International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Standardization-Aligned Generative Sensor-Fusion Digital Twins For Secure Cyber-Physical Ecosystems

Submission Date: January 03, 2026, **Accepted Date:** January 30, 2026,
Published Date: February 20, 2026

Theodore M. Wycliffe
Polytechnic University of Hauts-de-France, Valenciennes, France

Abstract

The accelerating convergence of cyber–physical systems, large-scale sensor networks, and advanced artificial intelligence has created a technological landscape in which the digital twin is no longer a passive mirror of physical assets but an active, reasoning, and increasingly autonomous cyber counterpart. In industrial production, logistics, smart cities, and emerging cyber-physical infrastructures, digital twins now mediate real-time decision making, resilience management, and operational optimization. However, as digital twins have evolved in scale, autonomy, and connectivity, they have simultaneously become a critical locus of cybersecurity risk. Attacks against data integrity, synchronization, model drift, and cross-domain interoperability can propagate from the cyber layer into the physical domain, producing safety, reliability, and trust failures that are qualitatively different from traditional information-technology breaches. Within this context, generative artificial intelligence and sensor fusion have emerged as foundational enablers for next-generation digital twin ecosystems, providing adaptive modeling, probabilistic inference, and real-time semantic alignment across heterogeneous cyber–physical components.

This article develops a comprehensive theoretical and methodological framework for secure digital twin ecosystems grounded in generative AI–driven sensor fusion and aligned with international standardization regimes. The analysis is anchored in the recently proposed standardization-aligned framework for generative AI sensor fusion in secure digital twin ecosystems for cyber-physical systems

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

presented by Hussain et al. (2026), which integrates probabilistic logic, fault detection, synchronization mechanisms, and compliance with ISO and 3GPP standards. Building upon this foundation, the present study situates generative sensor-fusion digital twins within the broader historical evolution of digital twin architectures, Industry 4.0, smart manufacturing, logistics, and urban systems, synthesizing contributions from foundational digital twin theory, industrial cyber–physical system research, and emerging cybersecurity scholarship.

Through an extensive conceptual methodology based on comparative framework analysis, architectural decomposition, and security-driven systems modeling, the study examines how generative AI enables digital twins to move from deterministic replication toward self-learning, context-aware, and anticipatory cyber–physical representations. The results demonstrate that when sensor fusion is governed by probabilistic reasoning and aligned with standardized synchronization and reliability models, digital twins can provide not only operational optimization but also intrinsic cybersecurity functions such as anomaly detection, fault localization, trust verification, and resilience orchestration. The discussion further explores tensions between autonomy and control, openness and security, and innovation and standardization, revealing that generative digital twins constitute a new class of cyber-physical governance infrastructure rather than merely a technological tool.

The article concludes that secure digital twin ecosystems require a paradigm shift from component-level protection to ecosystem-level intelligence, where generative AI and standardized sensor fusion collectively establish a continuously verified and self-adapting cyber–physical reality. By integrating theoretical, architectural, and cybersecurity perspectives, this work provides a unified foundation for future research, industrial deployment, and policy development in the rapidly evolving domain of digital twin–enabled cyber–physical systems.

Keywords

Digital twin ecosystems, generative artificial intelligence, sensor fusion, cyber-physical security, Industry 4.0, standardization frameworks.

Introduction

The digital twin has emerged over the last decade as one of the most transformative conceptual and technological innovations in cyber–physical systems, industrial engineering, and data-driven infrastructure management. Originally conceived as a high-fidelity virtual replica of a physical asset, the digital twin has progressively evolved into an intelligent cyber entity capable of real-time synchronization, predictive reasoning, and autonomous decision support across complex industrial and societal systems (Grieves and Vickers, 2017; Tao et al., 2018). This evolution has

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

been driven by the rapid proliferation of sensors, the maturation of big-data analytics, and the increasing interconnection of machines, logistics, and urban infrastructures within the broader vision of Industry 4.0 and smart systems (Lee et al., 2014; Wang et al., 2016; Wang and Wan, 2016).

