Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook

Matthias Eckhart and Andreas Ekelhart

Abstract Digital twins refer to virtual replicas of physical objects that, inter alia, enable to monitor, visualize and predict states of cyber-physical systems (CPSs). These capabilities yield efficiency gains and quality improvements in manufacturing processes. In addition, the concept of digital twins can also be leveraged to advance the security of the smart factory. More precisely, this concept can be applied as early as in the design phase by providing engineers the means to spot security flaws in the specification of the CPS. Security testing or intrusion detection are other security-enhancing technical use cases of digital twins that can be realized in systems engineering or during plant operation. In this chapter, we will discuss how digital twins can accompany their physical counterparts throughout the entire lifecycle and thereby strengthen the security of CPSs. The findings of this chapter indicate that the concept of digital twins will open up new paths to secure CPSs. However, efficiently creating, maintaining and running digital twins still represents a major research challenge, as the overhead costs hinder the adoption of this concept. We believe that these insights are valuable to shape future research in this emerging research area at the intersection of digital twins and information security.

Key words: Digital twin, Information security, Cyber-physical systems, Industrial control systems, Digital thread

---

Matthias Eckhart
Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI), Institute of Information Systems Engineering, Technische Universität Wien, Vienna, Austria
SBA Research, Vienna, Austria
e-mail: matthias.eckhart@tuwien.ac.at

Andreas Ekelhart
Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI), Institute of Information Systems Engineering, Technische Universität Wien, Vienna, Austria
SBA Research, Vienna, Austria
e-mail: andreas.ekelhart@sba-research.org

1 Introduction

Cyber-physical systems (CPSs) are essential for the realization of the Industry 4.0 vision (Kagermann et al. 2013), owing to their capabilities that blend physical and virtual components in order to interface both worlds (Baheti & Gill 2011). While these systems interact through sensors and actuators with the physical (real) world, the computational and networking elements allow them to function in the digital (cyber) space (Baheti & Gill 2011). In this way, physical processes in a variety of sectors (e.g., health care, energy, transportation (Shi et al. 2011)) can be fully automated but also operated in an intelligent fashion, leading to the emergence of multiple *smart* applications, e.g., *smart grid* and *smart factory*. In fact, CPSs are even considered the next computing revolution (Rajkumar et al. 2010).

Given that CPSs can impact the physical as well as the digital world, ensuring that these systems operate in a *secure* and *safe* manner is paramount. Multiple prominent cyber attacks against industrial control systems (ICSs), which we consider a subset of CPSs, have demonstrated how severe the consequences of these incidents can be. To give an example, an attack launched against the Ukrainian power grid in 2015 disconnected several substations, causing a power outage that affected approx. 225,000 households (Lee et al. 2016). As a result, successfully attacking ICSs, due to a lack of adequate security measures, can even represent a threat to public safety.

As the interconnectivity of ICSs increases in light of Industry 4.0 (Kagermann et al. 2013) and Information Technology (IT) and Operational Technology (OT) gradually converge (Hahn 2016), the attack surface expands substantially. This is also reflected in the past annual reports published by ICS-CERT (2017, 2015, 2013), as the reported incidents increased significantly over the past years.[1] The main reason for the increased susceptibility to security issues of ICSs is the fact that IT and OT are driven by different challenges and, in further consequence, pursue different objectives. While the typical (business) IT systems tend to place more weight on the confidentiality and integrity of data, OT systems (i.e., ICSs) primarily focus on the availability of industrial operations (Knowles et al. 2015). For instance, most industrial network protocols have not been designed with security in mind, but rather focus on reliability and meeting real-time requirements (Knapp & Langill 2014). Thus, ICSs often rely on the *security through obscurity* principle (McLaughlin et al. 2016). A recent study conducted by Dragos, Inc. (2018) supports this claim, as they have found that 64% of the patches for vulnerabilities discovered in ICSs, which have been released in 2017, cannot completely remedy the found weaknesses, due to an insecure design of these systems. Consequently, security aspects must be taken into account when engineering CPSs but then also be considered in subsequent phases of the systems' lifecycle.

Recently, researchers started to explore the concept of digital twins in order to implement security-enhancing technical use cases for CPSs (Bécue et al. 2018, Bitton et al. 2018, Eckhart & Ekelhart 2018*c*,*b*,*a*, Tauber & Schmittner 2018, Damjanovic-

[1] More specifically, the following number of ICS incidents were recorded by fiscal year, starting from 2010 to 2016: 39, 140, 197, 257, 245, 295, 290 (ICS-CERT 2017, 2015, 2013).

Behrendt 2018*a*, Damjanovic-Behrendt 2018*b*), suggesting that it may even qualify for the realization of a holistic approach to CPS security. Most of these works present a specific technical use case, such as privacy enhancement (Damjanovic-Behrendt 2018*b*), even though Eckhart & Ekelhart (2018*c*) give a general, brief overview of the applicability of the digital-twin concept in the CPS security context. However, little is known about the concept's full potential relating to information security as well as the research challenges that need to be addressed in order to overcome barriers to adoption. This chapter aims to fill this gap.

The contribution of this chapter is twofold and can be summarized as follows:

- We introduce the concept of digital twins for the purpose of enhancing the security of CPSs. First, we describe the origins of the digital-twin concept, discuss its use cases in the manufacturing domain, explain the term *digital thread* (Lubell et al. 2013, Singh & Willcox 2018), and clarify how it connects to digital twins. Second, we attempt to establish a coherent definition of the term *digital twin* in the context of information security and map the traditional use cases of the concept to security-related applications.
- We provide a comprehensive outlook on possible research directions worth pursuing. More precisely, we study existing work in the field and explore how current security challenges related to CPSs may be overcome by adopting the digital-twin concept.

The remainder of this chapter is structured as follows. First, in Section 2, we provide background information on the concept of digital twins and the digital thread. In Section 3, we propose a definition of the term *digital twin* in the context of information security and present technical use cases of this concept that aim to strengthen the security of CPSs. Section 4 suggests future research directions based on existing works in the literature. Finally, Section 5 concludes the chapter by summarizing the main findings of this work.

2 Background

This section introduces the concept of digital twins by first describing its origins and then explaining the concept's manifestations. Furthermore, traditional use cases of digital twins in the manufacturing domain are presented. A brief discussion on digital threads and how they relate to digital twins completes this section.

2.1 The Digital Twin

The concept of digital twins has attracted significant attention from both academia and industry in the past few years. In fact, Gartner has even recognized digital twins as a top strategic technology trend for 2019, ranking on place four (Panetta

2018). Upon first glance, it may seem that this term has been introduced merely for marketing purposes in order to revamp a long-established concept, namely the use of virtual models of systems during various phases of their lifecycle (e.g., engineering). The following subsections attempt to demystify this technology buzzword.

2.1.1 Origins of the Concept of Digital Twins

According to Rosen et al. (2015), the concept of digital twins has its origins in NASA's Apollo program, as a twin of a spacecraft was built for two purposes, viz., (i) training before the mission and (ii) supporting the mission by mirroring flight conditions based on data coming from the spacecraft in operation. However, owing to the technological progress concerning simulations and connectivity that has been achieved in the past decades, creating twins has evolved from building physical copies to virtual models of systems (Schleich et al. 2017). As stated in (Rosen et al. 2015, Schleich et al. 2017, Negri et al. 2017), the term *digital twin* was coined by Shafto et al. (2010), who published a report that includes the following definition of the term: "A digital twin is an integrated multiphysics, multiscale simulation of a vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin." While in this seminal work and a few subsequent papers (e.g., Glaessgen & Stargel (2012), Tuegel et al. (2011), Gockel et al. (2012), Reifsnider & Majumdar (2013)), the focus of the digital-twin concept was on mirroring the life of air vehicles, Lee et al. (2013) introduced it to the manufacturing sector in 2013 (Negri et al. 2017). Motivated by the need to utilize machine or process data for the purpose of prognostics, Lee et al. (2013) propose to run digital twins of production systems in the cloud that simulate the conditions of their physical counterparts based on physical models. With the advent of digital twins in the manufacturing domain, the concept expanded to health monitoring, systems engineering (e.g., optimizing the development of control algorithms (Grinshpun et al. 2016)), and managing other phases of the systems' lifecycle (e.g., virtual commissioning (Schluse & Rossmann 2016)) (Negri et al. 2017). Furthermore, Ríos et al. (2015) also investigate the role of digital twins in the Product Lifecycle Management (PLM) and how the digital-twin concept relates to *product avatars* (Hribernik et al. 2006, 2013), i.e., virtual counterparts of products (Negri et al. 2017).

Given the variety of applications for digital twins, multiple interpretations of the concept exist, which is also clearly reflected by the plethora of definitions that can be found in the literature. To clear up the confusion, Negri et al. (2017) provide a comprehensive overview of definitions of the term *digital twin* that appeared in existing works. Interestingly, the authors of (Negri et al. 2017) found that papers related to the digital-twin concept, which do not touch on the simulation aspects, exist, even though it originally emerged from research in this area. Moreover, although several digital-twin related proofs of concept have been developed (e.g., Haag & Anderl (2018), Alam & Saddik (2017), Schroeder, Steinmetz, Pereira & Espindola (2016), Uhlemann et al. (2017), Vachálek et al. (2017)) and some solutions are

already available on the market, there seems to be still a lack of clarity about what constitutes a digital twin. Durão et al. (2018) attempt to address this issue in their recent paper by gathering requirements for the development of digital twins based on a literature review and interviews with professionals from the industry. Their findings indicate that the requirements (i) real-time data, (ii) integration, and (iii) fidelity have been addressed by most of the reviewed works, while at the same time these are the ones that are the most desired properties of industry solutions according to the interviewees. The reason for this is that real-time data that is fed into a digital twin would reflect the actual state of its physical counterpart; thus, making a seamless data integration also a crucial component of digital twins (Durão et al. 2018). Furthermore, the fidelity of digital twins indicates how precisely they mirror their physical counterparts (Durão et al. 2018). However, simulations without real-time data flows still seem to be the state of practice concerning digital twins, even though the adoption of high-fidelity simulations that are able to integrate data in real-time is envisioned for the future (Durão et al. 2018).

