

Towards the Intelligent Acting Digital Twin: From Passive Monitoring to Autonomous Cyber-Physical Actuation

Navaneeth K N*, Ms. Riya K Prakash**, Dr. L C Manikandan***

*B.Tech Student, Department of CSE, Universal Engineering College, Thrissur, Kerala, India.

E-mail: navaneethkn.official@gmail.com

** Assistant Professor, Department of CSE, Universal Engineering College, Thrissur, Kerala, India.

E-mail: riyajothish13@gmail.com

*** Professor, Department of CSE, Universal Engineering College, Thrissur, Kerala, India.

E-mail: manikandanykcet@gmail.com

Abstract:

The paradigm of the Digital Twin (DT) is undergoing a critical evolution. As outlined in the structural blueprint that motivates this study, this paper examines the transition from existing technology which primarily functions as passive, data-gathering digital shadows to our proposed technology: the Intelligent Acting Digital Twin (IADT). Existing systems excel at mirroring physical assets but rely heavily on human-in-the-loop intervention for decision-making and actuation. The IADT framework proposed herein integrates advanced machine learning, continuous optimization algorithms, and bi-directional communication to enable autonomous, closed-loop physical actuation. By embedding Reinforcement Learning (RL) and deterministic control logic directly into the twin's cognitive layer, the IADT can predict state changes, synthesize optimal interventions, and execute them in the physical world without manual oversight. The framework further formalises the operating conditions under which such autonomy can be safely exercised, including bounded-autonomy safeguards, cryptographically verifiable actuation, and continuous state-fidelity checks between the virtual and physical domains. Finally, we explore the future scope of this technology, focusing on multi-twin orchestration, cognitive self-healing systems, and the integration of large-scale predictive models for fully autonomous industrial ecosystems.

Keywords — Intelligent Acting Digital Twin, Cyber-Physical Systems, Autonomous Actuation, Bidirectional Synchronization, Reinforcement Learning, Industry 4.0, Closed-loop Control, Edge Computing, Zero-Trust Security, Kalman Filtering.

I. INTRODUCTION

A. A. Background

The concept of the Digital Twin has historically been defined as a virtual representation of a physical asset, process, or system [1]. In its previous existing iterations, the digital twin has primarily served as a sophisticated dashboard a highly accurate simulation fed by unidirectional data streams from Internet of Things (IoT) sensors [2]. These legacy systems are more accurately classified as “Digital Shadows” or “Digital Models”

[3]. They allow human operators to monitor health, predict maintenance needs, and visualize telemetry data, but they inherently lack agency [4]. When an anomaly is detected or an optimization opportunity arises in the physical asset, the traditional digital twin can only trigger an alert; the physical intervention relies entirely on human execution or disjointed, localized Programmable Logic Controllers (PLCs) [5].

This distinction between observation and agency is not merely semantic. A digital shadow, however faithful its simulation, is fundamentally

reactive: it waits for a human to interpret its output and to initiate the corresponding physical response. In industrial settings that operate continuously across thousands of interdependent components, this reliance on manual interpretation introduces a structural ceiling on how quickly, and how consistently, an operation can respond to changing conditions. As data volumes generated by dense sensor networks continue to grow, the cognitive burden placed on human operators grows with them, making the passive digital twin increasingly difficult to act upon in a timely fashion even when its diagnostic accuracy is high.

It is useful to place this observation within the broader trajectory of digital twin research. Early work in the field concentrated almost entirely on establishing that a virtual model could track a physical asset with sufficient fidelity to be useful at all that is, on the modeling problem itself [1, 6]. As modeling techniques matured and sensor deployment became inexpensive and ubiquitous, attention shifted toward what could be done with an accurate twin once it existed, giving rise to monitoring, diagnostics, and predictive-maintenance applications [2, 4]. The Intelligent Acting Digital Twin (IADT) can be read as the natural next stage in this trajectory: having established that a virtual twin can know what is happening to its physical counterpart, the open question this paper addresses is what happens when that twin is also permitted to decide, and to act.

B. B. Positioning Relative to Existing Digital Twin Research

Several prior surveys have catalogued the enabling technologies, modeling techniques, and application domains of the digital twin at a broad level [6, 7, 8, 9]. These works are invaluable in mapping the landscape of what digital twins currently do, but by design they treat actuation as a peripheral concern rather than as a first-class architectural requirement. Systematic literature reviews of the field similarly emphasize definitional clarity and characterisation of existing systems [1, 3, 10], again largely within the passive-monitoring paradigm. This paper is positioned differently: rather than surveying the breadth of

existing digital twin applications, it focuses narrowly on the architectural, algorithmic, and security requirements that must be satisfied for a twin to safely close the loop and act on the physical world it represents.

