CYBER RISK ASSESSMENT FOR CYBER-PHYSICAL SYSTEMS: A REVIEW OF METHODOLOGIES AND RECOMMENDATIONS FOR IMPROVED ASSESSMENT EFFECTIVENESS

Asila AlHarmali[1], Saqib Ali[1], Waqas Aman[1], Omar Hussain[2]

[1]Department of Information Systems, Sultan Qaboos University, Muscat, Oman
[2] School of Business, University of New South Wales, Canberra, Australia

ABSTRACT

Cyber-Physical Systems (CPS) integrate physical and embedded systems with information and communication technology systems, monitoring and controlling physical processes with minimal human intervention. The connection to information and communication technology exposes CPS to cyber risks. It is crucial to assess these risks to manage them effectively. This paper reviews scholarly contributions to cyber risk assessment for CPS, analyzing how the assessment approaches were evaluated and investigating to what extent they meet the requirements of effective risk assessment. We identify gaps limiting the effectiveness of the assessment and recommend real-time learning from cybersecurity incidents. Our review covers twenty-eight papers published between 2014 and 2023, selected based on a three-step search. Our findings show that the reviewed cyber risk assessment methodologies revealed limited effectiveness due to multiple factors. These findings provide a foundation for further research to explore and address other factors impacting the quality of cyber risk assessment in CPS.

KEYWORDS

cyber risk assessment, Cyber-Physical Systems (CPS), real-time learning, cybersecurity incidents, effectiveness of risk assessment

1. INTRODUCTION

Since the late 18th century, humankind has been continuously improving the capabilities of the physical world from mechanization to mass production to digitization and, recently, to the fourth industrial revolution with Cyber-Physical Systems (CPS) and the Internet of Things and Services. CPS integrates cyber and physical processes, creating new capabilities for the physical environment, such as live communication and process monitoring and control. On the other hand, the emergence of computing and communication components brought new security challenges and exposed CPS physical resources to a range of cyber-attacks [1]. Securing CPS against attacks is vital to avoid catastrophic consequences of critical operations being manipulated or halted by attackers [2]. However, securing information and communication technology systems (ICT) in the context of CPS is a complex task [3]. This complexity stems mostly from the nature of CPS applications, which are safety- and mission-critical, with stringent requirements for high

David C. Wyld et al. (Eds): DSCC, AI&FL, SESBC, CSE– 2024
pp. 77-94, 2024. - CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141608

availability and real-time responsiveness [4]. This uptime requirement makes the system sensitive to security updates, reboots, and any security controls' restrictions. Another challenge is the complexity of cyber-physical interactions in a highly interconnected CPS infrastructure, which increases the number of attack points that must be protected [5].

Various security solutions exist for standard IT: the information technology systems consisting of computers and communication networks to process, store, and exchange electronic data. However, these solutions do not apply to CPS system requirements [1]. Various studies have been conducted on developing CPS-specific technical security controls, such as intrusion detection/prevention systems and security information and event management systems [6,7]. Much scholarly work exists on leveraging artificial intelligence (AI) to detect and prevent malicious events and handle monotonous security tasks in a fluctuating CPS environment [8–10]. Despite the capabilities of the existing technical solutions, cybersecurity breaches in CPS are on the rise and show no signs of abating [11–13]. Cyber-attacks have grown in sophistication and complexity, exploiting zero-day vulnerabilities and evading detection [14]. As noticed in [11], cyber-attacks are faced in various CPS sectors, making every OT system a possible target. The motivation of these attackers extends beyond financial gain, with many aiming to harm the public.

Technical security controls alone are insufficient to address the given state of CPS security. A common motto in the security field says that security is 30 percent by technology and 70 percent by management [15]. Therefore, risk management of inevitable cyber-attacks is vital to the organization's cybersecurity program [16]. Risk Assessment is a core function in the risk management process, encompassing the identification, analysis, and evaluation of cyber-attack risks to an organizational operation, assets, individuals, and other organizations [17]. Security risk assessment explains the system security posture and informs related risk management activities and decisions. The more effective an organization can assess the cyber risks, the more rational, effective, and valuable its cybersecurity investments and approach will become [18].

The effectiveness of risk assessment is multifaceted. For instance, effective risk assessment is, in part, determined by validity, how successfully an assessment measures what it is supposed to be measuring [19]. More precisely, valid risk assessment is determined by: (1) how accurate the risk assessment outcomes are compared to the underlying true risk, and (2) the degree to which risk assessment handles uncertainties [20]. Handling uncertainties requires compiling and presenting the missing information, subjective determinations, and assumptions made in the risk assessment process in a way that enables making informed risk management decisions [17]. According to the NIST guide for conducting risk assessment [17], effective risk assessment is also characterized by reliability, the consistency of the risk assessment method, where it can yield the same results when repeated. Reliable risk assessment should be repeatable (repeating the assessment in a manner consistent with prior assessments) and reproducible (producing the same results from the same data across different experts).

Although various cyber risk assessment approaches for CPS have been introduced in previous work, it is unclear how effective they are in assessing cyber risks. A number of available literature review studies present the state-of-the-art cyber risk assessment for CPS, but a detailed evaluation of the effectiveness of the existing approaches was not their primary focus. For example, the systematic literature review study [16] outlines contributions to security risk management in IoT/CPS, including the approaches for the risk assessment step. This study identifies some limitations in the risk identification and analysis techniques but does not analyze them in the context of effective risk assessment requirements.

This paper reviews twenty-eight cyber risk assessment approaches for CPS published in reputable databases between 2014 and 2023. This study seeks to identify the methods the researchers followed to evaluate their proposed cyber risk assessment methodologies and assess the potential effectiveness of the studied risk assessment methods in assessing cyber risks. It also identifies gaps causing limited assessment effectiveness and provides a recommendation of real-time learning from cybersecurity incidents to overcome the most challenging limitations. The rest of this paper is as follows: Section 2 provides essential contextual information on cyber risk assessment for CPS and real-time learning from cybersecurity incidents. We then present the review methodology in section 3. Section 4 provides an analysis of the reviewed risk assessment approaches and answers to the research questions. In Section 5, recommendations to improve cyber risk assessment for CPS are provided. Finally, we conclude the study in section 6.

