

Editorial

Liebe Leserinnen und Leser,

vor Ihnen liegt nunmehr die bereits siebzehnte Ausgabe des E-Journals **Anwendungen und Konzepte in der Wirtschaftsinformatik (AKWI)** – das Journal feiert dieses Jahr sein 10-jähriges Jubiläum – die erste Ausgabe erschien bereits im September 2013. Im Rahmen dieses Jubiläums möchten wir uns herzlich bei der Vielzahl von Lesern, Autoren und Gutachtern bedanken, ohne deren Interesse und deren Einsatz ein solches Journal nicht machbar wäre.

Die Artikel dieser Ausgabe lassen sich wieder in die verschiedensten Bereiche der Wirtschaftsinformatik einordnen, wobei wir hier wie gewohnt die klassische Strukturierung der Kernwirtschaftsinformatik verwenden. Die Ausgabe gliedert sich in gewohnter Weise in eigentliche Zeitschriftenartikel, wobei hier diesmal der noch recht neue Praxisteil einen relativ großen Platz einnimmt, sowie Kurzübersichten einiger spannender Abschlussarbeiten.

Die eigentlichen Zeitschriftenartikel inklusive Praxisteil stammen diesmal schwerpunktmäßig aus den Bereichen des Geschäftsprozessmanagements / Digitalisierung, der Business-Intelligence im Sinne von Analysen, aber auch zu Thematiken der Simulation, Optimierung sowie der Anwendung von KI-Verfahren. Des Weiteren spielt das Thema des Informationsmanagements unter dem Aspekt der IT-Sicherheit und des Systemmanagements eine Rolle. Zu guter Letzt wird auch das Gebiet der Internetökonomie im Sinne des E-Commerce behandelt.

Im Detail behandelt ein Artikel das Thema der Digitalisierung, indem ein Digitalisierungsprojekt für Klein- und Mittelständler in der Hauptstadt beschrieben wird. Im Bereich BI resultiert ein Artikel aus einem Forschungsprojekt, welches das Ziel hat, ein bereits eingeführtes BI System aus Sicht der Usability zu verbessern, ein weiterer Artikel befasst sich mit dem Bereich der diskreten Simulation im SCM-Umfeld. Die Anwendung der KI in der WIN wird von einem Artikel betrachtet, der einen Machine-Learning basierten Chatbot beschreibt, welcher Anfragen von Studierenden beantworten soll sowie in einem Artikel, der den Einsatz von KI in Unternehmen unterstützen soll; es werden hier der aktuelle Forschungsstand betrachtet und Handlungsempfehlungen gegeben. Die Rolle der IT-Sicherheit im Rahmen des Informationsmanagements wird in einem Artikel behandelt, der sich mit der Frage der Anonymisierung von personenbezogenen Daten befasst – hier werden aktuelle Verfahren sowie ihre Schwachstellen behandelt.

Die Artikel des Praxisteils behandeln das Thema der Optimierung – hier speziell die Auswirkungen der neuen europäischen Regulierungen bezüglich des Kerosinverbrauchs im Flugverkehr, der IT-Sicherheit bei Routern in der Fertigungsindustrie, das Thema des Systemmanagements, bei dem Anomalien im Betrieb automatisiert erkannt und gemeldet werden sowie ein digitales Lieferantenportal, welches letztlich die Zollabwicklung vereinfachen soll.

Auch wenn die Zeitschrift ursprünglich mit dem Anspruch gestartet war, Forschungsergebnisse sowie Abschlussarbeiten zu präsentieren, freut es uns natürlich auch sehr, wenn wir solche Praxisartikel aufnehmen können, denn ein solcher Praxisbezug liegt einfach in der Natur der Wirtschaftsinformatik.

Wir haben diesmal sechs Kurzdarstellungen von Abschlussarbeiten aufgenommen, die sich mit den Themen des Informationsmanagements, hier auch dem Projektmanagement, der Business-Intelligence sowie der Softwareentwicklung befassen. Konkret befasst sich eine Arbeit mit der Frage wie agile Methoden im Projektmanagement von IT-Dienstleistern skaliert werden können, ein Artikel befasst sich mit der automatisierten Texterkennung zur Erfassung von Daten sowie ein weiterer mit einer unternehmensweiten Suchlösung. Die Abschlussarbeit aus dem Bereich BI befasst sich mit einer Datenvorbereitungsumgebung für Machine-Learning-Modelle, während die Arbeiten aus dem Bereich der Anwendungsentwicklung sich mit einer Entwicklung zur Unterstützung von Angebotsvergleichen sowie der Unterstützung der Entwicklung / DevOps befassen.

Über Ihr Interesse an der Zeitschrift freuen wir uns und wünschen Ihnen Freude bei der Lektüre.

Regensburg, Fulda, Luzern und Wildau, im Juli 2023.

Frank Herrmann, Norbert Ketterer, Konrad Marfurt und Christian Müller



Christian Müller



Konrad Marfurt



Norbert Ketterer



Frank Herrmann

VERFÜGBARKEIT VON PERSONENBEZOGENEN DATEN UNTER DEM ASPEKT DER ANONYMISIERUNG

Fabian Engl

Ostbayerische Technische Hochschule Regensburg

Galgenbergstraße 32, 93053 Regensburg

Email: fabian1.engl@st.oth-regensburg.de

Abstract—Daten und Analyseverfahren bestimmen zunehmend den heutigen beruflichen sowie privaten Alltag. In den letzten Jahren gewannen besonders personenbezogene Daten immer mehr Relevanz. Während hyper-personalisierte Werbung auf Social Media immer wieder in die Kritik gerät, profitieren auch andere Bereiche von leicht zugänglichen persönlichen Informationen. Die medizinische Forschung oder die Entwicklung künstlicher Intelligenzen hängen enorm von der Verfügbarkeit derartiger Daten ab. Neue Gesetzgebungen und Normen schränken diese aber immer weiter ein und verpflichten die Anonymisierung von personenbezogenen Daten vor deren Verwendung.

In diesem Artikel erfolgen eine Auflistung aktueller Anonymisierungsverfahren sowie eine Analyse ihrer Schwachstellen. Letztere werden kritisch unter dem Risiko der Re-Identifizierung und dem einhergehenden Verlust an Datenqualität beurteilt. Die Untersuchung veranschaulicht, dass alle Verfahren die Aussagekraft von personenbezogenen Daten auf unterschiedliche Art und Weise vermindern. Der Artikel identifiziert dabei drei wichtige Anforderungskriterien an einen anonymen Datensatz und hebt die Bedeutung einer ausführlichen Auseinandersetzung mit diesen Kriterien hervor. So bedarf es möglicherweise der Kombination mehrerer Verfahren, um die Verfügbarkeit zu optimieren. Er schließt mit der These, dass unterschiedliche personenbezogene Attributklassen eine Auswirkung auf die Wahl eines passenden Anonymisierungsverfahrens haben können.

I. PROBLEMBESCHREIBUNG

Mit der Einführung neuer Digitalgesetze wie etwa der Datenschutz-Grundverordnung (DSGVO) nimmt der Schutz persönlicher Daten immer wieder eine zentrale Stellung in der Informationssicherheit ein. So garantiert die DSGVO Verbrauchern nicht nur die Aufrechterhaltung ihrer Privatsphäre, sondern verpflichtet Dritte sämtliche Verarbeitungsprozesse von personenbezogenen Daten offenzulegen (Bieker, Bremert und Hansen 2018). Als direkte Folge daraus mussten viele Betriebe ihre internen Datenauswertungen neu evaluieren und entsprechende Maßnahmen ergreifen.

Um dieses Problem zu lösen und den Schutz persönlicher Daten in allen Verarbeitungsschritten zu gewährleisten, kommen Anonymisierungsverfahren zum Einsatz. Deren zunehmende Bedeutung ist besonders an den Google Trends erkenntlich. Hier kam es im Mai 2018 nach Inkrafttreten der DSGVO zu einem starken Anstieg der Suchanfragen zum Thema *Anonymisierung und Pseudonymisierung*. Das Nachfrageniveau verdoppelte sich im Vergleich zum Zeitraum vor der Einführung (Google LLC 2022).

Die zunehmende Relevanz von Daten in allen Lebensbereichen erfordert einen stärkeren Fokus auf den Schutz von Individuen. Folglich ist eine kritische Auseinandersetzung mit existierenden Anonymisierungsansätzen sowie deren Auswirkungen auf die Verfügbarkeit von persönlichen Informationen notwendig. Dieser Artikel gibt zunächst einen Überblick über aktuelle Anonymisierungsverfahren, geht kurz auf deren Funktionsweise sowie Schwächen ein und zieht anschließend ein Fazit, wie stark deren Anwendung die Datenverfügbarkeit beeinflusst.

II. FUNKTIONSWEISE UND SCHWÄCHEN EXISTIERENDER ANONYMISIERUNGSVERFAHREN

Derzeit existieren viele verschiedene Methoden, um personenbezogene Daten zu anonymisieren. Alle Ansätze versuchen, den Bezug zwischen Personen und weiteren zu ihnen gehörenden Informationen unkenntlich zu machen. Die Trennung ist erreicht, wenn eine Person nicht mehr eindeutig durch einen Datensatz identifiziert werden kann. Bei Menschen unterscheidet man zwischen direkten und indirekten Identifikatoren (Kesarwani u. a. 2021). Ein Beispiel für Erstere sind Namen und private Kennnummern. Da diese ein Individuum eindeutig bestimmen, müssen sie vor der weiteren Verwendung entfernt werden. Indirekte Identifikatoren – auch Quasi-Identifikatoren (QI) genannt – lassen durch ihre Kombination Rückschlüsse auf eine einzelne Person oder eine kleine Personengruppe zu. Dazu zählen etwa das Geburtsdatum oder Postleitzahlen. Des Weiteren existieren sensible Daten wie beispielsweise eine Krankheit, die einer Person zuordenbar sind. Bei der Unkenntlichmachung sollen dabei möglichst viele Merkmale sowie deren Aussagekraft beibehalten werden.

A. *k*-Anonymität

Der Ansatz der *k*-Anonymität schreibt vor, dass jede Kombination der QI mindestens *k*-mal im Datensatz existieren muss (Kesarwani u. a. 2021). Auf diese Weise kann ein Angreifer selbst nach Reduzierung des Datensatzes die korrekte Person höchstens mit einer Wahrscheinlichkeit von $1/k$ identifizieren. Je höher der Wert *k*, desto schwieriger fällt die korrekte Bestimmung.

Dieser Ansatz weist allerdings viele Schwächen auf: Entsprechen ein oder mehrere Einträge nicht der *k*-Restriktion, müssen diese vollständig weggelassen oder deren Werte generalisiert werden. Beides verringert die Aussagekraft und verschlechtert die Datenqualität (Dubli

und Yadav 2017). Extreme Merkmalsausprägungen erschweren zudem die Definition von sinnvollen Wertebereichen (Li, Qardaji und Su 2011). Problematisch sind ebenfalls k -anonyme Gruppen, bei denen alle Mitglieder das gleiche sensible Merkmal wie etwa identische Diagnosen aufweisen (Krebs und Hagenweiler 2022). Bei dynamischen Zugriffen bietet sie zudem keinen Schutz vor *Brute-Force*-Angriffen, die gezielt QI-Kombinationen abfragen, um so Gruppen weiter aufzubrechen (Li, Qardaji und Su 2011). Das vorausschauende Erkennen von Abhängigkeiten zwischen Abfragen und deren systemseitiger Ablehnung, erfordert mit zunehmender Attributvielfalt enorme Rechenkapazitäten (Kesarwani u. a. 2021).

Aus diesen Gründen gilt die k -Anonymität alleine als zu schwache Form der Anonymisierung und benötigt in der Praxis eine Ergänzung durch andere Verfahren (Li, Qardaji und Su 2011).

B. ℓ -Diversity and t -Closeness

Der ℓ -Diversity-Ansatz erweitert die k -Anonymität durch eine zusätzliche Einschränkung der sensiblen Attribute. Eine k -anonyme Gruppe muss zusätzlich mindestens ℓ verschiedene Merkmalsausprägungen innerhalb einer sensiblen Attributklasse aufweisen (Krebs und Hagenweiler 2022). Das verringert zwar den Detaillierungsgrad der Daten, verhindert aber das Auftreten von Gruppierungen, in denen alle Teilnehmer identische sensible Merkmale besitzen (Zheng 2021).

t -Closeness schränkt zudem die Verteilung dieser Merkmale weiter ein. So muss die Variation der Werte innerhalb einer k -anonymen Gruppe ähnlich zu der Verteilung im Originaldatensatz sein (Lingala u. a. 2021). Die Variable t definiert dabei die erlaubte Abweichung zur ursprünglichen Verteilung.

Diese Ansätze verbessern zwar die k -Anonymität, gleichen aber nicht alle Schwächen aus. Da sie die ursprüngliche Überprüfung um weitere Voraussetzungen ergänzt, werden zusätzliche Generalisierungsmaßnahmen benötigt, um das Risiko einer Re-Identifizierung zu vermindern. Das verringert die Datenqualität, Aussagekraft und Verfügbarkeit drastisch. Zudem sind alle drei Verfahren primär für die Anonymisierung von Teildatensätzen geeignet, da sie die Absenz von einzelnen Werten oder deren sinnvolle Zuordnung in eine Gruppe voraussetzen.

Beide Methoden können durch weitere Maßnahmen wie etwa die Aufteilung der Daten in *Cluster* optimiert werden (Lingala u. a. 2021).

C. Differential Privacy

Differential Privacy gehört zur Klasse der statistischen Anonymisierungsverfahren und kommt besonders bei dynamischen Abfragen zum Einsatz (Krebs und Hagenweiler 2022). Ziel des Ansatzes ist es, Antworten nachträglich durch das Hinzufügen von zufällig generiertem Rauschen zu verzerren und einzelne Einträge so unkenntlich zu machen. Die Rauschmenge hängt dabei stark von der Art der Anfrage ab, so benötigen generelle statische Auswertungen im Gegensatz zu

stärker personengebundenen Analysen weniger Verzerrungen (Domingo-Ferrer, Sánchez und Blanco-Justicia 2021). *Differential Privacy* zielt dabei nicht darauf ab, den Personenbezug eines einzelnen Eintrags unkenntlich zu machen, sondern dessen Präsenz oder Absenz in einem Datensatz zu verbergen (Domingo-Ferrer, Sánchez und Blanco-Justicia 2021).

Die nachträgliche Verzerrung von Daten findet in der Regel nicht direkt in einer Datenbank oder einer Abfrage statt. In der Praxis übernimmt ein zusätzlicher vertrauenswürdiger Server diesen Anonymisierungsschritt, der als *Middleware*-Komponente arbeitet und die Anfragen entgegennimmt (Krebs und Hagenweiler 2022). Allerdings besteht auch hier die Gefahr, dass Angreifer die dynamischen Anfragen ausnutzen und durch die Verknüpfung der Antwortdatensätze einzelne Personen wieder finden.

Während in den zuvor genannten Verfahren eine Einschränkung auf syntaktischer Ebene erfolgt, versucht *Differential Privacy* eine Re-Identifikation durch zusätzliches Wissen einzuschränken (Krebs und Hagenweiler 2022). Besitzen Dritte ergänzende Kenntnisse über einen (Groß-)Teil der Daten, können sie dies nicht anwenden, wenn nicht ersichtlich ist, ob oder wie viele der bekannten Personen enthalten sind.

Die Bereitstellung von präzisen und trotzdem aussagekräftigen Informationen ist in der Praxis aber nur schwer umsetzbar, da eine detaillierte personenbezogene Datenauswertung dem Grundgedanken der *Differential Privacy* – die Existenz von bestimmten Personen im Datensatz zu verbergen – widerspricht (Domingo-Ferrer, Sánchez und Blanco-Justicia 2021). Die An- und Abwesenheit von bestimmten Personen(-gruppen) hat in derartigen Analysen direkte Auswirkungen auf deren Endresultate.

D. Datensynthese

Die Datensynthese ersetzt persönliche Merkmale durch synthetisch generierte Werte und erzeugt so einen vollständig neuen Datensatz (Raji 2021). Die neuen Charakteristika müssen dabei so gewählt werden, dass jeder künstlich geschaffene Eintrag einer Person im Originaldatensatz entsprechen könnte. Der Synthetisierungsvorgang greift dabei das Konzept der *Differential Privacy* auf (Krebs und Hagenweiler 2022). Eine Teil-Synthetisierung ist ebenfalls möglich (Drechsler und Jentzsch 2017).

Derartige synthetische Einträge können durch das Zusammenspiel zweier neuronaler Netze entstehen. Dabei besitzt ein solches Netz Zugang zu den Originaldaten, während das andere lediglich die syntaktischen Anforderungen sowie die einzelnen Wertebereiche kennt und basierend darauf synthetische Daten erzeugt. Schafft es das erste Netz diese einer realen Person im Datensatz zuzuordnen, muss das zweite den Syntheseprozess überarbeiten (Raji 2021). Synthetische Daten eignen sich für dynamische und statische Abfragen. Bei Ersteren bedarf es allerdings einer stetigen Anpassung des Synthetisierungsmodells (Krebs und Hagenweiler 2022).

Da die erzeugten Datensätze nicht auf reale Personen verweisen, gelten sie nicht mehr als personenbezogene Daten (Raji 2021). Allerdings müssen für ein

gutes Synthetisierungsmodell alle Relationen im Originaldatensatz erkannt und berücksichtigt werden. Durch die Abhängigkeit vom *Differential-Privacy*-Ansatz sinkt die Datenqualität linear mit jedem weiteren Attribut im Datenmodell (Krebs und Hagenweiler 2022). In der Praxis erschweren besonders hochdimensionale Datensätze mit vielen (versteckten) Relationen eine vollständige sowie korrekte Replikation und schränken so die Bereitstellung von Daten ein (Drechsler und Jentzsch 2017).

III. HERAUSFORDERUNG BEI DER ANONYMISIERUNG

Wie bereits an den Schwächen der einzelnen Anonymisierungsverfahren zu erkennen ist, verringern alle Ansätze die Verfügbarkeit von personenbezogenen Daten auf unterschiedliche Arten. Es existiert kein Verfahren, das sowohl maximale Anonymisierung als auch uneingeschränkte Aussagekraft bietet (Drechsler und Jentzsch 2017). Um einen bestmöglichen Anonymisierungsgrad zu erreichen, benötigt es deswegen die Kombination mehrerer Methoden. So kann die k -Anonymität die Re-Identifizierung einer einzelnen Person verhindern, während *Differential Privacy* diese Logik ergänzt und dem Wissenszuwachs durch gezielte Datenabfragen entgegenwirkt.

Aus den Schwächen lässt sich zudem schlussfolgern, dass bei der Auswahl von passenden Verfahren drei Kriterien eine wichtige Rolle spielen: die Größe des Datensatzauszuges in Relation zum Originaldatensatz, die Attributvielfalt und die Stärke der nachträglichen Datengeneralisierung sowie -verzerrung. Diese drei Einschränkungen müssen in Einklang miteinander stehen und können nie alle vollständig erfüllt sein (siehe Abbildung 1). Soll der vollständige Datensatz verwendet werden, erfordert das folglich entweder eine starke Reduzierung der Attribute oder deren Genauigkeit.

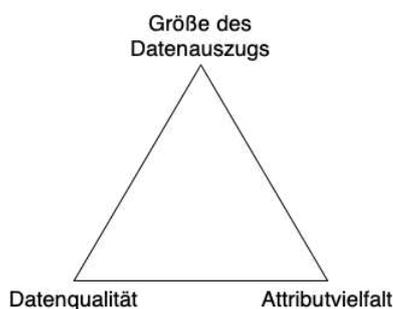


Abbildung 1. Anforderungsdreieck an ein Anonymisierungsverfahren (eigene Darstellung)

Die genannten Anonymisierungsverfahren schränken besonders die Präzision von personenbezogenen Daten stark ein und setzen fast immer Anpassungen der Merkmalsausprägungen voraus, denn werden persönliche Merkmale nur ausgetauscht, handelt es sich lediglich um eine Form der Pseudonymisierung. Diese Gefahr besteht besonders bei synthetischen Daten (Raji 2021).

Des Weiteren basieren alle Ansätze auf unterschiedlichen dynamischen Parametern. Die korrekte Wahl dieser Kenngrößen legt den finalen Grad der Anonymisierung fest. So bedarf es nicht nur der Zusammenführung von mehreren Vorgehensweisen, sondern auch der korrekten Festlegung ihrer Kenngrößen.

Die Anforderungen an den finalen Datensatz und die korrekte Auswahl der Anonymisierungsverfahren sowie deren Parameter haben folglich einen großen Einfluss auf den Detaillierungsgrad und die Menge der verfügbaren Daten.

IV. FAZIT UND ZUSAMMENFASSUNG

Die vorgestellten Anonymisierungsverfahren lösen zwar das Problem der Verarbeitung personenbezogener Daten, erschweren aber dadurch die Auswertung von großen und gleichzeitig detailreichen Datensätzen. Sie gewährleisten dennoch eine verhältnismäßig sichere Anonymisierung bei weniger umfangreicheren Datenauszügen. Da die Aussagekraft bei mehrdimensionalen Daten abnimmt, reicht es folglich nicht, diese Verfahren auf unveränderte existierende Datenextraktionen anzuwenden.

In stark durch persönliche Daten getriebenen Bereichen wie der medizinischen Forschung oder dem Trainieren von künstlichen Intelligenzen für personenbezogene Prognosen werden deswegen weitere Maßnahmen benötigt. Hier gilt es zunächst festzustellen, welchen Detaillierungsgrad die Auswertungen benötigen, denn das Weglassen irrelevanter Attribute kann schon zu einer höheren Aussagequalität führen. Die einzelnen Analysen verlieren dadurch zwar Zusammenhänge, aber der Verzicht ermöglicht die Verwendung einer größeren Datenmenge. Ein umfangreicher Datensatz mit vielen Wertdopplungen erfüllt beispielsweise Anonymisierungsansätze wie die k -Anonymität besser, erfordert weniger Generalisierungsmaßnahmen und erlaubt die Bereitstellung eines größeren Datenauszuges. Ist hingegen die Beständigkeit der Zusammenhänge relevant, verfügen synthetisch generierte Auszüge über mehr Aussagekraft.

Welche Verfahrenskombination die größtmögliche Verfügbarkeit persönlicher Daten sicherstellt, hängt dabei stark vom jeweiligen Anforderungsbereich ab. Dieser legt ebenfalls fest, wie nützlich die Zusammenführung mehrerer Verfahren ist. Hier bedarf es einer Evaluation, ob die Art der personenbezogenen Attribute eine Auswirkung auf die Auswahl der Anonymisierungsverfahren hat.

LITERATUR

- Bieber, F., B. Bremert und M. Hansen (Aug. 2018). „Die Risikobeurteilung nach der DSGVO“. In: *Datenschutz und Datensicherheit* 42.8, S. 492–496.
- Domingo-Ferrer, J., D. Sánchez und A. Blanco-Justicia (Juni 2021). „The Limits of Differential Privacy (and Its Misuse in Data Release and Machine Learning)“. In: *Communications of the ACM* 64.7, S. 33–35.

- Drechsler, J. und N. Jentsch (Mai 2017). *Synthetische Daten - Innovationspotential und gesellschaftliche Herausforderungen*. URL: https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf (besucht am: 22.11.2022).
- Dubli, D. und D. Yadav (Mai 2017). „Secure Techniques for Data Anonymization for Privacy Preservation“. In: *International Journal of Advanced Research in Computer Science* 8.5, S. 1693–1696.
- Google LLC (2022). *Google Trends: Anonymisierung und Pseudonymisierung*. URL: <https://trends.google.de/trends/explore?date=all&q=%2Fm%2F0277902> (besucht am 22. 11. 2022).
- Kesarwani, M. u. a. (2021). „Secure k-Anonymization over Encrypted Databases“. In: *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)* (Chicago, USA, 5.–10. Sep. 2021). IEEE Computer Society, S. 20–30.
- Krebs, H.-A. und P. Hagenweiler (2022). *Datenanonymisierung im Kontext von Künstlicher Intelligenz und Big Data*. 1. Aufl. Wiesbaden: Springer Vieweg, S. 91–100.
- Li, N., W. Qardaji und D. Su (Juni 2011). *Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy*. Techn. Ber. IN 47907-2086. West Lafayette, Indien: Center for Education, Research - Information Assurance und Security, Purdue University, S. 1–12.
- Lingala, T. u. a. (2021). „L-Diversity for Data Analysis: Data Swapping with Customized Clustering“. In: *Journal of Physics: Conference Series* 2089, S. 1–9.
- Raji, B. (Jan. 2021). „Rechtliche Bewertung synthetischer Daten für KI-Systeme“. In: *Datenschutz und Datensicherheit* 10.2, S. 303–309.
- Zheng, Y. (2021). „Personal Information Protection Based on Big Data“. In: *Journal of Physics: Conference Series* 2037, S. 1–7.

Towards Inter-organizational Decision Support in Supply Chains through Cloud-based Discrete Event Simulation – A Conceptual Business Model and Elements of a Research Agenda

Andreas Jede

Fakultät Wirtschafts- und Sozialwissenschaften

Hochschule Osnabrück
Caprivistraße 30a
49076 Osnabrück

E-Mail: a.jede@hs-osnabrueck.de

Jan Frie

Fakultät Wirtschafts- und Sozialwissenschaften

Hochschule Osnabrück
Caprivistraße 30a
49076 Osnabrück

E-Mail: j.frie@hs-osnabrueck.de

ABSTRACT

In general, cloud services enable new *inter-organizational* business improvements such as better coordination and collaboration tools as well as information and knowledge sharing. In contrast, discrete event simulation is a matured and highly helpful simulation technique on operational level that is currently used especially for optimizing supply chains *within an organization*. Therefore, this paper proposes a cloud-based discrete event simulation. Herein, the paper uses a mixed method approach and derives a new business potential in the intersection of both research fields. Thereby, we provide a wider understanding of cloud computing that goes beyond the technical functioning. Furthermore, the paper identifies the major future research directions for creating an economic and effective environment for applying cloud-based discrete event simulations.

KEYWORDS

Information Management, Cloud Computing, Discrete Event Simulation, Business Model, Supply Chain Management, Research Agenda, Design Science Research

1 INTRODUCTION

Whereas in the 1990s logistics research primarily studied the interaction of people, organization structures, and technologies *within* one enterprise, during the last 20 years, the major object of interest has shifted towards the *whole* supply chain (SC), which ranges from up-stream suppliers to down-stream distributors and final customers (e.g., Oliver and Webber, 1992; Handfield and Nicols, 1999; Swafford, et al. 2006; Hazen and Byrd, 2012; Sweeney et al., 2015; Wieland et al., 2021). Furthermore, for many years already, SCs have been dealing with IT-based optimization initiatives. It is self-evident that organizations manage today's market challenges better when investigating the construction and the IT processes of their SCs in more detail as well as aligning business processes and IT processes (Carter and Rogers, 2008; Pereira, 2009; Meer et al., 2012; Pashaei and Olhager, 2015; Tönnissen and Teuteberg, 2020).

For understanding the complex interactions of distributed SCs, stochastic influences, such as demand fluctuation, production site failure, or transportation delay, play an important role. The consideration of such effects is needed to assess the robustness and resilience of simulated SCs (Pereira, 2009; Pashaei and Olhager, 2015; Golrizgashfi et al, 2023) and to estimate the costs for various SC designs, resulting from operative activities. In

this connection, simulation models offer significant advantages because of the possibility of (i) testing their SCs in repeatable and controllable environments on a detailed modeling level and (ii) tuning the performance bottlenecks before deploying on real world (Gutenschwager and Alicke, 2004). This requires that the simulation results are robust, accurate and suitable.

Although the pressure for optimizing the entire network increases, most companies still tend to analyze their processes mainly isolated from SC partners (Tako and Robinson, 2012; Longo, 2023), which may not necessarily lead to the global optimum. And even if there are inter-company SC optimization efforts, these are often dominated and/or controlled by one company (e.g., the company that may have the higher market power), and possibly an economic buyer-supplier conflict may come up (Stern and Hesket, 1969; Willis and Jones, 2008; Rezapour et al., 2015), which may put one party at a disadvantage.

Discrete event simulation (DES) is an established analysis method for production and logistic systems and a widely used modeling tool which underpins decision support systems (e.g. Ridall et al., 2000; Huang et al., 2003; Agalianos et al., 2020; Greasley et al., 2021). DES is frequently used when important decisions have to be taken, where the far-reaching risks and consequences are not directly assessable. Besides, DES is applied when there are no suitable analytical solutions available (Willis and Jones, 2008; Zee, 2011). In general, simulations are applied to problems with stochastic influences within the analyzed processes (Siebers and Aickelin, 2011; Owen,

2013). Herein, a DES allows a high level of detail (Tako and Robinson, 2012; Kleijnen, 2005) when modeling SCs, calibrating SCs (e.g., transportation routes and frequencies, lot sizes, or safety stocks), and analyzing SC designs (e.g., production and warehousing locations with a given customer structure, insourcing vs. outsourcing or product allocation to central and regional hubs). In literature, there is a broad range of simulation studies analyzing SCs that cover various SC levels within one company (e.g. Lidberg et al., 2020; Melman et al., 2021; Lang et al., 2021). However, there are only few works that consider intercompany effects of specific elements of SC networks (Min and Zhou, 2002; Zee and Vorst, 2005; Greasley et al., 2021)

Simulations, and especially SC simulations, require a high level of expert knowledge of the simulation tools, the modeling, and the interpretation of results. Casual users, thus companies who only carry out such studies rarely, rather rely on external simulation services and abstain from the acquisition of the necessary simulation software as this would be uneconomical. Additionally, smaller companies within the SC do not have the capabilities to handle such simulation systems.

Therefore, this paper proposes a cloud-based DES concept, where a cloud service network offers the DES software to the SC network. This concept offers two major advantages. First, it enables to optimize enterprise-specific as well as global SC approaches that are not decoupled from external SC partners. Especially the global optimization possibilities may encourage organizations to increase their interactions such as coordination, collaboration, or information sharing in order to improve the overall SC network power and resilience. Second, the concept uses general advantages of cloud computing, namely pooling resources and cost efficiency. Even nowadays, the use of adequate simulation tools requires high investments for hardware and especially for software (e.g. Mansouri et al., 2020; Lang et al., 2021; Pan et al., 2022; El Kathib et al., 2022;). In general, the concept aims to meet the requirements of Demirkan and Delen (2013), who postulate already ten years ago the unchanged need for “affordable analytics for masses”.

The aim of the paper is to give cloud service providers and DES users as well as the scientific community a conceptual business model by means of a framework that is well-established in strategic management research. Thus, with our paper we extend the technological perspective of cloud computing (CC), by shifting the focus from the purely technical viewpoint to a wider understanding for new business opportunities. Instead of focusing on the advantages of the simulation results that have already been widely discussed in literature, we will investigate the major actors, roles, and requirements for enabling and running such a business model. The paper uses a construction-oriented mixed research methodology based on a systematic literature analysis (Webster and Watson, 2002), design science (Hevner et al., 2004), and expert

interviews (Cresswell, 2003). Thus, the underlying research questions are:

RQ1: How could an overall business model for cloud-based DES be structured?

RQ2: What are the general requirements for participating in the cloud-based DES?

The structure of the paper is as follows: In section 2, we discuss the theoretical background and the search for related work. Thereafter, we explain our mixed method research approach in section three. The section 4 outlines the underlying business model, consisting of actors and roles, including the important mediation role of an information broker. In section 5, we conceptualize the requirements for running such a business model. Finally, the paper discusses the evaluation in section 6 and concludes in section 7 with contributions, limitations and future research.

2 THEORETICAL BACKGROUND

To explore the status quo regarding the inter-organizational simulation of SC processes via CC, we conducted a systematic literature analysis (Webster and Watson, 2002). Knowing that the underlying research field is quite new and very specific, we consciously used a broad keyword range in order not to miss any pertinent research stream that might be helpful. The keyword based searching process started with using significant terms in various combinations: (operation* OR logistic* OR supply chain* OR value network* OR discrete event simulation) AND (cloud computing OR software-as-a-service OR grid computing OR service oriented architecture*). In order to identify relevant publications, we applied the searching process in four scientific databases (EBSCO, Science Direct, Google Scholar, Springer Link). With these searching parameters, we identified two broad fields of research: The first research field is not relevant for our research as it discusses simulation-based test environments for integrating cloud services, rather than providing simulation as a service for SC process optimization. As the consideration of this field may be fruitful in a more mature status of the underlying topic instead of for the actual conceptualization phase, we excluded it. And also the second field tackles our core topic only superficially in so far as it investigates the general advantages of cross-company cloud usage for operating real SCs (e.g., ordering by using cloud services).

Therefore, we expanded our literature searching procedure by seeking for exemplary papers that describe cloud-based value networks with related actors and interactions. We identified seven papers (cf. section 2.2) whose major insights have been transferred for our purposes of conceptualizing a value network through a cloud-based SC simulation tool. As this paper proposes a business model that integrates the fields of supply chain

management (SCM), discrete event simulation (DES), and cloud computing (CC), we discuss these terms successively in the upcoming sub-sections 2.1 and 2.2 through the lens of strategic theory (Mintzberg, 1987).

Our upcoming business model includes various actors and therefore varying strategic perspectives may be taken, e.g., the perspective of service providers, integrators, or information brokers. We focus mainly on the strategic relevance of the integrated simulation for users, namely the SC members, as the users decide whether they accept the business model or not. The value-chain model by Porter (1985) is very suitable for the purpose of this paper. Porter sought to understand the relevant factors of competitive advantage and found that *rigorous control* throughout all activities within the value chain may enable organizations to utilize cost-saving and differentiation potentials. Moreover, he postulates that running organizations successfully is about to *reconfigure the value chains* successfully (Porter, 1985). Although Porter only considered value chains within one organization, his concept can easily be transferred to a SC network. Hence, rigorous control can be assured by modeling real live SC processes within a detailed simulation with controllable variables. Following this approach in integrated simulation environments with related SC partners may open new dimensions for value chain reconfiguration. This reconfiguration process leads to a *process-based view on strategy*, where the question is *how* SCs reach a particular performance (Mintzberg, 1987). We aim to answer this question in section 4. Moreover, simulating the SC network can be justified with the process-based research concept of the so-called “*intermediate outcome*” (Chatterjee, 1998). For the SC members, the integrated simulation does not represent a product or service that can be offered to the market place nor does it create competitive advantage per se, but it has the potential to draw valuable conclusions on real SC processes, which in turn may lead to higher profits, higher revenues etc.

2.1 Supply Chain Simulation

In literature, SCM is defined as “the systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across businesses within the SC, for the purposes of improving the long-term performance of the individual companies and the SC as a whole” (Mentzer et al., 2001). Contrary to many other definitions (e.g., Cooper et al., 1997b; Handfield and Nicols, 1999), this definition puts an important and realistic emphasis on the individual companies on the one side and the SC network on the other side, which means that there are pre-existent SC conflicts (more details in section 5). Moreover, Mentzer et al. (2001) determine SCM as a set of entities directly involved in the upstream and downstream of three flows: (i) products and services, (ii) finances, and (iii) information.

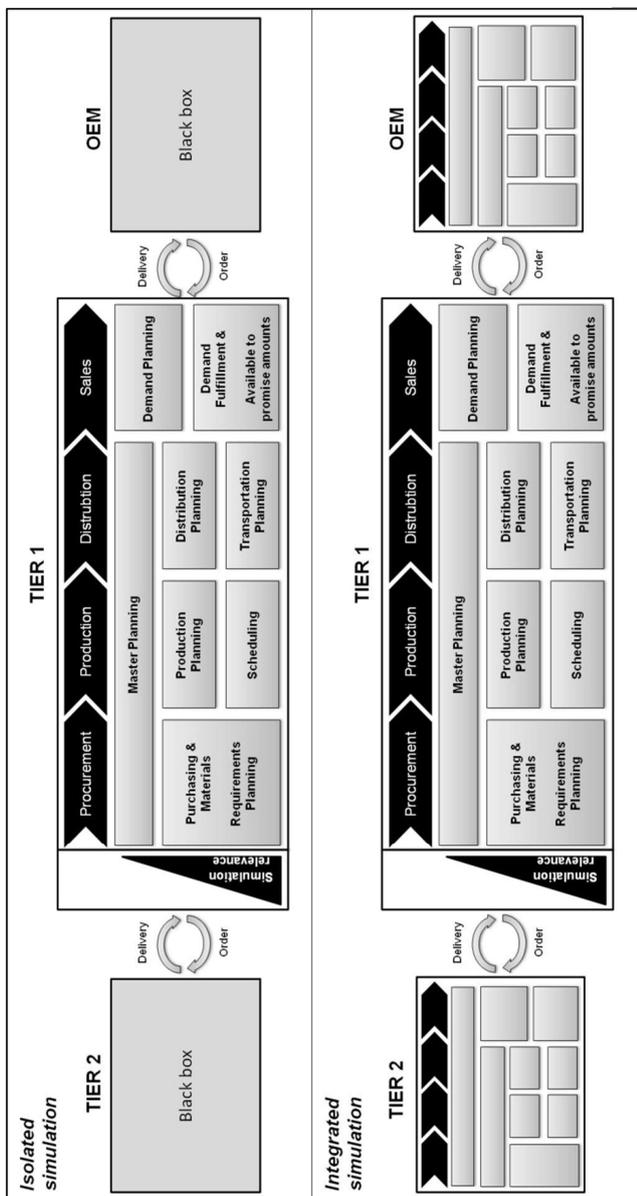
Supporting SCM processes, DES emerged in the late 1950s, modeling the operation of a SC system as a discrete sequence of events in time (Tako and Robinson, 2012; Agalinos et al., 2020). Each event occurs at a specific instant in time and constitutes a change of state in the system (Robinson, 2004). Hence, the SC system behavior and performance can be analyzed under various conditions (Sweetser, 1999; Sweeney, 2015). In contrast to other simulation methods such as system dynamics, DES is known to be useful at the tactical level by modeling a SC network of queues and activities, where randomness is created by statistical distributions (Brailsford and Hilton, 2001). Towards this end, this kind of incremental and tentative search for a better composition of the SC elements goes in line with *process-based view on strategy* that was introduced by Mintzberg (1987). Thereby, the pattern of action visible ex post makes up the “emergent strategy” (Mintzberg, 1987), which in the context of this paper may be derived from simulations.

In DES, entities (objects, people etc.) are modeled individually, where specific attributes are assigned to each entity. These attributes determine what happens to the entities during the simulation (Tako and Robinson, 2012). The relevant parameters and variables for simulating SCs have been investigated and discussed in literature intensively. Here we want to refer to some well recognized works such as Law and Kelton (2000), Fishman (2001), Min and Zhou (2002), and Chen et al. (2000) that provide a great amount of variables and parameters. There are diverse DES software tools available for the simulation of SCs. Usually, they have a graphical user interface that supports the modeling process. Modeling modules/entities are mostly defined by locations, customers, production sites, resources, and links of storages, hubs, and transportations (Gutenschwager and Aliche, 2004). Also important is the integration of ERP functions such as planning and forecasting of production, procurement, and transportation. Due to the high requirements for data quality and the large amounts of data, assist functions are often advantageous, e.g., for checking the data consistency in the input or to import bulk data. In case of very large amounts of data, table-oriented approaches with a database may be beneficial. As mentioned before, the adequate use of such simulations is still quite expensive as they require specific knowledge and high performance systems. Moreover, we only occasionally found papers that applied DES in cross-company SCs (e.g., Dorsch and Hackel, 2012; Chien and Kuo, 2013; Turner et al., 2016). This is criticized by Pereira (2009), Demirkan and Delen (2013), and Sweeney et al., (2015) as well, who motivate research and practice to investigate cross-company analytics more in detail.

Following this motivation, we depicted our intention in figure 1. Acknowledging the SC planning processes, Meyr et al. (2002, p. 99) presented the SC planning matrices which involve long and mid-term aspects (e.g., “master planning”) as well as short-term aspects (e.g., “transportation planning”). From the perspective of the

TIER1, we present an isolated simulation of the SC planning matrix in the upper case (which equals more or less today's situation) and an integrated approach in the lower case. In the isolated case, the TIER1 has to estimate the current as well as forecasted order statistics from the OEM and the delivery statistics from TIER2 in order to analyze his own supply chain. In the integrated case, all members simulate their SC by themselves, by enriching the SC network with higher information sharing and optimization possibilities. In case of a fully transparent DES, all members of the SC (TIER 1, TIER 2, and the OEM) are in a position to see the data of the other members (e.g., order and delivery statistics). Herein, DES addresses especially the tactical or operational level, which we depicted with "simulation relevance". Of course it is possible to derive long-term strategic decisions from the simulation results.

Figure 1: Comparison of isolated and integrated SC simulations (adopted from Meyr et al., 2002)



2.2 Cloud Computing

The term "cloud computing" emerged in 2007 and is classified as a next development level of service-oriented architectures (Youseff et al., 2008). The National Institute of Standards and Technology (NIST) defines CC as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance, 2011). But CC does not represent a new technology. Rather, it stands for a new paradigm for IT processes (Youseff et al., 2008) by consistently linking individual, existing technologies (Leimeister et al., 2010). The majority of the research literature distinguishes between three major service models (Hoberg et al., 2012, Mell and Grance, 2011): "Infrastructure as a Service (IaaS)", "Platform as a Service (PaaS)", and "Software as a Service (SaaS)". Furthermore, there are four deployment types (public, private, hybrid, community). In terms of this paper, we only consider public CC, where an external provider offers services through the Internet. (With the other deployment types, the involvement of a pre-existing, neutral information broker is hard to realize.) Research and practice gain a lot from CC as it provides various advantages such as collaboration and coordination increases as well as costs and time savings (e.g., Meer et al., 2012; Cegielski et al., 2012; Ahmed et al., 2015; Bharany et al., 2022; Saratchandra et al., 2022), which consequently also assigns strategic relevance to CC (Marston et al., 2011).

Coming back to the seven papers that we identified during the literature search, Böhm et al. (2010) have developed a CC network, in which the interaction of service creation and mediation are presented. Their main contribution is the determination of eight generic roles. All involved participants are shown in relation to each other via a market platform. The authors evaluated their model by expert interviews that confirmed the interrelation between the different identified roles. The paper by Leimeister et al. (2010) is similar to the model by Böhm et al. (2010) and puts emphasis on the business perspective of CC. For this reason, similar to the work of Böhm et al. (2010), the article contributed to a systematic description of major actors entering the CC market and modeled their interactions by conceptually developing a value network of cloud actors. Walterbusch et al. (2014) built on the two models and created a CC business model by including actors such as a mediator and a consultant. Their principal contribution consists of the hybrid creation of cloud services via various related roles, which was confirmed by expert interviews. Moreover, they outline the importance of service transparency during the creation process. A completely different CC view on the cross-organizational collaboration aspect is discussed by Martens et al. (2011). They investigate the topic from an interdependency-driven perspective, which results in the determination of three collaborative CC environments. Thereby, the envi-

ronments are constituted by *pooled* (public and community clouds), *sequential* (cloud chain) and *networked CC* (industrial cloud). This environment serves as a basis for a decision support process that includes risk and security factors for the selection of adequate partners. Also focusing on risk models, Keller and König (2014) asked how cloud actors can identify risks in cloud business networks and increase the transparency in network structures. Their real life application displays the dissemination of risks through the cloud network, where the actors are able to identify the impending risks. Lang et al., (2021) question whether or not free CC oriented discrete-event simulation software is an alternative to commercial tools for solving typical planning tasks in production and logistics. Herewith, they compare three open source solutions and two commercial simulation tools, including the supporting role of the IT-provider. Finally, the paper by Deng et al., (2021) explores via adaptive structuration theory how organizations attain organizational agility through IT-outsourcing appropriation. It examines the mediating role of IT alignment and the moderating roles of the adoption of cloud computing and knowledge transfer.

Grounding especially on the first three models, first we transfer empirically tested roles and the interactions of the roles on the subject of DES-based SC optimization.

3 RESEARCH APPROACH

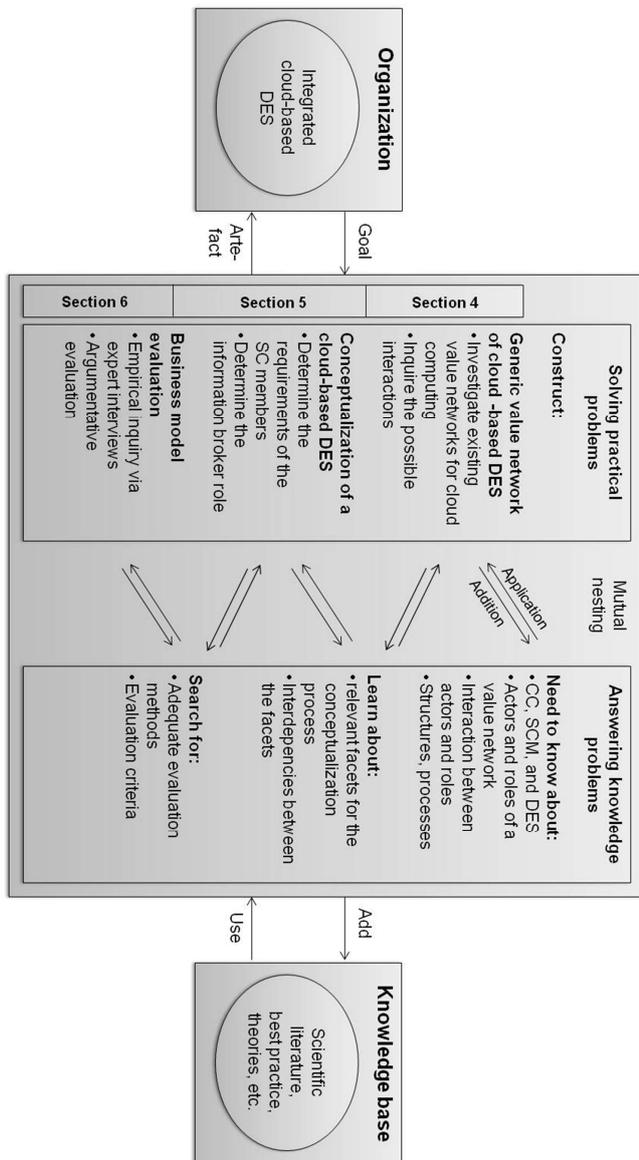
The underlying research approach is construction-oriented, because it involves “the construction of an information technology artifact and its evaluation” (Kuechler and Vaishnavi, 2011). Therefore, it is assigned to the design science research paradigm (Wieringa, 2010). Acknowledging Hevner et al., (2004), design science aims at the development of “technology-based solutions to important and relevant business problems”. These solutions have to lead to an improved environment by means of creating innovative artefacts, which can be constructs, models, methods, or instantiations (Hevner et al., 2004). To provide a scientific methodology for the initially stated research questions, we adopt the nested problem solving strategy (Wieringa, 2010), which is based on the design science paradigm of Hevner et al., (2004). Herein, the problem solving process is conducted by the researchers iteratively, and both the space of alternatives and the final design is entirely open at the beginning. During the process of problem solving, the problem is decomposed into interrelated sub-problems. This decomposition is repeated until sub-problems arise, which are considered to be solvable by stakeholders. According to Wieringa (2010), the sub-problems can be sub-divided into practical problems and knowledge problems (cf. figure 2).

In order to solve a practical problem, a certain change in the current state is required. It describes the difference between the current state and the state as it should be. On the other side, a knowledge problem represents some kind of knowledge deficit, which can be resolved by ad-

equately acquiring knowledge. In order to be able to provide the desired artifact and answer the paper’s research questions, knowledge about CC, SCM, and DES as well as their interrelations is needed. Such knowledge deficits can be investigated for instance by means of a literature search like it was conducted in the second section of this paper. The research outcome, the generic value network (cf. section 4) and the conceptualization of the cloud-based DES (cf. section 5) will be presented one after another. Herein, we will use the e³-method (Gordijn and Akkermans, 2001) as notation type.

Thereafter, the research outcome is evaluated in two ways (cf. section 6): through argumentative evaluation (Frank, 2006) and expert interviews (Cresswell, 2003). We conducted twelve semi-structured interviews with IT-experts from related business fields, all of them have at least two years of CC experience. Six of the IT-experts were from the SCM field of an industrial companies; three IT-experts are working for different CC service providers, and three IT-experts were from a SC simulation software company. All of them involved significant know-how and were able to contribute valuable feedback to the underlying paper. The interviews were conducted in December 2022 and took in average 45 minutes. With the approval of the interviewees, the interviews were audio-taped and transcribed by the researchers. The structure of the interviews consisted of three successively steps. In the first step, the questions covered the respective experiences of the interview partners with the CC and the SC network, their related job roles and their relationship amongst each other. In the second step, we included the presentation and discussion of our proposed value network. The IT-experts were also asked for their estimation of the value creation and the single value flows within an overall value network (cf. Figure 3). In the third step, we questioned the specific requirements for running such a value network (cf. section 5). In general, the valuable insights gained from the IT-experts led to an iterative construction of the paper.

Figure 2: Nested problem solving research approach (adopted from Wieringa, 2010)



4 ACTORS AND ROLES OF THE BUSINESS MODEL

We follow the business model definition by Timmers (1998). Herein, a business model includes (i) a description of the various business actors and their potential benefits, (ii) a description of the sources of revenues, and (iii) an architecture for the product, service, and/or information flows. In order to meet the conditions (i) and (ii) we use the e³-value method by Gordijn and Akkermans (2001). The third condition will particularly be specified in section 5. In general, the e³-value method is a semi-formal conceptual modeling method that recognizes the creation, exchange, and consumption of economically valuable objects in a multi-role network. Within this network, value is generated by providing services (related to cloud-based DES) that are valuable for other related par-

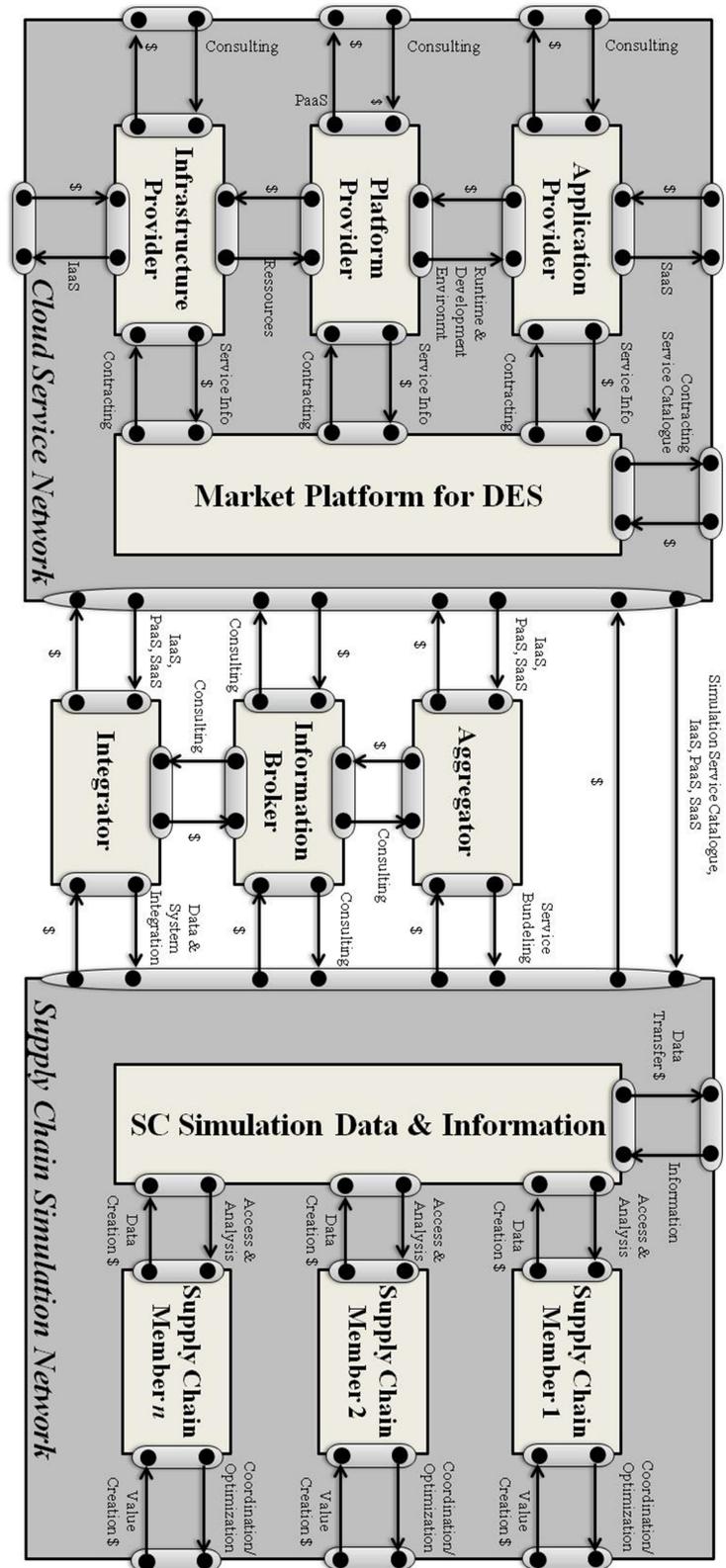
ties of the network. These services are exchanged in return of either money, which is the typical case, or other benefits that the participants value. Based on models by Leimeister et al. (2010) and Böhm et al. (2010), we extended the existing body of knowledge by combining the *value network of CC* with the *simulated value network of SCM*. In this context, it is important to mention that an actor may hold and act in various roles. Therefore, we take the abstracted viewpoint and speak of roles. In the following, we briefly discuss our understanding of the different roles emergent in the cloud-based DES ecosystem.

As mentioned before, CC literature generally differentiates between three service layers (Youseff et al., 2008; Mell and Grance, 2011; Marston et al., 2011), namely: infrastructure provider (IaaS), platform provider (PaaS), and application provider (SaaS). The *infrastructure provider* offers virtual hardware, network connections, and virtual storage for the cloud-based DES solution. The scalable nature of IaaS ensures enough infrastructure power, as additional machines can be instantiated on demand. The *platform provider* offers application programming interfaces and programming languages for developing, running, and testing DES software. And the *application provider* offers DES software via the web that runs on specific platforms and uses resources from the infrastructure provider. The modeling and simulation service can be perceived as a specific derivative of SaaS. The application provider ensures smooth operation of the DES software and provides new features and software improvements. The *market platform* constitutes a market place of different CC providers for SC customers, where suitable services may be combined. In addition, further services such as contracting, billing, and service level agreements may be offered to customers and providers (Leimeister et al., 2010; Walterbusch et al., 2014; Lang et al., 2021).

The *aggregator* is a DES cloud market expert, as he/she is able to aggregate various modular CC services into value-added DES-solutions in order to meet specific SC network requirements. Either the aggregator links existing services into a new service, or he/she adds value on top of a given service, creating certain features (Böhm et al., 2010). The *information broker* holds a central and trust-based position in our business model. The broker can provide a deep knowledge of the SC network's business processes and can recommend the SC network using adequate services. The broker offers analytical services to the SC members based on the respective accessible data. Herein, the broker acts as a mediator between the members in order to increase overall efficiency. The information broker has to ensure the fulfillment of all user requirements (cf. section 5.1). More details on the function of the information broker role will be outlined in section 5.4. Having found the right DES-service, the *integrator* helps to migrate data into the cloud and develops clear interfaces for a seamless interoperability between the SC members, the system, and the cloud-based DES.

Finally, the SC network obtains the DES services from the cloud. The network consists of the single *SC members*, whereby every member has to create certain data that is relevant for an adequate SC in the *simulation model*. The SC network does not create value within the cloud service ecosystem, nor does the SC network offer cloud services to other networks. All CC activities have to be paid by the network's members. In return, the gained information from the integrated DES simulation enable better coordination and optimization possibilities, which leads to value creation in the SCM ecosystem. The construction-oriented and literature-grounded business model is presented in figure 3. Herein, we extend the pre-existing body of knowledge by using existing business models (e.g., Böhm, 2010; Walterbusch et al., 2014) and breaking down their contained "user role" further into a linked network of users, namely the SC members.

Figure 3: Generic value network of cloud-based discrete event simulation



5 EMERGING CONCEPTUALIZATIONS OF THE CLOUD BASED DISCRETE EVENT SIMULATION

As mentioned before, the paper at hand focuses on requirements (*RQ2*), which have to be fulfilled in order to enable inter-company cloud-based DES, rather than presenting a specific and complete solution. Coming back to the presented business model's roles, research has investigated the requirements of the cloud service network (e.g., Marston et al., 2011; Hoberg et al., 2012; Denk et al., 2021) as well as for the aggregator and the integrator role (e.g., Leimeister et al., 2010). Hence, we will focus in particular on the SC members and specify the information broker role. The upcoming sub-sections discuss the requirements of the SC members, namely (i) security and trust, (ii) authorization concept, (iii) scenario analysis, (iv) buyer-supplier conflict, (v) coordination and collaboration, as well as (vi) financial benefits. The discussion of these aspects is grounded in scientific literature and augmented by the insights of IT-experts during the interview phase. Derived from the discussions we will present 12 research directions.

5.1 Requirements of supply chain members for participating the cloud-based DES

5.1.1 Security and trust

Even in the very beginning of CC, various early studies report that *security* risks and a lack of *trust* are the primary concerns when using cloud services (Marston et al., 2011; Zissis and Lekkas 2012; Venters and Whitley, 2012). However, there is a strong link between “ensuring security” and the lagging effect “trust formation”, which is critical for building and using cloud services (Walter et al., 2014; Walterbusch and Teuteberg, 2014; Alouffi et al., 2021). Even if the company's data that is transferred to the external provider is of “statistical nature” only, it may contain critical information with which SC competitors and other SC members may cause harm to the releasing company. Due to buyer-supplier conflicts, the SC members will certainly not share all their information with the related parties (e.g., information on production costs or resource utilization). Furthermore, compared with other encapsulated cloud services, the cloud-based DES trust issues are even more in the foreground, as by means of this service the SC members are brought together at a central place where they use the same data structures. This state of affairs makes it very interesting for SC members accessing and using unauthorized data. Hence, the cloud-based DES providers have to ensure secure data, information, and analytics. Looking at the business model, there is a trust issue of every SC member towards all cloud service providing parties, and there is a trust issue within the SC network between the members. Every SC member should be aware of who is providing which part of what service and at what security standards.

Following the “strategic network” understanding of Gulati et al., (2000), long term buyer-supplier partnerships might have higher degrees of trust within SC simulations. That is because traditional and latest literature argues that particularly strategic SC networks need to offer the potential to share risks, enforce knowledge building, and facilitate learning processes (Katz and Shapiro, 1985; Pashaei and Olhager, 2015; Rezapour et al., 2015; Alouffi et al., 2021). For further investigations of trust issues within the SC simulation network, there already exists a valuable and transferable knowledge base in literature (e.g., Kleijnen, 2005; Pashaei and Olhager, 2015). Nevertheless, more research is needed with respect to cloud-based DES as well as the special role of the information broker.

Research direction 1: How can the security concerns of SC members in the cloud-based DES be understood and decreased in order to increase the level of trust?

5.1.2 Authorization concept for simulation tools

After having determined the SC processes with the relevant parameters, the SC members have to transfer their data into the cloud. Herein, the SC member individually determines who should have access to what specific event data. With public CC usage, SC members normally suffer from limited control over their data (compared to running own IT systems). Hence, the cloud-based DES providers have to establish specific authorization concepts which ensure data confidentiality and data integrity. These authorization concepts should also include that the cloud service providers do not have access to the data of the SC members in order not to lower the level of trust in case of sensitive data (Li et al., 2011). In accordance with the separation of actors and roles in section 4, neither the DES providers (in all three layers) nor unrelated parties (e.g., competitors) should have access to a SC member's data. However, the data owners themselves can decide with whom they share their data. In other words, nobody in the SC has access to the data unless the data owner grants the access.

With cloud-based DES, there is an integrated simulation (cf. Figure 1), but it is not only one simulation for all members. Depending on their respective data access, the SC members may have separated fields of visible data. Hence, the integrated partial simulations run in parallel to each other and use data from each other so far as possible. Furthermore, it is of high interest for the SC network if there are potentials to carry out analytical evaluations for overall SCs using detailed data from different members, while still meet the limited data authorization of the individual members. Here, the authorization concept needs to ensure that the underlying model is not visible to the residual SC members and the “open” results do not allow statistical inference to unauthorized individual parameters. One way to increase the willingness for participation might be to consider relative changes, rather than absolute terms, e.g., financial values.

The research on CC provides diverse authorization concepts (e.g., Wang et al., 2010; Li et al., 2011; Li et al., 2010; Cao et al., 2014; Alouffi et al., 2021). We found the works by Zissis and Lekkas (2012), Zhao et al. (2010), and Khan et al. (2013) to be suitable for our purposes. Especially the work by Zhao et al. (2010) serves as a valuable basis for an authorization concept.

Research direction 2: How can an intelligent authorization concept (including instruments and tools) be created in order to increase trust and participation willingness of the related members and to facilitate statistically relevant SC network analysis?

5.1.3 Scenario analysis

The cloud-based DES should fulfill an adequate degree of “what-if analysis” and “how-to analysis” possibilities (Russel and Norvig, 2009, p. 337 ff.). Towards this end, what-if scenarios are useful for evaluating SC optimization initiatives. They facilitate the selection of best suited alternatives from a portfolio of possible SC modifications. In contrast, a how-to analysis starts with the desired outcome and determines the adequate structure of the SC and the underlying processes through “backward inference”. The optimization possibilities range from analyzing own data only (local optimization) to analyzing the entire SC across various members (global optimization).

Research direction 3: Which simulation environments, differentiating between individual parameters and overall statistical results from simulation models, are beneficial for improving local and global optimization possibilities?

If global optimization is envisaged, the various types of important and less important members may lead to a complete network simulation. However, due to the number of members added from tier level to tier level (Cooper et al., 1997a), the network becomes highly complex (Lambert et al., 2000) and overcrowded. It could be counterproductive, if not impossible, to involve and manage all process interactions with all members across the SC. It is crucial for the SC network to determine the critical members, processes and products (*simulation scope*), as well as the model’s level of detail.

Research direction 4: What are typical and useful simulation scopes in terms of intercompany analyses with respect to the potentials of cloud-based DES?

The interrelation between the security and trust requirement (cf. section 5.1.1) is obvious. Basically, every member has access to his/her own data and if authorized to foreign data. Even though the concept postulates an integrated DES, the degree of integration is determined by the single SC members. When the trust level is low, the data (if any) might suffer from low quality and infor-

mation sharing willingness might decrease. Research literature has impressively shown the importance between trust and information sharing (e.g., Prajogo and Olhager, 2012). Basically we hypothesize that the higher the trust and transparency willingness between the companies, the higher the information quality of the whole SC and the better the optimization possibilities. Moreover, the flexible and virtual nature of CC (Marston et al., 2011) with the standardized DES software enables easy addition of new members after the initial phase. It should also be possible to include adjoining members of the SC, which so far is modeled as a black box (cf. figure 1), in detail when providing respective data.

Research direction 5: How can the members’ trust be increased in order to also increase the transparency and the information sharing willingness in the cloud-based DES?

5.1.4 Considering the buyer-supplier conflict

As mentioned before, there is a pre-existent buyer-supplier conflict. Stern and Heskett (1969) proposed three classic types of conflict causes within SCs: (i) differences between members’ goals and objectives, (ii) disagreements over domain of decisions and actions, and (iii) differences in the perception of reality used in joined decision making. During the simulation phase, especially conflicts (i) may hinder members to join the CC service (e.g., customer wants the supplier to have a higher inventory stock for reducing lead times). When key members are missing in the simulation, it is much more difficult to run a global simulation and to achieve valuable results. If an important member in the middle of the SC (with direct upstream and downstream links to other important SC partners) declines to participate in the cloud-based DES simulation, the member might be modeled in the simulation chain as a black box, which means that the member’s processes are unknown. As the direct link is very important, also here statistics from historical data and further assumptions may be sufficient to fill the gap.

Research direction 6: How can a decline of members be handled, and what is the impact of declining members on the simulation results?

5.1.5 Coordination and collaboration

The next requirement is related to the interrelated fields of **coordination and collaboration**. In research literature, there is no doubt that the right degree of coordination and collaboration can bring competitive advantage to the related SC members (Cegielski et al., 2012; Demirkan and Delen, 2013). In terms of this paper, the intermediate outcome (cf. section 2) *cloud-based DES* may serve as a standardized platform for simulating advanced coordination and collaboration behaviors, which may help members to draw needful conclusions. Hence, the simulation tool might constitute a kind of training for coordination and collaboration interactions. This requirement may

have two linked dimensions, namely the technical and social coordination and collaboration. By means of the technical coordination and collaboration, we aim to improve the performance of the cross-company SC. From the social point a view, cloud-based DES may serve as a platform for discussions on common SC processes. Of course, this requirement cannot be seen loosely coupled from the prior mentioned requirements, as for instance a low level of trust within the SC network may hinder the collaboration intention.

Research direction 7: What is the impact of cloud-based DES on beliefs about collaboration and coordination initiatives in cross-company SCs?

Research direction 8: What is the impact of using cloud-based DES on real life collaboration and coordination in cross-company SCs?

5.1.6 Financial benefits

In the underlying business model we assume financial benefits for the SC members in terms of information acquisition through simulation analysis. Hence, the requirement is that the gained benefits of the SC network should overcompensate the costs for running such a cloud-based DES. At the same time we argue that the cloud-based DES might bring financial benefits to the cloud service network as well as to the integrator, the aggregator and the information broker, who all require compensation for their services. Herein, the SC network is the consumer of the obtained CC services and therefore, the SC network has to pay for the services as a customer.

