Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P539-cd

Critical Convergence for enhanced safety: A Literature Review on Integrated Cybersecurity Strategies for Information Technology and Operational Technology Systems within Critical Infrastructure

Fabien Sechi

Information Communication and Technology Department, University of Agder & Risk and Security Department, Institute for Energy Technology, Norway. E-mail: fesechi@uia.no & fabien.sechi@ife.no

Cyberattacks targeting critical infrastructure highlight that both information technology systems (IT) and industrial control systems (ICS) are vulnerable to cyber security events and that cyberattacks targeting IT can have effects on ICS and vice versa. These events indicate a need for an improved understanding of the similarities and differences between IT security and ICS/operational technology systems (OT) security. This paper explores the technological aspects of tools, methods, and approaches used to secure IT and OT systems, and the crisis decision-making processes related to management, strategy, organization, and governance. The methodology of this exploratory study is a literature methods approach using PRISMA methods that gather academic articles from the "Web Of Science" database. We discuss fifteen papers on IT and OT systems similarities in terms of security needs, and in terms of significant differences between the two that must be considered. The paper explores the trade-offs between applying IT-focused cyber security tools and approaches to ICS and OT. Results are disseminated in terms of two main research questions that are RQA) What are the similarities and differences between IT and OT security? And RQB), how can these disparities be effectively addressed to protect these systems from cyberattacks? We conclude by outlining future research directions aimed at expanding on the findings of research questions A and B.

Keywords: IT, OT/ICS, security, cyber crisis management, critical infrastructure.

1. Introduction

High-profile critical infrastructure companies have been targeted by high-impact cyber-physical attacks directed at information technology (IT) and operational technology (OT) systems. Such cyberattacks include:

- the Ukraine power grid attack in December 2015 (Dark Readings), where a hybrid IT and industrial control systems (ICS) attack tripped breakers in the grid.
- the Norwegian aluminium company in March 2019 (Hydro). suffered a global cyberattack causing operational challenges and financial losses,
- the Colonial Pipeline in May 2021 (US Department of Energy) where IT malware led to a management decision to stop the ICS.
- the attack on several European ports in February 2022 (Euronews) which prevented these ports to process load operations controlled by ICS,

The publications and reports addressing these cyberattacks reveal that there is still a lack of perfect understanding regarding the scope of IT and OT security, emphasizing the need for further improvement in comprehending their similarities and differences. Enhancing this understanding is crucial to strengthening security measures and reducing the likelihood of such attacks.

Security needs and priorities are context-dependent, indicating that diverse situations require distinct security measures and considerations. IT systems primarily concentrate on protecting data and information, whereas OT systems focus on controlling and monitoring physical processes. Consequently, comprehending these differences, including variations in architectures, protocols, and communication standards, is crucial for developing targeted and effective security strategies. Applying standard cybersecurity tools and approaches may not be as effective for OT systems compared to IT systems. For example, patch management in IT is streamlined and regularly deploy, while in OT, the complexity increases due to legacy equipment and the need for uninterrupted operation.

Furthermore, as the interconnectivity between IT and OT networks continues to grow, it becomes even more imperative to grasp the intricacies of their coexistence and interdependencies. By recognizing the increasing integration of these systems, we can better

anticipate potential vulnerabilities and develop robust security strategies that effectively protect critical infrastructure from cyber-physical threats. With the growing trend of digitalization, which includes cloud computing, automation through Industry 4.0, the utilization of digital twins, and the implementation of the Industrial Internet of Things (IIoT), the interconnection between IT and OT systems is becoming increasingly prevalent. The growing interconnectivity between IT and OT systems means that cyberattacks targeting one can have cascading effects on the other, leading to disruptions in critical processes and infrastructure. A holistic approach to cybersecurity, encompassing both IT and OT domains, is essential for protecting interconnected systems and mitigating the impact of cyber-physical attacks.

