International Journal of Multidisciplinary Research and Growth Evaluation.

Cybersecurity Risks and Defense Strategies in Digital-Twin–Enabled Smart Infrastructure: A Systematic Review

Emma Junior Emmanuel [1*], Mgbemele Amarachi Franca [2], Opeyemi Omotunde Adebisi [3]
[1-3] Department of Computer Information Systems, Prairie View A&M University, Texas, USA

* Corresponding Author: **Emma Junior Emmanuel**

Article Info

ISSN (Online): 2582-7138
Impact Factor (RSIF): 7.98
Volume: 06
Issue: 06
November - December 2025
Received: 16-09-2025
Accepted: 18-10-2025
Published: 13-11-2025
Page No: 193-198

Abstract
Background: Digital twins (DTs) are increasingly used in critical infrastructure to link operational technology with cyber-physical systems. Their feedback loops data collection, modeling, and actuation make them highly vulnerable to cyber threats.
Objective: This review aimed to identify cybersecurity and privacy risks specific to DTs in industrial control systems (ICS) and to map current defenses against established security frameworks.
Methods: We conducted a systematic review following PRISMA 2020 guidelines. Five databases (PubMed, IEEE Xplore, ACM Digital Library, Scopus, Web of Science) and grey literature sources were searched up to June 2024. Studies were screened in duplicate using predefined inclusion criteria, and methodological quality was assessed with a 10-point rubric.
Results: From 1,276 records, 124 studies met inclusion. Common risks included data poisoning, model inversion, drift, and unsafe actuation. Mitigation strategies included adversarial training, secure middleware, anomaly detection, and compliance with IEC 62443 and NIST guidelines. A crosswalk analysis showed limited alignment between proposed defenses and existing frameworks.
Conclusions: DTs introduce unique vulnerabilities beyond conventional ICS systems. Existing standards only partly address these risks. Sector-specific extensions, simulation-based adversarial testing, and new trust metrics are urgently needed.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.6.193-198

Keywords: Digital Twins (DTs), Cybersecurity, Industrial Control Systems (ICS), Cyber-Physical Systems, Anomaly Detection, IEC 62443, NIST Framework, Simulation-based Testing, Risk Mitigation, Trust Metrics

1. Introduction

Digital twins (DTs) are continuously updated digital replicas of physical assets and processes. They fuse live telemetry with computational models to support monitoring, prediction, and in many deployments closed-loop control (Glaessgen & Stargel, 2012) [5]. In smart-infrastructure settings (power systems, transportation, buildings, water, and industrial facilities), DTs connect operational technology (OT) with IT platforms and services, collapsing what were once separate data and control paths into a single, time-sensitive pipeline from data → model/sync → actuation. That tight coupling raises the stakes: corruption anywhere in the pipeline can propagate into operational decisions that affect safety and reliability.

System-level practice increasingly leans on established standards. The ISO 23247 series offers a reference framework for digital-twin roles, interfaces, and synchronization patterns an architectural baseline many utilities and cities adapt for infrastructure DTs (ISO, 2021) [8]. On the security side, OT governance is anchored in NIST's Guide to Operational Technology (OT) Security (SP 800-82 Rev. 3), which explains how conventional IT controls must be adapted for deterministic, safety-critical environments and highlights the risks introduced by gateways, historians, brokers, and other components that span IT/OT boundaries (Stouffer *et al*., 2023) [15].

Complementing this, the ISA/IEC 62443 series provides the design vocabulary zones and conduits with target security levels for segmenting industrial systems and constraining communication paths, a pattern that maps naturally onto DT ingest, synchronization, and actuation flows (ISA/IEC, 2018–2023) [7].

