From Stakeholder Needs to Secure Digital Twin Services

Critical Infrastructure Use Cases within the INTACT Framework

Ilinca-Laura Burdulea; Sonika Gogineni
Intelligent Integration Department
Fraunhofer Institute for Production Systems and Design Technology IPK
Berlin, Germany
e-mail: ilinca-laura.burdulea@ipk.fraunhofer.de, sonika.gogineni@ipk.fraunhofer.de

Stamatios Kostopoulos; Evangelos K. Markakis
Department of Electrical and Computer Engineering
Hellenic Mediterranean University
Heraklion, Greece
e-mail: s.kostopoulos@pasiphae.eu, emarkakis@hmu.gr

Kyriakos N. Manganaris; Fotis I. Lazarakis
Institute of Informatics and Telecommunications
National Centre for Scientific Research "Demokritos"
Athens, Greece
e-mail: kmangana@iit.demokritos.gr, flaz@iit.demokritos.gr

***Abstract*— Digital Twins (DTs) are a promising solution for enhancing the security and resilience of critical infrastructure. However, existing approaches rarely present systematic ways to capture stakeholder cybersecurity needs and map them to actionable functional requirements. This paper addresses that gap by presenting a user-centric methodology for deriving functional requirements for cybersecurity-focused DTs in critical infrastructures. As part of the EU-funded Integrated Software Toolbox for Secure IoT-to-Cloud Computing (INTACT) project, we apply this approach to two distinct use cases, namely a healthcare facility and a nuclear reactor facility. Stakeholder cybersecurity objectives are mapped to user stories, categorized into scenarios according to a taxonomy aligned with the Network and Information Systems (NIS2) directive, and translated into functional requirements using the INTACT reference architecture. The process highlights that cybersecurity needs are driven more by stakeholder roles than infrastructure type, enabling reuse of core DT functions across domains. By integrating user needs early in the design phase, this methodology supports systematic, replicable DT functional design with a focus on cybersecurity and human-factor risks.**

Keywords- Digital Twin; Cybersecurity; Critical Infrastructure; Functional Requirements; NIS2 Directive.

I. INTRODUCTION

Critical infrastructures can be facilities, assets, systems or processes of major importance to society and whose failure or disruption would cause dramatic consequences. As these infrastructures enable the secure, reliable, and effective function of communities, ensuring their resilience and continuous functioning becomes challenging due to the increasing level of automatization and digitalization [1].

DTs are virtual images of physical systems or assets that simulate and analyse their behaviour in real-time. The virtual and physical counterparts remain synchronized through a continuous data-exchange process known as "twinning" [2]. Robotics, data-driven modelling, cloud computing, the Internet of Things (IoT), and Artificial Intelligence (AI) are few of the technologies that enable the realization of DTs [3].

By creating DTs of their IT infrastructure, networks, and security systems, organizations can simulate cyber-attacks, analyse vulnerabilities, and test response plans in a controlled virtual environment before deployment in the actual system [4]. Since DTs enable continuous monitoring, threat detection, and risk mitigation, they can exploit real-time cyber intelligence and thus contribute to stronger and more resilient critical infrastructure systems [5][6].

However, effective implementation requires stakeholders to be considered from the concept development phase. Their roles and objectives should inform the design of DT functions to create relevant and user-centered services. While the "user focus" dimension in DT application dimensions, as defined by Uhlenkamp et al. [7], only distinguishes between single-user and multi-user approaches, accounting for a broader range of stakeholder perspectives can significantly enhance value creation within DT ecosystems [8].

Although cybersecurity is acknowledged in recent DT architectural frameworks, its functional implementation remains inconsistent. Despite rich literature on DT development, a comprehensive, user-centric methodology tailored to cybersecurity is yet to be established. Systematic reviews have identified key gaps, including the lack of standardized security modelling, the absence of integrated multi-domain frameworks, and the need for more proactive and adaptive security models [9][10].

To address these gaps, we propose a functional, user-centric modelling methodology for DTs with a strong focus on cybersecurity in critical infrastructure contexts. This methodology maps stakeholder needs and objectives concerning cybersecurity to user stories, from which system

requirements are derived. We demonstrate its applicability using two distinct use cases, namely a healthcare facility and a nuclear reactor facility, to highlight the potential for creating a unified, cross-domain cybersecurity framework for DTs in critical infrastructures. Embedding security by design, this approach makes cybersecurity more accessible, systematic, and scalable, ultimately contributing to enhanced protection and resilience of critical infrastructure systems.