Compliance with security and safety regulations and standards is crucial to address the unique requirements of both IT and OT systems and develop effective security strategies. For example, OT systems often need to adhere to industry-specific safety standards like IEC 62443, while IT systems must comply with more general security standards such as ISO/IEC 27001. Understanding these compliance requirements is essential for ensuring good security practices. Cyberattacks on either system can have significant consequences in terms of safety and security. Therefore, adopting an integrated IT-OT safety-and-security approach, considering the specific requirements and constraints of each system in conjunction with regulations, is imperative. This comprehensive approach enables the development of effective security measures to mitigate risks and ensure the resilience of critical infrastructure.

This study aims to investigate the technological aspects of IT and OT security, to enhance an understanding of their similarities and differences. The ultimate objective is to develop effective decision-making strategies for both types of systems that will improve their security.

To achieve this aim, the following research questions and objectives have been established:

Research Question A - RQA)

How do IT and OT systems differ in their technology (architecture, protocols, regulatory frameworks, and communication standards), and what are the trade-offs between implementing IT-focused and OT-focused security strategies?

The objective of this question is to detail the technological disparities and similarities between IT and OT systems, identify their unique security needs and challenges, and explore the implications of applying distinct security approaches to each.

Research Question B - RQB)

How can the disparities we identify be effectively addressed to protect IT and OT systems from cyberattacks?

The objectives of this question are to examine and discuss non-technological crisis decision-making processes related to IT and OT security, such as management, strategy, organization, and culture and governance, to understand their impact on security outcomes. With this research, we aim to contribute to the advancement of knowledge in the field of IT and OT security and its implication on safety and to provide insights that can be used to enhance the security and safety of both types of systems.

2. Methods

A literature review was conducted. While not following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method to its full extent, such as including a flowchart, or arguing each point of this method. PRISMA principles were partially adopted to facilitate a thorough examination of academic literature. This approach is an efficient choice given the constraints of time and being a sole researcher. The review was conducted, aiming to answer research questions A and B, as described in the following criteria:

Eligibility: Inclusion in the review was open to all types of studies provided they were written in English, had a focus on IT and OT security in critical infrastructure, contained at least two pages of content or more than 2000 words, and were relevant to the research objectives. Relevance was determined by whether a paper provided information on the technological or non-technological aspects of IT and OT security. No specific types of research methods were excluded, broadening the scope for diverse insights.

Search strategy: A systematic search was conducted involving 23 search queries run on the Web of Science database, using keywords related to IT security, OT security, and critical infrastructure. The process and outcomes of these searches are presented in Table 1.

Table 1. Search process including criteria.

#	Search Query	Results
1	IT security	199274
2	information technology security	30524
3	#1 OR #2	214967
4	OT security	481
5	operational technology security	2499
6	#4 OR #5	2863
7	industrial control systems	54000
8	ICS	29209
9	#7 OR #8	82233
10	security measures	49319
11	security culture	8071
12	security management	76688
13	security strategies	49377
14	security frameworks	55566
15	security technologies	84030
16	#10 OR #11 OR #12 OR #13 OR #14 OR #15	239827
17	case studies	2914982
18	real-world	284442
19	#17 OR #18 OR *	4061347
20	cyber-physical attacks	4689
21	cyber attacks	17482
22	#20 OR #21	17482
23	cybersecurity	10950
24	#3 AND #6 AND #9 AND #16 AND #19 AND #22 AND #23	15

**(Critical Infrastructures) OR (CI) OR (Chemical Sector) OR (Commercial Facilities Sector) OR (Communications Sector) OR (Critical Manufacturing Sector) OR (Dams Sector) OR (Defense Industrial Base Sector) OR (Emergency Services Sector) OR (Energy Sector) OR (Financial Services Sector) OR (Food and Agriculture Sector) OR (Government Facilities Sector) OR (Healthcare and Public Health Sector) OR (Information Technology Sector) OR (Nuclear Reactors, Materials, and Waste Sector) OR (Transportation Systems Sector) OR (Water and Wastewater Sector*)

The selection process: involved an initial screening of the search results based on the aforementioned eligibility criteria, which was conducted on Mon Apr 17 2023 21:46:28 GMT+0200 (Summer Oslo).

