A Survey on Cybersecurity through Digital Twins: Definition, Applications and Deployment

PHILIP EMPL, University of Regensburg, Germany
GÜNTHER PERNUL, University of Regensburg, Germany

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

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, Cyber Security, System of Systems, Internet of Things, Cyber-Physical Systems, Industrial Control System, Survey, Literature survey

ACM Reference Format:
Philip Empl and Günther Pernul. 2022. A Survey on Cybersecurity through Digital Twins: Definition, Applications and Deployment. In *ACM Computing Surveys, Vol. 1, No. 1, Article 1, Publication date: January 2022.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Digital Twins are gaining great attention in industry and science due to their promising opportunities. The application scenarios of Digital Twins are manifold. Bosch is instrumenting the Digital Twin mainly in the sphere of the Industrial Internet of Things (Industrial IoT) to envision a smart factory [21]. Siemens is computing Digital Twins for hearts (or of patients) to comprehend the divergent reactions to medicine [24] or, e.g., in times of SARS-CoV-2, vaccines. Herrenberg, a medieval German town with 30,000 citizens, lets tourists explore their urban digital twin through a virtual reality application [11]. One step bigger, the European Union is planning within the "Destination Earth" initiative a digital twin of the whole world to estimate, e.g., climate change impacts[1]. As can be seen from these application scenarios, the potential market seems to be inexhaustible. Thus, the market size is expected to grow rapidly and will reach roundabout $48.2 billion by 2026 (2028: $86.09 billion [42]) with a current market size value of $3.1 billion in 2020 [35]. The digital twin emphasizes a great hype, which summarizes Figure 1 to motivate this survey and to show the progression of the digital twin along the Gartner hype cycle of emerging technologies, aggregating its data for the digital twin from 2017-2020 []. Thereby, the figure also draws on digital twin research milestones, known cyberattacks, and several

[1] https://digital-strategy.ec.europa.eu/en/library/destination-earthgo

Manuscript submitted to ACM

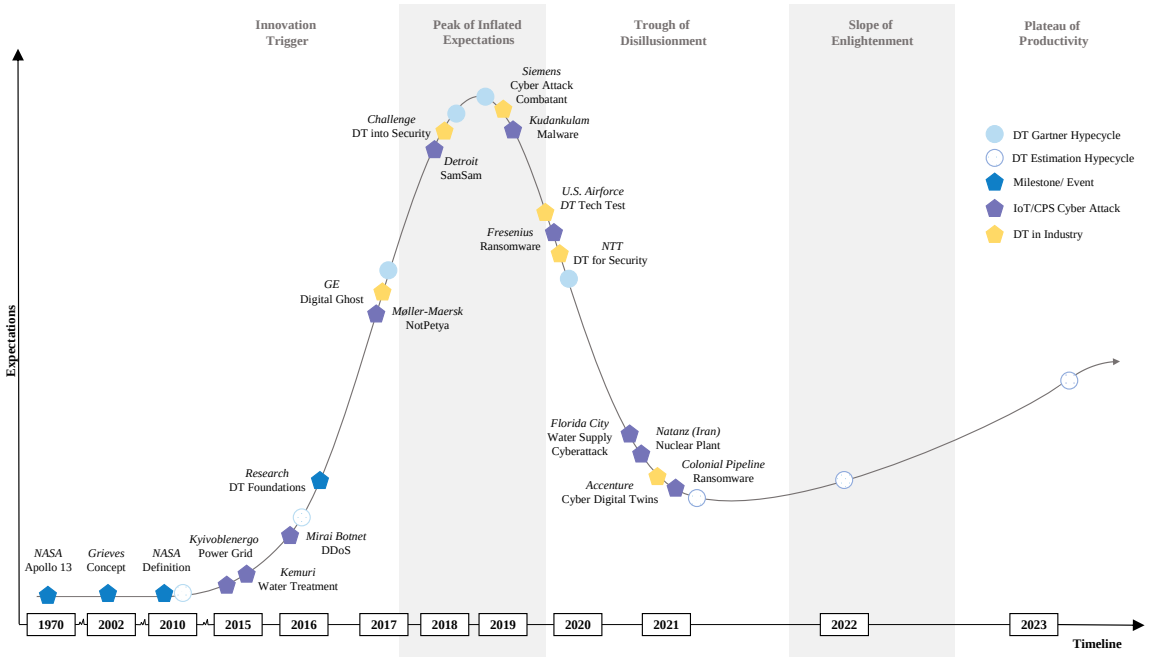

Fig. 1. History and security-oriented development of the emerging Digital Twin paradigm along critical ICS attacks.

industrial examples on the use of digital twins for cybersecurity. The following paragraphs describe and contextualize these events.

