ISSN: 1692-7257 - Volume 2 – Number 48 - 2026

RCTA Revista Colombiana de Tecnologías de Avanzada UNIPAMPLONA

Digital Object Identifier: 10.24054/rcta.v2i48.4366

Quantum resilience in critical infrastructures: cryptographic agility versus legacy hardware obsolescence

Resiliencia cuántica en infraestructuras críticas: agilidad criptográfica frente a la obsolescencia del hardware heredado

MSc. Katerine Márceles Villalba[1], PhD. César Jesús Pardo Calvache[2], PhD.(c) Siler Amador Donado[2]

[1] ***Universidad de Antioquia,*** *Facultad de Ingeniería, Grupo de Investigación In2Lab, Medellín, Antioquia, Colombia.*
[2]***Universidad del Cauca,*** *Facultad de Ingeniería Electrónica y Telecomunicaciones, Grupo de Investigación GTI. Popayán, Cauca, Colombia.*

Correspondence: *katerine.marceles@udea.edu.co*

Received: *february 22, 2026.* ***Accepted:*** *june 09, 2026.* ***Published:*** *july 03, 2026.*

How to cite: *K. Márceles Villalba, C. Pardo Calvache, and S. Amador Donado, "Quantum resilience in critical infrastructures: cryptographic agility versus legacy hardware obsolescence", RCTA, vol. 2, n.º. 48, pp. 30–44, jul. 2026. Recovered from https://ojs.unipamplona.edu.co/index.php/rcta/article/view/4366*

Abstract: Context: Quantum computing represents an emerging and increasingly relevant threat to the security of Cyber-Physical Systems (CPS) in critical infrastructure (CI), potentially compromising current cryptographic methods and exposing essential services to significant physical risks. Objective: This study analyzes the impact of the quantum threat on CPS and CI to identify semantic and technical requirements that underpin ontological assessment models and operational resilience strategies. Method: A systematic literature review (SLR) was conducted for the period 2020–2026 following the PRISMA and Kitchenham protocols. Through a parameterized search in high-impact databases, 39 primary studies were selected and analyzed. Results: A relevant systemic incompatibility was identified: a significant proportion of the analyzed studies report that legacy hardware (PLCs and RTUs) presents critical limitations in supporting the computational load of the new Post-Quantum Cryptography (PQC) standards. This limitation tends to generate operational latencies that could compromise the system's theoretical resilience against retrospective decryption and spoofing attacks. Conclusions: The evidence reviewed suggests that the effectiveness of defense frameworks could be compromised without a structural upgrade of Operational Technology (OT), as the mismatch between obsolete hardware and quantum mathematical rigor was identified as one of the weakest links in the infrastructure. The findings indicate that the operational resilience of CI would be strengthened through migration toward cryptographic agility and the adoption of ontological models that enable automated reasoning for real-time threat detection.

Keywords: critical infrastructures, cyber-physical resilience, cyber-physical systems, cybersecurity, industrial control systems, ontologies, operational technology, post-quantum cryptography, quantum era.

Resumen: Contexto: La computación cuántica representa una amenaza emergente y de

creciente relevancia para la seguridad de los Sistemas Ciberfísicos (SCF) en infraestructuras críticas (IC), lo que podría comprometer progresivamente los métodos criptográficos actuales y exponer servicios esenciales a riesgos físicos significativos. Objetivo: Este estudio analiza el impacto de la amenaza cuántica en SCF e IC para identificar requerimientos semánticos y técnicos que fundamenten modelos de evaluación ontológicos y estrategias de resiliencia operativa. Método: Se realizó una revisión sistemática de la literatura (RSL) del periodo 2020-2026 siguiendo los protocolos PRISMA y Kitchenham. A través de una búsqueda parametrizada en bases de datos de alto impacto, se seleccionaron y analizaron 39 estudios primarios. Resultados: Se identificó una incompatibilidad sistémica relevante: una proporción significativa de los estudios analizados reporta que el hardware heredado (PLCs y RTUs) presenta limitaciones críticas para soportar la carga computacional de los nuevos estándares de Criptografía Post-Cuántica (PQC). Esta limitación tiende a generar latencias operativas que podrían comprometer la resiliencia teórica del sistema frente a ataques de descifrado retrospectivo y suplantación de identidad. Conclusiones: La evidencia analizada sugiere que la eficacia de los marcos de defensa podría verse comprometida sin una actualización estructural de la tecnología de operación (OT), dado que el desfase entre el hardware obsoleto y el rigor matemático cuántico se identificó como uno de los eslabones más débiles de la infraestructura. Los hallazgos indican que la resiliencia operativa de las IC se vería fortalecida mediante la migración hacia la agilidad criptográfica y la adopción de modelos ontológicos que permitan el razonamiento automatizado para la detección de amenazas en tiempo real.

Palabras clave: ciberseguridad, criptografía post-cuántica, era cuántica, infraestructuras críticas, ontologías, resiliencia ciberfísica, sistemas ciberfísicos, sistemas de control industrial, tecnologías de operación.

1. INTRODUCTION

The Fourth Industrial Revolution has consolidated a significant articulation between the physical and digital domains through Cyber-Physical Systems (CPS). These systems have established themselves as the operational core of Critical Infrastructures (CI), spanning vital sectors such as energy, healthcare, transportation, and finance, among others. By integrating sensors, actuators, and distributed computing capabilities, CPS ensure the continuity of essential services for society [1], [2].

However, the transition toward hyper-connected environments supported by technologies such as the Industrial Internet of Things (IIoT), Artificial Intelligence, 5G networks, and Blockchain architectures has generated an expanded attack surface, transforming digital vulnerabilities into physical risks with tangible consequences [3]-[5].

For decades, trust in these ecosystems has relied on public-key protocols such as RSA (Rivest, Shamir, and Adleman) and Elliptic Curve Cryptography (ECC). Despite this, the emergence of quantum computing has triggered a paradigm shift in system security. Shor's algorithm possesses the theoretical capacity to break these schemes in polynomial time, representing an existential threat to the integrity of Industrial Control Systems (ICS) [6], [7]. Notwithstanding the urgency of this scenario, a critical gap persists in the scientific literature; most research is limited to analyzing algorithms in isolation, ignoring the technical complexity of implementing Post-Quantum Cryptography (PQC) in infrastructures with legacy components and latency-constrained protocols such as Modbus or SCADA [8], [9].

This gap becomes evident when contrasting the present review with the most representative works in the field (see Table 1). El-Kady et al. [7] and Turk et al. [18] address CPS cybersecurity from an organizational and risk management perspective, but neither incorporates the quantum threat nor critical infrastructures as an application domain. At the opposite end, reviews focused on quantum cryptography, such as those by Babu et al. [23] and Vasani et al. [37], delve into authentication and quantum communication protocols for IoT, but do not address CI resilience nor employ semantic models for its evaluation. The works closest to the present study are those of Sarker et al. [17], who propose an explainable AI taxonomy for CPS and

CI with a first level of semantic modeling, and Ahmad et al. [38], who integrate quantum-safe cybersecurity, CPS and CI in smart microgrids; however, neither of them simultaneously combines the four axes —quantum threat, CPS, CI and cybersecurity ontologies— that underpin this study. This absence of conceptual integration constitutes the specific knowledge gap that the present review seeks to close.

