CONCEPTUALIZING DIGITAL RESILIENCE FOR AI-BASED INFORMATION SYSTEMS

Research in Progress

Schemmer, Max, Karlsruhe Institute of Technology, Germany, max.schemmer@kit.edu

Heinz, Daniel, Karlsruhe Institute of Technology, Germany, daniel.heinz@kit.edu

Baier, Lucas, Karlsruhe Institute of Technology, Germany, lucas.baier@kit.edu

Vössing, Michael, Karlsruhe Institute of Technology, Germany, michael.voessing@kit.edu

Kühl, Niklas, Karlsruhe Institute of Technology, Germany, niklas.kuehl@kit.edu

Abstract

The increasing volume of external shocks, such as the financial crisis or the COVID-19 pandemic, emphasizes the need for businesses to increase their resilience, i.e., a system's ability to reduce the impact or recover from such shocks quickly. In the past, information systems were often viewed as a source of vulnerability and complexity. In contrast, we conceptualize digital resilience—a form of resilience that is enabled through information systems by taking an integrated approach. In this work, we develop a framework for the design of digital resilience in AI-based information systems. Based on this framework, we conduct and evaluate an illustrative study addressing demand shocks in the airline industry. We, thereby, show the technical feasibility of concept drift detection and discuss why digital resilience must be designed holistically.

Keywords: Digital Resilience, Resilience, Concept Drift Detection, Information System Resilience.

1 Introduction

The COVID-19 pandemic has shown the vulnerabilities of our society and economy. For the 21st century, research predicts an increase in external shocks—environmental disasters, economic crises, and pandemics (Heeks and Ospina, 2019; Sarkar, Wingreen, and Ascroft, 2020; WEF, 2013). Additionally, the increasing complexity of global systems enlarges the impact of these shocks (Zolli and Healy, 2012). Generally, such shocks are difficult to predict and have long-lasting and severe consequences for businesses and people (Zolli and Healy, 2012). Researchers refer to these shocks as *black swan events* (Bicanic, Brahm, and Brea, 2020) and argue that their existence limits the effectiveness of many currently applied risk management approaches (Fiksel, 2015). Traditionally, risk management aims to prevent a crisis, or if a crisis is not preventable, reduce its impact (Hynes et al., 2020). However, this is particularly difficult for black swan events. In contrast, building *resilience* takes these black swans into account by proactively developing capabilities to cope with such shocks by either reducing the impact or minimizing the recovery time (Jüttner and Maklan, 2011).

While in the past, information systems (IS) were seen as a source of vulnerability and complexity (Beese et al., 2016; Patel, Graham, and Ralston, 2008; Schilling et al., 2017), contemporary research shows the potential to enhance the resilience of society and organizations through IS (Sakurai and Chughtai, 2020), which is defined as *digital resilience* (Fong Boh, Padmanabhan, and Viswanathan, 2020). The COVID-19 pandemic has shown numerous examples of how IS were able to enhance the resilience of our society and economy, be it through contact tracing apps (Ahmed et al., 2020), e-learning (Almaiah, Al-Khasawneh, and Althunibat, 2020) or remote working solutions (Kylili et al., 2020). Consequently, the pandemic emphasizes the need to make digital resilience a key priority of decision makers and should be included in their IS strategy.

Due to the recent advances in Artificial Intelligence (AI) (Lecun, Bengio, and Hinton, 2015) and the consequent rise of AI-based IS (Buxmann, Hess, and Thatcher, 2021) especially with regards to the COVID-19 pandemic—e.g., AI-based IS for drug discovery or diagnostic tests (Vaishya et al., 2020)—we focus in this article on enabling digital resilience in AI-based IS.

Sakurai and Chughtai (2020) stress that current research on resilience in IS lacks considering the complexity of systems. They argue that researchers often focus on individual parts of a system and exclude those most vulnerable from the discussion (Sakurai and Chughtai, 2020). Therefore, we argue that structured models or frameworks are required to capture the system's complexity. However, as of now, the phenomenon of digital resilience is missing a clear conceptualization in IS research (Heeks and Ospina, 2019). Heeks and Ospina (2019) state that most IS research does not provide concrete frameworks or models to understand resilience in IS and "therefore offers only a narrow and shallow understanding of resilience." (Heeks and Ospina, 2019, p. 73). For this reason, we initiate our quest for digital resilience with a conceptualization of digital resilience and develop a framework of digital resilience in AI-based IS. This framework defines necessary building blocks of digital resilience and depicts its dependencies and effect channels. To highlight our framework's value, we conduct an illustrative study for the first component of our framework, namely the AI system. In future research, we plan to address the framework's other components and levels. Our contribution is threefold: First, we provide the IS community with a framework of digital resilience. Second, we show our framework's utility by presenting an illustrative study. Third, we outline possible future work on digital resilience. Our framework can guide decision-makers on how to build digital resilience in their organization.

The remainder of this article is structured as follows: In Chapter 2, we summarize related work on resilience. In Chapter 3, we develop a framework for digital resilience in AI-based IS. Based on the framework, we conduct an initial illustrative study in Chapter 4. Then, we discuss our research and future work. Lastly, we summarize and conclude our work.