The rest of this paper is organized as follows: Section II reviews related work and outlines the research gap. Section III presents the broader context of the INTACT project. Section IV introduces the proposed methodology for mapping stakeholder cybersecurity needs into functional requirements. Section V demonstrates the application of this methodology to two critical infrastructure use cases, and Section VI concludes with a discussion and outlook.

II. RELATED WORK

DTs are widely recognized as a transformative technology for managing complex systems, as they combine real-time data, simulations, visualizations, and predictions to enable system optimization and informed decisions. In the context of critical infrastructures, DTs are a relevant solution for improving operational efficiency, resilience, and overall security, since they address security, trust, and privacy challenges in these domains [11]. For example, in the healthcare sector, DTs can serve as a conceptual framework for analysing data-driven practices and improving both operational and clinical processes [12]. Cybersecurity applications include vulnerability detection [13] and securing Wireless Body Area Networks (WBAN) [14]. In the nuclear domain, DTs are still in the early stage of adoption but are gradually being implemented across the full lifecycle: from design to operation, maintenance and decommissioning [15]. However, cybersecurity applications remain limited, mostly focused on testbeds for physical protection systems [16] or high-level functional and risk assessments [17].

Although cybersecurity is acknowledged in most recent DT reference architectures, its implementation varies across frameworks and lacks methodological consistency:

1) Layered Security: Frameworks such as the Industrial Internet Reference Architecture (IIRA) [18] and IoT Reference Architecture (IoT RA) [19] treat cybersecurity as a cross-cutting concern, providing granular security mechanisms applied at each architectural layer. Eckhart and Ekelhart [20] exemplify this by implementing state replication to detect anomalies at each architectural layer.

2) Security Analytics as an External Function: In frameworks such as the DT2SA [21], DTs function as data aggregators and processors, while security analytics is applied sequentially rather than being inherently integrated. Similarly, Coppolino et al. [22] use external applications to process and analyse twin data, treating cybersecurity as an add-on rather than an integrated feature.

3) Security by Design: This type of approach embeds cybersecurity from the initial design phase, rather than adding it through external applications [23]. For example, De Benedictis et al. [24] extend the general 5D model proposed by Tao et al. [25] with a dedicated cross-component security layer, ensuring foundational protection.

Despite the diversity in approaches, a systematic methodology for developing cybersecurity-relevant system functions based on stakeholder needs is still missing. A systematic mapping study [9] highlights key gaps:

- *Lack of Standardized Security Modelling*: out of 261 DT papers analysed, only 17 explicitly considered security as a quality attribute, despite its relevance under the ISO25010 standard of software product quality.
- *Absence of Multi-Domain Flexibility*: Most solutions are domain-specific, with 86% of analysed proposals being designed for individual sectors. This limits scalability of security mechanisms across infrastructures.
- *Reactive Rather than Proactive Security*: Many existing frameworks adopt a reactive approach on cybersecurity, where security measures are applied post hoc, on top of the existing layers, through external analytics or monitoring tools.

As defined by Uhlenkamp et al. [7], the "user focus" dimension in DTs distinguishes between single- and multi-user frameworks. However, recent research shows that DTs generate significantly more value when designed to support multiple stakeholders with different objectives, responsibilities, and decision-making capabilities [8]. Since stakeholder actions and decisions are interdependent and affect the DT ecosystem evolution [26], supporting these varied needs within a single DT environment improves situational awareness, enhances decision-making, and improves alignment across organizational layers. This is particularly important in cybersecurity, where roles such as IT staff, compliance officers, risk managers, and engineers require coordinated access and responsibilities.

Given that human factors such as lack of awareness are perceived as one of the most dangerous issues in cybersecurity [27], directly mapping stakeholder needs and actions to DT system requirements helps anticipate and mitigate these risks by ensuring the system supports the users effectively and contributes to adequate cybersecurity governance.

Few studies examine stakeholder involvement in DT design methodologies. For example, De Benedictis et al. [24] mention a Human-Machine Interface (HMI) suitable for various user types but does not explain how stakeholder needs are translated into system design. A conceptually closer approach is presented in [8], which explores stakeholders and their requirements for DTs; however, its stakeholder categories are general for Industry 4.0 [28] and differ from the cybersecurity focus central to our methodology. A cybersecurity-oriented DT for critical infrastructures has been proposed by Masi et al. [23] using reference models and layered viewpoints, however stakeholder concerns are handled only abstractly through these views.

