






# Cyber Security Culture as a Resilience-Promoting Factor for Human-Centered Machine Learning and Zero-Defect Manufacturing Environments

Christina Marie Mitcheltree<sup>(✉)</sup> , Godfrey Mugurusi , and Halvor Holtskog 

Department of Industrial Economics and Technology Management in Gjøvik,  
Norwegian University of Science and Technology, Trondheim, Norway  
christina.mitcheltree@ntnu.no

**Abstract.** Humans have often been perceived as a leading cause of error in Zero-defect manufacturing (ZDM) processes. There is thus a reduction of human interventions in the deployment of industry 4.0 (I4.0) technologies used for ZDM such as Machine Learning (ML). However, as manufacturing (e.g., I4.0 context) is often placed within a socio-technological context involving the co-integration of humans and technology, the manufacturing processes are now more vulnerable to cyber risk and threats. System vulnerabilities also derive from limitations associated with ML. This paper highlights three challenges associated with ML: explainability, data privacy, and security for ZDM. We argue that due to the high level of data complexity and lack of flexibility in ML models, humans play a critical role in ZDM decision-making. The paper explores the concept of security culture as an enabler for transformative resilience and zero-defect manufacturing and contributes to rethinking the human-centered approach in ZDM. The paper stresses a need to enhance contextual and empirical understanding of transformative resilience and security culture in ML/ZDM environments to better address adverse events such as cyber threat situations.

**Keywords:** Zero-defect Manufacturing · Machine Learning · Cyber Security · Human-centered Manufacturing · Security Culture

## 1 Introduction

### 1.1 Industry 5.0 and Human-Centered Manufacturing

Technologies e.g., Machine learning (ML) have reduced human intervention, as humans are perceived as a leading cause of error [1]. Similarly, within the cyber security domain, 95% of cyber-attacks are argued to derive from human-related errors [2]. As technology may be adapted to humans, they might acquire an inadequate knowledge base (e.g., explainability and faulty decisions) [3]. This could lead to incorrect use, as well as harm information confidentiality, integrity, and availability [4]. Moreover, humans in Zero-defect Manufacturing (ZDM) may acquire various constraints (e.g., knowledge, time,

cognitive constraints, etc.) that may negatively impact their decision-making. Vulnerabilities in technology may thus facilitate cyber security risks [5]. Hence, humans' lack of awareness and knowledge might result in organizations becoming more vulnerable to threats such as cyber-attacks [3]. This is especially true in relation to adverse events such as the COVID-19 crisis or the ongoing Russian war against Ukraine, which has made cyber resilience an international policy priority [6]. Cyber resilience is thus about an organization's ability to recover and adapt after an adverse event, involving preparedness for known and unknown threats [7, 8]. According to the European Commission's science for policy report [9], the COVID-19 crisis has been a warning sign in that we are never completely safe from unforeseen events and that such events make the world vulnerable. The crisis has provided a need and thus an opportunity to progress through adaptation and transformation. Rather than "bouncing back" to a pre-crisis state, the concept of "transformative resilience" has been proposed to argue for the development of policies and interventions to "bounce forward" toward more sustainable solutions from a social, economic, and environmental perspective [9]. This may involve strengthening people and enhancing their creativity and commitment needed to handle such situations. Similarly, the concept of "resilience-promoting factors" emerges from Fisher et al., [10] who define it as those "variables representing characteristics and features of the self or one's environment that provide a protective or ameliorative function in the event that adversity occurs". They add that these factors infer the possibility of risk. As security practices usually are highly technocentric, information security attacks are becoming more successful [11]. Therefore, the most essential foundation for resilience in organizations is argued to be a security culture [12]. Hence, we argue that a security culture may be viewed as a resilience-promoting factor (e.g., [10]).