2. BACKGROUND

2.1. Cyber Risks in Cyber-Physical Systems

Cyber-physical systems represent a paradigm in automation technology, integrating physical and embedded systems with communication and information technology systems [21]. The integration between operational technology (OT) and IT systems creates intelligent systems that can sense, monitor, and control physical processes at anytime from anywhere. However, this integration exposes the OT infrastructures to cyber risks. Cyber risk is the likelihood of a threat actor, cyber attacker, exploiting a vulnerability within a digital system or network and the resulting impact of successful exploitation. Cyber risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and the potential impacts on organizational operations and assets, individuals, other organizations, and the nation [22]. Cyber risks in CPS may include unauthorized access to critical infrastructure, manipulation of control systems, disruption of critical operations, and compromise of sensitive data. The consequences of cyber risks in CPS, if materialized, extend beyond financial gain to encompass the physical world. Cyber risks in the CPS environment can cause catastrophic impacts, such as manipulating or halting critical physical processes, consequentially harming public health and safety [23].

2.2. Risk Assessment

Proactive cyber risk management is vital to the organization's cybersecurity program to prevent the probable risks or reduce their impact to a minimum. Cyber risk assessment is a foundation for informing cybersecurity risk management decisions on preventing cyber risks, mitigating their impact, or effectively handling them when they occur. Risk assessment explains the nature and severity of potential cyber-attacks by answering the question, "What can go wrong?", "What is the likelihood that it would go wrong?", and "What are the consequences if it goes wrong?" [24].

Organizations define a risk assessment methodology that includes a risk assessment process, a risk model, an assessment approach, and an analysis approach [17]. The risk assessment process comprises four steps: preparing for the risk assessment, conducting the assessment, communicating the assessment results, and maintaining the risk assessment over time. The risk assessment is conducted in three tasks: risk identification, analysis, and evaluation. Risk identification is identifying threat sources that could exploit the system vulnerabilities. Risk analysis determines or computes the extent to which an identified threat could harm the system and the likelihood that such events and harm will occur. Risk evaluation rates the system's exposure to risk against the organizational risk tolerance to prioritize risk response.

Due to the highly interconnected CPS infrastructure with complex cyber-physical interactions, the cybersecurity risk assessment methods for general IT systems do not fit the context of CPS [25]. These conventional methods are predominantly static designed to evaluate risks over a set period. CPS requires a cyber risk assessment method capable of assessing the risk at any specific time. A real-time cyber risk assessment that can autonomously learn about the potential cyber risks and adjust to the changing threat landscape and the dynamic nature of the system is crucial for CPS.

2.3. Real-Time Learning from Cybersecurity Incidents

Alongside the proactive security risk management process, organizations employ incident response (IR) to take immediate action to a successful attack to minimize effects and expedite system recovery. IR activities include preparing to handle the incidents, detecting signs of incidents and analyzing them, containing the incident and preventing it from spreading, eradicating the root cause, recovering the system operations, and performing post-incident analyses [26]. In cybersecurity, post-incident analysis leverages the organization's experiences with cyber incidents to guide the organization's cybersecurity management process and future cyber incident response activities.

As for the role of IR activities in the security risk assessment process, Shedden [27] says, “Incident response can be a source of concrete data, reflecting what is happening in the organization. This data can be used to inform the risk assessment process, resulting in much more accurate risk assessments and subsequent strategies”. Ahmad [28] pointed out the shortcoming of not leveraging opportunities for wider learning, such as improving security risk assessment and security policy development, in existing incident response methodologies. This study highlighted that not drawing broad security lessons can result in little prospect of improving the security of information systems. NIST's guide to OT security proposed leveraging post-incident analysis to update risk assessment with the impact level of the experienced incidents [29].

Real-time analysis of cybersecurity incidents allows learning from the incident as it occurs and avoids erosion of knowledge, which can update the cyber risk assessment with up-to-date, representative, and precise information about cyber risks. Machine Learning (ML), a form of artificial intelligence in which computers gain insights from data to make predictions or decisions, can enable real-time learning from cybersecurity incidents to update the risk assessment process. ML is widely used to develop cybersecurity solutions, such as detecting malicious events and preventing attacks before they commence [30]. ML can automatically learn from different cyber threat information sources, adjust to the changing threat landscape, and identify patterns that may not be immediately obvious to human analysts [30,31].

3. RESEARCH METHODS

This study adopted a literature review method to better understand the effectiveness of the existing cyber risk assessment approaches for CPS. The review process started with determining the research question and defining the search string and sources. Inclusion and exclusion criteria were then applied to select twenty-eight relevant studies. The research questions were then answered, and the results were synthesized.

3.1. Research Questions

This study primarily seeks to investigate the effectiveness of the existing cyber risk assessment approaches for CPS. Two questions are formulated to achieve this objective. Each question

addresses a key aspect of the cyber risk assessment methodologies under study. The first question looks for answers on the methods the researchers followed to evaluate their proposed cyber risk assessment methodologies, the evaluation criteria, and the thoroughness of the evaluation process. The second question investigates the extent to which the studied risk assessment methodologies meet the requirements of effective risk assessment. The effectiveness is evaluated by looking for characteristics within each methodology that, as per best practices, lead to effective assessment.

1. How were the reviewed cyber risk assessment methodologies evaluated?
2. What is the potential effectiveness of the studied cyber risk assessment methodologies?

3.2. Literature Search Process

A three-step search process was followed to search for scholarly contributions on cyber risk assessment for CPS. The first search step followed the criteria specified in Table 1. The search keywords were identified through brainstorming and preliminary research. They were expanded with synonyms and refined by testing them on database search queries. The keywords in the search string were searched in the full text of each research paper to avoid missing relevant publications. This initial search resulted in a total of 1329 publications.

Table 1. Search Sources

Sources of Research Paper	**Research Database**	**Initial Paper Count**
	IEEE Xplore	397: articles (106), conference papers (291)
	IEICE	30: articles (30)
	Science Direct	358: articles (358)
	SpringerLink	408: articles (146), conference papers (262)
	MDPI	57: articles (57)
	ACM	79: articles (16), conference papers (63)
Search string keywords	("cybersecurity risk" OR "cyber risk" OR "cyber-to-physical risk") AND (“assessment” OR “analysis” OR “evaluation”) AND ("cyber-physical system" OR "critical infrastructure" OR "SCADA" OR "DSC" OR "industrial control system")	
Search items	Journals’ articles, conference papers	
Search applied on	Full text	
Language	English	
Publication period	2014-2023 October	
Initial paper count	1329	
2nd search paper count	(328): 101 IEEE Xplore, 6 IEICE, 102 Science Direct, 56 SpringerLink, 28 MDPI, 35 ACM	
3rd search paper count	(275): 95 IEEE Xplore, 3 IEICE, 92 Science Direct, 48 SpringerLink, 17 MDPI, 20 ACM	
Papers selected for review	(28): 9 IEEE Xplore, 1 IEICE, 7 Science Direct, 5 SpringerLink, 4 MDPI, 2 ACM	

In the following search step, the abstract of each paper gathered in the initial search was scrutinized based on the inclusion and exclusion criteria presented in Table 2. At the end of this, 1001 of the 1329 papers failed to meet the defined inclusion criteria; hence, they were excluded. In the third search step, some sections in the remaining 328 papers were examined: the sections explaining the proposed approach components and steps and results and evaluation were examined against the level of contribution criteria, depicted in Table 2. After applying this

criterion, 53 studies were filtered out. The 275 papers left were preferenced based on their contribution level. From this preferencing, twenty-eight publications were selected for the review: the top fourteen papers (50%) published in recent years, 2022 and 2023, and the top fourteen (50%) published between 2014 and 2021. This approach was taken to balance the inclusion of the current with foundational research. The papers selected for review are listed in the following section.

