

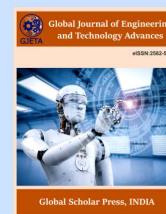


Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: <https://gjeta.com/>



(REVIEW ARTICLE)



CYBER-PHYSICAL SECURITY FRAMEWORKS FOR INTEGRATED CAD/CAM AND DIGITAL TWIN WORKFLOWS: A STATE-OF-THE-ART SYSTEMATIC REVIEW

Michael Matemavi, Bongani Anotidaishe Matimba, Pardon Mbulawa *, Tinomudaishe Mazarura and Herbert Mazodze

Department of Industrial and Manufacturing Engineering, National University of Science and Technology (NUST), P.O. Box AC 939, Ascot, Bulawayo, Zimbabwe.

* Corresponding Author

Global Journal of Engineering and Technology Advances, 2026, 29(01), 061–076

Publication history: Received on 20 August 2026; revised on 01 October 2026; accepted on 03 October 2026

Article DOI: <https://doi.org/10.30574/gjeta.2026.29.1.0268>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Integrated computer-aided design and manufacturing (CAD/CAM), product lifecycle management (PLM) and industrial control and digital-twin platforms provide a continuity from design to production, enhancing traceability, but they also enable an impersonated identity, model, toolpath, software component or sensor stream to travel through the entire workflow. The review brings together 56 peer-reviewed articles and six normative sources, most of which were from the period 2016 to September 2026. OpenAlex, publisher records (as retrieved from Crossref) and backward citation chaining were processed through a PRISMA 2020-driven workflows, and evidence was coded by workflow stage, asset, threat, security objective, control family, and validation strength. Network intrusion, theft or tampering of CAD models, manipulation of CAM parameters and post-processors, falsification of a digital-twin state, insecure cloud collaboration, supply-chain compromise, and unsafe shop-floor commands are the main threats. There are seven families of published countermeasures: standards-based governance, identity-centred access control, segmentation, verifiable provenance, blockchain-backed traceability, watermarking and fingerprinting, and twin-assisted anomaly detection. No family is big enough: source data were not necessarily correct; anomaly detection was based on representative data; and conventional IT controls under-represented operational safety and timing. Due to the influence of process parameters on part quality, such as feed rate, injection pressure or infill density, small, unauthorized changes to the process can result in parts that are defective but appear plausible. As such, a lifecycle defence-in-depth approach is proposed, featuring ownership of artefacts, trust boundaries, a signed manufacturing job package, least privilege, monitored hand-offs, process-aware detection and verified recovery. Future work should validate integrated frameworks on realistic CAD-to-machine testbeds, such as learning factories, and report the outcomes of security, production, safety and recovery in a combined manner.

Keywords: CAD/CAM; Cyber-Physical Security; Digital Twin; Digital Thread; Smart Manufacturing; Industry 4.0; Product Lifecycle Management; Defence in Depth

1 INTRODUCTION

The concept of computer aided design and manufacturing has gone from being single engineering tools to services that share product definition, process plans, toolpaths, machine data, and machine feedback on the lifecycle of the product (Hedberg et al., 2016). This connection is further enhanced by a digital twin that keeps a computational model of a physical asset or process updated and synchronises it with observations and models (Kritzinger et al., 2018; Jones et al., 2020).

There are many reported advantages of such integration, such as accelerated propagation of changes, prediction and closed-loop improvement, as well as unresolved issues regarding model fidelity, interoperability, ownership and governance (Rasheed, San and Kvamsdal, 2020; Jones et al., 2020; Sharma et al., 2022; Frechette, Shao and Pease, 2026). The same integration is now coming in fits and starts to developing industrial economies. A survey of Zimbabwean manufacturers revealed that the majority of the Industry 4.0 technologies were already in place but not well connected, that costs, policy support and skills were lack and even fear of cyber-attack was a deterrent (Muhla et al., 2025a). This is why connected engineering systems are often implemented in advance of the governance required to ensure their success.

Connectivity alters the target of cybersecurity. Mainly the information is threatened by a breach of an office network. An attacker may be able to steal a proprietary model, edit a tolerance, overwrites a post-processor, silences an alarm, poisons a learning model, or counterfeit the twin state or to shut down a machine in an integrated CAD/CAM chain. The impacts can be faulty components, hidden fatigue damage, decreased service life, unsafe motion, unplanned downtime or falsified quality record (Ani, He and Tiwari, 2017; Tuptuk and Hailes, 2018; Elhabashy et al., 2019; El-Kady et al., 2023; Rahman, Wuest and Shafae, 2023). Confidentiality, integrity and availability are the three Guidelines for manufacturing security, along with authenticity, traceability, product quality and human safety (Stouffer et al., 2023; Rahman and Shafae, 2025).

Digital-twin architecture, smart-manufacturing cyber security, industrial control, blockchain, additive manufacturing and artificial intelligence have been separately discussed in previous works (Alcaraz and Lopez, 2022; Mun et al., 2025; Alhamam, Rahman and Aljughaiman, 2025; Ahmmed et al., 2025). This renders it difficult to assess the effectiveness of a control in protecting engineering work in the engineering workflow as a whole, or in protecting one platform in it. The present review starts from CAD and follows information through collaboration, CAM, execution and twin feedback. It answers the following four research questions:

- RQ1. Which assets, trust boundaries and attack paths define the cyber-physical exposure of integrated CAD/CAM and digital-twin workflows?
- RQ2. How do established security frameworks and control families protect confidentiality, integrity, availability, authenticity, safety and resilience across the lifecycle?
- RQ3. What evidence supports these approaches, and where do their assumptions or validation methods limit industrial adoption?
- RQ4. What research and implementation priorities are needed for a coherent, testable and interoperable security framework?

The review consists of three contributions: a taxonomy of attacks surfaces, based on a stage model; a comparative synthesis of the families of frameworks; and a model of defence-in-depth for the lifecycle, based on a signed manufacturing job package. A digital twin is not a truth that is supposed to be automatically trusted; this is a lesson that is repeated in all three. It's a high-value security component whose models, interfaces, data provenance and decision rights need independent assurance (Alcaraz and Lopez, 2022).

2 BACKGROUND AND THEORETICAL FOUNDATION

2.1 From Digital Models to a Closed-Loop Workflow

When the geometry, materials, tolerances and configuration identifiers of a CAD model are utilized in the process planning and manufacture of the product, the model becomes operationally significant. Version and approvals are controlled by products lifecycle management systems, released design is translated into operations and toolpaths by computer aided process planning and CAM, toolpaths are translated into controller specific code by post-processors, and the code is executed by shop-floor systems, recording inspection and sensor data along the digital thread (Hedberg et al., 2016). The use of simulation has become more commonplace in the released definition upstream of CAM.

In applied design studies at NUST, finite-element analysis in Ansys was used to determine which of two variants (carbon-fibre or nylon) of a SolidWorks exoskeleton model would deform less, have less stress, and thus be more

structurally sound, while computational fluid dynamics was used to determine the aerodynamic design of a vertical-axis wind turbine for a highway road before it was prototyped (Tandi et al., 2025; Muyambo et al., 2025). Under these circumstances, the inputs to the simulation are equally as important as the geometry itself. Kritzinger et al. (2018), Barricelli, Casiraghi and Fogli (2019), Boyes and Watson (2022), and Segovia and Garcia-Alfaro (2022) classify three different types of Digital Twins: a digital model, a digital shadow, and a digital twin. Barricelli, Casiraghi and Fogli (2019), Boyes and Watson (2022), and Segovia and Garcia-Alfaro (2022) distinguish three different types of Digital Twins: the Digital Model, the Digital Shadow, and the Digital Twin.

The workflow is in reality a federation of software, devices, organizations, and data owners connected through exchange formats, application programming interfaces, cloud repositories, manufacturing execution systems, direct numerical control (DNC) and industrial gateways. Although terminology is harmonised in standards like ISO 23247 (ISO, 2021), there are no mappings of security (Jacoby and Usländer, 2020; Moyne et al., 2020) and implementations are not uniform in granularity. The following is a summary of the workflow, main asset in each step and an example threat.

