International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at :www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

Digital Twin-Enabled Vulnerability Assessment with Zero Trust Policy Enforcement in Smart Manufacturing Cyber-Physical System

Chima Nwankwo Idika [1], Ugoaghalam Uche James[2], Onuh Matthew Ijiga[3], Lawrence Anebi Enyejo[4]

[1]Department of Information Technology, De Meek Builders Ltd, Umuahia, Abia State, Nigeria.

[2]Department of Computer Information Systems. College of Engineering, Prairie View A&M University, Praire View ,77446, Texas, USA.

[3]Department of Physics, Joseph Sarwaan Tarkaa University, Makurdi, Benue State, Nigeria.

[4]Department of Telecommunications, Enforcement Ancillary and Maintenance, National Broadcasting Commission, Aso-Villa, Abuja, Nigeria

ARTICLEINFO

Article History:

Accepted: 01 Nov 2023

Published: 30 Nov 2023

Publication Issue

Volume 9, Issue 6

November-December-2023

Page Number

475-499

ABSTRACT

The convergence of digital twin (DT) technology and zero trust architecture (ZTA) offers a transformative framework for enhancing cybersecurity and operational resilience in smart manufacturing cyber-physical systems (CPS). This review explores how DTs—virtual representations of physical assets—can simulate, monitor, and evaluate vulnerabilities across complex manufacturing networks in real time. Traditional perimeter-based defenses are increasingly ineffective in distributed and interconnected industrial environments. In response, zero trust policy enforcement—anchored in the principles of "never trust, always verify"—introduces dynamic access controls, micro-segmentation, and continuous authentication that address latent security gaps in CPS. The integration of DTs with ZTA provides contextual awareness for asset behavior, enabling predictive threat modeling, anomaly detection, and proactive security orchestration. This paper reviews recent advancements in DT-enhanced vulnerability assessment tools, zero trust policy engines, and their interplay in manufacturing systems with high cyber-physical interdependence. Emphasis is placed on identifying research gaps, evaluating system architectures, and proposing future directions for implementing resilient, secure-by-design CPS infrastructures. By systematically reviewing case studies, industrial applications, and academic frameworks, this study underscores the critical role of DT and ZTA synergy in safeguarding smart manufacturing environments against evolving cyber threats.

Keywords : Digital Twin (DT); Zero Trust Architecture (ZTA); Cyber-Physical Systems (CPS); Smart Manufacturing; Vulnerability Assessment

1.Introduction

1.1 Background on Smart Manufacturing and Cyber-Physical Systems (CPS)

Smart manufacturing is the core of Industry 4.0, characterized by the integration of advanced digital technologies with physical manufacturing systems to enhance adaptability, efficiency, and intelligence across production lines. At the center of this transformation are Cyber-Physical Systems (CPS), which tightly couple computational resources with physical processes through real-time feedback loops, sensors, and intelligent control systems (Lee et al., 2016). These systems support seamless data flow from operational equipment to decision-making platforms, enabling predictive maintenance, autonomous quality control, and optimization of manufacturing processes. The incorporation of artificial intelligence (AI), Internet of Things (IoT), and cloud-edge architectures further intensifies the ability of CPS to function adaptively under dynamic production conditions. In a typical smart manufacturing environment, CPS enables machines, sensors, and controllers to self-organize and make informed decisions without centralized intervention. For example, AI-enabled robotic arms in an automotive production facility can detect anomalies in assembly tasks and recalibrate operations instantly, minimizing downtime and improving yield (Andronie, et al., 2021). However, this integration of digital intelligence introduces unprecedented security challenges, as each interconnected device and control node becomes a potential attack surface. Consequently, secure-by-design CPS architectures and frameworks such as Digital Twins and Zero Trust are increasingly essential to preserving the integrity, confidentiality, and availability of smart manufacturing systems.

1.2 The Growing Threat Landscape in Industrial CPS

The expansion of Industrial Cyber-Physical Systems (CPS) has significantly broadened the threat landscape in manufacturing and process industries. Unlike traditional isolated control environments, modern CPS are deeply interconnected with enterprise networks, cloud services, and third-party applications—exponentially increasing their vulnerability surface (He et al., 2021). The complexity of CPS arises from the confluence of diverse hardware, real-time software, and communication protocols, which often lack standardized cybersecurity controls. As industrial automation grows more intelligent and data-driven, cyber adversaries are exploiting these systemic weaknesses through sophisticated methods such as advanced persistent threats (APTs), ransomware, and lateral movement attacks.

Industrial control systems (ICS), supervisory control and data acquisition (SCADA), and programmable logic controllers (PLCs) are among the most targeted components due to their mission-critical role and historically weak security posture (McLaughlin, et al., 2016). For example, the Triton malware incident, which targeted safety instrumented systems in petrochemical plants, underscores how cyberattacks can have life-threatening consequences when targeting CPS. Moreover, the convergence of IT and operational technology (OT) domains in Industry 4.0 environments has blurred traditional security boundaries, complicating threat detection and response efforts. This evolving threat landscape necessitates a proactive cybersecurity paradigm built on real-time threat intelligence, system redundancy, and dynamic access controls—elements that digital twins and zero trust architectures are well-positioned to provide within the context of secure smart manufacturing.

1.3 Emergence of Digital Twin Technology in Security Applications

Digital twin (DT) technology has rapidly evolved from a simulation-based concept for predictive maintenance into a multifaceted cybersecurity tool in smart manufacturing environments. A digital twin, defined as a dynamic, real-time digital representation of a physical asset or system, enables continuous monitoring, simulation, and behavior analysis under

various operational conditions (Fuller et al., 2020). This duality of physical and virtual synchronization allows manufacturers to predict potential vulnerabilities and test mitigation strategies without disrupting live operations. In the context of cybersecurity, DTs provide critical insights into anomalous system behavior by establishing baseline models of normal operations and flagging deviations that could signal cyber intrusions or process anomalies.

By embedding security intelligence into DT architectures, organizations gain a proactive defense mechanism capable of conducting threat emulation, scenario simulation, and automated alert generation. For example, a DT of a robotic assembly line can detect suspicious command sequences or configuration changes that deviate from expected patterns, enabling early containment responses. Glaessgen and Stargel (2012) highlight that the digital twin paradigm offers strategic foresight in mission-critical systems by enabling continuous assurance of safety and performance integrity. These capabilities are essential for securing Industrial CPS, where real-time situational awareness and predictive anomaly detection are paramount. As threats grow in sophistication, DTs are positioned as integral assets in a resilient, secure-by-design manufacturing infrastructure.

1.4 Introduction to Zero Trust Architecture (ZTA) Principles

Zero Trust Architecture (ZTA) has emerged as a cornerstone framework for securing modern cyber-physical infrastructures by fundamentally challenging traditional perimeter-based security models. Rooted in the principle of "never trust, always verify," ZTA assumes that no user, device, or application—whether inside or outside the network perimeter—should be implicitly trusted. Instead, access is granted based on dynamic policy enforcement, user authentication, and continuous system monitoring (Rose et al., 2020). This principle is especially critical in smart manufacturing environments, where interconnected assets and remote access capabilities expand the attack surface exponentially.

A core feature of ZTA is micro-segmentation, which partitions networks into secure zones and restricts lateral movement by isolating workloads and enforcing strict access controls. This is complemented by identity-centric policies that evaluate attributes such as device posture, user behavior, and contextual risk before authorizing access to resources (Cunningham, & Pollard, 2017). For instance, a programmable logic controller (PLC) in a smart factory may only be allowed to communicate with predefined supervisory systems and only when encrypted protocols and trusted certificates are validated in real-time. In this architecture, trust is never assumed—it must be earned through verified compliance with security policies. ZTA thus provides a strategic paradigm for proactively mitigating threats, reducing breach impact, and ensuring cyber resilience in industrial CPS infrastructures.

1.5 Objectives and Scope of the Study

The primary objective of this study is to explore the integration of Digital Twin (DT) technology and Zero Trust Architecture (ZTA) as a unified framework for enhancing cybersecurity in smart manufacturing Cyber-Physical Systems (CPS). It seeks to demonstrate how DT-enabled systems can simulate, detect, and assess vulnerabilities in real time, while ZTA principles enforce continuous authentication, micro-segmentation, and dynamic access controls. The study also aims to highlight the advantages of combining these technologies for proactive threat detection, operational visibility, and risk mitigation in highly interconnected industrial environments.

The scope of the review encompasses recent developments in the application of DT technology for cybersecurity monitoring, with emphasis on behavioral analytics, threat simulation, and predictive vulnerability assessment. Additionally, it evaluates the core mechanisms of ZTA, including identity and

access management, trust evaluation, and policy enforcement, within the context of industrial CPS. Case studies, architectural models, and implementation frameworks are examined to assess real-world applicability and performance outcomes. This study is particularly focused on smart manufacturing sectors leveraging Industry 4.0 technologies, such as IoT, edge computing, and AI, where security threats are increasingly dynamic and complex. Ultimately, this review contributes to the broader discourse on resilient industrial systems by proposing an integrated security paradigm that bridges physical infrastructure and digital intelligence.