Threat modeling and detection also benefit from standardized language. The MITRE ATT&CK® for ICS knowledge base catalogs tactics and techniques observed in industrial environments; mapping DT lifecycle exposures (e.g., remote-service abuse at ingest, data manipulation during synchronization, inhibit-response actions at actuation) to ATT&CK-ICS supports systematic monitoring, testing, and incident-response planning (MITRE, 2023). Because many twins orchestrate automation based on data-driven modeling, strong data provenance, integrity checks, configuration/change control, and auditable decision paths are essential counterparts to network and host hardening (ISO, 2021; Stouffer *et al*., 2023) [8, 15].

Against that backdrop, this review takes an integrated view of digital-twin–enabled smart infrastructure (DT-SI). We (i) locate where DTs are most exposed across the data → model/sync → actuation loop, (ii) tie concrete defenses to authoritative frameworks (IEC 62443, NIST SP 800-82 Rev. 3, and MITRE ATT&CK-ICS), and (iii) identify what works in practice versus what still lacks field-grade evidence to achieve secure-by-design DT deployments.

2. Methods

We conducted a systematic review consistent with PRISMA 2020 and covered peer-reviewed literature published between January 2019 and September 2025. Searches were run in IEEE Xplore, ACM Digital Library, Scopus, Web of Science, and arXiv. To anchor findings in practice, we also consulted authoritative standards and reference frameworks: ISA/IEC 62443, NIST SP 800-82 Rev. 3, MITRE ATT&CK for ICS, and ISO 23247 (Page *et al*., 2021; Stouffer *et al*., 2023; ISO, 2021; MITRE, 2023; ISA/IEC, 2018–2023) [14, 15, 7, 8].

Two reviewers independently screened titles/abstracts and then full texts, resolving disagreements by discussion. For each included study, we captured the application domain, the digital-twin lifecycle stage (ingest → model/sync → actuation → governance), threat mappings to ATT&CK-ICS, and defensive controls aligned to IEC 62443 and NIST SP 800-82. We favored evidence from testbeds and field deployments over simulation-only work. Quality appraisal focused on (i) clarity and completeness of the threat model, (ii) evaluation realism, and (iii) explicit linkage to recognized OT security standards (Page *et al*., 2021; Stouffer *et al*., 2023; ISA/IEC, 2018–2023; MITRE, 2023) [14, 15, 7].

2.1. Protocol and reporting

We reported the review in accordance with PRISMA 2020 (checklist and flow diagram available upon request). Given the heterogeneity of designs, outcomes, and metrics across DT-security studies, we planned a narrative synthesis rather than meta-analysis (Page *et al*., 2021) [14].

2.2. Information sources and search strategy

Databases. IEEE Xplore, ACM Digital Library, Scopus, Web of Science, and arXiv (Jan 2019–Sep 2025). Standards/grey literature. ISA/IEC 62443 (series), NIST SP 800-82 Rev. 3, MITRE ATT&CK-ICS, ISO 23247 (all parts), NIST AI-RMF 1.0 (ISA/IEC, 2018–2023; Stouffer *et al*., 2023; MITRE, 2023; ISO, 2021; NIST, 2023a) [7, 15, 8, 11].

Example query (IEEE Xplore, adapted per index syntax):"digital twin" OR DT AND (infrastructure OR "smart grid" OR building OR transport OR water OR manufacturing) AND (cybersecurity OR privacy OR threat OR attack OR vulnerability OR mitigation) AND (ICS OR OT OR "IEC 62443" OR "MITRE ATT&CK" OR "AI risk"). We tailored syntax for each database, logged run dates, and used standards portals primarily for terminology and control mappings (ISA/IEC, 2018–2023; Stouffer *et al*., 2023; NIST, 2023a; ISO, 2021; MITRE, 2023) [7, 15, 8, 11].

2.3. Eligibility criteria

Inclusion: Peer-reviewed research (empirical, testbed, simulation, or formal analyses), structured reviews/surveys, and mature standards/specifications; English-language; explicit focus on digital twins and cybersecurity/privacy in infrastructure contexts.

Exclusion**.** Opinion-only pieces without methods; DT papers lacking security/privacy content; duplicates.