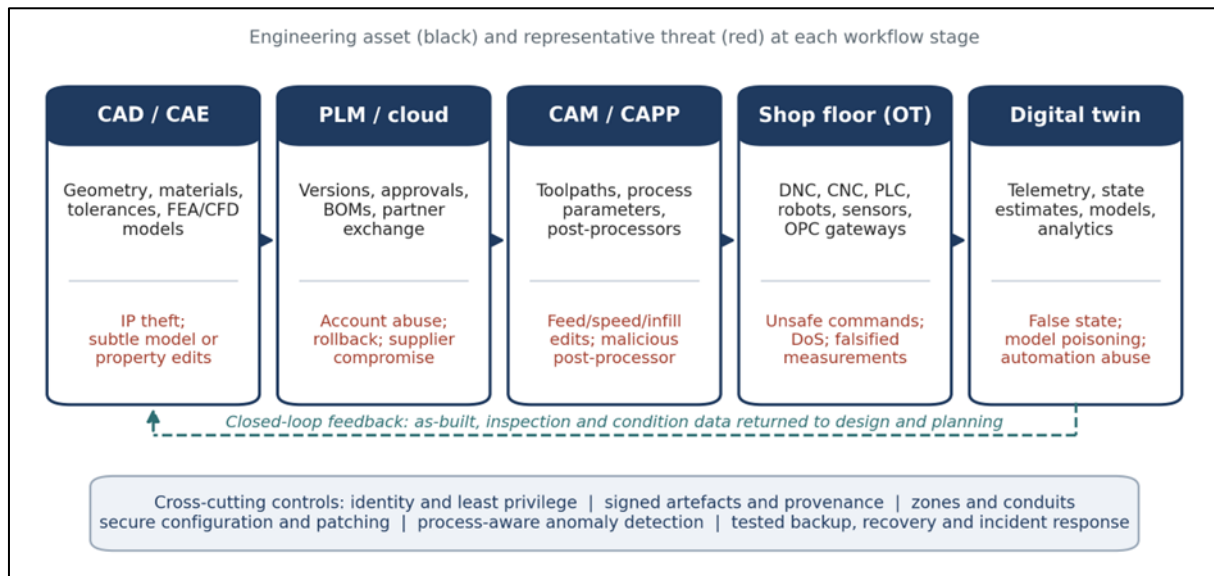


Figure 1: Connected CAD/CAM-digital-twin workflow, principal engineering assets and representative attack surfaces at each stage, with cross-cutting controls. Source: authors' synthesis, drawing on the digital-thread model of Hedberg et al. (2016), the production-system attack taxonomy of Elhabashy et al. (2019) and the cyber-physical defence-in-depth model of Rahman and Shafae (2025).

2.2 Security Objectives and Trust Assumptions

Confidentiality ensures that the company's proprietary information, customer information, and manufacturing process are confidential. Integrity assures proper and complete geometry, parameters, code and telemetry and availability assures engineering and production. Authenticity relates to artefacts and actions to known identities while non-repudiation and provenance create an evidence trail. Two additional goals are supported by these properties, namely safety, since commands are executed on real equipment and human beings; and resilience, to allow production to be brought into a known safe state and to recover without corrupted data being accepted. Process-aware security is more than just traditional IT security. It is important to note, however, that patching is not enough; the timing of operations is also key, controller stability is important, validated configurations and safe recovery are also important (Khorrami, Krishnamurthy and Karri, 2016; Stouffer et al., 2023; NIST, 2024; Rahman and Shafae, 2025).

3 REVIEW METHODOLOGY

3.1 Search Strategy

The review was conducted according to PRISMA 2020 reporting guideline, adapted to an engineering state-of-the-art review (Page et al., 2021). Searches were conducted on 19/09/2026. Discovery and DOI metadata was provided by OpenAlex and Crossref, high-relevance articles were checked using IEEE Xplore and publisher archives, and backward citation chaining was employed to determine standards and related studies. Nine Query families that included both security and workflow terms. The search window was from 1 January 2016 to 19 September 2026, when the concepts of cloud engineering, industrial Internet of Things (IIoT) and operational digital twins grew. Table 1 summarises the search protocol.

Table 1: Search protocol and eligibility criteria

Element	Specification
Databases and sources	OpenAlex; Crossref; IEEE-indexed publisher records; journal publisher pages; backward citation chaining.
Core search string	("digital twin" OR "digital thread" OR CAD OR CAM OR "smart manufacturing" OR "cyber-physical production") AND (cybersecurity OR security OR threat OR attack OR integrity OR provenance OR "access control")
Specialist strings	"additive manufacturing" AND (security OR sabotage OR fingerprint); CAD AND (watermark OR "intellectual property" OR tampering); manufacturing AND (blockchain OR "zero trust" OR "anomaly detection")
Date and language	English; 1 January 2016 to 19 September 2026. Earlier material was admitted only for essential standards or foundational concepts.
Inclusion	Peer-reviewed articles and proceedings with clear relevance to integrated engineering, manufacturing, digital twins, digital threads, cyber-physical production, control selection or empirical security evaluation.
Exclusion	Generic consumer or enterprise cybersecurity; non-technical commentary; duplicates; retracted papers; studies with no manufacturing, engineering-workflow or transferable cyber-physical contribution.
Quality dimensions	Relevance, architectural clarity, traceability of threats to controls, strength of validation, lifecycle coverage and reproducibility. Quality informed evidence weighting rather than automatic exclusion.

3.2 Selection, Quality Appraisal and Synthesis

540 records were found in the searches. Following the removal of 122 duplicate titles, 418 titles and abstracts were screened and 89 full texts or complete publication records were evaluated, resulting in 56 peer-reviewed studies (Figure 2). Citation chaining was used to add six normative sources for controls and architecture: IEC 62443-3-3, ISO 23247-1, NIST SP 800-207, NIST SP 800-161 Rev. 1, NIST SP 800-82 Rev. 3 and the NIST Cybersecurity Framework (CSF) 2.0. Three papers (5%) of the peer reviewed set are conference proceedings (in the Procedia series) and retained because they have some formal risk models which are not available elsewhere, but were down-weighted compared to the journal papers.

All studies were identified by workflow stage, asset, threat, security objective, control family and stated limitation. They reported the detection accuracy, network performance, framework coverage and robustness of the processes on incompatible scales and hence quantitative pooling was not possible, therefore only qualitative synthesis was possible. Conceptual work was accepted when it supported conceptual relationships of control and lifecycle boundaries, but testbed evidence was accorded greater weight than conceptual architecture.

The review is completed with studies in an applied context that are relevant to the development of manufacturing in a developing economy, namely in the context of process optimisation, condition monitoring, machine learning for maintenance, and design and adoption of Industry 4.0 in Zimbabwe, in the authors' department. These are sources of information that are applied in a context and used to demonstrate the behavior of engineering artefacts, process parameters and plant information in practice. To prevent self-selection bias, they were not retrieved by the search strings, were not counted as part of the 56 studies included, and do not add to the evidence weighting.

