ENFOQUE UTE
REVISTA
Facultad Ciencias de la Ingeniería e Industrias

REVIEW ARTICLE

ENFOQUE UTE, VOL. 16, NO. 4, pp. 9-18, E-ISSN: 1390-6542
RECEIVED MARCH 06, 2025; ACCEPTED SEPTEMBER 08, 2025; PUBLISHED ONLINE OCTOBER 01, 2025; DATA OF CURRENT VERSION OCTOBER 01, 2025; PUBLISHED IN VOLUME 16, ISSUE 4 (OCTOBER 2025).

Challenges of information security management in the industrial sector: A systematic review

Shonerly Bustamante[1*], Pedro Castañeda[2], and Ciro Rodríguez[3]

***Abstract* — Currently, in the industrial sector, technology can significantly increase productivity and efficiency. However, this advancement also generates multiple challenges related to information security that must be addressed. This systematic review aimed to analyze these challenges in information security management, focusing on three specific aspects: protection models and methodologies, factors that generate vulnerabilities in industrial control systems (ICS), and cyber risks that affect the supply chain. To this end, 45 articles published in journals indexed in databases such as Scopus, EBSCO and ScienceDirect over the last four years were examined. The results indicate that approaches based on Zero Trust, Shapley Additive Explanations (SHAP), Evolutionary Multi-Objective Optimization (EMO) algorithms, and the use of the Industrial Internet of Things (IIoT) offer greater effectiveness in protecting information. In addition, the following were identified as the main vulnerability factors in ICS: excessive connectivity, the use of obsolete operating systems, uncontrolled physical access, incorrect configurations, poor maintenance, cyberattacks, and human error. With regard to the industrial supply chain, the most relevant risks include successful cyberattacks, ransomware, and industrial espionage. In conclusion, security challenges range from interoperability between systems to a shortage of specialized personnel, requiring continuous monitoring and a multidisciplinary strategic approach.**

***Keywords*: Industrial control systems, supply chain, cybersecurity, critical infrastructures.**

***Resumen* — Actualmente, en el sector industrial, la tecnología puede aumentar significativamente la productividad y eficiencia. Sin embargo, este avance también genera múltiples desafíos relacionados con la seguridad de la información que deben ser abordados. Esta revisión sistemática tuvo como objetivo analizar dichos desafíos en la gestión de la seguridad de la información, enfocándose en tres aspectos específicos: los modelos y metodologías de protección, los factores que generan vulnerabilidades en los sistemas de control industrial (ICS), y los riesgos cibernéticos que afectan la cadena de suministro. Para ello, se examinaron 45 artículos publicados en revistas indexadas en bases de datos como Scopus, EBSCO y ScienceDirect durante los últimos cuatro años. Los resultados indican que los enfoques basados en Zero Trust, Shapley Additive Explanations (SHAP), algoritmos de Optimización Multiobjetivo Evolutiva (EMO) y el uso del Internet Industrial de las Cosas (IIoT) ofrecen una mayor efectividad en la protección de la información. Además, se identificaron como principales factores de vulnerabilidad en los ICS: la conectividad excesiva, el uso de sistemas operativos obsoletos, el acceso físico no controlado, las configuraciones incorrectas, el mantenimiento deficiente, los ataques informáticos y el error humano; respecto a la cadena de suministro industrial, los riesgos más relevantes incluyen los ciberataques exitosos, el ransomware y el espionaje industrial. En conclusión, los desafíos de seguridad abarcan desde la interoperabilidad entre sistemas hasta la escasez de personal especializado, lo cual requiere una vigilancia continua y un enfoque estratégico multidisciplinario.**

***Palabras Clave*: Sistemas de control industrial, cadena de suministro, ciberseguridad, infraestructuras críticas.**

I. INTRODUCTION

IN the context of the rapid adoption of digital technologies in the business world, information has become not only an indispensable resource for optimizing organizational performance, but also acquires crucial strategic value in decision-making processes [1] [2].

However, threats to information security are evolving at an unprecedented rate, driven by rapid advances in technology, which can materialize due to multiple factors, such as system vulnerabilities, human error, and, above all, intentionally malicious actions [3] [4].

Likewise, there has been a notable increase in the incidence of attacks and threats such as ransomware, phishing, malware, email breaches, and fund transfer fraud within organizations [5]. In line with these observations, a recent report by [6] focused on Latin America reveals that approximately 67.4 % of organizations have suffered significant information losses.

Similarly, the security challenges posed by the rise of technology and internet connectivity of devices seem to be incessant in the supply chain of industries [7], as sectors that depend on Industrial Control Systems (ICS) face multiple forms of attack due to the growing interconnection and integration of Information Technology (IT) systems with Operational Technology (OT) systems [8].

* *Corresponding autor:* shonerly.bustamante@unmsm.edu.pe
1. National University of San Marcos, Lima, Perú (e-mail: shonerly.bustamante@unmsm.edu.pe). ORCID number https://orcid.org/0000-0002-8173-203X.
2. National University of San Marcos, Lima, Perú (e-mail: pedro.castaneda@unmsm.edu.pe). ORCID number https://orcid.org/0000-0003-1865-1293.
3. National University of San Marcos, Lima, Perú (e-mail: crodriguezro@unmsm.edu.pe). ORCID number https://orcid.org/0000-0003-2112-1349.

DOI: https://doi.org/10.29019/enfoqueute.1152
Associate Editor: *Freddy Alvarez*

So what is happening in the industrial sector? According to [9], this sector constantly faces security challenges and is often the victim of information theft or loss. This vulnerability stems from limited resources, which make it difficult to strengthen security measures in terms of both technology and specialized personnel [10].

In a recent survey on ICS security, 45 % of participants admitted to having experienced cyber incidents in the last 12 months [11], highlighting that information security incidents represent a significant business risk for any organization [12].

Under this approach, the increase in attacks and vulnerabilities to industrial systems is closely related to factors such as their intrinsic nature, their dependence on computer networks for data transmission, and the implementation of specific protocols [13]; in addition, continuous 24/7 operation makes them more susceptible to intrusions, as any interruption in their functioning could have significant consequences for their operations.

For this reason, [14] [15] consider that the security challenges faced by industrial systems range from updates and real-time performance limitations to communication with legacy devices, physical mechanisms, infrastructure, and risk management. However, the question arises: What role does the human factor play in these challenges?

From this perspective, it should be noted that existing studies on information security management in the industrial sector have significant gaps, as many of them focus predominantly on specific technological solutions, such as the implementation of intrusion detection systems or the adoption of security architectures, without sufficiently considering the operational context and practical limitations of industries. Much less do they comprehensively address the human factor and its impact on industrial cybersecurity.