As industry 4.0 (I4.0) emphasizes digitalization and AI-driven technologies for production efficiency, the central principles of Industry 5.0 (I5.0) are sustainability, human-centricity, and resilience [13]. From this view, we argue that manufacturing processes of the future will become more human-centric. Human-centered manufacturing places worker needs and well-being at the center of the manufacturing process [14]. Consequently, we explore security culture as a human-centered precondition for transformative resilience towards ZDM. Thus, we examine the value of involving humans in the ZDM decision loop; viewing them as a resource rather than a threat in the operationalization of ML for ZDM. We further explore the concept of security culture as a mechanism for the development of transformative resilience to better address adverse events (e.g., cyber threats). Hence, the research question "*In what way may the interplay between transformative resilience and security culture concepts enable robust ML/ZDM?*". As such, we present a new way of thinking about ZDM, and propose that this could be an area that requires further empirical research.

Under these circumstances, our argument and thus the scientific contribution of this paper is that we provide a better understanding of transformative resilience as an outcome of how humans actively engage with ML in ZDM. Hence, we argue why transformative resilience is important to better be able to address adverse events such as a cyber threat situation (e.g., a defect), that may slow down or harm the manufacturing process (e.g., increasing vulnerability). Additionally, our contribution highlights the

reasons and thus importance of developing a cyber security culture for ZDM to enable a safe and transparent foundation for transformative resilience.

This paper is organized as follows. In the next section, the concepts I4.0, ZDM and ML, and ML challenges are explained. Further, we address cyber security as a critical aspect in relation to these concepts, presenting transformative resilience and security culture as new human-centric dimensions for ZDM. Finally, the method, discussion, concluding remarks, and suggestions for further research are presented.

## 2 Theory

### 2.1 Industry 4.0 and Zero-Defect Manufacturing (ZDM)

I4.0 has mainly centered on technology and the techno-centric approach in relation to industrial automation, predicting errors, identifying defects and defects causes, etc. From this view, humans have to a larger extent followed technology and not the other way around to adapt to human needs and ways of working [15]. The recent transition to I5.0 draws on the socio-technical systems approach where issues of human and technology reconciliation are heavily emphasized [16].

In the background though, the pursuit of both I4.0 and I5.0 saw the rapid advancement of technologies such as AI, ML, and industrial internet of things (IIoT) for production automation and the emergence of the ZDM concept to minimize the effects of traditional quality improvement methods targeting zero defects. Psarommatis et al., [17] have argued that the combination of advanced digital technologies with ZDM will become the new benchmark for companies working towards sustainable and resilient manufacturing.

I4.0 technologies have in the past been seen to support ZDM. The industrial application of ML in particular helps in defects management, e.g., defect detections, logging imperfections, or conducting root cause analyses [17]. Quality defects are costly and may ruin an organization's reputation. They also involve a waste of resources and time.

Zero-defect Manufacturing has been defined as a target-based approach where the goal is to decrease and mitigate failures within manufacturing processes and 'to do things right the first time' [17].

The augmentation of I4.0 technologies such as ML with ZDM has made it possible to reduce the costs often associated with defective products, and reduced inspection points throughout the manufacturing process, guaranteeing that no defective product is delivered to the customer [17].

Defects represent characteristics of products that do not conform to their quality standard [18]. Many proponents of ZDM and I4.0 have argued that most defects in manufacturing are due to human mistakes or errors hence the arguments for ML [1]. However, an alternative view offered by proponents of I5.0 is that ZDM needs the co-existence of humans and technology because of the inflexibility technology offers compared to humans. Using the example of a human operator in the production process, Oliveira et al., [19] argue that humans are the most important drivers of flexibility in manufacturing environments irrespective of how advanced automation systems are or how much artificial systems offer. Wan and Leirimo [20] argue that a "common pitfall on the journey towards ZDM is to implement cutting-edge technology, thinking that it will eliminate defects without prioritizing the role of humans in the manufacturing system".

In the next subsections, we examine the implications of the view from Pasquale et al., [1] where technologies such as ML have reduced human intervention because humans are viewed as a leading cause of error. Further on, we argue for the significance of human centrality applicable to the security aspect of ZDM and as a mechanism to enhance transformative resilience.

## 2.2 Why Resilience Matters

According to Psarommatis et al., [17] the combination of ZDM and I4.0 technologies such as ML increase not just flexibility in the production system but also resilience. According to Holling [21], resilience is an ecological concept describing a natural system's ability to continue functioning when facing an adverse event (e.g., shock). Resilience thus refers to "positive adaptation within the context of significant adversity" [22]. It involves an analysis following a "setback event" and emphasizes positive adaptation to such an event. A non-resilient response thus involves reintegration loss (e.g., lack of motivation, risk aversion) [23].

