computers

MDPI

Review

Cybersecurity Requirements and Certification Standards in Industrial Automation Systems: A Systematic Review

Said Zulfigarzada [1], Aysun Gadirli [2], Javid Karimov [3], Danas Cerneckas [1], Roma Rackiene [1] and Mindaugas Azubalis [1,*]

[1] Department of Electrical and Power Systems, Faculty of Electrical and Electronics Engineering, Kaunas University of Technology, Studentu St. 48, 51367 Kaunas, Lithuania; said.zulfigarzada@gmail.com (S.Z.); danas.cerneckas@ktu.lt (D.C.); roma.rackiene@ktu.lt (R.R.)
[2] Department of Applied Informatics, Faculty of Informatics, Kaunas University of Technology, Studentų St. 50, 51368 Kaunas, Lithuania; aysun.gadirli@gmail.com
[3] Laboratory of Nuclear Installation Safety, Lithuanian Energy Institute, Breslaujos St. 3, 44403 Kaunas, Lithuania; javid.karimov@lei.lt
* Correspondence: mindaugas.azubalis@ktu.lt; Tel.: +370-67676790

Abstract

Industrial automation systems are increasingly cyber-physical, interconnected, and software-dependent, which expands both their operational capability and their cybersecurity exposure. This article reports a systematic literature review, conducted following the PRISMA 2020 guidelines, of cybersecurity requirements and certification standards in industrial automation, with emphasis on Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs), and Industry 4.0 contexts. From 3570 records identified across five academic databases, 75 studies were retained after duplicate removal, title and abstract screening, and full-text eligibility assessment. The included studies were analyzed along three dimensions: cybersecurity requirements, standards and certification, and application context. Quantitative synthesis shows that network segmentation, intrusion detection, secure communication, access control, lifecycle security, and safety–security coordination are the six most frequently emphasized requirement categories, and that ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-82, and NERC-CIP are the four dominant certification frameworks. The review identifies four critical gaps between technical cybersecurity requirements and certification practice and proposes an integrated mapping framework linking requirement categories, standards, and application contexts. The findings indicate that effective industrial cybersecurity assurance depends on a layered compliance architecture rather than on dependence on any single framework.

Keywords: industrial automation; cybersecurity requirements; certification standards; IEC 62443

Academic Editor: Leandros Maglaras

Received: 28 April 2026
Revised: 1 June 2026
Accepted: 2 June 2026
Published: 4 June 2026

1. Introduction

Industrial automation systems are undergoing deep digital transformation. Environments once built around isolated programmable controllers and deterministic communication structures are now connected to enterprise platforms, cloud and edge services, distributed sensors, and intelligent analytics. In manufacturing, this transformation is most often framed through Industry 4.0, which links industrial performance to connectivity, data exchange, and adaptive production [1]. The same transition has been linked to sustainability

and resource-efficiency goals, indicating that industrial digitalization is both a technical and a strategic shift [2]. Industrial Artificial Intelligence extends this trajectory by enabling predictive, learning-based decision support beyond rule-based automation [3], while flexible robotic platforms such as mobile manipulators illustrate the parallel evolution of physical industrial assets [4].

The transformation is not limited to equipment. Human-centered concepts such as Operator 4.0 and the emerging Operator 5.0 describe production environments in which workers collaborate with cyber-physical systems and digitally supported processes [5]. Similar shifts are visible in process-heavy sectors such as mining, where intelligent control and predictive analytics are increasingly tied to competitiveness and operational continuity [6]. Together, these developments mean that industrial automation systems are more networked, more intelligent, and more deeply embedded in interdependent production settings—and, as a direct consequence, more exposed to cybersecurity risk.

The cybersecurity problem arises because digitalization expands capability and vulnerability simultaneously. As industrial environments incorporate larger numbers of connected devices, gateways, and remote interfaces, they become part of broader cyber ecosystems rather than bounded control domains. The general IoT literature has long emphasized that this scale and heterogeneity make conventional perimeter-based assumptions inadequate [7,8]. The Industrial IoT (IIoT) extends this challenge to operationally significant devices whose compromise may affect continuity, quality, safety, and physical processes [9], and the fusion of IIoT with edge and fog paradigms introduces additional trust boundaries and attack surfaces between field devices and higher-level services [10].

A central reason why these issues are so important is that industrial automation systems increasingly function as cyber-physical systems. In such systems, computation, communication, sensing, and control are directly coupled with physical processes, which means that cyber events may produce immediate real-world effects. Recent CPS security surveys define these environments as intelligent systems that bridge cyberspace and the physical world and that play an important role in critical and safety-relevant domains [11]. When this perspective is narrowed specifically to industrial cyber-physical systems, the implications become even clearer: industrial CPS security must account not only for confidentiality and access control, but also for integrity, availability, timing, reliability, resilience, and the operational constraints of real processes [12]. Unlike many enterprise IT environments, industrial systems cannot tolerate prolonged downtime, uncontrolled latency, or careless patching practices. They are frequently composed of legacy components, proprietary protocols, resource-constrained devices, and long-lifecycle assets, all of which complicate the application of conventional security models.

These cyber-physical properties make industrial cybersecurity separate from critical infrastructure protection. Industrial automation technologies are currently the backbone of important fields like utilities, smart grids, electric power, building management, logistics, and industrial services. In smart-grid studies, enhanced automation and communication capabilities are consistently associated with improved monitoring, reliability, and decision-making. However, these advanced digital characteristics also introduce new risks and security constraints [13]. In smart-building research, similar patterns emerge, as IoT-driven building management enhances energy efficiency, predictive maintenance, sustainability, and occupant comfort, while concurrently posing problems regarding interoperability, cybersecurity, and data privacy [14]. Research on building automation security makes this worry even more real by showing that cyber-physical risks in building automation systems can affect things like Heating, Ventilation, and Air Conditioning (HVAC), lighting, access control, and other operational services, especially when old assumptions and weak protection mechanisms are still in place [15]. Further research on green building manage-

ment systems supports the idea that sustainable infrastructure cannot be assumed to be secure; instead, cybersecurity must be integrated directly into the protection of digitally managed building assets and services [16]. These examples matter because they highlight that industrial automation cybersecurity is not confined to plant floors. It spans across energy, facilities, utilities, and other infrastructures whose disruption may have broader economic and societal effects.

The same principle applies to industrial safety and operational trust. As artificial intelligence (AI) and smart technologies are integrated into safety management across several industries, they facilitate enhanced monitoring, compliance, and decision support; yet, they also engender a heightened reliance on reliable digital functionalities [17]. In highly automated settings, unsafe data flows, corrupted control logic, or distorted analytics can harm both production outputs and the technologies that are meant to make things safer and more resilient. This is one reason why industrial cybersecurity cannot be reduced to a small technical concern. It is also a governance, assurance, and systems-engineering problem that requires alignment between operational needs, human aspects, technical structures, and institutional controls.

From this perspective, the challenge of certification becomes important. The rapid expansion of interconnected industrial systems has made it more important than ever to have defined cybersecurity requirements, formal assurance processes, and standards that can help with implementation and show that something is safe. But the standards landscape is still not very clear. An examination of security standards and frameworks for IoT-enabled smart environments reveals that numerous traditional standards and evaluation frameworks provide valuable foundations, yet fail to comprehensively meet the requirements of highly interconnected, diverse, and resource-limited operational settings [18]. This insight pertains directly to industrial automation. Industrial systems bring together Information Technology (IT) and Operational Technology (OT) assets, old and new technology, local and remote services, and varied levels of criticality all in one place. Consequently, certification is not simply a matter of assessing whether a generic set of controls has been deployed. It demands a deeper understanding of which cybersecurity requirements are most critical in industrial situations, how those requirements map to applicable standards, and where implementation gaps persist. The challenge is worsened by the special reality of ICSs. Industrial automation in manufacturing, energy, water, and transportation services is built on ICS, SCADA, distributed control, and PLC-based settings. Recent literature indicates that the integration of ICS with the IoT and networked architecture has significantly broadened the threat landscape, rendering industrial environments vulnerable to protocol-level deficiencies, malware, spoofing, denial-of-service attacks, advanced persistent threats, and various other complex attack vectors [19]. This same body of work also points out a second problem: it is often difficult to apply standard cybersecurity frameworks effectively in ICS environments because of old architecture, real-time requirements, proprietary communication methods, and the fact that industrial processes are very sensitive to changes [19]. These circumstances are exactly what make certification complexity such a big issue. A requirement that appears basic at the level of a standard may become technically demanding or operationally dangerous when translated into a real industrial context. Likewise, a control that is effective in one sector may be infeasible in another because of latency limits, interoperability concerns, or safety consequences.

Accordingly, the primary problem addressed in this research is not only that cyber dangers exist in industrial automation. Instead, industrial automation today works in a digital and cyber-physical world where cybersecurity requirements need to be more clearly defined, and certification standards need to be looked at more closely. Across this literature, three converging themes are visible. First, the same digitalization that drives industrial

performance also widens the cyber-attack surface, regardless of whether the setting is manufacturing, energy, buildings, or process industries [1–6,13–16]. Second, the cyber-physical coupling of modern industrial systems makes their security qualitatively different from enterprise IT security: integrity, availability, timing, and safety are inseparable from confidentiality, and legacy assets, real-time constraints, and proprietary protocols constrain which controls are operationally feasible [9–12,17]. Third, certification and standardization practice has not yet caught up with the pace of technical change, and frameworks designed for hierarchical or enterprise contexts must increasingly be adapted to distributed, IIoT-driven environments [18,19]. These convergences justify a focused systematic review of cybersecurity requirements and certification standards in industrial automation, and they frame the research questions stated at the end of this section.

To guide the review, the following research questions were formulated:

1. Which cybersecurity requirements are most frequently emphasized in the literature on industrial automation systems?
2. Which certification standards and frameworks dominate the field, and how do they compare in terms of scope, strengths, and limitations?
3. What gaps exist between technical cybersecurity requirements and certification practices?
4. How can cybersecurity requirements, certification standards, and application contexts be integrated into a coherent classification framework that supports both research and practice?

This study makes the following contributions:

- It proposes a structured classification framework linking cybersecurity requirements, certification standards, and industrial application contexts.
- It provides a comparative analysis of major cybersecurity standards in industrial automation environments.
- It identifies critical gaps between technical cybersecurity requirements and certification practices.
- It introduces a visual mapping model to support understanding of how security controls are operationalized across standards and domains.

2. Methodology

This study was produced as a systematic literature review to examine cybersecurity needs and certification criteria in industrial automation systems. The methodological approach was designed to make sure that it was clear, repeatable, and rigorous, following the logic that is usually used in high-quality review articles: defining the scope, doing a systematic database search, making the eligibility criteria clear, doing a multi-stage screening, structuring the data extraction, and classifying the final body of evidence by theme.

