Design of a Business Resilience Model for Industry 4.0 Manufacturers

Completed Research Full Papers

Marcel Morisse
University of Hamburg
Germany
morisse@informatik.uni-hamburg.de

Corvin Prigge
Deloitte GmbH
Wirtschaftsprüfungsgesellschaft
cprigge@deloitte.de

Abstract

For Industry 4.0, characterized by a high level of complexity due to the network integration of productions, manufacturers have to take radical steps to transform their organizations enabling intelligent industrial operations. As this transformation is accompanied by unforeseen risks and extreme events, organization must build up resilience to withstand them. This research paper develops a practice-oriented model of business resiliency for Industry 4.0 manufacturers. A literature research was performed to illustrate the absence of research in information systems (IS). For a better understanding of the challenges organizations face, a study among 15 experts from Europe was performed. The obtained challenges, requirements and solutions were clustered and used to develop a resilience model. The model is divided into six major components which are used to achieve six resilience characteristics. The developed model enables organizations to get a holistic and practical overview about the transformation they face while adopting to Industry 4.0.

Keywords

Industry 4.0, Resilience, Model, Design

Introduction

Industry 4.0, describing the intensive interconnectedness between IT and OT enabling intelligent operations, significantly disrupts existing value chains on an international scale. Until 2020, 85% of companies will have implemented Industry 4.0 solutions (Lee et al. 2014). The rise of Industry 4.0 "is taking place through the convergence of the global industrial system with the power of advanced computing, analytics, low-cost sensing and new levels of connectivity permitted by the internet" (Evans and Annunziata 2012, p. 3). Industry 4.0 or synonyms like the Industrial Internet of Things (IIoT) include concepts on a technical level due to the integration of cyber-physical-systems (CPS) but also on organizational levels. The majority of established production processes change towards highly flexible, interconnected and self-optimizing networks. Organizations are able to enhance their competitiveness, reduce their time-to-market, enhance speed and efficiency and therefore reduce costs and boost productivity. Due to this evolutionary process, unexpected and low probability - high impact events occur which may lead to a potential damage for organizations and supply chains. Resilience is the ability to persist in the face of substantial changes in the environment (Acquaah et al. 2011). Industry 4.0 organizations have to withstand these events with high resiliency.

Extreme events lead to financial losses, reputation damage or can throw organizations out of business. Especially in the changing environment of Industry 4.0, it is important for organizations to stay resilient, as continuous and unpredictable changes can stretch organizations to the breaking point, leaving them vulnerable and more susceptible to failure (Ismail et al. 2011). These topics are rather new for organizations, so the research community is only beginning their research on Industry 4.0. Especially the topic of resilience within Industry 4.0 has not been examined by the IS research community. Organizations are currently transforming. Those which are not undergoing this transformation will most likely not be competitive in the future. This paper asks the question, how Industry 4.0 organization can build up resiliency to handle unforeseen extreme events and support their organizational transformation.

The proposed resilience model is based on the design science paradigm from Hevner et al. (2004). The input comes from a literature research and a qualitative study among experts from manufacturers and a consultancy. It was decided to develop a practice-oriented model, as a model could be generic enough to cover more than one specific industry, but was also specific enough for the chosen context. The developed model supports organizations to identify challenges within the transformation to Industry 4.0 as well as to establish resiliency in a fast-moving environment. This paper begins by describing the context Industry 4.0 and defining resilience. We then describe our methodology, before presenting our model and a discussion of their implications for understanding resilience in Industry 4.0.

Context Industry 4.0

The term Industry 4.0 is used for the fourth industrial revolution based on cyber-physical-systems (Lee et al. 2014)], enabling intelligent industrial operations including data analytics, by converging the global industrial ecosystem, manufacturing, computer science and sensoring and ubiquitous network connectivity (Industrial Internet Consortium 2015). This so called 4th industrial revolution is characterized by a high level of complexity and a complete network integration of product and production processes (Dombrowski and Wagner 2014). The product life cycle will be increasingly oriented towards customer demands, e.g. mass personalization of products. CPS are transforming the massive data volume systematically into information, which makes invisible patterns of degradation and inefficiencies visible and supports optimal decision making (Lee et al. 2015). This data is available in real-time so decision making is based on transparent information, helping to improve actions on down-times, disruptions and global optimization. Production processes can be optimized among the entire value chain bringing potential in reducing cost and improving effectivity and efficiency. Industry 4.0 is based on the emergence of new technologies and a strong horizontal and vertical integration.