2.1.2 Types of Digital Twins

Due to the fact that the interpretation of the digital-twin concept varies among scholars as well as industry professionals and considering that the concept can be applied to solve different problems, several types of digital twins have been proposed so far. As pointed out by Kritzinger et al. (2018), a digital-twin solution is characterized by (i) its intended areas of application, (ii) the used technologies, and (iii) the data integration level. In the following, we focus on the technological characteristics and levels of data integration, as the next subsection, Section 2.1.3, is devoted to the use cases of the digital-twin concept in the manufacturing domain.

As already discussed in Section 2.1.1, the digital-twin concept emerged from advances in the field of modeling and simulation. Boschert & Rosen (2016) even declare digital twins as "the next wave in simulation technology". Over the past 50 years, the number of papers published related to simulation has steadily increased, reaching its peak between 2010 and 2014 with 5,677 published works (Mourtzis et al. 2014). Interestingly, literature analyses of simulation technology in the manufacturing domain (Negahban & Smith 2014, Polenghi et al. 2018) indicate that simulation applications for operational aspects (i.e., middle-of-life phase) attracted increasing research interest from 2002 to 2013, while interest in its applications in the beginning-of-life phase appeared to decline over the same period of time. To give a few examples of simulation applications, *system design*, *facility design/layout*, and *material handling system design* appear to be among the most used in the beginning-of-life phase of manufacturing systems (Polenghi et al. 2018). On the other hand, *operations planning*, *scheduling*, and *real-time control* are among the most used simulation applications in the middle-of-life phase (Polenghi et al. 2018). It is also worth noting that the use of simulation technology plays a little role in the end-of-life phase, even though specialized simulation applications may be vital when decommissioning entails high risks, e.g., as is the case with nuclear power plants (Polenghi

et al. 2018). Considering that a plethora of simulation applications have been studied for both the design and operation phase, adopting a holistic view on how digital twins (i.e., simulation applications) can be leveraged along the systems' lifecycle represents a reasonable next step to take in the light of Industry 4.0. In fact, several works (e.g., Boschert & Rosen (2016), Schluse & Rossmann (2016), Grieves & Vickers (2017)) suggest that the digital twin of a system evolves with its physical counterpart, meaning that fidelity tends to increase as the lifecycle progresses and, by implication, complexity too. An example of a digital twin's lifecycle is given by Schluse & Rossmann (2016), where animations of the system are created in the design phase, a discrete event simulation is then developed for examining the system's performance, followed by a rigid body simulation and a finite element method (FEM) simulation, which are used for further analysis. The authors of (Schluse & Rossmann 2016) expand their idea by proposing *experimentable digital twins*, i.e., interactive virtual replicas of systems that function in a *virtual testbed*, enabling engineers to interactively analyze the system in the environment in which it operates. In this context, 3D simulations play an important role, as accurate visual representations may facilitate certain engineering tasks. Besides adopting simulation technology for realizing the concept of digital twins, there are also a few works that do not associate it with simulation applications (Negri et al. 2017), even though the digital-twin concept evidently has its roots in this field. For example, mere visualizations (e.g., realized by utilizing augmented reality (Schroeder, Steinmetz, Pereira, Muller, Garcia, Espindola & Rodrigues 2016)) or data-driven models based on machine learning methods (e.g., Jaensch et al. (2018)) are also regarded as implementations of the digital-twin concept.

Integrating data, acquired either from past lifecycles or in real-time from live systems, into virtual replicas is a cornerstone of the concept of digital twins. However, in the literature, there appears to be no consensus concerning the minimum level of data integration required for qualifying as an actual implementation of the concept. Consequently, Kritzinger et al. (2018) proposed a classification of the digital-twin concept based on how the data exchange between the virtual replica and its physical counterpart is realized. As shown in Table 1, the authors introduced the terms *digital model* and *digital shadow*, in addition to *digital twin*, which are defined on the basis of the data flows to and from the virtual replica. For instance, according to the definitions proposed by Kritzinger et al. (2018), a digital twin is characterized by an automated, bidirectional data exchange between the real system and its digital representation.[2]

Now that an overview of types of digital twins, which have been covered in the literature, has been provided, views from industry professionals on this topic remain to be discussed. As indicated in Section 2.1.1, Durão et al. (2018) conducted, inter alia, interviews with six companies to gather requirements related to the digital-twin concept. Their study reveals that, from the point of view of industry professionals,

[2] In this work, we do not adopt the classification proposed in (Kritzinger et al. 2018) for the sake of simplicity, as the level of data integration plays only a secondary role for the security-related use cases.

Level of integration	Dataflow	
	Physical → Digital	Digital → Physical
Digital model	Manual	Manual
Digital shadow	Automatic	Manual
Digital twin	Automatic	Automatic

Table 1 Classification based on the level of data integration according to Kritzinger et al. (2018)

the digital-twin concept appears to be regarded as a simulation model of a physical object that does not receive data instantly or continuously (Durão et al. 2018).

2.1.3 Use Cases of Digital Twins in the Manufacturing Domain

Based on the literature reviews conducted by Negri et al. (2017) and Kritzinger et al. (2018), as well as the works published by Rosen et al. (2015) and Grieves & Vickers (2017), we determined the areas of application in the manufacturing domain of the digital-twin concept. In particular, Grieves & Vickers (2017) describe in detail how the concept of digital twins can be utilized in a variety of ways throughout the systems' lifecycle. Furthermore, Negri et al. (2017) identify the following three categories for use cases: (i) *monitoring* (e.g., health assessment), (ii) *mirroring the systems' life* (e.g., lifecycle management), and (iii) *decision support* (e.g., modeling, visualization, simulation, optimization). The works by Kritzinger et al. (2018) and Rosen et al. (2015) provide further details regarding the use cases of the digital-twin concept for cyber-physical production systems (CPPSs) and were therefore used supplementary to gather the areas of application in the manufacturing domain. Figure 1 depicts a CPPS-centric view on the areas of application without considering the product lifecycle (e.g., Ríos et al. (2015)). In the following, we briefly review the role of the digital-twin concept within the three high-level phases of the CPPSs lifecycle, viz., (i) engineering, (ii) operation, (iii) and end-of-life.

In (Grieves & Vickers 2017), the authors explain how the system evolves virtually during engineering until the fabrication of its physical twin. Owing to the use of 2D/3D models as well as physical models to simulate the behavior of systems, the efficiency of the engineering process can be drastically increased (Grieves & Vickers 2017). As already indicated in the previous section, this practice itself is not new per se, but the technological progress made in the past decades opened up new methods to develop realistic, high-fidelity models that facilitate the design, testing, fabrication, and commissioning of systems. On top of that, these models lay the foundation for supporting subsequent activities in the lifecycle (Rosen et al. 2015), making the data model an integral component of digital twins (Negri et al. 2017). Thus, efforts have been made by Schroeder, Steinmetz, Pereira & Espindola (2016) to improve the modeling and exchange of digital-twin-related data by utilizing AutomationML (AML) (Drath et al. 2008), i.e., an engineering data exchange format.

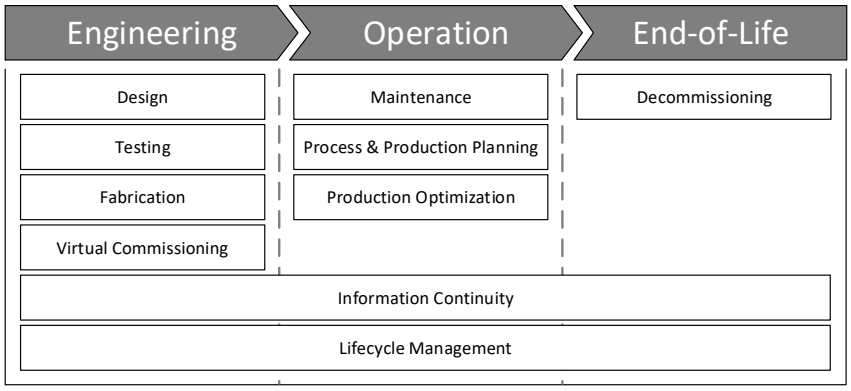

Fig. 1 Areas of application of the digital-twin concept based on (Negri et al. 2017, Rosen et al. 2015, Kritzinger et al. 2018, Grieves & Vickers 2017) within the lifecycle of CPPSs (inspired by Lüder et al. (2017))

Use cases of digital twins that belong to the operation phase typically rely on data coming from real systems. For instance, the health of the system can be continuously assessed by analyzing data collected during operation on the basis of physical models (e.g., as discussed by Glaessgen & Stargel (2012) in the context of air vehicles) in order to prevent failures, reduce downtime, and optimize maintenance. Besides monitoring the health of CPPSs, digital twins have also been adopted for the purpose of optimizing production processes (Uhlemann et al. 2017, Rosen et al. 2015).

Finally, when the end-of-life is reached and the CPPS is decommissioned, the respective digital twin can be of use in two different ways, viz., to retain knowledge about the system's life for reuse, and to properly dispose of its materials (Grieves & Vickers 2017).