The review was designed and reported in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines. The four PRISMA stages—identification, screening, eligibility, and inclusion—were applied sequentially and are visualized in Figure 1. PRISMA was chosen because it provides a transparent and widely adopted reporting framework for systematic reviews in engineering and applied informatics, and because its flow-based structure aligns naturally with the multi-stage selection process required for the size and heterogeneity of the corpus considered here.

The review centered on the convergence of three areas: industrial automation systems, cybersecurity prerequisites, and certification or standardization frameworks. In this context, industrial automation systems were widely defined to incorporate ICSs, SCADA environments, distributed control systems, programmable logic controllers, safety-related automation designs, and Industry 4.0-connected production environments. The purpose

of the review was not only to identify which cybersecurity standards are most frequently applied in industrial automation, but also to determine how security requirements are defined, reviewed, validated, and translated into certification procedures. This scope was selected because cybersecurity in industrial environments differs fundamentally from conventional IT security due to operational continuity constraints, safety implications, legacy technologies, heterogeneous communication protocols, and the critical-infrastructure role of many automated systems.

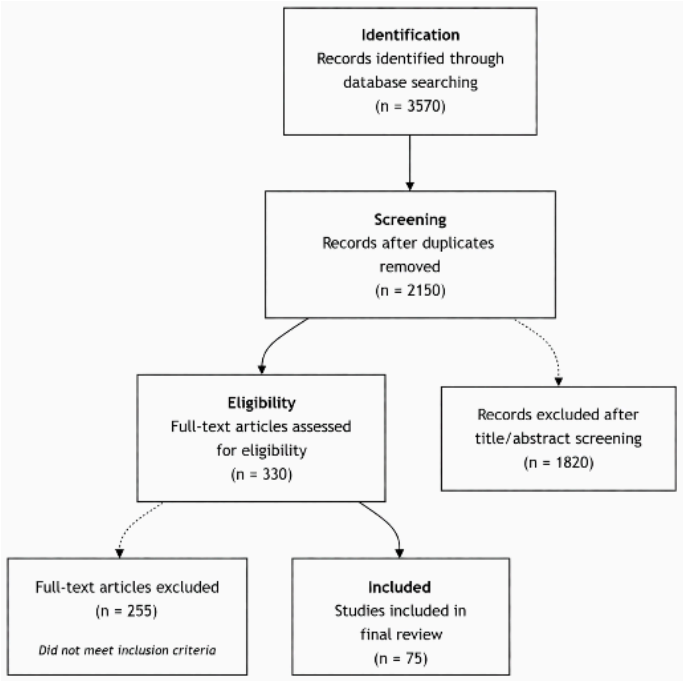

Figure 1. Study selection workflow.

2.1. Literature Search Strategy

A structured literature search was completed across the following academic databases: IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and ACM Digital Library. We chose these databases because they all cover engineering, industrial informatics, control systems, standards-oriented research, and cybersecurity research in enough depth. The search technique combines a mix of keywords and Boolean operators to acquire the most coverage while still being relevant to the topic. Representative search expressions included combinations of the terms such as 'industrial automation',' industrial control systems', 'SCADA', 'OT security', 'cybersecurity requirements', 'security standards', 'certification', 'IEC 62443', 'ISO/IEC 27001', 'NIST', 'functional safety', and 'compliance'. This keyword-based and Boolean-refined technique was developed to record both broad conceptual conversations and more targeted technical studies related to cybersecurity and certification in industrial automation. The identification process gave the following results: IEEE Xplore: 910, Scopus: 1240, ScienceDirect: 630, SpringerLink: 480, and ACM Digital Library: 310, producing a total of 3570 items. After bringing all the search results together, any duplicate records were removed out. A total of 1420 duplicates were identified and removed, leaving 2150 records for screening. This first reduction phase was significant because the topic covers overlapping technical and interdisciplinary databases, resulting in frequent repetition of the same findings across various sources.

The core Boolean string applied was: ('industrial automation' OR 'industrial control system*' OR 'SCADA' OR 'OT security' OR 'operational technology') AND ('cybersecurity requirement*' OR 'security standard*' OR 'certification' OR 'compliance' OR 'IEC 62443'

OR 'ISO/IEC 27001' OR 'NIST' OR 'functional safety'). This string was applied to the title, abstract, and keyword fields and adapted to the syntax of each platform: IEEE Xplore (command search with field tags), Scopus (TITLE-ABS-KEY), ScienceDirect (advanced search on title, abstract, and keywords), SpringerLink (full-text search with title/abstract refinement), and ACM Digital Library (advanced search on the same fields). The search was restricted to English-language peer-reviewed publications over the period 2016–2025. Where a database returned more records than could be screened against the keyword fields alone, relevance ranking was used to prioritize the most topically aligned records before screening.

2.2. Inclusion and Exclusion Criteria

The full texts were evaluated against predefined inclusion and exclusion criteria to ensure that only relevant and analytically useful studies were retained. The inclusion criteria were as follows:

1. Peer-reviewed journal articles, conference papers, and authoritative review papers;
2. Studies explicitly addressing cybersecurity requirements, controls, assurance measures, conformity assessment, certification schemes, or security standards relevant to industrial automation systems;
3. Publications containing technical, regulatory, architectural, or methodological discussion substantial enough to support comparative analysis;
4. Studies clearly situated within industrial automation, industrial control, smart manufacturing, SCADA, ICS, or critical infrastructure contexts.

The exclusion criteria were as follows:

1. Studies not related to industrial automation security;
2. Studies focused only on conventional IT security without OT or control-system relevance;
3. Publications lacking certification, compliance, standards, or technical cybersecurity analysis;
4. Purely descriptive industrial digitization papers without meaningful security substance;
5. Duplicated, editorial, or inaccessible records.
6. The inclusion and exclusion criteria are summarized in Table 1.

Table 1. Inclusion and exclusion criteria used in the systematic review.

Criterion Type	Criteria
Inclusion criteria	Peer-reviewed journal articles, conference papers, and review studies
Inclusion criteria	Studies addressing cybersecurity requirements, standards, certification, assurance, or compliance in industrial automation systems
Inclusion criteria	Studies related to ICS, SCADA, OT, Industry 4.0, smart manufacturing, or critical infrastructure automation
Inclusion criteria	Publications containing sufficient technical, architectural, methodological, or regulatory discussion for analysis
Exclusion criteria	Studies not related to industrial automation security
Exclusion criteria	Studies focused only on traditional IT security without OT/ICS relevance
Exclusion criteria	Studies without certification, standards, compliance, or technical cybersecurity analysis
Exclusion criteria	Purely descriptive digitization papers without meaningful security contribution
Exclusion criteria	Duplicate, editorial, or inaccessible publications

These criteria were designed to ensure that the final corpus directly addressed the technical and certification-related dimensions of cybersecurity in industrial automation rather than broader or unrelated cybersecurity discussions.

2.3. Study Selection Process

The study selection technique was carried out in three stages: identification, screening, and eligibility assessment. After receiving the data from the database and getting rid of duplicates, there were 2150 records left to filter. The second stage entailed screening the title and abstract. At this point, each record was appraised for topical relevance to the study objective. Publications were excluded if they focused exclusively on general IT security without connection to industrial automation, addressed cybersecurity in purely enterprise or cloud settings without operational technology implications, or discussed automation without meaningful treatment of cybersecurity requirements, assurance mechanisms, or certification-related issues. Through this filtering stage, 1820 records were deleted, and 330 full-text articles remained for eligibility assessment. The third phase was a full-text review and a detailed analysis of eligibility based on the stated criteria for inclusion and exclusion. Of the 330 full-text papers assessed, 255 were excluded for failing to meet the review criteria. Consequently, the review preserved 75 studies for decisive analysis. These 75 papers supplied the evidence base of the present review. The full review method, including identification, screening, eligibility evaluation, and final inclusion, is summarized in Figure 1.

One author conducted the title-and-abstract screening of all 2150 records against the inclusion and exclusion criteria. To reduce the risk of single-reviewer bias, the co-authors reviewed the borderline records and a sample of excluded records; any case in which a co-author disagreed with the initial decision was discussed by the full author team and resolved by consensus before the record was finalized.

An assessment of the publication years of the obtained resources reveals that the literature on cybersecurity standards and certification in industrial automation is primarily recent. The study that was looked at includes the years 2016 to 2025 (see Table 2), with a clear concentration on the recent few years. The years 2023–2025 account for 45 papers, or 60% of the dataset. The year 2025 alone accounted for 19 papers, or 25.3%. There were just two papers in the dataset that were published before 2020. This distribution indicates that the topic has gained substantial research attention only recently, likely due to the increasing adoption of Industry 4.0 technologies, stronger interconnection of industrial control systems, and the growing importance of standards such as IEC 62443 and related certification-oriented approaches. Overall, the publication trend implies that cybersecurity certification in industrial automation is a novel and swiftly emerging study subject.

Table 2. Distribution of reviewed studies by publication year.

Publication Year	Number of Papers	Percentage (%)
2016	1	1.3
2018	1	1.3
2020	10	13.3
2021	11	14.7
2022	7	9.3
2023	15	20.0
2024	11	14.7
2025	19	25.3
Total	75	100.0

2.4. Data Extraction and Analysis

After research selection, a structured data extraction approach was used to the final set of included studies. For each paper, the following information was recorded: publication metadata, industrial domain, system type, cybersecurity challenge addressed, applicable standard or certification framework, requirement categories, validation or assessment methodologies, and important conclusions. This extraction structure makes it possible to compare research not only at a descriptive level but also in terms of their technical contribution and relevance to certification-related cybersecurity practice. Particular attention was given to whether the studies discussed internationally recognized frameworks such as IEC 62443, NIST guidance, ISO/IEC-based information security approaches, sectoral conformity requirements, or security risk assessment methods tailored to industrial control and SCADA systems. This emphasis was significant since literature in this field consistently reveals that generic IT risk strategies typically require adaptation before they can be usefully implemented in SCADA and industrial-control environments.

Following extraction, the selected studies were synthesized through topic analysis. The objective of this synthesis was to discern prevailing standards, persistent demand patterns, methodological deficiencies, and unresolved certification obstacles. Special emphasis was paid to tensions between security, safety, availability, and legacy system limits, because these concerns continuously affect cybersecurity decision-making in industrial automation. In this approach, the research proceeded beyond mere description and aimed to explain how cybersecurity standards are operationalized in practice and why certification remains complicated in industrial situations.