A framework to describe resilience was developed by Fisher et al., [10] and included: adversity triggers, resilience outcomes, resilience mechanisms, and resilience-promoting factors. Powley et al., [24] built further on this framework and included novelty and thus the accumulation of knowledge as part of resilience-promoting factors. An adversity trigger may relate to an unforeseen event such as a type of threat [25]. The novelty aspect is thus related to the rarity of events impacting "the perception of relevance and probability that leads to larger impact" [26]. Hence, it constitutes available knowledge on triggers. Hence, with low novelty regarding triggers, performance is brought back or recovered by resilience to its initial level of "bounce back" (e.g., recovery resilience) [27].

However, with higher novelty profiles (involving human understanding and response required to adapt to the change associated with triggers), adaptive and transformative resilience (reaching higher levels of performance) is possible. Transformative resilience thus involves the ability to "bounce beyond" the original novelty level [23]. This major novelty profile requires knowledge of which organizational functioning and outcome are transformed. Building on March [28], transformative resilience involves exploration and thus the ability to take risks, search, play, experiment, innovate, be flexible, and discover [24]. However, there is little research on team resilience, involving the link between individual-level behaviors and organizational-level processes [23]. Moreover, transformative resilience is a context-dependent concept. Hence, the significance e.g., of a specific focus and capacity may vary [29]. As such, we explore the concept of security culture related to manufacturing as a human-centered precondition for transformative resilience for ML towards ZDM.

## 2.3 Challenges of Machine Learning (ML) in ZDM

As argued earlier, ML is one of the key I4.0 technologies where ZDM offers a lot of promise. ML is a subfield of AI where machines perform computational algorithms that

turn empirical data into usable models and make predictions with minimal human intervention [30]. Usually, ML comprises two categories: supervised ML and unsupervised ML were later no human interventions.

Because ML models generally learn from data fed into them to identify patterns and automatically make predictions, they are well suited for ZDM including quality improvement projects where traditional methods in manufacturing are used.

The literature has many examples where many ML techniques have been applied to manufacturing operations to gain more insight into frequently occurring problems, or to help investigate possible system errors and explore reasons for various issues [3]. Studies (e.g., [31]) suggest that ML models may also address operational planning, and environmental and social sustainability because they provide supply chain visualization and traceability solutions, analyzing data based on risk. This makes it easier to increase productivity, product quality, reduce rework and costs, and enhance the transparency of the production process [30].

And yet unsupervised ML models have unique challenges but the biggest of all is the enormous volumes of data required to enhance decision quality. Wuest et al., [30] note that because of these limitations including the availability, quality, and composition of the manufacturing data, the performance of ML algorithms tends to not be good enough.

Perhaps the most important study which directly associates ML challenges to ZDM application is that of Papageorgiou et al. [3]. In their study of ML methods for root cause analysis, they identified 6 challenges, namely (1) explainability, where the black box nature of AI/ML models is difficult to comprehend by humans; (2) quality of training, where the lack and scarcity of adequate and suitable sources of data to train AI/ML models is cited; (3) standardization and interoperability, where companies use different architectures and protocol, which makes collaboration difficult; (4) data privacy, where access to private databases to train AI/ML is a challenge, (5) data security, where industrial applications demand more secure transactions that the current complexity of AI/ML models can't guarantee; and (6) the emergence of new technologies which may make integration with AI/ML difficult.

In this paper, we elected to focus on explainability and security in this case including both data privacy and data security from the challenges cited by Papageorgiou et al. [3]. These three challenges from the study directly underscore the human-centric perspective that is the core of the paper.

