

The topic of SMEs' digitalization is characterized by a distinctive equifinality, which means that the outcome of a successfully digitalized enterprise can come from multiple causal conditions [18]. In our research, we try to detect these conditions by applying QCA, a set theoretic approach which bridges quantitative and qualitative research. This socio-scientific research method, which was first introduced by [19], allows the detection of relations without requesting statistical correlations. In terms of a specific outcome, it aims for the detection of necessary and sufficient conditions, as well as asymmetry and causation. We propose that this approach, when applied to the development of a FAMM, is an appropriate attempt to combine the complexity of digitalization with the flexibility of a set theoretic method. Our approach is based on the work by [20], who developed a method for the creation of MMs using set theory.

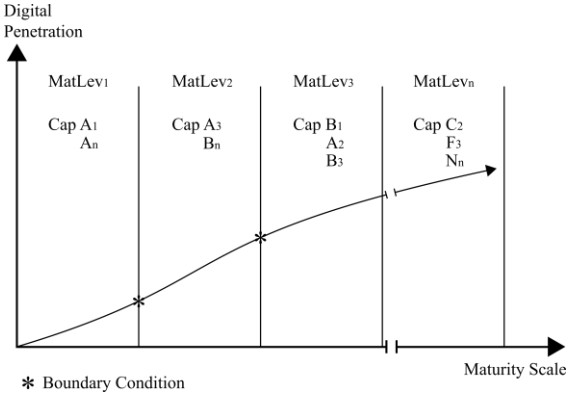


Figure 1. Exemplary illustration of a maturity model development using QCA [19]

The first step in conducting a QCA is the determination of conditions, called "critical success factors" (CSFs). These factors will represent capabilities of FAs in our FAMM later on. Each capability (or factor) represents a specific maturation level considering a FA - or rather, a maturity level consists of different capabilities (see Tab. 1). Initially, however, it is not clear which capabilities will represent the maturity level and in which

order they should appear. The combination of different predefined capabilities in sets, and their evaluation, will answer the question of whether these capabilities are necessary or sufficient conditions for achieving a specific outcome (for example, the first maturity level in the model). By using boundary conditions, we can set specific requirements that a company must meet in order to proceed to a higher level of maturity. A Necessary Condition Analysis will be applied in order to empirically define the influence of boundary and necessary conditions on the outcome [21, 22]. Fig. 1 illustrates an example of a graphical implementation of the development of maturity levels using QCA, with reference to Tab. 1. Although there is a single given maturity path, it does not mean maturity will appear in a predefined or linear way. By applying QCA, we already consider many different characteristics of digitalization, which are merely compiled by the method. Nevertheless, we do not yet know what the stages of the model or the maturity paths will look like.

4.2 Approach to the Development of a Digitalization FAMM

One of our main assumptions considering digitalization in SMEs is the complexity of ways to achieve it. We propose that, when focusing on a company's ability to reach a digitalization level, we can depict digitalization - almost to its full extent - by combining several conditions and relation sets. In order to transform the aforementioned method of MM development into a method that supports FAMM development, we will begin by reviewing relevant MM and FAMM literature. One possible approach could be extending and adapting the work of [4], who have already dealt with the subject matter. Afterwards, the driving factors (capabilities) of digitalization as well as appropriate focus areas in SMEs must be identified. We will do this in a two-stage procedure. First, we will conduct a comprehensive literature review, using key words of the digitalization phenomenon in combination with SME. After identifying possible driving factors and capabilities, we will review and (if necessary) expand these factors by conducting expert interviews. After completing our list of capabilities, we will apply QCA on our factor sets. We will determine which of the factors are necessary or sufficient for the digitalization of SME, then combine them in set configurations to detect their impact on specific outcomes. After we are able to reveal the combination and order of factors which lead to the desired outcomes, we will create a FAMM with the necessary and sufficient conditions for SMEs in order to determine their level of digital penetration.

5 Conclusion

In this research proposal, we attempt to demonstrate that a novel maturity model approach is needed to depict the multifaceted phenomenon of digitalization in SMEs. We intend to develop a Focus Area Maturity Model by using the socio-scientific method of QCA, which has never been done before in this research area despite its promising potential. Our aim is to detect more than one possible way of becoming a digitalized company other than following one linear maturity path, which is postulated in many existing staged maturity models.

References

1. Wendler, R.: The Maturity of Maturity Model Research: A Systematic Mapping Study. Inf. Softw. Technol. 54, 1317–1339 (2012).
2. Koomen, T., Pol, M.: Test Process Improvement: A Practical Step-By-Step Guide to Structured Testing. Addison-Wesley, Amsterdam (1999).
3. Van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I., Bekkers, W.: The Design of Focus Area Maturity Models. In: Global Perspectives on Design Science Research. pp. 317–332. Springer, Berlin (2010).
4. Sanchez-Puchol, F., Pastor-Collado, J.A.: Focus Area Maturity Models: A Comparative Review. In: Inf. Sys. pp. 531–544. Springer, Cham (2017).
5. De Bruin, T., Freeze, R., Kaulkarni, U., Rosemann, M.: Understanding the Main Phases of Developing a Maturity Assessment Model. ACIS 2005 Proc. (2005).
6. Becker, J., Knackstedt, R., Pöppelbuß, J.: Developing Maturity Models for IT Management. Bus. Inf. Syst. Eng. 1, 213–222 (2009).
7. Pöppelbuß, J., Röglinger, M.: What Makes a Useful Maturity Model? A Framework of General Design Principles for Maturity Models and Its Demonstration in Business Process Management. ECIS 2011 Proc. 28 (2011).
8. Lasrado, L.A., Vatrapu, R., Andersen, K.N.: Maturity Models Development in IS Research: A Literature Review. Proc. 38th Inf. Syst. Res. Semin. Scand. IRIS 38. 6, (2015).
9. Tilson, D., Lyytinen, K., Sørensen, C.: Digital infrastructures: The missing IS research agenda. Inf. Syst. Res. 21, 748–759 (2010).
10. Henfridsson, O., Bygstad, B.: The Generative Mechanism of Digital Infrastructure Evolution. MIS Q. 37, 907–931 (2013).
11. Blaschke, M., Winter, R., Aier, S.: Digital Infrastructure : A Service-dominant Logic Perspective. Proc. 37th Int. Conf. Inf. Sys. ICIS. (2016).
12. Leyh, C., Schäffer, T., Forstenhäusler, S.: SIMMI 4.0 – Vorschlag eines Reifegradmodells zur Klassifikation der unternehmensweiten Anwendungssystemlandschaft mit Fokus Industrie 4.0. Proc. Multikonf. Wirtschaftsinformatik (MKWI). pp. 1651–1662 (2016).
13. De Carolis, A., Macchi, M., Negri, E., Terzi, S.: A Maturity Model for Assessing the Digital Readiness of Manufacturing Companies. In: Lödding, H., Riedel, R., Thoben, K.-D., von Cieminski, G., and Kiritsis, D. (eds.) Advances in Production Management Systems. pp. 13–20. Springer International Publishing, Cham (2017).
14. Ganzarain, J., Errasti, N.: Three Stage Maturity Model in SME's Toward Industry 4.0. J. Ind. Eng. Manag. 9, 1119 (2016).
15. EY Innovalue, https://go.ey.com/2eOK6qw.
16. Kreher, M., Gundel, U.: Digitalisierung im Rechnungswesen, http://bit.ly/2wSPKTo.
17. Digital Controlling - Digitale Transformation im Controlling, https://pwc.to/2xuqqTn.
18. Rihoux, B., Ragin, C.C.: Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques. Sage (2009).
19. Ragin, C.: The comparative method: Moving Beyond Qualitative and Quantitative Methods. Berkeley Univ. Calif. (1987).
20. Lasrado, L.A., Andersen, K.N.: A Set Theoretical Approach to Maturity Models : Guidelines and Demonstration. Proc. 37th Int. Conf. Inf. Sys. ICIS (2016).
21. Lasrado, L., Vatrapu, R., Normann, K.: A Methodological Demonstration of Set-Theoretical Approach to Social Media Maturity Models Using Necessary Condition Analysis. In: PACIS 2016 Proc. (2016).
22. Dul, J.: Necessary Condition Analysis (NCA): Logic and Methodology of "Necessary but Not Sufficient" Causality. Organ. Res. Methods. 19, 10–52 (2016).

Approaching Digitalization with Business Process Management

Florian Imgrund[1], Marcus Fischer[1], Christian Janiesch[1], and Axel Winkelmann[1]

[1] University of Würzburg, Institute of Business Administration, Würzburg, Germany
{florian.imgrund,marcus.fischer,christian.janiesch,
axel.winkelmann}@uni-wuerzburg.de

Abstract. As digitalization sustainably alters industries and societies, small and medium-sized enterprises (SME) must initiate a digital transformation to remain competitive and to address the increasing complexity of customer needs. Although many enterprises encounter challenges in practice, research does not yet provide practicable recommendations to increase the feasibility of digitalization. Furthermore, SME frequently fail to fully realize the implications of digitalization for their organizational structures, strategies, and operations, and have difficulties to identify a suitable starting point for corresponding initiatives. In order to address these challenges, this paper uses the concept of Business Process Management (BPM) to define a set of capabilities for a management framework, which builds upon the paradigm of process orientation to cope with the various requirements of digital transformation. Our findings suggest that enterprises can use a functioning BPM as a starting point for digitalization, while establishing necessary digital capabilities subsequently.

Keywords: Business Process Management, Digital Transformation, Digitalization, Maturity Frameworks, PEMMDO

1 Introduction

As technological advancements have made the Internet ubiquitously available, customers have developed preferences for consistent information across multiple communication channels, innovative product-service combinations, and direct interactions with enterprises [1]. To address these needs, enterprises rely on holistic strategies that facilitate the streamlining of processes, the digitization of products and services, and the innovation of business and revenue models [2]. However, numerous studies suggest that especially small and medium-sized enterprises (SME) have not yet initiated digital transformation [3, 4] and, thus, have not yet embarked on the process of digitizing their business. As many SME operate in global markets shaped by competition, this can yield significant risks for their long-term business success.

While literature does not provide a generally accepted definition of digitalization, it is often referred to as a technology-induced transformation process that improves an enterprise's flexibility, agility, and responsiveness by simultaneously aligning its operations, strategy, business processes, and organizational and IT structures to

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

technological advancements [5, 6]. Digitalization widens the scope of traditional digitization, which has mainly focused on the transformation of analogous information into a digital representation [7]. Digitization has led to the development of various approaches for business-IT alignment, including concepts for technology adoption, procedures for software selection, or data and information integration using information systems [8, 9]. However, to cope with digitalization, enterprises rely on new perspectives that enable a holistic harmonization of all their strategies, processes, operations, and IT systems [10]. Despite a growing interest and frequently encountered challenges in practice, research still lacks practicable recommendations on the formulation, implementation, and evaluation of corresponding strategies [11, 12]. To address these shortcomings, we follow Legner et al. [7], who demand transdisciplinary research to develop feasible digitalization approaches. Hence, we operationalize Business Process Management (BPM), as both concepts share similar goals and characteristics. Due to the wide adoption and maturity of BPM methods, techniques, and systems, we argue that a functioning BPM constitutes an optimal starting point for embarking on the journey of digitalization and to design a holistic maturity model as a management framework for SME. We summarize our research questions as follows:

(1) What are the requirements of digitalization endeavors?
(2) How does BPM address the requirements and challenges of digitalization in SME?
(3) What capabilities are necessary for SME to cope with the requirements of digitalization and how can we use BPM to increase the feasibility of digitalization in SME?

This paper is organized as follows: In Section 2, we describe the applied research design to develop the artefact of this contribution. Section 3 introduces necessary foundations on BPM and digitalization. We present the results of a literature review on the challenges and requirements of digitalization in Section 4 and analyze how BPM maturity models support SME in addressing them. In Section 5, we use resulting implications to derive a set of necessary capabilities, which we integrate into a holistic management framework. This paper concludes with a summary of findings, limitations, and future research potentials.

2 Research Design

We apply a design-oriented research approach to develop our contribution. Following the knowledge contribution framework proposed by Gregor and Hevner [13], we consider our Design Science Research (DSR) contribution an exaptation of BPM to the design and implementation of strategies for the digitalization of SME. It has explanatory power and provides design practice theory for the formulation of digital strategies for SME. Hence, we use the guidelines provided by Peffers et al. [14] to answer our research questions. We summarize our research approach in Figure 1. Despite the importance of digital transformation for the future competitiveness of SME, literature does not yet provide practicable recommendations on the design and implementation of corresponding strategies.

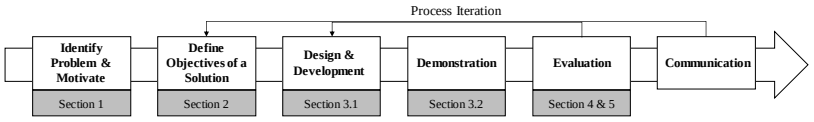


Figure 1: Research Methodology

Thus, we aim to develop a management framework that supports SME in coping with the requirements of digitalization by operationalizing existing organizational structures and systems. By defining design as a search process, we conduct a systematic literature review [15] to collect a representative set of requirements for successful digitalization. Subsequently, we analyze the capabilities of BPM to support and guide the underlying transformation process. We use the resulting implications for the design of our artefact, adapt the well-established Process and Enterprise Maturity Model (PEMM) [16] and extend it with an additional dimension for digitalization. We evaluate its applicability by controlling for its suitability to address the requirements of digitalization.

3 Business Process Management and Digitalization

3.1 Business Process Management

BPM constitutes a body of methods, techniques, and systems to identify, prioritize, analyze, improve, and monitor the business processes of an organization [17, 18]. It builds upon the paradigm of process orientation, which replaces the traditional functional perspective on organizational structures in order to address increasing market dynamics, a growing competitive pressure, and technological advancements [17, 18]. Potential benefits of BPM range from increases in flexibility, agility, and responsiveness to improvements in innovativeness and customer centricity [17-19].

Despite the manifold benefits, introducing BPM can be challenging, as it simultaneously affects multiple organizational levels and demands time, financial, and human resources [19]. For a successful BPM, enterprises must account for a variety of success factors that range from process standardization and automation, to stakeholder integration, and adequate employee training [17]. To support enterprises in managing BPM initiatives, several maturity models have been introduced to the literature. A comprehensive overview of these frameworks can be found in [20]. Due to the focus on SME, this paper builds upon Hammer [16], who introduce the PEMM framework to support all enterprises in planning and executing process-based transformations. As it does not require specific organizational characteristics, it is especially suitable for SME, which naturally differ by firm size, legal form, and organizational maturity [16].