Table 1 synthesizes this comparison across four analytical dimensions —quantum threat/PQC, resilience in critical infrastructures, cybersecurity ontologies and cyber-physical systems—, evaluated in each study under the following convention: the symbol ✓ indicates that the dimension is addressed explicitly and centrally in the study; the symbol X indicates that the dimension is not addressed; and the label "Partial" is reserved for cases in which the study touches on the dimension incidentally, without constituting a substantive methodological contribution to that dimension. The last row, corresponding to the present review, allows visualizing that no prior work satisfies all four dimensions simultaneously.

Table 1: *Dimension Comparison.*

Study	Year	Focus	A	B	C	D
Turk et al. [18]	2021	Systemic IT/OT/CPS framework (Parker Hexagon).	x	x	x	✓
El-Kady et al. [7]	2023	Safety and security challenges in CPS.	x	x	x	✓
Babu et al. [23]	2024	Taxonomy of quantum-attack-resistant AKA protocols for IoT.	✓	x	x	x
Vasani et al. [37]	2024	Quantum communication and cryptography (QKD).	✓	x	x	x
Sarker et al. [17]	2024	Rule-based AI taxonomy for cybersecurity in CI.	x	✓	P	✓
Wicaksana [35]	2025	Quantum-safe blockchain security infrastructure.	✓	✓	x	x
Singh et al. [26]	2025	Cyber resilience in e-government.	✓	✓	x	x
Lezzi et al. [9]	2025	AI for sustainable cybersecurity in industry.	x	✓	x	✓
Ahmad et al. [38]	2025	Quantum-safe cybersecurity in smart microgrids (blockchain-FL).	✓	✓	x	✓
This study	2026	Ontological assessment model for quantum resilience in CPS and CI.	✓	✓	✓	✓

Abbreviations: **A** = Quantum Threat / PQC, **B** = Resilience in CI, **C** = Cybersecurity Ontologies, **D** = Cyber-Physical Systems (CPS), **P** = Partial.

Source: Developed by the authors.

The relevance of this research extends beyond mere data protection; it is about maintaining systemic resilience. A security compromise derived from quantum strengths could trigger cascading failures in energy grids, compromising national stability and human safety [10], [11]. Therefore, the development of evaluation frameworks that articulate physical security with cybersecurity constitutes a strategic necessity [12], [13].

Under this premise, the present research is grounded in Cyber-Physical Resilience and Lattice-based Cryptography, the central pillar of NIST standardization for the transition toward quantum-resistant algorithms, such as Crystals-Kyber (standardized as ML-KEM in FIPS 203) and Crystals-Dilithium (standardized as ML-DSA in FIPS 204) [9], [14], [44], [45]. The integration of these solutions is vital to ensure interoperability in modern infrastructures, such as smart microgrids, where technological decentralization demands a robust defense against persistent threats [1], [15].

The scope of this review ranges from elementary cryptographic lines, technical threat characterization, and standards recognition to the integration of Semantic Models (Ontologies). The use of these models allows for the transformation of raw data into actionable knowledge, facilitating transparent decision-making in environments of high uncertainty [16], [17]. Thus, the study analyzes not only algorithmic complexity but also the system's intelligent response capacity to intrusions and operational failures [10], [18].

The central purpose of this article is to characterize—through a systematic literature review the standards, defense mechanisms, and evaluation metrics that facilitate the transition toward resilient infrastructures. It seeks to consolidate a technical roadmap that harmonizes hardware innovations, network robustness, and semantic models [19], [20]. To ensure scientific rigor, the process followed a hybrid protocol based on PRISMA 2020 and Kitchenham's guidelines, analyzing global scientific production between 2020 and 2026.

Finally, the remainder of the article is structured as follows: Section 2 describes the methodology; Section 3 presents the obtained results; Section 4 develops the discussion and limitations; and Section 5 presents the conclusions and future projections.

2. METHODOLOGY

This study adopted a hybrid methodological protocol that integrated the guidelines of Kitchenham and Brereton [21] with the transparency standards of PRISMA 2020 [22], complemented by the Goal-Question-Metric (GQM) model for the formulation and validation of research questions. This protocol ensured bias neutralization during the phases of question

formulation, source selection and pertinence evaluation. The complete activity flow is available for public consultation in the Zenodo repository [https://doi.org/10.5281/zenodo.18705771].

The synergy of these protocols facilitated the neutralization of bias during the formulation of questions, source selection, and relevance assessment, ensuring a precise delimitation of institutional and technical objectives [23], [24].

With the purpose of demonstrating reproducibility, the detailed workflow of the activities performed has been hosted in the Zenodo repository: https://doi.org/10.5281/zenodo.18705771.

The study focused on reviewing scientific research published between 2020 and 2026, prioritizing investigations that addressed the critical intersection among CPS, cybersecurity, and the disruptive effects of quantum computing on CI [17], [20]. Since the integration of quantum security into industrial environments is a recent discipline, a limited availability of specialized open-access sources was identified. Nonetheless, given its relevance, a search for peer-reviewed articles in high-impact databases was deemed necessary, thereby ensuring a robust characterization of the studied domain [9], [25], [26].

The activities carried out at each stage of the protocol, as applied to this research, are described below:

- *Definition of Objectives and Research Questions.* The central objective of this review was to analyze standards, frameworks, and emerging threats to characterize the key requirements for achieving resilience in the quantum era for CPS in CI. To achieve this purpose, the following search objectives were established:

Ob1: To determine the influence of quantum technologies on the evolution of cybersecurity practices for critical infrastructures.

Ob2: To determine the requirements for developing an ontology-based evaluation model for cybersecurity in CPS and CI.

The research questions were formulated using the GQM method [21] (see Table 2), grounded in the PICOC approach [27] (Population, Intervention, Comparison, Outcome, and Context) and validated through the FINER criteria [28] (Feasible, Interesting, Novel, Ethical, and Relevant). It is worth noting that the questions underwent expert evaluation before their final application.

Table 2: *Question, Metric, and Motivation.*

ID	Question	Metric	Motivation
Ob1.	Q1: Q1: How does quantum computing affect current cybersecurity practices and standards in CPS and CI?	Number of articles discussing the effects of quantum computing on cybersecurity models.	To analyze the impact of quantum computing on cybersecurity practices within CPS and CI.
Ob2.	Q2: What are the key requirements for developing an ontological cybersecurity evaluation model for CPS and CI?	Characterization of attributes, relationships, and semantic abstraction levels proposed for asset and risk representation.	To determine the structural components and logical reasoning necessary for a resilient semantic evaluation model.

Abbreviations used: Objective (Ob), Question (Q).
Source: Developed by the authors.