Quality assessment (QA): Studies were subjected to a quality assessment, ensuring that each paper included an introduction (or a short background explanation if missing in the introduction), a methodology, and a discussion section that included a short conclusion or a full conclusion. Moreover, each paper was required to have a minimum of two references. Any studies that failed to meet these criteria were excluded from the review. Therefore, Table 2 show the list of paper included for the discussion.

Table 2. ID and authors (15 results)

ID	Authors
A	Kapellmann, D
B	Evripidou, S
C	Rashid, SMZU
D	Shrivastava, S
E	Marino, DL
F	Alghassab, M
G	Wan, M
H	Boeding, M
I	Malatji, M
J	Fraile, F
K	Makrakis, GM
L	Ashley, TD
M	Iaiani, M
N	Phillips, T
O	Cervini, J

Data extraction process: This consisted of summarizing the key findings with my own interpretation from each paper related to the research questions and objectives. A standardized Microsoft Excel form was utilized to extract data from the full text of the included studies. The extracted data was then synthesized, analysed, and presented in the Results section.

3. Broad Technological analysis and aspects

My base technological analysis:

It suggests that the field's literature, originating as recently as 2018 (J), has seen a substantial increase, doubling in the past two years. Main research areas are computer science, electronic engineering, and telecommunication.

The predominant themes discernible from the analysed texts are cybersecurity and industrial control systems. Most frequent keywords including "security" (13), "cybersecurity" (12), "cyber" (10), "systems", "control", and "industrial" (8), indicate a strong thematic lean towards these domains. There is a distinct emphasis on critical infrastructure challenges and their respective solutions, signified by keywords

like "infrastructure" (7), "ICS" (6), "attack" (4), and "OT" (3). Other relevant terms, albeit less frequent, include "SCADA", "fuzzy" (2), "IIoT", "gamification", and "vulnerabilities" (each mentioned once), hinting at specific methodologies and strategies explored within the field.

Based on the research questions and objectives of these papers, from conferences, journals and books, I highlight six main areas that together focus on enhancing the cybersecurity resilience of critical infrastructure, particularly in industrial control systems (ICS) followed by the objectives:

Identifying vulnerabilities and threats to ICS, the objectives include assessing the feasibility and effectiveness of information-sharing platforms (A), developing a cybersecurity capability framework for critical infrastructure - CI operators (I) and advancing the ICS cybersecurity workforce through network defence training games (L).

Cybersecurity resilience and defence for critical infrastructure, the objectives include addressing cybersecurity risks in industrial control systems in the context of Industry 4.0 (D), evaluating various cybersecurity risks in ICS and their effects on availability, integrity, and confidentiality (H), and identifying the cybersecurity capabilities that critical infrastructure operators must have to attain good cybersecurity resilience (I).

Cybersecurity training and methodology, the objective is to develop effective training methods and systematic qualitative methodologies to support the identification of possible security events affecting the operability and/or system integrity of a process plant such as advancing the ICS cybersecurity workforce through network defence training games (L) and developing a methodology to identify security events resulting from malicious manipulations of Basic Process Control System - BPCS and Safety Instrumented System - SIS systems in industrial facilities (M).

On IIoT and security mechanisms, the objective is to design trustworthy gateways to provide security mechanisms between operational systems and information systems such as presenting the Device Drivers security architecture and evaluating its security countermeasures (J).

The threat landscape and security mechanisms for ICS/CI, objectives include assessing the threat landscape for internet-facing ICS (C), presenting the ICS Resilient Security Technology - IREST sensor for detecting cyber and physical anomalies (E), analysing uncontrollable cyber threats and proposing security mechanisms for ICS (G).

Literature review and technical evaluation for ICS/CI, the objectives include reviewing security culture literature and identifying gaps for future research (B), exploring objectives, tactics, and strategies involved in conducting international cyber-physical exercises (D), presenting the Device Drivers' security architecture, and evaluating its security countermeasures (J).