2 Related Work on Resilience

There are many different forms and views on resilience. In the following, we first outline the roots of resilience and, then, introduce existing research on IS resilience and digital resilience. We differentiate between the traditional view on resilience in IS research, which we call IS resilience, and the more recent concept of digital resilience. To fully grasp the particular characteristics of digital resilience, one also needs to take into account an IS's sub- and supra-systems. Sub-systems are precursor systems of the IS, whereas supra-systems are supported by the IS. While IS resilience is traditionally defined as the capacity of the system itself to cope with external shocks (Heeks and Ospina, 2019), digital resilience is enabling resilience in a supra-system of the IS, e.g., the resilience of the organization using the IS (Fong Boh, Padmanabhan, and Viswanathan, 2020). Nevertheless, both concepts of IS resilience and digital resilience are closely related, and IS resilience needs to be considered to enable digital resilience.

The general concept of resilience is rooted in two research streams: The ecologist Holling defined resilience as the robustness of an ecological system describing its survivability (Holling, 1973). In contrast, developmental psychologist Werner (1982) examines factors of personal resilience that help children to cope with psychological risk factors. Contemporary research adopts the concept of resilience in many different fields, such as ecology, engineering, sociology, psychology, economics, and organizational analysis (Heckmann, Comes, and Nickel, 2015). In this work, we adopt a system approach similar to Holling (1973) and follow-up research (Folke, 2006). Following this system approach, Hollnagel, Woods, and Leveson (2006) define resilience as a system property that can predict, recognize, anticipate, and defend against adversarial shocks. Besides lacking a common definition, resilience can be described with different forms and levels, e.g., enterprise resilience (Erol, Sauser, and Mansouri, 2010), business resilience (Avery and Bergsteiner, 2011), supply chain resilience (Heckmann, Comes, and Nickel, 2015) or cyber resilience (Björck et al., 2015). To provide a mutual understanding for our work, we define resilience as the *property of a system to reduce the negative impact of large exogenous shocks or to recover from such shocks quickly.*

So far, IS research examined multiple concepts related to resilience, such as disaster recovery (Wong, Monaco, and Sellaro, 1994), business continuity management (Gibb and Buchanan, 2006; Hecht, 2002), and IS risk management (Finne, 2000). However, there is little work specifically studying IS resilience (Heeks and Ospina, 2019). In 2019, Heeks and Ospina conducted a structured literature review (SLR) of articles addressing resilience in IS research. The authors identify 30 relevant articles and classify them into three categories, the input system, the "IS" itself, and the output system. Based on the SLR, the authors develop a framework for IS resilience and evaluate it in a field study in developing countries. Their SLR shows that IS research mainly defines resilience as a system property, which is in line with the definition we use in this paper. Furthermore, they identify one article that provides a clear framework of IS resilience: Erol, Sauser, and Mansouri (2010) define IS resilience through four attributes—vulnerability, flexibility, adaptability, and agility. Following this attribute-based development of a framework, which has also shown to be effective in other resilience research streams (Florio, 2013; Hollnagel, Woods, and Leveson, 2006), Heeks and Ospina (2019) develop an adopted set of attributes based on additional resilience literature—robustness, self-organization, learning, redundancy, rapidity, scale, diversity, and flexibility, and equality. Sarkar, Wingreen, and Ascroft (2020) build upon the framework of Heeks and Ospina (2019) and also develop a set of attributes for the planning and implementation of resilient IS. Furthermore, Sarkar, Wingreen, and Ascroft (2020) also emphasize the importance of resilience for IS strategy and governance.

While in the past, IS resilience was primarily seen as an attribute of the isolated IS (Heeks and Ospina, 2019), the COVID-19 pandemic strengthens the focus on IS output resilience due to the need for all potential sources of resilience. More contemporary research defines this IS output resilience as digital resilience (Fong Boh, Padmanabhan, and Viswanathan, 2020; Raj, Sundararajan, and You, 2020). In their call for papers Fong Boh, Padmanabhan, and Viswanathan (2020, p. 1) describe digital resilience as follows: "digital resilience [...] refer[s] to the phenomena of designing, deploying, and using information systems to quickly recover from or adjust to major disruptions from exogenous shocks." For example, Raj, Sundararajan, and You (2020) analyze how digital platforms can increase business resilience by providing a continuous connection to customers, and Rai (2020) discusses the building of digital resilience through public health surveillance systems. In this work, we explicitly focus on AI-based IS (Buxmann, Hess, and Thatcher, 2021), due to their importance for society that was especially highlighted during the COVID-19 pandemic. AI-based IS were for example used to develop vaccines (Arshadi et al., 2020), create diagnostic tests (Vaishya et al., 2020), or predict case numbers (Bragazzi et al., 2020).

After reviewing existing literature on resilience, IS resilience, and digital resilience, to the best of our knowledge, the only framework which includes the phenomena of digital resilience can be found in Erol, Sauser, and Mansouri (2010). However, their framework mainly focuses on extended enterprise resilience. They use IS as a means to reach connectivity between the enterprises. In contrast, we build a specifically tailored framework for digital resilience in AI-based IS.

3 Digital Resilience in AI-based Information Systems

We acknowledge the rigorous work of Heeks and Ospina (2019) and build on top of their SLR. To extend their work, we conducted a central literature review (Cooper, 1988). Our literature review results were then used to extract relevant components for our framework and define dependencies. Our framework (depicted in Figure 1) is based on three research foundations: system theory (Linkov and Trump, 2019), the concept of IS input and output systems developed by Heeks and Ospina (2019), and the work of Erol, Sauser, and Mansouri (2010) who discuss resilience-building attributes of systems.

