Journal of New Technology and Materials

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

Digital Twin Vulnerabilities in Industrial Cyber-Physical Systems: A Security Framework for Threat Simulation and Containment

Prof. Karim Benali[1], Dr. Samir Haddad[2]
[1]Department of Cyber-Physical Systems, University of Science and Technology Houari Boumediene, Algeria
[2]Institute of Computer Engineering, University of Oran, Algeria

Abstract
As part of Industry 4.0, digital twins (DTs) and industrial cyber-physical systems (CPS) have transformed predictive maintenance, real-time control, and operational efficiency. Data synchronization, communication interfaces, model logic, and deployment procedures are just a few areas where these integrations have shown serious flaws. This article presents a comprehensive security framework for DT-enabled CPS that can simulate and contain threats. It starts with classifying unique digital twin vulnerabilities and looking at the danger zone using situational modeling. For a more secure system, they offer a multi-tiered design with features like sandboxing, anomaly detection, model rollback, and quarantine. The architecture outperforms conventional CPS-only defenses in terms of detection accuracy, reaction time, and operational downtime in a smart factory case study. In order to safeguard the rapidly expanding DT-CPS ecosystem, this study shows that we need to look for integrated security solutions that combine monitoring, containment, and recovery.
Keywords: Digital Twin, Cyber-Physical Systems, Industrial Security, Threat Simulation, Vulnerability, Digital Twin Attacks, Cyber Defense Framework, Digital Shadows

Chapter 1: Introduction

1.1 Background and Motivation

Industry 4.0 and industrial Cyber Physical Systems (CPS) have made digital twins—representations of physical systems that are continuously updated with data from sensors and virtual models—an increasingly important component of CPS (Zhao, Foo, & Tian, 2022). DTs make it easier to manage complicated industrial assets through real-time monitoring, predictive maintenance, simulation, and optimization (Patel et al., 2024). By acting as a virtual mirror, DT enhances situational awareness and operational performance in CPS contexts, where the real-world process is strongly integrated with computing and networking (Patel et al., 2024; Zhao et al., 2022). The industrial CPS already has a large attack surface, but adding DTs makes it much worse. The main cause is the interconnectedness and interoperability of the physical and virtual worlds, which allows for two-way communication and leaves openings for attackers to take advantage of. According to Varghese et al. (2022) and ECSO WG (6/2023), physical systems and virtual twins are both susceptible to DOS assaults, command injection, insider compromise, and tampering. Notably, DT-based IDSs need to handle complicated attack scenarios that mimic real-world time, including command insertion and measurement spoofing (Varghese et al., 2022).

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

1.2 Problem Statement

Although DTs have a beneficial effect on operations, they also introduce new security vulnerabilities. The interplay between virtual twins and physical system vulnerabilities is currently ignored by security frameworks, which instead concentrate on individual instances of CPS or DT subsystems. Industrial control systems are vulnerable to cascading failures caused by this monitoring. Current literature on DT CPS studies lacks comprehensive frameworks that include vulnerability enumeration and the ability to realistically simulate and contain threats in DT CPS systems (Patel et al., 2024; Zhao et al., 2022; ECSO WG6, 2023).