Explainability of AI models, sometimes described as XAI, is about making AI-model outputs understandable to humans for decision-making [32]. The argument developed by Papageorgiou et al. [3] is that due to the high complexity, and ambiguity including the inexplicit learning methods they employ, these models are difficult for human comprehension or more specifically for ZDM, humans may fail to establish the cause-and-effect relationship. According to Mugurusi and Oluka [32] augmenting the AI/ML decision loops with humans and using them as a basis for decisions. In some cases, AI systems may thus produce the wrong results in individual cases. Data privacy is significant in this matter because e.g., root cause analysis towards ZDM requires datasets from different production stages that could potentially expose sensitive information about the industrial provider. Hence, there is a security issue because the industrial environment requires secure transactions. The security aspect is therefore very important in relation to ZDM,

to prevent the leakage of sensitive or confidential information. Moreover, data integrity is necessary to prevent corruption and information loss which may lead to production downtime, defective products or even threaten the security and safety of employees and users [33]. AI and “smart” algorithms are already being used today to improve IT security for detecting malware and blocking “illogical” access attempts. But as it may fail to recognize complex threats, humans are an important factor in terms of recognizing and exposing attacks.

## 2.4 The Cyber Security Context

In the cyber security domain, human error is the most frequent cause of adverse incidents and thus a serious threat to the industry at large [34]. Moreover, as manufacturing is often placed within a socio-technological context (exchanging information between systems, people, and other organizations), confidentiality may be broken, disclosing information in unapproved ways [35]. Organizations not considering socio-technical factors may therefore not be able to respond properly or defend themselves from threats as they are lacking understanding of what is identified as a threat, and the impact of attacks [36]. Threats may be external (e.g., a hacker) or insider threats (e.g., an employee) who intentionally or unintentionally misuse organizational information or information systems [37]. Or it can be contextual factors like unfamiliar tasks (performed rapidly), not understanding the consequences of actions, tasks given insufficient attention, lacking supervision, and complex tasks that require high levels of understanding [38]. Hence, one of the reasons the human aspect is important regarding information security is due to unintended errors associated with using technologies [39]. As the manufacturing setting becomes more complex and unpredictable (e.g., crises) there is a need for higher levels of understanding and skills [39]. Creating a cyber security culture could thus be one way to enhance transformative resilience.

## 2.5 Cyber Security Culture

A security culture is the collection of shared values and mindsets in organizations facilitating different ways of thinking, feeling, and action on expectations of how employees should go about security [12]. Consequently, it is key to limit information leakage and provide effective information sharing [40]. A security culture involves trust (in terms of aligning security practice with everyday routines/not assuming malicious behavior) [41], creating security awareness and knowledge of security procedures to such an extent that it becomes a part of employees’ work identity. Moreover, it involves understanding own vulnerabilities, risks, what is identified as a threat, and the impact of attacks [36].

Regarding risk, there exist disagreements on whether regulations are efficient mitigation tools as humans are perceived as the weakest link. Hence, securing system design involves understanding what makes it insecure [42]. Not trusting and constraining humans by assuming malicious behavior might thus impact responsible behavior negatively, facilitating “non-complacency”, and a culture of mistrust [34]. Creating a culture where humans willingly share cybersecurity responsibility, might thus result in early detection and prevention of threats in ML/ZDM environments [34]. Equally important,

the sense of community, involvement and open communication might enhance motivation to follow security requirements [43]. Furthermore, human needs and limitations should be given attention regarding system design [34]. This involves integrating humans in the decision-making and development of technologies (e.g., machine learning). Enhanced transparency and understanding across disciplines within the manufacturing process may thus make it easier to make better decisions.

In this paper, we further examine the role of security culture to mediate the relationship between human-centered ML/ZDM and transformative resilience.

### 3 Method

A conceptual approach has been adopted in this paper. The theory on ZDM is not well developed as it is a very recent concept even if there are notable applications in industry [17, 44]. The absence of descriptive or even exploratory models to allow the formulation of hypotheses and propositions that can be tested against reality can be detrimental to theory building [45]. Typically, the adoption of conceptual methods in this study of ZDM should remedy such inconsistency.

Conceptual research methods infer among other things, the development of an initial scheme of a few explored situations of interest, either quantitatively and/or qualitatively in order to simplify/classify/conceptualize/taxonomize the elements associated with those situations [46]. Besides their theory-building properties, Meredith [45] argued that conceptual methods increase the external validity of research conclusions and lead to a better balance between theory-building and theory-testing research.