- *Literature Search:* Three specialized databases were selected for the identification of scientific studies: IEEE Xplore, ACM Digital Library and ScienceDirect. This choice was not arbitrary, but rather the result of a thematic coverage analysis conducted prior to the formal search. IEEE Xplore concentrates relevant scientific output in industrial control systems, critical infrastructure cybersecurity and embedded systems, serving as the primary reference source for IEEE publications in electrical engineering and industrial computing. ACM Digital Library is the primary repository for applied cryptography, security protocols and computer science, where most PQC research at the implementation level is published. ScienceDirect (Elsevier) provides interdisciplinary coverage in applied engineering, IoT security and cyber-physical systems from an applied sciences perspective.

The exclusion of Scopus and Web of Science was due to both being secondary indexing platforms that aggregate records from multiple sources, including IEEE and ACM. Their simultaneous use alongside the selected primary databases would have significantly increased the volume of duplicates without adding exclusive specialized sources within the studied domain, thereby affecting the efficiency of the protocol. Regarding SpringerLink, a preliminary scoping search confirmed that its coverage at the specific intersection of PQC, ICS/OT and critical infrastructures was considerably lower than that of the three selected sources, with a high proportion of results not

pertinent to the technical domain of this review. Search strings were designed using Boolean operators, adapting the syntax to the technical parameters of each search engine under the PICOC framework (see Table 3).

Table 3: *PICOC Framework*

Element	Description	Search Term
P (Population)	Cyber-physical systems and critical infrastructures.	("cyber-physical systems" OR "CPS" OR "industrial control systems" OR "ICS" OR "SCADA" OR "operational technology" OR "OT")
I(Intervention)	Post-quantum cryptography, ontological models and cybersecurity assessment frameworks.	("post-quantum cryptography" OR "PQC" OR "quantum-safe" OR "lattice-based cryptography" OR "ontology" OR "semantic model" OR "cybersecurity evaluation model" OR "assessment framework")
C(Comparison)	Existing best practices and standards in industrial and cryptographic secur	("cybersecurity framework" OR "NIST standard" OR "cryptographic standard" OR "security best practices" OR "quantum-resistant")
O (Outcome)	Identification of improvement opportunities in system resilience	("resilience" OR "threat mitigation" OR "vulnerability assessment" OR "quantum resilience" OR "cryptographic agility")
C (Context)	Critical Infrastructure sectors AND/OR Quantum Era.	"quantum computing" OR "quantum threat" OR "quantum era" OR "critical infrastructure" OR "post-quantum transition")

Source: Developed by the authors.

Based on the PICOC elements, the following general search string was consolidated and applied as a conceptual basis across the selected databases:

("cyber-physical systems" OR "ICS" OR "SCADA" OR "OT") AND ("post-quantum cryptography" OR "PQC" OR "quantum-safe" OR "lattice-based") AND ("critical infrastructure" OR "resilience" OR "ontology" OR "cybersecurity")

This string was adapted to the specific syntax of each database (IEEE Xplore, ACM Digital Library and ScienceDirect), adjusting operators, search fields and truncations according to the technical parameters of each platform. The complete records of the database-specific adapted strings, together with the detail of the applied filters, are available in the Zenodo repository: [https://doi.org/10.5281/zenodo.20802392].

Following the application of the search strings, an initial universe of 841 records was identified. The cleaning process began with the removal of 147 duplicates, consolidating a set of 694 unique articles for evaluation. Subsequently, a preliminary screening was performed through a technical review of titles and abstracts, resulting in the exclusion of 539 articles that did not have a direct relationship with the core theme. This phase yielded a sample of 155 potential studies, distributed as follows: 47 from IEEE Xplore, 18 from ACM, and 90 from ScienceDirect.

Next, the inclusion and exclusion criteria defined in Table 4 were applied.

Table 4: *Inclusion and exclusion criteria.*

Inclusion Criteria	Exclusion Criteria
Articles regarding cybersecurity in cyber-physical systems and CI.	Articles not addressing cybersecurity in CPS and CI.
Articles on the use of ontology-based evaluation models.	Articles that do not mention ontological models or their application in cybersecurity.
Studies on the impact of quantum computing on CPS and CI cybersecurity.	Articles that do not consider quantum threats or quantum cybersecurity.
Articles published between 2020 and 2026.	Books, theses, or non-peer-reviewed articles.
Articles published in English.	Articles in languages other than English.
Articles addressing how ontological models, security best practices, and cybersecurity frameworks can be applied to prevent attacks in CPS and CI, with a focus on the quantum era.	Articles that do not focus on ontological models, security best practices, and cybersecurity frameworks applicable to preventing attacks in CPS and CI.

Source: Developed by the authors.

This process culminated in the identification of 52 relevant articles, of which 103 were excluded for failing to satisfactorily meet the required depth criteria. It is important to emphasize that this process revealed a marked scarcity of specialized literature integrating quantum cybersecurity, CPS, and CI, underscoring the need to consolidate dispersed knowledge to strengthen the resilience of critical infrastructures.

The selection of studies was conducted through a sequential and validated process. To ensure the rigor of the review, a structured assessment matrix was introduced to evaluate the quality of the potential articles. This tool enabled an analytical judgment-based approach, ensuring that each selected study made a significant contribution to the objectives of the review.

Each article underwent a quali-quantitative weighting system, assigning scores of 1.0 (Complies - High Quality), 0.5 (Partially complies - Moderate Quality), and 0 (Does not comply - Irrelevant). This method allowed for the quantification of finding relevance and the establishment of a minimum selection threshold of ≥ 0.75, ensuring that the review process remained systematic, reproducible, and free from individual bias.

- *Relevance Assessment*: To ensure the robustness of the selected evidence, a relevance assessment methodology based on four dimensions clarity, rigor, relevance, and credibility was applied, following the recommendations of Kitchenham et al. [21].

This approach facilitated both a qualitative and quantitative evaluation of each document, ensuring the identification of studies with high scientific value and enabling the mitigation of biases during the final selection phase.

Each article was individually evaluated using a scoring scale from 0 to 1 per criterion, employing the following weighting system to facilitate technical comparison:

- Fully met (1.0 point): The study fully satisfied the criterion.
- Partially met (0.5 points): The information was mentioned but lacked depth.
- Did not meet (0 points): The criterion was absent or not relevant.

The specific criteria that guided this technical evaluation were:

- **Clarity:** Did the article clearly state its objectives, focusing on the intersection of quantum cybersecurity, CPS, CI, or ontological modeling?
- **Rigor:** Is the methodological design explicit enough to allow for replicability and coherence with the stated objectives?
- **Relevance:** Did the findings present applicable contributions to the advancement of post-quantum security or propose future research paths for critical infrastructures?
- **Credibility:** Did the research justify its approach and present results that are coherent and consistent with its initial premises?

Following the assessment, the scores were consolidated into an aggregate scale from 0 to 4 points to determine the relevance level, establishing an acceptance threshold for final inclusion (see Table 5):

Table 5: *Relevance Level.*

Score range	Relevance level	Technical decision
<= 2.0	Moderate	Excluded
2.1 – 3.1	Medium	Detailed review
>= 3.2	High	Included as primary study

Source: Developed by the authors.