2.5. Classification Model Definition

For the analytical stage, the final studies were categorized using a classification model particularly created for this study. The classification model classified the literature into three basic dimensions. The first dimension concerns the type of cybersecurity requirement, including governance requirements, technical security controls, network and communication protection, access control, monitoring and incident response, lifecycle security, and safety-security coordination. The second pillar concerns the certification or standards perspective, encompassing standard families, conformity assessment methodologies, sector-specific certification practices, and assurance-related evaluation criteria. The third factor concerns the application context, such as manufacturing systems, SCADA networks, critical infrastructure automation, and Industry 4.0 environments. This classification structure allows both vertical analysis within each category and horizontal comparison across categories. Consequently, it established a definitive framework for discerning the various methodologies employed by studies in addressing cybersecurity requirements and certification challenges within industrial automation contexts. Overall, this methodological design provides a rigorous and technically informed basis for the systematic review given in this study. The classification framework utilized in this investigation is shown in Table 3.

To provide a clearer conceptual understanding of the relationships between cybersecurity requirements, certification frameworks, and industrial application domains, this study proposes an integrated mapping framework. The framework visually represents how technical security requirements are translated into certification standards and implemented across different industrial contexts, while also highlighting cross-cutting challenges that influence all layers. The proposed model is illustrated in Figure 2.

Table 3. Classification framework developed for organizing and synthesizing the selected studies.

Dimension	Category	Description
Cybersecurity requirements	Network and communication security	Secure industrial protocols, network zoning, intrusion detection, and communication resilience
Cybersecurity requirements	Monitoring and incident response	Logging, anomaly detection, event monitoring, response planning, and recovery
Cybersecurity requirements	Lifecycle and maintenance security	Secure design, deployment, operation, maintenance, and update practices
Cybersecurity requirements	Safety-security coordination	Interaction between cybersecurity controls and functional safety requirements
Standards/certification	Security standards	IEC 62443, ISO/IEC 27001-related approaches, NIST-oriented guidance, and sector-specific frameworks
Standards/certification	Certification/conformity assessment	Assurance schemes, evaluation methods, testing procedures, and certification mechanisms
Application context	Industrial domain	Manufacturing, SCADA systems, critical infrastructure, smart factories, and Industry 4.0
Application context	System focus	PLCs, DCS, ICS networks, IIoT-connected devices, and automation architectures

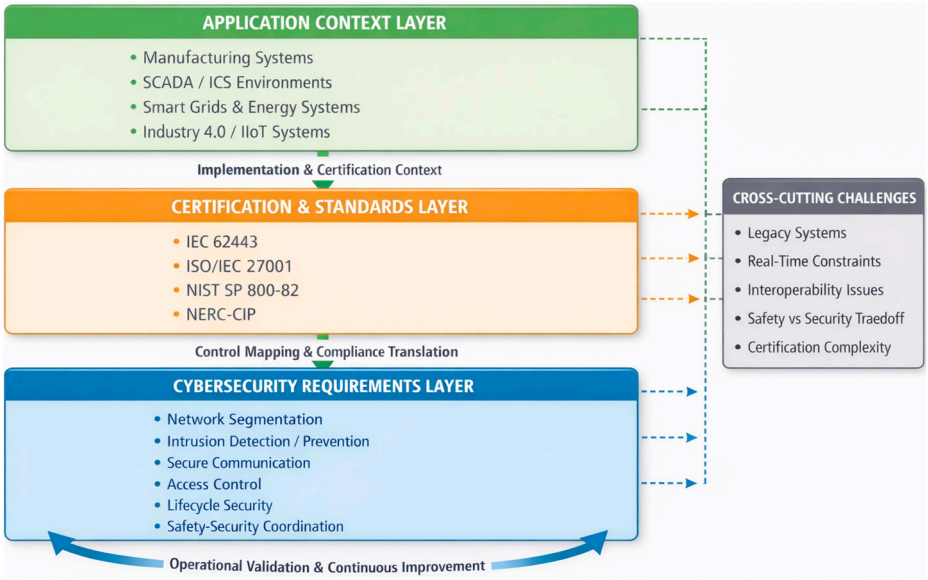

Figure 2. Integrated Mapping Framework for Cybersecurity Requirements and Certification Standards in Industrial Automation Systems.

To make the framework operational rather than purely conceptual, it can be applied as a four-step procedure. First, the relevant requirement categories for the target system are identified using the requirement dimension. Second, the applicable standards are selected for the sector and system type using the certification dimension. Third, each requirement is mapped to the framework or frameworks that address it, with the corpus-level frequencies used to prioritize the requirements most consistently emphasized in the literature. Fourth, residual gaps—requirements not adequately covered by the selected framework—are flagged for supplementary guidance or layered compliance. This stepwise

reading allows practitioners to move from the conceptual map of Figure 2 to a concrete requirement-to-standard assessment for their own environment.

The classification framework summarized in Table 3 was not imposed a priori but was refined iteratively through a content-analysis pass over the 75 included studies. Each paper was coded against the candidate requirement and framework categories; categories that recurred across multiple studies and sectors were retained, while those that appeared only in a single paper were merged or removed. The resulting frequency distribution is presented at the end of Section 4, which provides the quantitative basis on which the dimensions of the framework rest.

2.6. Validation and Reliability of the Review

To increase the credibility of the review, the selected research was examined comparably across many aspects rather than being treated as isolated sources. The consistency of conclusions was tested by analyzing how many studies treated parallel cybersecurity requirements, standards, and certification-related challenges inside industrial automation settings. We paid specific attention to patterns that kept showing up, such as those involving segmentation, intrusion detection, secure communications, access control, lifecycle security, and compliance-oriented governance frameworks. In addition, the classification system presented in this study was applied uniformly to all retained publications in order to remove interpretive fragmentation and to permit orderly cross-study comparison. This technique strengthened the intellectual coherence of the investigation and helped guarantee that the findings were developed from converging evidence rather than from isolated examples.

2.7. Quality Assessment of Included Studies

To strengthen the methodological transparency of the review and provide readers with an indicator of study credibility, each of the 75 included publications was assessed against a five-criterion quality rubric adapted from established systematic-review practice. The criteria were: (Q1) clarity of research aim and scope; (Q2) methodological transparency, including whether the study described its data, sources, or analytical procedure; (Q3) depth of evidence base supporting cybersecurity or certification claims; (Q4) relevance to industrial automation, ICS/SCADA, or certification-oriented contexts; and (Q5) clarity and reproducibility of conclusions. A score of 1 was assigned when the criterion was fully met (for example, for Q3, the study engaged substantively and in depth with technical or standards content); 0.5 when it was partially met (the topic was addressed only briefly or without supporting detail); and 0 when it was not met. Scoring was carried out by one author and then independently reviewed by a second author; where the two assessments differed by more than half a point on any criterion, the discrepancy was discussed by the author team and a consensus score agreed before totals were computed. The distribution of quality scores is shown in Table 4. On the 75 included studies, 28 achieved the maximum score of 5, 43 scored between 3 and 4.5, and 4 scored 2 to 2.5; no study score was below 2. The quality scoring described here is provided as a complementary credibility indicator.

Table 4. Distribution of quality-assessment scores across 75 included studies.

Quality Score	Number of Studies	Percentage (%)
5.0	28	37.3
4.0–4.5	28	37.3
3.0–3.5	15	20.0
2.0–2.5	4	5.3
Below 2.0	0	0.0
Total	75	100.0

3. Framework-Based Analysis of Cybersecurity Requirements and Certification Standards

Beyond restating individual requirements, the contribution of analyzing these 75 studies together lies in what their aggregation reveals: the relative emphasis the field places on each requirement, the structural gap between richly discussed technical controls and the scarcity of validated certification outcomes, and the complementary rather than competing relationship among the dominant standards. These corpus-level observations, rather than the description of any single control, constitute the analytical contribution of this section.

The reviewed literature shows that cybersecurity in industrial automation systems is best understood as a layered problem rather than a single set of isolated technical controls. Across the selected studies, two closely connected dimensions appear most consistently: network-level security and control-system security. The first concerns the protection of communication pathways, data exchange, remote connectivity, and protocol behavior. The second concerns the integrity and trustworthy operation of supervisory and control functions, including SCADA platforms, PLCs, firmware, field devices, and operator-facing control logic. Taken together, these dimensions form the core technical foundation of industrial cybersecurity.

3.1. Network-Level Security

A comparative reading of the literature indicates that the most recurrent network-level requirements are segmentation, intrusion detection and intrusion prevention, encryption and secure communication, and protocol hardening [20–26]. The most recurrent control-system requirements are SCADA/OT protection, PLC integrity, firmware validation, access control, and patch management [26–30]. At the same time, the strongest concentration of studies appears in smart-grid, cyber-physical power-system, SCADA, IIoT, and other critical-infrastructure contexts [20,28,29,31–34]. By contrast, the literature is comparatively weaker in directly validated cross-sector studies that connect these technical controls to real certification outcomes in manufacturing environments. This imbalance is important because it shows that industrial cybersecurity research is rich in technical discussion, but still less mature in demonstrating how technical requirements are translated into operational assurance and certification practice.

Another repeating result is that recent research moves away from static perimeter-oriented protection and toward more context-aware, layered, and architecture-sensitive security models. This tendency may be seen in studies on cyber-physical power systems, distributed energy resources, AI security for operational technology, SCADA risk assessment, and protective measures for PLCs [20,26,28–30,32–36]. The trend is driven by the increasing interdependence of industrial communication systems and control functions: vulnerabilities in communication design may propagate into control behavior, while deficiencies in controller integrity may compromise otherwise protected network environments. Accordingly, the literature repeatedly implies that industrial cybersecurity maturity depends less on a single robust mechanism and more on how defensive measures reinforce one another across the cyber-physical link. Network-level security carry measurements, alarms, control commands, synchronization signals, and state-related information whose disruption may affect not only confidentiality but also continuity, stability, and safe operation [26,37]. For this reason, network security in industrial settings is not treated merely as an IT traffic-management problem. It is framed as a core component of operational integrity.

3.1.1. Segmentation

Segmentation is one of the most consistently emphasized requirements in the literature. Its importance lies in limiting the propagation of compromise across interconnected industrial environments. Rather than treating the network as a flat space, segmentation organizes industrial assets into zones or layers according to function, trust level, and operational criticality [26,32]. This reduces the likelihood that compromise of one point in the system will immediately expose supervisory or process-critical components.

The literature presents segmentation not simply as inherited IT best practice, but as an architectural necessity for cyber-physical environments. In smart-grid and Distributed Energy Resources (DER) contexts, segmentation is repeatedly associated with the need to manage multiple devices, communication channels, stakeholders, and trust boundaries [20,32,34]. In PLC and nuclear-related contexts, it is linked to the protection of highly sensitive supervisory and substation-level functions from broader enterprise or remote-access exposure [26,30]. The practical message is clear: industrial systems cannot assume that external and internal communications are equally trustworthy and therefore must define explicit operational boundaries.