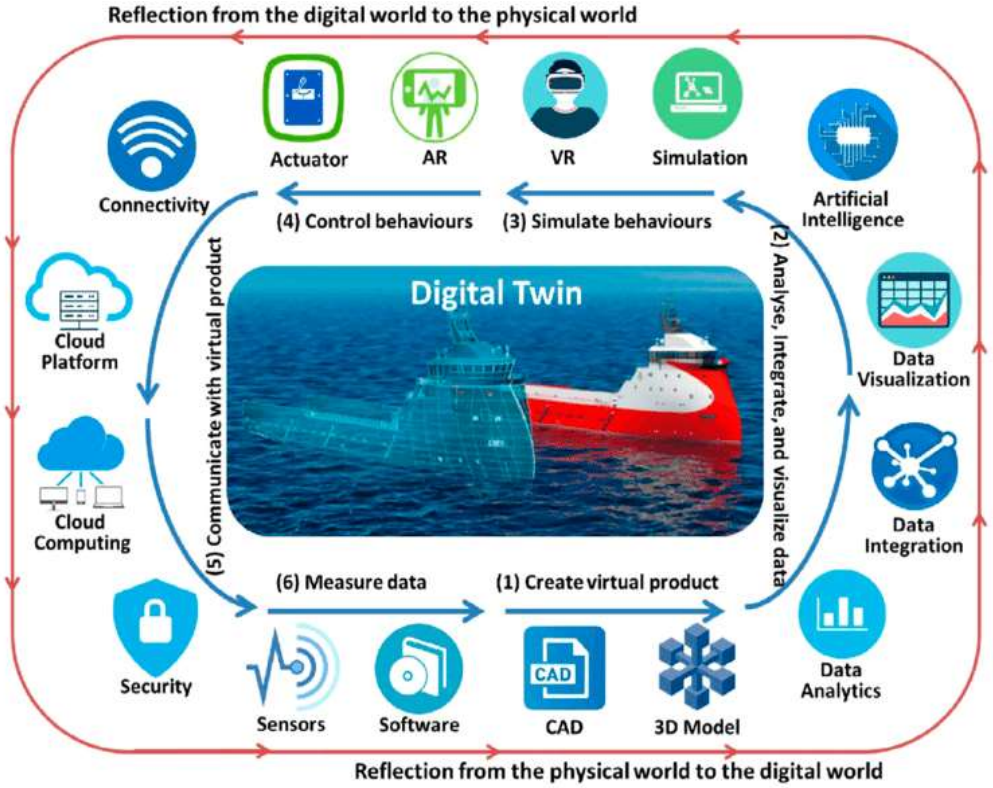

Figure 1: Digital Twin

1.3 Research Objectives

The purpose of this article is to provide a structured security model that is specific to industrial cyber-physical systems (CPS) that are enabled by digital twins (DT). It aims to accomplish three primary things: first, digital twin vulnerabilities in industrial CPS systems should be identified and categorized; second, threat simulation frameworks should be put in place to model and test realistic assaults on DTs and their direct interfaces, such as command injection, data poisoning, and malevolent code injection; and third, there should be an evaluation of these frameworks. Uses Thirdly, in order to construct a system that is more resilient to physical and virtual threats, it is necessary to create defense and mitigation mechanisms. These mechanisms should adhere to secure design principles and include techniques for anomaly detection, dynamic confinement, and recovery.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

2. Background and Related Work

2.1 Digital Twin Architecture in Industrial CPS

Digital twins (DTs) in industrial CPS settings typically have a physical layer, a virtual model, and data links. Operating technology (OT), edge devices, sensors, actuators, and the physical world are all part of the physical layer (Botin Sanabria et al., 2022, as quoted in Patel et al., 2024). A data-driven or model-driven approach allows the physical system to continually control the digital model, which is a dynamic virtual reproduction of the actual system (Wang et al., 2023; Patel et al., 2024). Connectors for data, such as Internet of Things gateways, edge nodes, and communication interfaces, allow for the ingestion, synchronization, and two-way control of real-time data between the twin and the actual world (Wang et al., 2023; Patel et al., 2024). The various interfaces that make up the communication channels in DT-enabled CPS are:

- **Physical-to-digital**: Internet of Things sensors transmit data to the DT, typically through cloud or edge computing.
- **Digital-to-physical**: The virtual model communicates with the actuators via control commands or adjustments.
- **Inter-twin communications**inter-DT communication for the purpose of coordinating or simulating many systems.
- **Human–machine interfaces**: Interfaces between operators and simulations, such as dashboards or control panels (Wang et al., 2023; Patel et al., 2024).

Interactions between operators are mediated by dashboards, control panels, or simulation APIs (Wang et al., 2023; Patel et al., 2024).

2.2 Threat Landscape in CPS and Digital Twin Integration

The combination of Cyber-Physical Systems (CPS) and Digital Twins opens the door to a wide array of sophisticated dangers. Bypassing the operator interface, digital model, and physical sensors allows cyber adversaries to exploit the data flow and two-way linkages. For instance, unauthorized individuals can gain control of the system or steal operational intelligence by utilizing real-time telemetry data. While invasive command injection can exploit passwords or unprotected APIs, the opposite is true. There is an increase in data integrity risks with digital twins: The physical CPS is vulnerable to erroneous choices and control orders in the event that an attacker gains access to the incoming sensor data or the virtual model's outputs. In light of the fact that inter-system communication increases the attack surface, you are correct. More attention is needed in both areas for devices that facilitate the Internet of Things and remote interfaces.

2.3 Review of Existing Security Models

Present methods for ensuring the integration of CPS and DT have substantial downsides. While traditional CPS security architectures pay attention to perimeter protection, network segmentation, and OT-specific security designs, they pay little attention to the specifics of DT systems. There has been promising experimental research on intrusion detection using DT. Industrial control systems are susceptible to attacks such as command injection, denial of service, and measurement tampering; Varghese et al. (2022) detail the implementation of a DT-based intrusion detection

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

system to monitor these systems. They were able to attain a high F1 Score and a classification latency of less than 0.1 seconds when they used their stacked ensemble classifier (Varghese et al., 2022).