The acceptance threshold was set at ≥ 3.2 points on a maximum scale of 4.0, based on a global compliance requirement of 80%. Since the evaluation encompasses four dimensions with a maximum value of 1.0 each (clarity, rigor, relevance and credibility), a score of 3.2 implies that the study must fully satisfy at least three criteria and partially meet the fourth. This threshold was chosen because it ensures that no included study lacks methodological rigor or direct thematic relevance, two non-negotiable dimensions in a review addressing a technical domain as specific as post-quantum cryptography in cyber-physical systems. Studies scoring between 2.1 and 3.1 were subjected to an additional detailed review and ultimately excluded, unless they provided unique evidence not reported in higher-scoring studies. This decision was documented in the extraction matrix available in the Zenodo repository: [https://doi.org/10.5281/zenodo.18706471].

This process ensured that only research with significant methodological robustness and thematic relevance was included in the final compendium. As a result, 39 articles exceeded the relevance threshold and were classified as the primary studies for this review (see the review traceability in Fig. 1). It is important to mention that although the GRADE system was not formally used, an equivalent three-level classification high, medium and low was adopted and duly documented in the data extraction matrix. This screening procedure allowed for the proper prioritization and filtering of the studies.

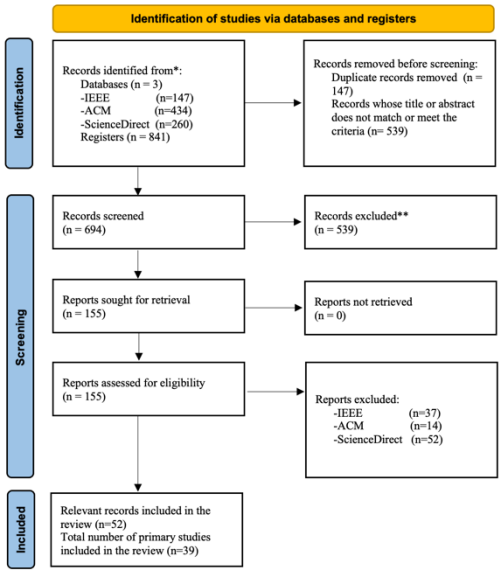

Fig. 1. *Study identification traceability.*
Source: *Developed by the authors.*

- *Data Extraction:* Data extraction was executed systematically, using the research questions and objectives defined in the initial phase of the protocol as a reference. To this end, a structured collection instrument was employed, which included fundamental fields such as unique article identifier (ID), title, publication source, abstract, keywords, research type, country of origin, as well as direct mapping to the research questions and objectives are available in the Zenodo repository: [https://doi.org/10.5281/zenodo.20802749].

This procedure allowed for the characterization of standards applied to CPS and CI, in addition to identifying emerging vulnerabilities linked to quantum computing. Furthermore, the disruptive impact of quantum technologies on critical infrastructures was analyzed, collecting the technical elements necessary to propose an ontology that provides a universal semantic definition of attacks, vulnerabilities, and risks within this new paradigm. The data obtained constituted the key inputs to demonstrate which primary studies supported the fulfillment of the global research objectives, ensuring traceability between the analyzed literature and the results presented.

- *Synthesis and Analysis of Results:* The analysis of the collected data revealed exponential growth in academic production related to quantum cybersecurity in CPS and CI. As observed in Figure 2, scientific interest intensified significantly toward the end of the study period, highlighting 2025 as the year of highest productivity with 17 articles (43.6%), followed by 2024 with 11 studies (28.2%). However, it is important to clarify that for the year 2026, partial results are presented, as only studies from the first month of the year (January) were included; therefore, Fig. 2 reflects a decline, though it is inferred that studies will continue to rise by the end of the year. This pattern reflected an urgent academic response to advancements in quantum computing and the imminent need to bolster CI.

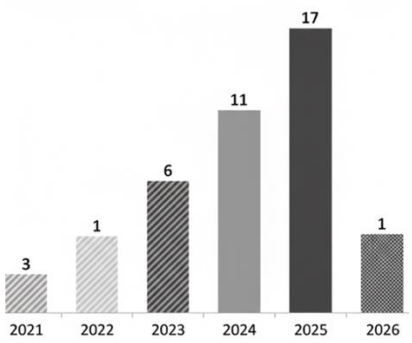

Fig. 2. *Temporal evolution of scientific production (2021-2026)*
Source: *Developed by the authors.*

However, there were no publications during the 2020 period; therefore, it does not appear in the previous graph. Regarding the geographical distribution, India was identified as having a prominent representation in studies related to the central theme of this research, contributing 10 studies (25.6%). This was followed in relevance by the United States with 6 publications (15.4%), South Korea with 3 (7.7%), and Canada also with 3 studies (7.7%). Consequently, it can be inferred that these countries, characterized as technological powerhouses with high industrial deployment, have prioritized quantum resilience as a strategic security pillar (see Fig. 3).

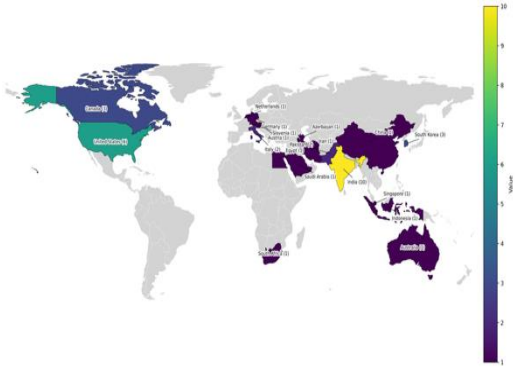

Fig. 3. *Geographical distribution.*
Source: *Developed by the authors.*

Regarding the frequency of keywords, an integral alignment with the objectives of the systematic review was evidenced. As shown in Fig. 4, the

theme of Cybersecurity acted as the cross-cutting axis of the research, with a presence in 100% of the analyzed articles (39 studies). This conceptual foundation allowed for the addressing of the quantum threat, a term identified in 25 articles (64.1%), confirming the scientific community's interest in the disruptive impact of quantum computing on current protocols.

Concerning the application domain, it was determined that CI was the most studied environment with 22 mentions (56.4%), closely followed by CPS with 17 records (43.6%). On the other hand, the presence of specialized terms such as Frameworks (5 studies, 12.8%) and Ontologies (2 studies, 5.1%) indicates emerging areas for predictive risk management.

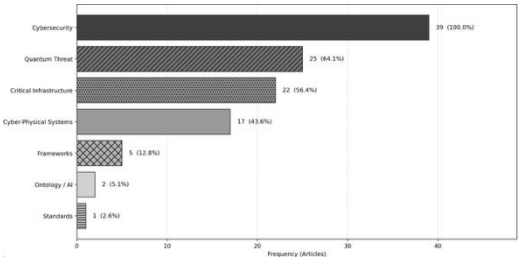

Fig. 4. *Frequency of keywords in the selected studies.*
Source*: Developed by the authors.*

Finally, the veracity of these findings was supported by the evidence from the primary studies. 74.4% (29 articles) were categorized as core research, while 25.6% (10 articles) corresponded to literature reviews. This distribution allowed the conclusions of the present work to be grounded in technical, experimental, and applied evidence across real industrial and academic environments (see Fig. 5).

