Employee Empowerment in the Context of domain-specific Risks in Industry 4.0

Claas Digmayer
RWTH Aachen University
c.digmayer@tk.rwth-aachen.de

Eva-Maria Jakobs
RWTH Aachen University
e.m.jakobs@tk.rwth-aachen.de

Abstract – This paper addresses risks in industry 4.0 as well as requirements that need to be considered in order to reduce such risks. The topic is investigated in interviews with experts from two domains: the production industry and the building construction industry. The results show that risks in industry 4.0 affect trends that span over industry domains such as the interconnection of systems and machines, the increasing use of digital systems, the increasing amount of digital data and changing demands placed on employees. Actual manifestations of such categories are domain-specific and within the domains phase-specific with regard to the value creation chain. The most important mean to reduce such risks are approaches that address the empowerment of employees. Knowledge about domain-specific risks of industry 4.0 is valuable for communication professionals that are engaged in intra-corporate change processes or risk communication.

Index Terms – Industry 4.0, safety culture 4.0, challenges and requirements of the digitalization for industry sectors, empowerment of employees

INTRODUCTION

Digitalization rapidly changes the modern world. Its impact is especially significant for professional contexts. The trend towards industry 4.0 (or smart manufacturing) places significant demands on those involved in industrial production – especially on technical communicators that shape and mediate the transformation process. Such decision makers need to know about risks that emerge in industry 4.0 and affect systems, machines, data and employees. Furthermore, they need to know how to limit such risks and how to involve those affected by risks in the transformation process. The present publication focuses these aspects and addresses means of employee empowerment in industry 4.0.

The term "industry 4.0" – formed by the German Government in 2011 – is an abbreviation of the fourth stage of industrialization. In the fourth stage, machines and components are interconnected with the help of computer-based systems: "Products and machines will be equipped with microchips to facilitate the operation and customizing of relevant processes over the Internet" [1]. Industry 4.0 enables suppliers and manufacturers to leverage new technological concepts like Internet of Things, Big Data, and Cloud Computing. Advantages of industry 4.0 are new or enhanced products and services, decreased productions costs, increased productivity [2], fast time to market, increasing innovation cycles, agile manufacturing, diminishing cross-company boundaries, autonomous data exchange between systems and machines and digital engineering strategies [3].

In spite of the broad spectrum of advantages, several challenges have yet to be met in order to establish an industry 4.0 at large scale [4]. As the trend towards an industry 4.0 will change drastically the way in which work is carried out, companies need to consider emerging risks and the way in which such risks are countered. Of particular importance in this context are two aspects:

First, the majority of studies on risks in industry 4.0 focus on the production industry. However, in this paper it is assumed that risks and corresponding requirements are subject to a variety of both domain-specific and cross-domain factors that should not be generalized industry-wide. Second, new risks emerge alongside to the technological transformation process that often affect the employees. Approaches towards industry 4.0 neglect bottom-up methods that empower employees to participate in decision-making processes related to risks.

To investigate these two gaps, an interview study is carried out that focuses on challenges and requirements in two domains (the production industry and the building construction industry). The study focuses on two research questions:

- RQ1: Which risks emerge in industry 4.0? Which of these risks are domain-specific, which ones span over both domains?
- RQ2: Which requirements need to be considered for industry 4.0 with risks in mind? Which of these requirements address technical issues, which ones address the empowerment of employees?

Related Work

I. Risks of an Industry 4.0

Risk is a multidimensional construct that various disciplines have examined with varying foci. The way in which a risk is evaluated depends significantly on the perspective of those who perceive the risk [5]. This paper uses a definition of the term *risk* by Rothkegel [6]: 'A risk is the occurrence of a transition from an initial to an undesired result state (e.g., loss, accident, attack, catastrophe) triggered by processes or (intended/not intended) actions'. Insights about emerging risks in industry 4.0 fall in four categories:

Risks that emerge due to the interconnection of systems and machines: The combination of increasing amounts of digital data and increasing interconnection of machines and devices in multiple contexts opens up an increased risk of cybercrime [7] and leads to further unpredictable risks [8]. Cybercime-induced sabotage comprises attacks on industrial plants leading to unnoticed loss of product quality and increased use of resources [9] as well as attacks on devices used by workers (e.g., augmented-reality glasses) leading to health damages, technical damages, process down time or loss of intellectual property [10].

