© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

Building Cyber-Resilient Industrial IOT Ecosystems in Saudi Arabia: A Risk-Based Security Framework for Smart Manufacturing Under Vision 2030

ISHAQ SIDDIQUI MOHAMMED
ORCiD - 0009-0004-9338-1662

Abstract- ***Industrial Internet of Things (IIoT) adoption is central to smart manufacturing because connected sensors, controllers, edge platforms, cloud services, and analytics can improve visibility, flexibility, and productivity. The same integration creates cyber-physical dependencies in which compromise of identity, firmware, communications, data, or control logic can propagate into downtime, unsafe states, quality loss, and supply-chain disruption. This structured integrative review synthesizes 30 peer-reviewed, DOI-verified studies published from 2020 to 2025 and separates that scholarly corpus from a second contextual layer of authoritative Saudi policy and cybersecurity documents. with inclusion limited to studies directly addressing IIoT threats, industrial detection and datasets, trust architecture, lifecycle security, cyber-resilience management, forensics, or Saudi smart-manufacturing context. Because the original record-export log was unavailable, the review does not claim PRISMA-complete record-flow counts or exhaustive coverage. The synthesis indicates that isolated preventive controls are insufficient for heterogeneous industrial environments with long-lived OT, constrained devices, remote support, and expanding cloud-edge connectivity. An evidence-informed six-dimension conceptual framework is therefore proposed, linking governance, asset and identity visibility, lifecycle assurance, monitoring, cyber-physical response and recovery, and measurable learning to operational consequences and ownership. The framework has been examined for contextual coherence across greenfield, brownfield, and multi-site scenarios but has not yet been empirically validated in Saudi manufacturing; validation through structured expert assessment, case studies, exercises, and longitudinal operational metrics is required.***

Keywords: Industrial Internet of Things (IIoT); cyber resilience; smart manufacturing; Saudi Arabia; Vision 2030; risk-based security; Industry 4.0; operational technology

I. INTRODUCTION

Saudi Arabia's industrial transformation increasingly involves data-intensive production, automation, connected equipment, and localization of manufacturing capability. Vision 2030 and the National Industrial Development and Logistics Program provide the policy context for advanced manufacturing, industrial diversification, technology transfer, and local value creation [31,32]. Saudi-specific manufacturing evidence is more limited than the international IIoT security literature; therefore, this review distinguishes two evidence layers. The first consists of peer-reviewed international and Saudi-authored studies used to establish technical and managerial propositions. The second consists of Saudi contextual and regulatory sources used only to adapt those propositions to national governance, OT, critical-system, and industrial-policy requirements. For example, Aljuaid et al. [27] directly examine Industry 4.0-enabled localization in the Saudi automotive context, while the National Cybersecurity Authority's Essential Cybersecurity Controls and Operational Technology Cybersecurity Controls establish national expectations for governance, asset protection, resilience, OT/ICS security, backup, recovery, access control, and third-party risk [33,34]. International evidence is therefore not presented as direct observation of Saudi factories; it is treated as transferable evidence whose applicability is conditioned by Saudi industrial priorities and regulatory controls.

The Industrial Internet of Things (IIoT) increases this difficulty since it brings together a variety of different devices, industrial protocols, edge and fog computing, enterprise platforms, cloud services and external suppliers. Repeated surveys have always found that

authentication, authorisation, integrity, availability, privacy and trustworthy device management are continuous requirements, yet they also indicate that no single security measure can address the entire IIoT stack [2,6,7,12]. Potential vulnerabilities occur at the perception or device level, along the network and transmission routes, in edge and cloud processing, and also in the applications and data exchanges. Furthermore, security failures may develop over time when industrial equipment that remains in use for long periods becomes hard to patch or when the update procedures clash with safety and availability requirements [5]. The outcome is that a security issue must be understood not just in terms of the likelihood of an intrusion, but also in relation to how quickly and to what extent a digital breach can lead to a cyber-physical failure.

A more appropriate approach than just prevention is cyber resilience, since resilience involves an organisation's ability to anticipate, endure, respond to, recover from and adapt following adverse cyber events while at the same time maintaining its essential functions. Research in the field of management indicates that resilience is influenced not only by technical controls but also by context, leadership, governance and organisational learning [19,20]. It is equally important to measure resilience because an organisation will not be able to make reliable improvements in this area if it cannot connect its protective capabilities to mission performance, recovery and risk [21]. IIoT standards and security literature similarly shows the value of connecting security requirements to the characteristics of industrial connectivity, safety and operational constraints rather than treating threats as an isolated catalogue [1]. This review builds on that principle while focusing specifically on cyber-resilience and its operationalization for the Saudi industrial context.

The goal of this review is to synthesize evidence published from 2020 to 2025 and develop an evidence-informed, risk-oriented conceptual framework for cyber-resilience in Saudi IIoT-enabled manufacturing. Four objectives guide the review: (1) examine how threats propagate across IIoT and industrial cyber-physical layers; (2) assess the strengths and limitations of current controls under industrial availability and safety constraints; (3) translate the evidence into governance, lifecycle, trust, monitoring, response, and recovery practices suitable for Saudi greenfield, brownfield, and supplier-connected environments; and (4) define measurable implementation priorities for continuous improvement. The review addresses four research questions: (RQ1) Which cyber-resilience capabilities recur across the IIoT smart-manufacturing literature? (RQ2) How can these capabilities be operationalized for Saudi manufacturing? (RQ3) How can controls be prioritized using production, safety, exposure, recovery and dependency risk? (RQ4) Which measurable indicators can assess resilience maturity? The paper makes four bounded contributions within the comparison set identified in this review: (1) an integrated six-dimension ecosystem treatment of IIoT cyber resilience; (2) operationalization of the literature against Saudi regulatory and industrial context; (3) a consequence-scaled prioritization approach that links production, safety, exposure, dependency and recovery considerations; and (4) measurable resilience assurance through ownership, evidence artifacts and operational metrics. Individual controls such as segmentation, Zero Trust, intrusion detection, secure updating and recovery are not claimed as novel inventions; the contribution lies in their evidence-informed integration and operationalization. Within the comparison set identified in this review, the framework differs from IIoT surveys that catalogue threats and controls [1,2,6,7,12], Zero Trust studies focused on trust architecture [15,16], resilience studies focused on management and measurement [19-21], and Saudi policy controls that prescribe requirements without providing this evidence-to-prioritization synthesis [33,34].

The study therefore presents an evidence-informed conceptual decision framework rather than a validated decision-support instrument or a new detection algorithm. It represents cyber risk as a chain linking assets, threats, vulnerabilities, exposure and propagation paths to operational consequences, controls, recovery capability, and residual risk. This framing is relevant to Saudi smart manufacturing because greenfield plants, brownfield modernization programs, and multi-supplier ecosystems can have markedly different levels of digital maturity and OT

constraint. A common risk vocabulary allows organizations to prioritize high-consequence systems, justify advanced analytics where the telemetry base is mature, and retain compensating controls where legacy constraints prevent immediate modernization. The framework was conceptually stress-tested against three representative manufacturing scenarios for internal coherence only; effectiveness has not been established empirically. Future validation should combine a Saudi expert Delphi assessment, plant case studies, simulated or digital-twin attack scenarios, and longitudinal measurement of containment, recovery, and production-impact outcomes.

II. CONCEPTUAL FOUNDATIONS AND SAUDI SMART-MANUFACTURING CONTEXT

IIoT security differs from conventional enterprise security because the protected object is a coupled production system. Device fleets include sensors, programmable controllers, actuators, human-machine interfaces, robots, cameras, gateways, and embedded computing platforms that may operate for years, while communications traverse field networks, industrial Ethernet, wireless links, edge servers, and cloud services [2,3]. The consequence model must therefore distinguish at least six outcome classes. Confidentiality loss exposes sensitive process, product, or business information; integrity loss corrupts measurements, commands, configurations, or models; availability loss interrupts access to control or information; safety impact can place personnel, equipment, or the environment at risk; quality impact can produce off-specification output or hidden process degradation; and production-continuity impact can reduce throughput, delay orders, or stop a line. These outcomes overlap but are not interchangeable. Conventional IT controls often optimize confidentiality and service availability, whereas OT decisions must also preserve deterministic behaviour, validated control logic, process safety, product quality, and recoverability. Risk assessment in IIoT must therefore connect cyber events to physical process consequences rather than treat every compromised endpoint as equivalent.