PEMM builds upon the two dimensions of *process enablers* and *enterprise maturity*. The former dimension focuses on individual processes and determines requirements for a high process performance, including the five characteristics *design*, *performers*, *owner*, *infrastructure*, and *metrics* [16]. Each characteristic is further specified by a variety of sub-constructs to provide more detailed action recommendations. To account for the interdependencies between the characteristics, the model distinguishes four

process maturity levels, ranging from *P1*, indicating a minimum degree of process orientation, to P4, enabling the delivery of the best possible results to all stakeholders [16]. In order to reach higher maturity levels, enterprises must successfully address the requirements of all previous levels. In addition, the dimension of enterprise maturity defines *organizational capabilities* that are necessary to develop high-performance processes, including the areas of *leadership*, *culture*, *expertise*, and *governance* [16]. Similar to process enablers, the model defines sub-constructs for each area to specify corresponding requirements and determines four maturity levels. Both maturity dimensions are mutually dependent in a way that enterprises must exhibit necessary organizational capabilities to deliver a certain level of process performance [16].

3.2 Digitalization and its relationship to BPM

By transforming information into a digital representation, digitization yielded significant improvements in enterprises' information processing capabilities [7, 11]. To fully harness those benefits, organizations relied on the use of IT and the implementation of IT strategies, for example by increasing the agility and consistency of business processes through the use of information systems [21].

Simultaneously, digitization initiated an extensive digital transformation process that is changing industries and societies of today [7, 22]. This transformation is fueled by the convergence of social, mobile, cloud, and smart technologies and the growing need for big data applications, automation, and integration [23, 24]. The Internet further provides means to share user experiences, opinions, and preferences immediately and established new opportunities for customers and enterprises to interact [22].

To address the challenges imposed by digitalization, it is essential for enterprises to initiate a holistic socio-technical transformation process [7]. According to Singh and Hess [25], this requires the implementation of a comprehensive digital strategy, which accounts for the opportunities and risks from digital technologies and fosters the creation of values and revenues based on digital assets. It further entails establishing adequate capabilities in the areas of digital leadership and empowerment, data-driven agility, consumer and partner engagement, digital platform management, business model innovation, IT architecture transformation, process digitization and automation, digital security, and compliance [7]. This facilitates improvements in business performances by continuously integrating technological advancements in the areas of social media, mobile access, or embedded systems into an enterprise's operations [25].

Although they describe different research domains, we argue that BPM and digitalization inherently share fundamental assumptions and characteristics. BPM provides methods and techniques to improve an enterprise's business performance, by optimizing efficiency and productivity, while reducing costs and fostering collaboration [18]. Both concepts further require enterprises to account for cross-functional interdependencies and, thus, draw upon the concept of process-orientation. By facilitating automation and integration, technology supports BPM by providing capabilities for information management, information processing, and communication [26]. Introducing IT to an organization can also trigger BPM initiatives, as enterprises must align their organizational structure to the system's characteristics to fully harness

the expected benefits. While technology is a key enabler for BPM, it is central to digitalization, as it drives the underlying transformation process.

4 Demystifying the Requirements of Digitalization

4.1 Sampling and Meta-Analysis

First, we conduct a literature review to derive a representative set of requirements. To determine the scope of our literature review, we draw upon the classification of Cooper [27], who distinguishes the dimensions *focus*, *goal*, *organization*, *perspective*, *audience*, and *coverage*. We focus on research outcomes and applications. Furthermore, we aim to integrate the findings from literature to obtain a comprehensive understanding of the requirements of digitalization in organizations. We structure our results based on conceptual clusters, take on a neutral perspective during the reviewing process, and direct our research to general scholars and practitioners. However, we do not claim our results to be exhaustive, but rather to be a representative collection of relevant contributions on the requirements of digitalization.

We initially defined search terms and literature databases to initiate the literature search process. To ensure a high-qualitative sample, we queried the databases *AISeL*, *EBSCO Business Source Complete*, and *EBSCO Academic Search Complete*, and exclusively considered peer-reviewed journals contained by the Senior Scholar's Basket of Journals, the AIS Toplist, or outlets with a VHB JOURQUAL Ranking of *A* or *B*. We also considered additional databases but did not get adequate results. As the requirements of digitalization continuously change, we limited our search to papers published between 2007 and 2017. To identify relevant publications, we created a list of keywords based on the terms *digitalization*, *digitization*, and *digital transformation*. We specified our query strings by adding the expressions *strategy*, *approach*, *requirements*, as well as other associated concepts. Based on these search terms, we performed the literature search process in multiple phases [27]. Figure 2 summarizes the search strategy and corresponding results.

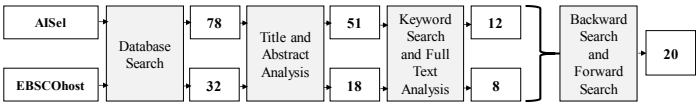


Figure 2: The Literature Search Process

First, we analyzed titles and abstracts of the identified contributions and eliminated papers that did not fit the thematic or organizational scope of our review. Second, we performed a keyword search and a full-text analysis to ensure the relevancy of our final sample. Finally, we performed forward and backward searches to widen the scope of our review, resulting in 20 publications that conformed to the predefined requirements. By analyzing the contributions' years of publications, the resulting distribution suggests that the focus on digital transformation has been continuously growing during the last decade. Eight papers were published only in 2017, with the same number of articles

introduced between 2011 and 2013. We consider our literature collection as high-qualitative, as 19 contributions were published in outlets ranked *B* or higher. With twelve papers from the journal MIS Quarterly Executive, more than half of the publications follow practice-oriented research approaches.

4.2 Literature Analysis and Synthesis

Our literature analysis comprises two phases. First, we examined all identified contributions to collect a comprehensive set of requirements for digitalization. Afterwards, a group of domain experts analyzed each item in order to reduce the initial collection to a smaller number of summarizing concepts. We repeated this process in multiple iterations until all participants agreed on a final sample of requirements. Second, we followed Webster and Watson [28], who suggest constructing a concept matrix to structure the body of knowledge. Based on this procedure, our initial sample contained 225 requirements, which we reduced to eight summarizing concepts within six iterations. Table 2 presents the resulting concept matrix.

Table 2: Requirements of Digital Transformation

Reference	*Req. 1:* Expertise	*Req. 2:* Org. Flexibility	*Req. 3:* Involve-ment	*Req. 4:* Digital Strategy	*Req. 5:* IT Strategy	*Req. 6*: Security	*Req. 7:* Collabo-ration	*Req. 8:* Culture
[1]		x		x	x		x	
[29]		x		x	x			x
[24]	x	x	x	x	x		x	x
[30]					x			
[31]	x	x		x	x	x	x	x
[32]					x			
[12]				x				
[33]	x		x	x	x		x	x
[34]		x	x	x	x		x	x
[2]	x	x		x	x			x
[6]	x	x		x	x		x	x
[35]				x				
[36]	x	x	x	x	x		x	x
[7]	x	x	x	x	x	x		
[37]			x	x	x			x
[11]				x	x			x
[10]				x				
[23]	x	x	x	x	x		x	
[25]			x	x			x	x
[38]	x	x	x	x	x		x	x

The identified requirements range from cultural and organizational to strategical and technological aspects. Various authors highlight the need for IT and data-related skills and capabilities (*Expertise*) [2, 7, 25, 36, 37]. As tasks become more complex, enterprises can benefit from employee specialization but rely on knowledge management mechanisms to ensure consistent outcomes and to facilitate co-creation and collaboration [23, 24, 31, 34, 36, 38].

Continuously changing market conditions require an adequate degree of *organizational flexibility*, which includes organizational agility, scalability, and adaptability [1, 6, 7, 11, 23, 37, 38]. Hence, enterprises must take on a cross-functional perspective, capture benefits from standardization, and enable organizational

responsiveness through coordination and communication [23, 24, 29, 31, 37, 38]. [2, 6, 11] emphasize that the success of digital transformation strongly depends on the provision of sufficient funding, as unforeseen developments can challenge the initiatives.

To enable a comprehensive transformation, enterprises must formulate and implement an adequate *digital strategy* that includes goals, as well as an action and communication plan [2, 6, 31, 34]. This entails adaptations to an enterprise's business model, product service portfolio, and the alignment of recruiting strategies to the needs of digitalization [1, 2, 6, 7, 11, 24, 35, 38]. According to [6, 36, 37], digital transformation further requires enterprises to refocus their core competencies and to rationalize non-performing activities. By implementing adequate monitoring systems, enterprises can continuously align their digital strategy to market dynamics [2, 6, 24, 31, 36]. Ultimately, enterprises should foster innovation opportunities, for example by introducing innovation incubators [24, 31] or concepts of open innovation [6, 31, 38].

Due to ubiquitous communication channels, digital transformation demands for a stronger *involvement* of internal and external stakeholders [7, 23-25, 33, 34, 36-38]. On the one hand, customers seek to participate in the design and development of new products and services. On the other hand, enterprises benefit from the integration of data and processes within their supplier network [6, 23, 24, 31, 38]. As digitalization requires new skills and capabilities and alters organizational procedures, enterprises must further avoid imbalances between different parts of the organization [24, 36].

As they drive digitalization, organizations must continuously align their business operations to new technologies by implementing a consistent *IT strategy* [6, 7, 32, 36, 37]. This entails facilitating digitization and automation, as well as implementing an IT architecture to enable data integration, process orchestration, and the deployment of adequate data analysis capabilities [1, 7, 23-25]. [29, 33, 36] further recommend the implementation of holistic benchmarking methods that build upon data from internal and external sources and allow for real-time adaptation and forecasting opportunities.

To fully harness potential benefits from *collaboration*, production models provide means to coordinate co-creation in decentralized activities [1, 23, 31, 38, 39]. By modularizing processes and activities to standardized building blocks, enterprises can further increase operational flexibility and foster efficiency and innovativeness [6, 36].

As digitalization constitutes a holistic change process, it requires enterprises to adapt their *organizational culture*. Thus, it is necessary to create an open-minded environment that facilitates creativity and risk-taking [6, 34, 37]. Further, organizations should offer training and education opportunities and adapt management structures by introducing new organizational roles and/ or responsibilities [2, 6, 24, 31, 34, 36].

Ultimately, as digitalization poses risks for IT and data *security*, enterprises must adapt compliance rules and account for IT security threats by formulating behavioral guidelines, risk management systems, and a comprehensive defense strategy [7, 31].

4.3 How BPM Addresses the Challenges of Digital Transformation

While digitalization result in organizational change processes, we argue that enterprises can increase their feasibility by establishing an adequate enterprise and process

maturity. Enterprises can address various requirements of digitalization with a process-based transformation, which we summarize in Table 3.

Table 3: Capabilities of BPM to Address the Requirements of Digitalization

Requirement	Facilitation through BPM	Reference
Expertise	• cross-functional knowledge spill-overs facilitate collaboration and co-creation • process models enable knowledge management and information exchange	[17]
Flexibility	• improved coordination and communication increase agility and flexibility	[40]
Involvement	• process-orientation connects all part of an organization	[17]
Digital Strategy	• process models facilitate focusing on core-competencies and foster innovation • supports the awareness and acceptance towards change	[41]
IT Strategy	• uses IT for process automation, digitization, and data integration • aligns technological and business structures	[17]
Collaboration	• uses production models to facilitate collaboration • facilitates modularization through process building blocks	[39]
Security	• entails the formulation of rules and guidelines	[18]
Culture	• creates a cross-functional culture and defines roles and	[17]

A functioning BPM addresses various requirements of digitalization. It can thereby increase the feasibility of the underlying transformation process. This entails that organizations can benefit from the mechanisms and structures established by BPM and use them as a starting point to initiate their digitalization journey.

5 PEMMDO – A Maturity Model for Digital Transformation

While BPM can serve as an enabler for digital transformation, it cannot fully address all requirements. Hence, organizations must establish additional capabilities to cope with digitalization successfully. To transform our findings into practicable recommendations for SME, we build upon the PEMM framework, which is universally applicable and, thus, accounts for the heterogeneity of SME. Although PEMM does not explicitly address the requirements of digital transformation, we have shown that process orientation and BPM constitute facilitating conditions (cf. Section 4.3).

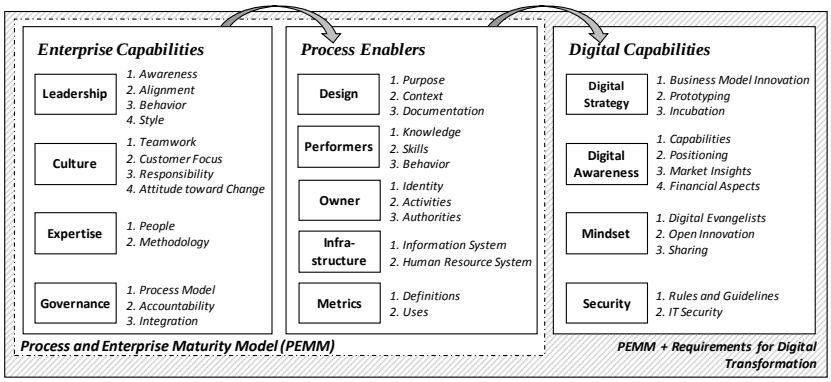


Figure 3: PEMMDO, PEMM enhanced by Requirements for Digital Transformation

However, to fully cope with the requirements of digital transformation, enterprises must further implement a *digital strategy*, increase *digital awareness*, adjust their *mindset*, and define *security standards*. We incorporate these *digital capabilities* and account for the facilitating effect of BPM by extending the PEMM framework with four digital capabilities. We illustrate the resulting *Process and Enterprise Maturity Model for Digitalized Organizations* (*PEMMDO*) in Figure 3. The framework intends to serve as an orientation for companies seeking to embark on the journey of digital transformation. As described by Hammer [16], the model's dimensions are mutually dependent, in a way that adequate enterprise capabilities foster operational excellence, which in turn facilitates digitalization.

Necessary capabilities to approach digitalization include:

- **Digital Strategy:** Enterprises must formulate a digital agenda that fosters innovation, aims for quick results, draws upon knowledge and resources from all available information sources, and facilitates customer-oriented products and services. Thus, enterprises must continuously challenge and innovate their business and revenue models. Furthermore, prototyping facilitates the adaptation of product and service specifications to dynamically changing consumer preferences, while reducing development times. Ultimately, incubation hubs can introduce new perspectives on digitalization, foster creativity, and lateral thinking, and augment existing structures with agile and flexible components.
- **Digital Awareness:** To cope with digitalization, it is essential for enterprises to monitor their distinct capabilities and business performance continuously. By implementing comprehensive benchmarking mechanisms, enterprises can evaluate and adjust their market positioning and use the resulting implications to adapt their business goals and strategy to customer preferences and market requirements. Ultimately, digital transformation requires enterprises to provide adequate financial resources that compensate for short-term setbacks and to support business models and strategies in competitive market environments.
- **Mindset**: Besides adaptations to organizational structures and strategies, digitalization requires an open-minded culture that fosters creativity and innovation. To facilitate the awareness towards and the adoption of digitalization respectively, enterprises rely on digital evangelists, which are typically well-connected and part of large social networks. Organizational culture must further promote risk-taking but also facilitate realistic expectations in a way that enterprises focus their available resources on the most feasible and beneficial projects and initiatives. In fact, not all projects yield cost reductions or performance improvement, but can also create new potentials for research and development. By providing comprehensive training and education opportunities, enterprises can equip employees with necessary skills and capabilities. These should address the concept of open innovation, the use of collaborative production models, and the benefits of knowledge sharing.
- **Security:** As digitalization seeks to digitize an enterprise's assets and operations, new threats for IT and data security arise, which can hamper the adoption of digital strategies and negatively influence business success. Enterprises must address those

risks in early stages of the digitalization process. Hence, they must define *rules and guidelines* that extend traditional compliance to account for digital risks. Furthermore, *risk management* can support enterprises in identifying critical organizational infrastructures as well as the most common threats. They must use the resulting implications to implement a comprehensive defence strategy.