Risks that emerge due to the increasing use of digital systems: The complexity of these systems and their interconnectedness open a greater surface area for cyber attacks that result in new types of attacks and corresponding threats [9]. In this context, many current IT security solutions do not satisfy requirements of processes in industry 4.0 [11] to prevent both accidental attacks and intentional attacks [12]. Despite the efforts of several institutions to make industry more aware of cyber-threats (e.g., with respect to increasing use of zero-day threats [13]), many of today's industrial networks remain vulnerable to cyber-attacks [11]. Other issues emerge due to missing standardization, specification and modeling languages for systems in industry 4.0 [2]. Current studies reveal a broad range of inconsistent design solutions among software systems applied in industries (e.g., computer-aided manufacturing) that lead to usability problems [14]. Low usability of systems used in industrial contexts may further result in security and safety issues [12].

Risks that emerge in the management of digital data: All of the elements in industry 4.0 (e.g., equipment, machines, applications, services) generate data, that by nature is large and complex and needs to be integrated and analyzed in the industrial production process. Tools for this task are underutilized due to their complexity and require expert knowledge that most companies do not possess [15]. Risks alongside this challenge concern information protection, privacy and security issues. [16] state that research and applications in this field still need further improvement. Another challenge arises if large amounts of collected data need to be separated in information which is 'fitting' for particular purposes from the remaining 'unfitting' information [17]. Furthermore, legal framework for handling such data is missing [12].

Risks that emerge for the employee: Several technologies in the context of industry 4.0 aim at supporting employees in their daily work, e.g. with the help of robots. However, this transformation leads to a removal of the separation of workspaces between robots and employees which means breaking with established safety procedures. Current research focuses on identifying and preventing employee-robot impacts by minimizing related risks [18]. Furthermore, the development of industry 4.0 will be accompanied by changing tasks and demands for the employee in the factory that require new forms of skill and knowledge [4]. There will be a shift towards more complex jobs which require new skills, continuous learning and education [19]. Estimations predict that medium-wage jobs are at highest risk of being replaced by intelligent machines [20].

II. Employee Empowerment in Industry 4.0

The aim of employee empowerment is '[…] to 'involve' or give employees opportunities to become involved in their work and their employing organisation, beyond simple performance of the contractual wage/work bargain […] in terms of participation in decision making' [21]. Empowering employees requires communicative efforts that combine information sharing in top-down approaches (from the management to the employees), participation in bottom-up approaches (from the employees to the management) und cooperation at the interface between top-down and bottom-up approaches [21],[22]. Such communicative efforts are part of corporate communications that support or realize business processes (value chains), supportive activities (e.g., administration), and management activities [23].

Some publications emphasize the importance of top-down approaches: Strategies are required that raise the awareness of employees to changes induced by industry 4.0 and strengthen continuously their qualification as preparation for a changing workplace. In this context, managers are responsible to provide such strategies top-down (e.g., as e-learning) and set a good example [19].

Some publications focus on bottom-up approaches: [24] state that '[…] the goal should be to make employees and teams in CPS production systems into equal or, even better, leading decision-making authorities within the production process in line with the principles of industry 4.0 and to organize the division of labor so that better decisions can be taken'. Networking and communication among employees (with the support of wireless communication technologies [25]) are perceived to be a key factor in achieving employee involvement [24] and increasing productivity due to cooperation efforts [26]. The relevance of risks is seldom highlighted in context of

employee empowerment: [3] states that collaborative networks pose potential for conflicts because companies often strive to limit information sharing.

However, information sharing, involvement and cooperation are key factors in establishing a safety-aware corporate culture (safety culture). It is yet to be examined which requirements industry 4.0 places on the development of safety cultures. The present study is part of a project that aims at developing a safety culture for industry 4.0.

Methodological Design

Data collection: In the study, two exemplary industry domains are examined: the production industry and the building construction industry (especially planning departments). An interview guide was developed and 10 interviews with experts from both industry domains were conducted (manufacturing SMEs: n=5, building construction industry: n=5). The interview guideline includes questions on the perception of risks in the development towards an industry 4.0, requirements for establishing a safety culture for industry 4.0 and means to foster employee empowerment in relation to risks. The interview guideline was evaluated in a pre-test and revised afterwards. All interviews were audio recorded. One interviewee could not attend the interview and answered the questions in writing.