At the same time, adjacent literature shows that industrial cyber-physical monitoring is becoming increasingly data driven. In power-system environments, machine-learning approaches applied to synchrophasor-based measurement and analysis illustrate the growing role of intelligent wide-area monitoring in security-relevant operational supervision [38]. This broader shift is accompanied by increased attention to cybersecurity awareness and educational tooling [39], as well as emerging interest in Large Language Model (LLM)-supported cybersecurity workflows [40]. Related Industry 4.0 research on maintenance performance, oil-and-gas analytics, and manufacturing big-data ecosystems further suggests that industrial resilience depends not only on controller protection, but also on the quality of maintenance intelligence, large-scale data handling, and analytics infrastructures [41–43].

Traditional fixed zoning remains important, but recent studies increasingly discuss micro-segmentation, software-defined policy enforcement, and more adaptive boundary control in environments requiring both security and deterministic performance [28,44]. This indicates that segmentation remains a central requirement, but one that is gradually becoming more dynamic and architecture aware.

3.1.2. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Detection-Centered Defense

Intrusion detection and intrusion prevention are also important. Their importance increases in industrial environments because static filtering alone is often insufficient in systems characterized by heterogeneous devices, variable communications, and protocol behaviors that may be operationally legitimate in one context and suspicious in another [22–24]. In IIoT and CPS settings especially, IDS is described less as an optional enhancement and more as a necessary part of maintaining situational awareness.

A key development is the movement from pure signature-based detection toward anomaly-based, specification-based, and hybrid approaches [24]. In industrial contexts, this transition is particularly important because many attacks are designed to mimic normal traffic patterns while altering timing, sequence, or process state implications. False data injection research in power systems illustrates this clearly: a communication event may appear syntactically valid while still undermining operational trust [27]. Accordingly, the literature increasingly favors detection approaches that combine network evidence with process awareness, state estimation, or controller-adjacent monitoring.

However, the literature is equally clear about the limitations of detection-centered defense. High reported accuracy in laboratory settings does not automatically translate

into deployment robustness. Common concerns include false positives, explainability, model drift, sparse labeled data, and adversarial manipulation of Machine Learning (ML)-based security models [21]. For industrial environments, these limitations are especially serious because excessive alerts can burden operators and reduce trust in monitoring systems. Thus, the dominant conclusion is not that IDS/IPS is sufficient on its own, but that it must be embedded into broader, layered monitoring architectures that combine communication-level, protocol-level, and process-level observation [28,29].

3.1.3. Encryption, Secure Communications, and Protocol Hardening

Encryption and secure communication are often highlighted as critical requirements because industrial networks convey telemetry, directives, authentication data, synchronization information, and other sensitive communications [32–36]. These channels are nonetheless open to eavesdropping, message manipulation, spoofing, replay, and man-in-the-middle attacks if they are not properly protected [33,34]. Yet the literature also highlights that encryption in industrial systems cannot be evaluated in the same way as in normal company contexts. Real-time performance, predictable timing, device restrictions, and interoperability with legacy components all define what is operationally feasible. This tension is especially obvious in protocol-oriented investigations. Work on power-system communication standards illustrates that secure messaging must fulfill both security and time requirements, especially in contexts where delayed or computationally heavy protections may degrade operational performance [33]. Thus, the examined literature addresses secure communication not as a binary issue of "encrypted versus unencrypted", but as a question of whether security solutions are consistent with industrial timing, authenticity, and control needs. The literature also distinguishes between generic encryption and secure protocol design. People typically talk about industrial protocols like Modbus, Distributed Network Protocol 3 (DNP3), IEC 61850, and other communication architectures as being historically better for availability and interoperability than for strong security guarantees [26,29,33]. Because of this, protocol hardening seems to be a separate and ongoing issue. The essential issue is not just whether messages are protected in transit, but if communication events are authenticated, contextually genuine, resistant to replay, and compatible with intended process behavior [27,29,31,33,34]. This is why recent research increasingly links secure communication with authentication, trust management, protocol-aware monitoring, and cyber-physical co-validation.

Overall, segmentation, detection, secure communication, and protocol hardening from the main defensive cluster at this layer.

3.2. Control-System Security

If network-level security addresses how industrial systems communicate, control-system security addresses how they decide and act. This layer includes SCADA platforms, Distributed Control System (DCS) functions, Human–Machine Interfaces (HMIs), Remote Terminal Units (RTUs), PLCs, field devices, firmware, and supervisory logic [26,29,30]. It is at this level that cyber compromise becomes most directly connected to physical consequence. A manipulated command altered controller logic, or compromised firmware component may shift an incident from information exposure to process disruption, unsafe behavior, or operational loss [29,33,37].

3.2.1. SCADA/OT Protection

SCADA and broader OT protection form the backbone of the control-system literature. SCADA systems remain central because they aggregate measurement data, support operator visibility, coordinate supervisory decisions, and mediate communications between

higher-level control logic and field devices [26]. Their position also makes them strategically attractive attack targets.

SCADA protection requires a broader control set than generic IT security models usually provide. Recurrent themes include communications management, access control, secure acquisition and development, incident response, business continuity, policy integration, and compliance-aware governance [26]. More recent CPS-oriented work adds a further point: it is not enough to secure supervisory software in isolation. Security mechanisms must also account for the relationship between communication events, physical process states, and operator interpretation [29,31,37]. This is why SCADA/OT protection increasingly appears as a coordination problem across communications, software, devices, operations, and recovery planning rather than as a single technical hardening task.

3.2.2. PLC Integrity

PLC integrity is one of the most prominent issues in industrial cybersecurity. PLCs are central to industrial automation because they translate supervisory intent into local control actions in real time [29,30]. Their importance also makes them an attractive target. Once compromised, PLCs may be used to alter logic, manipulate sequencing, disable safety functions, falsify I/O behavior, or create subtle deviations between sensed conditions and control actions [29].

A major contribution of the literature is that it treats PLC integrity as multidimensional. It is not limited to malware resistance or access restriction. Rather, it includes logic authenticity, configuration integrity, trustworthy runtime behavior, and consistency between executed control logic and expected process outcomes [27,29,30]. This broader interpretation is valuable because it shows why controller compromise is particularly dangerous: it may evade surface-level monitoring while directly affecting physical operation. The dominant research direction therefore favors not only device hardening, but also embedded monitoring, behavior analysis, and closer coupling between controller observation and process expectations.

3.2.3. Firmware Validation

Firmware validation appears as a closely related but distinct concern. Firmware is often harder to observe, harder to update, and more tightly tied to hardware-specific operation than higher-level software. As a result, compromise at this layer may remain hidden while still altering device behavior in meaningful ways.

The reviewed studies emphasize that firmware validation in industrial systems is constrained by both technical and governance realities. On the technical side, devices may lack built-in support for strong validation, attestation, or secure boot features. On the governance side, firmware changes may require extensive verification, vendor coordination, licensing approval, or regulatory review, especially in safety-critical environments [29,30]. This explains why firmware validation is widely recognized as essential but less fully operationalized than other network-oriented controls. The literature repeatedly points toward trusted baselines, signed updates, anomaly-aware behavioral checks, and lifecycle traceability as the most promising directions, although widespread practical implementation remains uneven.

3.2.4. Access Control

Access control is a persistent theme across both network and control layers, but its industrial form is especially demanding. In control environments, access is not only about who may log in, but who may configure, modify, command, or maintain operationally sensitive assets [25,26,34]. Because industrial systems often involve operators, engineers, vendors, and maintenance personnel with different roles and temporary access needs, the

challenge is not merely to authenticate users, but to manage privilege in a context-sensitive and operationally safe way.

The literature highlights several recurring weaknesses: shared credentials, excessive privilege, weak remote maintenance controls, and legacy systems that do not support fine-grained authorization models [25]. At the same time, recent studies increasingly interpret access control through broader trust models, including zero-trust ideas, stronger identity validation, and more explicit policy-driven access decisions in OT environments [28]. This suggests that industrial access control is moving beyond traditional role assignment toward more continuous and context-aware trust management.

3.2.5. Patch Management

Patch management is one of the clearest examples of how industrial cybersecurity differs from enterprise IT practice. Across the reviewed studies, patching is consistently described as necessary but operationally difficult [29,30]. In many industrial systems, updates may require restart, revalidation, recertification, or interruption of tightly coupled processes. In long-lifecycle infrastructures, patches may also be constrained by vendor support limitations, hardware compatibility, or uncertainty about downstream operational effects [30].

Effective practice requires identifying which vulnerabilities are exploitable in the real operational context, evaluating whether compensating controls can temporarily reduce exposure, validating changes before deployment, and scheduling implementation in ways compatible with safety and continuity [26]. This makes patch governance one of the clearest points where cybersecurity, reliability, and certification interact directly.

Taken together, network-level security and control-system security are analytically distinct but operationally inseparable. Segmentation without controller integrity may slow compromise but not prevent process manipulation after trusted zones are reached. Detection without secure communication may provide visibility while leaving message trust unresolved. Access control without patch governance may reduce unauthorized entry while leaving exploitable software in place. Firmware validation without process-aware monitoring may fail to detect subtle behavioral compromise. In each case, the effectiveness of one defensive measure depends partly on the strength of others.

Beyond communication and controller hardening, related industrial digitalization literature also points to the growing convergence of safety monitoring, immersive interfaces, data governance, and structured asset modeling. Time-sensitive networking supports reliable and deterministic communication in industrial environments [44], while computer-vision-based Personal Protective Equipment (PPE) compliance systems show how operational safety monitoring is becoming increasingly automated in industrial practice [45]. Augmented-reality-enabled smart environments likewise suggest that new digital interaction layers may expand both operational capability and cyber exposure [46]. Related work on cybersecurity risk assessment for engineering databases highlights that protection increasingly extends to the integrity and governance of technical data repositories [47]. A recent industrial case study in biomass power plants further illustrates how IEC 62443, NIST SP 800-82, ISA-95, and Purdue-style segmentation can be combined into an integrated IT/OT protection architecture [48]. In parallel, sustainability-oriented AI research reinforces the strategic role of intelligent digital systems in industrial transformation [49], while ontology-based modeling of IIoT security suggests a more formal basis for representing assets, threats, and controls in complex industrial ecosystems [50].

3.3. Certifications and Compliance

Certifications and compliance frameworks have become a crucial layer of cybersecurity governance in industrial automation and energy-oriented cyber-physical systems. They no longer just serve as formal audits or symbols of trust. Instead, these frameworks increasingly organize how firms define security obligations, manage risk, apply technical controls, enable lifecycle governance, and establish trustworthiness across complex industrial infrastructures [51–56]. This is especially visible in IIoT ecosystems, operational technology environments, battery management systems, smart grids, vehicle-to-grid infrastructures, solar plants, and connected building systems, where cybersecurity failures may affect not only data confidentiality but also continuity of service, operational safety, asset integrity, and system reliability [57–63].