Yet the same forces that have empowered digital twins to become indispensable instruments of optimization, resilience, and innovation have also amplified their exposure to cybersecurity threats. As digital twins integrate heterogeneous data streams, control signals, and decision-making algorithms across organizational and geographical boundaries, they form cyber–physical ecosystems in which any breach, manipulation, or loss of synchronization can cascade into real-world disruptions. This fundamental vulnerability has been increasingly recognized by recent scholarship emphasizing that the digital twin is not merely a data model but a security-critical control and cognition layer for cyber–physical systems (Jaber et al., 2025; Jiang et al., 2024; McLaughlin, 2023).

The challenge is particularly acute in environments characterized by high degrees of uncertainty, dynamic behavior, and heterogeneous sensing, such as smart factories, logistics networks, and city-scale digital twins. Traditional deterministic models and static security architectures are insufficient to cope with the volume, velocity, and variability of data and threats in such settings (Rong et al., 2017; Park et al., 2020; Masoumi et al., 2023). What is required instead is a form of digital twin intelligence that can continuously learn from its environment, fuse disparate sensor signals into coherent situational awareness, and reason probabilistically about risk, reliability, and trust.

It is within this context that generative artificial intelligence and advanced sensor fusion have become pivotal. Generative AI, understood not merely as a content-producing technology but as a probabilistic modeling paradigm capable of synthesizing, predicting, and reasoning about complex data distributions, offers the ability to construct digital twins that are adaptive rather than static, anticipatory rather than reactive. When coupled with sensor fusion, which integrates data from multiple, often noisy and partially reliable sources into a unified representation, generative AI can create digital twins that embody a continuously updated, uncertainty-aware understanding of the physical world (Hussain et al., 2026).

The work of Hussain et al. (2026) represents a landmark in this domain by proposing a standardization-aligned framework for generative AI sensor fusion in secure digital twin ecosystems for cyber-physical systems. By embedding probabilistic logic, synchronization mechanisms, fault detection, and compliance with ISO and 3GPP standards into the core of the digital twin architecture, their framework redefines what it means for a digital twin to be both intelligent and secure. Rather than treating cybersecurity as an external add-on, this approach integrates security, reliability, and trust directly into the generative and inferential

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

processes that govern the digital twin's perception of reality.

This article builds upon and extends that foundational contribution by situating generative AI sensor-fusion digital twins within the broader historical, theoretical, and practical evolution of cyber–physical systems and digital twin research. Early digital twin architectures, as articulated by Sallez et al. (2015), Stetter and Hirsch (2015), and Bai et al. (2017), were primarily concerned with achieving high-fidelity simulation and lifecycle integration of physical assets. These efforts laid the groundwork for later digital twin–driven manufacturing and product lifecycle management systems (Pan et al., 2015; Sajjadi and Wang, 2015; Zhang and Tao, 2018). However, they largely assumed stable, trusted data environments and did not fully anticipate the scale, heterogeneity, and adversarial nature of contemporary cyber–physical ecosystems.

As digital twins have expanded into supply chains, smart cities, and collaborative manufacturing platforms, new forms of interdependence and vulnerability have emerged. Blockchain-enabled digital twin platforms, for example, have been proposed to address trust and provenance in distributed manufacturing networks (Li et al., 2021; Suhail et al., 2022), while logistics-focused digital twin architectures have emphasized synchronization and control across geographically dispersed actors (Park et al., 2020; Huang et al., 2024). At the same time, cybersecurity-focused analyses have highlighted that the very integration and openness that make digital twins powerful also create novel attack surfaces, including data poisoning, model inversion, synchronization attacks, and cross-layer exploits (Jaber et al., 2025; Jiang et al., 2024).

Against this backdrop, the integration of generative AI and sensor fusion into digital twin ecosystems is not merely an incremental enhancement but a qualitative shift in how cyber–physical reality is constructed, interpreted, and governed. Generative models allow digital twins to infer latent states, predict future trajectories, and evaluate counterfactual scenarios, while sensor fusion ensures that these inferences are grounded in a coherent and statistically robust representation of the physical world (Hussain et al., 2026). When these capabilities are aligned with international standards for reliability, communication, and safety, they create the possibility of digital twin ecosystems that are not only operationally effective but also inherently trustworthy.