Production changes in order to meet demands for more individuality and shorter delivery times (Matt et al. 2015). The change of centralized large production plants towards decentralized smaller production units will continue as these structures are of higher flexibility to reflect local customer demands, lower logistics costs, and shorten delivery times (Matt et al. 2015). The change in business models, such as the offering of manufacturing related services is of risk for manufacturers (Nordas and Kim 2013). Risks increase as organizations often have to change on an organizational and technological scale.

Defining Resilience

The term resilience is used in ecosystems, economics and engineering. It can be broadly defined as maintaining positive adjustments under challenging conditions (Ismail et al. 2011) of a person, an organization or an ecosystem (Fiksel 2006). On an organizational level, resilience is understood as "the ability of a firm to persist in the face of substantial changes in the business and economic environment and/or the ability to withstand disruptions and catastrophic events" (Acquaah et al. 2011, p. 5528). Common to all definition of resiliency is the occurrence of an extreme or disruptive event. An extreme or disruptive event are low probability - high impact events, events which may not be anticipated and mitigated in a traditional manner (Weick 1988). Extreme events can lead to loss in market share, financial loss, loss of reputation, declined shareholder value or lost/missed marked opportunities. Organizational resilience for the Industry 4.0 environment includes all levels of an organization and is described as an organizational systems property which relates to inherent and adaptive capabilities. These capabilities enable organizations to adapt during turbulent periods and strive to improve an organizations situational awareness, reduce vulnerabilities and restore efficacy following the event of a disruption (Burnard and Bhamra 2011). Organizational resilience can be seen as a competitive advantage in a manufacturing environment (Thoma 2014).

Nevertheless, it is rarely understood, how extreme events are handled resiliently. The complex task of decision making during extreme events involves multiple decision makers, who have to act within limited time. Impacts of decision can oftentimes not be anticipated as extreme events are unforeseen with limited chance to train and learn from the situation (Mendonça 2007). Still, organizations can weather for storms by implementing a number of *ex-ante* resiliency concepts. Redundancy in financial, human and technical resources supports coping with an crisis (Sullivan-Taylor and Branicki 2011). Robust and stable organizational systems withstand event forces more easily (Tierney and Bruneau 2007). In contrast, organizations have to build up the flexibility to rearrange structures and processes (Hatum and Pettigrew 2006) by diversifying business offerings and models (Fiksel 2003). Organizations, who can offer a non-substitutable service to their peers, can "obtain resources, concessions, and assistance that other organizations are denied" (Lengnick-Hall and Beck 2005, p. 752). Resilient behavior is also supported by contextual awareness, which "incorporates an enhanced awareness of expectations, obligations, and limitations in relation to the community of stakeholders, both internally (staff) and externally (customer, supplier, consultants, etc.)" (McManus et al. 2008, p. 83). Nevertheless, it must be stated that implementing all *ex-ante* resiliency concepts can be a costly strategy for organizations as they might never be used. Therefore, a "one-size-fits-all" approach will not work, instead the resilience strategy has to be optimized to a specific environment, in this case Industry 4.0 manufacturers.

Methodology

Based design science paradigm from Hevner et al. (2004), the practice-oriented resilience model for Industry 4.0 organizations was developed by reviewing resilience literature and interviewing experts in the field of Industry 4.0.

Industry	Duration in minutes	Number of words in memo	Experts position
Consultancy	60	777	Senior Consultant
Consultancy	35	365	Senior Manager
Consultancy	60	543	Manager
Consultancy	45	475	Senior Manager
Automotive	120	856	Team leader Information Security
Tobacco	60	642	Team leader CoE (Center of Excellence) production
Construction/ Component production	35	549	Chief Automation Officer (CAO)
Mechanical Engineering	45	450	Chief Information Security Officer (CISO)
Aerospace	60	704	Head of ICT Industrial Security; External Consultant
Chemicals/ Pharmaceuticals	55	365	Group leader automation technology
Semiconductors	35	419	Responsible for the security within the business unit
Engineering	60	350	Chief Information Officer (CIO)
Aerospace	40	690	ICS Security responsible
Chemicals/ Automation/ Aerospace	40	485	Business leader Europe