2.2 The Digital Thread

According to several sources (West & Pyster 2015, Boschert & Rosen 2016, West & Blackburn 2017), the term *digital thread* has been introduced by the United States Air Force (USAF) (Maybury 2013) to describe the notion of linking data throughout various phases of the lifecycle (e.g., design, processing, manufacturing) in order to increase efficiency in the development and deployment of systems. However, as indicated in (West & Pyster 2015), there appears to be a lack of a consistent definition of this term in the literature. Some scholars (e.g., Boschert & Rosen (2016)) only see a negligible difference between the digital-thread and digital-twin concept, while others (e.g., Singh & Willcox (2018), West & Blackburn (2017)) prefer to keep these two concepts apart. In this work, we adopt the definitions proposed by Lubell et al. (2013) and Singh & Willcox (2018) who describe the digital thread as "[the]

unbroken data link through the lifecycle [. . .]" (Lubell et al. 2013) of a system that can be utilized "[. . .] [to] generate and provide updates to a Digital Twin" (Singh & Willcox 2018). In this context, the interoperability of tools used throughout the lifecycle represents a prerequisite for the implementation of the digital thread. As a result, technologies that foster semantic interoperability (e.g., OPC UA, AML) may become even more important with wider adoption of this concept. Although the works (Eckhart & Ekelhart 2018*c*,*b*, Schroeder, Steinmetz, Pereira & Espindola 2016) do not explicitly mention the digital-thread concept, they provide valuable insights into how AML supports the exchange of data for realizing digital twins.

Although the digital thread can be considered as an enabler for digital twins, which in turn may be leveraged to improve the security of CPSs, the digital thread represents an attractive target for attacks, as it links various assets that are high in value (e.g., design artifacts) (Glavach et al. 2017). Due to the fact that a compromised digital thread may lead to severe consequences (e.g., manipulated updates to put the digital twin into a malicious state), adequate security measures to protect each link within the digital thread are paramount.

3 Digital Twins in the Information Security Domain

In this section, we review the definitions given in earlier works that deal with security aspects of CPSs in conjunction with the concept of digital twins and attempt to make one step toward a coherent definition of the term *digital twin* in the context of information security. Furthermore, we extend the use cases presented in (Eckhart & Ekelhart 2018*c*) (viz., (i) intrusion detection, (ii) system testing & simulation, (iii) detecting misconfigurations, and (iv) penetration testing) in order to provide a more comprehensive view of the significance of the digital-twin concept for the information security community. Besides extending the research conducted by Eckhart & Ekelhart (2018*c*), we expand on the use cases that have been proposed in other previous works, viz., (Bécue et al. 2018, Bitton et al. 2018, Tauber & Schmittner 2018, Damjanovic-Behrendt 2018*a*, Damjanovic-Behrendt 2018*b*). Thus, this section shows the state of the art in using the concept of digital twins to increase the security of CPSs.

3.1 Definitions

In the recent past, a few works have appeared that explore how the concept of digital twins can be applied to secure CPSs. Table 2 provides an overview of the *digital twin* definitions given in these works and thereby extends the view of definitions presented in (Negri et al. 2017).

As can be seen in Table 2, the definitions overlap to some extent, yet include aspects that are relevant to the respective use cases presented in these papers. For

Reference	Definition of the term *Digital Twin*
Bécue et al. (2018)	"[. . .] [An] evolving digital profile of the historical and current behavior of a physical object or process."
Bitton et al. (2018)	"[. . .] [A] replica of a specific ICS; i.e., a model that consists of all of the components from the original industrial environment."
Damjanovic-Behrendt (2018*b*)	"[. . .] [A] virtual counterpart to actual physical devices (entities) that combines many Artificial Intelligence (AI)-based technologies and methods, real-time predictive analyses, and forecasting algorithms performing on top of Big Data derived from the Internet of Things (IoT) sensors and acquired historical data."
Eckhart & Ekelhart (2018*c*)	Refers to the definition proposed by Shafto et al. (2010), namely "[. . .] the use of holistic simulations to virtually mirror a physical system."
Eckhart & Ekelhart (2018*a*)	"[. . .] virtual replicas of the network and the logic layer of physical devices, closely matching the physical devices' behavior on these layers."
Eckhart & Ekelhart (2018*b*)	Semantically equivalent to the definition given in (Eckhart & Ekelhart 2018*a*).
Tauber & Schmittner (2018)	"[. . .] [A] digital representation of a real system, with the history of all changes and developments."

Table 2 Definitions of the term *digital twin* in papers published on information security

instance, Bécue et al. (2018), Damjanovic-Behrendt (2018*b*), Tauber & Schmittner (2018) express that a digital twin is not only composed of a system's virtual model but also includes historical information thereof. Furthermore, the definition given by Bécue et al. (2018) explicitly includes physical processes, which may be useful for implementing process-aware intrusion detection systems (IDSs) (e.g., Nivethan & Papa (2016), Chromik et al. (2016)).

To foster a common understanding of the term *digital twin* in the context of information security, we propose a definition that reflects the recent research progress made in this field. In particular, in the following, we introduce a uniform definition based on the synthesized interpretations from works cited in Table 2: A digital twin, which is used for the purpose of enhancing the security of a cyber-physical system, is a *virtual replica of a system that accompanies its physical counterpart during phases of its lifecycle, consumes real-time and historical data if required, and has sufficient fidelity to allow the implementation of the desired security measure*. It is worth noting that we assume that the knowledge about the process can be contained in a digital twin, depending on the implemented use case. For instance, the digital twins in (Eckhart & Ekelhart 2018*c*,*b*,*a*) represent simulated or emulated devices that can accurately mirror the physical counterparts on the logic and network layer, meaning that process knowledge is readily accessible through them. On the other hand, in (Damjanovic-Behrendt 2018*b*), the digital twins are composed of machine

learning methods that learn security- and privacy-relevant aspects based on sensor data. Thus, process knowledge can merely be learned, but not obtained directly through digital twins, as they are not aware of any control logic per se.

3.2 Security Use Cases of Digital Twins

Similarly to Section 2.1.3, we assigned the security-relevant use cases to the phases of the CPS lifecycle (cf. Figure 2). The following subsections discuss each of these uses cases in detail.

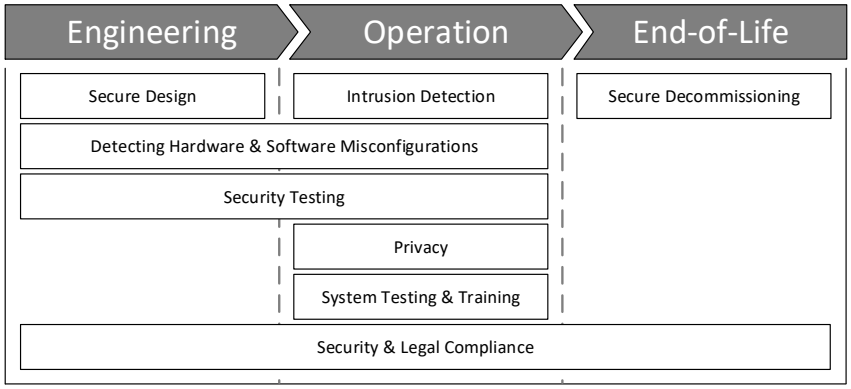

Fig. 2 Security-relevant use cases of the digital-twin concept based on (Bécue et al. 2018, Bitton et al. 2018, Eckhart & Ekelhart 2018*c*,*b*,*a*, Tauber & Schmittner 2018, Damjanovic-Behrendt 2018*a*, Damjanovic-Behrendt 2018*b*) within the lifecycle of CPSs (inspired by Lüder et al. (2017))

3.2.1 Secure Design of Cyber-Physical Systems

Digital twins that gradually evolve over the course of the engineering may support engineers in designing more secure CPSs.

For instance, Bécue et al. (2018) suggest to use digital twins in combination with a cyber range[3] to analyze how the system to be engineered behaves under attack. The authors state that this method would allow engineers to estimate potential damages, which may facilitate designing the security and safety mechanisms of CPSs. As

[3] Bécue et al. (2018) do not provide a definition of the term *cyber range*, but they indicate that it represents a virtual environment that provides the means to interact with the digital twins, e.g., to execute attacks against them.

a result, this security activity may yield more robust and fault-tolerant designs of CPSs.

Besides simulating attacks to evaluate whether the system fails securely and safely, a virtual representation of the CPSs may also support reducing the attack surface. In particular, security analyses conducted on the basis of digital twins can reveal weak spots in the architecture, unnecessary functionality of devices or even unprotected services that would allow an adversary to gain a foothold in the system. To give an example, digital twins that have been automatically generated from specification (Eckhart & Ekelhart 2018*c*) may allow security analysts to identify unused network services by first recording the network traffic while simulating plant operation and then mapping the captured traffic flows to the specified services. As a consequence, this activity would expose superfluous network services in the specification of the CPS, meaning that they can be removed entirely without restraining plant operation and thereby minimize the attack surface.

Additionally, digital twins that are equipped with logic and network features (Eckhart & Ekelhart 2018*c*) may aid in realizing a defense in depth strategy, as network security controls can be thoroughly tested by simulating attack scenarios layer-wise. For example, security analysts could test whether an attacker is able to pivot from a compromised data historian to a programmable logic controller (PLC) with the objective to steer the plant into an insecure state.

Another viable technical use case in this context is the evaluation of how damages can be limited in the event of a compromise. In particular, simulating attack scenarios may help in preparing a containment strategy for compromised devices and thereby facilitate incident handling in the operation phase.

3.2.2 Intrusion Detection

In 2017, Rubio et al. (2017) published a survey paper on IDSs for ICSs. In this paper, the authors discuss, inter alia, the role of IDSs in the context of Industry 4.0 and suggest that the concept of digital twins provides promising opportunities in this area.