Despite this promise, significant gaps remain in both theory and practice. Much of the existing digital twin literature treats security as a secondary concern, addressed through conventional network and application-level controls rather than through the epistemic and inferential core of the twin itself (Grieves and Vickers, 2017; Tao et al., 2018; Huang et al., 2024). Conversely, much of the cybersecurity literature has yet to fully engage with the distinctive characteristics of digital twins as dynamic, generative, and cyber–physical entities (McLaughlin, 2023; Jaber et al., 2025). There is therefore a pressing need for integrative

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

frameworks that bridge these domains and provide a coherent basis for the design, evaluation, and governance of secure digital twin ecosystems.

The present study addresses this gap by developing a comprehensive, standardization-aligned, generative sensor-fusion framework for digital twins that synthesizes insights from industrial digital twin theory, cyber–physical systems engineering, and emerging cybersecurity research. By grounding the analysis in the generative AI sensor-fusion framework of Hussain et al. (2026) and critically engaging with the broader literature, this article seeks to articulate not only how secure digital twin ecosystems can be built, but also what they mean for the future of cyber–physical governance, resilience, and innovation.

Methodology

The methodological approach of this study is rooted in interpretive, comparative, and theoretically grounded systems analysis rather than in empirical experimentation, reflecting the conceptual and architectural nature of the research problem. Digital twin ecosystems, particularly those incorporating generative artificial intelligence and sensor fusion, represent socio-technical systems whose properties cannot be fully captured through isolated metrics or laboratory simulations. Instead, they require an integrative methodology that combines architectural decomposition, theoretical synthesis, and critical evaluation across multiple domains of scholarship (Tao et al., 2018; Jaber et al., 2025).

The first methodological pillar of this research is comprehensive literature integration. The study systematically examines foundational digital twin theory, cyber–physical systems research, Industry 4.0 architectures, and emerging cybersecurity-oriented digital twin scholarship. Seminal works on digital twin architectures and lifecycle integration (Sallez et al., 2015; Grieves and Vickers, 2017; Bai et al., 2017; Stetter and Hirsch, 2015) are analyzed alongside more recent applications in manufacturing, logistics, supply chains, and cities (Pan et al., 2015; Park et al., 2020; Huang et al., 2024; Masoumi et al., 2023). This historical and thematic layering provides the contextual foundation necessary to evaluate how generative AI and sensor fusion alter the epistemic and operational role of the digital twin.

The second pillar is framework-driven comparative analysis centered on the generative AI sensor-fusion architecture proposed by Hussain et al. (2026). Rather than treating this framework as an isolated technical proposal, the methodology positions it as a reference architecture against which alternative digital twin and cybersecurity models are interpreted. Key architectural dimensions such as synchronization, probabilistic logic, fault detection, standard compliance, and multi-sensor integration are extracted from Hussain et al. (2026) and used as analytical lenses through which other digital twin frameworks are evaluated. This allows the study to identify where existing architectures implicitly align with,

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

diverge from, or fail to address the requirements of secure generative digital twins.

The third pillar is security-centric architectural decomposition. Drawing on cybersecurity-focused digital twin research (Jiang et al., 2024; McLaughlin, 2023; Jaber et al., 2025), the methodology examines how vulnerabilities, threats, and trust assumptions manifest at different layers of the digital twin ecosystem. These layers include physical sensing, data transmission, model generation, decision support, and control feedback. By mapping generative AI and sensor fusion capabilities onto these layers, the study elucidates how security can be embedded not merely at the perimeter but within the core inferential processes of the digital twin, as advocated by Hussain et al. (2026).

The fourth pillar is standardization-aligned analysis. International standards such as ISO reliability frameworks and 3GPP communication protocols play a crucial role in ensuring interoperability, safety, and regulatory acceptance of cyber–physical systems. The methodology therefore evaluates how generative sensor-fusion digital twins can be aligned with these standards, building on the explicit standardization focus of Hussain et al. (2026). This involves examining how synchronization, fault tolerance, and probabilistic reasoning can be expressed in forms that are compatible with standardized industrial and telecommunications architectures (Lee et al., 2014; Park et al., 2020).

Finally, the methodology incorporates critical and reflexive evaluation. Digital twin ecosystems are not neutral technologies but instruments of organizational, economic, and political power. By engaging with debates about autonomy, control, data ownership, and cybersecurity governance (McLaughlin, 2023; Suhail et al., 2022; Jaber et al., 2025), the study situates generative digital twins within a broader socio-technical landscape. This reflexive dimension ensures that the analysis does not reduce security to a purely technical property but recognizes it as a function of trust, accountability, and institutional alignment.