C. C. The Actuation Gap

This paper addresses the fundamental limitation of previous existing models: the actuation gap [11]. As cyber-physical systems scale in complexity, the latency introduced by human-in-the-loop decision making becomes a critical bottleneck [12]. The IADT represents the next frontier in this domain [6]. By closing the loop between the physical and virtual spaces, the IADT does not merely observe; it acts [7]. It utilizes continuous streams of real-time data to update its internal state, simulates thousands of potential future states using predictive AI, selects the optimal course of action, and autonomously sends control signals back to the physical asset's actuators [13, 14]. This shift from passive observation to intelligent action is essential for the realization of truly autonomous smart manufacturing, resilient energy grids, and self-optimizing supply chains [8].

The actuation gap can be understood as the cumulative delay and information loss that accrues at every handoff between the sensing system, the human interpreter, and the eventual physical actuator. Each handoff introduces the possibility of misread telemetry, delayed response, or inconsistent decision-making across shifts and operators. The IADT is proposed specifically to eliminate these handoffs for the class of decisions that can be safely delegated to an autonomous agent, while still preserving a clear escalation path back to human authority whenever the situation falls outside the bounds the system has been designed and verified to handle.

D. D. Scope and Organization

The remainder of this paper is organized as follows. Section II presents the layered architectural framework that underpins the IADT, describing the physical, communication, cognitive, and actuation layers and how they interoperate. Section III examines the role of artificial intelligence, and Reinforcement Learning in particular, in enabling autonomous decision-

making, together with the edge-computing considerations that make real-time actuation feasible. Section IV discusses closed-loop synchronization and the state fidelity mechanisms that keep the virtual and physical domains aligned. Section V presents an implementation case study drawn from precision manufacturing. Section VI addresses the security and trust requirements that must accompany any system capable of autonomous physical actuation. Section VII discusses open challenges and future directions, extending the future scope themes introduced above, and concludes the paper.

II. II. THE ARCHITECTURAL FRAMEWORK OF THE IADT

To transition from a passive monitor to an active participant, the IADT requires a robust, multi-layered architecture capable of handling ultra-low latency bi-directional data flow [15]. Unlike the largely one-directional data pipelines that characterize conventional digital twins, every layer of the IADT architecture must be designed with the expectation that information will flow back toward the physical asset in the form of executable commands, not merely forward toward a dashboard. The proposed framework is structured into four primary layers, summarized in Table I and described in detail below.

E. A. The Physical Layer

This comprises the tangible assets machinery, robotics, environmental systems, or entire facilities [9]. Crucially, this layer must be equipped not only with high-fidelity sensors (for state extraction) but also with network-addressable actuators capable of receiving and executing complex command arrays from the virtual space [1]. The sensing and actuation sub-systems within this layer must therefore be co-designed: a sensor suite that captures state at high resolution is of limited value if the corresponding actuators cannot respond at a comparable resolution and speed, and vice versa.

In practice, retrofitting a legacy physical asset to satisfy these requirements is often the single largest engineering effort in deploying an IADT, since many industrial actuators were originally designed to accept only local, manually configured setpoints

rather than dynamically generated command arrays from an external system. Bridging this gap typically requires an intermediary controller layer that exposes a standardized, network-addressable interface over the asset's existing actuation hardware without compromising the safety interlocks already built into that hardware.

F. B. The Communication Layer

Acting as the central nervous system, this layer requires high-bandwidth, deterministic networking (such as 5G URLLC or Time-Sensitive Networking) to ensure that control signals sent from the twin arrive at the physical asset with microsecond precision [2]. Determinism is emphasized here over raw throughput, because an autonomous actuation command that arrives late, or arrives out of order relative to a subsequent command, can be more dangerous than no command at all; the communication layer must therefore guarantee bounded, predictable latency rather than merely a high average data rate.

This requirement also shapes how the communication layer must handle network degradation. Rather than allowing latency to grow unbounded under congestion, a deterministic network fabric enforces admission control and traffic shaping so that safety-critical actuation traffic is never queued behind lower-priority telemetry, and so that the cognitive layer always has an accurate, bounded estimate of how stale any given piece of incoming sensor data may be before it commits to an action based on it.