Our work builds on the general methodology proposed by Lünnemann et al. [29] which maps user stories to functional requirements, by introducing a cybersecurity-specific focus

and a way to categorize scenarios accordingly. In doing so, we address an important methodological gap: how to systematically map stakeholder needs into functional requirements for DTs specifically designed for cybersecurity. Our approach provides a user-centric methodology that operationalizes Security by Design at the functional level.

III. INTACT Vision and Reference Architecture

The INTACT reference architecture is a modular, service-based DT framework designed for cybersecurity in IoT-to-Cloud infrastructures. It enables diverse stakeholders to secure and manage networked systems by supporting key objectives, such as device trustworthiness, information security, privacy, governance, employee training, and the simulation and evaluation of cybersecurity scenarios.

The architecture is structured across three layers: physical infrastructure, DT infrastructure, and DT services. The DT infrastructure replicates the physical system's behaviour, data, and control logic using twinning agents, while the DT services layer hosts cybersecurity capabilities provided by a dedicated toolbox. This toolbox may be deployed within the DT environment or accessed remotely (e.g., via a data space), depending on the use case. It offers interoperable services and a user dashboard for selecting, orchestrating, and monitoring security operations. These capabilities form the basis of six key functional requirement categories that support cybersecurity in DT, as illustrated in Figure 1:

1) Predictive Threat Intelligence Engine: processes data from automated inspection engines, twinning agents, and simulations to forecast threats and recommend mitigation;

2) Automated Software and Firmware Inspection Engine: uses static/dynamic analysis and AI-driven probes to identify vulnerabilities in system binaries and data flows;

3) Cybersecurity Orchestration Layer: coordinates responses across systems, integrating DT insights with live networks via interfaces and open connectors;

4) Dashboard and Assistance Layer: provides control over service deployment, integrates explainable AI outputs, and gives access to cybersecurity awareness training;

5) Digital and Broker Interfaces: enable communication with external data spaces, remote services, and interoperability with other DT environments;

6) User Interfaces: support stakeholder-specific views and interactions, including a virtual assistant.

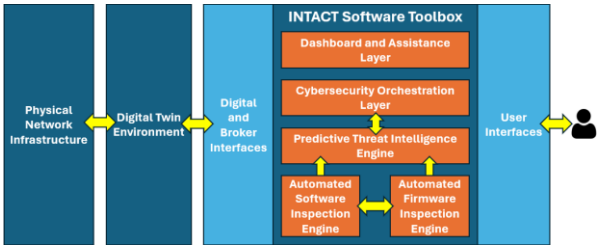

Figure 1. INTACT reference architecture, including the six functional cybersecurity elements previously mentioned.

Together, these functional components enable flexible, proactive cybersecurity services within DT ecosystems, designed to scale across domains while embedding cybersecurity at the architectural level.

IV. Methodology

The presented methodology is a structured, stakeholder-driven approach to deriving functional requirements for cybersecurity-specific DTs in critical infrastructures based on user stories. While inspired by the modular development sequence proposed by Lünnemann et al. [29], which extends Cockburn's functional requirements-based system design [30] with data flow considerations [31], this work follows a distinct trajectory focused on cybersecurity needs. Unlike Lünnemann et al. [29], who modularize scenarios to define DT sub-functions, our methodology uses a cybersecurity-specific taxonomy to categorize them. This approach keeps security concerns explicit throughout the process and aligns functional requirements with stakeholder cybersecurity objectives, rather than simply identifying necessary sub-functions. In this way, we maintain a continuous emphasis on security priorities and their traceability into the DT architecture.

Stakeholder input is first captured through user stories, which are grouped into operational scenarios. These scenarios are then categorized using a cybersecurity-specific taxonomy and ranked based on criteria such as potential impact and likelihood of occurrence. Finally, the categorized scenarios are mapped to functional requirements based on the INTACT reference architecture. This results in a complete and traceable path from user needs to system capabilities in the context of cybersecurity, maintaining conceptual clarity while being adaptable across critical infrastructure domains. The methodology lays a foundation for further development: identified functional requirements can be complemented by parallel data flow analysis [31] to derive the necessary system architecture, which can be iteratively refined as more sub-functions of the DT are developed.