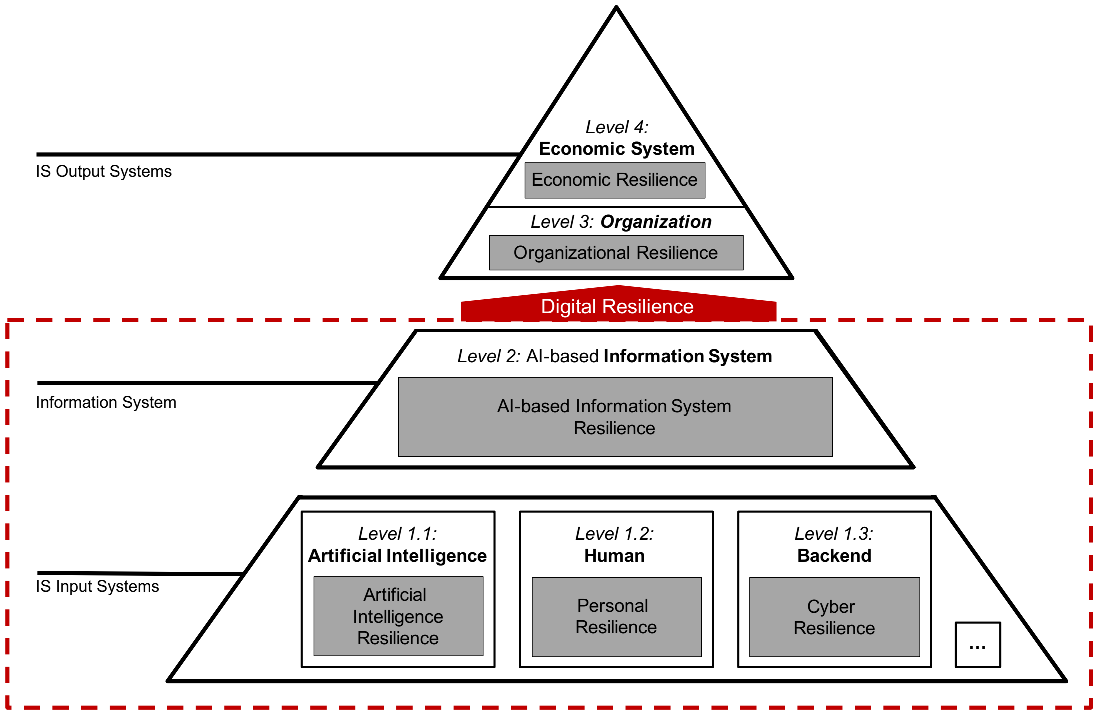

Figure 1: Framework for digital resilience in AI-based information systems.

As discussed in the previous section, resilience is often viewed as a system property and must be designed holistically (Erol, Sauser, and Mansouri, 2010). For this purpose, system theory provides three steps for conceptualizing resilience in systems (Linkov and Trump, 2019): (1) an understanding of how the considered system interfaces with other related systems, (2) the decomposition of a system to understand its sub-systems and supra-systems and (3) an understanding of resilience's cascading effect.

To model the interaction between IS and other systems, we follow the tripartite system approach from Heeks and Ospina (2019)—the IS input systems, the IS, and the IS output systems, which are discussed in more detail in the following paragraph. The resilience of a system is always directly related to the resilience of its sub- and supra-systems (Müller and Zinth, 2014; Walker et al., 2004). Furthermore, we differentiate between direct and indirect effects between these systems. Direct effects are created through explicit design to enable resilience on a supra-system. Indirect effects are created through cascading effects of resilience.

IS Input Systems: Maedche et al. (2019) define three major sub-systems of an AI-based IS, applying a socio-technical system view—the human, the technology, and the task. For our work, we focus on technology and the human but acknowledge the importance of the task. We differentiate the technology into two components, the backend system and the AI system leading into three key input systems—the human system, the AI system, and the backend system. However, other IS input systems can exist and may have an effect on digital resilience.

Regarding the AI system, we particularly focus on machine learning-based based systems, i.e., self-learning systems in contrast to expert systems (Russell and Norvig, 2002). Related work defines resilience in AI for situations where adversaries attack AI models, e.g., through data modified with adversarial intention (Kumar and Mehta, 2017). Furthermore, typical shocks affecting an AI algorithm are related to the database, e.g., data distribution shifts, missing values, and anomalies (Bohlke-Schneider, Kapoor, and Januschowski, 2020). These shocks can lead to significant loss of performance or even in life-threatening scenarios.

Regarding the backend system, there exists a lot of work on building cyber resilience, for example, against distributed denial-of-service (DDOS) attacks. As an example, cyber resilience can be build by providing redundancy or fail-safe mechanisms (Clark, 2005). A renowned practical implementation is the "Chaos Monkey" framework from Netflix, which actively injects failures into a production network system to increase its resilience (Bennett and Tseitlin, 2012). Netflix acknowledges the immense complexity of modern IS that makes it impossible to test their IS in a test environment (Basiri et al., 2016). For this reason, they test possible failures controlled in the production environment, which ultimately leads to more cyber resilience.