1.1 Digital Twin

Although the pre-mentioned industry projects represent innovative ideas on today's challenges, the Digital Twin paradigm is nothing new. Instead, the digital twin represents a composition of existing technologies, partly developed several decades ago [7]. For instance, Apollo 13 suffered an explosion inside the oxygen tanks 200,000 miles away in 1970 [4]. NASA modified the conditions of the simulators (usually practiced to train the astronauts) to match the needs of Apollo 13 and identified strategies to solve the hazardous situation. Of course, Digital Twins are more than a simulation. Still, NASA was the first institution that made advantage out of something that we refer in parts of to a "Digital Twin". In 2002, Grieves & Vickers [23] theorize a concept that relies on virtual replications of physical assets along their life cycle. Nearly ten years later, NASA aerospace and the U.S. Air Force applied Digital Twins to examine the life cycle of physical assets and to diagnose and predict an asset's particular behavior [20].

In general, definitions and viewpoints of the digital twin diverge depending on a particular application domain, resulting in plenty of definitions [44]. Glaessgen & Stargel [20] define the Digital Twin in Aerospace as a "*multi-physics, multi-scale, probabilistic simulation of an as-built vehicle or system, that uses the best available physical models, sensor updates, fleet history [...] to mirror the life of its corresponding flying twin*". In a Manufacturing context, a Digital Twin is a "*set of virtual information constructs that fully describes a potential of actual physical manufactured product from the micro atomic level to the macro geometrical level*" [23]. However, Rosen et al. [43] describe the digital twin along the life cycle exhibiting the following characteristics: i) simulation models, ii) descriptive data, iii) semantic technologies, iv) life

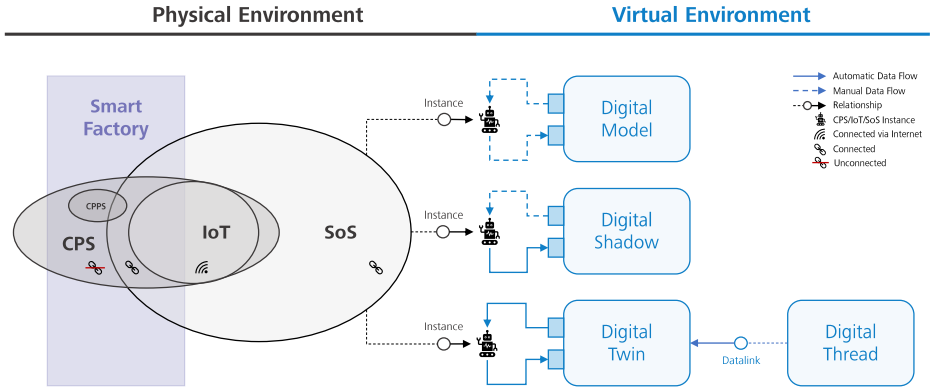

Fig. 2. Terminology used in this survey to describe the relation of CPS, IoT, SoS (adopted from Henshaw [10]) and related concepts to the Digital Twin (adopted from Kritzinger et al. [29]).

cycle centrality, v) linkage between physical and virtual world, vi) stand-alone service (optional), and vii) feedback loop. The digital twin benefits from Big Data, e.g., data out of the Internet of Things (IoT) that enable on-building statistics, artificial intelligence, machine learning, deep learning, and data visualizations [17].

Digital Twins are mainly employed in environments that consist of Systems-of-Systems (SoS) [12]. SoS summarize IoT devices, parts of the Cyber-Physical Systems (CPS) [10] and compose "*engineered, physical systems integrated with networking, data, computational systems linked via transducers and interacting with humans who may function as designers, operations, components*" [22]. Cyber-Physical Production Systems (CPPS) represent one possible instance of a CPS in an industrial context. Furthermore, digital twins are distinguished from digital models and digital shadows by the degree of automation of the data flow [29]. Some researchers consider Digital Twin and Digital Thread as equivalent [28]. However, the digital thread describes the link between the digital twin and various data sources that provide the twin with the relevant data at any time within its life cycle [14]. The terminology and the delineation of interrelated concepts adopted in this survey are shown in Fig. 2.

1.2 Digital Twin as Cyber Attack Combatant

Parts of SoS realize the intertwining of physical and virtual environments, i.e., operational technology and information technology alignment. Especially connected (via the internet) components constitute a potentially hazardous attack surface. As Figure 1 indicates, several severe IoT and CPS (i.e., Industrial Control Systems (ICS)) incidents appalled the world. Thereby, ransomware (e.g., Fresenius cyber attack in 2020 [47] or NotPetya [1]), malware (see Kudankulam power plant in 2019 [9]), worms (e.g., Stuxnet [1]), unpatched vulnerabilities (e.g., Cyberattack at Kemuri water treatment plant in 2015 [1]), and botnets play a crucial role. A prominent example is the attack on the Ukrainian power grid in December 2015, where attackers hijacked the Supervisory Control and Data Acquisition (SCADA) and affected 225,000 customers for several hours of the Kyivoblenergo energy distribution center [31]. A few years later, Mirai exploited the unmodified IoT device (e.g., cameras or routers) credentials (see Mirai dictionary) to misuse them within a botnet for distributed denial of service attacks [2]. The year 2021 is marked by a series of cyberattacks on ICS. In February 2021, an attacker boosted the level of sodium hydroxide level to 100 times more than normal via remote access software within a water treatment plant in Oldsmar, Florida [46]. Two months later, Iran's Natanz nuclear enrichment plant

was hit by a cyber attack/sabotage, which also demonstrates that war is becoming increasingly virtual in nature [5]. In April 2021, ransomware attackers connected through a virtual private network inside the local network of the Colonial Pipeline by using a compromised password and shut down the oil and gas distribution for days [18].