Table 1. Interview Partners

Initially, we reviewed existing literature on resiliency in Industry 4.0 organizations, based on the framework from vom Brocke et al. (2009), with focus on organizational resilience. For Industry 4.0 we used several synonyms like IIoT, CPS and cyber physical system. The first round, which includes searches in the AIS Senior Scholars' Basket of Journals and four largest IS conferences as well as four large journals and one conference focusing on production research, provided only limited results. As a next step, we enlarged our literature basis to electronic literature databases like ACM, AIS eLibrary, IEEE and

ProQuest. The literature found was reviewed based on a full text analysis. As the results of this has been insufficient, we developed interview questionnaires. We then conducted a qualitative study in our second phase. The goal of the study was the identification of non-researched concepts of resiliency in Industry 4.0 organizations. We performed semi-structured expert interviews (Wengraf 2001). To enhance rigor, the interview questionnaire was reviewed by Industry 4.0 experts and revised based on their feedback. The questions were sorted into categories: Industry 4.0, resilience, recent events on ICS, connectivity, technologies, complexity, risk management, business continuity management and crisis management, future questions and other statements. In total, five consultants specialized in Industry 4.0 and ten experts from Industry 4.0 manufacturers have been interviewed (see Table 1). The interview partners were based in Germany, the Netherlands, France and Austria and have between five and more than 20 years of experience in Cyber Security, manufacturing or Industrial Security. Most of them have a degree in engineering or computer science. Their roles within the organization are in middle or higher management. The interviews with the experts have been conducted via telephone or in person. To get sensitive and detailed information about resiliency in Industry 4.0, we were not allowed to record the interview. After the interviews, we created memos based on notes and observations during the interviews. We coded the memos in an iterative process (Fereday and Muir-Cochrane 2006) with codes partly grounded in the literature (Crabtree and Miller 1999) and partly derived from the data (Boyatzis 1998).

All information has been underpinned by literature, white papers and reports from practice if possible. The results of the study have been clustered to model components. After the development of the model, a presentation was built to provide the participants with an executive summary. The participants were asked to do a short evaluation of the model. The main focus of this evaluation was to determine the practicability of the model. This feedback was then build into the model. The model itself highlights six characteristics organizations should possess in order to be resilient in the Industry 4.0 environment.

Resilience Characteristics for Industry 4.0

Before detailing our developed model, we outline characteristics associated with resilience Industry 4.0 manufacturers need to face extreme events. These characteristics, named by our interview partners and literature, are flexibility, diversity, connectivity, knowledge, redundancy and robustness. The described model can be used to acquire these characteristics.

Flexibility

The transformation towards Industry 4.0 requires an enormous flexibility and adaptability of organizations (Kluth et al. 2014). Flexibility impacts all components of an organization, such as management including leadership and processes, policies, and practices, personnel including customers, suppliers, and partners and infrastructure including hardware, software, products and services (Patten et al. 2005). Flexibility can be broken down into three distinct organizational characteristics: anticipation, agility and adaptability (Patten et al. 2005). "Anticipation balances planning for expected change with preparing for unexpected change" (Patten et al. 2005, p. 2789). The preparation for events or changes is one of the key parts in limiting hazardous outcomes of an event. An example of anticipation is the alignment of IT and OT. Agility is the "ability of firms to sense environmental change and respond readily" (Overby et al. 2006, p. 120). Organizations need to be able to respond to change and recover from disturbing events. Agility relies on people, as it „requires employees to be trained to sense changes when they occur and use flexible processes and practices based on changes occurring" (Patten et al. 2005, p. 2790). Learning and adapting to changing environmental contingencies, also named organizational adaptability (Patten et al. 2005), shows need for an organization to include a continuous learning capability (Erol et al. 2010). Adaptability has a timely component, as any system can adapt to a changes, but the time for adaption is crucial (Erol et al. 2010).

Diversity

A diverse product portfolio, highly skilled employees, with diverse backgrounds, experiences and knowledge are concepts of diversity (Hagel III et al. 2015). Highly skilled employees enable an organization to quickly react to changes, rearrange processes and build up solutions based on their knowledge and experiences. Organizations within Industry 4.0 should create diverse business strategies and diversify their product and service portfolio to be able to react to spontaneous changing customer demands. Diversity contributes to a systems longevity and success (Fiksel 2003). Diversity in IT systems is important, as with technological adaptations an organizations retain its competitive position and complies with regulatory influences (Wolf et al. 2012). Standardization among the production environments enables organizations to control complexity and reduces costs for repairs, replacements and maintenance. Diversity within systems reduces the possibility of cascading system failures. Organizations need to find a balance between a standardized system environment and diversity.