Data preparation: The collected audio files were transcribed and anonymized so that no *conclusions can be drawn about the participants of the study* (e.g., the names of the interviewees were replaced with the acronym '*Number of the interview_gender_domain of the interviewee*'). The anonymized transcripts were converted into MAXQDA format.

Data analysis: Data were coded and analyzed with qualitative content analysis procedures: Passages of the transcripts were annotated in which the interviewees comment on risks or requirements (including means of employee empowerment). Annotations were categorized top-down (top-level categories: risks, requirements; second-level categories under each top-level category: increasing use of digital systems, interconnection of systems and machines, data management, the employee) and bottom-up (clustering annotations that focus on the same aspect under a second-level category).

Results

In the transcripts, 141 text passages were annotated. 46.1 percent of these annotations relate to production industry, 53.9 percent to the construction building industry (see Tab. 1). The majority of all annotations is related to requirements (65.25%), perceived risks were stated with a lower frequency (34.75%).

Regarding the requirements, experts of both domains emphasize that methods to empower employees are the key factor in establishing a risk-aware corporate culture: 45.39 percent of all annotations relate to such methods (top-down: 9.93%, bottom-up: 26.24%, interconnection between top-down and bottom-up: 9.22%).

TABLE 1. DISTRIBUTION OF ANNOTATIONS REGARDING TOP-LEVEL AND SECOND-LEVEL CATEGORIES RELATED TO THE PRODUCTION AND THE BUILDING CONSTRUCTION INDUSTRY

Categories		**Industry Domains**	
Top-Level	**Second-Level**	**Production**	**Building Construction**
Risks	Increasing use of digital systems	3.55%	5.67%
	Interconnection of systems and machines	3.55%	2.84%
	Data management	6.38%	3.55%
	The employee	2.84%	6.38%
Requirements	Increasing use of digital systems	7.09%	2.84%
	Interconnection of systems and machines	2.13%	2.13%
	Data management	2.13%	3.55%
	The employee	18.44%	26.95%

I. Risks of Industry 4.0 in the Production Industry

Three aspects were identified which belong to the second-level category *emerging risks due to the increasing use of digital systems*: The interviewees criticize that currently the *existing infrastructure is inadequate for industry 4.0.* Due to the inadequate infrastructure, companies have to rely on digital platforms of third-party providers that however offer *limited possibilities to influence security settings*. The third aspect deals with the problem that companies use a wide range of differing systems that are often incompatible to each other. Such *incompatible systems* impede secure communications and data exchange between companies as the following citation emphasizes:

I1_m_PI: There are no overarching value creation chains because everyone is only compatible with himself. ERP [enterprise resource planning] systems worsen the situation: they are individualized extensively instead of defining and using the lowest common denominator.

With regard to the second-level category *Risks that emerge due to interconnection of systems and machines,* four aspects were found: Connecting machines with the Internet without sufficient security measures allows unauthorized persons *remote access* and to damage the machines as stated in the following citation:

I3_m_PI: Interference can emerge from the outside if we interconnect machine data and work processes. Inside the company, this is okay. But with remote access from the outside, this means that the whole company can be compromised.

Another issue is *impractical legal specifications* that are not applicable in daily work routines, for instance specifications for the cooperation between robots and workers.

Other risks stated in the interviews are failures in machines that evoke failures in other machines (*cascading machine failures*) and *high expenses* for improving the security of machines.

The second-level category *risks that emerge in the management of digital data* comprises three aspects: *Data leakage* is the main problem perceived in this field as well as corresponding consequences such as trust issues, data manipulation or liability for data:

I5_f_PI: The topic how we handle data that our customers transfer to us, […] how can we guarantee the security of these data - this is a great challenge.

Another issue are *inadequate legal specifications* for the data management. As a result, data policies often do not consider threats induced by industry 4.0. Another issue stated in the interviews is *missing concepts for long-term storage* of big data created in industry 4.0.