The industry is responding to the threat situation by reshaping digital twins for cybersecurity. As one of the most significant vital players for digital twins, General Electric employs digital twins of machines to identify anomalies in their behavior. The so-called digital ghost maintains cybersecurity via detection, localization, prediction, and neutralization of harmful activities [19]. Siemens also perceives the digital twin as more than simply an instrument for measuring the performance of machines and exploits the potential of Digital Twins for detecting cyberattacks [16]. Several key players follow this hype, e.g., in the consulting sector (see NTT [30], Challenge Advisory Llp [36], or Accenture [27]).

Likewise, research increasingly focuses on the phenomenon of the digital twin for cybersecurity. Dietz & Pernul [13] describe the possibilities of a digital twin to enhance cybersecurity in ICS, identifying three modes of operation: simulation, replication, and analytics/optimization. Eckhart et al. [15] developed a prototype that models the cybersecurity awareness of CPSs with digital twins to allow assumptions about the cybersecurity state of the systems. Olivares-Rojas et al. [38] demonstrated that Digital Twins are applicable and feasible to test cybersecurity attacks on smart meters as the smart meters themselves are not harmed.

1.3 Contribution & Scope

Both research and industry are sending clear signals of an evolving digital twin in the direction of cybersecurity. Thus, one might question whether attacks could have been (partly) prevented with the help of digital twins. The power of the digital twin can be exploited and is not limited to the application in production only. In addition, the digital twin is currently in the "*Trough of Disillusionment*" (as can be depicted from Fig. 1), which indicates a suitable timing for this survey. In the past, researchers conducted a plethora of surveys involving the digital twin [4, 26, 29, 32, 34, 37, 48, 49]. Most of them concentrated on certain application domains (i.e., Smart Manufacturing) and considered security issues and future security challenges for the digital twin, among others [4]. Due to the security issues regarding the digital twin, research developed in the direction for provisioning security for the digital twin, e.g., through the combination of digital twins and distributed ledger technology [25, 41, 50]. However, surveys scarcely focus on the application of the digital twin for cybersecurity. Eckhart et al. [14] systematized the body of knowledge (SoK) and identified several use cases of the digital twin for cybersecurity in 2019. Pokhrel et al. [40] conducted a Multi-vocal Literature survey (MLR) on the application of the digital twin for cybersecurity incident prediction. Böhm et al. [6] deal with the combination of Digital Twins and Augmented Reality (AR) from a cybersecurity perspective. All these publications are compared to our survey in Tab. **??**.The greatest difference to our survey lies in the specialization of these, for example, one specific application domain [14], one specific application scenario (intrusion detection) [40] or only a given set of core technologies [6]. Our survey is intended to be all-encompassing and to combine all the perspectives of the previously written overviews.

With regard to the current development of the digital twin into a cyber security tool, a classification and a presentation of the state of the art must be made. This makes it possible to point the way to further research needs for both research and industry and to show the potential and diversity of the digital twin in use for cyber security. The contribution of this survey is then to:

(1) highlight the components of the digital twin from a cybersecurity perspective,
(2) define the paradigm digital twin in cybersecurity,
(3) describe the application domains and scenarios of the digital twin,

Aspects	Böhm et al. [6]	Pohkrel et al. [40]	Eckhart et al. [14]
Scope	*CPS* ∪ *IoT*	*CPS* ∪ *IoT*	*CPS* \ *IoT*
Methodology	*SLR*	*MLR*	*SoK*
Definition		●	●
Components		○	◑
Application Advantages		○	◑
Application Domains		◑	◑
Application Scenarios		◑	◑
Implementation Guidelines		○	○
Challenges/ future research		◑	●

○ = not covers topic; ◑ = partially covers topic; ● = covers topic

Table 1. Comparison of our survey to existing surveys in terms of the content and scope

(4) provide guidelines on proven techniques, implementations and deployments,
(5) shape research directions and underline open issues for both research and industry to fill existing gaps and thus, to exploit the potential of the digital twin for more secure SoS.

The methodology and organization of this survey is shown in detail in Section 2.

2 METHODOLOGY

Our survey demystifies the digital twin in cybersecurity. Thereby, we define the paradigm, describe its application, and highlight best practices. Section 3 starts with introducing the paradigm digital twin from a cybersecurity perspective, Section 4 describes the application domains and scenarios, Section 5 highlights best practices for the application, and Section 6 pictures open issues and future research. Our survey follows the methodology of a qualitative systematic review or systematic literature review in information systems research [39] by respecting the guidelines provided by Schryen [45] and thus, following the framing, searching & screening, and synthesis phases.