Connectivity

Connections between ICS and the internet enable the transformation to Industry 4.0. The number of connections will rise within and between organizations (CGI 2014). As products become more interconnected, intelligent and responsive their offering new opportunities for organizations (Hagel III et al. 2015). This enables organizations to create new services. Connectivity contributes towards resilience, as it facilitates new and more information which can be analyzed to predict changes and developments.

Knowledge

Without knowledge about technologies, risks and threats, it is impossible to anticipate and manage changes effecting organizations. The "'know-what' (where to find the needed information) and 'know-how' (how to run operations smoothly) are key components of manufacturing strategy formulation, and build resilience in the organization. In particular, when a firm is facing economic disruptions, know-what and know-how strategies are even more pertinent in making timely decisions to cope with these disruptive events thereby enhancing the firm's resilience profile" (Acquaah et al. 2011, p. 5531). Organizations therefore need a corporate culture committed to knowledge and innovation to build resilience capacities (Acquaah et al. 2011). In the Industry 4.0 environment social and environmental systems are complex. Knowledge of them and the ability to predict future changes will never be complete (Berkes 2007). It is important understand the own organization as well as the changing economic environment.

Redundancy

In manufacturing, production must never stop. This may be achieved through redundancy (Stouffer et al. 2015). Redundancy is defined "as keeping extra capacity or resources kept in reverse to be used in case of a disruption" (Erol et al. 2010, p. 116). Redundant data centers or production paths may be costly, but can be used worthwhile in case of extreme events. Redundancy increases the adaptive capacity of the organization, as it provides continuity of function and enhances the adaptive speed to new situations. (Erol et al. 2010).

Robustness

Robustness is a major contributor towards resilience as it "goes beyond reliability and robustness [to focus] on how systems can return to their original state in the event of partial damage" (Erol et al. 2010, p. 113). ICS need to be able to withstand cyber attacks and unanticipated events in production. Not every impact can be known by organizations and often the introduction of new technologies brings new risks into the production environment.

Resilience Model

The establishment of the described resilience characteristics require multifaceted strategies and concepts. These are grouped into a model, which we call the resilience house (see Figure 1). The model consists of six components. There are two basic components, understanding the environment and understanding the own system, which form a solid foundation. Four components, people, technology, processes and information are supporting components. Each component contains specific elements for resilience. The resilience model will be introduced from bottom to top.

1 Understanding the Environment

Knowing the environment in which the organization operates is important, as "any company that can make sense of its environment, generate strategic options, and re-align its resources faster than its rivals will enjoy a decisive advantage" (Fiksel 2003, p. 5538). The Industry 4.0 environment is complex and dealing with this growing complexity has become a key competitive factor (Kluth et al. 2014). Advanced complexity management which is the "target-oriented and value added utilization of available resources in order to harmonize internal and external complexity, using appropriate manipulating, coping or pricing strategies" (Kluth et al. 2014, p. 72).

An organization has to be *aware of its situation* (1.1), the changes in the present and in the future. These changes include new business models, new players on the market or changing customer demands. The interconnectedness between organizations increases issues in controlling and overseeing complexity. An *early warning system* (1.2) combines information from different sources to enable users to see upcoming threats and issues. This tracking of trends, understanding their likely impact and forecasting their timing are critical for leaders to make the right decisions (Prentice 2015).