Table 2. Inclusion and exclusion criteria

Inclusion Criteria	**Exclusion Criteria**
Second search step	
The central theme: papers that focus primarily on cyber risk assessment	• Papers that examine cybersecurity from more than one aspect, including risk assessment, but the discussion is not dedicated to the risk assessment process. • Papers addressing challenges in the risk management process, but the discussion of the risk assessment phase is limited. • Papers that are not specific about the category of information security on which the risks are assessed.
Relevance: the content is relevant to risk assessment related to the cybersecurity domain in the context of CPS, explicitly concentrating on cyber risks arising from external attacks.	• Articles that address risk assessment on dimensions other than security, such as resilience, privacy, and reliability. • Articles dedicated to risk assessment in security domains other than cybersecurity, such as physical, operational, and personal security. • Articles on assessing cyber risks arising from insider attacks. • Articles that assess the cyber risks of a CPS system under the design phase of the system life cycle.
Third search step	
Level of contribution: papers that add a unique, non-replicated, and sufficiently detailed assessment approach.	• Risk assessment approaches replicating guidelines found in risk assessment standards codified by regulatory bodies. • Papers that do not provide sufficient details about their risk assessment methodology component and steps.

4. RESULTS AND DISCUSSION

This section discusses the review findings of the selected twenty-eight papers, which are listed in Table 3. It answers the two research questions mentioned in 3.1. The first sub-section (4.1) answers how the reviewed risk assessment approaches are evaluated. The second sub-section (4.2) synthesizes results on the extent to which the studied risk methodologies meet the requirements of effective risk assessment.

Table 3. The cyber risk assessment approaches selected for review

S. No	**Study title & Reference**	**Publication Type**	**Publication Year**
1	Security-Oriented Cyber-Physical Risk Assessment for Cyberattacks on Distribution System [32]	Journal article	2023
2	Risk Assessments in Virtual Power Plants with NESCOR Criteria, Practical Application, Advantages and Disadvantages [33]	Journal article	2023

3	Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework [34]	Journal article	2023
4	Dependency-based security risk assessment for cyber-physical systems [35]	Journal article	2023
5	Development of the framework for quantitative cyber risk assessment in nuclear facilities [36]	Journal article	2023
6	Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach [37]	Journal article	2023
7	A Study of The Risk Quantification Method of Cyber-Physical Systems focusing on Direct-Access Attacks to In-vehicle networks [38]	Journal article	2023
8	A Quantitative Risk Assessment Model for Distribution Cyber Physical System under Cyber Attack [39]	Journal article	2023
9	Cyber security risk assessment in autonomous shipping [40]	Journal article	2022
10	Threat modelling for industrial cyber physical systems in the era of smart manufacturing [41]	Journal article	2022
11	An Integrated cyber security risk management framework and risk predication for the critical infrastructure protection [42]	Journal article	2022
12	A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure [43]	Journal article	2022
13	Managing cybersecurity risks of cyber-physical systems: The MARISMA CPS pattern [44]	Journal article	2022
14	Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs [45]	Conference Paper	2022
15	Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in consideration of digitalized ship [46]	Journal article	2021
16	Harmonizing safety and security risk analysis and prevention in cyber-physical systems [47]	Journal article	2021
17	Cyber security risk assessment for seaports: A case study of a container port [48]	Journal article	2021
18	Model-based risk assessment for cyber physical systems security [49]	Journal article	2020
19	Bayesian Network Based C2P Risk Assessment for Cyber-Physical Systems [50]	Journal article	2020
20	Quantitative Risk Modelling and Analysis for Large-Scale Cyber-Physical Systems [51]	Conference Paper	2020
21	MaCRA: a model-based framework for maritime cyber-risk assessment [52]	Journal article	2019
22	Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach [53]	Journal article	2019
23	Risk Assessment for Cyber Attacks in Feeder Automation System [54]	Conference Paper	2018
24	Security risk assessment framework for smart car using the attack tree analysis [55]	Journal article	2018
25	Network Topology Risk Assessment of Stealthy Cyber Attacks on Advanced Metering Infrastructure Networks [56]	Conference Paper	2017
26	Attack-Defence Trees based cyber security analysis for CPS [57]	Conference Paper	2016
27	Risk assessment framework for power control systems with PMU-based intrusion response system [58]	Journal article	2015
28	Cyber-related Risk Assessment and Critical Asset Identification in Power Grids [59]	Conference Paper	2014

4.1. Evaluation Methods of the Studied Cyber Risk Assessment Approaches

The reviewed cyber risk assessment approaches were demonstrated either through theoretical case studies of a CPS system subjected to cyber-attack scenarios or by applying them to real-world CPS systems. As in Figure 1, 89% of the risk assessment methodologies were demonstrated through case studies, and 11% were applied to real-world CPS systems. The case studies were informed by different sources of cyber-attacks. For example, fifteen case studies were inspired by practical demonstrations of cyber-attacks on a CPS system through simulations or experimental testbeds. The remaining ten were not based on any empirical setting but were informed by the authors' knowledge of CPS system security.