2.1 Goal & Scope

Section 1 is giving the motivation and necessity of this survey, which we summarize again in a few sentences. A range of attacks threatens the industry, the digital twin emphasizes excellent attention in both research and industry, and existing research lacks a comprehensive overview. The timing for this survey is considered relevant, and thus, we provide an overview to exploit the potential of the digital twin for cybersecurity SoS. We focus on SoS, which involves interconnected CPS and IoT devices representing the primary target for sophisticated cyber attacks. The OT/IT alignment is one cause for the plethora of cyber attacks, as the OT is not traditionally designed for communication. We depicted the differences and relations between CPS, IoT, and SoS in Section 1 and illustrated it in Fig. 2.

As this survey attempts to summarize past qualitative research and examines the body of knowledge of digital twins for cybersecurity. We would like to comprehensively illustrate the digital twin from a cybersecurity perspective and provide further research directions. Therefore, our survey aims at answering the following research questions (RQ):

(RQ1) What is the Digital Twin paradigm in cybersecurity?
(RQ2) How is the Digital Twin currently applied for cybersecurity?

Inclusion criteria	Exclusion criteria
IC1: Articles in English and full text is accessible	EC1: *Articles whose focus is irrelevant to* security
IC2: Conference proceedings, journals and books	EC2: *Articles which are lacking the digital twin*
IC3: Articles with a high quality and a strong research methodology	EC3: *Articles which are not in an IoT, CPS or SoS setting*

Table 2. Applied inclusion and exclusion criteria

(RQ3) How can the Digital Twin be implemented for cybersecurity?

(RQ4) What are the open challenges and future research directions for the Digital Twin in cybersecurity?

2.2 Search & Assessment

We conducted a database search, accompanied by subsequent backward and forward searches, to obtain relevant results and reach completeness. Since the search term *"digital twins" and "security"* generated excessively numerous results in the academic literature databases, we set the focus to CPS and IoT as parts of SoS in a few databases. In addition, we further wrapped the results with the keywords *'cybersecurity'* or *'information security'* and synonyms, as security is often referred to as safety. We combined these key terms and synonyms with the operators. Thus our search terms looked the following:

(1) *"digital twin"* ***AND*** *"security"*

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

Then we applied the search terms to the following academic databases: *ACM DL*$^{(1)}$, *AISeL*$^{(1)}$, *arXiv*$^{(1)}$, *dblp*$^{(1)}$, *IEEE CSDL*$^{(1)}$, *IEEE Xplore*$^{(1)}$, *ScienceDirect*$^{(2)}$, *SpringerLink*$^{(2)}$, *Wiley Online Library*$^{(2)}$, and *WoS*$^{(1)}$.[2] These academic databases retrieved a total set of XXX. Then we derived a set of inclusion and exclusion criteria to meet our research questions. The criteria are shown in Tab. 2.

First, we removed the duplicates from the literature corpus. We then decided whether the publication was relevant by applying the previously defined inclusion or exclusion criteria to the title and abstract. Afterward, we excluded publications by full text. We excluded literature that provides suggestions on how to secure digital twins, e.g., distributed ledger technology, or describes the benefits of the Digital Twin for operational usage, i.e., smart manufacturing. In addition, we eliminated literature that lacks in scope or if the quality or availability was not given. Subsequently, we first performed the backward search on the remaining literature corpus and then the forward search on the new accumulated literature corpus. A detailed overview of our research method can be seen in Appendix 6.

In the end, we yielded a set of 130 publications that met our research questions. This result confirms the increasing trend of using the digital twin cybersecurity in SoS, as can be seen in Fig. 5. The year 2021 was not considered entirely, so there is a decrease in the relevant publications. However, this does not allow any assumptions about the development of the trend in 2021.

[2] $^{(*)}$ indicates which search term was applied.

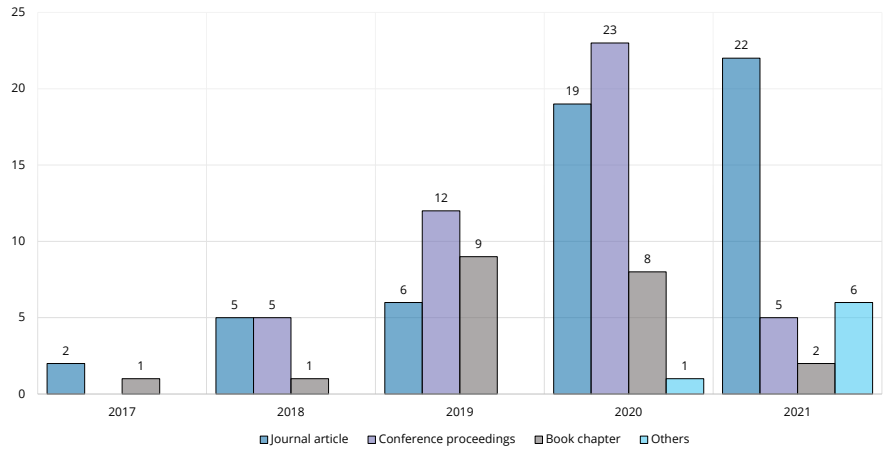

Fig. 3. Number of Digital Twin publications from a cybersecurity perspective by year from 2017 to 2021 (June) reviewed

2.3 Extraction & Synthesis

After selecting and reading the relevant literature, we focused on extracting, synthesizing, and analyzing the relevant literature. These steps are the most important ones of our survey, so we need to ensure that we summarize and classify the body of knowledge adequately to answer the previously defined research questions.

