A Survey of Cyber Security and Safety in Industrial Control Systems

*Yi-Wei Ma, Yi-Hao Tu, Chia-Wei Tsou, Yen-Neng Chiang, Jiann-Liang Chen**

Department of Electrical Engineering, National Taiwan University of Science and Technology, Taiwan
yiweimaa@gmail.com, itstuyihao@gmail.com, pat60407@gmail.com, 10601sos@gmail.com, Lchen@mail.ntust.edu.tw

Abstract

The utilization of network technology in Industrial Control Systems (ICS) is becoming increasingly prevalent due to advancements in the Fifth Generation Networks (5G), the Internet of Things (IoT), cloud computing, and big data. These technologies have significantly enhanced intelligent mobile device data transmission speed and interaction levels. The connection of ICS devices to a network gives rise to supplementary security considerations. Hence, this paper must analyze and synthesize pertinent scholarly works on cyber security and safety within the ICS sector. This paper further categorizes the security risks that ICS may encounter into six distinct areas: attack, detect, risk estimation, incident response, protect, and incident prevention. Extensive literature evaluations and rigorous research were conducted to examine the subject matter thoroughly. Based on the findings, comprehensive suggestions and strategic approaches were produced for each specific area. This paper proposed the ICS-based Purdue Enterprise Reference Architecture (PERA) to evaluate the threat and solution for enhancing ICS security and safety.

Keywords: Cyber security and safety, Industrial control systems, ICS-based Purdue Enterprise Reference Architecture (PERA)

1 Introduction

Industrial Control System (ICS) monitors and controls many industrial sectors [1]. Over the past decade, ICS has been characterized by a complete disconnection from external networks, which are used to mitigate infrastructure device attacks and risks. Unfortunately, ICS is currently unable to prevent the various attacks for many reasons; the typical cyber-attack events are given in Table 1, where each has caused significant global damage. For instance, most attacks on ICS have been executed through the utilization of Remote Access Trojans (RATs), illustrated by Stuxnet, one of the infamous malware. Stuxnet attacks can be performed through multiple methods, i.e., some attackers exploit the accessible USB ports to enable pass through the internal networks and targeted spear-phishing attempts involving email spoofing.

On the other hand, some attackers leverage Denial of Service (DoS) to overflow the system buffer when the process or program attempts to store data in a temporary area that exceeds the authorized storage space. There are instances where it might facilitate the execution of arbitrary code. This capability may grant unauthorized access to a vulnerable process, which enables the attacker to assume control over essential industrial infrastructure.

One of the main challenges associated with traditional ICSs is their reliance on outdated software and operating systems, which exhibit multiple vulnerabilities. Furthermore, many of these systems have autorun functionalities, making them vulnerable to exploitation by malicious software. According to the assessment of industrial security in 2022, it was determined that around 94% of firms had encountered various forms of security incidents [2]. Given the growing focus of researchers on the security of ICS [3-6], several works provide a broad outline of ICS attacks and recommend solutions [7-12]. Table 2 presents the related surveys on cyber security in ICS. This article investigated the state-of-the-art literature reviews within the 10 years for comprehensive analysis. In addition, this paper strengthens the focus on the domains of attack, detect, risk estimate, incident response, protect, and incident prevent for cyber security and safety in ICS and related manufacturing fields.

Table 1. The history of cyber-attack occurrences throughout time

Year	Location	Descriptions
2010	Iran	The Stuxnet attack caused the destruction of core controllers in various industries.
2015	Ukraine	There has been a BlackEnergy attack on the power grid, resulting in a widespread power outage.
2017	Russia, Ukraine, India, China	There is an ongoing WannaCry cyber attack that is targeting data encryption and demanding ransom payments.
2020	Brno University Hospital, Czech Republic	A Czech hospital's IT network was shut down by a cyber attack.
2020	US Dept. Health & Human Services	There has been an attack on the servers, but the details are currently unknown.
2021	Colonial Pipeline, US	A ransomware attack caused a critical fuel network shutdown in the US.

*Corresponding Author: Jiann-Liang Chen; E-mail: Lchen@mail.ntust.edu.tw
DOI: https://doi.org/10.70003/160792642024072504005

Table 2. Comparative analysis with other surveys on Industrial Control Systems (ICSs)

No.	Year	Study	Feature	Ref.
1	2020	Industrial Control Systems: Cyberattack trends and countermeasures	Analyzes attacks on ICSs in last 20 years and discusses each attack in terms of its goal, description, impact, and potential solution to mitigate it.	[7]
2	2020	Cybersecurity for industrial control systems: A survey	Surveys the shift of ICS from stand-alone systems to cloud-based enviroments, leveraging the advancement in the field on Machine Learning techniques.	[8]
3	2022	Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review	Surveys the cyber security challenges in Industry 4.0 scenarios and provides a guideline solution to deal with each element of their cyber security issues.	[9]
4	2022	Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review	Investigated the cyber security and information security awareness in ICS and IIoT, providing the model and tools to enhancing the cyber security awareness.	[10]
5	2023	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future	Presented the systematic review of different methods cutting-edge techniques and possible solutions approaches to cyber security in smart grids.	[11]
6	2023	Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review	Surveys the various complex attack characteristics and types from attack techniques and tactics perpectives in smart grid. Moreover, they provide their limitation and support the applicability of existing visualizations and co-simulation tools to the real world.	[12]
7	2023	This study	Presented broad overviews, strengthened focus on the domains of attack, detect, risk estimate, incident response, protect, and incident prevent for those cyber security and safety in ICS and related manufacturing fields.	