Based on this issue, the following research question arises: What are the main challenges facing the industrial sector in information security management? This question seeks to identify and analyze the various difficulties that industrial companies must overcome to protect their information systems and operational technologies from growing cyber threats, so that up-to-date information on this topic is made available to the scientific community and more effective strategies can be developed to mitigate risks and strengthen security in complex and interconnected industrial environments.

The rest of the document is structured as follows: first, the research methodology is explained and a description of the study is provided in four phases, from the identification approach to the inclusion of the selected articles. Second, the results and discussions are presented; and finally, the conclusions are shown, followed by the bibliographic references.

II. METHODOLOGY

The research was structured in accordance with PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, ensuring methodological rigor, transparency, and reproducibility at every stage [16]; in addition, it is considered essential for the proper accumulation of scientific knowledge [17], for which, following the procedure of [18]. The process was carried out in four phases: identification, selection, eligibility, and inclusion, complemented by the application of the AMSTAR tool for critical assessment of methodological quality.

A. Phase I: Identification

In order to answer the main research question, the following questions were posed:

- Q1: Which information security models and methodologies are most suitable for industrial environments?
- Q2: What factors contribute to the vulnerability of industrial control systems (ICS)?
- Q3: What are the biggest cybersecurity risks in the industrial sector supply chain?

To ensure comprehensive coverage of the literature, various databases were explored with the aim of compiling relevant material on information security management and industrial control systems. Given the dispersion of related articles across multiple sources, it was decided to limit the search to three specific databases: Scopus, Ebsco, and ScienceDirect, selected for their broad access to academic publications and peer-reviewed articles.

A total of 1,031 documents were selected, which were filtered using search strings to ensure accuracy in each query, as detailed in Table I.

TABLE I
SEARCH STRING

Database	Search string
Scopus	(“cybersecurity challenges” OR “information security challenges” AND “operational technology”) – (“industrial control systems” AND “cyberattacks” OR “cybersecurity threats”)
Ebsco	(“Information security management challenges AND industrial sector”) – (“Cybersecurity AND challenges AND industrial management”)
ScienceDirect	(“information security policies” AND “industry”) - (“IT and OT integration” AND “industry”) - (“industrial control systems” AND “cybersecurity” OR “cyberattacks”)

B. Phase II: Selection

With regard to search sources, selection and exclusion criteria were included, as shown below in Table II:

TABLE II
SELECTION CRITERIA

Selection criteria	Exclusion criteria
Published in journals evaluated by the SCImago (SJR) impact index.	Primary research such as theses, posters, books, conference proceedings, etc.
Spanish and English.	
Four years old.	Older than four years.
Open access articles.	
Closely related to the research question.	Context unrelated to the research.

C. Phase 3: Eligibility

After identifying the articles in the initial phase, they were subjected to a rigorous filtering and selection process. This process included the application of specific criteria related to the research objectives, such as thematic relevance, timeliness of the information, and quality of the sources. As this process progressed, articles were eliminated not meet these requirements were eliminated. Fig. 1 illustrates each step of the selection process, from initial identification to final refinement, ensuring that only the most relevant and high-quality articles are considered for the research.

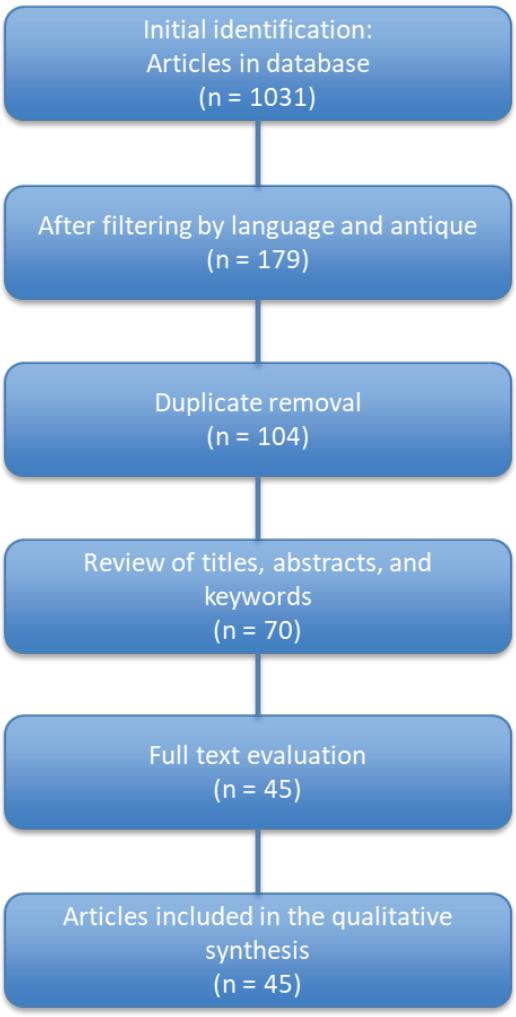

Fig. 1. Article selection process.

From an initial total of 1,031 scientific articles, the application of filters based on language and document age reduced the number to 179. Subsequently, an analysis of duplicate titles and authors was performed to avoid redundancies between different databases (Scopus, Ebsco, and ScienceDirect), reducing the set to 104 articles. After a thorough review of titles, abstracts, and keywords, 34 articles were excluded for not aligning with the study objectives. Next, a comprehensive evaluation of the content of the remaining 70 articles was carried out, revealing that some did not explicitly address the concepts of industrial control systems or include methods or models for security management in these environments. Finally, 45 articles were identified as highly relevant for examining emerging challenges and the current state of the industrial sector.

D. Phase 4: Inclusion

A total of 45 studies were included in the qualitative synthesis, representing the most up-to-date evidence on information security management in the industrial sector.

Fig. 2 shows the distribution of databases based on the number of publications, showing that Scopus accounts for more than 70 % of publications, positioning itself as the main source of reference. In contrast, 25.54 % of publications are found in Ebsco and ScienceDirect, indicating that, although these databases are also relevant, they have a lower representation.

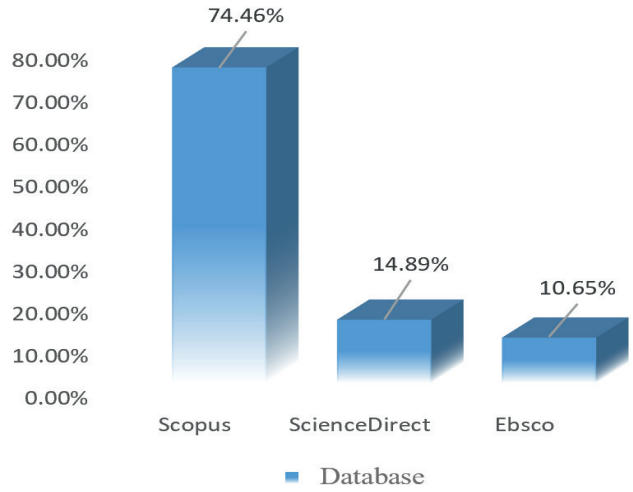

Fig. 2. Percentage of article per database.