We defined a data extraction pattern that was applied to each identified publication. This pattern helps to ensure that the same procedure is systematically applied inside the literature corpus. In addition, we collected bibliometric (i.e., authors or title) and contextual data (i.e., setting or scope) for further statistical analysis and insights. At the beginning of the extraction, we tested the pre-defined pattern on a small set of publications. We organized all the extracted data into a spreadsheet and managed it as a starting point for further synthesis.

Afterward, we synthesized the extracted data using thematic analysis [8]. The thematic analysis makes it feasible to split the extracted data pattern into individual themes, respectively (cf. Fig. 4). First, we specified central themes for each research question. In the next step, we defined a descriptive schema that helped relate the central themes and instantiated sub-themes when needed. Through this schema, we learn to understand the digital twin paradigm in cybersecurity as a whole (*what is it?*), details about its applications (*why*, *where*, *when*, apply it or *who* applies it?), implementation guidelines (*how to use it?*) and which open challenges future research should address (*which issues?*). Thereby, central themes summarize sub-themes, which describe a set of categories. Themes were specified partly inductive and deductive. While Section **??** the sub-theme *'Digital Twin Scenarios'* (utilization of the NIST cybersecurity framework [3]) and the central theme Section **??** *'Implementation Guidelines for Digital Twins in Cybersecurity'* (classification along the Industrial Internet Reference Architecture [33]) are generated deductively, the remaining section's themes were inductively created from the extracted data. We describe these central themes and respective sub-themes in the following Sections 3-6.

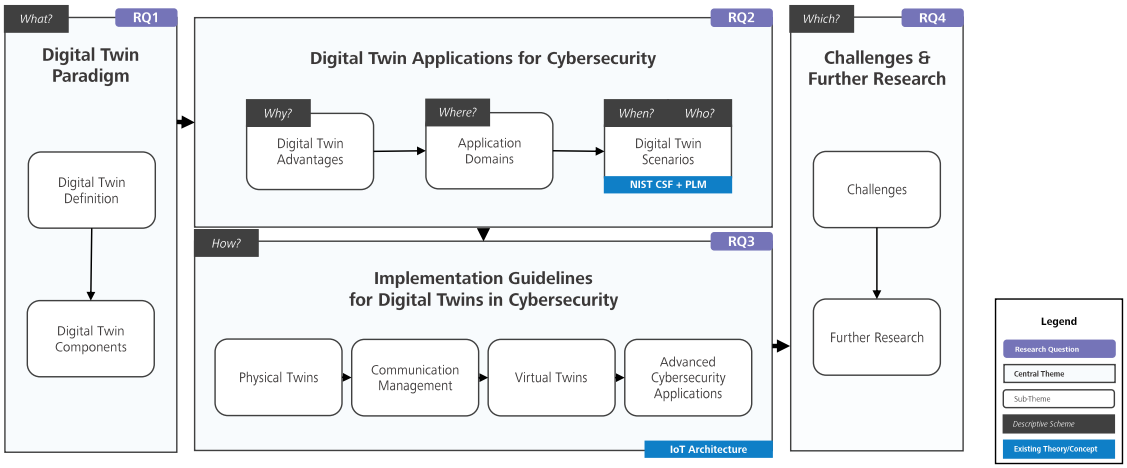

Fig. 4. Thematic classification of the survey

3 DIGITAL TWIN PARADIGM IN CYBERSECURITY

At the beginning we are emphasizing the nature of Digital Twins in a security context. Thus,

3.1 Definition of the Digital Twin

–> aus den Komponenten wird die Definition abgeleitet

Definition of the Digital Twin in a Cybersecurity Context:
"The digital twin describes the closely interrelated representation and synchronization of a physical asset (e.g., entity, system, process, or person) to its virtual counterpart along its lifecycle. A different set of techniques can instantiate the digital twin (e.g., mirroring, replication, simulation, or emulation) that model the physical asset's behavior and process its (environmental) data in real-time and retrospectively to improve security through selected security measures."

3.2 Components of the Digital Twin

Components	References
Physical asset	*Entity/ Object* *System* *Process* *Software* *Person*
Virtual asset	*Replication* *Behavioral Model* *Virtual Object* *Simulation* *Mirroring*
Interrelation	*Virtual → physical* *Physical → virtual* *Lifecycle* *Synchronization* *Fidelity* *Parameter/ State*

Reason	References
Reason A	
Reason B	
Reason C	
Reason D	
Reason E	
Reason F	

4 DIGITAL TWIN APPLICATIONS FOR CYBERSECURITY

This section is aimed at responding to RQ2. From our analysis, several application cases of Digital Twin emerge, and they are mainly grouped in three domains: manufacturing (which also includes model-based system engineering, MBSE), aviation, and healthcare.

