IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 July 2024, accepted 8 August 2024, date of publication 12 August 2024, date of current version 21 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3442443

SURVEY

The Impact of Integrating Information Technology With Operational Technology in Physical Assets: A Literature Review

ARNO KOK[1,2], ALBERTO MARTINETTI[1], AND JAN BRAAKSMA[1]
[1]Department of Design, Production and Management, University of Twente, 7522 NB Enschede, The Netherlands
[2]Nederlandse Spoorwegen N.V., 2031 CC Haarlem, The Netherlands

Corresponding author: Arno Kok (a.t.kok@utwente.nl)

This work was supported in part by Holland High Tech with a PPP grant for Research and Development in the Top Sector HTSM and Nederlandse Spoorwegen (NS).

ABSTRACT The convergence of information technology (IT) with operational technology (OT), within physical assets can enhance performance but also presents challenges due to higher performance expectations and increased complexity. This study reviews the research that has been conducted to address these convergence and integration challenges by using an in-depth review of academic papers, industry standards, and reports published during the last three decades. Our investigation reveals that about a third of the existing IT/OT research really focuses on the convergence of IT/OT, by including organizational aspects into the study. Three key research domains were identified: maintenance, cybersecurity, and configuration management. The introduction of IT in assets has necessitated changes in maintenance practices, as current approaches are not suitable for these converged lifecycles. Cybersecurity risks have received the most attention in the IT/OT domain. The integration requires the management of these changes; therefore, configuration management has become more crucial than it already is to keep of actual configuration of both the IT and the OT parts of the asset. This research hereby provides relevant observations for practitioners in industry and academics in the IT and the physical asset management domain. The identified gaps suggest the need for tools and methods to better align IT and OT standards, policies, tools, processes, and people throughout the lifecycle of an IT/OT converged physical asset in a sustainable way.

INDEX TERMS Asset management, maintenance management, maintenance engineering, systems integration, critical infrastructure, software maintenance, configuration management, fault diagnosis, industrial cybersecurity.

I. INTRODUCTION

Originally, physical assets consisted of physical electromechanical systems. In the last three decades, these systems are often controlled by operational technology (OT) [1]. The next step was the introduction of information systems (IT) into these assets. Initially, these IT systems were used as an addition to these assets, not impacting the availability of the asset. However, with IT being increasingly entwined within an asset, managing this IT integration becomes key. The integration of IT is different from the integration of physical or OT systems as IT consists of software and hardware for information processing [2] which is different from controlling physical processes. The focus of IT is on confidentiality, integrity, and availability [3], whereas the focus of OT is on safety and reliability. The OT that controls assets are also known as ''industrial control systems'' (ICS) [3]. The differences between IT, OT and Physical systems are depicted in Fig. 1. In this research when we talk about IT/OT converged assets or systems we talk about assets that consist of all three domains depicted in Fig 1. Furthermore, we view IT/OT converged systems from a mechatronic perspective and see them as a specific type of Cyber-physical system (CPS) [5]. This originates from Hehenberger [4], who describes that

The associate editor coordinating the review of this manuscript and approving it for publication was Porfirio Tramontana.

mechatronic systems can evolve into CPS and eventually into the Internet of Things (IoT). Notably, Bricogne et al. [6] observe that mechatronics and CPS communities have limited interaction but are both looking at the same thing from a different perspective.

There are several benefits of this IT/OT integration, such as improved performance, and lower costs [4]. System integration plays a role in several domains we have scoped system integration specifically to IT/OT integration on large systems and assets e.g., in railways, critical infrastructure etc. with an industrial application where the focus is on the effects of the integration in the physical system.

In this research, the following definitions are used:

IT/OT Integration: Focuses on bridging the gap between IT systems (business processes, data analysis, etc.) and OT systems (industrial operations, real-time control, etc.) within an organization [5].

IoT: Involves creating a broad network of interconnected devices that can operate across various domains and industries, extending beyond a single organization's boundaries [6].

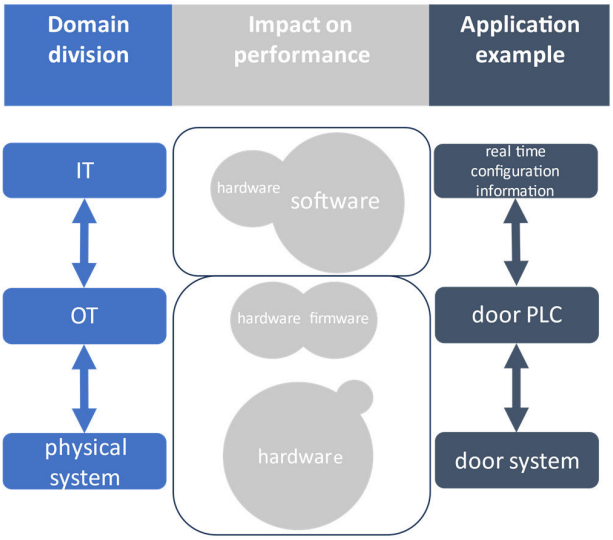

FIGURE 1. Difference between IT, OT, and physical systems.

IT/OT converged systems have become more complex with the introduction of IT in OT [7]. Therefore, traditional maintenance approaches aimed at managing OT do not always fit digital problems. Moreover, the lifecycles of IT and OT typically do not match. As a physical asset often has a lifecycle of multiple decades, an IT system is often replaced after a few years [8]. Al though the lifecycle stages of IT and OT might appear similar, they have two differences. Firstly, the software part of IT has no formal 'production stage', and instead quality assurance is essential [9]. Secondly, the software part of IT evolves during the deployment and maintenance phase, while physical assets need maintenance to counteract physical degradation [10]. Managing assets during the various stages of their life cycles is known as physical asset management. The objective of physical asset management is to optimize the usability and value of assets while minimizing risk and cost, which is recorded in the standard ISO 55000:2014 [11].

Although much has been written on IT/OT convergence, to the best of our knowledge, no specific review has been conducted on the integration of IT systems within OT systems in physical assets. This research was used to identify and group existing research gaps. Therefore, his research aims to understand the specific challenges of IT/OT converged systems through a literature review and to offer insights into how to better manage the challenges that arise when integrating IT within OT environments. In this review, the data collection was performed using (amongst others) published peer-reviewed journal articles, industry guidelines and standards.

II. METHODOLOGY

A. RESEARCH OBJECTIVES

This research aims to answer the following research question:

How can the impact of integrating IT systems within physical assets over their lifecycle be defined based on a literature review on managing distinct aspects of IT and OT?

Consequently, the specific objectives of this research are understanding the main challenges and differences in managing IT and OT and defining the concept of 'Asset Management of IT/OT converged systems'.

B. RESEARCH MATERIALS AND METHODS

In this research, the studies were reviewed using a five-step process depicted in Fig. 2. The first four steps are based on the work of Seuring & Müller [12]. These steps have been extended by adding a fifth step for making observations based on the work of Garg & Deshmukh [13].

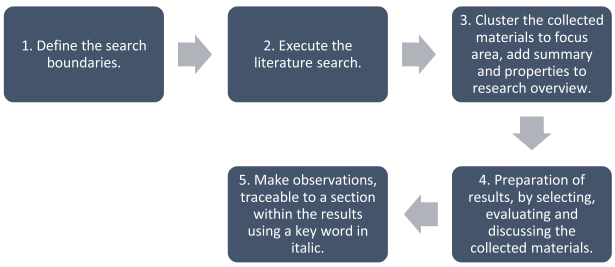

FIGURE 2. The research process that is adapted from Seuring and Müller [12] and Garg and Deshmukh [13].

The following four search boundaries are used within this research:

1. **Keywords**: The following keywords were used: 'physical asset management', 'literature review maintenance'. After scanning and reading the initial results closely, the following keywords were added: 'cyber physical systems', 'IT/OT', and 'operational technology'.

2. **Database**: This research was conducted using several databases, namely Google Scholar, Science Direct, IEEE Xplore, ACM Digital Library, Web of Science and Scopus. References cited in the relevant papers were used to find related materials and perform backwards snowballing [14].
3. **Analysis**: This analysis uses (conference) papers from scientific journals, dissertations, and theses, with a focus on maintenance, engineering, and interfaces within the domains of IT and OT. Interesting insights are also emerging within the corporate domain. Therefore, several industry studies (e.g., whitepapers) and industry standards are included in this research. This type of inclusion of non-academic sources is supported by a study by Dowdeswell et al. [15]. No restrictions were placed on the date of publication when selecting the studies.
4. **Exclusion criteria**: Studies, which only dealt with in-depth mathematical modelling and software were not within the scope of this research, it focusses not only on technical aspects but also on organizational ones. If the materials make bold claims about solutions, but in practice only show problems with IT/OT convergence and give no solutions, they are excluded from the review. Last, studies that did not fit within the content of the specific section were excluded after a close reading of the study.

This review investigates the trends within IT/OT converged systems and their practical implications for managing them. In each subsection of the results, a comparison between IT/OT and OT will be made in the form of a table. At the end of each results section observations will be presented.

III. RESULTS

Initially, 252 studies published till 2024 were identified using the selected keywords mentioned above. 139 studies were excluded based on the exclusion criteria. This brings the total number of studies included in this review to 113. The database containing the selected studies can be accessed via an online data repository, see Kok [16].

The first study in this review was published in 1985 and is about the management and maintenance of software systems. This first study does not discuss IT/OT, but the software management idea discussed here has many similarities with the asset management of OT assets. With the introduction of Industry 4.0 in 2010, research on these topics started to emerge, and the scientific community became more interested in it. In 2012 the concept of IT/OT convergence was introduced in a whitepaper by Chemdupati et al. [17]. Since 2015 the number of yearly publications within this field has been steadily increasing, see Fig. 3. Four individual studies, related to the history of IT/OT have been left out from Fig 3, to increase the readability of the figure.

