Computers & Security 150 (2025) 104295

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0

Nourhan Halawi Ghoson [a,b,*], Vincent Meyrueis [a], Khaled Benfriha [a], Thomas Guiltat [c], Stéphane Loubère [b]

[a] Arts et Métiers – Science et technologie, 151, Boulvard de l'Hopital, Paris, France
[b] PricewaterhouseCoopers, 63, Rue de Villiers, 92200 Neuilly-sur-Seine, France
[c] PricewaterhouseCoopers, 3, Cour du Midi, 69287 Lyon CEDEX 02, France

ARTICLE INFO

Keywords:
OT cybersecurity
Industry 4.0
Risk assessment
Dynamic risk assessment

ABSTRACT

The inherent vulnerabilities of Operational Technology (OT) systems to cyberattacks have historically been mitigated through the practice of air-gapping, effectively isolating them from broader industrial networks and thereby maintaining a level of security. However, the beginning of the fourth industrial revolution (Industry 4.0) signs a concept shift towards increased interconnectivity, enhanced visibility, and digital continuity. The transition towards Industry 4.0 has been characterized by a marked increase in security breaches within industrial settings, leading to a variety of hazardous outcomes. These incidents underscore the importance of cybersecurity within OT environments, necessitating the development and implementation of strict cybersecurity measures to safeguard against potential threats. In response to this emerging threat landscape, there has been a notable shift from static risk assessment methodologies towards more dynamic approaches, particularly with the incorporation of Artificial Intelligence (AI) technologies. This paper presents a comprehensive literature review that explores various risk assessment approaches within the context of Industry 4.0, focusing on industrial systems. It outlines the transition from traditional, static risk assessment methods to innovative, dynamic risk assessment strategies facilitated by the integration of AI.

1. Introduction

Industry 4.0, characterized by its integration of nine core technologies, has been fundamentally shaped by the Industrial Internet of Things (IIoT) (Vaidya et al., 2018). This development introduced numerous innovative concepts and technologies to the manufacturing sector. Key among these advancements is the interconnectedness facilitated by machine-to-machine and machine-to-control system communications, enabling direct and remote interactions. Moreover, the advent of cloud computing has been pivotal, as it provides the necessary infrastructure for handling and analyzing massive amounts of data, essential in today's industrial operations. These technological advancements, while raising operational capabilities, also expose the sector to various cyber threats, making cybersecurity a critical pillar of Industry 4.0 (Mohamed, 2018).

The concept of cybersecurity began to gather significant attention in the late 1970s, coinciding with the emergence of the commercial antivirus industry in the 1980s (Warner, 2012). As the importance of Information Technology (IT) infrastructure grew, the significance of cybersecurity expanded into the industrial sector, particularly within Operational Technology (OT) infrastructure. This shift has been further catalyzed by the beginning of the Industry 4.0 framework, which led to a greater number of systems becoming interconnected and accessible online—a transformation driven by the convergence of IT and OT (Kamal et al., 2016). This convergence is a foundation of Industry 4.0, seamlessly integrating digital technologies into manufacturing and industrial processes. The importance of cybersecurity in this context was highlighted by the creation of the first industrial cybersecurity standard, IEC 62443, in 2007 (Gordon). Furthermore, the 2010 Stuxnet attack on an Iranian nuclear facility, which targeted a Supervisory Control and Data Acquisition (SCADA) system and significantly impacted its operational technology, underscored the critical need for robust cybersecurity measures in OT systems. This incident played a crucial role in enhancing the focus on OT cybersecurity (Farwell and Rohozinski, 2011).

IT is the technological backbone of any organization, encompassing computer data storage, data flow, and networking infrastructure. It facilitates the processes used for information management and processing.

* Corresponding author.
E-mail address: Nourhan.halawi_ghoson@ensam.eu (N. Halawi Ghoson).

https://doi.org/10.1016/j.cose.2024.104295
Received 16 September 2024; Received in revised form 19 November 2024; Accepted 18 December 2024
Available online 21 December 2024
0167-4048/© 2024 Elsevier Ltd. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

Typically utilized in business activities, IT is managed by dedicated IT departments that oversee the development, implementation, and maintenance of systems to ensure efficient business operations. This critical function supports a wide range of organizational needs, from communication and data management to strategic decision making (What is Information).

OT systems primarily consist of hardware and software designed to detect or effect change by directly monitoring and controlling industrial equipment, assets, processes, and events. These systems are crucial in managing the physical operations within various industries, enabling real-time oversight and intervention to ensure optimal performance and safety. OT is integral to the infrastructure of manufacturing, energy, transportation, and other sectors where physical processes need to be precisely controlled and monitored (What is operational technology).

When comparing these definitions, it's clear that IT systems are crafted to support data-centric operations, focusing on data management, processing, and the infrastructure that facilitates business activities. In contrast, OT systems are vital in industrial environments, where they manage and control physical operations. This distinction underlines the different objectives and environments each technology is tailored for, emphasizing IT's role in data and communication management, and OT's critical function in direct control of industrial processes and equipment (Paes et al., 2020).

In terms of security it makes sense to apply some of the solutions to what was discovered—after what was known by the IT/OT convergence—into practice because cybersecurity for IT systems was discovered far earlier than cybersecurity for OT systems (Kamal et al., 2016). This led to unique challenges due to their differing nature in terms of design and functionality, that makes it difficult to do apply the same security. To put it in simple terms, OT systems prioritize:

1. Availability
2. Integrity
3. Confidentiality

whereas IT systems prioritize

1. Integrity
2. Confidentiality
3. Availability

This has made the problem of cybersecurity in OT systems extremely difficult to solve (Conklin, 2016).

Prior to the transformative phase of the industrial revolution, IT and OT systems functioned separately due to their distinct objectives and operational frameworks. However, the onset of Industry 4.0 marked a standard shift in this traditional configuration, raising an extraordinary era of connectivity and integration. This evolution was significantly propelled by the adoption of sophisticated architectural frameworks such as ISA-95 (Unver, 2013) which delineated the integration of enterprise and control systems. Moreover, the advent of microservice architectures (Pontarolli et al., 2023) further catalyzed this integration, offering modular and scalable solutions to enhance system interoperability and agility (Santos et al., 2023).

The convergence of IT and OT systems under modern architectural paradigms has exposed a multitude of previously unrecognized cyber vulnerabilities and threats, due to the historically isolated nature of these systems. Resulting increase in complexity and interconnectedness significantly expanded the attack surface, offering malicious actor's new opportunities to exploit these integrated systems. This situation has been further worsened by an increase in the sophistication of hacking techniques, posing significant challenges to the security of both standalone and interconnected systems. In response to these emerging threats, there has been a marked increase in research efforts by both academic and industrial communities. Promoting for robust and innovative cybersecurity solutions tailored to protect the complex interplay of IT and OT systems within the Industry 4.0 framework (Santos et al., 2023).

This review article delivers a comprehensive examination of past research, methods, and standards used in OT cybersecurity risk assessment. Section 2 outlines the research motivation and objectives, while Section 3 details the research methodology. Section 4 includes a theoretical analysis of the various methodologies available for risk assessment. In Section 5, the article presents dynamic risk assessment, followed by a discussion on Artificial Intelligence (AI) and risk assessment in Section 6. Section 7 covers the research findings and discussions, with limitations provided in Section 8. Future work is laid out in Section 9, and the conclusion is offered in Section 10.

2. Research motivation and objectives

The initiation of effective cybersecurity measures begins with a comprehensive "risk assessment," an analytical process aimed at identifying and evaluating the potential hazards inherent within an organizational infrastructure. This initial step is pivotal in understanding the security landscape of an enterprise (King et al., 2018). There has been a significant volume of scholarly work dedicated to examining various platforms and proposing a countless standard. These standards are primarily devised to guide industrial organizations regarding achieving enhanced security for their systems and underlying infrastructures.

This research paper is based on a systematic literature review methodology, with the goal of a complete investigating and defining the numerous methodologies associated with both static and dynamic risk assessments. It further explores the standards developed based on these risk assessments and the spectrum of risks they aim to mitigate. Such a detailed inquiry is crucial for grasping the full spectrum of cybersecurity implications prompted by the convergence of Information Technology (IT) and Operational Technology (OT) within the increasingly digital and networked industrial landscape.

As the research delves into the incorporation of IT and OT systems, particularly in cases where outdated technologies are upgraded and networked, it becomes apparent that the significance of this integration should not be underestimated by corporate leadership. This convergence exceeds critical infrastructures to involve industrial facilities, positioning them as vulnerable targets in the face of geopolitical conflict, economic challenge, and acts of terrorism. The consequences of attacks on OT systems are frequently more severe than those affecting IT systems alone, potentially leading to catastrophic outcomes such as the destruction of production line, the unpredictable behavior of robots, and extensive power outages affecting massive areas. Such incidents emphasize the critical importance of understanding the risks outlined by the methodologies discussed (PricewaterhouseCoopers).