The arguments made earlier, and the basis of our forthcoming discussion is based on three major important studies which include that of Powell et al., [44], Psarommatis et al., [17], and Caiazzo et al., [47]. Among these three formative literature reviews on ZDM, only Psarommatis et al., [17] cite a finite relationship between technology and AI/ML when the three ZDM strategies (i.e., detection, repair, prediction, and prevention) are analyzed. Powell et al., [44] recognize that AL/ML, Big data, IIoT, and extended reality will become key enabling technologies for ZDM in the future. Caiazzo et al., [47] believe that as smart factories become common, ZDM will exploit I4.0 for data acquisition and storage, automatic signal processing, data mining, and knowledge discovery for diagnosis and prognosis, monitoring of process parameters, online predictive maintenance, and re-configuration and re-organization of production. Seamless integration of humans and technology into ZDM contributes to better data-driven flexibility hence resilient production systems [3]. Oliveira et al., [19] believe the human worker represents a key driver for flexibility in manufacturing environments with high levels of automation irrespective of how flexible these systems are.

## 4 Discussion and Concluding Remarks

### 4.1 Security Culture as a Human-Centered Precondition for Transformative Resilience in ML/ZDM Environments

Building on the arguments of e.g., Pasquale et al., [1]; Oliveira et al., [19]; Lu et al., [14]; Wan and Leirimo [20] and thus the importance of involving humans in the manufacturing system, we suggest a new way of thinking about ZDM. As such, we emphasize

the security aspect of using ML for ZDM, by including the concepts of *security culture* and *transformative resilience*. Our argument derives from the importance of involving humans related to technology development and uses for ZDM. For example, in times of e.g., crisis and uncertainty, the manufacturing systems and networks involving technologies may become more vulnerable to threats, due to rapid changes. This enhances the need for new learning, flexible decision-making, and adaptation. Moreover, with the manufacturing setting becoming more complex and unpredictable, we need higher levels of understanding, and skills (e.g., [38]). In this sense, ML and ZDM involve a change in the way humans understand, use, and adapt to technologies, as well as how they make decisions.

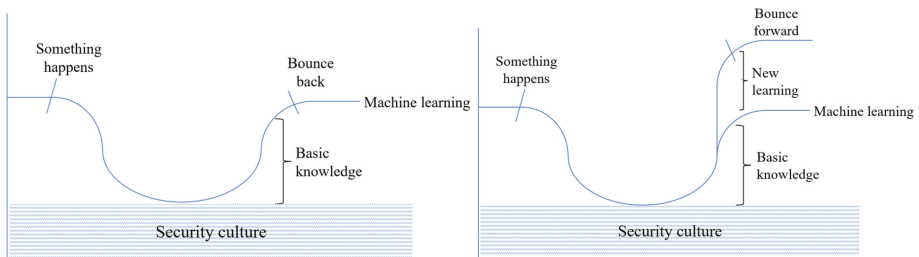
In addition to humans following and thus working in accordance with technologies such as ML, ML needs to be more understandable to humans (involving learning from ML) in the process of decision-making. Hence, as technologies such as ML require learning over time to make good decisions, ML may only be useful up to a certain level providing only basic knowledge (Fig. 1) in the absence of human involvement. Hence, if something happens e.g., a cyber threat, it may only be possible to “bounce back” to the original novelty level [23]. In the same way, humans must understand ML to contribute to new learning and thus higher levels of novelty [24] in relation to making the best decisions for ZDM. However, facing an adverse event/trigger such as a cyber threat situation requires flexible decision-making and creative ways of thinking (contributing to new or enhanced learning). Humans, as they are often left out and viewed as a threat, may due to their more flexible and playful nature [28] provide higher levels of novelty in such situations, given the right preconditions. As such transformative resilience means that problems may be solved at a higher level, making it possible to “bounce beyond” the original novelty level [44].