1.6 Structure of the Paper

This paper is organized into six main sections to provide a coherent and systematic exploration of Digital Twin-enabled vulnerability assessment and Zero Trust policy enforcement in smart manufacturing Cyber-Physical Systems (CPS). Following the introduction in Section 1, which outlines the background, threat landscape, emergence of relevant technologies, and research objectives, Section 2 delves into the foundational aspects of Digital Twin technology. This includes its architecture, real-time capabilities, and cybersecurity applications in industrial settings.

Section 3 introduces the principles and mechanisms of Zero Trust Architecture (ZTA), highlighting its departure from traditional security models and its specific relevance to industrial CPS. This section further discusses policy enforcement techniques, identity management, and monitoring strategies essential for ZTA implementation. Section 4 presents a synthesized view of how Digital Twins and Zero Trust models can be integrated to enhance vulnerability detection and response. It offers architectural frameworks, operational workflows, and real-world case studies demonstrating the synergy between these technologies. Section 5 outlines future trends, challenges, and open research directions, including emerging technologies like AI and edge computing in security contexts. Finally, Section 6 summarizes the key findings and offers strategic recommendations for researchers, engineers, and industrial cybersecurity professionals seeking to implement secure, resilient smart manufacturing systems.

2. Digital Twin Technology for Security in Manufacturing CPS

2.1 Architecture and Functional Components of Digital Twins

The architecture of Digital Twin (DT) systems in smart manufacturing encompasses a multilayered integration of physical assets, virtual models, and bidirectional data exchange. Fundamentally, a digital twin consists of three core components: the physical entity, its digital counterpart, and the data linkage that enables synchronization between the two environments as shown in table 1. This synchronization allows the virtual model to simulate the physical system in real time, providing actionable insights for monitoring, control, and optimization (Qi et al., 2021). These insights are essential in cyber-physical systems (CPS) for proactive decision-making, anomaly detection, and resilience under variable production conditions. Functionally, digital twins are composed of data acquisition layers, simulation engines, and predictive analytics modules. The data acquisition layer integrates sensors, IoT gateways, and embedded systems that continuously feed telemetry from the physical asset into the digital model. The simulation engine replicates the system's structural and behavioral dynamics, enabling engineers to test scenarios without disrupting live operations. Finally, the analytics module applies artificial intelligence and machine learning algorithms to detect patterns, forecast outcomes, and support real-time control.

Barricelli et al. (2019) emphasize that the scalability and interoperability of these components are vital for effective DT deployment in heterogeneous industrial environments. Modular architecture also enables digital twins to evolve dynamically, accommodating

system upgrades, security policies, and context-aware process adjustments necessary for robust smart manufacturing cybersecurity frameworks.

Table 1: Summary of Architecture and Functional Components of Digital Twins

Component	Description	Function in Smart Manufacturing	Example Application
Physical Entity	The real-world machine, device, or asset being mirrored	Source of real-time operational data through sensors and embedded systems	CNC machines, robotic arms, HVAC systems
Digital Model (Twin)	Virtual representation that simulates structure, behavior, and performance	Enables simulation, visualization, and state monitoring of physical assets	Simulating wear patterns in a robotic joint
Data Integration Layer	Infrastructure enabling bidirectional communication between physical and digital	Collects sensor data, sends control commands, and maintains synchronization	IoT platforms, SCADA interfaces, industrial gateways
Analytics & Simulation Engine	Processes telemetry using AI/ML models to generate insights and detect anomalies	Supports predictive maintenance, fault diagnostics, and cyber threat detection	Predicting motor failure or identifying command injection anomalies via DT analytics

2.2 Real-Time Data Acquisition and Simulation in DT Systems

Real-time data acquisition and simulation form the foundational pillars of digital twin (DT) functionality, enabling dynamic responsiveness and predictive control in smart manufacturing systems. These capabilities are achieved through continuous bidirectional communication between physical assets and their virtual representations. Embedded sensors and industrial IoT devices stream high-frequency data on operational variables—such as temperature, vibration, load, and cycle times—into cloud or edge-based DT platforms, where it is processed and synthesized into actionable insights (Leng et al., 2021). This real-time synchronization ensures that the digital twin mirrors the physical system's current state and behavior with high fidelity.

Simultaneously, simulation engines within the DT framework leverage the incoming data to conduct parallel modeling of system dynamics, stress responses, and failure probabilities. This allows for immediate feedback on potential anomalies or inefficiencies, which can be used to recalibrate system behavior or initiate preventive maintenance protocols. In the context of security, real-time simulations help detect command injection, process deviations, or unusual latency patterns that may indicate malicious interference.

Xie et al. (2021) emphasize that the performance of real-time DT systems is enhanced through adaptive learning models that incorporate historical data trends and predictive analytics to optimize operations under varying conditions. This real-time capability is vital in manufacturing CPS, where even milliseconds of delay can have significant implications for safety, productivity, and cyber-resilience.

2.3 Applications of DT in Predictive Maintenance and Process Optimization

Digital twin (DT) systems are transforming predictive maintenance and process optimization by enabling real-time monitoring, prognosis, and decision support across smart manufacturing environments. Predictive maintenance, empowered by DTs, goes beyond traditional condition-based monitoring by integrating real-time telemetry with historical degradation models and machine learning algorithms to forecast failure points before they occur. This allows industries to schedule maintenance operations with precision, minimize unplanned downtime, and extend asset lifecycles. For instance, in an automotive assembly plant, DTs can monitor the thermal load and vibration data of robotic arms to anticipate bearing wear and trigger automated service requests before faults propagate (Zheng et al., 2021).

In parallel, DTs enhance process optimization by simulating various production scenarios and adjusting operational parameters to achieve optimal performance under resource and time constraints. Through embedded feedback loops and closed-loop control mechanisms, DTs autonomously recalibrate process flows in response to material inconsistencies, equipment inefficiencies, or environmental changes. This real-time adaptation boosts throughput, reduces energy consumption, and increases manufacturing flexibility.

Leng et al. (2022) underscore the value of integrating DTs with AI-driven analytics and cloud-based platforms to facilitate large-scale optimization across distributed production networks. These capabilities are especially vital for smart factories aiming to balance operational efficiency with sustainability and resilience in rapidly evolving industrial ecosystems.

2.4 Role of DT in Cybersecurity Monitoring and Threat Modeling

Digital Twin (DT) systems are emerging as a powerful tool for cybersecurity monitoring and threat modeling in industrial environments, especially within the context of CPS. A DT's capacity to replicate real-time behavior of assets enables detailed visibility into system operations, thereby supporting the detection of anomalies and potential breaches as represented in figure 1. By continuously monitoring system parameters and comparing them against baseline behavior models, DTs can identify deviations that may signify cyber intrusions, insider threats, or data integrity violations (Alcaraz, & Lopez, 2022). These deviations, when analyzed with embedded AI algorithms, provide critical indicators for early threat detection and response.

In the domain of threat modeling, DTs allow manufacturers to simulate various cyberattack scenarios—such as man-in-the-middle, ransomware, or command injection attacks—within a controlled virtual environment. This simulation capability supports risk assessment, system hardening, and prioritization of mitigation strategies without affecting operational continuity. Balta, et al., (2023) emphasize that DT-enhanced threat modeling leverages reinforcement learning and anomaly detection techniques to evaluate system vulnerabilities under dynamic threat landscapes. Moreover, DTs support forensic analysis by preserving a digital trace of system activity, which aids in post-incident investigation and compliance reporting. As industrial systems evolve in complexity, the DT framework ensures scalable, proactive cybersecurity monitoring that aligns with real-time system demands and zero trust policy enforcement principles.

Figure 1 shows a highly digitized industrial facility where Digital Twin (DT) technology is actively integrated into the cybersecurity infrastructure of a smart manufacturing system. At the core of the image is a large refinery or process plant surrounded by sensors and advanced control units, overlaid with a transparent, holographic DT interface displaying real-time analytics, behavioral models, and network telemetry. This visual representation exemplifies how DTs function in cybersecurity monitoring by continuously synchronizing with physical assets to detect anomalies, simulate threat scenarios, and visualize system vulnerabilities. The interface shows dynamic charts, heat maps, and node connections, reflecting the DT's ability to perform predictive threat modeling by comparing live telemetry with historical baselines. Any deviations—such as unauthorized commands or unusual data flows—can be flagged for immediate risk analysis. The DT system, embedded with AI algorithms, also supports forensic capabilities, allowing operators to trace and understand potential intrusion paths within the cyber-physical environment. This fusion of real-time monitoring and threat intelligence encapsulates the critical role of DTs in strengthening situational awareness and enabling proactive cybersecurity defense mechanisms across complex, interconnected industrial control systems.

