Digital Twins in Security Operations: State of the Art and Future Perspectives

PHILIP EMPL, Chair of Information Systems, University of Regensburg, Regensburg, Germany
DAVID KOCH, Department of Privacy and Compliance, University of the Bundeswehr Munich, München, Germany
MARIETHERES DIETZ, Chair of Information Systems, University of Regensburg, Regensburg, Germany
GÜNTHER PERNUL, Chair of Information Systems, University of Regensburg, Regensburg, Germany

In an era of rapid technological advancements, digital twins are gaining attention in industry and research. These virtual representations of real-world entities, enabled by the Internet of Things (IoT), offer advanced simulation and analysis capabilities. Their application spans various sectors, from smart manufacturing to healthcare, highlighting their versatility. However, the rise of digital technologies has also escalated cybersecurity concerns. Historical cyberattacks underscore the urgency for enhanced security operations. In this context, digital twins represent a novel approach to cybersecurity. Industry and academic research are increasingly exploring their potential to protect their assets. Despite growing interest and applications, more comprehensive research synthesis needs to be done, particularly in security operations based on digital twins. Our article aims to fill this gap through a structured literature review aggregating knowledge from 201 publications. We focus on defining the digital twin in cybersecurity, exploring its applications, and outlining implementations and challenges. To maintain transparency, our data is documented and is publicly available. This survey serves as a crucial guide for academic and industry stakeholders, fostering digital twins in security operations.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Networks** → **Cyber-physical networks**; • **Information systems**; • **Computer systems organization** → **Embedded and cyber-physical systems**; • **Security and privacy**;

Additional Key Words and Phrases: Digital twin, security operations, cybersecurity, survey, literature review

ACM Reference Format:
Philip Empl, David Koch, Marietheres Dietz, and Günther Pernul. 2025. Digital Twins in Security Operations: State of the Art and Future Perspectives. *ACM Comput. Surv.* 58, 1, Article 18 (September 2025), 38 pages. https://doi.org/10.1145/3746279

Authors' Contact Information: Philip Empl, Chair of Information Systems, University of Regensburg, Regensburg, Germany; e-mail: philip.empl@ur.de; David Koch, Department of Privacy and Compliance, University of the Bundeswehr Munich, München, Germany; e-mail: david.koch@unibw.de; Marietheres Dietz, Chair of Information Systems, University of Regensburg, Regensburg, Germany; e-mail: marietheres.dietz@ur.de; Günther Pernul, Chair of Information Systems, University of Regensburg, Regensburg, Germany; e-mail: guenther.pernul@ur.de.

ACM 0360-0300/2025/09-ART18
https://doi.org/10.1145/3746279

1 Introduction

Offering opportunities like no technology before, digital twins are gaining significant attention in industry and science alike. Digital twins virtually represent real-world objects (e.g., products, systems, or even processes) and are thus able to forecast and simulate potential future happenings as well as to replicate current ones. Thereby, a digital twin bases its computations on data from the real-world object, adds context by semantically linking data, and produces results tailored to the asset in question. The extent of these results matches no current alternative regarding in-depth analysis of the investigated object and offers high degrees of individualization. While the notion of digital twins has been floating around for years, they only became realizable with the widespread adoption of the **Internet of Things** (**IoT**).

Thanks to these powerful features, the application scenarios of digital twins are manifold. For instance, the engineering company Bosch is instrumenting the digital twin mainly in the sphere of the Industrial IoT to envision a smart factory [93]: They begin with collecting raw data of their products, add semantics to generate contextual information and provide a digital representation of the individual product. On the other hand, Siemens is computing digital twins of patients' hearts to comprehend the divergent reactions to medicine [112] or, in times of SARS-CoV-2, to vaccines. On a greater level, the European Union is planning the *Destination Earth* initiative, which focuses on creating a digital twin of the whole world to estimate probabilities and impacts of future scenarios, such as in climate change. While the world is enhanced with digitization, crime is, too. Cybersecurity is turning into a major concern for companies these days. In the last decades, several cyberattacks (see Figure 1) greatly impacted the world, including:

- Ransomware attacks (e.g., *NotPetya* in 2017 [6], Fresenius in 2020 [225], and the Colonial Pipeline [84] in 2021)
- Malware attacks (e.g., Kudankulam power plant in 2019 [55])
- Worms (e.g., *Stuxnet* attack in 2010 [6])
- Exploits of unpatched vulnerabilities (e.g., the cyberattack at Kemuri water treatment plant in 2015 [6])
- Botnets (e.g., *Mirai* in 2016, exploiting IoT devices using default credentials for DDoS attacks [11])

One of the latest events highlights that more significant efforts to enhance cybersecurity are required. In 2023, the *Vulkan files* were published. These files implicate the Russian government of actively developing frameworks (e.g., *Amezit* until 2018 and *Krystal-2B* until 2020) to attack industrial systems. Figure 1 illustrates critical cybersecurity incidents while also informing on milestones of digital twins in research. Thereto, it adapts the Gartner hype cycle to show the (estimated) progression of the digital twin concept from 2017 to 2024. It also provides advances in practice concerning using digital twins for security. For instance, General Electric employs digital twins of machines to identify anomalies in their behavior. Their so-called "digital ghost" maintains cybersecurity via detection, localization, prediction, and even neutralization of harmful activities [90]. Meanwhile, Siemens also starts exploiting the potential of digital twins for detecting cyberattacks [70]. Others follow their lead (e.g., [125, 130, 158]).

Likewise, academic research increasingly focuses on the digital twin's potential for cybersecurity. Dietz & Pernul [61] describe the possibilities of a digital twin to enhance cybersecurity in industrial systems, identifying three modes of operation: simulation, replication, and analytics. Eckhart et al. [69] developed a prototypical digital twin to allow assumptions about the security state of industrial systems. Olivares-Rojas et al. [171] used the digital twin technology to test cybersecurity attacks on smart meters, while the real-world smart meters remain unaffected. Many more security-related digital twin applications have been introduced in research. However, they rarely rely on one another.

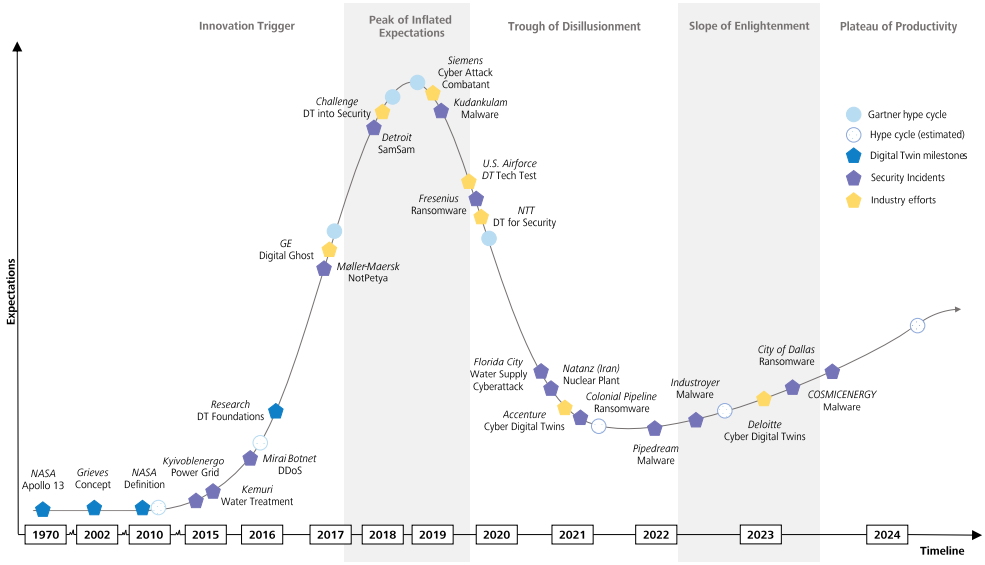


Fig. 1. Chronological development of digital twin (in security operations) research and industry efforts.

This is why providing an overview of the existing body of knowledge concerning enhancing security through digital twins is vital. Over the last years, there have been some surveys on digital twins in general (e.g., Ref. [168]). However, those literature reviews commonly do not consider the security perspective—despite its apparent adoption in science and practice. Thus, one of the scientific challenges remains to provide a comprehensible overview of how digital twins can be used for security. Our structured literature review will close this gap and follows the principles of open data[1].

1.1 Research Questions and Contribution

Regarding the current development of the digital twin turning into a cybersecurity tool, it is vital to classify and present the state-of-the-art. Such a survey allows us to study existing works and expand the body of knowledge by building on the already published research. Doing so, we investigate and aggregate 201 research paper. Next, to provide an overview of existing literature, the need for further research will be identified, showing the opportunities and diversity of the digital twin in cybersecurity. This survey not only endeavors to summarize previous research findings but also maps the landscape of digital twins for security operations following the NIST **Cybersecurity Framework (CSF)** [20]. Therefore, we focus on a dynamic and critical convergence point—where technology, cybersecurity, and industrial requirements intersect. The following *research questions* help to determine the status quo of digital twins for security operations:

- **RQ1** What constitutes a digital twin within the realm of cybersecurity?
- **RQ2** How is the digital twin harnessed to fortify cybersecurity?
- **RQ3** How can digital twin components be instantiated?
- **RQ4** What pivotal challenges remain unaddressed, and what promising avenues beckon for future research?

To answer **RQ1**, we will study the digital twin's components and how researchers understand the paradigm. Subsequently, exploring the applications of using the digital twin in security operations

[1] https://github.com/philipempl/DT4Sec

will respond to **RQ2**. This includes the benefits of using digital twins for cybersecurity. The answer to **RQ3** will include how digital twin components are set up, what data the digital twin consumes, and which tools and communication protocols are used. Finally, we will answer **RQ4** by extracting the authors' views from their publications to synthesize in which direction the digital twin in security operations needs to be explored as well as how to overcome challenges for designing and implementing digital twins in cybersecurity settings. In a nutshell, the *contribution* of this article is as follows:

(1) It confirms the components of the digital twin from a cybersecurity perspective,
(2) re-defines the paradigm digital twin in cybersecurity,
(3) describes the application domains and security operations based on digital twins,
(4) provides an overview of implementation techniques and tools,
(5) shapes future research directions and open issues.

1.2 Remainder

The remainder of this work is organized as follows. Section 2 will explore the theoretical background to fill in readers on the digital twin paradigm and to describe related work by other authors. The methodology of this survey is detailed in Section 3. Section 4 approaches the digital twin paradigm and essential components. Section 5 describes the application benefits, domains, and security operations. Section 6 highlights how implementing the digital twin components can be managed, and Section 7 pictures open issues and future research. In Section 8, we will conclude our article.

2 Background and Related Work

2.1 Digital Twin

Although the digital twin seems like a newly emerged concept, the notion of it has been around for quite some time. Historically, engineers and researchers relied on simulations, emulations, and physical testbeds to understand, evaluate, and optimize systems. Simulations offered reproducible experiments using abstract models, emulations allowed testing with real code in controlled environments, and testbeds provided high realism by deploying actual or virtualized hardware. However, these approaches typically focused on isolated scenarios and lacked continuous integration with real-world systems [50, 94]. The concept of the digital twin marks a significant shift in this trajectory. Unlike classical simulations or testbeds, digital twins introduce a persistent, bidirectional connection with their physical counterparts, enabling real-time synchronization, monitoring, and even control [5]. For instance, when Apollo 13 suffered an explosion inside its oxygen tanks in outer space in 1970, NASA modified the conditions of their simulators to match the specifications of Apollo 13 and identified strategies to solve this hazardous situation [21]. NASA first created something resembling an early-stage digital twin by customizing its generic simulator to an individual counterpart. Around 2012, NASA and the U.S. Air Force applied digital twins further to examine the life cycle of their physical assets and to diagnose as well as predict an asset's particular behavior [91]. Nowadays, digital twins go beyond mere simulations [98]. In science as well as in practice, the digital twin only gained a foothold with the maturity and deployment of the IoT: Data generated thanks to the IoT enable on-building statistics, artificial intelligence, machine learning, and data visualizations [83, 214]. So, only with the technology of the IoT have organizations been able to provide the twins with enough crucial data quickly. Essential data is usually stored and enriched with semantics to provide context [233]. On this basis, the digital twin can virtually represent its real-world counterpart, e.g., by using the data to create a digital model or simulation [189]. Digital twins can be classified into different types such as component twins, system twins, or process twins [98]. They also support the full lifecycle of a product, from design and development

Table 1. Comparison of Our Survey to Existing Surveys in Terms of the Content and Scope

Aspects	[26]	[67]	[179]	[216]	[228]
Methodology	*SLR*	*n/s*	*MLR*	*SLR*	*n/s*
Publication year	*2021*	*2019*	*2020*	*2023*	*2023*
Security perspective	Augmented Reality (technology-res.)	Industry (app-res.)	Intrusion detection (ops-res.)	Ind. intr. det. (app-&ops-res.)	IoT (app.-res.)
Studies considered/included	355/33	n.a./n.a.	751/17	158/10	n.a./n.a.
Applications	●	◑	◑	◑	●
Implementation	◑	○	○	○	◑
Challenges/ future research	○	●	◑	○	●

○ = not covered; ◑ = partially covered; ● = covered; app = application; ops =operations; res = restricted; n/s = not specified; n.a. = not available.

to decommissioning [204]. Also, current advances in digital twin technology attempt to create a bidirectional connection between the twin and its counterpart [129]. This enables the digital twin not only to monitor but also to control its counterpart. Nevertheless, there are open challenges, e.g., data quality, security, interoperability, and scalability [166].

2.2 Related Work

In recent years, numerous surveys have explored digital twins, often without considering cybersecurity aspects (e.g., Refs. [21, 120, 129, 141, 143, 168, 226, 231]). When it comes to cybersecurity, existing reviews primarily focus on securing digital twins themselves, as they frequently process sensitive data. Consequently, much of the research has centered on enabling cybersecurity for digital twins—for instance, by integrating digital twins with distributed ledger technologies[117, 181, 239]. However, only five surveys investigate the use of digital twins to enhance cybersecurity through security operations. Table 1 provides a comparative overview of those surveys that align closely with the scope of our work. First, Böhm et al. [26] systematically deal with combining digital twins and **Augmented Reality** (**AR**) by taking a cybersecurity perspective. Second, Eckhart et al. [67] systematized the body of knowledge in an unstructured way and identified several security operations of the digital twin for cybersecurity in 2019. Third, Pokhrel et al. [179] conducted a **Multi-vocal Literature Review** (**MLR**) on the application of the digital twin for incident prediction. Fourth, Thalpage and Nisansala [216] systematically analyzed the usage of digital twins for industrial intrusion detection. Last, Wang et al. [228] do not apply a structured method when focusing on digital twins and security for IoT.

The most remarkable difference of related surveys to our survey lies in the specialization of these. For example, some authors [67, 216, 228] focus on one specific application domain. Pokhrel et al. [179] as well as Thalpage and Nisansala [216] only target one specific security operation (intrusion detection), while Böhm et al. [26] review a given set of core technologies (e.g., AR). Our survey is intended to be all-encompassing and to combine all perspectives of previously written overviews. Moreover, we base our literature review on a profound methodology to gather the results in a structured way, fostering comprehensibility and transparency. It is also important to note that the research of digital twins in security operations only started around 2018, turning our literature review into a 7-year summary including more than 200 relevant articles on this issue in contrast to earlier reviews, where the maximum of relevant articles is 33 (see Table 1). Surely, there are still other works do provide an overview on digital twin security [68, 77, 121, 209, 212]. However, none of these works provided a method. Also, those works only cover a very specific part of the literature, offering little basis for comparison. In contrast, the two studies without a method [67, 228] reference a multitude of research to provide very comprehensive overviews. In summary, our article takes a comprehensive and methodological approach to investigate digital twins in

Table 2. Databases and Initial Search Results

Database Name	URL	Results
ACM	dl.acm.org	565
AISeL	aisel.aisnet.org	163
Arxiv	arxiv.org	77
dblp	dblp.org	64
IEEE CS	computer.org	504
IEEE Xplore	ieeexplore.ieee.org	1,075
Science Direct	sciencedirect.com	954
Springer Link	link.springer.com	1,631
Wiley	wiley.com	209
WoS	webofscience.com	318
Total		**5,560**

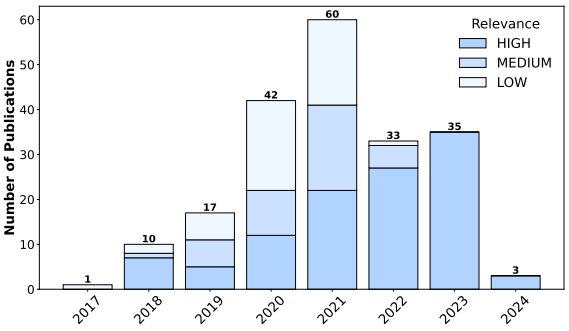


Fig. 2. Selected digital twin papers by year and relevance (*Total: 201*).

security operations by filling a significant gap through a wide-ranging synthesis, in contrast to previous work that are either outdated, lack methodological rigor, or focus only on specific topics.

3 Methodology

Our survey strictly adheres to the methodology of a qualitative systematic review, a widely recognized approach in information systems research [173]. We adopt the guidelines by Schryen [197], which structure our review into four key phases: framing, searching, screening, and synthesis. This approach ensures a comprehensive and well-organized examination of our subject matter. For an in-depth understanding of our methodology and the specific outcomes, more details can be found in our GitHub repository[2].

Search and Assessment. Our literature search process begins with queries in ten different scientific databases: ACM, AISeL, arXiv, dblp, IEEE CSDL, IEEE Xplore, ScienceDirect, SpringerLink, Wiley Online, and WoS (see Table 2). We also conduct backward searches by automatically parsing PDFs and forward searches using Google Scholar to enhance our search (> 3,000 results). It is worth noting that the search term *digital twins AND security* produces an exceptionally large number of results in a three databases where searches cannot be constricted to data fields. To manage this, we refine our search results by including additional keywords[3]. Our literature review process is started by cleaning the corpus to eliminate duplicate entries. Then, we assess each publication's relevance by considering the title (*screen 1*) and afterward the full-text (*screen 2*), where we apply specific inclusion and exclusion criteria established in advance. These criteria involve evaluating the publication's quality, language (English), relevance to digital twins, and cybersecurity topics. If a publication does not meet these criteria, it is excluded immediately. Through this rigorous process, we could identify a total of 201 publications that align with the scope of our survey, which is illustrated in Figure 2. We classified the relevance of the papers into three categories: high, medium, and low. Papers classified as high relevance (111) focused entirely on the use of digital twins for security operations—the topic formed the core of the article. Papers marked as medium relevance (41) addressed the topic in part, typically dedicating one or more sections or paragraphs to it. Finally, papers with low relevance (49) only mentioned digital twins for security operations in passing—often limited to a single sentence or brief reference. Moreover, this figure indicates a noticeable increase in highly relevant academic research on digital twins in security operations. Please note that our search only covers January 2024.