4.1 Application Advantages

Warum brauche ich diesen überhaupt? Reichen nicht andere Möglichkeiten auch aus?

Application Areas	References
Smart Manufacturing	
Healthcare	
Enterprise	
Smart Grid	
Smart City	
Smart Home	
Oil & Gas Industry	
Mobility	
Others	

4.2 Application Domains

4.2.1 Smart Manufacturing. About Machines etc. –> was wird hierbei überhaupt betrachtet

4.2.2 Smart City.

4.2.3 Smart Grid.

4.2.4 Smart Fishing.

4.2.5 Smart Home.

4.2.6 Oils & Gas Industry.

4.2.7 Smart Healthcare.

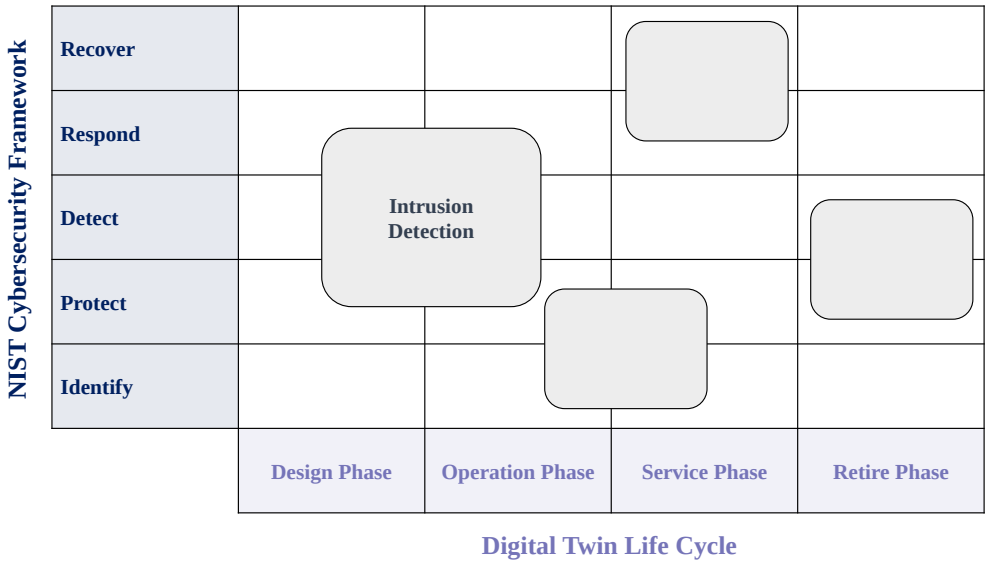

Fig. 5. Application Scenarios of the Digital Twin for Cybersecurity along the NIST Cybersecurity Framework [] and the Digital Twin Lifecycle []

4.3 Application Scenarios

Industry Living Healthcare Personel

5 DIGITAL TWIN IMPLEMENTATION GUIDELINES

In this section, we provide an overview of design implications we derived from this study. In particular, we frst illustrate the need of a sociotechnical and collaborative approach to the design process, and then we outline two different lifecycles that describe a DT's life, from its design to its dismissal. –> Betrachtung der verschiedenen Layer des digitalen Zwillings

5.1 Communication and Integration of Digital Twins

5.1.1 Communication Types.

5.1.2 Level-of-Integration.

5.1.3 Protocols & Techniques. Simulation Automation Replication security analytics prescriptive diagnostic etc.

5.2 Security-related Data Management

5.2.1 Data Classes & Types.

5.2.2 Data Formats.

5.2.3 Tools.

5.3 Advanced Security Practices

5.3.1 Data Aggregation & Fusion.

5.3.2 Data Extraction & Selection.

5.3.3 Data Analysis.

5.3.4 Digital Twin Creation.

- Mininet
- Mininet-Wifi
- CPS Twinning
- Eclipse Ditto

6 CHALLENGES & FURTHER RESEARCH (1 P.)

There are currently some important issues and challenges that need to be further studied and addressed, and are related to different aspects, all important for the future of the research in this field.

6.1 1. DASDASDAS

6.2 1. DASDASDAS

6.3 1. DASDASDAS

6.4 1. DASDASDAS

6.5 1. DASDASDAS

6.6 1. DASDASDAS

7 CONCLUSION (1 P.)

8 ACKNOWLEDGMENTS

Identification of funding sources and other support, and thanks to individuals and groups that assisted in the research and the preparation of the work should be included in an acknowledgment section, which is placed just before the reference section in your document.