Under those circumstances, our argument and thus the scientific contribution of this paper is that we view transformative resilience as an enabler for humans to actively engage with ML for ZDM. Hence, we argue that transformative resilience is important to better be address adverse events such as cyber threats (e.g., a defect), that may slow down and harm the manufacturing process. Additionally, our contribution highlights the importance of developing a security culture for zero defects to enable a safe and transparent foundation for transformative resilience. For example, as a security culture values trust, awareness, involvement, and open communication, it may lower the threshold for admitting mistakes (e.g., insider threats), facilitating better opportunities to correct the mistakes made and understand own vulnerabilities. An enhanced understanding of one’s vulnerabilities and risks might thus make it easier to respond properly to threats. Moreover, involving humans and cooperating across organizational levels in relation to ML, could facilitate understanding, meaning creation, positive emotions, clarity, and a sense of relevance. Hence, empowering and encouraging humans to embrace change and adopt technologies. As the European Commission stresses the importance of adaptation and transformation in relation to staying safe from adverse events (e.g., crises), we stress emphasizing the values consistent with a security culture as a highly relevant and sustainable (human-centered) intervention to enhance transformative resilience towards engagement and new learning in relation to ML towards ZDM. This means that managers and/or engineers should take a holistic perspective in creating technology and quality



standards that resonate with the operators. Conversely, engineers need to understand the needs of the operators to make technical changes. As such, using ML for quality inspection to predict and detect defects along with the involvement of human capabilities.

Rather than viewing humans as a threat in relation to ML and ZDM, we argue that humans should be viewed as a resource that can drive flexibility thus making better decisions (transformative resilience), given the right preconditions (e.g., security culture). In Fig. 1 we illustrate the reflexive impact of having humans in the loop. Humans bring a unique understanding of ZDM processes at the tacit knowledge level that even advanced deep learning and ML models lack. This knowledge is cognitively flexible and has been described by Willingham [48] as flexible knowledge. It is this kind of knowledge that provides manufacturing firms these bounce back and bound forward capabilities when technologies have blackbox challenges. Consequently, our contribution suggests a human-centric understanding of ML/ZDM environments by considering security culture as a resilience-promoting factor for transformative resilience in organizations. Thus, we propose a new way for industrial organizations to think about and approach ZDM.



**Fig. 1.** The mechanics of transformative resilience in ML/ZDM environments

## 4.2 Further Research

From a human perspective to secure system design, Bella et al., [42] we need to understand what makes it insecure. Hence, we argue that empirical research is needed. This may relate to qualitative methods on enhancing insight into what type of threats are associated with ML (or other AI technologies) and ZDM, and how this may be addressed from a human and organizational industry perspective. As such, management challenges in relation to the use of ML related to ZDM, involving decision-making, could be emphasized, as well as the barriers and possibilities of implementing ML. For example, identifying vulnerable areas, understanding what type of AI technology organizations use, in relation to what stages or areas in the manufacturing process they use them, type of information exchanged between what systems and people, etc. Under those circumstances, it is essential to know employees' needs and understanding of the ML technologies, and how engineers, managers, and operators cooperate in relation to developing these technologies for different parts of the manufacturing process. As such, exploring what factors may make it easier in relation to facilitating a safe, transparent, and resilient work environment (security culture) that involves and empower workers. Consequently,

there is a need for a contextual and empirical understanding of what security culture and transformative resilience are in relation to ML towards ZDM to better address adverse events such as a cyber threat situation.