[2] https://github.com/philipempl/DT4SEC

[3] *digital twin* ***AND*** *("internet of things"* ***OR*** *"IoT"* ***OR*** *"CPS"* ***OR*** *"cyber-physical systems"* ***OR*** *"cyber physical systems")* ***AND*** *("cybersecurity"* ***OR*** *"cyber-security"* ***OR*** *"information security")*

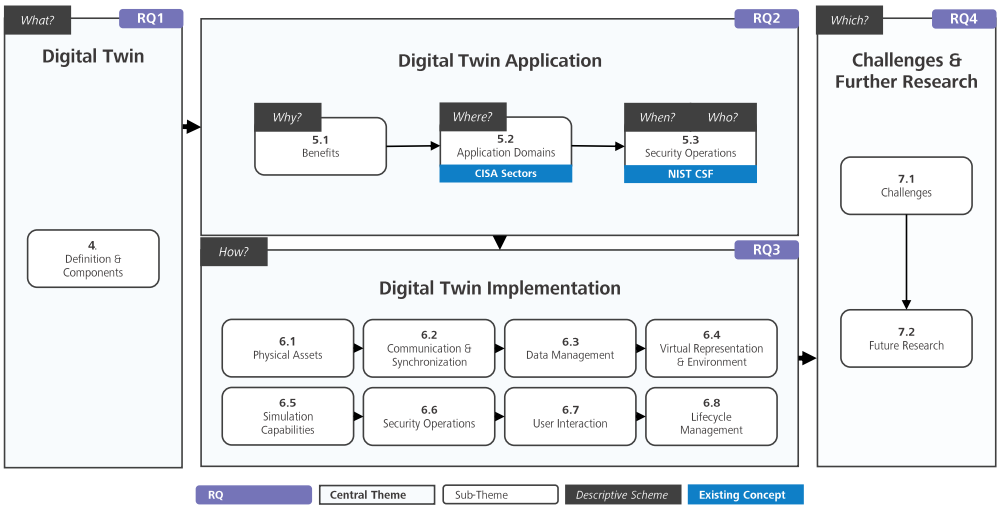


Fig. 3. Thematic classification of the survey's topic.

Extraction and Synthesis. In this phase, we focus on extracting and organizing the required data. This part is crucial because it supports answering our research questions. To enable data extraction, we create a structured template applied to each relevant research paper. This template contains 18 fields and ensures consistent handling of each paper. In addition to the data related to our research questions, we gathered bibliographic information like author names, publication years, and titles. We have created an additional template for the NIST CSF mapping. Before applying the extraction template to all the papers, it is tested on a small sample to ensure it works effectively. Once this step is completed, the data is synthesized using the thematic analysis method [49]. Thematic analysis helps identify common patterns in the data and group them into specific themes (see Figure 3). We first define central themes for each research question in this thematic analysis process. Afterward, sub-themes are linked to corresponding central themes. These central themes act as summaries for the sub-themes. Our approach to defining these themes combines inductive and deductive methods. While the sub-themes *Application Domains* and *Security Operations* are derived deductively, drawing from the NIST CSF and the critical infrastructure classification established by the **Cybersecurity and Infrastructure Security Agency** (**CISA**), the remaining sub-themes are generated inductively from our extracted data. We map the CSF functions to the publications based on the digital twins' characteristics and proposed use cases. This mapping is also open-source and available at Github. Our objective is to gain a comprehensive understanding of the digital twin paradigm in the context of cybersecurity (*what is a digital twin?*), with details about its applications (*why/where/when to use a digital twin?*, or *who applies a digital twin?*), implementations (*how to use a digital twin?*) and future research (*which open challenges and future research exist?*). Please note that we extract data from publications of all relevancy levels to address conceptual schemes. However, for the analysis of security operations aligned with the NIST CSF, we focus on papers classified as highly relevant. These papers are selected because they provide detailed insights. In the following sections (Sections 4–7), we delve into each of these central themes and their corresponding sub-themes.

4 Approaching the Digital Twin Paradigm

In this section, we delve into the paradigm of the digital twin. We face different perceptions of a digital twin ranging from *middleware* [75] to *holistic simulation* [66] and *virtual replica* [87].

Table 3. Functional Components of a Digital Twin Derived from Academic Definitions

Component	References
Virtual Representation	[2, 3, 8, 12, 14, 18, 23, 30, 36, 41, 47, 52, 56–58, 65, 67, 68, 73, 75, 76, 79, 80, 85, 87–89, 96, 104, 106, 108, 122, 126–128, 138, 140, 142, 146, 149, 153, 155, 156, 159, 160, 165, 167, 170, 176–178, 184, 185, 190–193, 195, 196, 199, 200, 205, 209, 211, 212, 216–222, 229, 235–238, 241, 242]
Data Management	[4, 8, 16, 18, 22, 47, 52, 67, 68, 140, 170, 211, 216]
User Interaction	[18, 27, 47, 68, 73, 76, 80, 86, 118, 140, 170, 171, 176, 220, 237, 242]
Simulation Capabilities	[13, 16, 23, 25, 33, 37, 48, 52, 53, 56, 61, 63, 66, 68, 69, 72, 73, 78, 81, 88, 96, 100, 101, 106, 111, 116, 118, 123, 127, 133, 136, 137, 145, 153, 157, 172, 196, 199, 200, 205, 206, 209, 212, 241, 242]
Lifecycle Management	[34, 52, 58–63, 67, 75, 100, 140, 157, 170, 176, 219, 242]
Communication & Synchronization	[1, 2, 4, 12, 25, 29, 30, 60, 64, 66, 75, 79, 100, 101, 108, 108, 111, 118, 118, 123, 131, 137, 144, 146–148, 157, 164, 170, 183, 208, 209, 218, 222]
Security Operations	[9, 10, 13, 23, 48, 62, 64, 67, 72, 78, 170, 177, 206, 212]

Additionally, there are differing viewpoints on what should be considered an integral part of the digital twin and what should be seen as external but still utilized by the digital twin. For instance, while data storage could externally provide data to a digital twin [28], it could also be a vital functional component [63, 123, 169] holding machine learning models [29, 42, 53, 235, 238]. We illustrate the digital twin by weaving together the functional components identified from academic literature (see Table 3). Considering these components (see Figure 4), we can define the digital twin paradigm for security operations as follows:

What is a digital twin in the realm of cybersecurity?
A digital twin in the realm of cybersecurity is a dynamic *virtual representation* of an entity that seamlessly integrates *real-time and historical data*, covering the entire *lifecycle* of its counterpart. Thereby, it can *simulate* and replicate its behavior and states. A digital twin engages users in the *interactions* and *security operations*.

1. **Virtual Representation.** A digital twin is a virtual representation or replica of a real-world entity. The virtual representation is close to the replication mode of a digital twin [61], where the stimuli triggering states in the real-world counterpart are reproduced in the digital twin to mimic system states. The virtual representation encompasses either a structural (e.g., JSON [202] or RDF [42]), functional (e.g., AutomationML [34]), or behavioral (e.g., finite-state machine [65] or Kalman filter [1]) aspect of the entity or a combination thereof, to capture its nuances and intricacies. The representation's fidelity determines the accuracy of the security operation.
2. **Data Management.** Central to the digital twin concept is its ability to manage data. This starts with the collection of data, where different types might be required (e.g., device [73] or network [63]). It also involves data transformation and its corresponding tools and methods (e.g., using Logstash as proposed by [222]). Dependent on the security operation, a digital twin can consume real-time (e.g., Ref. [136]) and historical data (like relational [134], document-oriented [224], graph-based [42], or distributed [178]) to provide a comprehensive data-backed view.
3. **User Interaction.** Digital twins should dynamically allow user interaction. This component can also be referred to as the analytics mode of a digital twin [61], where cybersecurity professionals can monitor and correlate variables making the virtual representation more

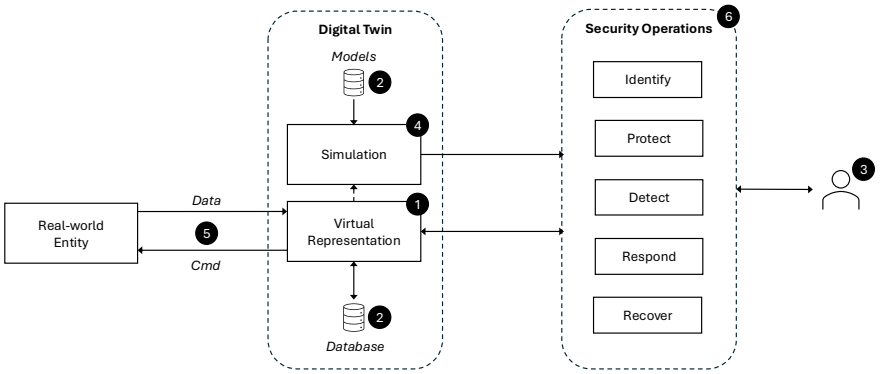


Fig. 4. Functional components of digital twins for security operations and their dependencies.

effective. In addition, cybersecurity novices can be introduced to the topic in a practical way [224]. Besides reporting (e.g., Kibana [63] or Prometheus [2]), cybersecurity professionals can interact with digital twins in different ways (like via virtual reality [137] or 3D models [242]).

4 **Simulation Capabilities.** Beyond being mere replicas, digital twins offer advanced simulation capabilities (*the process of generating data*). This is also named simulation mode [61]. Depending on the virtual representation, digital twins can simulate different scenarios and predict future states based on real-time and historical data. Digital twins are decoupled from the real-world entity and do not affect their physical counterparts [65]. Note that running a digital twin in the simulation mode requires behavioral models as virtual representations and appropriate software (e.g., MathWorks Simulink as shown by [108] or Cooja like in Ref. [123]).

5 **Communication and Synchronization.** The value of a digital twin is amplified by its connectivity. Seamless communication protocols ensure that there is a continuous flow of data between the digital twin and its physical counterpart (e.g., Ref. [14] focused on MQTT, Ref. [40] on Modbus, Ref. [230] on OPC UA). This connectivity is crucial for real-time monitoring, synchronization, and remote control. Regarding synchronization, a digital twin is characterized by bidirectional communication, where the entity and the digital twin share the same state.

6 **Security Operations.** Security operations, as outlined in the NIST CSF, refer to the structured processes and activities carried out by organizations or security teams to safeguard their assets, data, systems, and operations from various threats. Digital twins assist security operations given the framework's five phases:

— *Identifying* cybersecurity risks to establish a security baseline [64].
— *Protecting* assets through security measures, e.g., policies [48], access controls [35], and awareness [69].
— *Detecting* security incidents using monitoring, intrusion detection, and cyber threat intelligence [51].
— *Responding* to security incidents by defining and executing incident response processes [75].
— *Recovering* in the event of security incidents, emphasizing business continuity and resilience [2].

Considering these functional components, a digital twin in security operations is similar to one in the industrial context. The difference is that a digital twin in security operations addresses a different context, user group, and operations. We find different relevant data and different security operations. Regarding user groups, cybersecurity professionals are the main ones interacting with

the digital twin. In the next section, we detail these security operations where digital twins are currently used.

5 Understanding the Use of Digital Twins

In this section, we delve into why researchers increasingly turn to digital twins and examine the application domains where digital twins are applied. Additionally, we will explore where researchers actually use digital twins.

5.1 Benefits of Digital Twins

A digital twin encompasses a virtual representation at its core and enables in security operations. While digital twins alone cannot replace established tools like SIEM systems, they serve as a foundational technology that enhances and extends such use cases. In the following, we delve into the rationale behind researchers' choice of digital twins as the cornerstone of their security operations. Note that these benefits stem from the digital twins' components.

Asset Centrality. Security operations can significantly benefit from asset centrality, which is central to digital twins. Digital twins maintain a one-to-one relationship with their physical counterparts. They collect and manage vast amounts of historical and real-time data [87, 103, 143, 162, 167, 186, 192, 203] focused on their respective assets' states and history [60, 61, 146, 147]. Their strength lies in collecting and aggregating data even if distributed across various storage systems [118, 207]. To achieve this, digital twins extract data related to assets, such as firmware binaries [48, 81], and specifications [58]. Additionally, digital twins incorporate expert knowledge about the functions and behaviors of the assets they represent [82]. Digital twin models equip their counterparts with intelligence [180]. To ensure the security of the assets' data, digital twins manage access for their associated physical counterparts [31], typically through mechanisms like access control [147]. Beyond the physical counterpart, digital twins define sharing policies to regulate data access for relevant assets and stakeholders [32, 163, 185], including scenarios like training [145]. However, combining data and knowledge within digital twins necessitates high documentation standards akin to those used in digital forensics [224]. Asset centrality is about maintaining a one-to-one relationship, collecting and managing historical and real-time data, incorporating expert knowledge, and ensuring secure data access.

(High) Fidelity. Security operations derive significant benefits from using digital twins, particularly in terms of their models and semantics. These models are designed to capture the real world with a high degree of fidelity [110, 134, 159, 165, 172, 205, 242], ensuring a reliable reflection of reality when compared with testbeds [25, 33, 39]. Additionally, these models enable more comprehensive analytics [27, 75], when used with more advanced techniques [208], including monitoring [41, 42, 44, 57, 66, 111, 124, 131, 136, 150], machine learning [19, 23, 33, 38, 41, 128, 154, 222, 235], and simulations [34, 63, 64, 79, 105, 132, 133, 163, 178, 188, 213]. For instance, digital twins enhance the continuous monitoring (*the process of continuously collecting and analyzing data*) of physical asset specifications against pre-defined rules, facilitating the detection of deviations [66]. Simulation results can be compared with monitored data to assess security [54, 119]. Machine learning is commonly employed in manufacturing contexts to enable predictive maintenance [123]. However, all of these techniques prevent potential vulnerabilities [59, 80, 234], intrusions [62, 69], or configuration flaws [24] before they manifest [114]. Besides the mere detection, using advanced techniques with digital twins also provides actionable insights [45, 135, 182] that support organizations in becoming more proactive in mitigating security risks. Reporting [127] and visualizing [88, 139] digital twin information allows to present complex data in an easily comprehensible manner, enhancing situational awareness [100, 108, 194] and aiding decision-making processes [53, 169, 171, 195]. This, in turn, contributes to optimizing the security of physical assets [92, 95, 113], resulting in reduced

costs and operational risks [88, 169, 171, 174, 176, 215, 219]. In summary, integrating digital twins fosters hyper-automation in cybersecurity [118], offering a comprehensive approach to enhancing security operations through advanced modeling and analytics, leading to improved security posture, cost reduction, and risk mitigation.

Virtual Decoupling. The decoupled nature of digital twins confers several advantages to security operations, as highlighted in the literature [65]. Firstly, digital twins provide an environment rich in computational resources, enabling the execution of resource-intensive applications [2, 116, 148, 217, 222, 238]. This heightened resource availability enhances the effectiveness of security operations. Secondly, decoupling digital twins ensures the absence of interference with the physical asset [13, 15]. This separation guarantees that security operations do not inadvertently disrupt the regular functionalities of the physical environment. It also introduces an additional layer of testing, offering a means to evaluate security operations independently from the real infrastructure [85, 223]. Lastly, the increased computational resources made available by decoupled digital twins facilitate the concurrent execution of multiple simulations [34]. This parallel simulation capability enhances the overall performance of security operations, enabling faster and more comprehensive assessments. In summary, the decoupled nature of digital twins provides security operations with increased computational resources, safeguards against interference with the physical system, offers an additional layer of testing, and allows for efficient parallel simulations, collectively contributing to improved security operations.

Physical/Virtual Intertwining. Contrary to the benefits of virtual decoupling, there are advantages to intertwining the virtual representation with the physical counterpart, as discussed in the literature [37, 43, 202]. This intertwining also extends to business and security applications [51]. Integrating virtual and physical elements simplifies bidirectional communication management with assets [151], facilitating various security operations. Furthermore, this integration follows a *defense in depth* strategy by introducing an additional layer that separates assets and services [35]. This strategy aims to ensure reliable and low-latency communication within the digital twin [137], thereby reducing communication complexity between applications and assets and ensuring a seamless data flow. Additionally, it enables direct interaction with physical assets [218], which is valuable for gathering pertinent information required for decision-making processes. Moreover, the intertwining of digital twins plays a crucial role in orchestrating security operations effectively. In summary, intertwining virtual and physical elements within digital twins simplifies communication management, introduces a defense-in-depth strategy, enables low-latency communication, allows direct interaction with physical assets, and facilitates effective security task orchestration.

Throughout the Lifecycle. Digital twins are inherently lifecycle-centric and closely follow the journey of their physical counterparts. They encompass all activities and processes throughout the asset's lifecycle, from design to production and service phases [101, 183, 191, 230]. Remarkably, even if the physical asset has yet to be realized [206, 220], digital twins can offer valuable support, such as system configuration [29] and aid in making security by design decisions to harden the physical assets [22, 224]. Moreover, digital twins persist throughout the product lifecycle, remaining prepared to accompany identical future assets. In summary, digital twins are inherently lifecycle-centric, accompanying physical assets from design to service, even before their physical existence, ensuring robust security at every stage.

Overall, digital twins represent a sophisticated approach to enhancing security operations, offering benefits such as centralized asset management, advanced modeling, a decoupled environment intertwined with physical elements, and comprehensive lifecycle coverage. Collectively, these benefits aim at enhancing the overall security posture. Subsequent sections of this paper examine the application domains and security operations benefiting from digital twins.

5.2 Application Domains

Digital twins are applied to enhance security operations across various sectors. Our review of the application domains is based on the critical infrastructure classification established by the CISA[4].

Commercial Facilities Sector. *Public spaces such as shopping centers, sports stadiums, and hotels play a key role in public safety and economic activity.* Current research focuses on malicious attack detection to protect smart cities using digital twins [194]. One work proposes security with digital twins for the IoT-enhanced theater [140]. While we could only find this one digital twin security work on a smaller scale that concerns only commercial or public facilities, we included smart homes in this sector. Despite not being strictly commercial, smart homes have economic characteristics and require safety (albeit more for the individuals than the public). For instance, digital twins are used to detect and check for anomalies via security and safety rules [19] or use other attack detection mechanisms [161] to prevent attacks on smart systems for home automation [232]. One work proposes the use of honeypots in combination with digital twins to detect attacks in smart homes [170], while another tackles security testing [177].

Communications Sector. *Communication networks are essential for everyday communication and emergency responses.* Two works propose a training based on digital twin technology to enhance skills in cybersecurity for IoT and 5G networks [109, 118]. A similar work uses a digital twin to test 5G and attack models [56]. 6G technology enabled by digital twins is regarded in terms of digital forensics [218]. Another work uses a digital twin to verify a security decoupling approach for an IoT network [57]. Some papers focus on communication (network) security with digital twins. However, those are mainly industry-oriented, so we categorized them into the respective manufacturing sector.

Critical Manufacturing Sector. *Manufacturing processes are vital to national security, including aerospace and automotive.* Most works using digital twins for security can be associated with smart manufacturing. In a nutshell, certain aspects are concentrated on when dealing with digital twins for industrial security. Those comprise attack detection [1, 3, 18, 63, 65, 66, 89, 133, 142, 174, 217, 222] including anomaly detection [33, 150], attack mitigation [2, 190, 193, 208] as well as security testing [23, 25, 29, 80, 144, 198, 199] and security analysis or evaluation [39, 61, 64, 69, 97, 111, 119, 127, 152, 192, 234]. Few works specifically regard one security operation—such as security-by-design [59] or security-in-depth [113]. Quite a lot of publications propose the combination with other security operations, including cyber ranges [22, 156, 211, 220, 242], forensics [58], cyber threat intelligence [62] or cybersecurity playbooks [71]. At last, some offer a research overview [67, 179] or deal with security in general [160, 163, 164, 205, 212, 215, 216].