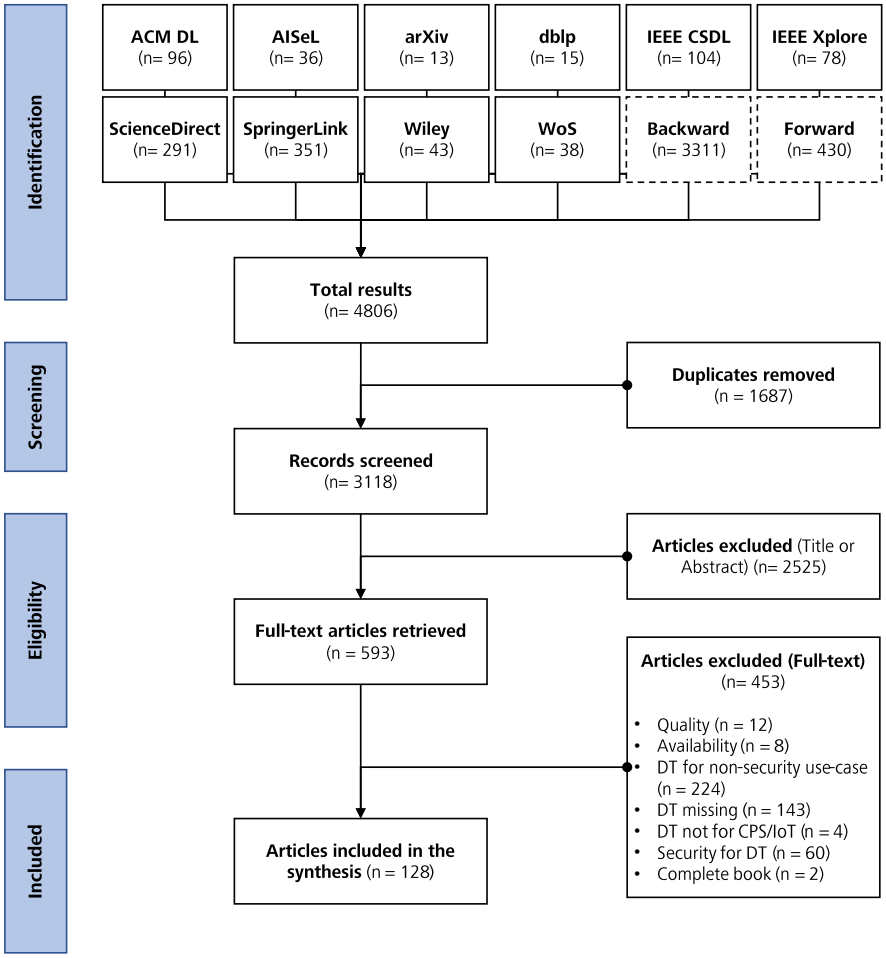

Fig. 6. Additional information about the survey process pictured within the PRISMA (be aware that the exclusion could also be on multiple exclusion criteria.).

REFERENCES

[1] Tejasvi Alladi, Vinay Chamola, and Sherali Zeadally. 2020. Industrial Control Systems: Cyberattack trends and countermeasures. *Computer Communications* 155 (2020), 1–8. https://doi.org/10.1016/j.comcom.2020.03.007

[2] 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. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[3] Matthew Barrett. 2018. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

[4] 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. https://doi.org/10.1109/ACCESS.2019.2953499

[5] Peter Beaumont. 2021. *Natanz 'sabotage' highlights Iran's vulnerability to cyber-attacks.* Retrieved June 28, 2021 from https://www.theguardian.com/world/2021/apr/12/natanz-nuclear-facility-sabotage-iran-vulnerability-to-cyber-attacks

[6] 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. https://doi.org/10.3390/jcp1030026

[7] Beate Brenner and Vera Hummel. 2017. Digital Twin As Enabler for an Innovative Digital Shopfloor Management System in the ESB Logistics Learning Factory at Reutlingen-university. *Procedia Manufacturing* 9 (2017), 198–205. https://doi.org/10.1016/j.promfg.2017.04.039

[8] Daniela S. Cruzes and Tore Dybå. 2011. Research synthesis in software engineering: A tertiary study. *Information and Software Technology* 53, 5 (2011), 440–455. https://doi.org/10.1016/j.infsof.2011.01.004 Special Section on Best Papers from XP2010.

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

[10] Michael J. de C Henshaw. 2016. Systems of Systems, Cyber-Physical Systems. the Internet of Things: Whatever Next? *INSIGHT* 19, 3 (2016), 51–54. https://doi.org/10.1002/inst.12109

[11] Fabian Dembski, Uwe Wössner, Mike Letzgus, Michael Ruddat, and Claudia Yamu. 2020. Urban Digital Twins for Smart Cities and Citizens: The Case Study of Herrenberg, Germany. *Sustainability* 12, 6 (2020), 2307. https://doi.org/10.3390/su12062307

[12] Marietheres Dietz and Günther Pernul. 2020. Digital Twin: Empowering Enterprises Towards a System-of-Systems Approach. *Business & Information Systems Engineering* 62, 2 (2020), 179–184. Issue 2. https://doi.org/10.1007/s12599-019-00624-0

[13] Marietheres Dietz and Gunther Pernul. 2020. Unleashing the Digital Twin's Potential for Ics Security. *IEEE Security & Privacy* 18, 4 (2020), 20–27. https://doi.org/10.1109/MSEC.2019.2961650

[14] 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. https://doi.org/10.1007/978-3-030-25312-7_14

[15] 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. https://doi.org/10.1109/etfa.2019.8869197

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

[17] Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow. 2020. Digital Twin: Enabling Technologies, Challenges and Open Research. *IEEE Access* 8 (2020), 108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358

