Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4283-cd

Industrial Cybersecurity: Current Trends and Challenges

Ravdeep Kour

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: ravdeep.kour@ltu.se

Ramin Karim
Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: ramin.karim@ltu.se

Amit Patwardhan

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: amit.patwardhan@ltu.se

Naveen Venkatesh

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: naveen.venkatesh@associated.ltu.se

Mohammed Amin Adoul
Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: mohammed.amin.adoul@associated.ltu.se

Abstract: Industrial cybersecurity has become a critical concern in today's interconnected world, as critical infrastructure systems increasingly rely on digital technologies. This paper explores the unique challenges and opportunities presented by industrial cybersecurity, highlighting the need for enhanced cybersecurity measures. The paper discusses the potential consequences of cyberattacks on industrial systems, including disruptions to critical services, economic losses, and even physical harm. To address these challenges, this paper discusses cybersecurity initiatives, standards, guidelines, directives, and acts that can provide a comprehensive framework for cybersecurity and AI governance. A systematic literature review has been conducted in this paper using Scopus and Google Scholar, which provide the foundation for identifying relevant publications. These publications show key trends and themes in industrial cybersecurity research, including the growing importance of education and training, as well as cybersecurity risk assessment and mitigation.

Keywords: Industrial Cybersecurity, operational technology, cyberattack, framework.

1. Introduction

Industry 5.0 implies a significant evolution from previous industrial revolutions. It prioritises human-centric, sustainable, and resilient approaches within the industrial sector. Building upon the advancements of Industry 4.0, it integrates emerging technologies to create a more efficient, flexible, and environmentally friendly industrial landscape. In 2021, the European Commission published the document “Industry 5.0: Towards a Sustainable, Human-centric, and Resilient European Industry", encouraging industries to re-think their positions and roles in society (Breque, De Nul, and Petridis 2021). Industry 5.0 involves various enabling technologies that facilitate digital transitions for asset management, including Artificial Intelligence (AI), the Industrial Internet of Things (IIoT), big data, cloud/edge/fog computing, Virtual Reality (VR), Augmented Reality (AR), extended Reality (XR), blockchains, digital twins, Brain-Computer Interfaces (BCI), and so on.

The effective utilisation of these enabling technologies within Industrial contexts needs more advanced software and hardware with a

wider range of interfaces. These interfaces require new frameworks, concepts, and architectures to ensure the industrial system's resilience against industrial cybersecurity challenges, including a lack of proactive measures, a lack of skill, a limited holistic perspective, and the obsolescence of safety systems in the face of evolving cyber threats (Kour et al. 2023). This requires immediate attention towards the safety and security of industrial systems.

History has shown how cyberattacks have affected many IT (Information Technology) and OT (Operational Technology) systems. IT systems manage information and communication, while OT systems control and monitor physical devices and processes in industrial settings. In this paper, we will focus on OT systems. Starting with the most known cyberattack called Stuxnet, a computer worm that infected computer networks of at least 14 industrial sites and switched off safety devices in Iran's nuclear facilities in 2010 (Langner 2011). Then, in another incident in Florida's 2021 water plant attack, an attacker attempted to increase the sodium hydroxide levels in the water supply (Cervini, Rubin, and Watkins 2022). However, a vigilant operator detected the intrusion and prevented any harm. Moreover, a list of some of the occurrences of cyberattacks that happened in the past in many industries like water supply, mining, railways, aviation, energy, and IT services has been provided by (Kour et al. 2024)The impacts of these cyberattacks include system failures, damage to organisational reputations, monetary losses, compromise of data accuracy, and risk to human safety.

Many initiatives have been taken to protect the data and industrial systems from these cyberattacks. These include:

- NIST SP 800-82r3- Guide to Operational Technology Security (Stouffer et al. 2023)
- European Union AI Act (EU AI Act 2023)
- ISO/IEC 27032:2023; Cybersecurity — Guidelines for Internet security (ISO/IEC 27032:2023 2023)
- Cyber Resilient Act (Europa 2022)
- NIS2 Directive (European Union 2022)
- Digital Operational Resilience Act (DORA 2022)
- European Commission Guidelines for Trustworthy AI (EU 2019)
- ISO/IEC 27001 (Information Security Management Systems) (ISO/IEC 27000:2018(en) 2018)
- Security for industrial automation and control systems (ISA/IEC 2018)
- GDPR (General Data Protection Regulation) (Regulation 2016)
- NIST Cybersecurity Framework (NIST 2014)

The EU AI Act aims to regulate AI systems based on their risk level, while the NIS2 Directive and Cyber Resilience Act enhance cybersecurity measures for critical infrastructure. DORA mandates robust ICT (Information and communications technology) risk management for the financial sector, including annual resilience testing and third-party risk assessments, by January 2025. The GDPR and NIST Cybersecurity Framework address data protection and risk management principles. Standards like ISO/IEC 27001, ISO/IEC 27032, and ISA/IEC 62443 provide specific guidance for information security management, internet security, and industrial control systems. Finally, the European Commission Guidelines for Trustworthy AI offer a framework for developing and deploying AI systems ethically and responsibly.

