Preliminary Review: Cybersecurity for Operation Technology in Quantum Age Against Network Attacks to Critical Infrastructures

Revisión Preliminar: Ciberseguridad Para Tecnología de la Operación en la Era Cuántica Contra Ataques De Red a Infraestructuras Críticas

DOI: https://dx.doi.org/10.17981/ingecuc.20.2.2024.06
Scientific Research Article. Date of Receipt: 08/15/2023, Date of Acceptance: 09/25/2023.

Siler Amador-Donado
Universidad del Cauca, Grupo GTI, Popayán, (Colombia)
samador@unicauca.edu.co

César Jesús Pardo-Calvache
Universidad del Cauca, Grupo GTI, Popayán, (Colombia)
cpardo@unicauca.edu.co

Gabriel ElíaS Chanchí-Golondrino
ENSTA Bretagne, Brest, (Francia)
raul.mazo@ensta-bretagne.fr

To cite this paper:
S. Amador-Donado, C. Pardo-Calvache, & R. Mazo-Peña, "Preliminary Review: Cybersecurity for Operation Technology in Quantum Age Against Network Attacks to Critical Infrastructures" INGE CUC, vol. 20, no. 2, 2024. pp.126-143. DOI: https://dx.doi.org/10.17981/ingecuc.20.2.2024.06

Abstract
Introduction– Cyber-Physical Systems (CPS) require change in cybersecurity due to cyber threats and the advent of quantum computing. Despite the interest, main obstacles for adoption are cybersecurity and dynamic protection. Research seeks to characterize Cybersecurity Reference Model for CPS in Critical Infrastructures, considering limitations.
Objective– To characterize the cybersecurity reference model to prevent CPS attacks in critical infrastructures in the face of the advent of quantum computing. Primary studies are analyzed to identify the development of cybersecurity in CPS.
Methodology– Process includes research objectives, research questions, search strategies, inclusion and exclusion criteria, quality of studies and data. Methods such as Goal Question Metrics (GQM) and the Population Intervention Comparison Outcome (PICO) model were used.
Results– From 630 initial studies, 133 were considered relevant, and 33 primary studies were finally selected. We identified 3 types of vulnerabilities, 25 challenges, 8 types of attacks and 20 types of reasons in CPS cybersecurity in the quantum era, including impact on cryptography. There are no known attacks on CPS using quantum equipment yet, but there are potential risks.
Conclusions– CPS cybersecurity in the quantum era is compromised by challenges in cryptography. Essential transition to resilient algorithms, but lack of preparedness and understanding of the cybersecurity community is a major obstacle. Emphasis on collaboration to address quantum challenges. Comprehensive response required to protect CPS in the quantum era.
Key Words– Cybersecurity, CPS, cyber-physical systems, quantum, reference model, critical infrastructure, network attack.

Resumen
Introducción– Los Sistemas Ciber-físicos (CPS) requieren cambio en ciberseguridad por amenazas cibernéticas y la llegada de computación cuántica. A pesar del interés, obstáculos principales para adopción son ciberseguridad y protección dinámica. Investigación busca caracterizar Modelo de Referencia de Ciberseguridad para CPS en Infraestructuras Críticas, considerando limitaciones.
Objetivo– Caracterizar el modelo de referencia de ciberseguridad que prevenga ataques en CPS en infraestructuras críticas ante la llegada de la computación cuántica. Se analizan estudios primarios para identificar desarrollo de ciberseguridad en CPS.
Metodología– Proceso incluye objetivos, preguntas, estrategias de búsqueda, criterios, calidad de estudios y datos. Se usaron métodos como Goal Question Metrics (GQM) y el modelo Population Intervention Comparison Outcome (PICO).
Resultados– De 630 estudios iniciales, 133 se consideraron relevantes, finalmente se seleccionaron 33 primarios. Se identificaron 3 tipos de vulnerabilidades, 25 desafíos, 8 tipos de ataques y 20 tipos de razones en ciberseguridad de CPS en la era cuántica, incluido impacto en criptografía. Aún no hay ataques a CPS mediante equipos cuánticos conocidos, pero hay riesgos potenciales.
Conclusiones– La ciberseguridad de CPS en la era cuántica se ve comprometida por desafíos en criptografía. Transición esencial a algoritmos resistentes, pero la falta de preparación y comprensión de la comunidad de ciberseguridad es un gran obstáculo. Se enfatiza en la colaboración para abordar desafíos cuánticos. Se requiere respuesta integral para proteger CPS en la era cuántica.
Palabras clave– Ciberseguridad, CPS, sistemas ciber-físicos, cuántica, modelo de referencia, infraestructura crítica, ataques a la red.

I. INTRODUCTION

Cyber-Physical Systems (CPS) require a paradigm shift in cybersecurity, as they drastically increase the attack surface by known cyber-threats [1] and with the advent of quantum equipment, cyber-threats can be completely new due to the inclusion of new devices and protocols, e.g.: the transition from traditional, closed Supervisory Control And Data Acquisition (SCADA) systems to Internet-connected systems can significantly expand the attack surface, allowing attack vectors to be exploited by threats such as interference, denial of service, intellectual property theft, loss of sensitive business data, data modification, and industrial espionage [2, p. 121]. Despite the growing interest of the international academic and scientific community, there are two main obstacles to the adoption of CPS: (i) cybersecurity problems that make it extremely difficult to exploit the full potential of this new paradigm, and (ii) the need to be so dynamic in terms of protection against cyberattacks. In addition, with respect to the number of connected devices that need protection, CPS show considerable growth. A recent example that shows what can happen when these threats are not taken into account when designing and implementing these new systems, was the December 2015 cyberattack on the Ukrainian power grid, where the adversary was able to use the Industrial Internet of Things (IIoT) infrastructure to disrupt power supply to thousands of homes [3, p. 2].

The best practices in Industry 4.0 implemented by the reference and evaluation models presented in the framework to improve cybersecurity in critical infrastructure (CI), represent a great saving in money and time that it would take for industries or organizations to prevent cyberattacks that take advantage of the absence of such practices when using vulnerable CPS in the automation of industrial processes in CI in the public and private sectors [4]. The prevention of cyber-attacks is not only for a Cyber-Physical Device (CPD), but for all the elements that make up a CPS, which can be made up of many devices connected to the network and possibly in different locations, so that each device faces cybersecurity threats, such as: denial of service attacks, botnets, brute force attacks, malware, among others. Currently there are a variety of Industry 4.0 technologies that are a great support to increase the security level of CPS, but a cybersecurity reference models (CRM) is required to prevent network cyber-attacks on these devices due to the advancement of quantum equipment. Therefore, this research aims to characterize an CRM that implements good practices for CPS in CI and prevents the challenges faced by the devices that comprise it, since its limited hardware does not allow configuring robust applications that are required to prevent possible cyber-attacks. As previously mentioned, the devices may be in remote areas, which to a certain extent may increase the number of threats, so the characterization of the proposed CRM aims to prevent network attacks.

It is important to mention that one of the most critical challenges of cybersecurity in CI is to apply the principles and best practices of risk management to reduce it and improve recovery capacity, all the above through the characterization of standards, regulations, guidelines, guides and best practices. Therefore, in this work the results of the systematic literature review (SLR) on the characterization in CRM are presented to prevent network attacks against CPS before the quantum advent, likewise, the primary studies found are analyzed, the main scientific initiatives on the exposed subject are studied and relevant information is collected such as: conceptual definitions, proposals, validations, processes and research methods to identify the degree of development of the initiatives based on the results obtained. After analyzing the information collected from the primary studies found, it has been possible to observe that there are some contributions in relation to the definition of the topic exposed.

The structure of the paper is as follows: **Section II** presents the research methodology that has been followed for the development of the SLR. **Section III** presents the research results, synthesizing, interpreting and highlighting what was obtained and why it is relevant. Finally, **Section IV** presents the discussion and conclusions.

II. RESEARCH METHODOLOGY

An SLR is a process that allows the collection, categorization and structuring of existing information on a topic of investigative interest, in this case, in cybersecurity. Thus, for the design of the SLR, the protocol proposed by Petersen et al. [5], In addition to the guidelines set forth by Kitchenham [6] and Budgen et al. [7], with which, the following activities were carried out: **(1)** Apply Goal-Question-Metric (GQM) approach; **(2)** Define search and selection strategy; **(3)** Conducting the review; and **(4)** Reporting the review. A detailed description of each of the activities carried out is presented in the

following sections. The following are the activities that were carried out in detail, as shown in (Fig.1).