In Fig. 4 the distribution by source of the publications can be found. In this figure, the category "other" represents sources such as industry standards.

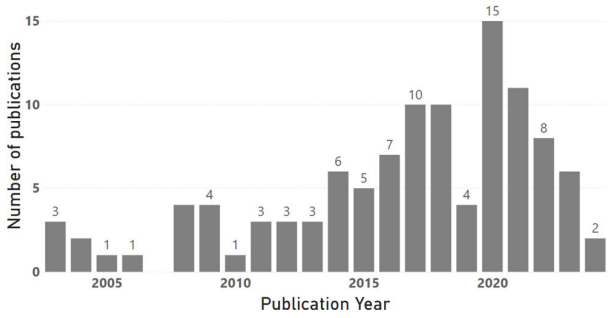

FIGURE 3. Distribution of reviewed publications by year, from 2003 onward.

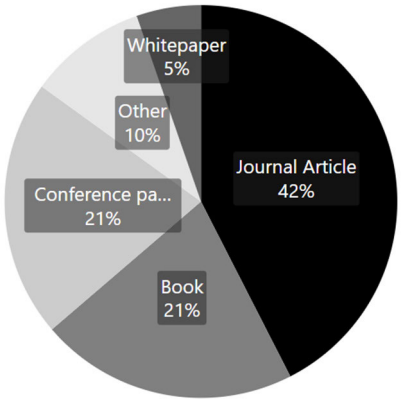

FIGURE 4. Distribution of studies according to source.

We have classified the different studies into four distinct categories.

1) IT only study, when the study is about IT-related aspects.
2) OT only study, when the study is about OT-related aspects.
3) IT/OT study, when the study is about IT and OT-related aspects.
4) Others, who do not fit in the above-mentioned categories e.g. studies on knowledge management

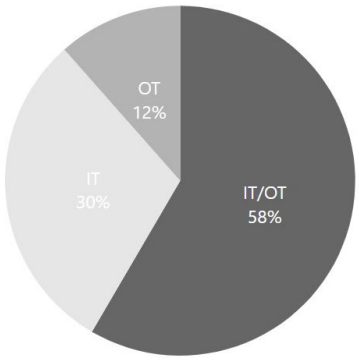

FIGURE 5. Classification of studies in the review into the topics of IT, OT, or IT/OT.

The high percentage of IT/OT studies in Fig 5 shows that there is a lively debate on IT/OT convergence and that the community is recognizing the struggles that are posed by this

convergence. However, only 29% of studies investigate how IT/OT convergence affects processes and organizations. Most of the studies focused on the technical requirements for IT/OT convergence and often on a single issue, such as cybersecurity aspects.

The differences between IT and OT lifecycles present various challenges to be overcome to ensure the long-term successful operation of IT/OT converged systems [18], [19], [4], [20], [21]. Based on these challenges we identified three key domains.

The first domain that we identified in the integration of IT with OT in physical assets through this review is maintenance. To ensure the performance and safety of an asset over its lifetime, maintenance is essential. Therefore, maintenance practices have evolved from unavoidable to a strategic concern [22]. Consequently, these maintenance practices need to evolve due to IT/OT convergence [23].

The second domain in the integration of IT with OT in physical assets is cybersecurity; in recent years, there have been numerous cybersecurity incidents, which have often led to financial and information losses. However, the effect of cyberattacks on IT/OT systems is much more severe than on IT assets since they can lead to physical injuries and even casualties [24]. This makes cybersecurity one of the main challenges during the lifecycle of an IT/OT converged system, as pointed out by Corallo et al. [21].

The third domain in the integration of IT with OT in physical assets is configuration management; to keep up with changes in assets, configuration management is essential. It provides traceability so that the locations of components, systems and software are known [25]. Additionally, as IT/OT convergence increases, so does the need for configuration management, due to shorter development times and greater product flexibility [26]. Unfortunately, the integration of configuration management practices of IT with those of OT remains difficult [27].

The three domains above will be discussed in further detail in the following subsections, see section A for maintenance, section B for cybersecurity and section C for configuration management.

TABLE 1. Maintenance - differences between IT, OT, and IT/OT, adapted from Pintelon & Parodi-Herz [22], Silvestri et al. [23] and Titu & Stanciu [29].

Aspect	IT	OT	IT/OT
Maintenance	Software updates	Physical components	Software updates & physical components
Access	Remote access via (open) networks	Physical access to the building or facility	Remote access via (open) networks and physical access to a building or facility
Connectivity	Remote connectivity, theoretically unlimited number of other systems	Components are not natively connectable, additional IT components are needed. Connectivity is limited to physically connected systems	Remote connectivity, theoretically unlimited number of other systems
Lifespan	Short, often much shorter than the OT lifecycle. Can reach end-of-life if supplier support stops	Long, typical lifetime of 20-40 years depending on the characteristics of an asset	The lifetime of the asset is long; however, the IT part of the asset is short, often much shorter than the OT lifecycle. Can reach end-of-life if supplier support stops

A. MAINTENANCE

1) DIGITIZATION OF MAINTENANCE

During the operational phase of an asset lifecycle, maintenance of both the hardware and the software is needed for the systems to continue to fulfil their functions. For hardware, maintenance is needed to keep up with degradation [28]. Several differences influence the maintenance of OT and that of IT systems, Table 1.

Maintenance practices can be improved due to IT/OT convergence, because the added connectivity can add functionality to predict/report possible failures. This reduces the need for corrective maintenance, which in return can increase uptime and minimize energy and material consumption. [28], [30]. So, to improve maintenance practices digitization of maintenance is needed, where remote monitoring and the management of assets is made possible [31]. Unfortunately, within the industry, there are many older systems without remote monitoring possibilities. Diaz-Elsayed et al. [32] argue that with limited investments, legacy hardware can be retrofitted so that remote monitoring becomes possible. Likewise, Sanchez-Londono et al. [33] provide a review of performance, risk, and cost optimization of assets by retrofitting legacy devices with remote monitoring capabilities.

Digital maintenance concepts can support this digitization process. Roda and Macchi [34] provide an overview and the differences between such maintenance concepts and conclude that these concepts will lead to better asset performance and lower costs. Using information from the manufacturing execution system (MES) is another way to improve maintenance activities as Skrzeszewska and Patalas-Maliszewska

[35] shows. The downside of this digitization is that the maintenance practitioner's role is becoming more difficult since not all traditional OT maintenance principles can be used in the IT/OT converged domain [18]. High level design principles for IT/OT convergence can help in overcoming this difficulty [36]; however, further work is needed to apply these ideas in an systems integration setting. Finally, Kuusk and Gao [37] suggest asset management companies to prepare for IT/OT integration in four steps, beginning with IT/OT convergence. In the next section, we will look at how the introduction of software affects maintenance.

2) SOFTWARE MAINTENANCE AND PERFORMANCE PREDICTION

On IT/OT converged systems not only the hardware needs maintenance but also the software part. However, software faults mostly occur due to defects that were introduced during the development phase [38]. This is in contrast with hardware faults, which often happen due to degradation [28]. In the 1970s the necessity of software maintenance was described by Lehman and is summarized in ''Lehman's Laws of Software Evolution'' [39]. One of the main points of this work is that a software program cannot be fully specified, because software requires constant evolution after it has been released. Which is different from hardware design, which can be fully specified.

Dvorak presents recommendations for software design when integrating IT systems within assets and shows that cultural aspects are hindering the implementation of these recommendations [40]. However, Osborne [38] states that software maintenance is frequently disregarded and managing the maintenance of software is a much broader practice than correcting errors. A thorough overview of the challenges around software maintenance is provided by Grubb and Takang [41].

Next, Koziolek [42] provides an overview of the characteristics of software architectures and explains that to maintain and develop long-lasting software systems, a software architecture is required. Then, Wong et al. [43] provide an overview of lessons learned from software bugs on software failures. Interestingly software failures are often discovered accidentally and usually resolved with troubleshooting e.g., by a system reset, instead of an in-depth investigation [44]. To counter software failures source code defects are often the place to start, however, timing, configuration and the environment of the system are a much bigger source of software failures in practice [45].

Due to the increased complexity of IT/OT converged systems, it is important to be able to predict the performance that includes both the software and the hardware aspects of an IT/OT converged system. During the development of physical assets, the Reliability, Availability, Maintainability, and Safety (RAMS) methodology is commonly used to achieve safe and reliable operation [46]. This OT approach to reliability evaluation, where failure modes are calculated along with their probabilities, does currently not automatically include IT/OT components [47].

However, there are examples of OT tools that do include software. First, Carlson [48], suggests that software aspects can be included in traditional failure mode and effect analysis (FMEA) analyses. Second, Oveisi and Ravanmehr [49] suggest evaluating the software component of an IT/OT system using both a software fault tree analysis (FTA) and software FMEA. Third, Medikonda and Ramiah [50] suggest combining FTA and FMEA techniques to improve the fault removal process of the software for systems that include both hardware and software components. They point out that these two methodologies are complementary to each other and are compatible with existing system-level techniques. Last, Zúñiga et al. [51] show that a traditional FMEA can be used on an IT/OT converged system, however modifications to the method seem necessary to improve risk prioritization. To overcome this, Tafur et al. [52] suggest combining FMEA with AutomationML, were the AutomationML is used to model the digital components of a system. In the next section, the effects of digitization on failure diagnosis are studied.