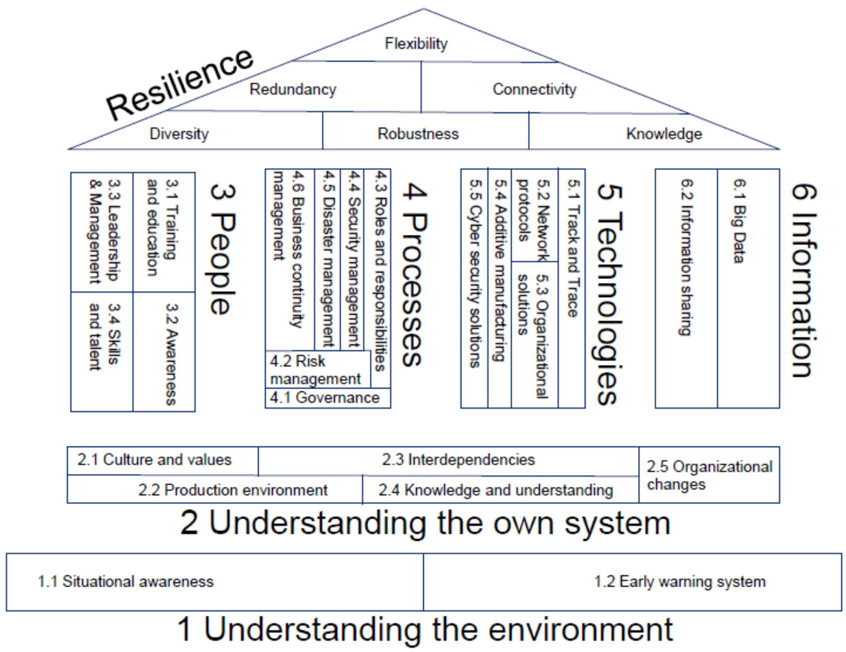

Figure 1. Resilience Model for Industry 4.0 Manufacturers

2 Understanding the Own System

For the transformation to Industry 4.0, organizations have to change on the inside, both on a technical as well as on an organizational, *cultural and value* (2.1) level. Often organizations have been grown through mergers and acquisition and are presenting a heterogeneous system and application landscape. This is particularly dangerous for organizations, as it hides risks. It becomes increasingly important to observe the developments both in IT and OT departments, as attacks are increasingly focusing on identifying and exploiting vulnerabilities in both IT and OT (Contu 2015).

ICS are increasingly interconnected, presenting additional challenges, such as production with quantity one, the reduction of costs and the improvement of quality and throughput. Organizations have to aim for a standardized *production environment* (2.2) to ensure modularity and interoperability (Mahoney and Roberts 2013). *Interdependencies between ICS* (2.3), applications and organizations increase. Especially critical infrastructure is often referred to as a 'system of systems' because of its interdependencies (Stouffer et al. 2015). Controlling this complexity is particularly difficult. To *understand and know the organizations environment* (2.4), architectural solutions are the first step towards controlling complexity, but will only work in conjunction with harmonization, standardization or reduction. Identifying, reducing and mitigating constraints of technical IT/OT interfaces and resources decrease the level of complexity and reduce costs and risks (Mahoney and Roberts 2013). An organization must define a target architecture and develop a road map on how to *change the organizational structure* (2.5) to become a more flexible, agile and competitive organization. Organizations have to define a 'normal' behavior to detect anomalies and prevent unintended interactions (Industrial Internet Consortium 2015).

One initial goal after an extreme event has to be the restoration of trust and resilience (Holling 1996). An organization which establishes viable culture and values rebuilds lost trust much faster. Guidelines for ethics must be centrally published and distributed and lived by management and employees.

3 People

People are often the first ones to detect anomalies. *Training and education* (3.1), *awareness building* (3.2) and *leadership and management* (3.3) as well as *skills and talent* (3.4) are important factors. Collaboration of organizations and employees is a key concept to rapidly answer market demands and to respond to extreme events (Camarinha-Matos et al. 2009).

The building of awareness is part of the detection of threats and the response to and recovery from an incident. Participation in online courses, workshops, special awareness trainings, in cyber security testing or emergency exercises ensure that employees have the same level of awareness and resiliency (Stouffer et al. 2015). Learning factories, competition or gamification are concepts which may be new approaches to train employees (Faller and Feldmüller 2015; Pittschellis 2015).

With the transformation to Industry 4.0, management and leadership among organizations change. Especially with the vanishing of borders between organizational business units, leaders and managers need to become more flexible and adaptable with a broader range of knowledge. The management should have stand-by expert teams in place to quickly react. These experts should show a continuous learning ability to adapt to the changes in technology, organizational structures and within the environment, as well as problem solving skills to autonomously deal with failures or new tasks (Schuh et al. 2015) .

4 Processes

Processes within an organization and among the supply chain change, as organizations have to keep up with developments from the environment. Shorter production life cycles are based on life cycle engineering. The integration of up to date technologies enable information and data flow. It reduces the effort for data provisioning and retrieval (Stark et al. 2014). With shorter production and more efficient life cycles, organizations will be able to reduce costs and time to market.

