sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXXI No 1 2025

BEYOND THE MIRROR: DIGITAL TWIN CYBERSECURITY FOR NATIONAL RESILIENCE

Maurice DAWSON*, Andreas VASSILAKOS, Sandra MOORE***, Annamaria SZAKONYI******

***Illinois Institute of Technology, Chicago, USA**
****NOVA School of Law, Universidade NOVA de Lisboa, Lisbon, Portugal**
*****University of New Mexico, Albuquerque, USA**
******Independent Researcher, St. Louis, USA**
mdawson2@iit.edu, 10863@novalaw.unl.pt, sandram@unm.edu, drannamariaszakonyi@gmail.com

Abstract: *Digital twins, dynamic virtual representations of physical systems, are being employed in critical infrastructure sectors to enhance monitoring, simulation, and decision-making. The incorporation of digital twins, although offering significant benefits in operational efficiency and predictive maintenance, introduces new cybersecurity challenges. This includes vulnerabilities from real-time data streams, remote access points, and Industrial Internet of Things (IIoT) device integrations, which adversaries may exploit for espionage, sabotage, or system manipulation. Current cybersecurity standards are insufficiently addressing these threats and require enhancement to effectively manage the complex and hyperconnected nature of digital twin ecosystems. This paper analyzes cybersecurity challenges, drawing insights from historical cyberattacks on critical infrastructure and the emerging threats posed by Industry 4.0 and 5G technologies. It advocates for a multifaceted defensive approach encompassing zero-trust frameworks, advanced behavioral analytics, continuous surveillance, and cooperative governance via public-private partnerships and international collaboration. Thus, digital twins can bolster national resilience and infrastructural dependability in the digital era.*

Keywords: digital twin, industry 4.0, cyber security, critical infrastructure

1. Introduction

Real-time mirrored digital mirror systems are called digital twins. To create novel system designs, this computer model can be investigated, modeled, and tested [1]. More significantly, they are dynamic models—that is, they are constantly updated using real-time data rather than static models. They can mimic the functionality and behavior of the genuine physical thing since they rely on real-time data. Since the digital twins are a real-time replica, they offer the most accurate representation of the actual object for simulations. The digital twin passes through its lifecycle just like the real system. Both the digital twin and the physical object are used to experience the whole system's lifespan.

2. Need for Cyber Security

According to Juarez, Botti, and Giret [2], integrating Digital Twins with Multi-Agent Systems enhances autonomous decision-making in cyber-physical environments, but it also necessitates robust cybersecurity measures to protect sensitive industrial

DOI: 10.2478/kbo-2025-0010
© 2025 Maurice Dawson et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

data. Digital Twins serve as virtual replicas of physical assets, enabling real-time monitoring, diagnosis, prognostics, and simulation of operational scenarios. The integration of Digital Twins with Multi-Agent Systems (MAS) enhances autonomous decision-making and collaborative problem-solving in cyber-physical environments. However, despite their advantages, deploying Digital Twins presents challenges related to secure data exchange, system interoperability, and safeguarding against cyber threats [2]. Ensuring robust cybersecurity measures is critical to protecting sensitive data and maintaining the integrity of Digital Twin ecosystems, particularly as they become increasingly connected and integral to industrial processes.

3. Cyber Security Challenges in Industry 4.0

The advent of Industry 4.0 has revolutionized manufacturing through extensive automation, data exchange, and the integration of cyber-physical systems, the Internet of Things (IoT), cloud computing, and robotics. This hyperconnected environment enables smarter production processes and significantly increases vulnerabilities to cyber attacks. As manufacturing systems become more interconnected, they present a larger attack surface for cyber adversaries, leading to heightened risks of data breaches, system disruptions, and even physical damage to infrastructure [3, 4].

Historically, manufacturing has been targeted by cyber threats for decades, beginning with incidents like the 1982 attack on Siberia's power grid, illustrating that industrial targets have long been attractive to malicious actors [6]. With the evolution towards Industry 4.0, the threat landscape has become more complex, with attackers exploiting security weaknesses in IoT devices, sensors, and networked control systems. As these systems often lack comprehensive security controls, they are vulnerable to a range of cyber attacks, such as malware, hacking, and insider threats [7, 8].