Therefore, the primary objective of this research is to provide a comprehensive overview of risk analysis processes relevant to OT systems. This groundwork is essential before addressing the specific hazards posed by potential cyberattacks. Our research raises a crucial question aimed at separating and understanding the desired outcomes in the subsequent sections of the study. This will lay the foundation for developing reinforced cybersecurity strategies, tailored to protect OT systems against a diverse array of threats.

3. Research methodology

The research conducted in this review follows the systematic literature review approach which is a thorough and organized method for compiling, assessing, and summarizing previous studies and publications on a particular subject or research question (Rother, 2007).

3.1. Systematic literature review

Systematic literature review is a precise and structured approach to synthesizing research on a specific topic, ensuring a comprehensive and unbiased assessment of existing studies. This method involves clearly

defining a set of research questions and establishing criteria for selecting relevant literature. Researchers systematically search databases and sources to gather pertinent academic papers, reports, and other scholarly articles, followed by a meticulous screening process to include only those studies that meet the predefined inclusion criteria. The data from these sources are then extracted, evaluated, and compared to identify patterns, trends, and gaps in the research (Kethavath and Kumari, 2024).

The research process focuses on 4 features: the research question, the keywords, the source for literature search, and the criteria of the included articles. These features are presented in Table 1.

Afterwards, the articles are divided into four categories: the key findings, the type of study, and IT/OT classification. The importance of this classification is to show the topic interest in the research field to highlight the gaps found in this research, and to evaluate the articles findings. The classifications are shown in Table 2.

These results demonstrate that the number of publications on cybersecurity in Industry 4.0 are taking interest in the research field. However, the other topics, like risk and security implementation, are limited. The topic of risk assessment is limited concerning the keywords that are used.

3.2. Detailed research and synthesis

As the publication gap centers on risk assessment and security measurement, the focus is now on studying the detailed keywords related to risks and security measures within Industry 4.0. For a more detailed analysis, an alternative approach involves using a tool from the French Institute of Scientific Research (CNRS), known as "BiblioGraph" (de recherche CNRS).

BilioGraph is a project offering for the first time the cartographic exploration of scientific oppositions and alliances present in the academic literature. It is a new method for analyzing controversies and scientific collaborations based on the visual analysis of co-citation networks. It allows the transformation of a corpus of bibliographic records into a scientometric landscape. In other words, it is a visualization taking the form of a network of references and metadata extracted from a corpus of bibliometric records.

To converge the research, the focus is on risk assessment, putting in forefront the following keywords: “cybersecurity” and “risk assessment”. The keywords for “Industry 4.0″ are changed to a more detailed set, like: “Industrial Control Systems (ICS)”, “Industrial Internet of Things (IIoT)”, “Cyber Physical Systems (CPS)”, and “cloud”. With these keywords, another research is launched to find the respective articles. The papers are then classified with the same process of the first study, represented in Table 3.

This second phase of the research illustrates how the number of articles has evolved, enhancing our understanding of the general topic and the solutions provided within each one. Another factor that can influence the number of findings is the manner in which keywords are written, specifically whether they are abbreviated or written in full. In this instance, using complete keywords yielded a broader range of papers.

To distinguish the relationships between these articles, it was necessary to match their references. At this stage, the tool known as BiblioGraph was employed.

The set of references are analyzed through this tool to have a graphical visualization. It is done through extracting the CSV file (Comma Separated Values) from SCOPUS database and then analyze this document through 8 filters that are found in this tool the: references, the sources, the author keywords, the index keywords, authors, affiliation institutions, affiliation countries, and the funders. In our case, the focus is mainly on the index keywords and authors keywords. This process is done on the 4 sets of references that are found through the keywords mentioned in Table 3.

An example of the graphs Fig. 1. is based on the first set of keywords that was found with 266 values as "author keywords" occurring in at least 1 record, 632 values for "index keywords" occurring in at least 1 record and then they connected these new nodes to the references co-appearing with them in the bibliographic records. By extracting the 2432 references present in this corpus and keeping the references cited by at least 6 records, they built the co-citation network of these references weighted by the frequency of their co-occurrence (aka bibliographic coupling). Then, they removed the nodes with no connection at all. The network is specialized in the ForceAtlas2 layout and fixed the position of the reference-nodes at equilibrium.

Table 1
Research features.

Research question	“How are risks are identified and treated in an industrial platform?”
First keyword set	“Cybersecurity” + “Industry 4.0″ “Risks” + “Cybersecurity” + “Industry 4.0″ “Risk assessment” + “Cybersecurity” + “Industry 4.0″ “Security implementations” + “Industry 4.0″
Source for literature Search	Scopus
Included articles	Language: English Search within: Keywords

Table 2
Classification of keywords IT/OT.

Keywords	Key findings	Type of study	IT/OT
“Cybersecurity” + “Industry 4.0″	285 documents	137 Conference paper 110 Article 20 Review 16 Book chapter 2 Book	IT: 109 OT: 130 Other: 46
“Risks” + “Cybersecurity” + “Industry 4.0″	42 documents	31 Conference paper 9 Article 1 Book chapter 1 Review	IT: 15 OT: 20 Other: 7
“Risk assessment” + “Cybersecurity” + “Industry 4.0″	29 documents	23 Conference paper 6 Article	IT: 11 OT: 13 Other: 5
“Security implementations” + “Industry 4.0″	23 documents	15 Conference paper 7 Article 1 Review	IT: 6 OT: 12 Other: 5

Table 3
Classification of references based on keywords.

Keywords	Key findings	Type of the study
“Cybersecurity” + “Risk assessment” + “industrial control systems”	72 documents	40 Conference paper 32 Article
“Cybersecurity” + “Risk assessment” + “industrial internet of things”	21 documents	12 Conference paper 8 Article 1 Review
“Cybersecurity” + “Risk assessment” + “Cyber physical systems”	119 documents	64 Conference paper 52 Article
“Cybersecurity” + “Risk assessment” + “cloud”	39 documents	32 Conference paper 5 Article 1 Conference review 1 Review

4. Theoretical framework analysis of the research

The objective of this research is to explore methodologies used for risk assessment. Following this process, the study provided clearer insights regarding the keywords used and the references found. According to the results depicted in the graph (Fig. 1.), it is evident that some criteria not previously considered emerge through these graphs. The

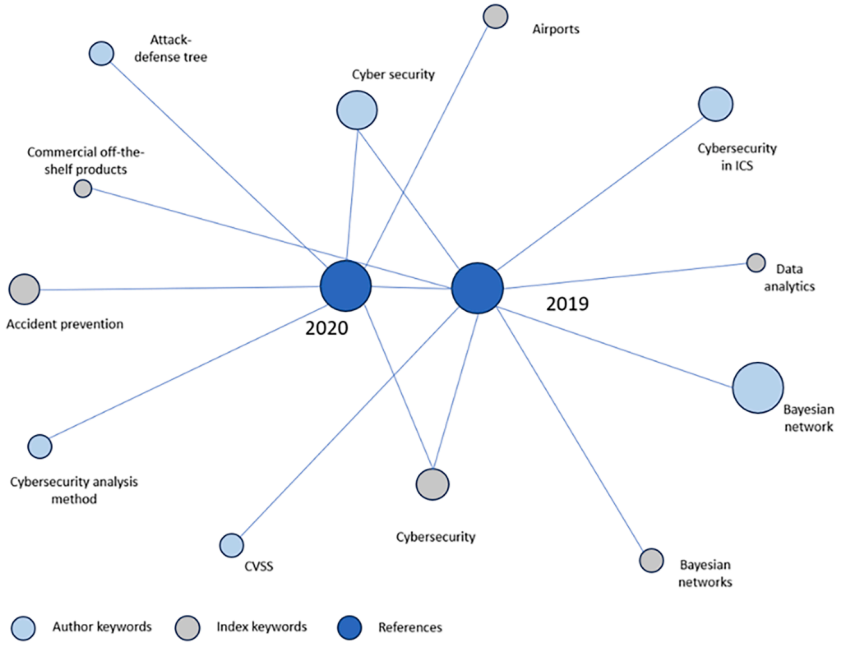

Fig. 1. BiblioGraph tool reference visualization based on keywords.

representation of terms, such as "cybersecurity," which can be written as one word or two, influences the findings. Additionally, variations in word form, such as singular or plural, can affect the number of references identified, depending on the specific keywords used in the research criteria.

After collecting the articles deemed relevant to our case, we found that the total number fitting our research or answering the research question was considerably less than those identified by keywords alone. This is because some articles mentioned "cyber physical systems" and "cloud" within industrial platforms but did not focus on these systems in this specific context, leading to their exclusion. Additionally, certain articles were reviews covering the same subject, causing repetition of concepts. As a result, some of these were also excluded, concluding our study with 70 articles.