This multi-layered methodological design allows the study to move beyond narrow technical description toward a holistic understanding of secure generative digital twin ecosystems. It enables the integration of theoretical, architectural, and governance perspectives, providing a robust foundation for the descriptive and interpretive results that follow (Hussain et al., 2026; Jiang et al., 2024).

Results

The results of this conceptual and comparative analysis reveal that the integration of generative artificial intelligence and sensor fusion fundamentally transforms the nature of digital twin ecosystems from passive representational tools into active, security-relevant cyber–physical agents. When examined through the standardization-aligned framework articulated by Hussain et al. (2026), several key patterns emerge that differentiate secure generative digital twins from their conventional counterparts.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

ISSN-2750-1396

First, generative sensor-fusion digital twins exhibit a qualitatively different relationship to data uncertainty and reliability. Traditional digital twins, as described in early manufacturing and lifecycle models (Sallez et al., 2015; Pan et al., 2015; Sajjadi and Wang, 2015), typically assume that sensor data is sufficiently accurate and that discrepancies can be managed through calibration and deterministic filtering. In contrast, the generative approach emphasizes probabilistic logic, allowing the digital twin to explicitly represent uncertainty, confidence levels, and alternative hypotheses about the state of the physical system (Hussain et al., 2026). This probabilistic representation is not merely a statistical convenience but a foundational security feature, as it enables the detection of anomalous or adversarial data patterns that deviate from learned distributions (Jiang et al., 2024).

Second, the results indicate that sensor fusion in a generative framework creates a form of epistemic redundancy that enhances resilience against both faults and attacks. By integrating heterogeneous sensors with different failure modes, communication channels, and noise characteristics, the digital twin can cross-validate incoming data streams and identify inconsistencies that may signal physical malfunctions or cyber intrusions (Rong et al., 2017; Hussain et al., 2026). This stands in contrast to many existing digital twin implementations in smart manufacturing and logistics, which often rely on narrow or siloed data sources and therefore remain vulnerable to localized data corruption (Park et al., 2020; Huang et al., 2024).

Third, the standardization-aligned synchronization mechanisms emphasized by Hussain et al. (2026) yield a more robust temporal and semantic coherence between physical and digital entities. In distributed cyber–physical systems such as supply chains and smart cities, latency, packet loss, and asynchronous updates can create divergent realities between the physical world and its digital twin, undermining both operational effectiveness and security (Masoumi et al., 2023; Park et al., 2020). By embedding synchronization and reliability constraints derived from ISO and 3GPP standards into the generative sensor-fusion process, the digital twin maintains a continuously verified alignment with the physical system, reducing the window of opportunity for stealthy attacks and undetected faults.

Fourth, the analysis shows that generative digital twins support a more proactive form of cybersecurity than conventional monitoring systems. Rather than merely detecting known signatures or threshold violations, generative models can simulate plausible future states, assess the likelihood of cascading failures, and evaluate the impact of hypothetical attack scenarios (Hussain et al., 2026; Jaber et al., 2025). This predictive capability transforms the digital twin into a strategic security instrument capable of guiding preventative interventions and adaptive defense strategies.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

ISSN-2750-1396

Fifth, the results reveal a convergence between blockchain-enabled trust mechanisms and generative sensor-fusion digital twins. Distributed ledger technologies have been proposed as a means of ensuring data integrity, provenance, and non-repudiation in digital twin ecosystems (Li et al., 2021; Suhail et al., 2022). When combined with generative AI, these mechanisms can be used not only to record what has happened but also to validate the plausibility and consistency of what is being inferred about the physical system, creating a multi-layered trust architecture that spans data, models, and decisions (Hussain et al., 2026).

Overall, the results indicate that secure generative digital twin ecosystems represent a distinct architectural paradigm in which sensing, inference, and security are inseparable. Rather than adding cybersecurity controls to an otherwise static digital model, the generative sensor-fusion approach embeds trust, reliability, and resilience into the very process by which the digital twin constructs and maintains its representation of reality (Jiang et al., 2024; McLaughlin, 2023).

Discussion

The implications of these results extend far beyond the technical domain of digital twin architecture into the broader theory and practice of cyber–physical governance. The emergence of generative AI sensor-fusion digital twins, particularly when aligned with international standards as proposed by Hussain et al. (2026), challenges long-standing assumptions about how physical systems should be modeled, controlled, and secured.