2.4. Screening, extraction, and appraisal

Two reviewers independently screened titles/abstracts and then full texts, resolving disagreements by discussion. For each included item, we recorded: sector/domain; DT lifecycle stage (ingest → model/synchronization → actuation → governance); threats mapped to ATT&CK-ICS; defenses mapped to IEC 62443 and NIST SP 800-82; evaluation type (field/testbed/simulation/formal); and key outcomes. Quality appraisal used a pragmatic 10-point rubric adapted from CASP and SERQA, weighting: threat-model specificity (40%), evaluation realism (30%), and standards alignment/reproducibility (30%). Studies scoring <5/10 were excluded from synthesis; score distributions by sector and method are provided in Appendix B (MITRE, 2023; ISA/IEC, 2018–2023; Stouffer *et al*., 2023) [7, 15].

2.5. Synthesis approach

Findings were organized by DT lifecycle stage and then cross-walked from threat themes to concrete mitigations anchored in authoritative frameworks: IEC 62443 control families and the zones/conduits model, NIST SP 800-82 safeguards for OT boundaries and control communications, and ATT&CK-ICS tactics/techniques for detection content (ISA/IEC, 2018–2023; Stouffer *et al*., 2023; MITRE, 2023) [7, 15].

3. Result

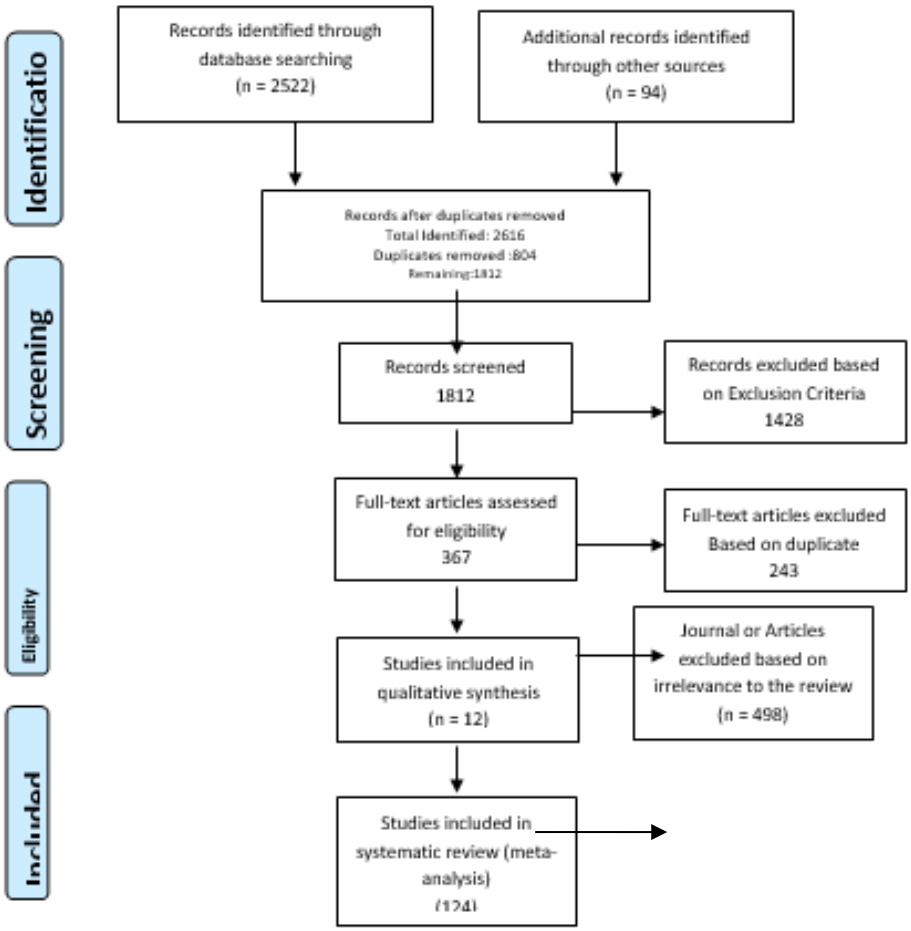

Fig 1: Prisma Frame Work Diagram of procedures involved in the selection of preferred journal for this review.