3) FAILURE DIAGNOSIS

During the life cycle of an asset, failure diagnosis helps in finding the root causes of problems; however, as assets become more digitized, finding faults becomes more difficult as multiple faults can lead to similar symptoms. This was observed by Kavulya et al. [53] who present an overview of automated fault diagnosis techniques for industrial applications. Dowdeswell et al. [15] present a very thorough overview of fault detection and diagnosis techniques of industrial cyber-physical systems. It is important to note that ''cyber-physical interactions can yield unpredictable cross-system failure propagations'' [54, p. 3]. Thus, good failure diagnosis is essential to discriminate between failures originating from the IT part of the system and the physical part of the system.

So, newly developed model-based and data-driven fault diagnostics have proven to be effective in identifying faults, not only in laboratories but also in real-world environments [15]. However, these models can only work correctly if they are trained with correct dat. Herzig et al. [55] examined more than 7000 reports and show that 39% never had a bug. This introduces bias in bug prediction models. As always preventing faults is better than correcting them, and this can be done by using prognostics, which involves predicting emergent failures [56]. Failures of software within IT/OT converged systems are still understudied as shown by Amusuo et al. [57]. In the last section, we will look at the organizational effects of this digitization of maintenance.

4) ORGANIZATIONAL ASPECTS

Simões et al. [58] provide a literature review into the performance of maintenance practices, they state that not only technical but also organizational aspects should be monitored.

Then Villar-Fidalgo et al. [59], also point in this direction as they state that the increased connectivity between assets, plants, and processes will result in more stakeholders needing to be managed and changes in the training of personnel are needed. Similarly, Bhatia and Kumar [60] demonstrate that companies that want to combine IT and OT should prioritize cooperation and teamwork. Makama and Telukdarie [61] propose an approach to improve the asset lifecycle management of an asset by improving the usage of data from these assets, it is essential that this approach is aligned with the goals of an organization.

Filz et al. [62] suggest that maintenance personnel can be employed more effectively by using a real-time failure mode and effect analysis (FMEA) to optimize maintenance planning. The main advantage of this approach is that risk assessment is no longer subjective. Similarly, He and Jin [63] indicate that by combining Industry 4.0 and CPS, it should be possible to create a self-organizing and self-maintaining production system, however, this is a costly solution which is only attainable for a handful of companies. However, as Temelkova [64] shows CPS and IT/OT converged assets are not the same, for example, a CPS consists often of an asset and a digital twin of this asset.

Therefore, they suggest that investing in human and organizational aspects seems more favorable. Next to organizational aspects Jantunen et al. [65] give an overview of technologies that can improve maintenance practices. Within this overview, they also identify several other non-technical barriers that hinder the implementation of available technologies e.g., uncertain return on investment.

5) OBSERVATIONS

By studying the literature on maintenance, several observations can be made that should be considered by the scientific community and industry.

1. *Digitization:* IT/OT convergence can improve maintenance performance. However, the role of the maintenance practitioner is becoming more difficult as traditional maintenance practices cannot always be applied to IT/OT converged systems.
2. *Performance prediction:* Tools are necessary to predict the reliability of IT/OT converged systems. Traditional OT tools do not include software and the nature of software faults is different from hardware faults.
3. *Failure diagnosis:* Failure diagnosis of IT/OT converged systems is only possible when a distinction can be made between failures originating in the IT or the OT components. More focus should be placed on preventing failures, as failure diagnosis becomes more complex due to the increasing complexity of IT/OT converged systems.
4. *Organizational aspects:* The literature strongly focuses on the technical aspects of asset digitization but indicates that organizational aspects also require attention due to the increased interconnections between systems and assets.

B. CYBERSECURITY

Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs, and data from attacks, damage, or unauthorized access. These techniques have received increasing attention in recent years, due to the increasing digitization within society and the growing convergence of IT with OT systems [66]. There are cyber threats specific to IT and OT. Combining IT and OT in an asset exposes the asset to the risks of both, see Table 2.

Therefore, IT/OT converged systems have a higher risk of suffering from unexpected failures due to increasing software and cybersecurity incidents [67], [68]. Industry guidance on how to control this risk can be found in a publication by Stouffer et al. [69]. However, a collective understanding and a standard principles on IT/OT converged system security seems to be absent [70]. Preventing these failures can be done by simulating cyber-attack and defense strategies by using digital twins, which are a representation of the real world in the cyber world [71]. The weak point in an IT/OT converged system is the link between IT and OT [72]. Kanamaru [73] shows that engineering measures are crucial to protect physical assets and that IT security measures are insufficient on their own.

TABLE 2. Cybersecurity - differences between IT, OT, and IT/OT, adapted from Sonkor & García de Soto [24].

ASPECT	IT	OT	IT/OT
Typical (possible) impact of attacks or security breaches	Financial and information losses	Physical injuries and casualties	Physical injuries, casualties, financial and information losses

In dealing with these increased cyber risks of IT/OT converged systems prevention is important, as described in the next section.

1) PREVENTION

In the prevention of cyber security incidents within IT/OT converged systems, several aspects are important. First, Alladi et al. [74] recommend monitoring and improvement of security practices to protect against cyber-attacks. Second, Khan et al. [75] make the case that current cybersecurity approaches are insufficient to protect IT/OT converged systems. Third intrusion detection using machine learning is a current research trend in providing a partial solution to cyber risks [76]. Besides the technical aspects of preventive action, companies need to have an organizational culture dedicated to cyber-security which should ensure that the company is continuously learning about aspects of cybersecurity.

Interestingly most of the studies on cybersecurity within the IT/OT context have a focus on the IT side and lack managerial perspective [77]. Alladi et al. [74] underline this

by providing an overview of several major cybersecurity incidents which occurred during the last two decades on existing OT assets and show that only 28% of organizations that had security incidents believe that preventing cyber-attacks is to be of high importance. This, as Annareli et al. [78] points out, is not how it should be as cybersecurity should be at the organization's core even more so for IT/OT converged systems. Nafees et al. [79] also emphasize the importance of human factors in achieving cybersecurity. Stouffer et al. [69] underline this by calling for a proactive collaboration between operators, OT engineers and management. Last, also Ani et al. [80] stress that the security of IT/OT integrated assets can only be achieved with a combination of people, process, and technology factors. Next to these factors, modelling can help in providing cybersecurity for IT/OT converged systems as pointed out in the next section.

2) MODELING

An overview of several important research areas of the current research on CPS security is provided by Alguliyev et al. [20]. One of these research areas is the modelling of CPS attacks. To defend an asset against a cyber-attack it is essential to understand how adversaries attack. Therefore, these models can be used to better understand this. For example, Assante and Lee [81] provide a model that helps defenders within the industry to understand a hostile cyberattack strategy.

A specific case of modelling is the identification of cyber risks, several authors have proposed frameworks for practitioners to help them manage those risks [82], [83], [84], [85]. Although these frameworks were not developed with IT/OT converged systems in mind, they are a useful place to start because they were developed by practitioners. A step towards IT/OT converged systems cyber risk management is proposed by Kriaa et al. [86], in which a traditional failure mode analysis is combined with a threat and vulnerability assessment to minimize the impact of a cybersecurity breach. A promising suggestion is made by Schmittner et al. [87] who propose an FMVEA, which extends a traditional FMEA analysis by including a vulnerability analysis.

3) OBSERVATIONS

By studying the literature on cybersecurity, three main observations can be made that should be considered by the scientific community and/or industry.

1. *Digitization*: Increasing IT/OT connection leads to more complex systems that pose a higher risk of unexpected failures due to software and cybersecurity incidents compared to unconnected systems.
2. *Organizational culture*: In addition to the technical aspects, companies need to have an organizational culture dedicated to cyber-security which should ensure that the company is continuously learning about aspects of cybersecurity.
3. *Models*: Models can be used to increase understanding of the risks and effects of cybersecurity incidents of IT/OT converged systems.

C. CONFIGURATION MANAGEMENT

The configuration of an asset is the combination of the requirements, architecture, and specific implementation of these aspects into the actual system or asset [88]. Configuration management (CM) consists of several distinct steps: planning, identification, change control, status accounting and configuration audit [89], [90], [91], [92]. Managing all this information during system development becomes increasingly important and more difficult since multiple disciplines need to work together, as Capilla et al. show [93]. However, the different tools that support CM of IT and that of OT do not match. There are two main differences between those tools. First, OT CM tools focus on the production phase whereas IT CM focuses on the development phase [94]. Second, IT CM tools need to be able to deal with more changes as software is easier to change due to its digital nature [95], [96]. Table 3 provides an overview of the differences between the configuration management aspects of OT and IT.

TABLE 3. Configuration management - differences between IT, OT, and IT/OT, adapted from Krikhaar et al. [26], Cline [25] and Barrios et al. [27].

ASPECT	IT	OT	IT/OT
Configuration management	Important, to keep track of the software components	Important, to be able to maintain the system	Essential for identification of (failing) components
Status after initial engineering	Permanently under construction with frequent upgrades	Moderate changes, several changes can occur during its lifecycle	Frequent upgrades
Development time	Short, changes are implemented after virtual testing	Long, changes are implemented after testing on-site and commissioning.	Medium, changes are implemented after virtual testing, testing on-site and commissioning.

In the case of IT/OT converged systems, the tools supporting configuration management should become more integrated [94], [97]. To support this CM/SCM integration harmonization and further development of existing industrial standards are needed [98] and, requirements should be formulated to guide this development process [99]. Unfortunately, this challenge is broader than the field of configuration management since it requires cross-sector collaboration between the fields of IT and OT [100], [101].

However, this is not an easy task as Kuusk et al. [102] emphasize that the IT and OT teams should work together to deal with these integration problems. As this integration can be difficult, Poliński and Ochociński [103] suggest that

partnerships between industry and educational providers are needed. Along these lines, Roda and Macchi [34] suggest that new interdisciplinary forms of education are required to achieve and sustain the necessary level of knowledge to maintain IT/OT converged systems. Last, traceability and reuse of knowledge are crucial components for executing shared design between OEM and supply chain partners within the system integration context [104]. The next section will discuss the importance of architecture to be able to keep track of the configuration of an IT/OT converged system.