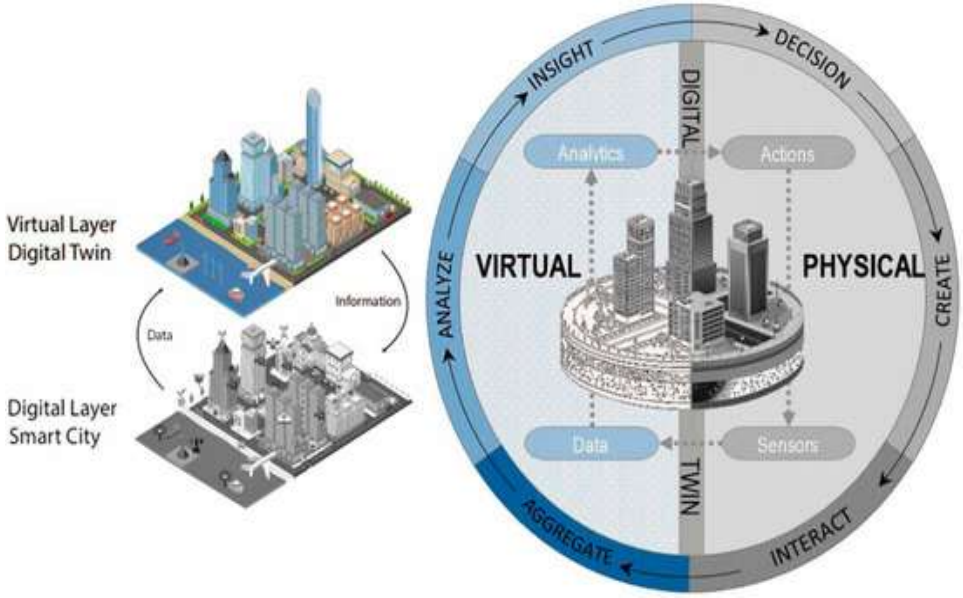

Figure 2: The twin city is the one that is made possible through the smart city: data sensors (physical-digital model) and new information, knowledge (virtual-DT model) allows adjustment of the city and its subsystems

There is a bias in these solutions toward detection, concentration, and restoration, though. Other works aim to contain and identify anomalies within the system, run simulations to assess its vulnerability to risk, and enhance situational awareness thereof; however, they do not promote such integrative approaches to containment or resilience (Eckhart et al., 2019; Wang et al., 2023). Digital twins (DTs) that aid in security operations but lack standardization in containment tactics and cycle resilience have been the subject of more contemporary discussions on security-enhancing digital twins (SEDTs). While certain digital twin-based cybersecurity models have matured—most notably in the areas of intrusion detection systems (IDS) and anomaly detection—none of them fully integrate security risk assessment, simulation of threats, containment, and recovery on both the digital twin and CPS scales.

3. Taxonomy of Digital Twin Vulnerabilities

3.1 Data-Level Vulnerabilities

Real-time data poisoning: Machine learning and artificial intelligence models built on data collected in real-time from sensors are the backbone of digital twins. In federated learning systems in particular, adversaries might poison inputs or model parameters, leading to poor performance or misclassification and severely limiting prediction.

Synchronization inconsistencies: The physical and digital representations of systems must remain in sync. Discordances between DT and CPS states might arise due to communication

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

delays, an improper protocol selection, or an overloaded network. It is possible to covertly exploit these discrepancies to trick operators into doing the wrong thing.

3.2 Communication and Interface Risks

Industrial cyber-physical systems (CPS) that incorporate digital twins have communication and interface pathways that are both vital and susceptible to attack. These gateways connect the digital and physical systems; they usually have APIs, communication protocols (such Modbus, OPC-UA, or MQTT), and interfaces hosted on the cloud. On the other hand, these interfaces leave vulnerable areas that malicious actors can use to steal critical data or impede system operations. Application Programming Interface (API) exploitation is a common security risk. In this type of attack, the attacker takes advantage of an unprotected or poorly protected API to send out harmful commands, gain access to sensitive information, or bypass the identification procedure. Protocol spoofing is another danger; in this type of attack, the perpetrators pose as legitimate users in order to fool the system into believing everything is normal so that they can modify the underlying operations. Furthermore, systems lacking adequate authentication or encryption for data flow between CPS and digital twins are more vulnerable to man-in-the-middle (MitM) attacks. Competitors can trade bogus information or change instructions that are passing through if they intercept and corrupt the transmissions. This leads to the twin making bad decisions or acting inappropriately inside the system since their view of the physical system is compromised. The lack of a unified security standard or encryption in heterogeneous environments, where equipment from different manufacturers and different generations coexist, increases the likelihood of these kinds of breaches. The integrity and reliability of digital twin processes in industrial CPS facilities are dependent on the safety of their internal communication and interface channels.

3.3 Model and Logic Exploits

For digital twins to be faithful representations of their physical counterparts, reliable and secure simulation logic is essential. In safety-critical settings, such as smart grids or industrial facilities, these systems are especially vulnerable to corruption from adversarial code or algorithmic parameters, which can lead to misleading simulations, inaccurate diagnostics, or control advice that is time-inappropriate (Suhail et al., 2023). Furthermore, in cases where proper security measures are not in place, proprietary model settings and simulation logic are used, making them vulnerable to copying or reverse engineering. Leaks like these put IP at risk and provide bad actors a chance to create malicious copies, which they can then use for infiltration, sabotage, or cyber-spying.

3.4 Deployment and Update Risks

Due to the widespread usage of Over-The-Air (OTA) update technologies, digital twin systems are particularly susceptible to vulnerabilities caused by updates. Updates without built-in cryptographic authentication or secure boot enforcement leave devices vulnerable to eavesdropping and the introduction of tainted or malicious firmware or model components. The use of cloud computing, third-party services, and hardware all increase the risks in the supply chain. Any resident danger can find their way into the DTCPS ecology through backdoors caused

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

by a maliciously poisoned part or outmoded libraries or providers. System dependability and trust could be jeopardized if these supply chain issues go unattended.