A. Stakeholder Identification and User Story Definition

The process begins by identifying stakeholders whose responsibilities intersect with cybersecurity concerns in both use cases. Stakeholder selection is based on operational duties, regulatory obligations, and interaction with the DT environment. User stories are then derived through interviews with relevant personnel, including operational staff, cybersecurity managers, and supporting roles. All stories follow a standardized format to ensure consistency and documentation: "*As a <role>, I would like to <function>, so that <value>*".

B. Scenario Definition and Cybersecurity Taxonomy

User stories are clustered into scenarios that describe the system functions required to achieve the expected added value in individual, operational steps. While Lünnemann et al. [29] use standardized dimensions to describe scenarios,

this work introduces a tailored cybersecurity-specific taxonomy for identifying corresponding functional requirements. The taxonomy is derived from Article 21 of the NIS2 Directive [32], the EU-wide regulatory framework governing cybersecurity risk management in critical infrastructures. Based on this, we define three categories:

1) Compliance and Governance: describing formal policies, governance structures, and audit mechanisms required to meet legal and regulatory obligations;

2) Operational Security: covering everyday security processes that maintain a protective posture;

3) Threat Modelling and Intelligence: referring to the identification and analysis of potential risks and vulnerabilities.

Each of these categories includes four subcategories, shown in Table I, which provide a more granular structure for classifying and prioritizing scenarios. While NIS2 does not prescribe a fixed taxonomy, this interpretation reflects the coverage of its risk management requirements in a way that is both actionable and adaptable to the context of DT development. It is important to note that several user stories naturally span multiple subcategories (or even categories), given the inherent overlap between compliance, operational practice, and risk-analysis in real-world cybersecurity settings. Therefore, the taxonomy shown in Table I supports flexible mapping that preserves the integrity of stakeholder input while enabling structured prioritization based on both operational relevance and regulatory alignment.

TABLE I. CYBERSECURITY-FOCUSED TAXONOMY FOR DEFINING SCENARIOS

Category	Subcategory	Description
Compliance and Governance	Regulatory Compliance	Ensuring adherence to legal frameworks and industry-specific mandates.
	Policy Monitoring	Monitoring enforcement of security policies and detecting compliance violations.
	Access Governance	Managing identity, authentication, and access control to secure systems and data.
	Organizational Awareness	Providing security insights and reports to stakeholders and decision-makers.
Operational Security	Network Monitoring	Observing traffic, performance, and behavior of systems for anomalies.
	Incident Management	Identifying security events and coordinating timely, effective incident responses.
	Security Configuration	Testing, configuring, and validating defensive setups and security policies.
	Device and Data Protection	Securing endpoints, sensitive data, and communications from compromise.
	Continuity and Recovery	Ensuring operational resilience through backups, recovery strategies, and testing.
Threat Modeling and Intelligence	Vulnerability Analysis	Discovering weaknesses in systems or configurations that attackers might exploit.
	Threat Simulation	Simulating potential attacks and modeling future threat scenarios based on current data.
	Trust and Behaviour Analysis	Analyzing user/device behavior and trustworthiness to detect anomalies and malicious intent.
	Risk Assessment	Evaluating the likelihood and impact of threats to prioritize mitigation strategies.

C. Importance Ranking and Mapping to Functional Requirements

Once scenarios are categorized, they are ranked based on their relevance to the specific use case and potential impact on security posture. This prioritization helps focus system development on high-value or high-risk areas first.

Instead of modularizing scenarios into detailed system modules, functional requirements are derived from the scenario content at the capability level. These requirements describe the system capabilities required to address stakeholder needs as reflected in the scenarios, while maintaining flexibility and abstraction.

The INTACT toolbox provides one potential reference architecture, consisting of the following functional components: predictive threat intelligence engine, automated software and firmware inspection engine, cybersecurity orchestration layer, dashboard and assistance layer, digital and broker interfaces, and user interfaces. Nevertheless, the functional requirements themselves can be adapted to alternative architectures. The upstream methodology (spanning user stories, taxonomy, and scenario categorization) remains generalizable and is compatible with future cybersecurity-focused system applications and architectures.

V. APPLICATION TO CRITICAL INFRASTRUCTURE USE CASES

The proposed methodology is applied to two critical infrastructure scenarios: a healthcare facility and a nuclear reactor facility. For each, we first provide an overview of selected key stakeholders, their responsibilities, and main cybersecurity concerns. A mapping example is presented, connecting selected user stories of a specific stakeholder to categorized scenarios, and linking them to functional requirements within the DT environment according to the INTACT reference architecture.