When analyzing studies over the years, we observe in Fig. 3 that the years 2022 and 2023 have the highest number of research projects. In contrast, 2021 shows lower scientific output in this field, which could reflect variations in research priorities and the evolution of cyber threats, and with regard to 2024, this is probably due to the state of scientific production in progress.

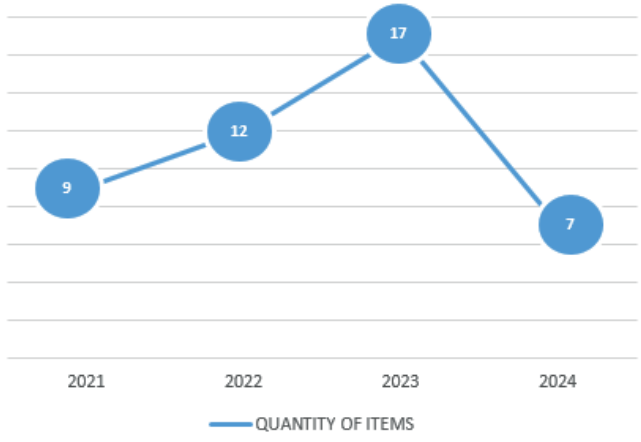

Fig. 3. Number of articles per year.

Similarly, a detailed analysis of the topics covered in the article is carried out, highlighting mainly industrial cyber threats (40 %), followed by vulnerabilities and threats in Industrial Control Systems (ICS) with 28.9 %. These topics are particularly relevant, as they provide a more precise and informed approach to effectively address and respond to the questions raised in the research (Figure 4). However, there is little literature on information security challenges in industries (8.9 %), which shows a lack of interest in this topic.

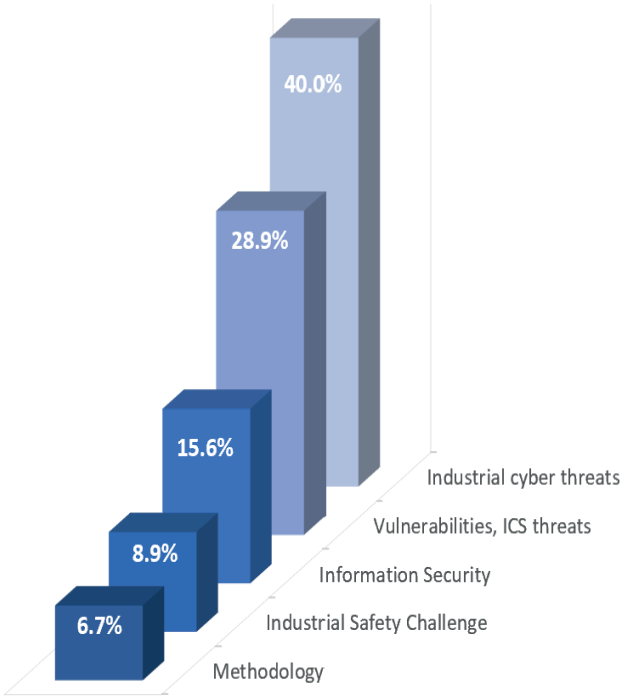

Fig. 4. Percentage of topic included.

E. Quality assessment - AMSTAR

In order to reinforce the internal and external validity of the results, the AMSTAR (A MeaSurement Tool to Assess Systematic Reviews) tool was used as a framework to assess the methodological quality of the 45 studies included. The criteria were adapted to the context of this research and applied as shown in Table III and Table IV:

TABLE III
QUALITY LEVEL

SCORE	NOT	PARTIAL	YES
	(0)	(0)	(1)
QUALITY	**LOW**	**MODERATE**	**HIGH**
	(0–3)	(4–7)	(8–10)

TABLE IV
QUALITY CRITERIA

ID	CRITERION	DESCRIPTION
A1	Clearly defined research question and inclusion criteria	Each article included was verified to ensure that it explicitly addressed the research questions.
A2	Exhaustive bibliographic search	We evaluated whether the selected articles had used comprehensive search strategies in relevant academic databases.
A3	Selection of duplicate studies.	We reviewed whether the selection process for the included articles was carried out by at least two researchers or through cross-checking.
A4	List of included and excluded studies.	We analyzed whether the articles transparently documented which studies were included in their analyses.
A5	Study characteristics adequately described.	We evaluated whether the articles described in detail the industrial context, control systems, methodological frameworks applied, and variables considered.
A6	Methodological quality of studies evaluated and documented.	It was verified whether the articles evaluated the methodological soundness of their own studies.
A7	Methodological quality is used in the conclusions.	We reviewed whether the authors of the articles included methodological limitations in their conclusions.
A8	Appropriate methods for synthesizing results.	We analyzed whether the studies used appropriate analytical methods to synthesize the evidence without interpretative bias.
A9	Probability of publication bias assessed.	It was verified whether the studies explicitly discussed the risk of publication bias.
A10	Declared conflicts of interest.	It was verified whether the articles included statements of conflicts of interest and funding.

After evaluating the 45 articles included in the review and considering the 10 criteria established, the results summarized in Fig. 5 show that all of the studies analyzed achieved a high level of quality (100 %), which guarantees the methodological soundness and validity of the findings reported.

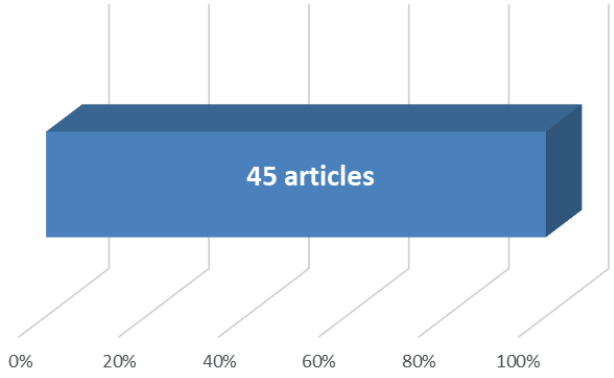

Fig. 5. Synthesis of reviewed articles.