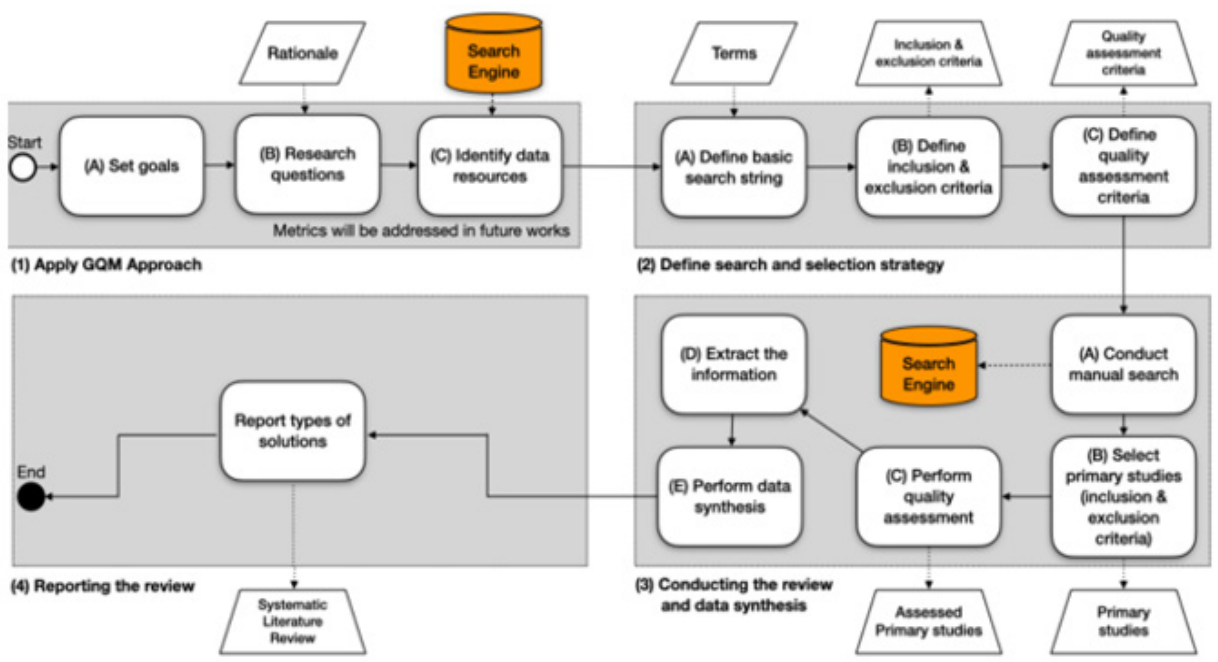

Fig. 1. Process steps for SLR
Source: Prepared by authors.

Each of the steps is explained in detail below:

(1) Apply GQM approach. A set of research questions was established for SLR, which have been elaborated following the GQM approach proposed by Basili and Caldiera [8]. This approach proposes a measurement model composed of three levels of abstraction: (i) conceptual level; where the objectives that will allow to establish, know and identify the purpose of the SLR to be carried out are defined, (ii) operative Level; where a set of research questions is designed based on the objectives obtained at the conceptual level, which will allow to focus, characterize and structure the evaluation of the articles identified and related to the research topic, and (iii) quantitative level; where a set of metrics associated with each question is established, this, with the purpose of answering them in a measurable way. A set of goals is described (business objectives) and a list of questions (measurement objectives) for SLR. The metrics of the GQM proposal will be developed in future works. Some of the sub-steps are explained below:

a. Set goals. In order to properly direct the SLR, the following search objectives (OB) have been established based on the following 4 domains: How?, What?, Which? and Why?, according to Edded et al. [9, p. 9]. OB1 (what?): Analyze the main studies in the research domain evidenced in the collected literature. OB2 (which?): Identify the different ways in which the studies demonstrate the contributions in the research domain. OB3 (how?): Characterize the evidenced management of the studies in the research domain. OB4 (why?): Justify the reasons why the research domain was chosen.

b. Research questions. Based on the fundamental reasons that motivated this research and the 4 domains mentioned above and described research questions in Table 1.

TABLE 1.
RESEARCH QUESTIONS ACCORDING TO 4 GOALS AND DOMAINS MENTIONED IN SECTION (1)A

Knowledge	¿What knowledge has been expressed in the research domain?	Manage	¿How to manage the research domain?
¿WHAT?	**RQ1**: ¿To what extent will the cybersecurity of cyber-physical devices be vulnerable in the quantum age?	¿HOW?	**RQ3**: ¿How to attack cyber-physical devices in the quantum age?
Form	**In which form(s) is the research domain expressed?**	**Use**	**¿Why use the research domain?**
¿WHICH?	**RQ2**: ¿What are the main challenges of cybersecurity applied to cyber physical devices with the arrival of the quantum era?	¿WHY?	**RQ4**: ¿Why do critical infrastructures see the cybersecurity of cyber-physical devices compromised in the quantum age?

Source: Prepared by authors.

c. Identify data resources. Based on many search engines, a preliminary consultation was carried out among the research team to choose the appropriate data sources for the research domain and finally a list of seven (7) was obtained as named below: Google Scholar, Scopus, Science Direct, Springer Link, ACM Digital Library, Web of Science and IEEE Xplore.

(2) Define search and selection strategy. Sub-steps are explained below:

a. Define basic search string. The PICO (Population, Intervention, Comparison and Outcome) model was used as a structured way to formulate research questions for SLR and the selection of appropriate search terms [10], described in Table 2.

TABLE 2.
APPLICATION OF THE PICO MODEL

P	I	C	O
Critical infrastructures.	Cybersecurity. Cyber-physical systems. Quantum computers.	Does not apply.	Effectiveness of cybersecurity measures. Impact of cyber-physical systems. Quantum applications to improve or threaten cybersecurity.

Source: Prepared by authors.

Eight (8) different versions of search strings were made, see them in Table 2-1, taking Google Scholar as the search source in all of them, and finally the one shown in Table 3 was selected.

TABLE 2-1.
SEARCH VERSIONS
Source: Prepared by authors.

#	Date	Google Scholar	Results
1	25/01/2022	(("cyber-physical system*" OR cps OR "cyber physical system*") AND ("Internet of Thing*" OR iot) AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND ("critical infrastructure" OR ci))	3530
2	25/02/2022	(("cyber-physical system*" OR cps OR "cyber physical system*") AND (Industrial) AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND ("critical infrastructure" OR ci))	5720
3	25/07/2022	(("cyber-physical system*" OR cps OR "cyber physical system*") AND ("Quantum computing") AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND ("critical infrastructure" OR ci))	182
4	25/07/2022	(("cyber-physical system*" OR cps OR "cyber physical system*") AND ("Quantum computing") AND ("cybersecurity" OR "cyber security" OR "cyber-security"))	672
5	08/08/2022	(("cyber-physical" OR "cyber physical") AND ("post-quantum" OR "post quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security"))	513
6	08/08/2022	(("cyber-physical" OR "cyber physical") AND ("quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security"))	5000
7	08/08/2022	(("cyber-physical" OR "cyber physical") AND ("quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND "critical infrastructure") -physics -chemistry -biology	466
8	16/08/2022	(("cyber-physical" OR "cyber physical") AND ("quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND "critical infrastructure") -physics -chemistry -biology	471

TABLE 3.
ULTIMATE SEARCH STRING

Google Scholar	Date August 16, 2022
((“cyber-physical” OR “cyber physical”) AND (“quantum”) AND (“cybersecurity” OR “cyber security” OR “cyber-security”) AND “critical infrastructure”) -physics -chemistry -biology	471 results

Source: Prepared by authors.

b. Define inclusion and exclusion criteria. Inclusion criteria. **I1**: Studies that have been reviewed by peers and published in journals, conferences or proceedings where the main topic of cybersecurity in CPDs of CI in the quantum era is addressed. **I2:** Studies within the period 2005-2023. Exclusion criteria. **E1:** Duplicate studies (considering only the most complete and recent that can be evidenced). **E2:** Studies where the cybersecurity of CPDs in CI in the quantum era is not addressed or superficially. **E3:** Studies that are reports, theses, books or book chapters. **E4:** Studies in languages other than English. **E5:** Studies whose content is not accessible.

c. Define quality assessment criteria (QC). An important process in the SLR is to evaluate the quality through a checklist with closed questions (YES/NO) that evaluate the following: Clarity: Evaluate whether the objectives and rationale for the study are sufficiently clear. **QC1:** Are the objectives of the study clearly defined? Credibility: Evaluates that the methodology used in the study guarantees the validity, effectiveness and significance of the results [11]. **QC2:** Were previous sources of knowle-

dge and work presented in the study? Relevance: Evaluates the importance and value of the study for the community of researchers on the subject [12]. **QC3:** Has the study been valued in the industrial or academic field? Rigor: Evaluates the characteristics of the research methods used to declare the validity of the tools and methods of analysis. **QC4:** Are the research methods used appropriate and consistent with the objectives of the study?