However, the SC network is composed of various parties and thus does not represent a homogeneous unit. Therefore, the SC network needs to determine a fair allocation of the costs among the SC members, which is probably strongly linked to the expected benefits of the respective members. Moreover, it may occur that the overall SC can be improved by worsening single elements of related parties. The question of benefit allocation leads to game theoretical approaches (e.g., Colman, 1982; Myerson, 2013; Bharany et al., 2021; Greasley et al., 2022). It is unlikely that companies voluntarily simulate elements and share the data with others although they realize that the associated improvement of the overall SC will only come to effect when they put themselves at a disadvantage. Therefore, it is necessary to reach respective agreements that regulate such circumstances in advance. Hence, this might be a game theory issue with the dimensions of sharing a certain degree of data with others (including the information broker) on the one side and the allocation of expected benefits (such as compensation payments to the directly disadvantaged members) on the other side. It is also possible to aim pareto-efficient solutions only (evaluated by the information broker), in order to encourage companies for joining cloud-based DES simulation network.

Research direction 9: Have the value flows in the business model been considered correctly? How can the specific value proposition of provider related services as well as the specific SC member related gains be evaluated and how can respective financial benefits be allocated?

5.2 The role of the information broker

The idea of an information broker has been known for many years in scientific literature. Considering the description of the role, many classic papers define an information broker to be a trusted intermediary who conducts validation and evaluation in order to provide highly specific information (Boss, 1979; Niehans 1980; Budgen et al., 2007). The term information broker attracted great attention in the financial service industry in the 1980s (Niehans 1980; Ramakrishnan and Thakor, 1984). From the financial perspective, Niehans (1980, p. 167) stated that an information broker might bring borrowers and lenders together at lower costs than if the related parties would have made direct transactions. In this paper, we propose to transfer the basic logic on a cloud-based DES, meaning that the intermediation function might increase the efficiency in the SC processes. Acknowledging Porter's (1985) value chain model (cf. section 2) and in order to achieve an efficient reconfiguration, it is needed to define the related strategic units, to identify critical activities, to define the critical items, and to determine the values of SC processes. Thus, this may constitute a procedure guideline for the information broker.

Research direction 10: How can the information broker be involved in an adequate manner?

The information broker is a neutral institution without own simulated SC processes. The broker's basis is the access to authorized data from SC members. The broker's incentive is an upfront defined service provision. As mentioned before, the cloud-based DES is an integrated simulation, where many interrelated simulations can be run in parallel, exchanging authorized data. This constitutes the local simulation analysis. As the information broker is a neutral institution, the global simulation analysis can be achieved when all members authorize the broker for all their data, meaning that the broker can run an overall and complete simulation. From a theoretical point of view, the broker is interested in optimizing the SC as a whole, which in an extreme case may disadvantage some members or events while the overall SC is benefitting. This leads to the already defined future research question of allocating the gains to the related SC members effectively. We associate four major functions with the information broker whereby the first two have company specific characters and the last two cross-company characters.

Firstly, prior research has shown that companies often tend to create an incomplete and/or incorrect picture of their SC processes due to restricted knowledge (Zee and

Vorst, 2005; Cimino et al., 2010). Hence, the broker with adequate expertise *validates the defined cloud-based DES pre-conditions* such as parameters or simulated processes for every SC member and provides the members with support for building models and experimentation plans. Along with that, the broker could make suggestions which key figures of the simulation experiments will be published for which members such that all authorization restrictions are met in case that data is needed from more than one participant of a SC. Within the validation, the broker may assist at the iterative reformulation of the simulation statistics and proposes alternative statistics that might provide additional, needful information and might better meet the member's real world requirements.

Secondly, the information broker helps to *discover inefficiencies in the SC of a member* by analyzing processes via simulation experiments. Here, the information broker has to bear in mind the overall SC performance, which means that every company-specific optimization may have an influence on other members. Solving this conflict represents one of the future research directions. In general, discovering inefficiencies requires a deep understanding of the real underlying processes. In this function, the broker demonstrates opportunities for improvement for every member.

Thirdly, the information broker *investigates the cross-company interactions* and the impacts of the single elements on the whole SC. The broker thereby acts as neutral mediator between the related members and gives explanations of the rationale for the relevance of information, clustered by more or less related members.

And finally, the information broker may encourage the *negotiation between the members* in order to increase the overall SC efficiency. This negotiation is related to authorization/control issues as well as to adjustments of simulated processes. With regards to the authorization concept, the negotiation process is a dynamic interaction in which the broker might assist two members in order to increase their intercompany transparency (if this transparency is beneficial from the overall perspective).

Research direction 11: What is the impact of the information broker on beliefs about successful reconfiguration of cross-company SCs?

Research direction 12: What is the influence of the information broker on the ongoing participation activities in the cloud-based DES?

6 EVALUATION

The "nested problem solving" research approach constitutes a design science problem (cf. section 3). Research literature describes many evaluation methods for design

science such as observational methods, analytical methods, experimental methods, or descriptive methods (e.g., Hevner et al., 2004). However, Frank (2006) noted that enough time is needed to allow innovative artefacts to be accepted by practice, which means that the evaluation of research approaches is often left to practice. Notwithstanding, the research approaches should be evaluated in an academic context during the early development phases as well. As already mentioned we carried out twelve interviews with IT-experts from related research fields (cf. section 3 for the three step interview procedure). Further, we used an argumentative descriptive way for indicating the validity of the paper.

The interviewees pointed out the pre-existing buyer-supplier conflict and emphasized the ongoing strong demand for suitable collaboration and simulation tools as proposed in our research approach. The experts agree that this paper proposes a new and promising business model for reengineering this issue. According to their assumptions, the benefit of creating these useful links to other companies in the SC via the cloud-based DES might lead to operational cost reductions and service improvements towards the end customers as well as resilience. The experts' deep practical background led to valuable contributions and iterative adjustments during the conceptual phase of the paper (determining relations and value flows in figure 3 and deriving specific requirements in section 4). In general, they indicated the validity of the generic model by emphasizing its clear and semantically correct structure. Moreover, the experts found the model to have reference character, namely by providing broad application possibilities and enforcing the understanding for the important link between CC and DES.

From the descriptive evaluation point of view, we follow Frank (2006) by assuming that validity of research is given, when three postulates are fulfilled: abstraction, originality, and justification. From the abstraction view point, the business model represents aggregated structures that focus on the determined requirements for running the cloud-based DES. With regard to originality, the new composition of the three different fields CC, SCM, and DES with predefined goals (cf. research questions in section 1) can be characterized as a novel approach. With respect to justification, we followed a methodologically sound research approach (cf. figure 2) and developed a plausible argumentative framework for running such an inter-organizational cloud-based DES.

7 CONCLUSION

It is not the intention of this article to present a complete cloud-based DES solution, as this research field is still in its infancy. We rather propose a first conceptual business model that benefits SC networks as well as the cloud service industry. Furthermore, we aimed to identify and investigate some critical issues within that constellation in order to enforce the development in this promising en-

deavor. In the upcoming sub-sections, we first summarize the main contributions of our work, then we discuss the limitation, and finally we structure the already mentioned future research directions.

7.1 Contributions to theory and practice

Although the numerous advantages of cross-company SC simulations are evident, analytical simulation tools that can exploit those advantages are scarce so far due to the complexity inherent in integrated simulation modeling. Furthermore, an adequate usage of DES is even today quite expensive when running company-specific simulations. Especially smaller companies with limited resources could experience a kind of technological breakthrough. CC has been established as the most flexible delivery service of providing IT. The scalability advantage of CC allows the cloud-based DES to be very detailed with further advantages concerning the overall runtime for experiments (Rosetti and Chen, 2012). CC is a predestinated basis for building a common simulation network with strong demands on expert knowledge, such as for DES. Furthermore, CC enforces the standardization process of DES by providing the same service to the whole SC network, which leads to harmonizing and simplifying cross-company simulations. However, combining the advantages of CC with the advantages of DES brings up a new business model that has so far not been studied in depth. Therefore, this paper takes a first step by systematically bringing together the cloud service network with the SC network, explaining major actors and roles. Furthermore, we outline the main requirements for a cloud-based DES for distributed cross-company SCs.

Within the presented business model, the information broker, also known to be useful in many other disciplines, has to ensure the validity of the simulated SC network and may constitute the key advantage in the SC network by acting as an intermediary in the optimization process. From an academic point of view, our business model framework has a strong impact, but also on practical business issues it has a major influence. We have no doubt that our concept constitutes a relevant part towards the need of “affordable analytics for the masses” (Demirkan and Delen, 2013).

7.2 Limitations

Considering the evaluation phase of the underlying research approach (section 3), we gained some first insights on value creation and value flow within our business model from the experts interviews. However, it is not yet possible to generate a comprehensive evaluation of the business model. As the proposed business model is a novel theoretical approach, the model is not in place in real life and the benefits are only assumed by the experts. Moreover, the provided underlying artifacts have not tested so far. Therefore, future research needs to investigate this business model in more depth and on a broader empirical basis. Further, the requirements may serve as

general guidelines that have more conceptual character rather than application-ready instructions. Furthermore, we would like to add a general limitation of simulation models by stating that no simulation can involve all managerial real-world SC issues, because many soft facts such as individual behavior can hardly be modeled correctly.

7.3 Summarizing future research

As this paper provides a more generic concept, there is a great and fruitful basis for future, more detailed research in various related fields. During the construction process of this paper, various open research fields appeared which we mentioned in section 5 and which we structured into a research agenda (Melville, 2010) in table 1. We clustered the questions with the help of the *belief-action-outcome* framework of Melville (2010).

Table 1: Research agenda

Phenomena	Research questions	Recomm. research methods
Belief	<ul style="list-style-type: none"> Research direction 1: How can the security concerns of SC members in the cloud-based DES be understood and decreased in order to increase the level of trust? Research direction 7: What is the impact of cloud-based DES on beliefs about collaboration and coordination initiatives in cross-company SCs? Research direction 11: What is the impact of the information broker on beliefs about successful reconfiguration of cross-company SCs? 	Expert interviews, surveys, case studies, participative observation
Action	<ul style="list-style-type: none"> Research direction 3: Which simulation environments, differentiating between individual parameters and overall statistical results from simulation models, are beneficial for improving local and global optimization possibilities? Research direction 5: How can the members' trust be increased in order to also increase the transparency and the information sharing willingness in the cloud-based DES? Research direction 4: What are typical and useful simulation scopes in terms of intercompany analyses with respect to the potentials of cloud-based DES? Research direction 6: How can a decline of members be handled, and what is the impact of declining members on the simulation results? Research direction 2: How can an intelligent authorization concept (including instruments and tools) be created in order to increase trust and participation willingness of the related members and to facilitate statistically relevant SC network analysis? Research direction 10: How can the information broker be involved in an adequate manner? 	Action research, prototyping, simulations, field and lab experiments,
Outcome	<ul style="list-style-type: none"> Research direction 8: What is the impact of using cloud-based DES on real life collaboration and coordination in cross-company SCs? Research direction 9: Have the value flows in the business model been considered correctly? How can the specific value proposition of provider related services as well as the specific SC member related gains be evaluated and how can respective financial benefits be allocated? Research direction 12: What is the influence of the information broker on the ongoing participation activities in the cloud-based DES? 	Action research, field and lab experiments, expert interviews, surveys

REFERENCES

- Cordeau, Laporte, et. al. "Vehicle Routing", aus Barnhart, Laporte (Eds.), *Handb. in Operations Research & Management Science*, Vol. 14, Chapter 6, Elsevier 2007
- Toth, Vigo, "An Overview of Vehicle Routing Problems" aus Toth, Vigo (Ed.) *The Vehicle Routing Problem*, Siam, 2002
- Agalianos, Ponis, Aretoulaki, Plakas, Efthymiou, "Discrete event simulation and digital twins: review and challenges for logistics", *Procedia Manufacturing*, 51, 1636-1641, 2020
- Ahmed, Akhuzada, Whaiduzzaman, Gani, Ab Hamid, Buyya, "Network-centric performance analysis of runtime application migration in mobile cloud computing", *Simulation Modelling Practice and Theory*, 50, 42-56, 2015
- Alouffi, Hasnain, Alharbi, Alosaimi, Alyami, Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies", *IEEE Access*, 9, 57792-57807, 2021
- Bharany, Sharma, Khalaf, Abdulsahib, Al Humaimeedy, Aldhyani, Alkahtani, "A systematic survey on energy-efficient techniques in sustainable cloud computing", *Sustainability*, 14(10), 6256, 2022
- Böhm, Koleva, Leimeister, Riedl, Krcmar, "Towards a generic value network for cloud computing. in: *Economics of Grids, Clouds, Systems, and Services*", Springer, Berlin Heidelberg, 129-140, 2010
- Boss, "The Library as an Information Broker", *College and Research Libraries*, 40(2), 136-40, 1979
- Brailsford, Hilton, "A Comparison of Discrete Event Simulation and System Dynamics for Modelling Healthcare Systems", *Proceedings of the 26th meeting of the ORAHS Working Group 2000*, Glasgow, Scotland, 18-3, 2001
- Budgen, Rigby, Brereton, Turner, "A data integration broker for healthcare systems", *IEEE Computer*, 40(4), 34-41, 2007
- Cao, Wang, Li, Ren, Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data", *IEEE Transactions on Parallel and Distributed Systems*, 25(1), 222-233, 2014
- Carter, Rogers, "A framework of sustainable supply chain management: moving toward new theory", *International journal of physical distribution & logistics management*, 38(5), 360-387, 2008
- Chatterjee, "Delivering desired outcomes efficiently: The creative key to competitive strategy", *California Management Review*, 40(2), 78-95.
- Chen, Drezner, Ryan, Simchi-Levi, "Quantifying the bullwhip effect in a simple supply chain: The impact of forecasting, lead times, and information", *Management science*, 46(3), 436-443, 2000
- Cegielski, Jones-Farmer, Wu, Hazen, "Adoption of cloud computing technologies in supply chains: An organizational information processing theory approach", *The International Journal of Logistics Management*, 23(2), 184-211, 2012
- Chien, Kuo, "Beyond make-or-buy: cross-company short-term capacity backup in semiconductor industry ecosystem", *Flexible Services and Manufacturing Journal*, 25(3), 310-342, 2013
- Cimino, Longo, Mirabelli, "A general simulation framework for supply chain modeling: state of the art and case study", *International Journal of Computer Science Issues*, 7(2), 1-9, 2010
- Colman, "Game theory and experimental games: The study of strategic interaction", Pergamon Press, Fairview Park, NJ, 1982
- Cooper, Ellram, Gardner, Hanks, "Meshing Multiple Alliances", *Journal of Business Logistics*, 18(1), 67-89, 1997a
- Cooper, Lambert, Pagh, "Supply chain management: more than a new name for logistics", *The International Journal of Logistics Management*, 8(1), 1-13, 1997b
- Cresswell, "Research Design: Qualitative, Quantitative and Mixed Research Methods", Sage, London, UK, 2003
- Demirkan, Delen, "Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud", *Decision Support Systems*, 55(1), 412-421, 2013
- Deng, Wang, , Teo, Song, "Organizational agility through outsourcing: Roles of IT alignment, cloud computing and knowledge transfer", *International Journal of Information Management*, 60, 102385, 2021
- Dorsch, Hackel, "Integrating business partners on demand: the effect on capacity planning for cost driven support processes", in: *45th Hawaii International Conference on System Science (HICSS)*, IEEE, 4796-4805, 2021
- El Khatib, Alhosani, Alhosani, Al Matrooshi, Salami, "Simulation in Project and Program Management: Utilization, Challenges and Opportunities", *American Journal of Industrial and Business Management*, 12(4), 731-749, 2022
- Fishman, "Discrete-event simulation: modeling, programming, and analysis", Springer Science and Business Media, New York, 2001
- Frank, "Towards a Pluralistic Conception of Research Methods in Information Systems Research", *ICB-Research Report No. 7*, University Duisburg-Essen, 2006
- Golrizgashti, Hosseini, Zhu, Sarkis, "Evaluating supply chain dynamics in the presence of product deletion",

- International Journal of Production Economics, 255, 108722, 2023
- Gordijn, Akkermans, "E3-value: Design and Evaluation of e-Business Models". IEEE Intelligent Systems, 16(4), 11-17, 2001
- Gulati, Nohria, Zaheer, "Strategic networks", Strategic Management Journal, 21(3), 203-215, 2000
- Gutenschwager, Alicke, "Supply Chain Simulation mit ICON-SimChain", Spengler, T., Voss, S., Kopfer, H. (Eds.), Logistik Management, Physica, Heidelberg, Germany, 161-178, 2004
- Greasley, Edwards, "Enhancing discrete-event simulation with big data analytics: A review", Journal of the Operational Research Society, 72(2), 247-267, 2021
- Handfield, Nichols, "Introduction to Supply Chain Management", Upper Saddle River, Prentice Hall, NJ, 1999
- Hazen, Byrd, "Toward creating competitive advantage with logistics information technology", International Journal of Physical Distribution & Logistics Management, 42(1), 8-35, 2021
- Hevner, March, Park, Ram, "Design science in information systems research", MIS quarterly, 28(1), 75-105, 2004
- Hoberg, Wollersheim, Krcmar, "The Business Perspective on Cloud Computing - A Literature Review of Research on Cloud Computing", Proceedings of the 18th American Conference on Information Systems (AMCIS), Seattle, Washington, 2021
- Huang, Lau, Mak, "The impacts of sharing production information on supply chain dynamics: A review of the literature", International Journal of Production Research, 41(7), 1483-1517, 2003
- Katz, Shapiro, "Network externalities, competition, and compatibility", American Economic Review, 75(3), 424-440, 1985
- Keller, König, "A Reference Model to Support Risk Identification in Cloud Networks", Proceedings of the 35th International Conference on Information Systems, Auckland, New Zealand, 2014
- Khan, Mat Kiah, Khan, Madani, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, 29(5), 1278-1299, 2013
- Kleijnen, "Supply chain simulation tools and techniques: a survey", International Journal of Simulation and Process Modelling, 1(1), 82-89, 2005
- Kuechler, Vaishnavi, "Promoting relevance in IS research: an informing system for design science research", International Journal of an Emerging Transdiscipline, 14(1), 125-138, 2011
- Lambert, Cooper, Pagh "Supply chain management: Implementation issues and research opportunities", International journal of logistics management, 9(2), 1-20, 1998
- Lang, Reggelin, Müller, Nahhas, "Open-source discrete-event simulation software for applications in production and logistics: An alternative to commercial tools?", Procedia Computer Science, 180, 978-987, 2021
- Law, Kelton, "Simulation Modeling & Analysis", 3rd Ed., McGraw-Hill, 2000
- Leimeister, Boehm, Riedl, Krcmar, "The Business Perspective of Cloud Computing: Actors, Roles and Value Networks", Proceedings of the 18th European Conference on Information Systems (ECIS), Pretoria, South Africa, 2010
- Li, Wang, Wang, Cao, Ren, Lou, "Fuzzy keyword search over encrypted data in cloud computing", Proceedings of the 29th Conference on Computer Communications, IEEE, San Diego, CA, 1-5, 2010
- Li, Yu, Cao, Lou, "Authorized private keyword search over encrypted data in cloud computing", 31st International Conference on Distributed Computing Systems (ICDCS), IEEE, 383-392, 2011
- Lidberg, Aslam, Pehrsson, Ng, "Optimizing real-world factory flows using aggregated discrete event simulation modelling: Creating decision-support through simulation-based optimization and knowledge-extraction", Flexible Services and Manufacturing Journal, 32(4), 888-912, 2020
- Longo, Mirabelli, Padovano, Solina, "The Digital Supply Chain Twin paradigm for enhancing resilience and sustainability against COVID-like crises", Procedia Computer Science, 217, 1940-1947, 2023
- Mansouri, Ghafari, Zade, "Cloud computing simulators: A comprehensive review", Simulation Modelling Practice and Theory, 104, 102144, 2020
- Marston, Li, Bandyopadhyay, Zhang, Ghalsasi, "Cloud computing - The business perspective", Decision Support Systems, 51(1), 176-189, 2011
- Martens, Zarvić, Teuteberg, Thomas, "Designing a risk-based partner selection process for collaborative cloud computing environments", Proceedings of the 4th International Workshop on Enterprise Modelling and Information Systems Architectures (EMISA), LNI 190, 237-242, 2011
- Meer, Dutta, Datta, "A cost-based database request distribution technique for online E-commerce applications", MIS Quarterly, 36(2), 479-507, 2021
- Mell, Grance, "The NIST definition of cloud computing", available at: http://pre-developer.att.com/home/learn/enablingtechnologies/The_NIST_Definition_of_Cloud_Computing.pdf, 2011

- Melman, Parlikad, Cameron, "Balancing scarce hospital resources during the COVID-19 pandemic using discrete-event simulation", *Health Care Management Science*, 24(2), 356-374, 2021
- Melville, "Information systems innovation for environmental sustainability", *MIS Quarterly*, 34(1), 1-21, 2010
- Mentzer, DeWitt, Keebler, Min, Nix, Smith, Zacharia, "Defining supply chain management", *Journal of Business Logistics*, 22(2), 1-25, 2001
- Meyr, Wagner, Rohde, "Structure of advanced planning systems", in: Stadler, H., Kilger, C. (Eds.), *Supply Chain Management and Advanced Planning—Concepts, Models Software and Case Studies*, Springer, Berlin, 99-104, 2002
- Min, Zhou, "Supply chain modeling: past, present and future", *Computers & Industrial Engineering*, 43(1), 231-249, 2002
- Mintzberg, "Patterns of Strategy Formulation", *Management Science*, 24(9), 934-948, 1987
- Myerson, "Game theory", Harvard university press, 2013
- Niehans, "Theory of money", John Hopkins University Press, Baltimore, 167-180, 1980
- Oliver, Webber, "Supply chain management: logistics catches up with strategy", in: Christopher, M. (Ed.), *Logistics: The Strategic Issues*, Chapman & Hall, London, UK, 63-75, 1992
- Owen, "Selection of simulation tools for improving supply chain performance", Doctoral Diss. Aston University, 2013
- Pan, Mason, Matar, "Data-centric Engineering: Integrating simulation, machine learning and statistics. Challenges and opportunities", *Chemical Engineering Science*, 249, 117271, 2022
- Pashaei, Olhager, "Product architecture and supply chain design: A systematic review and research agenda", *Supply Chain Management: An International Journal*, 20(1), 98-112, 2015
- Pereira, "The new supply chain's frontier: Information management", *International Journal of Information Management*, 29(5), 372-379, 2009
- Porter, "Competitive Advantage", The Free Press, NY, 1985
- Prajogo, Olhager, "Supply chain integration and performance: The effects of long-term relationships, information technology and sharing, and logistics integration", *International Journal of Production Economics*, 135(1), 514-522, 2012
- Ramakrishnan, Thakor, "Information reliability and a theory of financial intermediation", *The Review of Economic Studies*, 51(3), 415-432, 1984
- Rezapour, Zanjirani Farahani, Fahimnia, Govindan, Mansouri, "Competitive closed-loop supply chain network design with price-dependent demands", *Journal of Cleaner Production*, 93, 251-272, 2015
- Ridall, Bennet, Tipi, "Modeling the dynamics of supply chains", *International Journal of Systems Science*, 31(8), 969-976, 2000
- Robinson, "Simulation – The practice of model development and use", Palgrave Macmillan, 2004
- Rosetti, Chen, "Cloud Computing Architecture for Supply Chain Network Simulation", Winter Simulation Conference, Berlin, Germany, 1-12, 2012
- Russel, Norvig, "Artificial Intelligence: A Modern Approach (3rd Edition)", Prentice Hall, Englewood Cliffs, NJ, 2009
- Saratchandra, Shrestha, "The role of cloud computing in knowledge management for small and medium enterprises: a systematic literature review", *Journal of Knowledge Management*, 2022
- Siebers, Aickelin, "A First Approach on Modelling Staff Proactiveness in Retail Simulation Models", *Journal of Artificial Societies and Social Simulation*, 14(2), 1-25, 2011
- Swafford, Ghosh, Murthy, "The antecedents of supply chain agility of a firm: scale development and model testing", *Journal of Operations Management*, 24(2), 170-88, 2006
- Sweeney, Grant, Mangan, "The implementation of supply chain management theory in practice: an empirical investigation", *Supply Chain Management: An International Journal*, 20(1), 56-70, 2015
- Sweetser, "A Comparison of System Dynamics and Discrete Event Simulation", Proceedings of 17th International Conference of the System Dynamics Society (ICSDS), Wellington, New Zealand, 1999
- Stern, Heskett, "Conflict Management in interorganizational relations", *Distribution channels*, Boston, MA, 1969
- Tako, Robinson, "The application of discreteevent simulation and system dynamics in the logistics and supply chain context", *Decision Support Systems*, 52(4), 802-815, 2012
- Terzi, Cavaliere, "Simulation in the supply chain context: a survey", *Computers in industry*, 53(1), 3-16, 2004
- Timmers, "Business models for electronic markets", *Electronic markets*, 8(2), 3-8, 1998
- Tönnissen, Teuteberg, "Analysing the impact of block-chain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. *International Journal of Information Management*. 52, S. 101953, 2020

- Turner, Hutabarat, Oyekan, Tiwari, “Discrete event simulation and virtual reality use in industry: new opportunities and future trends”, *IEEE Transactions on Human-Machine Systems*, 46(6), 882-894, 2016
- Venters, Whitley, “A critical review of cloud computing: researching desires and realities”, *Journal of Information Technology*, 27(3), 179-197, 2012
- Walter, Öksüz, Walterbusch, Teuteberg, Becker, “May I help You? Increasing Trust in Cloud Computing Providers through Social Presence and the Reduction of Information Overload”, *Proceedings of the 35th International Conference on Information Systems (ICIS)*, Auckland, New Zealand, 2014
- Walterbusch, Teuteberg, “Towards an Understanding of the Formation and Retention of Trust in Cloud Computing: A Research Agenda, Proposed Research Methods and Preliminary Results”, *Proceedings of the 11th International Conference on Trust, Privacy & Security in Digital Business*, Munich, Germany, 2014
- Walterbusch, Truh, Teuteberg, “Hybride Wertschöpfung durch Cloud Computing”, Thomas, O., Nüttgens, N., (Eds.), *Dienstleistungsmodellierung*, Springer, Berlin, 155-174, 2014
- Wang, Cao, Li, Ren, Lou, “Secure ranked keyword search over encrypted cloud data”, *30th International Conference on Distributed Computing Systems (ICDCS)*, 253-262, 2010
- Webster, Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review”, *MIS Quarterly*, 26(2), xiii–xxiii, 2002
- Wieland, Durach, “Two perspectives on supply chain resilience”, *Journal of Business Logistics*. 42 (3), 315–322, 2021
- Wieringa, “Relevance and problem choice in design science” in: Winter, R., Zhao, J.L., Aier, S., (Eds.), *Global Perspectives on Design Science Research*, Springer, Berlin, 61-76., 2010
- Willis, Jones, “Multi-objective simulation optimization through search heuristics and relational database analysis”, *Decision Support Systems*, 46(1), 277-286, 2008
- Zee, Vorst, “A modeling framework for supply chain simulation: Opportunities for improved decision making”, *Decision Sciences*, 36(1), 65-95, 2005
- Zee, “Building insightful simulation models using Petri Nets - A structured approach”, *Decision Support Systems*, 51(1), 53-64, 2011
- Youseff, Butrico, Da Silva, “Toward a unified ontology of cloud computing”, *Grid Computing Environments Workshop (GCE)*, Austin, Texas, 2008
- Zhao, Rong, Li, Zhang, Tang, “Trusted data sharing over untrusted cloud storage providers”, *Proceedings of the 2nd International Conference on Cloud Computing Technology and Science*, IEEE, 97-103, 2010
- Zissis, Lekkas, “Addressing cloud computing security issues”, *Future Generation Computer Systems*, 28(3), 583-592, 2012

Anomaly Detection im Monitoring des Produktivbetriebs der ODAV AG anhand der Analyse der Error-Count Metrik

Benjamin Eder (M.Sc.)

ODAV AG

Gesellschaft für Informatik und Telekommunikation
Ernst-Heinkel-Str. 11, 94315 Straubing, Germany

E-Mail: b.eder@odav.de

Benjamin Neumann (Dipl.-Inf. (FH))

ODAV AG

Gesellschaft für Informatik und Telekommunikation
Ernst-Heinkel-Str. 11, 94315 Straubing, Germany

E-Mail: b.neumann@odav.de

Professor Dr. Frank Herrmann

Ostbayerische Technische Hochschule Regensburg
Innovationszentrum für Produktionslogistik
und Fabrikplanung

Galgenbergstraße 32, 93053 Regensburg, Germany
E-Mail: frank.herrmann@oth-regensburg.de

SCHLÜSSELWÖRTER

Anomaly Detection, Machine Learning

ABSTRAKT

Viele Firmen entwickeln Software und stellen diese auch gleichzeitig dem Kunden auf Servern bereit. Da es nötig ist, dass der Betrieb der Software 24 Stunden am Tag sieben Tage die Woche gewährleistet wird, soll ein System entwickelt werden, das Anomalien automatisch im Betrieb der Server erkennt und dies einer entsprechenden Stelle, wie zum Beispiel dem betreibenden Rechenzentrum, meldet.

1 EINLEITUNG

Da viele Firmen selbst entwickelte Software den Kunden auch bereitstellen, zum Beispiel in einem eigenen Rechenzentrum, wird es auch immer wichtiger sicherzustellen, dass die Software für den Kunden 24 Stunden am Tag sieben Tage die Woche zur Verfügung steht. Somit werden Systeme benötigt, die überwachen, ob die Server erreichbar sind und die Software funktionsfähig ist.

Deshalb soll am Beispiel der ODAV AG (ODAV AG, Gesellschaft für Informatik und Telekommunikation 1969), die zur Bereitstellung ihrer Software ein eigenes Rechenzentrum betreibt, ein System entwickelt werden, das Anomalien automatisch im Produktivbetrieb erkennen kann und damit die aktuelle manuelle Methode optimiert. Anomalien beschreiben dabei Muster in Daten, die nicht mit einer genau definierten Vorstellung von normalem Verhalten übereinstimmen (Chandola, Banerjee und Kumar 2009). Diese können aus verschiedenen Gründen in den Daten auftreten, zum Beispiel durch böswillige Aktivitäten wie Cyber-Angriffe und terroristische Aktivitäten oder durch Systemausfälle.

Zur Entwicklung des Systems werden zunächst in Abschnitt 2 die Probleme, die mithilfe des Systems gelöst werden sollen, definiert. Anschließend wird in

Abschnitt 3 ein Konzept erarbeitet, wie solche Anomalien am besten erkannt werden können. Anhand dieses Konzeptes soll dann in Abschnitt 4 ein System implementiert werden, das die Anomalien erkennt und entsprechend verantwortliche Personen im Falle einer Anomalie benachrichtigt. Schließlich soll in Abschnitt 5 evaluiert werden, wie das implementierte System die Abläufe in der Firma beeinflusst.

2 PROBLEMSTELLUNG

Im aktuellen Produktivbetrieb der ODAV AG (ODAV AG, Gesellschaft für Informatik und Telekommunikation 1969) werden Logmeldungen aus dem Produktivsystem gesammelt, jedoch nicht weitergehend automatisch analysiert. Die Probleme, die anhand der Analyse der Logmeldungen gelöst werden sollen, werden in Abschnitt 2.2 erläutert. Zunächst soll jedoch in Abschnitt 2.1 erläutert werden, wie das Produktivsystem aktuell aufgebaut ist.

2.1 Aktueller Aufbau des Produktivsystems

Das Produktivsystem für alle Kunden ist mit Kubernetes (The Kubernetes Authors 2014), einem System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerbasierten Anwendungen, aufgebaut. Darin sind alle Anwendungen als Container bereitgestellt, sodass die Kunden auf diese zugreifen können.

Die Logmeldungen dieser Anwendungen werden in einem Elasticsearch Server (Elasticsearch B.V. 2010), einer verteilten Such- und Analyse-Engine, gesammelt und für mindestens sechs Monate datenschutzkonform gespeichert. Eine Meldung kann dabei immer einem bestimmten Zeitpunkt zugeordnet werden. Zudem wird zwischen verschiedenen Typen unterschieden: *Info*, *Warn* und *Error*.

Im Folgenden bezeichnet die *Error-Count Metrik* die Anzahl der Logmeldungen des Typs *Error* innerhalb eines bestimmten Zeitintervalls. Das Zeitinter-

vall wird hier und im Folgenden als die vergangenen fünf Minuten definiert.

2.2 Probleme im bestehenden System

Im aktuellen Produktivsystem sind die folgenden Probleme vorhanden. Diese sollen zunächst erfasst werden, um im Verlauf der Arbeit entsprechend bearbeitet werden zu können.

a. Erkennen von Angriffen auf das System

Ein Angreifer kann mittels eines Brute-force Angriffes (Dave 2013) versuchen, sich Zugang zu den Anwendungen zu verschaffen. Dies kann beispielsweise geschehen, indem er versucht, das Passwort eines Benutzers, dessen Anmelde-name er kennt, zu erraten, was im Authentifizierungs-server zu fehlgeschlagenen Authentifizierungs-versuchen führt, die als Fehler erfasst werden.

Im aktuellen System können Angriffe durch die Firewall der Firma verhindert werden. Diese erkennt einen Angriff dadurch, dass viele Zugriffe innerhalb einer bestimmten Zeitspanne auf einen Port erfolgen. Die Erkennung erfolgt damit auf der Netzwerkebene entsprechend des Sieben-Schichten-Modells (Day und Zimmermann 1983). Problematisch dabei ist, dass die Firewall auch alarmieren könnte, wenn viele Benutzer gleichzeitig auf die Systeme zugreifen, da diese nicht erkennt, ob ein Zugriff einen Fehler verursacht oder nicht. Ein Problem ist somit, dass kein System existiert, das einen Angriff auf Applikationsebene erkennt.

b. Erkennen von ausgefallenen Anwendungen

Viele Anwendungen im Produktivsystem stellen Schnittstellen für andere Anwendungen zur Verfügung. Diese Schnittstellen können jedoch aus verschiedensten Gründen temporär nicht erreichbar sein. So können zum Beispiel Container, in denen die Client- und Serveranwendungen bereitgestellt werden, abgestürzt sein. Auch können die Anwendungen selbst in einen kritischen Fehler gelaufen sein und funktionieren deshalb nicht mehr. Tritt ein solcher Fall ein, können die entsprechenden Schnittstellen nicht mehr erreicht werden. Dies führt auf Seite der aufrufenden Anwendungen zu Fehlern, welche im Elasticsearch Server erfasst werden.

Im aktuellen Überwachungssystem wird eine Fehlermeldung angezeigt, sollte ein Pod über einen längeren Zeitraum nicht erreichbar sein. Um einen reibungslosen Betrieb aller Systeme zu gewährleisten, sollte dies automatisiert innerhalb kurzer Zeit angezeigt werden. Ein Problem des Systems ist somit, dass ausgefallene Anwendungen nicht sofort erkannt werden.

c. Erkennen von ausgefallenen Nodes

Das Kubernetes-Cluster der Firma besteht aus mehreren Nodes, welche zusammen alle Anwendungen bereitstellen. Eine Node ist dabei eine virtuelle oder physische Maschine (The Kubernetes Authors 2014). Nun kann jedoch eine oder mehrere Nodes unerwartet ausfallen, was darin resultiert, dass einige Anwendungen nicht mehr verfügbar sind. Ist dies der Fall, versucht das Kubernetes System zunächst, die Anwendungen der ausgefallenen Node(s) auf die restlichen zu verteilen, was jedoch unter Umständen die Antwortzeiten der Anwendungen verlangsamt und im schlimmsten Fall einen Timeout bei einer anfragenden Anwendung erzeugt. Auch kann es passieren, dass die vorhandenen Ressourcen der restlichen Nodes nicht ausreichen, um die ausgefallenen Anwendungen bereitzustellen. Dies führt dazu, dass einige Anwendungen eventuell gar nicht mehr verfügbar sind, was wiederum zu Fehlern bei anfragenden Anwendungen führt.

Im aktuellen Überwachungssystem wird eine Fehlermeldung angezeigt, sollte eine Node über einen längeren Zeitraum nicht erreichbar sein. Um einen reibungslosen Betrieb aller Systeme zu gewährleisten, sollte dies automatisiert innerhalb kurzer Zeit angezeigt werden. Ein Problem ist somit, dass ausgefallene Nodes im Kubernetes Cluster erst nach einiger Zeit erkannt werden.

Die genannten Probleme sollen durch das im Folgenden beschriebene Lösungskonzept vermieden werden.

3 LÖSUNGSKONZEPT

Zunächst soll kurz erläutert werden, was *Anomaly Detection* (Chandola, Banerjee und Kumar 2009) ist und wie dies im Allgemeinen im aktuellen System eingesetzt werden kann. Anschließend soll sowohl ein simpler Ansatz als auch ein weiterer mithilfe von Machine Learning konzipiert werden. Dabei werden verschiedene Modelle für das Problem erstellt und erläutert. Schließlich sollen die erarbeiteten Ansätze miteinander verglichen werden, um den besten Ansatz aus diesen auszuwählen und in einem Überwachungssystem umzusetzen.

3.1 Einsatz von Anomaly Detection

Die Erkennung von Anomalien, genannt *Anomaly Detection*, bezieht sich auf das Problem, Muster in Daten zu finden, die nicht dem erwarteten Verhalten entsprechen (Chandola, Banerjee und Kumar 2009). Dabei resultieren aus Anomalien in einer Vielzahl von Anwendungsbereichen bedeutende und oft kritische Informationen, die genutzt werden können. Bezogen auf diese Definition soll im Produktivsystem

der Verlauf der *Error-Count Metrik* auf Muster untersucht werden, die während eines normalen Betriebes des Systems nicht erwartet werden. Dafür muss zunächst definiert werden, wie die erfassten Daten auszusehen haben, damit diese miteinander verglichen werden können.

Im Folgenden besteht der Verlauf eines Tages aus 288 Datenpunkten, die die Daten der *Error-Count Metrik* des entsprechenden Tages darstellen. Diese Datenpunkte werden in einem Graphen dargestellt, wobei $t = 0$ den *Error-Count* um fünf Minuten nach Mitternacht des entsprechenden Tages abbildet. Dies ist so gewählt, damit der Verlauf eines Tages nur Fehlermeldungen berücksichtigt, die auch an diesem Tag aufgetreten sind. Abbildung 1 stellt einen unauffälligen Verlauf an einem Arbeitstag dar.

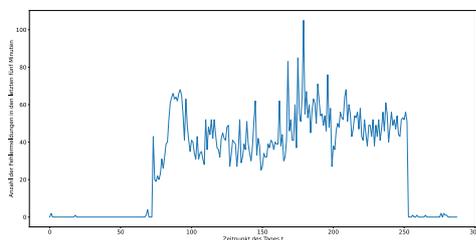


Abbildung 1: Unauffälliger Verlauf der *Error-Count Metrik* an einem Arbeitstag

Eine Anomalie ist für die vorliegenden Daten, wenn ein Datenpunkt deutlich höher angesiedelt ist als die restlichen Datenpunkte. Im Verlauf aus Abbildung 1 wäre dies zum Beispiel der Fall, wenn innerhalb von fünf Minuten mehr als 150 Fehlermeldungen eingegangen wären. Da das Maximum dieses Tages bei ungefähr 100 Fehlermeldungen pro fünf Minuten liegt, wäre dies eine Abweichung von 50 Prozent. Dies weist auf eine mögliche Störung im System hin.

Da die durchschnittlichen Verläufe der Tage abhängig vom Wochentag anders ausfallen, werden die Daten nach Wochentag gruppiert analysiert. Dies wird bei allen Ansätzen berücksichtigt.

3.2 Einfache Anomaly Detection

Zunächst soll ein simples Konzept zur *Anomaly Detection* entwickelt werden. Dabei wird ein Grenzwert erstellt, der während des Produktivbetriebes nicht überschritten werden darf. Auf einen unteren Grenzwert wird verzichtet, da bei allen in Abschnitt 2.2 genannten Szenarien die Anzahl der Fehlermeldungen ansteigt.

Ein Ansatz dafür ist das Errechnen eines Grenzwertes anhand der Verläufe vorheriger gleicher Wochentage. Mit D_i als die Datenpunkte des Wochentages vor i Wochen, errechnet sich der Grenzwert g wie folgt:

$$g(n) = \left(\frac{\sum_{i=1}^n Q_{0,9}(D_i)}{n} \right) \cdot 1,25 \quad (1)$$

Wie in Gleichung 1 zu erkennen ist, werden für die Berechnung des Grenzwertes die Daten der letzten n Wochen verwendet. Aus den Daten der jeweiligen Tagesverläufe wird das 90-Prozent-Quantil gebildet. Dies wurde gewählt, damit einzelne höhere Werte, die eine Anomalie anzeigen könnten, nicht berücksichtigt werden. Anschließend wird der Mittelwert der Quantile errechnet. Um einen Toleranzbereich zu erzeugen, wird dieser Wert schließlich um 25 Prozent erhöht. Bei mehreren Versuchen mit verschiedenen Werten, bei denen für dieselben Tagesverläufe die Grenzwerte errechnet wurden, stellte sich dieser Wert als bester heraus, da mit diesem die meisten Anomalien erkannt werden.

Der errechnete Grenzwert g wird nun für den aktuellen Tag zur *Anomaly Detection* verwendet. Dabei wird die *Error-Count Metrik* für den aktuellen Arbeitstag periodisch gegen dessen Grenzwert geprüft. Dieser Grenzwert ist dabei konstant für einen bestimmten Arbeitstag. Sollte zu irgendeinem Zeitpunkt der *Error-Count* größer als der Grenzwert sein, so wird dies als Anomalie angenommen.

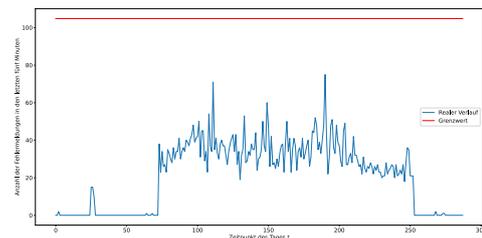


Abbildung 2: Prüfung eines vollständigen Arbeitstages gegen dessen Grenzwert

In Abbildung 2 ist ein Beispiel für die Prüfung gegen den Grenzwert dargestellt. Die blaue Kurve stellt dabei die *Error-Count Metrik* des Arbeitstages dar und die Gerade den Grenzwert für diesen Arbeitstag. Der Grenzwert beträgt in diesem Beispiel ungefähr 105 Fehlermeldungen pro fünf Minuten und wurde anhand der Daten der vorausgegangenen sechs Wochen berechnet. Die Werte während des Tages überschreiten diesen zu keinem Zeitpunkt, weshalb dieser Tag als unauffällig eingestuft werden würde. Jedoch ist zu Beginn des Tages, als die Werte noch nahezu null betragen, ein kleiner Ausschlag zu erkennen. Obwohl dort eine hohe Wahrscheinlichkeit für eine Anomalie vorliegt, da außerhalb der regulären Arbeitszeiten der Kunden kaum Fehlermeldungen auftreten sollten, wird dieser Ausschlag nicht erkannt.

Als Problem stellt sich dabei heraus, dass der Grenzwert auf den Peaks der vorhergehenden Tage

basiert. Dies führt dazu, dass bei der Berechnung des Grenzwertes lediglich die hohen Werte einfließen und somit der Grenzwert die geringere Anzahl von Fehlermeldungen außerhalb der regulären Arbeitszeiten nicht beachtet.

3.3 Anomaly Detection mit Machine Learning

Ein weiterer Ansatz zur *Anomaly Detection* ist, Machine Learning Modelle zu verwenden, um mithilfe dieser die Anomalien zu erkennen. Im Folgenden sollen verschiedene Modelle vorgestellt werden, wie dies im vorliegenden Fall umgesetzt werden könnte. Zunächst werden jedoch noch allgemeine Bedingungen definiert, die bei der Konzeption aller Modelle gelten.

Für alle Modelle stehen die Daten von acht Monaten zur Verfügung, mit denen diese trainiert werden. Die vorhandenen Daten sind für alle Modelle gleich. Das Trainieren eines Modells bezieht sich hier darauf, dass ein Algorithmus entwickelt wird, der, wie der Mensch auch, mit der Zeit und mit Erfahrung besser in einer bestimmten Aufgabe wird (Ketkar und Santana 2017).

Um die Modelle trainieren zu können, werden die Daten vor dem eigentlichen Training aufbereitet. Dabei werden diese zunächst nach Wochentag aufgeteilt, damit für jeden Wochentag ein separates Modell erstellt werden kann. Da die durchschnittlichen Verläufe an den verschiedenen Wochentagen unterschiedlich sind, hat dies den Vorteil, dass die Daten eines Wochentages die Vorhersagen der anderen Wochentage nicht beeinflussen. An dieser Stelle ist zu erwähnen, dass dies auch zu erreichen wäre, indem man den Wochentag als weitere Eingabe neben den Datenpunkten verwendet, was in diesem Paper jedoch nicht weitergehend analysiert wird.

Anschließend werden die Daten so aufbereitet, dass die Modelle als Eingabe den Verlauf eines Tages erhalten, also 288 Datenpunkte. Um einen einzelnen Tagesverlauf für die kommende Woche der erhaltenen Daten vorherzusagen, erhält das Modell als anzustrebende Ausgabe den Verlauf des Tages in der folgenden Woche. Somit hat das Modell als Ausgabe ebenfalls 288 Datenpunkte. Letztlich wird das letzte Datenpaar aus den Trainingsdaten entfernt und als Testdatum verwendet, das beim Trainingsprozess des Modells nicht berücksichtigt wird.

Als Vergleich wird bei beiden Modellen anhand des Testdatenpaares der Verlauf eines Tages vorhergesagt. Da im späteren Betrieb die Tagesverläufe dem Modell nicht bekannt sind, wie zum Beispiel die Verläufe des Testdatenpaares, kann damit ein Verlauf vorhergesagt werden, wie er auch im späteren Betrieb vorhergesagt werden würde. Dieser Verlauf wird mit dem tatsächlichen Verlauf des Tages verglichen.

Als erste Variante kann dabei eine Kurve abgeleitet werden, die die euklidische Distanz zwischen dem vorhergesagten und dem realen Verlauf dar-

stellt. Diese wird dabei verwendet, da sie die Differenz zwischen dem vorhergesagten und dem realen Wert an einem bestimmten Zeitpunkt darstellt und so die Vorhersage direkt mit dem realen Wert verglichen wird. Anhand der Kurve der euklidischen Distanz soll dann vorhergesagt werden, ob eine Anomalie vorliegt. Dabei wird der *Training Loss* des entsprechenden Modells als Grenzwert für die Werte der euklidischen Distanz am aktuellen Tag verwendet. Überschreitet die Distanz zwischen Vorhersage und realem Wert zu irgendeinem Zeitpunkt diesen Grenzwert, wird dies als Anomalie angenommen. Ein Vorteil dieser Variante ist, dass sowohl der Grenzwert als auch die euklidische Distanz zwischen Vorhersage und realem Wert schnell berechnet werden können. Ein Nachteil dabei ist, dass der errechnete Grenzwert konstant für den ganzen Tag ist.

Eine zweite Variante zur Vorhersage einer Anomalie ist die Festlegung eines Grenzwertes für den *Error-Count*. Dabei werden alle vorhergesagten Werte für den aktuellen Tag um einen gewissen Prozentsatz erhöht, um einen Toleranzbereich zu erzeugen. In mehreren Versuchen wurden für dieselben Tage mehrere Grenzwerte mit verschiedenen Toleranzbereichen errechnet. Bei einem Prozentsatz von 50 Prozent stellte sich dabei heraus, dass mit diesem Wert die meisten Anomalien erkannt wurden. Die dadurch entstehende Kurve dient schließlich als Grenzwert. Es existiert in diesem Falle ein separater Grenzwert für jeden Zeitpunkt des Tages. Überschreitet der reale Wert den zum Zeitpunkt gehörigen Grenzwert, wird dies als Anomalie angenommen. Ein Vorteil dieser Variante ist, dass der Grenzwert schnell berechnet werden kann. Ein Nachteil ist, dass der Grenzwert theoretisch an manchen Stellen null betragen könnte und somit bereits eine Fehlermeldung zur Meldung einer Anomalie führen könnte.

3.3.1 Modell: Autoregressiv

Zunächst soll ein autoregressives Modell vorgestellt werden. Die dabei verwendeten Werte und Funktionen wie die Anzahl der Schichten, die Anzahl der Neuronen pro Schicht, die Aktivierungsfunktion, die Anzahl der Trainingsepochen, der Optimizer, die *Learning Rate* sowie die *Loss Function* sind dabei in verschiedenen Versuchen verändert und getestet worden. Mit den im Folgenden beschriebenen Werten und Funktionen erzielt das Modell die besten Ergebnisse, weshalb diese letztlich auch verwendet werden.



Abbildung 3: Architektur des erstellten autoregressiven Modells

In Abbildung 3 ist die Architektur dieses Modells dargestellt. Es benötigt als Eingabe 288 Datenpunk-

te und erhält dafür die Daten eines vollständigen vergangenen Tages. Die Daten werden anschließend in drei *Hidden Layer* (Ketkar und Santana 2017), alle Schichten vor der Ausgabeschicht, weitergegeben. In diesem Modell sind dies drei *Dense Layer*. Dies sind Schichten, bei denen alle Neuronen mit den Neuronen der vor- und nachgelagerten Schicht vollständig vernetzt sind. Die erste Schicht enthält 512, die zweite 1024 und die dritte wieder 512 Neuronen. Als Aktivierungsfunktion wird bei allen drei Schichten die *hyperbolische Tangensfunktion*

$$f(x) = \tanh(x)$$

verwendet. Alternativ könnte hier auch die Rectified Linear Unit (ReLU) als Aktivierungsfunktion verwendet werden. Während der Konzeption konnte jedoch festgestellt werden, dass mit dieser die Vorhersagen teilweise nur einen konstanten Wert lieferten und somit nicht verwendet werden konnten. Die Ausgabeschicht besteht ebenfalls aus einem *Dense Layer* mit 288 Neuronen und erzeugt damit eine Ausgabe von 288 Datenpunkten, die den Verlauf der *Error-Count Metrik* für den Tag in der folgenden Woche beschreibt.

Das Trainieren des Modells erfolgt in 100 Epochen. Dabei wird der *Adam Optimizer* verwendet, da dies die gängigste Methode ist. Dessen *Learning Rate* wird in Abhängigkeit der aktuellen Trainingsepoche festgelegt. Die Funktion dafür ist wie folgt definiert, wobei e die aktuelle Epoche repräsentiert:

$$lr(e) = \begin{cases} 0,1 & \text{falls } e < 50 \\ 0,01 & \text{sonst} \end{cases} \quad \text{mit } e \in [0, 99] \quad (2)$$

Wie in Gleichung 2 zu erkennen ist, ist die *Learning Rate* in den ersten 50 Epochen des Trainings mit 0,1 definiert. Anschließend wird sie für die restlichen Epochen auf 0,01 verringert. Als *Loss Function* für den Trainingsprozess wird der *Mean Squared Error*

$$\sum_{i=1}^n (y - \hat{y})^2 \quad (3)$$

verwendet, da dieser in solchen Modellen ein Standardvorgehen ist.

Vorhersage im Vergleich zum realen Verlauf

In Abbildung 5a ist die Vorhersage des Modells im Vergleich zum realen Verlauf der *Error-Count Metrik* dargestellt. Der Tag ist dabei der gleiche wie in Abschnitt 3.2.

Es ist zu erkennen, dass der vorhergesagte Verlauf über den ganzen Tag hinweg etwas höher ist als der reale Verlauf. Dies liegt jedoch unter anderem daran, dass die Fehlermeldungen in den Wochen zuvor etwas höher waren, vor allem zu den Zeiten vor und nach Arbeitsbeginn der Kunden. Diese sind hingegen auch

in der Vorhersage gut zu erkennen und werden vom Modell berücksichtigt. Ebenfalls kann man die zwei Peaks im realen Verlauf in der Vorhersage erkennen.

Was beim realen Verlauf auffällt, ist der Ausschlag am frühen Morgen, der im Folgenden als Anomalie definiert wird.

Euklidische Distanz Wie in Abschnitt 3.1 beschrieben, soll zunächst mithilfe der euklidischen Distanz versucht werden, Anomalien zu erkennen. Dabei wird die euklidische Distanz zwischen einem Punkt in der Vorhersage und dem realen Wert zu diesem Zeitpunkt errechnet. Mit D_R als den realen Verlauf und D_P als den vorhergesagten Verlauf sowie D_R^i und D_P^i als den Werten aus dem jeweiligen Verlauf zum Zeitpunkt i , wird die Funktion zur Berechnung der euklidischen Distanz in Abhängigkeit zum Zeitpunkt wie folgt definiert:

$$e(i) = |D_R^i - D_P^i| \quad \text{mit } i \in [0, 288[\quad (4)$$

Die euklidische Distanz wird nun anhand der Funktion aus Gleichung 4 für alle Zeitpunkte berechnet. Schließlich muss noch ein Grenzwert gewählt werden. Dieser gibt an, wie hoch die euklidische Distanz zu einem Zeitpunkt maximal sein darf, und wird anhand des finalen *Training Loss* des Modells (*loss*) berechnet. Der Grenzwert wird definiert als:

$$g = \frac{loss}{288} \cdot 2 = \frac{loss}{144}$$

Im vorliegenden Beispiel ergibt dies einen Grenzwert von 76. Die Distanzen der Verläufe im hier verwendeten Beispiel sind zu keinem Zeitpunkt größer als der Grenzwert. Somit würde diese Methode die vorliegende Anomalie im Beispiel nicht erkennen.

Oberer Grenzwert

Als weitere Methode soll, wie in Abschnitt 3.1 beschrieben, ein oberer Grenzwert für den realen Verlauf festgelegt werden, der jedoch nicht konstant, sondern abhängig vom Zeitpunkt definiert sein soll. Mit D_P als den vorhergesagten Verlauf und D_P^i als den Wert zum Zeitpunkt i , soll die Funktion zur Berechnung des Grenzwertes wie folgt definiert werden:

$$g(i) = D_P^i \cdot 1,5 \quad \text{mit } i \in [0, 288[\quad (5)$$

Der Grenzwert wird anhand der in Gleichung 5 definierten Funktion errechnet und mit den Werten des realen Verlaufs aus dem vorliegenden Beispiel verglichen. Dabei stellt diese Methode eine Anomalie an zwei Zeitpunkten des Tages fest. Diese Zeitpunkte sind zwischen 02:05 und 02:10 Uhr und entsprechen dem Ausschlag in den frühen Morgenstunden, der in Abbildung 5a zu erkennen ist. Somit stellt diese Methode korrekt eine Anomalie im vorliegenden Beispiel fest.

3.3.2 Modell: LSTM

Als weitere Variante soll ein Modell auf Basis von Long Short-Term Memory (LSTM) (Ketkar und Santana 2017) erstellt werden. Wie in Abschnitt 3.3.1 geschildert werden auch hier die Werte und Funktionen verwendet, mit denen in verschiedenen Versuchen die besten Ergebnisse erzielt wurden.

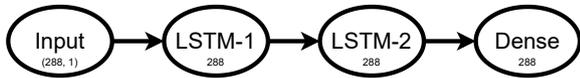


Abbildung 4: Architektur des erstellten LSTM Modells

Abbildung 4 stellt die Architektur des Modells dar. Es erhält als Eingabe 288 Datenpunkte, jedoch müssen hier alle Datenpunkte als Array übergeben werden. Somit ist die Eingabe ein zweidimensionales Array, welches 288 Einträge besitzt, die wiederum jeweils einen Eintrag beinhalten. Die Eingabe ist der Verlauf der *Error-Count Metrik* eines vollständigen vergangenen Tages. Als *Hidden Layer* werden zwei *LSTM Layer* verwendet, die jeweils aus 288 Neuronen bestehen. Die Ausgabeschicht besteht aus einem *Dense Layer* mit 288 Neuronen. Diese erzeugt damit die Vorhersage für den Tag in der folgenden Woche.

Das Trainieren des Modells erfolgt bei diesem Modell mit 100 Epochen. Dabei wird der *Adam Optimizer* verwendet, dessen *Learning Rate* abhängig von der Epoche festgelegt wird. Dafür wird die Funktion aus Gleichung 2 verwendet. Als *Loss Function* wird der *Mean Squared Error* (vgl. Gleichung 3) verwendet.

Vorhersage im Vergleich zum realen Verlauf

In Abbildung 5b ist die Vorhersage des Modells im Vergleich zum realen Verlauf der *Error-Count Metrik* dargestellt. Der Tag ist dabei der gleiche wie in Abschnitt 3.2.

Vergleicht man die beiden Vorhersagen in Abbildung 5, so stellt man fest, dass die Vorhersage des autoregressiven Modells aus Abschnitt 3.3.1 fast identisch ist mit der Vorhersage des LSTM Modells. Somit treffen alle Aussagen zum Vergleich des vorhergesagten zum realen Verlauf, die für das autoregressive Modell zutreffen, auch für das LSTM Modell zu.

Euklidische Distanz Zunächst soll mithilfe der euklidischen Distanz versucht werden, Anomalien zu erkennen. Dabei wird die euklidische Distanz anhand der in Gleichung 4 definierten Funktion berechnet.

Da die vorhergesagten Verläufe des autoregressiven und des LSTM Modells fast identisch sind, ergeben sich auch für die euklidischen Distanzen fast dieselben Werte. Da die Eingabedaten für beide Modelle gleich sind, ist auch der *Training Loss* bei beiden Modellen annähernd gleich, da diese fast identische Ausgaben erzeugen. Somit ist der Grenzwert

identisch zum autoregressiven Modell. Dadurch erkennt auch das LSTM Modell mit dieser Methode keine Anomalie im vorliegenden Beispiel.

Oberer Grenzwert Als weitere Methode soll ein oberer Grenzwert für den realen Verlauf festgelegt werden. Dieser wird anhand der in Gleichung 5 definierten Funktion in Abhängigkeit zum Zeitpunkt berechnet.

Der errechnete Grenzwert ist aufgrund der fast identischen Vorhersage des autoregressiven und LSTM Modells ebenfalls annähernd gleich. Somit erkennt das LSTM Modell mit dieser Methode die Anomalie korrekt im vorliegenden Beispiel an den zwei Zeitpunkten am frühen Morgen.

3.4 Vergleich der Ansätze

Um entscheiden zu können, welcher der Ansätze für die Implementierung verwendet werden soll, werden die verschiedenen Ansätze miteinander verglichen. Dabei soll hinsichtlich folgender Aspekte der beste Ansatz ermittelt werden:

a. Berechnungszeit

Die Implementierung soll den Ansatz schnell berechnen können, damit Anomalien sofort und zuverlässig erkannt werden. Der wöchentliche Trainingsprozess kann dabei auch mehrere Minuten benötigen, jedoch muss eine Vorhersage in maximal zehn Sekunden erfolgen.

b. Genauigkeit

Der Ansatz soll aufkommende Anomalien zuverlässig erkennen können, damit die Ausfälle aufgrund von Anomalien reduziert werden.

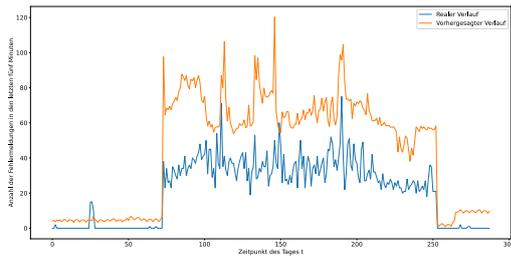
c. Komplexität

Die Implementierung des Ansatzes soll leicht verständlich sein, damit der Quellcode von anderen Entwicklern ohne größere Vorkenntnisse betreut werden kann. Dadurch wird die Wartbarkeit des Systems verbessert.

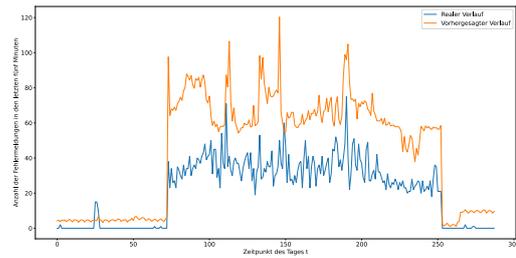
3.4.1 Einfacher Ansatz

Zunächst soll der einfache Ansatz (3.2) hinsichtlich der genannten Punkte analysiert werden.

Berechnungszeit Beim einfachen Ansatz wird ein Grenzwert wie in Gleichung 1 definiert berechnet. Zeitkritisch wäre dabei lediglich die Errechnung des Quantils, da jedoch die Anzahl der Datenpunkte, über der das Quantil errechnet wird, immer gleich ist, erfolgt die Berechnung des Grenzwertes in konstanter Zeit. Auch die Erkennung von Anomalien erfolgt in konstanter Zeit, da dies nur durch einen Vergleich des realen Wertes mit dem Grenzwert erfolgt.



(a) Vorhersage: Autoregressives Modell



(b) Vorhersage: LSTM Modell

Abbildung 5: Vorhersagen der Modelle im Vergleich zum realen Verlauf

Genauigkeit Überschreitet der *Error-Count* den üblichen Peak der letzten Wochen, so erkennt dies das Modell, was während des Arbeitstages die meisten Anomalien abdeckt. Tritt jedoch eine kleinere Anomalie auf, vor allem zu Zeiten, in denen das System nicht aktiv verwendet wird, wie zum Beispiel früh morgens, so wird dies vom einfachen Ansatz nicht erkannt, wie im Beispiel in Abschnitt 3.2 zu erkennen ist. Da außerhalb der regulären Arbeitszeiten solche kleineren Anomalien oft auftreten können, ist dies ein Nachteil dieses Ansatzes.

Komplexität Der einfache Ansatz beruht lediglich auf mathematischen Berechnungen, die in jeder Programmiersprache umzusetzen sind. In *Python* (vanRossum 1995) existiert zum Beispiel eine Bibliothek *NumPy* (Oliphant 2006), in der viele mathematische Operationen bereits implementiert sind. Dadurch kann dieser Ansatz einfach und verständlich implementiert werden.

3.4.2 Autoregressiver Ansatz

Als nächstes sollen die genannten Punkte beim autoregressiven Ansatz (3.3.1) analysiert werden.

Berechnungszeit Der autoregressive Ansatz basiert auf dem wöchentlichen Training eines autoregressiven Modells und dessen Vorhersagen. Für das Beispiel in Abschnitt 3.3.1 hat das Modell pro Epoche 0,2 Sekunden benötigt, für den gesamten Trainingsprozess 19,5 Sekunden. Für eine Vorhersage benötigt das Modell 0,1 Sekunden. Da die Rechenleistung im Produktivsystem, in dem die Implementierung später umgesetzt wird, stärker ist als die Leistung des Rechners, auf dem die Beispiele trainiert wurden, kann davon ausgegangen werden, dass diese Zeiten in der späteren Umsetzung tendenziell geringer sind.

Die Errechnung der euklidischen Distanz zum realen Wert mit der Funktion aus Gleichung 4 erfolgt in konstanter Zeit, ebenso wie die Errechnung des Grenzwertes. Die Erkennung von Anomalien geschieht in konstanter Zeit mit einem Vergleich.

Beim oberen Grenzwert erfolgt die Berechnung dieses ebenfalls in konstanter Zeit mit der Funktion aus Gleichung 5, da der Grenzwert immer aus 288 Datenpunkten besteht. Auch hier ist die Erkennung der Anomalie lediglich ein Vergleich und erfolgt somit in konstanter Zeit.

Sowohl die Prüfung mithilfe der euklidischen Distanz als auch mit dem oberen Grenzwert haben auf dem Entwicklungsrechner weniger als eine hundertstel Sekunde benötigt. Somit kann für beide Varianten angenommen werden, dass die Prüfung einer Anomalie ungefähr der Vorhersagezeit des Modells entspricht.

Genauigkeit Mit der euklidischen Distanz können höhere Abweichungen des *Error-Count* erkannt werden. Jedoch muss hier die Abweichung um einen gewissen absoluten Wert höher sein als der vorhergesagte Wert, um als Anomalie eingestuft zu werden. Dies führt dazu, dass kleinere Anomalien wie früh morgens im Beispiel nicht erkannt werden.

Beim oberen Grenzwert wird ein relativer Toleranzbereich errechnet, der überschritten werden darf, womit größere Abweichungen gut erkannt werden. Aber auch kleinere Abweichungen können so wie im Beispiel erkannt werden, da bei einer geringeren Anzahl zu erwartender Fehlermeldungen der Toleranzbereich niedriger ausfällt.

Komplexität Das autoregressive Modell kann nicht in jeder Programmiersprache implementiert werden. Für die Beispiele wurde dafür die Bibliothek *Keras* (Ketkar und Santana 2017) verwendet, welche zum Beispiel in *Python* verwendet werden kann. Die Erstellung des Modells gestaltet sich dabei recht simpel, da die Architektur des Modells aus Abbildung 3 übernommen werden kann. Die Berechnungen zur Erkennung einer Anomalie können ebenfalls einfach in *Python* umgesetzt werden. Somit kann dieser Ansatz verständlich implementiert werden, jedoch sollte ein Entwickler Vorkenntnisse im Bereich *Machine Learning* (Ketkar und Santana 2017) haben.

3.4.3 LSTM Ansatz

Nun soll der LSTM Ansatz anhand der genannten Punkte (3.3.2) analysiert werden.

Berechnungszeit Für diesen Ansatz wird wöchentlich ein LSTM Modell trainiert und dessen Vorhersage analysiert. Für das Beispiel in Abschnitt 3.3.2 hat das Modell 3,3 Sekunden pro Epoche und insgesamt 328,2 Sekunden benötigt. Eine Vorhersage dauert 1,0 Sekunden.

Für die Erkennung der Anomalie, sowohl mit der euklidischen Distanz als auch mit dem oberen Grenzwert, benötigt dieser Ansatz dieselbe Zeit wie der autoregressive Ansatz. Auch die Zeiten für die Prüfung mit den verschiedenen Varianten verhalten sich gleich.

Genauigkeit Da, wie in Abbildung 5 zu erkennen ist, die Vorhersagen des autoregressiven und des LSTM Modells fast identisch sind, ist die Genauigkeit sowohl für die euklidische Distanz als auch den oberen Grenzwert wie beim autoregressiven Ansatz.