To the best of our knowledge, only two papers, namely (Eckhart & Ekelhart 2018*c*,*b*), have been published thus far that demonstrate how the concept of digital twins can be leveraged to implement IDSs.[4]

In the first work by Eckhart & Ekelhart (2018*c*), the authors show how a knowledge-based intrusion detection system can be implemented. This particular intrusion detection technique relies on certain misuse patterns that the system would exhibit upon a compromise (Mitchell & Chen 2014). In (Eckhart & Ekelhart 2018*c*), these patterns have been specified with AML and are part of the specification of the CPS. More specifically, the authors defined two rules, namely a safety and security rule, that specific digital twins must adhere to. The safety rule specifies a threshold for a tag of a PLC (maximum velocity of a motor that the PLC controls), whereas

[4] In this work, we adopt the classification of intrusion detection techniques proposed by Mitchell & Chen (2014).

the security rule defines a consistency check between a tag of a PLC and a tag of an human-machine interface (HMI) (the velocity of a motor can be set by using the HMI, as it can send a request to the PLC that controls the motor; thus, it can be assumed that the respective tags on these two devices should match). During the operation of the CPS, the digital twins are checked continuously for any rule violations. However, the authors of (Eckhart & Ekelhart 2018*c*) do not touch on the aspects concerning the replication of states to digital twins and merely evaluate the implemented IDS in simulation mode, i.e., without incorporating real-time data from live systems into digital twins so that they do not mirror the behavior of their physical counterparts during plant operation. Furthermore, although this intrusion detection technique generally yields a low false-positive rate, it is limited to detecting known misbehavior (Mitchell & Chen 2014).

Their second work (Eckhart & Ekelhart 2018*b*) builds on (Eckhart & Ekelhart 2018*c*), as the authors introduce a passive state replication approach that aims to replicate the program states from physical devices to the corresponding digital twins. Based on this state replication approach, the digital twins follow the states of their physical counterparts and thereby allow to virtually mirror the behavior of the real CPS during operation. It is self-evident that the implementation of such a state replication approach represents a fundamental requirement for realizing the intrusion detection use case, as the digital twins are utilized for detecting abnormal behavior that the real CPS may exhibit. To demonstrate the viability of the proposed state replication approach, Eckhart & Ekelhart (2018*b*) implemented a behavior-specification-based IDS and evaluated the effectiveness thereof by launching a man-in-the-middle (MITM) and an insider attack against a real CPS. This intrusion detection technique requires that the correct, benign behavior of the system is defined, as this specification is utilized to determine whether the system's behavior during runtime diverges from it due to an intrusion (Mitchell & Chen 2014). The beauty of this intrusion detection technique is that it generally yields a low false-negative rate while also being capable of detecting attacks that were unknown at the time of defining the legitimate behavior (Mitchell & Chen 2014). On the contrary, creating the specification of the system's correct behavior typically requires effort (Mitchell & Chen 2014). In (Eckhart & Ekelhart 2018*b*), the authors evade this issue intentionally by making the assumption that the specification of the CPS is readily available, as it has been developed in the course of the engineering phase. The specification of the CPS can then be used to automatically generate the digital twins, which model the correct behavior of their physical counterparts. During operation, the states of the physical devices are passively observed in the real environment and then replicated virtually in order to ensure that the digital twins receive the same inputs (e.g., network packet, simulated digital input, user input) as their physical counterparts. If, for example, a programmer performs an insider attack by manipulating the source code of a PLC, its behavior will deviate from that of the corresponding digital twin, provided that the adversary was not able to tamper with the specification. As a result, an intrusion can simply be detected by comparing the inputs and outputs of physical devices and those of the digital twins.

3.2.3 Detecting Hardware and Software Misconfigurations

Assuming that the hardware and software of devices is simulated or emulated to form digital twins, these virtual representations should mimic the functionality of corresponding devices to a certain level of detail. For example, the digital twin of a PLC may have a similar (virtualized) communications interface and I/O modules for the hardware layer, while the software layer may be replicated by executing the control logic. Thus, it can be expected to observe the common features of a digital twin and its physical counterpart. If hardware and software configurations of real devices have been manipulated, the digital twin should exhibit noticeable differences in terms of its characteristics, which would be indicative of malicious actions. As a matter of fact, this technical use case is similar to implementing a behavior-specification-based IDS based on digital twins in the sense that any deviation between the virtual replicas and their physical counterparts may indicate an attack.

Moreover, detecting manipulated software configurations can also be achieved by comparing configuration data (e.g., parameterization) of physical devices to their corresponding digital twins (Eckhart & Ekelhart 2018*c*). Yet, instead of checking whether the behavior of the physical devices deviates from that of their corresponding digital twins, only the software configuration settings are checked.

It is also worth highlighting that for realizing this technical use case, we have to assume that the digital twins run in an isolated environment protected against malicious acts. Otherwise, an adversary could tamper with the digital twins' configurations to ensure that any manipulations of the physical devices' configurations go unnoticed.

As can be seen in Figure 2, this use case can be applied in two different phases of the CPSs' lifecycle. First, in the course of the commissioning of CPSs, the digital twins can be used to test if the devices have been set up according to their virtual replicas. Since security controls may be completely or partially deactivated during commissioning in order to ease the start-up phase, external or internal (i.e., commissioning staff) threat actors may be able to launch attacks even before the actual operation of the CPS. Thus, running final security checks to test the systems' configurations on the basis of their virtual replicas prior to the final acceptance may be worthwhile. Second, running these checks can be continued after commissioning in order to ensure that the integrity of configuration data is maintained throughout the operation phase. Evidently, if any legitimate changes to the physical devices' configurations are made during the operation phase, the configurations of the respective digital twins have to be adjusted.

3.2.4 Security Testing

Conducting security tests in OT environments represents a critical activity, especially when these tests are carried out during the operation of the CPS. In the past, multiple incidents occurred due to penetration tests that were carried out on live systems, causing severe physical damages and business interruption (Duggan et al. 2005).

Thus, a testbed may be used in order to avoid any interference with live systems. However, building and maintaining a testbed can be time- and cost-intensive, in particular, when it should accurately reflect the actual CPS in operation (Eckhart & Ekelhart 2018*c*, Bitton et al. 2018). The adoption of digital twins has been proposed to address this issue (Eckhart & Ekelhart 2018*c*, Bitton et al. 2018, Bécue et al. 2018). In essence, digital twins enable penetration testers to perform security tests virtually, i.e., on the digital twins instead of on real systems. In this way, it can be ensured that the execution of these tests does not negatively affect the operation of live systems while also sparing operators from having to deal with the costs associated with testbeds. However, in this context, the challenge is to balance the fidelity of digital twins and the costs involved in creating them, so that the conducted security tests still yield useful results whilst keeping expenses low. In the work published by Bitton et al. (2018), the authors attempt to solve this problem by proposing a method for developing a cost-effective specification of a digital twin that would support the execution of specific security tests under a certain budget.

Besides performing security assessments in the operation phase, this approach can be likewise applied during engineering in order to fix vulnerabilities early on in the lifecycle of the CPS.

3.2.5 Privacy

Damjanovic-Behrendt (2018*b*) studied how the concept of digital twins can be applied to protect the privacy of smart car drivers. In particular, this work explores how automated privacy assessments can be carried out based on a virtual replica of a smart car that continuously receives data (e.g., from on-board sensors) in real time. The author provides an exemplary use case in which an insurer offers a usage-based insurance product based on the data obtained from the digital twins of smart cars. Since the digital twins integrate machine learning methods to classify personal data that can then be anonymized prior to the data transfer to the insurer, the customers' privacy rights are preserved. In this way, the concept of digital twins assists *controllers* or *processors* in meeting General Data Protection Regulation (GDPR) requirements.

Although the work published by Damjanovic-Behrendt (2018*b*) focuses on smart cars, the presented approach appears to be also applicable to other types of CPSs. Nevertheless, privacy-enhancing techniques based on the digital-twin concept for smart grids, transportation systems and, in particular, medical CPSs may be worth exploring in greater detail.

3.2.6 System Testing and Training

Due to the fact that digital twins only exist virtually and are typically running in an environment that is isolated from live systems, they may also qualify to be used as a

testing and training platform. Similarly to a cyber range, users could test new defenses before putting them into production or train how to respond to cyber incidents.

In (Bécue et al. 2018), the authors propose to adopt digital twins in combination with a cyber range to realize this use case. In particular, their work suggests launching attacks against digital twins from the cyber range for training and testing purposes.

Eckhart & Ekelhart (2018*c*) describe system testing as a use case for their proposed digital-twin framework. For example, similar to hardware-in-the-loop (HIL) simulation, real devices may be interfaced with the digital-twin framework for the purpose of testing. The authors of (Eckhart & Ekelhart 2018*c*) also present a proof of concept, named *CPS Twinning*[5], which may provide rudimentary support for testing the network and logic layer of the CPS. This reason behind this claim is that the framework provides a virtual environment based on *Mininet* (Lantz et al. 2010) to emulate the network layer of the CPS but also supports a variety of device types (e.g., PLC, HMI, motor) whose logic can be virtually replicated to some extent. Based on this, it seems to be that their proposed digital-twin framework can also serve as a training tool, even though the authors do not explicitly mention this use case. Taking this idea one step further, *CPS Twinning* may also be suitable for carrying out red vs. blue team exercises that involve the network and logic layer of the CPS. Besides uncovering weaknesses resulting from the attacks launched by the red team, these exercises can also be used for training information security personnel (i.e., blue team) to implement adequate defenses in response to attacks. Collecting data over the course of such events, which may be helpful for risk assessments, can be a side benefit of these exercises (Sommestad & Hallberg 2012, Cook et al. 2016).

3.2.7 Secure Decommissioning

CPSs and, in particular, ICSs tend to have a long lifecycle, which can be up to 30 years (Macaulay & Singer 2016) or even longer. Yet, when the end-of-life phase is eventually reached, it must be ensured that components are disposed of in a secure manner.

In addition to supporting the proper disposal of materials (Grieves & Vickers 2017) (cf. Section 2.1.3), digital twins may also help to answer questions related to media sanitization. For instance, the NIST SP 800-88 (Kissel et al. 2014) guideline suggests considering, inter alia, confidentiality requirements of data as well as the costs associated with the sanitization process.

While the digital twins and the digital thread may facilitate secure disposal of physical devices, they can be equally affected by unauthorized access, if data security requirements are not met when disposing of them. Thus, it must be ensured that the digital thread is not only cut off but also properly archived and that the digital twins are finally laid to rest securely.