Another important criterion identified in this study is that the solutions provided can be categorized as either "qualitative" or "quantitative." Where qualitative solutions mainly focus on:

- The attack: by conducting a threat modeling session to understand how a hacker might target an organization.
- The system: by performing a security audit of a system to identify vulnerabilities like unpatched software, weak passwords, or inadequate firewall settings.
- The organization: by analyzing the impact of a data breach on an organization's reputation.

While the quantitative solutions focus on

- The likelihood: by using historical data to calculate the probability of a cyber-attack on a company's network.
- The consequences: by estimating the financial impact of a system downtime due to a cyber-attack.

By comparing these two set solutions, lately the quantitative solutions have attracted increasing attention, as they provide more accurate reflection of the system status (Qin et al., 2021).

Additionally, there are two other approaches that can be considered for risk assessment, that are not so considered in the case of cybersecurity risk assessment, which include (Vidalis, 2024):

- Knowledge-Based Approach: This approach involves leveraging established best practices from related systems. Historically widespread in the early years of computing, when the scale of system assets and their vulnerabilities were manageable manually, this method relies heavily on accrued expertise and proven strategies.
- Model-Based Approach: This strategy employs object-oriented modeling to describe and analyze risks. By using a structured framework, it systematically addresses the complexities of system vulnerabilities, facilitating a more comprehensive risk assessment process.

After the analysis we did and the help of the bibliograph tool it appears different methods that can be followed to analyze risks:

- Bayesian networks: are probabilistic graphical models that represent a set of variables and their conditional dependencies via a directed acyclic graph. They are used in risk analysis to model complex systems and to reason under uncertainty. Bayesian networks can combine expert knowledge and data to provide a comprehensive understanding of risk factors and their interactions (Żebrowski et al., 2022).
- CVSS (Common Vulnerability Scoring System): is a standardized framework for rating the severity of software vulnerabilities. CVSS scores provide a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity, which can be used to prioritize response efforts (Scarfone and Mell, 2009).
- Attack defense tree: is a variant of threat modeling tools used to conceptualize the pathways through which a system can be attacked. They are like fault trees but include the potential for active defenses. This method is used for analyzing the security of systems and networks and for identifying potential vulnerabilities (Kordy et al., 2014).
- Accident prevention: refers to the systematic approach to identifying and preventing circumstances that could lead to accidents, typically in a workplace or operational environment (Christian et al., 2009).
- Data analysis: involves the systematic application of statistical and logical techniques to describe, summarize, and compare data. This

method is crucial for identifying trends, patterns, and anomalies in large datasets, which can be indicative of potential risks (Cox, 2008).
- Attack graph: are a method of representing all possible attack paths through a system. They are used to understand how multiple vulnerabilities can be chained together to compromise a system and to prioritize which vulnerabilities to address first (Phillips and Swiler, 1998).

A key focus in cybersecurity risk assessment is ensuring safety. Some studies have explored this through the Multidisciplinary Early Design Risk Assessment Framework (MEDRAF) (Papakonstantinou et al., 2021). This framework conducts early, combined assessments of safety and security risks by utilizing interdisciplinary dependency models of a system. It primarily aims to estimate the probabilities of successful attacks on system components and to compute the overall safety-security risk by employing hybrid safety-security trees.

Before delving into the solutions presented for "industrial control systems" (ICS) and "cyber-physical systems" (CPS), it's important to note that their solutions are often integrated. This integration stems from the definitions of each term: Industrial Control Systems (ICS) are a specific category within Operational Technology (OT) systems, primarily focused on managing and controlling industrial processes. In contrast, Cyber-Physical Systems (CPS) encompass a broader range of systems that integrate physical operations with cyber elements, covering a wider array of applications.

4.1. Methodologies for Industrial Control System (ICS) and Cyber-Physical Systems (CPS)

Gao et al. (2014) present the security effect of the Supervisory Control and Data Acquisition (SCADA) layer and the different communication protocols.

SCADA and Distributed Control Systems (DCS) are under increasing and previously unanticipated cybersecurity danger because of the rising dependence on key infrastructures like interconnected physical and cyber-based control systems (DCSs) (Henrie, 2013). For that there are probability risk analysis that are applied to some SCADA systems which are the Fault Tree analysis (FTA) (Veeramany et al., 2019) and Event Tree Analysis (ETA) (Ralston et al., 2007).

Another study identifies these vulnerabilities. This study offers a method for detecting cyber-physical vulnerabilities and assessing their possible impact in intelligent manufacturing systems. The suggested method makes use of intersection mapping to find manufacturing's cyber-physical weaknesses. The manufacturer is then given a spotlight scale between low, medium, and high degrees of cyber-physical vulnerabilities for each production process via a cyber-physical vulnerability impact study utilizing decision trees. The spotlight scale enables producers to understand assessment results (DeSmit et al., 2017).

As the vulnerabilities increase the risks of cybersecurity increases and for that there have been different studies on how to identify risks, but techniques for designing Cyber-Physical Systems (CPS) security are either to approach the cyber and physical systems separately or to not address the vulnerabilities of real-time embedded controllers and networks used to monitor and control physical processes.

The integrated model-based approach for CPS security risk assessment, studied by Model-based risk assessment for cyber physical systems security (2020), makes use of a CPS testbed that has real-world industrial controllers and communication protocols. An exothermic Continuous Stirred Tank Reactor (CSTR) is monitored and managed by the testbed in real-time simulation.

Another methodology studies the risks by simulating the conflict between the attacker and the system as a game. This strategy applies the game theory approach and attempts to determine the likelihood of the attacker's activity (Zarreh et al., 2019).

Using the Association Network (AN) which determines the likelihood of security events. By mining the data of past attack records, the parameters of the AN are determined. To measure the cybersecurity risk of the system, an association matrix between the system state variables and the important security variables is derived from a distance correlation analysis of the target system's process data (Qin et al., 2021).

4.2. Methodologies for Industrial Internet of Things (IIoT)

IIoT (Industrial Internet of Things) systems, being distinct from traditional OT (Operational Technology) systems, present challenges in implementing solutions like IDS (Intrusion Detection Systems). IDS, designed to monitor network and system behavior, faces complexities in IIoT integration. To address this, researchers are exploring the use of Fog/edge computing, Machine Learning (ML) (Neshenko et al., 2024), and deep learning to facilitate effective and adaptable IDS deployment (Ünözkan et al., 2022). Additionally, other studies focus on developing unique methodologies. Some adopt an attack tree-based approach using graph theory (Arat and Akleylek, 2023), while others adapt tools for identifying CVSS (Common Vulnerability Scoring System), primarily used in IT environments, to suit industrial settings (Figueroa-Lorenzo et al., 2020).

Another important aspect, while studying the risk assessment of the IIoT systems, is to take into consideration the node interpretability, decentralization, real-time data relay, modularity, and required service alignment (Tariq et al., 2022).

Other studies focused on the OCTAVE allegro to define a new methodology to identify risks. OCTAVE allegro is a variation that offers an information asset-focused, simplified method. All of the OCTAVE approaches have wide applicability, so prospects can choose the one that suits their specific information security risk assessment requirements (Zahran et al., 2021).

4.3. Methodologies for cloud

Various techniques of abstraction are employed in public cloud computing architectures. A series of events involving cloud customer instantiations indicate that either customers' required security duties are not fully grasped, or the security concerns are difficult to understand (Bird, 2018).

The primary conclusions concern the dangers involved in sending data from a ship to a cloud server. The methodology is predicated on examining the likelihoods of cyberattacks, transpiring in relation to the likelihoods of thwarting these initiatives (Pöyhönen et al., 2022).

Also, some methodologies focused on the important aspects that should be taken into consideration for risk analysis as "Improving the internal control system", "Establishing a risk early warning system and evaluation mechanism" (Ma et al., 2023).

There hasn't been much research on how cloud providers might evaluate their own services, with much recent work concentrating on the risks encountered by businesses choosing or implementing cloud services. For that a literature review is done to compare the different methodologies found and the introduction of the new tool CSCCRA (Akinrolabu et al., 2019) which is a novel quantitative risk assessment model for SaaS (Software as a Service) Cloud Service Providers (Akinrolabu et al., 2019).

5. Dynamic risk assessment

The risks, that are present in systems, are changing based on the third-party service providers, data systems, the introduction of new digital assets, new threat intelligence on known risk, or even zero-day vulnerabilities, that are being exploited. For that having a dynamic risk assessment methodology is a necessity in Industry 4.0 platforms.

For this study, we tried to follow the same research methodology for searching the dynamic risk assessment, resuming it in Table 4. This study is continuously evolving, and new risks are found

For that it was necessary to go deeper into the papers found and the

Table 4
Classification of references based on keywords.