Control maturity and resilience maturity are related but distinct. Control maturity asks whether required safeguards are defined, implemented, governed and evidenced; resilience maturity asks whether critical industrial functions can withstand disruption, degrade safely, contain compromise, recover within required operational limits and return to a verified trusted state. A plant may therefore be compliant with a control baseline yet remain operationally fragile if recovery has not been tested or if controls fail under real OT constraints. This distinction is used throughout the framework to separate control presence from demonstrated operational resilience.

The risk surface is also temporal. Industrial assets are often expected to remain available continuously, which may delay patching and make replacement costly. Mugarza et al. [5] show that secure software maintenance must be integrated with safety processes because an update that reduces cyber exposure can still create unacceptable operational risk if it changes validated behaviour. Vulnerability management in manufacturing cannot simply copy an office-IT patch cadence. Asset owners need tested maintenance windows, rollback capability, supplier coordination, and compensating controls for devices that cannot be updated promptly. The implication for risk assessment is significant: vulnerability severity should be weighted by exploitability, exposure, safety function, production criticality, recovery options, and the feasibility of temporary containment.

Connectivity also changes trust. Traditional perimeter models assume internal location provides confidence, but IIoT estates include contractors, remote vendor support, mobile engineering laptops, cloud applications, and machine-to-machine identities. Zero-trust research favors explicit verification, least privilege, granular access, and continuous policy decisions [15,16]. In manufacturing, zero trust must be adapted rather than imposed mechanically. Excessive authentication latency or poor segmentation is able to disrupt deterministic processes. The useful principle is not to add friction everywhere but to remove implicit trust from pathways that could enable lateral movement. High-risk engineering access, remote maintenance, privileged changes, and data flows crossing production zones deserve stronger identity,

authorization, and monitoring than stable low-level communications inside tightly controlled cells.

Detection creates another conceptual tension. Machine-learning and deep-learning studies report strong classification results on datasets such as TON_IoT, Edge-IIoTset, and X-IIoTID [8-11], and Saudi-based researchers have proposed anomaly-detection and deep-learning approaches for industrial environments [13,26,28]. These studies expand the detection toolkit, but benchmark performance must not be equated with operational effectiveness. Public datasets may not represent a plant's protocols, equipment mix, maintenance states, traffic seasonality, rare legitimate events, or attack prevalence. Class imbalance can inflate aggregate accuracy; concept drift can degrade models after process or configuration changes; false positives can overload operators; and false negatives can leave persistent compromise undetected. Explainability becomes important where an alert may influence isolation or restart decisions [24]. Models may also be exposed to evasion, poisoning, or manipulated training data, while automated containment introduces a separate safety risk if a response changes deterministic communications or interferes with a safety-instrumented function. For OT use, detection should therefore be locally validated, monitored for drift and adversarial behavior, and coupled to human-authorized response rules for high-consequence actions.

Resilience requires layered control and recoverability. Annarelli et al. [19] connect cyber resilience with managerial actions and organizational context, while Loonam et al. [20] emphasize leadership, integration, and culture. Kebande and Ikuesan [23] add an IIoT digital-forensics perspective, highlighting the need for standardized evidence processes after an incident. Manufacturers therefore need synchronized logs, retained telemetry, trustworthy timestamps, and procedures that preserve useful evidence without jeopardizing production. A factory that blocks many attacks but cannot contain a compromised cell, restore trusted controller logic, or reconstruct a supply-chain intrusion remains fragile. A resilient design assumes that some preventive controls will fail and provides safe degraded operating states, protected backups, manual alternatives, escalation authority, and forensic readiness so recovery restores a trustworthy and safe process rather than only a functioning network.

For Saudi manufacturing, these principles intersect with localization, rapid technology adoption, and national cybersecurity requirements. Aljuaid et al. [27] provide direct Saudi manufacturing evidence that Industry 4.0 can support localized production, while Vision 2030 and the National Industrial Development and Logistics Program frame industrial diversification and local capability as national priorities [31,32]. The NCA Essential Cybersecurity Controls, where applicable and within the organization’s regulatory scope, establish governance, risk, access, continuity, and third-party expectations across national entities, and the Operational Technology Cybersecurity Controls extend those expectations to OT/ICS environments, including asset protection, secure access, data protection, backup and recovery, and technology-specific safeguards [33,34]. These sources do not prove that a particular control will be effective in every Saudi factory; rather, they define the Saudi contextual conditions under which international IIoT evidence should be adapted. The resulting security objective is to preserve industrial mission outcomes while enabling controlled digital expansion, with investment linked to production-loss scenarios, safety consequences, recovery time, supplier dependence, and strategic criticality.

As an author-developed implementation synthesis—not an official NCA roadmap—the framework can be sequenced as visibility → governance → protection → detection → response/recovery → optimization. Visibility establishes critical-asset, identity and dependency knowledge; governance assigns risk ownership and exception authority; protection applies lifecycle, segmentation and access controls; detection establishes trustworthy telemetry and analytics; response/recovery validates safe containment and trusted restoration; and optimization uses metrics, exercises and lessons learned to improve the system. The stages are mapped primarily to the NCA Essential Cybersecurity Controls and Operational Technology Cybersecurity Controls [33,34], with complementary implementation guidance from NIST SP 800-82 Rev. 3 for OT security and the IEC 62443 series for

industrial automation and control-system security [35,36].

III. REVIEW METHODOLOGY

This study uses a structured integrative review because the evidence base spans security surveys, intrusion-detection datasets and experiments, architectural studies, lifecycle research, resilience-management studies, forensics, and Saudi smart-manufacturing research with heterogeneous outcomes that are unsuitable for statistical pooling. The review is deliberately not presented as a meta-analysis or as a fully systematic PRISMA review. Instead, it uses a transparent, auditable search-and-coding protocol to support conceptual framework development. During revision, bibliographic details and DOIs of the included studies were re-verified against publisher or DOI records. The analytical aim was not to estimate a pooled effect size, but to identify recurring risk mechanisms, complementary control functions, OT implementation constraints, and measurable resilience outcomes that could be translated into a Saudi manufacturing context.

The peer-reviewed search window covered January 2020 through December 2025. A revision-stage search and bibliographic re-verification was completed on 17 September 2026. The revision protocol used IEEE Xplore, ScienceDirect, SpringerLink, Wiley Online Library, and publisher/DOI pages for bibliographic verification, with Google Scholar used only for supplementary backward/forward citation discovery. Three core Boolean strings were applied with syntax adapted to each platform: S1 = ("industrial internet of things" OR IIoT OR "industrial cyber-physical system*" OR "smart manufactur*") AND (cybersecurity OR "cyber security" OR "cyber resilien*" OR security); S2 = (IIoT OR "smart manufactur*") AND ("intrusion detection" OR "zero trust" OR "federated learning" OR "software update*" OR "digital forensic*" OR blockchain); and S3 = (Saudi OR "Saudi Arabia") AND (IIoT OR "Industry 4.0" OR "smart manufactur*") AND (cybersecurity OR security OR localization OR localisation). Filters were publication years 2020-2025, English language, peer-reviewed scholarly publication, and direct relevance to at least one analysis domain. Included studies addressed IIoT security requirements or threats; industrial datasets/detection; trust, segmentation or access architecture; lifecycle/supply-chain security; cyber-resilience management or measurement; digital forensics; or Saudi Industry 4.0/manufacturing context. Duplicates, non-peer-reviewed material, papers outside the date range, papers without a verifiable DOI, and studies lacking sufficient industrial relevance were excluded from the 30-study scholarly corpus. Authoritative Saudi controls and Vision 2030 policy documents were retained separately as contextual/regulatory evidence and were not counted among the 30 peer-reviewed studies.