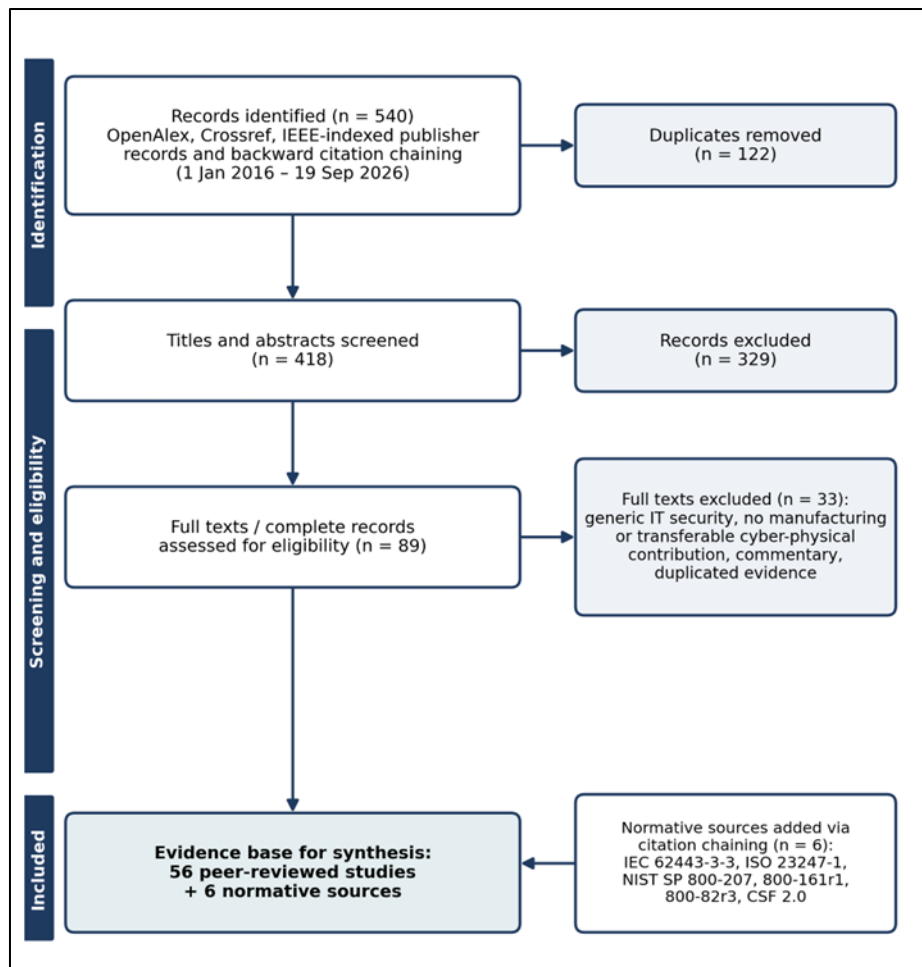


Figure 2: PRISMA 2020 flow diagram of study identification, screening and inclusion. Source: authors; layout adapted from the PRISMA 2020 flow-diagram template (Page et al., 2021).

4 ATTACK SURFACE AND THREAT TAXONOMY

4.1 CAD, CAE and Product Data

The first high-value assets are the CAD, neutral exchange models, the simulation parameters, the bill of materials and the design rationale. Confidentiality is commercial advantage, integrity is the product. Reusable libraries and automated conversion, and external suppliers and cloud sharing, expand the surface of the identity and software-supply-chain (Boyens et al., 2022; Rahman and Shafae, 2025). A valid login does not mean that an uploaded model is valid, and a checksum after the hack just means that the malicious version is saved. The same protection as geometry must be given to simulation artefacts. If a change in an exoskeleton material card changes the value of, say, a factor of safety from 2.1 (carbon fibre) to 1.38 (nylon) at the same loading point, then a change in the material card will enable an unsafe design, even though no change has been made to the CAD geometry. Thus, controlled authoring identities, protected source repositories, signed baselines, separation of design and review, and immutable evidence of approval are all requirements for security. Research on hardware and design security also reveals that it is critical to place trust in reusable intellectual property blocks (IPB), toolchains, and execution environments (Hu et al., 2021; Akter, Khalil and Bayoumi, 2023).

4.2 PLM, Cloud Collaboration and the Digital Thread

Authoritative Versions and Partner Interfaces are stored on Lifecycle and Cloud platforms. There may be many reasons why the thread may be compromised, such as excessive privilege, stolen credentials, unlogged exports and version rollbacks, and third party services add to dependency (Boyens et al., 2022). Recommended controls are asset inventories, supply-chain assurance, software and model bills of materials, provenance, incident reporting and tested recovery (Yousefnezhad, Malhi and Främling, 2020; Hammi, Zeadally and Nebhen, 2023; Stouffer et al., 2023). The same applies to process recipes in continuous industries – e.g., to bring the colour and free fatty acids in the edible oil within specification, while keeping the consumption of bleaching-earth limited, a vacuum-bleaching window is a designed

experiment (Jansen et al., 2025) and its unauthorized modification would result in product deterioration, just as an edited drawing would.

4.3 CAM, Post-Processing and Machine Execution

Critical trust boundary is CAM: it converts design intent to action. The use of different tools, feeds, speeds, offsets, datum definitions or post processor logic can change the part geometry without affecting the CAD geometry, resulting in dimensional or microstructural defects that are not caught by a visual inspection of the part (Yampolskiy et al., 2018; Elhabashy et al., 2019). Process-optimisation evidence demonstrates the margin's tightness. Feed rate (82.81%) and spindle speed (63.40%) were the dominant sources of variation of the surface roughness and flank wear respectively, in Taguchi-based CNC milling of mild steel; likewise, injection pressure (67.25%) and melt temperature (28.72%) were the major contributors of variation for shrinkage and warpage in injection moulding respectively (Mapindu et al., 2026). Similar parameter sensitivity has been reported for surface quality and energy consumption in the machining of teak, saligna and pine (Tayisepe et al., 2023) and honing of cast-iron cylinder relining sleeves (Tayisepe et al., 2024). The consequence of this is that the optimised parameter set itself is a security-sensitive artefact and an unauthorised change of the dominant part of the NC program or machine setup alone is enough to move parts out of specification.

Downstream DNC, CNC and PLC systems, and legacy protocols (Stouffer et al., 2023) provide long equipment lifecycles, strict availability requirements, and legacy protocols. To ensure safety-critical parameters are verified independently against an approved parameter envelope before running the job, controls must bind the generated code, machine configuration, post-processor version, process plan and released model into a signed job package (Tuptuk and Hailes, 2018; Mullet, Sonidi and Ramat, 2021; Rahman, Wuest and Shafae, 2023).

4.4 Digital-Twin Data, Models and Analytics

The twin add hazards in both directions. The poor recommendations can be caused by a stale or poisoned model, the compromised simulation parameters can normalise harmful behavior, the over-privileged twin can lead to a backdoor into control systems and falsified sensor data can lead to false virtual state (Alcaraz and Lopez, 2022). Data-Driven Maintenance Models describe the exposure. To determine preventive maintenance intervals and reliability targets for a coal fired power plant, a model constructed using 13 years of monthly boiler operation data was used (Senda et al., 2026). If the historical data were corrupted, or even the data flowing into the model, the model would then be used to guide maintenance decisions, which could change without any observable fault. On the other hand, a well-separated twin can be used for threat modeling, for comparing actual and expected behavior, and for rehearsing responses (Suhail et al., 2023; Alcaraz and Lopez, 2024; Erceylan, Akbarzadeh and Gkioulos, 2025). All of these are agreed upon as prerequisites: authenticity, model integrity, interface security, privacy, explainability and synchronisation (de Azambuja et al., 2024; Alhamam, Rahman and Aljughaiman, 2025; Erceylan, Akbarzadeh and Gkioulos, 2025; Mun et al., 2025). Table 2 summarizes the taxonomy.

Table 2: Lifecycle threat taxonomy and priority controls

Workflow stage	Assets and representative threats	Priority controls	Representative evidence
CAD and CAE	Geometry, tolerances, materials and simulation models; theft, unauthorised reuse, subtle model or material-property edits, malicious libraries.	MFA; role- and attribute-based access; signed baselines; separation of design and review; watermarking or fingerprinting.	Elhabashy et al. (2019); Rahman and Shafae (2025)
PLM and cloud	Version history, approvals, bills of materials, process recipes and partner exchanges; account abuse, leakage, rollback, dependency compromise.	Least privilege; zero trust; provenance; supplier assurance; model and software bills of materials; tested backup.	Rose et al. (2020); Boyens et al. (2022)
CAM and CAPP	Toolpaths, process parameters and post-processors; parameter manipulation, malicious translation, unauthorised regeneration.	Signed job package; two-person release; parameter-envelope rules; NC-code diffing; trusted post-processors.	Elhabashy et al. (2019); Rahman and Shafae (2025)
Machine and OT	DNC, CNC, PLC, robots, sensors and OPC gateways; unsafe commands, denial of service, firmware compromise, falsified measurements.	Zones and conduits; allow-listing; secure remote access; process-aware monitoring; safe-state and recovery procedures.	IEC (2013); Stouffer et al. (2023)

Digital twin	Models, state estimates, APIs and analytics; model poisoning, false synchronisation, privacy loss, automation abuse.	Mutual authentication; data provenance; uncertainty bounds; explainable detection; independent safety interlocks.	Alcaraz and Lopez (2022, 2024); Alcaraz, Meskini and Lopez (2025)
--------------	--	---	---

5 CRITICAL SYNTHESIS OF SECURITY FRAMEWORKS

5.1 Governance Standards and Defence in Depth

Guidance for manufacturing usually involves enterprise risk management along with operational-technology controls. NIST CSF 2.0 categorizes activities into the following six functions: Govern, Identify, Protect, Detect, Respond and Recover (NIST, 2024). The zones, conduits and security levels described in IEC 62443 (2013) have been mapped to production objectives in the NIST manufacturing profile (Stouffer et al., 2020), and reference structures for manufacturing twins are described in ISO 23247 (2021), which covers operational constraints (Stouffer et al., 2023). These frameworks have been backed by the literature but with limited connections to engineering artefacts. The primary things that are not included in asset registers are post-processors, simulation models, training data, CAD libraries and machine parameters.