G. C. The Cognitive Layer (Our Proposed Technology)

This is the brain of the IADT [4]. Unlike existing twins that rely purely on physics-based simulation, the IADT's cognitive layer merges mechanistic models with deep learning [5]. It continuously trains on streaming data to refine its understanding of the physical asset's degradation, operational limits, and environmental variables [11]. This hybrid design allows the cognitive layer to inherit the interpretability and safety guarantees of first-principles physical models while retaining the adaptability of data-driven learning, so that its predictions remain grounded even as the asset's behavior drifts over its operational lifetime.

The mechanistic component of this hybrid model also serves as a built-in sanity check on the learned component: because the physics-based model encodes known conservation laws and mechanical constraints, any learned policy whose recommended action would violate those constraints can be flagged and rejected before it is ever passed to the actuation layer, providing a lightweight but effective safeguard against learned behaviors that have drifted outside physically plausible bounds.

H. D. The Actuation Layer

The defining feature of the IADT. This layer translates the cognitive layer's strategic decisions into machine-readable control codes (e.g., altering a spindle speed, rerouting power, or adjusting chemical mixtures) and pushes them to the physical layer [12]. It is this layer, more than any other, that separates the IADT from every prior generation of digital twin: where earlier systems terminate their pipeline at a recommendation or an alert, the actuation layer closes the loop by converting that recommendation directly into a verified, executable instruction.

Because the actuation layer is the final point at which a purely virtual decision becomes an irreversible physical event, it is also the layer at which the safety and security mechanisms discussed in Sections IV and VI are most tightly enforced: every outgoing command passes through the state fidelity check described in Section IV and the cryptographic verification described in Section VI before it is ever dispatched to the physical asset.

TABLE I THE FOUR ARCHITECTURAL LAYERS OF THE IADT		
Layer	Primary Function	Key Enabling Technology
Physical	Houses the sensors and network-addressable actuators on the asset itself	High-fidelity sensing arrays; industrial actuators
Communication	Carries state data and control signals between physical and virtual domains	5G URLLC; Time-Sensitive Networking
Cognitive	Fuses physics-based models with deep learning to decide on optimal action	Hybrid mechanistic / deep-learning models
Actuation	Converts strategic decisions into verified, machine-readable control commands	Real-time control-code generation and dispatch

III. III. ARTIFICIAL INTELLIGENCE AND AUTONOMOUS DECISION-MAKING

I. A. Reinforcement Learning as the Core Decision Engine

The core differentiator of the IADT is its reliance on advanced AI to dictate action [6]. The implementation of Reinforcement Learning (RL) is particularly effective in this context [7]. In a standard RL setup, an agent learns to make decisions by performing actions in an environment to maximize a cumulative reward [10]. The IADT serves as the ultimate training ground for the RL agent. Because the twin is a high-fidelity replica, the RL agent can simulate millions of operational scenarios including catastrophic failures safely within the virtual environment [13]. Once an optimal policy is generated, it is deployed. As the physical asset operates, the IADT monitors the outcome of its autonomous actions, feeding the results back into the RL model for continuous, lifelong learning [14].

A central advantage of this simulate-then-deploy methodology is that the most valuable training experiences rare failure modes, edge-case operating conditions, and near-miss scenarios can be explored exhaustively in the virtual environment without ever placing the physical asset, or the people around it, at risk. The RL agent therefore accumulates exposure to a far broader distribution of operating conditions than could ever be safely encountered during live operation, which in turn allows the deployed policy to generalize more robustly once it begins to act on the physical asset.

J. B. Edge-Native Inference

Furthermore, the integration of edge computing prevents the latency typically associated with cloud-based AI [9]. By deploying the IADT's decision-making algorithms at the network edge (physically close to the asset), the system achieves the ultra-low latency required for real-time actuation and safety-critical interventions [5]. Running inference at the edge also reduces the system's dependence on continuous, high-

bandwidth connectivity to a remote data center, so that the cognitive layer can continue to make bounded, locally verified decisions even during transient network disruptions.

K. C. Safety-Constrained Policy Learning

A purely reward-maximizing RL agent, left unconstrained, could in principle learn a policy that achieves high cumulative reward through actions that are unsafe or undesirable in ways the reward function failed to anticipate. To guard against this, the IADT's training regime incorporates explicit safety constraints alongside the reward signal, so that the agent is trained not simply to maximize performance but to maximize performance subject to hard limits on variables such as mechanical stress, thermal load, or energy draw. Actions that would violate these constraints are excluded from the agent's action space during both training and deployment, rather than merely being discouraged through a reward penalty that a sufficiently aggressive policy might learn to override.