Figure 1: Picture of Digital Twin-Enabled Cybersecurity Monitoring and Threat Modeling in a Smart Industrial Plant (Vigna, R. 2023).

2.5 Challenges in DT Implementation for Security Operations

While DT systems hold immense promise for strengthening cybersecurity in industrial cyber-physical systems (CPS), their implementation introduces several critical challenges. First, constructing and maintaining a high-fidelity digital twin requires seamless integration of heterogeneous data sources from sensors, actuators, edge nodes, and enterprise systems. Achieving this integration across legacy and modern infrastructure can be difficult due to protocol incompatibilities, latency issues, and varying levels of system observability (Koulamas

& Kalogeras, 2018). Additionally, real-time synchronization between the physical and virtual environments must be accurate to avoid decision-making based on outdated or incomplete data—an issue that compromises the security value of the DT.

Another significant challenge lies in the computational overhead and scalability of DT systems in large-scale industrial environments. Modeling complex assets and simulating multiple failure or attack scenarios demand high-performance computing resources and robust data governance strategies. Grieves and Vickers (2017) also highlight the difficulty of modeling emergent behaviors in complex systems, where seemingly benign interactions can cascade into unpredictable vulnerabilities. This unpredictability complicates threat modeling and incident forecasting.

Moreover, securing the DT itself poses another layer of complexity. Because the DT mirrors operational assets, unauthorized access or manipulation of its data can lead to misinformation, incorrect threat responses, or exploitation of mirrored control systems. Therefore, cybersecurity operations must treat the DT as both a defense tool and a potential attack surface.

3. Zero Trust Architecture in Industrial Environments

3.1 Fundamentals of Zero Trust: Micro-Segmentation and Least Privilege

ZTA is grounded in two core principles: micro-segmentation and least privilege access, both of which are critical for securing distributed CPS. Micro-segmentation refers to the partitioning of a network into granular, isolated zones where access between zones is tightly controlled as represented in figure 2. Instead of relying on perimeter-based defenses, micro-segmentation ensures that even if an attacker breaches one segment, lateral movement within the system is significantly hindered. This is particularly important in smart manufacturing environments where CPS components, such as programmable logic controllers and IoT sensors, must be shielded from unauthorized interactions (Alsmadi & Xu, 2020).

Least privilege, on the other hand, dictates that users, processes, and devices should only be granted the minimum access necessary to perform their functions. This minimizes the risk of privilege escalation and reduces the attack surface available to insider threats or compromised credentials. Implementing least privilege policies requires context-aware access control systems that evaluate identity attributes, behavioral analytics, and risk levels in real time (Ray, 2023).

Together, micro-segmentation and least privilege enforce a denial-by-default posture that aligns with the Zero Trust philosophy. In dynamic industrial environments, this approach enables secure-by-design system architectures capable of withstanding advanced threats while maintaining operational continuity and safety.

Figure 2 illustrates the core principles of ZTA applied to industrial cyber-physical systems (CPS), emphasizing micro-segmentation and least privilege access. At the top, ZTA functions as the central policy engine enforcing the “never trust, always verify” doctrine. From this, two branches emerge. The first branch, micro-segmentation, divides the industrial network into granular security zones where each device—such as programmable logic controllers (PLCs), robots, or sensors—is isolated. This approach minimizes lateral movement by introducing internal firewalls, asset-specific containment, and zone-level monitoring, ensuring that a breach in one segment does not compromise others. The second branch, least privilege access, governs user and device interactions by enforcing role-based access control, device authentication, time-bound and task-specific permissions, and dynamic revocation in response to behavioral anomalies. These policies ensure that only verified and contextually authorized entities interact with CPS components. At the base of the

diagram lies the operational environment—comprising smart factory assets such as IoT sensors, SCADA systems, and HMIs—which is continuously protected through this layered, adaptive framework. Arrows depict the real-time flow of policy enforcement and monitoring, reflecting a tightly integrated, proactive security model that adapts to threats without disrupting industrial operations.

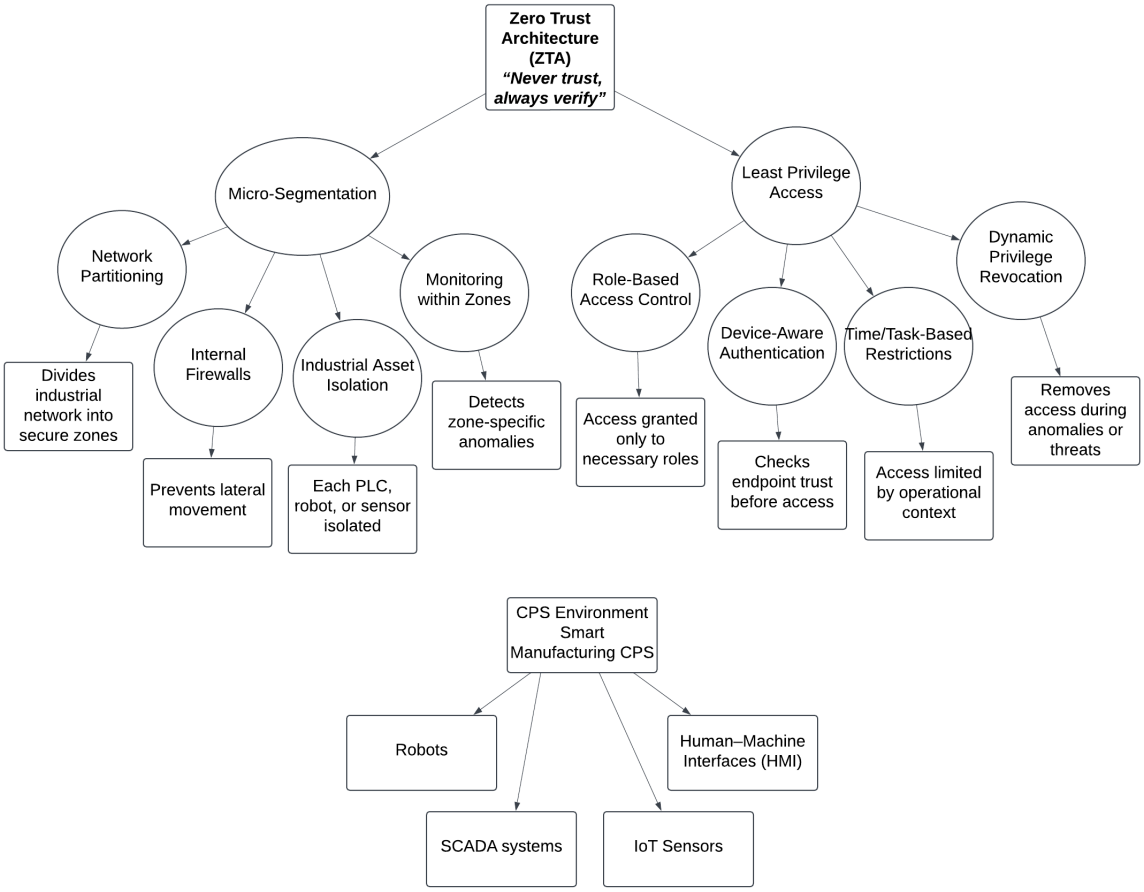

Figure 2: Diagram Illustration of Zero Trust Architecture in Industrial CPS – Micro-Segmentation and Least Privilege Enforcement

3.2 Policy Enforcement Mechanisms: Authentication and Authorization

Authentication and authorization are foundational mechanisms for policy enforcement in ZTA, especially within smart industrial environments that rely on interconnected CPS. Authentication validates the identity of users and devices attempting to access resources, while authorization determines their access rights based on predefined policies as presented in table 2. In contrast to traditional systems, where authentication is often performed once at login, ZTA requires continuous verification based on context, risk posture, and behavior (Li, et al., 2017). This ensures that access decisions are dynamically updated as system conditions change.

Modern authentication frameworks in industrial CPS employ multi-factor authentication (MFA), digital certificates, hardware-based security modules, and behavioral biometrics to strengthen identity assurance. These methods are reinforced by risk-based authentication systems that assess anomalies in login time, device fingerprint, or location to detect potential compromises. Once authenticated, authorization is enforced through fine-grained access control policies, typically governed by Attribute-Based Access Control (ABAC) models that account for user roles, system context, and operational states (Alzubaidi & Kalutarage, 2021).

For example, a maintenance technician may be authorized to access a robot controller only during a scheduled maintenance window and only from a trusted workstation. Such contextual enforcement mechanisms are vital for preventing privilege misuse and ensuring operational integrity in dynamic, threat-prone industrial environments.