From a classification perspective, frameworks such as ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-82, and NERC-CIP differ not only in scope but also in function [57–63]. This distinction is important because it shows that industrial organizations rarely benefit from depending on a single framework alone. Rather, the literature supports the idea that effective assurance emerges from combining governance, technical guidance, industrial suitability, and sector-specific protection.

3.3.1. ISA/IEC 62443

ISA/IEC 62443 is the one most closely aligned with industrial automation and control environments. The literature presents it as one of the best-known and most relevant standards families for industrial cybersecurity because it was designed specifically for industrial automation and control systems rather than adapted from enterprise IT models [51]. Its importance lies in its OT-centered logic: in industrial settings, availability and integrity often carry equal or greater importance than confidentiality, since interruption or incorrect control behavior may have direct implications for safety, continuity, and operational performance [51].

This explains why ISA/IEC 62443 appears so frequently in the reviewed literature on IIoT, industrial automation, cyber-physical infrastructure, and multivendor industrial environments [51,53–56,61–63]. Rather than functioning as a narrow checklist, it provides an architectural approach to industrial cybersecurity through lifecycle governance, risk-based system design, hardening, segmentation, patch management, and clearly differentiated responsibilities among asset owners, integrators, and service providers [51,53]. This makes it especially suitable for long-lived, heterogeneous industrial infrastructures where responsibility is distributed across multiple organizational actors.

The literature also shows that ISA/IEC 62443 becomes even more valuable when cybersecurity must be extended into emerging cyber-physical sectors. In battery systems, building management, solar plants, and distributed energy contexts, the framework helps translate general security objectives into industrially meaningful requirements tied to communication protection, operational continuity, and system lifecycle management [55,56,61–63]. At the same time, the literature acknowledges several limitations: implementation is resource-intensive, standards adoption often lags behind technical change, and overlapping frameworks may create complexity for organizations attempting cross-sector compliance [51]. Thus, ISA/IEC 62443 is consistently presented as a necessary foundation for industrial cybersecurity governance, but not as a sufficient solution in isolation.

Despite its prominence, IEC 62443 is not without contested aspects, and recent literature increasingly examines whether its core architectural assumptions remain adequate in modern IIoT contexts. The zone-and-conduit model, while powerful for hierarchical, Purdue-aligned plant networks, was conceived for relatively static, deterministically segmented environments. Modern IIoT deployments, by contrast, frequently exhibit flatter

topologies in which edge devices communicate directly with cloud services, mobile and software-defined assets cross traditional zone boundaries, and trust relationships are continuously renegotiated. Several authors have therefore argued that the model requires extension or reinterpretation to accommodate edge–cloud continua, micro-segmentation, and zero-trust principles [28,51]. A related discussion concerns the granularity of Security Levels (SL 1–4): while useful for system-level target setting, four discrete levels may be insufficient to differentiate the heterogeneous risk profiles found across IIoT devices that range from constrained sensors to high-capability gateways [51]. The implementation burden is a further point of contention, particularly for small and medium-sized industrial operators, where full lifecycle compliance with the standard's role-based responsibilities (asset owner, integrator, product supplier) is resource-intensive and may outpace organizational capacity. These critiques do not undermine the relevance of IEC 62443, but they suggest that it should be understood as an evolving framework whose architectural assumptions are still being aligned with the realities of distributed, cloud-connected, and software-defined industrial systems.

3.3.2. ISO/IEC 27001

If ISA/IEC 62443 is the main OT-specific framework, ISO/IEC 27001 is the dominant organization-wide governance framework in the examined literature. It is often called one of the most important standards for information security since it tells organizations how to set up, run, keep up, and keep improving an information security management system [52]. Unlike industrially specialized frameworks, ISO/IEC 27001 does not principally describe control-system security procedures. Instead, it provides the governance structure through which security policy, risk assessment, documentation, auditability, and organizational accountability are codified. This broad applicability explains why ISO/IEC 27001 remains relevant across industries, including smart buildings, data-intensive infrastructures, and digitally connected healthcare or public-service contexts [52,56,64]. The literature suggests that as digital transformation broadens the cyber risk surface, businesses increasingly need a formal management-system framework to combine technological, legal, organizational, and procedural components of cybersecurity [56]. In this respect, ISO/IEC 27001 serves as a crucial backbone for industrial cybersecurity governance, especially where numerous systems, teams, and regulatory duties must be coordinated. However, the literature is equally clear that the flexibility of ISO/IEC 27001 can also be a restriction in operational technology environments. Because it is generic, it frequently needs a lot of interpretation before it can be turned into specialized industrial controls. This is especially true in contexts where there are real-time restrictions, old infrastructure, and cyber-physical process sensitivity [52]. For this reason, the literature prefers to promote ISO/IEC 27001 as a governance layer rather than as a single technical solution for industrial control security. Its key strength is organizational discipline; its main shortcoming is that it often must be supported by industrially specific counsel.

3.3.3. NIST SP 800-82

NIST SP 800-82 is one of the most realistically oriented advice standards for industrial control system security. Unlike ISO/IEC 27001, which is primarily governance-oriented, NIST SP 800-82 is more closely related with implementation recommendations for ICS and SCADA environments. Its relevance is especially visible in the literature emphasizing the operational differences between industrial control systems and conventional IT systems, including time-critical operation, long equipment lifecycles, and the risk that some otherwise standard IT security countermeasures may disrupt industrial processes if applied without adaptation [26]. The practical value of NIST-oriented instruction is also

obvious in applicable industrial research. For example, recent work on biomass power plants combines NIST SP 800-82 Revision 2 with IEC 62443, ISA-95, and the Purdue model to form integrated IT/OT protection systems, including segmentation, detection, and layered security design [48]. In this respect, NIST SP 800-82 is best understood as an implementation-oriented reference framework that helps translate generic cybersecurity principles into ICS-specific practice. At the same time, the literature reveals a structural limitation: NIST SP 800-82 is guidance-oriented rather than an independent certification system. It consequently delivers substantial practical value for ICS protection but is best effective when utilized alongside larger governance and sector-specific compliance frameworks [26,48].

3.3.4. NERC-CIP

NERC-CIP occupies a distinctive position in the reviewed literature because it is associated with cybersecurity governance in bulk power and other reliability-critical energy environments. Unlike ISO/IEC 27001 and ISA/IEC 62443, which have broader cross-sector relevance, NERC-CIP is generally discussed in relation to electric-power infrastructure, grid resilience, and sector-specific compliance expectations [57–63].

In these environments, cybersecurity cannot be separated from reliability governance. Failures affecting control, communication, or protection functions may extend beyond information compromise to operational disruption, service instability, or broader infrastructure consequences. For this reason, NERC-CIP is best interpreted in this review as a sector-specific compliance regime linked to the protection and dependable operation of critical energy systems rather than as a general-purpose industrial framework.

Its main strength is its close relevance to high-criticality energy settings. Its main limitation is narrower applicability outside regulated power and energy environments [62,63].

3.3.5. Comparative Synthesis

Taken together, certifications and compliance frameworks in industrial cybersecurity should be interpreted as complementary rather than competing. ISA/IEC 62443 provides industrial automation specificity. ISO/IEC 27001 provides governance structure and auditability. NIST SP 800-82 provides practical technical guidance for ICS and SCADA environments, while NERC-CIP is discussed primarily in relation to resilience and reliability governance in critical power infrastructure [26,48,57–61].

This comparative pattern is one of the main findings of the reviewed literature. The strongest cybersecurity posture does not emerge from strict dependence on one framework, but from building a layered compliance architecture that combines governance maturity, industrial suitability, technical guidance, and sector-specific obligations. In practical terms, this means that industrial organizations increasingly require compliance architectures, not single-standard dependency.

Four gaps emerge from the corpus, each grounded in the evidence summarized in the preceding tables. First, multi-framework implementation remains resource-intensive and fragmented: the frequency data at the end of Section 4 shows that individual studies typically engage with a single framework in depth and that integration across frameworks is discussed in a minority of the corpus [51,52]. Second, the pace of standards adaptation lags behind technical change: 60% of the included studies were published in 2023–2025 (Table 2), but the standards revisions and certification practices they reference predate this period [56,65]. Third, evidence linking formal certification to measurable operational outcomes is limited: the corpus contains few validated cross-sector studies that connect certification to incident-response speed, downtime, or recovery capability, and this absence is itself a finding of the review. Fourth, certification-oriented evidence remains concen-

trated in energy and critical-infrastructure domains, with comparatively thin coverage of manufacturing, buildings, and process industries [57–63,65].

A deeper comparison along five dimensions clarifies how the frameworks differ. In scope, ISA/IEC 62443 is broadest for OT and control systems, ISO/IEC 27001 is broadest organizationally, and NERC-CIP is narrowest, being confined to bulk-power reliability. In assurance level, ISA/IEC 62443 and ISO/IEC 27001 provide formal certification pathways, NERC-CIP provides regulatory compliance enforcement, whereas NIST SP 800-82 is guidance only and offers no independent certification. In auditability, ISO/IEC 27001 is strongest through its management-system audit structure, with NERC-CIP also strong through mandatory compliance audits. In implementation burden, ISA/IEC 62443 is the most demanding given its lifecycle and role-based requirements, while NIST SP 800-82, being advisory, is the least prescriptive. In sector-specific applicability, NERC-CIP is the most targeted (electric power), ISA/IEC 62443 is industrial-automation-specific, and ISO/IEC 27001 is the most sector-agnostic. This comparison reinforces the review's central finding that the frameworks are complementary, since no single framework is strongest across all five dimensions.

4. Discussion

The outcomes of this research show that industrial cybersecurity has reached a point at which certifications and compliance frameworks can no longer be seen as peripheral governance devices. In industrial automation and cyber-physical environments, standards increasingly determine not just how security is documented, but also how systems are built, integrated, maintained, and validated. This is especially visible in businesses like energy, smart infrastructure, IIoT, and digitally controlled industrial services, where cybersecurity failures may damage not just information assets but also continuity, physical operation, and system reliability. One of the clearest conclusions of the research is that no single framework effectively fulfills the cybersecurity expectations of modern business environments. Some standards are mostly about governance and work well for putting up policy, accountability, auditing, and continuing improvement. Some are more focused on protecting critical infrastructure. As industrial systems become more distributed, connected, and software-dependent, several layers of governance must interact. The main compliance problem is therefore not the selection of one particular standard, but the creation of a unified security architecture that encompasses numerous frameworks without producing overlap, ambiguity, or audit fatigue.