At a theoretical level, the generative digital twin represents a shift from representational to epistemic modeling. Classical digital twin theory, as articulated by Grieves and Vickers (2017) and Tao et al. (2018), emphasized the importance of high-fidelity replication and lifecycle integration. While these goals remain relevant, they implicitly assume that the physical system is knowable and that the digital twin's task is to mirror it as accurately as possible. Generative AI disrupts this assumption by treating the digital twin not as a mirror but as a probabilistic reasoner that constructs its own understanding of the physical world based on incomplete, noisy, and potentially adversarial data (Hussain et al., 2026). This epistemic stance aligns more closely with theories of situational awareness and adaptive cognition in cyber–physical systems (Suhail et al., 2022; Jiang et al., 2024).

From a cybersecurity perspective, this shift has profound consequences. Traditional security architectures are largely perimeter-based and reactive, designed to protect static assets and detect known patterns of attack. In contrast, generative digital twins operate within the data and model space, continuously evaluating whether observed sensor patterns are consistent with learned or expected behavior. This enables a form of intrinsic security that is not dependent on predefined signatures but on the statistical and semantic coherence of the cyber–physical system itself (Hussain et al., 2026; Jaber et al., 2025).

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

ISSN-2750-1396

However, this same autonomy and intelligence introduce new risks and ethical challenges. If a digital twin is capable of generating its own hypotheses, predictions, and decisions, then questions of accountability, transparency, and control become more complex. In industrial and urban contexts, where digital twins may influence safety-critical operations, the opacity of generative models can be problematic (Masoumi et al., 2023; McLaughlin, 2023). Standardization-aligned frameworks, such as those proposed by Hussain et al. (2026), partially address this issue by embedding reliability, synchronization, and compliance requirements into the architecture. Yet the tension between innovation and regulation remains an open and contested space.

The discussion also highlights the importance of ecosystem-level thinking. Digital twins are increasingly embedded in networks of other digital twins, data platforms, and organizational processes. Blockchain-enabled collaboration platforms (Li et al., 2021) and logistics control architectures (Park et al., 2020) demonstrate that trust and coordination must be managed across institutional boundaries. Generative sensor-fusion digital twins can serve as a unifying layer that mediates these interactions, but only if they are designed with interoperability and governance in mind (Huang et al., 2024; Jaber et al., 2025).

Another critical dimension is resilience. Cyber–physical systems are inherently exposed to both random failures and intentional attacks. The probabilistic and predictive capabilities of generative digital twins provide a means of anticipating and mitigating these risks, but they also require continuous validation and updating. Model drift, data bias, and adversarial manipulation of training data represent new forms of vulnerability that must be addressed through both technical and organizational controls (Jiang et al., 2024; McLaughlin, 2023). The standardization-aligned approach of Hussain et al. (2026) offers a pathway for integrating these controls into a coherent framework, but its practical implementation will require sustained collaboration between industry, regulators, and researchers.

Finally, the broader societal implications of secure generative digital twin ecosystems must be considered. As digital twins become central to the management of factories, supply chains, and cities, they effectively become infrastructures of governance. Decisions about how they are designed, secured, and regulated will shape not only technical outcomes but also economic competitiveness, environmental sustainability, and social trust (Masoumi et al., 2023; Huang et al., 2024). The integration of generative AI and sensor fusion, therefore, should be understood not merely as a technological upgrade but as a transformation in how cyber–physical reality is collectively constructed and negotiated (Hussain et al., 2026).

Conclusion

This study has argued that the convergence of generative artificial intelligence, sensor fusion, and digital twin technology marks a fundamental

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

ISSN-2750-1396

turning point in the evolution of cyber–physical systems. Building on the standardization-aligned generative sensor-fusion framework proposed by Hussain et al. (2026), the analysis has demonstrated that secure digital twin ecosystems are no longer adequately described as static models or even as dynamic simulators. They are instead epistemic agents that continuously infer, predict, and validate the state of the physical world while embedding security, reliability, and trust into their core operations.