[5] `https://github.com/sbaresearch/cps-twinning`

3.2.8 Security and Legal Compliance

Recently, Tauber & Schmittner (2018) published an article that highlights the importance of monitoring the CPS's security and safety posture during operation. The authors emphasize that this activity could provide evidence of meeting security standards (e.g., IEC 62443 (IEC 2009)), which would, in turn, assist organizations in complying with legal requirements. In particular, Tauber & Schmittner (2018) suggest that the digital twins may provide an accurate reflection of CPSs throughout their entire lifecycle and thereby allow continuous monitoring and documentation of security and safety aspects. Considering that regulatory requirements for operators of CPSs appears to be increasing (e.g., the NIS Directive (European Parliament and the Council of the European Union 2016) for critical infrastructure providers), integrating security and legal compliance support into digital twins seems worthwhile.

4 Future Research Directions

This chapter has discussed several security-enhancing use cases for digital twins that may be worth researching in depth. Besides these use cases, we identified a variety of interesting questions in need of further investigation. In particular, we derived research directions as well as gaps from these questions and determined relevant work that may serve as a starting point for future studies. Furthermore, we classified the research directions according to their applicability in the three high-level lifecycle phases, viz., engineering, operation, and end-of-life. Table 3 summarizes the results of this assessment. In the following, we briefly discuss the identified research directions.

Practical Aspects

Examining the practicality of applying the digital-twin concept for securing CPSs focuses on answering fundamental research questions related to efficiently creating, maintaining, and running digital twins. These research topics are motivated by cost-benefit considerations, as implementing a digital-twin framework that supports the use cases presented in Section 3.2 seems to require substantial effort. Although such a digital-twin framework could leverage existing open-source tools (cf. Eckhart & Ekelhart (2018*c*)), there is still significant work required to achieve an implementation of digital twins that provides an adequate level of detail for the desired use cases. In fact, this issue appears to be a major barrier to adopting the digital-twin concept, as other non-digital-twin approaches to implementing these security-enhancing use cases (e.g., intrusion detection) may incur less overhead in terms of effort required for implementation and maintenance (in the CPS's operation phase). Thus, a necessary first step would be to determine the required fidelity of digital twins for realizing the use cases discussed in Section 3.2. Note that creating identical digital

Research direction	Research gaps	Phase		
		E	O	D
Practical aspects	• Limited understanding of the required fidelity for use cases • Accuracy and performance requirements for use cases are unknown • Evaluation in a real-world setting is required	●	●	●
Legacy systems	• Automated generation of digital twins despite non-existent specification • Dealing with proprietary hardware and software of CPSs		●	
Risk assessment	• Unknown how cyber risks can be (automatically) identified, quantified, and (re-)evaluated based on digital twins	●	●	●
Resilience improvements	• Little is known how resilience can be measured based on digital twins • Unknown how to simulate attacks against digital twins	●	●	
Automated security testing	• Little is known how security tests for CPSs can be generated and executed in the digital-twin environment	●	●	
Intrusion detection	• Monitoring the physics of CPSs based on digital twins to detect intrusions is unexplored thus far		●	
Intrusion prevention	• Feasibility is unknown • Introduced latency is an obstacle, especially when real-time requirements must be met		●	
Honeypots	• Questionable how the behavior of digital twins can be altered to avoid disclosing valuable information while ensuring that the honeypot is still realistic		●	
Incident response training	• Attack simulation is an obstacle • Unknown whether digital twins can be exploited as a cost-effective training environment		●	
Attacks based on digital twins	• Unknown how digital twins or the digital thread can be exploited for launching advanced, covert attacks	●	●	
Attacks against digital twins	• Consequences of attacks against digital twins are unknown	●	●	

E = Engineering, O = Operation, D = Decommissioning (End-of-Life)

Table 3 Overview of research directions related to digital twins and information security

representations that replicate the CPS in its entirety would defeat the concept's purpose, as the digital twin should merely provide support instead of a redundancy gain for protecting against failures of the real system. The work by Bitton et al. (2018) represents a valuable contribution toward the cost-efficient development of digital twins. However, it is still unknown how accurately the digital twins are required to follow the states of their physical counterparts. In this context, achieving sufficient performance of the digital twins represents an obstacle (Eckhart & Ekelhart 2018*b*). As a result, identifying the optimal balance between budget and the required fidelity as well as state replication accuracy is still a research direction worth pursuing.

Legacy Systems

Considering the typical long lifecycle of CPSs, implementing the digital-twin concept for brownfield sites will become increasingly important. These legacy systems tend to be insufficiently documented and detailed knowledge of their inner workings is rare. This, however, affects the accuracy of the virtual models to be developed, as a lack of understanding of the legacy system may lead to a flawed digital representation thereof. In (Eckhart & Ekelhart 2018*c*), the authors present a rudimentary prototype that allows to automatically generate digital twins based on the specification of the CPS. In their paper, the authors make the strong assumption that the specification is complete to the extent that the presented use case (i.e., intrusion detection) can be realized and that it is available in the engineering data exchange format AML. However, in a real-world setting, the specification of the CPS may be nonexistent or incomplete, at least for realizing the security-enhancing use cases discussed in Section 3.2. Nevertheless, this challenge may be overcome by first determining the information required to realize a specific use case (i.e., abstraction level of the digital twin), and then mining the specification from existing resources (e.g., monitoring systems, extracting data from other related artifacts). For example, Caselli et al. (2016) propose a specification mining approach for the implementation of an intrusion detection system used in building automation systems. Their work may be a starting point for researching mining methods capable of yielding a specification that can then be used to generate digital twins for the purpose of intrusion detection. On the other hand, if legacy virtual models are indeed available, research is required on how they can be retrofitted for digital-twin applications.

Risk Assessment

Cook et al. (2016) indicate the need for a CPS simulation environment, allowing the execution of attack scenarios that could then be factored into the risk assessment. The authors propose to adapt simulations of physical processes in a way that would allow consideration of boundary conditions caused by attacks, provided that these simulations already exist. In this way, the severity of potential cyber incidents would become apparent. Cook et al. (2016) also suggest that this could be realized by blend-

ing virtualized and physical devices, taking into account that such an environment must also support the representation of threat scenarios and potential consequences (e.g., financial loss) thereof. Thus, in the context of the digital-twin concept, this would mean that digital twins must be equipped with (i) accurate knowledge about the process under control (i.e., simulating the physical process) and not just replicating the control systems' logic (i.e., executing the programs that are running on their physical counterparts) and (ii) features to describe and simulate cyber risks. Both topics have been covered already in the literature, albeit not associated with digital twins. For instance, Krotofil et al. (2015) present a framework named *Damn Vulnerable Chemical Process (DVCP)* that leverages the Tennessee Eastman (Downs & Vogel 1993) and Vinyl Acetate (Chen et al. 2003) process models, enabling users to simulate attacks on the physical layer. Moreover, a considerable amount of literature has been published on simulating network attacks (e.g., Chabukswar et al. (2010)) and assessing the impact of (simulated) threats to CPSs (e.g., Bracho et al. (2018)).

It is also worth mentioning that a digital-twin approach to risk assessment may be suitable to deal with the dynamic nature of cyber risks. As a side note, both the probability of an attack and its impact can vary throughout the operation phase of the CPSs, meaning that risk mitigation strategies must be adapted accordingly. If digital twins run in parallel to their physical counterparts (i.e., they continuously mirror the behavior of real devices), this may be a viable approach to dynamic security risk assessment.

Resilience Improvements

In the context of ICSs, and presumably, also CPSs, (cyber) resilience refers to the systems' ability to maintain an adequate level of control of the physical process despite facing undesirable incidents (e.g., being under attack) (Wei & Ji 2010). As proposed by Wei & Ji (2010), improving the resilience of ICSs may be achieved by following a four-step process, which consists of (i) risk assessment, (ii) resilience engineering, (iii) resilience operation, and (iv) resilience enhancement. In essence, these four steps aim to minimize the probability of incidents occurring, their impacts, and the time required to recover from them, albeit at different phases of the ICSs's lifecycle. The concept of digital twins may support activities of this four-step process, as it may enable users to systematically introduce chaos (e.g., by simulating cyber attacks) into virtualized environments reflecting the real systems used for process control. In this way, users can determine the potential loss incurred (e.g., in terms of service degradation) and, in further consequence, mitigate these incidents.

A few works have been published on improving the (cyber) resilience of CPSs, which also give pointers for this future research direction of the digital-twin concept. For example, the work by Krotofil & Cárdenas (2013) investigates how the resilience of physical processes against manipulations of sensor readings can be increased. Their work shows that a well-versed adversary could maximize the economic and safety impact of malicious acts by strategically targeting specific sensors and manipulating readings at different points in time, depending on the process dynamics.

This, by implication, means that the control system may be designed in a way that could make the physical process more resilient to certain kinds of attacks (Krotofil & Cárdenas 2013). Krotofil & Cárdenas (2013) leverage a simulation of the Tennessee Eastman process (Downs & Vogel 1993) for conducting their experiments to analyze process resilience. If such process simulations provide an interface for digital twins, a more comprehensive analysis of plant resilience may be feasible, also allowing to examine resilience at the system level.

Automated Security Testing

Automating security analyses of CPSs is an emerging research area. Several works, such as (Lemaire et al. 2017) and (Depamelaere et al. 2018), propose methodologies that aim to automate the identification of vulnerabilities of CPSs based on system models, which, for example, have been created in SysML during engineering. Extending this idea to the concept of digital twins, security tests may be automatically executed against virtual models reflecting either early versions of the systems to be engineered or the actual system during operation. Put differently, instead of automatically analyzing the systems' specifications to spot weaknesses, automated security tests are run continuously aiming to discover newly introduced flaws in digital twins. The beauty of this approach is that a replica of the actual system's implementation (i.e., the digital twin) can be tested, rather than, or in addition to, verifying that its specification does not have security weaknesses. Furthermore, depending on the fidelity of digital twins, certain types of security tests may be feasible. To give an example, digital twins that mirror the network and logic layer of devices may allow performing automated vulnerability scanning of the CPS's infrastructure.