Since a crisis can severely affect humans in their behavior, they need to be proactively prepared to cope with stress and uncertainty. Cho, Mathiassen, and Robey (2007) show the influence of personal resilience on the adaption of an IS and long-term usage. Their findings suggest that, even though personal resilience has a positive effect on IS's initial adoption, it can harm long-term sustainability. Therefore, taking the human system into account is an integral part of successfully designing an IS for digital resilience.

AI-based Information System: As summarized in Chapter 2, IS resilience is the ability of an IS to cope with external shocks. It can be seen as a sub-system of the larger organizational resilience (Sarkar, Wingreen, and Ascroft, 2020). In crises, IS are seen as one of the most sensitive sub-systems of an organization because they affect the entire organizational ecosystem (Maurer and Lechner, 2014). AI-based IS are a subset of Intelligent Decision Support Systems that incorporate methods from the artificial intelligence field (Arnott and Pervan, 2012) and expand the input systems by the AI system.

IS Output Systems: Similar to IS input systems, there exist several IS output systems. In our framework, we focus on organizational resilience and the concept of economic resilience, which takes the resilience of the larger economic system into account. Other possible output systems, may be environmental resilience (Okvat and Zautra, 2011) and ecological resilience (Gunderson, 2000).

Research on organizational resilience, which has been broadly discussed in management research throughout the past two decades (Aldea et al., 2020), suggests resilient IS services as one key requirement for building organizational resilience (Sarkar, Wingreen, and Ascroft, 2020). By considering the economic system in our framework, we acknowledge the fact that building digital resilience through AI-based IS also has a large-scale impact on coping with large economic shocks, such as the COVID-19 pandemic. Economic resilience is defined as the "ability of an economy to withstand or recover from the effects of [...] shocks" (Briguglio et al., 2009, p. 1).

Erol, Sauser, and Mansouri (2010) define digital resilience as a function of vulnerability, flexibility, adaptability, and agility. A reduction of the vulnerability (i.e., the probability of disruptions) increases resilience (Erol, Sauser, and Mansouri, 2010). Flexibility is the ability to adapt to changes in an efficient manner (Erol, Sauser, and Mansouri, 2010). Adaptability is the capacity to adapt and recover (Erol, Sauser, and Mansouri, 2010). Lastly, agility is the ability to respond to changes quickly (Erol, Sauser, and Mansouri, 2010). We argue that these attributes of resilience need to be pursued across all levels of the framework. Building on this conceptual framework, we formally holistically define digital resilience: *Digital resilience is the property of an IS to increase the resilience of IS output systems while satisfying a sufficient resilience on sub-systems.* Following this, the main difference to traditional IS resilience is that digital resilience is not about the resilience of the IS itself, but the effect of an IS on an IS output system. To illustrate our framework, we will discuss two examples—one with indirect digital resilience and one with direct digital resilience:

To illustrate the indirect effect, let us assume that the overall ecosystem is perceiving a large exogenous shock, the COVID-19 pandemic. We focus on a specific organizational task—demand forecasting. This shock has an impact on multiple levels: On the first level, the data distribution might change, leading to worse predictive power of the implemented AI models. By using concepts to address this issue, resilience can be built, and the performance recovered. However, a resilient AI system does neither imply a resilient AI-based IS nor a resilient organization. To illustrate this, even though the system might be perfectly performing, the overarching information system had also experienced a shock and is now suffering from a loss of trust. After recalibrating the trust level, the AI system and the IS should be resilient. Since research shows that data-driven decision making increases organizational resilience (Barker et al., 2017), we can, thereby, indirectly build digital resilience.

In contrast to the indirect effect, direct digital resilience is built by explicitly designing IS to build resilience in a supra-system. Examples of digital resilient IS during the COVID-19 pandemic are the analysis of CT images, tracing apps, the prediction of the survival of patients, developing vaccines, and estimating unobserved cases (Vaid, Cakan, and Bhandari, 2020). The sub-systems' resilience is here still a necessary prerequisite for successful digital resilience. Considering contact tracing apps as an example, a key IS-input system might be its backend system: The best tracing app, applying flawless AI algorithms, can not positively influence a society's resilience when the app breaks down facing too many users due to a lack of scalability in its backend system.

These two examples highlight the need for sufficient sub-system resilience to build digital resilience with an AI-based IS. Therefore, in the following chapter, we conduct an illustrative study to explore how to build sub-system resilience. We focus on the common denominator of all AI-based IS, the AI system, and suggest an approach to build resilience in AI systems.

4 Illustration: AI Resilience as a Prerequisite of Digital Resilience

As already discussed, digital resilience in AI-based IS needs to build on resilience-building mechanisms in the respective sub-systems (cf. Figure 1). Therefore, we initiate our research by focusing on the AI sub-system. Effectively operating AI-based IS can be severely disturbed and impeded by exogenous shocks leading to huge performance losses. These shocks might lead to changes in the input data on which AI models heavily rely to identify patterns and suggest actions. One example for such AI systems are time-series predictions for demand forecasts that rely on past observations to predict future values.