Komplexität Wie auch das autoregressive Modell, kann das LSTM Modell mit *Keras* (Ketkar und Santana 2017) implementiert werden. Die Erstellung des Modells kann dabei anhand der Abbildung 4 erfolgen, jedoch gestaltet sich dies etwas komplexer als beim autoregressiven Modell. Die Berechnungen zur Erkennung von Anomalien sind gleich komplex wie beim autoregressiven Ansatz.

3.4.4 Wahl des besten Ansatzes

Abschließend soll anhand der analysierten Kriterien gewählt werden, welches der beste Ansatz ist, der dann realisiert werden soll. Um die Ansätze vergleichen zu können werden jedem Ansatz für jedes analysierte Kriterium Punkte von null bis fünf vergeben. Für die Realisierung ist es am wichtigsten, dass die Genauigkeit des Ansatzes möglichst gut ist.

Die Bewertungen der verschiedenen Ansätze sind in Tabelle 1 dargestellt. Anhand dieser soll nun das beste Modell ermittelt werden.

Der einfache Ansatz hat sowohl eine sehr schnelle Berechnungszeit als auch eine sehr geringe Komplexität, weshalb er in beiden Aspekten fünf Punkte erhält. Jedoch ist die Genauigkeit im Vergleich zu den anderen Ansätzen recht gering, weshalb er für diesen Aspekt nur zwei Punkte erhält.

Die Berechnungszeit und die Komplexität des autoregressiven Ansatzes sind ebenfalls recht schnell und einfach, jedoch etwas langsamer und komplexer als der einfache Ansatz, weshalb dieser jeweils vier Punkte für diese Aspekte erhält. Dafür ist die Genauigkeit mit diesem Ansatz höher als mit dem einfachen. Der Ansatz mit dem oberen Grenzwert erzielt

dabei bessere Ergebnisse als derjenige mit der euklidischen Distanz, jedoch sind beide nicht optimal. Darum erhält der Ansatz mit dem oberen Grenzwert vier, mit der euklidischen Distanz drei Punkte für die Genauigkeit.

Für den LSTM Ansatz werden zwei Punkte für die Berechnungszeit vergeben, da diese deutlich länger ist als die der beiden anderen Ansätze. Da auch die Komplexität höher ist als beim autoregressiven Ansatz, werden hierfür drei Punkte vergeben. Die Genauigkeit ist aufgrund der fast identischen Ergebnisse gleich zu bewerten wie beim autoregressiven Ansatz.

Betrachtet man die Bewertungen der Ansätze, so kann festgestellt werden, dass die Genauigkeit beim einfachen Ansatz niedriger ist als bei den anderen Ansätzen. Da die Genauigkeit das wichtigste Kriterium für die Realisierung ist, wird dieser Ansatz nicht verwendet. Bei den Machine Learning Ansätzen ist die Genauigkeit bei den Ansätzen mit der euklidischen Distanz niedriger als bei den Ansätzen mit dem oberen Grenzwert. Da sowohl die Berechnungszeit als auch die Komplexität beim autoregressiven Ansatz besser sind als beim Ansatz mit LSTM, wird im Folgenden der autoregressive Ansatz mit dem oberen Grenzwert für die Realisierung verwendet.

4 REALISIERUNG

Nach der Konzipierung mehrere Ansätze soll nun ein System erstellt werden, das mithilfe des besten Ansatzes die Anomalien im Produktivbetrieb erkennt. Dafür soll zunächst die Architektur des Systems sowie die Umsetzung der verwendeten Skripte erklärt werden. Anschließend wird dargestellt, wie das System im Produktivsystem bereitgestellt wird.

4.1 Architektur des Systems

Zunächst soll die Architektur des zu implementierenden *Anomaly Detection* Systems erklärt werden. Diese ist in Abbildung 6 dargestellt.

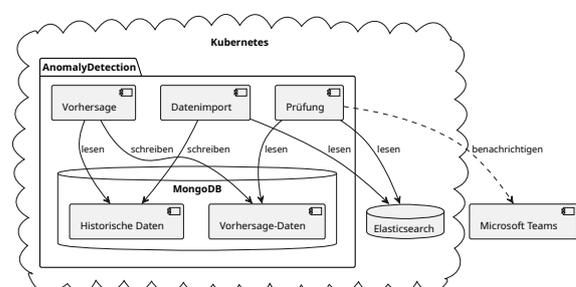


Abbildung 6: Architektur des *Anomaly Detection* Systems

Das *Anomaly Detection* System selbst besteht aus vier Komponenten und benutzt zusätzlich zwei externe Komponenten. Die erste externe Komponente

Ansatz	Genauigkeit	Berechnungszeit	Komplexität
Einfacher	2	5	5
Autoregressiver / euklidische Distanz	3	4	4
<i>Autoregressiver / oberer Grenzwert</i>	<i>4</i>	<i>4</i>	<i>4</i>
LSTM / euklidische Distanz	3	2	3
LSTM / oberer Grenzwert	4	2	3

Tabelle 1: Bewertungen der verschiedenen Ansätze

ist dabei der Elasticsearch Server (Elasticsearch B.V. 2010), der als Datenbank für alle vergangenen Fehlermeldungen agiert. Die zweite ist der Microsoft Teams Server (Ilag und Sabale 2022) der Firma.

Alle Daten im System selbst werden in einer MongoDB (Bradshaw, Brazil und Chodorow 2019) gespeichert, die hauptsächlich aus zwei Komponenten, in diesem Fall Datensammlungen, besteht. Die erste enthält die aufbereiteten Daten aus dem Elasticsearch Server, die zweite die vorhergesagten Verläufe für jeden Tag.

Die Funktionalität des Systems ist auf drei Komponenten aufgeteilt. Dabei existiert zunächst die Datenimport-Komponente, die historische Daten aus dem Elasticsearch Server liest, aufbereitet und in die MongoDB schreibt. Des Weiteren ist die Vorhersage-Komponente vorhanden, die die aufbereiteten historischen Daten liest, damit eine Vorhersage für einen bestimmten Tag erstellt und diese in die Datenbank schreibt. Schließlich existiert noch die Prüfungs-Komponente, die die Vorhersage für den aktuellen Tag sowie die realen Daten des aktuellen Tages liest und anhand dieser Daten entscheidet, ob eine Anomalie vorliegt oder nicht. Falls eine Anomalie erkannt wird, wird ein Verantwortlicher via Microsoft Teams benachrichtigt.

4.2 Umsetzung der Skripte

Die drei funktionalen Komponenten des *Anomaly Detection Systems* sind als *Python* (vanRossum 1995) Skripte realisiert. Im Folgenden soll kurz die Funktionsweise dieser drei Skript-Komponenten erläutert werden.

Datenimport Die Datenimport-Komponente stellt zunächst eine Anfrage an den Elasticsearch Server, wie viele Fehlermeldungen innerhalb der letzten fünf Minuten verzeichnet wurden. Die Anzahl, die der Server als Antwort liefert, wird anschließend zusammen mit dem aktuellen Zeitpunkt, an dem die Anfrage gestellt wurde, in die MongoDB geschrieben. Dabei werden zusätzlich zum normalen Zeitstempel Jahr, Monat, Tag, Stunde, Minute und Wochentag zusätzlich als Attribute gespeichert.

Um einen lückenlosen Datenbestand zu erhalten, läuft das Skript alle fünf Minuten.

Vorhersage Die Vorhersage-Komponente verwendet den erarbeiteten Lösungsansatz aus Abschnitt 3, um eine Vorhersage für den nächsten Tag zu treffen. Dabei werden die Daten der gleichen Wochentage aus der MongoDB gelesen. Diese werden anschließend so aufbereitet, dass sie für das Training des Modells verwendet werden können. Die Implementierung des autoregressiven Modells mit Keras (Ketkar und Santana 2017) ist in Listing 1 dargestellt.

```
model = Sequential([
    Input(shape=(288)),
    Dense(512, activation="tanh"),
    Dense(1024, activation="tanh"),
    Dense(512, activation="tanh"),
    Dense(288),
])
```

Listing 1: Implementierung des autoregressiven Modells in Keras

Ist das Training des Modells abgeschlossen, so wird anhand der Daten des letzten gleichen Wochentages eine Vorhersage erstellt. Diese wird schließlich in die Datenbank geschrieben.

Um immer eine aktuelle Vorhersage zu haben, läuft das Skript jeden Abend kurz vor Mitternacht und erstellt dabei eine Vorhersage für den kommenden Tag.

Prüfung Die Prüfungs-Komponente holt sich zunächst die Vorhersage für den aktuellen Tag aus der MongoDB. Anhand des aktuellen Zeitpunktes wird der vorhergesagte Wert für diesen ermittelt und daraus der obere Grenzwert für den aktuellen *Error-Count* berechnet. Anschließend wird die Anzahl der Fehlermeldungen innerhalb der letzten fünf Minuten, dem in Abschnitt 2.1 definierten Zeitintervall, am Elasticsearch Server abgefragt. Jetzt wird dieser Wert mit dem errechneten Grenzwert verglichen. Wird der Grenzwert überschritten, so wird ein verantwortlicher Mitarbeiter via Microsoft Teams benachrichtigt.

Um keine Anomalien zu übersehen, läuft das Skript alle fünf Minuten.

4.3 Bereitstellung im Kubernetes

Um die Skripte periodisch ausführen zu können, werden diese im Kubernetes (The Kubernetes Authors 2014) als *CronJob* bereitgestellt. Ein Beispiel, wie diese erstellt werden können, ist in Listing 2 dargestellt.

```
apiVersion: batch/v1beta1
kind: CronJob
metadata:
  name: anomaly-collect
  namespace: anomaly
spec:
  jobTemplate:
    metadata:
      name: anomaly-collect
    spec:
      template:
        spec:
          containers:
            - name: anomaly-collect
              image: anomaly-collect:1.0.0
              restartPolicy: OnFailure
  schedule: "*/5 * * * *"
```

Listing 2: Beispiel *CronJob* im Kubernetes

Das Beispiel in Listing 2 stellt den *CronJob* für das Datenimport-Skript dar. Dabei wird zunächst mit **apiVersion: batch/v1beta1** und **kind: CronJob** spezifiziert, dass ein *CronJob* erstellt werden soll. Anschließend wird in den Metadaten definiert, wie der *CronJob* benannt und in welchem *Namespace* er erstellt werden soll. Jetzt wird festgelegt, welche *Container* ausgeführt werden sollen. Dabei wird für jeden der Name und das *Container Image* definiert. In diesem Beispiel wird ein einzelner *Container* spezifiziert, der das Datenimport-Skript ausführt. Schließlich wird noch spezifiziert, wann der *CronJob* ausgeführt werden soll. Hier wird dieser mit **schedule: "*/5 * * * *"** alle fünf Minuten ausgeführt.

Für alle Skripte des Systems wird ein entsprechender *CronJob* erstellt. Die Ausführungszeiten werden dabei wie in Abschnitt 4.2 erläutert definiert.

5 EVALUATION UND FAZIT

Im Folgenden soll evaluiert werden, inwiefern das entwickelte *Anomaly Detection* System die Anomalien im Produktivbetrieb der Firma erkennt und dies einen Nutzen erbringt.

Als Evaluationsumgebung wird die Produktivumgebung der Firma verwendet. Dabei werden zunächst die Daten der *Error-Count Metrik* der letzten sechs Monate ausgelesen und gespeichert. Anschließend wird über einen Zeitraum von vier Wochen für jeden

Wochentag eine Vorhersage berechnet und anhand dieser versucht, Anomalien zu erkennen.

Nach diesen vier Wochen konnte festgestellt werden, dass, wie auch im Beispiel aus Abschnitt 3, Beginn und Ende der regulären Arbeitszeiten sehr gut vom System erkannt werden. Dies ist auch darin zu erkennen, dass Anomalien außerhalb der Arbeitszeiten immer erkannt werden. Problematisch während des Evaluationszeitraumes war jedoch, dass durch einen Hardwareausfall im Produktivsystem sehr viele Fehlermeldungen erzeugt wurden und dadurch das System fast durchgehend eine Anomalie gemeldet hat. Mehrere Mitarbeiter waren mit der Behebung dieses Ausfalls beschäftigt, sodass die Meldung einer Anomalie in diesem Zeitraum als korrekt angesehen werden kann.

Jedoch musste festgestellt werden, dass die Vorhersagen der Tage zwar oftmals nahe dem realen Verlauf gekommen sind, allerdings an einigen Tagen auch etwas weiter entfernt waren von diesem. Dadurch sind einige Anomalien gemeldet worden, die keine sind. Da im Laufe der Entwicklung des Systems die Vorhersagen durch mehr Trainingsdaten stetig besser wurden, kann davon ausgegangen werden, dass die vorhandene Datenmenge noch nicht ausreichend ist für zuverlässige Vorhersagen.

Auch wenn die Ergebnisse des Systems noch nicht optimal sind, erbringt es bereits jetzt einen Nutzen zur Überwachung des Systems, sodass dieses immer für die Kunden zur Verfügung steht. Dieser ist dahingehend vorhanden, dass Ausfallzeiten im Produktivsystem verkürzt werden, was somit auch lange Ausfallzeiten für die Kunden verhindert.

6 ZUSAMMENFASSUNG

In diesem Paper wurde gezeigt, welche Probleme im Produktivsystem der ODAV AG (ODAV AG, Gesellschaft für Informatik und Telekommunikation 1969) noch vorhanden sind (Abschnitt 2). Für diese Probleme wurde anschließend ein Lösungskonzept erstellt, indem mehrere Ansätze konzipiert und anschließend miteinander verglichen wurden (Abschnitt 3). Mit dem Konzept, das am besten abgeschnitten hat, wurde dann ein System erstellt, das mithilfe dieses Konzeptes Anomalien im Produktivbetrieb erkennen kann (Abschnitt 4). Dieses System wurde schließlich in einem Testzeitraum getestet und anhand der dort gesammelten Ergebnisse evaluiert (Abschnitt 5).

Es zeigt sich, dass mit einem System zur *Anomaly Detection* Ausfallzeiten in einem Produktivsystem, wie es zum Beispiel in der ODAV AG vorhanden ist, verhindert beziehungsweise verkürzt werden können. Jedoch hat sich auch gezeigt, dass für ein solches System, wenn es mit einem *Machine Learning* Modell aufgebaut ist, eine große Menge an Trainingsdaten benötigt wird, um zuverlässige Vorhersagen zu treffen, wobei dies noch nicht verlässlich evaluiert wer-

den konnte.

Als Erweiterung zu diesem Paper könnte man somit evaluieren, wie sich ein solches *Anomaly Detection* System entwickelt, wenn Daten ausgehend von wenigen Monaten bis hin zu mehreren Jahren verfügbar sind. Auch könnte man vergleichen, wie sich das dargestellte System im Vergleich zu anderen generischen System verhält.

LITERATUR

- Bradshaw, Shannon, Eoin Brazil und Kristina Chodorow (2019). *MongoDB: the definitive guide: powerful and scalable data storage*. O'Reilly Media.
- Chandola, Varun, Arindam Banerjee und Vipin Kumar (2009). „Anomaly detection: A survey“. In: *ACM computing surveys (CSUR)* 41.3, S. 1–58.
- Dave, Konark Truptiben (2013). „Brute-force Attack ‘Seeking but Distressing’“. In: *Int. J. Innov. Eng. Technol. Brute-force* 2.3, S. 75–78.
- Day, J.D. und H. Zimmermann (1983). „The OSI reference model“. In: *Proceedings of the IEEE* 71.12, S. 1334–1340. DOI: 10.1109/PROC.1983.12775.
- Elasticsearch B.V. (2010). *Free and Open Search: The Creators of Elasticsearch, ELK & Kibana / Elastic*. URL: <https://www.elastic.co/> (besucht am 28.09.2022).
- Ilag, Balu N und Arun M Sabale (2022). „Microsoft teams overview“. In: *Troubleshooting Microsoft Teams*. Springer, S. 17–74.
- Ketkar, Nikhil und Eder Santana (2017). *Deep learning with Python*. Bd. 1. Springer.
- ODAV AG, Gesellschaft für Informatik und Telekommunikation (1969). *Homepage - ODAV AG*. URL: <https://www.odav.de/> (besucht am 14.09.2022).
- Oliphant, Travis E (2006). *A guide to NumPy*. Bd. 1. Trelgol Publishing USA.
- The Kubernetes Authors (2014). *Kubernetes*. URL: <https://kubernetes.io/> (besucht am 28.09.2022).
- vanRossum, Guido (1995). „Python reference manual“. In: *Department of Computer Science [CS]* R 9525.

AUTOREN

Benjamin Eder (M.Sc.) schloss 2023 sein Masterstudium Informatik mit Schwerpunkt *Software Engineering* an der OTH Regensburg ab. Seit 2018 ist er bei der ODAV AG als Werkstudent tätig und ist dort seit 2023 als Softwareentwickler festangestellt.

Benjamin Neumann (Dipl.-Inf. (FH)) beendete 2009 sein Informatikstudium an der Fachhochschule Regensburg. Danach war er bis 2012 bei Continental Regensburg beschäftigt. Seitdem ist er bei der Firma ODAV AG in Straubing, anfangs als Softwareentwickler im DevOps Bereich, seit 2022 als Teamleiter

Basissysteme.

Prof. Dr. Frank Herrmann wurde in Münster geboren und studierte Informatik an der Rheinisch-Westfälischen Technischen Hochschule in Aachen. Nach seinem Diplom 1989 arbeitete er bei dem Fraunhofer Institut IITB in Karlsruhe. Während dieser Zeit promovierte er 1996 über Ressourcenbelegungsplanungsprobleme. Von 1996 bis 2003 arbeitete er für die SAP AG in verschiedenen Funktionen, zuletzt als Direktor. Im Jahr 2003 wurde er Professor für Produktionslogistik an der Ostbayerischen Technischen Hochschule in Regensburg. Seine Forschungsthemen sind Planungsalgorithmen, Optimierung und Simulation für die operative Produktionsplanung und -steuerung. Er ist Leiter des Innovations- und Kompetenzzentrums für Produktionslogistik und Fabrikplanung (IPF).

Konzeption einer hochsicheren TLS-Auth Infrastruktur zur Authentifizierung von Industrie-Routern an einer Management-Software

Christopher Neldner

INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22, 93049 Regensburg, Germany
E-Mail: cneldner@insys-icom.de

Djordje Gladovic

INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22, 93049 Regensburg, Germany
E-Mail: dgladovic@insys-icom.de

Professor Dr. Frank Herrmann

Ostbayerische Technische Hochschule Regensburg
Innovationszentrum für Produktionslogistik
und Fabrikplanung
Galgenbergstraße 32, 93053 Regensburg, Germany

ABSTRAKT

IT-Sicherheit spielt besonders im IoT-Bereich eine kritische Rolle. In dieser Arbeit soll eine bestehende Public-Key-Infrastruktur, die im *Router Management* der INSYS icom für die Authentifizierung von Routern eingesetzt wird, auf optimierbare Stellen untersucht werden, und diese durch ein neues, verbessertes Konzept optimiert werden. Ein *Proof of Concept* zeigt die Realisierbarkeit dessen.

1 EINFÜHRUNG

Das *Internet of Things* (IoT) und darauf aufbauende Konzepte wie Industrie 4.0 und das *Smart Grid* erlangen täglich an größerer Bedeutung [1]. Um diese Konzepte praktikabel in einem realen Anwendungsszenario umzusetzen, bedarf es passender Hardware- und Softwarelösungen.

Das mittelständische Unternehmen INSYS MICROELECTRONICS GmbH [2] beschäftigt sich mittlerweile seit über 30 Jahren mit der Entwicklung spezieller Hardware für Kommunikation in verschiedenen Branchen. Aber auch Softwarelösungen, welche sich auf den Lebenszyklus von Routern oder auf das Aufbauen sicherer Kommunikationskanäle beziehen, befinden sich im Portfolio des Unternehmens. Dabei ist zu beachten, dass Kunden, die sich mit der Bereitstellung von kritischer Infrastruktur befassen, wie beispielsweise Energie- oder Wasserversorger, den strengen KRITIS-Vorlagen unterliegen [3]. Um diesen Markt zu erschließen, müssen Softwarelösungen diese Vorlagen ebenfalls erfüllen. Das Softwareprodukt, welches in dieser Arbeit im Fokus steht, ist das INSYS Router Management (iRM). Dieses ermöglicht dem Nutzer, eine große Anzahl von Routern komfortabel und effizient mit Firmware- und Softwareupdates zu versorgen. Um unbefugten Zugriff auf die Anwendung zu verhindern, nutzt das Produkt Transport Layer Security (TLS)-Clientauthentifizierung. Dabei muss ein Router bei Verbindungsaufbau ein gültiges Zertifikat vorweisen um überhaupt erst mit dem iRM kommu-

nizieren zu können. Diese Funktionalität ist bereits funktionsfähig implementiert, weist jedoch Optimierungspotential in Handhabung und Implementierung auf.

In Abschnitt 2 wird dafür zunächst die Problemstellung erläutert und das Optimierungspotential der Implementierung aufgezeigt. Darauf folgend wird in Abschnitt 3 ein Konzept vorgestellt, welches eben genannte Stellen verbessern soll. In Abschnitt 4 werden im *Proof of Concept* verwendete Technologien vorgestellt sowie deren Zusammenspiel erläutert, um eine vollständige Public-Key-Infrastruktur zu erhalten. Abschnitt 5 greift die vorher aufgezählten optimierbaren Stellen wieder auf und analysiert, ob das neue Konzept diese tatsächlich beseitigt und alle weiteren Anforderungen erfüllt.

2 PROBLEMSTELLUNG

Das iRM nutzt eine eigene *Public-Key-Infrastruktur* (PKI) um Routern zu ermöglichen, sich am Backend des iRM zu authentifizieren. Diese Public-Key-Infrastruktur ist nicht für die Verschlüsselung der Daten und den sicheren Datentransport zuständig, sondern lediglich für die Authentifizierung, sodass nicht autorisierte Geräte erst keine Verbindung zum iRM aufbauen können. Der Aufbau eines TLS-Tunnels zur gesicherten Kommunikation erfolgt vor diesem Schritt an anderer Stelle. Die Prozesse und Gegebenheiten der bestehenden Public-Key-Infrastruktur sind dabei an einigen Stellen noch zu optimieren. Ziel der Arbeit ist es, durch die Konzeption einer neuen Public-Key-Infrastruktur die in Abschnitt 2.2 genannten Schwachstellen auszumerzen, sodass eine Public-Key-Infrastruktur entsteht, welche aktuellen Empfehlungen entspricht [4].

2.1 Analyse der bestehenden Public-Key-Infrastruktur

Die zurzeit eingesetzte Public-Key-Infrastruktur ist eine Eigenimplementierung. Diese benutzt gängige

kryptographische Bibliotheken und Pakete um alle nötigen Funktionen zu implementieren.

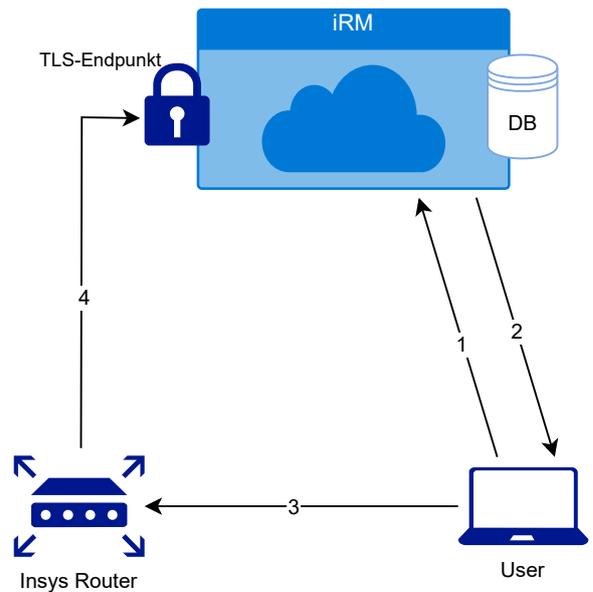
Funktionsweise Es wird für jedes neu angelegte Benutzerkonto im iRM eine eigene, selbst signierte *Root-CA* erstellt. Diese Zertifikatsautorität ist die *Wurzel* der Zertifikatsstruktur und dadurch der *Vertrauensanker*. Vertraut man dieser Autorität, kann man gleichzeitig allen Zertifikaten vertrauen, die diese ausstellt und signiert. Die *Root-CA* ist hier also dafür zuständig, die entsprechenden Client-Zertifikate für die Router auszustellen.

Die Auslieferung der Zertifikate erfolgt über eine sogenannte *Startkonfiguration*, welche beim einrichten eines Routers im iRM erstellt wird und jederzeit abrufbereit ist. Dies ist in Abbildung 1a zu sehen. Diese enthält verschiedenste Einstellungen als auch das Clientzertifikat samt privatem Schlüssel, um den Router mit dem iRM zu verbinden. Der Nutzer lädt diese über eine verschlüsselte Verbindung herunter und spielt die *Startkonfiguration* selber auf den Router ein. Der Router kann sich nun mit dem iRM verbinden und authentifizieren.

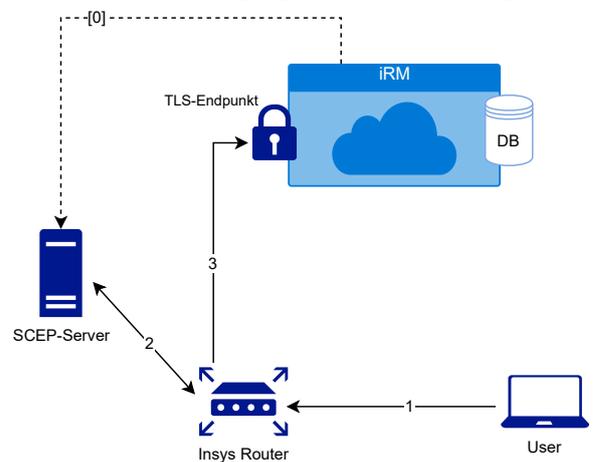
Ein weiterer Weg, Zertifikate auszuliefern, besteht darin, die bestehende Implementierung des Simple Certificate Enrollment Protocol (SCEP)-Protokolls im Betriebssystem des Routers zu nutzen, was in Abbildung 1b abgebildet ist. SCEP ist ein standardisiertes Protokoll zur Auslieferung und Erneuerung von Zertifikaten. Mehr dazu kann in Abschnitt 3.2 nachgelesen werden. Die Router können als SCEP-Klienten fungieren, wobei es jedoch zurzeit nötig ist, den SCEP-Server selber bereitzustellen. Dieser benötigt eine Zertifikatsautorität samt privatem Schlüssel um Zertifikate auf Anfrage zu signieren. Wird eine erfolgreiche Zertifikatsanfrage gestellt, wird dem Router ein gültiges Zertifikat zurückgesandt, mit welchem er sich am TLS-Endpunkt authentifizieren kann.

Zertifikatsstruktur Das System benutzt Standard *X.509-Zertifikate* der Version drei. Diese sind komplexe, definierte Datenstrukturen, welche über bestimmte Notationen und Kodierungen verfügen. Zudem ermöglicht dieser Standard in Version drei den Zertifikaten *Erweiterungen* hinzuzufügen, welche diese mit Informationen anreichern. Wird im Laufe der Arbeit von Zertifikaten gesprochen, ist damit immer ein *X.509v3-Zertifikat* gemeint.

In Abbildung 2 ist die aktuelle Zertifikatsstruktur zu sehen. Bei Erstellung eines Nutzerkontos wird eine eigene selbst signierte *Root-CA* ausgestellt, welche wiederum die Client-Zertifikate ausstellt. Dies bedeutet, dass mehrere voneinander komplett unabhängige Public-Key-Infrastrukturen nebeneinander existieren. Zudem ist die *Root-CA* die signierende Instanz, wenn ein Zertifikat ausgestellt werden soll. Dies sollte grundsätzlich vermieden werden, da bei



(a) Zertifikatsausbringung über die Startkonfiguration



(b) Zertifikatsausbringung über SCEP

Abbildung 1: Zertifikatsausbringung der PKI des iRM

der Signierung von Dokumenten der private Schlüssel in Benutzung ist und sich dieser daher nicht mehr an einem sicheren Ablageort befindet. Sollte der private Schlüssel der *Root-CA* kompromittiert werden, ist die komplette Public-Key-Infrastruktur nicht mehr sicher.

Ebenfalls wird das Überprüfen eines Zertifikates auf Gültigkeit am TLS-Endpunkt erschwert, da dieser die *Root-CA* jedes Nutzerkontos besitzen muss um das Zertifikat der entsprechenden *Root-CA* zuzuordnen zu können.

2.2 Schwachstellen der bestehenden Public-Key-Infrastruktur

Im Folgenden werden die Schwachstellen der Public-Key-Infrastruktur beschrieben, welche im Laufe der

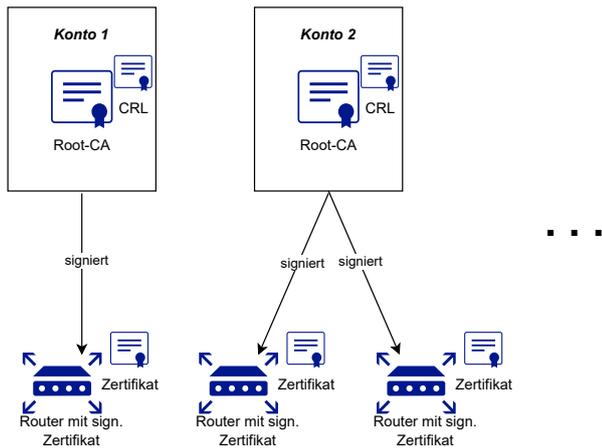


Abbildung 2: Bestehende Zertifikatsstruktur im System

Arbeit durch das angefertigte Konzept eliminiert werden sollen:

Rückdatierung und Laufzeit Router bekommen beim Aufspielen der ersten *Startkonfiguration* ein Zertifikat mitgesendet, welches von 1970 an rückdatiert ist und 10 Jahre ab Datum der Erstellung gültig ist. Somit hat das Zertifikat eine Laufzeit von über 50 Jahren, was für Zertifikate dieser Art sehr ungünstig ist. Diese Eigenheit ist durch die Weiterentwicklung der Produkte nicht mehr von Nöten. Es gilt dennoch ein System zu entwerfen, welches mit solchen möglichen Eigenheiten zurecht kommen würde. Ebenfalls ist Rückdatierung ein seltener Randfall, welcher im besten Fall vermieden werden sollte.

Ausbringung der Zertifikate Wenn die *Startkonfiguration* auf den Router übertragen wird, wird ebenfalls das Zertifikat samt Schlüsselmaterial mitgesendet. Dies führt dazu, dass der private Schlüssel des Zertifikates im Klartext in der *Startkonfiguration* vorhanden ist. Dies gefährdet die Integrität des Schlüsselmaterials, da nun die sichere Handhabung dessen beim Benutzer liegt und nicht mehr bei der eigenen Anwendung.

Rückziehung von Zertifikaten Client-Zertifikate sind in diesem Anwendungsfall relativ flüchtige Komponenten. Jedes mal, wenn ein Router im iRM angelegt wird, wird ebenfalls ein Zertifikat erzeugt. Wird ein Router aus der Managementsoftware entfernt, wird dieses Zertifikat deaktiviert. Dies wird in der Datenbank hinterlegt. Jedoch sollte dies eigentlich in einer Certificate Revocation List (CRL) hinterlegt werden und vielleicht sogar mittels dem Online Certificate Status Protocol (OCSP) abgefragt werden können. Mit OCSP kann die Gültigkeit eines bestimmten Zertifikats direkt abgefragt werden ohne erst die CRL herunterzuladen. In einer CRL wer-

den die Seriennummern von zurückgezogenen Zertifikaten gespeichert, sodass zu einem späteren Zeitpunkt die Gültigkeit von Zertifikaten überprüft werden kann. Der Grundstein für diese Funktionalität wurde gelegt, jedoch ist diese nicht funktionsfähig. Bei diesem Aspekt spielt ebenfalls die lange Laufzeit von Zertifikaten hinein. Werden viele Router angelegt und wieder entfernt, würde die CRL schnell anwachsen, da diese alle Zertifikate enthalten muss, die nach Rückziehung von sich aus noch gültig wären, und die Zertifikate nicht in naher Zeit ablaufen.

Terminierung der Verbindung Ist ein Router gelöscht worden, existiert das Zertifikat immer noch und ist zu jetzigem Stand in keiner abrufbaren CRL hinterlegt. Es gibt also keine Möglichkeit für solch einen Endpunkt zu überprüfen, ob ein Zertifikat gültig ist oder nicht. Erst am Backend des iRM wird die Verbindung abgelehnt, da dieses über die Deaktivierung des Zertifikats Bescheid weiß.

3 KONZEPTION EINER VERBESSERTEN PUBLIC-KEY-INFRASTRUKTUR

Um die Public-Key-Infrastruktur des Router Managements zu verbessern, wird eine neue Zertifikatsstruktur entworfen sowie die Verwaltung dieser weitestgehend auf bestehende und erprobte Protokolle und Softwarelösungen verlagert.

Eine Verbesserung der Public-Key-Infrastruktur anzustreben hat vielfältige Gründe. Zum einen wird der Wartungsaufwand der Anwendung bei Auslagerung von komplexen Public-Key-Infrastruktur-Funktionalitäten gesenkt. Das Signieren und Ausstellen von Zertifikaten sowie das Verwalten von Schlüsselmaterial dieser sind aufwendige und sicherheitskritische Aktionen. Wird dies auf erprobte Softwarelösungen und Protokolle ausgelagert, sinkt die Fehleranfälligkeit und Komplexität des Systems, sodass die Wartung dessen erleichtert wird. Außerdem wird durch ein modernes und schlüssiges Konzept die Sicherheit des iRM und der zugehörigen Komponenten verbessert. Dies erhöht die Attraktivität des Produkts, vor allem für Kunden, bei denen Sicherheit einen hohen Stellenwert hat.

Das entworfene Konzept wird in den nächsten Kapiteln erläutert.

3.1 Zertifikatsstruktur

Die Zertifikatsstruktur ist ein zentraler Teil einer Public-Key-Infrastruktur und bestimmt das Verhalten der einzelnen Komponenten sowie Vorgänge in dieser.

Alle in Abschnitt 2.2 genannten Punkte zeigen auf, dass an der Zertifikatsstruktur Verbesserungsbedarf besteht. Ein Weg dies zu erreichen besteht darin, das

Prinzip des *Hierarchischen Vertrauens* [5] zu nutzen. Dafür wird eine übergeordnete *Root-CA* erstellt, welche Zwischenzertifikate ausstellt; diese ersetzen bei den Benutzerkonten die eigenen *Root-CA*s. Die übergeordnete *Root-CA* übernimmt hier die Rolle des *Vertrauensankers*. Diese Zwischenzertifikate sind von der übergeordneten *Root-CA* signiert und können selber Client-Zertifikate ausstellen. Somit wird die Zertifikatshierarchie um eine weitere Ebene erweitert, wie in Abbildung 3 abgebildet.

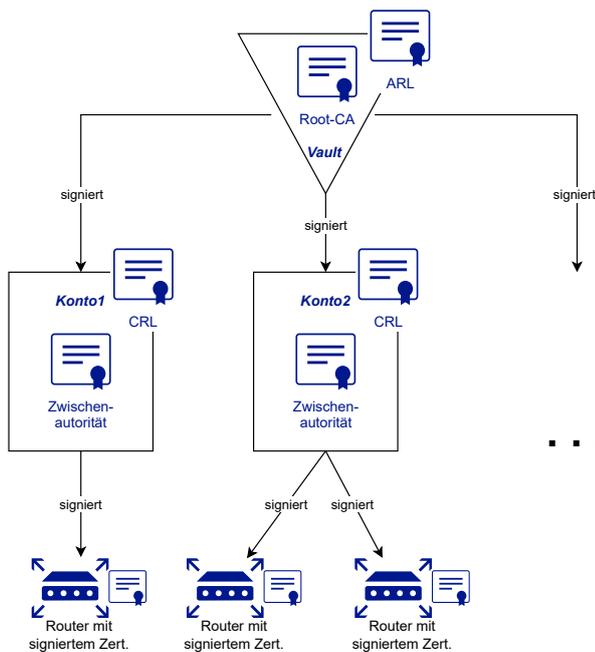


Abbildung 3: Neu angedachte Zertifikatsstruktur

Möchte man nun eine CRL pflegen, kann dies über die jeweiligen Zwischenautoritäten geschehen. Diese stellen und signieren CRLs für jegliche von ihnen ausgestellte Zertifikate bereit. Es wäre zwar möglich, dies über eine indirekte CRL, welche von der obliegenden Zertifikatsautorität ausgestellt wird, zu verwalten, jedoch wird davon abgeraten, da die Sicherheit des Systems darunter leidet. Bei der Signierung einer CRL wird der private Schlüssel der Zertifikatsautorität benötigt. Dadurch ist dieser in Benutzung und somit im Speicher des Systems geladen, wodurch das Risiko der Kompromittierung des Schlüsselmaterials steigt. Zwar bleibt der Verwaltungsaufwand der CRLs im Vergleich zum Bestandssystem ähnlich, jedoch verbessert sich die Sicherheit, da das Schlüsselmaterial der *Root-CA* sicher ruhen kann.

Auch besteht nun die Möglichkeit, eine *Authority Revocation List* (ARL) anzufertigen, sollte eine Zwischenautorität zurückgezogen werden, zum Beispiel bei Löschung oder Kompromittierung eines Nutzeraccounts. Dies ist möglich durch die Delegation der *Root-CA*-Aufgaben an eine ausgewiesene selbst signierte Zertifikatsautorität. Dies erleichtert diesen Randfall zu behandeln.

Soll die Gültigkeit eines Client-Zertifikates ermittelt werden, muss ein valider Zertifizierungspfad ermittelt werden. Solch ein Pfad ist eine endliche Sequenz aus Zertifikaten mit der Eigenschaft, dass das Subjekt der Aussteller des nächsten Zertifikates ist, außer dem Letzten [5]. Der Pfad ist gültig, wenn das Subjekt im letzten Zertifikat das zu prüfende Zertifikat ist und der Aussteller des ersten Zertifikates der Vertrauensanker ist.

3.2 Zertifikatsausbringung

Damit die ausgestellten Zertifikate auch genutzt werden können, müssen diese über einen sicheren und effizienten Mechanismus beantragt, ausgestellt und zugesandt werden. Solch einen Mechanismus kann SCEP bieten [6]. SCEP ist ein Protokoll zur Ausstellung, Erneuerung und Anfrage von Zertifikaten sowie zur Verteilung von öffentlichen Schlüsseln der Zertifikatsautoritäten. Ebenfalls können zumindest CRL-Anfragen über das Protokoll bedient werden.

SCEP wird bereits von den Routern der INSYS unterstützt, weswegen primär dieses Protokoll betrachtet wird. Zu Abwandlungen des Konzepts wird sich in späteren Kapiteln der Arbeit geäußert.

Das Protokoll sendet und empfängt Nachrichten unverschlüsselt über HTTP, weswegen die Nachrichten in gesicherten, verschlüsselten PKCS-Containern versendet werden. So kann verhindert werden, dass Dritte in-Transit Zugriff auf die Nachrichten haben könnten. Um zu verhindern, dass Zertifikate an nicht autorisierte Geräte ausgestellt werden, arbeitet SCEP mit *Challenge*-Passwörtern. Da diese Schnittstelle über das Internet erreichbar ist, muss diese entsprechend abgesichert werden. Das *Challenge*-Passwort ist ein geteiltes Geheimnis und muss dem Router vor der Zertifikatsanfrage zukommen. Hier eignet sich der Weg über die *Startkonfiguration*, welche zurzeit das gesamte Zertifikat samt privatem Schlüssel enthält. Das Passwort sollte kein konventionelles Passwort sondern ein schwer zu erratendes sein [6]. Im besten Fall ist dieses ein Einmal-Passwort, das nur für eine Zertifikatsanfrage gültig ist und eine begrenzte Lebenszeit besitzt. Die Passwörter an sich müssen natürlich auch sicher abgelegt werden.

Für das Router-Management bietet es sich an, diese Passwörter bei Anlegen des Routers im iRM zu erstellen und für jeden Router an sicherer Stelle abzuliegen. Möchte sich nun ein Router ein Zertifikat über SCEP ausstellen lassen, muss dieser das *Challenge*-Passwort mitliefern. Der SCEP-Server kann nun prüfen, ob das Subjekt für die Zertifikatsausstellung autorisiert ist. Wird ein Zertifikat nach Anfrage ausgestellt, wird das zugehörige Passwort ungültig. Sollte ein Router länger mit der Zertifikatsanfrage warten als die gesetzte Lebenszeit des Passworts, wird die Anfrage fehlschlagen.

Zertifikate können aber auch über SCEP erneuert

werden. Dabei sendet der Router eine Erneuerungs-Anfrage, welche mit dem alten Zertifikat signiert wurde, an den SCEP-Server. An dieser Stelle kann ein Zertifikat mit dem bestehenden Schlüsselmaterial oder mit neuem Schlüsselmaterial angefordert werden.

3.3 Eigenschaften der Zertifikate

An den Zertifikaten selbst werden keine großen Änderungen vorgenommen. Diese enthalten weiterhin nötige Felder wie Subjektkname, Aussteller, Gültigkeit, öffentlicher Schlüssel und Informationen zu benutzten Verschlüsselungsalgorithmen. Die Zertifikate enthalten ebenfalls Erweiterungen, welche in Version 3 von X.509-Zertifikaten vorhanden sind.

Für Zertifikatsautoritäten sind die Erweiterungen *Basiseinschränkungen*, welche angeben ob das vorliegende Zertifikat eine Zertifikatsautorität sein darf, und *Schlüsselnutzung*, welche die möglichen Anwendungsfälle der Schlüssel des Zertifikats definiert, wichtig. Diese müssen so gesetzt werden, dass vorliegende Zertifikate als Zertifikatsautoritäten fungieren und Zertifikate sowie CRLs signieren können. Die Zertifikatsautoritäten besitzen ebenfalls *Erweiterungen* für den Zugriff auf die CRLs, welche auf den Ablageort dieser verweisen.

Da Zertifikate nun über einen definierten Mechanismus nach Bedarf angefordert sowie auch erneuert werden können, kann die Laufzeit der Zertifikate niedrig gehalten werden. Beruhend auf der Annahme, dass die Router eine längerfristige Verbindung mit dem Router-Management aufbauen und sich trotz zeitweiliger Abschaltung wieder mit dem Router Management verbinden sollen, wäre eine Laufzeit von drei Monaten akzeptabel.

4 REALISIERUNG

Das folgende Kapitel beschäftigt sich mit der Implementation des im vorherigen Kapitel erarbeiteten Konzepts. Die Implementation und Integration des Konzepts zielt in dieser Arbeit auf einen *Proof of Concept* ab, welcher die Möglichkeiten als auch Grenzen des Konzepts im realen Produktivumfeld aufzeigen soll. Dafür werden bestehende Technologien untersucht und ihre Funktionen genutzt, um als Endergebnis eine performante, sichere und flexible Public-Key-Infrastruktur zu erhalten.

4.1 Technologien

Im Folgenden werden die ausgewählten Technologien beschrieben und Gründe für die Auswahl dieser dargelegt.

HashiCorp Vault *HashiCorp Vault* [7] ist eine Anwendung zur sicheren Verwaltung und Ablage von Geheimnissen, welche sehr vielfältig sein können.

Diese sind zum Beispiel Passwörter für Datenbanken, Tokens für Authentifizierung oder auch Zertifikate. Vault verwaltet solche Geheimnisse über *Secret Engines*. Diese sind nach Bedarf hinzufügbare Module, die verschiedene Funktionalitäten für Verwaltung und Ausstellung der Geheimnisse bieten. Solch eine Engine ist zum Beispiel die *Public-Key-Infrastruktur-Certificates Engine*, welche ermöglicht, Zertifikatsautoritäten zu erstellen, das Schlüsselmaterial dieser zu verwalten und mithilfe dieser Zertifikate auszustellen. Diese können ebenfalls bei Bedarf zurückgezogen werden. Auch werden Schnittstellen angeboten, welche den Zugriff auf etwaige CRLs und CA-Zertifikate bieten.

Bei der Verwaltung von Geheimnissen setzt HashiCorp auf das Prinzip von kurzlebigen Geheimnissen. Dies bedeutet, dass ausgestelltes Schlüsselmaterial so kurz wie möglich seine Gültigkeit behält. Im Fall dieser Arbeit bedeutet dies, dass Zertifikate nur so lange wie nötig für einen reibungslosen Lebenszyklus dieser gültig sind, also etwa drei Monate. Dabei können die Funktionen der Engine über eine HTTP- oder HTTPS-Schnittstelle aufgerufen werden.

Vault ist aber nicht nur eine gute Softwarelösung zur Bereitstellung einer Public-Key-Infrastruktur, sondern ebenfalls ein Technologiewunsch von Seiten der Produktentwicklung. Dies ist der Fall, da das Router-Management die Fähigkeit bietet, Konfigurationsdaten für Router in Vorlagen und eigenen Feldern zu speichern. Diese können vertrauliche Daten beinhalten und Aufschluss über etwaige Netzwerke geben, was als vertraulich anzusehen ist. Dabei kann *Vault* helfen, diese Daten über eine andere *Secret-Engine* sicher abzulegen. Dieser Mechanismus kann auch genutzt werden, um die Zertifikatsanforderung über SCEP mithilfe von *Challenge*-Passwörtern abzusichern. Mehr dazu in Abschnitt 4.2.

Alle genannten Anwendungsfälle kombiniert, sowie verwendete Algorithmen und Technologien in der Implementierung des *Vault*, ergeben ein großes Potenzial für den Einsatz dessen im bestehenden System der INSYS .

SCEP Wie bereits angemerkt, können Router Zertifikate für das iRM über eine SCEP-Implementation verwalten. Um diese Funktionalität zu nutzen, wird ein SCEP-Server benötigt, welcher kommende Aufrufe nach dem SCEP-Protokoll annehmen und verarbeiten kann. An dieser Stelle wurde sich für den *micromdm/scep* [8] Server entschieden. Dies hat vielfältige Gründe:

Zum einen ist das vorliegende Paket in der Programmiersprache *Go* implementiert, welche die verwendete Sprache des iRM-Backends ist. Dadurch passt sich dieses Paket gut in das Ökosystem des iRM ein.

Außerdem ist das Paket sehr flexibel was Erweiterbarkeit angeht. Im vorangehenden Punkt wur-

de geschildert, das die Public-Key-Infrastruktur über den *Vault* verwaltet werden soll. SCEP sowie auch die enthaltene Serverimplementierung im *micromdm/scep*-Paket beschreiben jedoch das Ausstellen und Erneuern von Zertifikaten als Aufgabe des Servers selbst. In Fall des erarbeiteten Konzepts soll der SCEP-Server als Proxy für etwaige Anfragen an den *Vault* dienen. So müssen Router nicht mit dem *Vault* direkt kommunizieren können, sondern können dafür das standardisierte SCEP-Protokoll nutzen. In der Beschreibung des betrachteten Pakets wird die Möglichkeit, dieses als Proxy für Anfragen zu nutzen, explizit genannt, was auch durch die generisch gehaltene Implementierung bestätigt werden kann.

So kann eine Eigenimplementierung eines SCEP-Servers mit getesteten Funktionen angefertigt werden, welche sogar in das bestehende Backend des iRM integriert werden kann.

Dabei ist jedoch zu beachten, dass SCEP nicht über verschlüsselte Kanäle kommuniziert. Dies bedeutet, dass SCEP sich selbst um Verschlüsselung der Daten in-Transit kümmert. Dafür wird der zu signierende Certificate Signing Request (CSR) mit dem öffentlichen Schlüssel der im Server hinterlegten Zertifikatsautorität verschlüsselt, welche diesen daraufhin bei Erhalt mit Hilfe des privaten Schlüssels entschlüsseln kann. Das signierte Zertifikat kann nun mit dem eigenen öffentlichen Schlüssel wieder verschlüsselt und zurückgeschickt werden. Der SCEP-Server benötigt also stets alle Zwischenautoritäten samt Schlüsselmaterial, unabhängig davon, an welcher Stelle Zertifikate signiert werden.

EST Enrollment over Secure Transport (EST) ist ein Protokoll, welches, ähnlich wie SCEP, das Ausstellen von Zertifikaten auf Anfrage sowie das Bereitstellen von Zertifikatsautoritäten ermöglicht [9].

Der größte Unterschied im Vergleich zu SCEP besteht im Mechanismus des sicheren Transports der Daten. Während SCEP sich selbst um die Verschlüsselung kümmert, nutzt EST den bereits vorhandenen TLS-Mechanismus, um die Daten verschlüsselt zu transportieren. Ebenfalls ist die Generierung von Schlüsselmaterial auf Klientenseite als auch auf Serverseite im Standard spezifiziert. Zudem ist im Standard von EST die Möglichkeit von Erweiterung des Protokolls nicht nur möglich, sondern auch vorhergesehen. Dies bietet mehr Freiheit bei der Gestaltung des Ausstellungsprozesses.

Außerdem bietet EST die Wahlmöglichkeit von Chiffretypen, wie zum Beispiel *Elliptic Curve Cryptography*.

EST ist jedoch noch nicht in der Firmware der Router implementiert.

4.2 Funktionsweise

Da nun etwaige Technologien und Gründe für deren Benutzung bekannt sind, können diese im Fol-

genden Kapitel miteinander kombiniert und deren Zusammenspiel erläutert werden, um im Anschluss eine vollwertige Public-Key-Infrastruktur zu erhalten. Dieses ist in folgender Grafik veranschaulicht, welche im Folgenden in Reihenfolge der angemerkten Schritte erläutert wird.

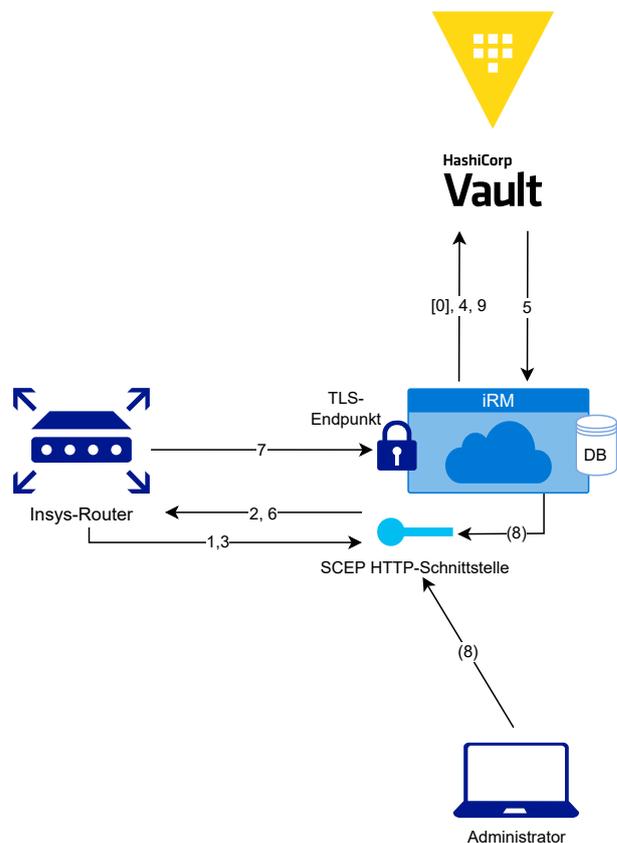


Abbildung 4: Abläufe in der PKI

In Abbildung 4 ist das Aufsetzen der Public-Key-Infrastruktur und der Ablauf bei Zertifikatsanforderung sowie der optionalen Zertifikatsrückziehung enthalten.

Begonnen wird mit dem Aufsetzen und Vorbereiten des *Vaults* für das Ausstellen und Verwalten von Zertifikaten, angemerkte durch Schritt null in eckigen Klammern, da dies nicht direkt zum Lebenszyklus der Zertifikate gehört. Das Vorbereiten des *Vaults* kann in zwei Arten aufgeteilt werden:

Beim ersten Start des Komplettsystems wird dieser hochgefahren und eine selbst signierte Root-CA ausgestellt. Diese bleibt im besten Fall bis Laufzeitende bestehen. Ebenfalls werden zugehörige Rollen und Konfigurationen erstellt.

Läuft das System, ist es bereit Nutzereingaben zu verwalten. Erstellt ein Nutzer nun einen Account, erzeugt das Backend eine Zwischenautorität, welche später genutzt wird, die Client-Zertifikate zu signieren. Diese Art ist in Abbildung 4 in Schritt null dargestellt.

Ist das System aufgesetzt, können Zertifikatsanfragen gestellt werden. In Schritt eins fragt der Router das Zertifikat der Zwischenautorität an, welches für das Generieren und Verschlüsseln des CSRs benötigt wird. Schritt zwei ist die zugehörige Antwort, also das Zertifikat der Autorität. Soll tatsächlich das richtige Zertifikat geliefert werden, ist es nötig, sich einen Mechanismus zu überlegen, welcher die Auswahl der richtigen, zum Nutzerkonto gehörigen, Zwischenautorität ermöglicht, da SCEP standardmäßig lediglich ein bestimmtes hinterlegtes Zertifikat zurückgibt.

Schritt drei beschreibt die eigentliche Zertifikatsanfrage. Dabei generiert der Router das Schlüsselmaterial für das Zertifikat und packt dieses in einen CSR, welcher verschlüsselt an den SCEP-Server gesendet wird. In Schritt vier reicht die Schnittstelle die Anfrage an den *Vault* weiter, welcher letztendlich die Anfrage erhält, das gewünschte Zertifikat über einen bestimmten Endpunkt signiert und dieses in Schritt fünf zurück an den SCEP-Server sendet. Dieser sendet wiederum in Schritt sechs das aufbereitete Ergebnis der Anfrage, verschlüsselt mit dem öffentlichen Schlüssel, an den Router weiter, welcher daraufhin alle nötigen Daten besitzt, um eine Verbindung mit dem Router-Management herzustellen.

Möchte man das Schlüsselmaterial serverseitig generieren lassen, wenn zum Beispiel das Generieren von Schlüsseln zu aufwendig für den Klienten ist, bietet die Spezifikation von SCEP jedoch keine Mechanismen. Zwar gibt es SCEP-Server-Implementationen, die diese Funktionalität bieten, jedoch ist diese nicht im Standard spezifiziert. An dieser Stelle ist der Einsatz des EST-Protokolls empfohlen, welches die Verschlüsselung der Daten an den TLS-Mechanismus abgibt, sofern alle Parteien diesen unterstützen.

Das Aufbauen der Verbindung passiert in Schritt sieben, wobei der Router sich an der TLS-Terminierung mit dem erhaltenen Zertifikat authentifiziert. Die TLS-Terminierung besitzt alle nötigen übergeordneten Zertifikatsautoritäten sowie Zugriff auf alle CRLs, wodurch diese in der Lage ist, die Gültigkeit des Zertifikats zu prüfen. Erst bei erfolgreicher Prüfung des Zertifikats kann der Router mit dem iRM kommunizieren.

Ist es zu einem späteren Zeitpunkt erforderlich, ausgestellte Client-Zertifikate zurückzuziehen, sollte dies über einen definierten Weg machbar sein. In Schritt acht wenden sich die Anwendung oder ein Administrator mit der Seriennummer des zu annullierenden Zertifikats an eine passende Schnittstelle. Soll diese die SCEP-Schnittstelle sein muss, dieser Endpunkt selber implementiert werden, da das SCEP-Protokoll keinen Mechanismus definiert, um Zertifikate zurückzuziehen, der *Vault* jedoch schon. Da Rückziehung nur von der Anwendung selber, zum Beispiel bei Löschung eines Routers, oder von Administratoren durchgeführt wird, kann der *Vault* auch

direkt mit einem passenden Token angesprochen werden. Schritt neun ist hier entweder die direkte Anfrage an den *Vault* für Rückziehung oder eine weitergeleitete Anfrage. Zurückgezogene Router sind nun in der vom *Vault* ausgestellten und bereitgestellten CRL aufzufinden.

4.3 Umsetzung

Damit gezeigt werden kann, dass das Konzept auch in der Realität umsetzbar ist, wurde ein *Proof of Concept* angefertigt. Dieser soll keine komplette Implementation darbieten, sondern zeigen, dass die einzelnen Schritte der automatisierten Zertifikatsausbringung tatsächlich implementierbar sind. Auch sollte sich nicht auf die Wahl eines bestimmten Protokolls zur Ausbringung der Zertifikate versteift werden.

Der *Proof-of-Concept* basiert auf *Bash*-Skripten. Hier wird größtenteils mit *Curl*-Befehlen gearbeitet, welche API-Aufrufe absetzen. Folgende Aufgaben sollen automatisiert werden:

Aufsetzen des Vault Der *Vault* muss zu Beginn konfiguriert und eingerichtet werden. In diesem Fall besteht dies daraus, die selbstsignierte *Root-CA* zu erstellen und zwei Public-Key-Infrastruktur-*Mounts* zu erzeugen. Einer fungiert als Ablageort für Zertifikatsautoritäten, der andere für Zertifikate. Weiterhin müssen noch einige URLs gesetzt werden und Rollen erstellt werden.

Erzeugen von Zertifikaten Einige Zertifikate müssen zur Laufzeit erzeugt werden, darunter fallen die Zwischenautoritäten und Client-Zertifikate. Hier wurden Skripte angelegt, die die minimal nötigen Daten sammeln und damit die geforderten Zertifikate anfordern.

Ausbringen von Zertifikaten Erstellte Zertifikate müssen ebenfalls zur anfragenden Instanz gesendet werden. Dabei ist ein Server, der ein passendes Protokoll wie SCEP implementiert und ebenfalls mit dem *Vault* kommunizieren kann, gefordert. Der Server ist somit das Bindeglied zwischen Public-Key-Infrastruktur und Klient.

Konfiguration der TLS-Terminierung Damit die TLS-Terminierung prüfen kann, ob ein Zertifikat gültig ist, muss diese alle nötigen Zertifikate, wie zum Beispiel die *Root-CA* und CRLs, erhalten können. Diese sollen ebenfalls an richtiger Stelle platziert werden.

5 ANALYSE DER NEUEN PUBLIC-KEY-INFRASTRUKTUR

Im Folgenden wird untersucht, ob die in Abschnitt 2 aufgezeigten Ungereimtheiten der bestehenden Public-Key-Infrastruktur durch das neue Vorgehen beglichen werden.

Rückdatierung und Laufzeit In der bestehenden Public-Key-Infrastruktur wurden Zertifikate rückdatiert und mit einer sehr hohen Laufzeit versehen. Im neuen Konzept können Zertifikate dynamisch nach Bedarf generiert und erneuert werden. So kann die Laufzeit beliebig klein gehalten werden. Diese kann zum Beispiel drei Monate betragen, welche jedoch in einem produktiven Test nachzuprüfen ist und gegebenenfalls optimiert werden kann.

Ausbringung der Zertifikate An dieser Stelle ist wieder die dynamische Generierung von Zertifikaten wichtig. In der bestehenden Implementierung werden generierte Zertifikate im Klartext mit der *Startkonfiguration* übertragen und dauerhaft abgelegt. Nun muss lediglich ein *Challenge*-Passwort mit beschränkter Laufzeit übertragen werden, damit ein Router autorisiert wird, sich ein Zertifikat signieren zu lassen.

Rückziehung von Zertifikaten Im bestehenden System ist das Zurückziehen von Zertifikaten nicht möglich. Durch Kombination von niedriger Laufzeit und erprobten Softwarelösungen können über den *Vault* die möglichst minimalen CRLs der jeweiligen Autoritäten bereitgestellt werden.

Terminierung der Verbindung Da nun, anders als im bestehenden System, CRLs an zentraler Stelle abrufbar sind, können diese auch an einem TLS-Endpunkt angefordert werden. Somit können ungültige Verbindungen terminiert werden, bevor sie am System eingehen.

Weitere Anforderungen Zusätzlich zur Optimierung der grundsätzlichen Abläufe sollte die Public-Key-Infrastruktur auch weitere Eigenschaften wie Flexibilität bei Chiffren und Schlüssellänge, aber auch bestimmte implementationstechnische Eigenschaften, vorweisen.

Eine Anforderung ist die freie Wahl des Ortes der Schlüsselmaterialgenerierung. Da das System Zertifikate mit CSRs anfragt, kann entweder Schlüsselmaterial mitgesendet werden oder diese Aufgabe an den *Vault* delegiert werden, sofern EST zum Einsatz kommt.

Zudem sollte die Ablage von Zertifikaten und Schlüsselmaterial sicher gestaltet werden. Um diesen Punkt kümmert sich der *Vault* selber, da dieser Paradigmen implementiert, welche wenig bis kaum

Möglichkeiten geben, an dieses Heranzukommen. Zusätzlich sollte die Public-Key-Infrastruktur so konzipiert sein, dass kein Zertifikat oder Schlüsselmaterial tatsächlich den *Vault* verlassen muss, um ein Zertifikat auszustellen. Hier sollte wieder EST in Betracht gezogen werden, um diese Anforderung vollends zu erfüllen.

Außerdem sollte die Public-Key-Infrastruktur im Kontext einer Cloudnative-Anwendung skalierbar sein, also zum Beispiel in Kubernetes ausgebracht werden können. *HashiCorp Vault* bietet diese Funktionalität. Da der Server für Zertifikatsanfragen in die Anwendung integriert werden soll, benötigt dieser kein weiteres Vorgehen für Skalierbarkeit.

6 ZUSAMMENFASSUNG

In diesem Paper wurde die bestehende Public-Key-Infrastruktur für TLS-Authentifizierung von Routern am *INSYS icom* Router Management beschrieben und einige optimierbare Stellen aufgezeigt (Abschnitt 2). Daraufhin wurde ein Konzept entworfen, welches diese ausmerzen soll sowie flexibel und einfach in der Handhabung ist (Abschnitt 3). Im darauffolgenden Abschnitt wurden Technologien und deren Zusammenspiel erläutert, welche solch ein System in der Realität implementieren können (Abschnitt 4). Schlussendlich werden die vorher genannten optimierbaren Stellen erneut aufgenommen und gegen das Lösungskonzept geprüft, um zu erschließen, ob diese verbessert und weitere Anforderungen erfüllt wurden (Abschnitt 5).

In diesem Paper zeigt sich, wie durch das geschickte Zusammenfügen von Technologien eine flexible und sichere Public-Key-Infrastruktur in ein Bestandssystem implementiert werden kann.

LITERATUR

- [1] A. Koohang, C. S. Sargent, J. H. Nord und J. Paliszkiwicz, „Internet of things (IoT): From awareness to continued use,“ *International Journal of Information Management*, Jg. 62, S. 102442, 1. Feb. 2022, ISSN: 0268-4012. DOI: 10.1016/j.ijinfomgt.2021.102442. Adresse: <https://www.sciencedirect.com/science/article/pii/S0268401221001353> (besucht am 28.01.2023).
- [2] „Insys-icom Homepage,“ *INSYS icom*. (), Adresse: <https://www.insys-icom.com/> (besucht am 03.01.2023).
- [3] „Was sind Kritische Infrastrukturen?“ Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: <https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine->

infos-zu-kritis.html?nn=126640 (besucht am 03.01.2023).

- [4] „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen,“ Bundesamt für Sicherheit in der Informationstechnik. (), Adresse: <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html?nn=433400> (besucht am 28.01.2023).
- [5] J. A. Buchmann, E. Karatsiolis und A. Wiesmaier, *Introduction to Public Key Infrastructures*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, ISBN: 978-3-642-40656-0 978-3-642-40657-7. DOI: 10.1007/978-3-642-40657-7. Adresse: <http://link.springer.com/10.1007/978-3-642-40657-7> (besucht am 04.10.2022).
- [6] P. Gutmann, „Simple Certificate Enrolment Protocol,“ Internet Engineering Task Force, Request for Comments RFC 8894, Sep. 2020, Num Pages: 42. DOI: 10.17487/RFC8894. Adresse: <https://datatracker.ietf.org/doc/rfc8894> (besucht am 11.10.2022).
- [7] „Vault by HashiCorp,“ Vault by HashiCorp. (), Adresse: <https://www.vaultproject.io/> (besucht am 10.01.2023).
- [8] *scep*, original-date: 2016-05-29T20:53:09Z, 8. Jan. 2023. Adresse: <https://github.com/micromdm/scep> (besucht am 10.01.2023).
- [9] M. Pritikin, P. E. Yee und D. Harkins, „Enrollment over Secure Transport,“ Internet Engineering Task Force, Request for Comments RFC 7030, Okt. 2013, Num Pages: 53. DOI: 10.17487/RFC7030. Adresse: <https://datatracker.ietf.org/doc/rfc7030> (besucht am 06.12.2022).

AUTOREN

Christopher Neldner ist Master of Science des Studiengangs Software Engineering.

Prof. Dr. Frank Herrmann wurde in Münster geboren und studierte Informatik an der Rheinisch-Westfälischen Technischen Hochschule in Aachen. Nach seinem Diplom 1989 arbeitete er bei dem Fraunhofer Institut IITB in Karlsruhe. Während dieser Zeit promovierte er 1996 über Ressourcenbelegungsplanungsprobleme. Von 1996 bis 2003 arbeitete er für die SAP AG in verschiedenen Funktionen, zuletzt als Direktor. Im Jahr 2003 wurde er Professor für Produktionslogistik an der Ostbayerischen Technischen Hochschule in Regensburg. Seine

Forschungsthemen sind Planungsalgorithmen, Optimierung und Simulation für die operative Produktionsplanung und -steuerung. Er ist Leiter des Innovations- und Kompetenzzentrums für Produktionslogistik und Fabrikplanung (IPF).