This collection of standards, guidelines, directives, and acts needs to be integrated together to provide a comprehensive framework for cybersecurity and AI governance. Thus, by implementing industrial cybersecurity measures within this comprehensive framework, industries can protect their critical assets, ensure business continuity, and mitigate the cybersecurity risks associated with Information Technology (IT) and Operational Technology (OT). To establish a foundation, this paper identifies and discusses current trends and challenges in industrial cybersecurity through a literature review.

2. Research Methodology

This research paper employs a systematic literature review methodology. Eligibility criteria for inclusion were publication within the last 2 decades, availability of full-text articles in Scopus and Google Scholar databases, peer-reviewed status, and English language availability. A search string ("Industrial Cybersecurity" OR ("Industrial Cyber security") within the titles of the paper was used to identify relevant literature. A total of 31

literature have been retrieved from the Scopus database. The authors of this paper then independently screened the retrieved articles, excluding those considered irrelevant and not following eligibility criteria. This process resulted in the selection of 18 relevant papers for further analysis.

3. Results and discussions

3.1. Industrial Cybersecurity Trend

All the selected literature has been analysed to conclude about the current state of the research in industrial cybersecurity. The authors of this paper have bifurcated the literature to show the current trends of industrial cybersecurity and how it has evolved over time in this subject. Figure 1 provides a trend of industrial cybersecurity, and Table 1 presents a summary of the reviewed literature. Figure 1, Top-Left shows the count of literature by year in a bar chart, indicating a peak in 2023 with 7 publications. Additionally, it provides valuable insights into the trends and themes within industrial cybersecurity research, highlighting the growing importance of education and training, as well as cybersecurity risk assessment and mitigation. The pie chart on the bottom-left breaks down the publication types, with conference papers being the most common (55.56%), followed by articles (38.89%) and book chapters (5.56%). The bar chart on the top-right shows the count of titles by country, with Spain having the highest number. Below, a word cloud highlights the most frequent keywords, emphasising concepts like "cybersecurity," "industrial," "control," and "systems." This suggests a focus on the security of industrial control systems, likely within the context of operational technology (OT).

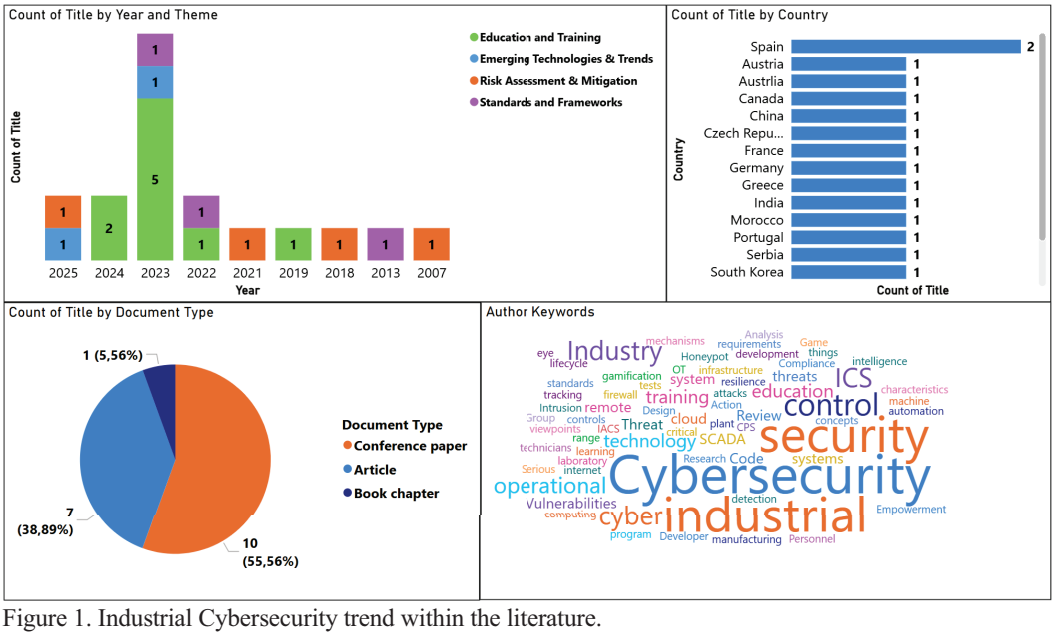

Figure 1. Industrial Cybersecurity trend within the literature.