The second-level category *risks that emerge for the employee* includes two aspects: First, concepts are missing that consider *demands of employees in the transformation process*. Second, traditional job profiles are expiring. Workers in industry 4.0 need to adapt tasks and skills that are not part of their job description. Such demands can overstrain the employees and may decrease acceptance of approaches towards industry 4.0.

II. Risks of Industry 4.0 in the Building Construction Industry

Risks that emerge due to the increasing use of digital systems comprise four items*: Insecure networks* are perceived as most significant risk in this category. Missing security measures allow attackers to record the data traffic within buildings. Furthermore, the experts criticize *inconsistent specifications of data formats* in software systems that are used by collaborating companies. This risk is most striking in processes (and related software tools) that aim at generating and managing digital representations of characteristics of buildings (BIM: Building information modeling):

I8_m_BCI: It is my concern that if we want to put BIM really into practice, we will also need to incorporate the results of our partners into BIM which means double effort instead of reduced workload.

BIM systems are also perceived as *highly complex expert systems* that are difficult to learn and use. Errors in using such expert systems may result in false information being passed into downstream processes. The last aspect in this category describes limited possibilities to influence the *security settings of digital platforms of third-party providers*.

In the second-level category *risks that emerge due to the interconnection of systems and machines,* two aspects were identified: First, the experts perceive critically the *missing development of concepts to predict and prevent potential threats* that emerge due to the interconnection of systems and machines:

I6_m_BCI: Our customers have no precise view on possible risks. They increasingly equip their buildings with PI-based technology without thinking about the consequences.

Second, difficulties are stated to introduce industry-4.0 approaches in the building construction industry because several manufacturing processes still rely on *manual work* which impedes digitalization.

Risks that emerge in the management of digital data: Infringement of intellectual property is perceived as the most important threat in this category. This risk originates from both attackers stealing digital data as well as partners changing data of collaborating companies (e.g., in BIM). Furthermore, the experts criticize *missing concepts to track changes in digital data* :

I7_m_BCI: Imagine several planning disciplines working on the same data model. In this case it is important to be able to reproduce who made a mistake.

Risks that emerge for the employee comprise one aspect, *missing concepts to consider demands of employees* in the transformation process as the following citation emphasizes:

I9_m_BCI: Solely the announcement of possible changes due to digitalization will cause questions, worries and troubles on side of the employees: What is happening to me? Will this have consequences for me? This is a huge factor of uncertainty.

III. Requirements on Industry 4.0 in the Production Industry

Four aspects were identified in the second-level category *requirements that emerge due to the increasing use of digital systems*: The most frequently mentioned requirement is to ensure *access control to systems* in order to prevent security breaches. The second aspect concerns means to *extend the existing infrastructure for industry 4.0*. Furthermore, the experts suggest that potential threats should be reconstructed in *risk analyses* in order to develop new security approaches:

I2_m_PI: Threat modeling can be achieved by formulating risk scenarios and by deciding whether I am prepared for this scenario: Are my employees sufficiently qualified? Do I have enough employees?

The last stated requirement is the frequent use of *confidentiality agreements* to prevent data leakage.

In the second-level category requirements that emerge due to the *interconnection of systems and machines*, two aspects were assigned: The interviewees recommend approaches that ensure the *access control to machines*:

I1_m_PI: We focus on 'tunneled' authentication via cloud and access parameterization as advancement of the current remote access of machine suppliers and their services.

Furthermore, it is suggested that *old machines need to be upgraded* in order to match the demands of industry 4.0.

Requirements that emerge in the *management of digital data*: In this category, the experts mention two requirements. The first requirement is the need to develop *instructions for employees* how to prevent security problems when handling digital data:

I5_f_PI: Safety is an important topic in my company because we work with large machines. If we digitalize these processes, surely, we need to develop new work instructions.

As second requirement, *cross-national cooperations* between companies are demanded that focus on developing shared strategies in managing security issues.

Requirements that emerge for the employee: Requirements stated in this category either refer to top-down approaches (19.2% of all annotations in this second-level category), bottom-up approaches (57.7%) or approaches at the interconnection between top-down and bottom-up (23.1%).