III. RESULTS

Q1: Which information security models and/or methodologies are most suitable for industrial environments?

In particular, the authors in [19] develop a systematic methodology for modeling and mitigating potential threats in industrial environments, with the aim of safeguarding assets and providing a comprehensive view of risks. To this end, they use digital twin methods and the smart manufacturing framework as variables, starting with the identification of the assets to be protected; then, possible attacks are evaluated considering two key factors: the attack vector and the type of attack based on the useful life, and finally, cyberattacks were modeled based on ICS ATT&CK® to develop a risk matrix that included levels, severity, and necessary treatments. This methodology was applied to a prototype production line at a Festo test bench, demonstrating that it enables comprehensive threat modeling, accurate risk identification, and the proposal of effective mitigation controls.

Likewise, [20] introduce an advanced multimodal federated model with the aim of detecting cyberattacks in industrial control systems. The model consists of three fundamental elements: first, representation learning, which converts the original customer data into a latent space; second, domain adaptation, which translates this data into a common representation space; and third, a federated approach that allows the model to be trained collaboratively to detect cyberattacks. To improve the transparency of the model, the Shapley Additive Explanations (SHAP) method was implemented, which provides detailed information on the model's results, helping cybersecurity experts in their decision-making. Experimental tests revealed an average improvement of 8.2 % in the score across three clients; furthermore, by applying SHAP for feature reduction, a 4.9 % improvement in the score was achieved, even when the feature set was reduced by half.

Similarly, the model proposed by [21] based on ZERO TRUST architecture, was designed with the aim of protecting vulnerable communication channels between manufacturing equipment in manufacturing industries. This approach included identifying devices connected to the network, managing access to manufacturing resources, and monitoring the network and communications using tools such as intrusion detection systems, an Enterprise Device Discovery System that verifies and validates the identity of each device newly connected to the network, and an Endpoint Compliance Management System that monitors the status of devices in relation to pre-established compliance policies. The results demonstrated the effectiveness of the security model for IT infrastructure in various industries, protecting the environment and managing access to resources in a controlled manner through specific policies.

In addition, [22] developed an Intrusion Detection System (IDS) model designed to identify and differentiate malicious actions in real time in Industrial Internet Control Systems (IICS) networks powered by IIoT. This model was created in response to the insufficient generalization, classification errors, and high false alarm rates of existing detection methods. Experimental results on two benchmark datasets demonstrated the model's superiority, achieving accuracy rates of 97.95 % and 97.62 %, respectively, compared to other methods. In conclusion, the model significantly improved the accuracy of cyberattack identification, strengthening security in interconnected industrial environments and protecting them against emerging cyber threats.

Finally, [23] present a methodology aimed at identifying vulnerabilities in heterogeneous and complex industrial control systems (ICS) using two Evolutionary Multi-Objective Optimization (EMO) algorithms: NSGA-II and SPEA2. To evaluate the performance of this methodology, two statistical tests were used: the Kruskal-Wallis test for non-normally distributed data and the ANOVA test for normally distributed data, with a 95 % confidence interval for all experiments. Following experimental evaluation in a chemical plant simulator, the EMO approach developed was shown to be an effective methodology for identifying vulnerabilities in industrial control systems, as well as weaknesses in existing detection systems.

To articulate the findings more analytically, Table V shows a cross-reference matrix identifying how each security model/methodology addresses or fails to address specific vulnerabilities and types of attack in industrial environments.

TABLE V
CROSS-REFERENCE MATRIX

Security model/ methodology	Vulnerabilities addressed	Types of mitigated attacks
Digital twins + ICS ATT&CK® (systematic threat modeling methodology)	Identification of critical assets, inadequate configurations, physical access.	Modeling of cyberattacks, operational disruptions, persistent intrusions.
Federated multimodal model + SHAP	Network connectivity, classification errors, dependence on multiple data sources.	Complex cyberattacks, undetected intrusions, adversarial attacks.
Zero Trust Architecture	Unauthorized access to devices, vulnerabilities in communication channels.	Intrusions through privilege escalation, internal and external network attacks.
Intrusion Detection Systems (IDS) based on IIoT	Weaknesses in real-time detection, exposed connectivity, weak configurations.	Ransomware, malware, denial-of-service (DoS) attacks.
Evolutionary Multi-Objective Optimization (EMO: NSGA-II and SPEA2).	Obsolete operating systems, vulnerable configurations, poor maintenance.	Exploitation of known vulnerabilities, attacks targeting heterogeneous ICS.

In addition, Fig. 6 shows a gap analysis in industrial security models, represented in a radar chart with seven key socio-technical dimensions:

- Data protection.
- Human factor.
- Physical protection.
- Access management.
- Intrusion detection.
- Explainability.
- Real applicability.

Each security model is evaluated on a scale of 0 = not covered, 1 = partially covered, and 2 = covered.

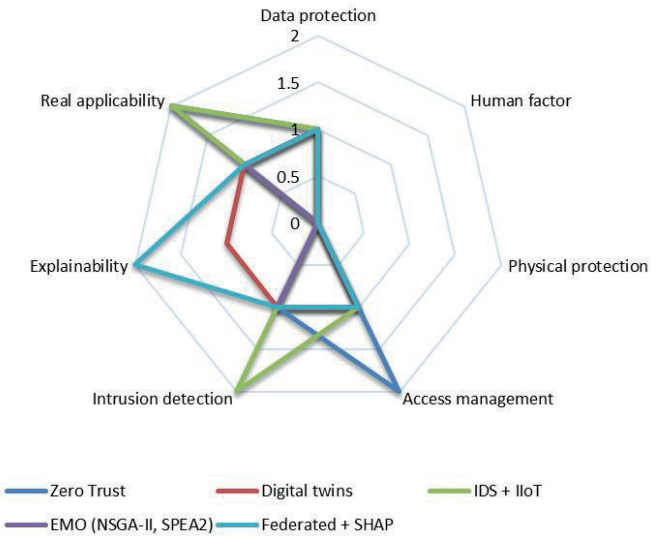

Fig. 6. Gap analysis – interpreted scale.

In summary, the graph allows us to see comparatively that:

- No model robustly covers the human factor or physical protection (all at "0").
- Zero Trust is strong in access management and practical applicability.
- IDS + IIoT excels in intrusion detection and also in real environments.
- Federated + SHAP stands out in explainability, while the other models do not.
- Digital twins and EMO show greater applicability in experimental or simulated scenarios, with limitations for real environments.

Q2: What factors contribute to the vulnerability of industrial control systems (ICS)?