The research also reveals that the notion of compliance is changing concurrently with the building of industrial systems themselves. The environments described in the literature are no longer confined to isolated enterprises or rudimentary supervisory networks. They are adding more and more smart inverters, DERs, Electric Vehicle (EV) charging systems, cloud-connected monitoring, predictive maintenance platforms, digital twins, and AI-enabled decision support. Under these scenarios, compliance is not merely a technique of proving vigilance after system deployment. It becomes a way of arranging security across technically interdependent and organizationally dispersed infrastructures. A further significant discovery is the continual tension between generality and specificity. Broad frameworks enable governance consistency, portability, and organizational auditability but they may lack the requisite granularity for industrial control situations. More specialized frameworks offer immediate practical relevance but may not scale effectively across industries or enable enterprise-wide governance by itself. The research therefore supports hybrid compliance strategies in which management-system discipline, industrially specialized control logic, practical implementation assistance, and sectoral reliability obligations are integrated rather than separated.

The report also underscores a crucial distinction between compliance maturity and security maturity. Compliance that is written down does not always lead to systems that are strong. If standards are perceived as things to check off, businesses may be formally compliant yet still have operational flaws. Conversely, technically strong organizations may nonetheless be exposed if their procedures are not documented, audited, or linked with legal and regulatory requirements. The actual aim is therefore not certification for its own sake, but the building of security capabilities that are repeatable, explainable, operationally credible, and resilient under industrial limits. Human and organizational variables intensify this issue. Compliant architecture on paper may yet fail in practice if processes are not followed, roles are not clear, implementation is not well-funded, or workers regard cybersecurity as less essential than production. So, industrial cybersecurity is not merely a technical or standards issue. It is also a coordination concern comprising management, engineering, operations, procurement, maintenance, and training. The literature repeatedly implies that compliance is most efficient when these processes work under a shared security rationale rather than as independent administrative layers. This issue becomes increasingly serious in sectors where reliability is inseparable from cybersecurity. In energy and other critical infrastructure situations, cyber incidents may influence not just information security but also voltage stability, energy supply, operational safety, asset condition, and public-facing service continuity. In such circumstances, sector-specific frameworks connected to dependability criteria remain particularly valuable since they incorporate fundamental security concepts into infrastructure-specific duties and minimal precautions. Overall, the research supports the idea of industrial compliance as a tiered socio-technical governance system. It is most effective when organizational discipline, technical execution, sector awareness, and human conduct reinforce one another. It is least successful when standards are applied in isolation or seen as disconnected administrative needs. Table 5 summarizes the comparative role of the four most influential compliance frameworks identified in the reviewed literature.

Table 5. Comparative Discussion of the Four Main Compliance Frameworks.

Framework	Primary Role	Main Advantage	Main Limitation	Most Suitable Context
ISA/IEC 62443	OT and industrial automation security	Industrial focus; lifecycle orientation; segmentation and service-provider logic	Resource-intensive implementation; uneven fit with flat IIoT topologies	Industrial automation, OT, IIoT, multivendor industrial systems
ISO/IEC 27001	Information security management system	Governance, auditability, continual improvement; broad applicability	Too generic for direct control-system implementation	Enterprise-wide security governance and cross-sector compliance
NIST SP 800-82	Practical ICS/SCADA security guidance	Implementation-oriented; useful for technical control environments	Guidance only; not a certification scheme	ICS, SCADA, operational control-system protection
NERC-CIP	Sector compliance for bulk electric systems	Direct alignment with grid reliability and sector protection	Narrow applicability outside regulated power infrastructure	Smart grids, bulk power, reliability-critical energy settings

Taken together, the discussion suggests that the next step for industrial cybersecurity is not broader certification alone, but better integration between compliance layers. The organizations most likely to succeed will be those able to translate standards into real engineering, governance, and operational behavior rather than those that merely accumulate formal certifications.

The frequencies reported in Table 6 reflect a content-analysis pass over the 75 included studies in which each paper was checked against the nine requirement categories and five framework categories used in the manuscript's classification structure. Counts are non-exclusive: a single study may be counted toward multiple items where it substantively engages more than one topic.

Table 6. Frequency of cybersecurity requirements and certification frameworks across the 75 included studies.

Category	Item	Number of Studies	% of Corpus (n = 75)
Cybersecurity requirements	Network segmentation	24	32.0
Cybersecurity requirements	Intrusion detection/IDS-IPS	19	25.3
Cybersecurity requirements	Secure communication/encryption	17	22.7
Cybersecurity requirements	Access control	14	18.7
Cybersecurity requirements	Lifecycle security	13	17.3
Cybersecurity requirements	Safety-security coordination	9	12.0
Cybersecurity requirements	PLC integrity	9	12.0
Cybersecurity requirements	Patch management	7	9.3
Cybersecurity requirements	Firmware validation	5	6.7
Certification frameworks	ISA/IEC 62443	12	16.0
Certification frameworks	Other/sector-specific frameworks	14	18.7
Certification frameworks	NERC-CIP	6	8.0
Certification frameworks	ISO/IEC 27001	5	6.7
Certification frameworks	NIST SP 800-82	4	5.3

5. Future Directions

The reviewed literature points toward several important future directions for research and practice in industrial cybersecurity certifications and compliance.

The first is cross-standard orchestration. Industrial systems increasingly operate at the intersection of enterprise IT, OT, IIoT, cloud services, AI-enabled monitoring, and sector-specific regulation. As a result, future governance models will need stronger mapping across management-system standards, industrial control standards, technical implementation guidance, and sectoral reliability obligations [51,52,66]. Research should therefore move toward interoperable compliance architectures that reduce overlap and help organizations build unified security governance rather than isolated certification silos.

A second direction is human-centered compliance design. The literature on security culture, behavioral cybersecurity, and training makes clear that standards will not produce robust outcomes if they are disconnected from how people work, make decisions, and respond to operational pressure [66–69]. Future models should therefore give greater attention to culture assessment, behavior-aware training, role-specific awareness, and organizational change mechanisms. This is especially important in industrial contexts, where usability problems, workarounds, and procedural bypass can weaken otherwise well-designed technical controls.

A third direction is sector-expanding compliance research. The reviewed studies show that cyber risk governance is no longer limited to traditional ICS and smart-grid environments. Healthcare, maritime systems, automotive cyber-physical platforms, smart buildings, construction systems, and digitally monitored workplaces are all developing distinctive combinations of safety, privacy, reliability, and cybersecurity requirements [54,56,60,64,70,71]. Future standards research should therefore examine how sector-specific overlays can be built without losing the value of shared security principles.

A fourth direction is AI-aware and explainable compliance. Multiple studies show that AI, machine learning, and deep learning are increasingly used for anomaly detection,

predictive maintenance, operational optimization, and cyber defense [72–75]. Yet standards ecosystems still lag behind these developments. Future compliance frameworks will need to address explainability, adversarial robustness, model drift, data governance, false-positive management, and assurance of AI-supported decisions. In industrial environments, this issue is especially important because AI output may influence physical processes and operational judgments with real-world consequences.

A fifth direction is integration of cyber threat intelligence into compliance practice. Threat intelligence literature increasingly emphasizes indicators, knowledge bases, detection logic, and evolving adversary models as tools for proactive defense [73,75]. Future compliance approaches should therefore move beyond static verification of controls and toward more adaptive models in which standard-based governance is informed by changing threat conditions. This would help reduce the gap between audit-based cybersecurity and adversarial reality.

A sixth direction is compliance for distributed, decentralized, and autonomous systems. Research on DER coordination, Vehicle-to-Grid (V2G) ecosystems, federated decision models, and AI-supported grid management shows that future infrastructures will depend more heavily on distributed control, privacy-preserving computation, and platform-based interaction [57–59]. Traditional centralized compliance assumptions may be insufficient in such contexts. More work is needed on how certification and governance can be adapted to decentralized architecture, edge-based intelligence, and multi-actor digital energy services.

A seventh direction is measurement of compliance effectiveness through operational outcomes. Much of the literature still evaluates standards in terms of adoption, conceptual relevance, or structural fit. Future research should examine whether compliance improves measurable outcomes such as incident response speed, operational downtime, resilience, recovery capability, maintenance performance, and detection quality. This would move the field from formal conformity analysis toward evidence-based evaluation of cybersecurity value.

A further reason for this direction is urgent comes from adjacent research on the security of perception-based autonomous and cyber-physical systems. Recent work has demonstrated stealthy, physically realizable attacks against the machine-learning components on which such systems depend: fluorescent-ink adversarial patches that remain invisible until triggered by ultraviolet light can cause traffic-sign-recognition models to misclassify signs [76], ground-view adversarial patches can manipulate the obstacle-detection models used by commercial service robots [77], and analogous fluorescent-ink triggers can implant backdoors in both object detectors and vision-language models while evading common defenses [78]. Although these studies target automotive and consumer-robot settings rather than industrial control systems, they carry a direct lesson for industrial automation: as AI-enabled perception, monitoring, and decision support are integrated into OT environments, the ML layer itself becomes an attack surface that conventional controls do not address. Notably, several of these attacks were shown to survive standard defensive measures, underscoring that AI-aware compliance frameworks will need to account for adversarial robustness, physical-domain manipulation, and assurance of model behavior rather than treating AI components as trusted black boxes.

Finally, a broader direction is the shift toward compliance by design. As digital twins, smart infrastructures, intelligent monitoring systems, and industrial AI continue to expand, cybersecurity requirements will need to be embedded earlier in the lifecycle rather than retrofitted after deployment. Future compliance practice should therefore begin at the stages of procurement, architecture, interoperability design, testing, and maintenance planning. In this sense, compliance is likely to evolve from a proof mechanism into a design discipline for secure industrial transformation.

6. Conclusions

This systematic review examined cybersecurity requirements and certification standards in industrial automation systems, drawing on a corpus of 75 peer-reviewed publications selected through a structured multi-stage screening process. The analysis was organized around a three-dimensional classification perspective, and application context. The findings consistently confirm that industrial cybersecurity is a layered, multi-framework governance problem rather than a problem solvable by any single technical control or standard.

At the technological level, the most recurrently stressed requirements across the examined literature are network segmentation, intrusion detection, secure communication and protocol hardening, access control, PLC and firmware integrity, and patch management. These needs are conceptually different but operationally interdependent: the efficiency of each protective measure depends greatly on the strength of the others. The literature further shows that industrial cybersecurity is shifting away from static perimeter-based protection toward context-aware, layered, and architecture-sensitive models that account for the unique constraints of cyber-physical environments, including real-time operation, long equipment lifecycles, legacy infrastructure, and safety-security interaction.

At the standards and certification level, the report cites ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-82, and NERC-CIP as the most prominent frameworks in industry. These frameworks are the best understood as complementing rather than competing. ISA/IEC 62443 gives the strongest OT-specific and lifecycle-oriented foundation for industrial control systems. ISO/IEC 27001 gives governance framework, organizational responsibility, and auditability across enterprise-wide activities. NIST SP 800-82 contains realistic, implementation-oriented recommendations for ICS and SCADA contexts. NERC-CIP addresses sector-specific reliability and compliance obligations in critical power infrastructure. The central findings are that effective industrial cybersecurity assurance does not emerge from dependence on a single framework, but from building a layered compliance architecture in which governance maturity, industrial suitability, technical guidance, and sectoral obligations are integrated and mutually reinforcing.