To evaluate quantitatively, the following rubric was established: For the first three criteria, three levels of compliance were considered (0, 0.5, 1), for rigor criteria, it was considered to use a list of two levels (0, 1). Each of the primary studies may be evaluated between 0 and 4, this value is the result of the sum of the scores of the questions of each evaluated criteria. Three categories were defined to classify the quality of the studies (High>=80%; 51%<=Medium<=79%; Moderate<=50%).

(3) Conducting the review and data synthesis. Sub-steps are explained below:

a. Conduct manual search. This activity began with the selection of the seven data sources, through initial test queries and suggestions from experts in their use, in the end the following were chosen: Scopus, IEEE Xplore, Google Scholar, ACM Digital library, Web of Science, Science direct and Springer link. See Table 4.

Table 4.
SEARCH STRING

Data sources	Search string
Scopus	(cyber-physical OR "cyber physical") AND (quantum) AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND ("critical infrastructure")
IEEE Xplore	(((cyber-physical) OR ("cyber physical") OR (cyberphysical)) AND (quantum) AND ((cybersecurity) OR (“cyber security”) OR (cyber-security)) AND (“critical infrastructure”))
Google Scholar	(("cyber-physical" OR "cyber physical") AND ("quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND "critical infrastructure") -physics -chemistry -biology
ACM Digital library	"query": { AllField:((("cyber-physical" OR "cyber physical") AND ("quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND "critical infrastructure")) }
Web of Science	#1 AND #2 AND #3 AND #4 Query #1: ((ALL=(cyber-physical) OR ALL=(cyber physical))) Query #2: (ALL=(quantum)) Query #3: ((ALL=(cybersecurity) OR ALL=(cyber security) OR ALL=(cyber-security))) Query #4: (ALL=(critical infrastructure))
Science direct	(("cyber-physical" OR "cyber physical") AND ("quantum") AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND "critical infrastructure")
Springer link	(cyber-physical OR cyberphysical OR "cyber physical") AND (quantum) AND ("cybersecurity" OR "cyber security" OR "cyber-security") AND ("critical infrastructure")

Source: Prepared by authors.

b. Select primary studies (inclusion and exclusion criteria). A total of 630 studies were initially obtained, when applying the inclusion and exclusion criteria, 133 remained relevant, the title, abstract and conclusions were analyzed to those 133 to obtain 33 primary studies, see Table 5.

Table 5.
PRIMARY STUDIES – SEARCH RESULTS BY DATA SOURCES

Data sources	Results	Exclusion criteria	Inclusion criteria	Primary
Scopus	94	47	47	13
IEEE Xplore	1	0	1	0
Google Scholar	471	401	70	17
ACM Digital library	12	11	1	0
Web of Science	2	1	1	0
Science direct	25	15	10	3
Springer link	25	22	3	0
Total	**630**	**497**	**133**	**33**

Source: Prepared by authors.

c. Perform quality assessment. By applying the quality criteria defined in section (2)c to the 33 primary studies, see first Table 5 and next Table 6.

TABLE 6.
PRIMARY STUDIES – SEARCH RESULTS BY DATA SOURCES

No.	Id.	Study name	QC1	QC2	QC3	QC4	Value	Percent	Level
1	A20	Trusted Node QKD at an Electrical Utility	1	1	1	1	4	100%	HIGH
2	A24	A Cyber Security Detection Framework for Supervisory Control and Data Acquisition Systems	1	1	1	1	4	100%	HIGH
3	A31	Cyber-physical systems and their security issues	1	1	1	1	4	100%	HIGH
4	A09	A Survey on Privacy for B5G/6G: New Privacy Goals, Challenges, and Research Directions	1	1	0,5	1	3,5	88%	HIGH
5	A11	Assessing the Maturity of National Cybersecurity and Resilience	1	1	0,5	1	3,5	88%	HIGH
6	A13	Cyber Security of an Electric Power System in Critical Infrastructure	1	1	0,5	1	3,5	88%	HIGH
7	A03	Development of a Testbed for Process Control System Cybersecurity Research	1	1	0	1	3	75%	MEDIUM
8	A05	Dynamic risk management response system to handle cyber threats	1	1	0	1	3	75%	MEDIUM
9	A07	SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures	1	1	0	1	3	75%	MEDIUM
10	A10	Cyber-Physical System Modeling for Assessment and Enhancement of Power Grid Cyber Security, Resilience, and Reliability	1	1	0	1	3	75%	MEDIUM
11	A18	A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology	1	1	0	1	3	75%	MEDIUM
12	A19	Use Case Based Blended Teaching of IIoT Cybersecurity in the Industry 4.0 Era	1	1	0	1	3	75%	MEDIUM
13	A21	Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues	1	1	0	1	3	75%	MEDIUM
14	A27	A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats	1	1	0	1	3	75%	MEDIUM
15	A28	On the importance of cryptographic agility for industrial automation	1	1	0	1	3	75%	MEDIUM
16	A30	Smart Grid Cybersecurity: Standards and Technical Countermeasures	1	1	0	1	3	75%	MEDIUM
17	A25	Authentication of smart grid communications using quantum key distribution	1	1	0,5	0	2,5	63%	MEDIUM
18	A01	A comprehensive cybersecurity framework for afghanistan's cyberspace	0	1	0	1	2	50%	MODERATE
19	A02	Attribution of Cyber Attacks on Industrial Control Systems	1	1	0	0	2	50%	MODERATE
20	A06	A security and authentication layer for SCADA/DCS applications	0,5	1	0,5	0	2	50%	MODERATE
21	A12	Development of the concept of electronic government construction in the conditions of synergetic threats	1	1	0	0	2	50%	MODERATE
22	A22	A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification	0	1	0	1	2	50%	MODERATE
23	A23	A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security	1	1	0	0	2	50%	MODERATE
24	A26	Physical Layer Security for the Smart Grid: Vulnerabilities, Threats and Countermeasures	1	1	0	0	2	50%	MODERATE
25	A33	Cyber-physical systems security: Limitations, issues and future trends	1	1	0	0	2	50%	MODERATE
26	A15	Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures	0	1	0	0	1	25%	MODERATE
27	A29	A Survey of Security in SCADA Networks: Current Issues and Future Challenges	0	1	0	0	1	25%	MODERATE
28	A32	Analysis of the likelihood of quantum computing proliferation	0	1	0	0	1	25%	MODERATE
29	A04	Refining Mosca's Theorem: Risk Management Model for the Quantum Threat Applied to IoT Protocol Security	0	0	0	0	0	0%	MODERATE
30	A08	Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats	0	0	0	0	0	0%	MODERATE
31	A14	Cyber Security in Healthcare Systems	0	0	0	0	0	0%	MODERATE
32	A16	Cyber-Attacks Against Critical Infrastructure	0	0	0	0	0	0%	MODERATE
33	A17	Insecure Firmware and Wireless Technologies as "Achilles' Heel" in Cybersecurity of Cyber-Physical Systems	0	0	0	0	0	0%	MODERATE
			80%	100%	20%	64%	0,66	66%	MEDIUM

Source: Prepared by authors.

d. The Id field corresponds to the identifier of the studies, from QC1 to QC4: Quality criteria from 1 to 4, Value is the sum of the four quality criteria evaluated in the study, Percent is the value in percentage of the Value field with respect to the four criteria and Level is the qualitative measurement scale explained in the section (2)c. Six (6) studies were classified with a high-quality level, eleven (11) studies were classified with a medium quality level and finally eleven (11) studies were classified with a moderate quality level. The five (5) studies with Id: A04, A08, A14, A16 and A17

were removed because all 4 quality criteria scored zero, see Table 6. Therefore, the total number of studies obtained was 28. When evaluating the 28 studies, the following results were obtained: quality criteria 1 (QC1) had an effective score of 80%, QC2 obtained the highest score of 100%, QC3 obtained the lowest with 20% and finally the QC4 with 64%. On average, the quality of the 28 studies was 66%, classifying them as medium.

e. Extract information. Next, the analysis carried out to answer each of the research questions is presented, the results are referenced to facilitate the analysis of the subject to other interested authors. After applying the four (4) research questions to the 28 studies obtained from the previous stage, six (6) were discarded because there was no answer to the 4 questions, the discarded were: A01, A02, A09, A15, A19, A27, see Table 6. By subtracting the 6 discarded, a total of twenty-two (22) studies remained, see data in Table 7.