Coding was conducted by one reviewer. A study was coded to a theme when its methods, findings or explicit review conclusions materially addressed that theme; studies could receive multiple non-exclusive codes where they supported more than one dimension. The thematic counts are therefore author-coded descriptive frequencies rather than effect estimates or statistically validated prevalence. Reviews, datasets, empirical experiments and conceptual frameworks were eligible when they were peer-reviewed, DOI-verifiable and directly relevant to at least one analysis domain. Opinion articles were excluded from the 30-study scholarly corpus. Contextual Saudi policy and regulatory documents were retained separately and were not counted as peer-reviewed evidence.

The final eligibility audit confirmed 30 DOI-verified peer-reviewed works meeting the stated inclusion criteria. The original database-export file used during initial drafting was not preserved; therefore, exact historical counts for records identified, duplicates removed, title/abstract exclusions, and full texts assessed cannot be reconstructed without fabrication. This limitation is stated explicitly rather than presenting unsupported PRISMA-style flow numbers. One reviewer conducted the revision-stage eligibility check and thematic coding, which introduces possible selection and interpretation bias. The corpus is therefore a traceable, purposive integrative sample rather than a claim of exhaustive coverage. Evidence was coded through a risk chain comprising protected asset/process, threat, enabling vulnerability or trust failure, propagation path, operational consequence,

preventive/detective control, recovery mechanism, and residual risk. A second coding layer captured OT implementation constraints including latency, deterministic behavior, legacy compatibility, patchability, maintenance windows, safety functions, compute/resource limits, skills, data availability, explainability, and multi-organization coordination. Themes were non-exclusive, allowing a study to support more than one dimension.

Framework derivation followed a transparent synthesis procedure rather than selecting six dimensions a priori. First, each of the 30 studies was coded against the risk chain and implementation constraints described above. Second, recurring control themes were clustered where they addressed related stages of the incident lifecycle and could be tied to an accountable owner and measurable outcome. Third, overlapping clusters were consolidated into six dimensions: (1) risk governance and ownership; (2) asset, identity and trust zoning; (3) secure lifecycle and supply-chain assurance; (4) adaptive monitoring and trustworthy analytics; (5) cyber-physical response and recovery; and (6) measurement, workforce and ecosystem learning. Fourth, each dimension was checked against Saudi contextual requirements in [31]-[34]. Finally, the integrated model was conceptually examined across a greenfield cloud-edge plant, a brownfield site with long-lived OT, and a multi-site manufacturer dependent on suppliers and remote support. This scenario exercise assessed contextual coherence only and did not constitute empirical validation. Table 2 makes the derivation auditable by linking each dimension to supporting studies, recurring evidence themes, Saudi contextual considerations, and recommended measures.

Table 2. Evidence-to-framework synthesis matrix.

Dimension	Supporting studies	Recurring evidence themes	Saudi contextual considerations	Control / measurement implication	Evidence type
1. Risk governance & ownership	[19-21], [6], [22]	Leadership, risk tolerance, resilience measurement, framework integration	ECC governance/risk expectations where applicable and within the organization's regulatory scope [33]; Vision 2030 industrial continuity context [31,32]	Named scenario owners; residual-risk approvals; critical-process/RTO coverage; overdue exceptions	Management and measurement studies; review evidence
2. Asset, identity & trust zoning	[2,3,6,7,12,15,16,25]	Asset visibility, least privilege, trust boundaries, lateral-movement reduction	OT/ICS access and asset protection requirements [34]	Critical-asset inventory coverage; privileged sessions recorded; unknown assets; unauthorized conduits blocked	Security surveys and Zero Trust reviews; architecture evidence

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

3. Lifecycle & supply-chain assurance	[4,5,7,12,22]	Secure update, vendor dependence, unsupported assets, provenance and maintenance risk	ECC third-party/risk controls [33]; OT lifecycle and configuration expectations [34]	Unsupported-asset exposure; signed-update coverage; supplier remediation time; approved compensating controls	Lifecycle and supply-chain studies; review/framework evidence
4. Adaptive monitoring & trustworthy analytics	[8-13], [17,18], [24], [26], [28]	Multi-source detection, explainability, federated learning, model drift and false alarms	OT operability constraints [34]; local validation for Saudi plant traffic	Detection coverage; false-positive burden; mean triage time; drift checks; missed high-consequence scenarios	Datasets and empirical detection studies plus reviews
5. Cyber-physical response & recovery	[14], [19-21], [23]	Safe containment, degraded modes, trusted restoration, forensic readiness	ECC/OTCC incident, backup and recovery expectations [33,34]	Containment time; tested restore rate; RTO attainment; exercise findings closed; evidence completeness	Cyber-physical/security and resilience studies; forensic review evidence
6. Measurement, workforce & ecosystem learning	[19-21], [23], [27]	Learning loops, leadership, skills, localization, supplier capability	Localization and capability development [27,31,32]; NCA governance expectations [33]	Repeat causes eliminated; exercise completion; supplier learning; workforce capability; trend review	Management, measurement and Saudi localization evidence

Figure 1. Risk propagation model for an IIoT-enabled smart factory. Source: Author's synthesis.

IV. EVIDENCE SYNTHESIS: THREATS, CONTROL GAPS AND RESILIENCE ENABLERS

The reviewed literature generally indicates that IIoT risk becomes systemic when connectivity turns local weaknesses into propagation pathways [2,3,6,7,12,14]. Non-exclusive thematic coding of the 30-study corpus identified recurring support for threat/security architecture (13 studies), detection and trustworthy analytics (10), lifecycle or supply-chain security (6), identity/trust/segmentation (5), resilience,

recovery or measurement (6), and Saudi-authored or Saudi-context technical/manufacturing evidence (7); because studies could support several themes, these counts intentionally overlap. Only a subset constitutes direct Saudi manufacturing evidence, with [27] providing the clearest localization-focused manufacturing study. Common attack paths include credential abuse, spoofing, denial of service, malware, protocol manipulation, data tampering, insecure interfaces, and compromised endpoints [2,3,7,12,25]. At the edge, constrained devices may lack strong identity, secure storage, or update capability; flat or permissive networks can increase lateral movement; and cloud credentials, APIs, data pipelines, and analytics create additional exposure. The relevant unit of risk is therefore not a vulnerable device in isolation but the device's position in a trust and dependency chain and the consequences reachable through that chain.

The importance of consequence-aware assessment is strengthened by industrial cyber-physical research. Zhang et al. [14] identify attacks such as denial of service and deception in cases where compromised communication or estimation can affect control performance. A standard vulnerability score might not do this adequately either. A similar software flaw could have a low consequence when it affects an individual monitoring sensor but a high consequence when it acts on an engineering workstation capable of altering controller logic. Risk ranking in the context of smart manufacturing should therefore integrate technical exploitability with process criticality, safety role, connectivity, privilege, and the difficulty of recovery. This method ensures that limited resources are directed towards the pathways which could lead to intolerable production or safety consequences rather than simply towards those with the greatest number of vulnerabilities.

Lifecycle security represents a continual control gap. Manufacturing environments end up with a number of firmware versions, vendor utilities, certificates, service accounts, and components that are no longer supported. Mugarza et al. [5] show that security issue management and software updates have to be co-ordinated between asset owners, service providers, and product suppliers. The supply-chain aspect extends this responsibility since a manufacturer can inherit risks from embedded libraries, remote diagnostic tools, or third-party updates. Radanliev et al. [4] do likewise stress the importance of cyber risk analytics in the supply chains of Industry 4.0. Resilience demands a reliable pathway from the acquisition of a component through to its commissioning, maintenance, updating, decommissioning, and the preservation of evidence. Supplier assurance must therefore involve security requirements, notification of vulnerabilities, specified supported lifetimes, authenticated updates, controls regarding remote access and recovery support, as well as commercial performance.