The technological aspects:

These are mentioned in the provided examples highlight the importance of cybersecurity in various technological domains, particularly in the areas of ICS, OT, and Cyber physical systems - CPS. Based on the technological aspects of the paper, here is a summary by family or group of technologies:

ICS and OT Security include (A, B, E, F, G, H, I, K, M, and O). They all relate to the security challenges, vulnerabilities, and risks associated with ICS and OT systems and the need to safeguard them against cyber-physical attacks and other threats.

CPS: include (C and D). They relate to developing them and testing them and evaluating their defense capabilities for defending national critical infrastructure.

IIoT includes (J), which focuses on the use of industrial IoT technology in manufacturing industries.

Cybersecurity training and education include L, which discusses the use of game-based learning and a cybersecurity training platform to train facility operators responsible for critical services in defending their systems against cyberattacks: In (A), Stuxnet and Triton are notable cyberattacks that exploited vulnerabilities in IT and OT assets. (C) describes the deployment of a T-pot honeypot in an Amazon Web Services Elastic Compute Cloud - AWS EC2 instance across six different regions collecting threat intelligence data. (E) highlights the testing of the IREST sensor under different cyber-physical scenarios using the Idaho CPS SCADA Cybersecurity - ISAAC testbed. In (N), a cyberattack targets controller proportional-integral-derivative gain values in a constant

setpoint control system. Lastly, (O) refers to an attempted cyberattack on a water treatment plant in Oldsmar, Florida, in which the attacker tried to manipulate sodium hydroxide levels.

4. Non-technological aspects

The managerial development of robust cybersecurity policies and procedures is essential to protect against cyber threats in any organization. This involves identifying, assessing, and mitigating cybersecurity risks (A, B, F, L), and developing a security culture (B) that prioritizes cybersecurity policies and controls (L). Adequate resources should be allocated to protect systems, including providing necessary resources, training, and guidance to employees (B) and developing effective management strategies to protect water treatment systems despite limited budgets (O). To integrate modern technologies while addressing cybersecurity risks, organizations must address challenges of digital evolution and new attack surfaces (C), design trustworthy gateways between operational and information technology (J), and integrate modern IT elements into monolithic OT architectures while addressing cybersecurity risks (K). Facilitating operational planning and execution includes conducting international cyber-physical exercises -CPX to improve defence capabilities (D), implementing technologies such as IREST sensors to ensure accurate detection (E), and managing cybersecurity in IT and OT systems to prevent intentional acts of manipulation of the BPCS and SIS systems (M).

The cultural development of a cybersecurity culture within organizations is critical for addressing cyber threats (A, B, C, E, G, I, J, K, L, N, O). This involves promoting security awareness, education, best practices, and prioritizing cybersecurity. Cross-disciplinary collaboration between stakeholders is essential for conducting successful cybersecurity preparedness exercises (D). A culture of reliability and accountability is necessary to maintain the availability rate of industrial control systems (F). To address unique challenges presented by OT systems, a cybersecurity culture must prioritize both OT and IT cybersecurity efforts (H) and prevent intentional manipulation of BPCS and SIS systems, especially in the front-end design phase and security review of operating plants (M).

The organizational and coordinated efforts in managing vulnerabilities in organizational systems and critical infrastructure are crucial (A, D, O). Effective coordination and collaboration between stakeholders is essential to enhancing the security of industrial control systems (B, C), designing and operationalizing cybersecurity controls (I, K), implementing security countermeasures in supply chain security (J), and defending against cyberattacks on critical infrastructure (E, F, L, M, N). Effective coordination and collaboration between academia and industry, as well as between operational technology and information technology systems, is necessary (G, H).

The strategical critical infrastructure protection requires balancing security and collaboration with stakeholders (A), global coordination for infrastructure defence (D), and developing an integrated cybersecurity capability framework (I). Developing a security culture (B), using honeypots for observing attack methods (C), and fuzzy-based methods to estimate cybersecurity (F) are critical for industrial control system (ICS) security. Implementing security mechanisms at different system layers (J) and OT network security mechanisms (L) is also essential. Developing a scalable framework for research (E), overcoming intrinsic vulnerabilities in networked control systems (G), applying contemporary security controls promptly (K), and developing a systematic methodology (M) are essential for CPS security research. Finally, mitigating cyber warfare attack-surface paradigms targeting critical infrastructure systems (O) is crucial in addressing emerging threats.