TABLE 7.
ANSWERS TO RESEARCH QUESTIONS BY PRIMARY STUDIES AND QUALITY LEVEL

No.	Id.	Study name	RQ1	RQ2	RQ3	RQ4	Quality Level
1	A20	Trusted Node QKD at an Electrical Utility	X	X	X	X	HIGH
2	A24	A Cyber Security Detection Framework for Supervisory Control and Data Acquisition Systems	X	X	X	X	HIGH
3	A31	Cyber-physical systems and their security issues	-	X	-	X	HIGH
4	A11	Assessing the Maturity of National Cybersecurity and Resilience	X	X	X	X	HIGH
5	A13	Cyber Security of an Electric Power System in Critical Infrastructure	X	X	-	X	HIGH
6	A03	Development of a Testbed for Process Control System Cybersecurity Research	X	X	-	X	MEDIUM
7	A05	Dynamic risk management response system to handle cyber threats	-	X	-	-	MEDIUM
8	A07	SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures	X	X	X	X	MEDIUM
9	A10	Cyber-Physical System Modeling for Assessment and Enhancement of Power Grid Cyber Security, Resilience, and Reliability	X	X	X	X	MEDIUM
10	A18	A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology	X	X	X	X	MEDIUM
11	A21	Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues	-	X	X	X	MEDIUM
12	A28	On the importance of cryptographic agility for industrial automation	X	X	-	X	MEDIUM
13	A30	Smart Grid Cybersecurity: Standards and Technical Countermeasures	X	X	X	X	MEDIUM
14	A25	Authentication of smart grid communications using quantum key distribution	X	X	-	X	MEDIUM
15	A06	A security and authentication layer for SCADA/DCS applications	X	X	-	X	MODERATE
16	A12	Development of the concept of electronic government construction in the conditions of synergetic threats	X	X	-	-	MODERATE
17	A22	A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification	-	X	-	X	MODERATE
18	A23	A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security	X	X	X	X	MODERATE
19	A26	Physical Layer Security for the Smart Grid: Vulnerabilities, Threats and Countermeasures	-	X	-	-	MODERATE
20	A33	Cyber-physical systems security: Limitations, issues and future trends	X	X	X	-	MODERATE
21	A29	A Survey of Security in SCADA Networks: Current Issues and Future Challenges	-	X	-	X	MODERATE
22	A32	Analysis of the likelihood of quantum computing proliferation	X	X	-	X	MODERATE
			73%(16)	100%(22)	45%(10)	82%(18)	MEDIUM

Source: Prepared by authors.

f. Regarding research question 1 (RQ1) of the 22 studies analyzed, answers were obtained from 73% (16) of the studies, with respect to RQ2, 100% (22) were obtained, with respect to RQ3, 45% (10) were obtained and finally regarding RQ4, 82% (18) of the studies with responses to this item were obtained, see data in the following link https://shorturl.at/ezE36. This is the list of articles according to: (i) their unique identifier that has been used throughout the document, (ii) name of the study, (iii) number of citations, (iv) year of study and (v) reference. See data in Table 8.

TABLE 8.
REFERENCED PRIMARY STUDIES

No.	Id.	Study name	CITE	YEAR	REFERENCES
1	A03	Development of a Testbed for Process Control System Cybersecurity Research	5	2013	[13]
2	A24	A Cyber Security Detection Framework for Supervisory Control and Data Acquisition Systems	87	2016	[14]
3	A02	Attribution of Cyber Attacks on Industrial Control Systems	26	2016	[15]
4	A05	Dynamic risk management response system to handle cyber threats	44	2018	[16]
5	A31	Cyber-physical systems and their security issues	385	2018	[17]
6	A30	Smart Grid Cybersecurity: Standards and Technical Countermeasures	4	2018	[18]
7	A21	Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues	116	2019	[19]
8	A28	On the importance of cryptographic agility for industrial automation	2	2019	[20]
9	A26	Physical Layer Security for the Smart Grid: Vulnerabilities, Threats and Countermeasures	39	2019	[21]
10	A29	A Survey of Security in SCADA Networks: Current Issues and Future Challenges	49	2019	[22]
11	A18	A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology	12	2020	[23]
12	A11	Assessing the Maturity of National Cybersecurity and Resilience	6	2020	[24]
13	A10	Cyber-Physical System Modeling for Assessment and Enhancement of Power Grid Cyber Security, Resilience, and Reliability	5	2020	[25]
14	A19	Use Case Based Blended Teaching of IIoT Cybersecurity in the Industry 4.0 Era	5	2020	[26]
15	A06	A security and authentication layer for SCADA/DCS applications	2	2020	[27]
16	A12	Development of the concept of electronic government construction in the conditions of synergetic threats	2	2020	[28]
17	A33	Cyber-physical systems security: Limitations, issues and future trends	269	2020	[29]
18	A20	Trusted Node QKD at an Electrical Utility	5	2021	[30]
19	A07	SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures	2	2021	[31]
20	A01	A comprehensive cybersecurity framework for afghanistan's cyberspace	0	2021	[32]
21	A22	A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification	10	2021	[33]
22	A09	A Survey on Privacy for B5G/6G: New Privacy Goals, Challenges, and Research Directions	0	2022	[34]
23	A13	Cyber Security of an Electric Power System in Critical Infrastructure	2	2022	[35]
24	A27	A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats	0	2022	[36]
25	A25	Authentication of smart grid communications using quantum key distribution	0	2022	[37]
26	A23	A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security	5	2022	[38]
27	A15	Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures	1	2022	[39]
28	A32	Analysis of the likelihood of quantum computing proliferation	8	2022	[40]

Source: Prepared by authors.

g. Perform data synthesis. Next, after solving the research questions, the synthesis of the data obtained in each of the answers was carried out. The list of studies and research questions can be consulted through the Table 7.

RQ1: To what extent will the cybersecurity of CPDs be vulnerable in the quantum age? Cybersecurity of CPDs will be vulnerable in the quantum age to extent emergence introduces challenges such as encryption threats, resource constraints, and interoperability issues. Exposure of previously safeguarded information due to quantum computing deepens vulnerability. A multidisciplinary approach, education, and integration of quantum-resistant measures underscore the extent of this vulnerability, as quantum technologies advance. To establish a classification that allows understanding the nature of each of the causes identified in the literature, different types of vulnerabilities were identified, which are presented in Table 9.

TABLE 9.
TYPE OF VULNERABILITIES IDENTIFIED IN STUDIES

No.	TYPE	REFERENCES
1	Both asymmetric and symmetric weak cryptographic algorithms and protocols.	A03,A06,A07,A10,A11,A12,A13,A18 A20,A23,A24,A25,A28,A30,A32,A33
2	Lack of preparation of the cybersecurity community to transition to algorithms resistant to quantum cyberattacks.	A07,A23,A25,A28
3	Difficulty in upgrade cyber-physical devices.	A32

Source: Prepared by authors.

Sixteen (16) from 16 studies that responded to RQ1, agreed that "Weak cryptographic algorithms and protocols, both asymmetric and symmetric", are an important vulnerability and that NIST is evaluating and standardizing the algorithms. Post-Quantum Cryptography (PQC) that guarantee cybersecurity in the face of the advent of quantum adversaries. A possible solution to this vulnerability is the development and implementation of cryptographic algorithms resistant to classical and quantum cyberattacks. Four (4) from 16 studies that responded to RQ1, agreed that the "Lack of preparation of the cybersecurity community to transition to algorithms resistant to quantum cyberattacks" are an important vulnerability, but ongoing research and collaboration between academia, industry, and government will be crucial in addressing the cybersecurity challenges posed by the quantum age. One (1) from 16 studies that responded to RQ1, agreed that the "Difficult to update CPDs" is an important vulnerability, because most of these devices use classical cryptographic algorithms that have vulnerabilities and are not prepared for the quantum advent.

RQ2: What are the main challenges of cybersecurity applied to CPDs with the arrival of the quantum era? The challenges presented in the study require a multidisciplinary approach encompassing cryptography, quantum computing, and system design. Among the 22 studies responding

to RQ2, there's a consensus on 25 key challenges, the studies and the relationship with each challenge can be consulted in Table 10:

TABLE 10.
MAIN CYBERSECURITY CHALLENGES IDENTIFIED IN STUDIES

No.	TYPE	REFERENCES
1	Quantum computing that breaks current encryption.	A03,A06,A07,A10,A11,A12,A13,A18,A20,A23,A24,A25,A28,A30,A32,A33
2	Schedule for transition to quantum resistance algorithms.	A03,A06,A07,A10,A11,A12,A13,A18,A20,A22,A23,A24,A25,A26,A28,A29,A30,A33
3	Adaptation of existing devices.	A12,A21,A28
4	Limited understanding of quantum threats.	A03,A07
5	Quantum Key Distribution.	A03,A07,A10,A11,A12,A18,A20,A22,A23,A24,A25,A26,A31
6	Supply chain security.	A03
7	Authentication and access control with quantum resistance.	A03,A05
8	Post-quantum cryptography.	A05,A06,A07,A21,A22,A23,A24,A25,A26,A28,A29,A33
9	Secure hardware with quantum resistance.	A05,A13,A22
10	Security standards and protocols with quantum resistance.	A05,A18,A22,A26,A31
11	Resource constraints.	A06,A11,A12,A26,A29,A31,A33
12	Interoperability and compatibility.	A05,A29
13	Security in depth.	A06
14	Compatibility vulnerabilities.	A21,A32
15	Long-term security.	A07,A28
16	Infrastructure and hardware vulnerabilities.	A05,A10,A21,A32
17	Awareness and education.	A10,A22,A24
18	Security lifecycle management.	A11
19	Integration with existing cyber security measures.	A12,A25,A33
20	Security guarantee.	A21
21	Security of legacy systems.	A11,A13,A31
22	Command infrastructure vulnerabilities.	A32
23	Secondary channel vulnerabilities.	A32
24	Exposure of previously protected details.	A32
25	Data access and theft.	A32

Source: Prepared by authors.