6 Conclusion

To address the challenges of SME when approaching digitalization, this paper sought to introduce a management framework by drawing upon established concepts of BPM. Based on the similarity of both concepts, we formulated three research questions, which we answered by applying a DSR approach. First, we conducted a literature review to identify relevant contributions on digitalization and corresponding strategies. Analyzing the body of literature, we collected 225 requirements associated with digitalization and reduced them to nine summarizing concepts. Subsequently, we analyzed the capability of BPM to address these requirements and demonstrated how it provides an optimal starting point for digital transformation in SME. As traditional BPM does not account for all requirements of digitalization, we derived a set of key capabilities, which we conceptualized by introducing the PEMMDO framework. Hence, we consider adequate enterprise and process capabilities as necessary preconditions for digitalization. The resulting framework supports enterprises in formulating and implementing a strategy for digitalization.

Approaches of this kind have a variety of well-known limitations. First, we only considered high-qualitative contributions for our literature review and aimed to identify a representative, rather than exhaustive, sample. Hence, requirements and implications from neglected publications were not included in our analysis. Second, our findings exclusively build upon implication from theoretical contributions. Hence, digital transformation remains an emerging topic and requires further research to provide more definitive evidence for the applicability of our framework to support implementation projects in practice.

References

1. Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., Venkatraman, N.V.: Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly 37, 471-482 (2013)
2. Hess, T., Matt, C., Benlian, A., Wiesböck, F.: Options for Formulating a Digital Transformation Strategy. MIS Quarterly Executive 15, 123-139 (2016)
3. Saam, M., Viete, S., Schiel, S.: Digitalisierung im Mittelstand: Status Quo, aktuelle Entwicklungen und Herausforderungen. (2016)
4. Leyh, C., Bley, K.: Digitalisierung: Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. HMD Praxis der Wirtschaftsinformatik 53, 29-41 (2016)
5. Chew, E.: Value Co- Creation in the Organizations of the Future. 9th European Conference on Management Leadership and Governance pp. 1-16, London (2013)

6. Holotiuk, F., Beimborn, D.: Critical Success Factors of Digital Business Strategy. 13. International Conference on Wirtschaftsinformatik pp. 991-1005, St. Gallen (2017)
7. Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., Ahlemann, F.: Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. Business & Information Systems Engineering 59, 301-308 (2017)
8. Fischer, M., Heim, D., Hösselbarth, M., Winkelmann, A.: Assessing Organization-System Fit in ERP Selection Procedures – A Literature Review. In: Kurosu, M. (ed.) 19th International Conference on Human-Computer Interaction, pp. 134-149, Vancouver (2017)
9. Gronau, N.: Enterprise Resource Planning und Supply Chain Management: Architektur und Funktionen. Oldenbourg Verlag, München (2004)
10. Mithas, S., Tafti, A., Mitchell, W.: How a Firm's Competitive Environment and Digital Strategic Posture Influence Digital Business Strategy. MIS Quarterly 37, 511-536 (2013)
11. Matt, C., Hess, T., Benlian, A.: Digital Transformation Strategies. Business & Information Systems Engineering 57, 339-343 (2015)
12. Grover, V.: The Information Systems Field: Making a Case for Maturity and Contribution. Journal of the Association for Information Systems 13, 254-272 (2012)
13. Gregor, S., Hevner, A.R.: Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly 37, 337-355 (2013)
14. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems 24, 45-77 (2007)
15. vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. Communications of the Association for Information Systems 37, 205-224 (2015)
16. Hammer, M.: The Process Audit. Harvard Business Rev. 85, 111-119, 122-113, 142 (2007)
17. Dumas, M., Rosa, M.L., Mendling, J., Reijers, H.A.: Fundamentals of Business Process Management. Springer, Berlin (2013)
18. Weske, M.: Business Process Management: Concepts, Languages, Architectures. Springer, Berlin (2012)
19. Becker, J., Kugeler, M., Rosemann, M.: Process Management: A Guide for the Design of Business Processes. Springer, Berlin (2013)
20. Röglinger, M., Pöppelbuß, J., Becker, J.: Maturity Models in Business Process Management. Business Process Management Journal 18, 328-346 (2012)
21. Goodhue, D.L., Wybo, M.D., Kirsch, L.J.: The Impact of Data Integration on the Costs and Benefits of Information Systems. MIS Quarterly 16, 293-311 (1992)
22. Janiesch, C., Imgrund, F., Fischer, M., Winkelmann, A.: Connected Customer sucht Connected Enterprise: Eine Standortbestimmung. In: Keuper, F., Schomann, M., Sikora, L.I. (eds.) Homo Connectus: Einblicke in die Post-Solo-Ära, Wiesbaden (2018)
23. Sebastian, I.M., Ross, J.W., Beath, C., Mocker, M., Moloney, K.G., Fonstad, N.O.: How Big Old Companies Navigate Digital Transformation. MIS Quarterly Executive 16, 197-213 (2017)
24. Dremel, C., Wulf, J., Herterich, M.M., Waizmann, J.-C., Brenner, W.: How AUDI AG Established Big Data Analytics in Its Digital Transformation. MIS Quarterly Executive 16, 81-100 (2017)
25. Singh, A., Hess, T.: How Chief Digital Officers Promote the Digital Transformation of their Companies. MIS Quarterly Executive 16, 1-17 (2017)

26. Sidorova, A., Torres, R., Al Beayeyz, A.: The Role of Information Technology in Business Process Management. In: vom Brocke, J., Rosemann, M. (eds.) Handbook on Business Process Management 1: Introduction, Methods, and Information Systems, pp. 421-444. Springer, Berlin (2015)
27. Cooper, H.M.: Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. Knowledge in Society 1, 104-126 (1988)
28. Webster, J., Watson, R.T.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26, xiii-xxiii (2002)
29. Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., Venkatraman, N.V.: Visions and Voices on Emerging Challenges in Digital Business Strategy. MIS Quarterly 37, 633-661 (2013)
30. Drnevich, P.L., Croson, D.C.: Information Technology and Nusiness-level Dtrategy: Toward an Integrated Theoretical Perspective. MIS Quarterly 37, 483-510 (2013)
31. Dürr, S., Wagner, H.-T., Weitzel, T., Beimborn, D.: Navigating Digital Innovation: The Complementary Effect of Organizational and Knowledge Recombination. 13th International Conference on Wirtschaftsinformatik, pp. 1363-1377, St. Gallen (2017)
32. Ehmke, J.F.: Interview with Hanno Schülldorf on "Computational Challenges in Planning of Mobility and Transportation Services". Business & Information Systems Engineering 59, 181-182 (2017)
33. Hansen, A.M., Kraemmergaard, P., Mathiassen, L.: Rapid Adaptation in Digital Transformation: A Participatory Process for Engaging IS and Business Leaders. MIS Quarterly Executive 10, 175-185 (2011)
34. Hansen, R., Sia, S.K.: Hummel's Digital Transformation Toward Omnichannel Retailing: Key Lessons Learned. MIS Quarterly Executive 14, 51-66 (2015)
35. Karimi, J., Walter, Z.: The Role of Dynamic Capabilities in Responding to Digital Disruption: A Factor-Based Study of the Newspaper Industry. Journal of Management Information Systems 32, 39-81 (2015)
36. Kohli, R., Johnson, S.: Digital Transformation in Latecomer Industries: CIO and CEO Leadership Lessons from Encana Oil & Gas (USA) Inc. MIS Quarterly Executive 10, 141-156 (2011)
37. Maedche, A.: Interview with Michael Nilles on "What Makes Leaders Successful in the Age of the Digital Transformation?". Business & Information Systems Engineering 58, 287-289 (2016)
38. Svahn, F., Mathiassen, L., Lindgren, R.: Embracing Digital Innovation in Incumbent Firms: How Volvo Cars Managed Competing Concerns. MIS Quarterly 41, 197-213 (2017)
39. Imgrund, F., Fischer, M., Janiesch, C., Winkelmann, A.: Managing the Long Tail of Business Processes. 25th European Conference on Information Systems, pp. 595-610, Guimarães (2017)
40. Rosemann, M., vom Brocke, J.: The Six Core Elements of Business Process Management. In: vom Brocke, J., Rosemann, M. (eds.) Handbook on Business Process Management 1: Introduction, Methods, and Information Systems, pp. 105-122. Springer, Berlin (2015)
41. Zairi, M.: Business Process Management: A Boundaryless Approach to Modern Competitiveness. Business Process Management Journal 3, 64-80 (1997)

ISIS12-Hack: Mitarbeiter sensibilisieren statt informieren

Kristin Weber[1] und Andreas Schütz[1]

[1] Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, Fakultät Informatik und Wirtschaftsinformatik, Würzburg, Deutschland
{kristin.weber,andreas.schütz}@fhws.de

Abstract. Mit zunehmender Digitalisierung stehen auch kleine und mittlere Unternehmen (KMU) vermehrt vor der Herausforderung sich mit der Thematik Informationssicherheit auseinanderzusetzen. Wie Mitarbeiter sich im Umgang mit Informationen und Informationssystemen verhalten, spielt hierbei eine entscheidende Rolle. Das Framework ISIS12 bietet ein Verfahren zur Etablierung eines Managementsystems für Informationssicherheit speziell für KMU. Die Bedeutung der Mitarbeiter für die Informationssicherheit wird in ISIS12 allerdings nur oberflächlich berücksichtigt. Diese Arbeit stellt ein Vorgehensmodell vor, das ergänzend zu ISIS12, die Sensibilisierung der Mitarbeiter für die Informationssicherheit zum Ziel hat. Um eine tatsächliche Verhaltensänderung bei den Mitarbeitern zu bewirken, werden hierfür Erkenntnisse der Sozialpsychologie genutzt. Das Vorgehensmodell analysiert zunächst vor allem die Kognition und Handlungsabsicht der Mitarbeiter. Eine individualisierte Security Awareness Kampagne geht anschließend gezielt auf die Bedürfnisse der jeweiligen Mitarbeiter ein und berücksichtigt dabei die besonderen Ansprüche eines KMU. Durch die Anpassung an den Ablauf von ISIS12 entsteht für Unternehmen nur wenig organisatorischer Mehraufwand.

Keywords: Informationssicherheit, Security Awareness, Mitarbeitersensibilisierung, ISMS

1 Motivation

Kleine und mittlere Unternehmen (KMU) haben für Deutschland eine enorme volkswirtschaftliche Bedeutung. KMU wollen, wie auch die großen Unternehmen, vom aktuell propagierten digitalen Wandel profitieren. Insgesamt weisen mittelständische Unternehmen der Digitalisierung eine hohe bis sehr hohe Bedeutung zu [1]. Dennoch geht der digitale Wandel nur langsam vonstatten. Gemäß einem Bericht des Bundesministeriums für Wirtschaft und Energie (BMWi) haben gerade KMU einen unterdurchschnittlichen Digitalisierungsgrad [2]. Die fortschreitende Digitalisierung stellt zweifelsohne hohe Anforderungen an die Informationssicherheit [3,4]. So bezeichnen viele KMU Herausforderungen im Bereich der Informationssicherheit als Hemmnis für den digitalen Wandel [2,5,6].

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Der „Faktor Mensch“ nimmt eine zentrale Stellung für die Gewährleistung der Informationssicherheit ein [7-9] und hat inzwischen die technischen Begebenheiten als beliebtestes Angriffsziel überholt [10]. Die eigenen Mitarbeiter sollten von Unternehmen als eine wertvolle Ressource zum Schutz sensibler Unternehmensinformationen und der IT-Infrastruktur verstanden werden. Durch Sensibilisierungsmaßnahmen kann der „Faktor Mensch“ von einer Schwachstelle zu einer Stütze des Informationssicherheitskonzeptes werden [7].

Die Sensibilisierung von Mitarbeitern ist ein komplexes, andauerndes Vorhaben, das letztendlich auf eine Verhaltensänderung der Mitarbeiter abzielt [11]. Erfolgreiche Verhaltensänderungen benötigen u. a. eine individuell auf die Überzeugungen des jeweiligen Mitarbeiters abgestimmte Vorgehensweise [12]. Umfragen zeigen jedoch, dass viele Unternehmen ein gemeinsames Maßnahmenpaket für alle Mitarbeiter schnüren und selten branchenspezifische Risiken berücksichtigen [13]. Die Individualisierung der Inhalte spielt häufig keine Rolle.

Vor dem Hintergrund, dass KMU vermehrt in den Fokus von Cyberkriminellen geraten und einen großen Nachholbedarf in der Sensibilisierung ihrer Mitarbeiter für das Thema Informationssicherheit sehen, verfolgt diese Arbeit das Ziel, das ISIS12-Vorgehensmodell zu optimieren. ISIS12 ist ein leichtgewichtiges Information Security Management Framework, das sich speziell an KMU richtet [14]. Die Arbeit schlägt ein Vorgehensmodell zur Mitarbeitersensibilisierung vor, das sich an der Abfolge von ISIS12 orientiert. Das Vorgehensmodell berücksichtigt Erkenntnisse aus der Verhaltensforschung und wird den Anforderungen von KMU nach zeit- und ressourceneffizienten Sensibilisierungsmaßnahmen gerecht. Das vorgeschlagene Modell wird derzeit im Rahmen eines Informationssicherheitsprojektes an einer Hochschule erprobt. Erste Erkenntnisse aus diesem Projekt fließen in die nachfolgende Betrachtung ein.

Der Rest der Arbeit ist wie folgt strukturiert: In Kapitel 2 werden die Besonderheiten von KMU in Bezug auf Informationssicherheit herausgearbeitet, Grundlagen von Security Awareness und der Beitrag der Sozialpsychologie diskutiert und ISIS12 hinsichtlich der Umsetzung der Mitarbeitersensibilisierung betrachtet. In Kapitel 3 wird die verwendete Forschungsmethodik vorgestellt. Kapitel 4 stellt schließlich das entwickelte Vorgehensmodell vor. In Kapitel 5 ziehen die Autoren ein Fazit und geben einen Ausblick auf weitere Forschungsarbeiten.