4. Threat Simulation Methodology for Digital Twins

In order to evaluate and enhance the robustness of cyber-physical systems (CPS) that integrate digital twins, a strategy for threat simulation needs to be put in place. Researchers and practitioners can uncover vulnerabilities, evaluate potential implications, and develop effective defensive methods through the simulation of settings and assault scenarios.This chapter lays out a theoretical framework for conducting impact assessments, which incorporates models of potential attacks, scenarios for configuring a simulation environment, and other elements that together provide a holistic view of cybersecurity readiness in digital twin deployment.

4.1 Simulation Environment Setup

Before we can assess digital twins' security, we need to build a model of a realistic, controlled simulation environment. The first step is to set up a virtual twin sandbox, which isolates the digital twin from the real-world operational systems while keeping it functionally correct enough to conduct useful tests. By design, sandboxing allows for the safe simulation of assaults without endangering real-world CPS processes, and it also encourages repetition, which is necessary for making comparisons. This virtualized environment incorporates threat emulators and intrusion agents to mimic the actions of real-world attackers. These tools offer an interactive and dynamic testing environment by simulating numerous attack vectors, such as protocol, spoofing, and command injection, among others. Furthermore, an adaptive environment becomes reactive and analytically sound by capturing the oblique impacts of simulated attacks via real-time telemetry feedback channels between the physical and virtual layers.

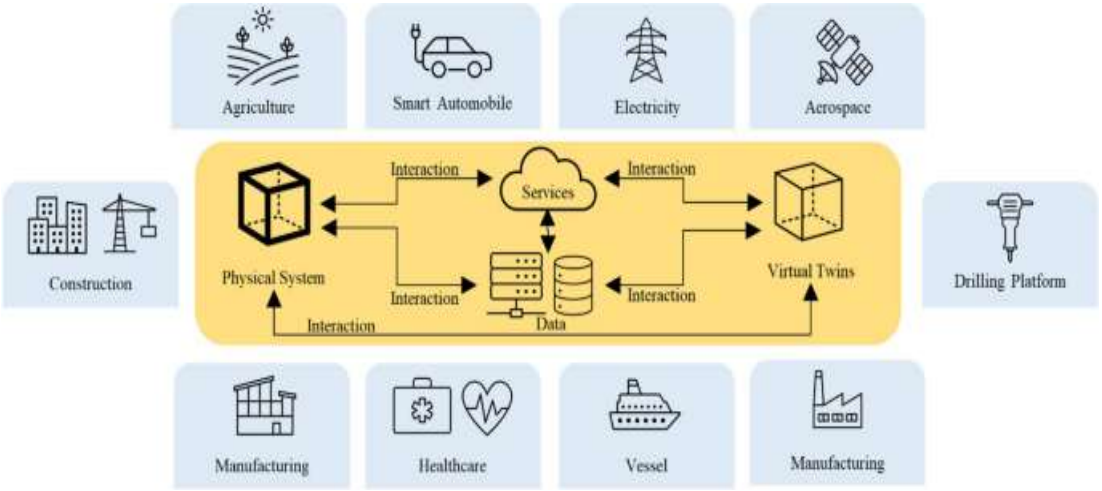

Figure 3: Application of Digital Twin

4.2 Attack Scenario Modeling

To find out how vulnerable digital twin systems are, it is important to construct realistic and technically sound attack scenarios. Insider threat simulation, in which authorized users do damage

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

to integrity either on purpose or by accident, is the main culprit. The CPS decision-making process may be tainted if this integrity was disrupted in any manner, including by changing telemetry data, triggering unauthorized upgrades, or even manipulating analytics results within the twin. Another form of assault on a digital twin that is considered severe alters the twin's decision-making logic, prediction models, or actuation routines by stealing its logic engine. Mechanisms, weak APIs, or malicious updates can all launch this kind of assault, which can then ripple through the CPS layer. Persistence, lateral mobility, and the potential for undetected stealth campaigns should all be factored into scenario modeling. This is done so that things like time-sensitive and safety-sensitive events may be understood, along with the repercussions that go beyond individual processes and interprocess implications.

4.3 Impact Assessment Metrics

To determine how effective threat simulations are and how they affect system performance, reaction, and integrity, various quantitative metrics are required. A measure of the accuracy of predictions generated with a digital twin in relation to the actual behavior of the physical system under assault is the twin deviation rate. The model's logic is corrupted or out of sync if the deviation rate is rising. Latency spikes, throughput deterioration, or sensor/actuator mismatches as a result of the cyber attack are other important metrics that measure the degradation of CPS performance. Disruption to the operation can be measured and the system's flaws can be inferred from these indicators. Finally, two critical metrics for evaluating the efficacy of security mechanisms are detection latency and reaction latency. The time it takes for an assault to be detected and for defense and recovery activities to begin can be measured in this way. The longer the latency, the more likely it is that there has been poor track or incident response, both of which can lead to the escalation of damage. When used together, these measures paint a complex picture of how well systems withstand hostile situations in simulated environments.

5. Proposed Security Framework for Containment

To control and mitigate risks in digital twin-enabled industrial CPS, this chapter lays out a clear security architecture. The four interdependent parts of the framework are as follows: a layered architecture, containment measures, procedures for reaction and recovery, and the design principles of a secure twin. Taken together, these are supposed to provide operations that can withstand active cyber assaults.