In general, automated security testing based on the concept of digital twins may be beneficial for both the engineering and operation phase of CPSs. In the engineering phase, this use case may be applied on low- to medium-fidelity digital twins to check for potential attack vectors after certain engineering activities have been performed. On the other hand, in the operation phase of CPS, automated security tests may be executed against high-fidelity digital twins when adaptations to the CPS are made.

Although this security-enhancing use case may appear far-fetched at the present state of digital-twin research, in particular, the work by Eckhart & Ekelhart (2018*c*) already provides initial insights into how a digital-twin framework may be realized, which seems to be also extensible to support automated security testing.

Intrusion Detection & Intrusion Prevention

As indicated in Section 3.2.2, the first steps in this research direction have already been taken, as a knowledge- and behavior-specification-based IDS, which both build on the digital-twin concept, is presented in (Eckhart & Ekelhart 2018*c*,*b*). These works primarily focus on mirroring the logic and network layer of real devices, leaving the CPS's physical properties out. However, due to the fact that CPSs interact

with the real world (e.g., for the purpose of controlling a physical process), it is possible to take advantage of the physical properties of these systems and use them as another dimension for detecting intrusions. In recent years, researchers have shown an increased interest in physics-based intrusion detection techniques (Giraldo et al. 2018). According to Giraldo et al. (2018), these techniques are characterized by the use of models of the physical system (e.g., autoregressive or linear dynamical state-space models) in order to predict system behavior. The predictions are then used to determine whether the sensor readings deviate from what is expected and whether the system reaches an unsafe state (Giraldo et al. 2018). Although digital twins may already include models that represent the physical properties of the system, researchers have not yet demonstrated how they can be utilized to detect intrusions. To date, only one paper (Eckhart & Ekelhart 2018*c*) mentions physics-based IDSs in the context of digital twins, albeit the work lacks further explanation on how this approach can be implemented. Thus, future research needs to be conducted in order to examine how digital twins that are composed of physical models can be leveraged for physics-based intrusion detection.

Besides investigating how physics-based IDSs can be implemented based on the digital-twin concept, realizing behavior-based IDSs by using data-driven digital twins may be another possible area of future research. Although no work has been published on this subject matter to date, we believe that the research conducted by Damjanovic-Behrendt (2018*b*) could represent the first step toward this direction, as this work covers digital twins that integrate machine learning methods to detect privacy-related anomalies.

Investigating new approaches to detect intrusions accurately is a major area of interest within the field of CPSs security. Yet, the mere detection of intrusions is of limited use if countermeasures cannot be taken in a timely manner, since the launched attacks may have already caused damages to equipment, environment or human health. Therefore, intrusion prevention systems (IPSs) may be required, as they provide the means to take active security measures (e.g., by blocking malicious control commands) before incidents occur. However, as, for example, indicated in (Cárdenas et al. 2011), developing IPSs for CPSs represents a challenging task, due to the fact that false alarms (e.g., dropped packets of benign control commands) may raise safety concerns. Overcoming this challenge seems to be also relevant for digital-twin research in general, since data flows from a digital twin (back) to its physical counterpart can serve as a response mechanism (Kritzinger et al. 2018). Thus, further research regarding the role of digital twins for realizing IPSs for CPSs would be worthwhile.

Honeypots

Honeypots are systems that are installed for the sole purpose of being attacked (Spitzner 2002). These systems have several advantages, for example, (i) detecting intrusions, (ii) deterring attackers, or (iii) capturing malicious actions (e.g., attack patterns) for subsequent analysis (Spitzner 2002). Thus, honeypots can be used by

defenders as a security measure, and by security researchers as a means to develop novel countermeasures.

If honeypots are deployed with the objective to lure adversaries who launch targeted attacks, they should be as realistic (in terms of mimicking the real systems) and attractive (i.e., worthwhile to attack) as possible. Physical honeypots are composed of real devices; therefore, representing the most realistic form of honeypots (Antonioli et al. 2016). In recent years, a few works have been published that demonstrate how these honeypots can be used for CPSs (e.g., *HoneyTrain* (Fichtner & Krammel 2015), *SIPHON* (Guarnizo et al. 2017)). Although physical honeypots may allow defenders to gain a deep understanding of attacks, the development and maintenance costs associated with them may be too high, especially when used for CPSs (Antonioli et al. 2016). To alleviate this problem, the systems designated to lure attackers can also be virtualized. Depending on the achieved fidelity or realism of virtual honeypots, they can be categorized into low- and high-interaction honeypots (Fan et al. 2015). Past research has explored low- (e.g., Vasilomanolakis et al. (2016), Rist et al. (n.d.)) as well as high-interaction (e.g., Antonioli et al. (2016), Zhao & Qin (2017)) virtual honeypots for CPSs, meaning that future work can build on a considerable body of research that deals with both types of honeypots.

Since digital twins can be considered as virtual replicas of physical devices, it appears that digital twins and virtual honeypots can also share commonalities in terms of their implementation. Thus, digital twins may also be exploited as a honeypot or, more precisely, honeynet (i.e., a network of honeypots (Fan et al. 2015)) solution. Implementation-wise, this similarity can already be observed between the works (Antonioli et al. 2016) and (Eckhart & Ekelhart 2018*c*), as both of the therein presented prototypes are based on *Mininet* (Lantz et al. 2010) to emulate the network layer, albeit they are unrelated to each other. If digital twins accurately reflect physical devices, except for the vulnerabilities that have been introduced deliberately, and follow the states of their physical counterparts, a significant increase of the honeynet's level of realism may be achieved. As a result, the simulated plant behavior may spark the adversary's interest in attacking the honeynet.

The primary issue of exploiting digital twins as honeypots is that defenders would give adversaries a detailed picture of the real plant upfront, making attacks against the real systems significantly easier, provided that adversaries are able to detect the trap. Based on this, we can derive the following research question: How can existing digital twins be modified in a cost-effective manner so that they can still mimic plausible plant behavior while ensuring that attackers do not gain valuable information about the real systems when they fall for these honeypots? Answering this research question will provide insights into the feasibility and applicability of realizing honeypots based on the concept of digital twins.

Incident Response Training

Section 3.2.6 discusses the idea of utilizing digital twins as a testing and incident response training platform, which resembles the notion of cyber ranges. Similar to

traditional training environments for CPSs and, in particular, ICSs (Plumley et al. 2017), the supported training scenarios vary depending on digital twins' fidelity. In this context, the cost-effectiveness of digital twins seems to be a major research challenge. Although Bitton et al. (2018) already made the first steps toward a cost-effective digital twin for the purpose of conducting security analyses, it is unknown whether exploiting the digital-twin concept for certain training purposes, which would require an advanced fidelity, is financially worthwhile. For instance, the cost associated with achieving the fidelity required to support forensic investigation training scenarios may potentially exceed the cost of the real device. Thus, further research regarding the cost-effectiveness of digital twins for incident response training would be interesting. The work by Plumley et al. (2017) may be used as a starting point, as they provide a categorization of ICSs training environments that aids in determining the required level of realism based on training needs and budget constraints.

Covert Attacks Based on Digital Twins and Attacks Against Digital Twins

Stuxnet, one of the most prominent examples of ICS-tailored malware, aimed to cause significant equipment damage at the nuclear facility at Natanz by covertly manipulating the speed of centrifuge rotors (Langner 2013). According to Langner (2013), the attackers behind Stuxnet had a deep understanding of the plant design, which enabled them to tailor the malware to the target plant. The discovery of the Stuxnet malware led to an increased interest in such covert attacks against CPSs, i.e., attacks that are executed based on in-depth knowledge about the physical process and corresponding control devices in order to manipulate plant behavior in a covert manner. Due to the fact that digital twins may constitute accurate virtual replicas of physical devices, they represent valuable knowledge that might be misused for launching covert attacks if they were to fall into unfriendly hands. Building upon existing research in the area of covert attacks (e.g., Smith (2015), de Sá et al. (2017)), it would be interesting to analyze the level of covertness that can be achieved based on digital twins, which have been obtained by attackers beforehand.

Another possible abuse case of digital twins is to launch targeted attacks against them in order to sabotage (security-enhancing) use cases and potentially also the behavior of their physical counterparts, provided that backflows to physical devices exist. Taking the example of intrusion detection (cf. Section 3.2.2), if attackers are able to manipulate the behavior of digital twins, they can ensure that the digital twins do not exhibit the defined pattern of misbehavior (to delude knowledge-based IDSs) nor deviate from their physical counterparts (to delude behavior-specification-based IDSs), hence allowing them to remain undetected when attacking the real systems. Furthermore, if digital twins directly affect plant operation (e.g., via an automatic data flow to field devices for optimizing manufacturing processes), attacks launched against them may have similar consequences as direct attacks against real devices.

To sum up, more research is definitely needed to better understand the threats posed by unsecured digital twins and to investigate how to mitigate them.

5 Conclusion

This chapter set out to provide a comprehensive overview of how the concept of digital twins can be applied to strengthen the security of CPSs. In particular, we have (i) provided relevant background information about the digital-twin concept, (ii) proposed a definition of the term *digital twin* in the context of information security, (iii) described security-enhancing use cases of the concept, and (iv) suggested future research directions.

The concept of digital twins appears to be an emergent stream of research in the information security field. Thus far, only a few papers have been published that merely scratch the surface of what seems to be possible with this concept. While some of the reviewed work only describe use cases and give general recommendations on how to realize them, there are also a few papers that discuss details regarding the implementation or even provide a proof of concept (Eckhart & Ekelhart 2018*c*,*b*, Bitton et al. 2018, Damjanovic-Behrendt 2018*b*).