Quantum Computing Impact: Sixteen studies agree that quantum computing threatens current encryption, potentially exposing sensitive data. The need to adopt quantum-resistant algorithms and upgrade existing devices is highlighted.

Transition to Quantum Resistance Algorithms: Eighteen studies point out resource constraints for quantum-resistant encryption, interoperability issues, and the complexity of implementing security measures, requiring a robust cybersecurity approach.

Adaptation of Existing Devices: Three studies emphasize the challenge of maintaining long-term cybersecurity against evolving quantum threats by updating cryptographic algorithms and protocols.

Limited Understanding of Quantum Threats: Two studies highlight new vulnerabilities introduced by quantum technologies and stress the importance of education among stakeholders.

Quantum Key Distribution (QKD): Thirteen studies acknowledge that quantum computing demands a comprehensive approach to security management throughout the life cycle of CPDs.

Supply Chain Security: One study highlights the complexity of integrating quantum-resistant measures with existing systems, requiring careful planning and coordination.

Authentication and Access Control with Quantum Resistance: Two studies underscore the need for robust mechanisms like secure design practices and continuous updates to ensure security in the quantum era. Post-Quantum Cryptography: Twelve studies stress the challenge of securing legacy devices against quantum threats, requiring upgrades or replacements.

Secure Hardware with Quantum Resistance: Three studies discuss the exposure of previously protected details due to quantum computing, facilitating non-cryptographic attacks.

Security Standards and Protocols with Quantum Resistance: Five studies highlight the importance of developing standards and protocols for quantum-resistant cybersecurity. Resource Constraints: Seven studies identify resource limitations as a significant challenge in achieving quantum-resistant cybersecurity.

Interoperability and Compatibility: Two studies emphasize the need for standardization and compatibility between devices with different encryption algorithms. Security in Depth: One study stresses the complexity of implementing security measures across various levels of cyber-physical systems.

Compatibility Vulnerabilities: Two studies point out the risk of critical vulnerabilities in devices relying on outdated, insecure quantum protocols.

Long-Term Security: Two studies highlight challenges in ensuring long-term security for CPDs, especially those difficult to upgrade.

Infrastructure and Hardware Vulnerabilities: Four studies discuss vulnerabilities introduced by quantum computing in infrastructure and hardware.

Awareness and Education: Three studies stress the importance of raising awareness and educating stakeholders about quantum cybersecurity challenges.

Security Lifecycle Management: One study highlights the need for effective management throughout the entire life cycle of CPDs.

Integration with Existing Cybersecurity Measures: Three studies emphasize integrating quantum algorithms with existing security measures.

Security Guarantee: One study underscores the importance of providing solid security guarantees in the quantum era.

Security of Legacy Systems: Three studies discuss the challenges of securing legacy systems against quantum threats.

Command Infrastructure Vulnerabilities: One study highlights the vulnerability of command infrastructure in the quantum age. Secondary Channel Vulnerabilities: One study points out vulnerabilities in secondary communication channels.

Exposure of Previously Protected Details: One study discusses the exposure of previously safeguarded information due to quantum computing.

Data Access and Theft: One study highlights the risk of unauthorized data access and theft. Overall, these challenges call for specialized solutions and awareness to address the evolving risks in the realm of quantum cybersecurity for CPDs.

RQ3: How to attack CPDs in the quantum age? So far, there are no known specific attacks on CPDs that harness the power of quantum computing. However, in the future, quantum computers could potentially break the cryptographic algorithms used to protect these devices, leading to vulnerabilities. This could include attacks on the encryption and authentication mechanisms used in CPS. It is important to note that these potential attacks assume that practical quantum computers capable of breaking current cryptographic algorithms will be developed and widely deployed. The timeline for the development and adoption of such quantum computers is uncertain, and efforts are underway to develop and standardize PQC algorithms that can withstand quantum computer attacks. Among the 10 studies responding to RQ3, there's a consensus on 8 potential attacks. The list of potential attacks and related studies can be consulted in Table 11:

TABLE 11.
TYPE OF ATTACKS IDENTIFIED IN STUDIES

No.	TYPE	REFERENCES
1	Exploitation of vulnerabilities in current cryptographic algorithms.	A07,A10,A18,A20
2	Interception and manipulation of communications between cyber-physical devices.	A07,A20
3	Manipulation of quantum devices used in cyber-physical systems.	A07,A10,A20,A30
4	Quantum side channel attacks.	A11,A18,A20,A21,A23,A24,A30,A33
5	Quantum replay attacks.	A11,A24,A33
6	Quantum Key Distribution (QKD) attacks.	A11,A20,A21,A23
7	Physical attacks.	A18,A21
8	Attacks on the supply chain.	A18

Source: Prepared by authors.

Exploitation of vulnerabilities in current cryptographic algorithms: Four studies about the analysis highlights potential attack scenarios in the quantum age, including the exploitation of vulnerabilities in current cryptographic algorithms due to quantum computers' ability to break encryption methods. Additionally, quantum computers could intercept and manipulate communication between CPDs, potentially compromising security protocols like the Diffie-Hellman key exchange. Mitigating these threats requires transitioning to quantum-resistant algorithms and ensuring the security of quantum key distribution protocols. It's important to acknowledge that these scenarios are speculative and based on the potential capabilities of quantum computing. Interception and manipulation of communications between CPDs: Two studies mention that there is limited research on specific attack methods targeting CPDs in the quantum age. However, potential attack scenarios could include the exploitation of vulnerabilities in current cryptographic algorithms due to quantum computers' ability to break them, interception, and manipulation of communication channels between devices, potential manipulation of quantum sensors, and the possibility of new side-channel attacks that exploit phy-

sical properties of quantum systems. It is important to note that these scenarios are speculative and require further research to understand the precise vulnerabilities and mitigation strategies.

Manipulation of quantum devices used in cyber-physical systems: Four studies mention that potential attack vectors could include exploiting vulnerabilities in encryption algorithms, manipulating quantum sensors, conducting quantum side-channel attacks, and targeting quantum-resistant algorithms. These speculative scenarios are based on the potential capabilities of quantum computing and the vulnerabilities it might introduce to cyber-physical systems. Further research is needed to fully understand and mitigate these potential threats.

Quantum side channel attacks: Eight studies mention that another potential attack vector could involve the interception and manipulation of quantum communication channels, compromising the security of CPDs. It is worth noting that these attack scenarios are speculative and based on the potential capabilities of quantum computing. Further research is needed to understand and mitigate the specific threats and vulnerabilities in CPDs in the quantum age.

Quantum replay attacks: Three studies mention that potential attack vectors could exploit vulnerabilities introduced by quantum computing. These include quantum attacks on encryption, manipulation of quantum sensors, quantum side-channel attacks, and potential attacks on post-quantum cryptographic algorithms. These scenarios are speculative and emphasize the need for proactive security measures and research to safeguard CPDs in the quantum era.

Quantum Key Distribution (QKD) attacks: Four studies mention that some possible attack scenarios include exploiting vulnerabilities in encryption algorithms, intercepting and manipulating quantum communication, and side channel attacks that exploit physical properties of quantum systems. These scenarios are speculative and based on the potential capabilities of quantum computing, requiring further research to understand and mitigate potential threats.

Physical attacks: Two studies mention that potential attack vectors could include exploiting vulnerabilities in encryption algorithms, intercepting and manipulating quantum communication, and leveraging side-channel vulnerabilities introduced by quantum technologies. These attacks are speculative and based on the vulnerabilities that quantum computing might introduce. Developing quantum resistant algorithms, securing quantum communication, and addressing potential side-channel vulnerabilities will be crucial to ensuring the security of CPDs in the quantum era.

Attacks on the supply chain: One study mention that potential attack scenarios could involve exploiting vulnerabilities in the encryption algorithms securing these devices. Quantum computers, if developed and powerful enough, could break traditional encryption algorithms like Rivest-Shamir-Adleman (RSA) or Elliptic Curve Cryptography (ECC), potentially leading to unauthorized access and manipulation of CPS. Additionally, interception and manipulation of quantum communication channels, as well as side-channel attacks on quantum systems, might also pose risks to the security of these devices. It's important to note that these scenarios are speculative, and further research is needed to fully understand the implications of quantum computing on CPD security.