The COVID-19 pandemic has led to an increased demand for *adaptive* forecasting concepts (Becdach et al., 2020). In general, a critical shock for demand forecasting systems can be triggered by both demand reduction as well as demand increases. For example, the demand for household supplies and basic food (e.g., toilet paper, flour and pasta) increased, whereas purchases in tourism severely decreased (Becdach et al., 2020). The airline industry is significantly affected by the COVID-19 pandemic (Maneenop and Kotcharin, 2020). Airlines need to make hundreds of operational decisions like which routes to fly, what crew size is required, or how many meals should be ordered (Sneader, Singhal, and Sternfels, 2020, p. 16). To steer these operational decisions, they need sophisticated demand forecasts.

In AI research, the shift in data distributions over time due to exogenous shocks is called *concept drift* (Widmer and Kubat, 1996). It is generally assumed that black swan events are not predictable. However, even though these shocks are not predictable, at least their realization should be detected in short time. As Erol, Sauser, and Mansouri (2010) suggest that systems need the ability to adapt to exogenous shocks, we argue that this can be achieved by applying the knowledge body of concept drift detection (CDD). CDD enables quick and reliable detection of black swans by detecting changes in the data distribution based on statistical measures (Widmer and Kubat, 1996). In competitive markets, a fast reaction time is crucial to achieve competitive advantages (Sheffi and Rice Jr, 2005). Beyond detecting the initial shock, CDD can support against the initial turbulence after the shock (i.e., if the demand has a higher variance in crises). Furthermore, it is necessary to not only detect but also handle concept drifts (Gama et al., 2014). The traditional handling strategies are model retraining and model updating. However, we additionally suggest implementing hybrid intelligence, which is the combination of human and artificial intelligence (Dellermann et al., 2019). Specifically, we suggest combining AI's particular strengths, namely extracting knowledge from large data sets, with human intelligence (i.e., developing creative solutions in crises). Human intelligence can then be fostered with structural methods like scenario analysis (Hsia et al., 1994). However, in this work, we focus on CDD and test the influence on AI resilience.

To illustrate and evaluate CDD as a means to build resilience in an AI system, we apply it to the jet fuel demand in the U.S.[1]. Since the jet fuel demand data exhibit strong seasonal patterns, we apply seasonal differencing to remove seasonal effects. Thereby, monotonic trends are still included in the data, which

[1] `https://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=WKJUPUS2&f=W`

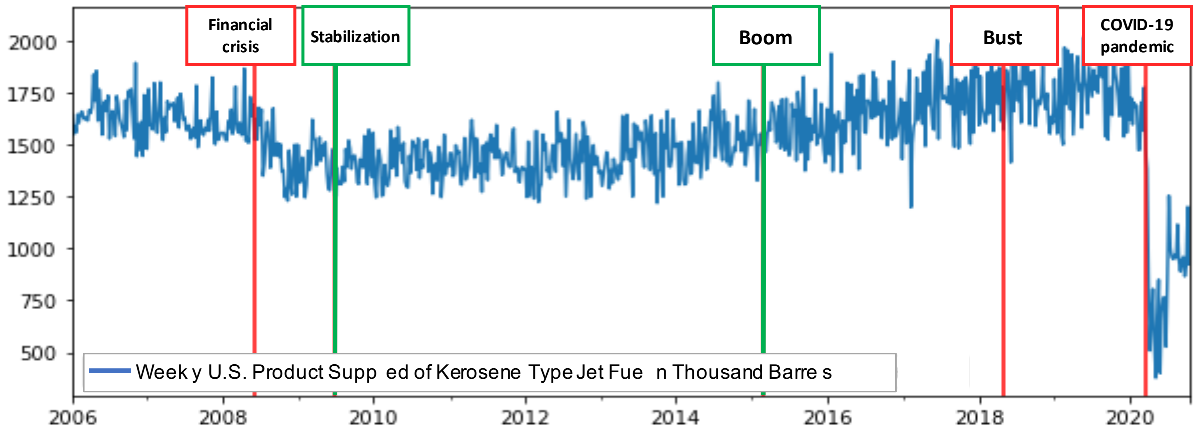

Figure 2: Concept drifts of jet fuel demand.

Data set	Approach	MSE
Jet fuel demand	Baseline	35,663
Jet fuel demand	Concept drift handling	**31,778**
Airline passenger	Baseline	20,693
Airline passenger	Concept drift handling	**12,671**

Table 1: Evaluation of Concept Drift Handling.

we want to detect with CDD. As a prediction model, we use simple exponential smoothing. Among the available drift detection algorithms, we choose the Page-Hinkley algorithm (Page, 1954), one of the most popular algorithms (Demšar and Bosnić, 2018).

The calibration of the Page-Hinkley algorithm is a challenging task because if the detection threshold λ is set too low, outliers might incorrectly be detected as concept drift. In contrast, a high value for λ is associated with the risk of missing relevant concept drifts. Therefore, we perform pretests on a validation set and finally set the threshold for change detection to $\lambda = 300000$. Figure 2 visualizes the time series as well as detected drifts of the jet fuel demand data set. We detected five different concept drifts, two obvious drifts, the financial crisis (2008) and the COVID-19 pandemic (2020), and three additional drifts. The first additional drift occurred in mid-2009 when the downwards trend of the financial crisis stabilized. The second drift visualizes a Boom phase at the beginning of 2015, which inflected in 2018, leading to the third concept drift. As a baseline, we assume that the forecast is retrained twice a year since companies need to balance the cost of retraining and the validity of their algorithms. We compare this baseline with a CDD approach followed by additional retrains after detection. To compare the baseline with our concept drift approach, we measure the mean squared error (MSE). To generalize our evaluation, we apply the steps above on a second data set covering the air traffic passenger demand in the U.S.[2] Table 1 visualizes our results. Our evaluation indicates that the approach, including concept drift detection, by far outperforms our baseline, proving the technical feasibility.