2 Related Work

2.1 Informationssicherheit in KMU

Ein System gilt als informationssicher, wenn es keine Zustände annimmt, die zu unautorisierter Informationsveränderung oder -gewinnung führen [15]. Im Unternehmen können hierfür verschiedene Schutzziele identifiziert werden. Vor allem die Ziele Vertraulichkeit, Integrität und Verfügbarkeit werden in diesem Zusammenhang häufig genannt [z. B. 15-17]. Um die Vertraulichkeit einer Information zu schützen, ist es notwendig, unautorisierten Zugriff auf sie zu

unterbinden. Mit der Integrität wird sichergestellt, dass die Informationen unverändert sind. Um dieses Schutzziel zu erreichen, müssen sie vor nicht autorisierten Änderungen geschützt werden. Mit der Verfügbarkeit soll sichergestellt werden, dass die gewünschte Information den autorisierten Nutzern zugänglich ist.

Informationssicherheit ist für KMU und Großunternehmen gleichermaßen wichtig. Bei KMU sind allerdings einige spezifische Besonderheiten zu beachten. Zum einen sind Bilanzsumme und Umsatz geringer. Aufgrund der hohen Kosten können sich KMU meist keine eigene IT-Abteilung leisten und müssen die IT-Nutzung mit weniger Ressourcen realisieren [1]. Maßnahmen zur Mitarbeitersensibilisierung müssen entsprechend kostensparend sein.

KMU haben gegenüber großen Unternehmen einen geringeren Formalisierungsgrad der zu einer niedrigen Standardisierung führt. 2016 hatten beispielsweise nur 32 Prozent der mittelständischen Unternehmen dokumentierte Sicherheitsrichtlinien [18]. Durch flache Hierarchien [19] und das stärkere Engagement der Eigentümer [20] haben die Führungskräfte in KMU einen stärkeren Einfluss auf das Verhalten der Mitarbeiter und können im Bereich der Informationssicherheit mit gutem Beispiel vorangehen. Charakteristisch ist außerdem der große Anteil der im eigenen Unternehmen ausgebildeten Facharbeiter [21]. Dies liefert Potential für Sensibilisierungsmaßnahmen, da man die Mitarbeiter bereits während der Ausbildung für die Thematik sensibilisieren kann. Dennoch bieten nur 27 Prozent regelmäßige Schulungen oder Informationen hinsichtlich der Informationssicherheit für Mitarbeiter an [18]. Zudem unterscheiden sich die KMU durch eine geringere Arbeitsteilung [19]. Ein breites Aufgabengebiet der Mitarbeiter erhöht die Ansprüche an die Informationssicherheit, da der einzelne Mitarbeiter auf mehr Informationen aus verschiedenen Bereichen zugreift. Gegenüber Großunternehmen haben KMU einiges aufzuholen: In den letzten Jahren konnten keine bedeutenden Verbesserungen der organisatorischen Maßnahmen zu Datenschutz und Sicherheit bei den Unternehmen festgestellt werden [19].

2.2 Security Awareness

Mit „Security Awareness“ wird grundsätzlich die Sensibilisierung von Mitarbeitern für Informationssicherheit umschrieben. Hänsch & Benenson [22] beschreiben drei mögliche Blickwinkel auf den Begriff Security Awareness. Die einfachste Sichtweise versteht unter Awareness, dass Mitarbeiter wissen, welche Bedrohungen es gibt und diese erkennen („Perception“). Eine weitere Sichtweise ergänzt, dass Mitarbeiter auch wissen, wie Sie sich vor Bedrohungen schützen können („Protection“). Und die dritte Sichtweise beschreibt, dass Mitarbeiter wissen, was eine Bedrohung ist und was sie dagegen tun können, und dass sie sich auch entsprechend verhalten („Behavior“). Nur der letzte Ansatz verspricht eine tatsächliche Erhöhung der Informationssicherheit im Unternehmen. Sensibilisierung heißt also, dass die Mitarbeiter wissen, wie sie sich informationssicherheitskonform verhalten (z. B. ein sicheres Passwort wählen), welche Konsequenzen ihnen und dem Unternehmen bei nichtkonformem Verhalten drohen (z. B. Imageverlust und finanzielle Schäden durch Verlust von Kundendaten) und dass sie dieses Wissen in kritischen Situationen tatsächlich anwenden.

Helisch & Pokoyski [23] nennen mit der Organisation noch einen weiteren Aspekt von Security Awareness. Die Organisation stellt sicher, dass Mitarbeiter sich im Unternehmen überhaupt informationssicherheitskonform verhalten können, dass also keine Barrieren einem entsprechenden Verhalten entgegenstehen. Gleichzeitig können organisatorische Maßnahmen, wie etwa die Erhöhung der Usability, die Informationssicherheit unterstützen. Security Awareness ist somit ein Zusammenspiel von Kognition (Verständnis des Problems und das Wissen zu dessen Lösung), Handlungsabsicht (Willen des Mitarbeiters sich informationssicherheitskonform zu verhalten) und der Organisation [23].

Um ein Verständnis für das menschliche Verhalten in Bezug auf Informationssicherheit zu entwickeln, kann die Sozialpsychologie wichtige Einsichten liefern [24]. Vor allem im Bereich der Gesundheitspsychologie hat sich in den letzten Jahrzehnten eine große Anzahl an Modellen etabliert, mit denen menschliches Verhalten erklärt werden kann. Das von Montaño & Kasprzyk [12] beschriebene Integrierte Verhaltensmodell (IBM) adaptiert die wichtigsten Konstrukte von gängigen Theorien und vereint diese in einem Modell (vgl. Abbildung 1).

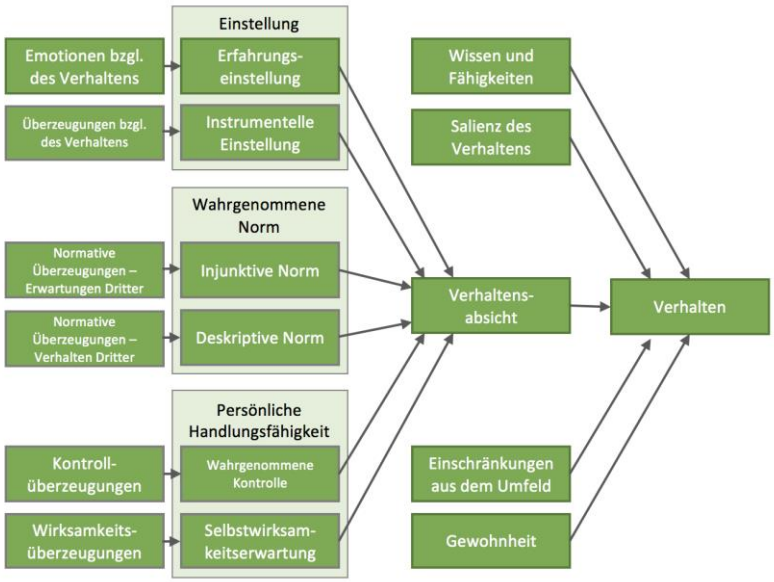


Abbildung 1. Das Integrierte Verhaltensmodell [12, S. 77].

Das Modell unterscheidet zwischen fünf verschiedenen Einflussfaktoren, die das Verhalten eines Menschen bestimmen. Dies sind zum einen das *Wissen und die Fähigkeiten* einer Person. Die *Salienz* des Verhaltens beschreibt wie prominent eine bestimmte Verhaltensweise für eine Person ist. Die von einem Mitarbeiter getroffene *Verhaltensabsicht* ist der stärkste Einflussfaktor [25] und auch der komplexeste. Sie wird wiederum durch die Einstellung, die wahrgenommene Norm und die persönliche Handlungsfähigkeit des Mitarbeiters bestimmt. Zudem können *Einschränkungen* aus

dem Umfeld die Ausführung des Verhaltens verstärken und die *Gewohnheit* eines Menschen die Wahrscheinlichkeit für die Ausführung erhöhen. Während Wissen und Fähigkeiten, Salienz, Einschränkungen und die Gewohnheit direkt vom Umfeld beeinflusst werden können, muss die Verhaltensabsicht über die Änderung von Überzeugungen und Emotionen indirekt beeinflusst werden.

Obwohl z. B. die Arbeiten [24,26,27] Ansätze aus der Sozialpsychologie nutzen, um konkrete Handlungsempfehlungen für die Steigerung der Security Awareness zu geben, ist in der Praxis der „One Size Fits All"-Ansatz bei der Mitarbeitersensibilisierung vorherrschend. Einer Umfrage der Allianz für Cybersicherheit zufolge berücksichtigen 54 Prozent der Unternehmen keine branchenspezifischen Risiken oder Gefährdungen bei der Auswahl von Security Awareness Maßnahmen [13]. 39 Prozent aller Unternehmen nutzen das gleiche Maßnahmenpaket für alle Mitarbeiter und 15 Prozent schulen nur IT-Mitarbeiter.

Bada et al. [13] zeigen, warum viele Maßnahmen zur Mitarbeitersensibilisierung versagen und identifizieren fünf Faktoren, welche die Effektivität von Security Awareness Kampagnen verbessern:

- Professionelle Vorbereitung und Organisation
- Keine Ängste bei Mitarbeitern schüren
- Zielgerichte und umsetzbare Schulungsinhalte
- Neue Verhaltensweisen kontinuierlich trainieren und Feedback geben
- Kulturelle Besonderheiten berücksichtigen

Auch das Integrierte Verhaltensmodell zeigt: Um einen Mitarbeiter zu informationssicherheitskonformen Verhalten zu bewegen, ist es notwendig zielgerichtet verschiedene Faktoren zu beeinflussen, die in einem komplexen Zusammenspiel stehen [12]. So müssen Sensibilisierungsmaßnahmen neben Wissen auch die Gewohnheit, die Salienz des Verhaltens, die Verhaltensabsicht und Einschränkungen aus dem Umfeld berücksichtigen.

2.3 ISMS: ISIS12

Um die zunehmende Komplexität der Informationssicherheit in Unternehmen zu beherrschen, empfiehlt sich eine organisierte, kontinuierliche und strukturierte Vorgehensweise durch die Etablierung eines Managementsystems für Informationssicherheit (ISMS). Mit ISIS12 wurde ein Framework zur Entwicklung und Umsetzung eines ISMS geschaffen, dass speziell für die Ansprüche mittelständischer Unternehmen ausgelegt ist [14]. ISIS12 orientiert sich an den Vorgaben der ISO/IEC 27000 Serie und den BSI IT-Grundschutz-Maßnahmen. Das ISIS12-Vorgehensmodell folgt dem aus dem Qualitätsmanagement bekannten PDCA-Zyklus (Plan, Do, Check, Act) (vgl. Abbildung 2). Dies bedeutet, dass die Phasen Planen, Tun, Überprüfen und Handeln wiederholt durchlaufen werden, um das ISMS kontinuierlich zu verbessern, auf aktuelle Bedrohungen zu reagieren und neue Anforderungen umzusetzen.

Der zweite Schritt des Vorgehensmodells heißt „Mitarbeiter sensibilisieren". Die Aktivitäten in diesem Schritt befassen sich mit dem Informieren der Mitarbeiter über

die Informationssicherheit im Unternehmen [14]: Vortrag über ISIS12, die Informationssicherheitsleitlinie des Unternehmens sowie spezifische Bedrohungen und Regelungen; Aushändigen und Unterschreiben der Unternehmensleitlinie für Informationssicherheit; Regelmäßige Information über Richtlinien, Fortgang von Projekten, Ansprechpartnern und anderen Informationssicherheitsthemen; sowie Informationen über Konsequenzen bei Verstößen.

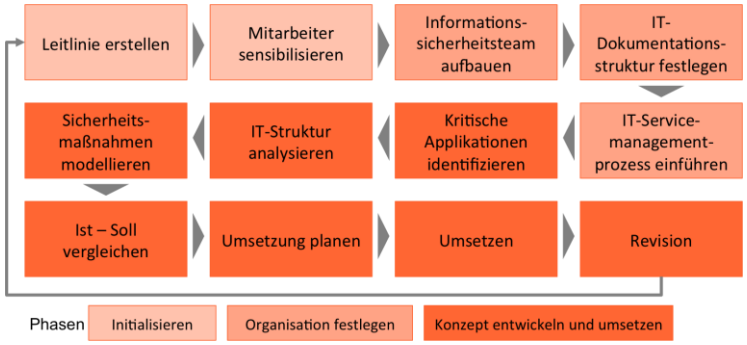


Abbildung 2. Das ISIS12-Vorgehensmodell (in Anlehnung an [14], S. 10).

Diese Art der Mitarbeitersensibilisierung beschränkt sich auf die Sichtweisen Perception und Protection von Security Awareness. Die individuelle Verhaltensabsicht (das Wollen) der Mitarbeiter wird vernachlässigt. Auch werden die meisten der o. g. Erfolgsfaktoren von Security Awareness Kampagnen in die Aktivitäten nicht berücksichtigt. Der Aspekt der Organisation gemäß [23] und der Faktor Einschränkungen aus dem Umfeld (vgl. IBM) werden hingegen in anderen Schritten des ISIS12-Vorgehensmodells adressiert. Organisatorische Maßnahmen, wie die Erstellung einer Leitlinie für Informationssicherheit (Schritt 1), der Aufbau eines Informationssicherheitsteams (Schritt 2) oder die Modellierung von Sicherheitsmaßnahmen (Schritt 8) können die Security Awareness erhöhen, indem die Organisation optimiert und Einschränkungen beseitigt werden.

3 Methodik

Die grundsätzliche Vorgehensweise dieser Arbeit orientiert sich am Design Science-Framework nach Hevner et al. [28] und ordnet sich der gestaltungsorientierten Wirtschaftsinformatik gemäß Österle et al. [29] zu. Demnach verläuft der Forschungsprozess in den vier Phasen Analyse, Entwurf, Evaluation und Diffusion, die iterativ wiederholt werden [29]. Nach Gesprächen mit Vertretern von KMU, Organisationen wie der IHK und Security Awareness Experten sowie einer Literaturrecherche wurde die Forschungslücke identifiziert (Analysephase). In der interdisziplinären Literaturrecherche wurden ISMS-Frameworks sowie wissenschaftliche Veröffentlichungen zu Security Awareness und der Sozialpsychologie einbezogen. Die dabei gewonnenen Erkenntnisse flossen in die

Entwicklung des Vorgehensmodells (Artefakt) ein (Entwurfsphase). Die Forschung befindet sich derzeit am Beginn der ersten Evaluationsphase.

Ein Vorgehensmodell beschreibt eine zeitlich logische Abfolge von Schritten eines Problemlösungsprozesses [30]. Es unterteilt den Prozess in einzelne Phasen und Aktivitäten mit klar definierten Ergebnissen. Der vorgeschlagene Prozess zur Sensibilisierung von Mitarbeitern in KMU stellt ein solches Vorgehensmodell dar.

Zur Vorbereitung der eigentlichen Evaluation in KMU wird das Vorgehensmodell derzeit in einem Projekt an einer bayerischen Hochschule erprobt. Das Bayerische E-Government-Gesetz verpflichtet in Artikel 8 alle bayerischen Hochschulen zur Erstellung und Umsetzung eines Informationssicherheitskonzeptes bis zum 01.01.2018. Um diese Anforderungen erfüllen zu können, werden in einem Teilprojekt die ersten Schritte des ISIS12-Vorgehensmodells durchgeführt. Das zweite Teilprojekt bereitet auf Grundlage des entwickelten Vorgehensmodells eine Kampagne zur Sensibilisierung von Hochschulangehörigen (Mitarbeiter und Studierende) für die Informationssicherheit vor. Hierfür wird bis zum Ende des Jahres 2017 die Ist-Situation analysiert und die Kampagne geplant. Diese soll im Jahr 2018 schließlich durchgeführt werden.