1) ARCHITECTURE

An architecture is a graphical representation of different (software) components of a system, and how they interact [105], [106]. This architecture helps to manage the configuration of a system during design and operation. Moreover, to develop an electromechanical system, a set of requirements must be fulfilled. However, in the development of large systems, like IT/OT converged systems creating and maintaining an architecture is essential [106], [107], since IT becomes the core of the system. Therefore, architecture becomes important to manage the configuration and different architectural models can be found in the literature to manage such architecture.

Multiple of these architectural models are created from the IT or software perspective, where limited attention is paid to the OT or hardware layer, such as [108], [109]. Others do include a hardware layer but mostly focus on the different software layers [110], [111], [112], [113], [114]. One of the main challenges for IT/OT converged systems is how to manage all those different layers, not only the software layers but also the hardware layers. So that they continue functioning during operation, especially when systems are interconnected. Therefore, Cardin [115] creates a model which identifies two layers: In the first layer the IT is clustered and in the second the OT is clustered, including the hardware itself. Last, Nakagawa et al. [116] find that interoperability and legacy industrial systems are not well represented in the current body of literature. To achieve interoperability interfaces between the various parts are essential. Therefore, in the next section, the importance of interface management will be highlighted.

2) INTERFACE MANAGEMENT

An architecture consists of different elements connected via *interfaces*. Francalanza et al. [117] state that interfaces form the main challenges when designing the physical side of an IT/OT converged system. Carlson [48] underscores this by arguing that 50% of the problems within systems occur at an interface. This generates a need to implement some type of interface management approach. Davies [118] emphasizes this and states that interface management is an essential element of engineering systems. When building upon the architecture, these interfaces need to be managed during the subsequent design phases. Blyler [119] provides a general overview of how to design interfaces, and how to use technical performance measurement as a tool for managing interfaces during these phases. As this does not necessarily work for IT/OT converged systems, David et al. [120] propose an architecture for the integration into existing production environments which includes physical, human and data interfaces. Yasseri and Bahai [121] propose a more cost-effective and efficient process method for interface management design, which involves decomposing the system into subsystems and mapping the dependencies between systems.

The methods mentioned above focus on the technical aspects of managing interfaces. Penas [122] observes that not only the physical interfaces should be considered, nonetheless it should also be considered that the organizational aspects of interfaces are important. For example, there should be a mutual understanding between system designers of the implications of data when it is exchanged between systems or software components [123]. When systems are designed, the governance of these systems becomes important since data is the backbone of an IT/OT converged system. Yebenes Serrano and Zorrilla [124] provide a data governance architecture for these types of systems. Kuusk [125] emphasizes that holistic data governance is necessary for successful IT/OT convergence, which can be regarded as one of the building blocks for IT/OT asset management. Lastly, Kääriäinen [126] underscores this by demonstrating that the difficulty of CM practices increases during the lifecycles of large, multisite hardware/software systems; they stress that interface management is crucial in the development of complex systems.

3) OBSERVATIONS

Several observations can be made based on the studied literature on configuration management that should be considered by the scientific community and/or industry.

1. *Tool integration*: CM of OT and CM of IT practices have some essential differences. For example, the focus on the production phase within OT CM tools. In case of IT/OT converged systems, these OT and IT CM practices and tools need to be integrated.
2. *Architecture*: Due to IT/OT convergence IT becomes increasingly the core of the system, making good architecture more important for reliable performance.
3. *Interfaces*: During the operational phase of an IT/OT converged system, interfaces need to be managed.
4. *Organizational aspects*: With the addition of IT to the OT teams, the organizational and cultural aspects of CM are increasingly important in addition to technical ones.

IV. DISCUSSION AND RESEARCH GAPS

In each of the results sections, IT and OT development are compared using the insights gained from the literature, see Table 4 for an overview. The table shows that there are several differences in managing IT, OT, and IT/OT systems.

TABLE 4. General observations - extended comparison between managing IT, OT and IT/OT systems based on the observations from the results sections.

Aspect	IT	OT	IT/OT
Interconnection with other systems (interfaces & integration)	Integrated, many software interfaces.	Stand-alone, only interfaces within the system itself.	Integrated, many soft and hardware interfaces.
Failure diagnosis	Medium, specialized IT tools and training are needed.	Fairly straightforward, basic tools and training are needed.	Difficult, specialized IT and OT tools and training are needed.
Digitization	High, fully interconnected.	Low, often electromechanical systems.	Medium, electromechanical systems with some sort of connectivity via IT.
Monitoring	Essential, without monitoring maintenance of the system is exceedingly difficult.	Optional, maintenance on the system is possible without monitoring.	Essential, without monitoring maintaining the system becomes exceedingly difficult. For example, finding faults becomes almost impossible.
Performance prediction	Optional, reliability of software systems is less important and can be improved more easily	Essential, the reliability of the system is key.	Essential, the reliability of the system is key.
Architecture	Essential, software design starts with architecture.	Generally optional, architecture is often not needed when designing an electromechanical system.	Essential, proper architecture is needed to design an IT/OT converged system.
Organizational aspects	Important, the focus is often on technical solutions	Important, the focus is often on technical solutions	Important, the focus is often on technical solutions

This review investigated three key domains that require attention when aligning IT/OT converged systems. First, maintenance practices change since the lifecycles of IT and OT do not necessarily match. This mismatch in lifecycles needs to be effectively managed by the different responsibilities (operations, maintenance, financial etc.) within an asset management organization. Therefore, asset management of IT/OT converged systems should be seen as a specific subgroup of these physical assets that are interconnected using IT components.

Second, these assets are prone to more failures because of increasing software and cyber risks. Due to those risks, there is increasing research interest in cybersecurity. Moreover, the failures of IT systems are less visible than failures of OT systems since failures of OT systems often give visual feedback to the mechanic. This increases the severity of the failures increasing the systems' criticality which potentially reduces the availability of these systems [127]. In addition, the interconnection between IT and OT is a source of failures and these failures are also often more resource-intensive to diagnose [128], which also reduces the availability of these systems.

Third, a system's configuration management is changing as IT becomes more dominant within the system, requiring additional different configuration management. For example, architecture becomes even more essential to integrate a system into an asset, for such an architecture technical constraints and system performance criteria are key input characteristics [129]. Therefore, research on configuration management has received a focus on tools that support the practitioner in managing the configuration of an IT/OT converged asset over its lifecycle.

Finally, more attention needs to be paid to organizational aspects, instead of focusing on technical aspects. For example, managing the addition of IT within an OT team, since the OT and IT departments have diverse cultural values [66], [130] and focus on improving the communication between the different departments within an organization. These results are consistent with the findings of several other researchers who have indicated the need for more attention to be paid to non-technical aspects of digitization, see for example Annarelli et al. [78] or Sanchez-Londono et al. [33].

A. TAKE HOME MESSAGE FOR PRACTITIONERS

Three major takeaways for practitioners working in an industrial environment can be derived from this research.

1. Maintenance of IT/OT converged systems requires a more mature digital organization to be able to diagnose and maintain these IT/OT converged systems. Because part of the system's performance is determined by parts hidden from view. This requires specialized data and monitoring to get insight into how the system is performing and where to look in case of non-performance. Considering that introducing IT elements into a physical asset makes maintenance more difficult, it can be argued that there should be more consideration on the necessity of these new or added digital functionalities.

2. Cybersecurity is an emerging topic as risks of possible cyber events on IT/OT converged assets need to be managed. To deal with these risks performance requirements on cyber aspects must be created during system development, together with a validation plan that clarifies when required performance is met.
3. The maintenance and configuration management of an IT/OT converged system needs constant attention. As opposed to OT & physical systems, IT is not static and is constantly under development. Therefore, not only should there be attention to the technical systems integration, but management should also be aligned with this integration. However, traditionally, IT and engineering professionals come from different siloed environments. It is needed to improve the understanding of each other's views and interests in managing and developing these converged systems.

B. IDENTIFIED GAPS FOR FURTHER RESEARCH

Even though we expected that the review would also find studies relating to current social research themes, some topics are missing or absent in this specific field. First, the maintenance processes around IT/OT converged systems impact sustainability, both by the performance of the maintenance itself and, by the effect of the maintenance on the product to be maintained [131]. Moreover, Maletič et al. [132] show that physical asset management can improve the social and environmental performance of companies. Also, Soori et al. [133] state that sustainability involves using advanced technologies while promoting social responsibility and minimizing impact on the environment. However, sustainability is not a priority that emerges from the review. During further research, the effects of IT/OT convergence on sustainability can be investigated. Since digitization can increase the environmental footprint.

Second, the lifecycle value, including financial, aspects of managing IT/OT converged systems did thus far not seem to play a role within the identified literature. Within the practice of managing assets over its lifecycle, however, economic, and commercial impact are important aspects [134].

Third, the primary focus of this research is on the physical integration of IT/OT in assets; when it comes to integration, topics like artificial intelligence (AI) and machine learning (ML) are not yet widely discussed in the maintenance and configuration management domain. Within cybersecurity, there is attention to these topics, but the specific details are beyond the research's scope.

Finally, to define and manage the specific complexities of the integration of IT within a physical asset in further research, this study, proposes a definition of IT/OT converged asset management, based on the observations from this literature review as well as the work of Pudney (2010):

"The process of aligning maintenance challenges, cybersecurity aspects and configuration management tasks over an IT/OT converged assets combined life cycle, cost-effectively, to achieve a predefined performance level for its stakeholders, while mitigating risks."