2 The ICS-based Purdue Enterprise Reference Architecture

This paper aims to examine the influence of the ICS sector comprehensively. Therefore, this paper proposed the ICS-based Purdue Enterprise Reference Architecture (PERA) to categorize Information Technology (IT) and Operational Technology (OT) into levels zero (L0) and five (L5). While the classification of equipment levels may vary among businesses and processes, it ultimately relies on the interconnection, reliance, and data transmission among its components. Figure 1 illustrates the PERA model as the case study in this work. Furthermore, this paper analyzes the prevailing attack and defensive techniques. Implementing the safety PERA is advantageous for ICS as it facilitates monitoring environmental facilities, hence ensuring compliance with safety standards throughout the ICS field.

- **Level 0 – Physical Process Zone**

This domain encompasses the assortment of sensors, actuators, and other apparatus that bear direct responsibility for the execution of assembling lubrication and other physical processes. Many contemporary sensors establish direct communication with cloud-based monitoring software through cellular networks.

- **Level 1 – Intelligent Devices Zone**

This domain encompasses devices that transmit instructions to L0 devices, i.e., Programmable Logic Controllers (PLC) and Intelligent Electronic Devices (IED).

- **Level 2 – Control Systems Zone**

This domain encompasses tangible operations' management, surveillance, and control, i.e., Human and Machine Interface (HMI).

- **Level 3 – Manufacturing Operations Systems Zone**

This domain monitors and manages production processes inside the shop floor area, i.e., Supervisory Control and Data Acquisition (SCADA) software and Distributed Control Systems (DCS).

- **Level 4/5 - Enterprise Zone**

These domains include the conventional information technology network, whereby the fundamental business functions, such as managing industrial operations, are conducted. The Enterprise Resource Planning (ERP) systems work production schedules, material consumption, shipping, and inventory levels.

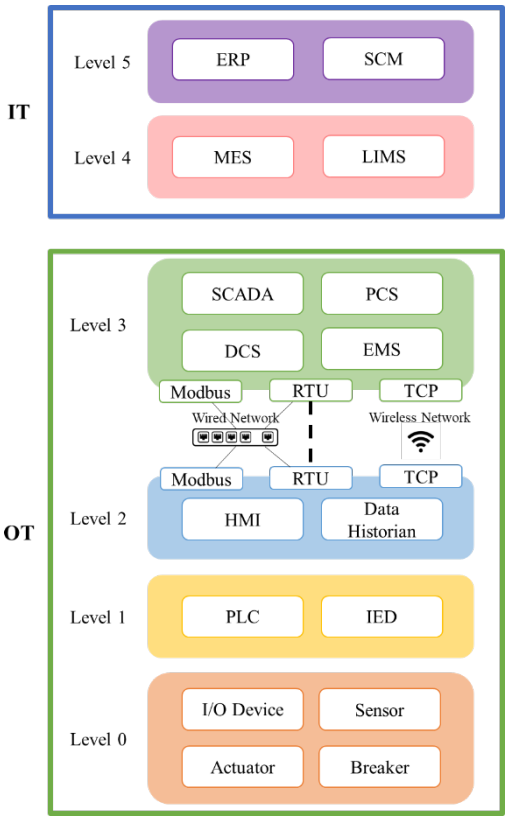

Figure 1. The ICS-based Purdue Enterprise Reference Architecture (PERA)

3 Survey of Cyber Security and Safety in ICS

This paper comprehensively reviewed the existing literature and focused on the domains of attack, detect, risk estimate, incident response, protect, and incident prevention. Moreover, this paper examines the current assaults and potential future trends to enhance relevant defensive mechanisms, hence mitigating attacks. Figure 2 displays the schematic diagram.

3.1 Attack

This paper aims to identify potential crises and prevent system operation paralysis, data theft, and unauthorized control permissions resulting from attacks in industrial control environments. The research investigates attack technologies and methods employed in such environments to achieve this. It analyzes common attacks on ICS based on the PERA framework, as presented in Table 3.

3.1.1 Cyber Security

Kravchik *et al.* [13] proposed using Neural Networks (NN) to monitor and detect attacks in ICS. Meanwhile, The author has presented two distinct attack algorithms and has successfully demonstrated their efficacy.

The single-point infiltration strategy suggested by Sarkar *et al.* [14] included using the HMI and employing control theory to develop a perturbation-based generic assault for ICS. The findings indicate that assailants can execute end-to-end assaults with notable precision. Additionally, the researchers put forward many defensive strategies in response to these attacks.

Babu *et al.* [15] performed a concise assessment of the risks to ICS, focusing on the security vulnerabilities of SCADA systems. Their study aimed to provide researchers with a comprehensive understanding of the security issues and difficulties SCADA systems encounter.

3.1.2 Safety

According to Jin *et al.* [16], there is a perceived need for a technological solution in ICS to address the compatibility between cyber security and functional security measures. This is crucial to maintain the dependable operational safety of ICS and effectively counter the growing threat of cyber assaults. Applicable safety measures are used to assess each cyber security measure, and any discrepancies are identified using standard Safety Integrity Level 3 (SIL3) and Security Level 3 (SL3). The results indicate that the coordination strategy used in their study demonstrates compatibility between cyber security measures and functional safety measures. Furthermore, the coordination method could facilitate advancements in cyber security for ICS.