Energy Sector. *Infrastructure for electricity, oil, and natural gas are essential for the functioning of other sectors.* Being the second-largest sector where digital twins are discussed for security, the papers show a manifold of application purposes: Some tackle the general protection of power system security [30, 37, 46, 47, 53, 54, 209], while others dive deeper into security testing and evaluation [14, 16, 122, 134, 171, 200, 201]. Few works specialize on security topics like real-time incident detection [147], incident response [4], self-security [114, 115], firmware patching [78] or network and data stream security of (distributed) power systems [108, 135, 136, 206].

Food and Agriculture Sector. *Food supply chain, from farms to consumers serve communities.* One group currently tackles this sector by enforcing security with an anomaly detection model of a digital twin in smart farming and attribute based access control in fishing applications [41, 42].

Healthcare and Public Health Sector. *Healthcare facilities and the public health system are critical during health crises.* Two works have been published to enforce security in healthcare using

[4] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

digital twins. They ensure that sensitive health data is protected and life-saving measurements are not disturbed by conducting security analyses [137, 176].

Information Technology Sector. *IT infrastructure and services are necessary for modern communication, data storage, and business operations.* Multiple security operations are covered in the works, focusing on digital twins to enhance IT security. Those include insider threats [27], security policies [31, 105, 106], network security and anomaly detection [95, 207], security testing and analysis [162, 186], software misconfigurations [149] as well as digital forensics [203] and security training [224]. Some works specifically focus on IoT, tackling security management [8, 73, 75, 99], attack detection [227] as well as combining blockchain and digital twin technology to secure IoT devices [107, 178, 191]. Another work reviews the use of digital twins for IoT security in general [221]. One work specifically targets the security of edge devices with digital twins [7]. Another work tackles the security of body area networks using digital twins [196]. Other publications regard cyber-physical systems and propose how sophisticated attacks can be mitigated using digital twins [238], tailor anomaly detection approaches [235, 236], manage synchronization [241], simulate attacks [76] or review the state of security research in this area [68].

Nuclear Reactors, Materials, and Waste Sector. *Nuclear facilities, materials, and waste are important for energy and medical applications.* Currently, few works concentrate on this sector. However, this sector is closely linked to the energy sector, which contains different power plants and a lot of relevant literature. The two works propose a digital twins to (a) test security [101] and (b) secure physical protection systems of nuclear power plants [102].

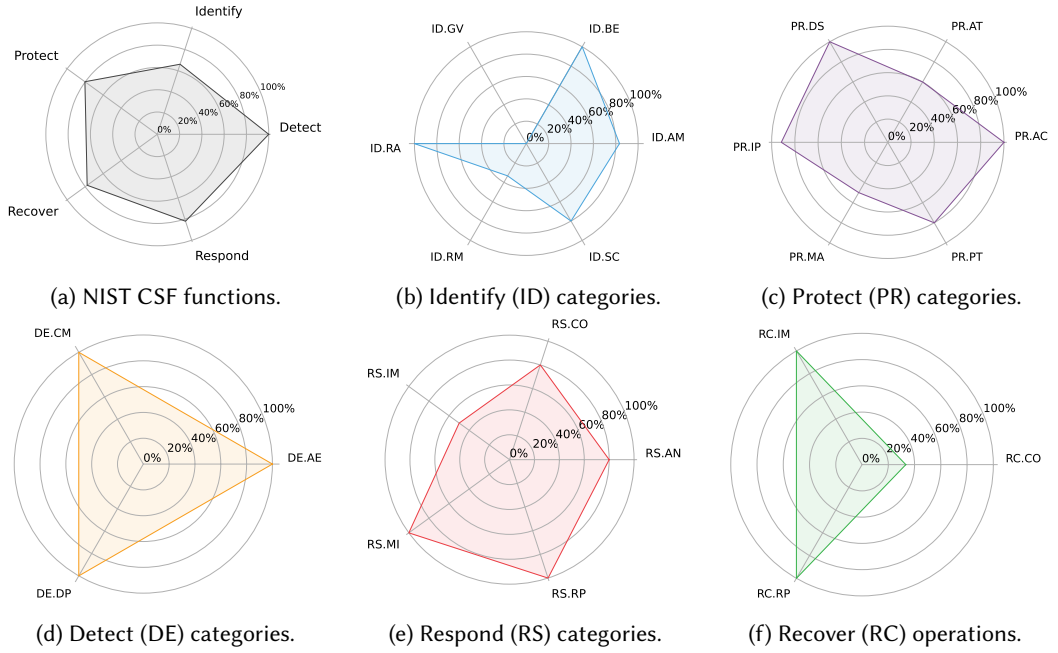
Transportation Systems Sector. *Transportation networks move people and goods.* Vehicular digital twins are also used for security testing and assessment purposes [9, 48, 51, 96, 153, 169] as well as to enforce privacy [52]. Nevertheless, it is remarkable that in this sector, privacy concerns seem to be of great importance [52, 223]. Other works tackle intrusion detection [12, 82, 104, 237, 240], secure communication [116, 138], access control [35], secure communication [32], security testing [126, 155] and security training [145].

Water and Wastewater Systems Sector. *Water supply and wastewater treatment facilities are essential for public health and environmental protection.* Interestingly, most works focus on anomaly detection [183, 210, 229]. Some extend their security focus and provide additional attack detection and security assessment mechanisms [36, 110, 165, 175]. One of these works provides a creative approach using a honeypot-like strategy [187].

Six out of the 16 CISA sectors are currently not addressed in terms of digital twin security: *Chemical Sector*, *Dams*, *Defense Industrial Base*, *Emergency Services*, *Financial Services*, and *Government Facilities*. Some of these sectors might be too specific (e.g., Dams) to be targeted. Meanwhile, other sectors can be seen as a subcategory or be strongly related to other fields and, therefore, not specifically addressed. For instance, many works from the critical manufacturing sector can be easily applied in the chemical sector. Also, the dams sector goes hand in hand with the water and waste systems sector. Moreover, the sectors concerning defense, emergency, and government might be too sensitive for publication.

5.3 Security Operations

In this section, we broaden our discussion on how digital twins can support security operations in alignment with the NIST CSF toward the diverse range of security operations facilitated by digital twins. Therefore, we conduct a comprehensive analysis and correlate the 111 research papers categorized as highly relevant to our survey with specific NIST CSF subcategories for improving cybersecurity in critical infrastructures. The detailed mapping and temporal development can be found in Appendix A (Figure 7 and Table 6). The mapping results are illustrated in Figure 5, where Figure 5(a) provides an abstract view at the CSF function level. Meanwhile, Figures 5(b)-5(f) delve



(a) NIST CSF functions. (b) Identify (ID) categories. (c) Protect (PR) categories.

(d) Detect (DE) categories. (e) Respond (RS) categories. (f) Recover (RC) operations.

Fig. 5. Digital twins in relation to the NIST Cybersecurity Framework (CSF) if they have been addressed at least once. Digital twins' security operations were coded and manually mapped to the corresponding NIST CSF functions and categories.

into more granular details at the CSF category level. For each category, we summarize whether the subcategories within this category have been addressed, denoting this with a simple binary (yes or no) indicator. For instance, we check whether for the category ID.GV (Identify – Governance), the research covers its subcategories ID.GV-1 to ID.GV-4. Figure 5(a) allows us to discern, for instance, that all categories of the *Detect* function have been covered in existing research, while not all categories of the *Identify* function have been equally addressed. In the following sections, we will delve into the specifics of the NIST CSF functions to provide detailed insights how digital twins contribute to each of these security functions.

The **Identify** function involves developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It ensures businesses know and understand their resources, risks, and overall cybersecurity posture. Figure 5(b) shows its categories *asset management* (ID.AM), *business environment* (ID.BE), *governance* (ID.GV), *risk assessment* (ID.RA), *risk management strategy* (ID.RM), and *supply chain risk management* (ID.SC). The asset management capabilities described in [14, 25, 28, 37, 42, 53, 75, 105, 119, 134, 144] revolve around creating and maintaining asset visibility in systems and subsystems. Each subsystem has multiple assets working in co-dependent states, and the whole system has a complex and decentralized state that must be maintained in the digital counterpart. Communication is only expected between very specific devices for business reasons or logging. The network traffic is lossy and devices are not online all of the time, leading to a complex interdependence between all devices. Hence, it is hard for human operators to grasp all assets and the connections between them. Therefore, it is important to ensure that *physical devices and systems within the organization are inventoried* (ID.AM-1) [7, 14, 25, 28, 37, 42, 46, 47, 53, 73, 75, 99, 105, 119, 126, 134, 138, 144, 149, 155, 156, 209] and *software platforms and applications within the organization are inventoried* (ID.AM-2) as well. Several authors

focus on this aspect [14, 25, 28, 48, 51, 52, 73, 75, 76, 81, 99, 105, 126, 134, 138, 149, 155, 156, 209]. In combination with mapping communication and data flows (ID.AM-3) [14, 25, 28, 75, 76, 99, 105, 126, 134, 138, 149, 155, 156], visibility within the organization can be secured. However, in comparison with aforementioned categories, the business environment and supply chain risk management categories are comparatively scarcely mentioned.

The **Protect** function is designed to establish protective measures for the uninterrupted provision of essential infrastructure services, encompassing robust access control, data security, and regular maintenance. Figure 5(c) details the categories *identity management and access control* (PR.AC), *awareness and training* (PR.AT), *data security* (PR.DS), *information protection processes and procedures* (PR.IP), *maintenance* (PR.MA), and *protective technology* (PR.PT). Most articles researching in the *Protect* function target PR.IP-1 [28, 51–53, 63, 65, 73, 76, 104, 118, 133, 149, 193, 195, 196, 200, 209, 236, 238, 240, 241], describing the need to keep a baseline configuration of systems, which is created and maintained incorporating security principles (e.g., the concept of least functionality). A baseline configuration describes a standard set of configuration settings (e.g., PLC configuration files or firewall settings). Additionally, data-in-transit protection (PR.DS-2) [3, 23, 35, 48, 51–53, 57, 116, 133, 238, 241] and general communication and control network protection (PR.PT-4) [3, 4, 12, 63, 65, 66, 76, 82, 89, 97, 100, 116, 123, 209] are supported through the use of digital twins as well.

The **Detect** function revolves around deploying strategic measures to detect cybersecurity events promptly. It entails ongoing surveillance and instantaneous analysis, ensuring rapid identification of cybersecurity incidents. Figure 5(d) highlights the categories *anomalies and events* (DE.AE), *security continuous monitoring* (DE.CM), and *detection processes* (DE.DP). The *Detect* function has received the greatest attention compared with all NIST CSF functions. It is therefore of utmost importance that *event data are collected and correlated from multiple sources and sensors* (DE.AE-3) [4, 7, 8, 12, 14, 16, 18, 23, 28, 29, 33, 42, 46–48, 53, 59, 62, 63, 65, 66, 69, 73, 76, 88, 89, 100, 106, 119, 122, 123, 126, 133, 138, 140, 142, 144, 149, 161, 170, 174, 177, 195, 196, 201, 206, 208, 209, 217, 222, 227, 235–238, 241] and to ensure that *the network is monitored to detect potential cybersecurity events* (DE.CM-1) [3, 4, 8, 12, 14, 18, 23, 33, 37, 42, 51–53, 57, 62, 63, 65, 66, 69, 73, 75, 76, 82, 89, 97, 100, 104, 116, 123, 126, 133, 134, 138, 140, 149, 161, 170, 174, 177, 193, 195, 196, 201, 206, 208, 209, 222, 227, 236, 240], with each being mentioned in over fifty research papers. Once again, the digital twin here shows its capability to bring together decentralized information from multiple operational sites, allowing for faster and more reliable intrusion detection than traditional methods as it holds semantic data. For instance, [29] includes different sensor data from human-close sensors (e.g., keyboard, mouse, camera, microphone, eye-tracking) to create a digital twin of a human to understand fatigue, stress, or even suspicious behavior in real-time. Additionally, Ref. [235] build an anomaly detection digital twin for CPSs called **Anomaly deTection with digiTAl TwIN** (**ATTAIN**). ATTAIN is based on generative adversarial networks to create malicious unlabeled data simulating CPS operation.

The **Respond** function emphasizes a systematic approach to managing cybersecurity incidents, incorporating predefined plans for response actions and effective communication strategies during and after an incident to minimize its impact. Figure 5(e) showcases the categories *response planning* (RS.RP), *communications* (RS.CO), *analysis* (RS.AN), *mitigation* (RS.MI), and *improvements* (RS.IM). The *Response* function focuses mainly on the control *incidents are reported consistent with established criteria* (RS.CO-2) [1, 2, 7, 8, 14, 18, 51–53, 57, 62, 63, 65, 66, 75, 76, 97, 104, 106, 133, 174, 177, 193, 209, 222, 240], but some papers also aim at highlighting the impact of an incident and enrich its context so that the *impact of the incident is understood* (RS.AN-2) [1, 2, 8, 37, 48, 75, 76, 133, 149, 200, 209, 224]. This allows a defender to conduct more in-depth root-cause analyses and respond to the incident faster and more precisely.

The **Recover** function focuses on formulating and executing strategies to uphold resilience plans and rehabilitate any functionalities or services disrupted by a cybersecurity incident. It

underscores the criticality of recovery planning, enhancements, and communication efforts to efficiently reinstate services and operations post-incident. Figure 5(f) illustrates the categories *recovery planing* (RC.RP), *improvements* (RC.IM), and *communications* (RC.CO). Within the *Recover* function, only a few researchers detail digital twin functionalities at all. These functionalities concentrate on the support of the following controls: *Recovery plan is executed during or after a cybersecurity incident* (RC.RP-1) [8, 75, 76, 149, 156, 193, 224], *Recovery strategies are updated* (RC.IM-2) [75, 224], *recovery plans incorporate lessons learned* (RC.IM-1) [76, 149, 224], and *recovery activities are communicated to internal and external stakeholders* as well as *executive and management teams* (RC.CO-3) [8, 75, 76]. However, compared with other NIST CSF functions, the *Recover* function is not yet as well researched, indicating potentials for recovery purposes, e.g., in case of a ransomware attack.

6 Implementing Digital Twins

In this section, we explore the components of digital twins in security operations in detail. To this end, we provide an overview on how to set up digital twins and discuss supportive tools.

6.1 Physical Assets and Data

Digital twins are virtual representations of physical assets. While physical assets may be resource-efficient devices like sensors or actuators, they could also have more computing resources (e.g., CPS). The following details different data used within a digital twin in security operations.

Sensor and Measurement Data. This category centers data gathered from various sensors, ranging from simple temperature sensors to complex multi-spectral cameras. Research [9, 10, 19, 31, 33, 88, 108, 137, 194, 238] delves into the nuances of sensor data, including its precision, reliability, and the challenges of integrating data from multiple sensors into coherent systems. They explore innovative ways to enhance sensor data accuracy and utility, such as advanced calibration techniques, noise reduction algorithms, and integration strategies for combining data from disparate sources. Additional research [57, 115, 128, 171, 186] investigates the application of sensor data in specific technologies like transformers, inverters, and IoT devices, addressing challenges like real-time data processing and the integration of sensor data into existing systems for monitoring, control, and predictive maintenance.

CPS Data. In the context of CPS, the data primarily revolves around operational parameters, performance metrics, and environmental interactions. The works of [32, 79, 81] represent significant advancements in utilizing data for enhancing vehicle performance and machinery efficiency. This includes the analysis of engine telemetry, fuel efficiency, emission levels, and machinery wear and tear. The data also encompasses feedback from control systems and user inputs, providing a comprehensive view of machine performance in real-world conditions. This contributes to developing more innovative, efficient, safer vehicles and machinery through data-driven optimizations and predictive maintenance.

Network Traffic Data. Research in this category [1, 14, 27, 39, 57, 58, 62, 65, 69, 108, 123, 133, 165, 172] focuses on the vast and complex datasets generated by network traffic. This data includes packet information, bandwidth usage, network topology, and security logs. The articles aim to optimize network performance, enhance data throughput, and ensure robust security against cyber threats. They leverage data analytics to understand network behavior, identify patterns, and predict potential issues. Their research is pivotal in designing more efficient and secure network systems capable of handling the increasing demands of modern digital communication.

Other Data. Data in this category [137, 145, 172, 224], includes a broad spectrum of information. This might involve user interaction data with devices, providing insights into user behavior, preferences, and use patterns. Additionally, specification sales documentation is used as a form

Table 4. Classification and Description of Protocols by ISO/OSI Layers

ISO/OSI Layer	Protocol	Description	References
L1 – Physical	Ethernet	Data framing & physical network transmission	[16, 62, 80, 122, 229, 237]
L2 – Data Link	ARP	IP address to physical address resolution	[224]
	WiFi	Wireless LAN communication	[36, 69, 232]
	Bluetooth	Short-range wireless communication	[232]
	Zigbee	Low-power wireless networking protocol	[73, 75, 126, 144]
L3 – Network	LoRaWAN	Long Range WAN protocol	[119, 240]
	DNP3	Distributed Network Protocol for utilities	[30, 80, 209]
L4 – Transport	TCP	Reliable, ordered data transmission	[14, 32, 34, 36, 58, 119, 137, 200, 201, 206, 208, 224]
	UDP	Fast, connectionless communication	[19, 108, 137]
L6 – Presentation	XML	Data format for structured documents	[195, 234]
	JSON	Lightweight data-interchange format	[34, 35, 63, 153, 171, 192, 193, 195]
	AutomationML	Data exchange in automation and engineering	[34]
	CAEX	Computer-Aided Engineering Exchange format	[234]
	SysML	Systems Modeling Language	[68]
	MSDL	Manufacturing Service Description Language	[34]
L7 – Application	AMQP	Messaging protocol for interoperability	[119]
	CoAP	Web transfer protocol for constrained nodes	[32, 34, 57, 191]
	HTTP/HTTPS	HyperText Transfer Protocol (Secure)	[46, 47, 73, 153, 191]
	MQTT	Lightweight messaging protocol for IoT	[14, 16, 32, 34–36, 73, 75, 119, 126, 134, 157, 159, 192, 193, 206, 230, 242]
	OPC UA	Machine to machine communication protocol	[67, 144, 230, 234, 242]
	REST	Representational state transfer	[34, 191, 224]
	SCADA	Supervisory control and data acquisition	[53, 61]
	SPARQL	Query language for graph databases	[42]
	SQLite	High-reliability database engine	[165]
	CIP	Common Industrial Protocol	[229]
	Modbus	Communication protocol for PLCs	[16, 30, 97, 122, 134, 200, 201, 206]
	S7comm	Communication protocol by Siemens	[23, 25, 242]
	Profinet	Industrial Ethernet standard for automation	[23]

of data, which could include information on product specifications, performance metrics, and customer feedback. Such data is invaluable in understanding how products are used in real-world environments and can guide design, functionality, and user experience improvements.