4 Erweiterung von ISIS12

4.1 ISIS12 und Mitarbeitersensibilisierung

Die Sensibilisierung der Mitarbeiter für Informationssicherheit wird im Framework ISIS12 nur unzureichend berücksichtigt. Insbesondere die Aspekte Behavior bzw. Handlungsabsicht von Security Awareness werden kaum beeinflusst. Daher wird im Folgenden eine Erweiterung von ISIS12 vorgeschlagen. Der zweite Schritt „Mitarbeiter sensibilisieren“ im ISIS12-Vorgehensmodell wird herausgenommen. Stattdessen wird ein Vorgehensmodell zur Sensibilisierung ergänzt, welches parallel zu den Aktivitäten von ISIS12 positioniert wird (vgl. **Tabelle 1**). Das Vorgehensmodell zur Mitarbeitersensibilisierung besteht aus den zwei Phasen Analyse (Aktivitäten A bis E) und Kampagne (Aktivitäten F bis H).

Die Parallelität beider Vorgehensmodelle hat folgende Vorteile:

- für beide Prozesse relevante Aktivitäten können gleichzeitig ablaufen,
- die Sensibilisierung kann einfach in das bestehende Framework integriert werden,
- die Sensibilisierung kann auch unabhängig von ISIS12 erfolgen.

Beispielsweise werden im Schritt 6 von ISIS12 kritische Applikationen identifiziert, indem u. a. Gespräche mit Mitarbeitern geführt werden [14]. Im Rahmen dieser Aktivität können die Mitarbeiter auch hinsichtlich ihrer Überzeugungen interviewt werden. Durch die Nutzung von Synergien können im Hinblick auf das Budget der KMU Zeit und Ressourcen gespart werden. Für die Gestaltung der ergänzenden Aktivitäten werden im Folgenden konkrete Handlungsempfehlungen auf Grundlage der Erkenntnisse der Verhaltensforschung gegeben.

Tabelle 1: Gegenüberstellung Vorgehensmodelle ISIS12 und Mitarbeitersensibilisierung

Schritt ISIS12	*Aktivität Mitarbeiter-sensibilisierung*	*Ergebnis*
1) Leitlinie erstellen	-	-
3) Informationssicher-heitsteam aufbauen	-	-
4) IT-Dokumentations-struktur festlegen	A) Verhalten identifizieren	Katalog mit relevanten Verhaltensweisen
5) IT-Servicemanage-mentprozess einführen	-	-
6) Kritische Applikationen identifizieren	B) Interviews führen	Transkribierte Interviews
7) IT-Struktur analysieren	C) Interviews analysieren	Katalog mit Wissensstand, Überzeugungen und Emotionen
8) Sicherheitsmaßnahmen modellieren	D) Fragebögen modellieren	Individuelle Online-Fragebögen
9) Ist – Soll vergleichen	E) Persönliche Faktoren messen	Übersicht Security Awareness Ist-Situation
10) Umsetzung planen	F) Kampagne planen	Ablaufplan der Sensibilisierungskampagne
11) Umsetzen	G) Kampagne durchführen	Zielgerichtet sensibilisierte Mitarbeiter
12) Revision	H) Erneut messen	Erfolgsmessung der Kampagne

4.2 Mitarbeitersensibilisierung – Analyse der Ist-Situation

Basis einer effektiven und zielgerichteten Sensibilisierung ist die Analyse der Ist-Situation im Unternehmen [11] (Aktivität A). Die Identifizierung der relevanten Verhaltensweisen, wie etwa „Ich wähle ein sicheres Passwort“, legt einen Grundstein für alle weiteren Schritte im Prozess. Im Hochschulprojekt wurden hierfür Maßnahmen des ISIS12-Kataloges ausgewählt, bei denen der Mitarbeiter beteiligt ist. Eine Auswahl könnte auch aufgrund von konkreten Sicherheitsvorfällen im Unternehmen erfolgen. Die ausgewählten Verhaltensweisen werden im weiteren Verlauf analysiert und in der späteren Sensibilisierung berücksichtigt.

Kritische Applikationen werden in ISIS12 vor allem mit Hilfe von Mitarbeiter-Interviews identifiziert. Die Interviews können genutzt werden, um Erkenntnisse für die späteren Sensibilisierungsmaßnahmen zu gewinnen. Diese qualitative Untersuchung (Aktivität B) fokussiert neben technischen Hürden gezielt auch kognitive Barrieren der Mitarbeiter. So kann beispielsweise festgestellt werden, welche Überzeugungen der Mitarbeiter das Fassen einer Handlungsabsicht blockieren und welche im Rahmen einer Kampagne besonders gefördert werden müssen. So konnte im Hochschulprojekt festgestellt werden, dass die Mitarbeiter wussten, dass ein Passwort regelmäßig geändert werden sollte, jedoch keine Verhaltensabsicht bestand, dies auch zu tun. Es zeigte sich, dass die Richtlinien der Hochschule hierzu

nicht kommuniziert wurden. So herrschte die normative Überzeugung, dass die Passwortänderung von den Mitarbeitern nicht erwartet wurde. Zusätzlich war die Funktion zum Ändern des Passwortes nicht leicht zugänglich. Diese Barriere wirkte sich negativ auf die Einschätzung der persönlichen Handlungsfähigkeit aus. Durch die Befragung von zirka zehn Prozent der Mitarbeiter aus unterschiedlichen Abteilungen sollen die größten Defizite in deren Verhalten identifiziert werden. KMU erhalten eine erste Übersicht über die im Betrieb vorherrschenden Überzeugungen und Emotionen hinsichtlich des Themas Informationssicherheit. Im Hochschulprojekt wurden Mitarbeiter aus verschiedenen Fakultäten und Serviceeinheiten der Hochschule befragt. Außerdem wurden Studentengruppen aus unterschiedlichen Studiengängen interviewt. Zum Zeitpunkt der Einreichung dieser Arbeit wurde gerade die qualitative Untersuchung abgeschlossen.

Die Analyse der Security Awareness der restlichen Belegschaft erfolgt in der anschließenden quantitativen Untersuchung in Form eines auf den Ergebnissen aus den Interviews basierenden Fragebogens (Aktivität C). Die Modellierung der Fragebögen erfolgt parallel zur Modellierung der Sicherheitsmaßnahmen in ISIS12. Die anschließende Befragung (Aktivität D) parallel zum Vergleich von Ist- und Soll-Situation. Der Fragebogen zur Ermittlung der Security Awareness nutzt unterschiedliche Methoden, um die Faktoren zu messen, die das Mitarbeiterverhalten beeinflussen. Das Wissen der Mitarbeiter kann über klassische Wissensfragen abgefragt werden. Um die Auswertung möglichst einfach zu gestalten, bieten sich hier vor allem Multiple Choice Fragen an. Um die Stärke der in Aktivität B ermittelten Überzeugungen zu messen und so auf die Verhaltensabsicht zu schließen, werden mit den Fragen verknüpfte Skalen verwendet, die je nach Konstrukt variieren können. Der Mitarbeiter drückt damit aus, wie stark seine Zustimmung oder Ablehnung hinsichtlich der Überzeugung ist. Es gibt ähnliche Ansätze, um die Gewohnheit zu messen (vgl. [31]). Lediglich für die Salienz des Verhaltens konnte keine hinreichend bestätigte Testmethode gefunden werden. Dieser Teil der Analysephase sollte möglichst automatisiert ablaufen, um dem geringen Budget von KMU Rechnung zu tragen und eine schnelle und zuverlässige Auswertung der im Betrieb vorherrschenden Security Awareness ermöglichen. Im Hochschulprojekt wird für diesen Zweck die Open-Source-Software LimeSurvey verwendet.

4.3 Mitarbeitersensibilisierung – Planung und Durchführung der Kampagne

Die Ergebnisse der Analysephase fließen in die Gestaltung der Kampagne zur Erhöhung der Security Awareness ein. Die Kampagne berücksichtigt somit die individuelle Ist-Situation im Unternehmen und geht gezielt auf die sensibilisierungsbedürftigen Verhaltensfaktoren und die Unternehmensspezifika ein. Eine Sensibilisierungskampagne kombiniert zielgruppenspezifisch verschiedene Maßnahmen über einen definierten Zeitraum und ähnelt somit einer Marketingkampagne [23]. Auswahl und Inhalte der Maßnahmen (Aktivität F) finden parallel zur Planung der Umsetzung der Sicherheitsmaßnahmen in ISIS12 statt. Die Maßnahmen müssen die Eignung besitzen auf die in der Analyse festgestellten Schwachstellen einzugehen. Fehlendes Wissen soll erhöht, mangelnde Gewohnheit

gefördert, falsche Überzeugungen korrigiert und negative Emotionen ins Positive gewandelt werden. Auch gängige Maßnahmen, wie Präsenzveranstaltung und soziales Marketing haben das Potential eine große Anzahl von Faktoren anzusprechen [32]. Konkrete Maßnahmen sind die Kommunikation der Leitlinie, Newsletter, Beiträge in der Mitarbeiterzeitung, Rollenspiele oder Computer-basierte Trainings. Allerdings sollten die Inhalte der Kampagnen gezielt auf die jeweiligen Faktoren einwirken [32]. Die Gestaltung der einzelnen Maßnahmen und wie diese anhand der Analyse ausgewählt werden, ist Teil von aktuellen Forschungsarbeiten.

Nach der Planung der Kampagne folgt deren Durchführung (Aktivität G). In Präsenzveranstaltungen kann ein Trainer beispielsweise Wissen vermitteln, falsche Überzeugungen durch die Präsentation von Gegeninformationen ändern oder durch Einübung positive Emotionen und Gewohnheit fördern. Soziales Marketing hat das Potential Verhalten zusätzlich salient zu machen, indem beispielsweise bei aktueller Bedrohungslage Newsletter versendet werden. Auf Basis der Analyseergebnisse können auch Erkenntnisse für organisatorische Maßnahmen gewonnen werden, deren Umsetzung die Mitarbeiter bei der Ausübung der Verhaltensweisen unterstützen. Wurde festgestellt, dass die Passwortregeln nicht klar sind, könnten diese bei der Wahl eines neuen Passworts direkt angezeigt werden. Dies wirkt sich positiv auf die Kontroll- und Wirksamkeitsüberzeugungen eines Mitarbeiters aus. In der Analysephase identifizierte unterstützende Faktoren können noch verstärkt werden. Auch Aktivität G könnte aus Budgetgründen zukünftig, in Kombination mit den automatisierten Fragebögen, z. B. durch ein digitales Lernprogramm mit individualisierten Lerninhalten unterstützt werden.

Ähnlich wie die Revision in ISIS12, sollte nach einer definierten Zeitspanne, z. B. nach einem Jahr, der Erfolg der Kampagne gemessen werden (Aktivität H). Dazu können die Fragebögen der Analysephase verwendet werden und die Ergebnisse verglichen werden. Idealerweise zeigt sich eine erhöhte Sensibilisierung der Mitarbeiter. Anschließend kann entschieden werden, ob das Vorgehen bei Aktivität A neu gestartet wird (beispielsweise, da sich die Rahmenbedingungen entscheidend verändert haben) oder ob die Erkenntnisse der Erfolgsmessung in die weitere Planung von Sensibilisierungsmaßnahmen einfließen (Aktivität F).

5 Zusammenfassung und Ausblick

Das Vorgehensmodell hilft KMU dabei einen wichtigen Faktor im Sicherheitskonzept zu analysieren und zu aktivieren: Die eigenen Mitarbeiter. Durch die Analyse der Situation im Unternehmen können zielführende, effektive Kampagnen geplant und durchgeführt werden. Statt die Mitarbeiter mit bereits bekannten Inhalten zu langweilen, werden ihre falschen Überzeugungen korrigiert. Sie werden überzeugt sich informationssicherheitskonform zu verhalten. Zum jetzigen Zeitpunkt ist die Analysephase noch sehr arbeitsintensiv. Durch weitere Forschung soll der Aufwand mit Rücksicht auf die Ressourcen der KMU auf ein Minimum reduziert werden. Die einfache Selektion der Verhaltensweisen, ein allgemeingültiger Überzeugungskatalog und ein standardisierter Wissenstest sollen einen bereits vorab entwickelten, digitalen

Fragebogen möglich machen, der in dem jeweiligen Unternehmen nur noch durchgeführt werden muss. Nach der automatisierten Auswertung der Ergebnisse soll eine Software zudem konkrete Maßnahmen und Inhalte empfehlen, die in einer Kampagne genutzt werden können.

Das Vorgehensmodell beachtet die von [11] identifizierten Erfolgsfaktoren weitgehend. Die Analyse stellt eine professionelle Vorbereitung dar und durch die Kombination mit einem ISMS wird die Organisation gewahrt. Es werden keine Ängste bei den Mitarbeitern geschürt, sondern es wird gezielt versucht negative Emotionen aufzuheben. Die Inhalte sind aufgrund der vorhergehenden Analyse zielgerichtet und können durch bekannte, umsetzbare Maßnahmen vermittelt werden. Auch das Trainieren der Verhaltensweisen wird durch den Faktor Gewohnheit berücksichtigt. Der PDCA-Zyklus sorgt für eine wiederholte Berücksichtigung von noch nicht etablierten Verhaltensweisen und lässt Feedback über den Erfolg der Kampagne zu. Kulturelle Unterschiede werden vor allem in der qualitativen Analyse sichtbar. Dies wird auch im allgemeingültigen Überzeugungskatalog berücksichtigt.