IV. CLOSED-LOOP SYNCHRONIZATION AND STATE FIDELITY

For an IADT to safely exert physical control, the synchronization between the physical asset and the digital twin must be virtually absolute [8]. The proposed technology utilizes a Dynamic Time Warping (DTW) algorithm combined with Kalman filtering to continuously align the virtual state with the physical state [15]. DTW allows the system to compare time series telemetry from the physical asset against the twin's simulated trajectory even when the two are not perfectly aligned in time, while the Kalman filter continuously fuses noisy sensor readings with the twin's predictive model to produce a best estimate of the asset's true state.

If the deviation between the twin's predicted state and the asset's actual state exceeds a predefined safety threshold, the IADT immediately degrades its autonomy, returning control to localized safety systems or human operators [4]. This “bounded autonomy” ensures that the acting twin can optimize operations aggressively while remaining within strict, deterministic safety envelopes [12]. Bounded autonomy can therefore

be understood as a graceful-degradation policy: rather than a binary switch between fully autonomous and fully manual operation, the IADT is designed to fall back progressively first to a more conservative autonomous policy, and only thereafter to human control so that the loss of state fidelity does not itself become a source of instability.

Maintaining this level of synchronization is a continuous, not a one-time, engineering effort. Sensor drift, mechanical wear, and firmware updates on the physical asset can each cause the real system to diverge gradually from the model the twin was originally calibrated against. The IADT therefore periodically re-estimates the parameters of its mechanistic model against recent operating data, so that small, benign discrepancies are absorbed through recalibration rather than being repeatedly flagged as safety-threshold violations that unnecessarily suspend autonomous operation.

V. IMPLEMENTATION CASE STUDY: AUTONOMOUS MANUFACTURING CELL

Consider a high-precision CNC machining cell [1]. A traditional digital twin would monitor tool wear and alert an operator when the tool is likely to fail [2]. The IADT, conversely, acts upon this information autonomously.

As the IADT detects micro-vibrations indicative of anomalous tool wear, its cognitive layer simulates the impact of this wear on the final product's tolerances [3]. Recognizing an impending quality failure, the IADT dynamically generates a new control program. It instructs the physical machine to reduce its feed rate by 12% and alter the coolant flow an action executed in milliseconds [13]. The IADT actively prolongs the tool's life, ensures the part remains within tolerance, and automatically schedules an autonomous mobile robot (AMR) to deliver a replacement tool exactly when the current run finishes, entirely without human intervention [11].

This single scenario illustrates the compounding value of closing the loop across the entire architecture described in Section II: the physical layer's vibration sensors supply the raw signal, the communication layer delivers it to the cognitive

layer within the deterministic latency budget, the cognitive layer reasons over the consequence of continued wear, and the actuation layer executes the corrective response and coordinates the downstream logistics of tool replacement all without a human operator ever needing to interpret a dashboard or issue a manual instruction.

It is instructive to contrast this outcome with what a conventional, passive digital twin would have produced in the same scenario. A passive twin would have detected the same micro-vibration signature and generated the same underlying diagnosis, but its output would have terminated at an alert queued for a human operator's attention. Depending on shift staffing and operator workload, that alert might be acted upon within minutes, or it might sit unaddressed until the tool fails outright and the batch is scrapped. The IADT collapses this variable response window into a fixed, millisecond-scale response, converting what was previously a matter of operator vigilance into a matter of engineered, verifiable system behavior.

The same pattern generalizes beyond this single manufacturing cell. Any process in which a physical asset produces a measurable early-warning signal ahead of a costly failure thermal creep in a power-distribution transformer, pressure anomalies in a chemical reactor, or vibration signatures in a wind-turbine gearbox is, in principle, a candidate for the same architecture: sense the precursor, simulate its consequence, select a corrective action, and execute it within a bounded-autonomy envelope. The manufacturing cell described above is therefore best read as a representative instance of a broader class of applications rather than as an isolated example.

VI. VI. SECURITY AND TRUST IN AUTONOMOUS ACTUATION

Granting a virtual entity the authority to manipulate physical reality introduces severe cybersecurity risks [10]. An exploited IADT could be used to cause catastrophic physical damage [9]. Therefore, the architecture mandates a Zero Trust framework. Every actuation command generated by the IADT must be cryptographically signed and verified by a localized hardware security module (HSM) on the physical asset before execution [4].