6.2 Communication and Synchronization

Digital twins communicate on the ISO/OSI stack (see Table 4), while they can interact with their physical counterparts, other digital twins, or human actors. In the physical layer (*ISO/OSI layer 1*), Ethernet is often applied in industrial settings [62, 80, 229]. At the data link layer (*ISO/OSI layer 2*), ARP, Wifi, Bluetooth, and Zigbee are noted for their diverse roles in systems [75, 144, 224, 232]. In the network layer (*ISO/OSI layer 3*), the importance of IP and LoRaWAN is highlighted [14] and [119]. The transport layer (*ISO/OSI layer 4*) sees applications of TCP and UDP [14, 19]. In the presentation layer (*ISO/OSI layer 6*), XML and JSON's roles are mentioned [34]. The application layer (*ISO/OSI layer 7*) features protocols like MQTT, OPC UA, REST, Profibus, and S7comm, with applications in various settings [23, 32, 34, 67, 75, 193, 206, 230, 230, 242]. In the field of digital twins in security operations, communication flows are categorized based on the nature of the interactions: digital twin ↔ physical asset, where digital twins communicate with physical assets; digital twin ↔ digital twin, involving interactions between multiple digital twins; and digital twin ↔ human,

which highlights the crucial collaboration between cybersecurity experts or novices and digital twins. Each type of flow plays a distinctive role in security operations:

Digital Twin ↔ Physical Asset. This flow is essential for collection data from physical assets and sending commands. In smart manufacturing, [1] demonstrates the digital twin's role in real-time security testing, affecting safety and efficiency. [9] applies this to autonomous vehicles, focusing on safety enhancements through data analytics. [10] shows how digital twins improve operational efficiency in manufacturing. [13] emphasizes simulation benefits, and [103] explores its impact in healthcare, enhancing decision-making and operational performance.

Digital Twin ↔ Digital Twin. This interaction fosters interconnectivity and shared intelligence among digital twins. [10] discusses data and insight sharing for system-wide efficiency in manufacturing. [108] and [118] show how twin collaboration enhances data analysis and system management. [183], [10], and [195] focus on predictive maintenance and energy management. [75] and [71] highlight how networks of digital twins improve industrial automation and security.

Digital Twin ↔ Human. This interaction is crucial for developing effective security strategies. [13] demonstrates how digital twins aid in testing security measures. Refs. [144] and [102] discuss the role of human interaction in refining security strategies. Refs. [80] and [128] emphasize vulnerability assessments and threat detection. Refs. [172], [224], and [109] show digital twins as training tools for cybersecurity professionals. Papers like [174], [75], and [134] highlight the importance of human expertise in system resilience, disaster response, and policy development.

6.3 Data Management

Managing data within digital twins is a complex yet crucial task, particularly when considering the challenges associated with time-stamping and data order. The approach to data collection, whether active or passive monitoring, significantly impacts how data arrives from the physical assets. As data might not arrive in the same order as it was generated [108, 116], it is essential to employ a **Network Time Protocol** (**NTP**) server [198, 199] to reconstruct the data sequence accurately. This is particularly important when data is used for machine learning, where the chronological order of data is vital for accurate modeling. However, data management mainly involves data collection, preprocessing, and storing.

Data Pre-processing and Machine Learning. Before storage, data pre-processing is a crucial step. It involves filtering, normalizing, and transforming raw data into a format suitable for analysis and storage. This process ensures data quality and usability, paramount in environments where data is used to model and simulate digital twins. Logstash (e.g., [63, 222, 224]), Filebeat (e.g., [63, 222, 224]), Apache Kafka (e.g., [136, 155]), and Node-RED (e.g., [16]) are used for data collection and log processing, crucial for handling large volumes of data generated by physical assets. Zigbee2MQTT (e.g., [73]) facilitates fast and secure data transfer, especially in IoT environments, by bridging Zigbee devices to MQTT. Tools and techniques like TensorFlow (e.g., [12, 33, 133]), Scikit-learn (e.g., [87, 89, 133]), and Keras (e.g., [33, 89, 133]) are leveraged for machine learning and data analysis, enabling advanced predictive analytics and pattern recognition.

Data Storage. Different approaches are utilized for data storage depending on whether the digital twin is specification-based or data-driven, where environmental data from the physical twin is consumed as input [222]. The nature of collected data varies across papers, depending real world asset and the twin's intended purpose. Beside SQL and NoSQL databases like MongoDB (e.g., [73, 74]) or PostgreSQL (e.g., [106]), Elasticsearch (e.g., [29, 63, 222, 224]) or OpenSearch

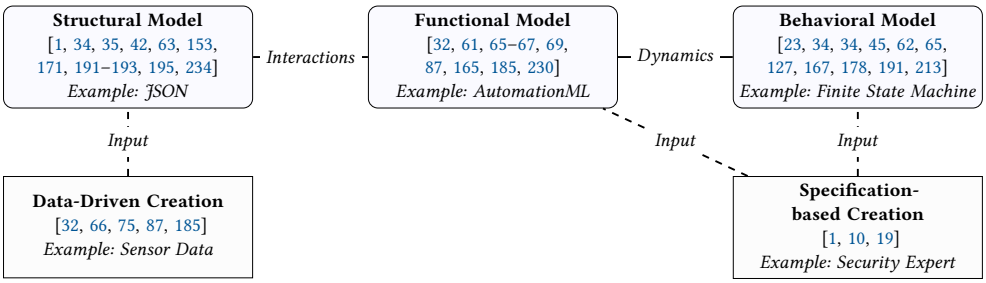


Fig. 6. Illustration of structural, functional, and behavioral models in digital twin research.

(e.g., [46, 47]) are employed for their powerful search and data indexing capabilities, ideal for the large-scale data storage needs of digital twins. Ethereum (e.g., [133, 178]) and Hyperledger Fabric (e.g., [178]) provide distributed ledger technologies for secure and immutable data storage, offering reliability and transparency in data management.

Supportive Software. Platforms provide architectural patterns and simplify digital twin (data) management. For instance, cloud platforms like AWS (IoT) (e.g., [34, 35, 193, 206]), Azure (IoT) (e.g., [34, 42]), Azure Digital Twins (e.g., [4]), and IBM Watson IoT (e.g., [34]) provide robust infrastructure for hosting and managing digital twins, offering scalability and high availability. Open source tools such as Eclipse Ditto (e.g., [34, 75, 163, 202]), OpenStack (e.g., [97, 172]), Kubernetes (e.g., [2, 3, 149]), and FIWARE (e.g., [46, 47]) facilitate the deployment and orchestration of digital twin applications, ensuring efficient and flexible management of digital twin environments. Additionally, Google Functions, AWS Lambda, and Amazon SageMaker (e.g., [76]) can be integrated to extend capabilities for data processing and analytics. These tools collectively enable the collection, storage, processing, and analysis of digital twin data.

Deployment Strategy. The location of digital twin deployment dramatically affects their performance and utility. On-device or embedded digital twins, as noted in Refs. [31], [57], and [60], offer low latency and immediate responsiveness, crucial for rapid decision-making. However, they face limitations in processing power and storage capacity, affecting the complexity of tasks they can manage. Edge computing, discussed in [87] and [88], mitigates some constraints by processing data near its source. This approach offers lower latency than cloud solutions and significant computational resources, proving beneficial in industrial settings for real-time data processing. Cloud-based digital twins, referenced in [1] and [9], provide expansive computational resources and storage. This deployment fits complex simulations and large-scale data analytics, which is ideal for in-depth analysis and strategic planning where latency is less critical. Each deployment model—embedded, edge, or cloud—has unique benefits and limitations. The selection depends on the security operation's specific needs, considering latency, computational power, and data processing scope.

6.4 Virtual Representation and Environment

Creating virtual models in digital twin research starts with a deep understanding of the systems involved [1, 10]. This process involves data collection and analysis to develop digital twins that accurately reflect their physical counterparts [15, 22]. As Figure 6 illustrates, digital twin research encompasses three core models: structural, functional, and behavioral. These categories were derived inductively through a detailed coding and analysis of the reviewed literature. Structural models, using formats like JSON, XML, OWL, or RDF, represent the physical aspects of systems

[1, 34, 35, 42, 63, 153, 171, 191–193, 195, 234]. These models descriptively represent a system. Functional models, often employing AutomationML, detail the operational processes and logic [32, 61, 65–67, 69, 87, 165, 185, 230]. They illustrate the interactions within a system. Behavioral models focus on dynamic behaviors over time, using approaches like finite state machines [23, 34, 34, 45, 62, 65, 127, 167, 178, 191, 213]. Figure 6 also shows that these models can be created either data-driven, like from sensor data [32, 66, 75, 87, 185], or specification-based, as in the case of security expert inputs [1, 10, 19]. Please note that some papers may have ambiguities and can be assigned to multiple categories.

Data-Driven Creation. In the data-driven approach to creating digital twins, the emphasis is on leveraging real-time data to construct and refine the digital twin. This method is highlighted in [32], [87], or [75] and primarily relies on the integration of IoT technologies for continuous state updates. The real-time data collected from IoT devices provides a dynamic and evolving representation of the physical counterpart. For instance, [66, 185] further demonstrate how advanced data analytics are employed to process and interpret this vast stream of information, facilitating the creation of a digital twin that is responsive and up-to-date. This approach is efficient in environments where operational data is abundant and can be used to update and improve the digital twin's accuracy continuously. The data-driven model excels in adaptability, reflecting the ever-changing state of the physical system it represents.

Specification-based Creation. Conversely, the specification-based approach to digital twin creation focuses on constructing a detailed and predefined functional or behavioral model of a system. This method is exemplified by [1], [10], or [19] and involves the use of simulation tools such as Simulink or Anylogic and security expert input to craft a virtual model that mirrors the physical system meticulously. The approach is grounded in deeply understanding the system's processes and operations. Furthermore, applying algorithms like the Kalman Filter and SVM, as seen in [1], enhances the model's capability to simulate complex environments. The specification-based approach is particularly suited to scenarios where the physical system's behavior is well-understood or documented and can be accurately represented through established models. This approach ensures control and predictability in the digital twin's behavior.

6.5 Simulation Capabilities

Simulations can be either in real-time or offline. Real-time simulation runs at the same pace as the real-world system, offering immediate feedback and interaction, while offline simulation operates at variable speeds for in-depth analysis, planning, and optimization without real-time processing constraints. The choice between them depends on the desired security operation. These simulations are supported through various tools.

Real-time Simulation. This type of simulation operates synchronously with system time. It supports *Detect* (DE) and *Respond* (RS) functions of the NIST CSF. In the *Detect* function, particularly in categories like anomalies and events (DE.AE) and security continuous monitoring (DE.CM), real-time simulations are crucial for the immediate collection and correlation of event data from diverse sources and sensors. This is further crucial in the prompt detection of unusual activities or cybersecurity incidents, thereby enhancing an organization's readiness and response capabilities, as demonstrated in papers like [63], [19], and [66]. In the *Respond* function, real-time simulations support the rapid execution of response plans (RS.RP-1) and consistent reporting of incidents (RS.CO-2), facilitating swift and efficient actions against cybersecurity threats. This minimizes potential damage and aids in quicker recovery [58, 62].

Offline Simulation. Offline simulations run at different (lower or higher) system speeds compared with the real world, like a Monte Carlo simulation. They significantly contribute to the *Identify* (ID) and *Protect* (PR) functions of the NIST CSF. In the "Identify" function, offline

Table 5. Classification of Simulation Technologies in Digital Twins

Domain	Simulation Technology	Open Source	Simulation Type	References
General	Anylogic		Real-time/Offline	[10]
	ANSYS Twin Builder		Offline	[185]
Cyber-Physical Systems	CPS Twinning	•	Real-time	[65–67, 69]
	MATLAB		Real-time/Offline	[7, 19, 87, 134, 136, 175, 192, 206, 242]
	Simulink		Real-time/Offline	[1, 16, 19, 53, 108, 175, 192, 206]
Automation Systems	ScadaBR	•	Real-time	[59]
	OpenPLC	•	Real-time	[58], [59], [80], [234]
Robotics	Gazebo	•	Real-time/Offline	[29]
	LabVIEW		Real-time/Offline	[78]
Networks	Mininet	•	Real-time	[63, 65–67, 69, 165]
	Cooja	•	Real-time	[123]
Water Systems	EPANET	•	Real-time/Offline	[165, 175]
	DHALSIM	•	Real-time	[165]
Industrial Simulations	SIMIT		Real-time	[174]
	Tecnomatrix Simulation		Offline	[242]
Electrical and Power Systems	SimpowerSystems		Real-time/Offline	[53]

simulations assist in comprehensively understanding and documenting an organization's assets, such as in ID.AM-1 and ID.AM-2, where physical devices and software platforms are inventoried. This role is underscored in papers like [14] and [25], highlighting the importance of offline simulations in asset management and risk assessment (ID.RA). These simulations provide a detailed view of the organization's resources and vulnerabilities, enabling better strategic planning and prioritization. In the *Protect* function, offline simulations aid in establishing safeguards and maintaining baseline configurations of IT and control systems (PR.IP-1). They offer a controlled environment to test and validate security operations without impacting operations [69].

Simulation Tools. To support these simulations, software is pivotal, catering to specific domains and types (see Table 5). General-domain tools like Anylogic (e.g., [10]) and ANSYS Twin Builder (e.g., [10, 185]) offer wide-ranging capabilities, from simulating physical systems to electronic. For cyber-physical systems, CPS Twinning integrates physical and computational models [66], complemented by MATLAB (e.g., [19]) and Simulink (e.g., [1]) for computation and multi-domain simulation. Automation systems benefit from ScadaBR's focus on supervisory control [59] and OpenPLC's open-source approach [58]. Robotics simulations are adeptly handled by Gazebo (e.g., [29]) and LabVIEW (e.g., [78]), while network environments are emulated by Mininet (e.g., [63]) and Cooja (e.g., [123]). EPANET (e.g., [123]) and DHALSIM (e.g., [165]) offer specialized solutions for water systems analysis, and industrial simulations are advanced by SIMIT (e.g., [174]) and Tecnomatrix Simulation (e.g., [242]) for process optimization. Lastly, electrical and power systems find a niche in SimpowerSystems [53], underlining the comprehensive scope of simulation technologies.

6.6 Security Operations

There is no universal best practice for designing security operation applications due to the variety of available tools and distinct system requirements. Each function of the NIST CSF demands specific tools and methodologies tailored to particular security needs. Therefore, selecting tools for digital twin-based security operations must be customized to each specific function's unique challenges and organizational specifics. However, in developing security operations based on digital twins, various programming languages, frameworks, and tools strategically support security operations by optimizing functionality, enhancing user experience, and bolstering security. Programming languages like C++ [87, 232], known for its performance efficiency, and Python [35, 134, 153, 206, 229, 232], celebrated for its versatility and user-friendliness, play a pivotal role in the backbone

of digital twin development. Javascript [224] is commonly used for its effectiveness in web-based applications, while Docker [73, 134] ensures application consistency across various environments. Frameworks such as Flask [73, 153, 224] enable the creation of robust web applications, while MATLAB App Designer [53] is instrumental in designing interactive apps. Nginx [2, 3] serves as a reliable web server and reverse proxy. In the realm of tools, SDN-Wise [123] is utilized for software-defined networking, enhancing network management, and security. Ettercap [39, 63, 224] is a crucial resource for network security, specializing in packet sniffing and protocol analysis. Tools like Nmap [15, 59, 73] and Nessus [15] are key for network mapping and vulnerability scanning, respectively. Pfsense [39, 126] offers firewall and routing capabilities, whereas Scapy [224], Dsiem [63, 222, 224], Beacon [185], and KDiff3 [39] provide various functionalities ranging from packet manipulation to security information and event management. Additional security-focused tools such as Metasploit [126] for penetration testing, Security Onion [126] for network security monitoring, and OSSIM AlienVault [126] for security information and event management, also contribute to security operations.

6.7 User Interaction

User interaction often transcends direct communication with the digital twin itself. Instead, users typically engage with digital twins through applications designed for security operations, such as cyber ranges or SOAR platforms, as discussed in papers [19, 75, 109, 172]. These applications act as intermediaries, facilitating user interaction with the underlying digital twin. A cyber range, for instance, is an interactive, simulated representation of an OT environment used for cybersecurity training. In this context, the digital twin is the foundational (simulation) model, mimicking real-world systems, as elaborated in Refs. [220] and [224]. Similarly, SOAR platforms integrate with digital twins to enhance cybersecurity incident response and management [75]. In these platforms, the digital twin provides a dynamic system representation using structural models, enabling users to visualize, analyze, and respond to security threats more effectively, as detailed in [45] and [75]. Users interact with the SOAR platform's interface, leveraging the insights the digital twin offers to make informed decisions and automate responses to security incidents through playbooks.

Different specialized technologies and tools simplify the access to digital twins, each adding a unique dimension to its functionality (*analytics mode*). Polygon Cruncher, as referenced in [144], plays a crucial role in optimizing 3D models, enhancing the efficiency of digital twin representations. Kibana, highlighted in [29, 63, 222], serves as an invaluable tool for data visualization, enabling users to analyze and interpret complex data streams effectively. Prometheus, cited in [2], offers critical capabilities in monitoring and alerting, ensuring the digital twin systems perform optimally. InTouch software, as seen in [39], is pivotal for industrial automation, providing robust management and visualization of operational data within digital twins. Lastly, WinCC, mentioned in [23], aids in process visualization for automated environments, playing a vital role in the control and oversight of digital twin systems. Together, these technologies and tools underscore the complexity and technological sophistication of accessing digital twins, highlighting their versatility and the necessity of a diverse toolkit to unlock their full potential.

7 Challenges and Future Research

7.1 Challenges

Lack of Standards. Digital twins face challenges due to the absence of standards, especially in real-world OT environments. These environments, often built upon existing infrastructures, vary significantly in design and technology, creating hurdles for developing standardized digital twins. Despite the availability of IEC 62443 for security and ISO 23247 for digital twins, the inherent uniqueness of each system means digital twins are custom-made, making widespread

adoption challenging [184, 215, 219]. Although organizations (e.g., IETF) are developing digital-twin networking protocols, these initiatives have yet to secure consensus or achieve broad industry uptake [123].

Automated Vulnerability Response. The dynamic nature of industrial environments makes manual vulnerability assessments impractical, highlighting the need for effective automated methods. Digital twins could play a crucial role in continuously monitoring and identifying vulnerabilities. The challenge lies in developing systems that can quickly detect weaknesses and automatically respond to the complexities and dependencies within these systems. However, these systems often fall short of the real-time performance demands of production-scale digital twins [17], and their latency limitations make it difficult to ensure automated countermeasures can react swiftly enough to threats [187].

High-Level Guidance and Access Management. Establishing high-level guidance and managing access to digital twins are vital challenges. Defining strategic frameworks that align with organizational objectives is complex due to the diverse applications of digital twins. Moreover, effective access management is critical to prevent unauthorized use, requiring a delicate balance between collaborative openness and strict control of access, emphasizing the need for clear policies and robust governance which is especially challenging within heterogeneous IoT environments [152, 164]. Moreover, evolving regulations (from the EU NIS Directive onward) require adaptable digital twin architectures, while regulatory gaps and shifting sector-specific policies hinder large-scale, cross-border deployment [46, 215].

Knowledge Requirements. Developing digital twins in security operations requires a unique blend of OT systems and cybersecurity expertise. There is a noticeable gap between the knowledge of cybersecurity experts and OT engineers, with the former often needing more insight into OT systems and the latter focusing more on operational excellence than security. This creates a demand for specialists proficient in both domains to develop effective digital twins for complex environments. Failing to adhere to such goals will limit the implementation success for creation and adoption of digital twins as the vast majority of companies and users will not be able to deploy an army of engineers to create custom digital twins and therefore the adoption of digital twins may be restricted to an industrial oligopoly [207].