Referring to the framework of Erol, Sauser, and Mansouri (2010), adaptability is a key property of resilient systems. Through CDD, we can build the AI-based IS as a learning agent (Kühl et al., 2019) that automatically adapts, and thus, is more resilient. While in some industries, the detection of a concept drift might be easy and can be conducted by humans, many industries need to forecast many different supplied goods. In these cases, the pure number of goods to be predicted makes manual detection not feasible.

[2] `https://www.transtats.bts.gov/TableInfo.asp`

5 Research Agenda

In the research at hand, we conducted a first illustrative study for one component of AI-based IS input systems—the AI system. Much work needs to be done on other input systems and consequent levels and their interaction effects. Following our framework's levels (see Figure 1), we propose a research agenda for digital resilience in AI-based IS.

In a subsequent study, we will further examine AI-based IS resilience with our first study results as a foundation. Exogenous shocks do not only influence the data available to the AI system but, for example, also the human operating the AI system. This interplay between human and AI systems (i.e., hybrid intelligence (Dellermann et al., 2019)) poses an exciting yet under-researched situation. For example, the initial performance loss, which, in case of black swan events, cannot be prevented, can lead to a loss of trust of the human in the system. For this reason, further studies should explore the re-calibration of trust after large exogenous shocks. Research has shown that explainable artificial intelligence (XAI) can be a valid method to support trust calibration (Lai and Tan, 2019) and even discussed the concept of explainable concept drift detection (Hinder and Hammer, 2020). This technique could allow communicating the fact that performance is temporally affected to analysts, creating transparency, and thereby, enabling trust calibration.

With results of the IS input system and AI-based IS at hand, a third study should evaluate the empirical influence of digital resilience for the IS output systems. Specifically, the focus on organizational and economic resilience needs to be analyzed in more detail. First case studies have shown success in increasing the resilience of these systems (Rai, 2020; Raj, Sundararajan, and You, 2020). However, a generalized and empirical analysis is yet missing. By analyzing COVID-19-related digital resilience, we aim to provide a profound analysis in the future. Overall, by guiding decision-makers on their path towards building digital resilience, our research aims to support the economy and society to navigate through turbulent times. Generalized design knowledge could be successively built that allows researchers and practitioners to prepare not only against the COVID-19 pandemic but against all kinds of external shocks.

6 Conclusion

In this work, we conceptualize the term *digital resilience* and develop a framework for digital resilience in AI-based IS. Based on this framework, we conducted a first illustrative study to discuss possibilities to build the AI system's necessary resilience and evaluate it within two cases. The study demonstrated the technical feasibility of applying so-called *concept drift detection* to enable resilience on the IS input level, more precisely, AI system resilience. However, this is only the first of many steps to create digital resilience since cascading effects need to be enforced through the complete chain of interrelated sub- and supra-systems. Therefore, future work needs to consider and analyze other resilience levels, particularly the AI-based IS level and the IS output system level.

References

Ahmed, N., R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha (2020). "A survey of covid-19 contact tracing apps." *IEEE Access* 8, 134577–134601.

Aldea, A., E. Vaicekauskaitė, M. Daneva, and J. P. S. Piest (2020). "Assessing Resilience in Enterprise Architecture: A Systematic Review." In: *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)*. IEEE, pp. 1–10.

Almaiah, M. A., A. Al-Khasawneh, and A. Althunibat (2020). "Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic." *Education and Information Technologies* 25, 5261–5280.

Arnott, D. and G. Pervan (2012). “Design science in decision support systems research: An assessment using the Hevner, March, Park, and Ram Guidelines.” *Journal of the Association for Information Systems* 13 (11), 1. ISSN: 1536-9323.

Arshadi, A. K., J. Webb, M. Salem, E. Cruz, S. Calad-Thomson, N. Ghadirian, J. Collins, E. Diez-Cecilia, B. Kelly, H. Goodarzi, et al. (2020). “Artificial intelligence for COVID-19 drug discovery and vaccine development.” *Frontiers in Artificial Intelligence* 3.

Avery, G. C. and H. Bergsteiner (2011). “Sustainable leadership practices for enhancing business resilience and performance.” *Strategy & Leadership*.

Barker, K., J. H. Lambert, C. W. Zobel, A. H. Tapia, J. E. Ramirez-Marquez, L. Albert, C. D. Nicholson, and C. Caragea (2017). “Defining resilience analytics for interdependent cyber-physical-social networks.” *Sustainable and Resilient Infrastructure* 2 (2), 59–67. ISSN: 23789697.

Basiri, A., N. Behnam, R. De Rooij, L. Hochstein, L. Kosewski, J. Reynolds, and C. Rosenthal (2016). “Chaos engineering.” *IEEE Software* 33 (3), 35–41.

Becdach, C., B. Brown, F. Halbardier, B. Henstorf, and R. Murphy (May 2020). *Rapidly forecasting demand and adapting commercial plans in a pandemic*. URL: https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/rapidly-forecasting-demand-and-adapting-commercial-plans-in-a-pandemic.