The next important factors are identity and segmentation. Rather than relying on a permanent trust based solely on network position, the zero-trust literature stresses the need for explicit verification and access that is limited to what is absolutely necessary [15,16]. In practice this means assigning unique identities to users, services, and devices; treating privileged engineering activities separately; providing vendors with access that is time-limited; and setting up segmented areas with controlled connections. The advantage is that the potential impact of an incident is reduced. For example, if a phishing attack breaches an enterprise account, that identity should not automatically have access to production control. If a gateway is compromised, it should not allow free movement across different cells. Segmentation is most effective when combined with an asset inventory and clear policy ownership, since it is not possible to properly manage an unknown device or an undocumented connection.

Objective evidence artifacts are used to distinguish claimed control presence from verifiable implementation and effectiveness. Examples include an approved critical-asset register, current zone/conduit diagrams, firewall and segmentation test results, privileged-session logs, authenticated-update records, configuration-integrity baselines, protected-backup inventories, successful restoration records and documented recovery-exercise results. These artifacts provide auditable evidence that controls exist and, where outcome testing is available, that they function under relevant OT conditions.

Research into detection is advancing quickly, but operational deployment in OT requires constraints that are often absent from benchmark studies. TON_IoT, Edge-IIoTset, and X-IIoTID provide valuable heterogeneous attack and telemetry datasets [8-10], while deep-learning and pretrained-model studies demonstrate promising detection capability [11,13,28]. In a factory, however, monitoring and response must coexist with legacy protocols, deterministic process timing, limited endpoint resources, continuous availability targets, safety-instrumented systems, and narrow maintenance windows. Passive network monitoring may be preferred where endpoint agents or active interrogation could disturb fragile devices. Detection latency must be assessed against both cyber risk and process response time. Automated containment should be restricted when blocking a route, resetting a controller, or isolating a cell could interrupt a safety function or create an unsafe state. High-consequence actions should therefore use staged response, operator or safety authorization, predefined safe-state logic, and tested rollback. Production acceptance criteria should include false-positive burden, detection coverage of critical pathways, time to triage, missed high-consequence scenarios, and demonstrated operability during normal, maintenance, start-up, and shutdown states rather than laboratory accuracy alone. The two particular weaknesses are dealt with by explainability and distributed learning. Attique et al. [24] have combined deep learning with explainable features so that analysts can examine the important features instead of considering each alert as an opaque score. This is important in plants since an operator may have to make a quick decision as to whether to isolate a line or to keep going with production. Federated methods such as SecureIIoT [17] and the asynchronous model proposed by Bukhari et al. [18] enable sites or edge nodes to take part in model learning without having to centralize all the raw data. While this helps to alleviate concerns regarding privacy and bandwidth, it does introduce new assumptions about trust in the model updates, the quality of the participants, and the possibility of poisoning. As a result, advanced analytics should be included within a controlled monitoring system that has validation, fallback rules, and the authority for human decision-making.

Data integrity is particularly important since smart manufacturing is becoming more and more reliant on analytics and automated decisions. As Toussaint et al. [22] point out, the security requirements for Industry 4.0 data call for frameworks which deal with manipulation, not just the problem of unauthorized disclosure. Sensor data can affect predictive maintenance, quality inspection, energy optimization, and production scheduling. An attacker who makes subtle changes to the data might conceal the occurrence of a destructive failure while gradually deteriorating the quality of the decisions. Integrity controls must therefore include authenticated data sources, protected time synchronization, logging, versioned models, change monitoring, and plausibility checks that link cyber telemetry to process physics. Although blockchain-based methods have been suggested as a means of achieving tamper resistance and decentralized trust [29,30], their use should still be restricted to situations in which the benefits of immutability and multi-party verification make the associated complexity and resource cost worthwhile.

The final aspect is recovery and organizational learning. Cyber-resilience research links prevention with continuity, response, recovery, and adaptation [19-21]. In IIoT, resilience may require controlled degradation to a safe operating state before full recovery; it therefore extends beyond restoration of IT service availability. Recovery extends beyond restoring files: it may require rebuilding trusted controller logic, validating recipes and set-points, re-establishing safe network routes, checking sensor calibration, reconciling production records, revoking supplier credentials, and confirming that persistence has been removed. IIoT forensic readiness supports reliable reconstruction of the incident [23]. Table 1 summarizes major risk pathways and complementary controls. The synthesis supports a chain rather than a single-control model: governance identifies critical outcomes, asset/identity visibility and segmentation reduce exposure, lifecycle practices reduce exploitable weakness, monitoring identifies abnormal behavior, response limits propagation, and tested recovery restores a trusted and safe operating state. The framework recommendation that these controls operate as a loop is an evidence-informed interpretation of these recurring themes, not an empirical claim that the proposed configuration has

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

already demonstrated superior performance in Saudi factories. A trusted operational state is reached only after the integrity of controller logic and configuration, privileged identities, network controls, time synchronization, safety/interlock status and observable process behaviour has been verified against approved baselines.

Table 1. Evidence synthesis of major IIoT risk pathways and resilience controls.

Risk pathway	Typical exposure	Operational consequence	Complementary controls	Residual issue	Evidence basis
Identity / remote-access compromise	Shared credentials, vendor access, weak privilege separation	Unauthorized engineering changes; lateral movement	Unique identities; MFA where feasible; jump access; time-bounded privilege; session logging	Legacy devices and emergency access may require compensating procedures	[15,16]; Saudi access-control context [33,34]
Protocol / network exploitation	Flat zones, insecure services, unmonitored conduits	Loss of view or control; propagation across cells	Segmentation; allow-listed conduits; protocol-aware monitoring; hardened gateways	Deterministic traffic and legacy protocols constrain redesign	[2,3,6,7,12,14,25]
Firmware / software lifecycle failure	Unsupported versions, delayed patches, insecure update path	Persistent compromise; instability; exploitable known flaws	Tested patch process; signed updates; baseline integrity; rollback; supplier SLAs	Safety and availability can delay remediation	[4,5,7,12,22]
Data / model manipulation	Compromised sensors, pipelines, timestamps or analytics	Poor maintenance decisions; quality loss; hidden degradation	Source authentication; integrity monitoring; physics-aware checks; model governance	Subtle attacks may resemble legitimate process variation	[22,24,29,30]
Detection blind spots	Incomplete telemetry, outdated datasets, high false positives	Late containment and larger blast radius	Multi-source monitoring; validated ML; explainability; local baselines	Concept drift and analyst workload remain material	[8-13,17,18,24,26,28]
Recovery / evidence failure	Untested backups, missing logs, unclear authority	Extended downtime; uncertain eradication; repeated compromise	Golden configurations; protected backups; exercises; forensic readiness	Recovery must prove a trusted and safe operating state	[19-21,23]

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

V. PROPOSED SAUDI RISK-BASED CYBER-RESILIENCE FRAMEWORK

The proposed framework translates the synthesis into six dimensions for Saudi smart manufacturing: risk governance and ownership; asset, identity and trust zoning; secure lifecycle and supply-chain assurance; adaptive monitoring and trustworthy analytics; cyber-physical response and recovery; and measurement, workforce and ecosystem learning. The dimensions form a feedback loop rather than a universal maturity checklist. Each informs the next, while incident, exercise, and performance evidence feeds back into governance. The framework is consequence-scaled: a safety-critical controller, production historian, quality sensor, and office printer should not receive identical control investment merely because all are networked. Table 3 compares this integrated model with representative IIoT surveys, Zero Trust research, resilience-management studies, manufacturing cybersecurity guidance, and Saudi OT governance. Differentiation is identified within the selected comparison set through integration and operationalization rather than claims that any individual control is novel. Figure 2 shows the architecture, and Table 4 provides implementation priorities, metrics, and accountable ownership.

Table 3. Differentiation from representative existing approaches.