While offering operational efficiencies, the hyperconnectivity characteristic of Industry 4.0 amplifies the potential impact of cyber incidents. For example, the infiltration of control systems in critical infrastructure like power plants or manufacturing facilities could lead to costly operational downtime or even physical destruction, as seen in previous incidents [9]. Ensuring the security of these systems from the design phase through ongoing operational management is crucial. This includes implementing security protocols, regular certification and accreditation processes, and adhering to emerging standards from organizations such as NIST and ISO [10]. Given the rising sophistication of cyber threats targeting industry, it is essential for organizations to adopt a security-first approach, focusing on risk management, proactive vulnerability assessments, and continuous monitoring to safeguard critical manufacturing assets against cyber adversaries in this interconnected era [11].

4. Manufacturing Sector

The manufacturing sector has increasingly become a prime target for sophisticated cyberattacks due to its growing dependence on digital infrastructures and complex interconnected systems brought about by Industry 4.0 advancements. The integration of technologies such as IoT, mobile computing, and BYOD amplifies operational efficiencies but simultaneously introduces significant security vulnerabilities [4]. Attackers exploit these dependencies to cause disruptions, impact production quality, brand reputation, and even create risks to human health and safety. The paper emphasizes that the root cause of many cyber threats in manufacturing arises from these interdependencies, necessitating a comprehensive approach to cybersecurity that addresses technical, organizational, and human factors [3, 5]. A significant challenge identified is the shallow cyber awareness and diagnostic capabilities within manufacturing industries, contributing to cyberattacks' success. This gap largely stems from the

friction and limited trust between industrial process experts and IT professionals, alongside insufficient training tailored to manufacturing-specific cybersecurity needs [3]. People remain the primary vulnerabilities in industrial control systems, as highlighted by reports indicating that lack of staff security awareness and inadequate vetting are major contributors to severe security breaches [11]. To address this, there is an urgent demand for educational programs that cultivate cybersecurity proficiency specifically in the manufacturing context, alongside business practices that view cybersecurity as an essential prerequisite for customer trust and market engagement [11].

4.1. Key Standards

Digital twin technology is crucial for the progression of smart manufacturing, as it facilitates digital representations of physical manufacturing components that improve process optimization, real-time monitoring, and lifecycle management. The implementation of digital twins encounters considerable problems, such as interoperability, consistency, security, and scalability among various systems and providers. Standards are essential in tackling these difficulties by offering uniform terminology, frameworks, interface standards, and validation procedures that guarantee the compatibility, reusability, and reliability of digital twins. The Organization for International Standardization (ISO) 23247 series serves as a comprehensive digital twin framework for manufacturing, illustrating continuous standardization initiatives that provide a generic reference architecture to facilitate efficient and successful digital twin creation [12, 13, 14, 15, 16, 17]. Furthermore, other Standards Development Organizations and consortia, including IEC, IEEE, and OMG, contribute to supplementary standards and best practices [18, 19, 20, 21, 22]. Future standardization efforts will focus on domains such as digital twin composition, digital threads, cognitive digital twins, and integration with new technologies, including the metaverse [23]. Collaborative standardization activities are essential for promoting interoperability, expediting acceptance, decreasing development costs, and allowing manufacturers to construct, manage, and implement digital twins more swiftly and economically [9, 13]. Table 1 below illustrates digital twin standards in manufacturing.

Table 1 Digital Twin Standards in Manufacturing

Standard/Framework	Organization	Focus	Reference
ISO 23247	ISO	Framework for manufacturing digital twins: architecture, info exchange, components	[20]
ISO/IEC 30173	ISO/IEC	Concepts and terminology for digital twins	[21]
ISO/IEC TR 30172	ISO/IEC	Use cases for digital twins in IoT	[22]

IEC 63278-1	IEC	Asset Administration Shell (AAS) for industrial applications	[23]
IEEE P2806	IEEE	Architecture for digital representation in factory environments	[24]
MTConnect-OPC UA Companion Specification	MTConnect & OPC	Standard for device-level interoperability and real-time data sharing	[25]
OPC Unified Architecture (OPC UA)	OPC Foundation	Machine-to-machine communication protocol for automation	[26]
Standard/Framework	**Organization**	**Focus**	**Reference**
ISO 10303 (STEP)	ISO	Standard for exchanging product model data	[27]
ISO 23952 (QIF)	ISO	Integrated model for manufacturing quality information	[28]
Digital Twin Core Conceptual Models	IIC	Core concepts and services for digital twin interoperability	[29]
Digital Twin and AAS White Paper	IIC & Plattform I4.0	Joint concept alignment and asset administration shell design	[30]
Digital Twin VV50 VVUQ Guidelines	ASME	Validation, verification, and uncertainty quantification for computational models	[18]