A. Healthcare Facility Use Case

1) Stakeholders: Out of six identified stakeholders, we describe here three primary ones selected for their central role in hospital operation and security. *The Information, Communications, and Technology (ICT) Administrator* ensures network security by monitoring performance, detecting anomalies, simulating network changes, and enforcing access controls. *The Cybersecurity Engineer* focuses on threat detection and mitigation by analyzing security logs, predicting attack vectors, simulating incident responses, and integrating threat intelligence. *The Biomedical Operator* supports safe device operation by reporting system issues, responding to device alerts, and maintaining secure authentication. These roles collaborate closely to secure both IT systems and clinical devices.

2) Cybersecurity Concerns: These include compromise of medical IoT devices (e.g., imaging systems or wearables) that can falsify readings or disrupt patient care, breaches of patient data leading to security violations, ransomware locking critical hospital systems and records, phishing or social engineering enabling credential theft and malware

deployment, and data exfiltration through insufficient monitoring or access controls.

3) Example Mapping: Table II presents a selected mapping of the three highest-priority user stories for the *Biomedical Operator*, categorized and linked to DT functional requirements. Each follows the standardized format introduced earlier. While some user stories resulted in multiple functional requirements, a single example for each user story is listed for conciseness. In total, 25 user stories were derived across the six identified stakeholders.

TABLE II. BIOMEDICAL OPERATOR EXAMPLE MAPPING (HEALTHCARE FACILITY USE CASE)

User story ***(As a Biomedical Operator…)***	**Category**	**Subcategory**	**Functional Requirement**
I want to be alerted if a medical device is compromised by a cyberattack so that I can take appropriate action.	Operational Security	Device and Data Protection	Issue real-time alerts when connected medical devices show signs of compromise or abnormal behavior (Cybersecurity Orchestration Layer).
I want to authenticate fast and securely in the IT systems of the hospital so that I am efficient in my patient care.	Compliance and Governance	Access Governance	Support secure and rapid user authentication compatible with badges or biometric access systems (User Interface).
I want to report suspicious IT behavior easily so that I can contribute to the hospital's security.	Compliance and Governance	Organizational Awareness	Provide a streamlined user interface for staff to report suspicious IT behavior to the cybersecurity team (User Interface).

B. Nuclear Reactor Facility Use Case

1) Stakeholders: Out of five identified stakeholders, we describe here three primary ones selected for their central role in the operation and security of the infrastructure. *The Operational Technology (OT) System Engineer* ensures system integrity by monitoring components, detecting anomalies, running failure tests, and tracking configuration changes. *The IT Administrator* oversees IT/OT integration, manages tools, checks access logs, handles alerts, and performs cross-domain tests. *The Cybersecurity Analyst* detects and mitigates threats by correlating logs, simulating incidents, prioritizing defenses, and enforcing zero-trust policies. These stakeholders work in close coordination, with *the OT System Engineer* providing operational insights to *the IT Administrator* for secure system integration, while both collaborate with *the Cybersecurity Analyst* to ensure comprehensive threat detection and response across IT and OT domains.

2) Cybersecurity Concerns: These include false data injection that can mislead network stakeholders or automated safety operations, misconfigurations of components such as remote access protocols, firewalls or switches that create vulnerabilities, malware or ransomware propagation that disrupts operations or damages critical assets, and Distributed Denial-of-Service (DDoS) attacks that overload safety-related systems.

3) Example Mapping: Table III presents a selected mapping of the four highest-priority *IT Administrator* user stories, categorized, and linked to their corresponding DT functional requirements. Across the five identified stakeholders, a total of 18 user stories were derived.

TABLE III. IT ADMINISTRATOR EXAMPLE MAPPING (NUCLEAR REACTOR FACILITY USE CASE)

User story ***(As an IT Administrator…)***	**Category**	**Subcategory**	**Functional Requirement**
I want to integrate IT/OT network monitoring tools into a unified dashboard so that I can assess system security and performance.	Operational Security	Network Monitoring	Provide a real-time dashboard that aggregates and visualizes IT/OT network monitoring data (Dashboard and Assistance Layer).
I want to monitor access logs across both IT and OT systems so that I can detect unusual access attempts.	Compliance and Governance	Access Governance	Collect and correlate IT and OT access logs to detect suspicious or unauthorized activity (Cybersecurity Orchestration Layer).
I want to receive real-time alerts for anomalies in IT-OT data flows so that I can react quickly to threats.	Operational Security	Incident Management	Identify anomalies in IT-OT data flows and generate real-time alerts for potential threats (Predictive Threat Intelligence Engine).
I want to simulate IT-originating cyberattacks into OT systems so that I can evaluate response strategies.	Threat Modeling and Intelligence	Threat Simulation	Enable simulation of IT-based cyberattacks propagating into OT systems for response evaluation (Digital and Broker Interfaces).