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

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

[20] 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. https://doi.org/10.2514/6.2012-1818

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

[22] Christopher Greer, Martin Burns, David Wollman, and Edward Griffor. 2019. Cyber-physical Systems and Internet of Things. https://doi.org/10.6028/NIST.SP.1900-202

[23] Michael Grieves and John Vickers. 2017. *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems.* Springer International Publishing, Cham, 85–113. https://doi.org/10.1007/978-3-319-38756-7_4

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

[25] Sihan Huang, Guoxin Wang, Yan Yan, and Xiongbing Fang. 2020. Blockchain-based Data Management for Digital Twin of Product. *Journal of Manufacturing Systems* 54 (2020), 361–371. https://doi.org/10.1016/j.jmsy.2020.01.009

[26] 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 (2020), 36–52. https://doi.org/10.1016/j.cirpj.2020.02.002

[27] 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

[28] Edward M. Kraft. 2016. The Air Force Digital Thread/Digital Twin - Life Cycle Integration and Use of Computational and Experimental Knowledge. In *Proceedings of the 54th. AIAA Aerospace Sciences Meeting.* American Institute of Aeronautics and Astronautics, 0897. https://doi.org/10.2514/6.2016-0897

[29] 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. https://doi.org/10.1016/j.ifacol.2018.08.474 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.

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

[31] Robert M. Lee, Michael J. Assante, and Tim Conway. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Technical Report 404-446-9780 #2. Washington D.C.

[32] 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. *Journal of Intelligent Manufacturing* 31, 6 (2019), 1313–1337. https://doi.org/10.1007/s10845-019-01512-w

[33] S. W. Lin, B. Miller, J. Durand, R. Joshi, P. Didier, A. Chigani, R. Torenbeek, D. Duggal, R. Martin, and G. Bleakley. 2015. *Industrial Internet Reference Architecture.* Technical Report.

[34] Mengnan Liu, Shuiliang Fang, Huiyue Dong, and Cunzhi Xu. 2021. Review of Digital Twin about Concepts, Technologies, and Industrial Applications. *Journal of Manufacturing Systems* 58 (2021), 346–361. https://doi.org/10.1016/j.jmsy.2020.06.017 Digital Twin towards Smart Manufacturing and Industry 4.0.

[35] MarketsandMarkets. 2021. *Market Report: Digital Twin Market by Technology, Type (product, Process, and System), Application (Predictive Maintenance, and Others), Industry (Aerospace & Defense, Automotive & Transportation, Healthcare, and Others), and Geography - Global Forecast to 2026.* Technical Report SE 5540. MarketsandMarkets™ INC., Northbrook, Illinois.

[36] Carlos Miskinis. 2018. *Incorporating Digital Twin into Internet Cyber Security – Creating a Safer Future.* Retrieved June 28, 2021 from https://www.challenge.org/insights/digital-twin-cyber-security/

[37] Elisa Negri, Luca Fumagalli, and Marco Macchi. 2017. A Review of the Roles of Digital Twin in CPS-based Production Systems. *Procedia Manufacturing* 11 (2017), 939–948. https://doi.org/10.1016/j.promfg.2017.07.198 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy.

[38] 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* (2021), 1–1. https://doi.org/10.1109/MIC.2021.3063674

[39] 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. https://doi.org/10.1016/j.im.2014.08.008

[40] 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. https://doi.org/10.1145/3387940.3392199

[41] Benedikt Putz, Marietheres Dietz, Philip Empl, and Günther Pernul. 2021. EtherTwin: Blockchain-based Secure Digital Twin Information Management. *Information Processing & Management* 58, 1 (2021), 102425. https://doi.org/10.1016/j.ipm.2020.102425

[42] Grand View Research. 2021. *Digital Twin Market Size, Share & Trends Analysis Report by End-Use (automotive & Transport, Retail & Consumer Goods, Agriculture, Manufacturing, Energy & Utilities), by Region, and Segment Forecasts, 2021 - 2028.* Technical Report GVR-2-68038-494-9. Grand View Research, Inc., San Francisco, California.

[43] 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. https://doi.org/10.1016/j.ifacol.2019.11.685

[44] Benjamin Schleich, Nabil Anwer, Luc Mathieu, and Sandro Wartzack. 2017. Shaping the Digital Twin for Design and Production Engineering. *CIRP Annals* 66, 1 (2017), 141–144. https://doi.org/10.1016/j.cirp.2017.04.040

[45] 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. http://aisel.aisnet.org/cais/vol37/iss1/12

[46] Amir Vera, Jamiel Lynch, and Christina Carrega. 2021. . Retrieved June 28, 2021 from https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html

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

[48] 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. https://doi.org/10.1109/ACCESS.2020.2998723

[49] Yiwen Wu, Ke Zhang, and Yan Zhang. 2021. Digital Twin Networks: A Survey. *IEEE Internet of Things Journal* (2021), 1–1. https://doi.org/10.1109/JIOT.2021.3079510

[50] 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. Issue 5. https://doi.org/10.1109/mnet.001.1900661