Approach	Primary coverage	Gap within the selected comparison set	What the proposed framework adds / combines
IIoT security surveys [2,6,7,12]	Threats, requirements, countermeasures, architecture	Broad cataloguing; limited Saudi operational sequencing and ownership	Consequence-scaled integration, accountable owners, metrics, phased implementation
Zero Trust research [15,16]	Explicit verification, least privilege, trust architecture	Trust-centric; does not cover full lifecycle, recovery or industrial learning	Selective OT-adapted trust zoning integrated with lifecycle, recovery and governance
Cyber-resilience management/measurement [19-21]	Leadership, resilience management, measurement	Less specific to IIoT asset/lifecycle/detection mechanisms	Links managerial resilience to IIoT technical controls and plant-operational metrics
Manufacturing/Industry 4.0 cybersecurity guidance [6,22]	Factory security guidance and data-security frameworks	Limited Saudi contextualization and cross-dimension prioritization	Maps evidence to Saudi industrial context and risk-based implementation loop
Saudi NCA ECC/OTCC [33,34]	National governance and OT/ICS cybersecurity requirements	Regulatory control baseline, not a peer-reviewed evidence synthesis or prioritization model	Uses Saudi controls as contextual constraints and connects them to literature-derived dimensions, owners and measurable outcomes

Figure 2. Proposed Saudi risk-based cyber-resilience framework for smart manufacturing. Source: Author's synthesis.

Dimension two combines asset visibility, identity, and trust zoning. Manufacturers should maintain an authoritative inventory linking devices to owners, process functions, software or firmware state, network location, criticality, and approved communication paths. Unknown assets should be treated as a risk signal, not a documentation inconvenience. Human and machine identities should be unique where

feasible, privileged access separated from routine accounts, and remote support time-bounded and monitored. Zero-trust principles [15,16] are applied selectively through segmentation and explicit policy enforcement at meaningful trust boundaries. The objective is to make compromise difficult to propagate. For legacy devices that cannot support modern identity, compensating controls include jump hosts, protocol-aware gateways, unidirectional paths, dedicated cells, and tightly controlled maintenance procedures.

Dimension one establishes risk governance and ownership. Plant leadership should define critical services, intolerable safety and production consequences, cyber-risk tolerance, exception authority, and ownership for high-consequence scenarios. Risk registers should connect technical findings to process impact, recovery difficulty, supplier dependence, and residual-risk decisions rather than rank assets only by vulnerability severity. Governance should also determine who can authorize remote access, production isolation, emergency exceptions, restart, and acceptance of unsupported equipment. This dimension aligns the evidence on resilience leadership and measurement [19-21] with Saudi governance expectations in the Essential Cybersecurity Controls [33]. Its measurable outputs include percentage of critical scenarios with named owners, age of unresolved high-risk exceptions, proportion of crown-jewel processes with tested recovery objectives, and documented executive acceptance of residual risk.

Dimension three covers secure lifecycle and supply-chain assurance. The third-party lifecycle begins with supplier selection and due diligence, continues through procurement, commissioning, maintenance, remote support and software/firmware updates, and ends with secure decommissioning. Contracts should address vulnerability disclosure, support lifetime, firmware/component provenance, shared-account prohibition or controlled exceptions, remote-access authorization, incident notification and remediation obligations. Procurement requirements should specify supported security lifetimes, vulnerability disclosure, authenticated update mechanisms, component provenance, secure default configurations, and responsibilities for remote maintenance. Commissioning should establish a known-good baseline, remove default credentials, record approved firmware, and verify communication paths. During operation, vulnerabilities should be triaged by industrial consequence, and updates tested against safety and process requirements, reflecting maintenance constraints identified by Mugarza et al. [5]. When immediate patching is impossible, the risk register should record compensating measures and an expiry date rather than allow permanent undocumented exceptions. Decommissioning should revoke identities, remove remote access, preserve required evidence, and securely erase sensitive configurations.

Dimension four is adaptive monitoring and trustworthy analytics. Monitoring should combine deterministic rules, asset-aware baselines, network telemetry, endpoint or gateway evidence, and, where useful, machine-learning models. Dataset research shows IIoT attacks can be represented through multiple telemetry sources [8-10], while deep-learning studies show potential for accurate detection [11,13,28]. The framework requires local validation before operational use. Models should be tested on representative plant traffic, including maintenance periods, production transitions, and rare legitimate states. Performance reporting should include false-positive burden, time to triage, and missed high-consequence scenarios, not accuracy alone. Explainable features [24] should be preferred for decisions that may trigger isolation, and federated learning [17,18] should include controls against untrusted participants and poisoned updates.

Dimension five establishes cyber-physical incident response and recovery. Response playbooks must be organised around industrial scenarios rather than generic malware labels. For example, a suspected compromise of an engineering workstation should define who can restrict remote access, how controller changes are validated, what evidence is preserved, when production can continue safely, and who authorises restart. Recovery assets should include offline or protected backups of configurations, controller logic, recipes, certificates, and golden images where applicable. Exercises should test

degraded modes and manual alternatives, not just communication chains. Recovery time objectives should reflect the process and supply commitments of each line. Forensic readiness [23] should be integrated so containment does not destroy evidence needed to confirm root cause and eradicate persistence. For this framework, "trusted operational state" means a verifiable post-recovery condition in which controller logic and configurations match approved baselines, privileged identities and credentials have been validated or rotated as required, network controls and time synchronization are correct, safety/interlock functions are confirmed, and process behaviour is within expected engineering limits.

Dimension six turns resilience into a measurable learning system. Kott and Linkov [21] argue that measurement is the basis for improvement, and that principle is critical when plants have different maturity levels. Metrics should include coverage and outcome indicators: percentage of critical assets with confirmed owners; percentage of privileged sessions recorded; unsupported assets with approved compensating controls; mean time to detect and contain high-risk events; proportion of critical configurations recoverable from tested backups; exercise success rate; supplier remediation time; and recurring alert causes eliminated. Operations and security should review metrics because a control that improves a cyber metric while degrading production reliability can create new risk. Trends are more valuable than isolated scores.

The framework also supports differentiated implementation across Saudi industry. A greenfield facility can embed secure identities, segmented architecture, telemetry and update support into design requirements before commissioning. A brownfield plant may begin with asset discovery, critical-path mapping, monitored jump access, compensating segmentation and recovery testing while gradually replacing unsupported equipment. A multi-site manufacturer can establish common governance and metrics while allowing site-specific control profiles. Saudi research on IIoT security and anomaly detection [12,13,25,26,28] provides a useful local technical base, while Industry 4.0 localisation research [27] emphasises the strategic importance of domestic capability. The framework therefore treats workforce development, supplier expectations and knowledge transfer as resilience controls rather than peripheral training activities.

Implementation should be phased using an explicit prioritization model rather than informal judgment alone. For each asset, pathway, or risk scenario, the framework proposes a locally calibrated 1-5 score for seven factors: production criticality (20%), safety impact (20%), exposure or remote-access reachability (15%), dependency/propagation potential (15%), exploitability (10%), asset age/support status (10%), and recovery-time difficulty relative to the required RTO (10%), assessed separately from recovery testing status. The weighted priority score is the sum of each rating multiplied by its weight; scores at or above 4.0 are candidate Phase-1 priorities, 3.0-3.99 are Phase-2, and lower scores are scheduled according to residual risk and dependencies. These weights and thresholds are illustrative and require validation against local risk appetite and incident history. Phase 1, owned by plant leadership with cyber risk and operations, establishes crown-jewel processes, critical pathways, unsupported assets, and recovery gaps; completion evidence includes approved risk scenarios, asset ownership, and tested RTOs. Phase 2, owned by OT engineering, network/security, and asset owners, closes high-consequence trust gaps through segmentation, privileged-access controls, backup validation, and controlled vendor access; evidence includes verified zone/conduit rules, recorded privileged sessions, and restore tests. Phase 3, owned by SOC/OT monitoring and data/AI owners, expands telemetry and analytics after trustworthy baselines exist; evidence includes site-validation results, false-positive targets, and model-governance records. Phase 4, owned by executive/site governance with procurement, safety, and suppliers, institutionalizes exercises, supplier assurance, cross-site learning, and continuous measurement; evidence includes exercise closure, supplier remediation metrics, and reviewed trend reports.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

Table 4. Framework implementation priorities, metrics and accountable ownership.