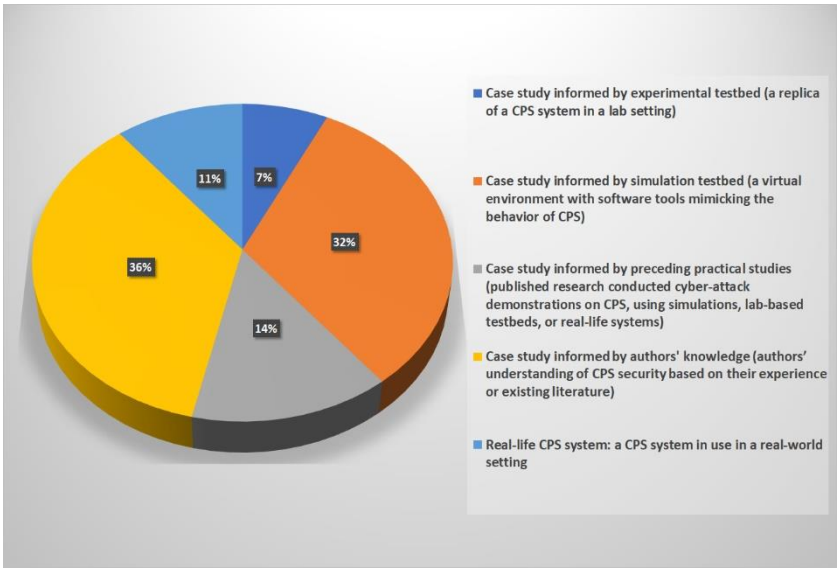

Figure 1. Demonstration methods and settings of the reviewed risk assessment methodologies

While informed by realistic sources of cyber-attacks encountered in CPS, case studies nonetheless do not reflect the actual complexity of a real-world CPS. For example, the case studies drawn from experimental and simulated testbeds are narrowed to a single or few most representative attack scenarios, often failing to reflect the constantly changing cyber threat landscape. Additionally, the case studies developed from the authors' knowledge might overlook the practical aspects of the CPS system and are susceptible to the authors' subjective interpretations and heuristics. Given these limitations, the thoroughness of the evaluation process based on case studies requires further examination.

In the three risk assessment approaches demonstrated in real-world settings [42,44,48], the CPS systems were accessed only once for the proactive risk assessment. They were not revisited for feedback on the effectiveness of the risk assessment method after the identified risks materialized. For a rigorous evaluation of a risk assessment methodology, comparing the proactive risk assessment results to the reactive assessment conducted after the identified risks materialize is required. Revaluation validates whether the proactive risk assessment effectively identified and assessed the risks encountered. Additionally, independent security experts or

system owners' analyses is needed to evaluate further and validate the risk assessment methodologies.

As explained in Section 1, multiple criteria indicate an effective risk assessment, including validity (determined by the degree of risk assessment results accuracy and handling uncertainties), reliability (determined by repeatability and reproducibility). Compared to these criteria, no methodology among the analyzed papers was found to be thoroughly evaluated for effectiveness. The evaluations in the reviewed studies predominantly focused on the applicability of the proposed approaches by showcasing their capabilities in performing the intended functionalities. The studied risk assessment approaches were not evaluated in terms of pivotal criteria that directly impact risk management decisions, like the validity and reliability. Validity and reliability indicate how correctly and consistently the risk assessment method understand and express risk [20]. The validity of the risk assessment in producing risk assessment results with an acceptable extent of accuracy plays a significant role in better prioritizing and managing the most significant risks. Inaccurate assessment creates a flawed picture of the organization's security posture, leading to inappropriate risk management decisions [60]. A subsequent result of inappropriate risk management decisions is a reduced organization's capability to respond to cyber risks; prevent them, mitigate their impact, or effectively handle them when they materialize.

Given the limitations in how the studied cyber risk assessment approaches were evaluated for effectiveness, demonstrating cyber risk assessment methodologies in a live CPS is needed for gaining confidence in the method's applicability to real-world settings. Equally important is engaging independent experts or system owners in evaluating the risk assessment method. Their feedback enables a realistic evaluation that reflects the system's intricacies and practical challenges and isolates biases. The effectiveness of a risk assessment methodology should be thoroughly evaluated across multiple criteria.

4.2. The Potential Effectiveness of the Studied Cyber Risk Assessment Methodologies

As discussed in Section 4.1, validity and reliability are pivotal criteria in determining the effectiveness of risk assessment. These criteria influence decision-makers' confidence in the risk assessment results when making risk management decisions. The literature has limited attention to the sub-criteria or the requirements for validity and reliability of the risk assessment. In the studies where these criteria are mentioned, there is limited specification about the features of the risk assessment method that indicate reliable and valid assessments. The review study [61] considered the source of data the risk assessment techniques rely on to rate their reliability, specifically repeatability, for the nuclear industry. The NIST guide for risk assessment mentioned that the age of information used in assessing risk is a particular concern when evaluating the validity of assessment results [17]. NIST also stated that the precision of the risk assessment is affected by the subjectivity, trustworthiness of the data drawn upon, and the interpretation of assessment results. Cherdantseva [62] described the essence of risk assessment methods in terms of aim, risk factors measurement, sources of data, and tool support.

Based on these theoretical views, for a risk assessment to be an effective, it is required to meet these key requirements: well-definition of the risk model, trustworthiness of the cyber threat intelligence on which it relies, consistency of cyber threat intelligence interpretations, and automation support. This following sub-sections investigate the potential effectiveness of the studied methodologies by examining how they align with these key factors.

4.2.1. Well-Definition of the Risk Model

The Risk model is a component of the risk assessment methodology that describes the risk determination process. It defines assessable risk factors and their relationships in a formula or a matrix. Risk factors are inputs to determining the overall risk value or level in risk assessments. Typical risk factors include threat, vulnerability, impact, and likelihood. Risk factors are usually decomposed into characteristics to gauge their values (e.g., impact is decomposed into impact on cyber and physical systems). Well-definition of the risk model prior to conducting risk assessments could have a significant effect on the effectiveness of the assessment results.

The risk models in the reviewed risk assessment methodologies revealed limitations that could impact the validity and reliability of the overall risk determination. First, using non-inclusive attributes to gauge the risk factors like impact and likelihood, the prevalent metrics in the literature, leads to imprecise assessment. For instance, some approaches assessed the impact of potential cyber-attack risk on either a cyber or a physical system layer but not both [46,51,57,58]. Similarly, in some approaches, the likelihood of a potential cyber-attack occurring was interpreted as the likelihood of successfully exploiting a vulnerability [57,58]. In a real attack scenario, successful vulnerability exploitation does not always result in a successful attack or impact on the system. Another gap is the determination of the overall risk based on only one factor, which could result in underestimating the cyber threats, like in [47,51,52,56]. Some approaches might produce overestimated risk values because they do not take into account the role of the defender's countermeasures in mitigating the system's exposure to risks [45,58].

4.2.2. Trustworthiness of Cyber Threat Intelligence

The trustworthiness of cyber threat information on which the risk assessment relies for identifying threats and gauging risk factors values affects the validity of the assessment results. Up-to-date and relevant threat intelligence contributes to correctly representing the cyber risks the organization is exposed to.