Despite the fact that the chapter at hand reveals the state of the art of present approaches related to digital twins and CPS security, our work is limited in the following ways: First, we analyzed only papers that discuss the digital-twin concept in the context of information security. There may also be other existing works, which do not explicitly mention digital twins per se but still propose to use virtual models or simulations in a way that would have a positive effect on the security of CPSs. Second, our analysis lacks consideration of what the commercial market currently has to offer. Companies may already provide digital-twin solutions adaptable or extensible for realizing some of the use cases discussed in Section 3.2.

Nevertheless, we believe our work could be the basis for ongoing research, as the presented findings enhance our understanding of the term *digital twin* and envision what role the concept can take on when securing CPSs. In the future, more research is definitely required to investigate the practicality of the concept for security-enhancing use cases.

Acknowledgements The financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development, and COMET K1, FFG - Austrian Research Promotion Agency is gratefully acknowledged. Furthermore, this work was supported by the Austrian Science Fund (FWF) and netidee SCIENCE under grant P30437-N31.

References

Alam, K. M. & Saddik, A. E. (2017), 'C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems', *IEEE Access* **5**, 2050–2062.

Antonioli, D., Agrawal, A. & Tippenhauer, N. O. (2016), Towards high-interaction virtual ics honeypots-in-a-box, *in* 'Proceedings of the 2Nd ACM Workshop on Cyber-Physical Systems Security and Privacy', CPS-SPC '16, ACM, New York, NY, USA, pp. 13–22.

Baheti, R. & Gill, H. (2011), 'Cyber-physical systems', *The impact of control technology* **12**, 161–166.

Bitton, R., Gluck, T., Stan, O., Inokuchi, M., Ohta, Y., Yamada, Y., Yagyu, T., Elovici, Y. & Shabtai, A. (2018), Deriving a cost-effective digital twin of an ics to facilitate security evaluation, *in* J. Lopez, J. Zhou & M. Soriano, eds, 'Computer Security', Springer International Publishing, Cham, pp. 533–554.

Boschert, S. & Rosen, R. (2016), *Digital Twin—The Simulation Aspect*, Springer International Publishing, Cham, pp. 59–74.

Bracho, A., Saygin, C., Wan, H., Lee, Y. & Zarreh, A. (2018), 'A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems', *Procedia Manufacturing* **26**, 1116 – 1127. 46th SME North American Manufacturing Research Conference, NAMRC 46, Texas, USA.

Bécue, A., Fourastier, Y., Praça, I., Savarit, A., Baron, C., Gradussofs, B., Pouille, E. & Thomas, C. (2018), Cyberfactory#1 — securing the industry 4.0 with cyber-ranges and digital twins, *in* '2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)', pp. 1–4.

Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y. & Sastry, S. (2011), Attacks against process control systems: Risk assessment, detection, and response, *in* 'Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security', ASIACCS '11, ACM, New York, NY, USA, pp. 355–366.

Caselli, M., Zambon, E., Amann, J., Sommer, R. & Kargl, F. (2016), *Specification Mining for Intrusion Detection in Networked Control Systems*, USENIX Association, pp. 791–806.

Chabukswar, R., Sinopoli, B., Karsai, G., Giani, A., Neema, H. & Davis, A. (2010), Simulation of network attacks on scada systems, *in* 'First Workshop on Secure Control Systems, Cyber Physical Systems Week 2010'.

Chen, R., Dave, K., McAvoy, T. J. & Luyben, M. (2003), 'A nonlinear dynamic model of a vinyl acetate process', *Industrial & Engineering Chemistry Research* **42**(20), 4478–4487.

Chromik, J., Remke, A. & Haverkort, B. (2016), *What's under the hood? Improving SCADA security with process awareness*, IEEE.

Cook, A., Smith, R., Maglaras, L. & Janicke, H. (2016), Measuring the risk of cyber attack in industrial control systems, *in* 'Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016', ICS-CSR '16, BCS Learning & Development Ltd., Swindon, UK, pp. 1–11.

Damjanovic-Behrendt, V. (2018*a*), 'A digital twin architecture for security, privacy and safety', *ERCIM News* **2018**(115).

Damjanovic-Behrendt, V. (2018*b*), A digital twin-based privacy enhancement mechanism for the automotive industry, *in* 'Proceedings of the 9th International Conference on Intelligent Systems: Theory, Research and Innovation in Applications'.

de Sá, A. O., d. C. Carmo, L. F. R. & Machado, R. C. S. (2017), 'Covert attacks in cyber-physical control systems', *IEEE Transactions on Industrial Informatics* **13**(4), 1641–1651.

Depamelaere, W., Lemaire, L., Vossaert, J. & Naessens, V. (2018), Cps security assessment using automatically generated attack trees, *in* 'Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018', British Computer Society (BCS).

Downs, J. & Vogel, E. (1993), 'A plant-wide industrial process control problem', *Computers & Chemical Engineering* **17**(3), 245 – 255. Industrial challenge problems in process control.

Dragos, Inc. (2018), Industrial control vulnerabilities: 2017 in review, techreport, Dragos, Inc.

Drath, R., Luder, A., Peschke, J. & Hundt, L. (2008), Automationml - the glue for seamless automation engineering, *in* '2008 IEEE International Conference on Emerging Technologies and Factory Automation', pp. 616–623.

Duggan, D., Berg, M., Dillinger, J. & Stamp, J. (2005), 'Penetration testing of industrial control systems', *Sandia National Laboratories* .

Durão, L. F. C. S., Haag, S., Anderl, R., Schützer, K. & Zancul, E. (2018), Digital twin requirements in the context of industry 4.0, *in* P. Chiabert, A. Bouras, F. Noël & J. Ríos, eds, 'Product Lifecycle Management to Support Industry 4.0', Springer International Publishing, Cham, pp. 204–214.

Eckhart, M. & Ekelhart, A. (2018*a*), 'Securing cyber-physical systems through digital twins', *ERCIM News* **2018**(115).

Eckhart, M. & Ekelhart, A. (2018*b*), A specification-based state replication approach for digital twins, *in* 'Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy', CPS-SPC '18, ACM, New York, NY, USA, pp. 36–47.

Eckhart, M. & Ekelhart, A. (2018*c*), Towards security-aware virtual environments for digital twins, *in* 'Proceedings of the 4th ACM Workshop on Cyber-Physical System Security', CPSS '18, ACM, New York, NY, USA, pp. 61–72.

European Parliament and the Council of the European Union (2016), 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG`. Accessed: 2019-02-11.

Fan, W., Du, Z. & Fernández, D. (2015), Taxonomy of honeynet solutions, *in* '2015 SAI Intelligent Systems Conference (IntelliSys)', pp. 1002–1009.

Fichtner, H.-P. & Krammel, M. (2015), Project HoneyTrain, techreport, Koramis GmbH.

Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N. O., Sandberg, H. & Candell, R. (2018), 'A survey of physics-based attack detection in cyber-physical systems', *ACM Comput. Surv.* **51**(4), 76:1–76:36.

Glaessgen, E. H. & Stargel, D. (2012), The digital twin paradigm for future nasa and u.s. air force vehicles, *in* '53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference', pp. 1–14.

Glavach, D., LaSalle-DeSantis, J. & Zimmerman, S. (2017), *Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems*, Springer International Publishing, Cham, pp. 173–194.

Gockel, B., Tudor, A., Brandyberry, M., Penmetsa, R. & Tuegel, E. (2012), Challenges with structural life forecasting using realistic mission profiles, *in* '53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference', American Institute of Aeronautics and Astronautics.

Grieves, M. & Vickers, J. (2017), *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*, Springer International Publishing, Cham, pp. 85–113.

Grinshpun, G., Cichon, T., Dipika, D. & Rossmann, J. (2016), From virtual testbeds to real lightweight robots: Development and deployment of control algorithms for soft robots, with particular reference to, *in* 'Proceedings of ISR 2016: 47st International Symposium on Robotics', pp. 1–7.

Guarnizo, J. D., Tambe, A., Bhunia, S. S., Ochoa, M., Tippenhauer, N. O., Shabtai, A. & Elovici, Y. (2017), Siphon: Towards scalable high-interaction physical honeypots, *in* 'Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security', CPSS '17, ACM, New York, NY, USA, pp. 57–68.

Haag, S. & Anderl, R. (2018), 'Digital twin – proof of concept', *Manufacturing Letters* **15**, 64 – 66. Industry 4.0 and Smart Manufacturing.

Hahn, A. (2016), *Operational Technology and Information Technology in Industrial Control Systems*, Springer International Publishing, Cham, pp. 51–68.

Hribernik, K. A., Rabe, L., Thoben, K. & Schumacher, J. (2006), 'The product avatar as a product-instance-centric information management concept', *International Journal of Product Lifecycle Management* **1**(4), 367–379.

Hribernik, K., Wuest, T. & Thoben, K.-D. (2013), Towards Product Avatars Representing Middle-of-Life Information for Improving Design, Development and Manufacturing Processes, *in* G. L. Kovács & D. Kochan, eds, '6th Programming Languages for Manufacturing (PROLAMAT)', Vol. AICT-411 of *Digital Product and Process Development Systems*, Springer, Dresden, Germany, pp. 85–96. Part 2: Digital Product- and Process- Development.

ICS-CERT (2013), Year in review 2012, Technical report, Department of Homeland Security.

ICS-CERT (2015), Year in review 2014, Technical report, Department of Homeland Security.

ICS-CERT (2017), Year in review 2016, Technical report, Department of Homeland Security.

IEC (2009), '62443: Industrial communication networks – network and system security', *International Standard, First Edition, International Electrotechnical Commission, Geneva* **1**.

Jaensch, F., Csiszar, A., Scheifele, C. & Verl, A. (2018), Digital twins of manufacturing systems as a base for machine learning, *in* '2018 25th International Conference on Mechatronics and Machine Vision in Practice (M2VIP)', pp. 1–6.

Kagermann, H., Helbig, J., Hellinger, A. & Wahlster, W. (2013), Recommendations for implementing the strategic initiative industrie 4.0 – securing the future of german manufacturing industry, Final report of the industrie 4.0 working group, acatech – National Academy of Science and Engineering, München.