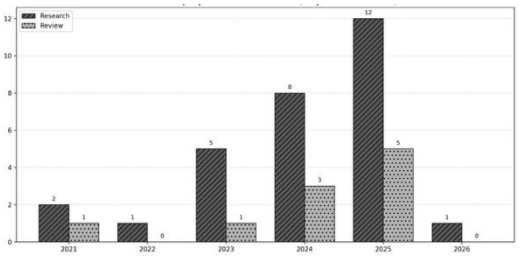

Fig. 5. *Distribution by study type: research vs. review (n=39).*
Source: *Developed by the authors.*

3. RESULTS ANALYSIS

In order to ensure complete process traceability and provide explicit answers to each research question, the Zenodo repository available at [https://doi.org/10.5281/zenodo.20790762] consolidates the 39 selected primary studies, specifying for each one the identifier, lead author, year, country of origin, type of research, technologies considered, main finding or contribution, and the research questions to which it provides direct evidence.

Below, the responses to the research questions that guided this review are presented:

RQ1: How does quantum computing affect current cybersecurity practices and standards in CPS and CI?

After analyzing the various studies, it was established that the impact of quantum computing is not limited to technical areas but represents a crisis of longevity and trust in current systems. The analyzed studies detected that the CPS providing water, energy, and other essential services were designed under security models that quantum computing has begun to place at risk.

A comparative analysis of the 39 primary studies allows the identification of relevant methodological convergences and divergences. Regarding convergences, there is a generalized agreement — present in studies [1], [4], [8], [9], [14], [15], [25], [30] — that Shor's algorithm represents the most immediate cryptographic threat to RSA and ECC systems currently deployed in ICS/OT environments. However, significant methodological differences are identified in the approach adopted to address it: while studies such as [1] and [9] propose solutions based on QKD and post-quantum blockchain, others such as [17] and [25] focus exclusively on the evaluation and standardization of lattice-based algorithms (Kyber, Dilithium) without considering hardware constraints. This divergence reveals a cross-cutting limitation in the literature: most proposals evaluate PQC algorithms in laboratory or simulation environments, without validating them on real industrial hardware subject to the memory and CPU cycle constraints inherent to PLCs and RTUs. Only studies [3], [19] and [42] worked directly on embedded hardware in ICS environments, representing the most specific evidence available on the operational viability of PQC in legacy infrastructure. An emerging trend identified in the most recent studies (2024–2025) is the adoption of hybrid architectures combining PQC with federation mechanisms and edge computing [12], [15], [21], suggesting a shift in the field from pure cryptography toward systemic resilience. In light of the foregoing.

The research determined that in industrial environments, trust has historically been based on

the certainty that every operational command such as opening a valve or regulating a generator originates from a legitimate source. However, it was identified that quantum computing breaks this premise.

Consequently, it was determined that one of the most critical vulnerabilities is real-time identity spoofing. Studies [1], [14], [15], [29] indicated that a quantum computer's ability to break asymmetric encryption would allow an attacker to generate forged digital signatures. This implies that a CPS could obey malicious commands believing they are legitimate, jeopardizing the physical safety of the entire infrastructure.

Furthermore, the danger of "harvest now, decrypt later" (capturing network traffic today to decrypt it in the future) was identified. This practice compromises the confidentiality of strategic data in critical infrastructures, necessitating an immediate technological transition ahead of the availability of commercial quantum computers [8], [14].

Another finding of high convergence among the reviewed studies was the limitation of industrial hardware to support the new PQC standards. Bandaru et al. [8] conducted an empirical evaluation of hardware and software implementations of the NIST finalist KEMs, determining that the computational resource consumption of Kyber-1024 exceeds that of RSA-2048 algorithms currently implemented in industrial microcontrollers by an average of 3.4 times. In line with this finding, Verchyk and Sepúlveda [11] demonstrated in a practical study on resource-constrained microprocessors that PQC-enhanced IBE encryption introduces latencies of up to 180 ms in authentication operations, which exceeds the real-time response margins of SCADA protocols. For their part, Trungadi et al. [42] specifically documented the case of Modbus devices in legacy ICS environments, concluding that the direct implementation of PQC without proxy intermediation is unfeasible, given that PLCs from generations prior to 2015 lack the storage capacity required for the parameters of the new algorithms. These three pieces of evidence, drawn from empirical studies conducted on real hardware, support the assertion that the limitation is not algorithmic but infrastructural, and that any post-quantum transition strategy in CI must contemplate a gradual renewal of the OT technology base or the use of proxy intermediary architectures.

In CI, synchronization is vital. It was observed that implementing quantum security rules consumes more processing time, generating latency. In the energy sector, this can cause failures, turning a security solution into a critical operational problem [5], [7], [19], [31].

To manage these vulnerabilities intelligently, the reviewed studies proposed several support tools, such as:

Ontologies as risk maps: Faced with emerging threats, studies [16], [32]-[34] proposed the use of ontologies to categorize and prioritize which infrastructure assets are most critical against a quantum attack, enabling an organized rather than reactive defense.

The need for agile standards: It was determined that the ideal standard is not one that is unbreakable, but one that is agile. The research highlighted that infrastructure must be capable of replacing its encryption algorithms without the need to be disconnected or physically replaced, in line with the new FIPS 203, FIPS 204 and FIPS 205 standards published by NIST [12], [17], [18], [35], [44]–[46]. This analysis confirms that the impact of quantum computing is cross-cutting: ranging from the impossibility of using current hardware to the necessity of rewriting the rules for security management in essential CI services.

RQ2: What are the key requirements for developing an ontological cybersecurity assessment model for CPS and CI?

After analyzing the various studies, it was determined that an ontological model for the quantum era should not be a simple glossary, but a formal knowledge artifact capable of mediating between the physical constraints of Operational Technology (OT) and the mathematical rigor of the new cryptography. For the model to be functional in CI environments, it must meet the following ontological design requirements:

1. Multi-domain Taxonomic Structure (Classes and Hierarchies). The model requires a class hierarchy that decomposes CPS into three interconnected levels, allowing for an integral semantic representation:

- Physical Layer: Represents assets such as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), which are fundamental to CPS architecture [19], [34].

- Cryptographic Layer: This refers to the classification of current (vulnerable) cryptographic primitives and post-quantum cryptography (PQC) families formally standardized in FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA), as well as quantum key distribution (QKD) as defense mechanisms [1], [14], [23], [35], [44]–[46].
- Threat Layer: Refers to the formal definition of quantum attack vectors, such as retrospective decryption and real-time identity spoofing [4], [8], [36].