Regarding *top-down approaches*, the experts suggest two requirements: The management should be responsible to *take the lead in the transformation process*, initiate mean of employee empowerment and ensure continuously that the applied approaches are adhered to:

I3_m_PI: The management is responsible to set the framework for all safety- and security-related means in an industry 4.0: Threat/risk analysis, IT security, documentation obligation, handling of safety/security incidents, encryption systems, and employee training.

The second mentioned requirement concerns the responsibility of the management *to initiate internal innovation processes* and therefore choose adequate methods (e.g., brainstorming, mind maps).

Regarding *bottom-up approache*s, two requirements were named in the interviews: First, risk-awareness needs to become a fixed part of the corporate culture –security and safety should be *'lived' by the employees*:

I5_f_PI: Employees should be involved completely in decision processes from the beginning because what they do not co-create, they will not live later on.

Second, employees are required to continuously enhance their *knowledge and skills regarding security and safety*.

Two *requirements at interconnection between top-down and bottom-up approaches* were identified in the analysis: *Communication between departments* needs to be strengthened: A risk-aware corporate culture can only be established if all parts of the value creation chain collaborate closely and exchange information about potential risks timely:

I1_m_PI: Desire to change current conditions is essential on all enterprise levels as well as […] experience exchange between departments and company locations.

The second requirement are *innovation workshops*. In such workshops, representatives of the management and departments share their opinions on how work conditions can be improved in order to make work safer and to prevent potential threats:

I1_m_PI: Critical faculties and dialogue do not always result in consensus but rather in an approximation to best realization of a safety culture in consideration of multiple perspectives and weightings. The result is a shared view and overall accepted understanding integrated in the corporate culture. […] In this way, all behaviors and information become apparent and comprehensible – a sure-fire success in the proper sense.

IV. Requirements on Industry 4.0 in the Building Construction Industry

Three aspects were identified in the second-level category *requirements that emerge due to the increasing use of digital systems*: First, adequate approaches to *control access to systems* need to be developed. Second, companies need to *prove their competencies* in dealing with security issues – especially if they want to become contractor in projects that are exposed to risks. Third, *consistent digital interfaces* need to be established between different BIM systems. In this way it is ensured that data exchange between companies does not result in data falsification.

One aspect was found regarding r*equirements that emerge due to the interconnection of systems and machines*: The interviewed experts state that the work of employees in industry 4.0 should be supported with *assistant systems*. In this way, safety and security issues in handling machines can be prevented:

I6_m_BCI: *We consider virtual reality and augmented reality because these methods allow planning in 3D in the building construction domain.*

Two aspects were identified in relation to *requirements that emerge in the management of digital data*: First, checking routines should be established that ensure data

quality. Second, approaches to visualize data in BIM systems may help to prevent errors in data handling:

I6_m_BCI: *Industry 4.0 approaches should provide methods that allow us to view and perceive all processes within a factory.*

Requirements that emerge for the employee: Aspects identified in this category refer to top-down approaches (23.7% of all annotations in this second-level category), bottom-up approaches (57.9%) or approaches at the interconnection between top-down and bottom-up (18.4%).

The interviewees stated four requirements regarding top-down approaches: The management is supposed to *take the lead* in all corporate transformation processes as the following citation highlights:

I10_m_BCI: First of all: Seek to be exemplary. And secondly: Tell and teach the employees how to participate creatively. This is the responsibility of the management: Uphold the corporate culture and do not limit yourself to talk about participation only in powerpoint presentations.

The second requirement is the task of the management to *determine persons in charge of risk issues* and define their responsibilities. The third requirement is to *provide an equal basis of information for all employees*. Only with information about potential threats, employees are enabled to make risk-related decisions.

Regarding *bottom-up approache*s, three requirements were identified: *Knowledge and skills* of employees regarding security and safety need to be enhanced continuously. As a second requirement, security and safety need to become *fixed parts of the corporate culture*. As a third requirement, employees need to become an active part of *corporate decision-making processes*:

I7_m_BCI: It is necessary to involve the whole team. This means that the team is able to determine how to improve processes and ensure maximal process safety – in a way that our products are faultless.