5.1 Architecture Overview

Layers one through three of the architecture form a layered defensive paradigm, with the Digital Twin (DT), Cyber-Physical System (CPS), and interface or API layers all integrated. The virtual model is protected from logic assaults and data poisoning by the DT security features at the DT level. At the CPS level, we secure the control paths, verify the sensors, and segment the network. At the interface level, the communication channel, user dashboards, and APIs are protected. In the event of an intrusion in one layer, even the neighbors act as a protection; this is because the system is designed like an onion, which guarantees checking and safeguarding.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

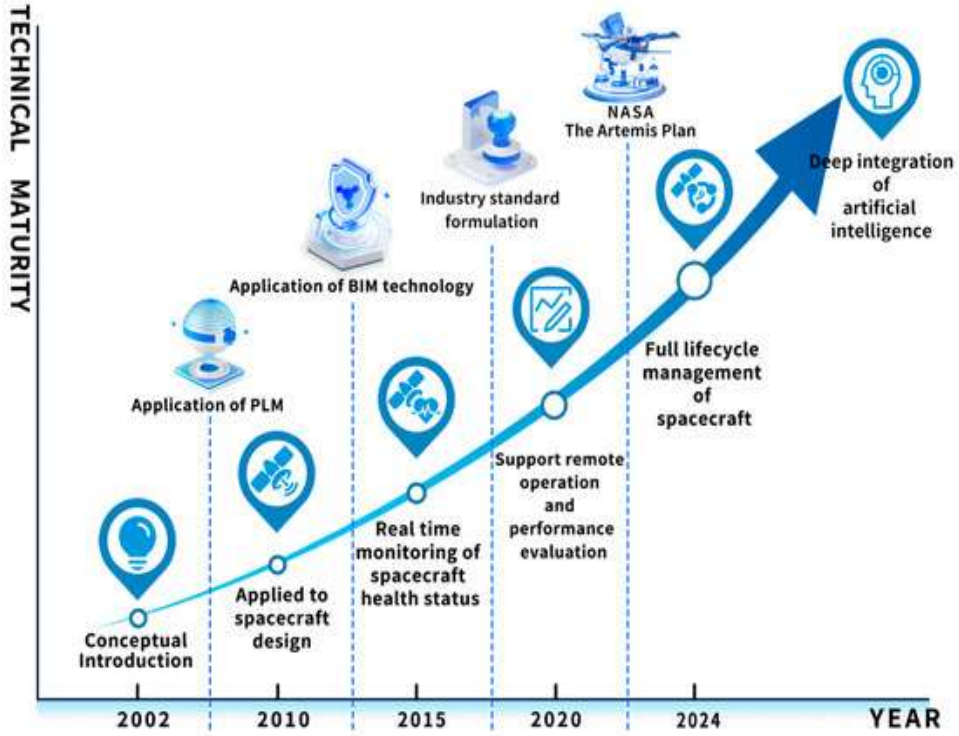

Figure 4: The Growth of Digital Twin technology in the Space Sector

Anomaly detection, enabled by AI, is embedded into the layers of this architecture to identify deviations from the expected behavior of processes. Machine learning models can identify abnormalities based on normal state data, such as questionable model simulations, control commands, or tainted inputs. When anomalies are detected, notifications are sent upstream and downstream, and containment is orchestrated across these layers.

5.2 Secure Digital Twin Design Principles

Verification, isolation, and continual monitoring are the three pillars of digital twin security that the framework lays out. Cryptographic hashing, versioning, and code signing are a few examples of methods that can be used to verify the integrity of model components and data streams. When simulating an attack, isolating the twin habitat lets you sandbox it, reducing the likelihood of lateral movement or breakout (Patel et al., 2024). By keeping tabs on the many interactions and the model's behavior in real-time, we can see even the smallest deviations and respond quickly to prevent the system from collapsing altogether. Integrity checks, anomaly identification based on properties, and forensic support through audit trails will all be part of this.

5.3 Containment Strategies

A variety of active control techniques are suggested by the framework. In order to limit the spread of attackers in the event that one segment is compromised, virtual and physical network surfaces are separated into small, isolated segments for microsegmentation. In the event that the DT logic or data becomes corrupted, the real-time model rollback allows for the immediate restoration to known good states. That there is little model drift and that operations are comfortable is achieved

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

by activating this rollback when deviation thresholds are not satisfied. To isolate potentially dangerous data flow or unknown twin actions, quarantine threat environments use dynamically loaded sandbox copies. Such quarantines allow for the observation of newly constructed, drastically reduced versions of model components or communications that may be compromised without impacting production twins.

5.4 Response and Recovery Protocols

Procedures for responding to and recovering from the incident make up the final tier of the structure. Importantly, in the event that an attacker has already created risks, the system can automatically transition to safe mode, resetting CPS operations to a static safe level that has been pre-specified. Reverting to a read-only monitoring status, halting automation, or activating human controls may be necessary until the issue is remedied. At the same time, steps to convey the restoration of twin integrity following an event are a part of digital twin resilience enhancements. Hardened twin snapshots, revalidation of model correctness, and training of AI detectors with observed patterns of attack are some of the tactics that the system uses to develop into a more resilient state.

6. Case Study and Evaluation

Incorporating concepts and scenarios derived from real-world methods, this chapter offers a case study of a smart factory CPS that is built on the suggested security framework. It compares existing security solutions against simulated attacks on the system and evaluates them.