Additionally, immutable ledger technology (such as a lightweight blockchain) is utilized to record every autonomous decision and its physical outcome, providing a transparent, auditable trail of the machine's behavior [12].

This combination of cryptographic verification and immutable logging serves two complementary purposes. First, the HSM-based signature check ensures that a command executed on the physical asset genuinely originated from the authorized cognitive layer and has not been tampered with in transit. Second, the auditable ledger allows engineers and regulators to reconstruct, after the fact, exactly why the IADT chose a given action, which is essential both for post-incident investigation and for building the long-term institutional trust required before autonomous actuation is extended to increasingly critical systems.

Beyond command-level verification, the overall threat model for the IADT must also account for attacks directed at the training pipeline itself. An adversary who can subtly poison the streaming data used to retrain the cognitive layer, for instance by injecting fabricated sensor readings over an extended period, could in principle bias the learned policy toward unsafe behavior without ever forging an individual command. Defending against this class of attack requires the same kind of provenance tracking and anomaly detection applied to the training data stream as is applied to the actuation commands themselves, so that the integrity of the loop is protected end-to-end rather than only at its final step.

VII. VII. OPEN CHALLENGES AND FUTURE DIRECTIONS

L. A. Multi-Twin Orchestration

The future scope of this technology extends far beyond isolated assets. The next generation of IADTs will feature multi-twin orchestration, where thousands of acting twins communicate, negotiate, and optimize entire smart cities, power grids, and global supply chains autonomously [8, 15]. Coordinating autonomous action across such large populations of twins introduces new challenges in negotiation and conflict resolution, since two twins acting independently but optimally from their own

local perspective may nonetheless issue commands that interfere with one another at the system level.

M.B. Cognitive Self-Healing Systems

A related direction is the development of cognitive self-healing systems, in which the IADT not only corrects the operating parameters of the physical asset but also diagnoses and, where possible, autonomously reconfigures around degraded or failing components before a full failure occurs. Realizing this capability requires the cognitive layer to reason not just about the asset's immediate operating state but about the long-term trajectory of its own components' health.

N. C. Integration with Large-Scale Predictive Models

Finally, the integration of large-scale predictive models into the cognitive layer promises to extend the IADT's planning horizon and its ability to generalize across asset types with limited additional training. Realizing this future requires continued advancement in deterministic networking, edge-native AI, and rigorous cyber-physical security protocols to ensure that as our virtual systems gain the power to act, they do so with absolute safety and precision [5, 11].

A foundation model pre-trained across a large and diverse population of physical assets could, in principle, provide a strong prior for a newly commissioned IADT, allowing it to arrive at a competent operating policy with far less asset-specific training data than would otherwise be required. This is particularly valuable for smaller operators who lack the years of historical operating data available to a large industrial fleet, and it echoes, at the level of cyber-physical actuation, the same transfer learning benefits that large pre-trained models have already demonstrated in other domains.

Realizing this benefit safely, however, requires the same bounded-autonomy and verification mechanisms described in Sections IV and VI to be applied with particular care, since a policy transferred from a foundation model has by definition not been validated against the specific mechanical tolerances of the newly commissioned asset.

O. D. Standardization and Regulatory Alignment

A further open challenge, less technical than institutional, concerns the absence of established standards and regulatory frameworks for certifying autonomous physical actuation in industrial settings. Existing safety certification regimes were largely developed around systems in which a human remains the final decision-maker before any physical action is taken, and adapting these regimes to systems in which the decision and the action are both delegated to software is likely to require new testing methodologies, new liability frameworks, and new categories of certification specifically tailored to bounded-autonomy cyber-physical systems such as the IADT.

VIII. CONCLUSION

The evolution toward the Intelligent Acting Digital Twin marks a paradigm shift in cyber-physical systems [6, 7]. By moving beyond the passive monitoring capabilities of previous existing technologies, the IADT introduces closed-loop, autonomous actuation driven by real-time artificial intelligence [14]. As detailed through the architectural framework and AI integration strategies, empowering digital twins to take direct physical action solves critical latency and optimization bottlenecks in complex industrial environments [2]. The future scope of this technology extends far beyond isolated assets; the next generation of IADTs will feature multi-twin orchestration, where thousands of acting twins communicate, negotiate, and optimize entire smart cities, power grids, and global supply chains autonomously [8, 15]. Realizing this future requires continued advancement in deterministic networking, edge-native AI, and rigorous cyber-physical security protocols to ensure that as our virtual systems gain the power to act, they do so with absolute safety and precision [5, 11].