Beese, J., S. Aier, K. Haki, and P. Aleatrati Khosroshahi (2016). “Drivers and Effects of Information Systems Architecture Complexity: A Mixed-Methods Study.”

Bennett, C. and A. Tseitlin (2012). *Netflix: Chaos monkey released into the wild. netflix tech blog*.

Bicanic, S., C. Brahm, and C. Brea (Apr. 2020). *What to Do Now That Your Demand Forecast Is Wrong*. URL: https://www.bain.com/insights/what-to-do-when-your-demand-forecast-is-wrong/.

Björck, F., M. Henkel, J. Stirna, and J. Zdravkovic (2015). “Cyber resilience–fundamentals for a definition.” In: *New contributions in information systems and technologies*. Springer, pp. 311–316.

Bohlke-Schneider, M., S. Kapoor, and T. Januschowski (2020). “Resilient Neural Forecasting Systems.” *Proceedings of the 4th Workshop on Data Management for End-To-End Machine Learning, DEEM 2020 - In conjunction with the 2020 ACM SIGMOD/PODS Conference*.

Bragazzi, N. L., H. Dai, G. Damiani, M. Behzadifar, M. Martini, and J. Wu (2020). “How big data and artificial intelligence can help better manage the COVID-19 pandemic.” *International journal of environmental research and public health* 17 (9), 3176.

Briguglio, L., G. Cordina, N. Farrugia, and S. Vella (2009). “Economic vulnerability and resilience: concepts and measurements.” *Oxford development studies* 37 (3), 229–247.

Buxmann, P., T. Hess, and J. B. Thatcher (2021). “AI-Based Information Systems.” *Business & Information Systems Engineering* 63 (1), 1–4. ISSN: 1867-0202.

Cho, S., L. Mathiassen, and D. Robey (2007). “Dialectics of resilience: a multi–level analysis of a telehealth innovation.” *Journal of Information Technology* 22 (1), 24–35.

Clark, T. (2005). *Storage virtualization: technologies for simplifying data storage and management*. Addison-Wesley Professional.

Cooper, H. M. (1988). “Organizing knowledge syntheses: A taxonomy of literature reviews.” *Knowledge in Society* 1 (1), 104–126. ISSN: 08971986. DOI: 10.1007/BF03177550.

Dellermann, D., P. Ebel, M. Söllner, and J. M. Leimeister (2019). “Hybrid intelligence.” *Business & Information Systems Engineering* 61 (5), 637–643.

Demšar, J. and Z. Bosnić (2018). “Detecting concept drift in data streams using model explanation.” *Expert Systems with Applications* 92, 546–559.

Erol, O., B. J. Sauser, and M. Mansouri (2010). “A framework for investigation into extended enterprise resilience.” *Enterprise Information Systems* 4 (2), 111–136. ISSN: 17517575.

Fiksel, J. (2015). “From risk to resilience.” In: *Resilient by design*. Springer, pp. 19–34.

Finne, T. (2000). “Information systems risk management: key concepts and business processes.” *Computers & Security* 19 (3), 234–242.

Florio, V. D. (2013). “On the constituent attributes of software and organizational resilience.” *Interdisciplinary Science Reviews* 38 (2), 122–148.
Folke, C. (2006). “Resilience: The emergence of a perspective for social–ecological systems analyses.” *Global environmental change* 16 (3), 253–267.
Fong Boh, W., B. Padmanabhan, and S. Viswanathan (2020). “Call for Papers MISQ Special Issue on Digital Resilience Guest Editors Motivation and Objectives for the Special Issue,” 1–3.
Gama, J., I. Žliobaitė, A. Bifet, M. Pechenizkiy, and A. Bouchachia (2014). “A survey on concept drift adaptation.” *ACM computing surveys (CSUR)* 46 (4), 1–37.
Gibb, F. and S. Buchanan (2006). “A framework for business continuity management.” *International journal of information management* 26 (2), 128–141. ISSN: 0268-4012.
Gunderson, L. H. (2000). “Ecological resilience—in theory and application.” *Annual review of ecology and systematics* 31 (1), 425–439.
Hecht, J. A. (2002). “Business continuity management.” *Communications of the Association for Information Systems* 8 (1), 30.
Heckmann, I., T. Comes, and S. Nickel (2015). “A critical review on supply chain risk - Definition, measure and modeling.” *Omega (United Kingdom)* 52, 119–132. ISSN: 03050483.
Heeks, R. and A. V. Ospina (2019). “Conceptualising the link between information systems and resilience: A developing country field study.” *Information Systems Journal* 29 (1), 70–96. ISSN: 13652575.
Hinder, F. and B. Hammer (2020). “Counterfactual Explanations of Concept Drift.” arXiv: `2006.12822`.
Holling, C. S. (1973). “Resilience and stability of ecological systems.” *Annual review of ecology and systematics* 4 (1), 1–23. ISSN: 0066-4162.
Hollnagel, E., D. D. Woods, and N. Leveson (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd. ISBN: 075468136X.
Hsia, P., J. Samuel, J. Gao, D. Kung, Y. Toyoshima, and C. Chen (1994). “Formal approach to scenario analysis.” *IEEE Software* 11 (2), 33–41.
Hynes, W., B. Trump, P. Love, and I. Linkov (2020). “Bouncing forward: a resilience approach to dealing with COVID-19 and future systemic shocks.” *Environment Systems and Decisions* 40 (2), 174–184. ISSN: 21945411.
Jüttner, U. and S. Maklan (2011). “Supply chain resilience in the global financial crisis: An empirical study.” *Supply Chain Management* 16 (4), 246–259. ISSN: 13598546.
Kühl, N., M. Goutier, R. Hirt, and G. Satzger (2019). “Machine learning in artificial intelligence: Towards a common understanding.” *HICSS 2019*.
Kumar, A. and S. Mehta (2017). “A Survey on Resilient Machine Learning.” arXiv: `1707.03184`. URL: `http://arxiv.org/abs/1707.03184`.
Kylili, A., N. Afxentiou, L. Georgiou, C. Panteli, P.-Z. Morsink-Georgalli, A. Panayidou, C. Papouis, and P. A. Fokaides (2020). “The role of Remote Working in smart cities: lessons learnt from COVID-19 pandemic.” *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, 1–16.
Lai, V. and C. Tan (2019). “On human predictions with explanations and predictions of machine learning models: A case study on deception detection.” *FAT* 2019 - Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency*, 29–38. arXiv: `1811.07901`.
Lecun, Y., Y. Bengio, and G. Hinton (2015). “Deep learning.” *Nature* 521 (7553), 436–444. ISSN: 14764687. DOI: `10.1038/nature14539`.
Linkov, I. and B. D. Trump (2019). *The science and practice of resilience*. Springer. ISBN: 303004565X.
Maedche, A., C. Legner, A. Benlian, B. Berger, H. Gimpel, T. Hess, O. Hinz, S. Morana, and M. Söllner (2019). “AI-based digital assistants.” *Business & Information Systems Engineering* 61 (4), 535–544. ISSN: 1867-0202.
Maneenop, S. and S. Kotcharin (2020). “The impacts of COVID-19 on the global airline industry: An event study approach.” *Journal of Air Transport Management* 89, 101920.
Maurer, F. and U. Lechner (2014). “From Disaster Response Planning to e-Resilience: A Literature Review.” In: *Bled eConference*, p. 32.