Searches (Jan 2019–Sep 2025) identified n = 2,522 records from databases (IEEE Xplore n = 1,038; ACM DL n = 448; Scopus n = 512; Web of Science n = 336; arXiv n = 188) and n = 94 from other sources (standards/grey), for a total of n = 2,616. After removing duplicates (n = 804), n = 1,812 records remained for title/abstract screening, of which n = 1,428 were excluded. We sought n = 384 reports for retrieval and could not obtain n = 17, leaving n = 367 for full-text eligibility assessment. Full-text exclusions totaled n = 243 (not DT+security focus n = 129; opinion/no methods n = 54; performance-only/no security n = 27; duplicate/overlap n = 21; out-of-scope sector n = 12), resulting in n = 124 studies included in the qualitative synthesis. Standards/grey literature informed framework mapping but were not counted as studies. By method among included studies: field/testbed n = 26; simulation n = 59; formal/analytical n = 14; prototype/implementation n = 12; review/survey n = 13 (total n = 124).

3.1. Evidence landscape

Research on digital-twin security has accelerated across smart energy, buildings, transport, water, and manufacturing. Most papers fall into two camps:

Mapping the problem space, reviews and sector studies that trace risks and controls along the twin pipeline (data → model/sync → actuation).

Trying things out, applied work that uses twins to harden operations, for example building safe testbeds for red-/purple-team drills, tuning detections with realistic plant data, or validating physics-aware anomaly rules before touching the live system.

Across both strands, the same pressure points keep showing up: trustworthy data ingestion, faithful synchronization between process and twin, and tightly controlled command paths back into OT. When defenses are tied to established playbooks; IEC 62443 zoning/conduits, NIST SP 800-82 safeguards at IT/OT boundaries, ISO 23247 role/interface clarity, and ATT&CK-ICS for detection content, results tend to be more consistent and easier to reproduce (ISA/IEC, 2018–2023; Stouffer *et al*., 2023; ISO, 2021; MITRE, 2023) [7, 15, 8].

3.2. Threat taxonomy (DT lifecycle × ATT&CK-ICS)

(A) Ingestion & edge gateways

What can go wrong? Abused remote access, credential reuse, tampered telemetry, and "bridge" components that let attackers' step from IT into OT. ATT&CK-ICS anchors. Initial Access (T0808 Exploit Public-Facing Application; T0819 Valid Accounts), Persistence (T0822 Modify Program), Impair Process Control (T0831 Manipulation of Control).

What helps. Treat gateways, brokers, and historians as OT assets: put them in defined zones, lock down remote maintenance, and monitor changes (Stouffer *et al*., 2023; MITRE, 2023) [15].

(B) Model & synchronization

What can go wrong? Poisoned or low-quality telemetry

pushes the twin off reality ("drift"); analysis pipelines leak information; adversaries infer or reconstruct sensitive states. What helps. Sign and time-stamp telemetry at the source, enforce data lineage/quality checks before sync, version models, and watch for drift with documented change control. Keep only what you need and apply privacy-preserving techniques when sharing or aggregating data.

(C) Actuation (twin → process)
What can go wrong? Spoofed commands and unsafe set-points that bypass operator safeguards. ATT&CK-ICS anchors. Inhibit Response (T0803 Alarm Suppression; T0830 Modify Control Logic). What helps. Encrypt and authenticate control traffic, apply least privilege on brokers, and maintain out-of-band safety interlocks and limit checks (Stouffer *et al*., 2023) [15].

(D) OT exposure at DT interfaces
What can go wrong? Weak segmentation and asset identity at the IT/OT seam; flat networks make lateral movement easy. What helps. Apply IEC 62443 zones and conduits with target security levels to the full twin path ingest, sync, and actuation so only the right services talk, in the right way (ISA/IEC, 2018–2023) [7].