Table 2: Summary of Policy Enforcement Mechanisms: Authentication and Authorization

Mechanism	Description	Role in Zero Trust Architecture	Example in Industrial CPS
Multi-Factor Authentication (MFA)	Requires users to verify identity using two or more factors (e.g., password, biometrics, token)	Enhances identity assurance and prevents unauthorized access	Maintenance engineer must verify identity via fingerprint and time-restricted access code
Risk-Based Authentication	Dynamically evaluates risk level based on device, location, and user behavior	Adjusts authentication requirements in real time based on risk context	User logging in from unfamiliar IP must pass additional verification steps
Attribute-Based Access Control (ABAC)	Grants access based on attributes like role, device health, and operational context	Enables fine-grained authorization tailored to dynamic operational states	PLC access allowed only for certified technicians during scheduled downtime
Context-Aware Policy Engine	Continuously enforces access policies based on real-time system and identity context	Aligns access privileges with security posture and system behavior	Automatically revokes access when behavioral anomalies or asset tampering are detected

3.3 Continuous Monitoring and Adaptive Access Control

Continuous monitoring and adaptive access control are critical enablers of ZTA, particularly in dynamic CPS where static policy enforcement is insufficient. Continuous monitoring involves real-time surveillance of system behaviors, network flows, user interactions, and device states to detect deviations from normal baselines. These telemetry inputs feed into machine learning models and rule-based engines that provide timely risk assessments, which are then used to trigger policy updates and enforce contextual restrictions (Wang, et al., 2021). Unlike traditional models that rely on perimeter-centric validation, ZTA ensures every access request is evaluated against the most current trust state. Adaptive access control builds upon this foundation by dynamically altering permissions based on trust scores, environmental variables, and behavior analytics. For example, if an industrial robot begins communicating with an unauthorized PLC, the system automatically reduces its privilege level or isolates it from the network until further investigation. Yan et al. (2020) describe how trust management frameworks in ZTA utilize attributes like historical reliability, behavior trends, and device reputation to continuously calibrate access decisions.

This real-time, feedback-driven loop strengthens CPS resilience by enabling proactive mitigation of insider threats, lateral movement, and advanced persistent threats. In industrial contexts, where uptime and safety are paramount, such adaptability is crucial for maintaining both operational efficiency and cyber integrity.

3.4 Zero Trust vs Traditional Perimeter-Based Security in CPS

The shift from perimeter-based security to ZTA in CPS marks a fundamental evolution in industrial cybersecurity strategy. Traditional perimeter-based models assume that once inside the network, users and devices can be trusted, enforcing minimal segmentation and static firewall policies. While effective in isolated, monolithic infrastructures, this model fails in dynamic CPS environments where IoT devices, remote access, and cloud integration are prevalent. As a result, lateral movement, credential theft, and insider threats often go undetected within trusted zones (Federici, et al., 2023).

In contrast, Zero Trust discards the notion of a trusted internal network. Every request for access—whether from inside or outside the system—is verified, authenticated, and authorized based on identity, context, and device posture. This granular verification includes real-time assessment of behavior anomalies, privilege level, and the sensitivity of the requested resource (Ihimoyan, et al. 2022). Unlike perimeter defenses, ZTA segments the network into micro-perimeters and enforces strict policies continuously, limiting attack propagation.

Xu and Duan (2020) highlight how CPS in Industry 4.0 demands continuous protection mechanisms due to high data velocity, distributed control, and remote operational environments. Therefore, ZTA provides superior resilience by aligning access control with operational dynamics rather than relying on static borders. This paradigm shift significantly enhances visibility, accountability, and system integrity across industrial networks.

3.5 Industrial Adoption Barriers and Compliance Considerations

Despite the clear advantages of ZTA in securing CPS, its adoption across industrial sectors faces several technological, organizational, and regulatory challenges. One of the primary barriers is legacy system integration. Many industrial environments still operate on outdated protocols and hardware that lack native support for micro-segmentation, dynamic policy enforcement, or continuous authentication. Upgrading these systems or retrofitting them with ZTA-compatible technologies requires significant investment in both infrastructure and training (Fernández-Caramés & Fraga-Lamas, 2020). Moreover, industrial organizations often face resistance to operational changes due to concerns over downtime, complexity, and the disruption of production workflows.

Another critical barrier is the lack of standardization in implementing ZTA across heterogeneous CPS ecosystems. While guidelines exist, many organizations struggle with aligning ZTA deployment with established compliance frameworks such as NIST SP 800-82, ISA/IEC 62443, and GDPR. Regulatory compliance is especially complex in multinational industrial operations where cybersecurity mandates vary by region. (Paul, & Rao, 2022) emphasize that achieving regulatory alignment under a ZTA framework necessitates rigorous documentation, auditability, and real-time monitoring—all of which demand scalable and interoperable security orchestration platforms. Additionally, industries must balance ZTA's technical rigor with usability and accessibility to avoid overburdening system users. Therefore, addressing industrial adoption barriers requires a phased, risk-based approach supported by strong governance, vendor cooperation, and policy harmonization.

4. Integrating Digital Twin with Zero Trust for Vulnerability Assessment

4.1 Framework for DT-Driven Security Risk Visualization

DT-driven security risk visualization offers a proactive and context-aware approach to identifying, analyzing, and mitigating vulnerabilities in smart manufacturing CPS. Unlike static risk models, DTs enable dynamic and real-time representations of physical processes, making it possible to visualize how security threats manifest and propagate within operational environments (Abiodun, et al., 2023) as represented in figure 3. A robust DT-driven security framework typically integrates three components: real-time sensor data ingestion, behavior modeling of system assets, and a visualization interface capable of reflecting threat states and impact trajectories across the digital replica of the physical system.

Wen, et al. (2022) highlight that digital twins in cybersecurity contexts act as "virtual security analysts," synthesizing telemetry from programmable logic controllers (PLCs), industrial control systems (ICS), and IoT endpoints. This data feeds into analytics engines equipped with machine learning models that classify threats and map them spatially and temporally across the digital twin interface. For instance, if a coordinated denial-of-service (DoS) attack is initiated, the DT visualizes affected nodes, their cascading dependencies, and potential countermeasure zones in real time. This enhances situational awareness and shortens response cycles.

Furthermore, DT-based risk visualization frameworks allow for simulation of “what-if” cyberattack scenarios, supporting proactive strategy planning. This dynamic and visual insight is essential for decision-makers and operators to prioritize mitigation steps, allocate cybersecurity resources efficiently, and maintain CPS continuity under evolving threat conditions.

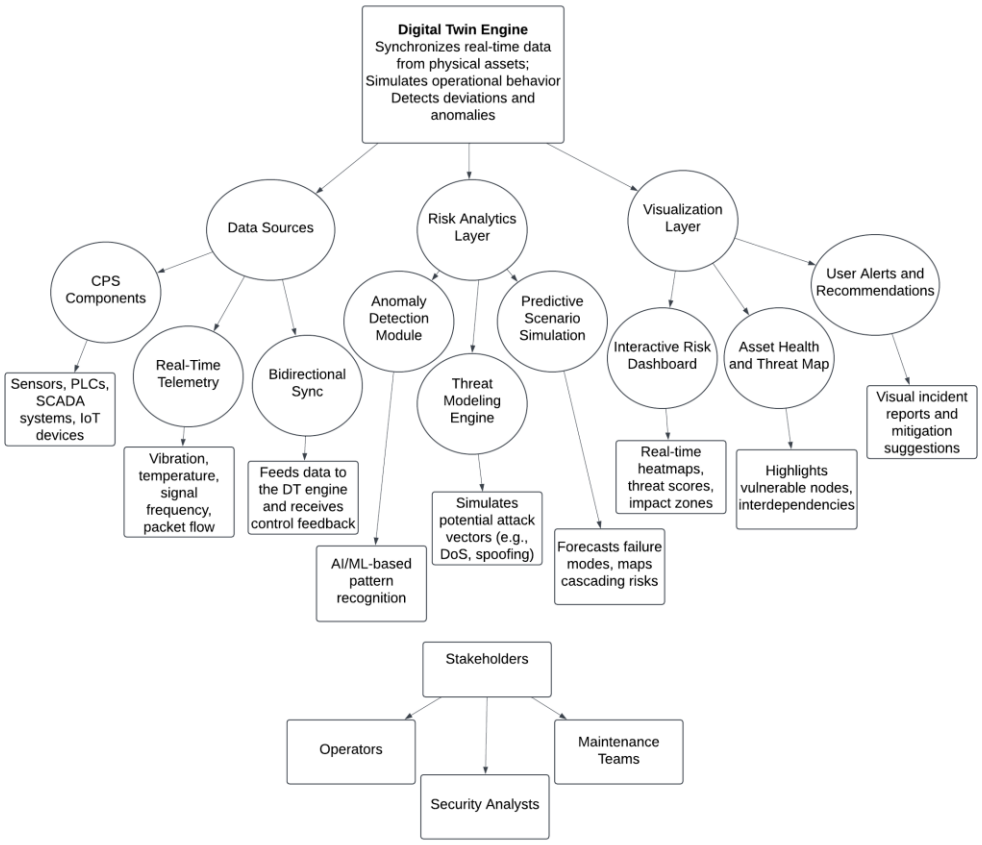

Figure 3: Diagram Illustration of Framework for Digital Twin-Driven Security Risk Visualization in Industrial CPS.