ISO 23247 Reference Architecture Analysis	NIST	Review and evaluation of functional alignment of digital twin architectures	[19]
ISO 23247 Industry Case Study	Wallner et al.	Application of ISO 23247 in flexible manufacturing environments	[31]
National Academies Digital Twin Gaps Report	National Academies	Research gaps and strategic future directions for digital twins	[32]

5. Revisiting Threats to Critical Infrastructure

Dawson et al. [44] highlight the urgent and growing threat of cybersecurity to US vital infrastructure in Table 2. Cyberattacks on 16 critical industries can harm health, safety, and the economy. The study uses Stuxnet and Flame to show how cyberwarfare has become a strategic weapon against ICS, such as SCADA and PLCs.

The scope and effectiveness of government responses, particularly PPD 21 and the NIST Cybersecurity Framework, are assessed. Industry 4.0 and 5G technologies enhance the attack surface due to hyperconnectivity and embedded IoT devices. The authors critique present policies' limited legal reach and regulatory enforcement, highlighting data theft and system manipulation concerns. The report recommends AI-driven threat detection, continuous monitoring, and behavioral analytics to protect these infrastructures. It stresses labor development and automation as crucial to sustainable security. Digital Twins are not addressed in this work. Overall, threats remain.

Table 2 Threats to Critical Infrastructure and Examples (Adapted and referenced from Dawson et al., 2021)

Threat Type	Example	Reference
Malware targeting SCADA systems	Stuxnet attacked Iranian nuclear centrifuges	[34]
Cyber espionage	Flame malware stealing data from Iran’s oil infrastructure	[35]
Data theft and integrity attacks in IoT	IoT thermostat manipulated to disrupt HVAC and data flow	[36]

Network activity inference in smart homes	Inferring home occupancy from network traffic	[37]
Cyber-physical sabotage	Power grid malware is causing blackouts or system failures	[38, 39]
Infrastructure jamming via 5G disruption	Disrupting 5G to disable device communications	[40]
Location tracking via 5G triangulation	Using signal strength to geolocate users	[41]
Nation-state cyberattacks	Coordinated attacks to cripple critical infrastructure systems	[42]
Workforce shortage in cybersecurity	Lack of skilled personnel to manage and respond to threats	[43]

6. Digital Twin Threats

The Digital Twins let an enemy utilize the simulated system to practice attacking the real thing. This virtual environment allows users to test weaknesses and identify ways to attack without worrying about being caught or causing damage immediately. The digital twin also acts as a digital object for learning how to take advantage of the changing threat scenario by pushing limits to get an edge. This kind of arrangement can mimic the goals and actions of black hat, grey hat, and white hat hackers, who have different psychological qualities and goals [43].

For instance, black hat hackers, usually motivated by excitement and personal gain, could use digital twins to practice breaking into systems without permission and devise ways to cause trouble. On the other hand, grey hats, known for being against authority, might use the environment to test security flaws in a moral or immoral way. At the same time, white hat hackers, who are legal and have traits like Machiavellianism and narcissism, could employ digital twins to make defenses stronger and predict attacks [45].

Also, the way these groups think about the chance of getting caught affects how they hack in different ways: black and gray hat hackers are less likely to do it than white hats, who may be motivated by ethics and pride in their work. Digital twins are a flexible way to simulate and compare different hacking scenarios, improving security by helping us understand hackers' different reasons and actions [45]. This method fits with the wider idea that hacking behavior is affected by more than just opportunity. It is also affected by psychological qualities, a need for excitement, and careful risk evaluations, all of which can be modeled and studied well in digital twin environments.

7. Conclusions

As critical infrastructure sectors progressively implement digital twins, cybersecurity becomes an essential responsibility to protect these real-time mirrored systems' accuracy, integrity, and availability. The progression of cyber threats—from specific malware such as Stuxnet and Flame to data manipulation within IoT ecosystems—highlights the

increased hazards associated with interconnected digital twin infrastructures. Mitigating these risks necessitates progression beyond conventional perimeter defenses to integrated cybersecurity frameworks that utilize zero-trust principles, encryption, AI-enhanced threat detection, and ongoing behavioral monitoring. Furthermore, addressing disparities in labor proficiency, legal frameworks, and technological standards is crucial for the sustainable security of digital twins. Public-private partnerships and international collaboration will be essential in aligning security protocols and disseminating threat intelligence. Executing these methods will guarantee that digital twins realize their potential for improved operational insight and efficiency while maintaining national resilience and safeguarding critical infrastructure security.