Dimension	Priority actions	Example metrics	Primary ownership
1. Risk governance	Define critical services, scenarios, tolerance and exception approval	High-risk scenarios with owners; overdue exceptions; residual-risk decisions reviewed	Plant leadership + cyber risk + operations
2. Asset / identity / zoning	Inventory, privilege separation, vendor access, segmented trust boundaries	Critical asset coverage; privileged sessions monitored; unknown assets; blocked unauthorized paths	OT engineering + network/security
3. Lifecycle / supply chain	Secure procurement, baseline, patch testing, vulnerability and supplier obligations	Unsupported assets; patch exposure days; supplier remediation time; signed-update coverage	Asset owner + procurement + vendors
4. Monitoring / analytics	Multi-source telemetry, plant validation, explainability, model governance	Detection coverage; false-positive burden; mean triage time; high-consequence misses	SOC/OT monitoring + data/AI owners
5. Response / recovery	Scenario playbooks, protected backups, safe isolation, forensic readiness, exercises	Mean containment time; tested restore rate; RTO attainment; exercise findings closed	Incident response + operations + safety
6. Measurement / learning	Trend metrics, workforce exercises, supplier learning, cross-site lessons	Repeat incident causes; training/exercise completion; maturity trend; control effectiveness	Executive sponsor + site governance

VI. DISCUSSION: IMPLICATIONS, LIMITATIONS AND RESEARCH AGENDA

The framework has three practical management implications, each of which can be expressed as a measurable decision. First, resilience investment should be tied to expected operational loss rather than tool adoption: management can prioritize scenarios using expected downtime, safety consequence, production value at risk, critical-process availability, and required recovery time. A proposed control should therefore show which high-consequence pathway it reduces and how the residual risk changes. Second, advanced analytics should be funded only after minimum visibility, access, and recovery prerequisites are met; acceptance criteria should include critical-asset telemetry coverage, false-positive burden, mean time to triage, mean time to contain, and the percentage of critical configurations restored successfully in exercises. Third, supplier and lifecycle risk should be managed as operational performance: procurement and plant leadership can monitor unsupported-asset exposure days, time to remediate supplier vulnerabilities, percentage of remote vendor sessions controlled and recorded, signed-update coverage, and exceptions past their approved expiry. These measures make cybersecurity investment reviewable alongside reliability, maintenance, safety, and continuity rather than as a separate technology budget. The research agenda should now test the conceptual framework rather than continue adding controls without validation. A first study should use a Delphi panel of Saudi OT engineers, cybersecurity leaders, safety specialists, plant managers, and suppliers to assess the relevance, completeness, and weighting of the six dimensions and the proposed prioritization factors. A second stream should apply the scoring model to at least one greenfield and one brownfield Saudi manufacturing case and compare predicted priorities with expert risk judgments. A third should use controlled cyber ranges or digital twins to simulate identity compromise, firmware/update compromise, data manipulation, and supplier remote-access scenarios, measuring time to detect, safe containment, process deviation, recovery time, and evidence completeness. A fourth should conduct longitudinal plant measurement to test whether improvements in coverage indicators are associated with reduced vulnerability exposure, faster containment, more reliable restoration, and lower production loss. Several proposed metrics require

local baselines before they can be treated as KPIs, particularly false-positive burden by operating state, normal containment time for high-risk incidents, acceptable supplier remediation time, restore success for critical configurations, and the relationship between resilience scores and actual downtime. These studies would provide the empirical basis needed to calibrate thresholds and determine whether the framework improves operational outcomes.

Illustrative end-to-end manufacturing scenario. Consider a brownfield production line in which a remote vendor account is compromised and used to reach an engineering workstation. The visibility stage identifies the workstation, controller dependencies and remote-support path as high-consequence assets; governance assigns the OT owner and restart authority; protection enforces time-bounded vendor access, jump-host control and segmented conduits; detection correlates privileged-session activity, engineering changes and process telemetry; response revokes vendor access and places the affected line in a predefined safe degraded state; recovery restores approved controller logic and validates identities, network rules, interlocks, time synchronization and process behaviour before restart. Evidence artifacts include the access approval, session recording, zone/conduit test, configuration hash, backup-restore result and exercise/incident record. The scenario illustrates how the six dimensions operate as one consequence-scaled loop rather than as independent controls.

This review has several limitations. The 30-study scholarly corpus is deliberately focused and DOI-based, so it may exclude relevant non-DOI studies and introduces database-coverage and publication-selection bias. Screening and thematic coding were conducted by a single reviewer during revision, which can introduce judgment bias; no inter-rater reliability statistic is therefore reported. The English-language restriction may also omit relevant Arabic or other non-English evidence. The original database-export log was unavailable, preventing defensible reconstruction of PRISMA-style record-flow counts. To address the mismatch between Saudi-specific claims and a peer-reviewed-only corpus, the revision adds a separate contextual/regulatory evidence layer comprising Vision 2030/industrial-policy sources and NCA cybersecurity controls [31-34] where applicable and within the organization's regulatory scope; these documents inform contextual adaptation but are not counted as peer-reviewed evidence of control effectiveness. Some regulatory or contextual webpages were re-verified after the 2020–2025 scholarly window; their later webpage update dates are reported as source metadata and do not expand the scholarly inclusion period. The heterogeneous study designs prevent pooled effect estimation, and the proposed framework remains conceptual. It has not been validated through real Saudi factory deployments, structured expert consensus, or comparative outcome studies. Future work should therefore test greenfield, brownfield, and multi-site applications across manufacturing subsectors and combine technical telemetry with interviews and exercise/incident data.

VII. CONCLUSION

The reviewed evidence indicates that IIoT-enabled manufacturing exposes interconnected cyber-physical pathways in which failures of identity, software lifecycle, trust boundaries, data integrity, monitoring, or recovery can affect availability, production continuity, quality, and safety. Across the reviewed studies, no single technical mechanism addresses the full lifecycle of industrial cyber risk. The literature instead supports complementary capabilities spanning governance, asset and identity visibility, segmented trust, secure lifecycle practices, context-aware detection, recoverability, and measurement. Saudi policy and regulatory sources further establish a national context in which industrial digitalization, OT protection, resilience, and accountable cybersecurity governance are relevant implementation requirements [31-34].

Based on that synthesis, this paper recommends a six-dimension, consequence-scaled conceptual framework for greenfield, brownfield, and multi-site Saudi manufacturers. The framework operationalizes existing evidence by linking controls to ownership, OT constraints, residual-risk decisions, measurable outcomes, and phased implementation priorities; it does not claim that the constituent controls are

individually novel or that the integrated model has already proved effective. Its principal proposition is that cybersecurity investment should be scaled to the industrial consequences and propagation potential of each scenario while preserving safe and recoverable operation. Effectiveness remains to be validated through real-world Saudi manufacturing deployments, structured expert assessment, case-study comparison, simulated attack exercises, and longitudinal measurement of containment, recovery, and production-impact outcomes.

VIII. SUPPLEMENTARY IMPLEMENTATION AND AUDIT MATERIAL

Supplementary Table S1. Revision-stage search protocol (17 September 2026).