Crisis decision-making: The analysis of the reviewed papers highlights the emphasis on cyber crisis management. Several papers specifically discuss managing cyber incidents or attacks (A, C, E, G, H, J, L, M, N, and O). Conversely, a few papers discuss topics related to cyber incidents or attacks, but without a particular focus on crisis management (B, D, F, K).

5. Discussion and future research direction for critical infrastructure

Historically ESREL papers published have typically a bottom-up approach notably with the use of a risk model whereas I posit a top-down approach that synthesises insights from the technological facets of cybersecurity with its non-

technological dimensions. Organizations can then cultivate a comprehensive cybersecurity culture that emphasizes the development of efficacious strategies for risk identification, mitigation, and policy prioritization, consequently augmenting the safety of critical infrastructure.

RQA

Literature Review and Technical Evaluation for ICS/CI

This underscores the crucial role that ongoing research and development initiatives play in advancing the field. Based on this analysis, the following suggestions are understood:

- Conduct comprehensive literature reviews to identify knowledge gaps and areas of opportunity for further research in ICS/CI security.
- Employ rigorous technical evaluation methods, such as testing, simulation, and experimentation, to assess the effectiveness of proposed security measures and solutions in real-world ICS/CI environments.
- Foster interdisciplinary collaboration between researchers, practitioners, and policymakers to promote the development and implementation of innovative security solutions that address the unique challenges of ICS/CI.
- Encourage the publication and dissemination of ICS/CI security research findings through conferences, journals, and other channels to facilitate knowledge sharing and promote best practices in the field.

Similarities and Differences between IT and OT Security

These are analysed in terms of their technological aspects, such as architectures, protocols, regulatory frameworks, and communication standards. Both IT and OT systems require protection against cyber threats, and both types of systems utilize security mechanisms such as firewalls, encryption, and authentication. However, there are notable differences between the two, including:

- Priorities: IT security prioritizes the confidentiality, integrity, and availability (CIA) of data, whereas OT security focuses on the safety, availability, and integrity of processes and systems.
- Architectures: IT systems are typically more centralized and reliant on standard hardware and software, while OT systems often use specialized and proprietary hardware and software designed for specific industrial processes.
- Protocols: IT systems use common internet protocols such as TCP/IP, while OT systems use industrial protocols specific to their domain, such as Modbus, DNP3, and IEC 61850.
- Regulatory frameworks: IT systems are subject to general data protection and privacy regulations, while OT systems are often subject to industry-specific regulations focused on safety and reliability.
- Communication standards: IT systems use common communication standards like Ethernet and Wi-Fi, while OT systems often use specialized communication methods designed for industrial environments, such as Fieldbus and WirelessHART.

RQB

Threat Landscape, Security Mechanisms, and ICS and IIoT Integration in CI

The evolving threat landscape for ICS and IIoT integration in CI demands continuous efforts to develop and implement effective security mechanisms that protect these systems from cyberattacks. Our analysis suggests the following recommendations to address the challenges in ICS, IIoT, and CI security:

- Conduct regular threat assessments to identify and prioritize potential risks and vulnerabilities in ICS, IIoT, and CI environments.
- Implement layered security measures that address both physical and cyber threats, including network segmentation, intrusion detection and prevention systems, access control mechanisms, and end-to-end encryption for data transmitted between IIoT devices, control systems, and cloud services.
- Design and implement secure IIoT architectures that consider the unique requirements of industrial environments, such as real-time data processing, remote monitoring, and control.
- Develop and maintain incident response plans that outline procedures for detecting, containing, and mitigating cyberattacks on ICS, IIoT, and CI systems.
- Employ strong authentication mechanisms to protect access to IIoT devices and control systems.
- Regularly assess and update security measures to address emerging threats and

vulnerabilities, including those related to device firmware, communication protocols, and data storage.