Conflict of Interest Statement

The research item does not necessarily represent the views of the U.S. Government, Department of State, or any other U.S. Government agency. The views and work presented within this item strictly represent the authors' academic work.

References

[1] Batty, M. (2018). Digital twins. Environment and Planning B: Urban Analytics and City Science, 45(5), 817-820.

[2] Juarez, M. G., Botti, V. J., & Giret, A. S. (2021). Digital twins: Review and challenges. Journal of Computing and Information Science in Engineering, 21(3), 030802.

[3] Dawson, M. (2018). Cyber security in industry 4.0: The pitfalls of having hyperconnected systems. Journal of Strategic Management Studies, 10(1), 19-28.

[4] CISA (n.d.). Critical manufacturing sector Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sectore Security Agency CISA

[5] Ferko, M., et al. (2023). Standardisation in Digital Twin Architectures in Manufacturing. IEEE 20th International Conference on Software Architecture (ICSA), L'Aquila, Italy, 70-81. https://doi.org/10.1109/ICSA56044.2023.00015

[6] Miller, D. C. Rowe, A survey scada of and critical infrastructure incidents., RIIT 12 (2012) 51–56.

[7] Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. (2011, March). Attacks against process control systems: risk assessment, detection, and response. In Proceedings of the 6th ACM symposium on information, computer and communications security (pp. 355–366). ACM.

[8] Chahid, Y., Benabdellah, M., & Azizi, A. (2017, April). Internet of things security. In 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS) (pp. 1–6). IEEE.

[9] Creery, A., & Byres, E. J. (2005, September). Industrial cybersecurity for power system and SCADA networks. In Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual (pp. 303–309). IEEE.

[10] Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. Future Generation Computer Systems, 74, 385–392.

[11] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32-74.

[12] Shao, G. (2023, September). Manufacturing Digital Twin Standards. In Proceedings of the ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems (pp.370-377)

[13] Attaran, M., & Celik, B. G. (2023). Digital Twin: Benefits, use cases, challenges, and opportunities. Decision Analytics Journal, 6, 100165. https://doi.org/10.1016/j.dajour.2023.100165
[14] Sharma, A., Kosasih, E., Zhang, J., Brintrup, A., & Calinescu, A. (2022). Journal of Industrial Information Integration, 30, 100383. https://doi.org/10.1016/j.jii.2022.100383
[15] Sharma, A., Kosasih, E., Zhang, J., Brintrup, A., & Calinescu, A. (2022). Digital Twinds: State of the art theory and practice, challenges, and open research questions. Journal of Industrial Information Integration, 30, 100383. https://doi.org/10.1016/j.jii.2022.100383
[16] Shao, G. (2021). Use Case Scenarios for Digital Twin Implementation Based on ISO 23247. Advanced Manufacturing Series (NIST AMS), National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AMS.400-2
[17] Attaran, M., & Celik, B. G. (2023). Digital Twin: Benefits, use cases, challenges, and opportunities. Decision Analytics Journal, 6, 100165. https://doi.org/10.1016/j.dajour.2023.100165
[18] Shao, G., & Helu, M. (2023a). Framework for A Digital Twin in Manufacturing: Scope and Requirements. Manufacturing Letters, 24, 105-107.
[19] Shao, G. (2023b, September). Manufacturing Digital Twin Standards. In Proceedings of the ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems (pp.370-377).
[20] International Organization for Standardization. (2021). ISO 23247-1: Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles.
[21] International Organization for Standardization. (2021). ISO/IEC 30173: Digital twin, Concepts and terminology.
[22] International Organization for Standardization. (2023). ISO/IEC TR 30172: Internet of Things (IoT). Digital twin. Use cases. https://www.iso.org/standard/81578.html
[23] International Electrotechnical Commission. (2023). IEC 63278-1:2023 ED1 Asset Administration Shell for industrial applications - Part 1: Asset Administration Shell structure. https://www.iec.ch/dyn/www/f?p=103:38:25763300038578:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,103536
[24] Institute of Electrical and Electronics Engineers. (2019). IEEE-P2806 System architecture of digital representation for physical objects in factory environments. https://standards.ieee.org/project/2806.html
[25] MTConnect Institute. (2022). MTConnect standardizes factory device data. https://www.mtconnect.org/
[26] OPC Foundation. (2023). OPC-UA services specification. https://opcfoundation.org/developer-tools/specifications-unified-architecture
[27] International Organization for Standardization (2021). ISO 10303: Industrial automation systems and integration - product data representation and exchange - Part 1: Overview and fundamental principles. https://www.iso.org/standard/72237.html
[28] International Organization for Standardization (2020). ISO 23952: Automation Systems and Integration – Quality Information Framework (QIF) - An Integrated Model for Manufacturing Quality Information. https://www.iso.org/standard/77461.html
[29] Lin, S., Kym Watson, K., Shao, G., Stojanovic, L. & Zarkout, B. (2023). Digital twin core conceptual models and services. Industry IoT Consortium. Retrieved https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/10/Digital-Twin-Core-Conceptual-Models-and-Services_20231102.pdf