Evaluierung und Optimierung von Business-Intelligence-Systemen in der öffentlichen Verwaltung -Ein Use-Case-basierter Ansatz

Jacob Sietas
Fachbereich Wirtschaft
Hochschule Flensburg
Kanzleistraße 91 - 93
24943 Flensburg
jacob.sietas@hs-
flensburg.de

Kai Petersen
Fachbereich Wirtschaft
Hochschule Flensburg
Kanzleistraße 91 - 93
24943 Flensburg
kai.petersen@hs-
flensburg.de

Jan M. Gerken
Fachbereich Wirtschaft
Hochschule Flensburg
Kanzleistraße 91 - 93
24943 Flensburg
jan.gerken@hs-
flensburg.de

KEYWORDS

Business Intelligence, User Experience, Use-Case-Szenarien, öffentliche Verwaltung

ABSTRACT

Business-Intelligence-Systeme nehmen in vielen Organisationen einen zunehmend höheren Stellenwert ein. Dies gilt auch für die öffentliche Verwaltung. Dabei entwickeln sich BI-Systeme immer mehr zu einer Anwendung für breite Nutzerschichten. Im Rahmen des Forschungsprojekts BI-F2022 wurde eine Tagebuchstudie durchgeführt, um Anwendungsszenarien und Maßnahmen zur Verbesserung für ein eingeführtes BI-System zu identifizieren. Die Tagebuchstudie wurde in drei Abteilungen in der Stadtverwaltung Flensburg durchgeführt. Es wurden 17 Anwendungsszenarien und 32 Verbesserungsmaßnahmen erhoben. Mit der Tagebuchstudie konnten Verbesserungspotentiale und Lücken bei der Unterstützung der identifizierten Anwendungsszenarien aufgezeigt werden. Durch eine weitere Systematisierung der erhobenen Daten, konnten wichtige Bereiche für zukünftige Entwicklungen ergänzend identifiziert werden.

EINLEITUNG

Business-Intelligence-Systeme (BI-Systeme) und datengetriebene Analysemöglichkeiten nehmen in Unternehmen bereits einen hohen und in der öffentlichen Verwaltung einen zunehmenden Stellenwert ein. Die Stadt Kaiserslautern hat beispielsweise im Jahr 2020 ein BI-System auf kommunaler Ebene etabliert (Sprockamp 2020). Im öffentlichen Sektor werden Dashboards mittlerweile zur Kommunikation von Informationen verwendet. So erlangten zu Beginn der Covid-

19-Pandemie Dashboards in Bezug auf die Pandemieentwicklung Bekanntheit.

Diese zunehmenden Bedeutung von BI-Systemen in der öffentlichen Verwaltung findet auch in der Forschungslandschaft Ausdruck. So wurden BI-Systeme in der öffentlichen Verwaltung für Smart Cities (z.B. Carli et al. 2015, Payne et al. 2020), für die öffentliche Sicherheit (z.B. de Freitas Neto et al. 2014), für die Haushaltsverwaltung (Correia et al. 2021) und die Finanzplanung (Ramos et al. 2017) vorgestellt.

Der Erfolg von BI-Systemen wurde in der Vergangenheit aus unterschiedlichen Perspektiven untersucht. Unter anderem wurde die positive Auswirkung von Informationsqualität, Datenqualität, Lösungsumfang von BI-Systemen und insbesondere von Business-Intelligence-Management auf die Qualität unternehmerischer Entscheidungsfindung (Wieder & Ossimitz 2015) betrachtet. Es wurden Auswirkungen von BI-Systemen auf unterschiedliche Bereiche, wie die interne Prozesseffizienz und die Beziehung zu Zulieferern und Geschäftspartnern, beobachtet (siehe hierzu Elbashir et al. 2008).

Mit der zunehmenden Verbreitung von BI-Systemen entwickeln sich BI-Systeme mehr und mehr zu Anwendungen für breitere Nutzerschichten. Bisher gibt es allerdings nur wenige Ansätze, die sich der Evaluation von BI-Systemen aus Sicht der Nutzer*innen - anders formuliert: der User Experience von BI-Systemen - widmen. Bei der Implementierung ist die Beteiligung von Nutzer*innen von hoher Bedeutung, da ein Zusammenhang dieser Beteiligung mit dem organisationalen Umsetzungserfolg und dem Projektumsetzungserfolg besteht (Wixom & Watson 2001). Die hohe Bedeutung der Nutzerpartizipation wurde auch für die öffentliche Verwaltung bestätigt (Magaireh et al. 2019). Über die Anforderungen an die User Experience an BI-Systeme in der öffentlichen Verwaltung ist bisher nur wenig bekannt und es fehlt an methodischen Möglichkeiten zur Evaluierung der User Experience. In der jüngeren Vergangenheit wurde die Notwendigkeit standardisierter Rahmenmodelle zur Evaluierung festgestellt (Eriksson & Ferwerda 2021), für die es auch einer operativen Umsetzung bedarf. Im Zuge des Projekts BI-F2022 wurde ein methodisches Vorgehen zur Eva-

luierung der User Experience eines eingeführten BI-Systems entwickelt und angewendet.

Aus inhaltlicher Sicht gewährt dieser Beitrag Einblicke in die Anforderungen an BI-Systeme in der öffentlichen Verwaltung. Zwar wurden in der Vergangenheit erste Untersuchungen zu kritischen Erfolgsfaktoren bei der Einführung von BI-Systemen in der öffentlichen Verwaltung durchgeführt. Jedoch sind die Anforderungen aus der UX-Perspektive bisher nur wenig bekannt. Im Rahmen der hier durchgeführten Fallstudie wurde ein bereits eingeführtes BI-System evaluiert. Dabei wurde zwischen Anwendungsszenarien und Verbesserungspotenzialen unterschieden.

Aus methodischer Sicht wurde die Nutzbarkeit einer Tagebuchstudie zur Verbesserung von BI-Systemen in der öffentlichen Verwaltung aufgezeigt. Mit dem gewählten Ansatz konnten gezielt Maßnahmen aufgezeigt werden, deren Umsetzungen teilweise erfolgten. Bei dem gewählten methodischen Ansatz steht die Zweckerfüllung des BI-Systems aus Sicht der Nutzenden im Mittelpunkt, in dem systematisch Anwendungsszenarien erhoben und deren Erfüllungsgrad aufgezeigt wird. Gleichermaßen werden Verbesserungspotenziale erfasst und umgesetzt.

Durch die Erhebung von Anwendungsszenarien und Verbesserungspotenzialen sowie Kategorisierung dieser werden erste Einblicke in Anforderungen an BI-Systeme in der öffentlichen Verwaltung gewährt. Die Ergebnisse deuten darauf hin, dass insbesondere die pragmatische Qualität und die systematische Unterstützung von Anwendungsszenarien für BI-Systeme in der öffentlichen Verwaltung in einer frühen Phase der Etablierung des Systems von Bedeutung sind. Aus praktischer Sicht ermöglichte die Erhebung von Anwendungsszenarien und deren notwendigen Basisoperationen die Ableitung und Priorisierung zukünftiger Entwicklungen des eingeführten BI-Systems. Es konnten zudem für das Projekt Maßnahmen zur Verbesserung des BI-Systems aufgezeigt werden, die teilweise unmittelbar umgesetzt werden konnten.

LITERATURÜBERSICHT

Studien zur User Experience von BI-Systemen in der öffentlichen Verwaltung sind bisher wenig verbreitet - und dies trifft nicht nur auf den Bereich der öffentlichen Verwaltung zu. Eine systematische Literaturrecherche von Jooste, Van Biljon & Botha (2018) zeigte sogar auf, dass es zum Zeitpunkt der Literaturanalyse (Juli 2017) keine UX-Rahmenmodelle gab, die explizit für BI-Systeme ausgelegt sind. Um die Lücke der letzten fünf Jahre zu schließen, wurde im Rahmen dieser Studie eine erneute Literaturrecherche in unterschiedlichen Datenbanken durchgeführt und zunächst auf den Bereich der öffentlichen Verwaltung beschränkt. In einer zweiten Recherche wurde diese Fokussierung aufgegeben. Die durchgeführte Recherche bestätigt die Ergebnisse von Jooste, Van Biljon & Botha (2018) und es konnten nur wenige Ansätze identifiziert werden.

Die erste Recherche kombiniert Begriffe der Domänenperspektive (Öffentliche Verwaltung), Begriffe der Systemperspektive (Business Intelligence) und Begriffe der Zweckperspektive (User Experience). Für die Domänenperspektive wurden die Begriffe „public sector“ und „public administration“ verwendet. Die Systemperspektive wurde über die Begriffe „business intelligence“, „bi system“ und „dashboard“

operationalisiert. Der Begriff „dashboard“ wurde ergänzt, da das Dashboard in der Regel die Benutzerschnittstelle darstellt und somit einen zentralen Stellenwert der User Experience einnimmt. Die Begriffe „user experience“ und „user interface“ bildeten die Zweckperspektive ab. Die Berücksichtigung des Begriffs „user interface“ folgt der Logik der Berücksichtigung des Begriffs „dashboard“ und dient der Betonung der Benutzerschnittstelle. Auf die entsprechenden Abkürzungen wurde bewusst verzichtet, so dass der Schwerpunkt der Recherche auf einer hohen Genauigkeit lag. Die Recherche beschränkt sich auf englischsprachige wissenschaftliche Publikationen (wissenschaftliche Aufsätze, Konferenzbeiträge) und auf die Jahre 2017 bis 2022. Die Recherche erfolgte maßgeblich in den Metadaten, der Zusammenfassung und dem Titel. Die Recherchemöglichkeiten der unterschiedlichen Datenbanken wichen voneinander ab, so dass je nach Datenbank entsprechende Anpassungen notwendig waren. Im Falle von Semantic Scholar war eine Recherche mit Boolean Operatoren nicht möglich. Aufgrund der semantischen Suchmöglichkeiten wurde lediglich ein Begriff je Perspektive für die Recherche verwendet. Zudem wurde das Screening der Ergebnisse auf die ersten zehn Ergebnisseiten mit jeweils zehn Einträgen beschränkt. Die Recherche wurde im Oktober 2022 durchgeführt. Die Ergebnisse der ersten Recherche mit der Fokussierung auf die öffentliche Verwaltung blieb ergebnislos, so dass die Domänenperspektive in einer zweiten Recherche keine Berücksichtigung fand. Die Recherchestrategien der zweiten Recherche für die unterschiedlichen Datenbanken sind nachfolgend dargestellt:

- Lens.org
Suchbefehl: (title: ("business intelligence") OR abstract: ("business intelligence") OR keyword: ("business intelligence") OR field_of_study: ("business intelligence") OR title: ("bi system") OR abstract: ("bi system") OR keyword: ("bi system") OR field_of_study: ("bi system") OR title: ("dashboard") OR abstract: ("dashboard") OR keyword: ("dashboard") OR field_of_study: ("dashboard")) AND (title: ("user experience") OR abstract: ("user experience") OR keyword: ("user experience") OR field_of_study: ("user experience") OR title: ("user interface") OR abstract: ("user interface") OR keyword: ("user interface") OR field_of_study: ("user interface"))
Suchergebnisse: 254
Screeningergebnis: 3
- IEEEExplore
Suchbefehl: ("All Metadata": "Business Intelligence" OR "All Metadata": "bi system" OR "All Metadata": "dashboard") AND ("All Metadata": "user experience" OR "All Metadata": "user interface")
Rechercheergebnisse: 78
Screeningergebnis: 1
- Semantic Scholar
Suchbefehl: "business intelligence" "user experience"
Rechercheergebnis: 38.600
Screeningergebnis: 3

Die Recherche bei lens.org führte zu drei relevanten Publikationen (Kadir et al. 2021, Jooste et al. 2018, Eriksson & Ferwerda 2021). IEEEExplore ermöglichte die Identifizierung einer relevanten Publikation (Jooste et al. 2018). Die Recherche bei Semantic Scholar führte zu insgesamt 38.600

Rechercheergebnisse, die eine weitere relevante Publikation enthielten (Burnay et al. 2020). Insgesamt konnten somit vier Publikationen gefunden werden, wobei hier bereits die Studie von Jooste et al. (2018) berücksichtigt ist.

Die identifizierten Publikationen definieren einerseits Faktoren zur Evaluierung, betonen andererseits den Kontext und den Zweck von BI-Systemen bei deren Evaluierung:

Evaluationsfaktoren

Eriksson & Ferwerda (2021) stellen ein Rahmenmodell vor, dass die Bereiche UX-Strategie, Produkt-Benutzer-Interaktion, Usability, Kontext, Evaluation und Agile/Lean berücksichtigt. Dabei adaptieren sie die Key-Performance-Indikatoren Nützlichkeit (Utility), Gebrauchstauglichkeit (Usability), visuelle Attraktivität (visual attractiveness) und hedonische Qualität (hedonic quality) vorheriger Arbeiten (Schulze & Krömker 2010, Beauchaud & Kroemker 2013). Die Nützlichkeit beschreibt dabei, in welchem Umfang eine Software die zu lösen beabsichtigte Aufgabe unterstützt. Gebrauchstauglichkeit hingegen, wendet sich der Frage zu, ob und wie gut eine Software durch eine bestimmten Personengruppe für einen Zweck verwendet werden kann. Die visuelle Attraktivität adressiert die visuellen ästhetischen Eigenschaften einer Benutzerschnittstelle. Diese können motivierend für die Nutzung sein (Eriksson & Ferwerda 2021). Die hedonischen Faktoren stehen in Bezug zu den Emotionen der Nutzer*innen. Die Autoren betonen für ein BI System die „needs to feel motivated by using the system“ (Eriksson & Ferwerda 2021). Schulze & Krömker (2010) verwenden für die hedonische Qualität den Begriff der *be-goals*, dem der Begriff der *do-goals* gegenübersteht (Hassenzahl & Roto 2007). Die Bedeutung der hedonischen und pragmatischen Faktoren wurde bereits in anderen Bereichen dargelegt. So konnte bspw. für Business Management Software nicht nachgewiesen werden, dass die pragmatische Qualität einen höheren Einfluss auf die Attraktivität der Software hat, als die hedonische Qualität (Schrepp et al. 2006).

Burnay et al. (2020) fokussieren sich bei der User Experience von BI-Systemen explizit auf die Dashboards. Sie identifizieren als Qualitätskonstrukte die Dashboard-Relevanz, die Dashboard-Effizienz und die Ausgeglichenheit von Dashboards.

Aufgabenkompatibilität

Eriksson & Ferwerda (2021) betonen den Kontext vor dem Hintergrund der Zielorientierung in Bezug auf die Nutzerfreundlichkeit. Mit Verweis auf Gaardboe et al. (2017) stellen Sie heraus, dass die UX mit der Aufgabenkompatibilität gesteigert wird. Gaardboe et al. (2017) fanden einen positiven Zusammenhang zwischen der Aufgabenkompatibilität und der Nutzung von BI-Systemen, der Nutzerzufriedenheit und der individuellen Auswirkung. Ebenso konnte ein signifikanter Zusammenhang zwischen der Aufgabenkompatibilität und der Benutzerzufriedenheit aufgezeigt werden (Gaardboe 2018). Weitere Studien zu kritischen Erfolgsfaktoren von BI-Systemen weisen auf die Bedeutung eines klaren Zwecks hin (Yeoh & Popović 2016).

Kadir et al. (2021) stellen einen Ansatz vor, der User Stories verwendet. Vor dem Hintergrund dieser User Stories erfolgt die Bewertung der Dashboards durch die Nutzer*innen in den Kategorien Wirksamkeit (effectiveness), Effizienz (efficiency), Erlernbarkeit (learnability), Attraktivität (attractiveness), Beherrschbarkeit (controllability), Nützlichkeit (hel-

pfulness) und Zufriedenheit (satisfaction).

Kontext

Die Bedeutung des Kontextes wird bei Burnay et al. (2020) deutlich. Ebenso wird der Kontext im Rahmenmodell von Eriksson & Ferwerda (2021) berücksichtigt. Unter anderem ist dabei die Aufgabe, die damit gelöst werden soll, zu berücksichtigen. Die Bedeutung des Kontexts wird auch in weiteren Arbeiten unterstützt (z.B. Law et al. 2009), so dass eine wiederholte Evaluation von Nutzungen sinnvoll ist (Eriksson & Ferwerda 2021).

Das hier im Folgenden dargestellte Vorgehen zielt darauf ab, die dargebotenen Faktoren zu berücksichtigen, gleichermaßen jedoch auch Zweck und Kontext einzubeziehen. Dabei werden die Interdependenzen, die insbesondere bei Zweck und Nützlichkeit offensichtlich sind, berücksichtigt.

FALLSTUDIE

Die Durchführung dieser Fallstudie erfolgte im Rahmen des Projekts BI-F2022. Das Projekt BI-F2022 zielt auf die Einführung eines BI-Systems in der Stadtverwaltung Flensburg ab. Die vorliegende Studie wurde nach der Einführung des BI-Systems in einer zweiten Nutzungsphase durchgeführt. In einer ersten Nutzungsphase erfolgte bereits die Erhebung von Informationsbedürfnissen der Nutzer*innen mit Hilfe von Interviews sowie die Anpassung des Designs. Im Rahmen der Interviews wurden Daten identifiziert, die für die Arbeiten der Abteilungen und Fachbereiche notwendig sind. Zudem halfen die Interviews bei der Identifizierung von Faktoren, die für die Fachbereiche und Abteilungen für die erfolgreiche Einführung des BI-Systems von besonderer Bedeutung sind. Beispielhaft sind hier die Aspekte Datenschutz und Datenqualität zu nennen. Das BI-System war zu dem Zeitpunkt somit in unterschiedlichen Bereichen prototypisch etabliert. Die Expert*innen waren bereits mit dem System vertraut. Im Rahmen dieser Tagebuchstudie wurden Expert*innen befragt, die in den Fachabteilungen beschäftigt sind, jedoch im Rahmen des Projekts zur Einführung des BI-Systems als sogenannte Multiplikatoren mitwirkten. Die Expert*innen waren somit unmittelbar am Projekt beteiligt und verfügten gleichzeitig über eine fachliche Expertise, die die Formulierung von Anwendungsszenarien voraussetzt. Die fachliche Expertise ermöglichte so das Formulieren von Änderungsbedarfen an das BI-System.

METHODISCHES VORGEHEN

Der für die Evaluierung gewählte Ansatz berücksichtigt unterschiedliche Evaluationsfaktoren und eröffnet eine Perspektivenvielfalt. Dabei sollten sowohl Verbesserungsvorschläge als auch der Umsetzungsgrad von Anwendungsszenarien erfasst werden. Der Zweck wird dabei berücksichtigt und in Form von Use-Case-Diagrammen dargestellt. Der Raum wurde für weiteres Feedback geöffnet, so dass auch weitere Aspekte der Nützlichkeit, der Gebrauchstauglichkeit, der visuellen Attraktivität und der hedonischen Qualität artikuliert werden konnten. Dieses Feedback wurde in einem Feedback Grid zusammengetragen. Für die Berücksichtigung des Kontexts wurde zur Datenerhebung eine Tagebuchstudie durchgeführt, die Expert*innen über mehrere Tage begleitete. Zwar verblieben die Expert*innen im Kontext ihrer Abteilung und

ihres Aufgabengebiets, jedoch variierten die durchgeführten Aufgaben und täglichen Rahmenbedingungen im Verlauf der Durchführung.

Datenerhebung

Es wurden drei Expert*innen aus dem Fachbereich Bildung, der Abteilung Verkehr und der Statistikstelle während ihrer täglichen Arbeit im Rahmen eine mehrtägige Tagebuchstudie begleitet. Durch die mehrtägige Begleitung wurde gewährleistet, dass der Kontext der Erhebung sowie die zu erfüllenden Aufgaben einer Unterschiedlichkeit unterlagen. Der Fachbereich Bildung und die Statistikstelle wurden zehn Tage und die Abteilung Verkehr aus organisatorischen Gründen lediglich fünf Tage begleitet. Die Expert*innen waren an der Entwicklung der ersten Versionen der Dashboards beteiligt und waren somit mit dem BI-System vertraut. Die Befragung der Expert*innen erfolgte im Rahmen von halbstrukturierten Interviews, wobei eine einheitliche Interviewstruktur (siehe Abbildung 1) und ein standardisierter Interviewleitfaden (siehe Tabelle 1) zum Einsatz kamen. Der Fragebogen sieht Fragen zu Anwendungsfällen und Verbesserungspotenzialen vor. Ergänzend kam die Snippet Technique (Brandt et al. 2007) zum Einsatz. Die Expert*innen erstellten Screenshots in ihrer täglichen Arbeit, a) wenn ihnen etwas Negatives bei der Arbeit mit den Dashboards aufgefallen ist und b) wenn die Experten und Expertinnen eine Aufgabe mit den Dashboards gelöst hatten. Die Aufzeichnung der Interviews erfolgte mit Open Broadcaster Software.

Datensystematisierung

Die erhobenen Verbesserungspotenziale wurden in ein Feedback Grid (siehe hierzu Tullis & Albert 2013) übertragen. Das Feedback Grid hat die Ausprägungen Kritik, offene Fragen und Verbesserungsvorschläge. Gleichermaßen wurden positive Anmerkungen aufgenommen, die jedoch für die weitere Analyse und die Verbesserung des BI-Systems von untergeordneter Bedeutung waren.

Von den Probanden erläuterte Anwendungen des BI-Systems wurden mit Use-Case-Diagrammen (siehe hierzu Rupp et al. 2012) aufbereitet und dargestellt. Die Use-Case-Diagramme wurden für den Anwendungskontext adaptiert, in dem Anwendungsszenarien über Systemgrenzen modelliert wurden. Somit umfasst ein Anwendungsszenario ein oder mehrere Anwendungsfälle im Sinne der ursprünglichen Verwendung von UML-Diagrammen. Dabei erfolgte zunächst eine unmittelbare Aufbereitung nach den täglichen Interviews. Am Ende der Tagebuchstudie wurde eine Synthese der Anwendungsszenarien über den gesamten Zeitverlauf erstellt. Ein beispielhaftes Use-Case-Diagramm ist in Abbildung 2 dargestellt.

Identifikation von Basisoperationen

Die kodifizierten Kontexte in Form von Use-Case-Diagrammen erlaubten die Überführung der Anwendungsfälle in die Nomenklatur von BI-Systemen und es wurden anhand der Anwendungsfälle notwendige Basisoperationen identifiziert. Basisoperationen stellen grundlegende Operationen dar, die mit einem Dashboard bzw. einem BI-System realisiert werden können. Beispiele für solche Basisoperationen sind Werte erheben und abrufen, filtern, abgeleitete Wert berechnen, Extremwert finden, sortieren, Bereiche bestimmen, Anomalien finden und clustern (Amar et al. 2005). Basisoperationen begründen somit den Funktionsumfang eines BI-

Systems. Es wurden ergänzende Schnittstellen berücksichtigt (z.B. für die Datenlieferung), die für ein zukünftiges Automatisierungspotenzial von Bedeutung sein können. Dies sei anhand des Anwendungsszenarios „Zahlenspiegel veröffentlichen“ (siehe Abbildung 2) dargestellt. Für dieses Anwendungsszenario wurden fünf Anwendungsfälle modelliert. Für den Anwendungsfall „Daten einholen“ wurden insgesamt acht Basisoperationen identifiziert, die sich auf die Integration unterschiedlicher Daten beziehen. Um diesen unterschiedlichen Daten gerecht zu werden, wurden diese als einzelne Basisoperationen berücksichtigt. Zu den übrigen Anwendungsfällen wurden jeweils eine Basisoperation identifiziert. Basisoperation können als Fragen dargestellt werden (Jacob et al. 2011). Für die Auswertung wurden Basisoperationen nach diesem Schema als Fragen paraphrasiert. So wird beispielhaft für die Veröffentlichung des Zahlenspiegels folgende Frage formuliert: „Kann die Datenlieferung von Altersgruppen der Einwohner automatisiert in das BI erfolgen?“

Identifikation von Maßnahmen

Aus den Feedback Grids wurden Maßnahmen definiert, die zur Realisierung des Verbesserungspotenzials dienen. Ein Beispiel einer solchen Maßnahme ist die Anpassung des User Interfaces, indem Slider durch Auswahllisten ersetzt werden oder das Korrigieren von fehlerhaften Werten.

Evaluation und Implikationen

Anhand der identifizierten Maßnahmen und der Basisoperationen wurde zunächst eine Evaluation des bisherigen BI-Systems vorgenommen. Dazu wurden die Anwendungsszenarien hinsichtlich des Umfangs der umgesetzten Basisoperationen evaluiert.

Die Maßnahmen und Basisoperationen wurden anhand von zwei unterschiedlichen Klassifikationsschematas für weitere Einblicke systematisiert. Die Systematisierung der Maßnahmen erfolgte anhand des von Eriksson & Ferwerda (2021) vorgestellte Schemas. Die Klassifikation der Basisoperationen erfolgte mit einem induktiven Vorgehen, wobei Kategorien während der Systematisierung aus den vorhandenen Basisoperationen gebildet wurden. Daran anschließend wurden weitere Implikationen für die Verbesserung der UX abgeleitet, die sich maßgeblich aus den bisher nicht umgesetzten Basisoperationen und Maßnahmen ergaben.

Ergänzend erfolgte für die Umsetzung eine Priorisierung der Maßnahmen. Mehrfach genannte Maßnahmen wurden vorrangig umgesetzt, wobei sich aus dieser Priorisierung keine Gesetzmäßigkeit ableitet.

ERGEBNISSE UND DISKUSSION

Nachfolgend werden zunächst die Ergebnisse hinsichtlich der Anwendungsszenarien dargestellt. Es folgen die Ergebnisse hinsichtlich der erhobenen Maßnahmen.

Anwendungsszenarien und Basisoperationen

17 Anwendungsszenarien wurden erhoben. Sechs Anwendungsszenarien sind dem Fachbereich Bildung, sieben Anwendungsszenarien der Abteilung Verkehr und vier Anwendungsszenarien der Statistikstelle zugeordnet. Die Anwendungsszenarien sind in Tabelle 2 dargestellt und zusammenfassend beschrieben.

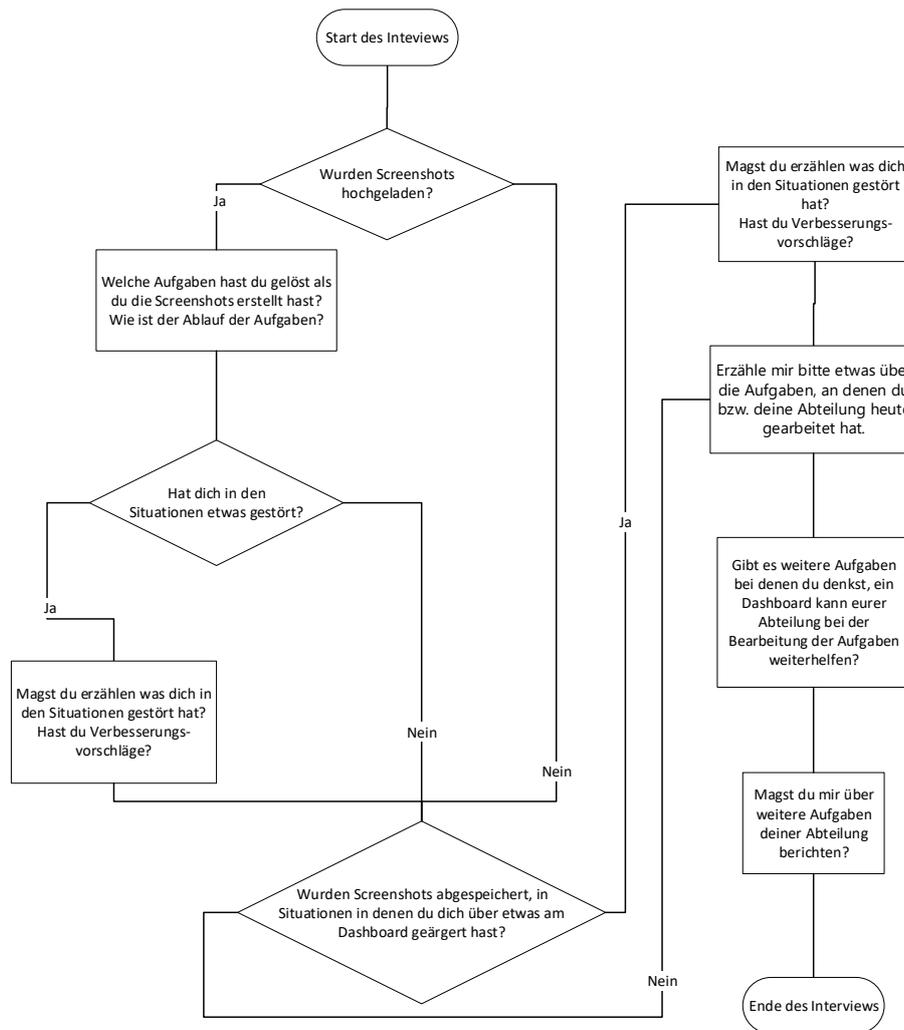


Abbildung 1: Flussdiagramm des Interviews

Für die Anwendungsszenarien konnten 84 Basisoperationen abgeleitet werden. Der Umsetzungsstand der Anwendungsszenarien der einzelnen Abteilungen und deren Basisoperationen ist in Tabelle 3 dargestellt. Hierauf wird nachfolgend eingegangen.

Bildung

In der Abteilung Bildung wurden insgesamt sechs Anwendungsszenarien abgebildet (siehe Tabelle 3). Gegenwärtig werden zwei der sechs Anwendungsszenarien teilweise von Basisoperationen unterstützt. Im Anwendungsszenario der „Bildungsberichterstattung“ werden sieben von elf Basisoperationen unterstützt. Im Anwendungsszenario „Dashboard zur Qualitätsmessung“ zur Unterstützung des Übergangs von der Schule in den Beruf werden zwei von vier Basisoperationen unterstützt. In den weiteren vier Anwendungsszenarien der Abteilung Bildung wird derzeit keine Basisoperation von den Dashboards ermöglicht.

Statistikstelle

In der Statistikstelle unterstützen Dashboards drei von vier Anwendungsszenarien teilweise. Im Anwendungsszenario „Analysen über Einwohnerstatistiken erstellen“ werden zwei von elf Basisoperationen unterstützt. Im Anwendungsszenario „Kleinräumige Gliederung aktualisieren“ wird eine von zehn Basisoperationen unterstützt und im Anwendungsszenario „Zahlenspiegel erstellen“ werden neun von zwölf Basisoperationen von den Dashboards unterstützt.

Verkehr

Das Anwendungsszenario „Geschwindigkeitsberuhigungsmaßnahmen prüfen“ wird in der Abteilung Verkehr vollständig unterstützt. In den anderen sechs Use-Case-Diagrammen in der Abteilung Verkehr unterstützt das BI-System keine Basisoperation. Einschränkend ist hier bereits festzustellen, dass im Erhebungszeitraum nicht alle durch das BI-System unterstützten Anwendungsszenarien umgesetzt worden sind. Aufgrund der induktiven Kategorisierung der Basisoperationen (siehe hierzu Abbildung 3) wird deutlich, dass insbe-

Tabelle 1: Interviewleitfaden Fragen und Zwecke der Fragen

Fragen	Zweck
Hat dich in den Situationen als du das Dashboard genutzt hast etwas gestört?	Mit dieser Frage wird der Proband angeregt darüber nachzudenken, ob ihm etwas bei der Nutzung des Dashboards gestört hat. Daraus kann ein Verbesserungspotential abgeleitet werden.
Magst du erzählen was dich in den Situationen gestört hat? Hast du Verbesserungsvorschläge?	Wenn dem Experten bzw. der Expertin etwas eingefallen ist, dass störend war, wurden Verbesserungspotentiale mit dieser Frage erhoben. Zudem wurden Vorschläge für bessere Darstellungsweisen auf dem Dashboard entgegen genommen.
Wurden Screenshots abgespeichert, in Situationen in denen du dich über etwas am Dashboard geärgert hast?	Mit dieser Frage können Verbesserungspotentiale erhoben werden.
Magst du erzählen was dich in den Situationen gestört hat? Hast du Verbesserungsvorschläge?	Mit dieser Frage wurden Verbesserungspotentiale erhoben, wenn ein Screenshot zu einem Problem abgespeichert worden ist.
Welche Aufgaben hast du gelöst, als du die Screenshots erstellt hast? Wie ist der Ablauf der Aufgaben?	Es wurde festgestellt, für welche Anwendungsszenarien die Dashboards derzeit genutzt werden.
Erzähle mir bitte etwas über die Aufgaben, an denen du bzw. deine Abteilung heute gearbeitet hat.	Es wurden Anwendungsszenarien erhoben an denen die Abteilung derzeit arbeitet. Anschließend wurde geprüft, ob diese durch Dashboards unterstützt werden können.
Gibt es weitere Aufgaben bei denen du denkst, ein Dashboard kann eurer Abteilung bei der Bearbeitung der Aufgaben weiterhelfen?	Die Experten und Expertinnen konnten bei dieser Fragestellung eigenständig Anwendungsszenarien nennen, bei denen sie durch Dashboards unterstützt werden können.
Magst du mir über weitere Aufgaben deiner Abteilung berichten?	Es wurden Anwendungsszenarien erhoben an denen die Abteilung gearbeitet hat. Es wurde geprüft, ob diese durch Dashboards unterstützt werden können.

sondere die Datenanalyse und die Datenlieferung von herausragender Bedeutung sind. Allerdings wird auch deutlich, dass sich die Bedürfnisse der Abteilungen unterscheiden. In der Abteilung Verkehr sind am meisten Basisoperationen der Kategorie Datenqualität zugeordnet. Hingegen sind es in der Abteilung Statistikstelle insbesondere Basisoperationen der Kategorie Datenanalyse. In der Abteilung Bildung sind die meisten Basisoperationen den Kategorien Datenlieferung und Datenverfügbarkeit zugeordnet. Hieraus kann bereits gefolgert werden, dass die Integration von weiteren Daten zukünftig von besonderer Bedeutung sein kann. Zudem kann die Auswertung auch ein Hinweis auf unterschiedliche Reifestadien des BI-Systems in den Abteilungen sein.

Maßnahmen

Ergänzend zu den bereits oben dargestellten 84 Basisoperationen wurden 32 Maßnahmen identifiziert. Die Maßnahmen ergaben sich aus zwölf Ideen, 17 Kritiken und drei offene Fragen. Darüber hinaus wurden sechs positive Rückmeldungen erhoben, aus denen keine unmittelbaren Maßnahmen entwickelt wurden. Diese wurde jedoch bei der Kategorisierung der Maßnahmen also solche berücksichtigt, um ein umfassenderes Bild zu erhalten. Für die Statistikstelle wurden insgesamt 15 Maßnahmen, für die Abteilung Bildung wurden sieben Maßnahmen und für die Abteilung Verkehr wurden zehn Maßnahmen erhoben. Fünf positive Rückmeldungen erfolgten durch die Statistikstelle. Eine positive Rückmeldung erfolgte durch die Abteilung Bildung. Eine Übersicht der Maßnahmenkategorisierung ist in Tabelle 4 zu finden.

In der Statistikstelle ordneten alle Experten die meisten Maßnahmen der Kategorie Nützlichkeit zu. Hier ist einschränkend zu erwähnen, dass zwei Expert*innen vier positive Rückmeldungen dieser Kategorie zuordneten (Bewerter*in 1 und 3). Der dritte Experte (Bewerter*in 2) ordnete drei positive Rückmeldungen dieser Kategorie zu. Bewerter*in 2 ordnete zwei, die übrigen Bewerter*Innen eine positive Rückmeldung der visuellen Attraktivität zu.

In der Abteilung Bildung wurde die positive Rückmeldung durchgängig von den Experten der Nützlichkeit zugeordnet. Ohne Berücksichtigung der positiven Rückmeldungen finden Benutzerfreundlichkeit und Nützlichkeit in der Abteilung Bildung insgesamt eine nahezu vergleichbare Anzahl von Kategoriezuordnungen.

Während in der Statistikstelle insbesondere die Nützlichkeit von hoher Bedeutung scheint und in der Abteilung Bildung die Benutzerfreundlichkeit und die Nützlichkeit nahezu ausgewogen sind, zeigt sich in der Abteilung Verkehr eine höhere Bedeutung der Benutzerfreundlichkeit. Allerdings ergibt sich hier ein abweichendes Bild zwischen den Expert*innen. Während zwei Expert*innen mehr Maßnahmen der Benutzerfreundlichkeit zugeordnet haben, hat der dritte bzw. die dritte Expertin mehr Maßnahmen der Nützlichkeit zugeordnet.

Insgesamt wird jedoch deutlich, dass die Nützlichkeit in der aktuellen Phase der Entwicklung des BI-Systems von besonderer Bedeutung scheint. Insgesamt sind hier 57 Kategoriezuordnungen festzustellen. 14 dieser Zuordnungen resultierten aus positiven Rückmeldungen. 40 Kategoriezuord-

Tabelle 2: Zusammenfassung der Anwendungsszenarien

Abteilung	Bezeichnung	Zeitintervall der Durchführung	Ziel
Bildung	Bildungsberichterstattung	jährlich	Veröffentlichung des Bildungsberichts
Bildung	Dashboard zur Qualitätsmessung	jährlich	Erleichterung des Überganges zwischen Schule und Beruf für junge Menschen
Bildung	Planung von Schulhöfen	unbekannt	Verbesserung der Planungsmöglichkeiten für die Instandhaltung, Wartung und Neuanschaffung von Spielgeräten auf den Schulhöfen
Bildung	Raumplanung an Schulen	jährlich	Planung der benötigten Räume für die Schulklassen
Bildung	Ressourcenverteilung anhand von Sozialindizes	jährlich	Verbesserung des Verfahrens der Ressourcenverteilung an die Schulen
Bildung	Verwaltung von Schulmöbeln	unbekannt	Planung von benötigtem Schulmöbeliar
Statistikstelle	Analysen über Einwohnerstatistiken erstellen	ad hoc	Beantwortung von Anfragen unterschiedlicher Personen und Organisationen zu Bevölkerungsdaten
Statistikstelle	Kleinräumige Gliederung aktualisieren	jährlich	Nachvollziehbarkeit von Grenzen in der Stadt
Statistikstelle	Straßenregister aktualisieren	monatlich	Führen eines Straßenverzeichnisses nach §3 StrWG
Statistikstelle	Zahlenspiegel erstellen	jährlich	Veröffentlichung von Daten für eine bessere Transparenz
Verkehr	E-Roller Nutzung	ad hoc	Darstellung des Nutzens von E-Rollern in der Mikromobilität
Verkehr	Fußgängerübergang planen	ad hoc	Gewährleistung sicherer Straßenübergänge für Fußgänger
Verkehr	Geschwindigkeitsberuhigungsmaßnahme überprüfen	unbekannt	Überprüfung der Wirkungsweise ergriffener Geschwindigkeitsberuhigungsmaßnahmen
Verkehr	Baumaßnahmen abstimmen	jährlich	Abstimmung von Baumaßnahmen zur Reduzierung von Baustellen
Verkehr	Monitoring über Einwohnerverhaltensweisen	ad hoc	Monitoring des Verhaltens der Einwohner der Stadt
Verkehr	Parkraumbewirtschaftungssystem	unbekannt	Prakraumbedarfabschätzung und Verbesserung des Parkleitsystems
Verkehr	Fahrradstellplatzbedarf prüfen	ad hoc	Steigerung der Attraktivität der Radnutzung

nungen wurden durch die Experten für die Benutzerfreundlichkeit vorgenommen. Positive Rückmeldungen sind nicht enthalten. Die visuelle Attraktivität wird insgesamt für 17 Kategoriezuordnungen verwendet. Vier dieser Zuordnungen erfolgen für positive Rückmeldungen.

Bei der Kategorisierung der Maßnahmen wurden keine Maßnahmen der hedonischen Qualität zugeordnet. Dies kann einerseits an der starken inhaltlichen Nähe zu der visuellen Attraktivität liegen, was explizit als Kategorie berücksichtigt wurde. Andererseits fanden von Wilamowitz-Moellendorff et al. (2006) eine Verschlechterung der hedonischen Qualität im Verlaufe der Zeit in Bezug auf die wahrgenommene Qualität. Dies wird maßgeblich durch die Vertrautheit mit einem Produkt getrieben. Die Durchführung der Tagebuchstudie erfolgte im Zuge der Einführung des BI-Systems. Zu dieser frühen Phase haben pragmatische Faktoren, die insbesondere die Zweckerfüllung in den Vordergrund stellen, eine höhere Bedeutung. Zudem muss der Aspekt der Zielorientierung von BI-Systemen (Eriksson & Ferwerda 2021) berücksichtigt werden, der die Erfüllung der Aufgabe - und damit die Nützlichkeit - betont.

Im Anschluss und während der Durchführung der Tagebuchstudie erfolgte die Umsetzung von insgesamt 27 Maßnahmen. 13 Maßnahmen davon entfallen auf die Statistikstelle, neun Maßnahmen auf die Abteilung Verkehr und fünf Maßnahmen auf die Abteilung Bildung.

Es wurden alle Maßnahmen umgesetzt, die keinen technischen Restriktionen unterlagen und die ohne eine zusätzliche Datenlieferung umgesetzt werden konnten. Fünf Maßnahmen konnten nicht umgesetzt werden. Dies betrifft die Verbesserung des responsive Designs, das Ergänzen eines Zurück-Buttons, das Hinzufügen von Altersgruppen, das Hinzufügen von individuellen Dashboards und eine automatische Anpassung von Tabellen an die Textbreite. Die Umsetzungen zu den Maßnahmen „Verbesserung vom responsive Design“, „das Hinzufügen eines Zurück-Buttons“ oder „eine automatische Anpassung der Spaltenbreite an die Textbreite“ ist technisch gesehen nicht bzw. nur mit sehr hohem Aufwand möglich. Für „das Hinzufügen von Altersgruppen“ und dem „Erstellen von individuellen Dashboards“ müssten weitere Daten in das BI-System geladen werden.

Tabelle 3: Anwendungsszenarien und deren Umsetzungsstand

Themengebiet	Bezeichnung	Anzahl Basisoperationen	Anzahl umgesetzter Basisoperationen	Umsetzungsgrad in %
Bildung	Bildungsberichterstattung	11	7	63,64
Bildung	Dashboard zur Qualitätsmessung	4	2	50,00
Bildung	Planung von Schulhöfen	3	0	0,00
Bildung	Raumplanung an Schulen	3	0	0,00
Bildung	Ressourcenverteilung anhand von Sozialindizes	9	0	0,00
Bildung	Verwaltung von Schulmöbeln	3	0	0,00
Statistikstelle	Analysen über Einwohnerstatistiken erstellen	11	2	18,18
Statistikstelle	Kleinräumige Gliederung aktualisieren	10	1	10,00
Statistikstelle	Straßenregister aktualisieren	2	0	0,00
Statistikstelle	Zahlenspiegel erstellen	12	9	75,00
Verkehr	E-Roller-Nutzung	3	0	0,00
Verkehr	Fußgängerübergang planen	2	0	0,00
Verkehr	Geschwindigkeitsberuhigungsmaßnahme überprüfen	2	2	100,00
Verkehr	Baumaßnahmen abstimmen	2	0	0,00
Verkehr	Monitoring über Einwohnerverhaltensweisen	3	0	0,00
Verkehr	Parkraumbewirtschaftungssystem	2	0	0,00
Verkehr	Fahrradstellplatzbedarf prüfen	2	0	0,00

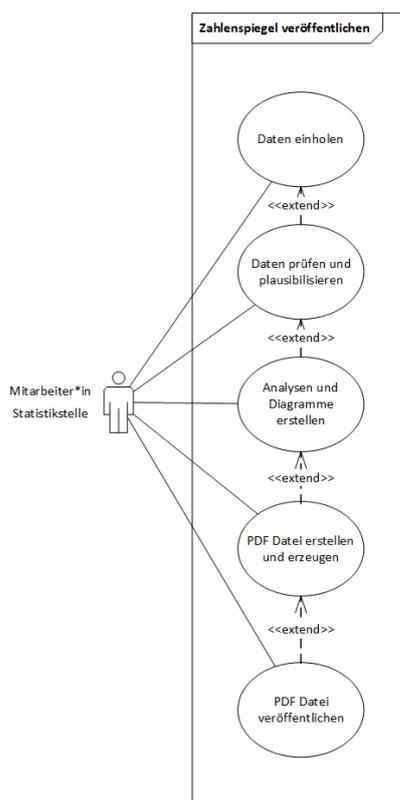


Abbildung 2: Beispielhaftes Use-Case-Diagramm

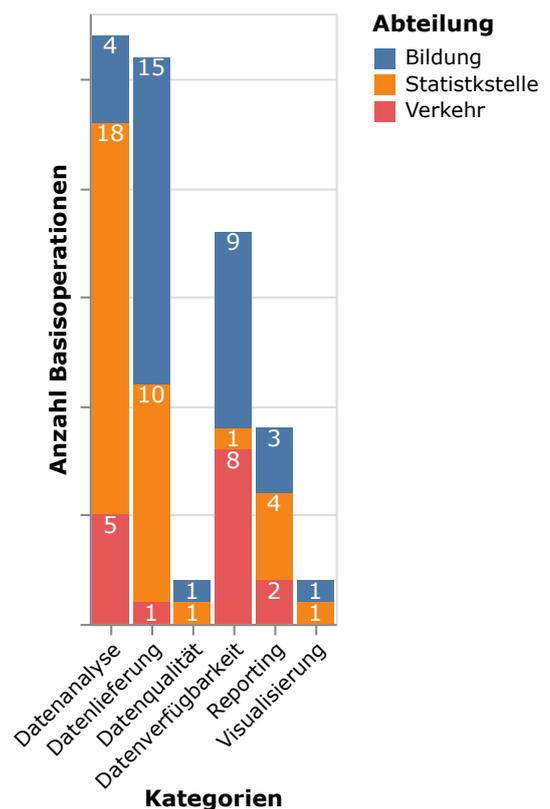


Abbildung 3: Basisoperationen je Abteilung

FAZIT UND AUSBLICK

Im Rahmen dieser Tagebuchstudie wurde ein Ansatz zur Erhebung der Unterstützung von Anwendungsszenarien ent-

wickelt, der eine Orientierung bei der Evaluierung der User

Tabelle 4: Die Maßnahmenkategorisierung je Abteilung

Statistikstelle							
	Bewerter*in 1	Bewerter*in 2	Bewerter*in 3	Minimum	Mittelwert	Median	Maximum
Benutzerfreundlichkeit	5	5	5	5	5	5	5
Nützlichkeit	12	10	11	10	11	11	12
Visuelle Attraktivität	3	5	4	3	4	4	5
Bildung							
	Bewerter*in 1	Bewerter*in 2	Bewerter*in 3	Minimum	Mittelwert	Median	Maximum
Benutzerfreundlichkeit	2	3	3	2	2,67	3	3
Nützlichkeit	5	4	3	3	4,00	4	5
Visuelle Attraktivität	1	1	2	1	1,33	1	2
Verkehr							
	Bewerter*in 1	Bewerter*in 2	Bewerter*in 3	Minimum	Mittelwert	Median	Maximum
Benutzerfreundlichkeit	6	7	4	4	5,67	6	7
Nützlichkeit	3	3	6	3	4,00	3	6
Visuelle Attraktivität	1	0	0	0	0,33	0	1
Gesamt							
	Bewerter*in 1	Bewerter*in 2	Bewerter*in 3	Minimum	Mittelwert	Median	Maximum
Benutzerfreundlichkeit	13	15	12	12	13,33	13	15
Nützlichkeit	20	17	20	17	19,00	20	20
Visuelle Attraktivität	5	6	6	5	5,67	6	6

Experience eines BI-System bietet. Zudem konnten so notwendige Maßnahmen zur Verbesserung aufgezeigt werden. Mit der hier dargelegten Methode konnten Verbesserungspotenziale aufgezeigt und Lücken des BI-Systems bei der Unterstützung von Anwendungsszenarien identifiziert werden.

Aus methodischer Sicht ermöglicht das hier vorgestellte Vorgehen die Erhebung und Operationalisierung von Anwendungsszenarien und Verbesserungspotenziale von BI-Systemen. Insbesondere wird eine Orientierung in Bezug auf die Unterstützung von Anwendungsszenarien durch das BI-System gegeben. Der Begriff der Orientierung wird bewusst gewählt, da das vorgestellte Vorgehen von einem konkreten Messmodell abzugrenzen ist. Beispielfhaft sei hier erneut die Veröffentlichung des Zahlenspiegels angeführt. Für diesen Systemrahmen konnten insgesamt zwölf Basisoperationen erfasst werden, von denen neun umgesetzt wurden. An dieser Stelle ist nicht die Schlussfolgerung zulässig, dass mit dem aktuellen Stand keine prozessuale Unterstützung gegeben sei. So ist bereits eine Unterstützung möglich, die zukünftig weiter ausgebaut werden kann. Ebenso kann damit nicht geschlossen werden, dass 75% des Prozesses der Veröffentlichung des Zahlenspiegels unterstützt werden. Den erhobenen Basisoperationen sind keine Aufwände, bspw. gemessen durch Durchführungszeiten, zugeordnet.

Aus inhaltlicher Sicht konnten im Rahmen des Projekts zudem unterschiedliche Anforderungen der Abteilungen aufgezeigt werden, die sich maßgeblich aus der Kategorisierung der Maßnahmen ergaben. Einschränkend ist festzustellen, dass die Kategorisierung lediglich durch einen Experten für die Basisoperationen und durch drei Experten für die Maßnahmen vorgenommen wurde. Hier kann zukünftig Notwendigkeit für eine umfassendere Erhebung bestehen.

Aus dem hier vorgestellten und angewendeten Ansatz ergeben sich ein praktischer Nutzen aus dem vorgestellten methodischen Ansatz sowie unmittelbar für das BI-System der Stadt Flensburg.

Für Unternehmen und öffentliche Institution wird mit dem hier dargelegten Ansatz ein Vorgehen vorgestellt, das eine systematische Erfassung der Unterstützung von Anwendungsszenarien eines BI-Systems ermöglicht. Fehlende Basisoperationen können identifiziert und, je nach Priorisierung, implementiert werden.

Im Rahmen des vorliegenden Projektes konnten gezielt Maßnahmen aus den Bereichen Benutzerfreundlichkeit, Nützlichkeit und visuelle Attraktivität adressiert und umgesetzt werden, die die User Experience des Systems verbessern.

Aus wissenschaftlicher Sicht konnten Einblicke an die Anforderungen an BI-Systeme in der öffentlichen Verwaltung gewonnen werden. Allerdings ergibt sich an dieser Stelle bereits weiterer Forschungsbedarf, der sich aus den Limitierungen der Studie ableiten lässt.

Das dargelegte Vorgehen unterliegt insbesondere methodischen Limitierungen, die sich (i) aus der Vertrautheit der Autoren mit dem System (ii) der kurzen Erhebungsphase und (iii) dem geringen Umfang der Interviewpartner*innen ergeben.

- (i.) Die Autoren begleiten zum Zeitpunkt der Durchführung der Studie das Projekt seit mehr als einem Jahr. So konnte umfassendes Kontextwissen in die Identifizierung der Basisoperationen einfließen. Diese Vertrautheit mit den Prozessen und dem BI-System ermöglicht die gezielte Identifizierung von notwendigen Basisoperationen. Diese Vertrautheit beider Perspek-

tiven kann bei der Einführung eines BI-Systems nicht immer gewährleistet werden.

- (ii.) Die Erhebungsphase war mit zehn bzw. fünf Tagen verhältnismäßig gering. Eine längere Erhebungsphase hätte weitere Verbesserungspotenziale, Anwendungsszenarien und daraus abgeleitete Basisoperationen aufzeigen können. Die Stadtverwaltung führte in dem Erhebungszeitraum nicht sämtliche Anwendungsszenarien durch, die ggf. bereits durch das BI-System bedient werden. So entsteht ein leicht verfälschendes Bild hinsichtlich des Unterstützungsgrads des bestehenden BI-Systems.
- (iii.) Die durchgeführten Interviews bieten nur einen kleinen Einblick in die Arbeit in der öffentlichen Verwaltung. In Rahmen des durchgeführten Projektes waren Bereiche involviert, die mit umfassenden Berichtsfunktionen betraut sind. Hier besteht eine gewissen Homogenität, die jedoch nicht gesamthaft für Entscheidungsprozesse in der öffentlichen Verwaltung gelten mag.

DANKSAGUNG

Das Projekt „Aufbau und Erprobung eines Business Intelligence Systems im realen Testbetrieb in der Flensburger Stadtverwaltung (BI-F2022)“ wurde im Rahmen der Innovationsinitiative mFUND durch das Bundesministerium für Digitales und Verkehr gefördert.

Im Rahmen der Innovationsinitiative mFUND fördert das BMDV seit 2016 datenbasierte Forschungs- und Entwicklungsprojekte für die digitale und vernetzte Mobilität der Zukunft. Die Projektförderung wird ergänzt durch eine aktive fachliche Vernetzung zwischen Akteuren aus Politik, Wirtschaft, Verwaltung und Forschung und durch die Bereitstellung von offenen Daten auf der Mobilithek. Weitere Informationen finden Sie unter www.mFUND.de.

Die Autoren danken dem Mittelgeber für die Unterstützung sowie den Projektpartnern für die Zusammenarbeit im Zug der Durchführung der Studie.

Literatur

Amar, R., Eagan, J. & Stasko, J. (2005), Low-level components of analytic activity in information visualization, in 'IEEE Symposium on Information Visualization, 2005. INFOVIS 2005.', IEEE, pp. 111–117.

URL: <https://doi.org/10.1109/INFVIS.2005.1532136>

Beauchaud, K. & Kroemker, H. (2013), 'Customer experience and user experience interaktiver produkte — ein metamodel für die produktentwicklung', *Zeitschrift für Arbeitswissenschaft* **67**, 105–111.

URL: <https://doi.org/10.1007/BF03373910>

Brandt, J., Weiss, N. & Klemmer, S. R. (2007), txt 4 l8r: lowering the burden for diary studies under mobile conditions, in 'CHI'07 extended abstracts on Human factors in computing systems', pp. 2303–2308.

URL: <https://dl.acm.org/doi/10.1145/1240866.1240998>

Burnay, C., Bouraga, S., Faulkner, S. & Jureta, I. (2020), User-experience in business intelligence - a quality construct and model to design supportive bi dashboards, in 'RCIS'.

URL: https://doi.org/10.1007/978-3-030-50316-1_11

Carli, R., Albino, V., Dotoli, M., Mummolo, G. & Savino, M. (2015), A dashboard and decision support tool for the energy governance of smart cities, in '2015 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS) Proceedings', pp. 23–28.

URL: <https://doi.org/10.1109/EESMS.2015.7175846>

Correia, A., Águas, P. B. & Luís, A. (2021), Business intelligence supporting budget management, in '2021 16th Iberian Conference on Information Systems and Technologies (CISTI)', pp. 1–6.

URL: <https://doi.org/10.23919/CISTI52073.2021.9476430>

de Freitas Neto, F. P., de Castro, A. F. & das Chagas de Lima, F. (2014), Business intelligence applied in decision support for public safety, in '2014 9th Iberian Conference on Information Systems and Technologies (CISTI)', pp. 1–6.

URL: <https://doi.org/10.1109/CISTI.2014.6876984>

Elbashir, M. Z., Collier, P. A. & Davern, M. J. (2008), 'Measuring the effects of business intelligence systems: The relationship between business process and organizational performance', *International Journal of Accounting Information Systems* **9**, 135–153.

URL: <https://doi.org/10.1016/j.accinf.2008.03.001>

Eriksson, M. & Ferwerda, B. (2021), 'Towards a user experience framework for business intelligence', *Journal of Computer Information Systems* **61**(5), 428–437.

URL: <https://doi.org/10.1080/08874417.2019.1693936>

Gaardboe, R. (2018), 'The relationship between system user's tasks and business intelligence (bi) success in a public healthcare setting', *Electronic Journal of e-Government* **16**(2), 87–97.

Gaardboe, R., Sandalgaard, N. & Sudzina, F. (2017), The importance of task compatibility for web-enabled business intelligence success in e-government, in 'Proceedings of the 19th international conference on information integration and web-based applications & services', pp. 353–357.

URL: <https://dl.acm.org/doi/10.1145/3151759.3151782>

Hassenzahl, M. & Roto, V. (2007), 'Being and doing: A perspective on user experience and its measurement', *Interfaces* **72**, 10–12.

Jacob, O., Weiß, N. & Schweig, J. (2011), Konzeption und Gestaltung von Management Dashboards, Technical Report 18, Neu-Ulm: Hochschule für angewandte Wissenschaften.

Jooste, C., Van Biljon, J. & Botha, A. (2018), A conceptual framework representing the user experience for business intelligence front-ends, in '2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)', pp. 1–8.

URL: <https://doi.org/10.1109/ICABCD.2018.8465464>

Kadir, N. T., Hartanto, R. & Sulistyono, S. (2021), 'Modified usability test scenario: User story approach to evaluate data visualization dashboard', *IJITEE (International Journal of Information Technology and Electrical Engineering)* **5**(1), 1–8.

URL: <https://doi.org/10.22146/ijitee.61201>

- Law, E. L.-C., Roto, V., Hassenzahl, M., Vermeeren, A. P. & Kort, J. (2009), Understanding, scoping and defining user experience: a survey approach, in 'Proceedings of the SIGCHI conference on human factors in computing systems', pp. 719–728.
URL: <https://doi.org/10.1145/1518701.1518813>
- Magaireh, A. I., bte Sulaiman, H. & Ali, N. (2019), 'Identifying the most critical factors to business intelligence implementation success in the public sector organizations', *The Journal of Social Sciences Research* **5**(2), 450–462.
- Payne, B., Ling, L. O. & Gorod, A. (2020), Towards a governance dashboard for smart cities initiatives: a system of systems approach, in '2020 IEEE 15th International Conference of System of Systems Engineering (SoSE)', pp. 587–592.
URL: <https://doi.org/10.1109/SoSE50414.2020.9130542>
- Ramos, J., Alturas, B. & Moro, S. (2017), Business intelligence in a public institution — evaluation of a financial data mart, in '2017 12th Iberian Conference on Information Systems and Technologies (CISTI)', pp. 1–6.
URL: <https://doi.org/10.23919/CISTI.2017.7975672>
- Rupp, C., Queins, S. et al. (2012), *UML 2 glasklar: Praxiswissen für die UML-Modellierung*, Carl Hanser Verlag GmbH Co KG.
- Schrepp, M., Held, T. & Laugwitz, B. (2006), 'The influence of hedonic quality on the attractiveness of user interfaces of business management software', *Interacting with Computers* **18**, 1055–1069.
URL: <https://doi.org/10.1016/j.intcom.2006.01.002>
- Schulze, K. & Krömker, H. (2010), A framework to measure user experience of interactive online products, in 'Proceedings of the 7th international conference on methods and techniques in behavioral research', pp. 1–5.
URL: <https://doi.org/10.1145/1931344.1931358>
- Sprockamp, E. (2020), 'Datengestützt handeln', *Kommune21* .
- Tullis, T. & Albert, W. (2013), *Measuring the user experience: collecting, analyzing, and presenting usability metrics*, Morgan Kaufmann.
URL: <https://doi.org/10.1016/B978-0-12-415781-1.00005-4>
- von Wilamowitz-Moellendorff, M., Hassenzahl, M. & Platz, A. (2006), Dynamics of user experience: How the perceived quality of mobile phones changes over time. in user experience—towards a unified view, p. 74–78.
- Wieder, B. & Ossimitz, M.-L. (2015), 'The impact of business intelligence on the quality of decision making—a mediation model', *Procedia Computer Science* **64**, 1163–1171.
URL: <https://doi.org/10.1016/j.procs.2015.08.599>
- Wixom, B. & Watson, H. (2001), 'An empirical investigation of the factors affecting data warehousing success', *MIS Quarterly* **12**, 17–41.
URL: <https://doi.org/10.2307/3250957>
- Yeoh, W. & Popovič, A. (2016), 'Extending the understanding of critical success factors for implementing business intelligence systems', *Journal of the Association for Information Science and Technology* **67**, 134–147.
URL: <https://doi.org/10.1002/asi.23366>

KONTAKT

JACOB SIETAS ist wissenschaftlicher Mitarbeiter an der Hochschule Flensburg. Derzeit forscht er im Projekt BI-F2022. Zuvor hat er seinen Master im Bereich angewandte Informatik an der Hochschule Flensburg erfolgreich absolviert. Zudem hat er in der Versicherungsbranche und im Verlagswesen in den Bereichen Data Science und Business Intelligence gearbeitet.

KAI PETERSEN ist Professor für Software Engineering an der Hochschule Flensburg und am Blekinge Institute of Technology. Im Kontext seiner Forschung beschäftigt er sich mit agiler Softwareentwicklung, Softwaretesten, Evidenz-basierter Software-Entwicklung und Softwaremetriken. Seine Forschung wurde in enger Industriekollaboration durchgeführt, beispielsweise mit Opel, Ericsson, Scania und Sony.

JAN GERKEN ist Professor für Data Science an der Hochschule Flensburg. Seine Forschungsinteressen umfassen unter anderem die Bereiche Data Science, Natural Language Processing, Künstliche Intelligenz und Scientometrics. Zuvor war er Mitgründer und Geschäftsführer eines Technologieunternehmens, das sich auf die semantische Analyse und die Visualisierung semantischer Zusammenhänge von umfassenden Dokumentenlandschaften fokussierte.

Digitisation funding for small and medium-sized enterprises in Germany using the example of the Digitalprämie Berlin

Paul Sonnenberg

Wirtschaft, Informatik, Recht

Technische Hochschule Wildau
Hochschulring 1, 15745 Wildau
15745 Wildau

E-Mail: paulsonnenberg@t-online.de

ABSTRACT

In the following article, the Digitalprämie Berlin (Digital Premium Berlin) and its effects and impacts will be analysed and put into context with its new edition. The evaluation of the first funding period directly influenced the structure of the new edition. In this article, the current state of digitisation support for small and medium-sized enterprises and its change will be exemplified using the Digitalprämie Berlin. This article is based on the "Bericht zur Auswertung der Digitalprämie Berlin" by the public DAB Digitalagentur Berlin GmbH (DAB), which the author contributed to as part of his employment at DAB. The Digitalprämie Berlin, initiated by the state of Berlin, is a public funding programme to promote the digitisation of small and medium-sized enterprises in Berlin. It ran from 02.11.2020 to 31.10.2021. The new funding period began on 15.08.2022.

KEY WORDS

Digitisation, Funding, Small and Medium Enterprises, Digitalprämie Berlin

INTRODUCTION

Digitalisation is a megatrend that is nourished by networked production and globalisation and makes the digitalisation of companies and administration necessary across the board. Last but not least, the Corona crisis, its impact on consumer behaviour and supply chains, as well as the changing geopolitical situation, reinforce the need for the digitalisation of companies (Zimmermann 2021).

Digitisation as a term has no clear definition, but has various dimensions in its meaning. In a narrower sense, digitalisation refers to the transformation and representation of analogue processes, products and business models into digital ones. In a broader sense, it also refers to the digital revolution, similar to the industrial revolution (Bendel 2021).

Digitalisation is changing the way companies are founded, built up and developed. In addition to new business areas, innovative products and technologies, the sustainable digitisation of fundamental business processes of all market participants, especially small and medium-

sized enterprises (SMEs), is increasingly at the centre of state funding in Germany. (Bundesregierung 2022) and Europe (European Commission 2008).

According to the European Commission, small and medium-sized enterprises are all enterprises with fewer than 250 employees and less than 50 million euros in annual turnover, or an aggregate balance sheet total not exceeding 43 million euros (European Commission 2003). Small and medium-sized enterprises play a prominent role in Germany, accounting for 99.4 percent of all enterprises, 56.3 percent of all employees and 29.4 percent of GDP (Statistisches Bundesamt 2019). Small and medium-sized enterprises are therefore often referred to as the backbone of the German and European economy, as the distribution of SMEs is similar throughout the European Union (EU) (Papadopoulos 2018). Their importance for society and politics is steadily increasing (European Commission 2008).

However, small and medium-sized enterprises still have significant potential in the context of the digitalisation of business processes and business models compared to large companies and corporations. For example, 17 percent of German SMEs employ IT specialists. In contrast, 78 percent of large companies employ IT specialists. Furthermore, while 22 percent of German SMEs are making efforts in the area of digital training, the figure for large companies is 73 percent (Institut für Mittelstandsforschung 2021). Overall, it is assumed that about 30 percent of large German companies are digitalised in the sense of using data and algorithms for business processes and models. In contrast, only 20 percent of SMEs are considered digitalised, with 80 percent still in the computerisation stage, using technical tools for analogue processes (Lichtblau 2018).

This statistical disparity also manifests itself directly in economic disparities, e.g. when 19 percent of SMEs were able to increase their online turnover compared to the previous year, but in contrast 38 percent of large companies were also able to increase their online turnover (Institut für Mittelstandsforschung 2021). In principle, the digital transformation of business processes and business models leads to more turnover and profit. In addition to higher profits and new customers, digitalised processes also

make it easier to find and recruit employees. Furthermore, digital processes are generally more efficient and effective than comparable analogue business processes, which is due to the scalability of digital products. (Lichtblau 2018).

This increased efficiency and scalability has a direct impact on the global competitiveness and innovative strength of Germany and Europe as a business location, which is why the promotion of digitisation, including for small and medium-sized enterprises, is increasingly becoming the focus of political attention (European Commission 2008). This is particularly evident in the Federal Government's new digitisation strategy. In a total of 24 areas of this strategy, lighthouse projects organised by the ministries are being promoted and implemented. SMEs play an outstanding role here, particularly in the context of artificial intelligence (Bundesregierung 2022).

Grants are awarded on the basis of European state aid law, Art. 107 et seq. TFEU3 and the criteria established by the European Commission for "de minimis" aid (European Commission 2013). Germany ranks 13th out of 27 EU member states in the European Commission's Digital Economy and Society Index (DESI). The DESI measures the socio-economic status of EU member states on the basis of criteria such as digital infrastructure, digitisation of companies and administration, and the ability of the population to use digital technologies (European Commission 2022). This placement of Germany and Berlin's position as the capital of the largest economy in the EU, combined with an exemplary diversified economy, make Berlin an ideal candidate for consideration.