Figure 3 illustrates a comprehensive framework for Digital Twin (DT)-driven security risk visualization in industrial CPS, highlighting the layered integration of data acquisition, threat analytics, and visual feedback. At the core is the DT engine, which synchronizes with real-world assets—such as sensors, programmable logic controllers (PLCs), SCADA systems, and IoT devices—via real-time telemetry. This engine models operational behavior and detects deviations that may indicate cyber threats or system anomalies. Data from the physical layer feeds into the risk analytics layer, where AI and machine learning modules perform anomaly detection, simulate attack vectors (e.g., denial-of-service or spoofing), and generate predictive scenarios to assess cascading vulnerabilities. These analyses inform the visualization layer, which presents security insights through interactive dashboards, heatmaps, and asset health indicators. This enables stakeholders—including plant operators, cybersecurity analysts, and maintenance engineers—to visualize threats spatially and temporally, prioritize mitigation actions, and understand the interdependencies between assets. The system operates as a closed feedback loop, allowing detected anomalies to trigger policy responses or adjustments in real time. Overall, the diagram demonstrates how DTs transform raw data into actionable security intelligence, enhancing visibility, responsiveness, and resilience in complex industrial environments.

4.2 Enhancing Threat Detection with DT-Powered Behavioral Analysis

DT-powered behavioral analysis significantly elevates the fidelity and responsiveness of threat detection systems in cyber-physical environments by establishing continuously adaptive baselines for normal operations and systematically identifying deviations that may indicate cyber intrusions or system compromise. Unlike traditional intrusion detection systems that often rely on static rules or signature-based detection, DT-enabled platforms leverage contextual intelligence and time-series analytics to understand asset behavior under real-world conditions and infer intent behind anomalies (Li, et al., 2023).

The behavioral analysis process begins with data ingestion from interconnected devices, including sensors, control units, and human-machine interfaces. This telemetry is mapped against the digital twin model to simulate expected operations in real time. When an observed behavior deviates from the predicted digital counterpart—such as unexpected packet routing, command injection attempts, or abnormal equipment cycles—the system flags it for investigation (Imoh, 2023). For example, if a robotic arm's movement trajectory unexpectedly changes during routine operation, the DT system can analyze whether the deviation stems from mechanical wear, calibration error, or unauthorized control override. Sun et al. (2021) demonstrate how integrating machine learning algorithms within the DT ecosystem enables early detection of zero-day threats and persistent anomalies that evade conventional detection tools. The DT's continuous feedback loop ensures the system remains adaptive and self-learning, offering intelligent, context-aware threat detection essential for maintaining the resilience of smart manufacturing systems.

4.3 Real-Time Access Verification Using DT State Awareness

Real-time access verification in smart manufacturing systems can be significantly strengthened by leveraging Digital Twin (DT) state awareness. In contrast to static access control models that grant permissions based solely on user roles or credentials, DT-based systems continuously assess the real-time operational state of physical assets and contextualize access decisions accordingly. This allows the system to evaluate not only who is requesting access, but also whether the system's current conditions justify that access under ZTA) principles (Liu et al., 2021). By maintaining a synchronized and dynamic model of the physical environment, DTs monitor process parameters such as machine health, workload status, maintenance cycles, and operational risks. For

example, if a technician attempts to remotely access a conveyor belt control panel during a high-speed production cycle, the DT can block the action if the system's real-time state analysis deems the access unsafe or suspicious. Conversely, during downtime or maintenance windows, verified access requests can be temporarily elevated based on contextual approval mechanisms.

Chen et al. (2021) demonstrate that integrating state-awareness into access control frameworks enhances both security and operational continuity. The digital twin not only authenticates identity but also validates system readiness, reducing the risk of misconfigurations, privilege misuse, or accidental disruptions. This approach aligns real-time decision-making with the operational posture of cyber-physical systems, enabling adaptive, risk-sensitive access control.

4.4 Coordinated Anomaly Response via DT-ZTA Fusion

The integration of DT capabilities with ZTA establishes a highly responsive framework for coordinated anomaly detection and mitigation within industrial CPS. This fusion leverages the predictive modeling and state-aware monitoring of DTs alongside the identity-centric, policy-enforced decision-making of ZTA to create a closed-loop security system capable of reacting to complex threats in real time (Balta, et al., 2023) as presented in table 3. While DTs identify deviations from baseline operational behavior, ZTA dynamically verifies identity, device posture, and access context before triggering corresponding response actions. In this combined model, anomaly detection through the DT initiates immediate trust reassessment in the ZTA domain. For example, if a programmable logic controller (PLC) begins exhibiting communication patterns inconsistent with its digital model, the DT flags the behavior and informs the ZTA policy engine (Atalor, 2019). The policy engine then enforces adaptive controls—revoking privileges, triggering multi-factor reauthentication, isolating affected nodes, or re-routing system operations—to contain the anomaly and prevent lateral movement.

Wang et al. (2021) demonstrate that this DT-ZTA coordination significantly reduces mean time to detect (MTTD) and respond (MTTR) to security incidents by synchronizing contextual threat intelligence with policy enforcement. The result is a proactive and resilient cybersecurity posture that enables industrial CPS to maintain operational continuity while dynamically adapting to evolving threat vectors.

Table 3: Summary of Coordinated Anomaly Response via DT-ZTA Fusion

Component	Description	Function in DT-ZTA Fusion	Example in Manufacturing CPS
Digital Twin Anomaly Detection	Uses real-time behavioral models to detect deviations from normal operations	Identifies irregular patterns indicating cyber threats or faults	DT detects abnormal vibration in robotic arm signaling possible malicious command injection
ZTA Trust Evaluation Engine	Reassesses identity and system trustworthiness upon detection of anomalies	Enforces access control changes, isolation, or remediation based on risk context	Automatically revokes user access after DT flags inconsistent command sequences

Policy-Based Automated Response	Executes predefined actions to contain threats (e.g., revoke access, segment system)	Enables real-time mitigation with minimal human intervention	Affected PLC is isolated from network while forensic analysis begins
Feedback Loop & System Update	Synchronizes DT models and ZTA policies post-incident	Ensures adaptive learning and continuous improvement of detection and response systems	DT updates its behavior model; ZTA modifies access thresholds based on the new risk signature

4.5 Case Studies of DT-ZTA Integration in Manufacturing Systems

Case studies on the integration of DT and ZTA in manufacturing systems offer compelling evidence of their synergistic impact on cybersecurity, operational intelligence, and system resilience. In a recent implementation within a smart automotive assembly facility, DTs were deployed to monitor robotic arms, CNC machines, and automated guided vehicles (Atalor, et al., 2023) as represented in figure 4. These DTs maintained real-time replicas of operational status, enabling proactive fault detection and behavior modeling. When abnormal signal fluctuations occurred in one of the robotic joints, the DT flagged the anomaly, prompting the ZTA framework to reevaluate trust credentials, limit access, and segment the affected control channel before any system-wide disruption occurred (Xu, et al., 2023). Another application was observed in a semiconductor fabrication plant, where DT-ZTA fusion was used to protect precision lithography equipment from unauthorized code execution. The DT monitored process consistency and machine telemetry, while the ZTA system employed continuous policy enforcement to restrict remote access and enforce real-time multifactor authentication. As a result, the integrated framework neutralized a credential spoofing attempt before it could escalate. Yin et al. (2021) demonstrate that these real-world use cases underscore the practical feasibility and benefits of DT-ZTA alignment—namely, early threat containment, minimal operational interference, and improved decision-making. Together, they represent a foundational shift toward cyber-resilient industrial architectures.

Figure 4 depicts a modern manufacturing environment where a worker in a smart factory is engaging with a holographic DT of a turbine component, illustrating a practical case study of DT-ZTA integration. The engineer appears to be conducting a simulation or inspection, supported by the DT's dynamic visualization of the turbine's internal structure. This use case exemplifies how digital twins can provide real-time feedback on asset performance, allowing the system to identify abnormalities such as excessive vibration, structural fatigue, or unauthorized command executions. When such anomalies are detected, the Zero Trust system dynamically reassesses access privileges, ensuring that only verified and authorized personnel can initiate further interactions with the physical equipment. In a full DT-ZTA deployment, this turbine would also be continuously monitored by ZTA's policy engine, which would enforce micro-segmentation and least-privilege access controls. If, for instance, an anomaly is triggered during an off-shift remote access attempt, the system could isolate the turbine's network segment and alert cybersecurity personnel. This integration demonstrates

the dual capability of DTs to enhance operational precision and of ZTA to protect critical assets through adaptive, context-aware security enforcement within industrial cyber-physical systems.