An effective framework has to therefore view the engineering artefacts themselves as assets and assign an owner, approved state, trust boundary, retention rule and recovery source to each artefact (Moustafa et al., 2018; Jacoby and Usländer, 2020; Mullet, Sondi and Ramat, 2021; NIST, 2024). Defence in depth is most effective when each layer has some degree of self-reliance and independence. These can be used to control identity (who is allowed to act), segmentation (how far can a breach go), signatures and provenance (how to identify unauthorised changes), process rules and monitoring (how to detect deviations), and recovery (how to restore a known-good engineering and machine state) (Zarreh et al., 2018; Rahman and Shafae, 2025).

In this context, game-theoretic analyses reveal the importance of explicitly modelling the behaviour of the attacker and defender (Zarreh et al., 2018, 2019). The main challenge is organisational: controls are spread across engineering, IT, operations, quality management and suppliers and are difficult to sustain when responsibilities are split between stakeholders. Security design should also maintain the responsiveness the manufacturers rely on. Agility – the ability to rapidly restructure when markets change due to economic and pandemic induced disruption – has been identified as a survival strategy for Zimbabwean manufacturers under disruption (Muhla et al, 2023) – release and verification controls that unnecessarily delay engineering changes should be proportionate to consequence.

5.2 Identity, Trust and Secure Collaboration

The value of zero trust is that connections with partners and cloud resources can't be trusted just because they're terminated within a company network. NIST SP 800-207 calls for (explicit) verification, least privilege and continuous evaluation (Rose et al., 2020). For CAD/CAM, the artefact, the project, the state of the project's life cycle, the target machine, and the desired action should be authorized. A designer can change the model but not approve it for release; a service can create a tool path, but cannot change the post processor; and a twin analytic service can suggest a correction but should not be able to override the safety interlock. Alcaraz, Meskini and Lopez (2025) raise the challenge to sharing controlled data between digital-twin communities. Their hybrid access-control approach covers the issue of confidentiality between organisations but the establishment of secure collaboration still requires reliable identity governance and revocation.

5.3 Provenance, Blockchain and Artefact Integrity

Proposals on the blockchain keep a record of the transactions, hashes and the changes of ownership in a ledger which is hard to modify, and are most useful where multiple organisations do not have a single trusted administrator (Yaga et al., 2018; Hasan et al., 2020). The development and updating of twins have been correlated to blockchain-based records, while smart contracts have been integrated with explainable AI in very automated security systems (Fernández-Caramés and Fraga-Lamas, 2019; Hasan et al., 2020; Kumar et al., 2024). The main drawback is the oracle problem: an immutable ledger does not guarantee that the value recorded in it was accurate at the time of entry, nor does it ensure that the CAD model, sensor measurement or identity was correct at the time of entry (Yaga et al., 2018).

These are all further hampered by the use of Ledger latency, confidentiality, key recovery and governance. Blockchain should thus be seen as a provenance layer, rather than a replacement for validation, access control or process-aware monitoring. Supporting evidence is watermarks, acoustic signatures and part fingerprints. An audio side channel has been used for the integrity verification of 3D printed parts (Belikovetsky et al., 2019) and a review of tagging approaches for additively manufactured parts is presented by Sola et al. (2022).

The methods have a value in detecting counterfeits and in chain-of-custody checks but their reliability is dependent on material, process, geometry and measurement conditions. Additive manufacturing exposes the whole chain of events from design theft to parameter sabotage to compromised firmware to hidden defects in parts, they are all interconnected threats (Yampolskiy et al., 2018; Graves et al., 2019; Gupta et al., 2020; Ahmmed et al., 2025). Data for process optimisation are the point made. The infill density accounted for 68.99% of the variation in tensile strength for fused deposition modelling of PLA (Mapindu et al., 2026c), meaning that a change in the infill density in the slicer profile could have a significant effect on the strength of a part that does not affect the external geometry of the part, and hence visual inspection.

5.4 Twin-Assisted Detection and Response

A security twin can signify the relationships between commands, states and outputs, and can flag deviations even if network traffic is seemingly legitimate. Various publications are associated with the concepts of twins and resilience, critical-infrastructure modelling, security analytics and cyber-physical production (Becue et al., 2020). Nevertheless, ENIGMA gives a special consideration to explainability (Suhail et al., 2023) and Alcaraz and Lopez (2024) tested twin-assisted anomaly detection in the presence of malicious perturbations on a real industrial control testbed. Another alternative, which is lighter, is agent-based architectures. In a hardware-in-the-loop testbed (Mashava et al., 2026), refractory overheating, cooling-water degradation and power deviations on an induction furnace were detected through the use of a multi-agent system based on a FIPA-compliant framework, which is integrated with infrared, flow, conductivity and level sensors, as well as a Siemens S7-1200 PLC and an OPC server.

The same architecture also represents the attack surface these systems introduce as OPC servers, rule bases, databases, and even automated e-mail alerting are all places where data can be spoofed or suppressed so it too must be authenticated and qualified for integrity checks as the controllers it reports back to. Limitations are significant. Operating a detector with a narrow operating range can trigger false alarms when the changeover or slow sabotage occurs.

The dataset presented by Ferrag et al. (2022) is realistic for IIoT; however, there is little public data that includes proprietary CAD/CAM transformations, controller timing and quality outcomes. Explainability helps analysts to assess alerts, but it cannot correct biased data or an insecure deployment. Therefore, twin assisted detection should be kept apart from the final safety authority and considered along with its cyber and manufacturing implications.

5.5 Interoperability and Human Factors

Table 3: Comparative assessment of the major framework families

Framework family	Primary contribution	Main limitation	Best role in an integrated workflow
Standards and governance	Common risk terminology, controls, zones, responsibilities and audit requirements.	May overlook engineering-specific artefacts and model trust.	Establishes ownership, baseline controls and assurance.
Zero trust and access control	Explicit verification, least privilege, contextual access and partner isolation.	Authorised access does not guarantee a safe engineering change.	Governs access to, and modification, approval, transfer and execution of, artefacts.
Provenance and blockchain	Version tracking, approvals and tamper-evident histories.	Does not verify the truth of source data; key, privacy and recovery governance required.	Supports signed job packages and inter-organisational provenance.
Watermarking and fingerprinting	Ownership verification, counterfeit detection and traceability.	Manufacturing variation can reduce identifier reliability.	Protects high-value designs and supports forensic verification.
Twin-assisted anomaly detection	Detects deviations between expected and observed process behaviour.	Vulnerable to model drift, limited data, manipulation and false positives.	Provides independent monitoring and diagnosis.
Process-aware resilience	Links cyber events to quality, safety, continuity and recovery.	Requires multidisciplinary models and realistic validation data.	Connects cybersecurity with production and safety outcomes.