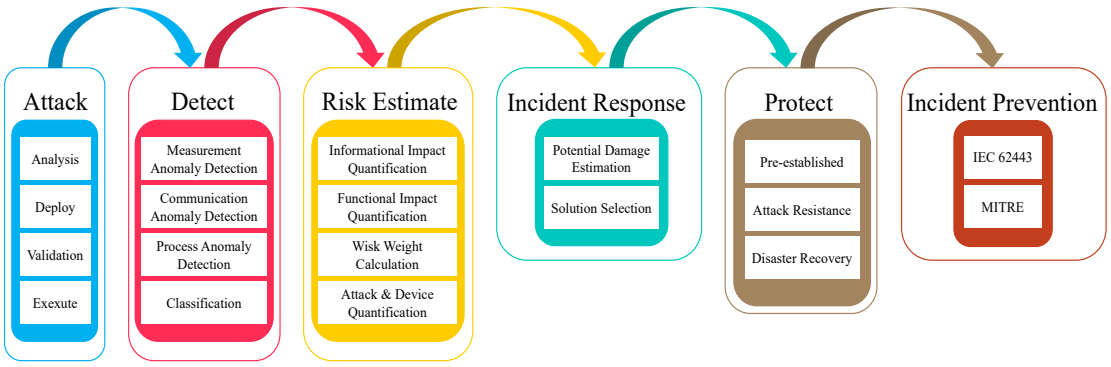

Figure 2. The systematic diagram for security and safety in ICS

Table 3. List of different major ICS attacks and threat level in proposed PERA model

ICS Attack		L0	L1	L2	L3	L4	L5
#1	ICS insider	✓	✓	✓	✓		
#2	IT insider					✓	✓
#3	Common ransomware					✓	✓
#4	Targeted ransomware					✓	✓
#5	Zero-day ransomware	✓	✓	✓	✓	✓	✓
#6	Ukrainian attack					✓	✓
#7	Sophisticated ukrainian attack					✓	✓
#8	Market manipulation					✓	✓
#9	Sophisticated market manipulation					✓	✓
#10	Cell-phone WiFi					✓	✓
#11	Hijacked two-factor					✓	✓
#12	IIoT pivot						✓
#13	Malicious outsourcing	✓	✓	✓	✓	✓	✓
#14	Compromised vendor website	✓	✓	✓	✓	✓	✓
#15	Compromised remote site					✓	
#16	Vendor back door	✓	✓	✓	✓	✓	✓
#17	Stuxnet			✓	✓	✓	✓
#18	Hardware supply chain	✓	✓	✓	✓	✓	✓
#19	Nation-state compromise crypto					✓	✓
#20	Sophisticated credentialed ICS insider	✓	✓	✓			

Wang *et al.* [17] address application scenarios of Trusted Computing 3.0 in the ICS of nuclear power firms, including the system's general structure, the building of trusted nodes, system deployment, and the establishment of the whole security system.

Zhou *et al.* [18] propose a security task scheduling technique for ICS that incorporates a risk-based perspective and considers the safe work system. This approach ensures a prompt response to security breaches while maintaining high protection. The process addresses the integration of security and safety duties by implementing a predetermined resolution plan, providing the seamless execution of security and safety activities. Subsequently, a technique is developed to enable real-time risk assessment, specifically focusing on capturing the marginal impact on system risk arising from implementing security and safety reconciliation processes.

While a wide range of attack methods exist, except for those that do not require system entry, i.e., Distributed DoS (DDoS) attacks, the primary objective of most attacks is to circumvent defensive and detection mechanisms or measures to gain access to the system. Once inside, the attacker identifies vulnerabilities within the system, equipment, or communication protocol, which are exploited to launch attacks. Hence, the effective execution of system infiltration and device scanning while evading detection and preventing device damage resulting from malicious activities is a significant concern in attacks.

3.2 Detect

Despite the existence of defensive mechanisms aimed at safeguarding the system from potential assaults, the possibility of a successful attack remains. Consequently, implementing detection methods becomes imperative to warn or alert the system during an ongoing attack promptly. Currently, prevalent techniques for detecting intrusions include malicious packet identification, Artificial Intelligence (AI), Indicator of Compromise (IoC), traffic analysis, aberrant behavior detection, and Intrusion Detection Systems (IDS), among others. Given that the majority of OT assaults often infiltrate the system via the IT side, the use of network behavior analysis to identify IoC becomes advantageous in facilitating early detection. Individuals use various techniques to discover and detect abnormalities inside the OT environment. These approaches include malicious packet identification, traffic analysis, and abnormal behavior detection.

3.2.1 Cyber Security

To address the problem, malware-based network threat modeling techniques are designed for more than just ICS. In their study, Mekdad *et al.* [19] introduced a framework for modeling malware threats in ICS. The framework incorporates the extraction and modeling level established via the diamond model. To assess the proposed model's efficacy, the researchers analyzed the TRISIS network assault as a case study. The results indicate that there is a likelihood of targeted assaults on specific industrial devices inside ICS networks via the use of malicious software.

The safety of Industrial Automation Control Systems (IACS) was examined by Cheminod *et al.* [20]. They summarized the risk assessment, preventive, and detection techniques associated with IACS. Additionally, the document acknowledges that the intricate nature of IACS poses challenges in promptly and efficiently addressing an attack and restoring the system.

Ali *et al.* [21] conducted research to identify Machine Learning (ML) algorithms that have the potential to detect assaults on various kinds and motives of ICS and SCADA attacks. The present study undertakes a comprehensive examination of safety procedures within the ICS, followed by the proposal of several preventative strategies aimed at mitigating potential threats.

3.2.2 Safety

Zonouz *et al.* [22] describe their research on PLC code analytics, which uses safety engineering to identify and classify PLC infections that attempt to damage power plants physically. Their approach also uses control theory to uncover complex and highly variable safety features used in the hybrid code analytics technique.

Paridari *et al.* [23] provide a novel cyber-physical security architecture for ICS. This design incorporates an analytics tool for detecting attacks and a reliable estimation-based technique for maintaining control resilience in the case of an assault. The proposed architecture demonstrates adaptability to existing ICS and has shown robustness and optimal performance in the face of attacks targeting the system. To evaluate the efficacy of the proposed framework, a reduced-scale replica of an actual EMS station is used, along with simulated attack scenarios.