Figure 4: Picture of Real-World Application of Digital Twin and Zero Trust Integration in Manufacturing (Terca, K. 2022).

5. Future Trends and Research Directions

5.1 AI-Augmented DT and Zero Trust Automation

Artificial Intelligence (AI) significantly enhances the fusion of DT technology and ZTA by enabling autonomous threat detection, dynamic access control, and predictive anomaly management in CPS. AI-augmented DTs continuously learn from operational data, building behavior profiles for assets and identifying deviations indicative of cyber threats or system degradation. This learning capability enables DTs to evolve beyond static monitoring, transforming into intelligent agents capable of simulating multiple risk scenarios and guiding automated responses (Trakadas, et al., 2020). ZTA complements this with policy-based enforcement mechanisms, where AI models refine access decisions in real time based on identity, behavior trends, device posture, and risk analytics. For instance, a manufacturing execution system (MES) monitored by an AI-driven DT may observe irregular command sequences targeting an industrial controller. The ZTA framework, informed by AI insights, can immediately revoke access, notify administrators, and revalidate authentication—without human intervention. Ttakadas et al., (2020) highlight that AI not only enhances the granularity of behavioral detection but also reduces false positives by contextualizing data through continuous training. The convergence of AI, DT, and ZTA creates a fully automated security ecosystem that adapts to dynamic manufacturing environments. This model enables proactive cyber defense strategies that are scalable, self-regulating, and optimized for real-time operational continuity in smart factories.

5.2 Edge-Cloud Interoperability in Security-Enabled CPS

The interplay between edge and cloud computing is essential for achieving robust, low-latency, and scalable cybersecurity in CPS within smart manufacturing environments. Digital Twins (DTs) operating at the edge enable localized real-time monitoring, threat detection, and decision-making close to physical assets. When integrated with cloud-based ZTA frameworks, this edge intelligence becomes part of a broader, policy-enforced, and dynamically scalable security ecosystem (Qi, et al., 2018). Edge-cloud interoperability facilitates layered defense by distributing security operations based on latency sensitivity and computational requirements. For instance, real-time anomaly detection and access verification occur at the edge, minimizing response time and reducing the risk of production delays (Ononiwu, et al., 2023). Simultaneously, cloud resources handle data aggregation, model training, system-wide threat correlation, and global policy updates. This division of labor enhances resilience against localized failures and ensures coordinated response across distributed assets. Qi, et al. 2018) demonstrate that secure data pipelines, encrypted communication protocols, and federated learning approaches can synchronize edge and cloud components without compromising data integrity or compliance. In practice, a robotic welding station can use an edge-resident DT to detect sensor tampering in milliseconds, while cloud-based ZTA evaluates broader risk patterns before issuing network-wide policy changes. This interoperability is pivotal for building adaptive, security-aware CPS architectures capable of withstanding both real-time and persistent cyber threats.

5.3 Standardization of DT-ZTA Frameworks for Industry 4.0

The standardization of integrated DT and ZTA frameworks is crucial for ensuring secure, interoperable, and scalable implementations in Industry 4.0 environments. As smart factories increasingly adopt CPS that rely on heterogeneous hardware, software, and networking protocols, the absence of unified standards for DT-ZTA fusion leads to compatibility issues, inconsistent security postures, and limited cross-vendor operability. Paul, & Rao, (2022) emphasize that standardization efforts must address architectural templates, data exchange protocols, policy definition languages, and compliance metrics to support trustworthy automation across distributed manufacturing ecosystems. A standardized DT-ZTA framework defines how digital replicas of physical assets communicate with zero trust policy engines to validate access, monitor real-time operations, and initiate security responses. This includes uniform APIs for identity verification, behavioral telemetry, and trust evaluation, enabling seamless integration with existing industrial systems. For example, in a multi-vendor industrial robotic cell, standardized communication and authentication protocols prevent fragmented security controls and allow synchronized threat response through shared digital twin models.

Paul & Rao, (2022) also highlight the role of international consortia, such as ISO/IEC JTC 1 and the Industrial Internet Consortium, in aligning cybersecurity and DT interoperability guidelines. Standardization not only facilitates regulatory compliance but also accelerates the deployment of resilient DT-ZTA architectures tailored for Industry 4.0's dynamic and decentralized production paradigms.

5.4 Privacy and Ethical Considerations in DT-ZTA Deployments

The integration of DT and ZTA in smart manufacturing systems introduces complex privacy and ethical challenges that must be addressed to ensure responsible deployment. DT systems continuously collect, process, and store high-frequency data from both machine assets and human operators, raising significant concerns over personal privacy, consent, and data ownership (Ononiwu, et al., 2023) as represented in figure 5. When

combined with ZTA's pervasive monitoring and access validation mechanisms, the potential for invasive surveillance and misuse of sensitive data increases substantially (Wang et al., 2023).

One of the foremost ethical concerns is the potential violation of workers' privacy when behavioral analytics and digital profiles are used to enforce access control and monitor productivity. Inadequate data anonymization and lack of transparency around data usage can lead to distrust among employees and conflict with privacy regulations such as GDPR or CCPA. Furthermore, the delegation of access decisions to AI-driven DT-ZTA systems introduces questions of accountability, especially in cases of erroneous denial of access or biased policy enforcement.

Wang et al. (2023) argue for the inclusion of privacy-preserving mechanisms such as federated learning, differential privacy, and edge-based data minimization in DT-ZTA systems. Ethical deployments must prioritize informed consent, data transparency, and explainability to ensure that cybersecurity gains do not come at the cost of human dignity and rights within industrial cyber-physical environments.

Figure 5 presents a digital environment populated by silhouettes of IT and cybersecurity professionals working within a high-security data center, surrounded by illuminated server racks and transparent padlock icons—some open, some closed—representing dynamic access control. This visual captures the core concerns discussed in 5.4 Privacy and Ethical Considerations in DT-ZTA Deployments, where the fusion of DT technology and ZTA introduces both enhanced security and complex privacy challenges. As DTs continuously harvest real-time data from cyber-physical systems, including user behavior and operational telemetry, they risk capturing sensitive or personally identifiable information. ZTA further intensifies this scrutiny through persistent identity validation, behavior monitoring, and context-aware access decisions. Without robust data governance and ethical AI frameworks, this hyper-surveillance model can erode user privacy, especially in industrial settings where employees may be unknowingly monitored (Ononiwu, et al., 2023). The transparent overlay of code and locks in the image symbolizes the need for privacy-preserving mechanisms—such as anonymization, edge-processing, and federated learning—to prevent unauthorized exposure or misuse of data. This scenario underscores the necessity for ethical policy design, transparent data practices, and inclusive consent mechanisms in securing DT-ZTA infrastructures without compromising individual rights or regulatory compliance in smart manufacturing environments.

Figure 5: Picture of Visualizing Privacy and Ethical Dimensions in Digital Twin–Zero Trust Deployments (Mutahi, D. 2023).

Figure 5 presents a digital environment populated by silhouettes of IT and cybersecurity professionals working within a high-security data center, surrounded by illuminated server racks and transparent padlock icons—some open, some closed—representing dynamic access control. This visual captures the core concerns discussed in 5.4 Privacy and Ethical Considerations in DT-ZTA Deployments, where the fusion of DT technology and ZTA introduces both enhanced security and complex privacy challenges. As DTs continuously harvest real-time data from cyber-physical systems, including user behavior and operational telemetry, they risk capturing sensitive or personally identifiable information. ZTA further intensifies this scrutiny through persistent identity validation, behavior monitoring, and context-aware access decisions. Without robust data governance and ethical AI frameworks, this hyper-surveillance model can erode user privacy, especially in industrial settings where employees may be unknowingly monitored. The transparent overlay of code and locks in the image symbolizes the need for privacy-preserving mechanisms—such as anonymization, edge-processing, and federated learning—to prevent unauthorized exposure or misuse of data. This scenario underscores the necessity for ethical policy design, transparent data practices, and inclusive consent mechanisms in securing DT-ZTA infrastructures without compromising individual rights or regulatory compliance in smart manufacturing environments.

5.5 Open Research Challenges and Opportunities

Despite significant advancements, the integration of DT and ZTA in cyber-physical systems (CPS) still presents a landscape filled with unresolved research challenges and transformative opportunities. A key technical hurdle is the lack of a unified semantic model for synchronizing multi-modal data streams across heterogeneous assets, which limits real-time consistency and cross-domain interoperability as presented in table 4. Moreover, ensuring low-latency access control in DT-ZTA systems remains complex, particularly when balancing cloud-edge workloads in dynamic industrial environments (Alcaraz, et al., 2022).