Keywords	Key findings	Type of the study	References
"Cybersecurity" + "Dynamic Risk assessment" + "industrial control systems"	3 documents	2 Article 1 Conference paper	(Ji et al., 2022; Nobili et al., 2023; Zhang et al., 2020)
"Cybersecurity" + "Dynamic Risk assessment" + "industrial internet of things"	No results found	No results found	
"Cybersecurity" + "Dynamic Risk assessment" + "Cyber physical systems"	4 documents	3 Conference paper 1 Article	(Wang et al., 2023; Lyvas et al., 2023; Golabi et al., 2022; Zhu et al., 2018)
"Cybersecurity" + "Dynamic risk assessment" + "cloud"	2 documents	1 article 1 conference	(Zmiewski et al., 2022; Ji et al., 2022)

methodologies that are used for cybersecurity in general. We ended by having a detailed study of the dynamic risk assessment, refer to Table 5. The references are defined by the method used, the year of publication, and the approach followed to have a dynamic risk assessment. These references are mainly for the OT systems, and the IT solutions are removed in this study.

Dynamic risk assessment in OT systems is a critical methodology for identifying, analyzing, and mitigating risks in real-time within industrial environments. This approach emphasizes the need for continuous monitoring and adaptation to emerging threats, considering the unique characteristics and vulnerabilities of OT systems. It moves beyond traditional risk assessment models by integrating live data feeds, threat intelligence, and the current state of OT environments to provide a more accurate and up-to-the-minute understanding of risk exposures. This dynamic nature allows for the immediate detection of anomalies and potential security breaches, enabling quicker response times and the implementation of proactive measures to protect critical infrastructure (Cheimonidis and Rantos, 2023).

Table 5
Dynamic risk assessment method classification.

Method used	Year	Approach	References
Bayesian networks	2016	attack evidence (IDS)+ anomaly evidence + system's knowledge (vulnerabilities related data included)	(Zhang et al., 2015)
	2017	IDS + vulnerability scanner/CVE+ historical data/experts' opinion	(Huang et al., 2017)
	2018	security Knowledge DB (vulnerabilities related data included) + real-time attack evidence	(Peng et al., 2018)
	2018	attack evidence (IDS) + system's knowledge + control strategies	(Zhu et al., 2018)
	2018	attack evidence (IDS) + anomaly evidence + system's Knowledge	(Zhang et al., 2018)
	2019	IDS	(Zhu et al., 2018)
Attack trees	2013	System's vulnerabilities	(Ji et al., 2016)
	2018	System's knowledge+ vulnerability inventory	(Gonzalez-Granadillo et al., 2018)
Neural networks	2017	big data analysis by experts	(Fu et al., 2017)
Association analysis	2021	IDS+ historical data+ system's knowledge	(Qin et al., 2021)
Mathematical model methods	2018	Experts' evaluation	(Tweneboah-Koduah and Buchanan, 2018)
	2019	Assets + threats events	(Vega-Barbas et al., 2019)
	2022	system's knowledge+ abnormal events	(Vaddia)
	2023	Attackers'/defenders' strategies + CVSS	(Yan et al., 2023)

5.1. Machine learning methods

Machine learning, a crucial surface of artificial intelligence, empowers systems to learn autonomously from data, recognize complex patterns, and make informed decisions with minimal human intervention. This technology significantly enhances dynamic risk assessment capabilities by enabling real-time analysis and prediction of potential threats (Yussuf et al., 2024).

Machine learning methods for risk assessment can be broadly classified into two categories: supervised learning and unsupervised learning.

5.1.1. Supervised learning

In supervised learning, the model is trained on labeled data, where each input is paired with the correct output. The model learns by comparing its predictions with the actual labels and adjusting its parameters to minimize the differences. This approach is commonly used for classification and regression tasks, such as determining whether an email is spam (Nasteski, 2017).

Classification methods:

- Support Vector Machines (SVM): A method that finds the hyperplane which best separates different classes in the data.
- Discriminant Analysis: A statistical technique used to classify a set of observations into predefined classes.
- Naïve Bayes: A probabilistic classifier based on applying Bayes' theorem with strong independence assumptions between features.
- Nearest Neighbor: A simple algorithm that classifies a sample based on the majority class of its nearest neighbors.

Regression methods:

- Linear Regression, GLM (Generalized Linear Models): Techniques that model the relationship between a dependent variable and one or more independent variables by fitting a linear equation.
- Support Vector Regression (SVR), Support Vector Regression (SVR): Extension of SVM for regression tasks, which tries to fit the data within a margin of tolerance.
- Ensemble Methods: Techniques that combine the predictions of multiple models to improve accuracy.
- Decision Trees: Models that use a tree-like graph of decisions and their possible consequences to make predictions.
- Neural Networks: Models inspired by the human brain that consist of interconnected layers of nodes, capable of learning and making complex predictions.

5.1.2. Unsupervised learning

Unsupervised learning involves training a model on unlabeled data, meaning the system must identify patterns and relationships without explicit guidance. This type of learning is often used for clustering and association tasks, such as grouping similar network activities together to identify potential anomalies (Naeem et al., 2023).

Clustering methods:

- K-means, K-medoids, Fuzzy C-means: Algorithms that partition data into clusters based on similarity, with K-means using the mean, K-medoids using the median, and Fuzzy C-means allowing data points to belong to multiple clusters.

- Hierarchical Clustering: A method that builds a hierarchy of clusters by either merging smaller clusters or splitting larger ones.
- Gaussian Mixture Models: Probabilistic models that assume the data is generated from a mixture of several Gaussian distributions.
- Neural Networks: Used in this context to discover intricate patterns in the data without predefined labels.
- Hidden Markov Model (HMM): A statistical model that represents systems with hidden states, commonly used for time-series data.

5.2. Case studies and methods used

Case Study: Darktrace's Use of Machine Learning for Threat Detection (Katiyar et al., 2024)

Overview: Darktrace is a leading cybersecurity company that uses machine learning (ML) to detect threats. Their Enterprise Immune System is a notable example of ML in cybersecurity.

Implementation: Darktrace employs unsupervised learning algorithms to establish normal behavior patterns for every device and user within an organization. By analyzing network traffic and user activities, the system identifies deviations from these patterns as potential threats.

Success Story: Darktrace's system identified an insider threat at a large financial institution. An employee began downloading large volumes of sensitive data after receiving a job offer from a competitor. The system flagged this behavior, allowing the organization to investigate and prevent data exfiltration.

Several major firms have successfully implemented AI-driven risk assessment tools in their audit processes. KPMG developed a tool using natural language processing and machine learning to analyze financial data, which helped auditors identify and prioritize high-risk areas more efficiently. Deloitte's AI-based fraud detection system analyzes transactional data, enabling real-time identification and mitigation of fraudulent activities. PwC tackled data quality issues in AI-driven risk assessment by implementing data cleansing and validation processes, resulting in more accurate risk assessments. EY addressed transparency and bias challenges through explainable AI techniques and bias mitigation strategies, ensuring fairness and understanding in their AI models (Onwubuariri et al., 2024).

These case studies highlight the significant impact of AI on improving audit planning and execution.

In summary, to achieve a dynamic and effective risk assessment, several methods can be employed. Anomaly detection can be carried out by continuously monitoring system logs and metrics to identify any unusual activities that may indicate potential security threats. Additionally, behavior patterns can be monitored using User and Entity Behavior Analytics (UEBA), which helps in understanding and detecting deviations from typical user and system behavior. Another essential method is predictive analytics, which utilizes historical, structured data to forecast potential risks and vulnerabilities. This approach helps in identifying patterns and trends that could lead to future security incidents, allowing for proactive measures to be put in place.

5.3. The role of AI in leveraging risk assessment

AI in OT cybersecurity represents a transformative approach to managing risks and enhancing the security of critical infrastructure systems, such as those used in manufacturing, energy production, and transportation. By leveraging artificial intelligence, cybersecurity frameworks can rapidly analyze vast amounts of data from sensors and machines to detect anomalies that may indicate potential security threats. AI algorithms are particularly adept at learning normal network behavior, enabling them to identify deviations that human analysts might miss. This capability is crucial for OT environments where any disruption can have significant consequences, ranging from economic losses to threats to human safety (M et al., 2023).

AI algorithms are adept at analyzing vast amounts of data generated by OT devices to detect anomalies that could signify potential security breaches or system failures. These algorithms leverage machine learning models to learn from historical data, enabling them to recognize patterns of normal behavior and flag deviations that might indicate malicious activities or operational issues. By integrating AI, cybersecurity systems can automate the detection process, reduce response times, and handle the complexity of modern OT environments, where traditional security measures often fall short (Rizvi, 2023).