With the growing adoption of Industry 4.0 and the digitization of industrial environments, advanced technologies are being adopted to improve communication and operational management, bringing improvements in reliability, efficiency, flexibility, and enabling more effective remote monitoring of systems [24]; however, they increase the vulnerability of infrastructures to cyberattacks, which can trigger serious security incidents [25].

Based on this premise, in a systematic review carried out by [26] on industrial cybersecurity, they found that connectivity and networks become factors that increase the vulnerability of industrial systems, since currently, many business applications and resources are hosted outside the traditional perimeter, where machines, computers, and people are networked and communicate simultaneously; these same factors were discovered by, [27] discovered when proposing a holistic approach to intrusion detection and mitigation, and also [28] when developing a model for protection against adversarial attacks, which was evaluated on three datasets, demonstrating the robustness of the model.

In research carried out by [29] with the aim of identifying gaps in current attack taxonomies, they mention that obsolete operating systems lacking updates represent a significant vulnerability risk for manufacturing systems. This risk is accentuated in the manufacturing industry, where, according to [30] 53 % of companies still rely on Windows XP and other operating systems that are no longer supported by vendors, as the use of these outdated platforms exposes companies to serious cyber threats.

Likewise, after an investigation to generally describe the security of ICS, [31] mention that physical access to industrial control systems, incorrect or inadequate system configurations, and poor maintenance practices are factors that create vulnerabilities and can compromise the security of industrial infrastructure. To this end, the authors conducted a thorough analysis of the main threats and weaknesses that compromise these systems, also evaluating the most effective defense strategies, including network segmentation, access controls, software update management, and constant monitoring of the security of the environment.

According to [32], computer attacks are determining factors that cause interruptions or failures in industrial systems; likewise, [33] agrees with these factors, thanks to a systematic review of attacks, vulnerabilities, and defense mechanisms in the industrial sector, also indicating that attacks have increased by 110 % since 2016. It should be noted that attacks exploit vulnerabilities, facilitating hacking, malware, and viruses; studies in various industries have shown that many of their IT systems were developed without implementing maximum security measures, lacking robust user authentication methods and also due to their dependence on open wireless communication channels [34] [35].

Despite the importance of technical and technological factors in security, the human factor remains a primary concern, constituting the greatest threat to privacy and information security [36] [37]. For this, the evaluation carried out by [38] through online surveys of organizations from different sectors in the city of León, Mexico, found that it is necessary to implement solutions with regard to people, in order to provide knowledge and skills about risks and their implications; they also point out that 39 % of security risks are linked to the human factor.

In order to provide a comprehensive socio-technical overview, it is important to highlight how organizational, cultural, and training-related factors directly affect the effectiveness or, in their absence, the vulnerability of the technical defenses implemented, as shown in Table VI.

TABLE VI
BEHAVIOR OF FACTORS WITH RESPECT TO SOCIOTECHNICAL DIMENSIONS

Sociotechnical dimension	Observed behavior/ evidence in ICS	Impact on technical defenses
Organizational behavior.	Resistance to technological change, rigid hierarchical structures, lack of leadership in security.	Delays the adoption of models such as Zero Trust or digital twins; obsolete practices remain in place.

Staff training.	Poor training in industrial cybersecurity; dependence on external suppliers.	Increases the likelihood of human error that neutralizes IDS or access policies.
Cybersecurity culture.	Perception of cybersecurity as a "cost" rather than a strategic investment; lack of shared protocols.	Weakens the implementation of technical measures, as there is no sustained compliance.
Resistance to technological change.	Lack of incentives to migrate to modern architectures; fear of loss of productivity.	Continued use of insecure protocols and flat networks that are easy to attack.
Sociotechnical dimensions of work.	Misalignment between IT experts and OT managers; poorly defined roles.	Coordination gaps that prevent rapid response to incidents.
Governance and internal policies.	Lack of clear access management and continuity policies.	This renders technical tools such as multi-factor authentication ineffective.

Similarly, Fig. 7 shows that ICS vulnerabilities do not stem solely from technical failures, but also from organizational, cultural, and physical dimensions. This reinforces the need for an integrated socio-technical approach to industrial cybersecurity.

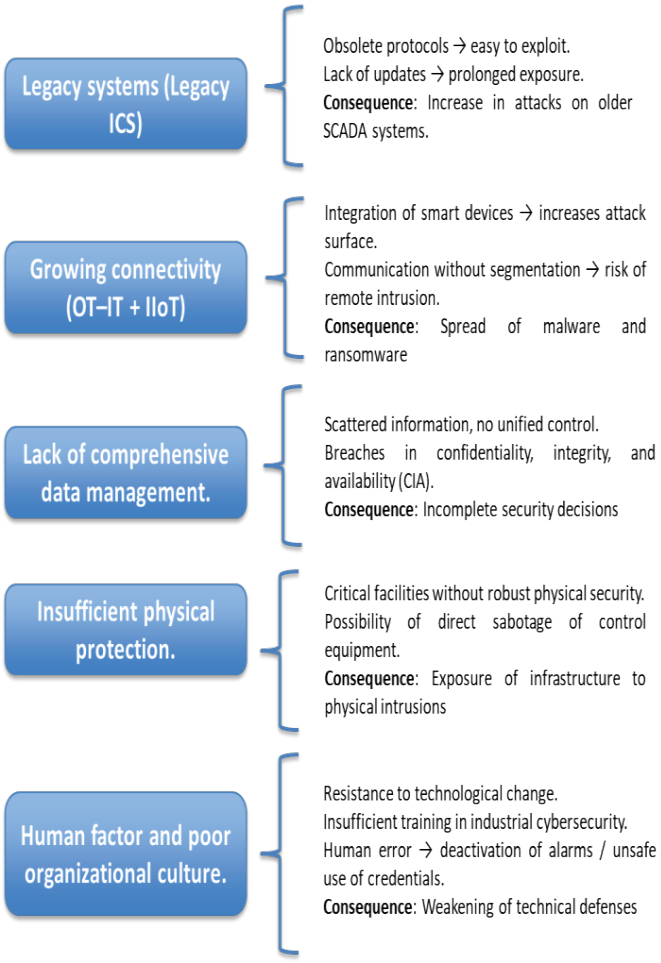

Fig. 7. Central factors.

Q3: What are the biggest cybersecurity risks in the industrial supply chain?

In an effort to optimize the loss expenses due to industrial cybersecurity breaches, using a linear optimization model, [39] [40] report that one of the greatest risks in the industry is a successful cyberattack on a node in the supply chain, which can result in the loss of intellectual property, a reduction in service levels, and a deterioration in customer trust and goodwill, causing significant disruptions in the production process. According to [41], approximately 48 % of industries have experienced some type of cyberattack, highlighting the vulnerability that exists in the manufacturing sector.