[30] Boss, B., Malakuti, S., Lin, S.-W., Usländer, T., Clauer, E., Hoffmeister, M., & Stojanovic, L. (2020). Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0, an Industrial Internet Consortium and Plattform Industrie 4.0 Joint White paper. https://www.iiconsortium.org/pdf/Digital-Twin-and-Asset-Administration-Shell-Concepts-and-Application-Joint-Whitepaper.pdf
[31] Wallner, B., Zwölfer, B., Trautner, T., & Bleicher, F. (2023). Digital Twin Development and Operation of a Flexible Manufacturing Cell using ISO 23247. Procedia CIRP, 120, 1149–1154. https://doi.org/10.1016/j.procir.2023.09.140
[32] National Academies of Sciences, Engineering, and Medicine. (2023). Foundational Research Gaps and Future Directions for Digital Twins. National Academies Press. http://nap.nationalacademies.org/26894
[33] Fischer, O. P., Matlik, J., Schindel, W., French, M., Kabir, M., Ganguli, J., Hardwick, M., Arnold, S., Byar, A., Lewe, J.-H., Mahadevan, S., Duncan, S., Dong, J., Kinard, D., & Maiaru, M. (2022). Digital Twin: Reference Model, Realizations, and Recommendations. https://doi.org/10.1002/inst.12373
[34] Denning, D. E. (2012). Stuxnet: What has changed? Future Internet, 4(3), 672–687. https://doi.org/10.3390/fi4030672
[35] Munro, K. (2012). Deconstructing Flame: The limitations of traditional defences. Computer Fraud & Security, 2012(10), 8–11. https://doi.org/10.1016/S1361-3723(12)70103-4
[36] Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K., & Kamhoua, C. (2017, November). Preserving data integrity in IoT networks under opportunistic data manipulation. In 2017 IEEE DASC/PiCom/DataCom/CyberSciTech (pp. 446–453). https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.86
[37] Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016, May). Is anybody home? Inferring activity from smart home network traffic. IEEE Security and Privacy Workshops, 245–251. https://doi.org/10.1109/SPW.2016.44
[38] Robles, R. J., Choi, M. K., Cho, E. S., Kim, S. S., Park, G., & Lee, J. (2008). Common threats and vulnerabilities of critical infrastructures. International Journal of Control and Automation, 1(1), 17–22.
[39] Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: Center for Strategic & International Studies. [40] Lichtman, M., Rao, R., Marojevic, V., Reed, J., & Jover, R. P. (2018, May). 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In 2018 IEEE ICC Workshops, 1–6. https://doi.org/10.1109/ICCW.2018.8403660
[41] Ge, X., Ye, J., Yang, Y., & Li, Q. (2016). User mobility evaluation for 5G small cell networks based on individual mobility model. IEEE Journal on Selected Areas in Communications, 34(3), 528–541. https://doi.org/10.1109/JSAC.2016.2525639
[42] Wilson, C. (2014). Cyber Threats to Critical Information Infrastructure. In Cyberterrorism (pp. 123–136)
[43] Dawson, M (2018). Cybersecurity in Industry 4.0: The pitfalls of having hyperconnected systems. Journal of Strategic Management Studies, 10(1), 19–28.
[44] Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. Land Forces Academy Review, Vol. XXVI, No. 1(101), 69–75. https://doi.org/10.2478/raft-2021-0011
[45] Gaia, J., Sanders, G.L., Sanders, S.P. Upadhyaya, S., Wang, X., & Yoo, C.W. (2021). Dark traits and hacking potential. Journal of Organizational Psychology, 21(3), 23-46.