Also, tools and methods are required to support practitioners in operationalizing this definition in practice and to manage this complexity sustainably. Future work will aim to create these tools and methods that help to integrate IT within OT environments to increase cooperation between IT and OT teams and demonstrate their application in practice.

V. CONCLUSION

A literature review was performed to study 113 studies from the last 20 years with a focus on three important domains regarding the integration of IT with OT in physical assets: Maintenance, cybersecurity, and configuration management. This literature review gives insight into the specific differences between IT, OT, and IT/OT converged systems.

The literature review reveals three aspects that pay more attention in managing IT/OT converged systems. Firstly, maintenance practices change as the life cycle of a system changes more frequently with the introduction of IT. Secondly, there has been considerably more research interest in cybersecurity due to the new risks that are introduced when IT and OT are connected. Lastly, configuration management has become even more important since the system's design changes as IT becomes the central element, making a system's architecture more important. Moreover, gaps have been identified together with some key messages for practitioners in the industrial sector.

This research suggests further research is needed to deal with the increased complexity of IT/OT converged systems. It can be argued that for IT/OT converged systems, balancing financial, technical, and organizational practices still needs research attention. Therefore, research towards integrated and sustainable approaches which deal with IT/OT-related challenges is necessary. This should be combined with the development of specific tools and methods for sustainably managing IT/OT converged systems.

ACKNOWLEDGMENT

The first author thanks his colleagues Leo van Dongen and Henrike Holwerda for their feedback and discussion on the previous versions of this paper.

REFERENCES

[1] Gartner. *Definition of Operational Technology (OT)—Gartner Information Technology Glossary*. Accessed: Jul. 13, 2021. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[2] Gartner. *Definition of Information Technology (IT)–Gartner Information Technology Glossary*. Accessed: Jul. 13, 2021. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/it-information-technology

[3] A. Hahn, "Operational technology and information technology in industrial control systems," in *Cyber-Security of SCADA and Other Industrial Control Systems* (Advances in Information Security), E. J. M. Colbert and A. Kott, Eds., Cham, Switzerland: Springer, 2016, pp. 51–68, doi: 10.1007/978-3-319-32125-7_4.

[4] P. Hehenberger, B. Vogel-Heuser, D. Bradley, B. Eynard, T. Tomiyama, and S. Achiche, "Design, modelling, simulation and integration of cyber physical systems: Methods and applications," *Comput. Ind.*, vol. 82, pp. 273–289, Oct. 2016, doi: 10.1016/j.compind.2016.05.006.

[5] Gartner Information Technology Glossary. *Definition of IT/OT Integration*. Accessed: Jul. 24, 2024. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/it-ot-integration

[6] Gartner Information Technology Glossary. *Definition of Internet of Things (IoT)*. Accessed: Jul. 24, 2024. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/internet-of-things

[7] H. van Vliet, *Software Engineering: Principles and Practice*, 3rd ed., Chichester, U.K.: Wiley, 2008.

[8] R. P. Kranendonk, "The convergence and integration of operational technology and information technology systems," M.S. thesis, Delft Univ. Technol., Delft, The Netherlands, 2016. Accessed: Oct. 2, 2023. [Online]. Available: https://repository.tudelft.nl/record/uuid:8d7890a7-3207-45ee-94d4-ddb3a10f5d0e

[9] *ISO/IEC/IEEE International Standard—Systems and Software Engineering—Life Cycle Management—Part 1: Guidelines for Life Cycle Management*, Standard ISO 24748-1: 2018, 2018. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=8526558

[10] D. D. Walden, G. J. Roedler, K. Forsberg, R. D. Hamelin, and T. M. Shortell, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 4th ed., International Council on Systems Engineering, Eds., Hoboken, NJ, USA: Wiley, 2015.

[11] *NEN-EN 55000—Asset Management—Overview, Principles and Terminology*, NEN, Delft, Feb. 2014, Accessed: Dec. 3, 2021. [Online]. Available: https://connect.nen.nl/Standard/Detail/193078?compId=16755&collectionId=0

[12] S. Seuring and M. Müller, "From a literature review to a conceptual framework for sustainable supply chain management," *J. Cleaner Prod.*, vol. 16, no. 15, pp. 1699–1710, Oct. 2008, doi: 10.1016/j.jclepro.2008.04.020.

[13] A. Garg and S. G. Deshmukh, "Maintenance management: Literature review and directions," *J. Quality Maintenance Eng.*, vol. 12, no. 3, pp. 205–238, Jul. 2006, doi: 10.1108/13552510610685075.

[14] S. Jalali and C. Wohlin, "Systematic literature studies: Database searches vs. backward snowballing," in *Proc. ACM-IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Lund, Sep. 2012, pp. 29–38, doi: 10.1145/2372251.2372257.

[15] B. Dowdeswell, R. Sinha, and S. G. MacDonell, "Finding faults: A scoping study of fault diagnostics for industrial cyber–physical systems," *J. Syst. Softw.*, vol. 168, Oct. 2020, Art. no. 110638, doi: 10.1016/j.jss.2020.110638.

[16] A. Kok, 2024, "Overview of literature belonging to—The impact of integrating information technology with operational technology in physical assets: A literature review," 4TU, Univ. Twente, Enschede, The Netherlands, 2024, doi: 10.4121/21311973.

[17] A. Chemudupati, S. Kaulen, M. Mertens, S. M. Mohan, P. Reynaud, F. Robin, and S. Zimmermann, "The convergence of IT and operational technology," Atos Ascent, 2012. Accessed: Sep. 3, 2021. [Online]. Available: http://ascent.atos.net/?wpdmdl=1069

[18] S. Ruiz-Arenas, I. Horváth, R. Mejía-Gutiérrez, and E. Z. Opiyo, "Towards the maintenance principles of cyber-physical systems," *Strojniški Vestnik J. Mech. Eng.*, vol. 60, no. 12, pp. 815–831, Dec. 2014, doi: 10.5545/sv-jme.2013.1556.

[19] M. Bricogne, J. Le Duigou, and B. Eynard, "Design processes of mechatronic systems," in *Mechatronic Futures*, P. Hehenberger and D. Bradley, Eds., Cham, Switzerland: Springer, 2016, pp. 75–89, doi: 10.1007/978-3-319-32156-1_6.

[20] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Comput. Ind.*, vol. 100, pp. 212–223, Sep. 2018, doi: 10.1016/j.compind.2018.04.017.

[21] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review," *Comput. Ind.*, vol. 137, May 2022, Art. no. 103614, doi: 10.1016/j.compind.2022.103614.

[22] L. Pintelon and A. Parodi-Herz, "Maintenance: An evolutionary perspective," in *Complex System Maintenance Handbook* (Springer Series in Reliability Engineering). London, U.K.: Springer, 2008, pp. 21–48, doi: 10.1007/978-1-84800-011-7_2.

[23] L. Silvestri, A. Forcina, V. Introna, A. Santolamazza, and V. Cesarotti, "Maintenance transformation through industry 4.0 technologies: A systematic literature review," *Comput. Ind.*, vol. 123, Dec. 2020, Art. no. 103335, doi: 10.1016/j.compind.2020.103335.

[24] M. S. Sonkor and B. G. de Soto, "Operational technology on construction sites: A review from the cybersecurity perspective," *J. Construction Eng. Manage.*, vol. 147, no. 12, Dec. 2021, Art. no. 04021172, doi: 10.1061/(asce)co.1943-7862.0002193.

[25] G. Cline. (2017). *Integrated Product Lifecycle Management in the Era of IoT*. Aberdeen Group. Accessed: May 22, 2024. [Online]. Available: https://resources.altium.com/sites/default/files/uberflip_docs/file_959.pdf

[26] R. Krikhaar, W. Mosterman, N. Veerman, and C. Verhoef, "Enabling system evolution through configuration management on the hardware/software boundary," *Syst. Eng.*, vol. 12, no. 3, pp. 233–264, Sep. 2009, doi: 10.1002/sys.20122.

[27] P. Barrios, C. Danjou, and B. Eynard, "Literature review and methodological framework for integration of IoT and PLM in manufacturing industry," *Comput. Ind.*, vol. 140, Sep. 2022, Art. no. 103688, doi: 10.1016/j.compind.2022.103688.

[28] S. Takata, F. Kirnura, F. J. A. M. van Houten, E. Westkamper, M. Shpitalni, D. Ceglarek, and J. Lee, "Maintenance: Changing role in life cycle management," *CIRP Ann.*, vol. 53, no. 2, pp. 643–655, 2004, doi: 10.1016/s0007-8506(07)60033-x.

[29] A. M. TITU and A. STANCIU, "Merging operations technology with information technology," in *Proc. 12th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*. Romania: IEEE, Jun. 2020, pp. 1–6, doi: 10.1109/ECAI50035.2020.9223235.

[30] I. C. Ehie and M. A. Chilton, "Understanding the influence of IT/OT convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation," *Comput. Ind.*, vol. 115, Feb. 2020, Art. no. 103166, doi: 10.1016/j.compind.2019.103166.

[31] E. Levrat, B. Iung, and A. C. Marquez, "E-maintenance: Review and conceptual framework," *Prod. Planning Control*, vol. 19, no. 4, pp. 408–429, Jun. 2008, doi: 10.1080/09537280802062571.

[32] N. Diaz-Elsayed, L. Hernandez, R. Rajamani, and B. A. Weiss, "Asset condition management: A framework for smart, health-ready manufacturing systems," in *Additive Manufacturing; Advanced Materials Manufacturing; Biomanufacturing; Life Cycle Engineering; Manufacturing Equipment and Automation*, vol. 1. New York, NY, USA: American Society of Mechanical Engineers, Sep. 2020, p. V001T04A002, doi: 10.1115/MSEC2020-8326.