In 50% of the approaches studied, risk assessment was based on a single source of cyber threat information, as presented in Figure 2. Specifically, risk determination in six methodologies drew upon the demonstration of cyber-attack scenarios. The assessment in three methodologies utilized public security databases or reports. In five approaches, the assessment was informed by the judgment of security experts, the system owners, or the authors' estimation. The other 50% of the surveyed approaches combined multiple sources to identify and estimate cyber risks. For instance, real-world CPS system historical cyber-attack information appeared in three approaches, complemented by other sources such as public security databases or the judgments of security experts.

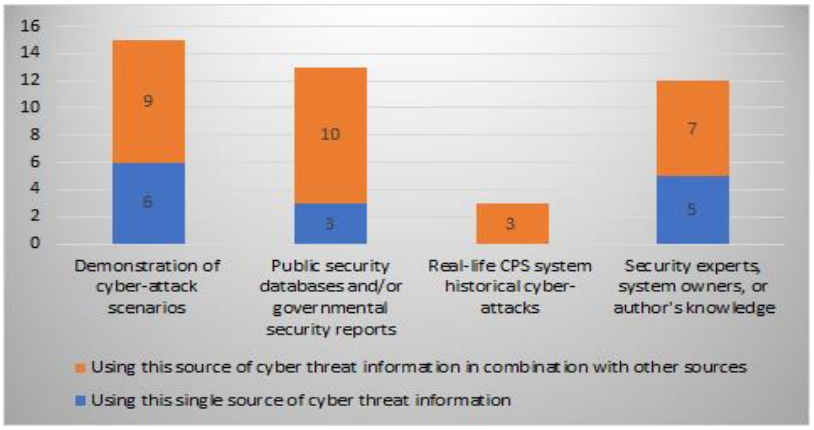

Figure 2. Cyber threat intelligence sources on which the studied risk assessment methodologies relied

Although these diverse cyber threat intelligence sources form a broader view of the cyber threat landscape, they possess limitations that diminish the assessment capacity to assess potential cyber risks correctly, as shown in Table 4. For instance, the cyber-threat information published in public security databases or governmental reports does not reflect the organization's unique experience. Public cyber threat intelligence can become outdated due to the evolving threat landscape, leading to an inaccurate representation of the risks to which the organization is exposed. Given the significant underreporting of OT incidents and a lack of scientifically verified data on cyber-physical attacks [43], such datasets are unreliable.

A demonstration of cyber-attack scenarios in a simulated or experimental testbed does not reflect the complexity of a real-world CPS system and the risks to which it is exposed. It is challenging for the threat event parameters in the attack scenario to keep up with the constantly changing threat landscape [37]. In the case of insufficient knowledge about threat characteristics, the authors either omitted them in their attack scenarios or relied on subjective assumptions. The scenario approach is further narrowed when researchers describe potential threats into a single or few most representative scenarios.

The past cyber-attacks experienced by a real-world CPS system do not correctly assess a potential cyber risk because the factors that led to attacks in the past are changing. The historical cyberattacks-based approach lacks real-time learning of a changing threat landscape. Furthermore, the assessment based on querying security experts, system owners, or researchers' judgment is susceptible to biases and misleading heuristics. The bias arises if the judgment is based on personal experiences or beliefs and what comes to mind rather than objective and quantifiable data.

Table 4. Limitations in the cyber threat intelligence

Limitations in the cyber threat intelligence trustworthiness	**Assessment approaches relied on this threat intelligence source (References)**
The public threat intelligence does not reflect the organization's unique experience and can become outdated.	[33,34,38,39,41,42,45,47,50–54]
Scenario-based approach does not accurately parameterize the threat events or represent the actual complexity of a CPS system.	[32,37-39,41,43,45,47,49,50,54–58]
Past cyber-attacks experienced by a real-world CPS system are nonrepresentative and lack real-time learning of the threat landscape.	[42,44,48]
Security experts, system owners, or researchers' judgments are susceptible to biases and misleading heuristics.	[32–36,40,41,44,46,48,58,59]

Based on the above analysis, the cyber threat intelligence sources on which the studied risk assessment approaches rely provide incomplete knowledge of the potential cyber risks. These cyber threat information sources can be outdated or irrelevant, leading to incorrect or risk assessment results with high uncertainty.

4.2.3. Consistency of Cyber Threat Intelligence Interpretations

The validity and reliability of the risk assessment can be further affected by how consistently the cyber threat intelligence is interpreted across different assessors. Inconsistent interpretation of cyber threat information can lead to discrepancies and high level of uncertainty. Inconsistent interpretation arises from individual assessors' bias, where their beliefs influence how they assign meaning to the information of a specific cyber-threat. Another source of inconsistency is the ambiguity in the cyber threat information, which may lead to different analysts coming to different conclusions. Furthermore, when a threat intelligence source provides incomplete information about a specific threat, assessors make assumptions, which might be subjective and varied, to fill these gaps.

Although the reviewed approaches provided detailed steps to guide conducting the risk assessment, this is inadequate to address the probable inconsistencies in cyber threat intelligence interpretations. These approaches lacked methods and techniques for structuring how to interpret lessons about potential cyber risks, leaving room for varied interpretations. Given that 50% of the surveyed approaches draw upon two or more cyber threat intelligence sources, the potential for variability in interpretations is heightened. The lack of standardization methods affects the uniformity of the assessment and, hence, its validity and reliability.

4.2.4. Automation Support

A further constraint to achieving reliable risk assessment and valid results is the manual efforts required to conduct the assessment process, especially if it is not supported by a software tool. Manual risk assessment methodologies are less scalable and prone to human errors and inconsistencies. Supporting the risk assessment methodology with automation that facilitates the risk assessment steps, from data acquisition to risk calculation and dissemination, is crucial for reliable assessment, especially in a highly interconnected CPS infrastructure.

Among the risk assessment methodologies reviewed in this study, 75% lack software support, relying entirely on manual efforts. In the remaining seven approaches [34,40–42,44,45,56], the authors developed software tools or created Python or MATLAB scripts to facilitate the risk assessment process. However, the intelligence these tools and scripts provide is limited. For instance, in identifying the potential cyber risks, these tools do not complement the assessors' knowledge with real-time learning from the publicly available threat intelligence sources and the cybersecurity incidents the organization undergoes. Similarly, in risk analysis, they do not automate the modeling and simulation of threat scenarios based on what they learn.

The automation support in the reviewed approaches has not yet reached a level of maturity where it facilitates a risk assessment process, from preparation for the risk assessment to conducting it, communicating its results, and maintaining it over time. With this lack of automation support, human assessors cannot effectively analyze the relevant cyber threat intelligence sources in real time. As a result, the ability of the studied assessment methodologies to maintain consistency and adapt to the constantly changing threat landscape will be hindered, thereby limiting assessment reliability and validity.