5.4. Limitations of AI

However, integrating AI into OT cybersecurity also presents specific risks that must be carefully managed. limitations that pose challenges to the effective implementation of AI in cybersecurity, especially in critical sectors. Adversarial attacks, where threat actors intentionally craft inputs to deceive AI systems, are a significant concern. These attacks can subtly alter data in ways that are difficult for AI models to detect, potentially compromising the security measures in place (Olafuyi, 2023).

Data quality is another crucial limitation, as AI systems require high-quality, comprehensive datasets to function accurately. Incomplete or biased data can lead to misinformed decisions or overlooked vulnerabilities. Additionally, the opacity of AI algorithms, often referred to as the "black box" problem, complicates the understanding and trust in AI decisions. This lack of transparency can hinder accountability and complicate the regulatory compliance ((PDF) Developing an AI-Enabled).

AI systems must also be adaptable to continuously evolving threats. Cyber threats are dynamic, with attackers constantly devising new strategies. AI models that cannot learn and adapt to new threats quickly become obsolete. Moreover, the complexity of integrating AI into existing cybersecurity architectures without disrupting operational processes poses a substantial challenge (Iyer and Umadevi, 2023).

The deployment of AI might also induce a false sense of security among users and administrators. Over-reliance on automated systems can lead to negligence in maintaining and updating other critical security practices. Additionally, AI requires significant computational and human resources, not only for initial deployment but also for ongoing operations, including monitoring AI performance and intervening when necessary (Rizvi, 2023).

False positives and false negatives are prevalent issues where AI incorrectly identifies threats or fails to detect actual ones. These inaccuracies can waste resources or leave systems vulnerable. Lastly, ethical concerns arise regarding privacy, surveillance, and decision-making, particularly about how data is used and who is responsible for AI-driven actions. Addressing these limitations requires a balanced approach that considers both technological enhancements and the broader implications of AI in cybersecurity (Rajendran and Vyas, 2023).

6. Discussion

The literature highlights the importance of incorporating dynamic risk assessment strategies to address the evolving cybersecurity landscape facing OT systems. For instance, studies have shown that dynamic risk assessment frameworks can significantly enhance the resilience of OT systems against sophisticated cyber-attacks. These frameworks leverage advanced analytics, machine learning algorithms, and simulation techniques to predict potential attack vectors and assess the impact of hypothetical security incidents. By doing so, they help organizations prioritize security investments and develop more effective incident response strategies tailored to the specific needs of their OT environments.

There having presented the outcomes and various solutions proposed by the research articles, it's crucial to acknowledge that OT systems are making significant advancements in this domain, particularly regarding risk assessments. Risk assessments are increasingly recognized as a fundamental tool for analyzing systems, determining their status, and

assessing the security maturity level of each system.

The important thing to mention is the presence of different standards that provide different methodologies and best practices for industrial companies to follow some standards:

- NIST SP800-82 (Stouffer et al., 2023): this publication is specifically tailored to protect Industrial Control and Monitoring Systems (ICS). It offers a comprehensive range of security measures, best practices, and recommendations. NIST SP 800-82 delves into several critical topics related to ICS security, including risk management. It provides guidance on identifying and mitigating ICS-specific risks, encompassing areas such as threat analysis and vulnerability management (Jillepalli et al., 2017).
- IEC 62443 (ISA/IEC 62443): this standard primarily focuses on ensuring both operational safety and security of industrial systems. It outlines a series of guidelines and safeguards that should be adhered to. Notably, IEC 62443 includes a detailed risk assessment methodology, specifically outlined in chapter 62443-3-2, offering an in-depth approach to evaluating and managing risks in industrial settings (Hassani et al., 2021).
- NIS 2 (Directive NIS 2) As an update to the 2016 Network and Information Systems (NIS) Directive, the NIS 2 Directive was adopted by EU member states in January 2023. This directive emerged as a response to several high-profile and damaging cyberattacks. It introduces stricter security measures, streamlines reporting processes, and establishes more stringent oversight and enforcement protocols. The directive's aim is to enhance the overall cybersecurity posture across EU member states (Schmitz-Berndt and Chiara, 2022).

Another feature that can be mentioned after this study is that the methodologies provided by these articles can be classified into static and dynamic risk assessment and this is due to different criteria. Static risk assessment is the study of risks based on specific knowledge of the systems and the system cannot adapt to new risks (Bhuiyan et al., 2019). While dynamic risk analysis is basically the system's ability to smoothly transition from one state to another by maintaining synchronization in the event of an interruption is the primary concern of dynamic risk-based security assessment (Villa et al., 2016).

7. Research limitation

This research encountered various limitations, one being the efficacy of keyword-based searches. While such searches can be effective, as seen in the initial phase of our study on risk assessment where the CNRS tool (de recherche CNRS) helped identify solutions for industrial system risk assessment, they are not always reliable. For instance, when shifting focus to dynamic risk assessment, the keyword approach was less successful in locating relevant articles. This highlights that the usefulness of keyword searches is highly dependent on the specific topic and the availability of related research.

This study encounters a significant limitation stemming from the paucity of literature specifically addressing dynamic risk assessment within Operational Technology (OT) systems. This scarcity underscores a critical research gap, primarily due to the persistent vulnerabilities and loads of uncertain risks that continue to plague the industry. As a result, there exists an obvious emphasis on static risk assessment methodologies, overshadowing the potential and necessity for dynamic approaches. Moreover, the adoption of dynamic risk assessment strategies in OT systems introduces its own set of challenges and risks, necessitating a focused investigation into these areas. Therefore, our future research activities will be dedicated to exploring the complexities and distinctions of dynamic risk assessments, including the identification of inherent risks and the elucidation of the benefits such methodologies can offer to enhance the security posture of OT systems.

Furthermore, this study sheds light on the limitations presents within existing methodologies aimed at securing systems in industrial environments. One such limitation is the usual contradiction between quantitative and qualitative risk assessment methods. This division often results in a fragmented approach that fails to capture the complex nature of cybersecurity risks. To bridge this gap, there is an urgent need for an integrative methodology that promotes a symbiotic relationship between quantitative and qualitative assessments. By pursuing a holistic strategy that combines these two dimensions, industries can more effectively navigate the complexities of adopting emerging technologies and achieving IT/OT convergence. It is imperative to recognize cybersecurity not merely as a defensive mechanism but as a strategic asset that enhances the operational efficiency and competitive edge of businesses within the industrial domain. Moving forward, our research will aim to develop such comprehensive solutions, thereby contributing to the advancement of cybersecurity practices in the context of Industry 4.0

8. Implication for future work

The concept of 'Security by Design' is paramount in the contemporary cybersecurity landscape, advocating for the incorporation of security considerations at the earliest stages of system design and development. This proactive approach seeks to identify and mitigate vulnerabilities from the outset, integrating security principles into the very fabric of each system. By prioritizing security during the initial design phase, it allows for a comprehensive assessment of potential threats, ensuring that security measures are not merely an afterthought but a foundational component of the system's architecture. This method extends beyond the technical specifications of individual systems to include the broader context of their physical deployment and the intricate network of interconnections among various systems, aiming for a holistic security posture that is embedded in the system's design from inception.

Advancing this concept necessitates a risk assessment process that carefully examines all factors capable of exposing a system to cyberattacks. To address this challenge effectively, our future methodology proposes a systematic classification of risks into four foundational pillars, providing a structured framework for vulnerability identification, risk analysis, and the implementation of specific security measures. This categorization facilitates the development of targeted strategies to bolster system defenses against cyber threats, establishing a comprehensive and resilient security infrastructure. The adoption of such a framework is instrumental in transitioning towards dynamic risk assessment, where the emphasis is on adaptive and responsive security strategies. The four pillars of risk can be delineated as follows:

- People: This pillar underscores the dual role of individuals within an organization - both as potential security vulnerabilities and as critical assets in safeguarding the system. It emphasizes the importance of having a well-informed and vigilant user base, alongside a team of skilled security professionals equipped with the necessary resources to identify and counteract threats. Educating and training all users on cybersecurity best practices is crucial in creating a security-conscious culture.
- Process: This aspect focuses on the establishment of robust strategies and architectures that facilitate the efficient prevention, detection, and response to cyber incidents. It involves a comprehensive review of existing systems, frameworks, and protocols to ensure that they are equipped to proactively address potential threats and swiftly mitigate any security breaches that may occur.
- Technology: Often the most discussed component, technology encompasses a wide array of tools and solutions designed to protect critical assets, infrastructure, and personnel. The key is to leverage technology not in isolation but as part of an integrated security approach that complements and enhances the other pillars of the framework.
- Suppliers: Recognizing that the security of a system extends beyond its immediate environment, this pillar considers the role of third-

party suppliers and partners. It highlights the need for rigorous security assessments and controls for external entities that interact with or impact the system, acknowledging that the supply chain can introduce additional risks that must be managed effectively.