The two use cases demonstrate the applicability of the proposed methodology across distinct critical infrastructures.

VI. CONCLUSION AND FUTURE WORK

This paper presented a methodology for systematically deriving functional requirements for cybersecurity-focused DTs by mapping stakeholder-derived user stories, categorized according to a cybersecurity-specific scenario taxonomy, to the INTACT reference architecture. The methodology was investigated through its application to two use cases in critical infrastructure (a healthcare facility and a nuclear reactor facility), demonstrating that the approach is valid and that the functional requirements derived are primarily informed by stakeholder needs rather than infrastructure type. By creating a mapping between stakeholder objectives and functional requirements, the methodology directly addresses human-factor risks, which are a recognized key vulnerability in cybersecurity.

However, it remains unclear whether the identified functional requirements fully reflect stakeholder objectives, as no downstream validation step is included. The current methodology models user needs upstream in a consistent and replicable way, but a validation procedure to confirm alignment during or after the implementation is still planned as future work. Another consideration is that outcomes may vary depending on the constraints of the chosen reference architecture. Interestingly, despite different stakeholders, functional requirements were also shared across use cases,

suggesting general applicability of the taxonomy, though some overlapping categories created modeling challenges.

This methodology offers a strong foundation for further development. Future steps will include supplementing this approach with data flow analysis to iteratively refine the sub-functions of the architecture by capturing additional details (e.g., data sources and sinks, potential data bottlenecks). This will support both the implementation and later validation of core functions against stakeholder needs.

ACKNOWLEDGMENT

The cybersecurity taxonomy used in this methodology was developed with valuable input from discussions with Bernhard Garn (SBA Research, Viena, Austria).

REFERENCES

[1] G. Smith, J. Brown, and A. Johnson, "Critical infrastructure protection: Requirements and challenges for the 21st century," International Journal of Critical Infrastructure Protection, vol. 8, no. 4, pp. 53-66, 2015.

[2] M. D. Nord, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in Transdisciplinary Perspectives on Complex Systems, F.-J. Kahlen, S. Flumerfelt, and A. Alves, Eds. Cham: Springer, pp. 85-113, 2017.

[3] Y. Jiang, S. Yin, K. Li, H. Luo, and O. Kaynak, "Industrial applications of digital twins," Philos. Trans. R. Soc. A Math. Phys. Eng. Sci, vol. 379, no. 2194, p. 20200360, 2021.

[4] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," IEEE Access, vol. 8, pp. 21980-22012, 2020.

[5] S. A. Varghese, A. D. Ghadim, A. Balador, Z. Alimadadi, and P. Papadimitratos, "Digital Twin-Based Intrusion Detection for Industrial Control Systems," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), pp. 611-617, 2022.

[6] M. H. Ḥomaei, O. Mogollón Gutiérrez, J. C. Sancho Núñez, and M. Ávila, "A review of digital twins and their application in cybersecurity based on artificial intelligence," Artif. Intell. Rev., vol. 57, no. 8, pp. 201-265, 2024.

[7] J.-F. Uhlenkamp, K. Hribernik, S. Wellsandt, and K.-D. Thoben, "Digital Twin Applications: A First Systemization of Their Dimensions," in Proc. 2019 IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC), pp. 1-8, 2019.

[8] R. Liyanage, N. Tripathi, T. Päivärinta, and Y. Xu, "Digital twin ecosystems: Potential stakeholders and their requirements," in Software Business, J. Springer and J. Manner, vol. 463, pp. 19-34, 2022.

[9] E. Ferko, A. Bucaioni, and M. Behnam, "Architecting digital twins," IEEE Access, vol. 10, pp. 50335-50350, 2022.

[10] D. M. Botín-Sanabria et al., "Digital twin technology challenges and applications: A comprehensive review," Remote Sens., vol. 14, no. 6, Art. no. 1335, 2022.