In order to offer an updated description of ransomware in industrial systems, [42] highlighted that ransomware attacks pose a considerable risk to the industrial sector, based on an analysis of the organizational and human factors that influence the behavior of this type of malware. In 2021, the Czech electricity company CEZ suffered a ransomware attack that shut down several power plants and left thousands of customers without power. In addition, in December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive following a ransomware attack on a natural gas compression facility, in which a variant of the TrickBot malware was used.

On the other hand, industrial espionage has emerged as a significant risk that encompasses various threats, both internal and external, aimed at stealing corporate secrets, as mentioned [43] after their investigation that sought to close all the spy's attack opportunities; however, despite companies' continued efforts to protect themselves, studies indicate that an alarming 75 % of companies in Germany have already fallen victim to this type of attack [44]. A notable example in the US is the attack on SolarWinds, where malicious code was discreetly inserted into SolarWinds Orion software updates, designed to spy and steal data, compromising the supply chain and affecting approximately 18,000 customers, underlining the sophistication and danger posed by espionage in industrial cybersecurity [45].

Fig. 8 shows that the most critical risks in the industrial supply chain are attacks on external suppliers and the manipulation of software or firmware in transit, located in the high probability and high impact quadrant due to their ability to compromise multiple links and generate systemic effects. This figure is strictly based on the evidence from the documents analyzed and weighted according to frequency (probability) and disruptive scope (impact).

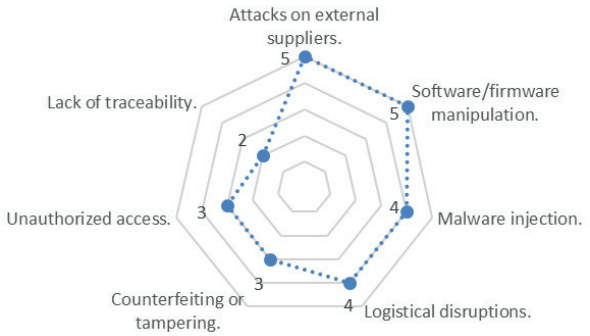

Fig. 8. Risk levels.

IV. DISCUSSION

In the field of information security management in industrial environments, considerable progress has been made in identifying risks and vulnerabilities, as well as in developing technological solutions to mitigate them. However, a significant gap persists in the literature regarding the comprehensive management of information security in industrial environments, since most research focuses on the detection and protection against specific vulnerabilities, leaving aside a holistic approach that includes not only technology, but also operational processes and the human factor.

In addition, the interconnection of devices and rapid technological advancement present critical challenges for industries, especially in terms of information security. However, although many studies agree on the importance of addressing these challenges, they often do not delve into the specific factors and behaviors that can increase the risk of information loss, so this omission can lead to a biased and less effective approach when implementing protection measures.

Consequently, we seek to answer the questions raised:

Q1: Which information security models and/or methodologies are most suitable for industrial environments?

Five models designed specifically for the protection of industrial information were identified, which provide various strategies and tools focused on the prevention and detection of threats. However, they have an important limitation: none of them addresses data management in a comprehensive and systematic manner; this means that there is no well-defined and structured process that fully guarantees the confidentiality, integrity and availability of information. In other words, although these models are useful for certain aspects of security, they lack a holistic approach that covers all the elements necessary for effective data management. This leaves a significant gap in the protection of industrial information, as it is not ensured that all data is protected in a consistent and continuous manner.

The models proposed by [19] [20] focus primarily on strategies for the prevention of cyber-attacks, providing a robust framework for defense against digital threats. However, these models are significantly lacking in two critical areas: physical data protection and guidelines on human behavior in security contexts; and the models [21] [22] [23] have common limitations in implementation, as the lack of real data to adjust the models can affect their effectiveness in practice.

Q2: What factors contribute to the vulnerability of industrial control systems (ICS)?

Industrial control systems (ICS) are vulnerable due to several factors, including connectivity and networks, which increase exposure to external attacks; outdated and unpatched operating systems, which leave known vulnerabilities open; unauthorized physical access, incorrect or inadequate system configurations, and poor maintenance practices can compromise security; cyber-attacks, such as malware and ransomware; and the human factor, including errors and lack of training, are also significant risks.

However, there are additional factors that have not been considered within the reviewed literature, but are equally important, such as the convergence of operational and information technologies (OT and IT) increases the attack surface, as vulnerabilities in IT systems can be exploited to access OT systems; the lack of monitoring and early detection of intrusions allows threats to go unnoticed until they cause significant damage; Furthermore, the absence of robust security procedures for managing updates can introduce new vulnerabilities, making ICS particularly attractive targets for attackers.

Q3: What are the biggest cybersecurity risks in the industrial supply chain?

After reviewing the literature, it was identified that a successful cyberattack, ransomware attacks and industrial espionage are the risks that cause the greatest impact on the industrial supply chain, since successful cyberattacks can disrupt production, cause significant financial losses and compromise the safety of employees and the public; in addition, they can result in the loss of intellectual property and sensitive data. On the other hand, ransomware attacks can paralyze operations by encrypting critical data and demanding a ransom for its release, generating high costs not only for the ransom, but also for data recovery and the implementation of additional security measures. Similarly, industrial espionage involves the theft of trade secrets and intellectual property, which can give competitors an unfair advantage, resulting in market losses and decreased competitiveness.

However, there are other risks that should also be considered but are not being mentioned in the literature, such as denial of service (DoS) attacks that can disrupt access to critical services, affecting the company's ability to operate and communicate with suppliers and customers; internal sabotage, carried out by disgruntled or infiltrated employees, can cause significant damage from within, whether by manipulating systems, stealing information or sabotaging operations; and supply chain failures due to logistical problems, natural disasters and other unforeseen events can cause delays and financial losses.

V. CONCLUSIONS

The selected articles reveal that interoperability and heterogeneous systems are the main challenges for industries, as most operate with legacy technologies that were not developed under strict cybersecurity protocols; this is compounded by the inherent complexity of industrial infrastructures, especially because many of them operate with devices that use obsolete systems, which are difficult to protect; the extensive and distributed nature of industrial networks complicates the visibility and effective control of all connected devices and systems.

Moreover, in the industrial sector, information security is compromised not only by the lack of specialized personnel but also by the inadequate use of technologies by employees, which creates an environment vulnerable to cyberattacks. The significant resistance of workers to adopting new technologies and protection policies also becomes relevant, which is rooted in organizational culture, and this also affects security challenges.