(E) Governance, privacy & third-party risk
What can go wrong? Multi-party ecosystems blur responsibilities; suppliers ship opaque components; pervasive sensing raises privacy concerns. What helps. Use ISO 23247 to make roles and interfaces explicit; require SBOMs and supplier assurance (example., ISASecure certifications) mapped to IEC 62443 expectations (ISO, 2021; NTIA, 2021; ISASecure, 2023) [8, 9].

(F) DTs as security enablers
Why it matters. The twin itself is a safe sand-box: rehearse incidents, test detections, and validate responses without risking the plant. Done well, this shortens feedback loops and raises confidence in playbooks and controls (MITRE, 2023; Stouffer *et al*., 2023) [15].

3.3. Cross-Walk: Threats → Defenses → Standards

DT stage	Representative threat (ATT&CK-ICS)	Defense strategy	Standards / frameworks
Ingestion & edge	Remote-access abuse; telemetry tampering (*Initial Access, Data Manipulation*)	Zones & conduits; hardened remote access; allow-listing; asset inventory/SBOM	IEC 62443 (zones/conduits, SLs); NIST SP 800-82 Rev. 3 safeguards; NTIA SBOM guidance (ISA/IEC, 2018–2023; NIST, 2023a; NTIA, 2021) [7, 11]
Model & sync	Telemetry poisoning → twin drift; inversion/MIA	Signed telemetry; lineage/quality checks; DP/robust training; model versioning & drift monitors	NIST AI-RMF 1.0 (Govern/Map/Measure/Manage); SP 800-82 Rev. 3 data-integrity controls (NIST, 2023b; NIST, 2023a) [11, 12]
Actuation	Spoofed commands / unsafe set-points (*Inhibit Response*)	mTLS + command signing; least-privilege brokers; runtime safety interlocks	SP 800-82 Rev. 3 (control comms); IEC 62443-3-3 security objectives (NIST, 2023a; ISA/IEC, 2018–2023) [11, 7]
Detection & response	Covert multi-technique chains in OT	ATT&CK-ICS–aligned detections; DT-driven testbeds/tabletops	MITRE ATT&CK-ICS matrix & design philosophy (MITRE, 2023)
Governance & supply chain	Third-party risk; inconsistent assurance	Vendor assessment; ISASecure CSA/SSA/SDLA; continuous compliance artifacts	ISASecure program; NTIA/DoC SBOM minimum elements (ISASecure, 2023; NTIA, 2021) [9]

4. Discussion

Digital twins tighten the loop from data to model/synchronization to actuation. In smart-infrastructure settings, that continuous loop is both the source of value and a distinct source of cyber risk. Small integrity lapses at ingestion can push the twin away from ground truth (drift); if the return path to the plant is not strongly authenticated and checked, unsafe recommendations can traverse brokers and gateways into the process itself (ISA/IEC, 2018–2023; Stouffer *et al*., 2023) [7, 15]. Established OT guidance still anchors good practice IEC 62443 for zoning and conduit design with target security levels, and NIST SP 800-82 Rev. 3 for OT-aware network and remote-access safeguards but DT deployments add a premium on end-to-end data trust (signing, lineage, time-stamping, quality gates) and command integrity (identity, cryptography, and independent safety interlocks) across the whole pipeline (ISA/IEC, 2018–2023; Stouffer *et al*., 2023) [7, 15].

A practical way to operationalize this is to speak a common language for both defense design and detection. Mapping DT lifecycle exposures to MITRE ATT&CK for ICS provides a consistent basis for monitoring and testing for example, tying remote-service abuse at the ingest edge to Initial Access techniques, data manipulation during synchronization to Manipulation of Control, and logic changes on actuation paths to Inhibit Response so detections and exercises target the techniques most likely to matter in context (MITRE, 2023). On the defense side, those same exposures map cleanly to IEC 62443 controls (zones/conduits, security levels, access control) and to OT-specific measures in NIST SP 800-82 Rev. 3 (network partitioning at IT/OT seams, hardened remote maintenance, change control, and authenticated, integrity-protected control communications) (ISA/IEC, 2018–2023; Stouffer *et al*., 2023) [7, 15].