There are numerous standards recorded in digital twins and cyber-physical systems reviews as well as numerous domain-specific architectures (Jones et al., 2020; Frechette, Shao and Pease, 2026). Typically, security metadata do not accompany the engineering object: the geometry of a neutral CAD file may be retained, while the approval context is lost; the toolpath from a CAD file may be separated from the post-processor version; sensor stream can be separated from uncertainty and calibration. AR and twin interfaces also increase risk as visual 'overlays' can influence the activities of the operator even if the controller is not breached. Human factors are also very critical.

Ergonomic design and training of the operators emerged as a significant factor affecting the incidence of accidents in Zimbabwean manufacturing, and it was suggested that the strengthening of a safety culture be considered a national mitigation (Muhla et al., 2025b). Because cyber-induced abnormal states act on the same people and interfaces, security alerts should be as ergonomically considered as a safety alarm: alerts that are "noisy" (too many or too infrequent), or trigger without context encourage workarounds.

There are also some local and independent protective functions that need to be taken into account. Examples of safety features that should continue to function even if the higher order digital commands are disrupted include a powered wheelchair with an automatic obstacle detection layer that automatically halts the wheelchair within 50 cm regardless of voice or joystick commands (Munotyaani et al., 2026), and a mechanically adjustable passive exoskeleton that does not rely on networked control (Tandi et al., 2025). Therefore, frameworks should have functional exception and recovery processes, not an ever-expanding list of controls. The families of tables 3 are compared.

6 PROPOSED LIFECYCLE SECURITY FRAMEWORK

The evidence suggests that there are six layers in the lifecycle (Figure 3): connect with art owners and suppliers, create identities, certificates, keys, and known-good baselines; protect artefacts by adhering to the principle of least privilege, signatures, and known-good behaviours and artefacts with separated approval; contain execution in zones and conduits, allow-listing, and independent safety functions; verify behaviour with parameter-envelope rules and process-aware detection; recover artefacts offline and with baseline, drill-down recovery, quarantine of suspect parts, and learn from incidents (IEC, 2013; Stouffer et al., 2023; NIST, 2024; Rahman and Shafae, 2025).

The job package for manufacturing should be a part of the assurance, and should be linked to approved CAD revision, material and tolerances, process plan, CAM project, post-processor version, code hash, machine identity, parameter envelope and inspection plan (Hedberg et al., 2016; Rahman and Shafae, 2025). The parameter envelope should be based on the same designed experiments used to optimize the process; then the factors found to have the greatest impact on the quality, such as feed rate in milling (Mapindu et al., 2026a), injection pressure in moulding (Mapindu et al., 2026b), infill density in extrusion printing (Mapindu et al., 2026c) and current and arc voltage in welding (Mapindu et al., 2026d), should be given the narrowest envelope and the most rigorous verification.

The package is checked before departure and after delivery with production telemetry and inspection. The recommendations, process control and safety authority should be different. While analytics can identify an anomaly, validated control limits the commands, and an independent safety system enforces hazardous limits (Stouffer et al., 2023). This separation enables the framework to capture the benefits of the digital twin but not become a single point of failure.

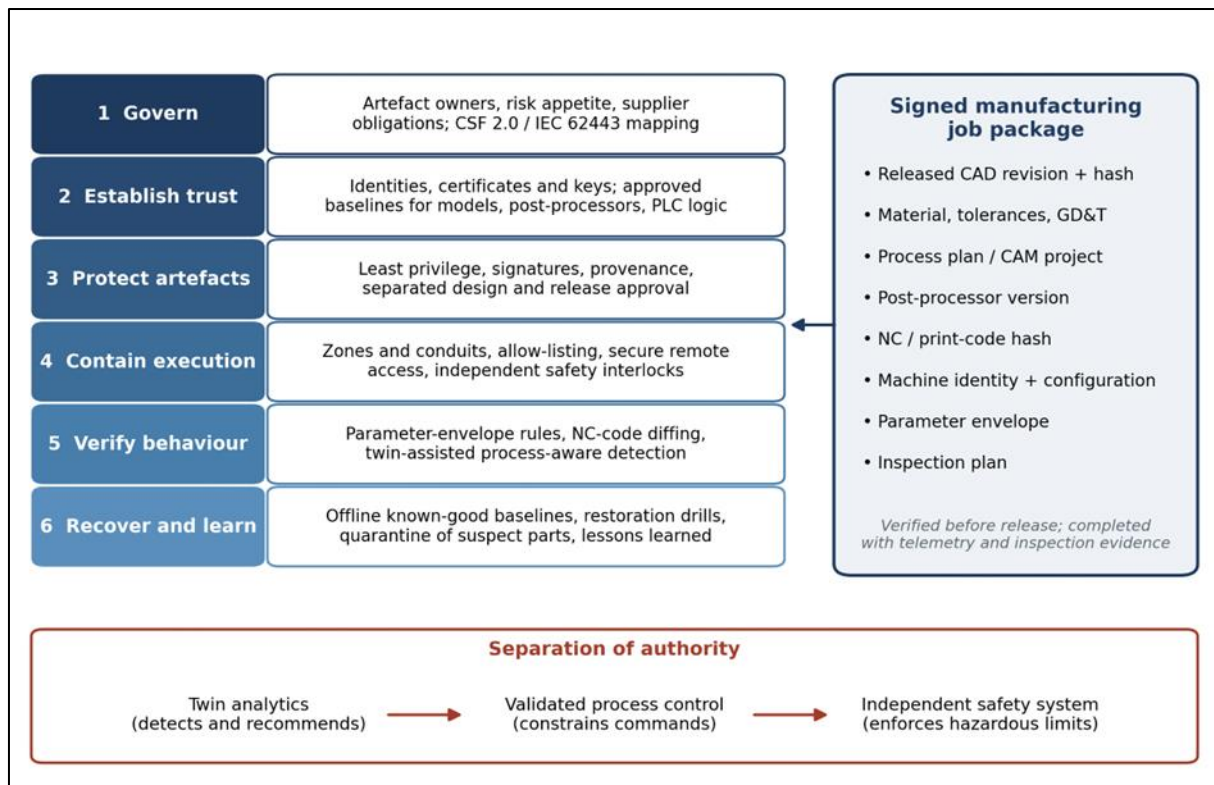


Figure 3: Proposed lifecycle defence-in-depth framework for integrated CAD/CAM and digital-twin workflows, showing the six control layers, the signed manufacturing job package and the separation of analytic, control and safety authority. Source: authors, synthesised from IEC (2013), Stouffer et al. (2023), NIST (2024) and Rahman and Shafae (2025).

7 RESEARCH GAPS AND FUTURE DIRECTIONS

7.1 End-to-End Validation

CAD/CAM, computer-integrated manufacturing, industrial Internet of Things, cloud platforms and digital twins have led to very connected cyber-physical manufacturing environments, but most cybersecurity research has focused on individual technologies and not the entire workflow. The threats to digital twins, manufacturing data and operational technology have been identified in the existing studies, but a comprehensive framework that spans the entire CAD-to-CAM-to-production lifecycle is still underdeveloped (Alcaraz and Lopez, 2022; Rahman and Shafae, 2025). Additionally, interoperability, verification and validation and uncertainty quantification, and cybersecurity are listed as ongoing challenges for digital twins in manufacturing by NIST (Frechette, Shao and Pease, 2026).

The first one is the lack of end-to-end security models. CAD files, manufacturing instructions, twin data move across multiple software, cloud and OT environments, introducing opportunities for intellectual property theft, malware injection and the manipulation of manufacturing parameters. NIST SP 800-82 Rev. 3 contains good protection principles, but additional research is required to develop principles for continuously moving information between engineering systems and physical production (Stouffer et al., 2023). The required tool is missing: realistic testbeds. In view of this, learning factories as environmental workplaces that simulate authentic production processes for teaching and applied research are an ideal context for conducting CAD-to-machine security experiments and thereby advance the solutions to the region's skills gaps (Ndiyamba et al., 2026), with cybersecurity being a proposed region-specific skill gap among the others.