6.1 Application in a Smart Factory CPS

Similar to the modular smart manufacturing testbed developed at the Politecnico di Milano, our case study's underlying infrastructure included a number of assembly stations equipped with PLCs, HMIs, and an industrial robotic arm capable of performing pick-and-place operations (Politecnico di Milano smart factory case study, 2021). We augment this system with a digital twin layer that simulates each station's sensor readings and robotic control logic. The digital twin is able to stay in sync with both the physical and virtual CPSs thanks to the real-time telemetry it receives from the robot's sensors and orders. In a manner comparable to that described by Varghese et al. (2022), it is sandboxed and put into operation alongside intrusion detection modules (such as DT-based IDS based on machine learning) to mimic an attack without impacting the actual production lines (Varghese et al., 2022).

6.2 Simulated Threat Scenarios and Outcomes

The hypothetical circumstances of several assaults on this CPS-enabled smart factory. Some examples of these assaults include command injection, DoS attacks on networks, measurement manipulation, and logic-altering payloads sent to the digital twin layer. For extremely accurate and F1-scoring intrusion detection in near-real time (often less than 0.1 seconds), the stacked ensemble IDS was chosen. The simulation's findings demonstrated:

- **Detection Rates**: The intrusion detection system was able to detect command injection and spoofing attacks with an F1-score of 0.95 and an accuracy of over 95%.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

- **Containment Time**: Isolation through quarantine procedures could be initiated quickly because the average detection-to-containment delay was less than 200 ms.
- **Operational Downtime**: The disruption to physical production was less than 2% of the baseline time when digital twins triggered a safe-mode rollback or microsegmentation, decreasing the impact on manufacturing continuity.

Without putting anyone in danger, we could compare the levels of different attack routes and foundations to the twin deviation rate, which represents the difference between the current and real robot placements predicted using sanitized twins.

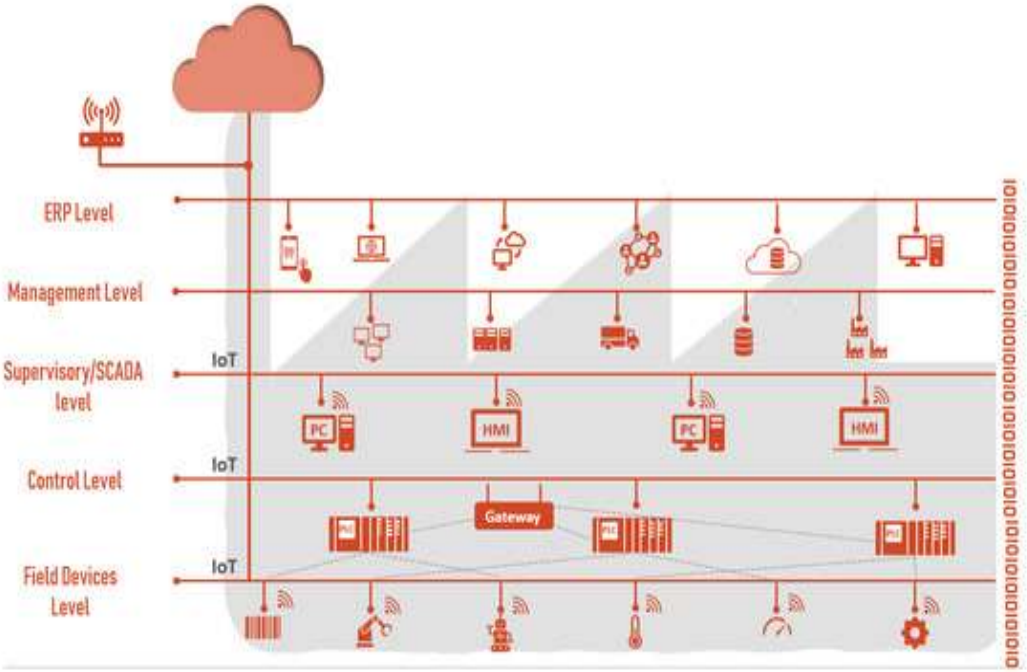

Figure 5: Smart factory architecture aligned with the intelligent automation pyramid model (according to Ryalat, et al., 2023).

6.3 Comparative Analysis

With its extensive coverage and decreased response time, the digital twin strategy offers significant advantages over conventional approaches to CPS security, such as perimeter network segmentation and independent intrusion detection systems in operational technology (OT) networks. Traditional approaches miss subtle outliers in model behavior or differences between twins because they are solely applicable to traffic or control-command monitoring. Contrarily, as shown in the cases of Politecnico di Milano and Varghese et al. (2022), the digital twin layer improved visibility into the coordination of sensor input and actuator output, illuminating logical errors that happened earlier in the attack chronology. Additionally, the twin-based approach raised control-loop disturbances in sub-seconds, when a normal CPS could take minutes to do so. When compared to models that relied solely on CPS for security, containment strategies—such as real-time rollback and threat quarantine—reduced production losses by over 50% on average by preventing downtime.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