TABLE 12.
TYPE OF REASONS IDENTIFIED IN STUDIES

No.	TYPE	REFERENCES
1	Decrypt current encryption algorithms.	A10,A23
2	Limited understanding of quantum threats.	A03,A07
3	Adaptation of existing devices.	A03,A07
4	Supply chain security.	A03
5	Quantum Resistant Authentication and Access Control.	A03,A07,A10,A11,A13,A18,A20,A22,A23,A25,A28,A29,A30,A31
6	Transition to PQC algorithms.	A06,A11,A13,A20,A22,A23,A25,A28,A29,A30
7	Extended lifespan and reliance on legacy technologies.	A07,A11,A13,A20,A30
8	Limited awareness and preparation.	A13,A22,A31
9	Compatibility challenges.	A11,A13,A20,A21,A25,A29,A32
10	Complexity and interconnectivity.	A22,A30
11	Potential impact on critical operations.	A06,A13,A21,A22,A24,A29,A30,A31
12	Command Infrastructure Vulnerabilities.	A32
13	Secondary channel vulnerabilities.	A21,A32
14	Exposure of previously protected details.	A32
15	Improper key distribution.	A21,A22
16	Limited implementation of post-quantum cryptography.	A22,A29
17	Exploitation of quantum side channel attacks.	A21,A32
18	Greater connectivity and interconnection of CPS with the Internet.	A24
19	Security approach by obscurity.	A24
20	Time sensitive operations.	A07,A11,A18,A22,A29

Source: Prepared by authors.

RQ4: Why do CI see the cybersecurity of CPDs compromised in the quantum age?

Among the 18 studies responding to RQ4, there's a consensus about of 20 cybersecurity reasons of CPDs compromised in the quantum age. The list of reasons and related studies can be consulted in the Table 12.

Decrypt current encryption algorithms: Two studies mention that Critical Infrastructures (CI) face compromised cybersecurity in the quantum age due to the vulnerability of current encryption algorithms to quantum computers. These advanced machines can break traditional encryption methods, exposing sensitive data and communication. To mitigate these risks, a holistic approach encompassing quantum-resistant cryptography development, awareness campaigns, and infrastructure updates is essential to ensure the security and integrity of CPDs in CI.

Limited understanding of quantum threats: Two studies mention that the unique and evolving nature of quantum-based attacks introduces challenges that demand specialized knowledge and expertise. This gap impedes the development of effective defenses and countermeasures against these emerging threats, leaving critical systems vulnerable to potential quantum attacks.

Adaptation of existing devices: Two studies mention that compromised cybersecurity of CPDs in CI due to the vulnerability of current encryption algorithms to quantum attacks is further exacerbated by the challenge of retrofitting existing devices. Many of these devices lack built-in quantum-resistant security measures and retrofitting them with such measures proves complex and expensive, requiring significant updates to hardware, software, and communication protocols.

Supply chain security: One study mention that in context of compromised cybersecurity for CPDs in the quantum age, supply chain security plays a crucial role. Ensuring the integrity and trustworthiness of components during the manufacturing and distribution of CPDs becomes increasingly important to prevent vulnerabilities from compromised or malicious components.

Quantum Resistant Authentication and Access Control: Fourteen studies mention that the context of compromised cybersecurity for CPDs in the quantum age, the development of quantum-resistant authentication and access control mechanisms becomes essential. The advent of practical quantum computers threatens the encryption and authentication mechanisms used in CI, potentially leading to unauthorized access, data manipulation, and compromised communication between CPDs.

Transition to PQC algorithms: Ten studies mention that in the face of the potential threat posed by quantum computing to traditional encryption algorithms, critical infrastructures must navigate the transition to post-quantum cryptography (PQC) to safeguard the cybersecurity of CPDs. Quantum computers' ability to break existing encryption methods, such as RSA and ECC, demands the adoption of PQC algorithms that can withstand both classical and quantum attacks. However, this transition presents challenges, including compatibility concerns, limited awareness, and the need to address resource constraints, while ensuring the security and operational continuity of critical systems.

Extended lifespan and reliance on legacy technologies: Five studies mention that cybersecurity of CI's CPDs is compromised in the quantum age due to the vulnerability of current cryptographic algorithms to quantum attacks. Quantum computers can break these algorithms, threatening data security and communication integrity. This is particularly concerning as critical infrastructures rely on legacy technologies, making the transition to quantum-resistant solutions complex and costly. The vulnerabilities introduced by quantum computing, combined with challenges in adopting PQC and addressing resource constraints, contribute to the compromised cybersecurity of these devices.

Limited awareness and preparation: Three studies mention that compromised cybersecurity of CPDs in CI during the quantum age is due, in part, to limited awareness and preparation. The emerging threat of quantum computing is not fully understood by many organizations, leaving them vulnerable to potential breaches. This lack of awareness hinders the implementation of necessary quantum-resistant security measures, exacerbating the risks posed by quantum attacks. Additionally, the long lifespan of CI systems and their interconnected nature further contribute to the challenges of addressing this vulnerability.

Compatibility challenges: Seven studies mention that during the quantum age, compatibility challenges contribute to compromised cybersecurity in CI. Older CPDs may struggle to integrate with new quantum-resistant encryption standards and hardware, relying on insecure protocols for compatibility. This vulnerability extends to command infrastructures, secondary channels, and even the exposure of previously protected details, posing risks to critical operations and overall cybersecurity.

Complexity and interconnectivity: Two studies mention that complexity and interconnectivity of CI contribute to compromised cybersecurity in the quantum age. These infrastructures consist of intri-

cate, interconnected systems including SCADA networks, IoT devices, and communication protocols, making the integration of quantum-resistant security measures challenging. This complexity increases the risk of vulnerabilities and potential cyber-attacks, highlighting the necessity for proactive measures to ensure the resilience and security of critical systems.

Potential impact on critical operations: Eight studies mention the potential impact of quantum computing on traditional encryption algorithms compromises the cybersecurity of CPDs in CI. Quantum computers can break widely used encryption methods like RSA and ECC, leaving sensitive data vulnerable to unauthorized access and manipulation. This vulnerability can lead to various security risks, including unauthorized control of critical infrastructure operations, potentially causing physical damage, economic losses, and public safety threats. The adoption of PQC is essential to address these vulnerabilities and ensure the security of critical infrastructures. Limited awareness and preparedness, along with the complexity of legacy systems, add to the challenges in securing CPDs in the quantum age.

Command Infrastructure Vulnerabilities: One study mention that cybersecurity of CPDs in CI is compromised in the quantum age due to various command infrastructure vulnerabilities. These vulnerabilities include compatibility issues with older devices, reliance on quantum-insecure protocols for command systems, potential exposure of sensitive system details through quantum computing, and persistent vulnerabilities in secondary communication channels. These weaknesses leave critical infrastructures susceptible to cyberattacks, posing significant risks to their functionality and security.

Secondary channel vulnerabilities: Two studies mention in the context of CI and the quantum age, secondary channel vulnerabilities refer to potential weaknesses in alternative communication channels or mechanisms beyond primary ones. These vulnerabilities could persist even after upgrading primary command channels to quantum-secure cryptography. Infrequently used systems like SCADA may remain susceptible, posing risks to the functioning and security of CPDs in CI.

Exposure of previously protected details: One study mention that pertains to the potential revelation of confidential information about critical systems due to quantum computing. This includes system locations, operations, vulnerabilities, and other sensitive characteristics. Adversaries can exploit this information to launch non-cryptographic attacks, leading to heightened risks for the functioning and security of CPDs within CI in the quantum age.

Improper key distribution: Two studies mention improper key distribution in CI during the quantum age poses a cybersecurity threat due to quantum computers' potential to compromise key distribution protocols like Diffie-Hellman. This vulnerability could compromise the confidentiality and integrity of cryptographic keys used in CPDs, adding to the challenges posed by quantum computing's impact on encryption methods and security measures in critical systems.

Limited implementation of PQC: Two studies mention while the transition to post-quantum security measures is crucial to counter quantum threats, the integration of these measures can be intricate and time-consuming. This inadequacy could leave critical systems vulnerable to quantum-based attacks, highlighting the need for comprehensive efforts to ensure the resilience of CPDs in CI. Similarly, the lack of standardized and widely adopted PQC solutions adds complexity to addressing the vulnerabilities posed by quantum computing.

Exploitation of quantum side channel attacks: Two studies mention the susceptibility of quantum technologies, like QKD, to exploitation through side-channel attacks poses a cybersecurity risk for CI. These attacks take advantage of the physical properties of quantum hardware to extract sensitive information, potentially compromising the security of CPDs that rely on quantum technologies. This vulnerability underscores the need for comprehensive security measures to mitigate potential side-channel threats in the quantum age.

Greater connectivity and interconnection of CPS with the Internet: One study mention increased connectivity and interconnection of CPS with the internet and other networks have exposed CI to new threats, making them susceptible to cyber-attacks exploiting vulnerabilities in open protocols. Additionally, the reliance on outdated and unsupported systems within CI, combined with the emergence of quantum computing, poses a significant cybersecurity risk. This combination of factors compromises the cybersecurity of CPDs in CI in the quantum age, necessitating comprehensive security measures to address these vulnerabilities.