7.2 Digital-Twin Trust and Data Integrity

The second one relates to digital-twin trust and data integrity. Accurate sensor, model, and process data are crucial for twins, as if they become corrupted, the twin may produce incorrect predictions or hide an attack (Alcaraz and Lopez, 2022). While a digital twin can aid in the detection of cyber-attacks, including differentiating them from anomalies in the production process, as described by Alcaraz and Lopez in 2024, further testing needs to be performed on various CNC machines, robots, as well as additive manufacturing systems and complex production lines. For the study of data poisoning propagation to maintenance and operational decisions, there are natural candidates in the form of data-

driven maintenance models such as those developed for thermal power plant boilers (Senda et al., 2026) and multi-agent condition monitoring of induction furnaces (Mashava et al., 2026).

7.3 Interoperability and Standardisation

The third gap is one of interoperability and standardisation. Heterogeneous CAD/CAM software, PLCs, CNC controllers, sensors, cloud services and twin platforms are used in manufacturing environments. One of the known challenges for scalable twin deployments is the lack of mature standards and common interfaces (Jones et al., 2020; Frechette, Shao and Pease, 2026). Future research is needed to create interoperable security architectures for merging digital-twin standards with existing OT and cybersecurity standards, and for embedding security metadata within engineering artefacts.

7.4 Implications for Developing Industrial Economies

The evidence reviewed is largely from highly resourced industrial contexts. Manufacturers in developing economies are likely to be using legacy machines as well as newly connected machines, which might require a limited number of security personnel and a limited budget (Muhla et al., 2025a). Three priorities follow. Firstly, controls should prefer low cost-high leverage techniques like artefact possession, signed job packages and parameter-envelope checks as opposed to costly platform replacement. Second, condition-monitoring and maintenance analytics that are embraced to enhance reliability (Mashava et al., 2026; Senda et al., 2026) should be well protected from the start of the project and not added on after the fact. Thirdly, there is a need to have capacity building through learning factories and Industry-Academy partnerships (Ndiyamba et al., 2026) that encompass cyber-physical security in addition to automation and data skills. Table 4 summarises the research agenda.

Table 4. Research gaps and future research directions

Research gap	Future research direction
Fragmented security across CAD/CAM, OT and cloud	Develop and validate an end-to-end cyber-physical security framework.
Digital-twin manipulation	Use integrity verification, trusted data pipelines and anomaly detection.
Third-party and supply-chain risk	Strengthen provenance and continuous monitoring of suppliers and services.
Heterogeneous technologies	Establish interoperable security metadata and interface standards.
AI/ML vulnerability	Develop explainable and adversarially robust models for detection and maintenance.
Limited industrial validation	Build realistic cyber-physical testbeds, including learning factories.
Vulnerable CAD/CAM data and process parameters	Use encryption, signatures, provenance and parameter-envelope verification.
Resource-constrained adopters	Design proportionate, low-cost controls and embed security in skills programmes.

Further research needs to develop adaptive cyber-physical resilience, integrating continuous authentication, risk-based access control, secure data exchange, anomaly detection, twin verification and rapid recovery. NIST's manufacturing profile already advocates a risk-based approach (Stouffer et al., 2020), and digital twins can further this idea by creating a virtual environment for monitoring, prediction and security analysis.

Limitations of this Review

Limitations of this review. Only English-language sources indexed by the services used were searched, and reporting by vendors and national agencies in other languages may have been overlooked. Conclusions regarding the relative effectiveness are qualitative only due to heterogeneous reporting. There are a number of included studies that are conceptual and have not been tested on production equipment. Lastly, the examples from the context were not systematic and are presented to show how the authors have used the department where they are located.

8 CONCLUSIONS

CAD/CAM, computer-integrated manufacturing, cloud computing, Internet of Things (IoT) for Industry, cyber-physical systems and digital twins are creating highly connected manufacturing environments that are clearly driving productivity, flexibility and real-time decision-making. The same connectivity opens the design data, process parameters, manufacturing systems, networks and twins for cyber-physical attacks. Due to the fact that a limited number of process parameters often dictate the quality of a part, part fraud on the CAM output and on machine settings can result in fabricated parts that look real.

Digital twins can provide very good security opportunities when comparing simulated and actual behaviour, provided the digital twin is authenticated, has provenance and is not connected to the final security authority. The current frameworks need to be adapted to consider the entire CAD/CAM–cloud–twin lifecycle. Future frameworks should take a lifecycle, secure-by-design approach that makes engineering artefacts the core assets and introduce authentication, access control, provenance, encryption, anomaly detection, interoperability and security of the supply chain around a signed manufacturing job package. This can be validated on realistic testbeds, and then scaled to the resources of the adopting organisation, to enhance the confidentiality, integrity, availability, safety and resilience of smart manufacturing systems, and secure the adoption of next generation digital manufacturing technologies.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

We acknowledge the Department of Industrial and Manufacturing Engineering Department of the National university of Science and Technology.

Disclosure of conflict of interest

The authors declare no conflict of interest.

REFERENCES

- [1] Ahmmed, M.S., Khan, L., Mahmood, M.A. and Liou, F. (2025) 'Digital twins, AI, and cybersecurity in additive manufacturing: a comprehensive review of current trends and challenges', *Machines*, 13(8), 691. Available at: <https://doi.org/10.3390/machines13080691>.
- [2] Akter, S., Khalil, K. and Bayoumi, M. (2023) 'A survey on hardware security: current trends and challenges', *IEEE Access*, 11, pp. 77543–77565. Available at: <https://doi.org/10.1109/ACCESS.2023.3288696>.
- [3] Alcaraz, C. and Lopez, J. (2022) 'Digital twin: a comprehensive survey of security threats', *IEEE Communications Surveys & Tutorials*, 24(3), pp. 1475–1503. Available at: <https://doi.org/10.1109/COMST.2022.3171465>.
- [4] Alcaraz, C. and Lopez, J. (2024) 'Digital twin-assisted anomaly detection for industrial scenarios', *International Journal of Critical Infrastructure Protection*, 47, 100721. Available at: <https://doi.org/10.1016/j.ijcip.2024.100721>.
- [5] Alcaraz, C., Meskini, I.H. and Lopez, J. (2025) 'Digital twin communities: an approach for secure DT data sharing', *International Journal of Information Security*, 24, 17. Available at: <https://doi.org/10.1007/s10207-024-00912-1>.
- [6] Alhamam, N., Rahman, M.M.H. and Aljughaiman, A. (2025) 'A comprehensive review on cybersecurity of digital twins: issues, challenges, and future research directions', *IEEE Access*, 13, pp. 45106–45124. Available at: <https://doi.org/10.1109/ACCESS.2025.3545004>.
- [7] Ani, U.P.D., He, H. and Tiwari, A. (2017) 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *Journal of Cyber Security Technology*, 1(1), pp. 32–74.
- [8] Barricelli, B.R., Casiraghi, E. and Fogli, D. (2019) 'A survey on digital twin: definitions, characteristics, applications, and design implications', *IEEE Access*, 7, pp. 167653–167671. Available at: <https://doi.org/10.1109/ACCESS.2019.2953499>.
- [9] Becue, A. et al. (2020) 'A new concept of digital twin supporting optimization and resilience of factories of the future', *Applied Sciences*, 10(13), 4482. Available at: <https://doi.org/10.3390/app10134482>.
- [10] Belikovetsky, S., Solewicz, Y.A., Yampolskiy, M., Toh, J. and Elovici, Y. (2019) 'Digital audio signature for 3D printing integrity', *IEEE Transactions on Information Forensics and Security*, 14(5), pp. 1127–1141.