## References

1. Pasquale, S., Miranda, S., Neumann, W.P., Setayesh, A.: Human reliability in manual assembly systems: a systematic literature review. *IFAC PapersOnLine* **51**(11), 675–680 (2018)
2. Global risks report 2022. World Economic Forum (2022). <https://www.weforum.org/reports/global-risks-report-2022>. Accessed 30 Jan 2023
3. Papageorgiou, T., et al.: A systematic review on machine learning methods for root cause analysis towards zero-defect manufacturing. *Front. Manuf. Technol.* **2**, 972712 (2022)
4. Mark, M.S., Tømte, C.E., Næss, T., Røsdal, T.: Leaving the windows open—økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk sosiologisk tidsskrift* **3**(3), 173–190 (2019)
5. Pollini, A., et al.: Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn. Technol. Work* **24**(2), 371–390 (2022)
6. Skierka, I.: When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Gov. Inf. Quarterly* **40**(1), 101781 (2023)
7. Kott, A., Linkov, I.: To improve cyber resilience, measure it. arXiv preprint [arXiv:2102.09455](https://arxiv.org/abs/2102.09455) (2021)
8. Groenendaal, J., Helsloot, I.: Cyber resilience during the COVID-19 pandemic crisis: a case study. *J. Contingencies Crisis Manag.* **29**(4), 439–444 (2021)
9. Giovannini, E., Benczur, P., Campolongo, F., Cariboni, J., Manca, A.R.: Time for transformative resilience: the COVID-19 emergency. No. JRC120489. Joint Research Centre (Seville site) (2020)
10. Fisher, J.M., Ragsdale, J.M., Fisher, E.C.S.: The importance of definitional and temporal issues in the study of resilience. *Appl. Psychol.* **68**(4), 583–620 (2019)
11. Malatji, M., Von Solms, S., Marnewick, A.: Socio-technical systems cybersecurity framework. *Inf. Comput. Secur.* **27**(2), 233–272 (2019)
12. Wen, K.M., Kowalski, S.: An empirical study of security culture in open-source software communities. In: 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 863–870 (2019)
13. Adel, A.: Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas. *J. Cloud Comput. Adv. Syst. Appl.* **11**(1), 40 (2022)
14. Lu, H., et al.: Outlook on human-centric manufacturing towards Industry 5.0. *J. Manuf. Syst.* **62**, 612–627 (2022)
15. Neumann, W.P., Winkelhaus, S., Grosse, E.H., Glock, C.H.: Industry 4.0 and the human factor—a systems framework and analysis methodology for successful development. *Int. J. Prod. Econ.* **233**, 107992 (2021)
16. Xu, X., Lu, Y., Vogel-Heuser, B., Wang, L.: Industry 4.0 and Industry 5.0—inception, conception and perception. *J. Manuf. Syst.* **61**, 530–535 (2021)
17. Psarommatas, F., May, G., Dreyfus, P.A., Kiritsis, D.: Zero defect manufacturing: state-of-the-art review, shortcomings and future directions in research. *Int. J. Prod. Res.* **58**(1), 1–17 (2020)
18. Crosby, D.C.: Quality is easy. *Quality* **45**(1), 58 (2006)
19. Oliveira, M., Arica, E., Pinzone, M., Fantini, P., Taisch, M.: Human-centered manufacturing challenges affecting European industry 4.0 enabling technologies. In: Stephanidis, C. (ed.) HCII 2019. LNCS, vol. 11786, pp. 507–517. Springer, Cham (2019). [https://doi.org/10.1007/978-3-030-30033-3\\_39](https://doi.org/10.1007/978-3-030-30033-3_39)