References

1. Schröder, C., Schlepphorst, S., Kay, R.: Bedeutung der Digitalisierung im Mittelstand. Institut für Mittelstandsforschung Bonn, Bonn (2015)
2. BMWi: Monitoring-Report Wirtschaft DIGITAL 2016. BMWi, Berlin (2016)
3. Hlavica, C., Hülsberg, F., Klapproth, U.: Tax Fraud & Forensic Accounting: Umgang mit Wirtschaftskriminalität. Springer Fachmedien, Heidelberg (2016)
4. Scholl, M., Fuhrmann, F.: Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt. In: Rätz, D. et al. (Hrsg.): Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung. S. 101-112. Gesellschaft für Informatik, Bonn (2016)
5. Leyh, C., Bley, K.: Digitalisierung: Chance oder Risiko für den deutschen Mittelstand? – Eine Studie ausgewählter Unternehmen. In: HMD Praxis der Wirtschaftsinformatik, 53 (1), S. 29-41. Springer, Heidelberg (2016)
6. Saam, M., Viete, S., Schiel, S.: Digitalisierung im Mittelstand: Status Quo, aktuelle Entwicklungen und Herausforderungen, ZEW GmBH, Mannheim (2016)
7. Schäfer, S., Pinnow, C.: Industrie 4.0 – Grundlagen und Anwendungen. Branchentreff der Berliner Wissenschaft und Industrie. DIN e.V., Berlin (2015)
8. Semba, B., Eymann, T.: Developing a Model to Analyze the Influence of Personal Values on IT Security Behavior. In: Nissen, V. et al. (Hrsg.): Multikonferenz Wirtschaftsinformatik (MKWI) 2016, S. 1083-1091. TU Ilmenau, Ilmenau (2016)
9. Hirshfield, L. et al.: The Role of Human Operators' Suspicion in the Detection of Cyber Attacks. In: International Journal of Cyber Warfare and Terrorism, 5(3), S. 28-44. IGI Global, Hershey (2015)
10. ISACA: State of Cybersecurity. Implications for 2016. An ISACA and RSA Conference Survey. ISACA, Rolling Meadows (2016)
11. Bada, M., Sasse, A., Nurse, J.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In: 1st International Conference on Cyber Security for Sustainable Society, S. 118-131. Coventry University, Coventry (2015)

12. Montaño, D., Kasprzyk, D.: Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavior Model. In: Glanz, K. et al (Hrsg.): Health Behavior and Health Education. Theory, Research and Practice. S. 67–96. John Wiley & Sons, Hoboken (2008)
13. Allianz für Cybersicherheit: Awareness-Umfrage 2015. Bundesamt für Sicherheit in der Informationstechnik, Bonn (2016)
14. Bayerischer IT-Sicherheitscluster (Hrsg.): Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand. Version 1.7. Bayerischer IT-Sicherheitscluster e.V., Regensburg (2014)
15. Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. 4., überarbeitete Aufl. De Gruyter, Oldenburg (2006)
16. Freiling, F. et al.: Technische Sicherheit und Informationssicherheit. In: Informatik Spektrum, 37 (1), S. 14-24. Springer, Berlin, Heidelberg (2014)
17. Kardel, D.: IT-Sicherheitsmanagement in KMU. In: HMD Praxis der Wirtschaftsinformatik, 48 (5), S. 44–51. Springer Vieweg, Wiesbaden (2011)
18. Brandl, S. et al.: DsiN-Sicherheitsmonitor Mittelstand 2016. Deutschland sicher im Netz e.V., Berlin (2016)
19. Pfohl, H.: Abgrenzung der Klein- und Mittelbetriebe von Großbetrieben. In: Pfohl, H. (Hrsg.): Betriebswirtschaftslehre der Mittel- und Kleinbetriebe. S. 1–24. Erich Schmidt Verlag, Berlin (2006)
20. Institut für Mittelstandforschung Bonn: Definitionen. http://www.ifm-bonn.org/definitionen/ (Aufgerufen: 25.10.2016)
21. Bussiek, J.: Anwendungsorientierte Betriebswirtschaftslehre für Klein- und Mittelunternehmen. Oldenbourg Wissenschaftsverlag, München (1996)
22. Hänsch, N., Benenson, Z.: Specifying IT security awareness. In: Morvan, F., Wagner, R., Tjoa, A. (Hrsg.): 25th International Workshop on Database and Expert Systems Applications 2014, S. 326-330. IEEE Computer Society, Los Alamitos, CA (2014)
23. Helisch, M., Pokoyski, D.: Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Vieweg+Teubner Verlag /GWV Fachverlage GmbH, Wiesbaden (2009)
24. Kabay, M.: Using Social Psychology to Implement Security Policies. In: Bosworth S., Kabay M. (Hrsg.): Computer Security Handbook. S. 1–22. Wiley, Hoboken (2002)
25. Fishbein, M., Ajzen, I.: Belief, attitude, intention, and behavior. An introduction to theory and research. Addison-Wesley Pub. Co., Reading (1975)
26. Siponen, M.: Five dimensions of information security awareness. In: ACM SIGCAS Computers and Society, 31 (2), S. 24–29. ACM, New York (2001)
27. Thomson, M., Solms, R.: Information security awareness: educating your users effectively. In: Information Management & Computer Security, 4 (6), S. 167–173. Emerald Group Publishing Limited, Bingley (1998)
28. Hevner A. et al.: Design Science in Information Systems Research. In: MIS Q 28, S. 75–105. University of Minnesota, Mineapolis (2004)
29. Österle, H. et al.: Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. In: Zeitschrift für betriebswirtschaftliche Forschung, 6, Nr. 62, S. 664-672 (2010)
30. Winter, R.: Business Engineering Navigator. Springer-Verlag. Berlin, Heidelberg (2011)
31. Verplanken, B., Orbell, S.: Reflections on Past Behavior: A Self-Report Index of Habit Strength. In: Journal of Applied Social Psychology (33), S. 1313–1330 (2003)
32. Schütz, A., Weber K.: Security Awareness: Nicht nur schulen – überzeugen Sie! In: Schartner, P., Baumann, A. (Hrsg): D•A•CH Security 2017, S. 1-12. Syssec, Frechen (2017)

Serviceplattformen als Digitalisierungsstrategie – Entwicklung und Anwendung eines Anforderungskatalogs für den Maschinen- und Anlagenbau

Friedemann Kammler[1], Florian Remark[1], Oliver Thomas[1]

[1] Informationsmanagement und Wirtschaftsinformatik, Universität Osnabrück, Germany
{friedemann.kammler,florian.remark,oliver.thomas}@uni-osnabrueck.de

Abstract. Der globale Wettbewerbsdruck stellt Unternehmen des deutschen Maschinen- und Anlagenbaus vor die Herausforderung, sich vom Produzenten zum digitalen Lösungsanbieter zu entwickeln. Potenziale werden unter anderem in Entwicklung digitaler Plattformenstrategien gesehen, die Dienstleistungen in Module zur kundenindividuellen Konfiguration organisieren und so eine mögliche Antwort auf den Wettbewerbsdruck bieten. Während bereits technische Lösungen zur Digitalisierung von Produkt- und Dienstleistungskomponenten entwickelt werden, bleibt offen, wie kleine und mittlere Unternehmen der einhergehenden Komplexität und Ausgestaltung einer Serviceplattform begegnen können. Gegenwärtig bestehen nur wenige Beispiele und Anforderungen, die eine konkrete Umsetzung anleiten. Vor diesem Hintergrund konsolidiert der vorliegende Beitrag eine generelle Anforderungsliste aus in der Literatur beschriebenen Anwendungsfällen. Nachfolgend nutzen wir die Liste für Experteninterviews im KMU-Umfeld und demonstrieren so die Anwendung als Werkzeug zur Konzeption einer Serviceplattform.

Keywords: Service Plattform, Anforderungskatalog, KMU, Maschinen- und Anlagenbau, Experteninterview

1 Einleitung

Im Rahmen der zunehmenden Digitalisierung werden kontinuierlich neue Konzepte zur zukünftigen Gestaltung von Produkten und Dienstleistungen vorgestellt [1]. Im Mittelpunkt der Diskussion im Maschinen- und Anlagenbau steht die Nutzung verfügbarer Daten und höhere Integration von Produkt- und Dienstleistungsanteilen, um im Wettbewerb zukünftig zum Lösungsanbieter zu avancieren und langfristige Alleinstellungsmerkmale zu sichern. Die zugrundeliegende Idee wird seit mehreren Jahren als Service Systems Engineering beforscht. Dabei handelt es sich um einen systemischen Ansatz, der nicht nur den Leistungserbringungsprozess als solchen, sondern auch dessen Gegenstand und beteiligte Akteure integriert und als gesamtheitlichen Gestaltungsraum begreift [2]. Diese Perspektive wandelt sich mit der zunehmenden Integration von informationstechnischen Komponenten, der daraus resultierenden Verfügbarkeit von Kontextdaten und der Erwartung an eine dynamische Anpassung des angebotenen Leistungsbündels. Derartige Systeme verschieben sich

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

vom Service System zum Smart Service System [3] und zielen neben der Abbildung von Dienstleistungen auf deren Anpassung bei Veränderung der Umweltbedingungen ab. Doch während diese Potenziale mindestens als vielversprechend betrachtet werden müssen, erhöht die steigende technologische und organisatorische Komplexität auch das Risiko des Ausschlusses kleinerer und mittlerer Unternehmen (KMU), die hohe Entwicklungsaufwände betreiben müssten, um derartige Lösungen anbieten zu können. Zwar werden gegenwärtig erste notwendige Komponenten, wie eingebetteten Systeme, Sensorik und Verarbeitungslogik, zur Produkterweiterung entwickelt, jedoch stellt die Schnittstelle zu Dienstleistungen die Digitalisierungsbemühungen vor Herausforderungen. So erfordert die „digitale Durchdringung“ von Dienstleistungen ein physisches Pendant, wie beispielsweise ein Assistenzsystem, das in Verbindung mit seiner Umwelt steht, Kontextdaten verarbeiten und die Dienstleistung flexibel anpassen kann. Darüber hinaus müssen organisatorische Notwendigkeiten, wie die Modularisierung von Dienstleistungen, erkannt und umgesetzt werden.

Serviceplattformen werden gegenwärtig als möglicher Kristallisationspunkt für die Abbildung solcher digitalen Service Systeme diskutiert [4]. Dabei steht die Idee im Mittelpunkt, Dienstleistungsmodule zu entwickeln, die individuell konfiguriert und abgerufen werden können [5]. Doch obwohl diese Grundidee bereits motiviert und beschrieben wurde, erschwert die Spannbreite der möglichen Anwendungsfälle nach wie vor die Formulierung eines konkreten Anforderungsprofils. Bisherige Forschungsarbeiten im Feld beschreiben einzelne Anwendungen, doch besteht bisher kein konsolidierter Katalog, der beschreibt, welche Anforderungen generell abgedeckt werden müssten. In der vorliegenden Arbeit wollen wir diese Lücke schließen und fokussieren daher die Forschungsfrage:

FF1: Welche Anforderungen werden an eine Serviceplattform gestellt?

Zur Beantwortung der ersten Forschungsfrage führen wir in Abschnitt 3 eine Analyse von bisherigen Forschungsarbeiten durch und leiten einen konsolidierten Anforderungskatalog ab. Aufgrund der bisher ungeklärten Anwendbarkeit des Katalogs formulieren wir eine zweite Forschungsfrage, die hinterfragt, ob die Anforderungen an eine Serviceplattform von Experten gleichermaßen eingeschätzt werden:

FF2: Inwiefern überschneidet sich der Anforderungskatalog mit dem praktischen Verständnis in einer konkreten Umsetzung?

Hierfür befragen wir in Abschnitt 4 Experten, die gegenwärtig im Rahmen eines Forschungsprojekts eine Serviceplattform für KMU im Maschinen- und Anlagenbau konzipieren und prüfen die Überschneidungen mit dem Katalog. In Abschnitt 5 analysieren wir die Überschneidungen und identifizieren verschiedene Anforderungsgruppen, die Kernaspekte der Serviceplattform herausstellen. Abschnitt 6 leitet aus den Erkenntnissen der Arbeit Implikationen für die Ergänzung weiterer Anforderungsperspektiven und das Verständnis von Serviceplattformen ab.

2 Verwandte Forschungsarbeiten

Plattformstrategien sind im Produktbereich seit Dekaden bekannt und wurden bereits in den 1980er Jahren praktisch umgesetzt [8]. Eines der bekanntesten Beispiele findet sich im Automotive-Bereich, in dem erfolgreich die Konfiguration von Modellvarianten mit dem Ziel der Anpassung an den Kundenwunsch vorangetrieben wird. Aber auch andere Branchen, wie der Maschinen- und Anlagenbau, setzen im Produktgeschäft auf die Modularisierung von Kernserien. Der Ansatz stellt den traditionellen, ingenieurswissenschaftlichen Ansatz zur direkten Optimierung von Leistung und Kosten in den Hintergrund und fördert an dessen Stelle die Flexibilität durch standardisierte Schnittstellen [8]. Dieser Paradigmenwechsel vermeidet hochintegrierte, schwer anpassbare Architekturen und ermöglicht die losgelöste Weiterentwicklung einzelner Komponenten. Der potenzielle Nutzen einer Plattformstrategie wurde ebenfalls im Dienstleistungssektor erkannt, in dem insbesondere die hohe Individualisierbarkeit einen Vorteil verspricht. Dabei stand ursprünglich die Idee der Modularisierung und Schnittstellendefinition auf Dienstleistungsebene im Mittelpunkt der Forschung. Diese wurde jedoch in der praktischen Umsetzung aufgrund der eingangs beschriebenen Immaterialitätsproblematik schnell durch technische Plattformen flankiert, die eine hinreichende Repräsentationsebene boten. Erste praxisbezogene Forschungsarbeiten erfolgten 2008 durch Lee et al. und dehnen sich seither auf unterschiedlichste Anwendungsfälle aus. Lee et al. beschreiben die konzeptuelle Umsetzung einer Serviceplattform im Gesundheitssektor und leiten einen allgemeinen Definitionsansatz ab [9]. Schmidt und van Hoof stellen ein prototypisches Beispiel im Energiesektor dar und formulieren hierfür eine Reihe spezifischer Anforderungen [10]. Aulkemeyer et al. nähern sich von technischer Seite und leiten ein Rahmenwerk für verschiedene Bestandteile von Serviceplattformen im Handelsumfeld ab [11]. Im Vergleich ist auffällig, dass einige Autoren dem technischen Schwerpunkt der digitalen Serviceplattform folgen und daher die Organisation verschiedener Applikationen innerhalb einer Plattform beschreiben, während andere den ursprünglichen Bezug zum eigentlichen Dienstleistungsprozess herstellen. Aus diesem diversen Forschungsfeld mit unterschiedlichsten Anwendungsdomänen leitet sich eine Liste heterogener Anforderungen ab, deren Übertragbarkeit bisher unklar ist. Vor diesem Hintergrund ist es kaum verwunderlich, dass allgemeingültige Definitionsversuche oftmals stark abstrahiert sind (vgl. [9]) und wenige allgemein anwendbare Anforderungen vorliegen.

3 Entwicklung des Anforderungskatalogs

Zur Entwicklung des konsolidierten Anforderungskatalogs folgt die Untersuchung Fettkes [12] Vorschlag der Analyse des aktuellen Forschungsstands. Dabei greifen wir auf die von Webster und Watson [13] postulierte Konzeptmatrix zurück, in der die seit 2008 zur Serviceplattform entstandenen Anforderungen gesammelt und verglichen werden. In unserer Recherche nutzten wir die Datenbanken *SpringerLink*, *AISeL*, *EBSCOhost* und *ScienceDirect* mit dem englischen Begriff „service platform“ sowie

„service plattform“. Für die Auswertung der Anforderungen nutzen wir ein mehrstufiges Schema. Tabelle 1 zeigt die Zuordnung der Beiträge zu den jeweiligen Anforderungen, deren Branchenbezug sowie die Einordnung in ein Phasenmodell, das den Umsetzungsgrad der jeweiligen Lösung verdeutlicht.