By elaborating and enhancing these pillars, we aim to create a dynamic and flexible risk assessment framework that not only addresses current security challenges but is also adaptable to the evolving cyber threat landscape. This holistic approach to cybersecurity, grounded in the principles of Security by Design, is fundamental in building inherently secure and resilient industrial systems capable of withstanding the sophisticated threats of the digital age.

9. Conclusion

The integration of advanced technologies into industrial operations has guided in a new era of complexity and potential vulnerability in cybersecurity. Adopting a proactive cybersecurity posture offers significant long-term benefits, enabling industries to advance in technological innovation while protecting against threats that could lead to financial losses, operational disruptions, or risks to human and environmental safety. This strategic approach not only encourages defenses against immediate cyber threats but also builds a resilient framework capable of adapting to evolving risks.

A proactive cybersecurity strategy emphasizes the importance of continuous monitoring, regular updates, and comprehensive training programs. By staying ahead of potential threats, industries can reduce the likelihood of successful cyber-attacks, minimize downtime, and protect sensitive data. This approach adopts a culture of vigilance and preparedness, empowering organizations to instantly respond to incidents and prevent escalation.

As there are significant benefits in adopting AI for dynamic risk assessment and cybersecurity, it is crucial to approach this integration with a comprehensive understanding of the associated risks and limitations. AI technologies can offer enhanced capabilities for identifying and mitigating threats, predicting vulnerabilities, and automating responses to incidents. However, the adoption of AI must be studied in a broader context to avoid potential pitfalls, such as biases in AI algorithms, over-reliance on automated systems, and the complexities of integrating AI with existing cybersecurity frameworks. A balanced approach that leverages the strengths of AI while mitigating its risks will be essential for building secure and resilient industrial systems.

Moreover, expanding research on AI adoption will provide deeper insights into best practices, effective strategies, and innovative solutions for enhancing cybersecurity. By fostering a culture of continuous learning and adaptation, organizations can ensure that their cybersecurity posture remains robust and capable of addressing the evolving threat landscape. This proactive stance will not only protect critical infrastructure but also enable industries to fully harness the potential of emerging technologies, thereby achieving lasting competitive advantages in the digital age.

Embracing a proactive cybersecurity posture and expanding research on AI adoption are crucial steps toward building secure and resilient industrial systems. These efforts will enable industries to employ the full potential of emerging technologies while maintaining robust defenses against sophisticated cyber threats. With strategic foresight and preparedness, organizations can navigate the complexities of the digital age and achieve lasting competitive advantages.

CRediT authorship contribution statement

Nourhan Halawi Ghoson: Writing – original draft. **Vincent Meyrueis:** Writing – review & editing. **Khaled Benfriha:** Writing – review & editing. **Thomas Guiltat:** Writing – review & editing, Conceptualization. **Stéphane Loubère:** Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this review article titled " A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0″ The content is solely the result of academic research and has been conducted impartially, without any external influence or bias.

Appendix

Table 6 provides a summary of the findings discussed in the article.

Table 6
Sum up of the literature findings.

Risk assessment	Key findings	Type of the study
"Cybersecurity" + "Risk assessment" + "industrial control systems"	72 documents	40 Conference paper 32 Article
"Cybersecurity" + "Risk assessment" + "industrial internet of things"	21 documents	12 Conference paper 8 Article 1 Review
"Cybersecurity" + "Risk assessment" + "Cyber physical systems"	119 documents	64 Conference paper 52 Article
"Cybersecurity" + "Risk assessment" + "cloud"	39 documents	32 Conference paper 5 Article 1 Conference review 1 Review
Dynamic risk assessment		
"Cybersecurity" + "Dynamic Risk assessment" + "industrial control systems"	3 documents	2 Article 1 Conference paper
"Cybersecurity" + "Dynamic Risk assessment" + "industrial internet of things"	No results found	No results found
"Cybersecurity" + "Dynamic Risk assessment" + "Cyber physical systems"	4 documents	3 Conference paper 1 Article
"Cybersecurity" + "Dynamic risk assessment" + "cloud"	2 documents	1 article 1 conference
Methods		

Method used	Year	Approach	References
Bayesian networks	2016	attack evidence (IDS)+anomaly evidence + system's knowledge (vulnerabilities related data included)	(Zhang et al., 2015)
	2017	IDS + vulnerability scanner/CVE+ historical data/experts' opinion	(Huang et al., 2017)
	2018	security Knowledge DB (vulnerabilities related data included) + real-time attack evidence	(Peng et al., 2018)
	2018	attack evidence (IDS) + system's knowledge + control strategies	(Zhu et al., 2018)
	2018	attack evidence (IDS) + anomaly evidence + system's Knowledge	(Zhang et al., 2018)
	2019	IDS	(Zhu et al., 2018)
Attack trees	2013	System's vulnerabilities	(Ji et al., 2016)
	2018	System's knowledge+ vulnerability inventory	(Gonzalez-Granadillo et al., 2018)
Neural networks	2017	big data analysis by experts	(Fu et al., 2017)

(*continued on next page*)

Table 6 (*continued*)

Method used	Year	Approach	References
Association analysis	2021	IDS+ historical data+ system's knowledge	(Qin et al., 2021)
Mathematical model methods	2018	Experts' evaluation	(Tweneboah-Koduah and Buchanan, 2018)
	2019	Assets + threats events	(Vega-Barbas et al., 2019)
	2022	system's knowledge+ abnormal events	(Vaddia)
	2023	Attackers'/defenders' strategies + CVSS	(Yan et al., 2023)

Data availability

No data was used for the research described in the article.

References

'What is Information Technology? Definition and Examples', Data Center. Accessed: Dec. 18, 2023. [Online]. Available: https://www.techtarget.com/searchdatacenter/definition/IT.

'What is operational technology (OT)?' Accessed: Dec. 20, 2023. [Online]. Available: https://www.redhat.com/en/topics/edge-computing/what-is-ot.

Model-based risk assessment for cyber physical systems security. Comput. Secur. 96, 2020, 101864. https://doi.org/10.1016/j.cose.2020.101864. Sep.

Akinrolabu, O., New, S., Martin, A., 2019. CSCCRA: a novel quantitative risk assessment model for saas cloud service providers. Computers 8 (3). https://doi.org/10.3390/computers8030066. Art. no. 3Sep.

Akinrolabu, O., Nurse, J.R.C., Martin, A., New, S., 2019. Cyber risk assessment in cloud provider environments: current models and future needs. Comput. Secur. 87, 101600. https://doi.org/10.1016/j.cose.2019.101600. Nov.

Arat, F., Akleylek, S., 2023. Attack path detection for IIoT enabled cyber physical systems: revisited. Comput. Secur. 128. https://doi.org/10.1016/j.cose.2023.103174.

Bhuiyan, M.Z.A., Anders, G.J., Philhower, J., Du, S., 2019. Review of static risk-based security assessment in power system. IET Cyber-Phys. Syst. Theory Appl. 4 (3), 233–239. https://doi.org/10.1049/iet-cps.2018.5080.

Bird, D., 2018. A conceptual framework to identify cyber risks associated with the use of public cloud computing. In: presented at the ACM International Conference Proceeding Series. https://doi.org/10.1145/3264437.3264466.

Cheimonidis, P., Rantos, K., 2023. Dynamic risk assessment in cybersecurity: a systematic literature review. Future Internet 15 (10). https://doi.org/10.3390/fi15100324. Art. no. 10Oct.

Christian, M., Bradley-Geist, J., Wallace, C., Burke, M., 2009. Workplace safety: a meta-analysis of the roles of person and situation factors. J. Appl. Psychol. 94, 1103–1127. https://doi.org/10.1037/a0016172. Sep.

Conklin, Wm.A., 2016. IT vs. OT security: a time to consider a change in CIA to include resilience. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 2642–2647. https://doi.org/10.1109/HICSS.2016.331. Jan.

Cox, L., 2008. What's wrong with risk matrices? Risk Anal. Off. Publ. Soc. Risk Anal. 28, 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x. May.

T.V.C. de recherche CNRS, 'BiblioGraph : un outil et une méthode pour visualiser les paysages scientométriques | CNRS sciences humaines & sociales'. Accessed: Nov. 16, 2023. [Online]. Available: https://www.inshs.cnrs.fr/fr/cnrsinfo/bibliograph-un-outil-et-une-methode-pour-visualiser-les-paysages-scientometriques.

DeSmit, Z., Elhabashy, A.E., Wells, L.J., Camelio, J.A., 2017. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. J. Manuf. Syst. 43, 339–351. https://doi.org/10.1016/j.jmsy.2017.03.004. Apr.