By integrating probabilistic logic, multi-sensor validation, synchronization mechanisms, and international standards, generative digital twins offer a pathway toward cyber–physical systems that are not only more efficient but also more resilient and trustworthy. At the same time, they introduce new challenges related to governance, transparency, and accountability that demand interdisciplinary attention. The future of digital twins, therefore, lies not only in technical innovation but in the development of frameworks that align intelligence with security, autonomy with control, and global standards with local realities.

REFERENCES

1. Huang, Y., Ghadge, A., and Yates, N. Implementation of digital twins in the food supply chain: A review and conceptual framework. International Journal of Production Research, 62(17), 6400–6426.
2. Jaber, A., Koufos, I., and Christopoulou, M. A comprehensive state-of-the-art review for digital twin: Cybersecurity perspectives and open challenges. In Advances on P2P, parallel, grid, cloud and internet computing. Lecture Notes on Data Engineering and Communications Technologies, Vol. 232. Springer, Cham.
3. Wang, J., Wan, J., Zhang, D., Li, D., and Zhang, C. Towards smart factory for Industry 4.0: A self-organized multi-agent system with big data based feedback and coordination. Computer Networks, 101, 158–168.
4. Masoumi, H., Shirowzhan, S., Eskandarpour, P., and Pettit, C. J. City digital twins: Their maturity level and differentiation from 3D city models. Big Earth Data, 7(1), 1–36.
5. Hussain, M. A., Meruga, V. B., Rajamandrapu, A. K., Varanasi, S. R., Valiveti, S. S. S., and Mohapatra, A. G. Generative AI Sensor Fusion for Secure Digital Twin Ecosystems: A Standardization-Aligned Framework for Cyber-Physical Systems. IEEE Communications Standards Magazine, doi: 10.1109/MCOMSTD.2026.3660106.
6. Grieves, M., and Vickers, J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Journal of Systems Science and Systems Engineering, 26(6), 681–705.
7. Li, M., Fu, Y., Chen, Q., and Qu, T. Blockchain-enabled digital twin collaboration platform for heterogeneous socialized manufacturing resource management. International Journal of Production Research, 61(12), 3963–3983.
8. Sallez, Y., Deneux, D., and Thomas, P. A platform architecture for cyber-physical systems: A digital twin concept for an

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 87-97
OCLC – 1368736135

industrial system. Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation.

9. Suhail, S., Malik, S. U. R., Jurdak, R., Hussain, R., Matulevicius, R., and Svetinovic, D. Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins. Computers in Industry, 141, 103699.
10. Lee, J., Kao, H. A., and Yang, S. Service innovation and smart analytics for Industry 4.0 and big data environment. Procedia CIRP, 16, 3–8.
11. Bai, Y., Harrison, R., and Eckert, C. Digital twin approach for simulating complex products across the lifecycle. Proceedings of the Design Society: DESIGN Conference.
12. Jiang, Y., Wang, W., Ding, J., Lu, X., and Jing, Y. Leveraging digital twin technology for enhanced cybersecurity in cyber–physical production systems. Future Internet, 16(4), 134.
13. Pan, Y., Gao, J., Li, Z., Guo, M., and Zhang, N. Digital twin driven smart production and services. Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems.
14. Park, K. T., Son, Y. H., and Noh, S. D. The architectural framework of a cyber-physical logistics system for digital-twin-based supply chain control. International Journal of Production Research, 59(19), 5721–5742.
15. Sajjadi, S., and Wang, L. Digital twin for predicting remaining useful life of rotating components in cyber-physical systems. Procedia CIRP, 38, 193–198.
16. Stetter, R., and Hirsch, M. Towards a digital twin for machine tools. Procedia CIRP, 36, 101–106.
17. Wang, B., and Wan, J. Smart city and the applications. In Internet of Things: Principles and Paradigms. Academic Press.
18. Tao, F., Cheng, J., Qi, Q., Zhang, M., and Luo, Y. Digital twin-driven product lifecycle management: A survey. Robotics and Computer-Integrated Manufacturing, 53, 1–10.
19. Zhang, H., and Tao, F. Digital twin-driven smart manufacturing system. IEEE Transactions on Industrial Informatics, 14(6), 2617–2628.
20. Rong, K., Hu, G., and Lin, Y. Cyber-physical systems for smart manufacturing: Issues and challenges. Journal of Industrial Information Integration, 8, 1–3.
21. McLaughlin, K. L. The power of digital twins in the cybersecurity mesh. EDPACS, 68(6), 35–39.