The review also calls attention to reoccurring issues. Implementation of multi-framework compliance remains resource-intensive and fragmented, particularly where standards overlap. Rapidly evolving technologies—including IIoT, AI-enabled monitoring, digital twins, and distributed energy systems—continue to outpace standards adoption timetables. Evidence relating formal certification to quantifiable operational security results is limited, especially outside the energy and critical infrastructure areas. We treat this scarcity not as a peripheral caveat but as one of the central findings of the review: the literature on industrial cybersecurity certification has grown rapidly in conceptual and architectural depth, but it has not yet matured into a body of validated cross-sector empirical evidence that links specific certification choices to measurable operational outcomes. This gap should be read as a direct call for future empirical work and as the principal boundary within which the conclusions of any review built on the present corpus must be interpreted. Human and organizational variables offer an underexplored dimension: compliance architectures may fail in practice if responsibilities are unclear, procedures are not followed, or security culture is weak. These gaps set the agenda for future research and practice.

A further methodological limitation of this review is that title and abstract screening was conducted by a single reviewer with cross-checking by co-authors, rather than by two reviewers independently. Because screening was not fully independent and parallel, inter-rater agreement statistics such as Cohen's kappa could not be computed, and the five-criterion quality rubric (Section 2.7) was introduced partly to mitigate this. We recommend that future reviews adopt fully independent dual screening so that formal reliability statistics can be reported.

Overall, this review contributes a consolidated, classification-driven analysis of industrial cybersecurity requirements and certification standards at a time when the field is expanding rapidly but its literature remains fragmented. The three-dimensional framework developed here offers a reproducible basis for future systematic comparisons, and the comparative synthesis of leading compliance frameworks provides practical guidance for organizations seeking to align technical controls, operational realities, and assurance obligations in industrial automation environments.

Author Contributions: Conceptualization, S.Z. and M.A.; methodology, S.Z., A.G., R.R. and M.A.; validation, S.Z., A.G., J.K. and M.A.; formal analysis, J.K., D.C. and M.A.; investigation, S.Z. and M.A.; resources, S.Z., A.G., R.R. and M.A.; data curation, J.K., D.C. and R.R.; writing—original draft preparation, S.Z., A.G., J.K. and M.A.; writing—review and editing, S.Z., A.G., J.K. and M.A.; visualization, S.Z. and A.G.; supervision, M.A.; project administration, D.C. and R.R.; funding acquisition, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the "Technology and Physics Science Excellence Center" (TiFEC) No. S-A-UEI-23-1, financed by the Research Council of Lithuania.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors acknowledge the KTU Center of Excellence in Technological and Physical Sciences (TiFEC) for their support.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
CPS	Cyber-Physical Systems
DCS	Distributed Control System
DER	Distributed Energy Resources
DNP3	Distributed Network Protocol 3
EV	Electric Vehicle
HMI	Human–Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Industrial Control Systems
IDS/IPS	Intrusion Detection Systems/Intrusion Prevention Systems
IIoT	Industrial Internet of Things
ISA/IEC 62443	International Society of Automation/International Electrotechnical Commission 62443
ISO/IEC 27001	International Organization for Standardization/International Electrotechnical Commission 27001
IT	Information Technology
IoT	Internet of Things
LLM	Large Language Model
ML	Machine Learning
NERC-CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST SP 800-82	National Institute of Standards and Technology Special Publication 800-82
OT	Operational Technology
PLC	Programmable Logic Controller
PPE	Personal Protective Equipment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
V2G	Vehicle-to-Grid

References

1. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
2. Jamwal, A.; Agrawal, R.; Sharma, M.; Giallanza, A. Industry 4.0 Technologies for Manufacturing Sustainability: A Systematic Review and Future Research Directions. *Appl. Sci.* **2021**, *11*, 5725. [CrossRef]
3. Peres, R.S.; Jia, X.; Lee, J.; Sun, K.; Colombo, A.W.; Barata, J. Industrial Artificial Intelligence in Industry 4.0—Systematic Review, Challenges and Outlook. *IEEE Access* **2020**, *8*, 220121–220139. [CrossRef]
4. Ghodsian, N.; Benfriha, K.; Olabi, A.; Gopinath, V.; Arnou, A. Mobile Manipulators in Industry 4.0: A Review of Developments for Industrial Applications. *Sensors* **2023**, *23*, 8026. [CrossRef]
5. Gladysz, B.; Tran, T.; Romero, D.; Van Erp, T.; Abonyi, J.; Ruppert, T. Current Development on the Operator 4.0 and Transition towards the Operator 5.0: A Systematic Literature Review in Light of Industry 5.0. *J. Manuf. Syst.* **2023**, *70*, 160–185. [CrossRef]
6. Rojas, L.; Yepes, V.; Garcia, J. Complex Dynamics and Intelligent Control: Advances, Challenges, and Applications in Mining and Industrial Processes. *Mathematics* **2025**, *13*, 961. [CrossRef]
7. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* **2020**, *12*, 157. [CrossRef]
8. Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors* **2023**, *23*, 4117. [CrossRef] [PubMed]
9. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]
10. Zhukabayeva, T.; Zholshiyeva, L.; Karabayev, N.; Khan, S.; Alnazzawi, N. Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors* **2025**, *25*, 213. [CrossRef]
11. Yu, Z.; Gao, H.; Cong, X.; Wu, N.; Song, H.H. A Survey on Cyber–Physical Systems Security. *IEEE Internet Things J.* **2023**, *10*, 21670–21686. [CrossRef]
12. Kayan, H.; Nunes, M.; Rana, O.; Burnap, P.; Perera, C. Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Comput. Surv.* **2022**, *54*, 229. [CrossRef]
13. Alotaibi, I.; Abido, M.A.; Khalid, M.; Savkin, A.V. A Comprehensive Review of Recent Advances in Smart Grids: A Sustainable Future with Renewable Energy Resources. *Energies* **2020**, *13*, 6269. [CrossRef]
14. Alshurideh, M.T.R. Digitization and IoT-Driven Transformation of Smart Buildings. *Int. J. Manag. Mark. Intell.* **2025**, *2*, 26–38. [CrossRef]
15. Li, G.; Ren, L.; Fu, Y.; Yang, Z.; Adetola, V.; Wen, J.; Zhu, Q.; Wu, T.; Candan, K.S.; O'Neill, Z. A Critical Review of Cyber-Physical Security for Building Automation Systems. *Annu. Rev. Control* **2023**, *55*, 237–254. [CrossRef]
16. Ige, A.B.; Kupa, E.; Ilori, O. Best Practices in Cybersecurity for Green Building Management Systems: Protecting Sustainable Infrastructure from Cyber Threats. *Int. J. Sci. Res. Arch.* **2024**, *12*, 2960–2977. [CrossRef]
17. Park, J.; Kang, D. Artificial Intelligence and Smart Technologies in Safety Management: A Comprehensive Analysis Across Multiple Industries. *Appl. Sci.* **2024**, *14*, 11934. [CrossRef]
18. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
19. Bajwa, A.; Tonoy, A.A.R.; Rana, S.; Ahmed, I. Cybersecurity in Industrial Control Systems: A Systematic Literature Review on AI-Based Threat Detection for Scada and IOT Networks. *Am. Sch. Res. Conf.* **2025**, *1*, 1–15. [CrossRef]
20. Du, D.; Zhu, M.; Li, X.; Fei, M.; Bu, S.; Wu, L.; Li, K. A Review on Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyber-Physical Power Systems. *J. Mod. Power Syst. Clean Energy* **2023**, *11*, 727–743. [CrossRef]
21. Ododo, F.R.; Sadiq, R.R.; Addotey, N. Adversarial Threats in Industrial Control Systems: A Machine Learning Approach to Securing the U.S. Energy Grid. *J. Sci. Innov. Technol. Res.* **2025**, *8*, 136–145. [CrossRef]
22. Heidari, A.; Jabraeil Jamali, M.A. Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions. *Clust. Comput.* **2023**, *26*, 3753–3780. [CrossRef]
23. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
24. Salem, A.H.; Azzam, S.M.; Emam, O.E.; Abohany, A.A. Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques. *J. Big Data* **2024**, *11*, 105. [CrossRef]
25. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process. *EURASIP J. Info. Secur.* **2020**, *2020*, 8. [CrossRef]
26. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A Review of Cyber Security Risk Assessment Methods for SCADA Systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
27. Ribas Monteiro, L.F.; Rodrigues, Y.R.; Zambroni De Souza, A.C. Cybersecurity in Cyber–Physical Power Systems. *Energies* **2023**, *16*, 4556. [CrossRef]