Tabelle 1. Ergebnisse der Literaturrecherche

Quelle	*Jahr*	*Branche*	*Umsetzung*	*Anforderung*							
				Multi-Agenten-Fähigkeit	Innovationsfähigkeit	Integrationsfähigkeit	Individualisierbarkeit	Interaktionsmöglichkeit	Automatisierung	Informationsbereitstellung	Sonstige
Dais et al.	2008	Verwaltung	Konzept	X		X		X		X	X
Baldwin et al.	2009	-	-		X	X	X				X
Haile/Altmann	2012	-	-	X				X			X
Anttiroiko et al.	2013	Verwaltung	Konzept	X	X	X		X			
Schmidt/ van Hoof	2013	Energie	Prototyp	X		X	X	X	X	X	X
Barthelmey et al.	2014	-	-				X		X	X	
Eggert et al.	2014	-	Umgesetzt		X						X
Elezi et al.	2014	-	-				X				X
Mikusz	2014	-	-				X		X		X
Gebregiorgis/ Altmann	2015	-	-			X	X				X
Herterich et al.	2015a	Anlagenbau	-					X	X	X	
Herterich et al.	2015b	Anlagenbau	-		X		X	X	X	X	
Saarikko	2015		Umgesetzt	X		X	X	X	X		X
Shu/Xiao	2015	-	-	X		X	X	X			X
Stich et al.	2015	-	-		X		X	X			X
Zhao et al.	2015	Verwaltung	Konzept	X		X	X	X	X	X	X
Aulkemeier et al.	2016	Handel	Prototyp	X		X	X	X	X	X	X
Anzahl				8	5	9	12	11	8	7	-

Nachfolgend werden die identifizierten Anforderungen anhand ihrer Beschreibung in der Literatur charakterisiert. Dabei werden die Begriffe bewusst aus Aspekten hergeleitet, die allen Nennungen gemein waren, anstatt einer einzelnen Definition zu folgen.

> *Multi-Agenten-Fähigkeit:* Die Plattform muss verschiedene Rollenkonzepte unterstützen. So müssen, neben Support-Oberflächen für Administratoren und Systembetreuer, beliebig konfigurierbare Systemoberflächen für verschiedene

Benutzergruppen bestehen. Diese Benutzergruppen können bspw. Kunden, Servicetechniker oder Service-Mitarbeiter umfassen.

Innovationsfähigkeit: Die Plattform muss um auftretende Innovationen erweiterbar sein. Diese können auf technischer Ebene (bspw. neue Endgeräte oder Schnittstellen), aber auch auf Dienstleistungsebene als neu abzubildende Leistungsmodelle entstehen.

Integrationsfähigkeit: Die Plattform muss Schnittstellen zu bestehenden Standardsystemen bieten und flexibel in diese integrierbar sein. Gleichzeitig soll auch die Serviceplattform Standard-Schnittstellen für zukünftige Systeme bieten.

Individualisierbarkeit: Die Plattform muss an unternehmensinterne Leistungsprozesse angepasst werden und auf Basis dieser instanziiert werden können. Hierzu zählt die Verknüpfung mit beteiligten Informationssystemen wie auch die Abbildung von Organisationsstrukturen und Prozessabläufen.

Interaktionsmöglichkeit: Zwischen den Akteuren der Plattform muss der Informationsaustausch ermöglicht werden. Die hierfür erforderlichen Kommunikationskanäle folgen klaren Richtlinien. Dabei entsteht durch die gemeinsame Nutzung der Plattform ein Mehrwert, der mit der zunehmenden Nutzerzahl skaliert.

Automatisierung: Die Plattform ermöglicht die Steuerung und Überwachung von Prozessabläufen. Hierzu zählen analytische Fähigkeiten, wie die automatisierte Visualisierung von Unregelmäßigkeiten, Identifikation von Fehlern und Optimierung der Betriebsabläufe.

Informationsbereitstellung: Datenhistorien der Serviceobjekte werden als Analysedaten in Form von Berichten gespeichert. Dies beinhaltet Sensordaten, aber auch Ereignisse, wie den normalen Betrieb, geplante Wartungen und Störungsfälle. Die Plattform stellt überdies für die verwendeten Systeme aktuelle und vollständige Dokumentationen bereit, die auch die visuelle Darstellung der einzelnen Komponenten beinhaltet.

Durch den beschriebenen konsolidierten Katalog beantworten wir Forschungsfrage 1, welche generellen Anforderungen an eine Serviceplattform bestehen. Über die einbezogenen Anforderungen hinaus wurde jedoch eine breite Basis an weiteren Anforderungen identifiziert, die jedoch aufgrund geringer Nennungshäufigkeit (in weniger als 3 Quellen identifiziert) weitere Untersuchung erfordern. Dabei handelt es sich um die Anforderungen an *Benutzerfreundlichkeit*, *Integration finanzieller Wertströme*, *Infrastrukturdesign*, *Sicherheit*, *Skalierbarkeit*, *Vertrauen* und *Verwaltung*.

4 Praktische Komplementierung des Anforderungskatalogs

Aufbauend auf dem entwickelten Katalog wurde ein Leitfaden-gestütztes Experteninterview entwickelt und durchgeführt. Die Teilnehmer sind Service-Manager aus drei

Unternehmen im Maschinen- und Anlagenbau, ein Senior-Consultant einer Prozess- und IT-Beratung sowie ein wissenschaftlicher Projektleiter. Die Unternehmen der Experten 2 und 3 sind dabei dem KMU-Umfeld zuzuordnen. Alle Teilnehmer entwickeln gegenwärtig an einer Serviceplattform für den After-Sales-Service des Maschinen- und Anlagenbaus. Die Untersuchung wurde zu Beginn des Forschungsprojekts durchgeführt, um ein möglichst unverfälschtes Bild des jeweiligen Plattform-Verständnisses zu erheben und keiner gemeinsamen Arbeitsdefinition zu folgen. Daher standen die Experten zum Zeitpunkt der Befragung noch vor einer vereinheitlichenden Diskussion von konkreten Anforderungen. Um den Fragenkatalog methodisch zu fundieren, folgten wir in der Entwicklung Helferrich [26]. Die Transkription erfolgte unter Berücksichtigung der Arbeiten von Meuser und Nagel [27], um die Ergebnisse möglichst transparent zu halten.

Tabelle 2. Ergebnisse der Expertenbefragung

			Experte				
Nr	*Stichwort im Interview*	*Anforderungszuordnung*	*1*	*2*	*3*	*4*	*5*
1	Rollenmanagement	Multi-Agenten-Fähigkeit	X	X			X
2	Kollaborationsfunktion	Interaktionsmöglichkeit		X			
3	Kommunikationsfunktion	Interaktionsmöglichkeit	X	X	X	X	X
4	Einheitliche Sprache	Interaktionsmöglichkeit		X			
5	Offene Schnittstellen	Integrationsfähigkeit	X		X		X
6	Transparenter Speicherort	Integrationsfähigkeit	X		X		X
7	Integration bestehender Services	Integrationsfähigkeit	X	X	X		X
8	Geräteunabhängigkeit	Integrationsfähigkeit	X	X	X	X	X
9	Wissensdatenbank	Informationsbereitstellung	X	X		X	X
10	Fernwartungsfunktion	Informationsbereitstellung	X	X	X		X
11	Falldatenbank	Informationsbereitstellung	X	X			X
12	Offlinefähigkeit	Informationsbereitstellung			X	X	X
13	Systemverfügbarkeit	Informationsbereitstellung	X	X			
14	Analysefunktion	Informationsbereitstellung				X	X
15	Predictive Maintainance	Automatisierung	X	X	X		
16	Customizing	Individualisierbarkeit		X			
17	Rechtliche Aspekte der Plattform	Sonstige	X	X	X		X
18	Usability	Sonstige	X				
19	Flexible Preismodelle	Sonstige		X			

Der jeweilige Experte wird eingangs nach seinem Verständnis einer Service-Plattform befragt, um den Einstieg in das Themengebiet des Interviews zu vereinfachen. Der Hauptteil der Befragung umfasst die in der Literaturrecherche identifizierten Anforderungen. Gleichzeitig werden abschnittsweise offene Fragen nach Ergänzungen gestellt, um eventuell über die Ergebnisse der Literaturrecherche hinausgehende Erkenntnisse zu erschließen. Dabei wird insbesondere der praktische Anwendungskontext der Ex-

perten berücksichtigt, der insbesondere in technischen Fragestellungen Zusatzinformationen ermöglichte. Die Zuordnung der Anforderungen des Katalogs erfolgte primär durch die Abschnitte der Befragung, wurde aber durch zwei Wissenschaftler unabhängig voneinander geprüft und angepasst, sofern der Experte innerhalb eines Komplexes das Thema gewechselt hat. Die Ergebnisse wurden diskutiert, vereinheitlicht und in Tabelle 2 als *Stichwort im Interview* und *Anforderungszuordnung* verdeutlicht.

5 Diskussion

Um Forschungsfrage 2 zu beantworten, analysieren wir im folgenden Abschnitt die Anwendung des Anforderungskatalogs. Hierfür werden die beiden Untersuchungsergebnisse übereinandergelegt und die Überschneidung interpretiert. Die eingeordneten Anforderungen der Experteninterviews werden anhand ihrer relativen Häufigkeit und der relativen Häufigkeit der Anforderung innerhalb der Literaturrecherche als Scatter-Plot dargestellt (Abbildung 1). Darüber hinaus wurde eine logische Clusterung der Daten erneut durch zwei Wissenschaftler vorgenommen, welche die Interpretierbarkeit der Ergebnisse erhöhen soll. Diese Clusterung folgt der Wichtigkeit der Anforderungen, bezieht jedoch inhaltliche Abhängigkeiten, wie der zwischen der *Systemverfügbarkeit* und der *Offline-Fähigkeit* mit ein und erweitert so die Gruppen um nicht eindeutig zuordenbare Anforderungen. Dies stellt an dieser Stelle der Untersuchung einen wesentlichen Vorteil gegenüber quantitativen Clusterverfahren wie bspw. dem *k-Means-Algorithmus* dar, die rein inhaltliche Aspekte nicht berücksichtigen.

Bereits bei einfacher Betrachtung ist eine Häufung von Anforderungen in der rechten oberen Gruppe festzustellen, die darauf hinweist, dass die Wichtigkeit von Anforderungen zwischen Literatur und Experteninterviews ähnlich eingeschätzt wird. Weiterhin existieren Faktoren, die entweder in der Literatur oder in der Praxis von vorrangigem Interesse waren. Im Rahmen dieser ist zu klären, inwiefern die konkreten Anforderungen der Interviews eventuell generelle Anforderungen abbilden, die in der Literatur bisher noch ungenügend berücksichtigt werden (rechte untere Gruppe). Gleichzeitig muss gefragt werden, ob Ergebnisse der Literatur bisher unzureichend in der praktischen Anwendung berücksichtigt sind und so weitere Potenziale genutzt werden könnten (linke obere Gruppe). Letztlich wurden einige Randanforderungen identifiziert, die aus beiden Perspektiven nur wenig Aufmerksamkeit erfahren (linke untere Gruppe). Diese sind für den gegenwärtigen Forschungsstand im Feld der Serviceplattformen mit Vorsicht zu betrachten, da diese sowohl aus praktischer wie auch aus wissenschaftlicher Perspektive bisher wenig betrachtet wurden.

Neben der ersten, visuellen Bewertung der Ergebnisse führten wir eine inhaltliche Charakterisierung der identifizierten Gruppen durch. Dabei standen erkennbare Zusammenhänge zwischen Einzelanforderungen sowie mögliche Rückkopplungen zwischen dem Anwendungsfall und dem Anforderungskatalog im Zentrum unseres Interesses. Im Folgenden sollen diese inhaltlichen Beziehungen zwischen einzelnen Anforderungen aufgezeigt werden.

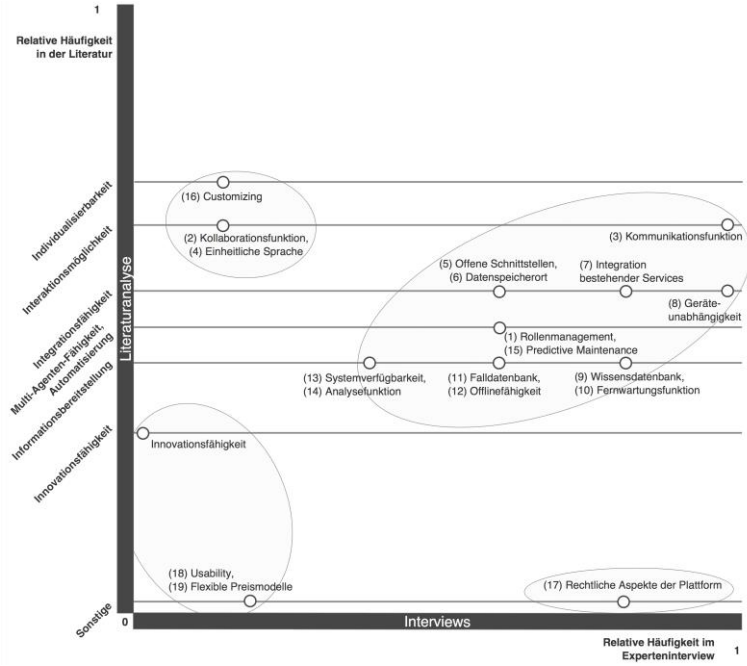


Abbildung 1. Einordnung der Anforderungen des Anwendungsfalls

Kernanforderungen an die Serviceplattform

Der größte Teil der Anforderungen wurde in beiden Erhebungsschritten als relevant identifiziert und dem oberen rechten Cluster zugeordnet. Auf der Ebene der generellen Anforderungen wird eine Reihe verschiedener Aspekte von diesem Cluster berührt: Von hoher Gesamtbedeutung sind daher die *Interaktionsmöglichkeit* und *Integrationsfähigkeit*, *Multi-Agenten-Fähigkeit*, *Automatisierung* und *Informationsbereitstellung*. Darunter fallen grundlegende Fragen der Implementierung, wie beispielsweise die Abbildung eines Rollenkonzepts (1), offener Schnittstellen zur Anbindung weiterer Systeme (5), Geräteunabhängigkeit (8), Transparenz des Speicherorts (6) und ständiger Verfügbarkeit des Systems (12, 13). Darüber hinaus wurden konkrete Systemfunktionen identifiziert, die sowohl im konkreten Anwendungsfall des Maschinen- und Anlagenbaus als auch in der generellen Betrachtung der Literaturstudie häufig genannt wurden. Genannt wurden Funktionen zur Kommunikation (3) und Fernzugriff auf das Serviceobjekt (10), zum Zugriff auf bestehendes Wissen (9, 11) sowie Analyse (14) und Prognose von Dienstleistungsbedarf (15). Abschließend wurde auch die Integration bestehender Services (7) als einzige rein dienstleistungsorientierte Anforderung in beiden Perspektiven genannt. Diese Anforderungen können als Kernanforderungen an digitale Serviceplattformen angesehen werden.