- Encourage information sharing and collaboration between ICS, IIoT, and CI stakeholders, including industry, government, and academia, to facilitate the development of effective security measures and best practices.
- Foster collaboration between IIoT device manufacturers, industrial organizations, and cybersecurity experts to develop and share best practices for securing IIoT systems.

Integrated Decision-Making Strategies for IT and OT Security

To effectively address the trade-offs between IT-focused and OT-focused security and safety strategies, decision-makers should adopt an integrated approach that considers the unique requirements and challenges associated with each domain.

- Develop a holistic understanding of both IT and OT security requirements, considering the unique priorities and challenges associated with each type of system.
- Establish cross-disciplinary collaboration between IT and OT teams to promote a unified approach to security that addresses the needs of both domains.
- Implement security controls and practices tailored to the specific requirements of IT and OT systems, considering the unique protocols, architectures, and communication standards.
- Foster a strong security culture that prioritizes the protection of both IT and OT systems, emphasizing the importance of security awareness, education, and best practices.
- Develop and implement robust cybersecurity policies and procedures that consider the unique challenges and requirements of both IT and OT systems.
- Encourage effective communication and coordination between IT and OT teams, as well as between internal and external stakeholders, to ensure a comprehensive and coordinated approach to security.
- Regularly assess and update security policies, procedures, technologies, and non-technological aspects, such as management strategies, organizational structure, and governance, to address emerging threats and vulnerabilities in both IT and OT environments.

Threat to validity: As a measure to improve the transparency and objectivity of the selection and QA processes, future studies could involve a second reviewer or a team of reviewers who can independently assess the eligibility and quality of the studies. Additionally, documenting the data extraction process more explicitly could enhance the robustness of the methodology. This can be achieved by including a detailed description of the variables of interest, the process used to extract the data, and any tools or software used to manage the data. Acknowledging any discrepancies or challenges encountered during the process, and the steps taken to overcome them, could further improve the transparency of the study.

Future Research Directions for IT and OT Security in CI

Based on the analysis, I suggest the following future research directions to advance knowledge in IT and OT security by prolonging research questions.

RQA: Investigate the impact of emerging technologies, such as artificial intelligence, machine learning, and quantum computing, on IT and OT security, and explore potential applications for enhancing the protection of these systems.

Explore innovative security architectures and mechanisms that can better address the unique requirements of IT and OT systems, particularly in the context of converging IT/OT environments. Assess the effectiveness of existing regulatory frameworks and industry standards for IT and OT security and identify opportunities for improvement and harmonization to better protect these systems.

RQB: Examine the role of human factors in IT and OT security, including the influence of organizational culture, decision-making processes, and individual behaviours on security outcomes.

References

U.S. Department of Energy (2021). Colonial Pipeline Cyber Incident. Retrieved January 30, 2023, from https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

Hydro (2019). "Cyber Attack." Retrieved January 30, 2023, from https://www.hydro.com/en/media/on-the-agenda/cyber-attack/.

Euronews (2022). Oil terminals disrupted after European ports hit by cyberattack. Retrieved

January 30, 2023, from https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack.

DarkReading (2016). Lessons From the Ukraine Electric Grid Hack. Retrieved January 30, 2023, from https://www.darkreading.com/vulnerabilities-threats/lessons-from-the-ukraine-electric-grid-hack.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974. doi: 10.1016/j.cose.2022.102974.

Garimella, P. K. (2018). IT-OT Integration Challenges in Utilities. In 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS) (pp. 199-204). Kathmandu, Nepal. doi: 10.1109/CCCS.2018.8586807.

Alghassab, Mohammed. 2022. 'Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector'. Energies 15 (1): 218. doi:10.3390/en15010218.

Ashley, Travis D., Roger Kwon, Sri Nikhil Gupta Gourisetti, Charalampos Katsis, Christopher A. Bonebrake, and Paul A. Boyd. 2022. 'Gamification of Cybersecurity for Workforce Development in Critical Infrastructure'. Ieee Access 10: 112487–501. doi:10.1109/ACCESS.2022.3216711.