Platform / source	Searched fields	Query set	Date filter	Language / type	Records retrieved	Screening counts	Final use
IEEE Xplore	Title/abstract/keywords where supported	S1-S3 adapted to platform syntax	2020-2025	English; peer-reviewed	Not reconstructed	Not reconstructed	Eligible studies retained in 30-study corpus
ScienceDirect	Title/abstract/keywords where supported	S1-S3 adapted to platform syntax	2020-2025	English; peer-reviewed	Not reconstructed	Not reconstructed	Eligible studies retained in 30-study corpus
SpringerLink	Title/abstract/keywords/full-text search interface	S1-S3 adapted to platform syntax	2020-2025	English; peer-reviewed	Not reconstructed	Not reconstructed	Eligible studies retained in 30-study corpus
Wiley Online Library	Title/abstract/keywords where supported	S1-S3 adapted to platform syntax	2020-2025	English; peer-reviewed	Not reconstructed	Not reconstructed	Eligible studies retained in 30-study corpus
Publisher/ DOI records	Bibliographic metadata and DOI landing pages	Reference-by-reference verification	No corpus expansion	Published record verification	N/A	N/A	Metadata, DOI and article-type verification
Google Scholar	Supplementary citation discovery only	Backward/forward citation checks	2020-2025 for scholarly additions	English; scholarly discovery	Not reconstructed	Not reconstructed	Supplementary discovery; not treated as a primary database

Historical record-flow counts are intentionally reported as “Not reconstructed” because the original export log is unavailable; no retrospective PRISMA counts were fabricated.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

Supplementary Table S2. Six-dimension coding traceability for the 30-study scholarly corpus.

Ref.	Evidence type	Primary inclusion rationale	Principal dimension(s)	Resilience phase	Key contribution used in synthesis
1	Review	Direct IIoT security/standards relevance	2,3	Anticipate/Protect	IIoT security, privacy and standards requirements
2	Systematic survey	IIoT security requirements and fog opportunities	2,4	Anticipate/Protect/Detect	Layered IIoT threat and control requirements
3	Survey	IoT/IIoT attacks and security mechanisms	2,4	Anticipate/Protect	Attack paths and countermeasure landscape
4	Review/framework	Industry 4.0 supply-chain cyber risk	1,3	Anticipate/Protect	Supply-chain and edge cyber-risk analytics
5	Empirical/lifecycle study	IIoT software-update and safety constraints	3	Protect/Recover	Secure update and maintenance constraints
6	Review	Manufacturing cybersecurity guidance	1,2,3	Anticipate/Protect	Factory-oriented security guidance
7	Survey	IIoT technologies, countermeasures and challenges	2,3,4	Protect/Detect	Security requirements and operational challenges
8	Dataset paper	IIoT intrusion-detection dataset	4	Detect	Heterogeneous telemetry for detection research
9	Dataset paper	IoT/IIoT centralized/federated dataset	4	Detect	Dataset support for centralized/federated detection
10	Dataset paper	Industrial intrusion dataset	4	Detect	Device/connectivity-agnostic IIoT attack data
11	Empirical ML study	IIoT intrusion detection	4	Detect	Lightweight deep-learning detection evidence
12	Survey	IIoT security/AI/edge opportunities	2,4	Anticipate/Detect	Threats, AI security and edge opportunities
13	Empirical ML study	Industrial intrusion detection	4	Detect	Deep-learning detection in IIoT
14	Survey/control study	Industrial cyber-physical attack detection/control	2,5	Detect/Respond	DoS/deception attack effects and control implications

15	Review	Zero Trust migration	2	Protect	Explicit verification and least privilege
16	Survey	Zero Trust architecture	2	Protect	Trust architecture and implementation challenges
17	Empirical federated-learning study	IIoT privacy/security detection	4	Detect	Federated learning for IIoT security
18	Empirical federated-learning study	Edge-IIoT asynchronous detection	4	Detect	Distributed detection with edge constraints
19	Management study	Cyber-resilient systems management	1,5,6	Anticipate/Recover/Adapt	Managerial actions and context for resilience
20	Leadership study	Digital-enterprise cyber resilience	1,6	Anticipate/Adapt	Leadership, integration and culture
21	Measurement perspective	Cyber-resilience measurement	1,6	Adapt	Measurement as basis for resilience improvement
22	Framework review	Industry 4.0 data security	3,4	Protect/Detect	Integrity and cybersecurity framework requirements
23	Peer-reviewed survey	IIoT security and digital forensics	5,6	Respond/Recover/Adapt	Forensic readiness, security and evidence challenges
24	Empirical XAI study	Explainable IIoT attack detection	4	Detect	Explainability for industrial detection
25	Review	IIoT cyber security and privacy	2,4	Protect/Detect	IIoT threats and privacy/security issues
26	Empirical anomaly-detection study	Fog-to-things IIoT detection	4	Detect	Anomaly detection in industrial fog environments
27	Saudi empirical/context study	Saudi Industry 4.0 localization	6	Adapt	Saudi localized manufacturing capability context
28	Empirical ML study	Edge-IIoT attack detection	4	Detect	Pretrained-model detection evidence
29	Survey	Blockchain for IoT/IIoT	3,4	Protect	Distributed trust and tamper-resistance options
30	Systematic review	Blockchain for IoT security/trust	3,4	Protect	Systematic evidence on blockchain security/trust

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

Supplementary Table S3. Author-proposed five-level maturity model.

Level	Observable characteristics across the six dimensions	Interpretation
1 – Initial	Incomplete asset visibility; ad hoc ownership; reactive controls; untested recovery; limited metrics.	Control presence and recovery capability are inconsistent.
2 – Managed	Critical assets identified; basic ownership and segmentation; backup procedures defined; selected monitoring and exercises.	Priority risks are managed but not consistently integrated.
3 – Defined	Documented lifecycle, trust zoning, supplier requirements, playbooks, evidence artifacts and common metrics across sites.	Processes are repeatable and governed.
4 – Resilient	High-consequence scenarios are exercised; safe degradation and trusted restoration are demonstrated; metrics influence risk decisions.	Operational resilience is evidenced, not only documented.
5 – Adaptive	Cross-site learning, drift monitoring, supplier feedback, trend-based thresholds and continuous control optimization are institutionalized.	Evidence and incidents continuously adapt the resilience system.

This maturity model is an author-proposed analytical aid and is not an NCA maturity standard, rating scale or endorsement.

Supplementary Table S4. Seven-factor risk-prioritization scoring rubric.

Factor	Weight	1	2	3	4	5
Production criticality	20%	Negligible production effect	Local minor delay	Material line degradation	Major line/site interruption	Plant/mission-critical interruption
Safety impact	20%	No credible safety effect	Minor reversible exposure	Potential recordable injury/process upset	Serious injury or major hazard potential	Catastrophic/fatal or major HSE consequence
Exposure / reachability	15%	Isolated/no remote path	Tightly local access	Controlled routed access	Frequent remote/enterprise path	Internet/external or broadly reachable path
Dependency / propagation	15%	Standalone	Few local dependencies	Multiple cell dependencies	Cross-line/site dependencies	Enterprise/multi-site or cascading dependency
Exploitability	10%	Highly impractical	Difficult/specialized	Feasible with prerequisites	Readily exploitable	Known active/easy exploitation path
Age / support status	10%	Current and fully supported	Supported with minor constraints	Aging/limited support	Near end-of-support	Unsupported/obsolete
Recovery-time difficulty vs RTO	10%	Recovery comfortably within RTO	Within RTO with margin	Near RTO	Likely exceeds RTO	No tested recovery or far exceeds RTO

Score directionality is increasing risk/priority from 1 to 5. The weighted score equals Σ(rating × weight). Illustrative thresholds are ≥4.0 for Phase 1 and 3.0–3.99 for Phase 2 because they separate scenarios with

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723366

consistently high consequence/exposure from mid-range scenarios; all weights and thresholds require local calibration against plant risk appetite, incident history and expert validation before operational use.

Supplementary Table S5. Metric dictionary for resilience assurance.