OT/IoT Network Assets Visibility. Gaining comprehensive visibility into OT and IoT networks is challenging, especially with devices that are not continuously connected. The first step in OT asset management is constantly gaining clear visibility, guided by the principle that effective management starts with thorough visibility of the network's assets [52, 108]. Note that field devices or sensors are hidden in IP networks (see Purdue model).

Communication Delays and Model Attacks. Digital twins in OT environments are susceptible to communication delays and model attacks. When applied in real-world scenarios, these issues can lead to performance problems like network congestion or computational overload, underscoring the importance of addressing these challenges for the successful implementation of digital twins [116, 144].

Cybersecurity and Privacy Concerns. Security vulnerabilities are significant concerns in digital twin development. Synchronization security, resilience against DoS attacks, and data privacy are critical. The insecurity of IoT devices and the lack of standards for securing digital twins add to these concerns, making them potential targets for cyber attacks [113, 174, 182]. Digital twins raise also serious privacy concerns: without robust protection of sensitive components, data, and interactions, existing privacy technologies may fall short, and the rapid growth of applications intensifies the need for ethical governance models to manage consent and data usage [113, 185].

Data Management and Quality. Ensuring high-quality data management is a crucial challenge in digital twins, especially when using machine learning algorithms. Handling data scarcity or

biases and ensuring the quality of the data are pivotal for the accuracy and effectiveness of digital twins.

Fidelity and Accuracy. Maintaining high fidelity in digital twin models is crucial but challenging. The diversity of OT environments and data quality issues make it difficult to achieve the desired level of model accuracy. Moreover, OT engineers are cautious about adopting new technologies that might disrupt manufacturing processes [82, 167, 205].

Interoperability, Integration and Scalability. Achieving interoperability and seamless integration with existing systems is a significant hurdle. Digital twins must be able to adapt to various protocols and integrate with different management tools, which is often challenging due to the proprietary nature of many OT protocols [150]. Scalability is another concern, especially in real-time environments where processing requirements increase with system complexity and the need for low-latency responses. For instance, [50] highlight that without structured model integration and modular simulation strategies, digital twins can become computationally infeasible as systems grow in size.

Explainable AI. The use of explainable AI in digital twins is essential for transparency and trust. This is especially important in safety-critical systems, where understanding AI decisions is crucial. Challenges include addressing the black-box nature of AI, ensuring model transparency, and protecting against attacks on the AI model itself [100, 174, 222].

7.2 Future Research

Future research should address these challenges and explore digital twins in lesser-investigated NIST CSF functions.

Governance, Risk Management, Incident Response, and Recovery. Within the NIST CSF framework, several subcategories are yet to be fully explored, presenting ripe opportunities for future research. These include governance and risk management (ID.GV-1 to ID.GV-4), remote maintenance (PR.MA-2), coordination with stakeholders (RS.CO-4), incorporation of lessons learned in response plans (RS.IM-1), and recovery and public relations management (RC.CO-1 to RC.CO-2). These areas lack extensive references and could significantly benefit from digital twins. By delving into these subcategories, researchers can uncover new ways to enhance security operations.

Exploring Application Domains for Digital Twins in Security Operations. The application of digital twins in various sectors promises to revolutionize security operations through situational awareness, predictive analytics, and strategic response mechanisms. In the *chemical sector*, digital twins can provide advanced simulations and monitoring capabilities essential for ensuring the security of chemical production and transportation. In the *defense industrial base sector*, digital twins could be invaluable in securing the supply chain for military operations. By replicating manufacturing and logistical processes, these digital twins can identify vulnerabilities, manage risks, and safeguard the integrity of critical military resources. In the *emergency services sector*, digital twins for simulating various emergency scenarios could significantly enhance resource allocation, response times, and inter-agency coordination in fire, medical, and police services, thus bolstering public safety. In the *financial services sector*, digital twins can simulate networks and transactions to detect anomalies, predict cyber threats, and strengthen financial infrastructure. In the *government facilities sector*, digital twins can be crucial in securing government buildings and infrastructure.

8 Conclusion

In conclusion, this comprehensive article has made significant strides in understanding the role of digital twins in security operations by rigorously analyzing a large scale of scientific article in this area. Our drawbacks are documented using Github. Our exploration of the multifaceted applications

of digital twins in cybersecurity contexts has illuminated the potential of this technology to revolutionize how we approach and think cybersecurity. We delved into the understanding of digital twins, their components, usage, and ways they can be implemented to detect, analyze, and respond to cyber threats, providing real-time, dynamic, and predictive capabilities that traditional security operations lack. Our analysis highlighted the efficiency gains and heightened security posture achievable through the integration of digital twins, particularly in complex and interconnected digital ecosystems. However, the journey does not end here. The potential of digital twins in security operations is vast, and numerous avenues remain unexplored. The challenges of scalability, interoperability, real-time data synchronization, and privacy concerns present fertile ground for future research. Moreover, standardization and best practices for the deployment of digital twins in security operations is crucial for their wider adoption and effectiveness. As we continue to navigate the ever-evolving digital landscape, the role of digital twins will undoubtedly expand and evolve. This research lays a solid foundation for future explorations in this exciting field. The journey toward a more secure digital future, with digital twins at the forefront, is just beginning.

Appendix

A NIST Cybersecurity Framework For Critical Infrastructures Mapping

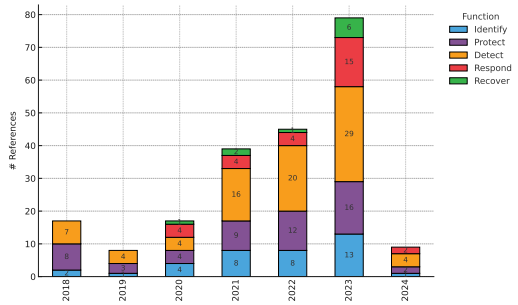


Fig. 7. NIST CSF function references (2018–2024), highlighting growth in response and recovery.

Table 6. Comprehensive Mapping of the NIST Cybersecurity Framework Subcategories with 111 Highly Relevant References

Subcategory	Description	References
Function: Identify		
ID.AM-1	Physical devices and systems within the organization are inventoried.	[7, 14, 25, 28, 37, 42, 46, 47, 53, 73, 75, 99, 105, 119, 126, 134, 138, 144, 149, 155, 156, 209]
ID.AM-2	Software platforms and applications within the organization are inventoried.	[14, 25, 28, 48, 51, 52, 73, 75, 76, 81, 99, 105, 126, 134, 138, 149, 155, 156, 209]
ID.AM-3	Organizational communication and data flows are mapped.	[14, 25, 28, 75, 76, 99, 105, 126, 134, 138, 149, 155, 156]
ID.AM-4	External information systems are catalogued.	[25, 75, 76, 99, 155]
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	[25, 51, 52, 76, 149, 155]
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	
ID.BE-1	The organization's role in the supply chain is identified and communicated.	[76, 81, 119]
ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated.	[37, 76, 119]
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated.	[37]
ID.BE-4	Dependencies and critical functions for delivery of critical services are established.	[37, 81, 99, 149]
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	[37, 81, 149, 193, 208]
ID.GV-1	Organizational cybersecurity policy is established and communicated.	

(Continued)

Table 6. Continued

Subcategory	Description	References
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	
ID.GV-4	Governance and risk management processes address cybersecurity risks.	
ID.RA-1	Asset vulnerabilities are identified and documented.	[14, 25, 37, 48, 56, 75, 76, 81, 149]
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources.	[14, 75, 76, 81, 105, 149]
ID.RA-3	Threats, both internal and external, are identified and documented.	[14, 37, 73, 76, 81, 99, 105, 149, 209]
ID.RA-4	Potential business impacts and likelihoods are identified.	[76, 81, 99, 119, 149, 209]
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	[48, 76, 99, 149]
ID.RA-6	Risk responses are identified and prioritized.	[76, 99, 193]
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders.	[76, 105]
ID.RM-2	Organizational risk tolerance is determined and clearly expressed.	
ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.	
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	[48]
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	[48]
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	[48]
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	[48, 81]
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	
Function: Protect		
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	[23, 133, 178]
PR.AC-2	Physical access to assets is managed and protected	[23, 76, 119, 186]
PR.AC-3	Remote access is managed	[23, 35, 57, 76, 118, 178]
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	[35, 51, 52, 57, 76, 118, 133, 178]
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).	[51, 52, 57, 76, 133]
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions.	[35, 51, 52, 76, 118, 133, 178]
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	[35, 51, 52, 76, 119, 178]
PR.AT-1	All users are informed and trained.	[22, 36, 69, 96, 156, 209, 211, 224]
PR.AT-2	Privileged users understand their roles and responsibilities.	[22, 36, 82, 156, 209, 224]
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	
PR.AT-4	Senior executives understand their roles and responsibilities.	
PR.AT-5	Physical and cybersecurity personnel understand their roles and responsibilities.	[22, 36, 63, 82, 156, 209, 211, 224]
PR.DS-1	Data-at-rest is protected.	[23, 35, 48, 51, 52, 104, 133]
PR.DS-2	Data-in-transit is protected.	[3, 23, 35, 48, 51–53, 57, 116, 133, 238, 241]
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.	[28, 51, 52, 76, 97]
PR.DS-4	Adequate capacity to ensure availability is maintained.	[53, 76]
PR.DS-5	Protections against data leaks are implemented.	[48, 51, 52, 57, 73, 76]
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.	[48, 53, 65, 66, 76, 81, 133]
PR.DS-7	The development and testing environment(s) are separate from the production environment.	[1, 2, 14, 48, 53, 66, 200, 209]
PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity.	[7, 23]
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).	[28, 51–53, 63, 65, 73, 76, 104, 118, 133, 149, 193, 195, 196, 200, 209, 236, 238, 240, 241]
PR.IP-2	A System Development Life Cycle to manage systems is implemented.	[48, 149]
PR.IP-3	Configuration change control processes are in place.	[48, 63, 97, 149, 201, 209]
PR.IP-4	Backups of information are conducted, maintained, and tested.	[63, 149]
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met.	[37, 51, 52, 66, 149]
PR.IP-6	Data is destroyed according to policy.	[51, 52, 133]
PR.IP-7	Protection processes are improved.	[8, 48, 54, 59, 66, 75, 149, 170, 200, 209]
PR.IP-8	Effectiveness of protection technologies is shared.	
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	[8, 75, 76, 149, 209]
PR.IP-10	Response and recovery plans are tested.	[8, 75, 76, 149, 186, 209, 224]
PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	[29, 76, 186]
PR.IP-12	A vulnerability management plan is developed and implemented.	[48, 75, 76]
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	[48, 76, 97, 149]
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	

(Continued)

Table 6. Continued

Subcategory	Description	References
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	[48, 58, 62, 63, 66, 69, 76, 119, 149, 178]
PR.PT-2	Removable media is protected and its use restricted according to policy.	
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	[35, 76]
PR.PT-4	Communications and control networks are protected.	[3, 4, 12, 63, 65, 66, 76, 82, 89, 97, 100, 116, 123, 209]
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	[54, 59, 65, 66, 82, 122, 149, 201, 209, 217]
Function: Detect		
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.	[4, 7, 8, 12, 28, 33, 42, 53, 63, 69, 73, 76, 106, 108, 119, 122, 123, 133, 144, 161, 174, 177, 196, 200, 201, 208, 209, 222, 235, 240, 241]
DE.AE-2	Detected events are analyzed to understand attack targets and methods.	[8, 12, 14, 23, 42, 46–48, 53, 59, 63, 66, 69, 73, 76, 119, 133, 144, 161, 174, 177, 195, 200, 201, 208, 209, 217, 222, 227]
DE.AE-3	Event data are collected and correlated from multiple sources and sensors.	[4, 7, 8, 12, 14, 16, 18, 23, 28, 29, 33, 42, 46–48, 53, 59, 62, 63, 65, 66, 69, 73, 76, 88, 89, 100, 106, 119, 122, 123, 126, 133, 138, 140, 142, 144, 149, 161, 170, 174, 177, 195, 196, 201, 206, 208, 209, 217, 222, 227, 235–238, 241]
DE.AE-4	Impact of events is determined.	[7, 8, 14, 28, 46–48, 53, 59, 63, 73, 76, 99, 108, 133, 144, 149, 161, 174, 209, 227]
DE.AE-5	Incident alert thresholds are established.	[7, 8, 33, 46, 47, 53, 59, 63, 65, 66, 73, 76, 89, 133, 149, 161, 174, 201, 208, 209, 222, 227]
DE.CM-1	The network is monitored to detect potential cybersecurity events.	[3, 4, 8, 12, 14, 18, 23, 33, 37, 42, 51–53, 57, 62, 63, 65, 66, 69, 73, 75, 76, 82, 89, 97, 100, 104, 116, 123, 126, 133, 134, 138, 140, 149, 161, 170, 174, 177, 193, 195, 196, 201, 206, 208, 209, 222, 227, 236, 240]
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events.	[3, 4, 7, 14, 18, 37, 46, 47, 51–54, 62, 65, 66, 69, 75, 76, 82, 88, 97, 104, 108, 119, 122, 134, 138, 140, 142, 174, 186, 193, 201, 206, 208, 209, 236]
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events.	[29, 73, 75, 76, 104, 186, 209]
DE.CM-4	Malicious code is detected.	[48, 73, 75, 76, 104, 209, 227]
DE.CM-5	Unauthorized mobile code is detected.	[48, 73, 75, 76, 104, 209, 227]
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events.	[51, 52, 75, 76, 81, 186]
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.	[51, 52, 65, 73, 75, 76, 119, 186, 209]
DE.CM-8	Vulnerability scans are performed.	[14, 48, 56, 59, 76, 81, 134, 221]
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability.	[51, 52]
DE.DP-2	Detection activities comply with all applicable requirements.	[48, 51, 52, 63, 133]
DE.DP-3	Detection processes are tested.	[1, 2, 48, 63, 76, 134, 237]
DE.DP-4	Event detection information is communicated.	[1, 2, 8, 53, 63, 75, 76, 97, 133, 174, 177, 201, 209, 222]
DE.DP-5	Detection processes are continuously improved.	[63, 75, 76, 104, 106, 133, 177, 193, 209]
Function: Respond		
RS.RP-1	Response plan is executed during or after an incident.	[2, 8, 75, 76, 106, 193, 224]
RS.CO-1	Personnel know their roles and order of operations when a response is needed.	[36, 76, 211, 224]
RS.CO-2	Incidents are reported consistent with established criteria.	[1, 2, 7, 8, 14, 18, 51–53, 57, 62, 63, 65, 66, 75, 76, 97, 104, 106, 133, 174, 177, 193, 209, 222, 240]
RS.CO-3	Information is shared consistent with response plans.	[51, 52, 62, 76, 104, 106, 133, 209]
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.	
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	[62, 76]
RS.AN-1	Notifications from detection systems are investigated.	[8, 75, 76, 133, 149, 209, 240]
RS.AN-2	The impact of the incident is understood.	[1, 2, 8, 37, 48, 75, 76, 133, 149, 200, 209, 224]
RS.AN-3	Forensics are performed.	[8, 48, 58, 76, 149, 209, 224]
RS.AN-4	Incidents are categorized consistent with response plans.	
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	[75, 76, 209]
RS.MI-1	Incidents are contained.	[1, 2, 73, 75, 76, 88, 149, 156, 193, 209, 240]
RS.MI-2	Incidents are mitigated.	[2, 3, 73, 75, 76, 88, 149, 156, 193, 209, 217, 224, 238, 240]
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks.	[59, 76, 149, 209]
RS.IM-1	Response plans incorporate lessons learned.	
RS.IM-2	Response strategies are updated.	[75, 76, 149, 156]
Function: Recover		
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident.	[8, 75, 76, 149, 156, 193, 224]
RC.IM-1	Recovery plans incorporate lessons learned.	[76, 149, 224]
RC.IM-2	Recovery strategies are updated.	[75, 76, 149, 224]
RC.CO-1	Public relations are managed.	
RC.CO-2	Reputation is repaired after an incident.	
RC.CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	[8, 75, 76]

References

[1] Fatemeh Akbarian, Emma Fitzgerald, and Maria Kihl. 2020. Intrusion detection in digital twins for industrial control systems. In *2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. 1–6.

[2] Fatemeh Akbarian, William Tärneberg, Emma Fitzgerald, and Maria Kihl. 2021. A security framework in digital twins for cloud-based industrial control systems: Intrusion detection and mitigation. In *IEEE International Conference on Emerging Technologies and Factory Automation*. 01–08.

[3] Fatemeh Akbarian, William Tärneberg, Emma Fitzgerald, and Maria Kihl. 2023. Detecting and mitigating actuator attacks on cloud control systems through digital twins. In *2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. 1–6.

[4] Abimbola Akerele, William Leppert, Shionta Somerville, and Guy-Alain Amoussou. 2023. The digital twins incident response to improve the security of power system critical infrastructure. *J. Comput. Sci. Coll.* 39, 3 (2023), 86–99.

[5] Zeeshan Ali, Raheleh Biglari, Joachim Denil, Joost Mertens, Milad Poursoltan, and Mamadou Kaba Traoré. 2024. From modeling and simulation to digital twin: Evolution or revolution? *Simulation* 100, 7 (2024), 751–769. DOI: https://doi.org/10.1177/00375497241234680

[6] Tejasvi Alladi, Vinay Chamola, and Sherali Zeadally. 2020. Industrial control systems: Cyberattack trends and countermeasures. *Comput. Commun.* 155, 0140-3664 (2020), 1–8.

[7] David Allison, Paul Smith, and Kieran McLaughlin. 2022. Digital twin-enhanced methodology for training edge-based models for cyber security applications. In *2022 IEEE 20th International Conference on Industrial Informatics (INDIN)*. 226–232.

[8] David Allison, Paul Smith, and Kieran Mclaughlin. 2023. Digital twin-enhanced incident response for cyber-physical systems. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES'23)*.

[9] Sadeq Almeaibed, Saba Al-Rubaye, Antonios Tsourdos, and Nicolas P. Avdelidis. 2021. Digital twin analysis to promote safety and security in autonomous vehicles. *IEEE Commun. Stand. Mag.* 5, 1 (2021), 40–46.

[10] Daniel Anthony Howard, Zheng Ma, Jesper Mazanti Aaslyng, and Bo Norregaard Jorgensen. 2020. Data architecture for digital twin of commercial greenhouse production. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*. 1–7.

[11] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1093–1110.

[12] Varsha Arya, Akshat Gaurav, Brij B. Gupta, Ching-Hsien Hsu, and Hojjat Baghban. 2023. Detection of malicious node in VANETs using digital twin. In *Big Data Intelligence and Computing*, Ching-Hsien Hsu, Mengwei Xu, Hung Cao, Hojjat Baghban, and A. B. M. Shawkat Ali (Eds.). Vol. 13864. 204–212.

[13] Giacomo Assenza, Valerio Cozzani, Francesco Flammini, Nadezhda Gotcheva, Tommy Gustafsson, Anders Hansson, Jouko Heikkila, Matteo Iaiani, Sokratis Katsikas, Minna Nissilä, Gabriele Oliva, Eleni Richter, Maaike Roelofs, Mehdi Saman Azari, Roberto Setola, Wouter Stejin, Alessandro Tugnoli, Dolf Vanderbeek, Lars Westerdahl, Marja Ylönen, and Heather Young. 2020. White paper on industry experiences in critical information infrastructure security. In *Critical Information Infrastructures Security*, Simin Nadjm-Tehrani (Ed.). Vol. 11777. 197–207.