On the other hand, the analysis carried out in this study shows that cyber threats targeting industrial control systems (ICS) significantly complicate existing challenges, as these systems, which are essential to critical infrastructure, are increasingly interconnected with IT networks, thus increasing the attack surface, which could lead to serious disruptions, physical damage, and security risks.

With regard to the limitations of this study, it should be noted that there is fragmented literature on information security management in the industrial sector, as many of the studies analyzed focus exclusively on technical aspects, which hinders the creation of holistic solutions. There is also a lack of comprehensive empirical studies exploring the impact of security in different industries, which limits the ability to generalize the findings globally. In addition, there is a scarcity of detailed studies on how to effectively address human error in the context of industrial cybersecurity.

Looking ahead, it is essential that studies in this field be expanded to integrate multidisciplinary approaches; that is, research must move toward the creation of adaptive risk management models that not only focus on current threats but also anticipate future attack vectors. It is also crucial to develop methodologies that specifically address the limitations of legacy systems and the growing interconnectivity between IT and OT. New international standards and regulations should also be explored to improve collaboration between industrial sectors and governments, with the aim of strengthening security throughout the supply chain. These perspectives could lay the foundations for a more resilient industrial environment that is better prepared to face emerging cyber threats.

REFERENCES

[1] C. A. Silva-Giraldo, Y. M. Rueda-Mahecha, and A. M. Moreno-Suarez, "La innovación en las MIPYMES por medio de redes colaborativas y el uso de las TIC," *TECHNO REVIEW. International Technology, Science and Society Review Revista Internacional de Tecnología, Ciencia y Sociedad,* vol. 14, no. 1, pp. 1–13, Feb. 2023. https://doi.org/10.37467/REVTECHNO.V14.4822.

[2] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustainability (Switzerland)*, vol. 15, no. 7, Apr. 2023. https://doi.org/10.3390/SU15075828.

[3] M. Pontoan, J. Sihotang, and E. Lompoliu, "Information Security Analysis of Online Education Management System using Information Technology Infrastructure Library Version 3," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 22, no. 2, pp. 207–216, Mar. 2023. https://doi.org/10.30812/MATRIK.V22I2.2474.

[4] D. Tin. R. Hata, F. Granholm, R. G. Ciottone, R. Staynings, and G. R. Ciottone, "Cyberthreats: A primer for healthcare professionals," *American Journal of Emergency Medicine*, vol. 68, pp. 179–185, Jun. 2023. https://doi.org/10.1016/J.AJEM.2023.04.001.

[5] B. Coutinho, J. Ferreira, I. Yevseyeva, and V. Basto-Fernandes, "Integrated cybersecurity methodology and supporting tools for healthcare operational information systems," *Comput Secur*, vol. 129, Jun. 2023. https://doi.org/10.1016/J.COSE.2023.103189.

[6] Kaspersky, "La negligencia de los empleados es ahora tan preocupante para las empresas como las filtraciones de datos por ciberataques," América Latina, Mar. 21, 2023. Accessed: Jun. 13, 2023. [Online]. Available: https://latam.kaspersky.com/about/press-releases/2023_la-negligencia-de-los-empleados-es-ahora-tan-preocupante-para-las-empresas-como-las-filtraciones-de-datos-por-ciberataques

[7] N. Ogbuke, Y. Yusuf, K. Dharma, and B. Mercangoz, "Big data supply chain analytics: ethical, privacy and security challenges posed to business industries and society," *Production Planning & Control*, vol. 33, no. 2-3, pp. 1–16, 2022. https://doi.org/10.1080/09537287.2020.1810764.

[8] D. Afenu, M. Asiri, and N. Saxena, "Industrial Control Systems Security Validation Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework," *Electronics (Switzerland)*, vol. 13, no. 5, pp. 1–18, Mar. 2024. https://doi.org/10.3390/electronics13050917.

[9] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales," *International Journal of Information Management Data Insights*, vol. 3, no. 2, p. 100191, Nov. 2023. https://doi.org/10.1016/J.JJIMEI.2023.100191.

[10] M. Figueredo, F. Martins, and B. Stiller, "A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises," *Gestão e Projetos*, vol. 13, no. 3, pp. 10–37, 2022. https://doi.org/10.5585/gep.v13i3.23083.

[11] M. Asiri, N. Saxena, R. Gjomemo, and P. Burnap, "Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 2, p. 15, Apr. 2023. https://doi.org/10.1145/3587255.

[12] B. von, M. Raschke, and F. Teuteberg, "Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach," *Geneva Papers on Risk and Insurance: Issues and Practice*, vol. 48, no. 2, pp. 463–501, Apr. 2023. https://doi.org/10.1057/s41288-023-00293-x.

[13] Ö. Aslan, S. Aktuğ, M. Ozkan-Okay, A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics (Basel)*, vol. 12, no. 6, pp. 1–42, Mar. 2023. https://doi.org/10.3390/ELECTRONICS12061333.

[14] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186–202, Jan. 2024. https://doi.org/10.1016/j.iotcps.2023.12.001.

[15] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems," *IEEE Trans Industr Inform*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021. https://doi.org/10.1109/TII.2020.3023430.

[16] A. Quispe, V. Hinojosa-Ticona, H. Miranda, and C. Sedano, "Serie de Redacción Científica: Revisiones Sistemáticas," *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*, vol. 14, no. 1, pp. 94–99, Mar. 2021. https://doi.org/10.35434/RCMHNAAA.2021.141.906.

[17] J. Sánchez-Meca, "Revisiones sistemáticas y meta-análisis en Educación: un tutorial," *RiiTE Revista Interuniversitaria de Investigación en Tecnología Educativa*, pp. 5–40, Dec. 2022. https://doi.org/10.6018/RIITE.545451.

[18] A. Corallo, A. Crespino, V. Vecchio, M. Lazoi, and M. Marra, "Understanding and Defining Dark Data for the Manufacturing Industry," *IEEE Trans Eng Manag*, vol. 70, no. 2, pp. 1–13, Feb. 2021. https://doi.org/10.1109/TEM.2021.3051981.

[19] M. Jbair, B. Ahmad, C. Maple, and R. Harrison, "Threat modelling for industrial cyber physical systems in the era of smart manufacturing," *Comput Ind*, vol. 137, pp. 1–14, May 2022. https://doi.org/10.1016/J.COMPIND.2022.103611.

[20] S. Bahadoripour, H. Karimipour, A. Jahromi, and A. Islam, "An explainable multi-modal model for advanced cyber- attack detection in industrial control systems," *Internet of Things*, vol. 25, pp. 1–14, Apr 2024. https://doi.org/10.1016/J.IOT.2024.101092.