Taken together, the architectural, algorithmic, and security foundations surveyed in this paper indicate that the transition from passive monitoring to autonomous actuation is best understood not as a single technological leap but as the disciplined integration of several mature fields control theory, reinforcement learning, deterministic networking, and cybersecurity into one coherent, safety-

bounded system. It is this integration, rather than any single component in isolation, that will determine how quickly the Intelligent Acting Digital Twin can be responsibly deployed across increasingly critical cyber-physical infrastructure.

The case study presented in Section V demonstrates that the value of this integration is not merely theoretical: even in a single, well-scoped manufacturing scenario, the ability to sense, reason, and act within a single closed loop yields a measurable improvement over the alert-and-wait pattern of conventional digital twins. As the underlying enabling technologies deterministic wireless networking, edge accelerators capable of running deep models locally, and hardware security modules suitable for deployment on industrial equipment continue to mature and fall in cost, the barrier to deploying IADT-style architectures across a wider range of industrial and infrastructural settings is expected to fall correspondingly.

Ultimately, the central argument of this paper is that the passive digital twin and the Intelligent Acting Digital Twin should not be viewed as competing technologies, but as successive stages in the same underlying project of building an ever more faithful, and ever more capable, virtual counterpart to the physical world. Where the passive twin answers the question of what is happening to an asset, the IADT extends that answer into a decision and, ultimately, into a verified physical response closing, for the first time, the full loop between sensing, reasoning, and acting in the cyber-physical domain.

IX. REFERENCES

- [1][1] Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N., & Devine, D. (2021). Digital Twin: Origin to Future. *Applied System Innovation*, 4(2), 36.
- [2][2] Tao, F., Qi, Q., Wang, L., & Nee, A. Y. C. (2019). Digital Twins and Cyber-Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. *Engineering*, 5(4), 653-661.
- [3][3] Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29, 36-52.
- [4][4] Semeraro, C., Lezoche, M., Panetto, H., & Dassisti, M. (2021). Digital twin paradigm: A systematic literature review. *Computers in Industry*, 130, 103469.
- [5][5] Leng, J., Wang, D., Shen, W., Li, X., Liu, Q., & Chen, X. (2021). Digital twins-based smart manufacturing system design in Industry 4.0: A review. *Journal of Manufacturing Systems*, 60, 119-137.
- [6][6] Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. *IEEE Access*, 8, 108952-108971.
- [7][7] Rasheed, A., San, O., & Kvamsdal, T. (2020). Digital Twin: Values, Challenges and Enablers from a Modeling Perspective. *IEEE Access*, 8, 21980-22012.
- [8][8] Qi, Q., Tao, F., Hu, T., Anwer, N., Liu, A., Wei, Y., ... & Nee, A. Y. C. (2021). Enabling technologies and tools for digital twin. *Journal of Manufacturing Systems*, 58, 3-21.
- [9][9] Minerva, R., Lee, G. M., & Crespi, N. (2020). Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models. *Proceedings of the IEEE*, 108(10), 1785-1824.
- [10][10] Barricelli, B. R., Casiraghi, E., & Fogli, D. (2019). A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications. *IEEE Access*, 7, 167653-167671.
- [11][11] Boje, C., Guerriero, A., Kubicki, S., & Rezgui, Y. (2020). Towards a semantic Construction Digital Twin: Directions for future research. *Automation in Construction*, 114, 103179.
- [12][12] Shao, G., & Helu, M. (2020). Framework for a digital twin in manufacturing: Scope and requirements. *Manufacturing Letters*, 24, 105-107.
- [13][13] Zheng, Y., Yang, S., & Cheng, H. (2019). An application framework of digital twin and its case study. *Journal of Ambient Intelligence and Humanized Computing*, 10(3), 1141-1153.
- [14][14] Lu, Y., Liu, C., Kevin, I., Wang, K., Huang, H., & Xu, X. (2020). Digital Twin-

driven smart manufacturing: Connotation, reference model, applications and research issues. *Robotics and Computer-Integrated Manufacturing*, 61, 101837.

- [15][15] Liu, M., Fang, S., Dong, H., & Xu, C. (2021). Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems*, 58, 346-361.