4.2.5. The Potential Effectiveness of the Risk Assessment Approaches

In light of the preceding analysis, the reviewed cyber risk assessment methodologies revealed limited effectiveness in assessing cyber risks. They fall short in conforming to different factors crucial for ensuring assessment effectiveness. Some methodologies lack well-defined risk models to evaluate the risk factors or the overall risk. Another shortcoming relates to the trustworthiness of cyber threat intelligence sources they rely on, which can be outdated, nonrepresentative, or imprecise. Another effectiveness requirement the studied risk assessment methodologies failed to

meet is addressing the probable inconsistencies in cyber threat intelligence interpretations. Finally, most reviewed risk assessment methodologies rely solely on manual efforts.

5. REAL-TIME LEARNING FROM CYBERSECURITY INCIDENTS FOR IMPROVED CYBER RISK ASSESSMENT EFFECTIVENESS

The more challenging factors impacting the risk assessment effectiveness, which have not been adequately discussed in the existing literature, are (1) the nature of cyber threat information sources on which the risk assessment relies and (2) the way human analysts interpret this information. The trustworthiness of cyber threat information contributes greatly to risk assessment effectiveness and must be up-to-date, relevant, representative, and precise. Consistency in interpreting the cyber threat information across different assessors is also crucial for effective assessment. Minimizing inconsistencies in the assessors' interpretations is challenging but not impossible if the sources of these inconsistencies are identified.

The multiple requirements for trustworthy cyber threat information and consistent interpretations underscore the need for a cyber risk assessment approach of more than a component collaboration to improve the risk assessment's effectiveness. Such an approach could leverage cybersecurity incidents the organization undergoes as a primary source to learn about potential cyber risks. As discussed in Section 2, real-time learning from cybersecurity incidents can complement the assessors' knowledge with up-to-date information about cyber risks representing an organization's unique experience and the complexities of real-world CPS systems. Automation support is crucial to enabling real-time learning from cybersecurity incidents and other cyber threat intelligence sources. A machine learning-based software tool is recommended to enable learning from the cyber incident as it occurs and update the risk assessment process. As discussed in Section 2, machine learning can reduce manual efforts, thereby better structuring the acquisition, retainment, dissemination, and application of knowledge about cyber risks. ML capabilities contribute to minimizing human errors and inconsistencies in cyber-threat interpretations.

6. CONCLUSION

This literature review examined how the studied cyber risk assessment approaches were evaluated. It also investigated to what extent these approaches meet the requirements of effective risk assessment. The findings revealed that the effectiveness of the examined risk assessment approaches was predominantly evaluated in terms of applicability but not other pivotal criteria like validity and reliability. The existing cyber risk assessment methodologies have been found to fall short in conforming to the assessment effectiveness requirements, which include a well-defined risk model, trustworthy cyber threat intelligence, consistent cyber threat intelligence interpretations, and automation support. This study identified the untrustworthiness of cyber threat intelligence and the inconsistent interpretations of this cyber threat information as the most challenging gaps that limit risk assessment effectiveness. It proposed real-time learning from cybersecurity incidents to overcome these limitations. Future research will deeply investigate the contribution of the given recommendations in addressing the most challenging gaps impacting the assessment effectiveness.

ACKNOWLEDGEMENTS

The authors would like to thank Sultan Qaboos University for their support throughout the various phases of this research. The resources provided by the university facilitated the completion and publication of this research paper.

REFERENCES

[1] Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," IEEE Internet Things J, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[2] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," Reliab Eng Syst Saf, vol. 152, pp. 137–150, Aug. 2016, doi: 10.1016/j.ress.2016.02.009.

[3] J. Madden, "Security analysis of a cyber physical system: A car example," Missouri University of Science And Technology, 2012.

[4] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of industrial cyber-physical systems: a review," ACM Comput Surv, vol. 54, no. 11s, pp. 1–35, Jan. 2022, doi: 10.1145/3510410.

[5] Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-Physical Systems and Internet of Things. NIST Special Publication 1900-202," Gaithersburg, MD, Mar. 2019. doi: 10.6028/NIST.SP.1900-202.

[6] J. Ali, "Intrusion detection systems trends to counteract growing cyber-attacks on cyber-physical systems," in 2021 22nd International Arab Conference on Information Technology (ACIT), IEEE, Dec. 2021, pp. 1–6. doi: 10.1109/ACIT53391.2021.9677429.

[7] P. Radoglou-Grammatikis et al., "SPEAR SIEM: A Security Information and Event Management system for the smart grid," Computer Networks, vol. 193, p. 108008, Jul. 2021, doi: 10.1016/j.comnet.2021.108008.

[8] A. Ahmed Jamal, A.-A. Mustafa Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using machine learning," Mater Today Proc, Jul. 2021, doi: 10.1016/j.matpr.2021.06.320.

[9] Z. Wang, W. Xie, B. Wang, J. Tao, and E. Wang, "A survey on recent advanced research of CPS security," Applied Sciences, vol. 11, no. 9, p. 3751, Apr. 2021, doi: 10.3390/app11093751.

[10] A. Albasir, K. Naik, and R. Manzano, "Toward improving the security of IoT and CPS devices: an AI approach," Digital Threats: Research and Practice, vol. 4, no. 2, pp. 1–30, Jun. 2023, doi: 10.1145/3497862.

[11] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems," International Journal of Critical Infrastructure Protection, vol. 35, p. 100464, Dec. 2021, doi: 10.1016/j.ijcip.2021.100464.

[12] DRAGOS, "ICS/OT Cybersecurity Year in Review," 2022. Accessed: May 09, 2023. [Online]. Available: https://www.dragos.com/year-in-review/

[13] DRAGOS, "ICS/OT Cybersecurity Year in Review," 2021. Accessed: May 09, 2023. [Online]. Available: https://www.dragos.com/year-in-review/

[14] H. Sedjelmaci, F. Guenab, S.-M. Senouci, H. Moustafa, J. Liu, and S. Han, "Cyber security based on Artificial Intelligence for Cyber-Physical Systems," IEEE Netw, vol. 34, no. 3, pp. 6–7, May 2020, doi: 10.1109/MNET.2020.9105926.

[15] X. Zhou, Z. Xu, L. Wang, and K. Chen, "What should we do? a structured review of SCADA system cyber security standards," in 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), IEEE, Apr. 2017, pp. 0605–0614. doi: 10.1109/CoDIT.2017.8102661.