2. Relationship and Dependency Modeling. The ontology must formalize the critical interactions that determine system resilience through specific semantic relationships:

Load Support Relationship: Linking cryptographic protocols with hardware memory and CPU capacities to prevent failures due to technological obsolescence [8], [11], [16].
Cascading Relationship: Mapping the network topology to identify how a quantum compromise in a specific node semantically impacts the global service continuity of the infrastructure [31], [33], [34].

3. Semantic Annotation of Performance Metrics. Unlike classical security ontologies, time is established as an ontological security requirement. The model must integrate data properties to measure the operational latency introduced by PQC algorithms, evaluating whether response times remain within the safety margins of real-time industrial processes [5], [7], [30].

4. Crypto-Agility as a Class Attribute. The model must assess the degree of infrastructure agility, defined as the capacity to dynamically instantiate or replace encryption algorithms without altering the physical structure of legacy hardware, allowing for a smooth transition toward secure standards [12], [18], [32].

5. Rule Base for Automated Reasoning. The final requirement is compatibility with inference engines, such as SWRL (Semantic Web Rule Language) rules. This allows the model to detect risks automatically: for instance, if the advancement of a threat's quantum computing capacity exceeds the security threshold of a current algorithm, the system should autonomously deduce a "critical vulnerability" alert based on the knowledge base [3], [10], [17].

In summary, the comparative analysis of the 39 primary studies allowed the identification of three structural trends in the field. First: there is a decoupling between the theoretical maturity of PQC algorithms — widely documented in studies such as [16], [17] and [27] — and their practical viability in OT environments, a gap that only three studies [3], [19] and [42] address with empirical evidence. Second: semantic modeling and cybersecurity ontologies are recognized as necessary by studies such as [2], [7] and [39], but none of the corpus proposes an ontology that simultaneously integrates quantum threats, OT assets and latency metrics, which precisely delimits the contribution of the present review. Third: scientific output in this domain shows a notable geographical concentration in India (10 studies, 25.6%) and the United States (6 studies, 15.4%), with scarce representation from Latin America and Southern Europe, suggesting a contextual validation gap in developing economies with less technologically updated critical infrastructures.

Based on the preceding analysis, it can be reaffirmed that the requirements for an ontological model in CPS and CI are not limited to the digital realm. The true effectiveness of the model lies in its ability to bridge the physical limitations of industrial machinery with the mathematical demands of the post-quantum era. Without this comprehensive approach, there is a risk of designing models that are theoretically secure but operationally impossible to implement.

4. DISCUSSION AND LIMITATIONS

The following items detail the limitations and discussion:

4.1. Contrast with previous systematic reviews

The present study does not develop in an academic vacuum, but rather in direct dialogue with the most representative reviews and surveys in the field. When contrasted with the ten reviews identified within the corpus itself, both convergences and relevant methodological differences emerge. El-Kady et al. [7] and Turk et al. [18] address security in cyber-physical systems from an organizational and process risk management perspective, without incorporating the quantum dimension or semantic modeling. Lezzi et al. [9] present a comprehensive systematic review on AI-based cybersecurity for sustainable industry, with broad coverage of detection techniques, but without analyzing quantum threats or assessment ontologies. Sarker et

al. [17] propose a rule-based AI taxonomy for cybersecurity in CI with semantic modeling elements, being the work most closely related to the present study in terms of conceptual structure; however, they do not integrate the quantum threat as a structuring axis either. Reviews focused on PQC, such as those by Babu et al. [23] and Vasani et al. [37], offer deep technical coverage of authentication and quantum communication protocols, but confine their analysis to the generic IoT domain, without considering the specific constraints of OT/ICS environments. Ahmad et al. [38] and Wicaksana [35] come closer to the intersection between PQC and critical infrastructures, but neither incorporates ontological models for semantic risk assessment. This comparison evidences that the differential contribution of the present review lies in being, to the extent of the analyzed evidence, the first to simultaneously integrate the four axes —quantum threat, CPS, CI and cybersecurity ontologies— in a systematic analysis oriented toward operational resilience assessment.

4.2. Differential contribution of this study

The review consolidates a specific contribution at three levels. At the conceptual level, it establishes a unified technical vocabulary that allows articulating the physical constraints of OT hardware (PLCs, RTUs) with the mathematical requirements of PQC algorithms, a terminological gap that previous reviews do not address systematically [7], [9], [18]. At the methodological level, it proposes five structural requirements for the design of an ontological assessment model —multi-domain taxonomic structure, relationship modeling, performance metrics annotation, cryptographic agility as a class attribute and rule base for automatic inference— which constitute an operationalizable technical roadmap, unlike the general conceptual frameworks proposed by Sarker et al. [17] or Singh et al. [26]. At the empirical level, the review documents and synthesizes the available evidence on the practical unfeasibility of implementing PQC directly on legacy industrial hardware [8], [19], [30], a finding that other reviews in the field mention incidentally, but without systematizing it as a central finding.

4.3. Consolidated evidence versus emerging findings

The distinction between consolidated evidence and emerging findings is fundamental for calibrating the scope of the conclusions of this study. Consolidated evidence is considered to be that supported by multiple independent studies of an empirical or experimental nature. Three findings fall into this category: first, the theoretical vulnerability of RSA and ECC cryptosystems to Shor's algorithm, widely documented in [1], [8], [14], [25] and recognized by NIST itself as the basis for PQC standardization; second, the computational incompatibility between NIST PQC candidate algorithms and industrial hardware from generations prior to 2015, evidenced with experimental data in [8], [19] and [26]; and third, the strategic necessity of cryptographic agility as a design attribute in industrial control systems, a convergence present in [12], [18], [32] and [35]. In contrast, the following are identified as emerging findings —supported by a limited number of studies and pending broader experimental validation—: the applicability of formal ontologies with SWRL inference rules for the autonomous detection of quantum threats in CI [2], [17], [39]; the viability of hybrid architectures combining PQC with federated learning for microgrid environments [38]; and the use of convolutional graphs to assess the criticality of components in cyber-physical power systems [43]. This distinction implies that conclusions linked to consolidated evidence have a prescriptive character, while those associated with emerging findings should be interpreted as priority research directions, not as immediate operational recommendations.

4.4. Implications of the limitations on the scope of the conclusions

The first limitation is the restriction of the search to three databases (IEEE Xplore, ACM Digital Library and ScienceDirect). Although these sources concentrate the most relevant scientific output in the studied domain, the exclusion of repositories such as Scopus, Web of Science and grey literature (NIST technical reports, ENISA or IEC guidelines) implies that some normative frameworks and restricted-access industrial implementation studies were not considered. This limitation primarily affects the completeness of the evidence on the actual state of PQC adoption in OT environments, so conclusions regarding the technological maturity of the sector should be interpreted as an approximation based on indexed academic literature, not as an exhaustive state of the art.

The second limitation is the scarcity of empirical validation studies in real critical infrastructures. Only three studies in the corpus [3], [19], [26] report experiments or implementations on functioning industrial hardware. Most of the analyzed works operate in simulation or laboratory environments.