DIGITALPRÄMIE BERLIN

Initial Situation

Berlin is also characterised primarily by small and medium-sized enterprises. These regard above all the financial investment in digitisation projects as a significant hurdle (Mittelstand 4.0 Kompetenzzentrum Berlin 2021). Based on this initial situation, the Senate Administration for Economic Affairs, Energy and Industry launched the Digitalprämie Berlin on 2 November 2020 and commissioned Investitionsbank Berlin Business Team GmbH (IBT), a wholly-owned subsidiary of the Investitionsbank Berlin Unternehmensverwaltung, to implement the funding programme (Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe 2019a).

As the central coordination agency for all digitalisation measures for companies in Berlin and as a spin-off of Investitionsbank Berlin (IBB) and sister company of IBT, it is the responsibility of DAB Digitalagentur Berlin GmbH to evaluate and interpret the Digitalprämie Berlin and to derive possible recommendations for further measures from the data (Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe 2019b).

The Digitalprämie Berlin was primarily intended to strengthen the competitiveness and future viability of Berlin's SMEs by creating financial incentives for SMEs and the self-employed to invest in digitisation projects. The Covid 19 pandemic intensified the need for companies to digitalise their business processes and to open up new digital sales channels as well as new digital business fields. At the same time, slumps in sales and the continuing reluctance of consumers created worse conditions for investment in their own modernisation projects. In this respect, the Digitalprämie Berlin not only had the task of securing the future and innovative strength of Berlin companies, but also of counteracting the economic consequences of the pandemic.

The Digitalprämie Berlin can be applied for entirely online and had a comprehensive scope of funding that was not limited to specific industries, trades or social or geographical characteristics. The support measures themselves were also not limited to certain software or hardware or services, as long as it followed the purpose of the digitalisation of the company. In this respect, the Digitalprämie Berlin pursued a broad funding approach with the aim of reaching as many SMEs as possible and supporting their initial digitisation with the broadest possible funding (Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe 2019a).

First funding period

Structure

In principle, the Digitalprämie Berlin was a non-repayable grant for private companies. The amount of the grant differed in the first funding period in the "Basic" and "Plus" modules. The "Basic" module of up to 7,000.00 euros was aimed at SMEs and solo self-employed persons with up to 10 employees. While companies with more than 12.5 and up to 249 employees were assigned to the "Plus" module and could receive subsidies of up to 17,000.00 euros. In principle, only digitisation projects that had not yet begun were eligible for funding. However, it was possible for companies in the "Basic" module to apply for an early start to the measures. This was intended to speed up the implementation of the digitisation projects and counteract a possible overload of the administration. This was not possible in the "Plus" module. Funding was provided for operational investments in the areas of:

- Digital work and production processes
- Digital management processes
- Introduction or improvement of IT security
- Digital consulting and qualification

The funding programme was aimed at all companies with up to 249 employees and a branch in Berlin that comply with the Berlin state minimum wage. Applicants did not have to choose one of the above categories, but could put together a package of a maximum of ten individual measures from different areas and apply for these once

only (Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe 2019a).

Research questions & methods

The evaluation and analysis of the funding program was basically already carried out during the funding period, but was not fully addressed until the end of the measure. A special feature of the evaluation is the way in which data can be processed and evaluated. The applications were submitted by the companies together with the desired measures, but were separated from each other during the process, so that it is not possible on the system side to link the companies with the respective measures. The separation of the data and its anonymization in the process is based on the DSGVO (DAB Digitalagentur Berlin 2022).

Another challenge arose from the large number of free text fields in the application, which should ensure a certain low-threshold. These factors resulted in less concrete data and more many complex texts. Thus, the data was sorted primarily using Natural Language Processing (NLP), logical clustering, and keywording, and then transferred into presentable data. The entire process took place in several iterations.

The most important questions for the evaluation were above all the type, industry and size of the respective companies, their funding objects and the amount of the respective funding. Furthermore, the motivation for digitization and their level of digital maturity were of interest. The main aim was to find out who applied for the funding and what conclusions could be drawn from this for Berlin as a location, the digitization of SMEs and the funding program, and whether the funding was allocated in the interests of the funding provider. In this respect, the question is whether so-called windfall effects have occurred, and if so, how and to what extent. This gives rise to further questions, in particular about the possible avoidability of these possible effects.

Evaluation

The dataset evaluated by the DAB consists of 1,720 superordinate entries, which contain the key data of the approved funding applications and answers of the funded companies to several questions to be answered during the application. Since one application could contain up to ten individual measures, the finally evaluated data set comprises a total of 4,020 individual measures. The answers to the questionnaire provided information on the company's activities, the goals of the digitisation measures, the exact purpose of the subsidies and the course of the project. Further information such as number of employees, annual turnover and project costs made it possible to categorise the applicants.

The 18 entries per application and the sometimes large number of words in the free text fields for more complex questions made a more thorough analysis of the available

data difficult. For the statistical evaluation of this unstructured data, it was logically grouped by hand and then analysed using a machine learning method. With the help of, the entries were then classified using keywords and assigned to a series of predefined categories. In this way, despite the diversity and size of the data set, insights into the use of the Digitalprämie Berlin as well as an overview of the funded companies could be gained.

Keywords such as product names were used to group the digitisation measures according to hardware, software and other expenditures and to sort them into subcategories. In order to guarantee the most precise data analysis possible, the keywords that could not be assigned by the NLP procedure were categorised again manually. Despite the relatively high accuracy of the procedure, a certain error rate cannot be ruled out.

The technical implementation of the NLP procedure was carried out in cooperation with an independent Berlin-based service provider. The evaluation and interpretation of the data was carried out by the DAB Digital Agency Berlin with the cooperation of the author. The aim of this evaluation was to gain knowledge from the application data about the funding recipients, the funded projects and the type of digitisation projects (DAB Digitalagentur Berlin 2022).“

RESULTS AND INTERPRETATION

Results

A total of 25 million euros was disbursed to over 4,000 companies (Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe 2022). In this context, 71 percent of all funded companies had measures for the "Basic" module funded, while 29 percent had the "Plus" module funded. Of 4,010 approved individual measures and 1,720 applications (as of 25.10.2021), 71 percent were part of the "Basic" module and 29 percent were part of the "Plus" module.

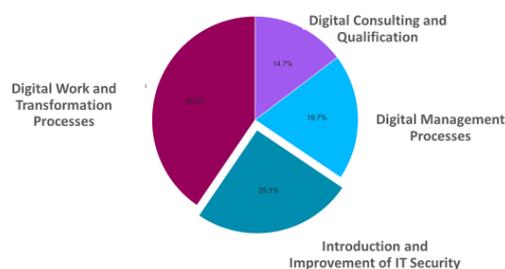


Figure 1 – Distribution of companies along modules

As can be seen in Figure 1, measures were registered primarily for the module Digital Work and Transformation Processes. This was closely followed by measures for IT security with 25.1 percent. The modules Digital Management Processes and Digital Consulting and Qualification accounted for 19.7 percent and 14.7 percent of the funded measures, respectively.

Mostly small projects with an average value of about 7,800 euros were funded by small and medium-sized enterprises with up to 180 employees. Of these, 66 per cent had fewer than 10 employees, 28.2 per cent had between 10 and 50 and only 5.8 per cent had between 50 and 249 employees, as can be seen in Figure 2.

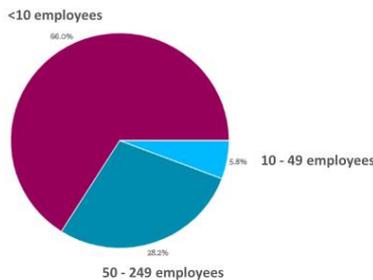


Figure 2 – Distribution along number of employees

Regarding the turnover of companies that partook in the Digitalprämie Berlin most ranged within the range of 10,000 to 1,000,000 euros. Logically the companies with the highest annual turnover applied for the module “Plus”. Otherwise the overall allocation above both modules as shown in Figure 3 shows that most companies were established SMEs.

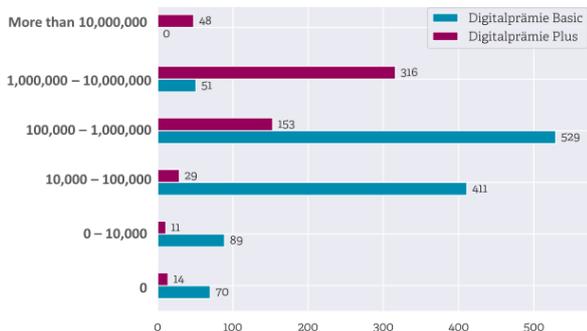


Figure 3 – Comparison of annual turnover along modules

The two largest individually stated sectors of the supported companies were information and communication technology (ICT) and medical technology. Construction and the food industry followed in third place. In total, there were 24 predefined sectors from which companies could choose. 45.9 per cent of all participating companies indicated otherwise. This is mainly due to the limited selection, which did not include important sectors such as trade or crafts. Nevertheless, the ICT and medical technology sectors are already well positioned in digitalisation in a cross-sector comparison. In turn, the evaluation of the economic sectors indicated independently shows that trade takes second place behind ICT.

As shown in figure 4, 44.7 percent of the approved grants were spent on the acquisition of software, another 29.7 percent went to the procurement of production-relevant hardware and 17.6 percent to hardware and software and 8 percent to qualification. Furthermore, 60.0 percent of

all projects were related to IT security, which underlines the increasing importance of the topic and corresponds to the overarching funding objective.

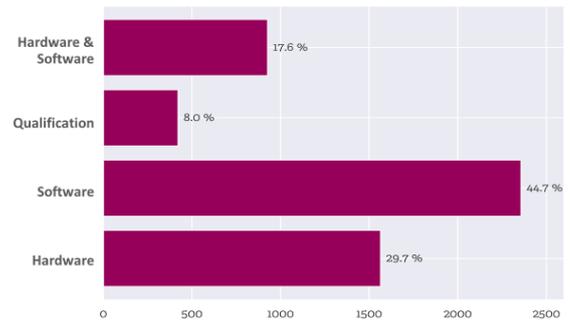


Figure 4 – Distribution of single measures along clustered use cases

37,4 percent of the funded measures of the cluster Software was also invested in IT security software, strengthening the importance of IT security. As shown in figure 5, another 22,6 percent of funded measures related to websites, web shops and merchandise management systems. 11,9 percent of measures related to tools for accounting and human resources tools.

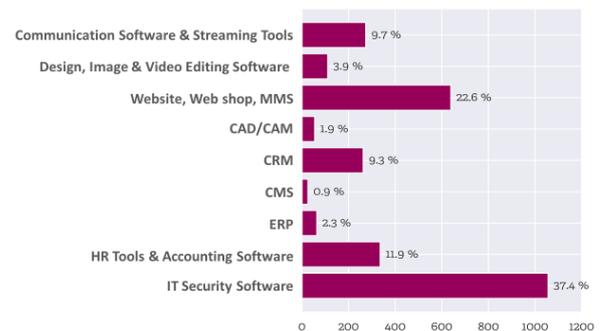


Figure 5 – Distribution of measures in the sub-cluster of Software

In the sub-category of Hardware 56,3 percent of all funded measures related to server and internet hardware, followed by 16,3 percent of funded measures relating to bureau hardware and another 9,5 percent relating to camera and video equipment. As figure 6 illustrates, the most invested hardware was either more advanced server hardware or either simple standard hardware.

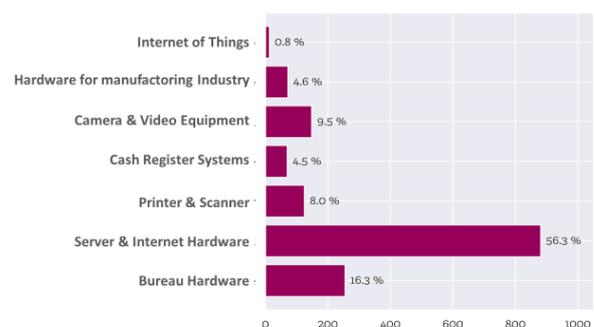


Figure 6 – Distribution of single measures in the sub-cluster of Hardware

The cluster of IT Security was mostly used for the acquisition of IT security-related hardware or licenses and certificates. Also more than two thirds of the funded companies came from the inner-city districts of Mitte, Charlottenburg-Wilmersdorf, Pankow and Friedrichshain-Kreuzberg.

Conclusion

Qualitatively, one of the greatest challenges of promoting digitisation measures is the measurement of actual digitisation progress and addressing companies that are particularly worthy of support. Furthermore, the correct and uniform recording of data before, during and after the individual digitisation measure is of extraordinary importance for a well-founded analysis.

In terms of content, it is particularly evident that the target group was recorded in its entirety, although most of the companies are established SMEs from the information and communication technology or medical technology sectors. This allows for several conclusions. Firstly, this suggests a windfall effect. A windfall effect is when a project is realised with funding that would have been implemented anyway. In other words, the funding was only taken along. Secondly, windfall losses and the sector distribution of the companies suggest that there is an information asymmetry between micro, small and medium-sized companies and between companies in the ICT sector and companies in other sectors. This indication of windfall effects also shows when looking at the distribution of funded single measures in the cluster hardware. Relatively sophisticated server hardware makes up over half of all funded measures in this cluster. This presumed information asymmetry can also be interpreted in the geographical distribution of the companies. Here there is a strong disparity between companies from Berlin's inner city and the outlying districts.

Otherwise the allocation of measures within biggest cluster Software and the high number of IT security related measures, together with the overall distribution of companies along number of employees and turnover shows a great need of SMEs for mostly basic services, software and hardware to overcome the initial burden of digitising.

The average funding level also shows that there are hardly any differences in the level of funding for small and medium-sized enterprises. It can be concluded here that both small and medium-sized enterprises, corresponding to the Basic and Plus categories, have a relative basic investment requirement, which for the Digitalprämie Berlin is 7,800 euros including a 50 percent deductible, i.e. 15,600 euros per enterprise. In practice, the funding requirements of the companies differ, but can be limited primarily to basic software and hardware.

However, many companies have had more than one individual measure funded. Furthermore, the costs of the digitisation projects did not increase the larger the company

was. This indicated some kind of shared initial investment obstacle small and medium companies need to overcome.

Second funding period

Structure

The first funding period, which expired on 31 October 2021, will be continued from 15 August 2022 until the end of 2023. The second funding period is also a non-repayable grant for SMEs with their registered office or place of business in Berlin and up to a maximum of 249 employees, including solo self-employed persons and freelancers in their main occupation without salaried employees. However, the foundation must now have taken place before 31 December 2021. The Basic and Plus modules have been combined and the distinction between SMEs has been removed. As a result, eligible applicants can apply for up to 17,000 euros. The maximum share of funding is still 50 percent of the eligible costs. Up to 10 individual measures can be funded in the areas of:

- Digital work and production processes and management processes
- Introduction or improvement of IT security
- Digital consulting and qualification

Changes

The most important changes are the combination of the two modules Basic and Plus and the introduction of a basic digital maturity measurement based on self-disclosure. Furthermore, the early start of measures is permitted for all applicants.

The disbursement of the approved subsidies will now take place after completion of the review of the proof of use, for which the subsidisation of the net costs is made possible regardless of the entitlement to deduct input tax. In addition to the adjustment of the cut-off dates, a binding limit of 27,000 euros in annual turnover is introduced for the income of solo self-employed persons. Furthermore, the possibility to subsequently submit proof of entry in the transparency database has been eliminated.

CONCLUSION AND OUTLOOK

From the evaluated data and the changes initiated by them, various possible conclusions emerge that must be further observed and documented in the course of the second period.

Windfall effects in digitisation funding result primarily from information asymmetry. At the same time, funding programmes are changing due to developments in digitisation such as the possibility of digital application and evidence management, the networking of data sources, user-centricity and real-time communication.

Instead of the previous, complex funding for specific projects in specific sectors with high application hurdles, funding programmes are becoming easier to access,

clearer in structure and more flexible in terms of the funding objects.

Simplifying the structure of funding programmes, their application and the use of evidence is a possible solution to make digitisation funding more accessible for companies that are not already digitised. There are three possible solutions here: On the one hand, the integration of a digital maturity model in the application process and the further standardisation of the application itself, a more sector-specific approach and the standardisation of the data requested during the application and the abolition of free text fields. Furthermore, it may be advisable to demand standardised short digitalisation concepts from companies that are willing to apply for funding. Combined with a commitment to follow-up appointments including a further maturity measurement after completion of the respective project, the data quality can be significantly increased.

The coordination of application and evaluation can not only help to increase data quality, but also provide continuous information on which measures are procured by which sectors and companies and when. In this respect, the second funding period of the Digitalprämie will also be analysed and documented by the DAB. The changes made to the second funding period and the standardisation and streamlining of the Digitalprämie Berlin are exemplary for a changing funding market, away from singular lighthouse projects with complex modalities towards simple, uncomplicated funding programmes for a large number of actors.

In order to improve the efficiency of public funding programmes for the digitisation of SMEs, public programmes have to overcome the tension between opening up and easing access to funding programmes and avoiding windfall effects.

A first consequence of this analysis was the recommendation to combine the "Basic" and "Plus" modules of the Digitalprämie Berlin and to set the maximum amount of funding that can be called up at 17,000 euros, including the self-employed and the liberal professions. This measure led to an expansion of the possible recipients and is intended to make the use of funding more participatory. Furthermore, the reduced complexity is expected to improve comprehensibility and communability. The extent to which this is successful will be the subject of the next evaluation of the Digitalprämie Berlin in 2023.

Furthermore, the number of free text fields was reduced and a basic self-assessment of the digital maturity of the applying companies was included in the application process. As a result of efforts by the Berlin administration, the application and approval of funds now only takes between one and three months, which should increase the plannability and flexibility of the program.

The expected improvement in data quality will enable a more in-depth analysis of individual companies and their measures for future funding periods of the Digitalprämie Berlin.

Nevertheless, there are further measures that could be taken to avoid windfall effects when promoting the digitization of small and medium-sized enterprises. For example, further harmonization and standardization of funding programs, especially in the application process and the required documents, would seem to be a possible means of countering the suspected information asymmetry. The consistent clarification and visualization of funding opportunities by public and private agencies is also essential in this regard.

Furthermore, the increasing digitization of administration and funding programs plays a crucial role in making funding more comprehensible and participatory, while at the same time avoiding possible windfall effects.

CONTACT

Paul Sonnenberg was born in Bergisch-Gladbach in 1991 and attended the Wildau University of Applied Sciences, where he received his Master's degree in European Management in 2019. Since then, he has been working in the field of digitalisation support for small and medium-sized enterprises. First at the Mittelstand-4.0 Kompetenzzentrum Berlin, since 2021 at the public Digitalagentur Berlin. His email address is paulsonnenberg@t-online.de/paul.sonnenberg@digitalagentur.berlin.

Publication bibliography

Bendel, Oliver (2021): Definition: Digitalisierung. In *Springer Fachmedien Wiesbaden GmbH*, 7/13/2021. Available online at <https://wirtschaftslexikon.gabler.de/definition/digitalisierung-54195>, checked on 7/4/2022.

Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe (2019a): Förderrichtlinie Digitalprämie Berlin. Available online at <https://www.ibb.de/media/dokumente/foerderprogramme/wirtschaftsfoerderung/digitalpraemie-berlin/digitalpraemie-berlin-foerderrichtlinie.pdf>, checked on 6/28/2022.

Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe (2019b): Zuschuss an die Digitalagentur GmbH. Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe. Available online at <https://www.parlament-berlin.de/ados/18/WiEnBe/vorgang/web18-0158-85-v.pdf>, checked on 7/6/2022.

Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe (2022): Neustart des Förderprogramms „Digitalprämie Berlin“ im August 2022. Berliner Senatsverwaltung für Wirtschaft, Energie und Betriebe. Available online at <https://www.berlin.de/sen/web/presse/pressemitteilungen/2022/pressemitteilung.1228694.php>, checked on 9/26/2022.

Bundesregierung (2022): Digitalisierungsstrategie Deutschland. Umsetzungsstrategie zur Gestaltung des digitalen Wandels. Edited by Bundesregierung. Available online at <https://digitalstrategie-deutschland.de/>, updated on 9/21/2022.

DAB Digitalagentur Berlin (2022): Die Digitalprämie Berlin. Bericht zur Auswertung des Förderprogramms. DAB Digitalagentur Berlin, checked on 6/22/2022.

European Commission (2003): Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422). 32003H0361. Europäische Kommission. Available online at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361>, updated on 6/26/2022, checked on 6/26/2022.

European Commission (2008): Small Business Act. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Vorfahrt für KMU in Europa. Europäische Kommission. Available online at <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A52008DC0394>, updated on 6/26/2022, checked on 6/26/2022.

European Commission (2013): Verordnung (EU) Nr. 1407/2013 der Kommission vom 18. Dezember 2013 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-BeihilfenText von Bedeutung für den EWR. Available online at <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:352:0001:0008:DE:PDF>, checked on 9/27/2022.

European Commission (2022): The Digital Economy and Society Index (DESI). Available online at <https://digital-strategy.ec.europa.eu/en/policies/desi>, updated on 9/23/2022, checked on 9/27/2022.

Institut für Mittelstandsforschung (2021): Digitalisierung der KMU im EU-Vergleich. Available online at <https://www.ifm-bonn.org/en/statistics/mittelstand-themes/digitalisierung-der-kmu-im-eu-vergleich>, updated on 7/1/2022, checked on 7/1/2022.

Lichtblau, Karl (2018): Digitalisierung der KMU in Deutschland. Konzeption und empirische Befunde. Available online at https://www.iwconsult.de/fileadmin/user_upload/projekte/2018/Digital_Atlas/Digitalisierung_von_KMU.pdf, checked on 7/1/2022.

Mittelstand 4.0 Kompetenzzentrum Berlin (2021): Insights aus dem Mittelstand. Digitalisierung von KMU in Brandenburg und Berlin 2021. Available online at https://hpi.de/fileadmin/user_upload/fachgebiete/H%C3%B6rle/ITE_Gemeinsam-Digital/Insights_aus_dem_Mittelstand.pdf, checked on 7/1/2022.

Papadopoulos, George (2018): Statistics on small and medium-sized enterprises. With assistance of Samuli Rikama, Pekka Alajääskö, Ziade Salah-Eddine (Eurostat, Structural business statistics), Aarno Airaksinen, Henri Luomaranta (Statistics Finland). Edited by Eurostat. Eurostat. Available online at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises, updated on 4/29/2022, checked on 6/26/2022.

Statistisches Bundesamt (2019): Anteile Kleine und Mittlere Unternehmen 2019 nach Größenklassen in %. Available online at <https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Tabellen/wirtschaftsabschnitt- insgesamt.html;jsessionid=4D515FBFD4EABDD66C5B7B7BBB6CBCDE.live712>, checked on 6/26/2022.

Zimmermann, Volker (2021): Innovationen steigern Wachstum und Produktivität und verbessern die Qualifikationsstruktur der Beschäftigten in mittelständischen Unternehmen. Kreditanstalt für Wiederaufbau. Available online at <https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Fokus-Volkswirtschaft/Fokus-2021/Fokus-Nr.-361-Dezember-2021-Innoeffekte.pdf>, checked on 6/26/2022.

IT-ASSISTED OPTIMISATION OF FUEL CONSUMPTION IN AIR TRANSPORT

Andreas Walter
Department of Industrial Engineering
Tor Vergata University of Rome
I-00133 Rome, Italy
E-Mail: walter.andreas@students.uniroma2.eu

KEYWORDS

Fuel Costs, Aviation Emission, Data Analytics, Big Data

ABSTRACT

Aviation continues to be an essential means of transport for passengers and cargo. In recent years, the COVID-19 pandemic led to a collapse. In 2022 Europe was back up to around 85% of 2019 levels (EASA, 2022). In 2021 van der Sman et al. predicted an recovery to 2019 levels in 2024 (van der Sman et al., 2021). However, fuel savings and emissions reduction have become increasingly important in recent years.

As part of a PhD thesis, possibilities for reducing fuel consumption by reducing the final reserve fuel were investigated. A smaller amount of tanked fuel required leads to a reduction in the transported (fuel) weight and, thus, a reduction in overall fuel consumption. This is because fuel consumption for a given route depends, among other factors, on the aircraft's weight. The more an aircraft weighs, the higher the fuel consumption. To keep fuel consumption as low as possible, carrying only the minimum weight required for the route in question is the most economical. Carrying more or even unnecessary weight increases the amount of fuel required and consumed in flight.

The overarching research aims to explore and evaluate how to reduce the fuel carried by aircraft and, thus, the total fuel required for a given flight. The main focus of this paper is on the opportunities and challenges that have arisen with introducing new fuel regulations in European aviation regulations. Operators with appropriate safety levels can apply more tailored provisions. This requires the demonstration of the safety level. This is achieved by defining specific safety performance indicators (SPIs), compliance with which is then continuously monitored and evaluated during operation. This requires the collection and evaluation of correspondingly large amounts of data. This is only possible using appropriate IT applications. Example below shows the amount of data that accumulates during flight operations. Recording, processing and saving pose a challenge in this respect.

On the other hand, performance-based regulations allow for a more individualised implementation on and by the respective companies via the demonstration of a corresponding level of safety. Safety indicators are used for this purpose, which must be obtained and evaluated from various existing data. A large amount of data, which can only be collected and processed with the help of various IT applications, represents a challenge. However, companies can benefit from the corresponding advantages if they can cope with this.

The following is an excerpt of the requirements and possible implementation, focusing on the amount of data and the associated challenges and opportunities.

INTRODUCTION

In 2015, around 3.5 billion passengers already used air transport for business and tourism purposes. Despite a downturn in 2020 and 2021, aviation is expected to recover to pre-pandemic levels. The high aviation traffic volume is associated with an enormous demand for aviation fuel and associated high emissions. Lee et al. provide an overview of CO₂ and other related emissions and impacts of aviation on the climate (Lee et al., 2009), likewise Fleming and Ziegler (Fleming and Ziegler) and Filippone (Filippone, 2008) - to name just a few examples.

Over the past 30 years, damages resulting from climate-related weather events increased by a factor of twenty. In 2017 the weather-related damages amounted to \$ 330 billion 2017, making it the most costly year on record (van der Sman et al., 2021). Some observed effects of climate change, which also affect the aviation sector (van der Sman et al., 2021), are Temperature changes, changes in precipitation and humidity, different wind patterns, different storm patterns, and sea level rise. This is an increase of around 6.4 % compared to 2014 (ICAO, 2016).

For 2037, an IATA forecast predicts the number of air travellers reaching 8.2 billion (IATA, 2018). The industry is facing significant challenges at the same time. Emissions from aviation, domestically and internationally, account for about 2% of total global CO₂ emissions (ICAO, 2014). The UK Civil Aviation Authority's Airspace Change Masterplan states that

“without significant changes to the system, increased congestion, vectoring and arrival holding will lead to a further degradation in environmental efficiency as traffic levels grow, with average per flight CO₂ emissions expected to rise by between 8% and 12% by 2030 compared to current levels” (Beevor and Alexander, 2022).

Reducing the effects of global warming due to emissions has become a goal. As a result, reducing emissions has become an important issue. Commercial aviation has already developed and implemented many techniques to reduce fuel consumption for economy and efficiency. On the operator side, these are primarily operational improvements, such as reducing the weight of onboard equipment or using a fixed ground power supply instead of the aircraft's auxiliary power unit on the ground. Airlines are searching for fuel-efficient routes or flight profiles most of the time. Airlines, airports and air navigation service providers take measures to reduce noise and pollution in their daily operations (IATA, 2019a). Effects on new aircraft generations introduced in recent years can be seen in Table 1 by IATA (IATA, 2019b).

Table 1: Aircraft technology effects

Reference	New generation	Fuel saving
ATR/CRJ	MRJ	20%
A320	A320neo	15% – 20%
B767	B787	20% – 25%
A330	A330 - 800neo	14% – 20%
A330	A330 - 900neo	14% – 20%

Corresponding developments are also taking place on the legislator's side. With amendments to Annex 6, ICAO has adopted a less prescriptive approach in the design of regulations. As a result, national regulators may work with air operators on new standards and adopt operational variations based on the individual ability to demonstrate an (equal) level of safety. Statistical data methods and safety risk management (SRM) are necessary. They enable a performance-based approach in the area of flight planning; this would improve fuel efficiency and therefore reduce emissions.

With the Executive Director's Decision 2022/005/R, the European Union Aviation Safety Agency (EASA) introduced new rules. Entry into force was on October 30th, 2022. These rules effectively adopt ICAO standards and recommended practices (SARPs) and integrate them into the current requirements of Air OPS Regulation (EU) No 965/2012, as well as the associated Guidance Material (GM) and Acceptable Means of

Compliance (AMC). The new rules offer three different fuel schemes: basic fuel scheme, fuel scheme with variations and individual fuel scheme—the individual fuel scheme, in particular, offers excellent potential for fuel savings.

SAFETY MANAGEMENT

Rules and regulations in aviation are drawn up for safety. Figure 1 (Shappell and Wiegmann, 2000) illustrates how the Swiss Cheese model helps to understand the interplay of different factors in accident causation. Several layers of defence are built into the aviation system to protect against variations, e.g. in human performance or decision-making, at all levels. But each layer typically has vulnerabilities, represented by the holes in the slices of "Swiss cheese" (ICAO, 2018).

Regulations, training and technology are some barriers (or slices) to preventing accidents. Safety management seeks to proactively mitigate safety risks before they result in aviation accidents and incidents (ICAO, 2018).

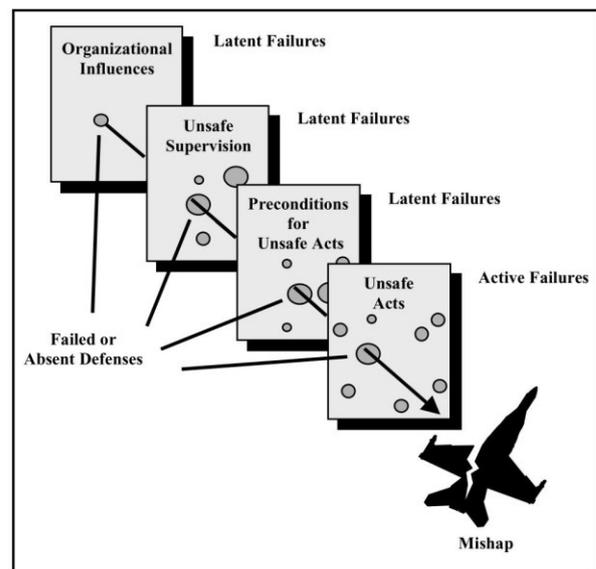


Figure 1: “Swiss cheese” model of human error causation

Safety management is one of the pillars to enable aviation safety and is subject to change and development. Namely, the performance-based approach to safety offers improvements as it focuses on achieving the desired outcome and not just on whether or not the regulation is complied with (ICAO, 2018). However, the theoretically possible level of safety is not always achieved. Scott A. Snook's theory, see Figure 2 (ICAO, 2018), is used to understand how the performance of a system deviates from its original design.

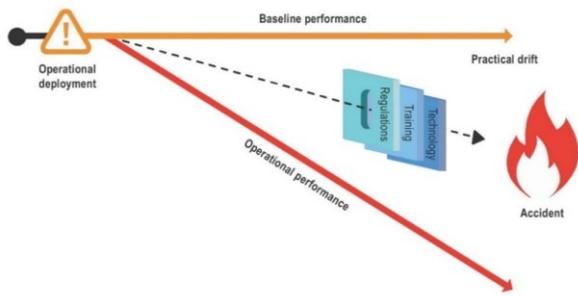


Figure 2: Concept of practical drift

The drift is a consequence of daily practice and is referred to as practical drift. Audits, observations and safety performance indicator (SPI) monitoring, as safety assurance activities, can help uncover activities that practically drift (ICAO, 2018). As Figure 3 (ICAO, 2018) shows, aviation is moving within a field of tension. Too little action in safety can lead to accidents, while too much can lead to financial bankruptcy. The relationship between the costs of a safety measure and the benefits can be examined, for example, with the "Total Judgement-value" method (Dietrich, 2016). Here, it can be determined how the costs are in relation to the increase in safety for the respective reference group.

Due to changes in Regulation (EU) No. 965/2012, which has been applied since the fall of 2022, there was an adjustment in the fuel requirements. These were previously regulated in CAT.OP.MPA.150, among others, will be referred to in CAT.OP in the future.MPA.180 and the following sections (EASA, 2020b). Operators demonstrating specific capabilities can use a basic scheme with variations or an individual fuel scheme.

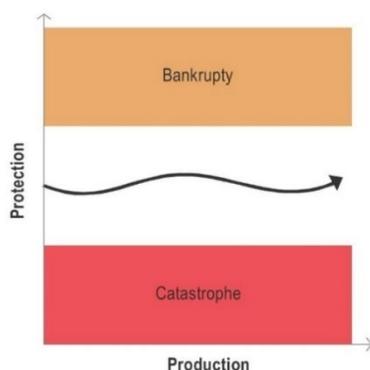


Figure 3: Concept of a safety space

This is intended for operators who can demonstrate a defined safety level, thus reflecting the move towards performance-based regulations (EASA, 2020b). Data supporting the intended deviation is required to implement the individual fuel scheme. The Annex to Opinion No. 02/2020 already contains preliminary

information on the draft Acceptable Means of Compliance (AMC) and Guidance Manual (GM) and information to be considered for the performance-based deviation. A non-exhaustive list of safety performance indicators (SPI) that can be used to measure safety performance are:

- flights with 100 % consumption of the contingency fuel;
- flights with a percentage consumption of the contingency fuel (e.g. 85 %), as agreed by the operator and the competent authority;
- difference between planned and actual trip fuel;
- landings with less than the final reserve fuel (FRF) remaining;
- flights landing with less than minutes of fuel remaining (e.g. 45 minutes), as agreed by the operator and the competent authority;
- 'MINIMUM FUEL' declarations;
- 'MAYDAY MAYDAY MAYDAY FUEL' declarations;
- in-flight replanning to the planned destination due to fuel shortage, including committing to land at the destination by cancelling the planned destination alternate;
- diversion to an en-route alternate (ERA) aerodrome to protect the FRF;
- diversion to the destination alternate aerodrome; and
- any other indicator with the potential to demonstrate the suitability or unsuitability of the alternate aerodrome and fuel planning policy (EASA, 2020a).

As can be seen from these indicators, airlines wishing to have an individual fuel scheme approved by a competent authority are required to gather a significant amount of data and information on fuel consumption. The collection, monitoring and storage of these indicators is a challenge. An example of a practical implementation follows below.

FUEL REDUCTION OPTIONS

Airbus has recently launched an initiative regarding sustainability, which can be found on its Worldwide Instructor News homepage (Airbus S.A.S., 2023). Part 1 of the series published there deals with flight planning and again emphasises the possibilities of saving fuel by reducing weight.

Table 2: Savings through 100 kg weight reduction

Aircraft	Fuel [kg]	CO ₂ [kg]
A220/A320	20	63
A330/A350	36	113

Table 2 shows the potential savings if the weight for a flight segment is reduced by 100 kg. Assumed were a loading of 80 per cent and a maximum range sector.

This paper focus researching and evaluating how to reduce the fuel carried by aircraft and, therefore, the total fuel requirement for a given flight under consideration of the necessary IT Data for the performance-based approach. This research aims to demonstrate, based on today's regulations in the field of aircraft certification and operation, that such a high level of safety has been achieved that it is possible, using a performance-based approach, to define a set of measures and circumstances that make it possible to reduce some of the fuel carried, and thus the weight and resulting emissions, almost immediately. Therefore, tracking, recording and evaluating vast amounts of Information is required - mainly to fulfil safety performance indicators.

The potential therein will be highlighted below using examples. The planning for two flights is adjusted so fuel is planned for five minutes less flight time. This is done using current flight, weather and aircraft data. Two flights are considered to highlight the potential for fuel savings: Hong Kong to Cincinnati and Hong Kong to Leipzig. Figure 4 and Figure 5 show these flights, planned with actual data and information as if they were carried out - but were not carried out.

Table 3 and Table 4 present an excerpt from the operational flight plan, fuel planning, and mass and loading. Table 3 shows the comparison of fuel planning for a flight from Hong Kong to Leipzig.

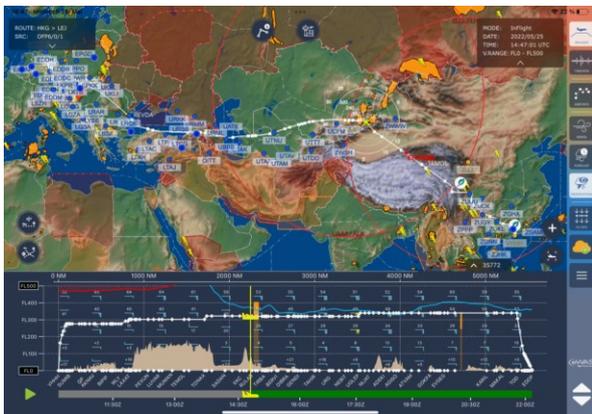


Figure 4: Flight information Hong Kong – Leipzig

Since the current approved planning is used, a value of 5 minutes of extra fuel was included as additional fuel for comparison. The alternate and final reserve values shown in Table 3 do not correspond to those that would result from an actual reduction. The 700 kg / 5 minutes in the right column only affects trip and contingency fuel, but not alternate and final reserve fuel. With an absolute fuel reduction, these values would also be lower, leading to a more significant reduction in trip and contingency fuel. Therefore, the resulting delta, in this

case, an additional consumption of 257 kg, is lower than an actual saving in the reduction case. But the trend and thus a rough figure for evaluation is evident. The average additional consumption for this route is 21.34 kg/flight hour, i.e. this would be the savings potential.

Table 3: Route comparison Hong Kong - Leipzig

	Origin	700 kg extra	Δ
TRIP	102090	102342	252
CONT 3%	3063	3070	7
ALTN	3832	3832	
FINRES	3136	3136	
REQTOF	112200	112400	
ADDFU		700	
TAXI	767	767	

Table 4 shows the same considerations for the route from Hong Kong to Cincinnati. Here, the difference in fuel, i.e. the savings potential, is 364 kilograms. The average additional consumption for this route is 25.1 kg per flight hour, i.e. this would be the saving potential in this case.

Both examples show savings opportunities. An aircraft with an average flight time of 15 hours would consume around 300 kg less fuel per day. Even if these savings seem small, with a relatively small fleet of only twenty aircraft, the total value is correspondingly high. A conservative projection of 20 kg fuel saved per flight hour and fifteen flight hours per aircraft per day results in a daily fuel saving opportunity of 6 000 kg - this applies to a fleet of twenty Boeing B777-200F aircraft. The associated savings in emissions are, for carbon dioxide ~18 900 kg, water ~7 500 kg and 30 to 150 kg of nitrogen oxides per day.

Table 4: Route comparison Hong Kong – Cincinnati

	Origin	700 kg extra	Δ
TRIP	117295	117649	354
CONT 3%	3519	3529	10
ALTN	3326	3326	
FINRES	2968	2968	
REQTOF	127200	127500	
ADDFU		700	
TAXI	767	767	

These considerations are conservative and do not reflect other further advantages or that of a fighter aircraft. The values of 21 - 25 kg of additional fuel consumption determined above correspond to a fuel penalty factor of approx.—3%. Further considering the savings effects, the savings of the 5-minute fuel weight (here 700 kg for 5 minutes) and the additional consumption added up per flight hour must also be considered cumulatively.

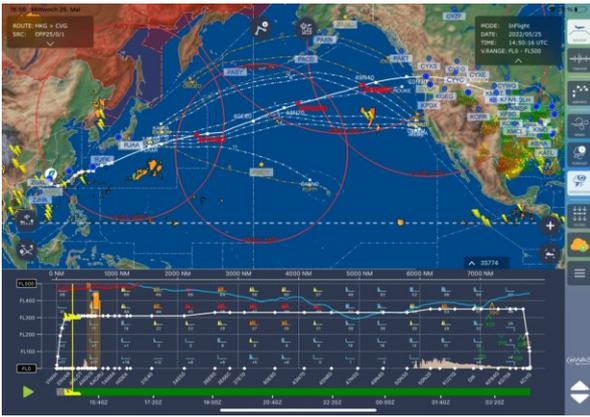


Figure 5: Flight information Hong Kong – Cincinnati

The two flights examined above result in approximately 1 000 kg difference at the take-off.

Figure 5 shows route optimisation options. These are presented to the crew during the planning process. As can be seen, the route already contains potential for shortcuts. These possibilities are statistically recorded and are considered in flight planning - by providing them as information to the crew in the IT application.

DATA COLLECTION - REPORTING SYSTEM

One significant change within the European airline operational rules through Regulation (EU) 2021/1296 was the introduction of fuel schemes. Operators who can demonstrate an equivalent level of safety may be approved to use a basic with variations or individual fuel scheme, as regulated in AMC1 CAT.OP.MPA.180. This reflects the move towards performance-based regulations (EASA, 2020b). Data supporting the intended application is required to support the implementation of such advanced fuel schemes. An Annex to Opinion No. 02/2020 already contained preliminary information on AMC and GM to be considered for the performance-based approach. GM2 CAT.OP.MPA.180 now shows a non-exhaustive list of safety performance indicators (SPI) that can be used to measure safety performance.

To shed light on the number of data and the challenges, examine real flight data of a worldwide operating European airline where chosen. Therefore, data from a roughly 5-year (4 years and ten months) period, from March 2016 to the end of December 2020, of a cargo airline was provided. The utilized aircraft are Boeing B777-200 in a freighter version. It has a maximum take-off mass of around 347 800 kg, a maximum landing mass of 260 800 kg and a dry operating weight of around 141 600 kg. That explains a maximum resultant revenue payload capability of roughly 103 metric tons. Maximum fuel capacity for that version ~ 144 000 kg.

The operated network contains large airports, together with regional airports. The network destinations are a mix of short, medium and long-haul flights.

The data was provided in different reports. The following standard components of data analysis were done:

- Pre-processing - accounting for outliers, missing values and smoothing data,
- Summary - calculating basic statistics to describe the general position, scale and shape of the data,
- Visualisation - plotting data to identify patterns and trends.

The data were analysed to obtain information for other evaluation purposes—two ways of analysing fuel information. In the first step, available and valuable data and information from the airline reporting system are evaluated, together with background information on limitations. In the second step, a detailed evaluation is done for some unique routings based on information gathered in the first step. The evaluation was conducted with the help of Excel and MATLAB. For advantages and possibilities of MATLAB, compare, e.g. Saivenkatesh et al. (Saivenkatesh et al., 2020).

The evaluation and the consequences are not the focus of this paper, but the focus is on the amount of data and the processing of the information to meet the performance-based approach.

A starting point for possible relevant information can be found in ICAO Doc 9976, the Flight Planning and Fuel Management (FPFM) Manual. It provides a non-exhaustive list of data required to demonstrate performance-based compliance.

- Actual versus planned taxi times;
- Taxi and ground delays;
- En-route speed restrictions (ATC, turbulence, etc.);
- En-route deviations (route and altitude for ATC, Wx, etc.);
- Air traffic delays experienced;
- ATC flow management and aerodrome capacity/congestion and demand;
- Runway closures or reductions in aerodrome capacity;
- Any ATC or aerodrome factors that could contribute to the planned fuel consumption being exceeded;
- 100 per cent consumption of contingency fuel;
- 100 per cent consumption of holding fuel;
- Low fuel state (as defined by operator or Authority);
- Minimum fuel state (as defined by operator or Authority);
- Emergency fuel state (as defined by operator or Authority);

- *Less than final reserve fuel remaining;*
- *Actual versus planned time spent holding;*
- *Actual versus planned SID/STAR ground track flown (including portion of Point Merge STAR actually flown, if applicable);*
- *Missed approaches;*
- *Additional approaches;*
- *Proceeding to destination alternate aerodrome or diversions prior to destination;*
- *Proceeding to en-route alternate aerodrome (e.g. due to in-flight re-dispatch or re-planning);*
- *Ground-based approach facilities malfunctions;*
- *Destination or alternate aerodrome meteorological conditions below forecast conditions;*
- *Other factors or occurrences identified by the Authority or the operator as having caused delays, diversions, additional fuel consumption or other undesirable outcomes (ICAO, 2015).*

As shown above, GM2 CAT.OP.MPA.180 of Regulation (EU) No 965/2012 also contains similar parameters. ICAO Doc 9976 emphasises the special evaluation for respective city pairs. As seen from this SPI list, various information must be collected and stored for each flight. As mentioned, various reports are used for this purpose, two of which are presented by example.

As shown below, a large amount of information and data is simultaneously created, collected and stored during each flight. Filtering the necessary information while making data efficiently available for future flights is a challenge that can only be met with the support of appropriate software.

Fuel Analyzer App Data

The Fuel Analyzer App Data report contains data represented to the flight crews on the electronic flight back (EFB) application for fuel planning information. It is possible to choose a Flight number / City-Pair and get multiple information (e.g. Minimum, Maximum, Average, 25% Quantile, Median and 75% Quantile) for relevant factors like trip time deviation, PIC extra fuel uplift, company extra fuel uplift, fuel amount above legal reserve at touch down, fuel amount at touch down (actual, corrected only for tankering), tankering information, taxi out time, taxi out fuel, trip fuel deviation, extra fuel consumed, zero fuel weight (ZFW) fuel correction and taxi out fuel deviation. An overview is shown below.

The crew gets a recommendation for extra fuel, the share of flights that needed extra fuel, the number of flights considered and a general overview about the fuel status of the considered flights at the destination. It is possible to choose between 100% of all flights, 90% of all flights or to exclude invalidated flights. When compiling the

information, it is possible to select equal or similar flight conditions and to consider or ignore the Cost Index.

The following information is provided in the Fuel Analyzer App. Data in the report is distinguished between original, general, and ZFW corrected values.

Original:

Trip fuel deviation: planned trip fuel versus actual trip fuel

Company extra fuel uplift: extra fuel ordered by company (except tankering)

PIC extra fuel uplift: extra fuel ordered, calculated as actual off block fuel minus planned off block fuel

Extra fuel consumed: PIC extra fuel (ordered) minus extra fuel remaining (fuel above legal reserve at touch down)

Fuel at touch down (actual, corrected only for tankering): ACARS fuel message minus tankering

Above legal reserve at touch down: touch down fuel above legal reserve

ZFW corrected:

Trip Fuel deviation corrected: planned trip fuel versus actual trip fuel* (ZFW corrected)*

ZFW fuel correction kg

PIC extra fuel uplift corrected: corrected for ZFW deviation, displayed only if more than 200 kg or less than -200 kg

Extra fuel consumed corrected

Fuel at touch down corrected

Above legal reserve at touch down corrected

General:

Trip time deviation: taxi out time + flight time (planned vs actual)

Taxi out time: times from ACARS

Taxi out fuel: fuel consumption during taxi out from ACARS

Taxi out fuel deviation

Tankering: fuel ordered for economic reasons

For a flight from Leipzig (LEJ) to East Midlands (EMA) on the 09th of May 2021, the crew would have been provided with the following general information:

Without PIC extra fuel and without tankering an AVG: 10 370 kg [MIN: 6 800 kg, MAX: 30 294 kg kg] would have been available on touchdown at destination

Is PIC extra fuel recommended: False

Extra fuel needed percentage: 0

Number of flights considered: 83

As described above, the Fuel Analyzer App is an application that is available to the crews and obtains the data from a system behind it. This data basis is presented in the next step.

Excerpt of the Fuel Analyzer App Data

During the flight planning, the crew used the collected and provided information, for example, for a flight from Hong Kong to Leipzig. Table 4 contains excerpts of the information; the following list contains the information for the crew. The information in Tables 4 and 5 is cut off behind the data contained in the original table, such as median, quantile 75, Bar Value1, Bar Value2, Bar Value3, Bar Value4, Bar Value5, Bar Value6, Bar Value7, Bar Value, for better presentation.

Similar flight conditions

Without PIC Extra Fuel and without tankering an AVG: 9 678 kg [MIN: 3 803 kg, MAX: 78 364 kg] would have been available on touchdown at destination
Is PIC Extra Fuel Recommended: WAHR
Extra Fuel Needed Percentage: 10
Amount Of Flights Considered: 725

Table 4: Excerpt, HKG-LEJ, 06th May 2021

Measure	Min	Max	AVG
Trip Time deviation	-40	76	-7.19
PIC Extra Fuel Uplift corr	-96 665	8 133	1 058.8
Company Extra Fuel Uplift	0	4 000	53.86
Above Legal Reserve @TD	-601	23 279	3 841.34
actual Fuel @TD	5 600	30 100	10 490.48
Summary	3 803	78 364	9 678.25
Tankering	0	20 000	259.78
Taxi Out Time	10	116	21.18
Taxi Out Fuel	-98 700	2 600	706.62
Trip Fuel Deviation	-99 201	6 108	-469.85
PIC Extra Fuel Uplift	-97 400	7 400	781.10
Extra Fuel consumed	0	2 990	51.20
Trip Fuel Deviation corr	-99 200	6 108	-469.85
ZFW Fuel Correction kg	-2 994	2 737	-934.42
Extra Fuel consumed corr	0	3 160	69.32
Above Legal Reserve @TD corr	-993	23 959	3.559.24
Fuel @TD corr	5 687	30 042	10 208.37
Taxi Out Fuel Deviation	-1 833	99 467	60.61

As can be seen, the crew can choose between the similar and the equal conditions. Table 5 shows the evaluation for the equal conditions; the information to the crew is listed below.

Equal flight conditions

Without PIC Extra Fuel and without tankering an AVG: 9.031 kg [MIN: 4.501 kg, MAX: 13.674 kg] would have been available on touchdown at destination
Is PIC Extra Fuel Recommended: WAHR
Extra Fuel Needed Percentage: 19
Amount Of Flights Considered: 81

Table 5: Excerpt, HKG-LEJ, 06th May 2021

Measure	Min	Max	AVG
Trip Time deviation	-32	26	-4.70
PIC Extra Fuel Uplift corr	-269	5 834	1 467.58
Company Extra Fuel Uplift	0	1 225	15.12
Above Legal Reserve @TD	-14	22 378	3 499.53
actual Fuel @TD	6 600	28 700	10 244.44
Summary	4 501	13.674	9 031.56
Tankering	0	20 000	246.91
Taxi Out Time	11	48	21.78
Taxi Out Fuel	400	2 100	944.44
Trip Fuel Deviation	-3 412	2 891	-78.09
PIC Extra Fuel Uplift	-400	5 600	1 196.30
Extra Fuel consumed	0	1 549	95.81
Trip Fuel Deviation corr	-3 412	2 891	-78.09
ZFW Fuel Correction kg	-2 961	2 498	-860.89
Extra Fuel consumed corr	0	1 690	98.17
Above Legal Reserve @TD corr	-480	21 661	3 226.14
Fuel @TD corr	6 133	27 983	9 971.04
Taxi Out Fuel Deviation	-1 333	367	-177.44

In total, an 18 by 15 matrix entry is created for each flight analysis. This relates to the connection for a city pair which shows the amount of information. With 20 aircraft flying between 2 and four sectors a day, you can see the large amount of data that is being collected.

Fuel Analyzer App Reference List

In another report, additional information is stored for each flight. The Fuel Analyzer App References List Report contains information for 31 315 flights, period 1st March 2016 to the end of December 2020. This report is, amongst other things, fed by planning information and return information sent from the aircraft. It contains planned (p), actual (a) and corrected (c) information. As planned figures are self-explanatory, e. g. scheduled departure time, actual figures are accurate figures, like actual departure time. Actual figures describe the figures as sent from the aircraft. The report contains corrected figures. Corrected figures describe the difference between planned and feedback figures based on the actual fuel decision and the flight payload. The Fuel Analyzer App References List comprises the data used to feed the Fuel Analyzer App. It contains: Flight Leg Event ID, Flight Designator, STD, ATD, STA, ATA, Month, Zero Fuel Weight (ZFW) Deviation Fuel, Off Block Fuel Deviation, Final Reserve Fuel, Min Alternate Fuel, Company Extra Fuel (p, c), Needed Extra Fuel (p, c), PIC Extra Fuel (p, c), Additional consumption for PIC Extra Fuel (c), Is Extra Fuel Needed (p, c), Touchdown Fuel (a, c) Company Eco Tankering Fuel, Trip Fuel (p, a, c), Taxi Out Time, Taxi Out Fuel (a, p), Above Legal Reserve At Touchdown Fuel (a, c), Trip Time Deviation, Cost Index - this means a large amount of data.

Thirty-eight single entries are stored for every flight in the Fuel Analyser Analyzer References List. The number of entries adds up with the associated number of aircraft movements. In the area of long-haul flights in the investigated cargo flight sector, there were 20 aircraft with 2 to 3 flight segments per day. Therefore, an average of 40 new data sets were added per day. For example, 36 flights with respective entries were recorded on 13th December 2022. If the type of flight operation varies, e.g. short- to medium-haul passenger operations where each aircraft flies 4 to 8 sectors per day and the fleet is correspondingly more extensive, the number of data records generated will be more significant.

A lot of data is collected, stored and analysed for a flight. Fast and manageable evaluation is only possible with IT support. This can also be used to provide evidence of the requirements for SPI by Regulation (EU) No 965/2012.

IT systems such as eWAS Dispatch and eWAS pilot collect and process the amount of information per flight. For example, eWAS Dispatch provides continuously EFB Weather Awareness (Aircraft IT, 2022).

Position messages are reported every 20 seconds, with information such as altitude, speed, deviations from the flight plan or fuel situation.

In addition, information is exchanged between the operations centre on the ground and the aircraft. For a company with 20 aircraft in the air for between 15 and 16 hours, this amounts to approximately 8000 messages per day.

For the airline under consideration, this means for one year:

- 4 087 038 messages processed
- 58 213 electronic flight plans generated
- 638 963 eWAS (Positions, Progress and OOOI) messages processed
- 1 758 727 Aircraft Status Reports generated

The manual evaluation and monitoring of this data, 24 hours a day throughout the year, is no longer possible.

In the meantime, commercial providers offer the possibility of using off-the-shelf software to give crews in the air and dispatchers on the ground the comprehensive possibility of planning and executing flights with a uniform programme. In particular, the possibility of almost immediate communication between the crew on board and the ground crew makes it possible to react to unforeseen events.

The connection between aircraft in-flight and dispatch personnel on the ground becomes increasingly important (SITA, 2023b).

During the coming three years, airlines will continue to drive investments in emerging technologies. The top four priorities remain the same, as airlines focus on data management to enhance their business models and operational efficiencies through technologies such as business intelligence software (74%), data exchange technologies (82%), artificial intelligence (76%), and Radio Frequency Identification (RFID) tracking (80%). Two areas look set for significant growth in the future, despite showing low implementation at the present moment. Airlines have doubled R&D plans for Near Field Communications (57%) and 'augmented/virtual reality tech' (42%) suggesting they have the potential to become areas of focus in years to come (SITA, 2023a).

CONCLUSION

Operational regulations in aviation are adapted to take account of the reliability of aircraft, better avionics and possibilities out of it, and technical developments in-

flight monitoring and communication with the crews on board. The collection and processing of large amounts of data, using appropriate IT hardware and software, allow the definition and control of safety performance indicators and move away from prescriptive regulations towards performance-based approaches.

Operators with appropriate safety levels can apply more tailored provisions. This requires the demonstration of the safety level. This is achieved by defining specific safety performance indicators (SPIs), compliance with which is then continuously monitored and evaluated during operation. This requires the collection and evaluation of correspondingly large amounts of data. This is only possible using appropriate IT applications. The example above shows the amount of data that accumulates during flight operations. Recording, processing and saving pose a challenge in this respect.

Implementing the latest technologies for flight planning operations offers advantages. Improved process management, decision-making and profitability are possible through modern IT systems. This can reduce the amount of fuel used, thus reducing emissions and costs. At the same time, flight availability can be increased and regulatory compliance granted.

If the operator makes the necessary effort, he can apply a basic with a variation or individual fuel scheme. This, in turn, enables operational advantages, plus saves fuel and thus emissions.

The use of artificial intelligence is one of the challenges but also one of the options that can help companies meet the numerous regulatory requirements. In some cases, companies are taking the first steps in this area (Travelnews, 2023), but further research is necessary.

AUTHOR BIOGRAPHIES



ANDREAS WALTER was born in Görlitz, Germany and started his career as a cadet in the German Air Force in 1997. As a young officer, he completed his studies in aerospace engineering at the University of the German Armed Forces in Munich. He then served as a technical officer in the German Air Force for seven years, dealing with all technical aspects of aviation. During this time, he studied business administration alongside his job at the FernUniversität in Hagen. After his military career, he moved to the German Civil Aviation Administration. Within the framework of a broad education, he got to know all the facets of aviation and eventually became an air operations inspector. He obtained the authorisation to fly various Airbus aircraft within the scope of commercial aviation, up to the authorisation as an instructor. His experience in supervisory work, his

commercial and technical background provided the impetus and motivation to write a thesis in the field of fuel consumption. With the aim of combining his extensive and almost unique technical, organisational and operational experience, he is currently working on his PhD thesis at the Tor Vergata University of Rome and TH Wildau. His e-mail address is: walter.andreas@students.uniroma2.eu.

REFERENCES

- Airbus S.A.S. (2023) *WorldWide Instructor News: FLIGHT OPERATIONS SUPPORT AND TRAINING STANDARDS*. See <https://www.airbus-win.com/> (accessed 08/01/2023).
- Aircraft IT (2022) *EFB Weather Awareness Solution (eWAS) App Demo and Overview Webinar: [inc: eWAS App Pilot Walkthrough Demo; Turbulence & Thunderstorms; High Ice Water Content; Latest Developments; Airline Case Studies; more...]*. See <https://www.aircraftit.com/webinars/sitaonair-efb-weather-awareness-software-solution-ewas-app-demo-on-demand-webinar/#&gid=1&pid=4> (accessed 20/06/2022).
- Beevor J and Alexander K (2022) *Missed Targets: A brief history of aviation climate targets of the early 21st century*. Possible.
- Dietrich A (2016) *Increasing Effectiveness of Investment in Aviation Safety*. City University London, London.
- EASA (2020a) *Appendix to Opinion No 02/2020: Draft Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Annexes I-VIII to Commission Regulation (EU) No 965/2012*. See <https://www.easa.europa.eu/downloads/119252/en> (accessed 06/02/2022).
- EASA (2020b) *EASA Opinion No 02/2020: Fuel/energy planning and management*. See <https://www.easa.europa.eu/downloads/119248/en> (accessed 06/02/2022).
- EASA (2022) *Annual Safety Review 2022*. See <https://www.easa.europa.eu/en/document-library/general-publications/annual-safety-review-2022#group-easa-downloads> (accessed 03/01/2023).
- Filippone A (2008) Analysis of Carbon-Dioxide Emissions from Transport Aircraft. *Journal of Aircraft* **45(1)**: 185–197, 10.2514/1.31422.
- Fleming GG and Ziegler U *ICAO Environmental Report: ENVIRONMENTAL TRENDS IN AVIATION TO 2050*. See https://www.icao.int/environmental-protection/Documents/EnvironmentalReports/2016/ENV_Report2016_pg16-22.pdf (accessed 01/01/2022).
- IATA (2018) *Press Release No: 62: IATA Forecast Predicts 8.2 billion Air Travelers in 2037*. See <https://www.iata.org/en/pressroom/pr/2018-10-24-02/> (accessed 19/04/2020).
- IATA (2019a) *Aircraft Technology Roadmap to 2050*, Geneva. See <https://www.iata.org/contentassets/8d19e716636a47c184e7221c77563c93/technology20roadmap20to20205020no20foreword.pdf> (accessed 19/04/2020).

- IATA (2019b) *Technology Roadmap for Environmental Improvement: Fact Sheet*. See <https://iata.org/xy2401.com/> (accessed 02/01/2022).
- ICAO (2014) *Doc 10013: Operational Opportunities to Reduce Fuel Burn and Emissions*. International Civil Aviation Organization, Montréal.
- ICAO (2015) *Doc 9976: Flight Planning and Fuel Management (FPFM) Manual*. International Civil Aviation Organization, Montréal.
- ICAO (2016) *Air Navigation Report*. International Civil Aviation Organization, Montréal.
- ICAO (2018) *Doc 9859: Safety Management Manual*, 4th edn. International Civil Aviation Organization, Montréal.
- Lee DS, Fahey DW, Forster PM et al. (2009) Aviation and global climate change in the 21st century. *Atmospheric environment (Oxford, England 1994)* **43(22)**: 3520–3537, 10.1016/j.atmosenv.2009.04.024.
- Saivenkatesh T, Prema A and Renugadevi R (2020) Data mining in cloud storage data with MATLAB statistics & machine learning toolbox. *Journal of Information and Computational Science* **10(5)**: 685–690.
- Shappell SA and Wiegmann DA (2000) *The Human Factors Analysis and Classification System--HFACS*. FAA Civil Aeromedical Institute.
- SITA (2023a) *2022 Air Transport IT insights*. See <https://www.sita.aero/globalassets/docs/surveys--reports/2022-air-transport-it-insights.pdf> (accessed 16/04/2023).
- SITA (2023b) *SITA Mission Control: Real-time, collaborative airline operations, in one place*. See <https://www.sita.aero/mission-control/> (accessed 16/04/2023).
- Travelnews (2023) *Revolution beim Boarding der Swiss*. See <https://www.travelnews.ch/flug/23712-revolution-beim-boarding-der-swiss.html> (accessed 05/04/2023).
- van der Sman E, Peerlings B, Lieshout R, Kos J and Boonekamp T (2021) *Destination 2050: A Route To Net Zero European Aviation*. See <https://www.destination2050.eu/>.

KONZEPTION ERFORDERLICHER RAHMENBEDINGUNGEN FÜR DEN EINSATZ VON KÜNSTLICHER INTELLIGENZ IM UNTERNEHMEN

Jennifer Zwarg

Fakultät Wirtschafts- und Sozialwissenschaften

Hochschule Osnabrück

Caprivistraße 30a
49076 Osnabrück

E-Mail: j.zwarg@pm.me

Andreas Jede

Fakultät Wirtschafts- und Sozialwissenschaften

Hochschule Osnabrück

Caprivistraße 30a
49076 Osnabrück

E-Mail: a.jede@hs-osnabrueck.de

Frank Bensberg

Fakultät Wirtschafts- und Sozialwissenschaften

Hochschule Osnabrück

Caprivistraße 30a
49076 Osnabrück

E-Mail: f.bensberg@hs-osnabrueck.de

KEYWORDS

Systematic literature review, Artificial Intelligence, Guideline, Requirements, Company

ABSTRACT

Die Zukunftstechnologie Künstliche Intelligenz wird zunehmend in Unternehmen etabliert, um innovative Prozesse zu gestalten und nachhaltig zu optimieren. Kleine und mittlere Unternehmen nehmen KI-Einführungen nur zögerlich wahr, da diverse Ungewissheiten mit dieser Thematik verbunden sind. Ein Leitfaden soll Unternehmen eine Orientierung zu notwendigen Voraussetzungen und Handlungsbedarfen von KI-Projekten aufzeigen und Sicherheit schaffen, um weitere Unternehmen zur Realisierung zu motivieren. Eine systematische Literaturanalyse unterstützt dabei, den aktuellen Forschungsstand zu eruieren und Handlungsempfehlungen abzuleiten.

The future technology artificial intelligence is increasingly being established in companies in order to configure and sustainably improve innovative processes. Small and medium-sized businesses are hesitant to implement AI, due to various uncertainties which are associated with this subject matter. A guideline that gives companies orientation on necessary requirements and need for action in AI projects may achieve certainty and motivation to implement AI in further companies. A systematic literature review maintains to determine the current state of research and derives recommendations for action.

EINLEITUNG

Der Begriff Künstliche Intelligenz (KI) ist in der aktuellen Zeit omnipräsent und im technischen Sinne nahezu unverzichtbar. Die breite Bekanntheit dieses Trends ist insbesondere auf digitale Sprachassistenten, wie Amazon Alexa oder Google Assistant zurückzuführen. KI ist heutzutage in Smart TVs, Smartphones und Smart Watches integriert und wird als fester Bestandteil des menschlichen Alltags betrachtet. Vor allem die Bereiche autonomes Fahren und Robotik rücken zunehmend in den Vordergrund (Bolkart 2022). KI unterstützt dabei nicht nur im privaten Umfeld, sondern erzielt auch in der Industrie

Potenziale bei der Wertschöpfung in verschiedenen Anwendungsgebieten (VDMA - Verband Deutscher Maschinen- und Anlagenbau e.V. 2021).

Bei einer Umfrage von Bitkom aus dem Jahr 2020 wurden rund 600 deutsche Unternehmen ab einer Unternehmensgröße von über 20 Mitarbeitern zur Verwendung von KI befragt. Demnach sprechen sich etwa 73% der Befragten für großes Zukunftspotenzial aus. Nur etwa 6% der Unternehmen haben KI bereits im Einsatz, wohingegen 71% auch zukünftig keine Anwendung von KI planen. Ein ausschlaggebender Faktor für den Einsatz von KI wird der Größe des Unternehmens zugesprochen. Während 53% der Unternehmen mit einer Größe von 20 bis 99 Mitarbeitern KI als Potenzial für sich sehen, sind es bei einer Größe von über 2.000 Mitarbeitern bereits 84% (Streim & Uhl 2020). Ein Grund für die zögerliche Implementierung bei kleinen und mittleren Unternehmen (KMU) lässt sich auf die Komplexität von KI-Algorithmen sowie den Mangel an Fachkräften zurückführen (Deloitte Deutschland 2020). Denn 69% der Befragten geben an, dass es zu wenig KI-Fachpersonal gibt (Streim & Uhl 2020), um das vielfältige Anwendungsfeld erfolgreich in die Praxis umzusetzen.

Als neues und komplexes Forschungsfeld bringt KI für Unternehmen diverse Unsicherheiten mit sich. Vor diesem Hintergrund sollen Verantwortliche über eine Handlungsempfehlung Klarheit über notwendige Voraussetzungen im Unternehmen erhalten, die den zukünftigen Einsatz von KI ermöglichen.