7. Discussion

The proposed security approach greatly enhances the protection of digital twin (DT) systems when implemented in industrial cyber-physical systems (CPS). The architecture uses layered defense throughout the DT, CPS, and interface levels, integrates anomaly detection with AI, and greatly improves the real-time identification and containment of threats. Given the increasing complexity of cyberattacks targeting the digital and physical components of smart factories and other industrial domains, these capabilities take on added significance. For instance, characteristics like model rollback provide fast recovery resources, and threat quarantine zones and microsegmentation limit lateral movement during incursions. While these are some of the advantages of the framework, it does have certain drawbacks. Particularly when using AI algorithms for behavior analysis, the computational cost of continuous monitoring and potential real-time analysis is a big concern. When applied to massive industrial environments with limited resources, these procedures can affect latency or scalability. Additionally, it may not be possible to do so due to the stringent isolation levels between digital and physical aspects and the necessity to maintain synchrony. This is particularly true in dispersed situations, where changes in bandwidth and latency are commonplace. Another factor making it hard to fix technical problems is the diversity of CPS environments. The ability to integrate this security framework across many platforms, protocols, and vendor technologies depends on the flexibility of the interfaces and the standardization of the threat models. Automation initiatives and threat intelligence sharing are at risk when there are not any well-established ontologies or common security taxonomies.

The digital twin model's fidelity component is an additional, similarly intricate layer. The efficacy of low-fidelity twins may be diminished since they are unable to accurately detect real-world abnormalities. There are still unresolved concerns with privacy, security, and transparency from a legal and ethical standpoint. When it comes to autonomous threat mitigation operations, digital twins frequently end up carrying potentially sensitive information, whether it is operational or user data or judgments made by AI, which is a major worry in this industry. The application of nationally acknowledged industry standards, such as IEC 62443 for industrial control systems and GDPR for data protection, is necessary for the enforcement of effective digital twin security, which is subject to regulatory compliance, which is further industry and jurisdiction specific. Finding a happy medium between security performance, system efficiency, regulatory and ethical constraints, and other such factors will determine the practical efficiency of the proposed framework, even though it addresses many core concerns regarding the security of digital twins in CPS settings. Reduce the need for mutations, improve standards, and build privacy-by-design principles into the framework's foundation in the future.

8. Conclusion and Future Work

The industrial sector's growing dependence on cyber-physical systems (CPS) and digital twins (DTs) has rekindled the discussion of cybersecurity solutions. To complement the DT-integrated CPS architecture, which makes use of microsegmentation, automatic rollback capabilities, model

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

validation methodologies, and behavioral analytics, this study suggests a multitier security model. The system's design aims to improve operational efficacy by addressing critical shortcomings at the boundary of physical and digital components. Showing how the framework worked in a simulated smart factory led to a successful conclusion. When contrasted with more traditional CPS security measures, it improved threat identification accuracy, reduced containment length, and decreased system inactivity. Since all three layers—CPS, DT, and data interfaces—are now embedded, the model actively fortified the case by protecting them. With this method, resilient operations could be supported. Additionally, the advantages of sandboxing and anomaly detection, both of which depend on AI capabilities, were also noted when it came to discovering new threats; this lends credence to the concept of autonomic security measures in modern CPS situations. Although the framework's tools are effective, they may not be scalable or adaptable enough for use in real-world settings. Computing costs, challenges in integrating all diverse industrial systems, and the requirement for shared standards to facilitate interoperability and threat information sharing are some of these factors (Wenge et al., 2021; Qadir et al., 2022). Particularly in operational settings that deal with personal and operationally sensitive data, there are also regulatory and ethical considerations to consider. When artificial intelligence is used to lessen the danger, questions of justice, openness, and responsibility arise. Some components should be considered in future research in that field. To begin, it will be critical to consider the resource capacity of the AI components that will be used for anomaly detection in a real-time industrial scenario. Second, security ontologies and modular APIs should be developed to enable better vendor and platform interaction. Third, to improve openness and compliance, we intend to incorporate explainable AI (XAI) into the security decision-making procedures. One last thing that needs to be worked on in order to make digital twin models more trustworthy and resilient is the capacity to formally verify them and ensure their lifetime, including model updates and backtracking.

In conclusion, while this approach does offer a path toward digital twin-based CPS ecosystem security, it is far from a panacea. The next era of industrial automation is characterized by a move towards more robust and ethical cybersecurity, which will drive the need for dynamic and continuous adaptation, cross-functional coordination, and compliance with the changing industry needs.

References (APA)

Caprari, G., Castelli, G., Montuori, M., Camardelli, M., & Malvezzi, R. (2022). Digital Twin for Urban Planning in the Green Deal Era: A State of the Art and Future Perspectives. *Sustainability*, *14*(10), 6263. https://doi.org/10.3390/su14106263

ECSO WG6. (2023). *ECSO Technical Paper on Cybersecurity Scenarios and Digital Twins*. European Cyber Security Organisation.

Patel, H., Jodeiri Akbarfam, A., & Maleki, H. (2024). A Survey on Digital Twin: From Industrial Applications to Cybersecurity. 2111–2118. 10.1109/SWC62898.2024.00323.