This limits the generalization of conclusions regarding the behavior of PQC algorithms under real operational conditions of latency, temperature or electromagnetic interference — conditions inherent to SCADA environments, electrical substations or treatment plants. The technical recommendations derived from this review should therefore be interpreted as hypotheses to be validated through case studies in real environments before large-scale implementation.

The third limitation is the speed of evolution of the studied domain. The NIST standards FIPS 203 (ML-KEM) [44], FIPS 204 (ML-DSA) [45] and FIPS 205 (SLH-DSA) [46], published in 2024, represent a normative milestone that several of the primary studies in this corpus anticipated as proposals, but which now constitute formal standards. This implies that some assertions regarding the emerging nature of PQC have been partially superseded by normative reality, which reinforces the urgency of the conclusions but also requires that future research in this field incorporate these standards as a starting point, not as a horizon.

5. CONCLUSION

The findings of this systematic review allow the following conclusions to be established, organized into two blocks: evidence derived from the analysis of the 39 primary studies and research directions proposed from the identified gaps.

The present research evidence that the protection of CPS and CI against quantum computing demands a progressive paradigm shift: the transition from reactive perimeter security toward operational semantic resilience. Based on the systematic analysis of the evidence, it is established that a significant proportion of the primary studies report relevant technical limitations of legacy hardware in OT environments. The analyzed evidence indicates that OT-associated devices (such as PLCs and RTUs) present, in the majority of documented cases, computational constraints that hinder the direct implementation of the new post-quantum cryptography standards [8], [19], [26], [30]. These constraints manifest primarily as operational latencies that, according to the reviewed empirical studies, can compromise the real-time response margins of industrial protocols such as SCADA and Modbus. This situation warns that certain adaptation attempts without considering the actual capabilities of OT hardware could compromise the stability of real-time processes.

In this transition scenario, semantic modeling was identified as a strategic decision-making component in the most recent studies of the corpus [2], [17], [39]. The review findings demonstrate that the development of ontological models transcends the organization of concepts to become a tool for automated reasoning. By semantically characterizing assets, threats and metrics, the evidence suggests that systems are enabled to autonomously detect vulnerabilities through inference engines [17], [39].

Likewise, the analyzed studies converge in indicating that cryptographic agility and the standardization of information technology and OT constitute strategic requirements for the transition toward resilient infrastructures [12], [18], [32], [44]–[46]. The terminological unification identified in this review as a requirement of the ontological model provides the formal language necessary for a coordinated response among the sector's stakeholders.

From the gaps identified in the literature, the following priority research directions are derived. First, future work should prioritize the optimization of PQC primitives specifically designed for resource-constrained microcontrollers, seeking a balance between security and operational latency in real ICS environments, given that the empirical evidence available in this domain is still scarce.

Second, the formal construction of a cyber-resilience ontology integrating SWRL rules is proposed, so that infrastructure defense can rely on a logical orchestration between the physical rigidity of industry and the mathematical complexity of quantum computing, reducing dependence on human judgment in real-time threat detection.

Third, the path toward the creation of dynamic hybrid architectures represents an open research opportunity. These architectures should be capable of alternating between algorithmic methods and QKD according to the detected risk level and should be validated in real infrastructure environments before widespread deployment.

Finally, the field's prospective suggests that the integration of these intelligent models into Digital Twins could constitute a relevant validation direction, enabling the simulation of quantum-era attacks and the evaluation of automated responses in virtual environments before deployment in real critical infrastructures, which would contribute to

minimizing the potential risks associated with failures during technological migration.

ACKNOWLEDGMENTS

Thanks to the University of Cauca, especially the GTI research group, and to the University of Antioquia and its In2lab group for providing the resources and support for the development of this proposal.

REFERENCES

[1] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, "Quantum-Key-Distribution-Based Microgrid Control for Cybersecurity Enhancement," *IEEE Trans. Ind. Appl.*, vol. 58, no. 3, pp. 3076–3086, 2022, doi: 10.1109/TIA.2022.3159314.

[2] A. Alabdulatif, "FedCognis: An Adaptive Federated Learning Framework for Secure Anomaly Detection in Industrial IoT-Enabled Cognitive Cities," Saudi Arabia, Sep. 2025. doi: https://doi.org/10.32604/cmc.2025.066898.

[3] A. Babar, T. Halabi, and M. Zulkernine, "Autonomous and Adaptive Cyber Incident Detection and Response in Industrial Cyber-Physical Systems using Hierarchical Reinforcement Learning," *ACM Transactions on Cyber-Physical Systems*, Jan. 2025, doi: 10.1145/3765622.

[4] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition," *Comput. Secur.*, vol. 150, Mar. 2025, doi: 10.1016/j.cose.2024.104272.

[5] R. Iqbal, M. Afzaal, and G. Rathee, "Hybrid and adaptive framework for secure and scalable authentication in healthcare IoT," *Array*, vol. 28, Dec. 2025, doi: 10.1016/j.array.2025.100527.

[6] A. K. Kar, W. He, F. C. Payton, V. Grover, A. S. Al-Busaidi, and Y. K. Dwivedi, "How could quantum computing shape information systems research – An editorial perspective and future research directions," Feb. 01, 2025, *Elsevier Ltd*. doi: 10.1016/j.ijinfomgt.2024.102776.

[7] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Safety and Environmental Protection*, vol. 173, pp. 384–413, May 2023, doi: 10.1016/j.psep.2023.03.012.

[8] M. Bandaru, S. E. Mathe, and C. Wattanapanich, "Evaluation of hardware and software implementations for NIST finalist and fourth-round post-quantum cryptography KEMs," Dec. 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.compeleceng.2024.109826.

[9] M. Lezzi, P. Montefusco, M. Lazoi, and A. Corallo, "AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions," Nov. 01, 2025, *Elsevier B.V.* doi: 10.1016/j.jii.2025.100980.

[10] D. Lakshmi, N. Nagpal, S. Chandrasekaran, and J. H. D., "A quantum-based approach for offensive security against cyber attacks in electrical infrastructure," *Appl. Soft Comput.*, vol. 136, Mar. 2023, doi: 10.1016/j.asoc.2023.110071.

[11] D. Verchyk and J. Sepúlveda, "A practical study of post-quantum enhanced identity-based encryption," *Microprocess. Microsyst.*, vol. 99, Jun. 2023, doi: 10.1016/j.micpro.2023.104828.

[12] M. T. Naz, W. Elmedany, and M. Ali, "Securing SCADA systems in smart grids with IoT integration: A Self-Defensive Post-Quantum Blockchain Architecture," *Internet of Things (The Netherlands)*, vol. 28, Dec. 2024, doi: 10.1016/j.iot.2024.101381.

[13] C. Mangla, S. Rani, N. M. Faseeh Qureshi, and A. Singh, "Mitigating 5G security challenges for next-gen industry using quantum computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 6, Jun. 2023, doi: 10.1016/j.jksuci.2022.07.009.