Potenziale für die Weiterentwicklung der Serviceplattform

Die Literatur verortet zusätzlich drei Anforderungen im hohen Bereich, die in den Experteninterviews nur vereinzelt genannt wurden. Hierzu zählt die Implementierung von Kollaborationsfunktionen (2) und die Individualisierbarkeit der Plattform (16). Eine weitere Anforderung ist die Definition einer einheitlichen Sprache (4), die auf der Plattform genutzt wird und so zur Verbesserung der Verständigung beiträgt. Diese wurden den generellen Anforderungen der *Individualisierbarkeit* und *Interaktionsmöglichkeit* zugeordnet, wodurch Überschneidungen mit den Kernanforderungen entstehen. Interessanterweise wird die Interaktion zwischen Akteuren durch die Experten wesentlich stärker in Kommunikations- als in Kollaborationswerkzeugen verortet. Dies kann auf den Anwendungsfall zurückzuführen sein, da der After-Sales-Service im Maschinen- und Anlagenbau durch einen hohen Grad an unterschiedlichsten Informationsbedarfen gekennzeichnet ist [28], die aufgrund der starken Ausdifferenzierung von Fehlerursachen und erforderlichen Maßnahmen schon jetzt eher in direkter Kommunikation anstelle von strukturierten Kollaborationswerkzeugen bedient werden. Die Gruppe zeigt, dass die konkrete Ausprägung einer generellen Anforderung durchaus anwendungsfallspezifisch erfolgen kann. So wird die Abbildung von Interaktionsmöglichkeiten von den Experten unterschiedlich ausgestaltet, jedoch insgesamt als wichtig bewertet. Inwiefern die vereinzelt identifizierten Anforderungen für alle Experten im Anwendungsfeld lohnenswerte Entwicklungspotenziale verkörpern, könnte in einem nächsten Schritt durch eine dezidierte Befragung untersucht werden und so eine iterative Weiterentwicklung motivieren.

Identifikation zukünftigen Forschungsbedarfs

In den Experteninterviews wurde lediglich eine Anforderung identifiziert, die in der Literatur von geringerer Bedeutung war. Hierbei handelt es sich um die Berücksichtigung der rechtlichen Rahmenbedingungen der Serviceplattform (17). In der Befragung wurden insbesondere Themen des Datenschutzes sowie der Haftung und Gewährleistung im Falle digitaler Dienstleistungserbringung angesprochen. Das Thema des Datenschutzes wurde dabei in enger Verbindung zu der Transparenz des Speicherorts (6) gesehen. Die Anforderung liegt in der Gruppe *Sonstige*, da rechtliche Rahmenbedingungen nur in einer der Quellen als Anforderung an Serviceplattformen gesehen wurden. Aufgrund der interdisziplinären Ausrichtung dieser Anforderung kann allerdings nicht abschließend beurteilt werden, ob die Untersuchung in der Literatur bisher aussteht oder außerhalb der Suchparameter der Recherche lag. Dies könnte beispielsweise durch gezielte Nachrecherche überprüft werden. Stellt sich heraus, dass die Anforderungen der Experten bisher in unzureichendem Maße bearbeitet wurden, bietet dies Möglichkeiten zur gerichteten Beforschung.

Randanforderungen an Serviceplattformen

Drei verbleibende Anforderungen finden bisher aus beiden Perspektiven nur geringe Aufmerksamkeit. Die Fähigkeit, auf Innovationen reagieren und diese flexibel in die Plattform integrieren zu können, wurde im Rahmen der Experteninterviews nicht genannt, erfährt in der Literatur hingegen mehr Aufmerksamkeit. Damit liegt sie zwischen der Gruppe der Potenziale für die praktische Anwendung und der Randanforderungen,

die weitere Beforschung erfordern, bevor deren Relevanz klar bewertet werden kann. Die Berücksichtigung von Usability-Fragestellungen (18), wie auch die Anpassung von Preismodellen an die flexiblen Dienstleistungsmodule (19) wurden in beiden Untersuchungen nur teilweise berücksichtigt. Damit fallen diese beiden Faktoren auch in der Literaturanalyse unter die Kategorie *Sonstige* und müssen hinsichtlich Relevanz untersucht werden. Die Bedeutung der in dieser Gruppe identifizierten Anforderungen sollte unserer Ansicht nach vorsichtig betrachtet werden. Zwar erscheinen die Ergebnisse von geringer Relevanz zu sein, gleichzeitig besteht aber auch die Möglichkeit, dass das Interesse an diesen Fragestellungen lediglich in der frühen Phase der Entwicklung von Serviceplattformen gering ist. Sowohl die Optimierung des bestehenden Systems im Sinne der Usability, als auch die Adaption neuer Strukturen im Geschäftsmodell könnten als nachgelagerte Arbeitsschritte betrachtet werden, deren grundsätzliche Relevanz nicht ausgeschlossen werden sollte.

6 Implikationen zur Entwicklung von Serviceplattformen

Aus unserer Untersuchung ergibt sich, dass Serviceplattformen Anforderungen insbesondere in den Feldern *Interaktion*, *Integration* und *Automatisierung* sowie in der Abbildung unterschiedlicher *Agenten* stellen. Das Experteninterview zeigt jedoch auch, dass die Ausprägungen der generellen Anforderungen durchaus unterschiedlich ausfallen können. Dies unterstützt die eingangs beschriebenen Beobachtung, dass ein diverses Feld an Anforderungen vorliegt, die nicht ohne Weiteres zwischen Anwendungsfällen übertragen werden können. Diese Lücke wird durch die erarbeitete Liste überbrückt, die generelle Anforderungen definiert, deren Ausgestaltung jedoch offenlässt. Wie im Rahmen der Experteninterviews gezeigt wurde, kann die Liste zugrunde gelegt werden, um einen ersten Rahmen zu definieren, der anwendungsfallspezifisch konkretisiert werden kann. Über die Beantwortung der Forschungsfragen hinaus lassen sich aus der vorliegenden Arbeit Schlüsse auf das Funktionsspektrum und das Architekturverständnis der Serviceplattform ableiten. So wird deutlich, dass die Plattform als Nexus verschiedener Informationssysteme und bestehender Dienstleistungen dient (Integration) und Interaktionsmöglichkeiten für verschiedene Akteure und Stakeholder der Erbringung schaffen soll. Für das After-Sales-Service-Geschäft im Maschinen- und Anlagenbau handelt es sich somit um eine Strategie zur Digitalisierung von Dienstleistungen, der Verknüpfung mit Stakeholdern und Serviceobjekten und deren zentraler Organisation im Sinne eines Service Systems. Die durchgeführte Untersuchung berücksichtigt bisher nicht dezidiert die umfangreichen Bemühungen des Software- und Service-Engineerings, die jeweils auf eine Perspektive isoliert weitere Beiträge zur Entwicklung und Schnittstellendefinition für Serviceplattformen bieten. Dies begründet sich in der bisher stark begrenzten, praktischen Umsetzung der Konzepte. Nichtsdestotrotz ist zu vermuten, dass die frühe Integration von servicespezifischen Fragestellungen die durch die Plattform erschlossenen Potenziale weiter erhöht und der Abbildung starrer Servicekonzepte auf einer flexiblen technischen Lösung entgegenwirkt. Vor diesem Hintergrund gilt es, den Anforderungskatalog gegen weitere Forschungsperspektiven zu prüfen und gegebenenfalls zu erweitern.

7 Zusammenfassung

Im vorliegenden Beitrag beantworten wir die Frage, welche Anforderungen in der Literatur an Serviceplattformen gestellt werden und inwiefern sich diese mit den praktischen Anforderungen überschneiden. Wir entwickelten hierfür einen Katalog genereller Anforderungen und zeigen im Rahmen eines Anwendungsfalls aus dem KMU-Umfeld im Maschinen- und Anlagenbau, wie eine anwendungsfallspezifische Anforderungsliste mit Hilfe des Katalogs abgeleitet wird. In der Analyse zeigt sich, dass verschiedene Anforderungsgruppen identifizierbar sind, diese jedoch noch primär die technische Umsetzung der Plattform fokussieren. Wir diskutieren abschließend die Integration weiterer Perspektiven und schlagen die Berücksichtigung von Anforderungen aus dem Software- und Service-Engineering vor. Diese Ergänzung wird weiter dazu beitragen, den Anwendungsbereich von Serviceplattformen zu definieren und die Entwicklung bereits frühzeitig auf erforderliche Perspektiven auszuweiten.

Literaturverzeichnis

1. Arbeitskreis Smart Service Welt / Acatech: Smart Service Welt - Umsetzungsempfehlungen für das Zukunftsprojekt Internetbasierte Dienste für die Wirtschaft. Berlin (2015)
2. Böhmann, T., Leimeister, J.M., Möslein, K.: Service Systems Engineering: A Field for Future Information Systems Research. Bus. Inf. Syst. Eng. 6, 73–79 (2014)
3. Peters, C., Maglio, P., Badinelli, R., Harmon, R.R., Maull, R., Spohrer, J.C., Tuunanen, T., Vargo, S.L., Welser, J.J., Demirkan, H., Griffith, T.L., Moghaddam, Y.: Emerging Digital Frontiers for Service Innovation. Commun. Assoc. Inf. Syst. 37, 136–149 (2016)
4. Saarikko, T.: Digital platform development: A service-oriented perspective. In: ECIS 2015 Completed Research Papers. Paper 152 (2015)
5. Thomas, O., Kammler, F., Özcan, D., Fellmann, M.: Digitale Plattformstrategien als Treiber der Dienstleistungsflexibilisierung im Maschinen-und Anlagenbau. In: Dienstleistungen 4.0. 481–494. Springer (2017)
6. Porter, M.E., Heppelmann, J.E.: How smart, connected products are transforming competition. Harv. Bus. Rev. 92, 64–88 (2014)
7. Larson, R.C.: Commentary—Smart Service Systems: Bridging the Silos. Serv. Sci. 8, 359–367 (2016)
8. Sanchez, R., Mahoney, J.T.: Modularity, flexibility, and knowledge management in product and organization design. Strateg. Manag. J. 17, 63–76 (1996)
9. Lee, Y., Meurk, C., Harris, M., Diminic, S., Scheurer, R., Whiteford, H.: Developing a Service Platform Definition to Promote Evidence-Based Planning and Funding of the Mental Health Service System. Int. J. Environ. Res. Public. Health. 11, 12261–12282 (2014)
10. Schmidt, J., van Hoof, A.: Architektur einer Service Plattform zur Unterstützung des Betriebs erneuerbarer Energieanlagen. In: Wirtschaftsinformatik 19 (2013)
11. Aulkemeier, F., Paramartha, M.A., Iacob, M.-E., van Hillegersberg, J.: A pluggable service platform architecture for e-commerce. Inf. Syst. E-Bus. Manag. 14, 469–489 (2016)
12. Fettke, P.: State-of-the-Art des State-of-the-Art: Eine Untersuchung der Forschungsmethode „Review" innerhalb der Wirtschaftsinformatik. Wirtschaftsinformatik. 48, 257–266 (2006)
13. Webster, J., Watson, R.T.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Q. 26, xiii–xxiii (2002)

14. Dais, A., Nikolaidou, M., Alexopoulou, N., Anagnostopoulos, D.: Introducing a Public Angency Networking Platform towards Supporting Connected Governance. In: Proceedings of the 7th International Conference on Electronic Government. Springer, Turin, Italy (2008)
15. Baldwin, C., Woodard J., Gawer., A.: Platforms, markets and innovation. In: The Architecture of Platforms: A Unified View, 19-44 (2009)
16. Gebregiorgis, S.A., Altmann, J.: IT Service Platforms: Their Value Creation Model and the Impact of their Level of Openness on their Adoption. Procedia Comput. Sci. 68, 173–187 (2015)
17. Haile, N., Altmann, J.: Value creation in IT service platforms through two-sided network effects. Econ. Grids Clouds Syst. Serv. 139–153 (2012)
18. Anttiroiko, A.-V., Valkama, P., Bailey, S.J.: Smart cities in the new service economy: building platforms for smart services. AI Soc. 29, 323–334 (2014)
19. Barthelmey, A., Störkle, D., Kuhlenkötter, B., Deuse, J.: Cyber Physical Systems for Life Cycle Continuous Technical Documentation of Manufacturing Facilities. Procedia CIRP. 17, 207–211 (2014)
20. Eggert, M., Häussling, R., Henze, M., Hermerschmidt, L., Hummen, R., Kerpen, D., Pérez, A.N., Rumpe, B., Thissen, D., Wehrle, K.: SensorCloud: towards the interdisciplinary development of a trustworthy platform for globally interconnected sensors and actuators. In: Trusted Cloud-Computing. 203–218. Springer (2014)
21. Mikusz, M.: Towards an Understanding of Cyber-physical Systems as Industrial Software-Product-Service Systems. Procedia CIRP. 16, 385–389 (2014)
22. Herterich, M., Uebernickel, F., Brenner, W.: Nutzenpotentiale cyber-physischer Systeme für industrielle Dienstleistungen 4.0. HMD Prax. Wirtsch. 52, 665–680 (2015)
23. Herterich, M., Uebernickel, F., Brenner, W.: Empowering Technical Customer Service by Cyber-Physical Industrial Equipment: Exploring Rationales, Opportunities, and Impediments. In: Proceedings of the 19th Pacific Asia Conference on Information System (PACIS), Singapore (2015)
24. Shu, N., Xiao, Y.: The Research Status of Value Co-creation in Service Platforms. (2015)
25. Stich, V., Kurz, M., Optehostert, F.: Framework Conditions for Forming Collaborative Networks on Smart Service Platforms. In: Camarinha-Matos, L.M., Bénaben, F., and Picard, W. (eds.) Risks and Resilience of Collaborative Networks. 193–200. Springer International Publishing (2015)
26. Zhao, R., Kou, Y., Du, R., Gu, L., Yang, H.: Research on Construction of Cloud Service Platform of Sci-tech Information for Agricultural Research System. In: Li, D. and Chen, Y. (eds.) Computer and Computing Technologies in Agriculture VIII. 556–564. Springer International Publishing (2015)
27. Helfferich, C.: Leitfaden- und Experteninterviews. In: Baur, N. and Blasius, J. (eds.) Handbuch Methoden der empirischen Sozialforschung. 559–574. Springer Fachmedien Wiesbaden, Wiesbaden (2014)
28. Meuser, M., Nagel, U.: ExpertInneninterviews - vielfach erprobt, wenig bedacht. In: Garz, D. and Kraimer, K. (eds.) Qualitativ-empirische Sozialforschung: Konzepte, Methoden, Analysen. Westdeutscher Verlag, Opladen (1991)
29. Daeuble, G., Oezcan, D., Niemoeller, C., Fellmann, M., Nuettgens, M., Thomas, O.: Information Needs of the Mobile Technical Customer Service - A Case Study in the Field of Machinery and Plant Engineering. Proceedings of the 49th Hawaii International Conference on System Sciences (2015)