Another challenge involves the explainability of AI-driven decisions within DT-ZTA frameworks. While machine learning enhances threat prediction and policy automation, the absence of interpretable decision-making models impedes trust, auditability, and regulatory compliance. There is a pressing need for explainable AI (XAI) mechanisms that can contextualize risk scoring, access revocations, and anomaly detection processes for system administrators and auditors.

Alcaraz, et al. (2022) also point to an untapped opportunity in leveraging quantum-safe cryptographic protocols within DT-ZTA pipelines to future-proof industrial security frameworks. Furthermore, there is increasing potential for adaptive digital twin models that evolve with the system's operational context, enabling predictive rather than reactive trust assessments (Ononiwu, et al., 2023). Future research must also address ethical AI integration, resilience against coordinated multi-vector attacks, and cross-border governance models for data integrity, sovereignty, and cyber-physical compliance in globally distributed manufacturing networks.

Table 4: Summary of Open Research Challenges and Opportunities in DT-ZTA Integration

Research Area	challenge	Opportunity	Potential Impact
Semantic Interoperability	Lack of standardized data models across heterogeneous assets	Develop unified semantic frameworks for DT-ZTA synchronization	Enables seamless integration and real-time coordination across platforms
Explainable AI in Security	Limited transparency in AI-driven threat detection and policy decisions	Integrate explainable AI (XAI) techniques for DT-ZTA systems	Improves trust, auditability, and regulatory compliance
Quantum-Resilient Architectures	Emerging risks from quantum computing threatening current encryption schemes	Design quantum-safe cryptographic protocols for DT-ZTA communications	Future-proofs industrial security against advanced computational threats
Adaptive Digital Twin Modeling	Static models struggle to capture dynamic, evolving system behaviors	Implement self-evolving DTs that learn from real-time data and context	Enhances predictive capability and response accuracy in fast-changing environments
Global Governance and Compliance	Regulatory fragmentation across jurisdictions complicates secure DT-ZTA deployment	Develop cross-border data governance and compliance frameworks	Facilitates global adoption of secure, standardized smart manufacturing infrastructures

6. Conclusion

6.1 Summary of Key Insights

This review highlights the transformative potential of integrating Digital Twin (DT) technology with ZTA to enhance the cybersecurity, resilience, and operational intelligence of smart manufacturing cyber-physical systems (CPS). DTs enable real-time behavioral modeling, predictive risk visualization, and anomaly detection by maintaining dynamic digital replicas of physical assets. When fused with ZTA, which enforces continuous authentication, micro-segmentation, and least-privilege access, the result is a self-adaptive and context-aware security framework. Key insights reveal that DT-powered behavioral analytics significantly reduce detection latency and support fine-grained access control through real-time state awareness. Furthermore, DT-ZTA synergy enables coordinated threat response by fusing system telemetry with policy enforcement engines.

The deployment of AI-enhanced DTs further amplifies security automation and predictive capabilities, while edge-cloud interoperability ensures scalable and latency-aware operations. Case studies demonstrate that such integration supports proactive mitigation of advanced persistent threats without compromising operational continuity. However, challenges persist around standardization, data privacy, and model explainability. Despite these, the convergence of DT and ZTA provides a future-proof foundation for secure-by-design industrial infrastructures. This study emphasizes the need for continued research into interoperable architectures, ethical AI, and compliance-aligned frameworks that support real-time trust evaluation, decentralized governance, and resilient automation in Industry 4.0 environments.

6.2 Implications for Industrial Cybersecurity

The integration of DT technology with ZTA presents a paradigm shift in industrial cybersecurity by enabling intelligent, adaptive, and real-time protection for cyber-physical systems (CPS). Unlike traditional perimeter-based models, the DT-ZTA approach supports continuous threat monitoring, behavior-based anomaly detection, and contextual access control rooted in real-time operational awareness. This ensures that industrial systems can autonomously detect and mitigate sophisticated attacks, such as command injection or lateral movement, by correlating deviations in digital twin behavior with dynamic trust scoring mechanisms.

For instance, in a smart manufacturing plant, if a CNC machine controlled via a DT begins executing unauthorized instructions outside of its normal operating parameters, ZTA policies can instantly revoke access, isolate the machine from the network, and trigger forensic analysis—all without human intervention. This elevates the cybersecurity posture from reactive to predictive, reducing mean time to detect (MTTD) and mean time to respond (MTTR).

Additionally, DT-ZTA frameworks support fine-grained micro-segmentation and enforce least-privilege principles, ensuring that users and devices only access resources essential to their roles. These implications underscore the necessity of incorporating DT-ZTA strategies into cybersecurity blueprints for Industry 4.0, establishing a scalable, resilient, and intelligent defense model for modern industrial environments.

6.3 Strategic Recommendations for Stakeholders

To realize the full potential of Digital Twin (DT) and ZTA integration in smart manufacturing environments, stakeholders must adopt a multi-pronged strategic approach that aligns cybersecurity with operational resilience and innovation. First, industrial leaders should prioritize the deployment of DTs across critical assets to enable real-time visibility, behavioral analytics, and predictive threat modeling. These DTs must be synchronized with ZTA policy engines that enforce continuous authentication, dynamic access control, and

micro-segmentation across the production network. Stakeholders must also invest in scalable edge-cloud infrastructures to support latency-sensitive security decisions at the edge while leveraging centralized policy management and AI-driven anomaly detection in the cloud. IT and OT teams should collaborate to ensure interoperability, secure data pipelines, and consistent identity governance across cyber-physical boundaries. For example, access to robotic assembly arms should be contextually approved based on DT state data, user behavior, and role-based constraints.

Regulatory and compliance teams must be involved early to ensure adherence to data protection and audit requirements. Additionally, vendors and integrators should align with emerging standards for DT-ZTA interoperability to avoid lock-in and promote system modularity. Finally, continuous workforce training in AI-enhanced security operations is essential to ensure human oversight, reduce response delays, and build cyber resilience across all industrial layers.

REFERENCES

[1]. Abiodun, K., Ogbuonyalu, U. O., Dzamefe, S., Vera, E. N., Oyinlola, A., & Igba, E. (2023). Exploring Cross-Border Digital Assets Flows and Central Bank Digital Currency Risks to Capital Markets Financial Stability. International Journal of Scientific Research and Modern Technology, 2(11), 32–45. https://doi.org/10.38124/ijsrmt.v2i11.447

[2]. Alcaraz, C., & Lopez, J. (2022). Digital twin: A comprehensive survey of security threats. IEEE Communications Surveys & Tutorials, 24(3), 1475-1503.

[3]. Alsmadi, I., & Xu, D. (2020). Security of cyber-physical systems using zero trust architecture. Computers & Security, 92, 101751. https://doi.org/10.1016/j.cose.2020.101751

[4]. Alzubaidi, A., & Kalutarage, H. K. (2021). Policy-based access control for Zero Trust architecture in smart industrial systems. Computers & Security, 106, 102286. https://doi.org/10.1016/j.cose.2021.102286

[5]. Andronie, M., Lăzăroiu, G., Ștefănescu, R., Uță, C., & Dijmărescu, I. (2021). Sustainable, smart, and sensing technologies for cyber-physical manufacturing systems: A systematic literature review. Sustainability, 13(10), 5495.

[6]. Atalor, S. I. (2019). Federated Learning Architectures for Predicting Adverse Drug Events in Oncology Without Compromising Patient Privacy ICONIC RESEARCH AND ENGINEERING JOURNALS JUN 2019 | IRE Journals | Volume 2 Issue 12 | ISSN: 2456-8880

[7]. Atalor, S. I., Ijiga, O. M., & Enyejo, J. O. (2023). Harnessing Quantum Molecular Simulation for Accelerated Cancer Drug Screening. International Journal of Scientific Research and Modern Technology, 2(1), 1–18. https://doi.org/10.38124/ijsrmt.v2i1.502

[8]. Atalor, S. I., Raphael, F. O. & Enyejo, J. O. (2023). Wearable Biosensor Integration for Remote Chemotherapy Monitoring in Decentralized Cancer Care Models. International Journal of Scientific Research in Science and Technology Volume 10, Issue 3 (www.ijsrst.com) doi : https://doi.org/10.32628/IJSRST23113269

[9]. Balta, E. C., Pease, M., Moyne, J., Barton, K., & Tilbury, D. M. (2023). Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems. IEEE Transactions on Automation Science and Engineering, 21(2), 1695-1712.

[10]. Balta, E. C., Pease, M., Moyne, J., Barton, K., & Tilbury, D. M. (2023). Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems. IEEE Transactions on Automation Science and Engineering, 21(2), 1695-1712.