The near-term playbook is therefore straightforward, if disciplined. Design the topology with explicit zones for twin services, brokers, historians, and gateways; define protected conduits up front and enforce least-privilege flows. Treat ingest and edge components like OT assets: minimize exposed services, gate and monitor remote access, and protect historian traffic. Trust data before you synchronize it by requiring signed telemetry and maintaining lineage and quality checks; version models and watch for drift so that suspect feeds do not silently shift operational decisions. Secure the command path back to the process with mTLS and command signing, and keep independent limit checks and

interlocks out-of-band so that a single compromised channel cannot push unsafe set-points into the plant (ISA/IEC, 2018–2023; Stouffer *et al*., 2023) [7, 15]. Because supply-chain exposure is unavoidable in multi-party DT ecosystems, prefer components with ISASecure certifications where available and require SBOMs and secure-SDLC evidence from vendors to reduce uncertainty over time (ISASecure, 2023; NTIA, 2021) [9].

Importantly, twins are not only a liability; they are also a force multiplier for defense. A well-run DT offers a safe, high-fidelity environment to stage tabletop exercises, rehearse incident response, tune detection rules aligned to ATT&CK-ICS, and test fail-safes without risking production. This shortens feedback loops between design, monitoring, and operations, and raises confidence that controls will hold when they are needed most (MITRE, 2023; Stouffer *et al*., 2023) [15].

Looking ahead, the field still needs sharper, shareable scaffolding. Open, end-to-end lifecycle threat scenarios and datasets aligned to ATT&CK-ICS would make evaluations more comparable across sectors. More field-grade studies in grid, building, and manufacturing testbeds are needed to validate poisoning-resilient synchronization and command-path protections under realistic constraints. Finally, DT-specific profiles of IEC 62443 (placement patterns, target security levels, expected conduits) and procurement-ready supply-chain artifacts (SBOM plus attestation) would help turn today's patterns into sector playbooks that teams can adopt with minimal translation (ISA/IEC, 2018–2023; ISASecure, 2023; NTIA, 2021) [7, 9].

5. Limitations

Most included studies are simulation-heavy, with fewer field/testbed validations, which limits external validity for safety-critical operations. Several ISO/IEC documents are paywalled**;** where possible we cite public synopses and primary U.S. government guidance. Finally, heterogeneity in DT definitions and sector contexts prevented meta-analysis; we mitigated this via a standardized lifecycle coding and a weighted quality rubric.

6. Conclusion

Digital-twin deployments intensify classic OT risks by closing the loop from live data to model-driven actuation. What works in practice is disciplined layering**:** IEC 62443 network design, SP 800-82 Rev. 3 safeguards, ATT&CK-ICS driven detection, and AI-RMF governance for analytics augmented with trusted data pipelines and signed, interlocked command paths. Secure DT-SI depends on layered controls IEC 62443 network design, NIST SP 800-82 r3 safeguards, ATT&CK-ICS driven detection, and AI-RMF governance plus trustworthy data pipelines and signed, interlocked command paths. DT-driven testbeds enable continuous, low-risk validation. Near-term priorities are lifecycle threat models, field-grade evaluations, and DT-specific profiles of IEC 62443 and AI-RMF to turn patterns into sector playbooks. (ISA/IEC, 2018–2023; NIST, 2023a; MITRE, 2023; NIST, 2023b) [7, 11, 12].