[11] G. Lampropoulos, X. Larrucea, and R. Colomo-Palacios, "Digital twins in critical infrastructure," Information, vol. 15, no. 8, Art. no. 454, 2024.

[12] R. Zhang, F. Wang, J. Cai, and Y. Wang, "Digital twin and its applications: A survey," Int. J. Adv. Manuf. Technol., vol. 123, no. 3, pp. 4123–4136, 2022.

[13] J. Zhang et al., "Cyber resilience in healthcare digital twin on lung cancer," IEEE Access, vol. 8, pp. 201900-201913, 2020.

[14] V. Rajasekar and K. Sathya, "Healthcare cyberspace: medical cyber physical system in digital twin," in Digital Twin Technologies for Healthcare 4.0, Chapter 7, pp. 113-130, 2023.

[15] H. Mengyan, X. Zhang, C. Peng, Y. Zhang, and J. Yang, "Current status of digital twin architecture and application in nuclear energy field," Annals of Nuclear Energy, vol. 202, p. 110491, 2024.

[16] Y. Guo, A. Yan, and J. Wang, "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 (POWERCON), pp. 1889-1892, 2021.

[17] X. Lou, Y. Guo, Y. Gao, K. Waedt, and M. Parekh, "An Idea of Using Digital Twin to Perform the Functional Safety and Cybersecurity Analysis," in GI-Jahrestagung, pp. 283-294, 2019.

[18] The Industrial Internet of Things: Reference Architecture, Version 1.9, Industrial Internet Consortium, 2019.

[19] ISO/IEC 30141:2024 - Internet of Things (IoT) - Reference architecture, International Organization for Standardization and International Electrotechnical Commission, Geneva, Switzerland, 2024.

[20] M. Eckhart and A. Ekelhart, "A Specification-based State Replication Approach for Digital Twins," in Proc. 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC '18), Toronto, ON, Canada, pp. 36-47, 2018.

[21] A. Alsarhan and M. Al-Jarrah, "Digital-twin-based security analytics for the Internet of Things," Information, vol. 14, no. 2, p. 95, 2023.

[22] L. Coppolino, R. Nardone, A. Petruolo, and L. Romano, "Building cyber-resilient smart grids with digital twins and data spaces," Applied Sciences, vol. 13, no. 24, p. 13060, 2023.

[23] M. Masi, G. P. Sellitto, H. Aranha, and T. Pavleska, "Securing critical infrastructures with a cybersecurity digital twin," Software Syst. Model., vol. 22, no. 2, pp. 1-19, 2023.

[24] A. De Benedictis, N. Mazzocca, A. Somma, and C. Strigaro, "Digital Twins in Healthcare: An Architectural Proposal and Its Application in a Social Distancing Case Study," IEEE J. Biomed. Health Inform., vol. 27, no. 10, pp. 5143-5154, 2023.

[25] F. Tao et al., "Five-dimension digital twin model and its ten applications," Comput. Integr. Manuf. Syst., vol. 25, no. 1, pp. 1-18, 2019.

[26] M. Tsujimoto, Y. Kajikawa, J. Tomita, and Y. Matsumoto, "A review of the ecosystem concept - Towards coherent ecosystem design," Technol. Forecast. Soc. Change, vol. 136, pp. 49-58, 2018.

[27] A. Hussain, A. Mohamed, and S. Razali, "A Review on Cybersecurity: Challenges & Emerging Threats," in Proc. 3rd Int. Conf. Networking, Information Systems & Security (NISS), Art. no. 28, pp. 1-7, 2020.

[28] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," Bus. Inf. Syst. Eng., vol. 6, pp. 239-242, 2014.

[29] P. Lünnemann, K. Lindow, and L. Goßlau, "Implementing digital twins in existing infrastructures," Forsch. Ingenieurwes., vol. 87, pp. 1-9, 2023.

[30] A. Cockburn, Writing Effective Use Cases, 16th ed. Boston: Addison-Wesley, 2006.

[31] A. Seegrün, P. Lünnemann, and K. Lindow, "Methodische Analyse bestehender Wertschöpfungssysteme zur Integration Digitaler Zwillinge [Methodical Analysis of Existing Value Creation Systems for the Integration of Digital Twins]," ProduktDatenJournal, no. 2, pp. 42-47, 2021.

[32] European Parliament and Council, "Directive (EU) 2022/2555 on high common cybersecurity level (NIS 2)," Off. J. Eur. Union, vol. L 333, pp. 80-152, 2023.