'Directive NIS 2: ce qui va changer pour les entreprises et l'administration françaises | ANSSI'. Accessed: Nov. 15, 2023. [Online]. Available: https://cyber.gouv.fr/directive-nis-2-ce-qui-va-changer-pour-les-entreprises-et-ladministration-francaises.

Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the future of cyber war. Survival 53 (1), 23–40. https://doi.org/10.1080/00396338.2011.555586. Feb.

Figueroa-Lorenzo, S., Añorga, J., Arrizabalaga, S., 2020. A survey of IIoT protocols: a measure of vulnerability risk analysis based on CVSS. ACM Comput. Surv. 53 (2). https://doi.org/10.1145/3381038.

Fu, Y., Zhu, J., Gao, S., 2017. CPS information security risk evaluation system based on petri net. In: 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). IEEE, Shenzhen, China, pp. 541–548. https://doi.org/10.1109/DSC.2017.65. Jun.

Gao, J., et al., 2014. SCADA communication and security issues. Secur. Commun. Netw. 7 (1), 175–194. https://doi.org/10.1002/sec.698.

Golabi, A., Erradi, A., Tantawy, A., 2022. Towards automated hazard analysis for CPS security with application to CSTR system. J. Process Control 115, 100–111. https://doi.org/10.1016/j.jprocont.2022.04.008.

Gonzalez-Granadillo, G., et al., 2018. Dynamic risk management response system to handle cyber threats. Future Gener. Comput. Syst. 83, 535–552. https://doi.org/10.1016/j.future.2017.05.043. Jun.

J. Gordon, 'The Essential Guide to the IEC 62443 industrial cybersecurity standards', Industrial Cyber. Accessed: Nov. 16, 2023. [Online]. Available: https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/.

Hassani, H.L., Bahnasse, A., Martin, E., Roland, C., Bouattane, O., Mehdi Diouri, M.E., 2021. Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443. Procedia Comput. Sci. 191, 33–40. https://doi.org/10.1016/j.procs.2021.07.008. Jan.

Henrie, M., 2013. Cyber security risk management in the SCADA critical infrastructure environment. Eng. Manag. J. 25 (2), 38–45. https://doi.org/10.1080/10429247.2013.11431973. Jun.

Huang, K., Zhou, C., Tian, Y.-C., Tu, W., Peng, Y., 2017. Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. In: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, Melbourne, VIC, pp. 1–6. https://doi.org/10.1109/ATNAC.2017.8215355. Nov.

'ISA/IEC 62443 Series of Standards - ISA', isa.org. Accessed: Jun. 14, 2023. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

A.A. Iyer and K. Umadevi, 'Role of AI and its impact on the development of cyber security applications', 2023, pp. 23–46. doi: 10.1007/978-981-99-2115-7_2.

Ji, X., Wei, H., Chen, Y., Ji, X.-F., Wu, G., 2022. A three-stage dynamic assessment framework for industrial control system security based on a method of W-HMM. Sensors 22 (7). https://doi.org/10.3390/s22072593.

Ji, X., Yu, H., Fan, G., Fu, W., 2016. Attack-defense trees based cyber security analysis for CPSs. In: 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE, Shanghai, China, pp. 693–698. https://doi.org/10.1109/SNPD.2016.7515980. May.

Jillepalli, A.A., Sheldon, F.T., de Leon, D.C., Haney, M., Abercrombie, R.K., 2017. Security management of cyber physical control systems using NIST SP 800-82r2. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1864–1870. https://doi.org/10.1109/IWCMC.2017.7986568. Jun.

Kamal, S.Z., Al Mubarak, S.M., Scodova, B.D., Naik, P., Flichy, P., Coffin, G., 2016. IT and OT Convergence - Opportunities and Challenges. In: presented at the SPE Intelligent Energy International Conference and Exhibition. OnePetro. https://doi.org/10.2118/181087-MS. Sep.

Katiyar, D., Tripathi, M., Kumar, M., Verma, M., Sahu, D., Saxena, D., 2024. AI and cyber-security: enhancing threat detection and response with machine learning. Educ. Adm. Theory Pract. 30. https://doi.org/10.53555/kuey.v30i4.2377. Apr.

N. Kethavath and V. Kumari, 'Systematic techniques for review of literature', 2024, pp. 320–336.

King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B., Sample, C., 2018. Characterizing and measuring maliciousness for cybersecurity risk assessment. Front. Psychol. 9. Accessed: Nov. 16, 2023[Online]Available: https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00039.

Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P., 2014. Attack-defense trees. J. Log. Comput. 24. https://doi.org/10.1093/logcom/exs029. Feb.

Lyvas, C., et al., 2023. A hybrid dynamic risk analysis methodology for cyber-physical systems. Lect. Notes Comput. Sci. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma. 13785, 134–152. https://doi.org/10.1007/978-3-031-25460-4_8. LNCS.

M. M. et al., 'Artificial intelligence in cyber security', 2023, pp. 366–385. doi: 10.4018/978-1-6684-8098-4.ch022.

Ma, J., Zhang, B., Ullah, A., 2023. An analysis of internet financial risk prevention strategies from the perspective of network security. Lect. Notes Data Eng. Commun. Technol. 170, 12–19. https://doi.org/10.1007/978-3-031-29097-8_2.

Mohamed, M., 2018. Challenges and Benefits of Industry 4.0: an overview. Int. J. Supply Oper. Manag. 5, 256–265. https://doi.org/10.22034/2018.3.7. Jul.

Naeem, S., Ali, A., Anam, S., Ahmed, M., 2023. An unsupervised machine learning algorithms: comprehensive review. IJCDS J. 13, 911–921. https://doi.org/10.12785/ijcds/130172. Apr.

Nasteski, V., 2017. An overview of the supervised machine learning methods. Horizons.B 4, 51–62. https://doi.org/10.20544/HORIZONS.B.04.1.17.P05. Dec.

Neshenko, N., Bou-Harb, E., Furht, B., Behara, R., 2024. Machine learning and user interface for cyber risk management of water infrastructure. Risk Anal. 44 (4), 833–849. https://doi.org/10.1111/risa.14209.

Nobili, M., et al., 2023. DRIVERS: a platform for dynamic risk assessment of emergent cyber threats for industrial control systems. In: presented at the 2023 31st Mediterranean Conference on Control and Automation, MED 2023, pp. 395–400. https://doi.org/10.1109/MED59994.2023.10185686.

Olafuyi, B., 2023. Artificial intelligence in cybersecurity: enhancing threat detection and mitigation. Int. J. Sci. Res. Publ. 13, 194–200. https://doi.org/10.29322/IJSRP.13.12.2023.p14419. Dec.

Onwubuariri, E., Adelakun, B., Olaiya, O., Ziorklui, J., 2024. AI-Driven risk assessment: revolutionizing audit planning and execution. Finance Account. Res. J. 6, 1069–1090. https://doi.org/10.51594/farj.v6i6.1236. Jun.

Paes, R., Mazur, D.C., Venne, B.K., Ostrzenski, J., 2020. A guide to securing industrial control networks: integrating IT and OT systems. IEEE Ind. Appl. Mag. 26 (2), 47–53. https://doi.org/10.1109/MIAS.2019.2943630. Mar.

Papakonstantinou, N., Van Bossuyt, D.L., Linnosmaa, J., Hale, B., O'Halloran, B., 2021. A zero trust hybrid security and safety risk analysis method. J. Comput. Inf. Sci. Eng. 21 (050907). https://doi.org/10.1115/1.4050685. May.

'(PDF) Developing an AI-Enabled Cybersecurity solution for proactive patch management and vulnerability assessment: leveraging machine learning algorithms and predictive analytics to enhance threat detection and response'. Accessed: Apr. 26, 2024. [Online]. Available: https://www.researchgate.net/publication/373557548_Developing_an_AI-Enabled_Cybersecurity_Solution_for_Proactive_Patch_Management_and_Vulnerability_Assessment_Leveraging_Machine_Learning_Algorithms_and_Predictive_Analytics_to_Enhance_Threat_Detection_?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoic2VhcmNoIiwicG9zaXRpb24iOiJwYWdlSGVhZGVyIn19.

Peng, Y., Huang, K., Tu, W., Zhou, C., 2018. A model-data integrated cyber security risk assessment method for industrial control systems. In: 2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS). IEEE, Enshi, pp. 344–349. https://doi.org/10.1109/DDCLS.2018.8516022. May.

Phillips, C., Swiler, L.P., 1998. A graph-based system for network-vulnerability analysis. In: *Proceedings of the 1998 workshop on New security paradigms*, in NSPW '98. Association for Computing Machinery, New York, NY, USA, pp. 71–79. https://doi.org/10.1145/310889.310919. Jan.

Pontarolli, R.P., Bigheti, J.A., de Sá, L.B.R., Godoy, E.P., 2023. Microservice-oriented architecture for industry 4.0. Eng 4 (2). https://doi.org/10.3390/eng4020069. Art. no. 2, Jun.