Kissel, R. L., Regenscheid, A. R., Scholl, M. A. & Stine, K. M. (2014), 'Guidelines for media sanitization', *NIST special publication* **800**(88r1).

Knapp, E. D. & Langill, J. T. (2014), *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*, Syngress.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. & Jones, K. (2015), 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection* **9**, 52 – 80.

Kritzinger, W., Karner, M., Traar, G., Henjes, J. & Sihn, W. (2018), 'Digital twin in manufacturing: A categorical literature review and classification', *IFAC-PapersOnLine* **51**(11), 1016 – 1022. 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.

Krotofil, M. & Cárdenas, A. A. (2013), Resilience of process control systems to cyber-physical attacks, *in* H. Riis Nielson & D. Gollmann, eds, 'Secure IT Systems', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 166–182.

Krotofil, M., Isakov, A., Winnicki, A., Gollmann, D., Larsen, J. & Gurikov, P. (2015), Rocking the pocket book: Hacking chemical plants for competition and extortion, resreport, Black Hat.

Langner, R. (2013), 'To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve'.

Lantz, B., Heller, B. & McKeown, N. (2010), A network in a laptop: Rapid prototyping for software-defined networks, *in* 'Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks', Hotnets-IX, ACM, New York, NY, USA, pp. 19:1–19:6.

Lee, J., Lapira, E., Bagheri, B. & an Kao, H. (2013), 'Recent advances and trends in predictive manufacturing systems in big data environment', *Manufacturing Letters* **1**(1), 38 – 41.

Lee, R. M., Assante, M. J. & Conway, T. (2016), Analysis of the cyber attack on the ukrainian power grid, techreport, SANS Institute.

Lemaire, L., Vossaert, J., Jansen, J. & Naessens, V. (2017), 'A logic-based framework for the security analysis of industrial control systems', *Automatic Control and Computer Sciences* **51**(2), 114–123.

Lubell, J., Frechette, S. P., Lipman, R. R., Proctor, F. M., Horst, J. A., Carlisle, M. & Huang, P. J. (2013), Model based enterprise summit report, Technical Report 1820, National Institute of Standards and Technology.

Lüder, A., Schmidt, N., Hell, K., Röpke, H. & Zawisza, J. (2017), *Fundamentals of Artifact Reuse in CPPS*, Springer International Publishing, Cham, pp. 113–138.

Macaulay, T. & Singer, B. (2016), *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*, CRC Press.

Maybury, M. T. (2013), Global horizons: Final report, resreport AF/ST TR 13-01; Air Force/Small Business Technology Transer 13-01, United States Air Force.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M. & Karri, R. (2016), 'The cybersecurity landscape in industrial control systems', *Proceedings of the IEEE* **104**(5), 1039–1057.

Mitchell, R. & Chen, I.-R. (2014), 'A survey of intrusion detection techniques for cyber-physical systems', *ACM Comput. Surv.* **46**(4), 55:1–55:29.

Mourtzis, D., Doukas, M. & Bernidaki, D. (2014), 'Simulation in manufacturing: Review and challenges', *Procedia CIRP* **25**, 213 – 229. 8th International Conference on Digital Enterprise Technology - DET 2014 Disruptive Innovation in Manufacturing Engineering towards the 4th Industrial Revolution.

Negahban, A. & Smith, J. S. (2014), 'Simulation for manufacturing system design and operation: Literature review and analysis', *Journal of Manufacturing Systems* **33**(2), 241 – 261.

Negri, E., Fumagalli, L. & Macchi, M. (2017), 'A review of the roles of digital twin in cps-based production systems', *Procedia Manufacturing* **11**, 939 – 948. 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy.

Nivethan, J. & Papa, M. (2016), A scada intrusion detection framework that incorporates process semantics, *in* 'Proceedings of the 11th Annual Cyber and Information Security Research Conference', CISRC '16, ACM, New York, NY, USA, pp. 6:1–6:5.

Panetta, K. (2018), 'Gartner top 10 strategic technology trends for 2019', `https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/`. Accessed: 12-12-2018.

Plumley, E., Rice, M., Dunlap, S. & Pecarina, J. (2017), Categorization of cyber training environments for industrial control systems, *in* M. Rice & S. Shenoi, eds, 'Critical Infrastructure Protection XI', Springer International Publishing, Cham, pp. 243–271.

Polenghi, A., Fumagalli, L. & Roda, I. (2018), 'Role of simulation in industrial engineering: focus on manufacturing systems', *IFAC-PapersOnLine* **51**(11), 496 – 501. 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.

Rajkumar, R., Lee, I., Sha, L. & Stankovic, J. (2010), Cyber-physical systems: The next computing revolution, *in* 'Design Automation Conference', pp. 731–736.

Reifsnider, K. & Majumdar, P. (2013), Multiphysics stimulated simulation digital twin methods for fleet management, *in* '54th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference', American Institute of Aeronautics and Astronautics.

Ríos, J., Hernández, J. C., Oliva, M. & Mas, F. (2015), Product avatar as digital counterpart of a physical individual product: Literature review and implications in an aircraft., *in* 'ISPE CE', pp. 657–666.

Rist, L., Vestergaard, J., Haslinger, D., Pasquale, A. & Smith, J. (n.d.), 'Conpot ICS/SCADA Honeypot', `http://conpot.org/`. Accessed: 2019-02-11.

Rosen, R., von Wichert, G., Lo, G. & Bettenhausen, K. D. (2015), 'About the importance of autonomy and digital twins for the future of manufacturing', *IFAC-PapersOnLine* **48**(3), 567 – 572. 15th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2015.

Rubio, J. E., Alcaraz, C., Roman, R. & Lopez, J. (2017), Analysis of intrusion detection systems in industrial ecosystems, *in* '14th International Conference on Security and Cryptography (SECRYPT 2017)'.

Schleich, B., Anwer, N., Mathieu, L. & Wartzack, S. (2017), 'Shaping the digital twin for design and production engineering', *CIRP Annals* **66**(1), 141 – 144.

Schluse, M. & Rossmann, J. (2016), From simulation to experimentable digital twins: Simulation-based development and operation of complex technical systems, *in* '2016 IEEE International Symposium on Systems Engineering (ISSE)', pp. 1–6.

Schroeder, G. N., Steinmetz, C., Pereira, C. E. & Espindola, D. B. (2016), 'Digital twin data modeling with automationml and a communication methodology for data exchange', *IFAC-PapersOnLine* **49**(30), 12 – 17. 4th IFAC Symposium on Telematics Applications TA 2016.

Schroeder, G., Steinmetz, C., Pereira, C. E., Muller, I., Garcia, N., Espindola, D. & Rodrigues, R. (2016), Visualising the digital twin using web services and augmented reality, *in* '2016 IEEE 14th International Conference on Industrial Informatics (INDIN)', pp. 522–527.

Shafto, M., Conroy, M., Doyle, R., Glaessgen, E., Kemp, C., LeMoigne, J. & Wang, L. (2010), 'Draft modeling, simulation, information technology & processing roadmap', *Technology Area* **11**.

Shi, J., Wan, J., Yan, H. & Suo, H. (2011), A survey of cyber-physical systems, *in* '2011 International Conference on Wireless Communications and Signal Processing (WCSP)', pp. 1–6.

Singh, V. & Willcox, K. E. (2018), 'Engineering design with digital thread', *AIAA Journal* **56**(11), 4515–4528.

Smith, R. S. (2015), 'Covert misappropriation of networked control systems: Presenting a feedback structure', *IEEE Control Systems Magazine* **35**(1), 82–92.

Sommestad, T. & Hallberg, J. (2012), Cyber security exercises and competitions as a platform for cyber security experiments, *in* A. Jøsang & B. Carlsson, eds, 'Secure IT Systems', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 47–60.

Spitzner, L. (2002), *Honeypots: Tracking Hackers*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.

Tauber, M. & Schmittner, C. (2018), 'Enabling security and safety evaluation in industry 4.0 use cases with digital twins', *ERCIM News* **2018**(115).

Tuegel, E. J., Ingraffea, A. R., Eason, T. G. & Spottswood, S. M. (2011), 'Reengineering aircraft structural life prediction using a digital twin', *International Journal of Aerospace Engineering* **2011**.

Uhlemann, T. H.-J., Lehmann, C. & Steinhilper, R. (2017), 'The digital twin: Realizing the cyber-physical production system for industry 4.0', *Procedia CIRP* **61**(Supplement C), 335 – 340. The 24th CIRP Conference on Life Cycle Engineering.

Vachálek, J., Bartalskỳ, L., Rovnỳ, O., Šišmišová, D., Morháč, M. & Lokšík, M. (2017), The digital twin of an industrial production line within the industry 4.0 concept, *in* '2017 21st International Conference on Process Control (PC)', pp. 258–262.

Vasilomanolakis, E., Srinivasa, S., Cordero, C. G. & Mühlhäuser, M. (2016), Multi-stage attack detection and signature generation with ics honeypots, *in* 'NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium', pp. 1227–1232.

Wei, D. & Ji, K. (2010), Resilient industrial control system (rics): Concepts, formulation, metrics, and insights, *in* '2010 3rd International Symposium on Resilient Control Systems', pp. 15–22.

West, T. D. & Blackburn, M. (2017), 'Is digital thread/digital twin affordable? a systemic assessment of the cost of dod's latest manhattan project', *Procedia Computer Science* **114**, 47 – 56. Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS October 30 – November 1, 2017, Chicago, Illinois, USA.

West, T. D. & Pyster, A. (2015), 'Untangling the digital thread: The challenge and promise of model-based engineering in defense acquisition', *INSIGHT* **18**(2), 45–55.

Zhao, C. & Qin, S. (2017), A research for high interactive honepot based on industrial service, *in* '2017 3rd IEEE International Conference on Computer and Communications (ICCC)', pp. 2935–2939.