[33] D. Sanchez-Londono, G. Barbieri, and L. Fumagalli, "Smart retrofitting in maintenance: A systematic literature review," *J. Intell. Manuf.*, vol. 34, no. 1, pp. 1–19, Jan. 2023, doi: 10.1007/s10845-022-02002-2.

[34] I. Roda and M. Macchi, "Maintenance concepts evolution: A comparative review towards advanced maintenance conceptualization," *Comput. Ind.*, vol. 133, Dec. 2021, Art. no. 103531, doi: 10.1016/j.compind.2021.103531.

[35] M. Skrzeszewska and J. Patalas-Maliszewska, "Assessing the effectiveness of using the MES in manufacturing enterprises in the context of industry 4.0," in *Distributed Computing and Artificial Intelligence* (Advances in Intelligent Systems and Computing), E. Herrera-Viedma, Z. Vale, P. Nielsen, A. Martin Del Rey, and R. Casado Vara, Eds., Cham, Switzerland: Springer, 2020, pp. 49–56, doi: 10.1007/978-3-030-23946-6_6.

[36] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 3928–3937, doi: 10.1109/HICSS.2016.488.

[37] A. G. Kuusk and J. Gao, "Consolidating people, process and technology to bridge the great wall of operational and information technologies," in *Engineering Asset Management—Systems, Professional Practices and Certification* (Lecture Notes in Mechanical Engineering), P. W. Tse, J. Mathew, K. Wong, R. Lam, and C. N. Ko, Eds., Cham, Switzerland: Springer, 2015, pp. 1715–1726, doi: 10.1007/978-3-319-09507-3_147.

[38] J. A. McCall, M. A. Herndon, and W. M. Osborne, "Computer science and technology: Software maintenance management," NBS Special Publication, National Bureau of Standards, Gaithersburg, MD, USA, Tech. Rep. NBS/SP-500/129, 1985.

[39] M. W. Godfrey and D. M. German, "On the evolution of Lehman's laws," *J. Software: Evol. Process*, vol. 26, no. 7, pp. 613–619, Jul. 2014, doi: 10.1002/smr.1636.

[40] D. L. Dvorak, "NASA study on flight software complexity," in *Proc. AIAA Infotech@Aerospace Conf.* Washington, DC, USA: American Institute of Aeronautics and Astronautics, Apr. 2009, pp. 1–20, doi: 10.2514/6.2009-1882.

[41] P. Grubb and A. A. Takang, *Software Maintenance: Concepts and Practice*, 2nd ed., River Edge, NJ, USA: World Scientific, 2003.

[42] H. Koziolek, "Sustainability evaluation of software architectures: A systematic review," in *Proc. Federated Events Compon.-Based Softw. Eng. Softw. Archit. (QoSA+ISARCS)*, vol. 11, Jun. 2011, pp. 3–12, doi: 10.1145/2000259.2000263.

[43] W. E. Wong, X. Li, and P. A. Laplante, "Be more familiar with our enemies and pave the way forward: A review of the roles bugs played in software failures," *J. Syst. Softw.*, vol. 133, pp. 68–94, Nov. 2017, doi: 10.1016/j.jss.2017.06.069.

[44] J. Eloff and M. B. Bella, "Software failures: An overview," in *Software Failure Investigation: A Near-Miss Analysis Approach*, J. Eloff and M. B. Bella, Eds., Cham, Switzerland: Springer, 2018, pp. 7–24, doi: 10.1007/978-3-319-61334-5_2.

[45] L. Feinbube, P. Tröger, and A. Polze, "The landscape of software failure cause models," 2016, *arXiv:1603.04335*.

[46] V. H. Guthrie, J. A. Farquharson, R. W. Bonnett, and E. F. Bjoro, "Guidelines for integrating RAM considerations into an engineering project," *IEEE Trans. Rel.*, vol. 39, no. 2, pp. 133–139, Jun. 1990, doi: 10.1109/24.55870.

[47] A. Kok, A. Martinetti, and J. Braaksma, "RAMS never dies! Applying the approach to IT/OT converged systems," in *Proc. 33rd Eur. Saf. Rel. Conf. (ESREL)*, Southampton, U.K.: Research Publishing, Sep. 2023, pp. 3181–3187, doi: 10.3850/978-981-18-8071-1_P286-cd.

[48] C. Carlson, *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis* (Quality and reliability engineering series). Hoboken, NJ, USA: Wiley, 2012.

[49] S. Oveisi and R. Ravanmehr, "SFTA-based approach for safety/reliability analysis of operational use-cases in cyber-physical systems," *J. Comput. Inf. Sci. Eng.*, vol. 17, no. 3, Sep. 2017, Art. no. 031018, doi: 10.1115/1.4037228.

[50] B. S. Medikonda and P. S. Ramaiah, "Software safety analysis to identify critical software faults in software-controlled safety-critical systems," in *Proc. 48th Annu. Conv. Comput. Soc. India-ICT Crit. Infrastruct.*, vol. 249, S. C. Satapathy, P. S. Avadhani, S. K. Udgata, and S. Lakshminarayana, Eds., Cham, Switzerland: Springer, 2014, pp. 455–465, doi: 10.1007/978-3-319-03095-1_48.

[51] A. A. Zúñiga, A. Baleia, J. Fernandes, and P. J. D. C. Branco, "Classical failure modes and effects analysis in the context of smart grid cyber-physical systems," *Energies*, vol. 13, no. 5, p. 1215, Mar. 2020, doi: 10.3390/en13051215.

[52] H. D. Tafur, G. Barbieri, and C. E. Pereira, "An FMEA-based methodology for the development of control software reliable to hardware failures," *IFAC-PapersOnLine*, vol. 54, no. 1, pp. 420–425, 2021, doi: 10.1016/j.ifacol.2021.08.047.

[53] S. P. Kavulya, K. Joshi, F. D. Giandomenico, and P. Narasimhan, "Failure diagnosis of complex systems," in *Resilience Assessment and Evaluation of Computing Systems*, K. Wolter, A. Avritzer, M. Vieira, and A. van Moorsel, Eds., Berlin, Germany: Springer, 2012, pp. 239–261, doi: 10.1007/978-3-642-29032-9_12.

[54] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electric Power Syst. Res.*, vol. 163, pp. 396–412, Oct. 2018, doi: 10.1016/j.epsr.2018.07.015.

[55] K. Herzig, S. Just, and A. Zeller, "It's not a bug, it's a feature: How misclassification impacts bug prediction," in *Proc. 35th Int. Conf. Softw. Eng. (ICSE)*. San Francisco, CA, USA: IEEE, May 2013, pp. 392–401, doi: 10.1109/ICSE.2013.6606585.

[56] W. Tiddens, "Setting sail towards predictive maintenance: Developing tools to conquer difficulties in the implementation of maintenance analytics," Ph.D. dissertation, Dept. Des., Prod. Manag., Univ. Twente, The Netherlands, 2018, doi: 10.3990/1.9789036546034.

[57] P. C. Amusuo, A. Sharma, S. R. Rao, A. Vincent, and J. C. Davis, "Reflections on software failure analysis," in *Proc. 30th ACM Joint Eur. Softw. Eng. Conf. Symp. Found. Softw. Eng.* Singapore: ACM, Nov. 2022, pp. 1615–1620, doi: 10.1145/3540250.3560879.

[58] J. M. Simões, C. F. Gomes, and M. M. Yasin, "A literature review of maintenance performance measurement: A conceptual framework and directions for future research," *J. Quality Maintenance Eng.*, vol. 17, no. 2, pp. 116–137, May 2011, doi: 10.1108/13552511111134565.

[59] L. Villar-Fidalgo, A. C. Márquez, V. G. Prida, A. De la Fuente, P. Martínez-Galán, and A. Guillén, "Cyber physical systems implementation for asset management improvement: A framework for the transition," in *Safety and Reliability—Safe Societies in a Changing World*, 1st ed., S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik, and J. E. Vinnem, Eds., Boca Raton, FL, USA: CRC Press, 2018, doi: 10.1201/9781351174664.

[60] M. S. Bhatia and S. Kumar, "Critical success factors of industry 4.0 in automotive manufacturing industry," *IEEE Trans. Eng. Manag.*, vol. 69, no. 5, pp. 2439–2453, Oct. 2022, doi: 10.1109/TEM.2020.3017004.

[61] L. Makama and A. Telukdarie, "Improving maintenance management of reservoir structures using smart systems," in *Proc. IEEE 28th Int. Conf. Eng., Technol. Innov. (ICE/ITMC) 31st Int. Assoc. Manage. Technol. (IAMOT) Joint Conf.*, Jun. 2022, pp. 1–5, doi: 10.1109/ICE/ITMC-IAMOT55089.2022.10033213.

[62] M.-A. Filz, J. E. B. Langner, C. Herrmann, and S. Thiede, "Data-driven failure mode and effect analysis (FMEA) to enhance maintenance planning," *Comput. Ind.*, vol. 129, Aug. 2021, Art. no. 103451, doi: 10.1016/j.compind.2021.103451.

[63] K. He and M. Jin, "Cyber-physical system for maintenance in industry 4.0," Master thesis, School Eng., Jönköping Univ., 2016. [Online]. Available: https://ju.diva-portal.org/smash/get/diva2

[64] M. Temelkova, "Similarities and differences between the technological paradigms 'production system' 'cyber-physical system' and 'cyber-physical production system,'' in *Proc. Int. Conf. Commun., Inf., Electron. Energy Syst. (CIEES)*, Nov. 2022, pp. 1–7, doi: 10.1109/CIEES55704.2022.9990698.