Motivation und Methodik

KI ist eine vielfältig einsetzbare und komplexe Technologie, mit der Unternehmen sich einerseits wirtschaftliche Vorteile sichern können, die andererseits mit unterschiedlichen Herausforderungen behaftet ist. Bei der Einführung von KI sind verschiedene unternehmensspezifische als auch externe Faktoren zu berücksichtigen. Bereits zu Beginn eines KI-Projektes können Herausforderungen, wie die Verfügbarkeit von Fachpersonal, technische Voraussetzungen oder die Selektion eines geeigneten Algorithmus auftreten.

Vor diesem Hintergrund wird ein Konzept erarbeitet, das erforderliche Rahmenbedingungen für die erfolgreiche Implementierung einer KI-Lösung identifizieren soll.

Projektverantwortliche erhalten somit einen Überblick und erlangen Sicherheit bei der Umsetzung des zukünftigen KI-Projektes, um den erwünschten Mehrwert im Unternehmen zu generieren. Inhalt dieser Konzeption ist die Ausarbeitung der erforderlichen Rahmenbedingungen und Maßnahmen für die erfolgreiche Umsetzung eines KI-Projektes. Dabei findet eine thematische Abgrenzung zur Implementierung in die technische Infrastruktur statt, die nicht betrachtet wird. Inhaltlich werden zunächst die Grundlagen zu den Themengebieten Data Mining, KI und Maschinelles Lernen (ML) vermittelt, die im weiteren Verlauf zum Verständnis im weiteren Verlauf von Bedeutung sind.

Die systematische Literaturanalyse (SLA) dient als Forschungsmethode, mit der eine sukzessive Selektion und nachvollziehbare Auswertung der ermittelten Publikationen dargestellt wird, um relevante Voraussetzungen und Maßnahmen zu identifizieren. Die theoretischen Untersuchungsergebnisse werden in einem Modell zusammengefasst, das als Grundlage zur Anwendung in der Praxis dient. Mithilfe der theoretischen Untersuchungsergebnisse aus der SLA werden Handlungsempfehlungen abgeleitet und konzeptionell aufbereitet. Im Fazit werden die gewonnenen Erkenntnisse zusammengeführt und kritisch reflektiert.

DATA MINING UND DATA SCIENCE

Data Mining ist die Verarbeitung großer Rohdatenmengen, die aus Datenbanken extrahiert werden (Alpaydin 2022), um daraus Regeln, Muster oder Zusammenhänge zwischen verschiedenen Datensätzen zu finden (Shi & Zhu 2022). Die Begriffe Data Mining und ML werden oft miteinander in Verbindung gebracht. Dabei bestehen diese beiden Begriffe aus unterschiedlichen Konzepten (Kotu & Deshpande 2019), die im Zusammenhang mit KI im nachfolgenden Abschnitt und anhand der Abbildung 1 dargestellt werden. Während Data Mining sich u. a. auf die statistische und datenbankbezogene Anwendung konzentriert, basiert ML auf der Anwendung von Algorithmen. Generell besteht der Data Mining Prozess aus vier Schritten: Der Datenvorbereitung und -extraktion, Vorverarbeitung der Daten, der eigentlichen Durchführung des Data Mining und der Evaluation der Ergebnisse (Shi & Zhu 2022). Bereits 1996 wurde dieser Prozess von Fayyad et al. (1996) als KDD-Prozess (Knowledge Discovery in Databases) vorgestellt, auf dem viele der heutigen Modelle aufbauen. Bekannte Vorgehensmodelle sind der Cross Industry Standard Process for Data Mining (CRISP-DM) oder Analytics Solution Unified Method for Data Mining (ADUM-DM), das als Erweiterung zum CRISP-DM gilt (Brenner et al. 2021).

Mit Data Mining wird auch der Begriff Data Science in Verbindung gebracht. Dieser umfasst jedoch ein breiteres Themenspektrum als Data Mining und synthetisiert u. a. die Bereiche Statistik, Informatik, Kommunikation und Management (Cao 2017). Nach Luber & Litzel (2020) kommen im Data Science die Fachgebiete wie Data Mining, KI und ML zum Einsatz. Fachpersonal für Datenwissenschaften wird im Rahmen eines Studienganges oder durch Fortbildungen ausgebildet. Im Unternehmen

sind Data Scientists beispielsweise im Umfeld Online-Handel, Logistik und Produktion tätig (Luber & Litzel 2020).

RELEVANTE KÜNSTLICHE INTELLIGENZ

Der Begriff KI (engl. artificial intelligence, AI) lässt sich schwer abgrenzen. Bisher gibt es keine eindeutige Definition, da es sich um ein recht neues und dynamisches Forschungsgebiet handelt (Gethmann et al. 2022). Technisch betrachtet ist KI der Informatik zuzuordnen, die intelligentes Verhalten mit einem Computer simuliert (Kleesiek et al. 2020). Heutzutage gilt KI als Trend, mit dem sich viele Arten von Problemen lösen und Prozesse vereinfachen lassen. Im Forschungsumfeld ist KI beispielsweise in den Bereichen Klimaforschung, Medizin oder in der Physik etabliert (Gethmann et al. 2022).

Der Ausdruck Artificial Intelligence ist bereits 1956 durch John McCarthy, Marvin Minski, Allen Newell und Herbert Simon entstanden (Humm et al. 2022). Ein Grundstein zu intelligenten Maschinen wurde bereits 1950 durch Alan Turing (1912-1954) gelegt, der sich mit der Frage „Can machines think?“ (TURING 1950) auseinandersetzte und grundlegende Arbeiten zu Berechnungen im ‚Turing-Test‘ durchführte (Humm et al. 2022).

Ein KI-Trend fand in den USA bereits in den 60er bis 80er Jahren statt. Voreilige Schlüsse und zu optimistische Erwartungen ließen den Trend jedoch wieder abklingen. Das Wissen und die technischen Kapazitäten konnten zu dem Zeitpunkt nicht den erforderlichen Entwicklungsstand erfüllen (Humm et al. 2022). Erst mit den Sprachassistenten Siri (Apple) im Jahr 2011, gefolgt von Cortana (Microsoft) 2014 und Alexa (Amazon) 2015, nimmt KI im Alltag der Menschen wieder einen bedeutenden Aspekt ein (Robert Bosch GmbH o. J.; Wittpahl 2019). KI bietet Möglichkeiten wie Sprach- und Bilderkennung, maschinelle Übersetzungen bis hin zum autonomen Fahren. Diese Beispiele werden anhand verschiedener Teilbereiche (siehe Abbildung 1) der KI ermittelt. Aufgrund des noch recht jungen Forschungsfeldes sind diese bisher nicht einheitlich definiert (Humm et al. 2022).

KI kann in starke und schwache KI eingeordnet werden (engl. strong und weak AI). Der schwachen KI sind Anwendungen zuzuordnen, die zur Handhabung bestimmter Anwendungsfälle (AWF) konzipiert sind und mittels mathematischer und informationstechnischer Methoden das menschliche Denken unterstützen. Ohne die Zuarbeit des Menschen kann schwache KI nicht agieren. Im Gegensatz dazu soll starke KI nicht mehr auf den Menschen angewiesen sein und selbstständig wirken können. Es soll ermöglicht werden, dass sie die Intelligenz des Menschen adaptiert und ihr sogar voraus sein wird. Starke KI befindet sich derzeit noch in der Forschung (Mockenhaupt 2021).

Mit KI werden auch negative Aspekte assoziiert. In der Vergangenheit kam es zu Fehlentscheidungen der KI-Anwendungen, die zu diskriminierenden oder rassistischen Entscheidungen führten. Diese Fehlbewertungen werden Data Bias genannt und können sowohl anhand der vorliegenden Daten als auch auf die Konstruktion der

Modelle zurückzuführen sein. Jede Phase im Modellbau enthält bestimmte Praktiken und Entscheidungen, die zu einem unerwünschten Ergebnis führen können (Suresh & Guttag 2021). Eine Fehlentscheidung aufgrund von Bias kann für Unternehmen z. B. im Fall von Diskriminierung schwere wirtschaftliche Folgen und Reputationsschäden nach sich ziehen (Brenner et al. 2021).

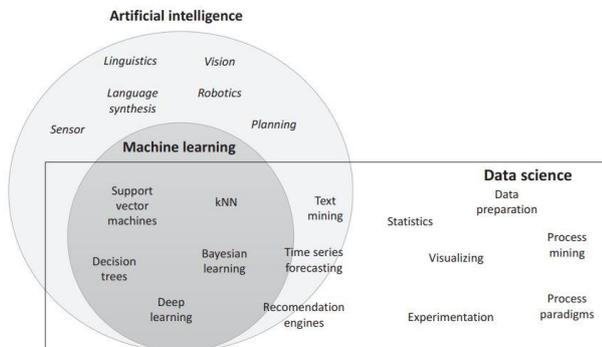


Abbildung 1: Abgrenzungen AI, ML und Data Science nach Rode-Schubert & Müller, 2020

Die Abbildung 1 verdeutlicht beispielhaft das Zusammenwirken zwischen KI, ML und Data Science. Als übergeordneter Begriff beinhaltet KI verschiedene Verfahrensmöglichkeiten. ML enthält als untergeordnete Kategorie weitere abgestimmte Verfahren, die mit den Methoden aus Data Science umgesetzt werden. Der Bereich Data Science verwendet zudem Methoden, die zur statistischen oder visuellen Auswertung angewandt werden. Durch die Abbildung 1 ist anhand der Vielzahl der einsetzbaren Algorithmen und nicht immer klaren Abgrenzung erkennbar, dass KI ein komplexes Themenfeld darstellt.

MASCHINELLES LERNEN

ML (engl. Machine Learning) ist ein Teilbereich der KI, der oft als Synonym für KI verwendet wird (Kleesiek et al. 2020; Weber 2020). Als ML wird die Fähigkeit einer Software oder Maschine bezeichnet, die mittels historischer Daten (Erfahrungen) trainiert wird (Buxmann & Schmidt 2019) und daraus Wissen generiert. Durch die Anwendung von Algorithmen wird ein komplexes Modell erstellt, mit dem das erworbene Wissen auf artgleiche Datensätze angewendet werden kann (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. 2018). Als Algorithmus wird dabei eine Handlungsvorschrift bezeichnet, die schrittweise zur Lösung eines Problems beiträgt (Gethmann et al. 2022). Mit trainierten Modellen können Prognosen und Entscheidungen getroffen werden. Auswertbare Daten können Bilder, Texte oder Sensordaten sein (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. 2018). Modelle können prädiktiv oder deskriptiv sein. Bei prädiktiven Modellen werden anhand historischer Daten Vorhersagen (Prognosen) erstellt, während deskriptive Modelle die beobachtete Realität beschreiben (Alpaydin 2022). Mit den Methoden des ML können offene und versteckte Zusammenhänge in Datensätzen ermittelt werden (Murphy 2012). Der Fokus des ML liegt dabei auf der

kontinuierlichen Verbesserung der Lösung einer zuvor definierten Aufgabe und ist abhängig von qualitativ hochwertigen Trainingsdaten. Es werden verschiedene Arten von ML verwendet, die grob in drei Lernkategorien eingeteilt werden. Das überwachte, unüberwachte und bestärkende Lernen (Murphy 2012; Weber 2020). Diese drei Lernkategorien des ML gehören zu den gebräuchlichsten Algorithmen, die jeweils auf unterschiedlichen Lösungsansätzen basieren (Pokorni et al. 2021). Die Einstufung der Lernkategorien ist nicht abschließend geklärt, weswegen in diversen Publikationen weitere Lernkategorien zu finden sind. In den folgenden Abschnitten erfolgt eine nähere Ausführung der drei genannten Lernkategorien.

Überwachtes Lernen

Das überwachte Lernen (engl. Supervised Learning) gehört zu den mehrheitlich angewandten ML-Verfahren in der Praxis. Beim Trainieren von vorhandenen Daten wird zwischen Trainings-, Test- und Validierungsdaten unterschieden. Mit den Trainingsdaten lernt das System die Muster und Zusammenhänge. Dabei ist darauf zu achten, dass keine Überanpassung (engl. Overfitting) auftritt, da die Trainingsdaten hierbei ‚auswendig‘ gelernt werden. Das Ziel, die Trainingsdaten auf weitere Aufgaben anwenden zu können, ist im Falle einer Überanpassung nicht mehr gegeben. Das trainierte Modell wird daher zunächst zur Bewertung der Qualität auf die Testdaten angewendet und mit den zusätzlichen Validierungsdaten validiert (Mockenhaupt 2021).

Bei diesem Verfahren ist zwischen Klassifikation und Regression zu unterscheiden. Klassifikationsaufgaben haben als Output einen nominalen Wert, wie z. B. männlich oder weiblich (Murphy 2012). Ein E-Mail Spam-Filter erkennt beispielsweise eingehende E-Mails und klassifiziert sie in die Kategorien ‚Spam‘ oder ‚kein Spam‘. Anhand eines vorliegenden Datensatzes mit Informationen zu Spam und normalen E-Mails werden Merkmale bestimmt, die einer bestimmten Klasse zugeordnet werden (Weber 2020).

Die Regressionsanalyse ermöglicht Vorhersagen von stetigen, numerischen Werten. Beispielsweise kann mittels historischer Verkaufsdaten in einem Geschäft der Umsatz für die zukünftige Periode ermittelt werden (Han et al. 2011). Somit können beispielsweise prädiktive Analysen zum Umsatz eines Geschäftes anhand von zuvor definierten Produktpreisen erstellt werden (Weber 2020).

Unüberwachtes Lernen

Beim unüberwachten Lernen (engl. Unsupervised Learning) findet im Vergleich zum überwachten Lernen, keine vorherige Definition der Inputvariablen als Merkmal einer bestimmten Klasse (Han et al. 2011) oder eines bestimmten Outputs statt. Unüberwachtes Lernen dient dazu, anhand der gegebenen Inputdaten, selbstständig potenziell verborgene Muster und Strukturen zu erkennen (Murphy 2012). Beispielsweise werden Kunden aufgrund ihres Kaufverhaltens einer bestimmten Gruppe zugeordnet. Neben dem Clustering wird im unüberwachten Lernen die Assoziationsanalyse (Association Analysis)

verwendet. Dieses Verfahren kann angewendet werden, um Regeln innerhalb dieser Kundengruppenzuordnung zu identifizieren. Dabei kann z. B. anhand des historischen Kaufverhaltens ermittelt werden, in welchem Ausmaß Kunden zu einem Primärprodukt X auch ein assoziiertes Sekundärprodukt Y kaufen (Weber 2020).

Bestärkendes Lernen

Das bestärkende Lernen (engl. Reinforcement Learning) ist in der Praxis weniger verbreitet. Dieser Algorithmus basiert darauf, Verhalten mit Belohnungen oder Bestrafungen zu erlernen (Murphy 2012). Bei diesem Lernverfahren werden keine Trainingsdaten oder zuvor definierte Ergebnisse vorausgesetzt. Stattdessen müssen Regeln sowie ein Signal festgelegt werden, das die erfolgte Handlung als positiv oder negativ einstuft. Anhand der Rückmeldungen wird ein Lerneffekt erzeugt, mit dem auch bisher unbekannte Ergebnisse erreicht werden können (Mockenhaupt 2021). Mit der Häufigkeit der auftretenden Rückmeldung (positiv oder negativ) erhöht sich die Stärke und der Erkenntnisgewinn für zukünftigen Handlungen. Diese Art von Algorithmen wird z. B. bei sogenannten Agenten verwendet (Weber 2020). Mockenhaupt (2021) definiert verschiedene Arten von Agenten. Sie können beispielsweise für das Sammeln von Daten konzipiert werden oder auf ihr Umfeld einwirken. In einem Netzwerk können Agenten zum Sammeln von Daten eingesetzt werden. Dabei selektieren sie notwendige Informationen zur weiteren Übertragung und können die Auslastung regulieren (Mockenhaupt 2021).

SYSTEMATISCHE LITERATURANALYSE

Der aktuelle Forschungsstand notwendiger Voraussetzungen zur Implementierung von KI soll mit einer SLA zu mehr Handlungssicherheit führen. Mit einer gezielten Suche werden schrittweise verschiedene Forschungs- und Anwendungsergebnisse zusammengefasst und ausgewertet. Die Synthese der reduzierten Literatur wird zur Beantwortung der Forschungsfragen herangezogen.

Begriffsbestimmung und Anwendungsbereich

Die Durchführung einer SLA kann diverse Gründe haben. Einerseits bietet ein noch wenig erforschtes Thema eine geringe Anzahl theoretischer Publikationen. Zudem liegt die Herausforderung in der Strukturierung und Darstellung vorhandener Literatur (Webster & Watson 2002). Im Gegensatz zu einem jungen Forschungsfeld sind Literaturrecherchen bereits gut erforschter Themenfelder aufgrund der Masse an Publikationen zunehmend aufwändiger und unübersichtlicher geworden. Eine gezielte Suche kann dabei unterstützen, vorhandene Forschungserkenntnisse zusammenzufassen (Fettke 2006). Somit wird ein solides Grundlagenwissen über den aktuellen Forschungsstand generiert. Zudem können neue Erkenntnisse über das jeweilige Forschungsfeld erschlossen werden. Die Auswahl und Analyse relevanter Literatur ist dabei ein elementarer Bestandteil wissenschaftlicher Forschungsprojekte. Hochwertige Literaturanalysen zeichnen sich durch eine vollständige und systematische

Vorgehensweise aus. D.h., es findet keine Einschränkung auf eine bestimmte Zeitschriftenart oder der geographischen Region statt. Bei der Suche kann zusätzlich die Vorwärts- und Rückwärtssuche angewendet werden. Diese Methode dient als Ergänzung zur Datenbanksuche. Die Vorwärtssuche basiert dabei auf der Suche nach Literatur, welche die gefundene Quelle zitiert. Bei der Rückwärtssuche werden dagegen die zitierten Quellen aus der gefundenen Literatur identifiziert. Beide Suchmethoden zielen darauf ab, weitere relevante Publikationen zu eruieren (Webster & Watson 2002).

Vorgehensmodell

Die SLA wird in mehreren Schritten durchgeführt. Eine übersichtliche Basis bietet das Vorgehensmodell von vom Brocke et al. (2009), das in fünf Phasen gegliedert ist (Abbildung 2).

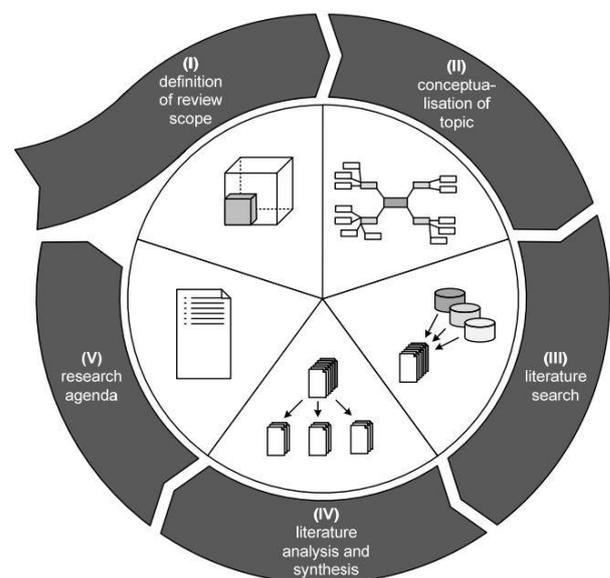


Abbildung 2: Vorgehensmodell der SLA nach vom Brocke et al., 2009

In Phase I wird zunächst der thematische Suchbereich definiert. Hierbei werden relevante Suchkriterien festgelegt (s. Tabelle 1). Phase II beinhaltet die Erstellung eines Suchkonzepts, das ein solides Wissen über das Thema voraussetzt. Der Suchprozess in Phase III umfasst das Anwenden von Datenbanken, Keywords, die Reduzierung auf relevante Literatur sowie die Vorwärts- oder Rückwärtssuche. Der Ausschluss von Literatur erfolgt anhand der Auswertung von Titel, Abstract und Volltexten. Nachdem eine ausreichende Menge relevanter Literatur zusammengetragen werden konnte, wird in Phase IV die Analyse und Synthese der Quellen durchgeführt. Dieser Sortierungsprozess ermöglicht eine Kategorisierung der Publikationen. Schließlich kann eine thematische Einordnung gem. Phase V mit einer Konzeptmatrix von Webster & Watson zusammengefasst und zur Auswertung des aktuellen Forschungsstandes sowie zum Aufdecken von Forschungslücken herangezogen werden (vom Brocke et al. 2009).

Anwendung des Vorgehensmodells

Bevor eine gezielte Literatursuche durchgeführt wird, ist die Definition des zu untersuchenden Forschungsfeldes von entscheidender Bedeutung. Mithilfe des Vorgehensmodells nach vom Brocke et al. (2009), sollen folgende Forschungsfragen beantwortet werden:

1. Welche Rahmenbedingungen müssen zur Umsetzung eines erfolgreichen KI-Projektes in einem Unternehmen gegeben sein?
2. Welche weiteren Maßnahmen ergeben sich nach Evaluierung der Rahmenbedingungen, um die Implementierung von KI erfolgreich zu realisieren?

Das Vorgehensmodell beginnt mit Phase I, bei der zunächst ein grober Rahmen der Ein- und Ausschlusskriterien zur Literatur festgelegt werden. Diese sind in der Tabelle 1 definiert. Da es sich bei dem Thema KI um ein aktuelles und dynamisches Thema handelt, wird die Suche auf veröffentlichte Publikationen der letzten drei Jahre (2019 bis 2022) beschränkt.

Kriterium	Beschreibung
Sprache	Deutsch und Englisch
Zugänglichkeit	Frei zugänglich, Online
Publikationstyp	Keine kurzen Paper (weniger als 2 Seiten, z. B. Poster, redaktionelle Beiträge etc.), keine Abschlussarbeiten
Publikationsinhalt	Keine Duplikate (nach Titel und Inhalt)
	Publikationen mit relevanten Informationen zur Beantwortung der Forschungsfragen

Tabelle 1: Ein- und Ausschlusskriterien der Literatursuche in Anlehnung an Sanchez-Puchol & Pastor-Collado, 2017

Für den nächsten Schritt (Phase II) konnte eine Vorrecherche Aufschluss über den zu untersuchenden Themenbereich geben. Unter Einbeziehung der Ein- und Ausschlusskriterien werden themenbasierte Schlüsselwörter (Keywords) zur Beantwortung der Forschungsfragen definiert. Datenbankeingaben mit Test-Keywords geben Hinweise auf weitere Keywords bzw. Synonyme. Daraus ergibt sich die folgende Abfrage:

((„Künstliche Intelligenz“ OR „artificial intelligence“) AND („Unternehmen“ OR „company“) AND („Einführung“ OR „implement*“ OR „Umsetzungsstrategie“ OR „Konzept*“ OR „concept*“ OR „framework“ OR „Voraussetzung*“ OR „requirement“))

Gem. Phase III werden adäquate Datenbanken festgelegt. Hierzu werden wissenschaftliche und internationale Inhalte herangezogen. Aufgrund der hohen Praxisrelevanz werden zusätzlich praxisorientierte (nicht wissenschaftliche) Quellen betrachtet. Inkludiert werden die Suchmaschinen Google Scholar, IEEE (Institute of Electrical and Electronics Engineers), scinos (scientific information osnabrück) der Hochschule Osnabrück und SpringerLink. Über Google findet zudem eine manuelle Suche

praxisorientierter Quellen statt. Die Suche wurde im Zeitraum vom 20.06. bis 24.06.2022 durchgeführt. Aufgrund des zeitlichen Umfangs wird auf eine Vor- bzw. Rückwärtssuche verzichtet.

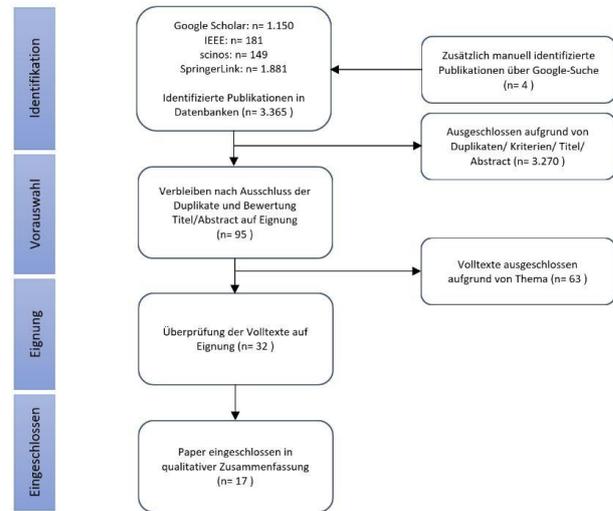


Abbildung 3: Flussdiagramm für den Aussortierungsprozess von Publikationen (in Anlehnung an prisma-statement.org)

Mit der Abfrage wurden 3.365 Treffer in den angegebenen Datenbanken gefunden. Die Abbildung 3 stellt die durchlaufenen Phasen des angewandten Verfahrens dar. Nach Ausschluss der Duplikate, anhand der festgelegten Kriterien, des Titels sowie Sichtung des Abstracts, konnte die Treffermenge um 3.270 Publikationen reduziert werden. Die verbleibenden 95 Publikationen werden nach einer groben Sichtung der Volltexte auf 32 reduziert. In einer finalen Sichtung und Prüfung auf Eignung der 32 Publikationen, werden 17 Paper in die qualitative Zusammenfassung eingeschlossen.

Die inhaltliche Strukturierung der 17 Publikationen erfolgt in einer Konzeptmatrix nach Webster & Watson (s. Tabelle 2). In den Zeilen sind Autor und Erscheinungsjahr und in den Spalten die gefundenen Konzepte dargestellt. Um das systematische Vorgehen bei der Einführung von KI zu strukturieren, sind die Konzepte grob in die beiden Kategorien Ausgangsbasis und Folgemaßnahmen unterteilt. Die Kreuze markieren die inhaltlichen Konzepte der jeweiligen Publikation. Diese werden schließlich aufsummiert und können Aufschluss über die Relevanz spezifischer Handlungsschritte geben.

Konzepte	Ausgangsbasis						Folgemeasures						
	KI-Fachkompetenzen intern/extern	Qualität/ Zugang Datenbasis	Eignung Hardware/ IT-Infrastruktur	(Agiles) Projektmanagement	Klare Zieldefinition/ Konzeption AWF	Kostenfaktoren/ Budget	KI-Plattform (SaaS/Onpremise)	Echtzeitverarbeitung (5G)/ Performance	KPI / Bewertungskriterien	Akzeptanz im Unternehmen/ Geschäftsprozesse anpassen	Datensicherheit/ -schutz	Vorgehensmodell	
Rode-Schubert & Müller, 2020	x	x	x	x		x		x					
Regnerl, 2021		x						x	x		x		
Haarmeier, 2021	x	x	x			x	x						
Stowasser, 2021					x				x	x			
Kern & Sattler, 2020	x	x	x										
Brenner et al., 2021	x	x	x	x	x				x			x	
Pokorni et al., 2021	x	x	x	x	x	x		x	x	x		x	
Petry, 2021	x	x	x			x	x	x	x	x	x	x	
Matzka, 2021		x			x	x						x	
van Giffen et al., 2020	x	x	x		x	x	x	x	x			x	
Herremans, 2021	x	x	x	x	x		x	x				x	
Wuttke, 2022	x	x	x		x		x		x				
Rainsberger, 2021	x	x	x	x	x	x			x	x		x	
Aichele, 2021	x			x	x	x							
Vollhardt et al., 2021	x	x	x	x	x		x					x	
Müller et al., 2021	x	x	x		x	x	x		x	x	x		
Diab et al., 2022		x	x				x	x				x	
Gesamt	13	15	13	7	11	9	8	3	6	9	5	7	3

Tabelle 2: Konzeptmatrix in Anlehnung an Webster & Watson, 2002

Quantitative Literaturlauswertung

Mit der Konzeptmatrix konnte eine quantitative Übersicht der themenbezogenen Konzepte ermittelt werden. In der Kategorie Ausgangsbasis sind die Konzepte definiert, welche die Rahmenbedingungen für den zukünftigen Einsatz von KI festlegen. Diese werden als Voraussetzung erachtet und sollten vor Projektbeginn erfüllt sein. Von diesen sechs Konzepten wurden fünf identifiziert, die in mindestens 50% der vorliegenden Publikationen genannt werden. Am häufigsten werden die Qualität der Datenbasis (88%), KI-Fachkompetenzen (76%) sowie die Eignung der IT-Infrastruktur und Hardware (76%) genannt. Etwa 65% der Publikationen thematisiert zudem, dass eine klare Definition der Ziele bzw. der Entwurf des AWF notwendig sei. Die Bestimmung eines Budgets für die Umsetzung wird dabei in 53% der Fälle genannt. Das (agile) Projektmanagement (PM) erhält mit 41% den kleinsten Anteil aus den genannten Konzepten dieser Kategorie.

Nach Erfüllung der Ausgangsbasis sollten relevante Folgemeasures bei der Projektdurchführung umgesetzt werden. Eines der sieben Konzepte wird in über 50% der Publikationen definiert. Obwohl die weiteren sechs Konzepte diese Schwelle nicht erreicht haben, werden sie als bedeutsamer Bestandteil eines KI-Projektes erachtet. Den höchsten Wert haben in diesem Fall die Schaffung der Akzeptanz und das Vertrauen in KI im Unternehmen (53%) erreicht. Weiterhin sind im oberen Drittel die Nutzung einer KI-Plattform (47%) und die Gewährleistung von Datensicherheit/-schutz (41%) einzuordnen. In den mittleren Bereich fallen das Festlegen von KPIs und Bewertungskriterien (35%), die zur Leistungsmessung der KI-Anwendung notwendig sind, sowie die Anpassung und Optimierung der Geschäftsprozesse (29%), in denen die KI implementiert wird. Die Echtzeitverarbeitung, die über ein 5G Netz realisiert wird und die Anwendung

eines standardisierten Vorgehensmodells, wie dem CRISP-DM, werden dagegen in nur 18% der Fälle beschrieben.

KONZEPTION UND PRAKTISCHE UMSETZUNG

Die quantitative Literaturlauswertung legt die Basis für die Synthese der Ergebnisse und Umsetzung in die Praxis. Aufbauend auf der quantitativen Literaturlauswertung erfolgt in den folgenden Abschnitten die qualitative Literaturlauswertung. Die Rahmenbedingungen und weiteren Maßnahmen für den Einsatz von KI werden anschließend in einem Konzept zusammengefasst.

Voraussetzungen für KI-Projekte

Die Evaluation der qualitativen Literaturlauswertung zeigt die konzeptionelle Relevanz verschiedener Bereiche auf, die bei der Umsetzung von KI-Projekten im Unternehmen als wichtig erachtet werden. KI-Einführungen sind nicht mit der Einführung von Software zu vergleichen. KI setzt sich aus einem Algorithmus, einer qualitativ hochwertigen Datenbasis und Business Intelligence zusammen (Rainsberger 2021). Dabei ist der Algorithmus in den meisten Fällen vom AWF abhängig und kann nicht auf andere AWF übertragen werden (Diab et al. 2022).

Nach Matzka (2021) ist ein sinnvoller Einsatz von KI nur gegeben, wenn der technische und wirtschaftliche Nutzen im Vergleich zum vorherigen Zustand höher ist und der Ressourcenaufwand verringert wird. Zur technischen Umsetzung gibt es bereits standardisierte, methodische Ansätze wie z. B. CRISP-DM. Dieses Modell stellt jedoch nur eine von vielen Projektphasen dar und darf nicht isoliert betrachtet werden (Matzka 2021). Zu Beginn eines KI-Projektes besteht oftmals die Notwendigkeit veraltete IT-Systeme abzulösen oder zu optimieren. KI-Anwendungen können daher erhebliche Investitionen mit sich bringen (Brenner et al. 2021). Nach einer KI-Implementierung sollte der Entwicklungsprozess nicht als abgeschlossen betrachtet werden. KI als neue Technologie wird stetig weiterentwickelt und erfordert die Weiterbildung des Fachpersonals (Herremans 2021).

In den nachstehenden Abschnitten werden die einzelnen Konzepte ausformuliert. Betrachtet werden dabei die wesentlichen Voraussetzungen für den Einsatz von KI, bei denen ein prozentualer Anteil von über 50% in den vorliegenden Publikationen der SLA gegeben ist. In dieser Größenordnung ist davon auszugehen, dass die Konzepte in der Vergangenheit bereits ausreichend erprobt wurden. Die verbleibenden Konzepte werden aufgrund des geringen Bewertungsanteils im Abschnitt ‚Zusammenfassung Ausgangsbasis und Folgemeasures‘ lediglich zusammengefasst.

Trotz weitreichender Recherche haben die aufgeführten Voraussetzungen keinen Anspruch auf Vollständigkeit. Zudem ist zu berücksichtigen, dass KI ein dynamisches Forschungsfeld darstellt (Gethmann et al. 2022) und sich aufgrund neuer Forschungserkenntnisse zukünftig verändern kann.

Qualität der Datenbasis

Daten sind in den vorliegenden Publikationen ein entscheidender Faktor für die erfolgreiche Einführung von KI. Für KI- und ML-Anwendungen bilden Daten die Ausgangsbasis. Dabei nehmen die Beschaffung und die Aufbereitung der Daten in der erforderlichen Qualität etwa 80% des Projektaufwands in Anspruch. Das Scheitern von KI-Projekten ist in vielen Fällen auf eine schlechte Datenverfügbarkeit und -qualität zurückzuführen (Brenner et al. 2021). Dies trifft ebenfalls bei einer zu kleinen Datenbasis zu, da zum Trainieren eines brauchbaren Modells eine ausreichend große Datenbasis zur Verfügung stehen muss (Müller et al. 2021).

Nach Rode-Schubert & Müller (2020) muss im Unternehmen die Voraussetzung erfüllt sein, dass die relevanten Daten aus dem System ausgelesen und von Fachpersonal aufbereitet und bereinigt werden können. Hierbei sind die korrekte Selektion und eine geringe Fehlerquote der Daten, wie auch ein ausreichendes Datenvolumen entscheidend. Eine schlechte Datenbasis mit geringem Umfang kann zu fehlerhaften oder ungenügenden Ergebnissen führen. Dabei müssen teils auch Daten aus heterogenen Anwendungssystemen zusammengeführt und integriert werden. Werden diese Schritte nicht gewissenhaft durchgeführt, könnte eine Nutzung fehlerhafter oder unvollständiger Daten dazu führen, dass der Algorithmus keinen Zusammenhang findet. Eine hohe Datenqualität bildet die Voraussetzung zur Gewinnung verwendbarer Analyseergebnisse (Rode-Schubert & Müller 2020).

KI-Fachkompetenzen

Eine gute Datenqualität ist neben dem umfangreichen Know-how im Bereich KI und Data Science von entscheidender Bedeutung. Mithilfe der Techniken aus dem Bereich Data Science können Berechnungsmethoden zur Identifikation von Mustern und Strukturen in Datensätzen beitragen und prägnante Modelle zur Visualisierung generiert werden (Pokorni et al. 2021). Data Scientists verfügen über methodische Kenntnisse in der Anwendung von KI und ML. Die Tätigkeiten eines Data Scientist beinhalten einerseits die Auswahl und Bereinigung sowie die Herstellung der geforderten Datenqualität. Darüber hinaus ist die Vorbereitung für die Modellierung, Transformation und Integration der Daten und deren Verarbeitung ebenso wichtig wie die Analyse und Bewertung von statistischen Ergebnissen. Die Fähigkeit zum Visualisieren der erstellten Modelle verhilft dabei, bessere Aussagen bei der Untersuchung der Qualität und potenziellen Fehlerquellen zu treffen (Keim & Sattler 2020). Beim Aufbau dieser Kompetenzen müssen Unternehmen entscheiden, ob eine interne Ausbildung durchgeführt wird oder ob externe Dienstleister oder Berater herangezogen werden. Eine weitere Möglichkeit bietet die Einstellung von Fachpersonal. Aufgrund des Fachkräftemangels kann sich diese Entscheidung jedoch als langwieriger Prozess herausstellen (Rainsberger 2021). Neben den Kompetenzen als Data Scientist sind in KI-Projekten aus technischer Sicht weitere Fähigkeiten erforderlich. Beispielsweise programmieren Softwareentwickler notwendige Schnittstellen in der IT-Infra-

struktur, während weiteres Fachpersonal den Überblick auf Anforderungen und Probleme im Unternehmen behalten und diese analysieren muss (Pokorni et al. 2021; Rainsberger 2021). Die Verfügbarkeit von adäquaten Fachkompetenzen stellt für KI-Projekte einen wesentlichen Bestandteil dar und kann bereits zu Beginn der Planung eine Herausforderung bedeuten.

Eignung der IT-Infrastruktur

Die IT-Infrastruktur dient dazu, Daten über Hard- und Softwarekomponenten für die Analyse verfügbar zu machen. Im Sinne von KI soll die IT-Infrastruktur eine effiziente, störungssichere und skalierbare Datenverfügbarkeit bereitstellen. Verschiedene Komponenten sollen optimal aufeinander abgestimmt sein, um die technischen Voraussetzungen für KI zu ermöglichen (Petry 2021). Dabei ist die technische Leistung der IT-Infrastruktur vom Innovationsgrad der KI abhängig. Ein stärkerer Innovationsgrad benötigt leistungsstarke Server, Speicher sowie Hard- und Software (Brenner et al. 2021). Bei der Datenspeicherung ist festzulegen, ob und welche Daten auf eigenen Servern abgelegt werden und inwiefern auf eine Cloud-Lösung zurückgegriffen werden soll. Dabei sollten die Aspekte Datenschutz bei sensiblen Daten (Herremans 2021) und die Datentransferrate in Bezug auf KI beachtet werden. Die notwendigen Schnittstellen für die Datenströme der IT-Infrastruktur müssen eine gute Performance für die KI bieten. Hierbei ist insbesondere die Möglichkeit zur Verarbeitung von großen Datenmengen zu berücksichtigen. Außerdem kann bei einigen Algorithmen eine spezielle Hardware erforderlich sein (Diab et al. 2022), die es zu beachten gilt. Zudem muss bei der eingesetzten Software Interoperabilität gegeben sein, die bei einem Einsatz von verschiedenen KI-Softwarekomponenten eine leistungsfähige KI ermöglicht (Rode-Schubert & Müller 2020).

Klare Zieldefinition

Mit einer präzisen Zieldefinition können Lösungsansätze im angemessenen Umfang entwickelt werden. Dabei sollte der Algorithmus nicht im Vordergrund stehen. Generell sollte der Fokus auf die Optimierung des wirtschaftlichen Mehrwertes liegen (Wuttke 2022). Eine objektive Analyse soll Aufschluss über die Fragen geben, welchen Nutzen die zukünftige KI-Anwendung erfüllen soll. Dies können z. B. die Steigerung des Return on Investment (ROI) oder ein Wettbewerbsvorteil gegenüber der Konkurrenz sein (Petry 2021). Neben der Zieldefinition sorgt eine Potenzialanalyse und Abschätzung der technischen und sozialen Auswirkungen für den nötigen Weitblick. Zielkonflikte und Risiken können bereits im Vorfeld identifiziert und Potenziale ergriffen werden (Stowasser 2021). Der Einsatz von Planungswerkzeugen (z. B. KI-Canvas) kann bei der Formulierung unterstützend wirken, um den Prozess strukturiert und übersichtlich abzubilden. Dabei können einzelne Karten mit der konkreten Fragestellung oder Zieldefinition formuliert und schrittweise konkretisiert werden. Diese geben beispielsweise Aufschluss über die erforderlichen Input-

Daten für das KI-Modell, den erwarteten Output oder die Definition relevanter KPIs (Müller et al. 2021).

Kostenfaktoren

Ein weiteres Kriterium sind die entstehenden Kosten, die mit einem KI-Projekt einhergehen. Das vorhandene Budget sollte vor Beginn des KI-Projektes mit den zukünftigen Kosten abgeglichen werden. Eine gründliche Abschätzung entstehender Kosten ist für den Erfolg des KI-Projektes unabdingbar. Diese können grob in Verwaltungs-, Entwicklungs-, Software- und Implementierungskosten unterteilt werden (Rainsberger 2021).

Wie bereits im Abschnitt ‚KI-Fachkompetenzen‘ beschrieben, ist qualifiziertes Fachpersonal in verschiedenen Bereichen erforderlich. Je nach Vorhandensein von verfügbarem Fachpersonal im Unternehmen sind interne und externe Personalkosten zu berücksichtigen. Diese sind mit der richtigen Qualifikation und in angemessener Anzahl einzusetzen. Alternativ sind Kosten für die Aus- und Weiterbildung zu berücksichtigen. Beim Einsatz einer Cloud sind die anfallenden Kosten abhängig von der Nutzung und der Speicherkapazität sowie der Preisgestaltung des Anbieters. Betriebskosten der zukünftigen KI-Anwendung fallen ebenfalls in die Kostenschätzung (Petry 2021). KI-Software wird für z. B. die Erstellung eigener Modelle genutzt. Die Kosten sind abhängig vom Funktionsumfang. Zu den Implementierungskosten zählen u. a. die Programmierung von Schnittstellen und die Integration in bestehende Systeme (Rainsberger 2021).

Im ersten Projektjahr ist vor allem mit Entwicklungskosten für die KI-Anwendung zu rechnen und evtl. mit Investitionen zur Anpassung der IT-Infrastruktur. Kosten für Weiterentwicklung, Wartung, interne und externe Personalkosten und sonstige Kosten fallen im gesamten Betrachtungszeitraum des Projektes an (Aichele 2021).

Zusammenfassung Ausgangsbasis und Folgemaßnahmen

In diesem Abschnitt werden die Konzepte der Ausgangsbasis mit der Bewertung unter 50% betrachtet und mit den Folgemaßnahmen zusammengeführt.

Das PM erreicht in der Auswertung einen Wert von 41% einen eher geringen Anteil, obwohl die sorgfältige Planung und Durchführung von KI-Projekten nach eigener Einschätzung einen hohen Stellenwert haben. Das aufgestellte Personal in einem KI-Team sollte dabei über grundlegendes Fachwissen digitaler Prozesse (Pokorni et al. 2021) und interner Betriebsabläufe verfügen (Herremans 2021). Bei der Wahl der PM-Methode wird zwischen dem klassischen und agilen PM unterschieden. Der klassische Ansatz wird zunehmend durch das agile PM ersetzt. Bei KI-Projekten eignet sich das agile PM mit iterativen Vorgehen (Aichele 2021; Rode-Schubert & Müller 2020).

Nach Definition der Voraussetzungen, die zu Beginn eines KI-Projektes bestimmt sein sollten, sind weitere Maßnahmen zu ergreifen. Die ermittelten Konzepte in der Kategorie Folgemaßnahmen sind alle mit einem Wert unter 50% bewertet. Dennoch sind die Folgemaßnahmen

Bestandteil eines KI-Projektes und nicht auszuschließen. Im Folgenden werden die zentralen Aussagen zusammengeführt.

Die größte Relevanz fällt mit 47% auf KI-Plattformen sowie Akzeptanz von KI im Unternehmen. Haarmeier (2021) definiert KI-Plattformen als Cloud-basierte Services (KI-as-a-Service), mit denen Lösungen als Entwicklungsumgebung für ML-Modelle zur Verfügung gestellt werden. Da die Plattformen auf bestimmte AWF spezialisiert sind, sollte vor Auswahl der KI-Plattform der konkrete AWF definiert sein. Für KMU bieten sie einen guten Einstieg, da eine Einrichtung eigener Hard- und Software entfällt. Ein weiterer Vorteil ist die Skalierbarkeit, die z. B. bei Modellen mit großer Rechenleistung angepasst werden kann (Haarmeier 2021). Bei KI-Plattformen ist auf Datenschutz zu achten, der bei der Verarbeitung personenbezogener Daten zu gewährleisten ist. Flexible Plattformen sollten sich leicht um neue Komponenten erweitern lassen und neue Technologien und Datentypen zulassen (Petry 2021).

In der Vergangenheit haben Verzerrungen von Daten oder Bias zu fehlerhaften Entscheidungen von KI-Algorithmen beigetragen. Diese Bias sind auf unvollständige Trainingsdaten zurückzuführen und haben daraufhin z. B. ethnische Gruppen unterschiedlich behandelt. Dies ist eines von vielen Beispielen, die das Vertrauen und die Akzeptanz von KI reduzieren (van Giffen et al. 2020). Nach Stowasser (2021) sollten vor der Implementierung von KI-Anwendungen die Akzeptanz der Mitarbeiter im Unternehmen und das allgemeine Vertrauen in KI gewährleistet sein. Es ist daher erforderlich für Transparenz im Unternehmen zu sorgen und das Verfahren der KI zu erläutern. Mitarbeiter sollten über technische, soziale und positive wirtschaftliche Auswirkungen geschult werden. Dabei sollen die Transparenz und Erklärbarkeit der Entscheidungen von KI nachvollzogen werden können. Je nach AWF müssen Mitarbeiter ggf. auf neue Arbeitsprozesse vorbereitet und qualifiziert werden (Stowasser 2021). Bei einer Interaktion zwischen Mensch und Maschine muss dem Menschen die Möglichkeit gegeben sein, bei der endgültigen Entscheidung auf die maschinelle Entscheidungsunterstützung zu verzichten (Pokorni et al. 2021).

In puncto Vertrauen nehmen Datenschutz und Datensicherheit im Unternehmen einen hohen Stellenwert ein, der insbesondere durch die hohe Datenabhängigkeit der KI bedingt wird. IT-Systeme müssen daher bestimmte Sicherheitsstandards erfüllen (Diab et al. 2022) und die datenschutzkonforme Verarbeitung personenbezogener Daten gemäß Datenschutz-Grundverordnung (DSGVO) sicherstellen (Rainsberger 2021).

Mit KPIs kann die wirtschaftliche Leistung eines Unternehmens gemessen werden. Diese können auch zur Leistungsbewertung der KI-Anwendung herangezogen werden, um dessen Kosten-Nutzen-Verhältnis zu eruieren (Herremans 2021). Die Leistung der KI-Anwendung kann ohne die Bestimmung von KPIs nicht gemessen werden (Petry 2021). Nach Pokorni et al. (2021) sollten vor der betrieblichen Einführung umfassende Prüfungen im Hinblick auf die Funktionalitäten, Genauigkeit, Bias,

Nutzerakzeptanz und Usability sowie der Mehrwert für das Unternehmen vorgenommen werden. Auffälligkeiten können daraufhin behoben und ggf. weiter verfeinert werden (Pokorni et al. 2021).

Wie bereits im Abschnitt ‚Eignung der IT-Infrastruktur‘ beschrieben, müssen mit einer KI-Einführung individuelle Anpassungen in der IT-Infrastruktur vorgenommen werden. Unternehmen sollten die Chance ergreifen, den jeweiligen AWF vor der Digitalisierung zu optimieren oder neu zu gestalten. Damit soll vermieden werden, dass ein schlechter Prozess in einen schlechten Prozess mit einer KI-Anwendung überführt wird (Rainsberger 2021).

In 18% der Fälle wird auf ein Vorgehensmodell zurückgegriffen, das einen iterativen Ansatz zur Strukturierung von KI-Projekten beschreibt. Ein standardisiertes Modell ist CRISP-DM, das die sechs Projektphasen Business Understanding, Data Understanding, Data Preparation, Modeling, Evaluation und Deployment beschreibt (Matzka 2021). Brenner et al. (2021) schildern, dass die wachsende Komplexität, die z. B. bei der Datenverarbeitung und -speicherung im Sinne von Big Data mit sich bringt, kaum berücksichtigt wird. Aufgrund von weiteren Kritikpunkten erarbeitete IBM die Analytics Solution Unified Method for Data Mining (ASUM-DM) als optimiertes Modell in Anlehnung an CRISP-DM. Ein weiteres Vorgehensmodell stellt der Team Data Science Process (TDSP) von Microsoft dar. Dieses Modell involviert u. a. die Aspekte Teamzusammenarbeit, Lernen, Agilität und ist primär für Projekte der prädiktiven Analytik geeignet, z. B. in Verbindung mit KI (Brenner et al. 2021). Je nach AWF kann eines dieser Modelle als Ergänzung dienen bzw. in das KI-Projekt integriert werden.

Große Datenmengen, insbesondere Big Data, erfordern eine robuste Netzwerk- und IT-Infrastruktur sowie eine angemessene Bandbreite und Latenz. Sind die Voraussetzungen nicht gegeben, kann die KI-Anwendung nicht zuverlässig arbeiten (Diab et al. 2022). Sofern diese für eine Echtzeitverarbeitung eingesetzt wird, ist die Verwendung einer 5G Breitbandverbindung vonnöten (Rode-Schubert & Müller 2020).

Empfehlungen zur Vorgehensweise

Aufgrund der chronologisch absteigenden Aufstellung nach der quantitativen Auswertung der Publikationen ist keine Handlungsreihenfolge vorgegeben. Diese basiert primär auf der ausführlichen Erläuterung. Für eine praxisorientierte Anwendung kann ein Schaubild zur besseren Übersicht beitragen. In Abbildung 4 wird eine Handlungsreihenfolge als modellhafte Nachbildung der einzelnen Projektphasen beispielhaft dargestellt. Dabei wird die bisherige Kategorisierung in ‚Ausgangsbasis‘ und ‚Folgemaßnahmen‘ aus der SLA verfeinert. Die einzelnen Projektphasen fassen die Handlungen zur besseren Orientierung zusammen. Dabei können die Handlungen fließend in die nachfolgende Phase übergehen.

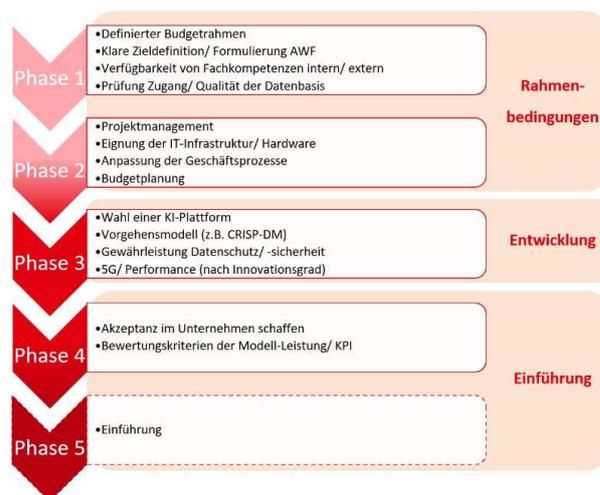


Abbildung 4: Überblick der Projektphasen zur Orientierung für KI-Projekte (Eigene Darstellung)

In Phase 1 sollte zunächst ein vorhandener Budgetrahmen vorliegen. Ohne ein ausreichendes Budget können nachfolgende Schritte nicht oder nur teilweise umgesetzt werden. Hierbei wird die kombinierte Kalkulation mit der Budgetplanung in Phase 2 empfohlen. Weiterhin ist es erforderlich das Ziel des KI-Projektes zu benennen. Eine zusätzliche Formulierung des AWF schafft Klarheit und Handlungssicherheit bei der Planung weiterer Schritte. Zudem ist zu berücksichtigen, ob interne oder externe Fachkompetenzen mit der richtigen Niveaustufe und in ausreichendem Umfang verfügbar sind. Ein erfolgsentscheidender Faktor ist der Zugang zur Datenbasis sowie eine ausreichende Quantität und Qualität. Diese ist durch Fachpersonal zu bewerten und nach Notwendigkeit aufzubereiten. Sofern diese Bedingungen gegeben sind, kann in Phase 2 sowohl das PM-Team zusammengestellt als auch die PM-Methode festgelegt werden. Der mit einer KI-Anwendung auszustattende Geschäftsprozess ist auf Optimierungspotenzial zu untersuchen und muss bei Bedarf angepasst werden. In einem weiteren Schritt besteht die Anforderung, die bestehende IT-Infrastruktur und Hardware von Fachpersonal auf Eignung zu überprüfen. Einzelne Anpassungen bis hin zur kompletten Umstrukturierung sind dabei denkbar. Diese sind neben den zusätzlichen Kosten gemäß der genannten Kostenfaktoren in der Budgetplanung zu berücksichtigen. Sofern diese Rahmenbedingungen zur Realisierung des KI-Projektes gegeben sind, findet ab Phase 3 die Umsetzung weiterer Maßnahmen statt. Da in dieser Phase die Entwicklung des Modells durchgeführt wird, kann sie auch als Entwicklungsphase bezeichnet werden. Für die Modellierung wählt das Fachpersonal in Anlehnung an die Anforderungen des AWF eine adäquate KI-Plattform als Entwicklungsumgebung. Die vorgestellten Vorgehensmodelle, wie etwa CRISP-DM, sollten nicht isoliert betrachtet werden und Teil des Projektes sein. Da in diesem Fall bereits ein Grundgerüst definiert ist, könnte eines der vorgestellten Vorgehensmodelle als Ergänzung und Unterstützung in der Modellentwicklung eingesetzt werden. Dies betrifft beispielsweise die Phasen Datenanalyse, -visualisierung, -vorbereitung, -bereinigung,

sowie maschinelle Modellbildung und Evaluation des maschinellen Modells (Matzka 2021). Bereits während der Entwicklungsphase ist es sinnvoll zu eruieren, inwiefern die Aspekte Datenschutz und -sicherheit integriert werden müssen. Je nach Innovationsgrad der KI-Anwendung ist die Bereitstellung einer 5G Breitbandverbindung zur Verarbeitung von Echtzeitdaten frühzeitig zu veranlassen, damit dieser termingerecht zur Implementierung bzw. zu Testzwecken zur Verfügung steht. In der Einführungsphase bedarf es in Phase 4 die Akzeptanz von KI im Unternehmen, die beispielsweise mit Mitarbeiterschulungen die Entscheidungsfindung der KI-Anwendung näherbringt und Vertrauen schafft. In diesem Zusammenhang können Mitarbeiter ausgebildet werden, die unmittelbar mit der KI-Anwendung arbeiten. Schließlich sollten ausgiebige Tests vor der Einführung durchgeführt werden, um mögliche Funktionsfehler zu eliminieren. Mit definierten KPIs kann zudem die Modelleleistung gemessen werden. Der anschließende Einführungsprozess ist nicht Bestandteil dieser Konzeption, weswegen auf diesen Teil nicht weiter eingegangen wird. Resümierend stellt die Konzeption wichtige Handlungsfelder dar, mit denen die Einführung von KI realisiert werden kann. Aufgrund der Individualität, die beispielsweise vom technischen Fortschritt im Unternehmen oder dem Innovationsgrad der zukünftigen KI-Anwendung abhängig ist, stellen die Konzepte lediglich eine mögliche Verfahrensweise dar. Da ein starrer Leitfaden bei einer neuen und dynamischen Technologie als nicht zielführend erachtet wird, sollte eine Handlungsempfehlung ebenso dynamisch einsetzbar sein. Das Überspringen von Konzepten oder Ergreifen unternehmensspezifischer Angleichungen kann für die Umsetzung ebenfalls erforderlich sein und unterliegt einer individuellen Bewertung.

FAZIT

Mit der konzipierten Handlungsempfehlung können Unternehmen mehr Sicherheit bei der Planung und Umsetzung von KI-Projekten erlangen. Relevante Rahmenbedingungen konnten mithilfe der SLA den Handlungsbedarf bei KI-Projekten ermitteln. Mit den zusätzlich identifizierten Maßnahmen stellen sie zusammengefasst die Handlungsempfehlung dar. Diese ist dabei als allgemeine Orientierung zu betrachten und an die internen Gegebenheiten im Unternehmen und den Innovationsgrad des KI-Projektes anzupassen.

Als relevante Rahmenbedingungen wird die Definition des Budgetrahmens, eine klare Zieldefinition des AWF sowie die Verfügbarkeit von Fachpersonal mit umfassenden Methoden- und Anwendungswissen herauskristallisiert. Im PM-Team erfolgt die Planung des KI-Projektes, die unter Berücksichtigung der vorliegenden Voraussetzungen evaluiert wird. Dazu zählen die Eignung der IT-Infrastruktur und Hardware sowie die Ausführung von unternehmensspezifischen Optimierungen am Geschäftsprozess. Fehlendes Know-how muss durch Aus- und Weiterbildung interner Fachkräfte oder Einstellung externer Dienstleister kompensiert werden. Aus diesen Aspekten resultiert u. a. die Budgetplanung, deren sorgfältige Ausgestaltung aufbauend zum vorhandenen Budget

sorgfältig kalkuliert werden sollte und wesentlich zum Projekterfolg beiträgt.

In der Entwicklungsphase sollte ein geeignetes Vorgehensmodell (z. B. CRISP-DM) zur Strukturierung des Datenmanagements verwendet werden. Eine AWF-spezifische KI-Plattform kann dabei als Entwicklungsumgebung dienen. Zudem sollte ein Konzept zur Umsetzung des Datenschutzes und der Datensicherheit frühzeitig geplant werden. Dies gilt entsprechend für eine gute Bandbreite und Performance über eine 5G Breitbandverbindung bei potenzieller Echtzeitverarbeitung. Aus Gründen der Transparenz und Steigerung des Vertrauens in die KI-Anwendung, sollten Mitarbeiter in die Entscheidungsfindung und Funktionsweise mit einbezogen werden. Schließlich ist eine Bewertung zur Leistung der KI-Anwendung mit ausgewählten KPIs vorzunehmen, die zur Messung des Erfolges herangezogen werden. Im Idealfall weist das Ergebnis einen positiven Nettonutzen auf.

Die Handlungsempfehlungen zeigen die Anforderungen verschiedener Tätigkeitsbereiche auf, die bei der Einführung von KI entstehen. Eine KI-Implementierung lässt sich mit der strukturierten Vorgehensweise über die Handlungsempfehlung und unter Berücksichtigung der unternehmensspezifischen Gegebenheiten umsetzen.

Mit kleinen KI-Projekten wird schrittweise Klarheit und Know-how aufgebaut. Der umfangreiche Handlungsbedarf, der mit KI-Projekten einhergeht, ist nicht zu unterschätzen. Andererseits kann eine erfolgreich implementierte KI bedeutende Entwicklungschancen freisetzen. In den nächsten Jahren werden KI-Einführungen aufgrund des großen Potenzials voraussichtlich weiter voranschreiten. Die Vorteile von automatisierten und ressourcensparenden Prozessen können zum zukünftigen Erfolg und einer soliden Wettbewerbsfähigkeit beitragen.

LITERATUR

- Aichele, C. (2021): „Vorgehensweise zur Anwendung Digitaler Geschäftsprozesse auf Basis von Künstlicher Intelligenz“. In: Aichele, C. & Herrmann, J. [Hrsg.] (2021): *Betriebswirtschaftliche KI-Anwendungen*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 75–119.
- Alpaydin, E. (2022): *Maschinelles Lernen*. De Gruyter Oldenbourg, Berlin, Boston. DOI: 10.1515/9783110740196.
- Bolkart, J. (2022): *Statistiken zum Thema Künstliche Intelligenz*. Verfügbar unter: <https://de.statista.com/themen/3103/kuenstliche-intelligenz/?msclkid=bb26b736cf7611ec88069f361bfe263c#dossierKeyfigures>, [Letzter Zugriff: 11 Mai 2022].
- Brenner, W., van Giffen, B., Koehler, J., Fahse, T. & Sagodi, A. (2021): „Stand in Wissenschaft und Praxis“. In: Brenner, W., van Giffen, B., Koehler, J., Fahse, T. & Sagodi, A. [Hrsg.] (2021): *Bausteine eines Managements Künstlicher Intelligenz*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 17–23.
- Buxmann, P. & Schmidt, H. (2019): *Künstliche Intelligenz*, Berlin, Heidelberg, Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-57568-0.

- Cao, L. (2017): „Data science“. In: *Communications of the ACM*, Vol. 60, No. 8, S. 59–68. DOI: 10.1145/3015456.
- Deloitte Deutschland (2020): *KI-Studie 2020: Wie nutzen Unternehmen Künstliche Intelligenz?: KI-relevante Technologien, Strategien, Skills & Herausforderungen in der Praxis*. Verfügbar unter: <https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/ki-studie-2020.html>, [Letzter Zugriff: 11 Mai 2022].
- Diab, W. W., Ferraro, A., Klenz, B., Lin, S.-W., Liongosari, E., Tannous, W. E. & Zarkout, B. (2022): *Industrial IoT Artificial Intelligence Framework*. Verfügbar unter: <https://www.iiconsortium.org/pdf/Industrial-AI-Framework-Final-2022-02-21.pdf>, [Letzter Zugriff: 24 Juni 2022].
- Fayyad, U., Piatetsky-Shapiro, G. & Smyth, P. (1996): *Knowledge Discovery and Data Mining: Towards a Unifying Framework*. Verfügbar unter: <https://www.aaai.org/Papers/KDD/1996/KDD96-014.pdf>, [Letzter Zugriff: 17 Juli 2022].
- Fettke, P. (2006): „State-of-the-Art des State-of-the-Art“. In: *WIRTSCHAFTSINFORMATIK*, Vol. 48, No. 4. DOI: 10.1007/s11576-006-0057-3.
- Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (2018): *Maschinelles Lernen: Eine Analyse zu Kompetenzen, Forschung und Anwendung*. Verfügbar unter: https://www.bigdata-ai.fraunhofer.de/content/dam/bigdata/de/documents/Publikationen/Fraunhofer_Studie_ML_201809.pdf, [Letzter Zugriff: 31 Mai 2022].
- Gethmann, C. F., Buxmann, P., Distelrath, J., Humm, B. G., Lingner, S., Nitsch, V., Schmidt, J. C. & Spiecker genannt Döhmann, I. (2022): *Künstliche Intelligenz in der Forschung*, Berlin, Heidelberg, Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-63449-3.
- Haarmeier, M. (2021): „Künstliche Intelligenz für den Mittelstand“. In: Haarmeier, M. [Hrsg.] (2021): *Künstliche Intelligenz für den Mittelstand*, Wiesbaden, Springer Fachmedien Wiesbaden.
- Han, J., Kamber, M. & Pei, J. (2011): *Data mining: Concepts and techniques*, 3. Aufl., s.l., Elsevier professional. Verfügbar unter: <http://lib.myilibrary.com/detail.asp?id=317117>, [Letzter Zugriff: 20 Juli 2022].
- Herremans, D. (2021): „aiSTROM—A Roadmap for Developing a Successful AI Strategy“. In: *IEEE Access*, Vol. 9, S. 155826–155838. DOI: 10.1109/ACCESS.2021.3127548.
- Humm, B. G., Buxmann, P. & Schmidt, J. C. (2022): „Grundlagen und Anwendungen von KI“. In: Gethmann, C. F., Buxmann, P., Distelrath, J., Humm, B. G., Lingner, S., Nitsch, V., Schmidt, J. C. & Spiecker genannt Döhmann, I. [Hrsg.] (2022): *Künstliche Intelligenz in der Forschung*, Berlin, Heidelberg, Springer Berlin Heidelberg, S. 13–42.
- Keim, D. & Sattler, K.-U. (2020): *Von Daten zu KI: Intelligentes Datenmanagement als Basis für Data Science und den Einsatz Lernender Systeme*, München. Verfügbar unter: https://www.plattform-lernendesysteme.de/files/Downloads/Publikationen/AG1_Whitepaper_Von_Daten_zu_KI.pdf, [Letzter Zugriff: 27 Juni 2022].
- Kleesiek, J., Murray, J. M., Strack, C., Kaissis, G. & Braren, R. (2020): „Wie funktioniert maschinelles Lernen?“. In: *Der Radiologe*, Vol. 60, No. 1, S. 24–31. DOI: 10.1007/s00117-019-00616-x.
- Kotu, V. & Deshpande, B. (2019): „Introduction“ (2019): *Data Science*, Elsevier, S. 1–18.
- Luber, S. & Litzel, N. (2020): *Was ist Data Science?* Verfügbar unter: <https://www.bigdata-insider.de/was-ist-data-science-a-979153/>, [Letzter Zugriff: 29 Juli 2022].
- Matzka, S. (2021): „Daten vorbereiten und bereinigen“. In: Matzka, S. [Hrsg.] (2021): *Künstliche Intelligenz in den Ingenieurwissenschaften*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 59–97.
- Mockenhaupt, A. (2021): „Weitere Werkzeuge der Künstlichen Intelligenz“. In: Mockenhaupt, A. [Hrsg.] (2021): *Digitalisierung und Künstliche Intelligenz in der Produktion*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 199–215.
- Müller, A., Schröder, H. & Thienen, L. von (2021): „Künstliche Intelligenz: Roadmap zur Aufdeckung und Realisierung der KI-Potenziale in der Prozessdigitalisierung“. In: Müller, A., Schröder, H. & Thienen, L. von [Hrsg.] (2021): *Digineering*, Berlin, Heidelberg, Springer Berlin Heidelberg, S. 77–92.
- Murphy, K. P. (2012): *Machine learning - a probabilistic perspective: Adaptive computation and machine learning series*. The MIT Press. Verfügbar unter: <https://www.cs.ubc.ca/~murphyk/MLbook/pml-intro-22may12.pdf>, [Letzter Zugriff: 1 Juni 2022].
- Petry, S. (2021): „KI – von der Strategie zum Projekt“. In: Terstiege, M. [Hrsg.] (2021): *KI in Marketing & Sales – Erfolgsmodelle aus Forschung und Praxis*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 337–387.
- Pokorni, B., Braun, M. & Knecht, C. (2021): *Menschenzentrierte KI-Anwendungen in der Produktion: Praxiserfahrungen und Leitfaden zu betrieblichen Einführungsstrategien*. Verfügbar unter: <http://publica.fraunhofer.de/dokumente/N-6249564.html>, [Letzter Zugriff: 27 Juni 2022].
- Rainsberger, L. (2021): „Was tun: Handlungsempfehlungen für Vertriebsorganisationen“. In: Rainsberger, L. [Hrsg.] (2021): *KI – die neue Intelligenz im Vertrieb*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 119–148.
- Robert Bosch GmbH (o. J.): *Die Geschichte der Künstlichen Intelligenz: Von Turing bis Watson: Die Entwicklung der denkenden Systeme*. Verfügbar unter: <https://www.bosch.com/de/stories/geschichte-der-kuenstlichen-intelligenz/>, [Letzter Zugriff: 1 Juni 2022].
- Rode-Schubert, C. & Müller, P. (2020): „Welche Fähigkeiten benötigt ein Unternehmen um Künstliche Intelligenz nachhaltig erfolgreich einzusetzen?“. In: Pfanstiel, M. A. & Steinhoff, P. F.-J. [Hrsg.] (2020): *Transformationsvorhaben mit dem Enterprise*

- Transformation Cycle meistern*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 143–171.
- Sanchez-Puchol, F. & Pastor-Collado, J. A. (2017): „Focus Area Maturity Models: A Comparative Review“. In: Themistocleous, M. & Morabito, V. [Hrsg.] (2017): *Information Systems*, Cham, Springer International Publishing, S. 531–544.
- Shi, L. & Zhu, Q. (2022): „Association Rule Analysis of Influencing Factors of Literature Curriculum Interest Based on Data Mining“. In: *Computational intelligence and neuroscience*, Vol. 2022, S. 6866134. DOI: 10.1155/2022/6866134.
- Stowasser, S. (2021): „Erfolgreiche Einführung von KI im Unternehmen“. In: Knappertsbusch, I. & Gondlach, K. [Hrsg.] (2021): *Arbeitswelt und KI 2030*, Wiesbaden, Springer Fachmedien Wiesbaden, S. 145–153.
- Streim, A. & Uhl, M. (2020): *Unternehmen tun sich noch schwer mit Künstlicher Intelligenz*. Verfügbar unter: <https://www.bitkom.org/Presse/Presseinformation/Unternehmen-tun-sich-noch-schwer-mit-Kuenstlicher-Intelligenz>, [Letzter Zugriff: 11 Mai 2022].
- Suresh, H. & Guttag, J. (2021): „A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle“, *Equity and Access in Algorithms, Mechanisms, and Optimization*. -- NY USA, 05 10 2021 09 10 2021. New York, NY, USA, ACM, S. 1–9.
- TURING, A. M. (1950): „I.—COMPUTING MACHINERY AND INTELLIGENCE“. In: *Mind*, LIX, No. 236, S. 433–460. DOI: 10.1093/mind/LIX.236.433.
- van Giffen, B., Borth, D. & Brenner, W. (2020): „Management von Künstlicher Intelligenz in Unternehmen“. In: *HMD Praxis der Wirtschaftsinformatik*, Vol. 57, No. 1, S. 4–20. DOI: 10.1365/s40702-020-00584-0.
- VDMA - Verband Deutscher Maschinen- und Anlagenbau e.V. (2021): *Künstliche Intelligenz – Navigator durch die globale KI-Startup-Szene für den Maschinen- und Anlagenbau*. Verfügbar unter: <https://www.werkstatt-betrieb.de/a/news/erfolgsworter-kuenstliche-intelligenz-316466>, [Letzter Zugriff: 22 Juli 2022].
- vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R. & Cleven, A. (2009): *Reconstructing the giant: On the importance of rigour in documenting the literature search process*. Verfügbar unter: <https://aisel.aisnet.org/ecis2009/161>, [Letzter Zugriff: 29 Juli 2022].
- Weber, F. (2020): *Künstliche Intelligenz für Business Analytics: Algorithmen, Plattformen und Anwendungsszenarien*, Wiesbaden, Heidelberg, Springer Vieweg. DOI: 10.1007/978-3-658-29773-2.
- Webster, J. & Watson, R. T. (2002): *Analyzing the past to prepare for the future: writing a literature review*, MIS Quarterly Vol. 26 No. 2, pp. xiii–xxiii. Verfügbar unter: https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf, [Letzter Zugriff: 24 Mai 2022].
- Wittpahl, V. (2019): *Künstliche Intelligenz*, Berlin, Heidelberg, Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-58042-4.
- Wuttke, L. (2022): *Praxisleitfaden für Künstliche Intelligenz in Marketing und Vertrieb*, Wiesbaden, Springer Fachmedien Wiesbaden. DOI: 10.1007/978-3-658-35626-2.