In the category *requirements at interconnection between top-down and bottom-up approaches,* three aspects were found: *Strengthening the communication between departments* is a necessary requirement to establish a risk-aware corporate culture. As a second requirement, *innovation workshops* need to be conducted to shape the risk-related work conditions of the future. The last requirement in this sub category are *apps for intercultural communication*:

I10_m_BCI: Sometimes it is difficult to communicate with subcontractors on a construction site due to multilingualism. But it is necessary to tell them precisely how to perform particular works in order to minimize safety issues. What we need is an app that visualizes such works to lower the language barrier.

DISCUSSION

The present study investigates consequences of the increasing digitalization for companies. Insights on potential emerging risks depending on particular industry domains (RQ1) and means to address such risks (RQ2) – especially from the employee's point of view – are essential to successfully develop, introduce and keep up communication strategies that foster a transformation towards a security-and safety-aware corporate culture, as prepared by professional communication experts.

Regarding *RQ1*, results show that both representatives of the production industry and of the building construction industry perceive risks that emerge in the development towards an industry 4.0 due to *cross-domain* trends such as the interconnection of systems and machines, the increasing use of digital systems, the increasing amount of digital data and changing demands placed on employees. However, such aspects manifest in ways that are *domain-specific* and within the domains *phase-specific* with regard to the value creation chain: Regarding the *increasing use of digital systems*, representatives of both domains emphasize the relevance of data security. In manufacturing enterprises, this challenge become apparent if information needs to be shared in secure ways with suppliers and customers and unauthorized third parties need to be excluded at the same time. The problem may occur in different phases of the value creation chain, e.g., in the development of new products, in the production phase, or in after-sales services. In the construction industry, this challenge relates to two different phases in the value creation chain: the need for collaborative work between project partners in planning processes (e.g., in BIM) and in the maintenance phase after a building has been constructed (e.g., setting up security measures in smart buildings).

With regard to the *interconnectedness of systems and machines*, both industry domains are concerned with the question which safety concepts are required for the introduction of novel intelligent machines. In the production industry, this question is focused on how to control such machines (e.g., against unauthorized access) mainly in the production phase. In the building construction industry, this issue is yet not as apparent as in the production industry. That could be due to the fact that most processes in the construction phase still rely on manual work and have yet not reached the readiness level for digitalization [11]. This is a significant contrast to the planning phase that is revolutionized digitally with technologies such as BIM.

Regarding the *handling of digital data*, perceived risks relate to differing types of data depending on the domain: In the production industry, such data comprise product data and related machine data that are relevant throughout the value creation chain. In the building construction

industry, perceived risks relate to 3D models that are mainly relevant in the planning phase.

Emerging risks for the employee is the only second-level category in which risks perceived by experts of both domains match: The greatest challenge is to consider the role of the employee in transformation processes towards industry 4.0. Most of such approaches solely focus on the security and safety of *objects* (e.g., software, components) and not on *processes* in which the employee plays a key role. Security and safety concepts are therefore predominantly *technology-centered* and not *human-centered* leaving the employee a passive role as recipient of either positive (e.g., work assistance by smart devices) or negative consequences of Industry-4.0 technologies (e.g., job loss).

Results show that generic concepts for security and safety that do not consider domain-specific issues fall short. Furthermore, domain-specific concepts that focus on security or safety in isolation will not be suited for the demands of an industry 4.0. Both aspects are embedded in a complex framework of mutually influential effects in socio-technical systems. From this perspective, further aspects such as the dependability (usually summarized as RAMSS – reliability, availability, maintenance, security, safety) of products, machines and processes need to be considered. In this context, the statements of the experts indicate uncertainty in estimating the probability of occurrence as well as the damage extent of perceived risks. Innovative automated approaches are needed that support the prediction of risks in domain-specific forms of industry 4.0.

Regarding *RQ2*, experts of the production industry state requirements that coincide with findings from the literature. An emphasis is on requirements regarding the increasing use of digital systems. Experts of the building construction industry state some domain-specific requirements that are not covered by the literature. The majority of statements on requirements refers to employee-centered approaches towards a safety- and security-aware corporate culture in industry 4.0. This aspect is scarcely considered in the literature. In contrast, experts of the production industry as well as of the building construction industry in the present study agree that empowering employees is the key element in all transformation processes towards digitalization in industry domains. Concepts that are limited to the sole introduction of digital tools for communication and networking are not sufficient [] – effective eemployee empowerment requires the interplay of approaches that are initiated top-down as well as bottom-up and approaches that connect methods of both top-down and bottom-up.