20. Wan, P.K., Leirimo, T.L.: Human-centric zero-defect manufacturing: state-of-the-art review, perspectives, and challenges. *Comput. Ind.* **144**, 103792 (2023)
21. Holling, C.S.: Resilience and stability of ecological systems. *Annu. Rev. Ecol. Syst.* **4**(1), 1–23 (1973)
22. Luthar, D., Cicchetti, D., Becker, B.: the construct of resilience: a critical evaluation and guidelines for future work. *Child Dev.* **71**(3), 543–562 (2000)
23. Hoegl, M., Hartmann, S.: Bouncing back, if not beyond: challenges for research on resilience. *Asian Bus. Manag.* **20**(4), 456–464 (2021)
24. Powley, E.H., Barker Caza, B., Caza, A. (eds.): *Research Handbook on Organizational Resilience*. Edward Elgar Publishing, Cheltenham (2020)
25. Westrum, R.: A typology of resilience situations. In: Hollnagel, E., Woods, E. (eds.) *Resilience Engineering*, 1st edn., pp. 55–65. CRC Press, Boca Raton (2006)
26. Lampel, J., Shamsie, J., Shapira, Z.: Experiencing the improbable: rare events and organizational learning. *Organ. Sci.* **20**(5), 835–835 (2009)
27. Shen, Y., Cheng, Y., Yu, J.: From recovery resilience to transformative resilience: how digital platforms reshape public service provision during and post COVID-19. *Public Manag. Rev.* **20**(5), 835–845 (2022)
28. March, J.G.: Exploration and exploitation in organizational learning. *Organ. Sci.* **2**(1), 71–87 (1991)
29. Asadzadeh, A.R., Khavarian-Garmsir, A.R., Sharifi, A., Salehi, P., Kötter, T.: Transformative resilience: an overview of its structure, evolution, and trends. *Sustainability* **14**(22), 15267 (2022)
30. Wuest, T., Weimer, D., Irgens, C., Thoben, K.D.: Machine learning in manufacturing: advantages, challenges, and applications. *Prod. Manuf. Res.* **4**(1), 23–45 (2016)
31. Ni, D., Xiao, Z., Lim, M.K.: A systematic review of the research trends of machine learning in supply chain management. *Int. J. Mach. Learn. Cybern.* **11**, 1463–1482 (2020)
32. Mugurusi, G., Oluka, P.N.: Towards explainable artificial intelligence (XAI) in supply chain management: a typology and research agenda. In: Dolgui, A., Bernard, A., Lemoine, D., von Cieminski, G., Romero, D. (eds.) *APMS 2021. IAICT*, vol. 633, pp. 32–38. Springer, Cham (2021). [https://doi.org/10.1007/978-3-030-85910-7\\_4](https://doi.org/10.1007/978-3-030-85910-7_4)
33. Von Faber, E., Kohler, A.: The gap: information security in systems with artificial intelligence How algorithms and artificial intelligence can pose a threat to IT security. *Datenschutz und Datensicherheit - DuD.* **43**(7) (2019)
34. Zimmermann, V., Renaud, K.: Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *Int. J. Hum. Comput. Stud.* **131**, 169–187 (2019)
35. Song, G.A., Fink, G.A., Jeschke, S.: *Security and Privacy in Cyber-Physical Systems*, 1st edn. Wiley, Chichester (2017)
36. McEvoy, R., Kowalski, S.: Cassandra’s calling card: socio-technical risk analysis and management in cyber security systems. In: *STPIS@ ECIS*, pp. 65–80
37. Liu, L., De Vel, O., Han, Q.-L., Zhang, J., Xiang, Y.: Detecting and preventing cyber insider threats: a survey. *IEEE Commun. Surv. Tutor.* **20**(2), 1397–1417 (2018)
38. Williams, J.C.: *A User Manual for the HEART Human Reliability Assessment Method*. DNV Technica (1992)
39. Evans, M.G., He, Y., Yevseyeva, I., Janicke, H.: Published incidents and their proportions of human error. *Info. Comput. Secur.* **27**(3), 343–357 (2019)
40. Wong, W.P., Tan, K.H., Govindan, K., Li, D., Kumar, A.: A conceptual framework for information-leakage-resilience. *Ann. Oper. Res.* 1–21 (2021)
41. Burdon, M., Coles-Kemp, L.: The significance of securing as a critical component of information security: an Australian narrative. *Comput. Secur.* **87**, 101 (2019)

42. Bella, G., Curzon, P., Lenzini, G.: Service security and privacy as a socio-technical problem: literature review, analysis methodology and challenge domains. *J. Comput. Secur.* **23**(5), 563–585 (2015)
43. McGregor, S.E., Watkins, E., Caine, K.: Would you slack that? *Proc. ACM Hum.-Comput. Interact.* **1**(CSCW), 1–22 (2017)
44. Powell, D., Magnanini, M.C., Colledani, M., Myklebust, O.: Advancing zero defect manufacturing: a state-of-the-art perspective and future research directions. *Comput. Ind.* **136**, 103596 (2022)
45. Meredith, J.: Theory building through conceptual methods. *Int. J. Oper. Prod. Manag.* **13**(5), 3–11 (1993)
46. Mora, M., Gelman, O., Paradice, D., Cervantes, F.: The case for conceptual research in information systems. In: *CONF-IRM 2008 Proceedings*, p. 52 (2008)
47. Caiazzo, B., Di Nardo, M., Murino, T., Petrillo, A., Piccirillo, G., Santini, S.: Towards Zero Defect Manufacturing paradigm: a review of the state-of-the-art methods and open challenges. *Comput. Ind.* **134**, 103548 (2022)
48. Willingham, D.T.: Inflexible knowledge: The first step to expertise [blog]. *American Educator* (2002). <https://www.aft.org/periodical/american-educator/winter-2002/ask-cognitive-scientist>. Accessed 4 Jan 2020