Entwicklung eines KI-basierten FAQ-Chatbots für die Hochschule im Bereich Prüfungsangelegenheiten

Prof. Dr. Harald Ritz
Technische Hochschule Mittelhessen
Fachbereich MNI
Wiesenstraße 14
35390 Gießen
harald.ritz@mni.thm.de

Dogus Tansel (B.Sc.)
Technische Hochschule Mittelhessen
Fachbereich MND
Wilhelm-Leuschner-Straße 13
61169 Friedberg
dogus.tansel@mnd.thm.de

ABSTRACT

Es ist davon auszugehen, dass die Nutzung von Chatbots in den nächsten Jahren enorm ansteigen wird. Seit zum ersten Mal der KI-Chatbot „ChatGPT“ Ende 2022 vorgestellt wurde [1, p. 423], ist dieser Trend auch in der breiten Öffentlichkeit angekommen. Es wird erwartet, dass im Jahr 2027 der weltweite Chatbot-Markt einen Umsatz von 454,8 Millionen US-Dollar erzielen wird, gegenüber 40,9 Millionen US-Dollar im Jahr 2018 [2]. Als Hochschule, bei der das Leitbild auf das Bewältigen von Herausforderungen unter Verwendung neuester Erkenntnisse ausgerichtet ist [3], lag es nahe, zur Verbesserung der studentischen Beratungssituation, diesen Trend frühzeitig aufzugreifen.

Der vorliegende Artikel stellt das vom Prüfungsausschuss-Vorsitzenden der Wirtschaftsinformatik an der Technischen Hochschule Mittelhessen im Verlauf des Jahres 2021 initiierte Projekt vor, das die Entwicklung eines KI-basierten FAQ-Chatbots im Bereich Prüfungsangelegenheiten zum Ziel hat.

Der Chatbot wurde entworfen, um Studierende bei häufig gestellten Fragen (FAQs) im Zusammenhang mit Prüfungsangelegenheiten im Bereich Wirtschaftsinformatik zu unterstützen. Es ist vorgesehen, dass mit Hilfe von Machine-Learning-Algorithmen der KI-basierte Chatbot kontinuierlich dazulernt und seine Antwortgenauigkeit und -effektivität verbessert. Der Chatbot bietet den Studierenden eine einfache Möglichkeit, schnell und unkompliziert Antworten auf ihre Fragen zu erhalten und kann auch außerhalb der regulären Bürozeiten genutzt werden. Die Integration des Chatbots in die Website der Hochschule trägt dazu bei, die Effizienz der Studierendenberatung zu erhöhen und das Nutzererlebnis für die Studierenden zu verbessern.

SCHLÜSSELWÖRTER

Adam Optimizer, Angular, Chatbot, Deep Learning, Docker, FAQ-Bot, Flask-Framework, Unicorn, Hochschulberatung, Keycloak, Künstliche Intelligenz (KI), Machine Learning (ML), MongoDB, Natural Language Processing (NLP), Natural Language Toolkit (NLTK), Neuronale Netze, NGINX-Webserver, Python, PyTorch, Reinforcement Learning, REST-API, Sentence Similarity Model, spaCy, Transformers

I. AUSGANGSSITUATION

Studierende an einer Hochschule sind oft mit vielen Fragen und Unsicherheiten im Zusammenhang mit Prüfungsangelegenheiten konfrontiert. Dies kann zu einem hohen Beratungsbedarf führen, der Ressourcen und Zeit des ohnehin eingeschränkten Hochschulpersonals in Anspruch nimmt. Darüber hinaus können sich Studierende aufgrund von begrenzten Büro- und Wartezeiten frustriert und unzufrieden fühlen. Um diese Herausforderungen zu bewältigen, wird im Rahmen eines internen Hochschulprojektes an der Technischen Hochschule Mittelhessen (THM) ein KI-basierter FAQ-Chatbot entwickelt,

der den Studierenden eine schnelle und effektive Möglichkeit bietet, Antworten auf ihre Fragen zu erhalten und dadurch Unsicherheiten zu beseitigen. Der Chatbot soll die Effizienz der Studierendenberatung erhöhen und das Nutzererlebnis der Studierenden verbessern sowie optimieren.

II. VERWANDTE ARBEITEN

In der Forschung gibt es inzwischen vielfältige Arbeiten, die sich mit der Entwicklung von Chatbots und virtuellen Assistenten für die Hochschulberatung beschäftigen. Einige dieser Arbeiten haben sich auf die Verwendung von Natural Language Processing (NLP) und Machine-Learning (ML)-Algorithmen zur Verbesserung der Antwortgenauigkeit und -effektivität von Chatbots konzentriert [4]. Andere Arbeiten setzen ihren Schwerpunkt auf die Integration von Chatbots in bestehende Hochschul-Websites und -Plattformen, um eine nahtlose Benutzererfahrung für die Studierenden zu gewährleisten [5]. Insgesamt haben diese Arbeiten gezeigt, dass Chatbots ein großes Potenzial für die Verbesserung der Hochschulberatung und der Studierendenerfahrung haben, insbesondere in Bezug auf die Beantwortung häufig gestellter Fragen (FAQs) und die Entlastung des Hochschulpersonals.

III. ANFORDERUNGEN

Das Ziel des Hochschulprojektes „Winfy“ ist es, einen KI-basierten Chatbot und eine entsprechende administrative Verwaltungsplattform für den Bereich Prüfungsangelegenheiten für die gemeinsam von den Fachbereichen MND und MNI angebotenen Studiengänge B.Sc. und M.Sc. Wirtschaftsinformatik an der THM zu entwickeln. Die Umsetzung eines solchen Vorhabens erfordert eine sorgfältige Analyse der Anforderungen, die von den Stakeholdern des Systems gestellt werden. Um dieses Ziel zu erreichen, sind insbesondere folgende Anforderungen zu erfüllen [6] [7]:

Benutzerfreundlichkeit

Der Chatbot sollte unkompliziert zu bedienen sein und eine intuitive Benutzeroberfläche bieten. Die Benutzer sollten in der Lage sein, ihre Fragen schnell und einfach zu stellen und die Antworten auf ihre Fragen in kurzer Zeit zu erhalten.

Zuverlässigkeit

Der Chatbot sollte in der Lage sein, zuverlässige und genaue Antworten basierend auf den Fragen der Benutzer zu liefern. Dabei sind die gestellten Fragen effektiv und effizient zu verarbeiten und Antworten auf klare und verständliche Weise zu präsentieren.

Flexibilität

Der Chatbot sollte flexibel genug sein, um auf die verschiedenen Bedürfnisse der Benutzer eingehen zu können. Hierbei soll realisiert sein, auf eine Vielzahl von Fragen zu antworten und eine breite Palette von Themen abzudecken. Der Chatbot sollte auch in der Lage sein, sich an neue Situationen und Anforderungen anzupassen und schnell auf Veränderungen zu reagieren.

Sicherheit und Datenschutz

Aufgrund der Möglichkeit mit der Plattform im öffentlichen Netz zu interagieren, ist es wichtig sicherzustellen, dass die Daten auf den zugrundeliegenden Server sicher und geschützt sind. Daher sollten alle notwendigen Sicherheitsmaßnahmen implementiert werden, um zu gewährleisten, dass das System vor unbefugten Zugriff und Missbrauch geschützt ist.

Barrierefreiheit

Der Chatbot sollte barrierefrei und allen Benutzern zugänglich sein, unabhängig von ihrer Fähigkeit oder Behinderung. Es sollte in der Lage sein, die Fragen der Benutzer in einer Vielzahl von Formaten zu verarbeiten, einschließlich Sprache und Text, und die Antworten auf eine Weise zu präsentieren, die für alle Benutzer leicht verständlich ist.

Das Erfüllen dieser (geplanten) Anforderungen wird dazu beitragen, dass der Chatbot effektiv und nützlich für die Studierenden der Wirtschaftsinformatik ist und dazu

beiträgt, die Effizienz und Genauigkeit der Prüfungsverwaltung an der Hochschule zu verbessern.

IV. ENTWICKLUNG VERSION 1.0

Methodik

In einer ersten Entwicklungsstufe des Hochschul-Chatbots „Winfy“ wurde ein regelbasiertes System in Python implementiert, um die Fähigkeit zu verbessern, menschliche Sprache zu verstehen und auf Fragen ordnungsgemäß zu antworten [8].

Für die Entwicklung des FAQ-Bots wurden verschiedene Bibliotheken und Technologien verwendet. Zum einen wurde die Python-Bibliothek Transformers genutzt, die eine breite Palette von vortrainierten Modellen für NLP anbietet. Insbesondere wurde das „German Semantic“ (Sentence Similarity Model) [9] eingesetzt, das es dem Chatbot ermöglicht, Texte semantisch zu vergleichen. Des Weiteren wurde die Bibliothek spaCy [10] genutzt, die ebenfalls NLP-Technologien bereitstellt. Hierbei wurde das spaCy (Sentence Similarity Model) eingesetzt, um die Ähnlichkeit zwischen verschiedenen Eingabemessages und Antworten des Chatbots zu bestimmen.

Zur Datenhaltung wurde mit MongoDB eine NoSQL-Datenbank verwendet, die eine flexible und skalierbare Speicherung von Daten ermöglicht. Diese ist mit den häufig gestellten Fragen und Antworten ausgestattet, um dem System, als auch dem Benutzer, schnelle und präzise Antworten zur Verfügung zu stellen.

Um eine RESTful-Webanwendung zu ermöglichen, wurde eine REST-API mit Hilfe des Flask-Frameworks [11] in Python erstellt, das in der Lage ist, Nachrichten zu empfangen und zu senden. Das Flask-Framework ist ein beliebtes Python-Web-Framework, das für seine Einfachheit und Flexibilität bekannt ist. Durch die Implementierung des RESTful-Web Services ist der Chatbot in der Lage, mit anderen Anwendungen und Services zu kommunizieren. Mit Hilfe von HTTP-Anfragen kann der Chatbot Nachrichten von außerhalb empfangen und darauf antworten. Das RESTful-Design macht den Chatbot skalierbar, da er auf einfache Weise in andere Anwendungen integriert werden kann.

Zur Bereitstellung des Webservers wurde der NGINX-Webserver [12] in der Funktion eines Reverse Proxys eingesetzt, der die Anfragen an den Chatbot weiterleitet. Unicorn [13] wurde als Webserver Gateway Interface HTTP Server genutzt, um den Service bereitzustellen.

Für das Backend des Chatbots wurde das TypeScript-basierte Webapplikationsframework Angular [14] genutzt. Die Landingpage wurde mit einem HTML-Grundgerüst, einer JavaScript-Datei für die Funktionalitäten des Chatbots und einer CSS-Datei für das Styling der Oberfläche erstellt. Die Benutzeroberfläche des Chatbots wurde so gestaltet, dass sie einfach und intuitiv zu bedienen ist. Eine Kompatibilität mit verschiedenen Endgeräten wie

Mobiltelefon und Tablet wurde zunächst nicht realisiert. Zum Zeitpunkt des Starts der Entwicklung bestand der Fokus auf die Umsetzung einer Version für den Desktop-Computer (siehe Abbildung 1).



Abbildung 1: Landingpage - Startbildschirm

Zusätzlich zu den oben genannten Bibliotheken und Frameworks wird der Chatbot in einer Docker-Container-Umgebung betrieben. Hierfür wurden verschiedene Services, wie MongoDB, Keycloak, PostgreSQL und NGINX, als separate Container aufgebaut und über Docker Compose orchestriert. Dies erleichtert die Bereitstellung und Skalierung des Chatbots sowie die Integration in die vorhandene IT-Infrastruktur der Hochschule. Durch die Containerisierung können auch Abhängigkeiten zwischen den verschiedenen Komponenten des Chatbots einfach verwaltet werden. Weiterhin wird dadurch eine hohe Flexibilität in Bezug auf die Infrastruktur erreicht, da so der Chatbot problemlos auf verschiedenen Servern und Cloud-Plattformen betrieben werden könnte.

Funktionalitäten

Nach dem Aufruf der Webseite des Frontends wird der Anwender vom Chatbot in einer Dialogbox aufgefordert zu entscheiden, ob er Fragen bezüglich des Bachelor- oder Masterstudiums hat. Hierfür muss der Nutzer die entsprechende Fläche auf der Webseite anklicken. Erst nach dieser Selektion steht es dem Chatbot frei, Fragen des Nutzers zu beantworten. Diese Fragen können in Form eines üblichen Chat-DIALOGS gestellt werden (siehe Abbildung 2). Der Chatbot bietet dem Nutzer auch vordefinierte Fragen in Form einer Autovervollständigung an, die aufgrund der vorselektierten Studienrichtung ausgewählt werden können.

Aktuell ist im Produktivbetrieb das „German Semantic“-Sprachmodell eingestellt. Erreichbar für Studierende ist der FAQ-Chatbot „Winfy“ auf der Hochschulseite über die URL: <https://www.thm.de/mnd/studium/service/chatbot-wirtschaftsinformatik>.

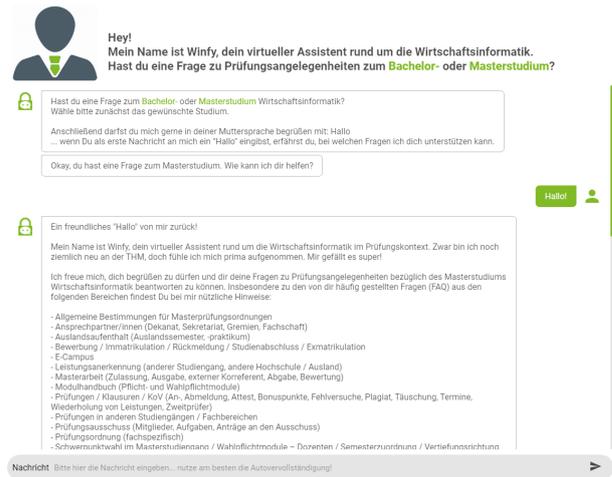


Abbildung 2: Landingpage - Dialogfenster

Beim Aufruf der Oberfläche erfolgt eine Anmeldung im REST-Service des Backends über das Authentifizierungs- und Autorisierungssystem Keycloak, das in den Docker-Containern des Backends integriert ist. Nach erfolgreicher Anmeldung werden notwendige Ressourcen, wie zum Beispiel die Antwort auf eine gestellte Frage, geladen. Über die in der JavaScript-Datei hinterlegten Methoden werden Inhalte an die entsprechenden TypeScript-Funktionen gesendet. Diese Funktionen rufen wiederum HTTP-Requests im Python-Code des Chatbots auf, um die notwendigen Ressourcen anzufordern. Dieser Prozess ermöglicht eine schnelle und effiziente Kommunikation zwischen dem Front- und Backend des Chatbots (siehe Abbildung 3).

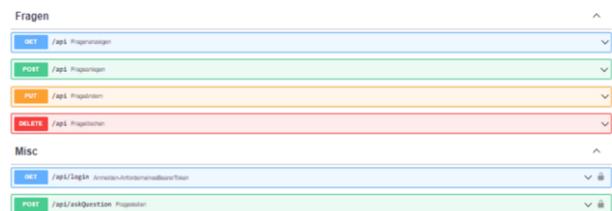


Abbildung 3: Auszug REST-Aufrufe

Das Backend ist für Administratoren und Verantwortliche zugänglich und bietet eine Weboberfläche zur Verwaltung des Chatbots und dessen Inhalte. Innerhalb des Backends haben berechtigte Benutzer die Möglichkeit, neue Inhalte wie Fragen und Antworten in die Umgebung einzuspielen, Sprachmodelle zu ändern oder auf neue FAQ-Inhalte zu trainieren, Benutzerkonten zu erstellen und Log-Dateien bzw. Chat-Protokolle zu analysieren sowie die errechneten Score-Werte für Anfragen einzusehen. Dies ermöglicht eine einfache Verwaltung des Chatbots und eine schnelle Anpassung an neue Anforderungen und Inhalte.

Auf der Startseite des Backends wird der Nutzer aufgefordert, seine Anmeldedaten einzugeben. Dabei handelt es sich um einen Benutzernamen und ein Passwort, die vordefiniert sind und innerhalb der Plattform geändert werden können. Nach der Eingabe und dem Bestätigen

mit dem Login-Button sendet die Webanwendung eine REST-Anfrage an den Host-Server. Der Host-Server prüft daraufhin, ob die Benutzerdaten gültig sind, und gleicht sie in einer separaten HTTP-Anfrage mit dem Keycloak-Authentifizierungsserver ab. Wenn der Benutzer vorhanden ist und die eingegebenen Daten mit dem Nutzerprofil übereinstimmen, wird der Benutzer erfolgreich angemeldet und erhält ein Session- bzw. Bearer-Token zugewiesen. Dieser Token ist für eine bestimmte Laufzeit innerhalb der Umgebung gültig und ermöglicht dem Benutzer den Zugriff auf die verschiedenen Funktionen des Backends.

Diese Funktionsbereiche, z.B. das Management des Chatbots mit Verwalten der Anfragen und Antworten, der Einstellungsbereich mit Auswahl der Sprachmodelle und Verwalten der Log-Einträge, das Dashboard zur Analyse der Ergebniswerte des Chatbot-Verhaltens und die Benutzerverwaltung, sind aus der Abbildung 4 ersichtlich.

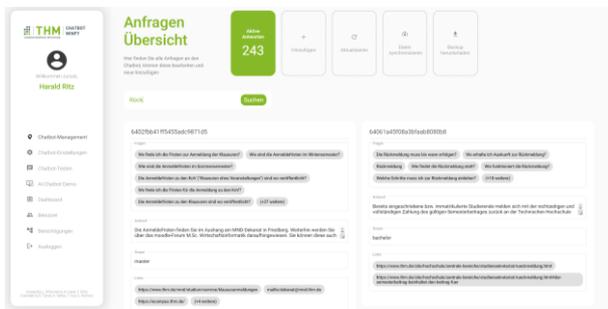


Abbildung 4: Backend-Oberfläche

V. THEORETISCHER RAHMEN

Um auf der Grundlage der entwickelten Plattform eine Erweiterung im Rahmen eines KI-Chatbots zu realisieren, wird in diesem Abschnitt zunächst auf den theoretischen Hintergrund und dann im darauffolgenden Kapitel auf die Implementierung eingegangen.

Die einfachste Form computergesteuerter Dialoge bilden regelbasierte Chatbots, die auch als Entscheidungsbaum-Chatbots bezeichnet werden. Diese Art der Chatbots lernen im Laufe der Zeit nicht dazu und arbeiten lediglich in den vordefinierten Szenarien, für die sie konzipiert wurden. In diese Kategorie ist die aktuell schon im Hochschulbetrieb befindliche Version 1.0 des FAQ-Chatbots „Winfy“ einzuordnen. Ein Beispiel für fortschrittlichere Chatbots sind Chatbots mit maschinellem Lernen, auch als Chatbots mit künstlicher Intelligenz (KI) bezeichnet. Sie ermöglichen den Benutzern, offene Fragen zu stellen und bieten die natürlichsten Antworten. Im Gegensatz zu einfachen regelbasierten Chatbots lernen sie aus Gesprächen und verbessern ihre Antworten im Laufe der Zeit [15].

Im Folgenden werden einige grundlegende Begriffe und Definitionen erläutert, die für das Verständnis von KI-Chatbots und deren Funktionsweise relevant sind.

Machine Learning

Machine Learning ist ein Teilbereich der künstlichen Intelligenz, bei dem Algorithmen entwickelt werden, die aus Daten lernen können. Es geht darum, automatisch Muster in Daten zu erkennen, um Vorhersagen treffen zu können. Dabei werden verschiedene Techniken wie Klassifikation, Regression, Clustering und Reinforcement Learning eingesetzt [16, pp. 1-14].

Deep Learning

Deep Learning ist ein Teilbereich des maschinellen Lernens, der sich mit künstlichen neuronalen Netzen beschäftigt. Hierbei werden mehrere Schichten von Neuronen hintereinandergeschaltet, um komplexe Funktionen zu approximieren. Durch das Lernen aus Daten können neuronale Netze komplexe Aufgaben wie Bild- oder Spracherkennung ausführen [17].

Neuronale Netze

Neuronale Netze sind ein Konzept aus der Neurobiologie, welches in der Informatik adaptiert wurde. Ein neuronales Netz ist eine Verbindung von Neuronen, die in Schichten organisiert sind und Signale durch das Netzwerk weitergeben. Ein Vorwärtsnetz ist eine spezielle Art von neuronalem Netzwerk, in dem die Signale nur in eine Richtung fließen, von der Eingangsschicht zur Ausgangsschicht [18].

Natural Language Toolkit

Natural Language Toolkit (NLTK) ist eine Open-Source-Bibliothek für die Sprachverarbeitung mit Python. NLTK bietet Funktionen wie Tokenisierung, Lemmatisierung und POS-Tagging, um Texte automatisch zu analysieren und zu verarbeiten [19]. Es ist eine wichtige Bibliothek für die Entwicklung von KI-Chatbots.

Lemmatisierung

Lemmatisierung ist ein Prozess der Textnormalisierung, bei dem die Grundform eines Wortes, das Lemma, ermittelt wird. Es ist eine wichtige Technik der Sprachverarbeitung, um verschiedene Formen eines Wortes in eine einheitliche Form zu bringen [19]. Durch Lemmatisierung können KI-Chatbots besser verstehen, was der Nutzer meint, da verschiedene Formen desselben Wortes als gleichwertig behandelt werden (siehe Abbildung 5).

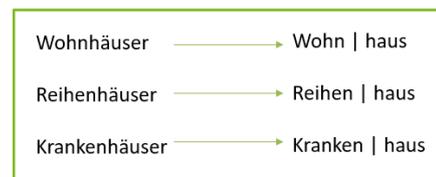


Abbildung 5: Lemmatisierung

Tokenisierung

Tokenisierung ist der Prozess der Aufteilung eines Textes in sinnvolle Einheiten, genannt Tokens. Ein Token

kann ein Wort, Satzzeichen oder eine Phrase sein. Durch die Tokenisierung kann ein Text automatisch analysiert werden, um Muster zu erkennen [19]. Dies ist eine essenzielle Technik für KI-Chatbots, um die Absichten des Nutzers zu verstehen.

Bag of Words

Bag of Words ist ein Konzept der Textklassifizierung, bei dem jeder Text als eine Sammlung von Wörtern betrachtet wird, ohne Berücksichtigung ihrer Reihenfolge oder Grammatik. Jedes Wort wird als Merkmal angesehen und ein Modell wird trainiert, um Texte auf Basis dieser Merkmale zu klassifizieren [20]. Bag of Words wird verwendet, um die Absichten des Nutzers zu verstehen und passende Antworten zu generieren.

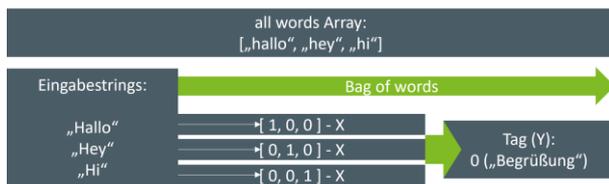


Abbildung 6: Bag of Words

In der Abbildung 6 wird Bag of Words eingesetzt, um jedes Muster aus den Tokens der gegebenen Strings als Vektor abzubilden, damit diese zum Training und Klassifizierung eines Modells genutzt werden können. Dabei bildet jedes Pattern eine Reihung mit der Größe des „all words“-Array, um zu überprüfen, ob die Tokens der Eingabe sich im „all words“-Array befinden, um diese einem Tag zuzuweisen und die Eingabe zu klassifizieren. Jeder Tag wird in einem Array mit einem Label versehen und erhält eine Nummer, die ebenfalls als Vektor agiert und das Y der Trainingsdaten darstellt.

VI. ENTWICKLUNG VERSION 2.0

Nachfolgend wird der Prozess beschrieben, wie der Chatbot mit Machine-Learning-Technologien weiterentwickelt wurde. Dazu werden die genutzten Technologien, die Architektur und die Implementierungsschritte erläutert [21].

Technologien

Der KI-Chatbot „Winfy“ in Version 2.0 wurde auf Basis von PyTorch entwickelt und verwendet gängige Verarbeitungsmethoden sowie Bibliotheken. PyTorch überzeugt als Open-Source-Bibliothek im Rahmen von Deep-Learning-Anwendungsfällen mit einer hohen Geschwindigkeit und enormer Flexibilität zur Entwicklung und Implementierung von künstlichen neuronalen Netzen. Während der Nutzung von PyTorch kann ohne Komplikationen auf etablierte Python-Bibliotheken wie NumPy, SciPy und Cython zugegriffen werden. Modelle werden mittels des Compilers und Torch-Skripten erstellt [22]. Ein zentrales Konzept ist der Aufbau eines neuronalen Netzes zur Vorhersage der Absicht des Benutzers und des Erstellens der Antwort des Chatbots.

Architektur

Die Architektur des KI-Chatbots (siehe Abbildung 7) besteht aus einem zentralen Knoten, dem Chatbot selbst, der durch PyTorch umgesetzt wurde. Das Modelltraining ist in zwei Bereiche unterteilt: das Trainingsdatenset und die Ergebnisse.

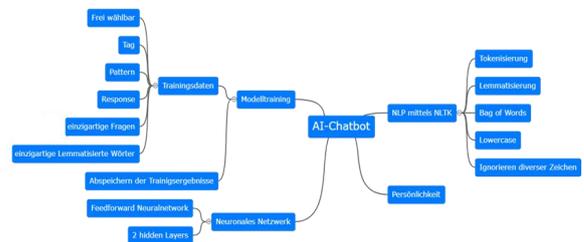


Abbildung 7: KI-Chatbot-Architektur

Das neuronale Netzwerk wird als Feedforward Neural Network mit zwei Hidden-Layern erstellt (siehe Abbildung 8), um die Verarbeitung von Informationen zu ermöglichen.

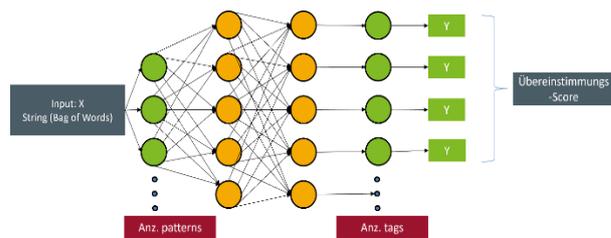


Abbildung 8: Feedforward-Netz

Zum Verstehen und Verarbeiten der menschlichen Sprache wird NLP und das NLTK eingesetzt. Um Textdaten in eine strukturierte Form umzuwandeln, werden die Methoden der Tokenisierung, Bag of Words und Lemmatisierung verwendet. Diese Technologien bilden die Grundlage für das Verarbeiten der Benutzeranfragen und das Erstellen von Antworten durch den Chatbot, um eine effektive Sprachverarbeitung zu gewährleisten.

Datensatz

Der Trainingsdatensatz basiert auf dem Inhalt der MongoDB. Diese Daten beziehen sich auf die Studiengänge Bachelor und Master Wirtschaftsinformatik der THM. Im Bereich Datensatz bildet eine FAQ-Liste der Hochschule die Grundlage für die Entwicklung des KI-Chatbots. Um diesen Datensatz in PyTorch verarbeiten zu können, wird er im Rahmen einer JSON-Datei strukturiert. Dabei wird ein "intents" als Fragenkatalog erstellt, der Fragen einer bestimmten Kategorie einem "tag" zuordnet. Innerhalb jedes "intents" werden "patterns" definiert, die mögliche Fragen darstellen, die von einem Nutzer gestellt werden könnten. Weiterhin werden "responses" definiert, die eine mögliche Antwort des Chatbots auf die jeweiligen Fragen inklusive relevante URLs beinhalten.

```

{
  "intents": [
    {
      "tag": "Anerkennung von Leistungen",
      "patterns": [
        "Kann ich Prüfungen aus einem anderen Studiengang anrechnen lassen?",
        "Ich benötige eine Auskunft zum Anrechnen von Leistungen",
        "Wie kann ich meine bereits bestandenen Prüfungen anrechnen lassen?",
        "...",
      ],
      "responses": [
        "Sie müssen zunächst selbst tätig werden und prüfen, was anerkennbar sein könnte. Welche Module ggf. anerkennbar sind, können Sie dem Modulhandbuch entnehmen, das Sie auf der WWW-Seite des Prüfungsausschusses Wirtschaftsinformatik finden. (...)"
      ]
    }
  ]
}

```

Modellaufbau

Der Modellaufbau des KI-Chatbots basiert, wie erwähnt, auf einem Feedforward-Neuronalen-Netzwerk, welches mit PyTorch erstellt wurde. Das Netzwerk besteht aus drei Schichten: Input-, Hidden- und Output-Layer. Der Input-Layer erhält die Eingabedaten und leitet diese an die Hidden-Layer weiter, welche die Daten verarbeiten und transformieren. Der Output-Layer gibt schließlich das Ergebnis aus. Die Anzahl der Hidden-Layer und die Größe der Neuronen in diesen Schichten wurden experimentell ermittelt und optimiert. Der Modellaufbau wird durch die verwendete Activation Function „ReLU“ unterstützt, der zur Beschleunigung des Trainings beiträgt.

```

class NeuralNet(nn.Module):
    def __init__(self, input_size, hidden_size, num_classes):
        super(NeuralNet, self).__init__()
        self.l1 = nn.Linear(input_size, hidden_size)
        self.l2 = nn.Linear(hidden_size, hidden_size)
        self.l3 = nn.Linear(hidden_size, num_classes)
        self.relu = nn.ReLU()

    def forward(self, x):
        out = self.l1(x)
        out = self.relu(out)
        out = self.l2(out)
        out = self.relu(out)
        out = self.l3(out)
        return out

```

Das neuronale Netzwerk des KI-Chatbots ist in der Lage, die Daten im Training zu verarbeiten und dadurch Muster zu erkennen, um die korrekten Antworten auf Benutzeranfragen zu generieren. Der Input-Layer besteht aus einer

Anzahl von Neuronen, die der Anzahl der Token entspricht, die als Eingabe erwartet werden. Der Output-Layer enthält so viele Neuronen, wie es Tags gibt, die von der FAQ-Liste abgedeckt werden. Jeder Knoten im Output-Layer entspricht einem Tag und ist mit einer ReLU-Aktivierungsfunktion verknüpft, die eine Wahrscheinlichkeitsverteilung über die möglichen Tags ausgibt.

Datenverarbeitung

In diesem Abschnitt wird die Datenverarbeitung für den Chatbot beschrieben. Hierbei wird die Eingabe der Fragen und Antworten in einzelne Wörter (Tokens) zerlegt und auf den Wortstamm zurückgeführt (Lemmatisierung). Dies dient dazu, Synonyme und verschiedene Formen eines Wortes als identisch zu behandeln, und somit die Trefferquote bei der Erkennung von Nutzeranfragen zu erhöhen. Anschließend werden diese Wörter in eine Bag-of-Words-Repräsentation umgewandelt, die angibt, welche Wörter in der Eingabe vorhanden sind und welche nicht. Dies ermöglicht es dem Chatbot, die Intention des Nutzers zu erkennen und die passende Antwort darauf zu generieren.

```

def tokenize(sentence):
    return nltk.word_tokenize(sentence)

def lem(word):
    return lemmatizer.lemmatize(word.lower())

def bag_of_words(tokenized_sentence, words):
    sentence_words = [lemmatizer.lemmatize(word.lower()) for word in tokenized_sentence]

    bag = np.zeros(len(words), dtype=np.float32)
    for idx, w in enumerate(words):
        if w in sentence_words:
            bag[idx] = 1
    return bag

```

Modelltraining

Das Trainieren des Modells beginnt mit dem Erstellen der Trainingsdaten. Hierzu werden die Sätze aus der intents.json-Datei durchlaufen und jedes einzelne Wort wird in einem Array gespeichert. Die Tokens werden lemmatisiert und in Kleinbuchstaben umgewandelt, um Duplikate entfernen und eine Sortierung durchführen zu können. Anschließend werden die Trainingsdaten erstellt, indem jedes Muster in eine Bag-of-Words-Repräsentation umgewandelt wird, die es dem Modell ermöglicht, die Ähnlichkeit zwischen verschiedenen Mustern zu berechnen.

Die Trainingsdaten werden dann in eine PyTorch-Dataset-Klasse verpackt, um sie in einem DataLoader zu laden und den Trainingsprozess zu beschleunigen. Anschließend wird das Modell definiert, das aus Input-, Hid-

den- und Output-Layer besteht. Es wird ein Cross-Entropy-Loss als Verlustfunktion und Adam als Optimizer verwendet. Mit Blick auf die Hyperparameter wurde eine Trainingsdauer von 1000 Epochen mit einer Lernrate von 0.001 festgelegt.

Das Modell wird auf der GPU oder CPU trainiert, je nachdem, was verfügbar ist. Der Trainingsprozess wird für die festgelegte Anzahl von Epochen durchlaufen. In jeder Epoche werden die Daten in Batches von bestimmter Größe geladen und für jedes Batch die Vorhersage, der Verlust und die Gradienten berechnet. Nachdem die Gradienten berechnet wurden, werden sie zurückpropagiert, um die Gewichte des Modells zu aktualisieren. Wenn die Anzahl an angegebenen Epochen durchlaufen ist, wird das Modell gespeichert. Nach der erfolgreichen Anbindung an das Frontend steht dem Nutzer eine neue Version des erweiterten KI-Chatbots zur Verfügung.

VII. ERGEBNISSE

Innerhalb des Projektes wurde zunächst mit „Winfy v1.0“ ein regelbasierter FAQ-Chatbot konzipiert und implementiert. Dieser kann verschiedene vortrainierten NLP-Modellen nutzen und liefert mit dem eingestellten „German Semantic“-Modell sehr gute Ergebnisse, wie die ersten Erfahrungen und eingegangenen Rückmeldungen der studentischen Nutzer seit der Freischaltung zum Sommersemester 2023 im Hochschulalltag zeigen.

Anschließend wurde mit der Version 2.0 von „Winfy“ ein KI-Chatbot mithilfe von Deep Learning erstellt. Der Chatbot ist in der Lage, Texteingaben zu interpretieren und passende Antworten zu generieren. Dazu wurden die Python-Bibliotheken PyTorch und NLTK verwendet. Die Daten für das Training des Modells wurden aus einer JSON-Datei gelesen. Nach der Vorverarbeitung der Daten wurden sie in Trainings- und Testdaten aufgeteilt und in Form von Batches an das Modell übergeben.

Es kann im Prototyp festgestellt werden, dass „Winfy v2.0“ vielversprechende Antworten liefert und mit einer Vielzahl von Nutzeranfragen umgehen kann. Natürlich gibt es noch Verbesserungsmöglichkeiten, insbesondere in Bezug auf die Handhabung von unerwarteten oder unbekanntem Nutzereingaben. Ein Beispiel dafür bildet das Verarbeiten von Buchstabendreher beim Versenden der Anfrage an den Chatbot. Um diese Probleme anzugehen, könnte der Chatbot mit erweiterten Funktionen zur Textnormalisierung ausgestattet werden. Dies würde sicherstellen, dass Buchstabendreher automatisch korrigiert werden.

Auf unbekanntem Nutzereingaben reagiert der Chatbot derzeit abweisend, da diese nicht in seinem Trainingsdatensatz enthalten sind. Ist die Eingabe der Plattform nicht bekannt, verweist diese auf das Umformulieren der Frage oder unzutreffenden Antworten. Dies könnte der Chatbot durch die Implementierung einer Intent-Erkennung verbessern, die es dem System ermöglicht, unbekanntem Anfragen zu erkennen und angemessen zu reagieren. Dies

könnte durch die Integration eines Fallback-Mechanismus oder einer Fehlerbehandlungsfunktion erreicht werden.

Ein weiteres Problem bildet die Misskommunikation mit dem System ab. Der Chatbot hat Schwierigkeiten, Anfragen zu interpretieren, die mehrdeutig oder missverständlich sind. Dies führt zu ungenauen oder fehlerhaften Antworten, da der Chatbot möglicherweise nicht die Absicht des Benutzers erkennt oder falsche Annahmen trifft.

Aufgrund der Datenbasis und der jungen Implementierung der KI-Variante hat der Chatbot Schwierigkeiten, Sarkasmus oder Ironie in den Nutzereingaben zu erkennen und angemessen darauf zu reagieren. Diese Formen der sprachlichen Nuancierung verwirren den Chatbot und führen zu unangemessenen oder unpassenden Antworten.

Derzeit bietet der Chatbot keine Fähigkeiten der kontextbezogenen Konversation an, um darauf basierend angemessene Antworten an den Nutzer zurückzugeben. Dies schränkt die Möglichkeiten der Antwortgenerierung erheblich ein, da sich dadurch Ausgaben nur auf die letzte Anfrage beziehen. Angemessener wäre es, dass sich das System auf den Kontext früherer Fragen oder Aussagen bezieht, die der Chatbot möglicherweise nicht ausreichend berücksichtigt oder erfasst hat.

Letztlich *fühlt* sich der Chatbot mit Fachsprache oder Jargon konfrontiert. Hierbei weist er Schwierigkeiten in dem Verständnis nicht-trainierter Fachsprache auf. Dies kann zu Verwirrung oder fehlerhaften Antworten führen, da die Datenbasis bzw. der Chatbot nicht über das erforderliche Wissen in spezifischen Domänen verfügt.

Das Training von Chatbots basierend auf neuronalen Netzen erfordert eine solide und umfangreiche Datengrundlage, um genaue Ergebnisse zu erzielen. Je größer die Datenmenge ist, desto besser kann das Modell Muster und Zusammenhänge erkennen und somit präzise Vorhersagen treffen.

Wichtig ist zu betonen, dass Chatbots im Laufe der Zeit und mit der kontinuierlichen Erweiterung der Datengrundlage besser werden können. Durch das ständige Training und die Verarbeitung von Benutzerinteraktionen kann das Modell seine Fähigkeit zur Beantwortung von Fragen und zur Erbringung von Dienstleistungen verbessern. Daher ist es sinnvoll, die Datenbank des Chatbots für eine bessere Leistung kontinuierlich zu erweitern und das Modell regelmäßig zu trainieren.

Das Aufnehmen von Informationen für eine mögliche Erweiterung der Datenbank mit neuem und verwertbarem Inhalt für das Training des Modells kann wie folgt aussehen:

Der Chatbot kann so konzipiert werden, dass er Interaktionen und Feedback von Benutzern erfasst. Durch die

Analyse dieser Interaktionen können neue Fragen, Muster oder Themen identifiziert werden, die der Chatbot bisher nicht abdeckt. Diese neuen Informationen können genutzt werden, um die Datenbank des Chatbots zu erweitern und ihn auf häufig auftretende Nutzeranfragen besser vorzubereiten. Dies kann in Form von Active Learning stattfinden. Mit der Implementierung von Active Learning kann gezielt nach Rückmeldungen von Benutzern gefragt werden, um sein Verständnis und seine Antworten zu verbessern. Durch die Integration von Mechanismen des aktiven Lernens kann der Chatbot seine Fähigkeiten kontinuierlich weiterentwickeln und sich an die spezifischen Bedürfnisse der Benutzer anpassen.

Durch die Analyse von Chatprotokollen und statistischen Auswertungen der Nutzerinteraktionen können Muster, häufig gestellte Fragen oder Problembereiche identifiziert werden. Diese Erkenntnisse können genutzt werden, um die Datenbank des Chatbots gezielt zu erweitern und das Training zu verbessern, um genau auf die Bedürfnisse der Benutzer einzugehen.

Die Integration von Multimodalität ermöglicht dem Chatbot die Verarbeitung und Interpretation von mehreren Modalitäten wie Text, Bildern, Sprache oder Videos. Durch die Einbeziehung zusätzlicher Modalitäten kann der Chatbot ein tieferes Verständnis der Nutzeranfrage erlangen und präzisere Antworten liefern.

Das Lernverhalten der Chatbot-Komponente ist abhängig von der eingesetzten Technologie und den verwendeten Lernalgorithmen. Im Allgemeinen wird der Chatbot durch das maschinelle Lernen trainiert, um aus den vorhandenen Daten zu lernen und seine Antworten entsprechend anzupassen. Mit einem Blick auf die Laufzeit des Trainingsprozesses kann festgehalten werden, dass sich die Ergebnisse in Abhängigkeit des Modellaufbaus variieren. In der Regel erfordert das Training eines Sprachmodells wie German Semantic eine beträchtliche Rechenleistung und kann mehrere Stunden oder sogar Tage und in unserem Konstrukt über eine Viertelstunde in Anspruch nehmen.

Ähnlich handhabt es das spaCy-Modell, welches ebenfalls hohe Rechenleistung erfordert und je nach Umfang des Trainingsdatensatzes und der spezifischen Konfiguration des Modells variiert.

Die Laufzeit des Trainingsprozesses für die KI-Version des Chatbots hängt von der Architektur des neuronalen Netzwerks, wie bei den anderen Modellen von der Größe des Trainingsdatensatzes und den verwendeten Trainingsstrategien ab. Das Training des KI-Modells kann dadurch in unserem Konstrukt bis zu 20-30 Minuten in Anspruch nehmen, insbesondere wenn große Datensätze und komplexe Modelle verwendet werden. Das Antwortzeitverhalten der KI-Version hängt von der Größe und Komplexität des Modells sowie von der Rechenleistung des Systems ab. Dieses erweist sich jedoch verlässlich

und bringt mit einer geringen Latenz die Antwort an die Oberfläche des Chatbots.

Um das Lernverhalten des Modells positiv zu beeinflussen, können nachfolgende Maßnahmen ergriffen werden:

- Qualität des Trainingsdatensatzes: Ein qualitativ hochwertiger und vielfältiger Trainingsdatensatz ist entscheidend, um eine gute Lerngrundlage für den Chatbot zu schaffen.

- Kontinuierliche Aktualisierung der Datenbank: Durch regelmäßige Updates und Erweiterungen der Datenbank kann der Chatbot kontinuierlich neue Informationen und Muster aufnehmen.

- Berücksichtigung von Benutzerfeedback: Rückmeldungen und Bewertungen von Benutzern sind wertvolle Informationen, um das Lernverhalten des Chatbots zu verbessern.

- Anpassung der Modellarchitektur: Die Wahl der richtigen Modellarchitektur kann einen großen Einfluss auf das Lernverhalten haben. Es kann erforderlich sein, verschiedene Architekturen auszuprobieren und zu vergleichen, um diejenige zu finden, die am besten zu den Anforderungen des Chatbots passen.

- Erweiterte NLP-Techniken: Durch die Integration fortgeschrittenerer NLP-Techniken wie Named Entity Recognition (NER), Sentiment-Analysen oder Kontextverständnis kann der Chatbot ein tieferes Verständnis der Benutzeranfragen entwickeln und präzisere Antworten liefern.

Im Rahmen der Anfragenverwertung haben das German Semantic und spaCy-Modell ähnliche Verhaltensmuster. Ihnen fällt es leicht Fragen zu beantworten, die eine große Ähnlichkeit zum Trainingsdatensatz aufweisen. Das Beantworten von verschachtelten Fragen fällt wiederum dem KI-Modell einfacher. Eine Herausforderung, welche sich alle Modelle teilen, liegt in der Beantwortung von größeren und dadurch komplexeren Anfragen. Hierbei kann sich die Antwortzeit auf mehrere Sekunden erhöhen. Zusammenfassend kann gesagt werden, dass alle Modelle ähnliche Antwort-Zeit-Verhalten nachweisen.

VIII. FAZIT UND AUSBLICK

Zusammenfassend lässt sich sagen, dass das Modellkonzept hinter dem Chatbot „Winfy“ vielversprechend ist. Die Verwendung von noch mehr Daten und ein regelmäßiges Training werden dazu beitragen, dass der Chatbot noch präzisere und vollständigere Antworten liefert. Insgesamt ist dieses Hochschulprojekt jedoch ein gutes Beispiel dafür, wie Deep Learning verwendet werden kann, um ein nützliches Software-Werkzeug für den täglichen Gebrauch zu erstellen.

Ein vielversprechender Ansatz zur Verbesserung der Leistung des Chatbots wäre, ihn durch die Integration von Reinforcement Learning dazu zu befähigen, im Laufe der Interaktion mit Benutzern kontinuierlich zu lernen und seine Leistung zu verbessern (Session-Konzept). Dabei soll der Nutzer auf gegebene Antworten eine Bewertung geben, die im Nachhinein vom Administrator oder dem Chatbot selbst ausgewertet werden und dadurch die Usability und Performance verbessern [23]. Eine Herausforderung, der sich dabei besonders zu widmen sein wird, ist, dass der KI-Bot von Nutzern zu einem falschen Antwortverhalten verleitet werden könnte.

Darüber hinaus könnten neue Funktionen, wie die Integration von Sprach- oder Bilderkennung, entwickelt werden, um dem Chatbot ein noch breiteres Anwendungsspektrum zu ermöglichen. Hierbei sind Sprachverarbeitungstechnologien (Speech-to-Text) zu erforschen, um dem Nutzer die Möglichkeit zu geben, mit dem Chatbot mündlich zu interagieren, anstatt nur textbasiert zu kommunizieren [24].

Eine andere Möglichkeit wäre die Verwendung von fortgeschrittenen Deep-Learning-Techniken wie beispielsweise Transformer-Netzwerken, die in der Lage sind, lange und komplexe Sätze besser zu verstehen und zu interpretieren. Die Einbettung neuer Sprachmodelle wie GPT-4 oder BERT können dazu beitragen, dass Konversationen noch natürlicher und menschenähnlicher wirken. GPT-4 findet bereits innerhalb von ChatGPT sowie in der Suchmaschine Bing in der Text- und Bilderkennung Anwendung [25].

Ein weiterer interessanter Forschungsbereich ist die Integration von KI-gestützten Emotionserkennungs-Tools, um den Chatbot in der Lage zu versetzen, Emotionen des Nutzers zu erkennen und dementsprechend zu reagieren. Dies könnte dazu beitragen, dass der Chatbot auf eine noch persönlichere Art und Weise mit dem Nutzer kommunizieren kann [26].

Insgesamt gibt es eine große Anzahl von Möglichkeiten zur Weiterentwicklung des KI-basierten Chatbots, sowohl in Bezug auf die Datenbank, die verwendeten Technologien als auch die Funktionen des Chatbots selbst. Aktuell wird u.a. eine plattformunabhängige Frontend-Anwendung zur Nutzung von „Winfy“ auf verschiedenen Endgeräten implementiert.

LITERATUR

- [1] H. Else, „Abstracts written by ChatGPT fool scientists,“ *Nature*, 12 Januar 2023. [Online]. <https://www.nature.com/articles/d41586-023-00056-7>. [Zugriff: 06 Mai 2023].
- [2] B. Thormundsson, „Chatbot market revenue worldwide from 2018 to 2027,“ *The Insight Partners*, April 2019. [Online]. <https://www.statista.com/statistics/1007392/worldwide-chatbot-market-size/>. [Zugriff: 06 Mai 2023].
- [3] Technische Hochschule Mittelhessen, „Leitbild der TH Mittelhessen (THM),“ o.D. [Online]. <https://www.thm.de/site/hochschule/profil/leitbild-2019.html>. [Zugriff: 06 Mai 2023].
- [4] S. B. Sonawane, A. S. Badwar, R. H. Dalvi, G. N. More und S. Talekar, „Design of Chatbot System for Student,“ *International Journal of New Innovations in Engineering and Technology*, p. 6, 2020.
- [5] L. H. Su, T. Dang-Huy, T. Thi-Yen-Linh, N. Thi-Duyen-Ngoc, L. Bao-Tuyen und N. Ha-Phuong-Truc, „Development of an AI Chatbot to Support Admissions and Career Guidance for Universities,“ *International Journal of Emerging Multidisciplinary Research*, Nr. 4, p. 9, 2020.
- [6] A. Dietrich, „Chatbots – Wie müssen sie gestaltet sein, um den Anforderungen zu genügen?,“ Hochschule Luzern, 29. April 2019. [Online]. <https://hub.hs-luzern.ch/retailbanking/chatbots-wie-muessen-sie-gestaltet-sein-um-den-anforderungen-zu-genuegen/>. [Zugriff: 30 April 2023].
- [7] Y. Altmann, „8 Funktionen, die jeder Chatbot haben sollte,“ Userlike UG, 21 Januar 2021. [Online]. <https://www.userlike.com/de/blog/chatbot-funktionen>. [Zugriff: 26 April 2023].
- [8] N. Inerle, T. Ochs und L. Offermanns, „Entwicklung eines FAQ-Chatbots zur Beratung im Hochschulbereich,“ Abschlussdokumentation des Master-Entwicklungsprojekts Wirtschaftsinformatik WS21/22 (intern), THM, Friedberg, März 2022.
- [9] S. Tomar, „Sahajtomar/German-semantic,“ hugging face, o.D. [Online]. <https://huggingface.co/Sahajtomar/German-semantic>. [Zugriff: 30 April 2023].
- [10] ExplosionAI GmbH, „Industrial-Strength Natural Language Processing,“ ExplosionAI GmbH, o.D. [Online]. <https://spacy.io/>. [Zugriff: 27 April 2023].
- [11] Pallets, „Flask,“ palletsprojects, o.D. [Online]. <https://flask.palletsprojects.com/en/2.3.x/>. [Zugriff: 27 April 2023].
- [12] I. Sysoev, „NGINX,“ F5 Inc., o.D. [Online]. <https://www.nginx.com/>. [Zugriff: 30 April 2023].
- [13] B. Chesneau, „Gunicorn,“ o.D. [Online]. <https://gunicorn.org/>. [Zugriff: 30 April 2023].
- [14] Google LLC, „Angular,“ Google LLC, o.D. [Online]. <https://angular.io/>. [Zugriff: 27 April 2023].
- [15] I. W. Advertising, „The ultimate guide to machine-learning chatbots and conversational AI,“ 28 September 2022. [Online]. <https://www.ibm.com/watson-advertising/thought-leadership/machine-learning-chatbot>. [Zugriff: 28 April 2023].
- [16] E. Alpaydm, *Introduction to Machine Learning*, Cambridge, Massachusetts: The MIT Press, 2004.
- [17] S. Bhattacharyya, V. Snasel, A. E. Hassanien, S. Saha und B. K. Tripathy, *Deep Learning: Research and Applications*, Berlin: De Gruyter, 2020.

- [18] L. Wuttke, „Künstliche Neuronale Netzwerke: Definition, Einführung, Arten und Funktion,“ datasolut GmbH, o.D. [Online]. <https://datasolut.com/neuronale-netzwerke-einfuehrung/>. [Zugriff: 30 April 2023].
- [19] S. Bird, E. Klein und E. Loper, *Natural Language Processing with Python*, Sebastopol, Kalifornien: O'Reilly Media, 2009.
- [20] J. Brownlee, „A Gentle Introduction to the Bag-of-Words Model,“ *Machine Learning Mastery*, 09 Oktober 2017. [Online]. <https://machinelearningmastery.com/gentle-introduction-bag-words-model/>. [Zugriff: 29 April 2023].
- [21] T.-A. Hua, S. Kirchner, S. Sahba und D. Tansel, „KI-basierter FAQ-Chatbot für eine Hochschule im Bereich Prüfungsangelegenheiten,“ Abschlussdokumentation des Master-Entwicklungsprojekts Wirtschaftsinformatik SoSe22 (intern), THM, Friedberg, Oktober 2022.
- [22] Simplilearn, „What is PyTorch, and How Does It Work: All You Need to Know,“ simplilearn, 31 März 2023. [Online]. <https://www.simplilearn.com/what-is-pytorch-article>. [Zugriff: 30 April 2023].
- [23] D. Biswas, „Self-improving Chatbots based on Deep Reinforcement Learning,“ *towardsdatascience*, 14 September 2020. [Online]. <https://towardsdatascience.com/self-improving-chatbots-based-on-reinforcement-learning-75cca62debce>. [Zugriff: 02 Mai 2023].
- [24] A. Singh, P. Murugeswari, S. D. P. Ragavendiran, A. Kaur, G. Singh und S. Margabandu, „AI-based Chatbot for Physically Challenged People,“ in *International Conference on Edge Computing and Applications (ICECAA)*, Tamilnadu, India, 2022.
- [25] R. Spitko, „Was ist GPT-4? – Fähigkeiten, Limitierungen, Grenzen, Einstazmöglichkeiten, Kosten, Nutzen, API und vieles mehr,“ *onlinemarketing-mastermind*, 16 März 2023. [Online]. <https://onlinemarketing-mastermind.de/ki/gpt-4/>. [Zugriff: 03 Mai 2023].
- [26] M. Karna, D. S. Juliet und R. Joy, „Deep learning based Text Emotion Recognition for Chatbot applications,“ in *4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184)*, Tirunelveli, India, 2020.

Anhang

THM | CHATBOT WINFY
TECHNISCHE HOCHSCHULE MITTELHESSEN

Herzlich willkommen!

Ich bin Winfy, der Chatbot der Prüfungsausschüsse B.Sc. u. M.Sc. Wirtschaftsinformatik der beiden gemeinsamen MND/MNH-Studiengänge an der Technischen Hochschule Mittelhessen.
Über ein Feedback freue ich mich!

Impressum:
Vorsitzender Prüfungsausschuss Wirtschaftsinformatik (B.Sc. & M.Sc.)
Prof. Dr. Harald Riz
@pa_wk@mnd.thm.de
☎ +49/6031/604-7620
📍 Technische Hochschule Mittelhessen
Campus Friedberg
Fachbereich MND
Wilhelm-Leuschner-Str. 13
D-61169 Friedberg
Büro 82.0.02

Prüfungsausschuss WK **Fachbereich MND**
THM ZPA **Feedback**

Disclaimer: Alle Angaben ohne Gewähr
Für die Inhalte und Richtigkeit der Informationen ist stets der jeweilige Informationsanbieter der verlinkten Webseite verantwortlich. Zum Zeitpunkt der Verlinkung waren keine Rechtsverstöße erkennbar. Zugleich wird darauf hingewiesen, dass aktuelle und verbindliche Auskünfte lediglich dem Webauftritt des Zentralen Prüfungssamts der THM zu entnehmen sind.
Bitte nutze hierzu den Button 'THM ZPA'.

Hey!
Mein Name ist Winfy, dein virtueller Assistent rund um die Wirtschaftsinformatik.
Hast du eine Frage zu Prüfungsangelegenheiten zum **Bachelor-** oder **Masterstudium**?

Hast du eine Frage zum **Bachelor-** oder **Masterstudium** Wirtschaftsinformatik?
Wähle bitte zunächst das gewünschte Studium.

Anschließend darfst du mich gerne in deiner Muttersprache begrüßen mit: Hallo
... wenn Du als erste Nachricht an mich ein "Hallo" eingibst, erfährst du, bei welchen Fragen ich dich unterstützen kann.

Nachricht Bitte hier die Nachricht eingeben... nutze am besten die Autovervollständigung!

Abbildung 1: Landingpage – Startbildschirm

Hey!
Mein Name ist Winfy, dein virtueller Assistent rund um die Wirtschaftsinformatik.
Hast du eine Frage zu Prüfungsangelegenheiten zum **Bachelor-** oder **Masterstudium**?

Hast du eine Frage zum **Bachelor-** oder **Masterstudium** Wirtschaftsinformatik?
Wähle bitte zunächst das gewünschte Studium.

Anschließend darfst du mich gerne in deiner Muttersprache begrüßen mit: Hallo
... wenn Du als erste Nachricht an mich ein "Hallo" eingibst, erfährst du, bei welchen Fragen ich dich unterstützen kann.

Okay, du hast eine Frage zum Masterstudium. Wie kann ich dir helfen?

Hallo!

Ein freundliches "Hallo" von mir zurück!

Mein Name ist Winfy, dein virtueller Assistent rund um die Wirtschaftsinformatik im Prüfungskontext. Zwar bin ich noch ziemlich neu an der THM, doch fühle ich mich prima aufgenommen. Mir gefällt es super!

Ich freue mich, dich begrüßen zu dürfen und dir deine Fragen zu Prüfungsangelegenheiten bezüglich des Masterstudiums Wirtschaftsinformatik beantworten zu können. Insbesondere zu den von dir häufig gestellten Fragen (FAQ) aus den folgenden Bereichen findest Du bei mir nützliche Hinweise:

- Allgemeine Bestimmungen für Masterprüfungsordnungen
- Ansprechpartner/innen (Dekanat, Sekretariat, Gremien, Fachschaft)
- Auslandsaufenthalt (Auslandssemester, -praktikum)
- Bewerbung / Immatrikulation / Rückmeldung / Studienabschluss / Exmatrikulation
- E-Campus
- Leistungsanerkennung (anderer Studiengang, andere Hochschule / Ausland)
- Masterarbeit (Zulassung, Ausgabe, externer Korreferent, Abgabe, Bewertung)
- Modulhandbuch (Pflicht- und Wahlpflichtmodule)
- Prüfungen / Klausuren / KoV (An-, Abmeldung, Attest, Bonuspunkte, Fehlversuche, Plagiat, Täuschung, Termine, Wiederholung von Leistungen, Zweitprüfer)
- Prüfungen in anderen Studiengängen / Fachbereichen
- Prüfungsausschuss (Mitglieder, Aufgaben, Anträge an den Ausschuss)
- Prüfungsordnung (fachspezifisch)
- Schwerpunktwahl im Masterstudiengang / Wahlpflichtmodule – Dozenten / Semesterzuordnung / Vertiefungsrichtung

Nachricht Bitte hier die Nachricht eingeben... nutze am besten die Autovervollständigung!

Abbildung 2: Landingpage – Dialogfenster

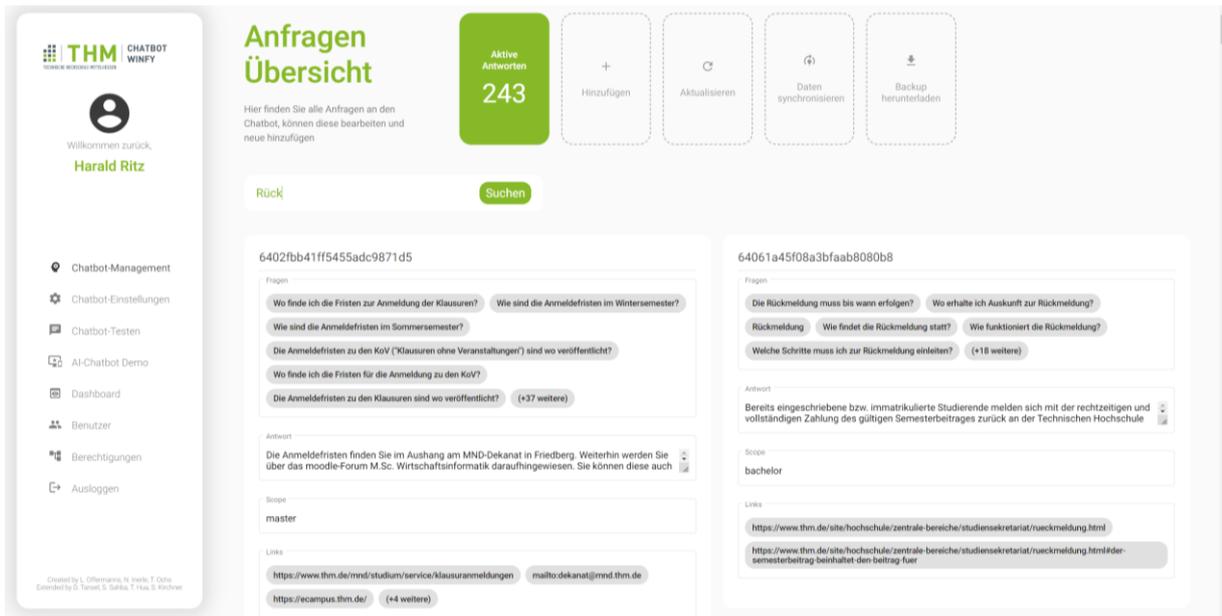


Abbildung 4: Backend-Oberfläche

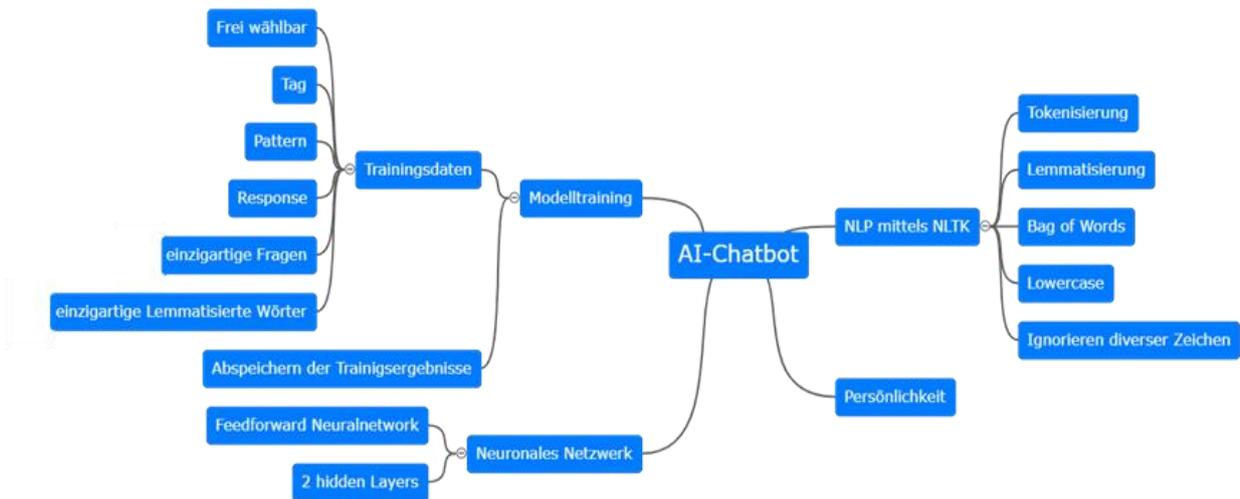


Abbildung 7: KI-Chatbot-Architektur

Improving Software Delivery and Operational Performance with DORA (DevOps Research and Assessment) Best Practices

Peter Bohanec

Hochschule Pforzheim
Tiefenbronner Straße 65
76175 Pforzheim
bohanecp@hs-pforzheim.de

Frank Morelli

Hochschule Pforzheim
Tiefenbronner Straße 65
76175 Pforzheim
frank.morelli@hs-pforzheim.de

Category

Master Thesis

Keywords

DevOps Research and Assessment, DORA, Software Delivery and Operational performance, SDO, best practices, software development

Introduction

With the world digitalizing at a faster pace than ever before, demands for swift and stable software delivery are rising alongside it. New and refined development methodologies and practices must be implemented in order to keep up. Software development methodologies have been evolving since the 1950s, with the pace only increasing in the last few years. From the rigid waterfall model to the dynamic agile development and introduction of DevOps, there have been many different iterations and attempts at finding the best way of developing software. While there is no universal solution that would perfectly fit all scenarios, there likely exist some practices that can improve the software delivery and operational (SDO) performance in all organizations. This is exactly what a team at the DevOps Research and Assessment (DORA) is looking into (Forsgren et al., 2018).