Organizations will have to establish holistic *governance processes* (Mingay et al. 2014), especially within the IT/OT environment (4.1). Regulatory and compliance requirements have to be fulfilled. Having an effective governance structure in place decreases the risk of a threat from a regulatory perspective. *Risk management* (4.2) has to be adapted and extended to the production environment and the overall supply network. *Security management processes* (4.4) will increase in importance, as cyber security and interconnections will be challenging for organizations. Understanding potential vulnerabilities is part of a solid security strategy, supporting the focus of effort and resources (Contu 2015). Following a crisis, *disaster management* (4.5) enables effective crisis management. *Business continuity* must be defined flexible and agile to support organizations to stay compatible once production stops (4.6). Especially for production environments, a short recovery time is important, as a production stops have a high financial impact on organizations. Defined roles and responsibilities (4.3) beyond organizational borders support people in case of an extreme event. This supports the development of trust among organizations.

5 Technology

The developments and advancements in technology, such as *additive manufacturing* (5.4), are one of the concepts which are enabling the transformation towards Industry 4.0. High availability is often seen critical in production. Virtualization is used to achieve high availability and to reduce costs and energy consumption. Organizations should not only invest in technologies, but also in acquiring the necessary knowledge (Schuh et al. 2014).

Organizations are able to monitor their products to enable remote maintenance or have to track their products due to legal and compliance requirements (Brettel et al. 2014). *Tracing product parts* will enhance resilience, as organizations are able to know where their product parts are and enables them to quickly react to disturbances in the delivery process (5.1). The introduction of mobile devices in production environments enables employees and the organization to be more flexible (5.3 *Organizational solutions*). Operating an organization wide frequency management prevents disruptions.

In production environments, *special network protocols* (5.2) are used (Scherer and Heinickel 2014). The global roll-out of M2M-communication may be entered by standardization. Communication channels, between different plants or locations, have to be safe and secure. *Cyber Security solutions* (5.5) such as End-to-End encryption and multi-factor-authentication ensure this. In addition, Anti-Virus solutions, firewalls, IDS and DMZs need to be implemented both in the IT and OT environments.

6 Information

The large amount of sensors in production environments collect extreme amount of data which can be extracted and visualized (Brettel et al. 2014). Organizations have to analyze this information to gain value. Handling data will be a challenge for organizations. Cloud computing is a possibility to manage information. It can also contribute to an organizations' agility, innovation and flexibility (Mingay et al. 2014). *Big Data* (6.1) is necessary to handle data generated and collected (Lee et al. 2014).

Information Sharing (6.2) about attacks, events or procedures successfully taken contributes strongly to the building of trust. But, organizations should also establish an information classification to know which information they need to protect.

Discussion and Conclusion

Industry 4.0 will change existing value chains on an international scale. This fundamental change is accompanied by unforeseeable risk. We believe, that organizational resilience will support Industry 4.0 organizations to transform and sustain in this volatile setting. This claim is supported by all experts interviewed, who stated that resiliency is an important topic in the not-yet stable environment of Industry 4.0. They showed diverse strategies to prepare for extreme events. However, none of the companies have acquired a holistic picture of resiliency in Industry 4.0 yet and have difficulties to establish resilience due to missing guidance from research. The practice-oriented model, described in the previous section, will support organizations to overcome the difficulties. To the best of our knowledge, the proposed model is the first of its kind and will support the important discussion in IS community.

During the literature research, a focus has been set on journals and conferences from the IS research field. Including more journals and conferences from the IS and other research disciplines, such as business, manufacturing or logistics might have revealed other insights which could have influenced the development of the model. Due to this, the research has to be presented to a broader range of experts to gain valuable feedback. During the interviews, the experts had difficulties answering questions towards resilience. In those cases, a definition and an example was given. Another difficulty has been the different backgrounds of the experts, as the focus on topics during the interviews varied. Especially in the Cyber Security area, cyber resilience becomes a more important topic, as organizations seem to understand that perfect security is not possible. Organizations have to go beyond shielding from cyber-attacks and develop resilient concepts to cope with the changing cyber environment. It is to assume that companies will adopt the resilience term from the cyber concept and start to grow a better understanding of business resilience and may include the term within their strategies.

The implementation of the resilience model in an organization would be the next necessary step to evaluate the practicability. It would detect flaws and missing components, highlight the usability of the approach and how well organizations can adapt the model to suit their individual needs. The implementation would also highlight next steps to improve the model. An implementation of the model would also show, if organizations intensively using information systems would be able to use the model.