Boeding, Matthew, Kelly Boswell, Michael Hempel, Hamid Sharif, Juan Lopez, and Kalyan Perumalla. 2022. 'Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid'. Energies 15 (22): 8692. doi:10.3390/en15228692.

Cervini, James, Aviel Rubin, and Lanier Watkins. 2022. 'Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack'. Proceedings of the 17th International Conference on Cyber Warfare and Security (Iccws 2022), 19–25.

Evripidou, Stefanos, Uchenna D. Ani, Jeremy D. Mck Watson, and Stephen Hailes. 2022. 'Security Culture in Industrial Control Systems Organisations: A Literature Review'. Edited by N. Clarke and S. Furnell. Human Aspects of Information Security and Assurance, Haisa 2022 658: 133–46.doi:10.1007/978-3-031-12172-2_11.

Fraile, Francisco, Takuya Tagawa, Raul Poler, and Angel Ortiz. 2018. 'Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems'. IEEE Internet of Things Journal 5 (6): 4506–14. doi:10.1109/JIOT.2018.2832041.

Iaiani, Matteo, Alessandro Tugnoli, Paolo Macini, and Valerio Cozzani. 2021. 'Outage and Asset Damage Triggered by Malicious Manipulation of the Control System in Process Plants'. Reliability Engineering & System Safety 213 (September): 107685. doi:10.1016/j.ress.2021.107685.

Kapellmann, Daniel, and Rhyner Washburn. 2019. 'Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure'. Edited by T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky. 2019 11th International Conference on Cyber Conflict (Cycon): Silent Battle, 37–59.

Makrakis, Georgios Michail, Constantinos Kolias, Georgios Kambourakis, Craig Rieger, and Jacob Benjamin. 2021. 'Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents'. IEEE Access 9: 165295–325. doi:10.1109/ACCESS.2021.3133348.

Malatji, Masike, Annlize L. Marnewick, and Sune Von Solms. 2022. 'Cybersecurity Capabilities for Critical Infrastructure Resilience'. Information and Computer Security 30 (2): 255–79. doi:10.1108/ICS-06-2021-0091.

Marino, Daniel L., Chathurika S. Wickramasinghe, Kasun Amarasinghe, Hari Challa, Philip Richardson, Ananth A. Jillepalli, Brian K. Johnson, Craig Rieger, and Milos Manic. 2019. 'Cyber and Physical Anomaly Detection in Smart-Grids'. 2019 Resilience Week (Rws), 187–93.

Phillips, Tyler, Hoda Mehrpouyan, John Gardner, and Stephen J. Reese. 2019. 'A Covert System Identification Attack on Constant Setpoint Control Systems'. 2019 Seventh International Symposium on Computing and Networking Workshops (Candarw 2019), 367–73. doi:10.1109/CANDARW.2019.00070.

Rashid, S. M. Zia Ur, Ashfaqul Haq, Sayed Tanimun Hasan, Md Hasan Furhad, Mohiuddin Ahmed, and Abu S. S. M. Barkat Ullah. 2022. 'Faking Smart Industry: A Honeypot-Driven Approach for Exploring Cyber Security Threat Landscape'. Edited by H. Jin, C. Liu, A. S. K. Pathan, Z. M. Fadlullah, and S. Choudhury. Cognitive Radio Oriented Wireless Networks and Wireless Internet 427: 307–24. doi:10.1007/978-3-030-98002-3_23.

Shrivastava, Siddhant, Francisco Furtado, Mark Goh, and Aditya Mathur. 2022. 'The Design of Cyber-Physica Exercises (CPXs)'. Edited by T. Jancarkova, G. Visky, and I. Winther. 2022 14th International Conference on Cyber Conflict: Keep Moving (Cycon), 347–65.

Wan, Ming, Jiawei Li, Ying Liu, Jianming Zhao, and Jiushuang Wang. 2021. 'Characteristic Insights on Industrial Cyber Security and Popular Defense Mechanisms'. China Communications 18 (1): 130–50.