Peng *et al.* [24] presented a fuzz test-based approach to identify malware in ICS. The ICS software configuration file is utilized as the sample file for fuzzing and as the corrupt source file for corrupt analysis in the recommended approach. First, use dynamic taint analysis to identify critical data in the configuration file that likely contains a possible safety issue. Then, modify the data and create an anomalous data file. Lastly, execute the fuzz test. This method detects the majority of security threats.

The primary focus in the field of detection is currently on utilizing AI. However, exploring methods for acquiring more efficient information and addressing the issue of preventing attacks on AI is crucial. Neglecting the former may lead to inaccurate detection, while ignoring the latter may compromise the security of the detection system, allowing attackers to exploit vulnerabilities.

3.3 Risk Estimate

To maintain the continuous availability of ICS, it is essential to promptly assess the significance level after detecting an attack. This assessment ascertains the urgency with which the system must be remediated. When there are several dangers and limited resources, it becomes imperative to prioritize establishing the most necessary system while deferring attention to the less crucial system. Before an attack, most ICS strategies include doing a comprehensive risk analysis of the whole system to identify potential areas for improvement.

3.3.1 Cyber Security

Nicholson *et al.* [25] proposed the threats and vulnerabilities encountered in classifying and integrating SCADA systems. Moreover, they review and establish best practices to protect critical infrastructure.

Yampolskiy *et al.* [26] proposed a novel Cyber-Physical Attack Description Language (CPADL). The proposed method offers structured descriptions of known assaults, qualitative and quantitative evaluations of known Cyber Physical System (CPS) attacks, and system vulnerability analysis. It helps construct and populate a database of known attacks and aids in analyzing assaults.

Catelani *et al.* [27] developed the analysis of failure mode, effects, and criticality methods for critical infrastructure systems. To remove subjectivity, a new analytical program was proposed to assess value at risk thresholds. To differentiate between very few failure modes and severe failure modes.

3.3.2 Safety

Abdo *et al.* [28] proposed an innovative method for integrating security and safety into industrial risk analysis. This method includes the bowtie and attack tree to give a detailed picture of potential safety and security situations. Simultaneously, an example of a risk situation in a chemical industry case study illustrates the usefulness of this strategy.

Joksimovic *et al.* [29] presented and described a novel ARCADIS behavioral model and a real-world case outcome. As input, the model takes track-condition data and user performance requirements. The model simulates and estimates infrastructure conditions (i.e., system states) for various scenarios. The results, which include information on important sites, are utilized in an optimization process to minimize risk and costs.

Vusmari *et al.* [30] used the Fluid Stochastic Petri Net (FSPN) modeling formalism to suggest an approach that involves the comparison of safety metrics produced from simulations of both the new and old system models. This paper aims to evaluate the safety implications of a new method for air traffic monitoring called Autonomous Dependent Monitoring-Broadcasting (ADM-B). In addition to conducting safety assessments, it is possible to extend the scope of evaluation to include other types of systems. The specific metrics used in this process may include, but are not limited to, accessibility, reliability, and economic feasibility, among other relevant qualities.

Currently, a limited number of risk analysis techniques tailored explicitly to ICS exist. Most of these methods continue to depend on expert opinion or use more generalist risk analysis approaches. Several methodologies specialized to ICS only evaluate the severity of established attack or failure modes, while others are exclusively designed for power plants or grid domains. Nevertheless, it is essential to note that conventional approaches may not align seamlessly with the specific requirements of ICS, which include a wide range of safeguarded systems extending beyond power plants and grids. Henceforth, it is necessary to establish methodologies or instruments to analyze unidentified assaults in the broader context of the ICS or to devise independent approaches tailored to specific domains.

3.4 Incident Response

Some of it is essential for users or systems to undertake measures aimed at mitigating the impact of the assault or restoring the system to limit the extent of damage incurred. This research aims to provide a comprehensive overview of effective strategies for achieving desired outcomes in response to various situations. Given the intricate nature of ICS, most systems that come under assault are primarily addressed by experts in the field or substituted with redundant resources. There are a limited number of techniques capable of autonomously restoring the system.

3.4.1 Cyber Security

Combita *et al.* [31] found two primary categories of reaction in their analysis: preventative response and reactive response. The approach may be categorized into

two main methods: using game theory and utilizing a model. Simultaneously, the authors also propose potential avenues for further growth. The scope of this research is limited to examining reactionary responses to accidents, with preventative responses being categorized as part of the protective response.

Rondeau *et al.* [32] introduced a forensic investigation framework specifically designed for the Industrial IoT (IIoT) in their study. This framework complements the forensic approaches used in the lowest-layer physical and highest-layer digital domains. The use of IIoT in Internet forensics aims to maximize investigative benefits, reduce the time required for reactive responses, and improve the effectiveness of forensic investigation tools and procedures used in courtrooms.

Ghosh *et al.* [33] presented the fault and behavior monitoring tool to recognize behavioral anomalies and isolate faults in PLC. Firstly, their methods collect the signal log data from fault-free manufacturing systems and resolve the problem of inaccurate log data with a result-oriented approach. Then, a deterministic finite-state automaton is constructed as a fault-free model of the PLC control process to detect the PLC's behavior abnormalities and faults. They were finally isolating the abnormal device and notifying the staff to repair it when the behavior abnormalities or defects occur.

3.4.2 Safety

Spyridopoulos *et al.* [34] examined the solid digital evidence to generate access security events. Meanwhile, some recommendations for data storage and processing in their studies have been proposed.