Overall this research paper has highlighted challenges organizations face in the evolution to Industry 4.0. The broad literature research has shown an absence of research in the IS field and little guidance for practicing IS executives. The extensive qualitative study among experts from manufacturing companies and a consultancy in different countries in Europe has enables a holistic view on this topic. A broad range of solutions organizations have implemented or are considering has been identified. These have been on both a technical and an organizational level. Solutions organizations use and have implemented will change over time, as technology and knowledge advances. The developed model can be used to guide the resilience establishment and organizational transformation of Industry 4.0 manufacturers.

REFERENCES

Acquaah, M., Amoako-Gyampah, K., and Jayaram, J. 2011. "Resilience in family and nonfamily firms: an examination of the relationships between manufacturing strategy, competitive strategy and firm performance," *International Journal of Production Research*, pp. 5527–5544.

Berkes, F. 2007. "Understanding uncertainty and reducing vulnerability: lessons from resilience thinking," *Natural Hazards*, Kluwer Academic Publishers, pp. 283–295.

Boyatzis, R. E. 1998. *Transforming qualitative information: Thematic analysis and code development*, London: Sage Publications.

Brettel, M., Friederichsen, N., and Keller, M. 2014. "How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective," *International Journal of*, pp. 37–44.

Brocke, J. vom, Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., and Cleven, A. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature," in *ECIS 2009 Proceedings*, pp. 1–11.

Burnard, K., and Bhamra, R. 2011. "Organisational resilience: development of a conceptual framework for organisational responses," *International Journal of Production Research*, Taylor & Francis Group , pp. 5581–5599.

Camarinha-Matos, L. M., Afsarmanesh, H., Galeano, N., and Molina, A. 2009. "Collaborative networked organizations – Concepts and practice in manufacturing enterprises," *Computers & Industrial Engineering*, pp. 46–60.

CGI. 2014. "Cybersecurity in Modern Critical Infrastructure Environments,"CGI's SECURE-ICS White Paper.

Contu, R. 2015. "Market Trends: Industrial Control System Security, 2015,"Gartner Report.

Crabtree, B. F., and Miller, W. L. 1999. "Using codes and code manuals: a template organizing style of interpretation," in *Doing qualitative research*B. F. Crabtree and W. L. Miller (eds.), Thousand Oaks: Sage Publications, pp. 163–177.

Dombrowski, U., and Wagner, T. 2014. "Mental Strain as Field of Action in the 4th Industrial Revolution," *Procedia CIRP*, pp. 100–105.

Erol, O., Sauser, B. J., and Mansouri, M. 2010. "A framework for investigation into extended enterprise resilience," *Enterprise Information Systems*, Taylor & Francis , pp. 111–136.

Evans, P. C., and Annunziata, M. 2012. "Industrial Internet: Pushing the Boundaries of Minds and Machines,"Report from General Electric.

Faller, C., and Feldmüller, D. 2015. "Industry 4.0 Learning Factory for regional SMEs," *Procedia CIRP*, pp. 88–91.

Fereday, J., and Muir-Cochrane, E. 2006. "Demonstrating rigor using thematic analysis: A hybrid approach of inductive and inductive coding and theme development," *International Journal of Qualitative Methods*, pp. 80–92.

Fiksel, J. 2003. "Designing Resilient, Sustainable Systems," *Environment Science Technology*, pp. 5330–5339.

Fiksel, J. 2006. "Sustainability and resilience: toward a systems approach," *Sustainability: Science, Practice, & Policy*, pp. 14–21.

Hagel III, J., Brown, J. S., Kulasooriya, D., Giffi, C., and Chen, M. 2015. "The future of manufacturing - Making things in a changing world,"Deloitte Center for the Edge.

Hatum, A., and Pettigrew, A. M. 2006. "Determinants of Organizational Flexibility: A Study in an Emerging Economy," *British Journal of Management*, pp. 115–137.

Hevner, A. R., March, S. T., and Park, J. 2004. "Design Science in Information Systems Research," *MIS Quarterly*, pp. 75–105.

Holling, C. S. 1996. "Engineering Resilience versus Ecological Resilience," in *Engineering Within Ecological Constraints*P. C. Schulze (ed.), Washington, D.C.: National Academies Press, pp. 31–44.

Industrial Internet Consortium. 2015. "Industrial Internet Reference Architecture,"Industrial Internet Consortium Report.

Ismail, H. S., Poolton, J., and Sharifi, H. 2011. "The role of agile strategic capabilities in achieving resilience in manufacturing-based small companies," *International Journal of Production Research*, Taylor & Francis Group , pp. 5469–5487.