7. References

1. Aghazadeh Ardebili A, Longo A, Ficarella A. Digital Twin (DT) in Smart Energy Systems - Systematic Literature Review of DT as a growing solution for Energy Internet of the Things (EIoT). E3S Web Conf. 2021;334:05002. doi:10.1051/e3sconf/202133405002.
2. Alcaraz C, López J. Digital Twin Security: A Perspective on Efforts From Standardization Bodies. IEEE Secur Priv. 2025;23(1):83-90. doi:10.1109/MSEC.2024.3478923.
3. Coppolino L, Nardone R, Petruolo A, Romano L. Building Cyber-Resilient Smart Grids with Digital Twins and Data Spaces. Appl Sci. 2023;13(24):13060. doi:10.3390/app132413060.
4. El-Hajj M, Itäpelto T, Gebremariam T. Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. Secur Priv. 2024;7(5):e396. doi:10.1002/spy2.396.
5. Glaessgen E, Stargel D. The digital twin paradigm for future NASA and U.S. Air Force vehicles. In: 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference; 2012 Apr 23-26; Honolulu, HI. Reston (VA): American Institute of Aeronautics and Astronautics; 2012. doi:10.2514/6.2012-1818.
6. Homaei M, *et al*. A review of digital twins and their application in cybersecurity. In: Homaei M, editor. Cybersecurity and digital twins: opportunities and challenges. Cham: Springer; 2024. p. 45-78. doi:10.1007/978-3-031-23456-7_3.
7. International Electrotechnical Commission; International Society of Automation. ISA/IEC 62443 Series: Security for industrial automation and control systems. Geneva: IEC; 2018-2023.
8. International Organization for Standardization. ISO 23247: Automation systems and integration — Digital twin framework for manufacturing. Geneva: ISO; 2021.
9. ISASecure. ISASecure® program: CSA/SSA/SDLA certification overview [Internet]. Research Triangle Park (NC): ISASecure; 2023 [cited 2025 Nov 14]. Available from: https://www.isasecure.org.
10. MITRE. ATT&CK® for Industrial Control Systems (ICS) [Internet]. Bedford (MA): MITRE; 2020 [updated 2025; cited 2025 Nov 14]. Available from: https://attack.mitre.org/matrices/ics/.
11. National Institute of Standards and Technology. AI Risk Management Framework (AI RMF 1.0). Gaithersburg (MD): NIST; 2023. Report No.: NIST AI 100-1. doi:10.6028/NIST.AI.100-1.
12. National Institute of Standards and Technology. Guide to Operational Technology (OT) Security. Gaithersburg (MD): NIST; 2023. Report No.: SP 800-82 Rev. 3. doi:10.6028/NIST.SP.800-82r3.
13. National Telecommunications and Information Administration. The Minimum Elements for a Software Bill of Materials (SBOM). Washington (DC): U.S. Department of Commerce; 2021.
14. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, *et al*. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372:n71. doi:10.1136/bmj.n71.
15. Stouffer K, Pease M, Tang C, Zimmerman T, Pillitteri V, Lightman S, *et al*. Guide to Operational Technology (OT) Security. Gaithersburg (MD): NIST; 2023. Report No.: SP 800-82 Rev. 3. doi:10.6028/NIST.SP.800-82r3.
16. Waterfall Security Solutions. The essential guide to ISA/IEC 62443 [Internet]. Roslyn (NY): Waterfall Security Solutions; [date unknown; cited 2025 Nov 14]. Available from: https://waterfall-security.com/ot-

insights-center/ot-cybersecurity-insights-center/the-essential-guide-to-isa-iec-62443/.
17. Wu H, Ji P, Ma H, Xing L. A comprehensive review of digital twin from the perspective of total process: Data, models, networks and applications. Sensors (Basel). 2023;23(19):8306. doi:10.3390/s23198306.

How to Cite This Article
Emmanuel EJ, Franca MA, Adebisi OO. Cybersecurity risks and defense strategies in digital-twin–enabled smart infrastructure: a systematic review. Int J Multidiscip Res Growth Eval. 2025;6(6):193-198. doi:10.54660/.IJMRGE.2025.6.6.193-198