Security approach by obscurity: One study mentions the reliance on a security-by-obscurity approach, characterized by proprietary or poorly documented technologies, within the design of SCADA systems has left CI vulnerable to cyber threats. This outdated security approach, combined with the increased

connectivity of CPS to the internet and the potential threat of quantum computing, compromises the cybersecurity of CPDs in CI in the quantum age.

Time sensitive operations: Five studies mention time-sensitive operations of CI pose a challenge to cybersecurity in the quantum age. The increased computational overhead introduced by implementing complex PQC algorithms can impact the efficiency and timeliness of operations. This additional burden on CPDs may affect their real-time responsiveness and compromise the overall functioning of critical systems.

III. RESEARCH RESULTS

This section synthesizes the results and significance of the review. It highlights the vulnerability of cyber-physical devices' (CPDs) cybersecurity in the quantum age due to current cryptographic weaknesses. Urgent implementation of quantum-resistant solutions, like Quantum Key Distribution (QKD), is stressed. However, the lack of readiness and understanding in the cybersecurity community for this transition is noted. The importance of research and collaboration in quantum-resistant cryptography to counter quantum threats is emphasized. Ongoing efforts to develop and standardize post-quantum cryptography (PQC) algorithms are highlighted. Addressing cybersecurity challenges in CPDs through quantum-resistant solutions and community collaboration is crucial.

The research questions were applied to the selected studies, revealing vulnerabilities in the cybersecurity of critical cyber-physical systems in the quantum era and highlighting key challenges, such as the impact of quantum computing, the transition to quantum-resilient algorithms, and the need for quantum cybersecurity awareness and education.

The review revealed that the cybersecurity of critical cyber-physical devices is threatened in the quantum era due to weaknesses in cryptographic algorithms, lack of preparedness in the cybersecurity community, and difficulties in upgrading existing devices. Challenges include adapting to quantum computing, supply chain security, and the need for quantum-resistant authentication and access measures. Although no specific attacks leveraging quantum computing were identified, potential attack scenarios were highlighted, such as exploiting vulnerabilities in current cryptographic algorithms and intercepting communications. These findings underscore the importance of addressing security in the quantum era through multidisciplinary approaches and proactive measures.

The systematic review provides a detailed overview of vulnerabilities and challenges in securing critical cyber-physical systems in the quantum era, emphasizing the need for quantum-resilient measures and comprehensive security approaches.

IV. DISCUSSION AND CONCLUSION

The analysis of the results obtained is specifically described and the authors' appreciations on the development of the review carried out focus on various aspects. The vulnerability of cybersecurity in cyber-physical devices in the quantum era is highlighted due to the weakness of asymmetric and symmetric cryptographic algorithms and protocols. To address this problem, the implementation of cryptographic solutions resistant to quantum attacks, such as QKD, is suggested. However, the lack of preparation of the cybersecurity community to make the transition to algorithms resistant to quantum cyberattacks is mentioned, which underscores the importance of research and collaboration in the field of quantum resistant cryptography. Ongoing efforts to develop and standardize PQC algorithms that can withstand quantum cyberattacks are emphasized, and the relevance of staying up to date on advances in quantum-resistant cryptography is highlighted. In addition, the difficulty in updating cyber-physical devices is pointed out, since the compatibility mechanisms for older devices that use insecure quantum encryption represent critical vulnerabilities in the cybersecurity system. This is especially relevant in CI, where the availability of the service does not allow continuous or long-term interruptions to update said devices. The review focuses on various challenges and considerations in the context of cybersecurity in cyber-physical devices in the quantum age. First, quantum computing threatens to break current encryption, exposing sensitive information and allowing unauthorized access to devices. The urgent need for a transition to quantum resistance algorithms to counter this threat is highlighted. Adapting existing devices to the quantum age is a complex and costly process due to resource constraints and compatibility vulnerabilities. The lack of preparation and limited understanding of quantum threats in the cybersecurity community presents an additional challen-

ge. QKD is a promising solution, but it faces technical and infrastructural obstacles to its effective implementation. Supply chain security is crucial to prevent vulnerabilities introduced during device manufacturing or distribution. Likewise, the importance of developing access control and authentication mechanisms resistant to quantum technology to protect devices from unauthorized access and manipulation is highlighted. On the other hand, the need for adequate security lifecycle management is highlighted to guarantee the continuous protection of cyber-physical devices. The integration of quantum algorithms with existing security measures and security assurance are crucial aspects in the transition process towards quantum resistance. Concerns about long-term security and exposing previously protected details in the quantum age are also mentioned.

The analysis of the results and the authors' appreciations focus on the vulnerabilities and risks associated with quantum computing in the field of cybersecurity of cyber-physical devices. Firstly, it is highlighted that cryptographic algorithms such as RSA or ECC would be vulnerable to attacks from quantum computers due to their ability to factorize large numbers and solve the discrete logarithm problem more efficiently than classical computers. This compromises the security of the cyber-physical devices that use these algorithms. In addition, several types of potential quantum attacks that can exploit vulnerabilities in cyber-physical devices are identified. Quantum side channel attacks involve the analysis of unintentional information leaks, such as power consumption or electromagnetic emissions, to obtain sensitive information. Quantum replication attacks would allow attackers to capture and store quantum states of devices to later manipulate or disrupt their operations. QKD attacks would compromise the security of cyber-physical devices by intercepting or tampering with securely exchanged keys. In addition, the risk of physical attacks on cyber-physical devices is highlighted through the manipulation of hardware components or the injection of malicious code into firmware or software. This is enhanced using quantum technologies, such as quantum sensors or quantum hacking techniques, which allow attackers to develop new methods to physically attack these devices. Some of the authors' insights focused on the challenges and risks associated with quantum computing in the field of cybersecurity of cyber-physical devices. It is highlighted that quantum computers can compromise many of the current encryption algorithms used to protect these devices, exposing sensitive information and allowing unauthorized access to systems. It is noted that understanding of quantum threats is limited in the cybersecurity community, making it difficult to develop effective defenses against quantum attacks. Furthermore, adapting existing devices to make them resistant to quantum technology can be complex and expensive, especially in CI with legacy systems and technology dependency. Supply chain security is critical, as the introduction of vulnerable or compromised components during manufacturing or distribution can create significant vulnerabilities in CI. The review highlights the need to develop quantum-resistant authentication and access control mechanisms to protect cyber-physical devices from unauthorized access and tampering. It also emphasizes the importance of the transition to PQC algorithms to ensure security in the quantum age. Furthermore, it is mentioned that the long lifespan and reliance on legacy technologies make cyber-physical devices more vulnerable to attacks in the quantum age, especially if they cannot be easily upgraded or replaced. On the other hand, several specific threats related to the quantum era are identified, such as quantum side channel attacks, quantum replay attacks, QKD attacks, and physical attacks. The exposure of previously protected details due to quantum computing is also mentioned.

In conclusion, the following is highlighted:

- The importance of collaboration and constant adaptation to address cybersecurity challenges in the quantum age and ensure the security of cyber-physical devices in the future.
- The challenges require specialized solutions and close collaboration between academia, industry and government to mitigate cybersecurity risks and ensure a successful transition to the quantum age.
- The review analysis highlights the importance of addressing cybersecurity vulnerabilities and risks in the quantum age, and the need to develop resilient security solutions and measures to protect cyber-physical devices in this new technological age.
- In general, the analysis highlights the need to develop cybersecurity solutions and measures to adequately protect cyber-physical devices in this new technological era and face the challenges posed by quantum computing about cybersecurity.

CRediT AUTHORSHIP CONTRIBUTION STATEMENT

Siler Amador-Donado: conceptualization, data curation, formal analysis, research, software, visualization and writing - original draft. César Jesús Pardo-Calvache: conceptualization, project management, methodology, supervision and writing - review and editing. Raúl Iván Mazo-Peña: conceptualization, project management and writing - review and editing.

ACKNOWLEDGMENTS

Professors Siler Amador Donado and César Pardo Calvache are grateful for the contribution of the University of Cauca, where they work as titular professors respectively.

REFERENCES

[1] A. Souag, C. Salinesi, R. Mazo, and I. Comyn-Wattiau, “A security ontology for security requirements elicitation”, en Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, vol. 8978, pp. 157–177, doi: 10.1007/978-3-319-15618-7_13.

[2] A. A. Nazarenko and G. A. Safdar, “Survey on security and privacy issues in cyber physical systems”, AIMS Electronics and Electrical Engineering, vol. 3, núm. 2. American Institute of Mathematical Sciences, pp. 111–143, abr. 16, 2019, doi: 10.3934/ElectrEng.2019.2.111.