The experts agree that the aim of employee empowerment is to get from the aims initially determined by the management to a self-perpetuating, shared understanding of safety and security that is lived and further developed by the employees as part of the corporate culture. The results indicate that innovation methods are suitable tools to foster the involvement of employees. However, approaches such as innovation workshops, design thinking and open-innovation platforms require in-depth knowledge about types of innovators and how to address them adequately [27].

There some implications of the findings for communication professionals that are engaged in intra-corporate change processes or risk communication: Communication professionals need to take up the task to translate vague corporate aims regarding values for safety and security to be achieved by transformation processes into concrete recommendations for action. The result are codes of conduct that are tailored towards employees and their tasks, roles and goals as well as towards the company, its domain and culture. In this way, expected behavior in the context of safety and security becomes reconstructable and measureable – ranging from simple lists of do's and dont's to the modelling of error inheritance in industrial process chains. Storytelling may be a powerful tool to exemplify such expected behaviors. Knowledge about domain-specific risks of industry 4.0 is valuable in this context, e.g., for the development of instructions, trainings, and behavior guidelines.

Other tasks of communication professionals include designing the interfaces of expert software systems in a way that supports the user in preventing risks (e.g., by embedding relevant knowledge into the interface). Recent approaches strife to achieve this in computer-aided manufacturing systems (CAM) for the production industry [14]. Further research should adapt such features for systems of the building construction industry (e.g., for BIM).

There are some limitations to this study: First, it is a qualitative study that should be validated with quantitative means in further research. Second, the interviewees consisted only of domain experts. As the perception of experts and laymen often differs [5], employees should be interviewed in a follow-up study.

CONCLUSION

The present study investigates risks and requirements in industry 4.0. The results reveal the need for a deeper understanding of the domain-specific professional situations that are affected by the trend towards industrial digitalization. Communication professionals should be involved in developing and introducing adequate concepts that foster the transformation process and consider demands of the most important element: the employee.

ACKNOWLEDGEMENTS

This research and development project is funded by the German Federal Ministry of Education and Research (BMBF) within the "Innovations for Tomorrow's

Production, Services, and Work" Program and by the European Social Fund (ESF) (funding number 02L15A002) and implemented by the Project Management Agency Karlsruhe (PTKA). The author is responsible for the content of this publication.

REFERENCES

[1] P. Marçon *et al.,* "Communication technology for industry 4.0," *Progress In Electromagnetics Research Symposium*, pp. 1694–1697, 2017.

[2] R. Petrasch and R. Hentschke, "Process modeling for industry 4.0 applications: Towards an industry 4.0 process modeling language and method," *in Proc. JCSSE*, 2016, pp. 1–5.

[3] M. Brettel and M. Rosenberg, "How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective," *International Journal of Information and Communication Engineering*, vol.8, no.1, pp. 37–44, 2014.

[4] Acatech, *Cyber-Physical Systems. Driving force for innovation in mobility, health, energy and production*. Sankt Augustin: Acatech, 2011.

[5] C. Digmayer and E. M. Jakobs, "Risk perception of complex technology innovations: Perspectives of experts and laymen," in *Proc. ProComm*, 2016, pp. 1–9.

[6] A. Rothkegel, "Sicherheitsmodelle und Kommunikations-Risiko," in *Sicherheitsforschung-Chancen und Perspektiven*, P. Winzer, E. Schnieder, and F.-W. Bach, Eds., Berlin: Springer, 2010, pp. 207–220.

[7] D. Sopori, T. Pawar, M. Patil, and R. Ravindran, "Internet of Things: Security Threats," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 6, no. 3, pp. 263–267, 2017.

[8] O. Jaradat, I. Sljivo, I. Habli, and R. Hawkins, "Challenges of Safety Assurance for Industry 4.0," in *Proc. EDCC*, 2017, pp. 103–106.

[9] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. DAC*, 2015, pp. 1–6.