This thesis aims to introduce the capabilities identified by the DORA initiative to improve the SDO performance of teams in an organization. Through research findings it also explores possible difficulties, drawbacks, and advantages that implementing these best practices might have in a real-life scenario.

DevOps Research and Assessment

DevOps Research and Assessment (DORA) initiative started when a team of researchers wondered what are the characteristics of development teams that impact software delivery and operational performance. In 2014 Nicole Forsgren, Gene Kim and Jez Humble started working on the annual State of DevOps report. They developed a valid and reliable way to measure SDO performance and surveyed teams from many different companies and industries. Additionally, they looked at which capabilities predicted SDO performance. Today, the DORA initiative is a part of Google Cloud with a

mission to find new insights and help to improve the SDO performance of software development teams all over the world. There are two key tools that DORA framework provides: metrics and capabilities (Humble, 2019).

DORA metrics

For measuring performance of a software development team the researchers identified four key metrics. They are divided into two categories: throughput and stability. Each metric also has four levels of performance success, from low to elite performer. These metrics are often used by management because they provide an easy-to-understand and comparable way of measuring performance. The key metrics in the throughput category are deployment frequency (how often does the team deploy code to production) and lead time for changes (how long does it take to go from code committed to code successfully running in production). In the stability category the key metrics are time to restore service (how long does it take to restore services when an incident occurs) and change failure rate (what percentage of changes to production result in degraded service) (Forsgren et al., 2019).

DORA capabilities

However, more crucial for improving the SDO performance are the 27 capabilities that were identified by the researchers as important for every team and organization. The capabilities are divided by content into four categories: technical, process, measurement and cultural. Regardless of the division (within the categories or across them) the capabilities are intertwined with each other and can rarely be looked at in isolation. The list of these capabilities is updated annually with every publication of the State of DevOps report.

Technical capabilities are those that are most closely related to the technological and engineering practices carried out by the team or organization. They are version control, trunk-based development, continuous integration, deployment automation, continuous testing, continuous delivery, loosely coupled architecture, cloud infrastructure, test data management, empowering teams to choose tools, shifting left on security, database change management, and code maintainability.

Process capabilities relate to the organizational practices that affect the processes in the development lifecycle.

They are team experimentation, streamlining change approval, customer feedback, visibility of work in the value stream, and working in small batches.

Measurement capabilities relate to practices that teams and management uses to track activity performance in the organization. They are monitoring and observability, work in process limits, visual management capability, monitoring systems to inform business decisions, and proactive failure notification.

Cultural capabilities relate to the organizational or team-level practices that affect every-day lives of developers. They are transformational leadership, learning culture, Westrum organizational culture, and job satisfaction (DORA, 2022).

Research methodologies

The main part of the thesis research focused on assessing whether and in what way DORA best practices can help to improve the SDO performance of development teams in one of the biggest IT companies in the world. With the use of various research methodologies, such as expert interviews, observations, comparison, and literature review data was gathered and analyzed in a way that yielded the most information regarding the topic. Firstly, the current state of software development practices was observed, and available internal literature and tools used were analyzed and compared. After that, through expert interviews an eagle-eye perspective was established and possible implementation inhibitors were discussed. Finally, all the gathered information was consolidated, and implementation suggestions developed.

Implementation considerations

While the DORA capabilities are likely not revolutionary, their implementation still requires a lot of forethought and planning. Especially, if the initiative comes from the top management and targets the entire organization. Four main areas of consideration came up during research: company's business focus (B2C or B2B, cloud or on-premises), scale of the company, tools and practices already in place, and impact of company culture.

Whether a company focuses on business-to-business (B2B) or business-to-customer (B2C) software has a big impact on the way DORA metrics and capabilities should be approached and understood. While B2C companies do almost exclusively benefit from fast deployment of new software, B2B companies must take other considerations into account. These include contract dates (delivering before the agreed date does not have any additional value), more legal requirements, increased liability (very high cost of failure), user resistance, and so on. Additionally, DORA capabilities focus heavily on developing on the cloud, which means that the usefulness of these best practices is limited in case the company is focusing predominantly on-premises software.

Scale of the company and the IT development platform uses to play an integral part in deciding how to go about introducing these practices. In the case of a relatively

small company, implementation of DORA capabilities is not too demanding. However, when it comes to large corporations a top-down approach is not suitable. Rather, teams must be provided with all the support they require and have to be left on their own to decide the specifics of when and how to go about implementing these practices. This is because a lot of capabilities require cultural and management changes that can only effectively take form if they are developed naturally within the teams. The company as whole should focus on enabling the transformation by providing knowledge to managers and, wherever possible, implement company-wide technical solutions. If the company uses multiple development platforms, this poses an additional challenge and increases the complexity of implementation of some of the technical best practices.

As DORA does not introduce any completely new practices it is likely that the company already has some tools and practices in place to improve development performance. These should not be discarded, but only upgraded using the DORA research. By utilizing already established tools less resistance can be expected from the teams. DORA metrics should also be used with caution since they can be too general and are prone to being gamed. While they can provide excellent and easily graspable insight, they might also discourage teams that already know that they are not performing well and encourage unhealthy competition (Mortimer, 2022).

Perhaps the most significant aspect of a successful implementation is the company culture and management. It is very hard to transform the working process of an organization if the culture there does not support it. DORA research emphasizes technological excellence, which might be something that companies are not too keen on if they do not perceive a direct business benefit. For the company claiming to have undergone a full transformation in accordance with the DORA capabilities it must also have a properly technologically oriented core culture. While in small companies and startups this is rarely an issue, big corporations with established businesses practices and company culture have a harder time with this kind of transformation.

In order to be able to start with the implementation of DORA best practices, the topic must first be introduced to the developer teams (and other interested parties) in the organization. As a part of the thesis work a promotional tool was developed using Microsoft PowerApps. The tool introduces DORA initiative, its metrics, and capabilities as a guided experience that is interactive, visually engaging, and easily understandable. It also enables teams to roughly evaluate their current performance and even compare it with others if they choose to do so. The main objective of the promotional tool was to raise awareness of these best practices and to motivate teams to start their improvement journey.

Conclusion and Outlook

There are a lot of potential benefits for learning about DORA framework and integrating it into an organization. While there are no completely new concepts or practices

introduced, the main advantage of DORA lies in its science-based shortlist of the practices that were shown to actually work. This is valuable, since it provides a good starting point for any team or organization that wants to improve their SDO performance without wasting time on practices that do not work.

Anyone looking to implement DORA best practices should take into consideration the four key areas outlined in the article: company's business focus (B2C or B2B, cloud or on-premises), scale of the company, tools and practices already in place in the company, and company culture. DORA metrics should serve primarily to generate intrinsic motivation for the teams to look into the DORA best practices and secondarily as a control tool for the management. Implementing these best practices takes a lot of planning, time, and patience as people's attitude and behavior should not be expected to change overnight.

As a part of the thesis an assessment of DORA best practices' suitability was delivered to the management of the company and an introductory tool of DORA research was created. The management team now uses these findings to inform their decisions regarding the initiative and the tool as a short introduction to DORA for the interested parties. Whether the initiative will be successful remains to be seen.

On the other hand, DORA research continues in earnest, as the interest in and relevance of the topic grows. Reports with the latest findings are published annually and are freely available (DORA, 2022).

References

DORA. (2022). DORA capabilities. *Google Cloud DevOps*. <https://dora.dev>

Forsgren, N., Humble, J., & Kim, G. 2018. *Accelerate: The science of lean software and DevOps: Building and scaling high performing technology organizations*. IT Revolution.

Forsgren, N., Smith, D., Humble, J., & Frazelle, J. 2019. "2019 Accelerate State of DevOps report". Google Cloud DevOps.

Humble, J. (2019). DORA's Journey: An Exploration. *Medium*. <https://medium.com/@jezhumble/doras-journey-an-exploration-4c6bfc41e667>

Mortimer, L. (2022). State of DORA DevOps Metrics in 2022. *isthisit* blog. <https://isthisit.nz/posts/2022/state-of-the-dora-devops-metrics/>.

ABAP-Entwicklung, SAP Customizing und SAP Fiori: Digitalisierung und Optimierung des Bestell- und Kontraktanlageprozesses mithilfe von Angebotsvergleichen

Aylin Bolat

Technische Hochschule
Mittelhessen

Fachbereich Mathematik,
Naturwissenschaften,
Datenverarbeitung
Wilhelm-Leuschner-Straße 13
61169 Friedberg
aylin.bolat@mnd.thm.de

Prof. Dr. Harald Ritz

Technische Hochschule
Mittelhessen

Fachbereich Mathematik,
Naturwissenschaften und
Informatik
Wiesenstraße 14
35390 Gießen
harald.ritz@mni.thm.de

Rüdiger Schlossnikl

Evonik Industries AG

Business Processes - Process
Officer Procurement
Rodenbacher Chaussee 4
63457 Hanau
ruediger.schlossnikl@evonik.com

Kategorie

Masterarbeit

Schlüsselwörter

ABAP, Applikation, Beschaffung, Bestellung, Cloud, Customizing, Digitalisierung, Einkauf, Entwicklung, ERP, Fiori App, Geschäftsprozess, OData, Kontrakt, Launchpad, Procurement, Sourcing, UI5

Zusammenfassung

Oftmals fällt es Menschen schwer, sich von Prozessen und altbewährten Abläufen innerhalb einer Organisation zu trennen und diese neu zu definieren, um eine Steigerung der Effizienz zu verwirklichen. Insbesondere in großen Konzernen werden oft dieselben Prozesse jahrelang unverändert durchgeführt, da häufig auf Widerstand seitens der Mitarbeiter gestoßen und der Aufwand zur Neudefinition der Prozesse als zu hoch geschätzt wird. Im Zuge der Digitalisierung ist das Optimieren von Prozessen durch Neudefinition jedoch unumgänglich, wenn es darum geht, sich im Wettbewerb zu behaupten.

Mithilfe der SAPUI5-Technologie soll gemeinsam mit den Fiori-Designrichtlinien eine Applikation entwickelt werden, welche das Erfassen von Bestellungen und Kontrakten mithilfe von Angebotsvergleichen vereinfacht, beschleunigt und gleichzeitig eine verbesserte Nutzererfahrung bei den Anwendern hervorruft. Bisher wurden diese Angebotsvergleichsdokumente durch strategische Einkäufer in Form von unstrukturierten Dateien erfasst und per E-Mail an den zuständigen operativen Einkäufer gesendet. Dieser wertet die Datei für die weitere Verarbeitung aus, indem die in der Datei enthaltenen Informationen manuell in entsprechenden Transaktionen im ERP-System zum Erfassen von Bestellungen und Kontrakten eingetippt werden.

In diesem Prozess besteht offensichtlicher Optimierungs- und Standardisierungsbedarf. Die durch die strategischen Einkäufer erstellten Dateien unterliegen unter anderem keiner Struktur und unterscheiden sich stark voneinander. Dadurch ist es kaum möglich Auswertungen basierend auf diesen Angebotsvergleichen durchzuführen. Darüber hinaus besteht eine gewisse Fehleranfälligkeit, wenn es darum geht, die Informationen aus den Angebotsvergleichen manuell im ERP-System zu erfassen. Auch das Versenden der Dateien per E-Mail ist zeitaufwändig und kann automatisiert werden.

Im Rahmen eines Projektes im Konzern Evonik Industries AG wurde eine Fiori-Applikation zum Erfassen von Angebotsvergleichen konzipiert und entwickelt. Zudem wurden entsprechende Transaktionen durch Customizing und einhergehender ABAP-Entwicklung im ERP-System erweitert, sodass operative Einkäufer nun die Möglichkeit haben, Angebotsvergleiche, die über die Fiori-Applikation erfasst wurden, im ERP-System zu referenzieren. Das Informieren der operativen Einkäufer per E-Mail verläuft nun automatisiert durch die Fiori App, sobald ein Angebotsvergleich angelegt wird. Durch das Referenzieren werden die Informationen aus dem Angebotsvergleich automatisch in der entsprechenden Transaktion eingesetzt, sodass der operative Einkäufer nicht mehr alle Informationen manuell eintippen muss.

Da die Angebotsvergleiche mithilfe der Fiori-Applikation nun in Form von Datensätzen strukturiert in der Datenbank abgelegt werden, können diese für Analysezwecke verwendet und technisch in nachgelagerten Schritten zusätzlich mit eingebunden werden. Dadurch, dass das manuelle Versenden der E-Mails und das Eintippen der Daten aus den Angebotsvergleichen im ERP-System nun durch das Referenzieren wegfallen, wurde der Prozess erheblich beschleunigt. Zudem verwenden die strategischen

Einkäufer zur Erfassung der Angebotsvergleiche nun eine rollen- und aufgabenspezifisch konzipierte Fiori-Applikationen, die auf verschiedenen Endgeräten verfügbar ist und zu einer besseren Nutzererfahrung beiträgt, anstelle von unstrukturierten Dateien, die sie selbst Anlegen müssen.

Mithilfe des Projektes konnte die Effizienz im Prozess zur Anlage von Bestellungen und Kontrakten mithilfe von Angebotsvergleichen gesteigert werden. Bevor jedoch ein solches Projekt, welches Customizing im Standard eines ERP-Systems erfordert, durchgeführt wird, muss je nach Anwendungsfall klar abgewogen werden, ob dieses wirklich notwendig ist. Die Erweiterung des Standards geht oft mit einem hohen Implementierungs- und Wartungsaufwand einher und sollte nur in Kauf genommen werden, wenn der Nutzen das Risiko überwiegt. Oft wird an Grenzen im Customizing gestoßen, da nur Schnittstellen verwendet werden können, die im ERP-System zur Verfügung stehen. Dies kann zu Limitierungen führen, die vorab genau analysiert werden sollten.

Literatur

Bönnen, Carsten, et al. 2014. OData und SAP Gateway. [Hrsg.] SAP PRESS. Bonn : Rheinwerk, 2014. 978-3-8362-2538-0.

Deutsche Telekom. 2022. Digitalisierungsindex Mittelstand 2021/2022 - Der digitale Status quo des deutschen Mittelstandes. [Online] April 2022.

URL: <https://www.digital-x.eu/de/magazin/digitalisierungsindex/gesamtbericht>

Feldbrügge, Rainer. 2021. Systemisches Prozessmanagement: Unternehmen digitalisieren - Teams mobilisieren. Freiburg: Schäffer-Poeschel, 2021. 978-3-7910-5263-2.

Freilinger-Huber, Sebastian, et al. 2021. ABAP-Entwicklung für SAP S/4HANA : Das Programmiermodell für SAP Fiori. Bonn: Rheinwerk Verlag, 2021. 978-3-8362-7878-2.

Gerbershagen, Johannes. 2020. SAP-Praxishandbuch ABAP Core Data Services (CDS). [eBook] Gleichen: Espresso Tutorials, 2020. 978-3-9601-2710-9 .

Konzeption und Erstellung eines Prototyps zur automatischen Texterkennung und Übernahme von Belegdaten für die digitale Projektbuchhaltung

Tim Luca Eggers

Technische Hochschule
Mittelhessen

Fachbereich MNI
Wiesenstraße 14
35390 Gießen

E-Mail:

tim.luca.eggers@mni.thm.de

Prof. Dr. Harald Ritz

Technische Hochschule
Mittelhessen

Fachbereich MNI
Wiesenstraße 14
35390 Gießen

E-Mail:

harald.ritz@mni.thm.de

Tobias Ebert

mbi GmbH

Konrad-Adenauer-Promenade 17
35578 Wetzlar

E-Mail:

tobias.ebert@mbi.de

Kategorie

Bachelorarbeit

Schlüsselwörter

Digitale Buchhaltung, Künstliche Intelligenz, Automatisierte Rechnungserfassung, Software-as-a-Service, Transformer, LayoutLMv3, Transfer Learning, Fine-Tuning.

Zusammenfassung

Die Verwendung von künstlicher Intelligenz verspricht Automatisierung und Zeit- sowie Kosteneinsparungen. Diese Potenziale können auch in der Rechnungserfassung für die digitale Buchhaltung angewendet werden. So wird die bisherige, manuelle Belegerfassung der digitalen Belege von WINPACCS, einer Projektbuchhaltungsanwendung für internationale Entwicklungszusammenarbeit der mbi GmbH, bezüglich einer KI-Optimierung untersucht.

Im Rahmen dieser Bachelorarbeit wird zunächst die Vorgehensweise einer KI-Umsetzung innerhalb eines Unternehmens dargestellt, welche als Grundlage der Analyse und des Entwurfs dienen. Die Nachteile der bisherigen, manuellen Rechnungserfassung in Form von schlechter Skalierbarkeit, geringerer Geschwindigkeit, Fehleranfälligkeit und hoher Kosten durch menschliche Arbeitskraft können durch einen KI-basierten Ansatz möglichst eliminiert werden. Einzig eine Human-in-the-Loop-Funktionalität erfordert menschliche Kontrolle der erfassten Daten und kann so Fehler reduzieren und zum bestmöglichen Erfassungsergebnis führen.

In Hinblick den Einsatz von KI in der Rechnungserfassung sind einige Herausforderungen zu bewältigen. Die zu erfassenden Belege weisen unterschiedlichste Formate und Qualitäten auf, welche sich in Form von Sprachen, Handschriften, schlechter Scanqualität und Bildartefakten manifestieren. Zudem werden für die eigene Implementierung einer robusten KI qualitativ

hochwertige Trainingsdaten in großen Mengen benötigt. Weiterhin spielen Datenschutz und Integration in die bestehende Anwendung eine entscheidende Rolle für den KI-Einsatz, welcher durch externe Anbieter oder Eigenentwicklung stattfinden kann.

Die Nutzung eines SaaS-Anbieters für die automatisierte Rechnungserfassung bietet einige Vorteile wie die direkte Verfügbarkeit der Funktionalität, die geringe Entwicklungsdauer und Erstinvestition sowie skalierbare Infrastruktur und Kostenabrechnung. Nachteilig sind allerdings die hohe Abhängigkeit und Bindung an den Dienstleister sowie die geringere Kontrolle über die Funktionen. Für die Entscheidung einer Anbieter-nutzung wurde eine Analyse mit 14 Anbietern anhand ausgewählter Vergleichskriterien wie Funktionalitäten, Datenschutz oder Preis-Leistung-Verhältnis durchgeführt. Dabei konnten sich die großen Cloudanbieter Google Cloud, Amazon Web Services und Microsoft Azure durch ihre jeweiligen Dokumentenerfassungen deutlich von kleineren Anbietern abheben. Vor allem Microsoft Azure mit dem Form Recognizer hob sich im Rahmen dieser Analyse durch Datenschutz und Leistung positiv hervor.

Die eigene Implementierung einer KI-Rechnungserfassung wird im Verlauf der Thesis prototypisch dargestellt. Dazu wurde anhand von aktuellen Forschungsständen das LayoutLMv3-Modell ausgesucht und durch Transfer Learning mit den vorliegenden Rechnungsdaten feinjustiert. Diese werden dabei vor dem Training des Modells entsprechend vorverarbeitet und annotiert. Die Steuerung des Trainings erfolgte durch unterschiedliche Hyperparameter. Es konnte mit 900 Trainingsdaten eine Genauigkeit von 0,74 erzielt werden mit stichprobenartig sehr genauen Erfassungen. Eine Inferenz für unbekannte Rechnungen kann durchgeführt werden. Durch diese Umsetzung wurde gezeigt, dass eine eigene Umsetzung unter entsprechenden Voraussetzungen möglich ist. Allerdings muss dafür viel Fachwissen und ein starkes Team aus KI-Entwicklern im

Unternehmen vorhanden sein, welches eine lange Entwicklungszeit begleitet und enorme Mengen an Trainingsdaten und Aufbereitung benötigt, die bei der Nutzung eines SaaS-Anbieters nicht erforderlich sind. So ist im Kontext von WINPACCS generell das Nutzen eines Anbieters auch im Hinblick einer schnell einsetzbaren Lösung sinnvoll und eine Konzentration auf das eigentliche Kerngeschäft erstrebenswerter.

Literatur

Ebener, Stefan (2020): Natural Language Processing in der KI, in: Rüdiger Buchkremer; Thomas Heupel und Oliver Koch (Herausgeber) Künstliche Intelligenz in Wirtschaft & Gesellschaft: Auswirkungen, Herausforderungen & Handlungsempfehlungen, Springer Fachmedien

Evelson, Boris; Katz, Aaron; Lozada, Angela und Barton, Jen (2022): Document-Oriented Text Analytics Platforms, The Forrester Wave

Haneke, Uwe; Trahasch, Stephan; Zimmer, Michael und Felden, Carsten (2019): Data Science: Grundlagen, Architekturen und Anwendungen, dpunkt.verlag

Huang, Yupan; Lv, Tengchao; Cui, Lei; Lu, Yutong und Wei, Furu (2022): LayoutLMv3: Pre-training for Document AI with Unified Text and Image Masking, arXiv, [URL https://arxiv.org/abs/2204.08387](https://arxiv.org/abs/2204.08387)

Konzeption und Implementierung einer globalen, unternehmensweiten Suchlösung für Dokumente und Informationen

Niklas Inerle

Technische Hochschule
Mittelhessen

Fachbereich MND
Wilhelm-Leuschner-Str. 13
61169 Friedberg
E-Mail:
niklas.inerle@mnd.thm.de

Prof. Dr. Harald Ritz

Technische Hochschule
Mittelhessen

Fachbereich MNI
Wiesenstraße 14
35390 Gießen
E-Mail:
harald.ritz@mni.thm.de

Michael Förtsch

Siemens Healthcare GmbH

Modern Workplace
Henri-Dunant Straße 50
91058 Erlangen
E-Mail:
michael.foertsch@siemens-healthineers.com

Kategorie

Masterarbeit

Schlüsselwörter

Unternehmenssuche, Microsoft 365, SharePoint, Sinequa, Elastic Workplace Search, Governance, API, PowerPlatform, Information Retrieval.

Zusammenfassung

Mitarbeitende sind häufig auf der Suche nach Informationen und Ansprechpartnern. Deshalb ist es wichtig, eine gute Unternehmenssuche zu etablieren, um Mitarbeitenden den Zugang zu Informationen zu ermöglichen. Durch die Informationsbereitstellung über eine Suche wird zudem auch das Wissensmanagement in einem Unternehmen unterstützt, da Wissen leichter zu finden ist und durch Mitarbeitende effizienter konsumiert werden kann.

Aktuell weist die Unternehmenssuche bei Siemens Healthineers Problemstellungen auf, welche zukünftig behoben werden sollen. Darunter fallen Punkte wie zum Beispiel, dass nicht alle benötigten Quellen an den Suchindex angeschlossen oder die Ergebnisse nicht relevant genug sind. Das Ziel der Ausarbeitung ist, die Anforderungen an eine Unternehmenssuche zu identifizieren, diese Anforderungen in ein Konzept zu bringen und dieses dann am Beispiel von Siemens Healthineers zu etablieren.

In der Arbeit werden die Anforderungen an eine neue Unternehmenssuche aufgenommen. Dabei ist es wichtig, die Anforderungen verschiedener Personengruppen aufzunehmen, da jeder Mitarbeitende andere Informationen sucht. Anforderungen an die neue Unternehmenssuche sind u.a. die Integration in verschiedene Programme, wie zum Beispiel Microsoft SharePoint oder Teams, Indexierung von SharePoint auf Basis der Benutzerberechtigung sowie eine Sortierung basierend auf den Metadaten der Mitarbeitenden. Aufgrund der ermittelten Anforderungen und den bisherigen Einstellungen der Suche wurde ein

ganzheitliches Konzept erstellt, welches zudem auch organisatorische Elemente beinhaltet.

Das ganzheitliche Konzept enthält die wesentlich benötigten Quellsysteme zur Indizierung. In diesem konkreten Fall werden verschiedene Microsoft-Services, ServiceNow, AzureDevOps und eine Azure Cognitive Search in das Konzept aufgenommen. Damit die Anwender eine konsistente Sucherfahrung haben, wird die Suche an möglichst vielen Orten eingebunden und andere Suchlösungen durch diese Suche ersetzt. Zudem müssen in dem Konzept organisatorische Faktoren betrachtet werden. So muss die Suche Dokumente oder Informationen, welche als „streng vertraulich“ gekennzeichnet sind, ausblenden. Zudem ist ein weiterer wichtiger organisatorischer Faktor die Schulung der Mitarbeitenden auf die neue Suchlösung, dazu werden verschiedene OnePager vorgesehen, ein Video, welches die Suche erklärt sowie einzelne Schulungstermine.

Ein zusätzlich benötigtes organisatorisches Element des Konzepts ist dabei die regelmäßige Prüfung der Ergebnisse auf falsch abgespeicherte Informationen, um die Sicherheitsklassifizierung der zugrunde liegenden Systeme zu gewährleisten sowie die Korrektheit des Eintrages im Verzeichnis von Verarbeitungstätigkeiten sicherzustellen. Zum Umsetzen dieses Elementes wird die Schnittstelle der Suche genutzt, um die Ergebnisse bestimmter Schlüsselwörter abzuspeichern, sodass diese einzeln geprüft werden, um mögliche Fehler zu korrigieren. Diese Korrektur erfolgt über einen in dem Konzept definierten Prozess, welcher Erinnerungen vorsieht. Falls diese Erinnerungen ignoriert werden, werden die Ergebnisse der Prüfung über die bisher bestehende Prozesse zur Meldung von internen Datenschutzproblemen abgebildet.

Auf Basis des Konzeptes wurden die Suchlösungen von Microsoft, Sinequa und Elastic mithilfe einer Nutzwertanalyse verglichen. Es zeigt sich, dass für diesen Anwendungsfall die Suche von Microsoft aufgrund der Integrationsmöglichkeiten, Ergebnisdarstellung sowie des Nutzerbezugs die geeignete

Lösung ist. Das erarbeitete Konzept wird aufgrund dieser Entscheidung mithilfe der Microsoft Search umgesetzt. Dabei wird ein Fokus auf die Indexierung der Services SharePoint, OneDrive, Exchange und Teams gelegt, da diese Programme innerhalb des Unternehmens die zentrale Kollaborationsplattformen darstellen. Zudem werden auch externe Quellen in die Unternehmenssuche mithilfe vorgefertigter Konnektoren eingebunden. Weitere Faktoren der Nutzwertanalyse waren die semantischen Suchfunktionalitäten sowie die Berücksichtigung bestehender Berechtigungen. Dadurch wird sichergestellt, dass ein Nutzender keine Informationen angezeigt bekommt, auf die er kein Zugriff hat.

Nachdem die grundlegende Funktionalität der Suche sichergestellt ist, werden die bestehenden Quicklinks mithilfe von drei Power Automate Flows in die Bookmarks der Microsoft-Suche transformiert. Dazu wird der entsprechende Endpunkt der GraphAPI genutzt. Zudem werden spezielle Filter aufgebaut, um den Nutzenden spezielle Kategorien bereitzustellen. Standardmäßig werden alle Ergebnisse auf das Dateisicherheitslevel gefiltert, sodass streng vertraulicher Inhalt nicht über die Suche gefunden werden kann. Dazu wird ein Filter mithilfe der Kusto Query Language definiert.

Auf Basis des Search-Maturity-Modells von Microsoft lassen sich Organisationen in verschiedene Level der Suchkompetenz einordnen. Es gibt fünf verschiedene Level innerhalb des Modells, dabei ist das Level 100 das erste mögliche Niveau. Die Suche wird aktiviert, aber es stehen keine Prozesse bereit, um Inhalte zu kuratieren oder Mitarbeitende zu schulen. Zudem sind in der Suche wenig Quellen vorhanden. Dies steigert sich stufenweise, bis das Level 500 erreicht ist, in dem es standardisierte Prozesse gibt, Mitarbeitende geschult und syntaktische Suchelemente vorhanden sind.

Anhand dieses Maturity-Modells lässt sich auch der Erfolg des entwickelten Konzeptes bestimmen. Ausgehend von einer Suche, welche wenig relevante Quellen indiziert, wenig Mitarbeitende mit der Suche vertraut und die Ergebnisse der Suche meistens nicht relevant sind. Damit lässt sich die Ausgangslage der Unternehmenssuche auf ein Maturity Level von 100 bis 200 einordnen. Mithilfe des neuen Unternehmenssuchkonzepts wurde die Anzahl der zu indizierenden Quellen stark erhöht und relevante Systeme integriert. Zudem bestehen Anleitungen, welche Besonderheiten der Suche beschreiben und Hinweise für Mitarbeitende geben. Zudem ist durch das neue Konzept sichergestellt, dass die Berechtigungen der Nutzenden berücksichtigt werden und durch vordefinierte Filter bestimmte Elemente angezeigt. Mit der Einführung des neuen unternehmensweiten Suchkonzepts befindet sich die Organisation auf einem Suchlevel zwischen 300 und 400.

Somit können Mitarbeitende durch das neue Unternehmenssuchkonzept quantitativ mehr Quellen durch-

suchen und erhalten durch die größere Informationsvielfalt und die vorteilhaftere Ergebnissortierung qualitativ bessere Ergebnisse der Suche. Es gilt festzuhalten, dass eine Unternehmenssuche kein einmaliges Projekt ist, sondern ein kontinuierlicher Prozess, um eine stetige Verbesserung zu erzielen und diese aufrecht zu erhalten.

Literatur

Croft, W. Bruce; Metzler, Donald; Strohman, Trevor: Search engines. Boston, Columbus, Indianapolis, New York. Addison Wesley (2010).

Hoppe, Thomas: Semantische Suche. Wiesbaden. Springer Vieweg (2020).

Kamath, Uday; Liu, John; Whitaker, James: Deep learning for NLP and speech recognition. Cham. Springer (2019).

Lewandowski, Dirk: Suchmaschinen verstehen. Berlin. Springer Vieweg (2021).

Erfolgsfaktoren eines digitalisierten Lieferantenportals der Adolf Würth GmbH & Co. KG

Paulina Külpmann	Axel Böttcher	Florian Haas	Frank Schätter
Hochschule Pforzheim Fachbereich Einkauf und Logistik Tiefenbronner Str. 65 75175 Pforzheim paulina.kuelpmann@gmail.com	Adolf Würth GmbH & Co. KG Einkauf Zentrale Dienst Reinhold-Würth-Str. 12-17 74653 Künzelsau Axel.Boettcher@wuerth.com	Hochschule Pforzheim Fachbereich Einkauf und Logistik Tiefenbronner Str. 65 75175 Pforzheim florian.haas@hs-pforzheim.de	Hochschule Pforzheim Fachbereich Einkauf und Logistik Tiefenbronner Str. 65 75175 Pforzheim frank.schaetter@hs-pforzheim.de

Schlüsselwörter

Digitalisierung, Lieferantenportal, Langzeit-Lieferantenerklärung, Lieferanten-Incentivierung

Problemstellung und Zielsetzung

Um als Handelsunternehmen mit einem hohen Exportanteil nicht erforderliche Zollabgaben zu vermeiden, werden häufig Zollpräferenzen genutzt. Hierbei können durch die Angabe des präferenziellen Warenursprungs einer Exportware Zollkosten eingespart werden, sofern zwischen dem Exportland und dem Bestimmungsland der Ware ein Präferenzabkommen abgeschlossen wurde¹, wie dies beispielsweise zwischen EU und Japan der Fall ist. Soll eine Ware aus Japan in die EU importiert werden, fallen die Zollkosten für den Warenimport durch die Angabe des Ursprungs Japan geringer aus als ohne Ursprungsangabe. Gleiches gilt für Exporte aus der EU nach Japan.² Beschaffungskosten können so niedrig gehalten und die eigene Wettbewerbsposition in stetig wachsenden Märkten gestärkt werden.³

Der Einsatz der Zollpräferenzen setzt den Nachweis des Ursprungs der Waren in Form einer Lieferantenerklärung voraus. Um den Aufwand hierfür zu verringern, werden von den Lieferanten üblicherweise Langzeitlieferantenerklärungen (LLE) an die exportierenden Kunden ausgestellt. Diese sind an einen durch den Lieferanten festzulegenden Lieferzeitraum gekoppelt mit einer maximalen Laufzeit von 24 Monaten unter der Voraussetzung, dass sich das Ursprungsland der Ware nicht ändert. Eine LLE ist somit ein offizielles Nachweispapier, damit eine Zollpräferenz bei Warenexport genutzt werden kann.⁴

Der Prozess zur Einholung einer LLE bei Lieferanten ist seit Jahren nahezu unverändert und nur wenig digitalisiert. Häufig werden die Erklärungen kaum standardisiert per PDF oder per Post von den Lieferanten an ihre exportierenden Kunden übermittelt und müssen anschließend manuell, z.B. in ein ERP-System,

eingepflegt werden. Diese Medienbrüche erschweren eine Prozessautomatisierung und nichtwertschöpfende Tätigkeiten führen zu hohen Prozesskosten – woraus sich erhebliche Einsparpotenziale für Unternehmen ergeben. Hinzu kommt, dass die Nutzung von Zollpräferenzen aufgrund einer Zunahme internationaler Handelsbeschränkungen in letzter Zeit stärker in den Fokus gerückt ist. Auch bei behördlichen Prüfinstanzen, wie Industrie- und Handelskammern (IHK) und Zollbehörden hat das Thema der Ursprungsnachweise in den letzten Jahren an Beachtung gewonnen, was die Anforderungen an eine vollständige und jederzeitige Verfügbarkeit und Rechtssicherheit der Ursprungsdaten erhöht. Als Reaktion auf diese Entwicklungen wird bei der Adolf Würth GmbH & Co. KG ein Lieferantenportal implementiert, welches den Lieferanten des Konzerns eine digitale Übermittlung ihrer LLE ermöglicht.

Um den oben genannten Anforderungen gerecht zu werden, ist es notwendig, dass möglichst viele Lieferanten an das LLE-Portal angebunden werden. Dabei ist zu erwarten, dass nicht alle Lieferanten die erforderliche Bereitschaft zur Nutzung des neuen Portals zeigen, da mit jeder Portaleinführung ein Aufwand zur Anbindung und Schulung der Anwender verbunden ist. Darüber hinaus nutzen viele Lieferanten bereits eine Vielzahl unterschiedlicher Portale abseits des eigenen ERP-Systems. Es gilt also, die Bereitschaft der Lieferanten zur Nutzung des Portals durch den strategischen Einsatz geeigneter Maßnahmen zu steigern.⁵ Ziel und Aufgabe der Abschlussarbeit war es daher, Faktoren zu ermitteln, die zur Akzeptanz der Lieferanten und damit zum Erfolg des LLE-Portals beitragen. Neben der Ermittlung der für die Lieferanten relevanten Anforderungen an das Portal sind dabei insbesondere auch wirksame Motivatoren von Bedeutung, die die Lieferanten von der Nutzung des Portals überzeugen.

¹ Industrie- und Handelskammer Heilbronn-Franken, o.S.

² Butz, o.S.

³ Möller und Schumann 2019, S. 65.

⁴ Möller und Schumann 2019, S. 153.

⁵ Stählström 2020, S. 34.

Methodisches Vorgehen

Zunächst werden mögliche Erfolgsfaktoren für die Implementierung und Anwendung eines LLE-Portals ermittelt. Hierzu bietet die Fachliteratur bereits einige Ansätze, die zur Ableitung von Erfolgsfaktoren herangezogen werden können.⁶ Im Rahmen einer Expertenbefragung werden die identifizierten Erfolgsfaktoren dann validiert. Die Testphase mit ausgewählten Lieferanten der Adolf Würth GmbH & Co. KG bildet den Abschluss der Untersuchung und soll Aufschluss über die Wirkung der aufgestellten Erfolgsfaktoren in der Praxis geben.

Erfolgsfaktoren für das LLE-Portal

Bei Erfolgsfaktoren handelt es sich um eine begrenzte Anzahl an Größen, die ausschlaggebend für die Erreichung von Zielen und somit für den Erfolg eines Projekts sind.⁷ In Abhängigkeit der Art und der individuellen Ziele eines Projektes variieren diese Erfolgsfaktoren. Dabei ist kein einzelner Erfolgsfaktor allein für den Projekterfolg verantwortlich. Vielmehr sind die Erfolgsfaktoren interdependent und tragen ganzheitlich zum Erfolg des Projektes bei.⁸

Die Qualität von IT-Systemen beeinflusst auch im Bereich der Lieferantenportale deren Akzeptanz bei den Lieferanten und stellt somit einen Erfolgsfaktor dar. Dabei wird zwischen der System-, der Informations- und der Servicequalität differenziert.⁹

Abbildung 1 visualisiert die vier wesentlichen identifizierten Erfolgsfaktoren für die Implementierung und Nutzung eines LLE-Portals: Qualität, Nutzensgewinn, Marktmachtverhältnis und Plausibilität der Prozessänderung.

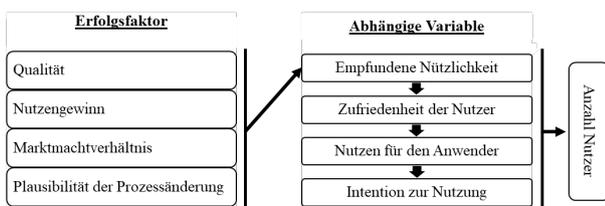


Abbildung 1: Mögliche Erfolgsfaktoren für das LLE-Portal

Die Erfolgsfaktoren stehen im Zusammenhang mit Variablen, um diese zu bewerten. Mit zunehmendem Nutzen der Anwender steigt die Intention zur Nutzung des Portals und damit die Anzahl der Lieferanten, die an das Portal angebunden werden können.

Nachfolgend werden die ermittelten Erfolgsfaktoren näher betrachtet.

1) Qualität

Systemqualität

Eine hohe Systemqualität äußert sich beispielsweise in der Gewährleistung einer hohen Systemzuverlässigkeit, einer einfachen Zugänglichkeit des Portals, sowie einer

hohen Systemflexibilität und Benutzerfreundlichkeit. Potenzielle Hürden, die die Portalnutzung behindern könnten, müssen frühzeitig eliminiert werden.¹⁰

Informationsqualität

Der Anwendernutzen des Portals wird durch eine hohe Informationsqualität erhöht. Die Informationen, die wie im Falle des LLE-Portals den Lieferanten vom Kunden zur Ver- und Bearbeitung im Portal bereitgestellt werden, sollten stets richtig, genau, vollständig und konsistent sein.

Servicequalität

Es sollte gewährleistet sein, dass die Anwender zu jeder Zeit auf einen kompetenten Supportmitarbeiter zugreifen können, um Anwendungsprobleme nach Möglichkeit sofort zu beheben. So sollen Verzögerungen bei der Portalnutzung, die zur Unzufriedenheit der Anwender führen, möglichst vermieden werden.¹¹

2) Nutzensgewinn

Zu nennen ist hier zunächst der Imagegewinn der Lieferanten, die eine Portalnutzung in Erwägung ziehen. Ein kooperatives Verhalten der Lieferanten kann die Geschäftsbeziehung zu ihrem Kunden stärken. Darüber hinaus kann der Lieferant von einer Reduktion des Aufwands zur Ausstellung seiner LLE aufgrund der digitalen Übertragung der Ursprungsdaten an seinen Kunden profitieren. Viele Funktionen innerhalb des Portals ermöglichen dem Lieferanten ein effizientes Arbeiten. Ein weiterer Vorteil für den Lieferanten ist die höhere Rechtssicherheit der angegebenen Ursprungsdaten durch integrierte Prüfmechanismen im Portal. Außerdem können Lieferanten, die selbst regelmäßig LLEs einholen, von der digitalen Lösung profitieren, indem sie das Portal für ihre eigenen Lieferanten nutzen.

Es gilt, bei der Portalimplementierung ein Bewusstsein für die genannten Vorteile bei den Lieferanten zu schaffen, indem man die Lieferanten beispielsweise bei Schulungsterminen über die vielfältigen Vorteile des LLE-Portals informiert.

3) Marktmachtverhältnis

Eine eventuelle Abhängigkeit der Lieferanten von großen Kunden sorgt für ein Interesse der Lieferanten an einer gut funktionierenden Geschäftsbeziehung. Ein solches Machtverhältnis verleiht dem Kunden im Rahmen einer Chancenrealisierungsstrategie¹² die Möglichkeit, Druck auf die Lieferanten auszuüben, so dass diese das LLE-Portal nutzen.¹³

4) Plausibilität der Prozessänderung

Zuletzt könnte die Nennung der Beweggründe für die Änderung des bisherigen Prozesses zur Nachvollziehbarkeit der Portalimplementierung bei den

⁶ De Wit 1988, Benedict et al. 2015, Dinesh et al. 2017.

⁷ Dinesh et al. 2017, S. 477.

⁸ King 1996, S. 23.

⁹ Adeyemi und Issa 2020, S. 75.

¹⁰ Kollmann 2019, S. 776.

¹¹ Ebd., S. 778

¹² Arnolds et al. 2016.

¹³ Stählström 2020, S. 34.

Lieferanten beitragen. Ein Verständnis der Lieferanten für die Beweggründe des Kunden, das LLE-Portal einzuführen, könnte zu einer höheren Akzeptanz des Portals führen.¹⁴

Anwendung der Erfolgsfaktoren in der Praxis

Die Wirkung der ermittelten Erfolgsfaktoren auf die Akzeptanz der Lieferanten wurde im Rahmen einer Testphase mit ausgewählten Lieferanten überprüft. Es zeigte sich, dass für die Akzeptanz der Lieferanten eine hohe Qualität des Portals erforderlich ist. Außerdem trägt eine überlegene Machtposition des einkaufenden Unternehmens sowie das Bemühen vieler Lieferanten, die Vorgaben des Kunden zu erfüllen - sofern es sich um einen strategisch wichtigen Kunden handelt - zur Akzeptanz des Portals bei. Oft wurde mit den Lieferanten auch die Kompatibilität des Portals zu den Prozessen und Systemen beim Lieferanten diskutiert. Es hat sich gezeigt, dass einige Lieferanten bereits über IT-Systeme verfügen, aus denen eine LLE automatisch erstellt werden kann. Somit würde die Nutzung des Portals für sie einen beachtlichen Mehraufwand darstellen. Hier wäre eine große Offenheit des Portals hinsichtlich der Nutzung verschiedener Schnittstellen für den automatisierten Datenaustausch ein wesentlicher Erfolgsfaktor.

Fazit

Das Ziel der Abschlussarbeit war es, die relevanten Erfolgsfaktoren für ein digitalisiertes LLE-Portal zu identifizieren und zu bewerten. Es wurden die Erfolgsfaktoren Qualität, Nutzensgewinn, Marktmachtverhältnis sowie Plausibilität der Prozessveränderung analysiert und im Rahmen einer Testphase validiert. Es hat sich gezeigt, dass sich alle Erfolgsfaktoren positiv auf die Akzeptanz des LLE-Portals auswirken. Insbesondere das Marktmachtverhältnis in Form einer überlegenen Wettbewerbsposition des einkaufenden Unternehmens sowie ein von den Lieferanten erhoffter Imagegewinn tragen maßgeblich zur Bindung der Lieferanten bei. Auch eine hohe Qualität des Portals beeinflusst die Akzeptanz der Lieferanten maßgeblich. Zusätzlich sollte die Kompatibilität des Portals mit den bei den Lieferanten im Einsatz befindlichen Systemen als weiterer relevanter Erfolgsfaktor sichergestellt werden. Bei der Einführung eines Lieferantenportals sollten zudem die individuellen Gegebenheiten bei den Lieferanten, beispielsweise hinsichtlich ihrer Kenntnisse zu zollrechtlichen Themen, beachtet werden. Die Wirkung der Erfolgsfaktoren könnte bei Lieferanten mit unterschiedlichen Voraussetzungen unterschiedlich ausgeprägt sein. Es sollte in Zukunft daher eine Kategorisierung der Lieferanten vorgenommen werden, um die richtigen Erfolgsfaktoren bei den richtigen Lieferanten einzusetzen.

¹⁴ Stählström 2020, S. 34.

Literaturverzeichnis

- Arnolds, H.; Heege, F.; Röh, C.; Tussing, W. (2016): *Materialwirtschaft und Einkauf*, 13. Aufl., Springer Gabler, Wiesbaden.
- Adeyemi, I.O.; Issa, A.O. (2020): Integrating Information System Success Model (ISSM) And Technology Acceptance Model (TAM). Proposing Students' Satisfaction with University Web Portal Model. In: *Record and Library Journal* 6 (1), S. 69–79.
- Benedict, A.; Emmanuel, U.C.; Enoch, O.O.; Uchenna, A.; Perpetua, N. (2015): Critical Success Factors for Public Sector Construction Project Delivery. A Case of Owerri, Imo State. In: *International Journal of Research in Management, Science & Technology* (3), S. 11–21.
- Butz, C.: Die Zollpräferenzbeziehungen der EU – Alle Infos zum Präferenzabkommen: Abkommen, Länder & Zonen.
- De Wit, A. (1988): Measurement of project success. In: *International Journal of Project Management* 6 (3), S. 164–170.
- Dinesh, S.; Sethuraman, R.; Srimathi, S. (2017): A Review On Critical Success Factors In Construction Project. In: *International Journal of Scientific Research in Science, Engineering and Technology* (3), Artikel 2, S. 477–481.
- Industrie- und Handelskammer Heilbronn-Franken: Merkblatt Zollvorteile (Präferenzen).
- King, I. (1996): The road to continuous improvement: BPR and Project Management. In: *IIE solutions* 28 (10), S. 22–28.
- Kollmann, T. (2019): *E-Business. Grundlagen elektronischer Geschäftsprozesse in der digitalen Wirtschaft*. 7. überarbeitete und erweiterte Aufl. Wiesbaden: Springer Fachmedien.
- Möller, T.; Schumann, G. (2019): *Warenursprung und Präferenzen. Handbuch und systematische Darstellung*. 9. aktualisierte Aufl. Köln: Bundesanzeiger Verlag GmbH.
- Stählström, M. (2020): *Improving supplier relationship management with supplier portal*. Masterthesis. Aalto University. School of Science.

Aufbau einer Datenvorbereitungsumgebung für Machine-Learning-Modelle zur Berechnung von kundenindividuellen Produktabschlüssen

Laura Offermanns

Technische Hochschule
Mittelhessen

Fachbereich MND
Wilhelm-Leuschner-Straße 13
61169 Friedberg
E-Mail:

laura.offermanns@mnd.thm.de

Prof. Dr. Harald Ritz

Technische Hochschule
Mittelhessen

Fachbereich MNI
Wiesenstraße 14
35390 Gießen

E-Mail:

harald.ritz@mni.thm.de

Dr. Michel Becker

Mittelstand.ai GmbH & Co. KG

Schiffenberger Weg 110
35394 Gießen

E-Mail:

michel.becker@mittelstand.ai

Kategorie

Masterarbeit

Schlüsselwörter

PySpark, SQL, Apache Beam, Datenvorbereitung, Machine Learning, Python, Google Cloud, Dataflow, Dataproc

Zusammenfassung

Große Datenmengen, auch Big Data genannt, können oftmals mit traditionellen Datenverarbeitungswerkzeugen nicht adäquat verarbeitet werden. Es stellt eine Herausforderung dar, diese zu transformieren und zu aggregieren. Bei der Mittelstand.ai GmbH & Co. KG in Gießen können Banken kundenindividuelle Produkte bestellen, welche auf Basis von Machine-Learning-Algorithmen eine Empfehlung geben, welches Bank- oder Versicherungsprodukt ein Kunde als Nächstes abschließen würde. Dazu wurde eine Analyse-Plattform entwickelt, in welcher Banken ihre individuellen Produkte bestellen und abrufen können. Weiterhin wird diese zum Hochladen der Daten verwendet. Die Machine-Learning-Algorithmen basieren auf den vergangenen Kundendaten der Banken und werden für jede Bank differenziert angewendet.

Die Transformation und Aggregation der einzelnen Daten wurde mit Python und den Bibliotheken Pandas und Numpy realisiert. Die Durchlaufzeit einer Datenvorbereitung für eine Bank ist sehr hoch und nicht automatisiert. Das bedeutet, bei jedem Durchlauf wird ein Mitarbeiter-PC benötigt, welcher in dieser Zeit aufgrund der hohen Rechenleistung nicht anderweitig verwendet werden kann. Außerdem werden die csv-Dateien mit den zu analysierenden Daten manuell heruntergeladen und nehmen somit viel Speicherplatz ein. Jede Bank lädt pro Monat vier Dateien hoch, welche über die Monate hinweg verarbeitet werden. Dadurch kommt die lokale Ausführung schnell an ihren

Grenzen, in der Verarbeitung und auch im Datenspeicher.

Mit einer neuen Datenvorbereitungsumgebung soll die Laufzeit der Transformations-, Filter- und Aggregationsvorgänge verringert werden sowie eine Umgebung geschaffen werden, welche nicht lokal auf den PCs ausgeführt wird, sondern in der Google Cloud realisiert werden kann. Eine weitere Anforderung ist die Automatisierung der Umgebung. Durch die Einbindung von Google-Cloud-Produkten, welche bereits in der Mittelstand.ai verwendet werden, soll es möglich sein, geplante Datenvorbereitungen durchzuführen, da jede Bank monatlich ihre Daten in die Analyse-Plattform hochlädt.

Unter diesem Aspekt wurde eine Testumgebung entwickelt, welche mithilfe von Apache Beam und Dataflow die Daten der Banken verarbeitet. Dabei wurden Filterfunktionen, welche das Alter der Kunden, die Geschäftsform und beispielsweise die Einwilligung in die Verarbeitung der personenbezogenen Daten berücksichtigt, angewandt. Weiterhin konnten erste Transformationen durchgeführt werden, welche sich mit der Aufarbeitung des Datensatzes beschäftigen. Im Schritt der Datenaggregation konnte Apache Beam nicht überzeugen, da das vorgegebene Datenformat mit einzelnen Iterationen in Python verarbeitet werden musste und somit den Aspekt der Zeiteinsparung in einem Anwendungstest nicht erfüllte. Durch das Iterieren der Datensätze, welche durch die speziellen Anforderungen der Vorbereitung entstanden ist, mussten eigene Funktionen definiert werden. Diese Funktionen arbeiten nicht optimal mit dem Apache Beam Framework aufgrund der fehlenden Parallelisierung zusammen. Die Automatisierung mit Dataflow war jedoch erfolgreich und konnte planbar gestaltet werden.

Um auch Erfolge in der Effizienz zu erzielen, wurde

eine weitere Testumgebung eingerichtet. Diese nutzt als Basis das Framework PySpark und zusätzlich SQL-Abfragen, um die Daten vorzubereiten. Die SQL-Abfragen werden individuell für jede Bank generiert. Dazu dient ein String Builder, welcher in der PySpark Umgebung implementiert wurde. Dieser beachtet Informationen wie beispielsweise die eindeutige ID der Bank und die Konfigurationen, welche eine Bank bei einer Produktbestellung angeben kann. Dazu gehört ebenso die Tiefe der Analyse, da die Datengrundlage die Möglichkeit bietet, Kundenverhalten sehr genau zu analysieren. Eine weitere Möglichkeit, die Bestellung zu konfigurieren, liegt in der Einstellung der miteinander zubeziehenden Daten. Das hat den Vorteil, dass eine Bank die Möglichkeit hat, die letzten 15 Monate oder auch nur sechs Monate in ihr Ergebnis miteinzubeziehen. Dadurch können bankenindividuelle Ereignisse, welche zu einem abweichenden Verhalten der Bankkunden geführt hat, ausgeschlossen werden und verfälschen somit das Ergebnis nicht.

PySpark ist ebenfalls in der Lage, in den Funktionen die Konfigurationen der Banken miteinzubeziehen. Die wichtigste PySpark-Funktion ist die Pivot-Tabelle, mit welcher die Daten auf bestimmte Kennzahlen transformiert und aggregiert werden. Im Gegensatz zur alten Umgebung arbeitet diese effizienter und kann tiefere Datenebenen verarbeiten. Zur Ausführung in der Google Cloud wurde Dataproc verwendet. Die Clusterkonfiguration entspricht den Bankenanforderungen und stellt somit sicher, dass die Daten ordnungsgemäß verarbeitet werden. Sobald ein Dataproc-Cluster hochgefahren wurde, kann ein PySpark-Job auf diesem ausgeführt werden. Mit der aktivierten Option des Autoscalings ist es möglich, die Clusterauslastungen automatisch zu regeln und somit eine optimale Auslastung der Rechenkapazität und der Kosten zu bieten. Des Weiteren besteht die Möglichkeit Durchläufe für Banken zu planen und diese regelmäßig durchzuführen, ohne dass ein Mitarbeiter eingreifen muss.

Die Kombination der PySpark-Funktion mit den SQL-Befehlen führte zu einer effizienten Verarbeitung. In einer Testumgebung konnte die Durchlaufzeit etwa halbiert werden. Neben der Implementierung eines Bankproduktes ist die modulare Erweiterung des Codes anzumerken. Durch die Modularität können weitere Filter, Transformationen, Aggregationen und Berechnungen eingeführt werden. Ebenfalls sind die Mitarbeiter vertraut mit der Nutzung von Python und den Datentypen des PySpark-Frameworks, da im Vorfeld bereits mit Pandas gearbeitet wurde und Tabellenstrukturen bekannt sind. Aufgrund einer parallelen Entwicklung konnte ein Data Warehouse verwendet werden und ermöglichte den Beginn einer Automatisierung der Datenvorbereitungsumgebung. Mit der Nutzung von SQL-Abfragen konnte die Anbindung an das Data Warehouse realisiert werden. Nachdem alle Dateien der Bank vorbereitet wurden, ist es möglich, diese wieder zusammenzuführen und weitere

Aufbereitungen, beispielsweise der Spaltennamen, durchzuführen.

Eine Tabelle in dem Data Warehouse mit einem vorbereiteten Enddatensatz stellt die Schnittstelle zur Umgebung dar, auf welcher die Machine-Learning-Algorithmen angewendet werden. Auch diese bietet die Möglichkeit, automatisiert auf die neue Tabelle zuzugreifen.

Abschließend lässt sich erwähnen, dass erfolgreich eine Umgebung implementiert wurde, welche die vorhandenen Anforderungen an eine neue Datenvorbereitungsumgebung erfüllt und einen Ansatz für viele Erweiterungs- und Automatisierungsmöglichkeiten mit sich bringt.

Literatur

D'Onofrio, Sara; Meier, Andreas. Big Data Analytics. Wiesbaden. Springer Vieweg (2021)

Drabas, Tomasz; Lee, Denny. Learning PySpark. Birmingham. Packt Publishing (2017)

Frochte, Jörg. Maschinelles Lernen. München. Hanser (2021)

Anwendung von agilen skalierbaren Frameworks im Projektmanagement von IT-Dienstleistern

Anna-Lena Pütt

Hochschule Pforzheim
Tiefenbronner Straße 65
75175 Pforzheim
anna-lena.puett@gmx.de

Frank Morelli

Hochschule Pforzheim
Tiefenbronner Straße 65
76175 Pforzheim
frank.morelli@hs-pforzheim.de

SCHLÜSSELWÖRTER

Projektmanagementmethoden, Agiles Projektmanagement, Agile skalierbare Frameworks

Problemstellung und Zielsetzung

Die vorliegende Bachelorarbeit beschäftigt sich mit der Frage, wie agile Methoden im Projektmanagement von IT-Dienstleistern skaliert werden können, um Kunden bei der Einführung neuer Software bestmöglich zu unterstützen. Dazu werden agile Frameworks (ASFs) wie Scaled Agile (SAFe), Large Scale Scrum (LeSS), Disciplined Agile Delivery (DAD) und Nexus vorgestellt und analysiert. Die Auswahl der hier beschriebenen Frameworks basiert auf dem „Status Quo Agile Report 2020“ von Prof. Dr. A. Komus in Kollaboration mit der Hochschule Koblenz. Der Fokus der Arbeit liegt darauf, wie diese Frameworks eingesetzt werden können, um den Herausforderungen bei der Umsetzung von Software-Projekten zu begegnen.

Agile skalierbare Frameworks

Die Literaturanalyse sowie die Befragung ergaben, dass ASFs einen vielversprechenden Ansatz für das Projektmanagement von IT-Dienstleistern darstellen, da sie eine schnelle und flexible Anpassung an Kundenbedürfnisse ermöglichen. Der Einsatz von ASFs im Projektmanagement von IT-Dienstleistern stellt jedoch eine komplexe Herausforderung dar, da die Auswahl des richtigen ASFs nicht nur auf die Anforderungen des eigenen Unternehmens, sondern auch auf die Kompatibilität mit den Kunden abgestimmt werden muss. Eine falsche Wahl kann zu erheblichen Problemen in der Projektarbeit führen.

Methodisches Vorgehen

Bei der Befragung handelte es sich um eine explorative Studie, welche an 115 Großunternehmen verschickt wurde. Die Befragung umfasste 27 Fragen, welche in mehrere Abschnitte unterteilt war. Diese Abschnitte waren „Demographie“, „Vorabfragen zur Agilität“, „Scrum und Projektmanagementmethoden“, „ASF-Fragen“ und „Meinungsfragen“. Innerhalb der Befragungszeit haben insgesamt 21 der 115 Unternehmen an der Befragung teilgenommen. Daraus wurde eine Beteiligungsquote von 18,26% errechnet.

Auswahl der ASF

Die durchgeführte Befragung zeigt, dass Unternehmen bei der Auswahl von ASFs insbesondere auf die Skalierbarkeit, Flexibilität und Kompatibilität mit bestehenden Systemen achten sollten. Keines der Frameworks stellt jedoch die perfekte Lösung dar, da sowohl SAFe als auch LeSS Vor- und Nachteile haben, die bei der Auswahl eines geeigneten Frameworks berücksichtigt werden müssen. SAFe ermöglicht eine strukturierte und hierarchische Organisation, die besonders für große Unternehmen geeignet ist, die komplexe Projekte mit vielen Beteiligten und Abhängigkeiten managen müssen. Die Anwendung von Agile Release Trains kann jedoch in kleineren Projekten zu Problemen führen. LeSS hingegen ist auf kleinere Skalierungen ausgerichtet und i.d.R. mit den bestehenden Arbeitsweisen und Methoden kompatibel. Allerdings ist die Flexibilität bei der Anwendung verschiedener Projektmanagementmethoden gering, was eine optimale Nutzung verhindert.

Hindernisse im Projektmanagement

Aus den Erkenntnissen der Befragung lässt sich eine Rangfolge der Haupthindernisse in der Projektarbeit ableiten. Diese sind in Tabelle 1 dargestellt.

Rank	Haupthindernis	Auswahl	Arith. Mittel	SD
1	<i>Budget- oder Terminüberschreitungen</i>	12x	1,92	1,31
2	<i>Zu hohe Komplexität des Projekts</i>	12x	2,58	1,56
3	<i>Gestörter Informationsfluss</i>	12x	2,83	1,27
4	<i>Unrealistisch oder unbekannte Ziele</i>	12x	3,08	1,31
5	<i>Fehlende Identifikation mit dem Projekt bei den Projektbeteiligten</i>	8x	2,88	1,64
6	<i>Unstrukturierte Kommunikation</i>	8x	3,38	1,06
7	<i>Unklare Erfolgskriterien</i>	8x	3,75	1,28
8	<i>Fehlende Kompetenzen bei Projektmitarbeitenden</i>	6x	3,83	0,98
9	<i>Mangelnde Erfahrung in der Projektleitung</i>	1x	1,00	-

Tabelle 1: Rangfolge der Haupthindernisse.

Die Hindernisse korrelieren mit den angegebenen Verbesserungspotentialen. Auch diese lassen sich in eine Rangfolge bringen, die in Tabelle 2 zu sehen ist.

Rank	Verbesserungspotentiale	Auswahl	Arith. Mittel	SD
1	<i>Präzisere Definition von Inhalten, Zielen und Erfolgskriterien</i>	15x	2,33	1,11
2	<i>Verbesserte Kommunikation</i>	14x	3,36	1,28
3	<i>Klare Priorisierung der Projekte</i>	13x	2,00	0,5
4	<i>Etablierung von Projektstandards</i>	9x	2,44	1,74
5	<i>Training der Projektbeteiligten</i>	9x	2,89	1,27
6	<i>Unterstützung durch erfahrene Projektbeteiligten</i>	8x	3,63	1,41
7	<i>Mehr Unterstützung durch das Management</i>	4x	3,25	1,26

Tabelle 2: Rangfolge der Verbesserungspotentiale

Eine klare und transparente Kommunikation ist entscheidend für eine erfolgreiche Projektarbeit und minimiert Missverständnisse. Die Ergebnisse zeigen, dass ein gestörter Informationsfluss und eine unstrukturierte Kommunikation die Projektarbeit behindern bzw. eine klare und transparente Kommunikation gewünscht wird. Um die Erwartungen an eine Zusammenarbeit mit externen IT-Dienstleistern zu erfüllen, muss der Fokus auf Expertise, Erreichbarkeit und Support gelegt werden. Die Befragungsergebnisse zeigen, dass Expertise und Support vom Dienstleister gewünscht werden. Hierzu muss ein Dienstleister den regelmäßigen Austausch mit den Kunden, eine hohe Erreichbarkeit sowie einen technischen Support und Expertise, unter anderem durch ein erfahrenes Projektmanagement, ermöglichen.

Um die Kompetenzen der Mitarbeitenden zu stärken und damit eine effiziente Projektarbeit zu ermöglichen, müssen diese geschult werden. Die Befragungsergebnisse haben gezeigt, dass bei den Mitarbeitenden Kompetenzen fehlen, die man durch Schulungen verbessern kann. Um eine erfolgreiche Einführung der Software zu ermöglichen, müssen die Kompetenzen der Mitarbeitenden durch Trainings im Umgang mit der IT-Lösung gestärkt werden.

Fazit

Abschließend lässt sich festhalten, dass der Einsatz agiler skalierbarer Frameworks im Projektmanagement von IT-Dienstleistern eine vielversprechende Möglichkeit darstellt, um den sich schnell ändernden Kundenbedürfnissen gerecht zu werden. Dabei müssen jedoch die Vor- und Nachteile der verschiedenen Frameworks sowie die Herausforderungen bei der Einführung berücksichtigt

werden. Es bedarf einer sorgfältigen Planung und Umsetzung, um die Vorteile der agilen Arbeitsweise voll auszuschöpfen. Die Ergebnisse der Befragung zeigen, dass bei Unternehmen, die SAFe erfolgreich implementiert haben, das SAFe Framework sich offenbar auch mit einer geringeren Anzahl von Mitarbeitern pro ART implementieren lässt. In diesem Kontext stellt sich die Frage, ob beim Einsatz von SAFe die Skalierung von IT-Dienstleistungen auch ohne den Einsatz von ARTs erfolgen kann. Ferner sollte im Hinblick auf einen möglichen Einsatz eines ASFs zur Skalierung von IT-Dienstleistungen auch eine mögliche Implementation von unterschiedlichen Projektmanagementmethoden bei LeSS näher untersucht werden. Im Hinblick auf eine allgemeine erfolgreiche Projektarbeit steht die Kommunikation als Problemfeld im Vordergrund. Für die genannten Aspekte erweisen sich weitere Forschungsaktivitäten als erforderlich, um eine adäquate Implementation zu begünstigen.

LITERATUR

- Beck, K. u.a. (2001): Manifest für Agile Softwareentwicklung. URL: <https://agilemanifesto.org/iso/de/manifesto.html>, abgerufen am 26.12.2022.
- Komus, A. u.a. (2020): Ergebnisbericht: Status Quo (Scaled) Agile 2020: 4. Studie zu Nutzen und Erfolgsfaktoren agiler Methoden. URL: <http://www.processand-project.net/studien/studienunterseiten/status-quo-scaled-agile-2020/>, abgerufen am 18.01.2023.
- Larman, Craig; Vodde, Bas (2017): Large-Scale Scrum: Scrum erfolgreich skalieren mit LeSS. 1. Aufl., dpunkt, Heidelberg.
- Lines, Mark; Ambler, Scott W. (2012): Disciplined Agile Delivery: A Practitioner's Guide to Agile Software Delivery in the Enterprise. Illustrated Edition, IBM Press, Upper Saddle River, NJ.
- Project Management Institute (2023): Disciplined Agile Delivery (DAD), URL: <https://www.pmi.org/disciplined-agile/process/introduction-to-dad>, abgerufen am 05.01.2023.
- Scaled Agile Framework (2021): SAFe 5.0 Framework. URL: <https://www.scaledagileframework.com/>, abgerufen am 18.12.2022.
- Schwaber, Ken (2021): Der Nexus™ Guide: Der gültige Leitfaden zur Skalierung von Scrum mit Nexus. URL: <https://www.scrum.org/resources/onlinenexus-guide>, abgerufen am 12.12.2022.
- Schwaber, Ken; Sutherland, Jeff (2020): The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game. URL: <https://scrumguides.org/scrum-guide.html>, abgerufen am 18.12.2022.
- The LeSS Company B.V. (2022): LeSS: More with LeSS. URL: https://less.works/less/framework?preferred_lang=de&setlang=true, abgerufen am 18.12.2022.