[14] S. K. Singh *et al.*, "Quantum-Resistant Cryptographic Primitives Using Modular Hash Learning Algorithms for Enhanced SCADA System Security," *Computers, Materials and Continua*, vol. 84, no. 2, pp. 3927–3941, 2025, doi: 10.32604/cmc.2025.059643.

[15] R. Pal, R. X. Sequeira, X. Yin, S. Zeijlemaker, and V. Kotala, "How Should Enterprises Quantify and Analyze (Multi-Party) APT Cyber-Risk Exposure in their Industrial IoT Network?," *ACM Trans. Manag. Inf. Syst.*, Oct. 2023, doi: 10.1145/3605949.

[16] C. Ma, A. Shankar, S. Kumari, and C. M. Chen, "A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security," *Internet of Things (The Netherlands)*, vol. 28, Dec. 2024, doi: 10.1016/j.iot.2024.101391.

[17] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, "Multi-aspect rule-based AI:

Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures," Apr. 01, 2024, *Elsevier B.V.* doi: 10.1016/j.iot.2024.101110.

[18] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," *Autom. Constr.*, vol. 133, Jan. 2022, doi: 10.1016/j.autcon.2021.103988.

[19] D. Allison, K. McLaughlin, and P. Smith, "Goosewolf: An Embedded Intrusion Detection System for Advanced Programmable Logic Controllers," *Digital Threats: Research and Practice*, vol. 4, no. 4, Oct. 2023, doi: 10.1145/3617692.

[20] C. I. Okafor, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "PureQuantum: Towards A Scalable Blockchain Channel Security in IoT Networks," *Blockchain: Research and Applications*, p. 100372, Aug. 2025, doi: 10.1016/j.bcra.2025.100372.

[21] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, Dec. 2013, doi: 10.1016/j.infsof.2013.07.010.

[22] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.

[23] P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," Nov. 01, 2024, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2024.100676.

[24] A. M. Aslam, A. Bhardwaj, and R. Chaudhary, "Quantum-resilient blockchain-enabled secure communication framework for connected autonomous vehicles using post-quantum cryptography," *Vehicular Communications*, vol. 52, Apr. 2025, doi: 10.1016/j.vehcom.2025.100880.

[25] S. Sadeghi, V. Chouhan, M. Aldarwbi, A. Ghorbani, A. Chow, and R. Burko, "Securing financial sector applications in the quantum era: a comprehensive evaluation of NIST's recommended algorithms through use-case analysis," *Expert Syst. Appl.*, vol. 288, Sep. 2025, doi: 10.1016/j.eswa.2025.128243.

[26] P. Singh, S. Sirpal, and O. Pal, "Cyber resilience in e-governance: A review of strategies, challenges, and directions," Sep. 01, 2025, *Elsevier B.V.* doi: 10.1016/j.iot.2025.101702.

[27] L. Liyanage, N. A. G. Arachchilage, and G. Russello, "SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs)," *arXiv preprint arXiv:2408.16140*, 2024.

[28] S. Mohanan and N. Parameswaran, "FINER criteria – What does it mean?," *Cosmoderma*, vol. 2, p. 115, Nov. 2022, doi: 10.25259/csdm_123_2022.

[29] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G. J. Ahn, "ExSol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems," *Digital Threats: Research and Practice*, vol. 2, no. 3, Jun. 2021, doi: 10.1145/3428156.

[30] S. Y. Moon, B. H. Jo, A. El Azzaoui, S. K. Singh, and J. H. Park, "Edge-Fog Enhanced Post-Quantum Network Security: Applications, Challenges and Solutions," 2025, *Tech Science Press*. doi: 10.32604/cmc.2025.062966.

[31] O. O. Tooki and O. M. Popoola, "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems," Oct. 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.ref.2024.100628.

[32] I. Kong, M. Janssen, and N. Bharosa, "Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions," *Gov. Inf. Q.*, vol. 41, no. 1, Mar. 2024, doi: 10.1016/j.giq.2023.101884.

[33] Monika and S. K. Sood, "A scientometric analysis of quantum driven innovations in intelligent transportation systems," Dec. 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.engappai.2024.109258.

[34] R. Alguliyev, R. Aliguliyev, and L. Sukhostat, "An approach for assessing the functional vulnerabilities criticality of CPS components," *Cyber Security and Applications*, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2024.100058.

[35] A. Wicaksana, "A survey on quantum-safe blockchain security infrastructure," Aug. 01, 2025, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2025.100752.

[36] U. Song, G. Hur, S. Lee, and J. Park, "Unraveling the dynamics of the cyber threat landscape: Major shifts examined through the recent societal events," *Sustain. Cities Soc.*, vol. 103, Apr. 2024, doi: 10.1016/j.scs.2024.105265.

[37] V. Vasani, K. Prateek, R. Amin, S. Maity, and A. D. Dwivedi, "Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions," *J. Ind. Inf. Integr.*, vol. 39, 2024, doi: 10.1016/j.jii.2024.100594.

[38] J. Ahmad, M. Rizwan, S. F. Ali, U. Inayat, H. A. Muqeet, M. Imran, and T. Awotwe, "Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review," *Appl. Energy*, vol. 393, 2025, doi: 10.1016/j.apenergy.2025.126118.

[39] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, doi: 10.1016/j.ipm.2021.102549.

[40] K. Jain and A. Singh, "IHKEM: A post-quantum ready hierarchical key establishment and management scheme for wireless sensor networks," *Microprocess. Microsyst.*, vol. 118, Sep. 2025, doi: 10.1016/j.micpro.2025.105205.

[41] M. M. Moslehi, "Exploring coverage and security challenges in wireless sensor networks: A survey," *Comput. Netw.*, vol. 260, Feb. 2025, doi: 10.1016/j.comnet.2025.111096.

[42] F. Trungadi, M. Fabiano, D. Aloisio, G. Brunaccini, F. Sergi, G. Merlino, and F. Longo, "Securing Modbus in legacy industrial control systems: A decentralized approach using proxies, Post-Quantum Cryptography and Self-Sovereign Identity," *J. Inf. Secur. Appl.*, vol. 94, Nov. 2025, doi: 10.1016/j.jisa.2025.104199.

[43] S. Soleimani, A. Afshar, and H. Atrianfar, "Critical component analysis of cyber-physical power systems in cascading failures using graph convolutional networks: An energy-based approach," *Sustain. Energy Grids Netw.*, vol. 42, Jun. 2025, doi: 10.1016/j.segan.2025.101653.

[44] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Key-Encapsulation Mechanism Standard," *Federal Information Processing Standards* (NIST FIPS), NIST FIPS 203, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.203.

[45] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Digital Signature Standard," *Fed. Inf. Process. Stds.* (NIST FIPS), NIST FIPS 204, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.204.

[46] National Institute of Standards and Technology (NIST), "Stateless Hash-Based Digital Signature Standard," *Fed. Inf. Process. Stds.*(NIST FIPS), NIST FIPS 205, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.205.