[16] M. Zahid, I. Inayat, M. Daneva, and Z. Mehmood, "Security risks in cyber physical systems—A systematic mapping study," Journal of Software: Evolution and Process, vol. 33, no. 9. John Wiley and Sons Ltd, Sep. 01, 2021. doi: 10.1002/smr.2346.

[17] R. Ross, "Guide for conducting risk assessments. NIST Special Publication 800-30," Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.

[18] M. Barrett, "Framework for improving critical infrastructure cybersecurity Version 1.1, NIST Cybersecurity Framework," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[19] National Council on Crime and Delinquency (NCCD), "Understanding Validity of Risk Assessment Instruments," 2015, Accessed: Mar. 29, 2024. [Online]. Available: www.nccdglobal.org;

[20] T. Aven and B. Heide, "Reliability and validity of risk analysis," Reliab Eng Syst Saf, vol. 94, no. 11, pp. 1862–1868, Nov. 2009, doi: 10.1016/j.ress.2009.06.003.

[21] M. Torngren et al., "Characterization, Analysis, And Recommendations For Exploiting The Opportunities Of Cyber-Physical Systems," in Cyber-Physical Systems: Foundations, Principles and Applications (Intelligent Data-Centric Systems), 1st ed., vol. 514, S. Houbing, D. B. Rawat, J. Sabina, and B. Christian, Eds., London: Academic Press, 2016, pp. 3–14.

[22] NIST, "Glossary- Cybersecurity Risk." Accessed: Feb. 14, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/cybersecurity_risk

[23] T. Sanislav, G. Dan Mois, S. Folea, and L. Miclea, "Integrating wireless sensor networks and cyber-physical systems: challenges and opportunities," in Cyber-Physical System Design with Sensor Networking Technologies, vol. 368, S. Zeadally and N. Jabeur, Eds., London, United Kingdom: The Institution of Engineering and Technology, 2016.

[24] S. Kaplan and B. J. Garrick, "On The Quantitative Definition of Risk," Risk Analysis, vol. 1, no. 1, pp. 11–27, Mar. 1981, doi: 10.1111/j.1539-6924.1981.tb01350.x.

[25] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, "Cyber-physical System Risk Assessment," in 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, Oct. 2013, pp. 442–447. doi: 10.1109/IIH-MSP.2013.116.

[26] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," Gaithersburg, MD, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.

[27] P. Shedden, A. Ahmad, and A. B. Ruighaver, "Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process," in 8th Australian Information Security Mangement Conference, Perth: School of Computer and Information Science, Edith Cowan University, 2010. doi: 10.4225/75/57b6771734788.

[28] A. Ahmad, S. B. Maynard, and G. Shanks, "A case analysis of information systems and security incident responses," Int J Inf Manage, vol. 35, no. 6, pp. 717–723, Dec. 2015, doi: 10.1016/j.ijinfomgt.2015.08.001.

[29] Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, and Suzanne Lightman, "Guide to Operational Technology (OT) Security- NIST Special Publication 800-82r3," 2022, doi: 10.6028/NIST.SP.800-82r3.ipd.

[30] A. Gupta, R. Gupta, and G. Kukreja, "Cyber Security Using Machine Learning: Techniques and Business Applications," in Applications of Artificial Intelligence in Business, Education and Healthcare. Studies in Computational Intelligence , vol. 954, A. Hamdan, A. E. Hassanien, R. Khamis, and B. Alareeni, Eds., Cham: Springer , 2021, pp. 385–406. doi: 10.1007/978-3-030-72080-3_21.

[31] R. Calderon, "The Benefits of Artificial Intelligence in Cybersecurity," 2019. Accessed: Mar. 06, 2023. [Online]. Available: https://digitalcommons.lasalle.edu/ecf_capstones/36

[32] Y. Zhang and M. Ni, "Security-oriented cyber-physical risk assessment for cyberattacks on distribution system," Applied Sciences, vol. 13, no. 20, p. 11569, Oct. 2023, doi: 10.3390/app132011569.

[33] G. Gkoktsis, H. Lauer, and L. Jaeger, "Risk assessments in virtual power plants with NESCOR criteria, practical application, advantages and disadvantages," in Proceedings of the 18th International Conference on Availability, Reliability and Security, New York, NY, USA: ACM, Aug. 2023, pp. 1–11. doi: 10.1145/3600160.3605179.

[34] A. Amro, V. Gkioulos, and S. Katsikas, "Assessing cyber risk in cyber-physical systems using the ATT&CK framework," ACM Transactions on Privacy and Security, vol. 26, no. 2, pp. 1–33, May 2023, doi: 10.1145/3571733.

[35] Akbarzadeh and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems," Int J Inf Secur, vol. 22, no. 3, pp. 563–578, Jun. 2023, doi: 10.1007/s10207-022-00608-4.

[36] K.-S. Son, J.-G. Song, and J.-W. Lee, "Development of the framework for quantitative cyber risk assessment in nuclear facilities," Nuclear Engineering and Technology, vol. 55, no. 6, pp. 2034–2046, Jun. 2023, doi: 10.1016/j.net.2023.03.023.

[37] G. Moraitis et al., "Exploring the cyber-physical threat landscape of water systems: a socio-technical modelling Approach," Water (Basel), vol. 15, no. 9, p. 1687, Apr. 2023, doi: 10.3390/w15091687.

[38] Y. KAWANISHI, H. NISHIHARA, H. YAMAMOTO, H. YOSHIDA, and H. INOUE, "A Study of the risk quantification method of cyber-physical systems focusing on direct-access attacks to In-vehicle networks," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E106.A, no. 3, p. 2022CIP0004, Mar. 2023, doi: 10.1587/transfun.2022CIP0004.

[39] S. Deng, J. Zhang, D. Wu, Y. He, X. Xie, and X. Wu, "A quantitative risk assessment model for distribution cyber physical system under cyber attack," IEEE Trans Industr Inform, Mar. 2023, doi: 10.1109/TII.2022.3169456.

[40] H. M. Tusher, Z. H. Munim, T. E. Notteboom, T.-E. Kim, and S. Nazir, "Cyber security risk assessment in autonomous shipping," Maritime Economics & Logistics, vol. 24, no. 2, pp. 208–227, Jun. 2022, doi: 10.1057/s41278-022-00214-0.

[41] 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, p. 103611, May 2022, doi: 10.1016/j.compind.2022.103611.

[42] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," Neural Comput Appl, vol. 34, no. 18, pp. 15241–15271, Sep. 2022, doi: 10.1007/s00521-022-06959-2.