Takagi *et al.* [35] provided a systematic approach to designing cyber-attack prevention systems for ICS. The decision-making method allows for development and evaluation by process. Furthermore, incident reaction scenarios to ensure safety and security are addressed.

Alotaibi *et al.* [36] presented a concept for an intelligent system for tunnel and subway operations; the proposed method can ensure the oxygen saturation level of inside temperature of tunnel. The control system starts a quick succession of fan operations when there is a high temperature and carbon monoxide concentration, which enhances tunnel ventilation.

This paper revealed that most systems still allow professionals to deal with the problem once detected, while most ICS scenarios are large and complex. Therefore, it is critical to develop immediate and effective incident response systems to reduce response time and human costs.

3.5 Protect

Defense in depth and DMZ are essential strategies to strengthen asset security in the ICS fields. To prevent abnormal attacks from external networks, the objective of defense in depth is to set up a series of security barriers, and the goal of DMZ is to separate the system between internal and external networks. This paper presented some solutions based on our proposed PERA for various attacks in ICS, as shown in Table 4.

Table 4. List of defense strategies in proposed PERA model

Defensive Strategy		L0	L1	L2	L3	L4	L5
#1	Two-factor authentication	✓	✓	✓	✓	✓	✓
#2	Firewall	✓	✓	✓	✓	✓	✓
#3	DMZ	✓	✓	✓	✓		
#4	Antivirus software				✓	✓	✓
#5	Encryption	✓	✓	✓	✓	✓	✓
#6	Defense in depth	✓	✓	✓	✓	✓	✓
#7	Least privilege	✓	✓	✓	✓	✓	✓
#8	Need-to-know	✓	✓	✓	✓	✓	✓
#9	Patch management	✓	✓	✓	✓	✓	✓

3.5.1 Cyber Security

McLaughlin *et al.* [37] proposed a method for vulnerability assessment step to find potential threats in ICS. In addition, they addressed strategies and control architectures to mitigate attacks and trends in current ICS attacks and defenses.

Ren *et al.* [38] incorporated the possible identity resolution system of IIoT and addressed its significance and design principles from the identity resolution system's viewpoint. Provides the capabilities and characteristics of the proposed identity resolution system and a broad framework for evaluating them. In addition, the author categorizes current identity resolution systems, examines prominent strategies in use today, and compares them based on their design principles and technology selections.

Hou *et al.* [39] proposed the evaluate and oversee framework. This framework considers all security risks throughout the ICS supply chain, from technical aspects to people and organizational issues, enabling effective risk decisions and identification of security requirements.

3.5.2 Safety

Safety and security must be thoroughly studied to keep ICS from failing due to purposeful attacks from outside the system or inside flaws. First, outside security breaches undermine internal devices, leading to safety hazards. Second, each sector is individual, with different goals, but if sectors simultaneously contain security and safety, which can achieve various goals in ICS. As a result, this paper

investigates the other methods to link security and safety.

Gu *et al.* [40] analyzed and categorized the connections between safety and security needs. Two examples are offered to illustrate how to implement the proposed technique.

Khan *et al.* [41] perform a design strategy for trustworthy ICS. Three different methodologies were proposed that simultaneously work together. Firstly, a reliable and secure-by-design creation of secure industrial control applications. Secondly, provide a real-time comparison tool between application execution and application specifications execution at the ICS middleware level to safeguard field ICS operations. Lastly, a vulnerability assessment for False Data Injection (FDI) attacks results in the creation of ICS application architectures.

Yuan *et al.* [42] analyze the reason for axel bearing failure and provide ways to reduce the risk. It is recommended that a condition monitoring system be devised to monitor the axle bearing to keep functioning failure under control. The author suggests gathering data on the axle bearing's condition monitoring system from various angles, i.e., vibration, current, voltage, and temperature, to increase failure detection accuracy. The multiple signals should be analyzed using a physical and a data-driven model to optimize the maintenance strategy.

This paper concluded that the potential hazards can be eliminated through structured guidelines and processes to provide recommendations and applicable countermeasures. Defenders can help break the cyber kill chain before attackers can carry out attacks by assessing system vulnerabilities and detecting security incidents that have not escalated into accidents. This includes detecting faulty equipment and unavailable services and resources, which is critical to determining the correctness and security of industrial controls. Then, the company and the developer can decide the implementation sequence of improvement according to their operational requirements, from the priority level, system risk assessment, and needed resources and costs, so that the company can effectively improve the level of security protection every time the system is strengthened.

3.6 Incident Prevention

A platform audit solution is needed to examine the current ICS to provide valid reference values and safety level assessments to facilitate subsequent control and improvement of the operational system. People mainly use the NIST cyber security framework, i.e., NIST 800-53, NIST 800-82, and other network security standards, i.e., IEC 62443.

3.6.1 Cyber Security

Chaudhry *et al.* [43] compiled a summary of critical security characteristics and constructed feature vectors that could be used to assess database system security. In terms of data storage and administration, this would assist researchers in maintaining the security of CPS.

Lyu *et al.* [44] reviewed existing risk assessment and management methods from the safety and security perspective and integrated both. SIL is used for risk assessment, and security is based chiefly on NIST 800-82, NIST 800-53, and IEC 62443. In addition, the Security Assurance Level (SAL) is used for risk assessment, which makes it difficult to conduct comprehensive risk analysis and evaluation. Therefore, they suggested that researchers pay attention to extensive risk assessment methods from the safety and security perspective.

Zahid *et al.* [45] reviewed the research on CPS security requirements and CPS security risk management. They integrated the standard approaches, methods, models, techniques, assessment mechanisms, indicators, and deficiencies of risk identification, assessment, management, and mitigation. Through the literature review, some suggestions for future research are put forward.