[11]. Barricelli, B. R., Casiraghi, E., & Fogli, D. (2019). A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications. IEEE Access, 7, 167653–167671. https://doi.org/10.1109/ACCESS.2019.2953499

[12]. Cunningham, C., & Pollard, J. (2017). The eight business and security benefits of zero trust. Forrester Reseach November.

[13]. Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in

industrial IoT infrastructures. Electronics, 12(3), 566.

[14]. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. IEEE Access, 7, 45201–45218. https://doi.org/10.1109/ACCESS.2019.2908780

[15]. Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. IEEE Access, 8, 108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358

[16]. Glaessgen, E., & Stargel, D. (2012). The digital twin paradigm for future NASA and U.S. Air Force vehicles. 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, 1–14. https://doi.org/10.2514/6.2012-1818

[17]. Grieves, M., & Vickers, J. (2017). Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In Transdisciplinary Perspectives on Complex Systems (pp. 85–113). Springer. https://doi.org/10.1007/978-3-319-38756-7_4

[18]. He, Y., Xu, X., & Wang, L. (2021). Cybersecurity challenges for industrial cyber–physical systems: A comprehensive review. Robotics and Computer-Integrated Manufacturing, 68, 102114. https://doi.org/10.1016/j.rcim.2020.102114

[19]. Ihimoyan, M. K., Enyejo, J. O. & Ali, E. O. (2022). Monetary Policy and Inflation Dynamics in Nigeria, Evaluating the Role of Interest Rates and Fiscal Coordination for Economic Stability. International Journal of Scientific Research in Science and Technology. Online ISSN: 2395-602X. Volume 9, Issue 6. doi : https://doi.org/10.32628/IJSRST2215454

[20]. Imoh, P. O. (2023). Impact of Gut Microbiota Modulation on Autism Related Behavioral Outcomes via Metabolomic and Microbiome-Targeted Therapies International Journal of Scientific Research and Modern Technology (IJSRMT) Volume 2, Issue 8, 2023 DOI: https://doi.org/10.38124/ijsrmt.v2i8.494

[21]. Koulamas, C., & Kalogeras, A. P. (2018). Cyber-Physical Systems and Digital Twins in the Industrial Internet of Things: A Review. Computer Science Review, 30, 100–112. https://doi.org/10.1016/j.cosrev.2018.10.002

[22]. Lee, J., Bagheri, B., & Jin, C. (2016). Cyber-physical systems for predictive production systems. CIRP Annals, 65(1), 715–728. https://doi.org/10.1016/j.cirp.2016.06.001

[23]. Leng, J., Liu, Q., Ye, S., Jing, J., Wang, Y., & Zhang, H. (2021). Digital twin-driven manufacturing cyber-physical system for parallel controlling of smart workshop. Journal of Manufacturing Systems, 58, 52–64. https://doi.org/10.1016/j.jmsy.2020.06.017

[24]. Leng, J., Wang, D., Shen, W., Li, X., & Liu, Q. (2022). Digital twins-based smart manufacturing system design in Industry 4.0: A review. Journal of Manufacturing Systems, 62, 731–749. https://doi.org/10.1016/j.jmsy.2022.01.007

[25]. Li, X., Peng, J., Niu, J., Wu, F., Liao, J., & Choo, K. K. R. (2017). A robust and energy efficient authentication protocol for industrial internet of things. IEEE Internet of Things Journal, 5(3), 1606-1615.

[26]. Li, Y., Tao, Z., Wang, L., Du, B., Guo, J., & Pang, S. (2023). Digital twin-based job shop anomaly detection and dynamic scheduling. Robotics and Computer-Integrated Manufacturing, 79, 102443.

[27]. Liu, Q., Leng, J., Yan, D., Zhang, D., Wei, L., Yu, A., ... & Chen, X. (2021). Digital twin-based designing of the configuration, motion, control, and optimization model of a flow-type smart manufacturing system. Journal of Manufacturing Systems, 58, 52-64.

[28]. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. Proceedings of the IEEE, 104(5), 1039-1057.

[29]. Mutahi, D. (2023). Navigating The Delicate Balance: Privacy and Data Security In Computing, https://www.linkedin.com/pulse/navigating-delicate-balance-privacy-data-security-computing-mutahi

[30]. Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2023). Exploring Influencer Marketing Among

Women Entrepreneurs using Encrypted CRM Analytics and Adaptive Progressive Web App Development. International Journal of Scientific Research and Modern Technology, 2(6), 1–13. https://doi.org/10.38124/ijsrmt.v2i6.562

[31]. Ononiwu, M., Azonuche, T. I., Imoh, P. O. & Enyejo, J. O. (2023). Exploring SAFe Framework Adoption for Autism-Centered Remote Engineering with Secure CI/CD and Containerized Microservices Deployment International Journal of Scientific Research in Science and Technology Volume 10, Issue 6 doi : https://doi.org/10.32628/IJSRST

[32]. Ononiwu, M., Azonuche, T. I., Okoh, O. F., & Enyejo, J. O. (2023). AI-Driven Predictive Analytics for Customer Retention in E-Commerce Platforms using Real-Time Behavioral Tracking. International Journal of Scientific Research and Modern Technology, 2(8), 17–31. https://doi.org/10.38124/ijsrmt.v2i8.561

[33]. Ononiwu, M., Azonuche, T. I., Okoh, O. F.. & Enyejo, J. O. (2023). Machine Learning Approaches for Fraud Detection and Risk Assessment in Mobile Banking Applications and Fintech Solutions International Journal of Scientific Research in Science, Engineering and Technology Volume 10, Issue 4 doi : https://doi.org/10.32628/IJSRSET

[34]. Paul, B., & Rao, M. (2022). Zero-trust model for smart manufacturing industry. Applied Sciences, 13(1), 221.

[35]. Paul, B., & Rao, M. (2022). Zero-trust model for smart manufacturing industry. Applied Sciences, 13(1), 221.

[36]. Qi, Q., Tao, F., Zuo, Y., Zhao, D., & Lin, Y. (2021). Digital Twin Service Towards Smart Manufacturing. Journal of Manufacturing Systems, 58, 185–195. https://doi.org/10.1016/j.jmsy.2020.06.017

[37]. Qi, Q., Zhao, D., Liao, T. W., & Tao, F. (2018). Modeling of cyber-physical systems and digital twin based on edge computing, fog computing and cloud computing towards smart manufacturing. In International manufacturing science and engineering conference (Vol. 51357, p. V001T05A018). American Society of Mechanical Engineers.

[38]. Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. Internet of Things and Cyber-Physical Systems, 3, 213-248.

[39]. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[40]. Terca, K. (2022). Digital twin: Manufacturing case studies, smart factories and predictive maintenance, https://blog.3ds.com/brands/netvibes/digital-twin-manufacturing-case-studies-smart-factories-and-predictive-maintenance/

[41]. Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. Sensors, 20(19), 5480.

[42]. Vigna, R. (2023). The Tangible Benefits of Digital Twins: A New Era of Efficiency and Optimization https://www.linkedin.com/pulse/tangible-benefits-digital-twins-new-era-efficiency-rodrigo-vigna-x0zkc

[43]. Wang, P., Xu, N., Zhang, H., Sun, W., & Benslimane, A. (2021). Dynamic access control and trust management for blockchain-empowered IoT. IEEE Internet of Things Journal, 9(15), 12997-13009.

[44]. 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 future prospects. IEEE Internet of Things Journal, 10(17), 14965-1498

[45]. Wen, J., Gabrys, B., & Musial, K. (2022). Toward digital twin oriented modeling of complex networked systems and their dynamics: A comprehensive survey. Ieee Access, 10, 66886-66923.

[46]. Xie, J., Ma, H., Yu, L., & Fan, X. (2021). Real-time data-driven digital twin framework for complex equipment operation and maintenance in smart manufacturing. Advanced Engineering

Informatics, 47, 101230. https://doi.org/10.1016/j.aei.2020.101230

[47]. Xu, H., Wu, J., Pan, Q., Guan, X., & Guizani, M. (2023). A survey on digital twin for industrial internet of things: Applications, technologies and tools. IEEE Communications Surveys & Tutorials, 25(4), 2569-2598.

[48]. Xu, L. D., & Duan, L. (2020). Big Data for Cyber-Physical Systems in Industry 4.0: A Survey. Enterprise Information Systems, 14(2), 148–169. https://doi.org/10.1080/17517575.2019.1652321

[49]. Yan, Z., Zhang, P., & Wang, Y. (2020). Dynamic trust management and adaptive access control for Zero Trust in smart industrial environments. Future Generation Computer Systems, 108, 1232–1244. https://doi.org/10.1016/j.future.2020.03.010

[50]. Zheng, Y., Yang, S., Cheng, H., & Wang, T. (2021). Intelligent predictive maintenance strategy with digital twin for sustainable manufacturing systems. Journal of Cleaner Production, 316, 128321. https://doi.org/10.1016/j.jclepro.2021.128321