[43] K. Ntafloukas, D. P. McCrum, and L. Pasquale, "A cyber-physical risk assessment approach for internet of things enabled transportation infrastructure," Applied Sciences (Switzerland), vol. 12, no. 18, Sep. 2022, doi: 10.3390/app12189241.

[44] G. Rosado et al., "Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern," Comput Ind, vol. 142, Nov. 2022, doi: 10.1016/j.compind.2022.103715.

[45] Semertzis, V. S. Rajkumar, A. Stefanov, F. Fransen, and P. Palensky, "Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs," in 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems, MSCPES 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/MSCPES55116.2022.9770140.

[46] Y. Yoo and H.-S. Park, "Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship," J Mar Sci Eng, vol. 9, no. 6, p. 565, May 2021, doi: 10.3390/jmse9060565.

[47] Z. Ji et al., "Harmonizing safety and security risk analysis and prevention in cyber-physical systems," Process Safety and Environmental Protection, vol. 148, pp. 1279–1291, Apr. 2021, doi: 10.1016/j.psep.2021.03.004.

[48] Gunes, G. Kayisoglu, and P. Bolat, "Cyber security risk assessment for seaports: A case study of a container port," Comput Secur, vol. 103, Apr. 2021, doi: 10.1016/j.cose.2021.102196.

[49] A. Tantawy, S. Abdelwahed, A. Erradi, and K. Shaban, "Model-based risk assessment for cyber physical systems security," Comput Secur, vol. 96, Sep. 2020, doi: 10.1016/j.cose.2020.101864.

[50] X. Lyu, Y. Ding, and S. H. Yang, "Bayesian network based C2P risk assessment for cyber-physical systems," IEEE Access, vol. 8, pp. 88506–88517, 2020, doi: 10.1109/ACCESS.2020.2993614.

[51] A. A. Malik and A. A. Tosh, "Quantitative risk modeling and analysis for large-scale cyber-physical systems," in 2020 29th International Conference on Computer Communications and Networks (ICCCN), IEEE, Aug. 2020, pp. 1–6. doi: 10.1109/ICCCN49398.2020.9209654.

[52] Tam and K. Jones, "MaCRA: a model-based framework for maritime cyber-risk assessment," WMU Journal of Maritime Affairs, vol. 18, no. 1, pp. 129–163, Mar. 2019, doi: 10.1007/s13437-019-00162-2.

[53] Zarreh, H. Da Wan, Y. Lee, C. Saygin, and R. Al Janahi, "Risk assessment for cyber security of manufacturing systems: A game theory approach," in Procedia Manufacturing, Elsevier B.V., 2019, pp. 605–612. doi: 10.1016/j.promfg.2020.01.077.

[54] Q. Dai, L. Shi, and Y. Ni, "Risk assessment for cyber attacks in feeder automation system," in 2018 IEEE Power & Energy Society General Meeting (PESGM), IEEE, Aug. 2018, pp. 1–5. doi: 10.1109/PESGM.2018.8586312.

[55] H.-K. Kong, M. K. Hong, and T.-S. Kim, "Security risk assessment framework for smart car using the attack tree analysis," J Ambient Intell Humaniz Comput, vol. 9, no. 3, pp. 531–551, Jun. 2018, doi: 10.1007/s12652-016-0442-8.

[56] Yao, P. Venkitasubramaniam, S. Kishore, L. V. Snyder, and R. S. Blum, "Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks," in 2017 51st Annual Conference on Information Sciences and Systems, CISS , Institute of Electrical and Electronics Engineers Inc., 2017. doi: 10.1109/CISS.2017.7926147.

[57] X. Ji, H. Yu, G. Fan, and W. Fu, "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, May 2016, pp. 693–698. doi: 10.1109/SNPD.2016.7515980.

[58] J. YAN, M. GOVINDARASU, C.-C. LIU, M. NI, and U. VAIDYA, "Risk assessment framework for power control systems with PMU-based intrusion response system," Journal of Modern Power Systems and Clean Energy, vol. 3, no. 3, pp. 321–331, Sep. 2015, doi: 10.1007/s40565-015-0145-8.

[59] F. Farzan, M. A. Jafari, D. Wei, and Y. Lu, "Cyber-related risk assessment and critical asset identification in power grids," in ISGT 2014, IEEE, Feb. 2014, pp. 1–5. doi: 10.1109/ISGT.2014.6816371.

[60] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of security management and incident response enables organizational learning," J Assoc Inf Sci Technol, vol. 71, no. 8, pp. 939–953, Aug. 2020, doi: 10.1002/asi.24311.

[61] S. Eggers and K. Le Blanc, "Survey of cyber risk analysis techniques for use in the nuclear industry," Progress in Nuclear Energy, vol. 140, p. 103908, Oct. 2021, doi: 10.1016/j.pnucene.2021.103908.

[62] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Computers and Security, vol. 56. Elsevier Ltd, pp. 1–27, Feb. 01, 2016. doi: 10.1016/j.cose.2015.09.009.

AUTHORS

Asila AlHarmali is a PhD student in information systems at Sultan Qaboos University in Muscat, Oman. She holds a Master of Science in Internet Computing and Networking Security from Loughborough University in the UK. Before her Ph. D., Asila was a lecturer at the Computing and Information Sciences College at the University of Technology and Applied Sciences in Oman. Her research interest is cybersecurity for cyber-physical systems.

Professor Saqib Ali is a cybersecurity expert in the Department of Information Systems at Sultan Qaboos University, Muscat, Oman. His research spans cybersecurity for cyber-physical systems, information systems, and industrial informatics. He has a prolific record of publications and actively contributes to the field through editorial boards, conference committees, and postgraduate student supervision. Professor Ali currently serves as the Assistant Dean for Postgraduate Studies and Research.

Waqas Aman is an Assistant Professor at the Department of Information Systems, Sultan Qaboos University (SQU), Oman. Holding a PhD in Information Security from Norwegian University of Science and Technology (NTNU), Norway, he actively explores emerging cybersecurity challenges posed by advancingtechnologies. With experience as an Information Security professional, Dr. Aman contributes to industry and academia, and holds international certifications such as CEH, CEI, ECSA, ENSA, EDRP, and ITIL. He has also served as a Certified Instructor for EC Council™ certifications.

Omar Hussain is an Associate Professor at the University of New South Wales, Canberra. Hisresearch interests are in business intelligence, cloud computing and logistics informatics. In these areas, his research work focuses on utilizing decision making techniques for facilitating smart achievement of business outcomes. His research work has been published in various top international journals such as Information Systems, The Computer Journal, Knowledge Based Systems, Future Generation of Computer Systems etc. He has won awards and funding from competitive bodies such as the Australian Research Council for his research.