Metric	Formula / definition	Data source	Frequency	Owner	Target logic	Limitation
MTTD	Mean time from detectable event onset to validated detection	SOC/OT monitoring timestamps	Monthly/quarterly	SOC/OT monitoring	Trend downward by risk class	Event onset may be uncertain
Mean time to contain	Mean time from validated detection to effective containment	Incident records and OT logs	Per incident; quarterly trend	Incident response + operations	Trend downward without unsafe actions	Containment definition varies by scenario
Tested recovery rate	Critical configurations successfully restored / critical configurations tested × 100	Backup/restore exercise records	Quarterly/semi-annual	Operations + OT engineering	Increase toward complete tested coverage	Successful restore does not alone prove safe process state
RTO attainment	Recovery exercises/incidents meeting approved RTO / total tested × 100	BC/DR and exercise records	Quarterly	Operations + continuity owner	Meet risk-approved service targets	RTO may need revision as process changes
Critical-asset visibility	Critical assets with confirmed owner, location, firmware/software state and dependency map / total critical assets × 100	Asset register/CMDB	Monthly	OT engineering	Sustain near-complete verified coverage	Inventory accuracy depends on discovery and reconciliation
Privileged-access monitoring coverage	Recorded privileged sessions / privileged sessions requiring recording × 100	PAM/jump-host logs	Monthly	IAM/security + OT	Increase to policy-required coverage	Emergency access may require documented exceptions
High-consequence detection misses	Number of exercised/known high-consequence scenarios not detected within required window	Exercise results, incident reviews	Per exercise/incident; quarterly	SOC/OT monitoring	Drive toward zero; investigate each miss	Requires representative scenarios

Exercise success	Exercise objectives achieved / total objectives × 100	Exercise reports	Per exercise	Site governance + safety	Trend upward with closure of findings	Success may be overstated without objective acceptance criteria
Control effectiveness	Controls meeting predefined operational test criteria / controls tested × 100	Assurance test evidence	Quarterly/semi-annual	Cyber risk + control owners	Improve by criticality tier	Test scope and criteria can differ across controls

REFERENCES

[1] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020, doi: 10.1109/ACCESS.2020.3016937. Crossref

[2] K. P. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020, doi: 10.1109/COMST.2020.3011208. Crossref

[3] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, Art. no. 102481, 2020, doi: 10.1016/j.jnca.2019.102481. Crossref

[4] P. Radanliev, D. De Roure, K. Page, J. R. C. Nurse, R. M. Montalvo, O. Santos, L. Maddox, and P. Burnap, "Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 3, Art. no. 13, 2020, doi: 10.1186/s42400-020-00052-8. Crossref

[5] I. Mugarza, J. L. Flores, and J. L. Montero, "Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era," *Sensors*, vol. 20, no. 24, Art. no. 7160, 2020, doi: 10.3390/s20247160. MDPI

[6] V. Mullet, P. Sondi, and E. Ramat, "A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0," *IEEE Access*, vol. 9, pp. 23235–23263, 2021, doi: 10.1109/ACCESS.2021.3056650. Crossref

[7] S. F. Tan and A. Samsudin, "Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey," *Sensors*, vol. 21, no. 19, Art. no. 6647, 2021, doi: 10.3390/s21196647. MDPI

[8] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862. Crossref

[9] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809. Crossref

[10] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-IIoTID: A Connectivity-Agnostic and Device-Agnostic Intrusion Data Set for Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3962–3977, 2022, doi: 10.1109/JIOT.2021.3102056. Crossref

[11] R. V. Mendonca, J. C. Silva, R. L. Rosa, M. Saadi, D. Z. Rodriguez, and A. Farouk, "A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms," *Expert Systems*, vol. 39, no. 5, Art. no. e12917, 2022, doi: 10.1111/exsy.12917. Wiley

[12] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," *Sensors*, vol. 23, no. 17, Art. no. 7470, 2023, doi: 10.3390/s23177470. MDPI

[13] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things," *Alexandria Engineering Journal*, vol. 81, pp. 371–383, 2023, doi: 10.1016/j.aej.2023.09.023. Crossref

[14] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber-physical systems," *ISA Transactions*, vol. 116, pp. 1–16, 2021, doi: 10.1016/j.isatra.2021.01.036. Crossref

[15] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges," *Security and Communication Networks*, vol. 2021, Art. no. 9947347, 2021, doi: 10.1155/2021/9947347. Crossref

[16] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679. Crossref

[17] A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J. H. Park, "SecureIIoT Environment: Federated Learning Empowered Approach for Securing IIoT from Data Breach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6406–6414, 2022, doi: 10.1109/TII.2022.3149902. Crossref

[18] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, Z. Qadir, S. K. R. Moosavi, and F. Sanfilippo, "Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model," *Internet of Things*, vol. 27, Art. no. 101252, 2024, doi: 10.1016/j.iot.2024.101252. Crossref

[19] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Computers & Industrial Engineering*, vol. 149, Art. no. 106829, 2020, doi: 10.1016/j.cie.2020.106829. Crossref

[20] J. Loonam, J. Zwiegelaar, V. Kumar, and C. Booth, "Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3757–3770, 2022, doi: 10.1109/TEM.2020.2996175. Crossref

[21] A. Kott and I. Linkov, "To Improve Cyber Resilience, Measure It," *Computer*, vol. 54, no. 2, pp. 80–85, 2021, doi: 10.1109/MC.2020.3038411. Crossref

[22] M. Toussaint, S. Krima, and H. Panetto, "Industry 4.0 data security: A cybersecurity frameworks review," *Journal of Industrial Information Integration*, vol. 39, Art. no. 100604, 2024, doi: 10.1016/j.jii.2024.100604. Crossref

[23] V. R. Kebande and A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 5, Art. no. 131, pp. 1–37, 2024, doi: 10.1145/3635030. ACM

[24] D. Attique, W. Hao, W. Ping, D. Javeed, and P. Kumar, "Explainable and Data-Efficient Deep Learning for Enhanced Attack Detection in IIoT Ecosystem," *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 38976–38986, 2024, doi: 10.1109/JIOT.2024.3384374. IEEE

[25] N. Z. Jhanjhi, M. Humayun, and S. N. Almuayqil, "Cyber Security and Privacy Issues in Industrial Internet of Things," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 361–380, 2021, doi: 10.32604/csse.2021.015206. Tech Science Press

[26] T. Alatawi and A. Aljuhani, "Anomaly Detection Framework in Fog-to-Things Communication for Industrial Internet of Things," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 1067–

1086, 2022, doi: 10.32604/cmc.2022.029283. Crossref

[27] A. A. Aljuaid, S. A. Masood, and J. A. Tipu, "Integrating Industry 4.0 for Sustainable Localized Manufacturing to Support Saudi Vision 2030: An Assessment of the Saudi Arabian Automotive Industry Model," *Sustainability*, vol. 16, no. 12, Art. no. 5096, 2024, doi: 10.3390/su16125096. MDPI

[28] A. Alablani and M. J. F. Alenazi, "Robust Attack Detection Framework Using Pretrained CNN Model for the Edge Industrial IoT Networks," *Concurrency and Computation: Practice and Experience*, vol. 37, Art. no. e70206, 2025, doi: 10.1002/cpe.70206. Wiley

[29] I. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey," *Security and Communication Networks*, vol. 2021, Art. no. 7142048, 2021.

[30] S. Almarri and A. Aljughaiman, "Blockchain Technology for IoT Security and Trust: A Comprehensive Systematic Literature Review," *Sustainability*, vol. 16, no. 23, Art. no. 10177, 2024, doi: 10.3390/su162310177. MDPI

[31] Saudi Vision 2030, "Vision 2030 and Vision Realization Programs," Official Government Portal. Accessed: Sep. 17, 2026. Saudi Vision 2030

[32] Saudi Vision 2030, *National Industrial Development and Logistics Program Delivery Plan 2021–2025*. Kingdom of Saudi Arabia, 2021. Saudi Vision 2030

[33] National Cybersecurity Authority, *Essential Cybersecurity Controls (ECC 2-2024)*. Kingdom of Saudi Arabia, 2024. NCA

[34] National Cybersecurity Authority, *Operational Technology Cybersecurity Controls (OTCC-1:2022)*. Kingdom of Saudi Arabia, 2022. NCA

[35] National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3. NIST

[36] International Electrotechnical Commission, "IEC 62443 Series: Security for Industrial Automation and Control Systems." IEC