- [11] Boyens, J. et al. (2022) *Cybersecurity supply chain risk management practices for systems and organizations*. NIST Special Publication 800-161 Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-161r1>.
- [12] Boyes, H. and Watson, T. (2022) 'Digital twins: an analysis framework and open issues', *Computers in Industry*, 143, 103763. Available at: <https://doi.org/10.1016/j.compind.2022.103763>.
- [13] de Azambuja, A.J.G., Giese, T., Schützer, K., Anderl, R., Schleich, B. and Almeida, V.R. (2024) 'Digital twins in Industry 4.0 – opportunities and challenges related to cyber security', *Procedia CIRP*, 121, pp. 25–30. Available at: <https://doi.org/10.1016/j.procir.2023.09.225>.
- [14] El-Kady, A.H., Halim, S., El-Halwagi, M.M. and Khan, F. (2023) 'Analysis of safety and security challenges and opportunities related to cyber-physical systems', *Process Safety and Environmental Protection*, 173, pp. 384–413.
- [15] Elhabashy, A.E., Wells, L.J., Camelio, J.A. and Woodall, W.H. (2019) 'A cyber-physical attack taxonomy for production systems: a quality control perspective', *Journal of Intelligent Manufacturing*, 30(6), pp. 2489–2504.
- [16] Erceylan, G., Akbarzadeh, A. and Gkioulos, V. (2025) 'Leveraging digital twins for advanced threat modeling in cyber-physical systems cybersecurity', *International Journal of Information Security*, 24(3), 151. Available at: <https://doi.org/10.1007/s10207-025-01043-x>.
- [17] Fernández-Caramés, T.M. and Fraga-Lamas, P. (2019) 'A review on the application of blockchain to the next generation of cybersecure Industry 4.0 smart factories', *IEEE Access*, 7, pp. 45201–45218.
- [18] Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L. and Janicke, H. (2022) 'Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning', *IEEE Access*, 10, pp. 40281–40306.
- [19] Frechette, S., Shao, G. and Pease, M. (2026) *Digital twins workshops summary report*. NIST Interagency/Internal Report 8620. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.IR.8620>.
- [20] Graves, L.M.G., Lubell, J., King, W. and Yampolskiy, M. (2019) 'Characteristic aspects of additive manufacturing security from security awareness perspectives', *IEEE Access*, 7, pp. 103833–103853. Available at: <https://doi.org/10.1109/ACCESS.2019.2931738>.
- [21] Gupta, N., Tiwari, A., Bukkapatnam, S.T.S. and Karri, R. (2020) 'Additive manufacturing cyber-physical system: supply chain cybersecurity and risks', *IEEE Access*, 8, pp. 47322–47333. Available at: <https://doi.org/10.1109/ACCESS.2020.2978815>.
- [22] Hammi, B., Zeadally, S. and Nebhen, J. (2023) 'Security threats, countermeasures, and challenges of digital supply chains', *ACM Computing Surveys*, 55(14s), 316. Available at: <https://doi.org/10.1145/3588999>.
- [23] Hasan, H.R. et al. (2020) 'A blockchain-based approach for the creation of digital twins', *IEEE Access*, 8, pp. 34113–34126. Available at: <https://doi.org/10.1109/ACCESS.2020.2974810>.
- [24] Hedberg, T.D., Lubell, J., Fischer, L., Maggiano, L. and Feeney, A.B. (2016) 'Testing the digital thread in support of model-based manufacturing and inspection', *Journal of Computing and Information Science in Engineering*, 16(2), 021001.
- [25] Hu, W., Chang, C.-H., Sengupta, A., Bhunia, S., Kastner, R. and Li, H. (2021) 'An overview of hardware security and trust: threats, countermeasures, and design tools', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(6), pp. 1010–1038.
- [26] IEC (2013) *IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*. Geneva: International Electrotechnical Commission.
- [27] ISO (2021) *ISO 23247-1:2021 Automation systems and integration – Digital twin framework for manufacturing – Part 1: Overview and general principles*. Geneva: International Organization for Standardization.
- [28] Jacoby, M. and Usländer, T. (2020) 'Digital twin and Internet of Things – current standards landscape', *Applied Sciences*, 10(18), 6519. Available at: <https://doi.org/10.3390/app10186519>.
- [29] Jansen, K.C., Mapindu, I., Muhla, T.M., Kanyemba, G. and Mashava, D. (2025) 'Optimization of edible oil quality through vacuum bleaching: an experimental design and analysis study', *Open Access Research Journal of Science and Technology*, 13(2), pp. 68–78. Available at: <https://doi.org/10.53022/oarjst.2025.13.2.0051>.
- [30] Jones, D., Snider, C., Nassehi, A., Yon, J. and Hicks, B. (2020) 'Characterising the digital twin: a systematic literature review', *CIRP Journal of Manufacturing Science and Technology*, 29, pp. 36–52. Available at: <https://doi.org/10.1016/j.cirpj.2020.02.002>.

- [31] Khorrami, F., Krishnamurthy, P. and Karri, R. (2016) 'Cybersecurity for control systems: a process-aware perspective', *IEEE Design & Test*, 33, pp. 75–83.
- [32] Kritzinger, W., Karner, M., Traar, G., Henjes, J. and Sihn, W. (2018) 'Digital twin in manufacturing: a categorical literature review and classification', *IFAC-PapersOnLine*, 51(11), pp. 1016–1022. Available at: <https://doi.org/10.1016/j.ifacol.2018.08.474>.
- [33] Kumar, R., Aljuhani, A., Javeed, D., Kumar, P., Islam, S. and Islam, A.K.M.N. (2024) 'Digital twins-enabled zero touch network: a smart contract and explainable AI integrated cybersecurity framework', *Future Generation Computer Systems*, 156, pp. 191–205. Available at: <https://doi.org/10.1016/j.future.2024.02.015>.
- [34] Mapindu, I., Foya, A., Muhla, T.M., Chinguwo, K.N. and Kanyemba, G. (2026a) 'Minimizing defects in injection molding using the Taguchi method', *World Journal of Advanced Engineering Technology and Sciences*, 20(2), pp. 240–252. Available at: <https://doi.org/10.30574/wjaets.2026.20.2.0419>.
- [35] Mapindu, I., Munhuwamambo, G., Mashava, D. and Ngwenya, L. (2026b) 'Optimization of cutting parameters in CNC milling using the Taguchi method', *Global Journal of Engineering and Technology Advances*, 28(2), pp. 149–162. Available at: <https://doi.org/10.30574/gjeta.2026.28.2.0223>.
- [36] Mapindu, I., Muhla, T.M., Chinguwo, K.N. and Foya, A. (2026c) 'Process parameter optimization for 3D printing using the Taguchi method', *Open Access Research Journal of Science and Technology*, 18(1), pp. 34–45. Available at: <https://doi.org/10.53022/oarjst.2026.18.1.0082>.
- [37] Mapindu, I., Mashava D., Shangwa, V., Chigavazira-Gwara, T.T., Munhuwamambo, G (2026d) 'Taguchi-based optimization of GMAW welding parameters for joint strength', *World Journal of Advanced Engineering Technology and Sciences*, 20(3), pp. 206–219. Available at: <https://doi.org/10.30574/wjaets.2026.20.3.0448>
- [38] Mashava, D., Muhla, T.M., Munhuwamambo, G., Mapindu, I., Chinguwo, K.N. and Wachenuka, T. (2026) 'A multi-agent system framework for real-time self-diagnostic condition monitoring of induction furnace equipment in developing industrial economies', *Open Access Research Journal of Science and Technology*, 17(2), pp. 28–43. Available at: <https://doi.org/10.53022/oarjst.2026.17.2.0071>.
- [39] Moustafa, N., Adi, E., Turnbull, B. and Hu, J. (2018) 'A new threat intelligence scheme for safeguarding Industry 4.0 systems', *IEEE Access*, 6, pp. 32910–32924. Available at: <https://doi.org/10.1109/ACCESS.2018.2844794>.
- [40] Moyne, J., Qamsane, Y., Balta, E.C., Kovalenko, I., Faris, J., Barton, K. and Tilbury, D.M. (2020) 'A requirements driven digital twin framework: specification and opportunities', *IEEE Access*, 8, pp. 107781–107801. Available at: <https://doi.org/10.1109/ACCESS.2020.3000437>.
- [41] Muhla, T., Mapindu, I., Munyau, M., Mashava, D., Mhlanga, S. and Goriwondo, W. (2023) 'Agility as a strategy in Zimbabwean manufacturing industries', *Zimbabwe Journal of Science & Technology*, 18, pp. 1–11. e-ISSN 2409-0360.
- [42] Muhla, T.M., Mashava, D., Kanyemba, G., Mapindu, I. and Goriwondo, W.M. (2025a) 'An assessment of the implementation of Industry 4.0 in Zimbabwean manufacturing industries', *World Journal of Advanced Engineering Technology and Sciences*, 15(2), pp. 970–984. Available at: <https://doi.org/10.30574/wjaets.2025.15.2.0653>.
- [43] Muhla, T., Kanyemba, G., Mapindu, I., Chinguwo, N., Mashava, D. and Goriwondo, W. (2025b) 'Enhancing safety in Zimbabwean manufacturing industry: the role of human factors engineering in reducing workplace accidents', *Open Access Research Journal of Science and Technology*, 13(2), pp. 19–30. Available at: <https://doi.org/10.53022/oarjst.2025.13.2.0037>.
- [44] Mullet, V., Sondi, P. and Ramat, E. (2021) 'A review of cybersecurity guidelines for manufacturing factories in Industry 4.0', *IEEE Access*, 9, pp. 23235–23263. Available at: <https://doi.org/10.1109/ACCESS.2021.3056650>.
- [45] Mun, H., Han, K., Damiani, E., Yeun, H.K., Kim, T.-Y., Martino, L. and Yeun, C.Y. (2025) 'A comprehensive survey on digital twin: focusing on security threats and requirements', *IEEE Access*, 13, pp. 73362–73390. Available at: <https://doi.org/10.1109/ACCESS.2025.3563621>.
- [46] Munotyaaani, S., Bawono, N.M.H., Tayisepi, N., Mapindu, I., Anggoro, P.W., Bawono, B., Pamosoaji, A.K. and Adi, A.Y.N.M.P. (2026) 'Design and development of a dual-mode smart wheelchair prototype with obstacle detection for Zimbabwe', *Jurnal Rekayasa Mesin*, 21(1), pp. 51–66. Available at: <https://doi.org/10.32497/jrm.v21i1.6954>.
- [47] Muyambo, R.D., Muhla, T., Kanyemba, G., Mashava, D., Munhuwamambo, G. and Mapindu, I. (2025) 'Design and development of a vertical axis wind turbine for slip stream energy harvesting', *Global Journal of Engineering and Technology Advances*, 23(3), pp. 10–20. Available at: <https://doi.org/10.30574/gjeta.2025.23.3.0166>.
- [48] Ndiyamba, D., Murena, E., Kasukusa, S., Mafuratidze, F., Nenzhelele, T., Mpofu, K. and Mapindu, I. (2026) 'Learning factories as a catalyst for innovation in Southern African engineering education', in *CLF 2026 Book of Short Papers*