28. Rodriguez-Casavilca, H.M.; Mauricio, D.; Villanueva, J.M.M. Evolution of Artificial Intelligence-Based OT Cybersecurity Models in Energy Infrastructures: Services, Technical Means, Facilities and Algorithms. *Energies* **2025**, *18*, 5163. [CrossRef]
29. Ayodeji, A.; Mohamed, M.; Li, L.; Di Buono, A.; Pierce, I.; Ahmed, H. Cyber Security in the Nuclear Industry: A Closer Look at Digital Control Systems, Networks and Human Factors. *Prog. Nucl. Energy* **2023**, *161*, 104738. [CrossRef]
30. Adeoye, M.B.; Annankra, J.A.; Yakin, Z. A Review of Programmable Logic Controllers in Advanced Nuclear Plant Automation: Challenges and Future Prospects. *Int. J. Frontline Res. Sci. Technol.* **2025**, *5*, 001–008. [CrossRef]
31. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive Survey and Taxonomies of False Data Injection Attacks in Smart Grids: Attack Models, Targets, and Impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [CrossRef]
32. Chen, J.; Yan, J.; Kemmeugne, A.; Kassouf, M.; Debbabi, M. Cybersecurity of Distributed Energy Resource Systems in the Smart Grid: A Survey. *Appl. Energy* **2025**, *383*, 125364. [CrossRef]
33. Tatipatri, N.; Arun, S.L. A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. *IEEE Access* **2024**, *12*, 18147–18167. [CrossRef]
34. Rekeraho, A.; Cotfas, D.T.; Cotfas, P.A.; Bălan, T.C.; Tuyishime, E.; Acheampong, R. Cybersecurity Challenges in IoT-Based Smart Renewable Energy. *Int. J. Inf. Secur.* **2024**, *23*, 101–117. [CrossRef]
35. Khan, H.U.; Khan, R.A.; Alwageed, H.S.; Almagrabi, A.O.; Ayouni, S.; Maddeh, M. AI-Driven Cybersecurity Framework for Software Development Based on the ANN-ISM Paradigm. *Sci. Rep.* **2025**, *15*, 13423. [CrossRef]
36. Wylde, V.; Rawindaran, N.; Lawrence, J.; Balasubramanian, R.; Prakash, E.; Jayal, A.; Khan, I.; Hewage, C.; Platts, J. Cybersecurity, Data Privacy and Blockchain: A Review. *SN Comput. Sci.* **2022**, *3*, 127. [CrossRef]
37. Mtukushe, N.; Onaolapo, A.K.; Aluko, A.; Dorrell, D.G. Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems. *Energies* **2023**, *16*, 5206. [CrossRef]
38. Lal, M.D.; Varadarajan, R. A Review of Machine Learning Approaches in Synchrophasor Technology. *IEEE Access* **2023**, *11*, 33520–33541. [CrossRef]
39. Zhang-Kennedy, L.; Chiasson, S. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.* **2022**, *54*, 12. [CrossRef]
40. Zhang, J.; Bu, H.; Wen, H.; Liu, Y.; Fei, H.; Xi, R.; Li, L.; Yang, Y.; Zhu, H.; Meng, D. When LLMs Meet Cybersecurity: A Systematic Literature Review. *Cybersecurity* **2025**, *8*, 55. [CrossRef]
41. Werbińska-Wojciechowska, S.; Winiarska, K. Maintenance Performance in the Age of Industry 4.0: A Bibliometric Performance Analysis and a Systematic Literature Review. *Sensors* **2023**, *23*, 1409. [CrossRef]
42. Nguyen, T.; Gosine, R.G.; Warrian, P. A Systematic Review of Big Data Analytics for Oil and Gas Industry 4.0. *IEEE Access* **2020**, *8*, 61183–61201. [CrossRef]
43. Cui, Y.; Kara, S.; Chan, K.C. Manufacturing Big Data Ecosystem: A Systematic Literature Review. *Robot. Comput.-Integr. Manuf.* **2020**, *62*, 101861. [CrossRef]
44. Satka, Z.; Ashjaei, M.; Fotouhi, H.; Daneshtalab, M.; Sjödin, M.; Mubeen, S. A Comprehensive Systematic Review of Integration of Time Sensitive Networking and 5G Communication. *J. Syst. Archit.* **2023**, *138*, 102852. [CrossRef]
45. Vukicevic, A.M.; Petrovic, M.; Milosevic, P.; Peulic, A.; Jovanovic, K.; Novakovic, A. A Systematic Review of Computer Vision-Based Personal Protective Equipment Compliance in Industry Practice: Advancements, Challenges and Future Directions. *Artif. Intell. Rev.* **2024**, *57*, 319. [CrossRef]
46. Alzahrani, N.M.; Alfouzan, F.A. Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review. *Sensors* **2022**, *22*, 2792. [CrossRef]
47. Islam, T.; Mission, R.; Refat, K.; Kynatun, M. Cybersecurity Risk Assessment Frameworks For Engineering Databases: A Systematic Literature Review. *Strateg. Data Manag. Innov.* **2025**, *2*, 224–243. [CrossRef]
48. Wiboonrat, M. Cybersecurity of Industrial Automation and Control System (IACS) Networks in Biomass Power Plants. In *Proceedings of the 2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE), Helsinki, Finland, 19–21 June 2023*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.
49. Nishant, R.; Kennedy, M.; Corbett, J. Artificial Intelligence for Sustainability: Challenges, Opportunities, and a Research Agenda. *Int. J. Inf. Manag.* **2020**, *53*, 102104. [CrossRef]
50. Jarwar, M.A.; Watson, J.; Ali, S. Modeling Industrial IoT Security Using Ontologies: A Systematic Review. *IEEE Open J. Commun. Soc.* **2025**, *6*, 2792–2821. [CrossRef]
51. Cindrić, I.; Jurčević, M.; Hadjina, T. Mapping of Industrial IoT to IEC 62443 Standards. *Sensors* **2025**, *25*, 728. [CrossRef]
52. Culot, G.; Nassimbeni, G.; Podrecca, M.; Sartor, M. The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda. *TQM J.* **2021**, *33*, 76–105. [CrossRef]
53. Marat Muratuly, C. Methodology for the Implementation and Operation of Multivendor Automation Systems at Large-Scale Industrial Facilities. *Univers. Libr. Eng. Technol.* **2025**, *2*, 89–93. [CrossRef]
54. Luo, F.; Zhang, X.; Yang, Z.; Jiang, Y.; Wang, J.; Wu, M.; Feng, W. Cybersecurity Testing for Automotive Domain: A Survey. *Sensors* **2022**, *22*, 9211. [CrossRef] [PubMed]

55. Gabbar, H.; Othman, A.; Abdussami, M. Review of Battery Management Systems (BMS) Development and Industrial Standards. *Technologies* **2021**, *9*, 28. [CrossRef]
56. Jørgensen, B.N.; Ma, Z.G. Impact of EU Laws on the Adoption of AI and IoT in Advanced Building Energy Management Systems: A Review of Regulatory Barriers, Technological Challenges, and Economic Opportunities. *Buildings* **2025**, *15*, 2160. [CrossRef]
57. Huo, X.; Huang, H.; Davis, K.R.; Poor, H.V.; Liu, M. A Review of Scalable and Privacy-Preserving Multi-Agent Frameworks for Distributed Energy Resources. *Adv. Appl. Energy* **2025**, *17*, 100205. [CrossRef]
58. Ahmad, B.; Ding, J.; Ali, T.; Sarwatt, D.S.; Arshad, R.; Philipo, A.G.; Ning, H. Vehicle-to-Grid Integration: Ensuring Grid Stability, Strengthening Cybersecurity, and Advancing Energy Market Dynamics. *arXiv* **2025**, arXiv:2509.13393.
59. Razzaque, M.A.; Khadem, S.K.; Patra, S.; Okwata, G.; Noor-A-Rahim, M. Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review. *Appl. Energy* **2025**, *398*, 126364. [CrossRef]
60. Sedar, R.; Kalalas, C.; Vazquez-Gallego, F.; Alonso, L.; Alonso-Zarate, J. A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths. *IEEE Open J. Commun. Soc.* **2023**, *4*, 325–391. [CrossRef]
61. Ige, A.B.; Kupa, E.; Ilori, O. Analyzing Defense Strategies against Cyber Risks in the Energy Sector: Enhancing the Security of Renewable Energy Sources. *Int. J. Sci. Res. Arch.* **2024**, *12*, 2978–2995. [CrossRef]
62. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.-S.; et al. A Review of Cyber–Physical Security for Photovoltaic Systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 4879–4901. [CrossRef]
63. Ledmaoui, Y.; El Maghraoui, A.; El Aroussi, M.; Saadane, R. Review of Recent Advances in Predictive Maintenance and Cybersecurity for Solar Plants. *Sensors* **2025**, *25*, 206. [CrossRef]
64. Wasserman, L.; Wasserman, Y. Hospital Cybersecurity Risks and Gaps: Review (for the Non-Cyber Professional). *Front. Digit. Health* **2022**, *4*, 862221. [CrossRef]
65. Ba, L.; Tangour, F.; El Abbassi, I.; Absi, R. Analysis of Digital Twin Applications in Energy Efficiency: A Systematic Review. *Sustainability* **2025**, *17*, 3560. [CrossRef]
66. Uchendu, B.; Nurse, J.R.C.; Bada, M.; Furnell, S. Developing a Cyber Security Culture: Current Practices and Future Needs. *Comput. Secur.* **2021**, *109*, 102387. [CrossRef]
67. Maalem Lahcen, R.A.; Caulkins, B.; Mohapatra, R.; Kumar, M. Review and Insight on the Behavioral Aspects of Cybersecurity. *Cybersecurity* **2020**, *3*, 10. [CrossRef]
68. Amjad, K.; Ishaq, K.; Nawaz, N.A.; Rosdi, F.; Dogar, A.B.; Khan, F.A. Unlocking Cybersecurity: A Game-Changing Framework for Training and Awareness—A Systematic Review. *Hum. Behav. Emerg. Technol.* **2025**, *2025*, 9982666. [CrossRef]
69. Prümmer, J.; Van Steen, T.; Van Den Berg, B. A Systematic Review of Current Cybersecurity Training Methods. *Comput. Secur.* **2024**, *136*, 103585. [CrossRef]
70. Akinosho, T.D.; Oyedele, L.O.; Bilal, M.; Ajayi, A.O.; Delgado, M.D.; Akinade, O.O.; Ahmed, A.A. Deep Learning in the Construction Industry: A Review of Present Status and Future Innovations. *J. Build. Eng.* **2020**, *32*, 101827. [CrossRef]
71. Bolbot, V.; Kulkarni, K.; Brunou, P.; Banda, O.V.; Musharraf, M. Developments and Research Directions in Maritime Cybersecurity: A Systematic Literature Review and Bibliometric Analysis. *Int. J. Crit. Infrastruct. Prot.* **2022**, *39*, 100571. [CrossRef]
72. Alzahrani, A.; Aldhyani, T.H.H. Design of Efficient Based Artificial Intelligence Approaches for Sustainable of Cyber Security in Smart Industrial Control System. *Sustainability* **2023**, *15*, 8076. [CrossRef]
73. Saeed, S.; Suayyid, S.A.; Al-Ghamdi, M.S.; Al-Muhaisen, H.; Almuhaideb, A.M. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors* **2023**, *23*, 7273. [CrossRef] [PubMed]
74. Wiafe, I.; Koranteng, F.N.; Obeng, E.N.; Assyne, N.; Wiafe, A.; Gulliver, S.R. Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access* **2020**, *8*, 146598–146612. [CrossRef]
75. Cascavilla, G.; Tamburri, D.A.; Van Den Heuvel, W.-J. Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review. *Comput. Secur.* **2021**, *105*, 102258. [CrossRef]
76. Yuan, S.; Han, X.; Li, H.; Xu, G.; Jiang, W.; Ni, T.; Zhao, Q.; Fang, Y. The Fluorescent Veil: A Stealthy and Effective Physical Adversarial Patch Against Traffic Sign Recognition. *Adv. Neural Inf. Process. Syst.* **2026**, *38*, 98864–98890.
77. Yuan, S.; Xu, G.; Li, H.; Zhang, R.; Cao, H.; Qian, X.; Ni, T.; Zhao, Q.; Fang, Y. No Trespassing: Ground-View Adversarial Patches for Privacy-Aware Management in COTS Robot Vacuum Cleaner. *IEEE Trans. Dependable Secur. Comput.* **2025**, *23*, 17–33. [CrossRef]
78. Yuan, S.; Xu, G.; Li, H.; Zhang, R.; Qian, X.; Cao, H.; Zhao, Q. FIGhost: Fluorescent Ink-Based Stealthy and Flexible Backdoor Attacks on Physical Traffic Sign Recognition. *IEEE Trans. Dependable Secur. Comput.* **2026**, *23*, 6522–6535. [CrossRef]