[14] Manolya Atalay and Pelin Angin. 2020. A digital twins approach to smart grid security testing and standardization, In International Workshop on Metrology for Industry 4.0 & IoT. *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, 435–440.

[15] Abiodun Ayodeji, Yong-kuo Liu, Nan Chao, and Li-qun Yang. 2020. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nucl. Eng. Technol.* 52, 12 (2020), 2687–2698.

[16] V. Ayyalusamy, B. Sivaneasan, N. K. Kandasamy, J. F. Xiao, K. Abidi, and A. Chandra. 2022. Hybrid digital twin architecture for power system cyber security analysis. In *IEEE PES Innovative Smart Grid Technologies*. 270–274.

[17] Mohit Bajaj and K. B. Akhilesh. 2020. Understanding the need for cybersecurity in manufacturing environment. In *Smart Technologies*, K. B. Akhilesh and Dietmar P. F. Möller (Eds.). 147–157.

[18] Efe C. Balta, Michael Pease, James Moyne, Kira Barton, and Dawn M. Tilbury. 2024. Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems. *IEEE Trans. Autom. Sci. Eng.* 21, 2 (2024), 1695–1712.

[19] Xinbo Ban, Ming Ding, Shigang Liu, Chao Chen, Jun Zhang, and Yang Xiang. 2022. TAESim: A testbed for IoT security analysis of trigger-action environment. In *Computer Security. ESORICS 2021 International Workshops*, Sokratis Katsikas, Costas Lambrinoudakis, Nora Cuppens, John Mylopoulos, Christos Kalloniatis, Weizhi Meng, Steven Furnell, Frank Pallas, Jörg Pohle, M. Angela Sasse, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Jorge Maestre Vidal, and Marco Antonio Sotelo Monge (Eds.). Vol. 13106. 218–237.

[20] Matthew Barrett. 2018. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

[21] Barbara Rita Barricelli, Elena Casiraghi, and Daniela Fogli. 2019. A survey on digital twin: Definitions, characteristics, applications, and design implications. *IEEE Access* 7 (2019), 167653–167671.

[22] Adrien Becue, Yannick Fourastier, Isabel Praca, Alexandre Savarit, Claude Baron, Baptiste Gradussofs, Etienne Pouille, and Carsten Thomas. 2018. Cyberfactory#1 — securing the industry 4.0 with cyber-ranges and digital twins. *International Workshop on Factory Communication Systems* (2018), 1–4.

[23] Adrien Bécue, Martin Praddaude, Eva Maia, Nicolas Hogrel, Isabel Praça, and Reda Yaich. 2022. Digital twins for enhanced resilience: Aerospace manufacturing scenario. In *Advanced Information Systems Engineering Workshops*, Jennifer Horkoff, Estefania Serral, and Jelena Zdravkovic (Eds.). Springer International Publishing, Cham, 107–118.

[24] Stefan Biffl, Matthias Eckhart, Arndt Lüder, and Edgar Weippl. 2019. Conclusion and outlook on security and quality of complex cyber-physical systems engineering. In *Security and Quality in Cyber-Physical Systems Engineering*, Stefan Biffl, Matthias Eckhart, Arndt Lüder, and Edgar Weippl (Eds.). 497–507.

[25] Ron Bitton, Tomer Gluck, Orly Stan, Masaki Inokuchi, Yoshinobu Ohta, Yoshiyuki Yamada, Tomohiko Yagyu, Yuval Elovici, and Asaf Shabtai. 2018. Deriving a cost-effective digital twin of an ics to facilitate security evaluation, In Computer Security, Javier López, Jianying Zhou, and Miguel Soriano (Eds.). *Ifip. Trans. A.* 11098, 533–554.

[26] Fabian Böhm, Marietheres Dietz, Tobias Preindl, and Günther Pernul. 2021. Augmented reality and the digital twin: State-of-the-art and perspectives for cybersecurity. *Journal of Cybersecurity and Privacy* 1, 3 (2021), 519–538.

[27] James Bore. 2020. Insider threat. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Hamid Jahankhani, Stefan Kendzierskyj, Nishan Chelvachandran, and Jaime Ibarra (Eds.). 431–450.

[28] Tobias Brockhoff, Malte Heithoff, Istvan Koren, Judith Michael, Jerome Pfeiffer, Bernhard Rumpe, Merih Seran Uysal, Wil M. P. Van Der Aalst, and Andreas Wortmann. 2021. Process prediction with digital twins. In *2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*. 182–187.

[29] Adrien Bécue, Eva Maia, Linda Feeken, Philipp Borchers, and Isabel Praça. 2020. A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied sciences-basel* 10, 13 (2020), 4482.

[30] Umit Cali, Berhane Darsene Dimd, Parisa Hajialigol, Amin Moazami, Sri Nikhil Gupta Gourisetti, Gabriele Lobaccaro, and Mohammadreza Aghaei. 2023. Digital twins: Shaping the future of energy systems and smart cities through cybersecurity, efficiency, and sustainability. In *2023 International Conference on Future Energy Solutions (FES)*. 1–6.

[31] Seraphin Calo, Dinesh Verma, Supriyo Chakraborty, Elisa Bertino, Emil Lupu, and Gregory Cirincione. 2018. Self-generation of access control policies. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies (SACMAT'18)*. 39–47.

[32] Claudia Campolo, Giacomo Genovese, Antonella Molinaro, and Bruno Pizzimenti. 2020. Digital twins at the edge to track mobility for maas applications. In *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT) (DS-RT'20)*. 1–6.

[33] Andrea Castellani, Sebastian Schmitt, and Stefano Squartini. 2021. Real-world anomaly detection by using digital twin systems and weakly supervised learning. *arXiv preprint arXiv:2011.06296* 17, 7 (2021), 4733–4742.

[34] Tiziana Catarci, Donatella Firmani, Francesco Leotta, Federica Mandreoli, Massimo Mecella, and Francesco Sapio. 2019. A conceptual architecture and model for smart manufacturing relying on service-based digital twins. In *2019 IEEE International Conference on Web Services (ICWS)*. 229–236.

[35] Glen Cathey, James Benson, Maanak Gupta, and Ravi Sandhu. 2021. Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems. In *Proceedings of the 3rd. IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 70–79.

[36] Nikitha Donekal Chandrashekar, Kenneth King, Denis Gračanin, and Mohamed Azab. 2023. Design & development of virtual reality empowered cyber-security training testbed for IoT systems. In *Intelligent Cybersecurity Conference*. 86–94.

[37] Yu Chen, Ziqian Zhang, and Ning Tang. 2022. Application of digital twin in the security protection of the internet of things in power system. In *Big Data and Security*, Yuan Tian, Tinghuai Ma, Muhammad Khurram Khan, Victor S. Sheng, and Zhaoqing Pan (Eds.). Vol. 1563. 218–229.

[38] Sujit Rokka Chhetri, Sina Faezi, Nafiul Rashid, and Mohammad Abdullah Al Faruque. 2018. Manufacturing supply chain and product lifecycle security in the era of industry 4.0. *Journal of Hardware and Systems Security* 2, 1 (2018), 51–68.

[39] Taejun Choi, Guangdong Bai, Ryan K. L. Ko, Naipeng Dong, Wenlu Zhang, and Shunyao Wang. 2020. An analytics framework for heuristic inference attacks against industrial control systems. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 827–835.

[40] Taejun Choi, Ryan K. L. Ko, Tapan Saha, Joshua Scarsbrook, Abigail M. Y. Koay, Shunyao Wang, Wenlu Zhang, and Connor St Clair. 2021. Plan2Defend: AI planning for cybersecurity in smart grids. In *2021 IEEE PES Innovative Smart Grid Technologies—Asia (ISGT Asia)*. 1–5.

[41] Sai Sree Laya Chukkapalli, Shaik Barakhat Aziz, Nouran Alotaibi, Sudip Mittal, Maanak Gupta, and Mahmoud Abdelsalam. 2021. Ontology driven Ai and access control systems for smart fisheries. In *ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*. 59–68.

[42] Sai Sree Laya Chukkapalli, Nisha Pillai, Sudip Mittal, and Anupam Joshi. 2021. Cyber-physical system security surveillance using knowledge graph based digital twins - a smart farming usecase. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 1–6.

[43] Tudor Cioara, Ionut Anghel, Marcel Antal, Ioan Salomie, Claudia Antal, and Arcas Gabriel Ioan. 2021. An Overview of Digital Twins Application Domains in Smart Energy Grid. In *Proceedings of the 18th International Conference on Intelligent Computer Communication and Processing (ICCP)*. 25–30.

[44] Emilia Cioroaica, Thomas Kuhn, and Barbora Buhnova. 2019. (do Not) trust in ecosystems. In *2019 IEEE/ACM 41st International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER) (ICSE-NIER'19)*. 9–12.

[45] Silvia Colabianchi, Francesco Costantino, Giulio Di Gravio, Fabio Nonino, and Riccardo Patriarca. 2021. Discussing resilience in the context of cyber physical systems. *Comput. Ind. Eng.* 160, 0360-8352 (2021), 107534.

[46] Luigi Coppolino, Roberto Nardone, Alfredo Petruolo, and Luigi Romano. 2023. Building cyber-resilient smart grids with digital twins and data spaces. *Applied Sciences-Basel* 13, 24 (2023), 13060.

[47] Luigi Coppolino, Roberto Nardone, Alfredo Petruolo, Luigi Romano, and Andrej Souvent. 2023. Exploiting digital twin technology for cybersecurity monitoring in smart grids. In *18th International Conference on Availability, Reliability and Security*.

[48] Ana Cristina Franco da Silva, Stefan Wagner, Eddie Lazebnik, and Eyal Traitel. 2021. Using a Cyber Digital Twin for Continuous Automotive Security Requirements Verification.

[49] Daniela S. Cruzes and Tore Dybå. 2011. Research synthesis in software engineering: A tertiary study. *Inform. Software Tech.* 53, 5 (2011), 440–455. Special Section on Best Papers from XP2010.

[50] Ulrich Dahmen, Tobias Osterloh, and Jürgen Roßmann. 2022. Verification and validation of digital twins and virtual testbeds. *International Journal of Advances in Applied Sciences* 11, 1 (2022), 47–64. DOI: https://doi.org/10.11591/ijaas.v11.i1.pp47-64

[51] V. Damjanovic-Behrendt. 2018. A digital twin architecture for security, privacy and safety. ercim news no. 115, special issue "digital twins. *A Digital Twin Architecture for Security, Privacy and Safety. ERCIM News No. 115, Special Issue "Digital Twins* (2018).

[52] Violeta Damjanovic-Behrendt. 2018. A digital twin-based privacy enhancement mechanism for the automotive industry. *2018 International Conference on Intelligent Systems (IS)* 115 (2018), 272–279.

[53] William Danilczyk, Yan Sun, and Haibo He. 2019. Angel: An intelligent digital twin framework for microgrid security, In 2019 North American Power Symposium (NAPS). *2019 North American Power Symposium (NAPS)*, 1–6.

[54] William Danilczyk, Yan Lindsay Sun, and Haibo He. 2021. Smart grid anomaly detection using a deep learning digital twin. In *2020 52nd North American Power Symposium (NAPS)*. 1–6.

[55] Debak Das. 2019. *An Indian Nuclear Power Plant Suffered a Cyberattack. Here's what you Need to Know*. Retrieved from https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/ Retrieved June 28, 2021 from

[56] Danielle Dauphinais, Michael Zylka, Harris Spahic, Farhan Shaik, Jingda Yang, Isabella Cruz, Jakob Gibson, and Ying Wang. 2023. Automated vulnerability testing and detection digital twin framework for 5G systems. In *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*. 308–310.

[57] Jorge David de Hoz Diego, Anastasios Temperekidis, Panagiotis Katsaros, and Charalambos Konstantinou. 2022. An IoT digital twin for cyber-security defence based on runtime verification. In *Leveraging Applications of Formal Methods, Verification and Validation. Verification Principles (Lecture Notes in Computer Science, Vol. 13701)*, Tiziana Margaria and Bernhard Steffen (Eds.). 556–574.

[58] Marietheres Dietz, Ludwig Englbrecht, and Günther Pernul. 2021. Enhancing industrial control system forensics using replication-based digital twins. In *Advances in Digital Forensics XVII*, Gilbert Peterson and Sujeet Shenoi (Eds.). Vol. 612. 21–38.

[59] Marietheres Dietz, Leon Hageman, Constantin von Hornung, and Günther Pernul. 2022. Employing digital twins for security-by-design system testing. In *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (Sat-CPS'22)*. 97–106.

[60] Marietheres Dietz and Günther Pernul. 2020. Digital twin: Empowering enterprises towards a system-of-systems approach. *Bus. Inform. Syst. Eng+.+* 62, 2 (2020), 179–184.

[61] Marietheres Dietz and Gunther Pernul. 2020. Unleashing the digital twin's potential for ics security. *IEEE Security & Privacy* 18, 4 (2020), 20–27.

[62] Marietheres Dietz, Daniel Schlette, and Gunther Pernul. 2022. Harnessing digital twin security simulations for systematic cyber threat intelligence. In *46th IEEE Annual Computers, Software, and Applications Conference*, Hong Va Leong, Sahra Sedigh Sarvestani, Yuuichi Teranishi, Alfredo Cuzzocrea, Hiroki Kashiwazaki, Dave Towey, Ji-Jiang Yang, and Hossain Shahriar (Eds.). 789–797.

[63] Marietheres Dietz, Manfred Vielberth, and Günther Pernul. 2020. Integrating digital twin security simulations in the security operations center. In *15th International Conference on Availability, Reliability and Security*, Melanie Volkamer and Christian Wressnegger (Eds.). 18:1–18:9.

[64] Matthias Eckhart, Bernhard Brenner, Andreas Ekelhart, and Edgar R. Weippl. 2019. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. *J. Internet Serv. Inf. Secur.* 9, 3 (2019), 52–73.

[65] Matthias Eckhart and Andreas Ekelhart. 2018. 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, Vol. 18)*. 36–47.

[66] Matthias Eckhart and Andreas Ekelhart. 2018. Towards security-aware virtual environments for digital twins, In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, CPSS@AsiaCCS 2018, Incheon, Republic of Korea, June 04-08, 2018*, Dieter Gollmann and Jianying Zhou (Eds.). *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security -CPSS'18*, 61–72.

[67] Matthias Eckhart and Andreas Ekelhart. 2019. Digital twins for cyber-physical systems security: State of the art and outlook. In *Security and Quality in Cyber-Physical Systems Engineering*, Stefan Biffl, Matthias Eckhart, Arndt Lüder, and Edgar Weippl (Eds.). 383–412.

[68] Matthias Eckhart, Andreas Ekelhart, David Allison, Magnus Almgren, Katharina Ceesay-Seitz, Helge Janicke, Simin Nadjm-Tehrani, Awais Rashid, and Mark Yampolskiy. 2023. Security-enhancing digital twins: Characteristics, indicators, and future perspectives. *IEEE Security & Privacy* 21, 6 (2023), 64–75.

[69] Matthias Eckhart, Andreas Ekelhart, and Edgar Weippl. 2019. Enhancing cyber situational awareness for cyber-physical systems through digital twins. In *Proceedings of the 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. 1222–1225.

[70] Ian Elsby. 2019. *Digital Twin Does More Than Designing, Analysing and Processing; It's the Cyber Attack Combatant!* Retrieved from https://news.siemens.co.uk/news/digital-twin-does-more-than-designing-analysing-and-processing-its-the-cyber-attack-combatant Retrieved June 28, 2021 from

[71] Philip Empl, Henric Hager, and Günther Pernul. 2023. Digital twins for IoT security management. In *Data and Applications Security and Privacy XXXVII: 37th Annual IFIP WG 11.3 Conference, DBSec 2023, Sophia-Antipolis, France, July 19–21, 2023, Proceedings* (Sophia-Antipolis, France). Springer-Verlag, Berlin, Heidelberg, 141–149.

[72] Philip Empl and Günther Pernul. 2021. A flexible security analytics service for the industrial iot. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SAT-CPS'21)*. 23–32.

[73] Philip Empl and Günther Pernul. 2023. Digital-twin-based security analytics for the internet of things. *Information* 14, 2 (2023).

[74] Philip Empl, Daniel Schlette, Lukas Stöger, and Günther Pernul. 2023. Generating ICS vulnerability playbooks with open standards. *Int. J. Inf. Secur.* 23 (2023), 1215–1230.

[75] Philip Empl, Daniel Schlette, Daniel Zupfer, and Günther Pernul. 2022. SOAR4IoT: Securing IoT assets with digital twins. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES'22)*.

[76] Gregory Epiphaniou, Mohammad Hammoudeh, Hu Yuan, Carsten Maple, and Uchenna Ani. 2023. Digital twins in cyber effects modelling of IoT/CPS points of low resilience. *Simul. Model. Pract. Th.* 125, 1569-190X (2023), 102744.

[77] Rajiv Faleiro, Lei Pan, Shiva Raj Pokhrel, and Robin Doss. 2022. Digital twin for cybersecurity: Towards enhancing cyber resilience. In *Broadband Communications, Networks, and Systems*, Wei Xiang, Fengling Han, and Tran Khoa Phan (Eds.). Springer International Publishing, Cham, 57–76.

[78] Chris Farnell, Estefano Soria, Justin Jackson, and H. Alan Mantooth. 2021. Cyber protection of grid-connected devices through embedded online security. In *2021 IEEE Design Methodologies Conference (DMC)*. 1–6.

[79] Apostolos P. Fournaris, Andreas Komninos, Aris S. Lalos, Athanasios P. Kalogeras, Christos Koulamas, and Dimitrios Serpanos. 2019. Design and run-time aspects of secure cyber-physical systems. In *Security and Quality in Cyber-Physical Systems Engineering*, Stefan Biffl, Matthias Eckhart, Arndt Lüder, and Edgar Weippl (Eds.). 357–382.

[80] Guillermo Francia and Gregory Hall. 2021. Digital twins for industrial control systems security. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. 801–805.

[81] Ana Cristina Franco da Silva, Stefan Wagner, Eddie Lazebnik, and Eyal Traitel. 2023. Using a cyber digital twin for continuous automotive security requirements verification. *IEEE Softw.* 40, 1 (2023), 69–76.

[82] Benjamin Fraser, Saba Al-Rubaye, Sohaib Aslam, and Antonios Tsourdos. 2021. Enhancing the security of unmanned aerial systems using digital-twin technology and intrusion detection. In *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*. 1–10.

[83] Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow. 2020. Digital twin: Enabling technologies, challenges and open research. *IEEE Access* 8 (2020), 108952–108971.

[84] Brian Fung and Geneva Sands. 2021. *Ransomware attackers used compromised password to access Colonial Pipeline network*. Retrieved from https://edition.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html Retrieved June 28, 2021 from

[85] Zach Furness. 2019. *Perspectives on Securing Cyber Physical Systems*. 287–299.

[86] Sebastian Gajek, Michael Lees, and Christoph Jansen. 2020. Iiot and cyber-resilience. *AI & SOCIETY* 36, 3 (2020), 725–735.