Müller, C. and C.-P. Zinth (2014). *Managementperspektiven für die Zivilgesellschaft des 21. Jahrhunderts: Management als Liberal Art*. Springer-Verlag. ISBN: 3658025239.

Okvat, H. A. and A. J. Zautra (2011). "Community gardening: A parsimonious path to individual, community, and environmental resilience." *American journal of community psychology* 47 (3-4), 374–387.

Page, E. S. (1954). "Continuous inspection schemes." *Biometrika* 41 (1/2), 100–115.

Patel, S. C., J. H. Graham, and P. A. Ralston (2008). "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements." *International Journal of Information Management* 28 (6), 483–491.

Rai, A. (2020). "The COVID-19 pandemic: Building resilience with IS research." *MIS Quarterly: Management Information Systems* 44 (2), III–VIII. ISSN: 21629730.

Raj, M., A. Sundararajan, and C. You (2020). "COVID-19 and Digital Resilience: Evidence from Uber Eats." *SSRN Electronic Journal*, 1–26. ISSN: 1556-5068. arXiv: 2006.07204.

Russell, S. and P. Norvig (2002). "Artificial intelligence: a modern approach."

Sakurai, M. and H. Chughtai (2020). "Resilience against crises: COVID-19 and lessons from natural disasters." *European Journal of Information Systems* 00 (00), 1–10. ISSN: 14769344.

Sarkar, A., S. Wingreen, and J. Ascroft (2020). "Towards a Practice-based View of Information Systems Resilience Using the Lens of Critical Realism." *Proceedings of the 53rd Hawaii International Conference on System Sciences* 3, 6184–6193.

Schilling, R., J. Beese, K. Haki, S. Aier, and R. Winter (2017). "Revisiting the impact of information systems architecture complexity: a complex adaptive systems perspective."

Sheffi, Y. and J. B. Rice Jr (2005). "A supply chain view of the resilient enterprise." *MIT Sloan management review* 47 (1), 41.

Sneader, K., S. Singhal, and B. Sternfels (Sept. 2020). *What now? Decisive actions to emerge stronger in the next normal*.

Vaid, S., C. Cakan, and M. Bhandari (2020). "Using machine learning to estimate unobserved COVID-19 infections in North America." *The Journal of bone and joint surgery. American volume*.

Vaishya, R., M. Javaid, I. H. Khan, and A. Haleem (2020). "Artificial Intelligence (AI) applications for COVID-19 pandemic." *Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 14 (4), 337–339.

Walker, B., C. S. Holling, S. R. Carpenter, and A. Kinzig (2004). "Resilience, adaptability and transformability in social–ecological systems." *Ecology and society* 9 (2). ISSN: 1708-3087.

WEF (2013). "Global risks 2013. Geneva: World Economic Forum."

Werner, E. E. (1982). "Vulnerable but invincible." *A longitudinal study of resilient children and youth*.

Widmer, G. and M. Kubat (1996). "Learning in the presence of concept drift and hidden contexts." *Machine learning* 23 (1), 69–101.

Wong, B. K., J. A. Monaco, and C. L. Sellaro (1994). "Disaster recovery planning: suggestions to top management and information systems managers." *Journal of Systems Management* 45 (5), 28.

Zolli, A. and A. M. Healy (2012). *Resilience: Why things bounce back*. Hachette UK.