on Learning Factories: Proceedings of the 16th Conference on Learning Factories, Bolzano, Italy, 5–7 May 2026. Bolzano: Free University of Bozen-Bolzano, pp. 93–99. Available at: <https://doi.org/10.5281/zenodo.20780648>.

- [49] NIST (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.CSWP.29>.
- [50] Page, M.J. et al. (2021) 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *BMJ*, 372, n71. Available at: <https://doi.org/10.1136/bmj.n71>.
- [51] Rahman, M.H. and Shafae, M. (2025) 'Cyber-physical security vulnerabilities identification and classification in smart manufacturing: a defense-in-depth driven framework and taxonomy', *Journal of Computing and Information Science in Engineering*, 25(9), 091005. Available at: <https://doi.org/10.1115/1.4068844>.
- [52] Rahman, M.H., Wuest, T. and Shafae, M. (2023) 'Manufacturing cybersecurity threat attributes and countermeasures: review, meta-taxonomy, and use cases of cyberattack taxonomies', *Journal of Manufacturing Systems*, 68, pp. 196–208.
- [53] Rasheed, A., San, O. and Kvamsdal, T. (2020) 'Digital twin: values, challenges and enablers from a modeling perspective', *IEEE Access*, 8, pp. 21980–22012. Available at: <https://doi.org/10.1109/ACCESS.2020.2970143>.
- [54] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) *Zero trust architecture*. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-207>.
- [55] Segovia, M. and Garcia-Alfaro, J. (2022) 'Design, modeling and implementation of digital twins', *Sensors*, 22(14), 5396.
- [56] Senda, S., Muhla, T.M., Mapindu, I., Ngwenya, L., Mushangure, R.O. and Mashava, D. (2026) 'Machine learning enabled preventive maintenance strategy for improving boiler reliability of a thermal power station', *Open Access Research Journal of Science and Technology*, 17(2), pp. 18–27. Available at: <https://doi.org/10.53022/oarjst.2026.17.2.0070>.
- [57] Sharma, A. et al. (2022) 'Digital twins: state of the art theory and practice, challenges, and open research questions', *Journal of Industrial Information Integration*, 30, 100383. Available at: <https://doi.org/10.1016/j.jii.2022.100383>.
- [58] Sola, A. et al. (2022) 'How can we provide additively manufactured parts with a fingerprint? A review of tagging strategies in additive manufacturing', *Materials*, 15(1), 85.
- [59] Stouffer, K. et al. (2020) *Cybersecurity Framework Version 1.1 Manufacturing Profile*. NISTIR 8183 Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.IR.8183r1>.
- [60] Stouffer, K. et al. (2023) *Guide to operational technology (OT) security*. NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-82r3>.
- [61] Suhail, S., Iqbal, M., Hussain, R. and Jurdak, R. (2023) 'ENIGMA: an explainable digital twin security solution for cyber-physical systems', *Computers in Industry*, 151, 103961.
- [62] Tandi, O., Mapindu, I., Muhla, T.M., Chinguwo, N.K. and Tayisepi, N. (2025) 'Design and analysis of a passive upper limb exoskeleton for augmented construction worker strength', *Open Access Research Journal of Science and Technology*, 13(2), pp. 79–88. Available at: <https://doi.org/10.53022/oarjst.2025.13.2.0050>.
- [63] Tao, F., Qi, Q., Wang, L. and Nee, A.Y.C. (2019) 'Digital twins and cyber-physical systems toward smart manufacturing and Industry 4.0: correlation and comparison', *Engineering*, 5(4), pp. 653–661. Available at: <https://doi.org/10.1016/j.eng.2019.01.014>.
- [64] Tayisepi, N., Svosve, R., Tigere, G., Mnkandla, A.N. and Mapindu, I. (2023) 'Comparative optimisation of the cutting parameters for surface quality and energy efficiency during the machining manufacturing of teak, saligna and pine wood materials', *Journal of Engineering Research and Reports*, 25(11), pp. 73–87. Available at: <https://doi.org/10.9734/JERR/2023/v25i111023>.
- [65] Tayisepi, N., Mugwagwa, L., Mnkandla, A.N., Mapindu, I. and Muhla, T.M. (2024) 'Experimental investigation and simultaneous optimisation of honing parameters of dry cast iron cylinder relining sleeves of motor vehicle engine blocks for surface finish and energy use', *Computational Engineering and Physical Modeling*, 7(4), pp. 88–103. Available at: <https://doi.org/10.22115/cepm.2024.473138.1324>.
- [66] Tuptuk, N. and Hailes, S. (2018) 'Security of smart manufacturing systems', *Journal of Manufacturing Systems*, 47, pp. 93–106. Available at: <https://doi.org/10.1016/j.jmsy.2018.04.007>.

- [67] Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018) *Blockchain technology overview*. NISTIR 8202. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.IR.8202>.
- [68] Yampolskiy, M. et al. (2018) 'Security of additive manufacturing: attack taxonomy and survey', *Additive Manufacturing*, 21, pp. 431–457. Available at: <https://doi.org/10.1016/j.addma.2018.03.015>.
- [69] Yousefnezhad, N., Malhi, A. and Främpling, K. (2020) 'Security in product lifecycle of IoT devices: a survey', *Journal of Network and Computer Applications*, 171, 102779.
- [70] Zarreh, A., Saygin, C., Wan, H., Lee, Y. and Bracho, A. (2018) 'Cybersecurity analysis of smart manufacturing system using game theory approach and quantal response equilibrium', *Procedia Manufacturing*, 17, pp. 1001–1008.
- [71] Zarreh, A. et al. (2019) 'Risk assessment for cyber security of manufacturing systems: a game theory approach', *Procedia Manufacturing*, 38, pp. 605–612.