[65] E. Jantunen, U. Zurutuza, and M. Albano, "The way cyber physical systems will revolutionise maintenance," presented at the Conf. Condition Monit. Diagnostic Eng. Manag., Lancashire, Jul. 2017. Accessed: Jul. 16, 2021. [Online]. Available: https://recipp.ipp.pt/bitstream/10400.22/10072/1/COM_CISTER_2017.pdf

[66] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," in *Proc. 15th Austral. Inf. Secur. Manag. Conf.*, C. C. Valli, Ed., Perth, WA, Australia: Edith Cowan University, Dec. 2017, pp. 149–155.

[67] E. Willems, *Cyberdanger: Understanding and Guarding Against Cybercrime*. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-04531-9.

[68] M. P. C. Weijnen, Z. Lukszo, and S. Farahani, *Shaping an Inclusive Energy Transition*. Cham, Switzerland: Springer, 2021. Accessed: Aug. 9, 2024. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-74586-8

[69] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, "Guide to operational technology (OT) security," Nat. Inst. Standards Technol. (U.S.), Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-82r3, Sep. 2023, doi: 10.6028/NIST.SP.800-82r3.

[70] G. K. Hanssen, T. Onshus, M. G. Jaatun, T. Myklebust, M. Ottermo, and A. Lundteigen. (2021). *Principles of Digitalisation and IT-OT Integration*. Sintef Digit. Accessed: Jul. 3, 2024. [Online]. Available: https://www.havtil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef—report—principles-of-digitalisation-and-it-ot-integration.pdf

[71] A. J. G. de Azambuja, T. Giese, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Digital twins in industry 4.0–opportunities and challenges related to cyber security," *Proc. CIRP*, vol. 121, pp. 25–30, 2024, doi: 10.1016/j.procir.2023.09.225.

[72] S. Mantravadi, R. Schnyder, C. Møller, and T. D. Brunoe, "Securing IT/OT links for low power IIoT devices: Design considerations for industry 4.0," *IEEE Access*, vol. 8, pp. 200305–200321, 2020, doi: 10.1109/ACCESS.2020.3035963.

[73] H. Kanamaru, "The extended risk assessment form for IT/OT convergence in IACS security," in *Proc. 60th Annu. Conf. Soc. Instrum. Control Engineers Jpn. (SICE)*, Sep. 2021, pp. 1365–1370. Accessed: Jul. 8, 2024. [Online]. Available: https://ieeexplore-ieee-org.ezproxy2.utwente.nl/document/9555360/?arnumber=9555360

[74] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Comput. Commun.*, vol. 155, pp. 1–8, Apr. 2020, doi: 10.1016/j.comcom.2020.03.007.

[75] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Anal. Prevention*, vol. 148, Dec. 2020, Art. no. 105837, doi: 10.1016/j.aap.2020.105837.

[76] A. S. Mohammed, P. Reinecke, P. Burnap, O. Rana, and E. Anthi, "Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective," *ACM Trans. Cyber-Physical Syst.*, vol. 6, no. 3, pp. 1–27, Jul. 2022, doi: 10.1145/3548691.

[77] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, Dec. 2018, doi: 10.1016/j.compind.2018.09.004.

[78] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Comput. Ind. Eng.*, vol. 149, Nov. 2020, Art. no. 106829, doi: 10.1016/j.cie.2020.106829.
[79] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, "Smart grid cyber-physical situational awareness of complex operational technology attacks: A review," *ACM Comput. Surveys*, vol. 55, no. 10, pp. 1–36, Oct. 2023, doi: 10.1145/3565570.
[80] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, Jan. 2017, doi: 10.1080/23742917.2016.1252211.
[81] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," SANS Inst., North Bethesda, MD, USA, 2015. Accessed: May 22, 2024. [Online]. Available: https://www.sans.org/white-papers/36297/
[82] National Institute of Standards and Technology. (Feb. 2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Accessed: Jan. 18, 2023. [Online]. Available: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
[83] Department for Transport. (Feb. 2016). *Rail Cyber Security—Guidance to Industry*. Accessed: Nov. 9, 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897091/rail-cyber-security-guidance-to-industry-document.pdf
[84] Idaho National Laboratory, "Consequence-driven cyber-informed engineering (CCE)," Idaho Nat. Lab., Idaho Falls, ID, USA, Tech. Rep. INL/EXT-16-39212, Oct. 2016. Accessed: Sep. 29, 2021. [Online]. Available: https://inl.gov/cce/
[85] *Industrial Control Systems: Securing the Systems That Control Physical Environments*, Inf. Secur. Forum Ltd., West Sussex, U.K., Dec. 2017, p. 88. Accessed: Aug. 13, 2024. [Online]. Available: https://www.securityforum.org/solutions-and-insights/industrial-control-systems-securing-the-systems-that-control-physical-environments/
[86] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Rel. Eng. Syst. Saf.*, vol. 139, pp. 156–178, Jul. 2015, doi: 10.1016/j.ress.2015.02.008.
[87] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Computer Safety, Reliability, and Security* (Lecture Notes in Computer Science), vol. 8666, A. Bondavalli and F. Di Giandomenico, Eds., Cham, Switzerland: Springer, 2014, pp. 310–325, doi: 10.1007/978-3-319-10506-2_21.
[88] *Configuration Management Guidance*, Department of Defense Handbook MIL-HDBK-61B, Richmond, VI, USA, Apr. 2020. Accessed: Jun. 30, 2022. [Online]. Available: https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=202239
[89] A. D'Souza and P. Thota, "Configuration management for model based systems engineering—An example from the aerospace industry," in *Proc. INCOSE Int. Symp.*, 2022, vol. 32, no. 1, pp. 648–664, doi: 10.1002/iis2.12955.
[90] *Quality Management—Guidelines for Configuration Management*, NEN, Standard NEN-ISO-10007, Delft, May 2017.
[91] *Programme Management—Configuration Management—Part 100: A Guide for the Application of the Principles of Configuration Management*, NEN, Standard NEN-EN-9223-100, Delft, Mar. 2018.
[92] *Systems and Software Engineering—System Life Cycle Processes*, NEN, Standard NEN-ISO/IEC/IEEE 15288:2023, Delft, May 2023.
[93] R. Capilla, J. C. Dueñas, and R. Krikhaar, "Managing software development information in global configuration management activities," *Syst. Eng.*, vol. 15, no. 3, pp. 241–254, Sep. 2012, doi: 10.1002/sys.20205.
[94] I. Crnkovic, U. Asklund, and A. P. Dahlqvist, *Implementing and integrating product data management and software configuration management*. Boston, MA, USA: Artech House, 2003.
[95] W. Tichy, "Software configuration management overview," in *Software Configuration Management* (Trends in Software), vol. 2. New York, NY, USA: Wiley, 1995, p. 26. Accessed: Apr. 20, 2022. [Online]. Available: https://grosskurth.ca/bib/entries.html
[96] J. Estublier, D. Leblang, A. V. D. Hoek, R. Conradi, G. Clemm, W. Tichy, and D. Wiborg-Weber, "Impact of software engineering research on the practice of software configuration management," *ACM Trans. Softw. Eng. Methodology*, vol. 14, no. 4, pp. 383–430, Oct. 2005, doi: 10.1145/1101815.1101817.
[97] A. Deuter and S. Rizzo, "A critical view on PLM/ALM convergence in practice and research," in *Proc. Technol.*, vol. 26, 2016, pp. 405–412, doi: 10.1016/j.protcy.2016.08.052. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212017316303991
[98] S. Rachuri, E. Subrahmanian, A. Bouras, S. J. Fenves, S. Foufou, and R. D. Sriram, "Information sharing and exchange in the context of product lifecycle management: Role of standards," *Computer-Aided Design*, vol. 40, no. 7, pp. 789–800, Jul. 2008, doi: 10.1016/j.cad.2007.06.012.
[99] A. Deuter, A. Otte, M. Ebert, and F. Possel-Dölken, "Developing the requirements of a PLM/ALM integration: An industrial case study," in *Product Lifecycle Management (Volume 4): The Case Studies* (Decision Engineering), J. Stark, Ed., Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-16134-7_11.
[100] S. Elliot, A. Plant, M. Smith, and Young. (2014). *The Connected Train*. Atos. Accessed: Sep. 3, 2021. [Online]. Available: https://atos.net/wp-content/uploads/2017/10/01042013-AscentWhitePaper-ConnectedTrain.pdf
[101] R. Baheti and H. Gill, "Cyber-physical systems," Nat. Sci. Found., Alexandria, VI, USA, Mar. 2011. Accessed: Aug. 9, 2024. [Online]. Available: https://ieeecss.org/impact-control-technology-1st-edition
[102] A. G. Kuusk, A. Koronios, and J. Gao, "Overcoming integration challenges in organisations with operational technology," in *Proc. ACIS*, Melbourne, VIC, Australia, Dec. 2013, p. 16. Accessed: May 22, 2024. [Online]. Available: https://aisel.aisnet.org/acis2013/121
[103] J. Poliński and K. Ochociński, "Digitization in rail transport," *Problemy Kolejnictwa Railway Rep.*, vol. 64, no. 188, pp. 137–148, Sep. 2020, doi: 10.36137/1885e.
[104] W. J. C. Verhagen, P. Bermell-Garcia, R. E. C. van Dijk, and R. Curran, "A critical review of knowledge-based engineering: An identification of research challenges," *Adv. Eng. Informat.*, vol. 26, no. 1, pp. 5–15, Jan. 2012, doi: 10.1016/j.aei.2011.06.004.
[105] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice* (SEI Series in Software Engineering), 2nd ed., Boston, MA, USA: Addison-Wesley, 2003. Accessed: Mar. 8, 2022. [Online]. Available: https://people.ece.ubc.ca/matei/EECE417/BASS/index.html
[106] M. van Steen and A. S. Tanenbaum. (2017). *Distributed systems*, 3rd ed., Version 3.01. [Online]. Available: https://www.distributed-systems.net/
[107] M. Broy, "Engineering cyber-physical systems: Challenges and foundations," in *Complex Systems Design & Management*, M. Aiguier, Y. Caseau, D. Krob, A. Rauzy, Eds., Berlin, Germany: Springer, 2013, pp. 1–13.
[108] Y. Tan, S. Goddard, and L. C. Pérez, "A prototype architecture for cyber-physical systems," *ACM SIGBED Rev.*, vol. 5, no. 1, pp. 1–2, Jan. 2008, doi: 10.1145/1366283.1366309.
[109] H. J. La and S. D. Kim, "A service-based approach to designing cyber physical systems," in *Proc. IEEE/ACIS 9th Int. Conf. Comput. Inf. Sci.*, Aug. 2010, pp. 895–900, doi: 10.1109/ICIS.2010.73.
[110] W. Stallings, *Handbook of Computer-Communications Standards; Volume 1:, The Open Systems Interconnection (OSI) Model and OSI-Related Standards*. New York, NY, USA: Macmillan Publishing, 1987. [Online]. Available: https://archive.org/details/trent_0116300225301
[111] A. Koubaa and B. Andersson, "A vision of cyber-physical internet," in *Proc. 8th Int. Workshop Real-Time Netw.*, Jun. 2009, p. 6.
[112] P. Spiess, "SOA-based integration of the Internet of Things in enterprise services," in *Proc. IEEE Int. Conf. Web Services*, Jul. 2009, pp. 968–975, doi: 10.1109/ICWS.2009.98.
[113] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015, doi: 10.1016/j.mfglet.2014.12.001.
[114] A. Ahmadi, C. Cherifi, V. Cheutet, and Y. Ouzrout, "A review of CPS 5 components architecture for manufacturing based on standards," in *Proc. 11th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Colombo, Sri Lanka, Dec. 2017, pp. 1–6. Accessed: Jul. 13, 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01679977
[115] O. Cardin, "Classification of cyber-physical production systems applications: Proposition of an analysis framework," *Comput. Ind.*, vol. 104, pp. 11–21, Jan. 2019, doi: 10.1016/j.compind.2018.10.002.
[116] E. Y. Nakagawa, P. O. Antonino, F. Schnicke, R. Capilla, T. Kuhn, and P. Liggesmeyer, "Industry 4.0 reference architectures: State of the art and future trends," *Comput. Ind. Eng.*, vol. 156, Jun. 2021, Art. no. 107241, doi: 10.1016/j.cie.2021.107241.
[117] E. Francalanza, M. Mercieca, and A. Fenech, "Modular system design approach for cyber physical production systems," *Proc. CIRP*, vol. 72, pp. 486–491, Jan. 2018, doi: 10.1016/j.procir.2018.03.090.
[118] P. Davies, "Interface management—The neglected orphan of systems engineering," in *Proc. INCOSE Int. Symp.*, Jul. 2020, vol. 30, no. 1, pp. 747–756, doi: 10.1002/j.2334-5837.2020.00752.x.