[21] P. Biplob and R. Muzaffar, "Zero-Trust Model for Smart Manufacturing Industry," *Applied Sciences*, vol. 13, no. 1, pp. 2–20, Dec. 2023. https://doi.org/10.3390/APP13010221.

[22] I. Khan, M. Keshk, D. Pi. N. Khan, Y. Hossain, and H. Soliman, "Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems," *Ad Hoc Networks*, vol. 134, pp. 1–11, Sep. 2022. https://doi.org/10.1016/J.ADHOC.2022.102930.

[23] N. Tuptuk and S. Hailes, "Identifying vulnerabilities of industrial control systems using evolutionary multiobjective optimisation," *Comput Secur*, vol. 137, p. 103593, Feb. 2024. https://doi.org/10.1016/J.COSE.2023.103593.

[24] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, "Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations," *Sensors 2023, vol. 23, Page 4539*, vol. 23, no. 9, pp. 1–17 May 2023. https://doi.org/10.3390/S23094539.

[25] A. Ayodeji, M. Mohamed, L. Li, A. Di, I. Pierce, and H. Ahmed, "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors," *Progress in Nuclear Energy*, vol. 161, pp. 1–12, Jul. 2023. https://doi.org/10.1016/J.PNUCENE.2023.104738.

[26] A. Corallo, M. Lazoi, M. Leezi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Comput Ind*, vol. 137, p. 1–16, May 2022. https://doi.org/10.1016/J.COMPIND.2022.103614.

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

[28] M. Kravchik and A. Shabtai, "Efficient cyber attack detection in industrial control systems using Lightweight Neural Networks and PCA," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 4, pp. 2179–2197, 2022. https://doi.org/10.1109/TDSC.2021.3050101.

[29] M. Rahman, T. Wuest, and M. Shafae, "Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies," *J Manuf Syst*, vol. 68, pp. 196–208, Jun. 2023. https://doi.org/10.1016/J.JMSY.2023.03.009.

[30] J. Hajda, R. Jakuszewski, and S. Ogonowski, "Security Challenges in Industry 4.0 PLC Systems," *Applied Sciences 2021, Vol. 11, Page 9785*, vol. 11, no. 21, pp. 1–26, Oct. 2021. https://doi.org/10.3390/APP11219785.

[31] M. Nankya, R. Chataut, and R. Akl, "Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies," *Sensors*, vol. 23, no. 21, pp. 1–41, Oct. 2023. https://doi.org/10.3390/S23218840

[32] A. Clim, A. Toma, R. Zota, and R. Constantinescu, "The Need for Cybersecurity in Industrial Revolution and Smart Cities," *Sensors*, vol. 23, no. 1, pp. 1–20, Dec. 2022. https://doi.org/10.3390/S23010120.

[33] V. Pedreira, D. Barros, and P. Pinto, "A Review of attacks, vulnerabilities, and defenses in industry 4.0 with new challenges on data sovereignty ahead," *Sensors 2021, Vol. 21, Page 5189*, vol. 21, no. 15, p. 5189, Jul. 2021. https://doi.org/10.3390/S21155189.

[34] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *Int J Inf Secur*, vol. 21, no. 1, pp. 115–158, Mar. 2021. https://doi.org/10.1007/S10207-021-00545-8.

[35] M. Iaiani, A. Tugnoli, S. Bonvicini, and V. Cozzani, "Analysis of Cybersecurity-related Incidents in the Process Industry," *Reliab Eng Syst Saf*, vol. 209, p. 107485, May 2021. https://doi.org/10.1016/J.RESS.2021.107485.

[36] N. Chowdhury, E. Nystad, K. Reegård, and V. Gkioulos, "Cybersecurity training in Norwegian Critical Infrastructure Companies," *International Journal of Safety and Security Engineering,* vol. 12, no. 3, pp. 299–310, Jun. 2022. https://doi.org/10.18280/IJSSE.120304.

[37] S. Saniuk, D. Caganova, and A. Saniuk, "Knowledge and Skills of Industrial Employees and Managerial Staff for the Industry 4.0 Implementation," *Mobile Networks and Applications,* vol. 28, no. 1, pp. 220–230, Feb. 2023. https://doi.org/10.1007/S11036-021-01788-4/FIGURES/5.

[38] F. García, Í. Donoso, A. Flores, C. Pon, V. Flores, and R. Martínez-Peláez, "Examining cybersecurity culture in Leon city organizations: Insights from 2022," *Revista chilena de ingeniería*, vol. 32, pp. 1–16, 2024, Accessed: Aug. 04, 2024. [Online]. Available: https://revistas.uta.cl/pdf/3130/revista%20ingeniare%20volumen%2032%20articulo%2011.pdf.

[39] T. Sawik, "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains," *Int J Prod Res*, vol. 60, no. 4, pp. 1–91, Feb. 2022. https://doi.org/10.1080/00207543.2020.1856442.

[40] Y. Qin, Y. Kaixing, C. Zhou, and Y.-C. Tian, "Association Analysis-Based Cybersecurity Risk Assessment for Industrial Control Systems," *IEEE Syst J*, vol. 15, no. 1, pp. 1423–1432, Mar. 2021. https://doi.org/10.1109/JSYST.2020.3010977.

[41] L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, Cyber Threats, and Standars Landscape: Evaluation and Roadmap," *Sensors 2021, Vol. 21, Page 3901*, vol. 21, no. 11, pp. 1–30, Jun. 2021. https://doi.org/10.3390/S21113901.

[42] M. Gazzan and Frederick Sheldon, "Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems," *Future Internet 2023, Vol. 15, Page 144*, vol. 15, no. 4, pp. 1–18, Apr. 2023. https://doi.org/10.3390/FI15040144.

[43] P. Phillips and G. Pohl, "Industrial espionage: window of opportunity," *Information Security Journal: A Global Perspective*, pp. 1–14, Jul. 2024. https://doi.org/10.1080/19393555.2024.2378755.

[44] R.-C. Härting, L. Bühler, K. Winter, and A. Gugel, "The threat of industrial espionage for SME in the age of digitalization," *Procedia Comput Sci*, vol. 207, pp. 2940–2949, Jan. 2022. https://doi.org/10.1016/J.PROCS.2022.09.352.

[45] M. Ibiyemi and D. Olutimehin, "Cybersecurity in supply chains: Addressing emerging threats with strategic measures," *International Journal of Management & Entrepreneurship Research*, vol. 6, no. 6, pp. 2042–2047, Jun. 2024. https://doi.org/10.51594/IJMER.V6I6.1241.