[10] M. Langfinger, M. Schneider, D. Stricker, and H. D. Schotten, "Addressing security challenges in industrial augmented reality systems," in *Proc. INDIN*, 2017, pp. 299–304.

[11] N. Benias and A. P. Markopoulos, "A review on the readiness level and cyber-security challenges in Industry 4.0," in *Proc. SEEDA-CECNSM*, 2017, pp. 1–5.

[12] M. Waidner and M. Kasper, "Security in industrie 4.0 - challenges and solutions for the fourth industrial revolution," in *Proc. DATE*, 2016, pp. 1303–1308.

[13] A. Pye, "Connecting the unconnected," *Engineering Technology*, vol. 9, no. 11, pp. 64–70, 2014.

[14] E.-M. Jakobs, C. Digmayer, S. Vogelsang, and M. Servos, "Not Ready for Industry 4.0: Usability of CAx Systems," in *Proc. AHFE,* 2017, pp. 51–62.

[15] M. O. Gokalp *et al.*, "Big Data for Industry 4.0: A Conceptual Framework," in *Proc. CSCI*, 2016, pp. 431–434.

[16] K. Zhou, T. Liu, and L. Zhou, "Industry 4.0: Towards future industrial opportunities and challenges," *in Proc. FSKD*, 2015, pp. 2147–2152.

[17] T. Wuest, S. Wellsandt, and K.-D. Thoben, "Information Quality in PLM: A Production Process Perspective," in *Proc. PLM*, 2015, pp. 826–834.

[18] S. Robla-Gómez *et al.,* "Working Together: A Review on Safe Employee-Robot Collaboration in Industrial Environments," *IEEE Access*, vol. 5, pp. 26754–26773, 2017.

[19] L. Bonekamp and M. Sure, "Consequences of Industry 4.0 on Employee Labour and Work Organisation," *Journal of Business and Media Psychology*, vol. 6, no. 1, pp. 33–40, 2015.

[20] Z. Rajnai and I. Kocsis, "Labor market risks of industry 4.0, digitization, robots and AI," in *Proc. SISY*, 2017, pp. 343–346.

[21] M. Marchington, J. Goodman, A. Wilkinson, and P. Ackers, "New developments in employee involvement," *Management Research News*, vol. 14, no. 1/2, pp. 34–37, 1991.

[22] R. E. Quinn and G. M. Spreitzer, "The road to empowerment: Seven questions every leader should consider," *Organizational Dynamics*, vol. 26, no. 2, pp. 37–49, 1997.

[23] E.-M. Jakobs, "Unternehmenskommunikation. Arbeitsfelder, Trends und Defizite," in *Profession und Kommunikation*, S. Niemeyer and H. Dieckmannshenke, Eds., Frankfurt a.M.: Peter Lang, 2008, pp. 13–31.

[24] W. Bauer, M. Hämmerle, S. Schlund, and C. Vocke, "Transforming to a Hyper-connected Society and Economy – Towards an "Industry 4.0"," *Procedia Manufacturing*, vol. 3, pp. 417–424, 2015.

[25] V. Roblek, M. Meško, and A. Krapež, "A Complex View of Industry 4.0," *SAGE Open*, vol. 6, no. 2, pp. 1–11, 2016.

[26] G. Schuh et al., "Collaboration Mechanisms to increase Productivity in the Context of Industrie 4.0," *Procedia CIRP*, vol. 19, pp. 51–56, 2014.

[27] C. Digmayer, *Communitybasierte Open Innovation-Plattformen für ältere Nutzer. Kommunikative Usability, Sociability und eTrust.* Aachen: RWTH Aachen University, 2016.

About the Authors

Dr. phil. Claas Digmayer is a research assistant at the Human-Computer Interaction Center at RWTH Aachen University (Germany), department of text linguistics and technical communication. He graduated in technical communication and computer science at RWTH Aachen University. Main research interests are: risk perception and communication, text mining, industry 4.0, open innovation.

Prof. Dr. phil. Eva-Maria Jakobs is a full professor of text linguistics and technical communication at RWTH Aachen University, Germany. She is co-director of the Institute for Industrial Communication and Business Media, the Human-Computer Interaction Center at RWTH Aachen University, and the study program technical communication. Main research fields are: technical and digital communication, text technologies, usability research and writing at work.