[87] Rogelio GAmez Díaz, Qingtian Yu, Yezhe Ding, Fedwa Laamarti, and Abdulmotaleb El Saddik. 2020. Digital twin coaching for physical activities: A survey. *Sensors-Basel.* 20, 20 (2020), 5936.

[88] Humberto E. Garcia, Steven E. Aumeier, Ahmad Y. Al-Rashdan, and Bri L. Rolston. 2020. Secure embedded intelligence in nuclear systems: Framework and methods. *Ann. Nucl. Energy* 140, 0306-4549 (2020), 107261.

[89] Akshat Gaurav, Brij B. Gupta, Kwok Tai Chui, Varsha Arya, and Elhadj Benkhelifa. 2023. A DDoS attack detection system for industry 5.0 using digital twins and machine learning. In *Global Conference on Consumer Electronics*. 1019–1022.

[90] General Electric Research. 2017. *Digital Ghost: Real-Time, Active Cyber Defense*. Retrieved from https://www.ge.com/research/offering/digital-ghost-real-time-active-cyber-defense Retrieved June 28, 2021 from

[91] Edward Glaessgen and David Stargel. 2012. The digital twin paradigm for future NASA and U.S. air force vehicles. In *Proceedings of the 53rd. AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*. American Institute of Aeronautics and Astronautics.

[92] M. Glawe, L. Feeken, B. Wudka, C.-Y. Kao, E. Mirzaei, T. Weinhold, and A. Szanto. 2020. Towards resilient factories of future—defining required capabilities for a resilient factory of future. (2020), 755–768.

[93] Gerald Glocker. 2019. *A Primer on Digital Twins in the IoT*. Retrieved from https://blog.bosch-si.com/bosch-iot-suite/a-primer-on-digital-twins-in-the-iot/ Retrieved June 28, 2021 from

[94] Jose Gomez, Elie F. Kfoury, Jorge Crichigno, and Gautam Srivastava. 2023. A survey on network simulators, emulators, and testbeds used for research and education. *Comput. Netw.* 237, 1389-1286 (2023), 110054. DOI: https://doi.org/10.1016/j.comnet.2023.110054

[95] Janis Grabis, Janis Stirna, and Jelena Zdravkovic. 2021. A capability based method for development of resilient digital services. In *Enterprise Information Systems*, Joaquim Filipe, Michał Śmiałek, Alexander Brodsky, and Slimane Hammoudi (Eds.). Vol. 417. 498–516.

[96] Chiara Grasselli, Andrea Melis, Roberto Girau, and Franco Callegati. 2023. A digital twin for enhanced cybersecurity in connected vehicles. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)*. 1–4.

[97] Chiara Grasselli, Andrea Melis, Lorenzo Rinieri, Davide Berardi, Giacomo Gori, and Amir Al Sadi. 2022. An industrial network digital twin for enhanced security of cyber-physical systems. In *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. 1–7.

[98] Michael Grieves and John Vickers. 2017. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. *Transdisciplinary Perspectives on Complex Systems* (2017), 85–113.

[99] Amal Guittoum, Francois Aïssaoui, Sébastien Bolle, Fabienne Boyer, and Noel De Palma. 2023. Inferring threatening IoT dependencies using semantic digital twins toward collaborative IoT device management. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (SAC'23)*. 1732–1741.

[100] Jiajie Guo, Muhammad Bilal, Yuying Qiu, Cheng Qian, Xiaolong Xu, and Kim-Kwang Raymond Choo. 2022. Survey on digital twins for internet of vehicles: Fundamentals, challenges, and opportunities. *Digital Communications and Networks* 10, 2 (2022), 237–247.

[101] Yun Guo, Xinxin Lou, Edita Bajramovic, and Karl Waedt. 2020. Cybersecurity risk analysis and technical defense architecture: Research of ICS in nuclear power plant construction stage. In *3rd IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts*.

[102] Yun Guo, Aijun Yan, and Junjie Wang. 2021. Cyber security risk analysis of physical protection systems of nuclear power plants and research on the cyber security test platform using digital twin technology. In *2021 International Conference on Power System Technology*. 1889–1892.

[103] Deepti Gupta, Olumide Kayode, Smriti Bhatt, Maanak Gupta, and Ali Saman Tosun. 2021. Hierarchical Federated Learning Based Anomaly Detection Using Digital Twins for Smart Healthcare. In *Proceedings of the 7th International Conference on Collaboration and Internet Computing (CIC)*.

[104] Deepti Gupta, Shafika Showkat Moni, and Ali Saman Tosun. 2023. Integration of digital twin and federated learning for securing vehicular internet of things. In *International Conference on Research in Adaptive and Convergent Systems*.

[105] Ethan Hadar, Dmitry Kravchenko, and Alexander Basovskiy. 2020. Cyber digital twin simulator for automatic gathering and prioritization of security controls' requirements. In *2020 IEEE 28th International Requirements Engineering Conference (RE)*, Travis D. Breaux, Andrea Zisman, Samuel Fricker, and Martin Glinz (Eds.). 250–259.

[106] Kim Hammar and Rolf Stadler. 2023. Digital twins for security automation. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*. 1–6.

[107] Mohammad Hammoudeh. 2020. Blockchain, internet of things and digital twins in trustless security of critical national infrastructure. In *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS) (ICFNDS'20)*. 43:1.

[108] Jiaxuan Han, Qiteng Hong, Zhiwang Feng, Mazheruddin Syed, Graeme Burt, and Campbell Booth. 2022. Design and implementation of a real-time hardware-in-the-loop platform for prototyping and testing digital twins of distributed energy resources. *Energies* 15, 18 (2022), 6629.

[109] George Hatzivasilis, Sotiris Ioannidis, Michail Smyrlis, George Spanoudakis, Fulvio Frati, Chiara Braghin, Ernesto Damiani, Hristo Koshutanski, George Tsakirakis, Torsten Hildebrandt, Ludger Goeke, Sebastian Pape, Oleg Blinder, Michael Vinov, George Leftheriotis, Martin Kunc, Fotis Oikonomou, Giovanni Magilo, Vito Petrarolo, Antonio Chieti, and Robert Bordianu. 2021. The threat-arrest cyber range platform. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 422–427.

[110] Zhongyuan Hau, John Henry Castellanos, and Jianying Zhou. 2020. Evaluating cascading impact of attacks on resilience of industrial control systems: A design-centric modeling approach. In *Proceedings of the 6th ACM on Cyber-Physical System Security Workshop (CPSS'20)*. 42–53.

[111] Rui He, Guoming Chen, Che Dong, Shufeng Sun, and Xiaoyu Shen. 2019. Data-driven digital twin technology for optimized control in process systems. *ISA Transactions* 95, 0019-0578 (2019), 221–234.

[112] Siemens Healthineers. 2019. *The Value of Digital Twin Technology*. Technical Report 7144 0819. Siemens Healthcare GmbH, Erlangen, Germany.

[113] David Holmes, Maria Papathanasaki, Leandros Maglaras, Mohamed Amine Ferrag, Surya Nepal, and Helge Janicke. 2021. Digital twins and cyber security—solution or challenge?. In *2021 South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference*. 1–8.

[114] Tareq Hossen, Mehmetcan Gursoy, and Behrooz Mirafzal. 2021. Digital twin for self-security of smart inverters. In *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*. 713–718.

[115] Tareq Hossen, Dushyant Sharma, and Behrooz Mirafzal. 2021. Smart inverter twin model for anomaly detection. In *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*. 1–6.

[116] Zhe Hou, Qinyi Li, Ernest Foo, Jin Song Dong, and Paulo de Souza. 2022. A digital twin runtime verification framework for protecting satellites systems from cyber attacks. In *2022 26th International Conference on Engineering of Complex Computer Systems (ICECCS)*. 117–122.

[117] Sihan Huang, Guoxin Wang, Yan Yan, and Xiongbing Fang. 2020. Blockchain-based data management for digital twin of product. *J. Manuf. Syst.* 54, 0278-6125 (2020), 361–371.

[118] Jithin Jagannath, Keyvan Ramezanpour, and Anu Jagannath. 2022. Digital twin virtualization with machine learning for IoT and beyond 5G networks: Research directions for security and optimal control. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning*. abs/2204.01950 (2022), 81–86.

[119] Sergej Jakovlev, Tomas Eglynas, Miroslav Voznak, Pavol Partila, Jaromir Tovarek, Mindaugas Jusis, Edvinas Pocevicius, and Zane Purlaura. 2021. Development of an intelligent digital twins framework for secure container terminal operations. In *2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*. 1–4.

[120] David Jones, Chris Snider, Aydin Nassehi, Jason Yon, and Ben Hicks. 2020. Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology* 29, 1755-5817 (2020), 36–52.

[121] Siavash H. Khajavi, Müge Tetik, Zixuan Liu, Pasi Korhonen, and Jan Holmström. 2023. Digital twin for safety and security: Perspectives on building lifecycle. *IEEE Access* 11 (2023), 52339–52356.

[122] Mohammed Masum Siraj Khan, Jairo Giraldo, and Masood Parvania. 2023. Real-time cyber attack localization in distribution systems using digital twin reference model. *IEEE Transactions on Power Delivery* 38, 5 (2023), 3238–3249.

[123] Mehdi Kherbache, Moufida Maimour, and Eric Rondeau. 2022. Network digital twin for the industrial internet of things. In *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. 573–578.

[124] Andreas Kind. 2021. The power of industrial cybersecurity. *Digitale Welt* 5, 1 (2021), 18–21.

[125] Dan Klein and Gal Engelberg. 2021. *Get Ahead of Cyberattacks with Digital Twins*. Retrieved June 28, 2021 from https://www.accenture.com/us-en/blogs/technology-innovation/klein-engelberg-get-ahead-of-cyberattacks-with-digital-twins

[126] Nickolaos Koroniotis, Nour Moustafa, Francesco Schiliro, Praveen Gauravaram, and Helge Janicke. 2021. The sair-IIoT cyber testbed as a service: A novel cybertwins architecture in IIoT-based smart airports. *IEEE Trans. Intell. Transp. Syst.* 24, 2 (2021), 1–14.

[127] Prabhakar Krishnan, Kurunandan Jain, Rajkumar Buyya, Pandi Vijayakumar, Anand Nayyar, Muhammad Bilal, and Houbing Song. 2021. Mud-based behavioral profiling security framework for software-defined Iot networks. *IEEE Internet Things J.* 9, 9 (2021), 1–1.

[128] Priya R. Krishnan and Josephkutti Jacob. 2021. Asset management and finite element analysis in smart grid. In *2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA)*. 497–503.

[129] Werner Kritzinger, Matthias Karner, Georg Traar, Jan Henjes, and Wilfried Sihn. 2018. Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine* 51, 11 (2018), 1016–1022. 16th IFAC Symposium on Information Control Problems in Manufacturing.

[130] Jens Krüger. 2020. *Digital Twin for Maximum Cyber Security*. Technical Report. NTT DATA Deutschland GmbH, Munich, Germany.

[131] K. Kruger, A. J. H. Redelinghuys, A. H. Basson, and O. Cardin. 2021. Past and future perspectives on digital twin research at sohoma. In *Service Oriented, Holonic and Multi-Agent Manufacturing Systems for Industry of the Future*, Theodor Borangiu, Damien Trentesaux, Paulo Leitão, Olivier Cardin, and Samir Lamouri (Eds.). Vol. 952. 81–98.

[132] V. M. Krundyshev. 2020. Ensuring cybersecurity of digital production using modern neural network methods. *Autom. Control Comput. Sci.* 54, 8 (2020), 786–792.

[133] Prabhat Kumar, Randhir Kumar, Abhinav Kumar, A. Antony Franklin, Sahil Garg, and Satinder Singh. 2022. Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network. *IEEE Trans. Netw. Sci. Eng.* (2022), 1–13.

[134] Nandha Kumar Kandasamy, Sarad Venugopalan, Tin Kit Wong, and Leu Junming Nicholas. 2021. Epictwin: An electric power digital twin for cyber security testing, research and education. *Computers and Electrical Engineering* 101 (2021).

[135] Andre Kummerow, Cristian Monsalve, Dennis Rosch, Kevin Schafer, and Steffen Nicolai. 2020. Cyber-physical data stream assessment incorporating digital twins in future power systems. In *2020 International Conference on Smart Energy Systems and Technologies (SEST)*. 1–6.

[136] Andre Kummerow, Steffen Nicolai, Christoph Brosinsky, Dirk Westermann, Andre Naumann, and Marc Richter. 2020. Digital-twin based services for advanced monitoring and control of future power systems. In *2020 IEEE Power Energy Society General Meeting (PESGM)*. 1–5.

[137] Heikki Laaki, Yoan Miche, and Kari Tammi. 2019. Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery. *IEEE Access* 7 (2019), 20325–20336.

[138] Zeqi Lai, Yangtao Deng, Hewu Li, Qian Wu, and Qi Zhang. 2023. Space digital twin for secure satellite internet: Vulnerabilities, methodologies and future directions. *IEEE Netw.* 38, 1 (2023), 1–1.

[139] Zhongcheng Lei, Hong Zhou, Wenshan Hu, Guo-Ping Liu, Shiqi Guan, and Xingle Feng. 2021. Towards a web-based digital twin thermal power plant. *IEEE Trans. Ind. Inf.* (2021).

[140] Qian Li, Dongdong Huo, and Lizhong Jiang. 2022. A digital twin system for monitoring the security of theatrical stages. In *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*. 2224–2230.

[141] Kendrik Yan Hong Lim, Pai Zheng, and Chun-Hsien Chen. 2019. A state-of-the-art survey of digital twin: Techniques, engineering product lifecycle management and business innovation perspectives. *J. Intell. Manuf.* 31, 6 (2019), 1313–1337.

[142] Yu-Zheng Lin, Sicong Shao, Md Habibor Rahman, Mohammed Shafae, and Pratik Satam. 2023. DT4I4-secure: Digital twin framework for industry 4.0 systems security. In *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. 0200–0209.

[143] Mengnan Liu, Shuiliang Fang, Huiyue Dong, and Cunzhi Xu. 2021. Review of digital twin about concepts, technologies, and industrial applications. *J. Manuf. Syst.* 58 (2021), 346–361. Digital Twin towards Smart Manufacturing and Industry 4.0.

[144] Zhen Liu, QingLei Zhang, Jianguo Duan, and Dong Liu. 2022. Digital twin–based testing process management for large and complex equipment components. *International Journal of Advanced Manufacturing Technology* 121, 5-6 (2022), 3143–3161.

[145] Salvador Llopis Sanchez, Robert Mazzolin, Ioannis Kechaoglou, Douglas Wiemer, Wim Mees, and Jean Muylaert. 2020. Cybersecurity space operation center: Countering cyber threats in the space domain. In *Handbook of Space Security*, Kai-Uwe Schrogl (Ed.). 921–939.

[146] Andreas Locklin, Manuel Muller, Tobias Jung, Nasser Jazdi, Dustin White, and Michael Weyrich. 2020. Digital twin for verification and validation of industrial automation systems—a survey. In *25th International Conference on Emerging Technologies and Factory Automation*, Vol. 1. 851–858.

[147] Javier Lopez, Juan E. Rubio, and Cristina Alcaraz. 2021. Digital twins for intelligent authorization in the B5g-enabled smart grid. *IEEE Wirel. Commun.* 28, 2 (2021), 48–55.

[148] Tom H. Luan, Ruhan Liu, Longxiang Gao, Rui Li, and Haibo Zhou. 2021. The paradigm of digital twin communications. *arXiv preprint arXiv:2105.07182* (2021).

[149] Rivera Luis F., Villegas Norha M., Tamura Gabriel, Müller Hausi A., Watts Ian, Erpenbach Eric, Shwartz Laura, and Liu Xiaotong. 2023. Using digital twins for software change risk assessment toward proactive AIOps. In *Proceedings of the 33rd Annual International Conference on Computer Science and Software Engineering (CASCON'23)*. 211–216.

[150] Azad M. Madni. 2021. Mbse testbed for rapid, cost-effective prototyping and evaluation of system modeling approaches. *Applied Sciences-Basel* 11, 5 (2021), 2321.

[151] David Maher. 2018. On software standards and solutions for a trusted internet of things. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.

[152] Laurent Maillet-Contoz, Emmanuel Michel, Mario Diaz Nava, Paul-Emmanuel Brun, Kevin Lepretre, and Guillemette Massot. 2020. End-to-end security validation of iot systems based on digital twins of end-devices. In *2020 Global Internet of Things Summit (GIoTS)*. 1–6.
[153] Stefan Marksteiner, Slava Bronfman, Markus Wolf, and Eddie Lazebnik. 2021. Using cyber digital twins for automated automotive cybersecurity testing. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 123–128.
[154] Beatriz F. Martins, Lenin Serrano, José F. Reyes, José Ignacio Panach, Oscar Pastor, and Benny Rochwerger. 2020. Conceptual characterization of cybersecurity ontologies. In *The Practice of Enterprise Modeling*, Janis Grabis and Dominik Bork (Eds.). Vol. 400. 323–338.
[155] Massimiliano Masi, Giovanni Paolo Sellitto, Helder Aranha, and Tanja Pavleska. 2023. Securing critical infrastructures with a cybersecurity digital twin. *Softw. Syst. Model.* 22, 2 (2023), 689–707.
[156] Aditya P. Mathur. 2023. Reconfigurable digital twin to support research, education, and training in the defense of critical infrastructure. *IEEE SECURITY & PRIVACY* 21, 4 (2023), 51–60.
[157] Roberto Minerva, Gyu Myoung Lee, and Noel Crespi. 2020. Digital twin in the iot context: A survey on technical features, scenarios, and architectural models. In *Proceedings of the IEEE*, Vol. 108. 1785–1824.
[158] Carlos Miskinis. 2018. *Incorporating Digital Twin into Internet Cyber Security—Creating a Safer Future*. Retrieved from https://www.challenge.org/insights/digital-twin-cyber-security/ Retrieved June 28, 2021 from
[159] Saurabh Mittal, Andreas Tolk, Andrew Pyles, Nicolas Van Balen, and Kevin Bergollo. 2019. Digital twin modeling, co-simulation and cyber use-case inclusion methodology for Iot systems. In *2019 Winter Simulation Conference (WSC) (WSC'19)*. 2653–2664.
[160] Alvaro Cárdenas Mora, Simin Nadjm-Tehrani, Edgar Weippl, and Matthias Eckhart. 2022. Digital twins for cyber-physical systems security (dagstuhl seminar 22171). *Dagstuhl Reports* 12, 4 (2022), 54–71.
[161] Fereidoun Moradi, Bahman Pourvatan, Sara Abbaspour Asadollah, and Marjan Sirjani. 2024. Tiny twins for detecting cyber-attacks at runtime using concise rebeca time transition system. *J. Parallel Distr. Com.* 184, 0743-7315 (2024), 104780.
[162] Jose Andre Morales, Thomas P. Scanlon, Aaron Volkmann, Joseph Yankel, and Hasan Yasar. 2020. Security impacts of sub-optimal devsecops implementations in a highly regulated environment. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*.
[163] Evandro Pioli Moro. 2021. Semantic digital twins: Security and scale for constrained Iot devices. (2021).
[164] Valentin Mullet, Patrick Sondi, and Eric Ramat. 2021. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access* 9 (2021), 23235–23263.
[165] Andres Murillo, Riccardo Taormina, Nils Tippenhauer, and Stefano Galelli. 2020. Co-simulating physical processes and network data for high-fidelity cyber-security experiments. In *Sixth Annual Industrial Control System Security (ICSS) Workshop (ICSS 2020)*. 13–20.
[166] Engineering National Academies of Sciences and Medicine. 2023. Foundational research gaps and future directions for digital twins. (2023). Retrieved from https://www.nationalacademies.org/our-work/foundational-research-gaps-and-future-directions-for-digital-twins Available at:.
[167] S. Neethirajan and B. Kemp. 2021. Digital Twins in Livestock Farming. *Animals* 11 (2021), 1008.
[168] Elisa Negri, Luca Fumagalli, and Marco Macchi. 2017. A review of the roles of digital twin in CPS-based production systems. *Procedia Manufacturing* 11, 2351-9789 (2017), 939–948. 27th International Conference on Flexible Automation and Intelligent Manufacturing.
[169] Luong Nguyen, Mariana Segovia, Wissam Mallouli, Edgardo Montes de Oca, and Ana R. Cavalli. 2022. Digital twin for IoT environments: A testing and simulation tool. In *Quality of Information and Communications Technology*, Antonio Vallecillo, Joost Visser, and Ricardo Pérez-Castillo (Eds.). Vol. 1621. 205–219.
[170] Maria Nintsiou, Elisavet Grigoriou, Paris Alexandros Karypidis, Theocharis Saoulidis, Eleftherios Fountoukidis, and Panagiotis Sarigiannidis. 2023. Threat intelligence using digital twin honeypots in cybersecurity. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. 530–537.
[171] Juan C. Olivares-Rojas, Enrique Reyes-Archundia, Jose A. Gutierrez-Gnecchi, Ismael Molina-Moreno, Jaime Cerda-Jacobo, and Arturo Mendez-Patino. 2021. Towards cybersecurity of the smart grid using digital twins. *IEEE Internet Computing* 26, 3 (2021), 52–57.
[172] Vittorio Orbinato. 2021. A next-generation platform for cyber range-as-a-service. In *2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. 314–318.
[173] Guy Paré, Marie-Claude Trudel, Mirou Jaana, and Spyros Kitsiou. 2015. Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management* 52, 2 (2015), 183–199.
[174] Abhi Patel, Tim Schenk, Steffi Knorn, Heiko Patzlaff, Dragan Obradovic, and Andrés Botero Halblaub. 2021. Real-time, simulation-based identification of cyber-security attacks of industrial plants. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 267–272.