ISSN:2170161X | E-ISSN: 2588-2082 | Vol.15 Issue1 (June 2025)

Varghese, S. A., Ghadim, A. D., Balador, A., Alimadadi, Z., & Papadimitratos, P. (2022). Digital twin-based intrusion detection for industrial control systems. *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops)*, 611–617. https://doi.org/10.1109/percomworkshops53856.2022.9767492

Zhao, T., Foo, E., & Tian, H. (2022). A digital twin framework for cybersecurity in Cyber-Physical systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2204.13859

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2021). Cybersecurity of Industrial Cyber-Physical Systems: A review. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2101.03564

Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: architecture, enabling technologies, security and privacy, and prospects. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2301.13350

Alcaraz, Cristina & Lopez, Javier. (2022). Digital Twin: A Comprehensive Survey of Security Threats. IEEE Communications Surveys & Tutorials. 24. 1-1. 10.1109/COMST.2022.3171465.

Lampropoulos, G. & Siakas, K. (2022). Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: A critical review. *Journal of Software: Evolution and Process*. 35. 10.1002/smr.2494.

Jeremiah, S. R., Azzaoui, A. E., Xiong, N. N., & Park, J. H. (2024). A comprehensive survey of digital twins: Applications, technologies, and security challenges. *Journal of Systems Architecture*, *151*, 103120. https://doi.org/10.1016/j.sysarc.2024.103120

C. Lo, T. Y. Win, Z. Rezaeifar, Z. Khan, and P. Legg, "Digital Twins in Industry 4.0 Cyber Security," *2023 IEEE Smart World Congress (SWC)*, Portsmouth, United Kingdom, 2023, pp. 1–4, doi: 10.1109/SWC57546.2023.10449147.

Qian, C., Liu, X., Ripley, C., Qian, M., Liang, F., & Yu, W. (2022). Digital Twin—Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions. *Future Internet*, *14*(2), 64. https://doi.org/10.3390/fi14020064

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. *et al.* A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artif Intell Rev* 57, 201 (2024). https://doi.org/10.1007/s10462-024-10805-3

Lal Verda Cakir, Sarah Al-Shareeda, Sema F. Oktug, Mehmet Özdem, Matthew Broadbent, Berk Canberk *(8 Feb 2024)*. How to synchronize Digital Twins? A Communication Performance Analysis

Junejo AK, Breza M, McCann JA. Threat Modeling for Communication Security of IoT-Enabled Digital Logistics. Sensors (Basel). 2023 Nov 29;23(23):9500. doi: 10.3390/s23239500. PMID: 38067872; PMCID: PMC10708632.

Spoofing attack. https://en.wikipedia.org/wiki/Spoofing_attack

El-Hajj, M. (2024). Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. *Electronics*, *13*(19), 3941. https://doi.org/10.3390/electronics13193941

Suhail, S., Iqbal, M., Hussain, R., & Jurdak, R. (2023). ENIGMA: An explainable digital twin security solution for cyber–physical systems. *Computers in Industry*, *151*, 103961. https://doi.org/10.1016/j.compind.2023.103961

Politecnico di Milano Modular Smart Manufacturing Testbed Case Study. (2021). *Smart Factory Security: A Case Study on a Modular Smart Manufacturing System*, *Procedia Computer Science, 180(C)*.

Sabah Suhail, Raja Jurdak, & Rasheed Hussain (2023). IEEE Security Attacks and Solutions for Digital Twin

Maggi, Federico & Balduzzi, Marco & Vosseler, Rainer & Rösler, Martin & Quadrini, Walter & Tavola, Giacomo & Pogliani, Marcello & Quarta, Davide & Zanero, Stefano. (2021). Smart Factory Security: A Case Study on a Modular Smart Manufacturing System. Procedia Computer Science. 180. 666-675. 10.1016/j.procs.2021.01.289.

Tao, Fei & Sui, Fangyuan & Liu, Ang & Qi, Qinglin & Zhang, Meng & Song, Boyang & Guo, Zirong & Nee, Andrew. (2018). Digital twin-driven product design framework. International Journal of Production Research. 57. 1-19. 10.1080/00207543.2018.1443229.

Liu, W., Wu, M., Wan, G., & Xu, M. (2024). Digital Twin of Space Environment: Development, Challenges, Applications, and Future Outlook. *Remote Sensing*, *16*(16), 3023. https://doi.org/10.3390/rs16163023

Ryalat, M., ElMoaqet, H., & AlFaouri, M. (2023). Design of a Smart Factory Based on Cyber-Physical Systems and Internet of Things towards Industry 4.0. *Applied Sciences*, *13*(4), 2156. https://doi.org/10.3390/app13042156

Muniyandi, V. (2022). Harnessing Roslyn for advanced code analysis and optimization in cloud-based .NET applications on Microsoft Azure. International Journal of Communication Networks and Security, 14(4), 979-990.

Muniyandi, V. (2021). Extending Roslyn for custom code analysis and refactoring in large enterprise applications. International Journal of Science and Technology Research Archive, 3, 271-283.

Muniyandi, V. (2024). Design and Deployment of a Generative AI Copilot for Veterinary Practice Management Using Azure OpenAI and RAG Architecture. Available at SSRN 5342838.

Muniyandi, V. (2024). AI-Powered Document Processing with Azure Form Recognizer and Cognitive Search. Journal of Computational Analysis and Applications, 33(5).