3.6.2 Safety

Wang *et al.* [46] built a unified safety supervision system for handling hazardous chemicals, improving the management of dangerous chemical safety.

Zhang *et al.* [47] created a safety audit approach by examining the characteristics of typical hazardous chemicals used to produce polychlorinated biphenyls and the mechanisms behind frequent occurrences. Their method is intended to enhance hazardous chemical safety management.

Deng *et al.* [48] presented a generic approach for avoiding hazardous chemical accidents based on an incident information clustering analysis using K-means clustering. Dangerous chemical accidents were categorized using a K-means clustering technique, which may help field specialists or safety specialists divide many occurrences and provide accident reference categorization. The proposed approach may be utilized to prevent accidents with hazardous chemicals. Developing an unsafe chemical accident prevention information system would improve the security and dependability of hazardous chemical manufacturing, usage, transportation, and storage.

Although it is a shared recognition that safety and security should be integrated for common consideration, and the academic community has made efforts to this end, there still needs to be relevant results that the public can trust. In addition to the two sides using different standards for audit, part of the reason is due to the time gap. Safety is usually considered before the establishment of the system. At the same time, security is primarily a measure or mechanism added after establishing the strategy. In the face of ever-changing attack methods, people often need to add or update some systems, tools, mechanisms, and procedures to ensure security.

4 Discussion

According to the above case studies review, this paper recommends some measures for ICS and related fields.

- Vulnerabilities in ICS can primarily be attributed to outdated software and firmware utilization. Consequently, maintaining the system's current state is of utmost importance.
- Implementing regular password changes and utilizing two-factor authentication are employed to enhance the system's security.
- Accessing the critical system using the USB drive is strictly prohibited unless it has undergone thorough examination by robust antivirus software.
- To enhance communication network protection

in ICS, state-of-the-art detection and prevention methods [49-56] can be implemented in industrial sites.

5 Conclusion

This paper aimed to investigate and integrate the literature on cyber security and safety in the ICS field. This paper examines the methods used to defend against and launch attacks on ICS by ICS-based Purdue Enterprise Reference Architecture (PERA). In addition, this paper classifies the potential security concerns that ICS may face into six domains based on the attack, detect, risk estimation, incident response, protect, and incident prevention. To conclude, we hope that this review article positively impacts academics and manufacturing to guide and motivate researchers and ICS engineers to enhance their existing systems or works by leveraging cyber security and safety mechanisms.

References

[1] K. Stouffer, J. Falco, K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standard and Technology (NIST) special publication, NIST SP 800-82, pp. 16-16, May, 2014.

[2] Barracuda, The state of industrial security in 2022, July, 2022, [Online]. Available: https://assets.barracuda.com/assets/docs/dms/NetSec_Report_The_State_of_IIoT_final.pdf.

[3] H. Xu, W. Yu, D. Griffith, N. Golmie, A survey on industrial internet of things: A cyber-physical systems perspective, *IEEE Access*, Vol. 6, pp. 78238-78259, December, 2018.

[4] C. Alcaraz, S. Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, *International Journal of Critical Infrastructure Protection*, Vol. 8, pp. 53-66, January, 2015.

[5] A. Jindal, A. K. Marnerides, A. Scott, D. Hutchison, Identifying security challenges in renewable energy systems: a wind turbine case study, *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, Phoenix, AZ, USA, 2019, pp. 370-372.

[6] G. S. Aujla, A. Singh, N. Kumar, AdaptFlow: Adaptive flow forwarding scheme for software-defined industrial networks, *IEEE Internet of Things Journal*, Vol. 7, No. 7, pp. 5843-5851, July, 2020.

[7] T. Alladi, V. Chamola, S. Zeadally, Industrial Control Systems: Cyberattack trends and countermeasures, *Computer Communications*, Vol. 155, pp. 1-8, April, 2020.

[8] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, Cybersecurity for industrial control systems: A survey, *Computers & Security*, Vol. 89, Article No. 101677, February, 2020.

[9] D. Ghelani, Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review, *American Journal of Science, Engineering and Technology*, September, 2022. https://doi.org/10.22541/au.166385207.73483369/v1

[10] A. Corallo, M. Lazoi, M. Lezzi, A. Luperto, Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review, *Computers in Industry*, Vol. 137, Article No. 103614, May, 2022.

[11] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future, *Electric Power Systems Research*, Vol. 215, Article No. 108975, February, 2023.

[12] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, P. Burnap, Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review, *ACM Computing Surveys*, Vol. 55, No. 10, pp. 1-36, October, 2023.

[13] M. Kravchik, B. Biggio, A. Shabtai, Poisoning attacks on cyber attack detectors for industrial control systems, *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, Virtual Event, Republic of Korea, 2021, pp. 116-125.

[14] E. Sarker, H, Benkraouda, M. Maniatakos, I came, I saw, I hacked: Automated Generation of Process-independent Attacks for Industrial Control Systems, *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, Taipei, Taiwan, 2020, pp. 744-758.

[15] B. Babu, T. Ijyas, P. Muneer, J. Varghese, Security issues in SCADA based industrial control systems, *Proceeding of International Conference on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia, 2017, pp. 47-51.

[16] J. Jin, Z. Zhao, Y. Wang, Coordination Method of Functional Safety and Cyber Security for Industrial Control Systems, *Proceeding of China Automation Congress*, Beijing, China, 2021, pp. 122-127.

[17] Y. Wang, G. Cui, L. Zhang, H. Li, Research on application of trusted computing 3.0 in industrial control system of nuclear power plant, *Proceeding of International Conference on Communications Software and Networks (ICCSN)*, Chongqing, China, 2020, pp. 297-301.