Pöyhönen, J., Hummelholm, A., Lehto, M., 2022. Cybersecurity risk assessment subjects in information flows. In: presented at the European Conference on Information Warfare and Security. ECCWS, pp. 222–230.

PricewaterhouseCoopers, 'Industrial cybersecurity: the elephant on the factory floor', PwC. Accessed: Nov. 17, 2023. [Online]. Available: https://www.pwc.ie/services/consulting/insights/industrial-cybersecurity.html.

Qin, Y., Peng, Y., Huang, K., Zhou, C., Tian, Y.-C., 2021. Association analysis-based cybersecurity risk assessment for industrial control systems. IEEE Syst. J. 15 (1), 1423–1432. https://doi.org/10.1109/JSYST.2020.3010977.

Rajendran, R., Vyas, B., 2023. Cyber security threat and its prevention through artificial intelligence technology. Int. J. Multidiscip. Res. 5, 1–18. Dec.

Ralston, P.A.S., Graham, J.H., Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Trans. 46 (4), 583–594. https://doi.org/10.1016/j.isatra.2007.04.003. Oct.

Rizvi, M., 2023. Enhancing cybersecurity: the power of artificial intelligence in threat detection and prevention. Int. J. Adv. Eng. Res. Sci. 10, 055–060. https://doi.org/10.22161/ijaers.105.8. Jan.

Rizvi, M., 2023. Enhancing cybersecurity: the power of artificial intelligence in threat detection and prevention. Int. J. Adv. Eng. Res. Sci. 10, 055–060. https://doi.org/10.22161/ijaers.105.8. Jan.

Rother, E.T., 2007. Systematic literature review X narrative review. Acta Paul. Enferm. 20. https://doi.org/10.1590/S0103-21002007000200001 pp. v–viJun.

Santos, S., Costa, P., Rocha, A., 2023. IT/OT Convergence in industry 4.0 : risks and analisy of the problems. In: 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6. https://doi.org/10.23919/CISTI58278.2023.10211415. Jun.

Scarfone, K., Mell, P., 2009. An Analysis of CVSS Version 2 Vulnerability Scoring, p. 525. https://doi.org/10.1109/ESEM.2009.5314220.

Schmitz-Berndt, S., Chiara, P.G., 2022. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. Int. Cybersecurity Law Rev. 3 (2), 289–311. https://doi.org/10.1365/s43439-022-00058-7. Dec.

Stouffer, K., et al., 2023. Guide to Operational Technology (OT) security. National Institute of Standards and Technology. NIST Special Publication (SP). https://doi.org/10.6028/NIST.SP.800-82r3, 800-82 RevSep.

Tariq, U., Ahanger, T.A., Ibrahim, A., Bouteraa, Y.S., 2022. The Industrial Internet of Things (IIoT): an anomaly identification and countermeasure method. J. Circuits Syst. Comput. 31 (12). https://doi.org/10.1142/S021812662250219X.

Tweneboah-Koduah, S., Buchanan, W.J., 2018. Security risk assessment of critical infrastructure systems: a comparative study. Comput. J. 61 (9), 1389–1406. https://doi.org/10.1093/comjnl/bxy002. Sep.

Ünözkan, H., Ertem, M., Bendak, S., 2022. Using attack graphs to defend healthcare systems from cyberattacks: a longitudinal empirical study. Netw. Model. Anal. Health Inform. Bioinforma 11 (1). https://doi.org/10.1007/s13721-022-00391-1.

Unver, H.O., 2013. An ISA-95-based manufacturing intelligence system in support of lean initiatives. Int. J. Adv. Manuf. Technol. 65 (5), 853–866. https://doi.org/10.1007/s00170-012-4223-z. Mar.

'Vaddia: Dynamic probabilistic risk assessment for... - Google scholar'. Accessed: Nov. 14, 2023. [Online]. Available: https://scholar.google.com/scholar_lookup?title=Dynamic+Probabilistic+Risk+Assessment+for+Cyber+Security+Risk+Analysis+in+Nuclear+Reactors&conference=Proceedings+of+the+Probabilistic+Safety+Assessment+&+Management+Conference%E2%80%94PSAM+16&author=Vaddi,+P.K.&author=Zhao,+Y.&author=Smidts,+C.&publication_year=2022.

Vaidya, S., Ambad, P., Bhosle, S., 2018. Industry 4.0 – A Glimpse. Procedia Manuf. 20, 233–238. https://doi.org/10.1016/j.promfg.2018.02.034. Jan.

Veeramany, A., Hutton, W.J., Sridhar, S., Gourisetti, S.N.G., Coles, G.A., Skare, P.M., 2019. A framework for development of risk-informed autonomous adaptive cyber controllers. J. Comput. Inf. Sci. Eng. 19 (041004). https://doi.org/10.1115/1.4043040. Jun.

Vega-Barbas, M., Villagrá, V.A., Monje, F., Riesco, R., Larriva-Novo, X., Berrocal, J., 2019. Ontology-based system for dynamic risk management in administrative domains. Appl. Sci. 9 (21). https://doi.org/10.3390/app9214547. Art. no. 21Jan.

S. Vidalis, 'A critical discussion of risk and threat analysis methods and methodologies'. 2024.

Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016. Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. Saf. Sci. 89, 77–93. https://doi.org/10.1016/j.ssci.2016.06.002. Nov.

Wang, Y., Li, Y., Xu, T., Zhu, M., 2023. Cascading failure risk assessment based on event-driven model in a cyber-physical power system. In: presented at the 2023 IEEE International Conference on Power Science and Technology, ICPST 2023, pp. 123–128. https://doi.org/10.1109/ICPST56889.2023.10164915.

Warner, M., 2012. Cybersecurity: a Pre-history. Intell. Natl. Secur. 27 (5), 781–799. https://doi.org/10.1080/02684527.2012.708530. Oct.

Yan, K., Liu, X., Lu, Y., Qin, F., 2023. A cyber-physical power system risk assessment model against cyberattacks. IEEE Syst. J. 17 (2), 2018–2028. https://doi.org/10.1109/JSYST.2022.3215591. Jun.

Yussuf, M., Lamina, A., Mesioye, O., Nwachukwu, G., Aminu, T., 2024. Leveraging machine learning for proactive threat analysis in cybersecurity. Int. J. Comput. Appl. Technol. Res. 13, 53–64. https://doi.org/10.7753/IJCATR1309.1005. Aug.

Zahran, B., Hussaini, A., Ali-Gombe, A., 2021. IIoT-ARAS: IIoT/ICS automated risk assessment system for prediction and prevention. In: presented at the CODASPY 2021 - Proceedings of the 11th ACM Conference on Data and Application Security and Privacy, pp. 305–307. https://doi.org/10.1145/3422337.3450320.

Zarreh, A., Wan, H., Lee, Y., Saygin, C., Janahi, R.A., 2019. Risk assessment for cyber security of manufacturing systems: a game theory approach. Procedia Manuf. 38, 605–612. https://doi.org/10.1016/j.promfg.2020.01.077. Jan.

Żebrowski, P., Couce-Vieira, A., Mancuso, A., 2022. A Bayesian framework for the analysis and optimal mitigation of cyber threats to cyber-physical systems. Risk Anal 42 (10), 2275–2290. https://doi.org/10.1111/risa.13900.

Zhang, F., Hines, J.W., Coble, J.B., 2020. A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. Nucl. Technol. 206 (7), 939–950. https://doi.org/10.1080/00295450.2019.1666599.

Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., Hu, B., 2018. A fuzzy probability bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. IEEE Trans. Ind. Inform. 14 (6), 2497–2506. https://doi.org/10.1109/TII.2017.2768998. Jun.

Zhang, Q., Zhou, C., Xiong, N., Qin, Y., Li, X., Huang, S., 2015. Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. IEEE Trans. Syst. Man Cybern. Syst. 46, 1–16. https://doi.org/10.1109/TSMC.2015.2503399. Jan.

Zhu, Q., Qin, Y., Zhou, C., Gao, W., 2018. Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems. Int. J. Distrib. Sens. Netw. 14 (6), 1550147718779564. https://doi.org/10.1177/1550147718779564. Jun.

Zhu, Q., Zhao, Y., Fei, L., Zhou, C., 2018. A dynamic decision-making approach for cyber-risk reduction in critical infrastructure. In: 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER). IEEE, Tianjin, China, pp. 595–600. https://doi.org/10.1109/CYBER.2018.8688105. Jul.

Zmiewski, S.S., Laufer, J., Mann, Z.Á., 2022. Automatic online quantification and prioritization of data protection risks. In: presented at the ACM International Conference Proceeding Series. https://doi.org/10.1145/3538969.3539005.