[3] A. Sundararajan, A. Chavan, D. Saleem, y A. Sarwat, “A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security”, Energies, vol. 11, núm. 9, p. 2360, sep. 2018, doi: 10.3390/en11092360.

[4] M. P. Barrett, “Framework for improving critical infrastructure cybersecurity”, Natl. Inst. Stand. …, 2018, [En línea]. Available in: https://n9.cl/ozj9u.

[5] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic Mapping Studies in Software Engineering”, in BASE - Revista de Administração e Contabilidade da Unisinos, jun. 2008, pp. 1–10, doi: 10.14236/ewic/EASE2008.8.

[6] B. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering”. UK, 2007.

[7] D. Budgen y P. Brereton, “Performing systematic literature reviews in software engineering”, ACM, New York, NY, USA, may 2006. doi: 10.1145/1134285.1134500.

[8] R. van Solingen, V. Basili, G. Caldiera, y H. D. Rombach, “Goal Question Metric (GQM) Approach”, in Encyclopedia of Software Engineering, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2002.

[9] S. Edded, S. Ben Sassi, R. Mazo, C. Salinesi, and H. Ben Ghezala, “Collaborative configuration approaches in software product lines engineering: A systematic mapping study”, J. Syst. Softw., vol. 158, p. 110422, dic. 2019, doi: 10.1016/j.jss.2019.110422.

[10] M. B. Eriksen and T. F. Frandsen, “The impact of patient, intervention, comparison, outcome (PICO) as a search strategy tool on literature search quality: a systematic review”, J. Med. Libr. Assoc., vol. 106, num. 4, oct. 2018, doi: 10.5195/jmla.2018.345.

[11] L. Yang et al., “Quality Assessment in Systematic Literature Reviews: A Software Engineering Perspective”, Inf. Softw. Technol., vol. 130, p. 106397, feb. 2021, doi: 10.1016/j.infsof.2020.106397.

[12] M. Ivarsson and T. Gorschek, “A method for evaluating rigor and industrial relevance of technology evaluations”, Empir. Softw. Eng., vol. 16, num. 3, pp. 365–395, jun. 2011, doi: 10.1007/s10664-010-9146-4.

[13] D. Chen, Y. Peng, and H. Wang, “Development of a Testbed for Process Control System Cybersecurity Research”, in Proceedings of the 3rd International Conference on Electric and Electronics, nov. 2013, vol. 69, doi: 10.2991/eeic-13.2013.37.

[14] T. Cruz et al., “A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems”, IEEE Trans. Ind. Informatics, vol. 12, num. 6, pp. 2236–2246, dec. 2016, doi: 10.1109/TII.2016.2599841.

[15] A. Cook, A. Nicholson, H. Janicke, L. Maglaras, and R. Smith, “Attribution of Cyber Attacks on Industrial Control Systems”, EAI Endorsed Trans. Ind. Networks Intell. Syst., vol. 3, num. 7, p. 151158, apr. 2016, doi: 10.4108/eai.21-4-2016.151158.

[16] G. Gonzalez-Granadillo et al., “Dynamic risk management response system to handle cyber threats”, Futur. Gener. Comput. Syst., vol. 83, pp. 535–552, 2018, doi: 10.1016/j.future.2017.05.043.

[17] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, “Cyber-physical systems and their security issues”, Comput. Ind., vol. 100, pp. 212–223, sep. 2018, doi: 10.1016/j.compind.2018.04.017.

[18] S. Hussain, M. Meraj, M. Abughalwa, and A. Shikfa, “Smart Grid Cybersecurity: Standards and Technical Countermeasures”, in 2018 International Conference on Computer and Applications (ICCA), aug. 2018, pp. 136–140, doi: 10.1109/COMAPP.2018.8460390.

[19] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues”, IEEE Commun. Surv. Tutorials, vol. 21, num. 3, pp. 2886–2927, 2019, doi: 10.1109/COMST.2019.2899354.

[20] S. Paul and M. Niethammer, “On the importance of cryptographic agility for industrial automation”, - Autom., vol. 67, núm. 5, pp. 402–416, may 2019, doi: 10.1515/auto-2019-0019.

[21] S. N. Islam, Z. Baig, and S. Zeadally, “Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures”, IEEE Trans. Ind. Informatics, vol. 15, num. 12, pp. 6522–6530, dic. 2019, doi: 10.1109/TII.2019.2931436.

[22] S. Ghosh and S. Sampalli, “A Survey of Security in SCADA Networks: Current Issues and Future Challenges”, IEEE Access, vol. 7, pp. 135812–135831, 2019, doi: 10.1109/ACCESS.2019.2926441.

[23] M. K. Choi, C. Y. Yeun, and P. H. Seong, “A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology”, IEEE Access, vol. 8, pp. 118732–118740, 2020, doi: 10.1109/ACCESS.2020.3005134.

[24] G. Sharkov, “Assessing the Maturity of National Cybersecurity and Resilience”, Connect. Q. J., vol. 19, num. 4, pp. 5–24, 2020, doi: 10.11610/Connections.19.4.01.

[25] B. W. Tuinema, J. L. R. Torres, A. I. Stefanov, and ..., “Cyber-physical system modeling for assessment and enhancement of power grid cyber security, resilience, and reliability”, … Reliab. Anal. …, 2020, doi: 10.1007/978-3-030-43498-4_8.

[26] T. M. Fernández-Caramés and P. Fraga-Lamas, “Use Case Based Blended Teaching of IIoT Cybersecurity in the Industry 4.0 Era”, Appl. Sci., vol. 10, núm. 16, p. 5607, aug. 2020, doi: 10.3390/app10165607.

[27] A. Homay, C. Chrysoulas, B. El Boudani, M. de Sousa, and M. Wollschlaeger, “A security and authentication layer for SCADA/DCS applications”, Microprocess. Microsyst., vol. 87, num. November, p. 103479, 2021, doi: 10.1016/j.micpro.2020.103479.

[28] A. Mohammad, “Development of the concept of electronic government construction in the conditions of synergetic threats”, Technol. Audit Prod. Reserv., vol. 3, num. 2(53), pp. 42–46, jun. 2020, doi: 10.15587/2706-5448.2020.207066.

[29] J. P. A. J.-P. A. Yaacoub, O. Salman, H. N. H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, “Cyber-physical systems security: Limitations, issues and future trends”, Microprocess. Microsyst., vol. 77, p. 103201, sep. 2020, doi: 10.1016/j.micpro.2020.103201.

[30] P. G. Evans et al., “Trusted Node QKD at an Electrical Utility”, IEEE Access, vol. 9, pp. 105220–105229, 2021, doi: 10.1109/ACCESS.2021.3070222.

[31] C. Hemminghaus, J. Bauer, and K. Wolsing, "SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures", in 2021 International Symposium on Networks, Computers and Communications (ISNCC), oct. 2021, pp. 1–6, doi: 10.1109/ISNCC52172.2021.9615738.

[32] A. N. Ahmadi, "A comprehensive cybersecurity framework for afghanistan's cyberspace", Int. J. Eng. Appl. Sci. Technol., vol. 6, num. 2, jun. 2021, doi: 10.33564/ijeast.2021.v06i02.032.

[33] O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and K. O. A. Alimi, "A Review of Research Works on Supervised Learning Algorithms for SCADA Intrusion Detection and Classification", Sustainability, vol. 13, num. 17, p. 9597, aug. 2021, doi: 10.3390/su13179597.

[34] C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, and ..., "A Survey on Privacy for B5G/6G: New Privacy Goals, Challenges, and Research Directions", arXiv Prepr. arXiv …, 2022, [On line]. Available in: https://arxiv.org/abs/2203.04264.

[35] J. Pöyhönen, "Cyber Security of an Electric Power System in Critical Infrastructure", pp. 217–239, 2022, doi: 10.1007/978-3-030-91293-2_9.

[36] A. Konev, A. Shelupanov, M. Kataev, V. Ageeva, and ..., "A Survey on Threat-Modeling Techniques: Protected Objects and Classification of Threats", Symmetry (Basel)., 2022, [On line]. Available in: https://www.mdpi.com/1532736.

[37] M. Alshowkan, P. G. Evans, M. Starke, D. Earl, and N. A. Peters, "Authentication of smart grid communications using quantum key distribution", Sci. Rep., vol. 12, num. 1, p. 12731, jul. 2022, doi: 10.1038/s41598-022-16090-w.

[38] P.-Y. Kong, "A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security", IEEE Syst. J., vol. 16, núm. 1, pp. 41–54, mar. 2022, doi: 10.1109/JSYST.2020.3024956.

[39] P. Vähäkainu, M. Lehto, and A. Kariluoto, "Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures", en Cyber Security, Springer, 2022, pp. 255–292.

[40] D. Rosch-Grace y J. Straub, "Analysis of the likelihood of quantum computing proliferation", Technol. Soc., vol. 68, feb. 2022, doi: 10.1016/j.techsoc.2022.101880.