[18] C. Zhou, B. Hu, Y. Shi, Y. C. Tian, X. Li, Y. Zhao, A unified architectural approach for cyberattack-resilient industrial control systems, *Proceedings of the IEEE*, Vol. 109, No. 4, pp. 517-541, April, 2021.

[19] Y. Mekdad, G. Bernieri, M. Conti, A. E. Fergougui, A Threat Model Method for ICS Malware: the TRISIS Case, *Proceedings of the 18th ACM International Conference on Computing Frontiers*, Virtual Event, Italy, 2021, pp. 221-228.

[20] M. Cheminod, L. Durante, A. Valenzano, Review of security issues in industrial networks, *IEEE Transactions on Industrial Informatics*, Vol. 9, No. 1, pp. 277-293, February, 2013.

[21] R. F. Ali, A. Muneer, P. D. D. Dominic, E. A. A. Ghaleb, A. A. Ashmori, Survey on Cyber Security for Industrial Control Systems, *Proceeding of International Conference on Data Analytics for Business and Industry (ICDABI)*, Sakheer, Bahrain, 2021, pp. 630-634.

[22] S. Zonouz, J. Rrushi, S. McLaughlin, Detecting Industrial Control Malware Using Automated PLC

Code Analytics, *IEEE Security & Privacy*, Vol. 12, No. 6, pp. 40-47, November-December, 2014.

[23] K. Paridari, N. O'Mahony, A. E. D. Mady, R. Chabukswar, M. Boubekeur, H. Sandberg, A Framework for Attack-Resilient Industrial Control Systems: Attack Detection and Controller Reconfiguration, *Proceedings of the IEEE*, Vol. 106, No. 1, pp. 113-128, January, 2018.

[24] Y. Peng, J. Liang, G. Xu, Malware detection method for the industrial control systems, *Proceeding of International Conference on Cloud Computing and Intelligence Systems (CCIS)*, Beijing, China, 2016, pp. 255-259.

[25] A. Nicholson, S. Webber, S. Dyer, T. Patel, H. Janicke, SCADA Security in the Light of Cyber-Warfare, *Computers & Security*, Vol. 31, No. 4, pp. 418-436, June, 2012.

[26] M. Yanpolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, J. Sztipanovits, A language for describing attacks on cyber-physical systems, *International Journal of Critical Infrastructure Protection*, Vol. 8, pp. 40-52, January, 2015.

[27] M. Catelani, L. Ciani, D. Galar, G. Guidi, S. Mutucci, G. Patrizi, FMECA Assessment for Railway Safety-Critical Systems Investigating a New Risk Threshold Method, *IEEE Access*, Vol. 9, pp. 86243-86253, June, 2021.

[28] H. Abdo, M. Kaouk, J. M. Flaus, F. Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis, *Computers & Security*, Vol. 72, pp. 175-195, January, 2018.

[29] P. Joksimovic, G. V. D. Werf, Innovative track behavioural model estimating risk of incidents, *Proceeding of IET Conference on Railway Condition Monitoring and Non-Destructive Testing (RCM)*, Derby, UK, 2011, pp. 1-4.

[30] L. F. Vismari, J. B. C. Junior, An Absolute-Relative Risk Assessment Methodology Approach to Current Safety Critical Systems and its Application to the ADS-B based Air Traffic Control System, *Proceeding of Symposium on Reliable Distributed Systems*, Naples, Italy, 2008, pp. 95-104.

[31] L. F. Cómbita, J. Giraldo, A. A. Cárdenas, N. Quijano, Response and reconfiguration of cyber-physical control systems: A survey, *Proceeding of IEEE Colombian Conference on Automatic Control (CCAC)*, Manizales, Colombia, 2015, pp. 1-6.

[32] C. M. Rondeau, M. A. Temple, J. Lopez, Industrial IoT cross-layer forensic investigation, *Wiley Interdisciplinary Reviews: Forensic Science*, Vol. 1, No. 1, Article No. e1322, January/February, 2019.

[33] A. Ghosh, S. Qin, J. Lee, G. N. Wang, FBMTP: An Automated Fault and Behavioral Anomaly Detection and Isolation Tool for PLC-Controlled Manufacturing Systems, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 47, No. 12, pp. 3397-3417, December, 2017.

[34] T. Spyridopoulos, T. Tryfonas, J. May, Incident analysis & digital forensics in SCADA and industrial control systems, *Proceeding of IET International System Safety Conference incorporating the Cyber Security Conference*, Cardiff, UK, 2013, pp. 1-6.

[35] H. Takagi, T. Morita, M. Matta, H. Moritani, T. Hamaguchi, S. Jing, I. Koshijima, Y. Hashimoto, Strategic security protection for industrial control systems, *Proceeding of 54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, Hangzhou, China, 2015, pp. 986-992.

[36] H. S. Alotaibi, R. Mahjoub, M. Faezipour, An intelligent system to control the operation of tunnels and subways: Application in Makkah and Madina traffic and pedestrian tunnels, *Proceeding of Annual Connecticut Conference on Industrial Electronics, Technology & Automation (CT-IETA)*, Bridgeport, CT, USA, 2016, pp. 1-5.

[37] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, R. Karri, The Cybersecurity Landscape in Industrial Control Systems, *Proceedings of the IEEE*, Vol. 104, No. 5, pp. 1039-1057, May, 2016.

[38] Y. Ren, R. Xie, F. R. Yu, T. Huang, Y. Liu, Potential Identity Resolution Systems for the Industrial Internet of Things: A Survey, *IEEE Communications Surveys & Tutorials*, Vol. 23, No. 1, pp. 391-430, Firstquarter, 2021.