Kluth, A., Jäger, J., Schatz, A., and Bauernhansl, T. 2014. "Method for a Systematic Evaluation of Advanced Complexity Management Maturity," *Procedia CIRP*, pp. 69–74.

Lee, J., Ardakani, H. D., Yang, S., and Bagheri, B. 2015. "Industrial Big Data Analytics and Cyber-physical Systems for Future Maintenance & Service Innovation," *Procedia CIRP*, pp. 3–7.

Lee, J., Kao, H.-A., and Yang, S. 2014. "Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment," *Procedia CIRP*, pp. 3–8.

Lengnick-Hall, C. A., and Beck, T. E. 2005. "Adaptive Fit Versus Robust Transformation: How Organizations Respond to Environmental Change," *Journal of Management*, pp. 738–757.

Mahoney, J., and Roberts, J. P. 2013. "Top Impacts of IT/OT Convergence and How CIOs Should Deal With Them,"Gartner Report.

Matt, D. T., Rauch, E., and Dallasega, P. 2015. "Trends towards Distributed Manufacturing Systems and Modern Forms for their Design," *Procedia CIRP*, pp. 185–190.

McManus, S., Seville, E., Vargo, J., and Brunsdon, D. 2008. "Facilitated Process for Improving Organizational Resilience," *Natural Hazards Review*, pp. 81–90.

Mendonça, D. 2007. "Decision support for improvisation in response to extreme events: Learning from the response to the 2001 World Trade Center attack," *Decision Support Systems*, pp. 952–967.

Mingay, S., Iyengar, P., and Potter, K. 2014. "How CIOs Need to Prepare for Industrializing and Mutualizing IT in the Digital Economy,"Gartner Report.

Nordas, H. K., and Kim, Y. 2013. "The Role of Services for Competitiveness in Manufacturing,"OECD Trade Policy Papers.

Overby, E., Bharadwaj, A., and Sambamurthy, V. 2006. "Enterprise agility and the enabling role of information technology," *European Journal of Information Systems*, pp. 120–131.

Patten, K., Whitworth, B., Fjermestad, J., and Mahindra, E. 2005. "Leading IT Flexibility: Anticipation, Agility and Adaptability," in *AMCIS 2005 Proceedings*.

Pittschellis, R. 2015. "Multimedia Support for Learning Factories," *Procedia CIRP*, pp. 36–40.

Prentice, S. 2015. "Agenda Overview for the Agenda for the Future, 2015,"Gartner Report.

Scherer, J., and Heinickel, C. 2014. "Regulating Machine-to-Machine Applications and Services in the Internet of Things," *European Networks Law and Regulation Quarterly (ENLR)*.

Schuh, G., Gartzen, T., Rodenhauser, T., and Marks, A. 2015. "Promoting Work-based Learning through INDUSTRY 4.0," *Procedia CIRP*, pp. 82–87.

Schuh, G., Potente, T., Varandani, R., Hausberg, C., and Fränken, B. 2014. "Collaboration Moves Productivity to the Next Level," *Procedia CIRP*, pp. 3–8.

Stark, R., Grosser, H., Beckmann-Dobrev, B., and Kind, S. 2014. "Advanced Technologies in Life Cycle Engineering," *Procedia CIRP*, pp. 3–14.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. 2015. "Guide to Industrial Control Systems (ICS) Security,"National Institute of Standards and Technology Report, Gaithersburg, MD.

Sullivan-Taylor, B., and Branicki, L. 2011. "Creating resilient SMEs: why one size might not fit all," *International Journal of Production Research*, pp. 5565–5579.

Thoma, K. 2014. *Resilien-Tech - "Resilience-by-Design": Strategie für die technologischen Zukunftsthemen* (K. Thoma, ed.), Herbert Utz Verlag.

Tierney, K., and Bruneau, M. 2007. "Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction," *TR News*, pp. 14–18.

Weick, K. E. 1988. "Enacted Sensemaking in Crisis Situations," *Journal of Management Studies*, pp. 305–317.

Wengraf, T. 2001. *Qualitative Research Interviewing - Biographic Narrative and Semi-Structured Methods*, London: Sage Publications.

Wolf, M., Beck, R., and Pahlke, I. 2012. "Mindfully resisting the bandwagon: reconceptualising IT innovation assimilation in highly turbulent environments," *Journal of Information Technology*, pp. 213–235.