[175] Riccardo Patriarca, Francesco Simone, and Giulio Di Gravio. 2022. Modelling cyber resilience in a water treatment and distribution system. *Reliab. Eng. Syst. Safe.* 226 (2022), 108653.
[176] Sandeep Pirbhulal, Habtamu Abie, and Ankur Shukla. 2022. Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications. In *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*. 1–5.
[177] Sandeep Pirbhulal, Habtamu Abie, Ankur Shukla, and Basel Katt. 2023. A cognitive digital twin architecture for cybersecurity in IoT-based smart homes. In *Sensing Technology*, Nagender Kumar Suryadevara, Boby George, Krishanthi P. Jayasundera, and Subhas Chandra Mukhopadhyay (Eds.). Vol. 1035. 63–70.
[178] Iakovos Pittaras and George C. Polyzos. 2022. (POSTER) SmartTwins: Secure and auditable DLT-based digital twins for the WoT. In *2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 82–84.
[179] Abhishek Pokhrel, Vikash Katta, and Ricardo Colomo-Palacios. 2020. Digital twin for cybersecurity incident prediction: A multivocal literature review. In *Proceedings of the IEEE/ACM 42nd. International Conference on Software Engineering Workshops (ICSEW'20)*. 671–678.
[180] J. Pushpa and S. A. Kalyani. 2020. Using fog computing/edge computing to leverage digital twin. In *The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases*, Pethuru Raj and Preetha Evangeline (Eds.). Advances in Computers, Vol. 117. 51–77.
[181] Benedikt Putz, Marietheres Dietz, Philip Empl, and Günther Pernul. 2021. EtherTwin: Blockchain-based secure digital twin information management. *Inform. Process. Manag.* 58, 1 (2021), 102425.
[182] Pethuru Raj. 2021. Empowering digital twins with blockchain. *Adv. Comput.* 121, 0065-2458 (2021), 267–283.
[183] Roza Ranjbar, Eric Duviella, Lucien Etienne, and Jose-Maria Maestre. 2020. Framework for a digital twin of the canal of calais. *Procedia Comput. Sci.* 178, 877-0509 (2020), 27–37.
[184] Adil Rasheed, Omer San, and Trond Kvamsdal. 2020. Digital twin: Values, challenges and enablers from a modeling perspective. *IEEE Access* 8 (2020), 21980–22012.
[185] M. Mazhar Rathore, Syed Attique Shah, Dhirendra Shukla, Elmahdi Bentafat, and Spiridon Bakiras. 2021. The role of ai, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities. *IEEE Access* 9 (2021), 32030–32052.
[186] Elaine M. Raybourn and Ray Trechter. 2018. Applying model-based situational awareness and augmented reality to next-generation physical security systems. In *Cyber-Physical Systems Security*, Çetin Kaya Koç (Ed.). 331–344.
[187] Lúcio Henrik A. Reis, Andrés Murillo Piedrahita, Sandra Rueda, NatAlia C. Fernandes, Dianne S. V. Medeiros, Marcelo Dias Amorim, and Diogo M. F. Mattos. 2020. Unsupervised and incremental learning orchestration for cyber physical security. *Transactions on Emerging Telecommunications Technologies* 31, 7 (2020), e4011.
[188] Michael Riegler and Johannes Sametinger. 2021. Multi-mode systems for resilient security in industry 4.0. *Procedia Comput. Sci.* 180, 1877-0509 (2021), 301–307.
[189] Roland Rosen, Jan Fischer, and Stefan Boschert. 2019. Next generation digital twin: An ecosystem for mechatronic systems?, In Proc. tmce. *IFAC-PapersOnLine* 52, 15, 265–270.
[190] Juan Enrique Rubio, Cristina Alcaraz, Rodrigo Roman, and Javier Lopez. 2019. Current cyber-defense trends in industrial control systems. *Comput. Secur.* 87, 0167-4048 (2019), 101561.
[191] Johnson S. A. Osho and David A. Umphress. 2022. IoT security: Modeling, development and validation of IoT. In *SAIS 2022 Proceedings*.
[192] Ahmed Saad, Samy Faddel, and Osama Mohammed. 2020. Iot-based digital twin for energy cyber-physical systems: Design and implementation. *Energies* 13, 18 (2020), 4762.
[193] Ahmed Saad, Samy Faddel, Tarek Youssef, and Osama A. Mohammed. 2020. On the implementation of Iot-based digital twin for networked microgrids resiliency against cyber attacks. *IEEE Trans. Smart Grid* 11, 6 (2020), 5138–5150. Issue 6.
[194] Zoheir Sabeur, Constantinos Marios Angelopoulos, Liam Collick, Natalia Chechina, Deniz Cetinkaya, and Alessandro Bruno. 2021. Advanced cyber and physical situation awareness in urban smart spaces. In *Advances in Neuroergonomics and Cognitive Engineering*, Hasan Ayaz, Umer Asgher, and Lucas Paletta (Eds.). Vol. 259. 428–441.
[195] Radhya Sahal, Saeed H. Alsamhi, John G. Breslin, Kenneth N. Brown, and Muhammad Intizar Ali. 2021. Digital twins collaboration for automatic erratic operational data detection in industry 4.0. *Applied Sciences* 11, 7 (2021), 3186.
[196] Najm Us Sama, Kartinah Zen, Aziz Ud Din, Nazia Azim, and Atiq Ur Rahman. 2023. Security of cloud-assisted BANs using digital twin. In *2023 13th International Conference on Information Technology in Asia (CITA)*. 37–42.
[197] Guido Schryen. 2015. Writing qualitative is literature reviews - guidelines for synthesis, interpretation, and guidance of research. *Communication of the Association for Information Systems* 37 (2015), 12.
[198] Kirill Semenkov, Vitaly Promyslov, and Alexey Poletykin. 2020. Verification of large scale control systems with hybrid digital models and digital twins. In *2020 International Russian Automation Conference (RusAutoCon)*. 325–329.
[199] Kirill Semenkov, Vitaly Promyslov, Alexey Poletykin, and Nadir Mengazetdinov. 2021. Validation of complex control systems with heterogeneous digital models in industry 4.0 framework. *Machines* 9, 3 (2021), 62.

[200] Omer Sen, Florian Schmidtke, Federico Carere, Francesca Santori, Andreas Ulbig, and Antonello Monti. 2022. Investigating the cybersecurity of smart grids based on cyber-physical twin approach. In *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 439–445.

[201] Ömer Sen, Nathalie Bleser, and Andreas Ulbig. 2023. Digital twin for evaluating detective countermeasures in smart grid cybersecurity. In *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 1–6.

[202] Karan Shah, T. V. Prabhakar, Sarweshkumar C. R., Abhishek S. V., and Vasanth Kumar T. 2021. Construction of a digital twin framework using free and open-source software programs. *IEEE Internet Comput.* 26, 5 (2021), 50–59.

[203] Andrii Shalaginov, Igor Kotsiuba, and Asif Iqbal. 2019. Cybercrime investigations in the era of smart applications: Way forward through big data. In *2019 IEEE International Conference on Big Data (Big Data)*. 4309–4314.

[204] Ramesh Chandra Sharma, Arunansu Choudhury, and Ravi Vohra. 2023. Digital twin applications toward industry 4.0: A review. *Smart Manufacturing* 3 (2023), 100041.

[205] Lei Shi, Shanti Krishnan, and Sheng Wen. 2022. Study cybersecurity of cyber physical system in the virtual environment: A survey and new direction. In *Australasian Computer Science Week 2022 (ACSW 2022)*. 46–55.

[206] Amardeep B. Shitole, Nandha Kumar Kandasamy, Lin Shen Liew, Lewin Sim, and Anh Khoa Bui. 2021. Real-time digital twin of residential energy storage system for cyber-security study. In *2021 International Conference on Smart Technologies for Power, Energy and Control*. 1–6.

[207] Datta Shoumen Palit Austin. 2017. Emergence of digital twins. *Emergence of Digital Twins* 5 (2017), 14–33.

[208] Bruno Sousa, Miguel Arieiro, Vasco Pereira, João Correia, Nuno Lourenço, and Tiago Cruz. 2021. Elegant: Security of critical infrastructures with digital twins. *IEEE Access* 9 (2021), 107574–107588.

[209] Anurag Srivastava, Chen-Ching Liu, Alexandru Stefanov, Sagnik Basumallik, Mohammed M. Hussain, Baza Somda, and Vetrivel S. Rajkumar. 2024. Digital twins serving cybersecurity: More than a model: Cybersecurity as a future benefit of digital twins 2. *IEEE Power Energy Mag.* 22, 1 (2024), 61–71.

[210] Gayathri Sugumar and Aditya Mathur. 2019. Assessment of a method for detecting process anomalies using digital-twinning. In *2019 15th European Dependable Computing Conference (EDCC)*. 119–126.

[211] Sabah Suhail, Mubashar Iqbal, Rasheed Hussain, and Raja Jurdak. 2023. ENIGMA: An explainable digital twin security solution for cyber–physical systems. *Comput. Ind.* 151, 0166-3615 (2023), 103961.

[212] Sabah Suhail, Mubashar Iqbal, and Raja Jurdak. 2024. The perils of leveraging evil digital twins as security-enhancing enablers. *Commun. ACM* 67, 1 (2024), 39–42.

[213] Koen Tange, Michele De Donno, Xenofon Fafoutis, and Nicola Dragoni. 2020. A systematic survey of industrial internet of things security: Requirements and fog computing opportunities. *IEEE Communications Surveys & Tutorials* 22, 4 (2020), 2489–2520.

[214] Fei Tao, Qinglin Qi, Ang Liu, and Andrew Kusiak. 2023. Digital twin: Benefits, use cases, challenges and opportunities. *J. Manuf. Syst.* 66 (2023), 270–278.

[215] Fei Tao, Meng Zhang, and A. Y. C. Nee. 2019. Applications of digital twin. In *Digital Twin Driven Smart Manufacturing*, Fei Tao, Meng Zhang, and A.Y.C. Nee (Eds.). 29–62.

[216] Nipuna Sankalpa Thalpage and Thebona Arachchige Dushyanthi Nisansala. 2023. Exploring the opportunities of applying digital twins for intrusion detection in industrial control systems of production and manufacturing – a systematic review. In *Data Protection in a Post-Pandemic Society*, Chaminda Hewage, Yogachandran Rahulamathavan, and Deepthi Ratnayake (Eds.). 113–143.

[217] William Tärneberg, Per Skarin, Christian Gehrmann, and Maria Kihl. 2021. Prototyping intrusion detection in an industrial cloud-native digital twin. In *International Conference on Industrial Technology*.

[218] Latif U. Khan, Walid Saad, Dusit Niyato, Zhu Han, and Choong Seon Hong. 2021. Digital-twin-enabled 6g: Vision, Architectural Trends, and Future Directions. *Comm. Mag.* 60, 1 (2021), 74–80.

[219] Miriam Ugarte Querejeta, Leire Etxeberria, and Goiuria Sagardui. 2020. Towards a devops approach in cyber physical production systems using digital twins. In *International Conference on Computer Safety, Reliability, and Security*. 205–216.

[220] Stanislav Vakaruk, Alberto Mozo, Antonio Pastor, and Diego R. López. 2021. A digital twin network for security training in 5g industrial environments. In *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*. 395–398.

[221] Ewout Willem van der Wal and Mohammed El-Hajj. 2022. Securing networks of IoT devices with digital twins and automated adversary emulation. In *2022 26th International Computer Science and Engineering Conference*. 241–246.

[222] Seba Anna Varghese, Alireza Dehlaghi Ghadim, Ali Balador, Zahra Alimadadi, and Panos Papadimitratos. 2022. Digital twin-based intrusion detection for industrial control systems. In *International Conference on Pervasive Computing and Communications Workshops*. 611–617.

[223] Omar Veledar, Violeta Damjanovic-Behrendt, and Georg Macher. 2019. Digital twins for dependability improvement of autonomous driving. In *Systems, Software and Services Process Improvement*, Alastair Walker, Rory V. O'Connor, and Richard Messnarz (Eds.). Vol. 1060. 415–426.

[224] Manfred Vielberth, Magdalena Glas, Marietheres Dietz, Stylianos Karagiannis, Emmanouil Magkos, and Günther Pernul. 2021. A digital twin-based cyber range for soc analysts. In *Data and Applications Security and Privacy XXXV*, Ken Barker and Kambiz Ghazinour (Eds.). Vol. 12840. 293–311.

[225] Olivia von Westernhagen. 2020. *Malware-Infektionen: Fresenius schränkt Produktion vorübergehend ein.* Retrieved from https://www.heise.de/newsticker/meldung/Malware-Infektionen-Fresenius-schraenkt-Produktion-voruebergehend-ein-4715856.html Retrieved June 28, 2021 from

[226] Thumeera R. Wanasinghe, Leah Wroblewski, Bui K. Petersen, Raymond G. Gosine, Lesley Anne James, Oscar De Silva, George K. I. Mann, and Peter Warrian. 2020. Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges. *IEEE Access* 8 (2020), 104175–104197.

[227] Huan Wang, Xiaoqiang Di, Yan Wang, Bin Ren, Ge Gao, and Junyi Deng. 2023. An intelligent digital twin method based on spatio-temporal feature fusion for IoT attack behavior identification. *IEEE J. Sel. Areas Commun.* 41, 11 (2023), 3561–3572.

[228] Yuntao Wang, Zhou Su, Shaolong Guo, Minghui Dai, Tom H. Luan, and Yiliang Liu. 2023. A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. *IEEE Internet Things J.* 10, 17 (2023), 14965–14987.

[229] Yuying Wei, Adrian Wing-Keung Law, Chun Yang, and Di Tang. 2022. Combined anomaly detection framework for digital twins of water treatment facilities. *Water* 14, 7 (2022), 1001.

[230] Xuan Wu, Virginie Goepp, and Ali Siadat. 2020. Concept and engineering development of cyber physical production systems: A systematic literature review. *The International Journal of Advanced Manufacturing Technology* 111, 1-2 (2020), 243–261.

[231] Yiwen Wu, Ke Zhang, and Yan Zhang. 2021. Digital twin networks: A survey. *IEEE Internet of Things Journal* 8, 18 (2021), 1–1.

[232] Yinhao Xiao, Yizhen Jia, Qin Hu, Xiuzhen Cheng, Bei Gong, and Jiguo Yu. 2022. CommandFence: A novel digital-twin-based preventive framework for securing smart home systems. *IEEE Trans. Dependable Secure Comput.* 20, 3 (2022), 1–17.

[233] Jinzhi Lu Xiaochen Zheng and Dimitris Kiritsis. 2022. The emergence of cognitive digital twin: Vision, challenges and opportunities. *Int. J. Prod. Res.* 60, 24 (2022), 7610–7632.

[234] Lou Xinxin, Yun Guo, Gao Yuan, Karl Waedt, and Mithil Parekh. 2019. An idea of using digital twin to perform the functional safety and cybersecurity analysis. In *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik Informatik für Gesellschaft (Workshop-Beiträge).* 283–294.

[235] Qinghua Xu, Shaukat Ali, and Tao Yue. 2021. Digital twin-based anomaly detection in cyber-physical systems. In *2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST).* 205–216.

[236] Qinghua Xu, Shaukat Ali, and Tao Yue. 2023. Digital twin-based anomaly detection with curriculum learning in cyber-physical systems. *ACM Trans. Softw. Eng. Methodol.* 32, 5 (2023), 1–32.

[237] Qinghua Xu, Shaukat Ali, Tao Yue, Zaimovic Nedim, and Inderjeet Singh. 2023. KDDT: Knowledge distillation-empowered digital twin for anomaly detection. In *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2023).* 1867–1878.

[238] Zhiheng Xu and Arvind Easwaran. 2020. A game-theoretic approach to secure estimation and control for cyber-physical systems with a digital twin. In *2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS).* 20–29.

[239] Ibrar Yaqoob, Khaled Salah, Mueen Uddin, Raja Jayaraman, Mohammed Omar, and Muhammad Imran. 2020. Blockchain for digital twins: Recent advances and future research challenges. *IEEE Network* 34, 5 (2020), 290–298.

[240] Yagmur Yigit, Omer Kemal Kinaci, Trung Q. Duong, and Berk Canberk. 2023. TwinPot: Digital twin-assisted honeypot for cyber-secure smart seaports. In *2023 IEEE International Conference on Communications Workshops.* 740–745.

[241] Tianyu Zhao, Ernest Foo, and Hui Tian. 2022. A digital twin framework for cyber security in cyber-physical systems. *CoRR* abs/2204.13859 (2022).

[242] Haifeng Zhou, Mohan Li, Yanbin Sun, Zhihong Tian, and Lei Yun. 2022. Digital twin based cyber range for industrial internet of things. *IEEE Consumer Electronics Magazine* 12, 6 (2022), 66–77.

Received 15 February 2024; revised 26 May 2025; accepted 31 May 2025