[39] Y. Hou, J. Such, A. Rashid, Understanding security requirements for industrial control system supply chains, *Proceeding of IEEE/ACM International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, Montreal, QC, Canada, 2019, pp. 50-53.

[40] T. Gu, M. Lu, L. Li, Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems, *Proceeding of International Conference on Reliability Systems Engineering (ICRSE)*, Beijing, China, 2015, pp. 1-8.

[41] M. T. Khan, D. Serpanos, H. Shrobe, ARMET: Behavior-based secure and resilient industrial control systems, *Proceedings of the IEEE*, Vol. 106, No. 1, pp. 129-143, January, 2018.

[42] F. Q. Yuan, J. M. Lu, Improved condition monitoring system to protect railway axle bearing safety from electric corrosion, *Proceeding of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Singapore, 2015, pp. 1634-1638.

[43] N. Chaudhry, M. M. Yousaf, M. T. Khan, Security assessment of data management systems for cyber physical system applications, *Journal of Software: Evolution and Process*, Vol. 32, No. 2, Article No. e2241, February, 2020.

[44] X. Lyu, Y. Ding, S. H. Yang, Safety and security risk assessment in cyber-physical systems, *IET Cyber-Physical Systems: Theory & Applications*, Vol. 4, No. 3, pp. 221-232, September, 2019.

[45] M. Zahid, I. Inayat, M. Daneva, Z. Mehmood, Security risks in cyber physical systems—A systematic mapping study, *Journal of Software: Evolution and Process*, Vol. 33, No. 9, Article No. e2346, September, 2021.

[46] X. L. Wang, L. J. Zhao, How to improve the safety management of hazardous chemicals in China-based

on the big data analysis of hazardous Accidents, *Exploration and Free Views*, No. 2, pp. 73-77, February, 2016.
[47] Z. D. Zhang, D. Zhang, Accident analysis and preventive safety risk management of hazardous chemicals in PCB enterprises, *Printed Circuit Information*, Vol. 27, No. 3, pp. 51-59, March, 2019.
[48] F. Deng, W. Gu, W. Zeng, Z. Zhang, F. Wang, Hazardous Chemical Accident Prevention Based on K-Means Clustering Analysis of Incident Information, *IEEE Access*, Vol. 8, pp. 180171-180183, October, 2020.
[49] J. Kim, J. Shin, J. T. Seo, Detection and Blocking Method against DLL Injection Attack Using PEB-LDR of ICS EWS in Smart IoT Environments, *Journal of Internet Technology*, Vol. 23, No. 4, pp. 875-888, July, 2022.
[50] J. Cui, B. Gao, B. Guo, A novel detection and defense mechanism against false data injection attack in smart grids, *IET Generation, Transmission & Distribution*, Vol. 17, No. 20, pp. 4514-4524, October, 2023.
[51] X. Luo, X. Wang, X. Pan, X. Guan, Detection and isolation of false data injection attack for smart grids via unknown input observers, *IET Generation, Transmission & Distribution*, Vol. 13, No. 8, pp. 1277-1286, April, 2019.
[52] M. Dehghani, A. Kavousi-Fard, M. Dabbaghjamanesh, O. Avatefipour, Deep learning based method for false data injection attack detection in AC smart islands, *IET Generation, Transmission & Distribution*, Vol. 14, No. 24, pp. 5756-5765, December, 2020.
[53] W. Fu, Y. Yan, Y. Chen, Z. Wang, D. Zhu, L. Jin, Temporal false data injection attack and detection on cyber-physical power system based on deep reinforcement learning, *IET Smart Grid*, Vol. 7, No. 1, pp. 78-88, February, 2024.
[54] J. C. Huang, G. Q. Zeng, G. G. Geng, J. Weng, K. D. Lu, SOPA-GA-CNN: Synchronous optimisation of parameters and architectures by genetic algorithms with convolutional neural network blocks for securing Industrial Internet-of-Things, *IET Cyber-systems and Robotics*, Vol. 5, No. 1, Article No. e12085, March, 2023.
[55] Y. Kim, S. Hakak, A. Ghorbani, Smart grid security: Attacks and defence techniques, *IET Smart Grid*, Vol. 6, No. 2, pp. 103-123, April, 2023.
[56] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, S. Zonouz, Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems, *IET Cyber-Physical Systems: Theory & Applications*, Vol. 6, No. 4, pp. 208-227, December, 2021.

Biographies

Yi-Wei Ma is an associate professor at Department of Electrical Engineering in National Taiwan University of Science and Technology. His research interests include Internet of Things, Cloud Computing, and Future Network.

Yi-Hao Tu received his B.S. and M.S. degrees from the Department of Computer Science and Information Engineering, and the Department of Information Technology and Application at National Quemoy University, Kinmen, Taiwan, in 2020 and 2022, respectively. He is currently a doctoral student at Department of Electrical Engineering at National Taiwan University of Science and Technology, Taipei, Taiwan. His current research interests include wireless networks, software defined networks, and reinforcement learning.

Chia-Wei Tsou received his B.S. and M.S. degrees from the Department of Electrical Engineering at National Taiwan University of Science and Technology, in 2021 and 2023, respectively. His research interests include the industrial control system.

Yen-Neng Chiang received his B.S. and M.S. degrees from the Department of Electrical Engineering at Chung Yuan Christian University and National Taiwan University of Science and Technology, Taiwan, in 2021 and 2023, respectively. His research interests include the Internet of Things, software engineering development, and network technology research and development.

Jiann-Liang Chen Prof. Chen received his Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan, in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering of National Dong Hwa University, where he is a professor and Vice Dean of Science and Engineering College. Prof. Chen joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a Distinguished Professor and Dean. His research interests cellular mobility management, cybersecurity, personal communication systems, and Internet of Things.