[119] J. Blyler, "Interface management–managing complexity at the system interface," *IEEE Instrum. Meas. Mag.*, vol. 7, no. 1, pp. 32–37, Mar. 2004, doi: 10.1109/MIM.2004.1288741.
[120] A. David, M. Birtel, A. Wagner, and M. Ruskowski, "Architecture concept for the integration of cyber-physical transport modules in modular production environments," *Proc. Manuf.*, vol. 51, pp. 1111–1116, Jan. 2020, doi: 10.1016/j.promfg.2020.10.156.
[121] S. F. Yasseri and H. Bahai, "Interface and integration management for FPSOs," *Ocean Eng.*, vol. 191, Nov. 2019, Art. no. 106441, doi: 10.1016/j.oceaneng.2019.106441.
[122] O. Penas, R. Plateaux, S. Patalano, and M. Hammadi, "Multi-scale approach from mechatronic to cyber-physical systems for the design of manufacturing systems," *Comput. Ind.*, vol. 86, pp. 52–69, Apr. 2017, doi: 10.1016/j.compind.2016.12.001.
[123] L. A. Estrada-Jimenez, "Integration of cutting-edge interoperability approaches in cyber-physical production systems and industry 4.0," in *Advances in Systems Analysis, Software Engineering, and High Performance Computing*, P. Rea, E. Ottaviano, J. Machado, and K. Antosz, Eds., Hershey, PA, USA: IGI Global, 2021, pp. 144–172, doi: 10.4018/978-1-7998-6721-0.ch007.
[124] J. Yebenes Serrano and M. Zorrilla, "A data governance framework for industry 4.0," *IEEE Latin Amer. Trans.*, vol. 19, no. 12, pp. 2130–2138, Dec. 2021, doi: 10.1109/TLA.2021.9480156.
[125] Y.-L. The and A. G. Kuusk, "Aligning IIoT and ISA-95 to improve asset management in process industries," in *Proc. 14th WCEAM*, in Lecture Notes in Mechanical Engineering, A. C. Márquez, D. Komljenovic, and J. Amadi-Echendu, Eds., Cham, Switzerland: Springer, 2021, pp. 153–163, doi: 10.1007/978-3-030-64228-0_14.
[126] J. Kääriäinen, "Practical adaptation of configuration management: Three case studies," VTT, Espoo, Finland, 2006. [Online]. Available: http://www.vtt.fi/publications/index.jsp
[127] "MIL-STD-1629A—Procedures for performing a failure mode, effects and criticality analysis," Dept. Defence, Commanding Officer, Eng. Specifications Standards Dept., Washington, DC, USA, Tech. Rep. MIL-STD-1629A, Nov. 24, 1980. Accessed: Mar. 26, 2024. [Online]. Available: https://extapps.ksc.nasa.gov/Reliability/Documents/milstd1629_FMEA.pdf
[128] S. Scheffer, A. Martinetti, R. Damgrave, and L. van Dongen, "Augmented reality for IT/OT failures in maintenance operations of digitized trains: Current status, research challenges and future directions," *Proc. CIRP*, vol. 100, pp. 816–821, 2021, doi: 10.1016/j.procir.2021.05.038.
[129] A. P. Sage and C. L. Lynch, "Systems integration and architecting: An overview of principles, practices, and perspectives," *Syst. Eng.*, vol. 1, no. 3, pp. 176–227, 1998, doi: 10.1002/(SICI)1520-6858(1998)1:3%3C176::AID-SYS3%3E3.0.CO;2-L.
[130] V. Upadrista, "IT-OT integration," in *Formula 4.0 for Digital Transformation*, 1st ed., New York, NY, USA: Productivity Press, 2021, pp. 243–270, doi: 10.4324/9781003159070-chapter14.
[131] C. Franciosi, A. Voisin, S. Miranda, S. Riemma, and B. Iung, "Measuring maintenance impacts on sustainability of manufacturing industries: From a systematic literature review to a framework proposal," *J. Cleaner Prod.*, vol. 260, Jul. 2020, Art. no. 121065, doi: 10.1016/j.jclepro.2020.121065.
[132] D. Maletič, M. Maletič, B. Al-Najjar, and B. Gomišček, "Development of a model linking physical asset management to sustainability performance: An empirical research," *Sustainability*, vol. 10, no. 12, p. 4759, Dec. 2018, doi: 10.3390/su10124759.
[133] M. Soori, B. Arezoo, and R. Dastres, "Virtual manufacturing in industry 4.0: A review," *Data Sci. Manage.*, vol. 7, no. 1, pp. 47–63, Mar. 2024, doi: 10.1016/j.dsm.2023.10.006.
[134] R. J. Ruitenburg, "Manoeuvring physical assets into the future," Ph.D. dissertation, Dept. Des., Prod. Manag., Univ. Twente, Enschede, The Netherlands, 2017, doi: 10.3990/1.9789036543958.

ARNO KOK received the B.S. and M.S. degrees in mechanical engineering from Twente University, Enschede, The Netherlands, in 2008 and 2011, respectively. He is currently pursuing the Ph.D. degree in asset management and maintenance engineering. Since graduation, he has been working in the field of reliability, availability, maintainability, and safety (RAMS) engineering. He is currently a Reliability Engineer with NS's Revision and Overhaul facility in Haarlem, The Netherlands. His research concentrates on design for maintenance, system integration, IT/OT convergence, and asset management within the railway industry.

ALBERTO MARTINETTI received the M.Sc. degree in geo-resources and geo-technologies engineering and the Ph.D. degree in safety and health on the prevention through design approach in mining activities from the Polytechnic of Turin, in 2009 and 2013, respectively. He is currently an Associate Professor with the Chair of Maintenance Engineering within the Department of Design, Production, and Management, University of Twente. He leads the Group of Humanitarian Engineering positioned in the Chair of asset management and maintenance engineering. His research focused for years on maintenance technology before moving forward with the new challenge in Humanitarian Engineering Design (appropriate and sustainable technological interventions for short- and long-term scenarios). He has published more than 70 publications in peer-reviewed journals and conferences, and he has co-chaired and organized several conferences and guest-edited several special issues in scientific journals.

JAN BRAAKSMA received the master's degree in business and ICT and the Ph.D. degree in economics and business. He is currently an Adjunct Professor and the Manager of the Chair of Asset Management and Maintenance Engineering, University of Twente. He is the Director of the WCM Summer School part of World Class Maintenance. He has worked for the University of Groningen (RuG) and the Dutch Defense Academy (NLDA). His research focuses on asset management and maintenance engineering with special attention for sustainable asset management, asset life cycle planning, systems integration, and design for Maintenance.