Table 1. Summary of literature showing various tools/technologies/standards used within Industrial cybersecurity along with themes.

Year	Study	Tools/Technologies/Data sources used	Theme	Summary
2025	(El Kouari, Lazaar, and Achoughi 2025)	Industrial internet of things (IIoT), Wazuh with Elasticsearch, Snort intrusion detection system (IDS), Kibana as a	Risk Assessment & Mitigation	This research develops a robust IIoT industrial cybersecurity strategy with layered defences, integrated tools (Wazuh, Snort, SIEM), and proactive threat intelligence to mitigate risks in industrial environments.

		security information and event management (SIEM)		
2025	(Bhole, Sauter, and Kastner 2025)	Threat Group Cards ThaiCERT, Malpedia by Fraunhofer FKIE, MITRE ATT&CK, and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	Emerging Technologies & Trends	This article analyses cyber threats to Operational Technology (OT) by examining real-world incidents, threat actors, and their tactics and the importance of using open-source intelligence platforms and databases to improve OT security.
2024	(Iosif et al. 2024)	Serious game	Education and Training	The paper investigates how a serious game can improve code review practices among industrial developers, specifically in identifying and addressing security issues and promoting more effective code review techniques.
2024	(Correia et al. 2024)	Gazepoint GP3 Eye-tracking device, Open Gaze and Mouse Analyzer (OGAMA) software, C++	Education and Training	This paper uses eye-tracking technology to analyse how industrial cybersecurity professionals perform code reviews to identify vulnerabilities with the goal of improving code review training and tools.
2023	(Sasikumar, Karthikeyan, and Murugan 2023)	Blockchain	Education and Training	This chapter highlights blockchain's applications in Industry 4.0, its limitations, and its privacy and security requirements.
2023	(Tharot et al. 2023)	Serious game, MITRE ATT&CK and STRIDE Frameworks	Education and Training	This paper uses serious game scenarios based on the MITRE ATT&CK framework to teach industrial cybersecurity concepts to students with limited prior knowledge.
2023	(Prada et al. 2023)	Microsoft Hyper-V Virtual machines, PLC (programmable logic controller), HMI (human-machine interface), switch, Tofino Xenon an industrial firewall, Vijeo Designer software, OpenVAS software, Unity Pro software	Education and Training	This paper presents a hands-on activity on a remotely accessible training platform to supplement the theoretical aspects of a Master's degree course in industrial cybersecurity
2023	(Kuchar, Blazek, and Fujdiak 2023)	BUTCA (Brno University of Technology Cyber Arena) platform, industrial protocol Modbus/TCP, Cyber Kill Chain Model	Education and Training	This paper presents an education platform to educate users about the potential impact of human error, specifically phishing attacks, on industrial cybersecurity through a gamified learning experience
2023	(Abbas and Myeong 2023; Sell and Dupuis 2023)	Support Vector Machine, XGBoost, and Artificial Neural Networks	Industrial Cloud Security	This paper explores the use of machine learning techniques to enhance cloud computing security in industries, with XGBoost demonstrating the highest accuracy in predicting and mitigating security threat
2023	(Sell and Dupuis 2023)	NIST SP 800-171 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations")	Education and Training	This paper implements an industrial cybersecurity program for a manufacturing firm, bridging the gap between IT and OT security standards by applying NIST SP 800 guidance to an OT environment.
2023	(Djebbar	ETSI EN 303 645 v2.1.1	Standards	This paper analyses the overlap between three

	and Nordstrom 2023)	for consumer devices connected to the internet, ISA/IEC 62443-3-3:2019 for industrial automation and control systems, and ISO/IEC 27001:2022 for information security management systems.	and Frameworks	cybersecurity standards (ETSI EN 303 645, ISA/IEC 62443-3-3, and ISO/IEC 27001) to help organisations identify common security requirements and controls, streamline compliance efforts and reduce duplication.
2022	(Babić et al. 2022)	NA	Standards and Frameworks	This paper examines cybersecurity for Industrial Control Systems (ICS) in the context of Industry 4.0, exploring security concepts, classifications, and strategies for defending against cyberattacks.
2022	(Domínguez et al. 2022)	PLCs, actuator, virtual machines with automation software (such as workstations, SCADAs, or historians)	Education and Training	This paper presents a Critical Infrastructure Cybersecurity Laboratory (CICLab) for industrial cybersecurity research and training of specialized personnel
2021	(Wan et al. 2021)	NA	Risk Assessment & Mitigation	This paper analyzes cyber threats and vulnerabilities in networked control systems, compares them to IT systems, and discusses security mechanisms and viewpoints to enhance industrial cybersecurity in the context of the Industrial Internet.
2019	(Karampidis 2019)	NA	Education and Training	This paper presents the InCyS 4.0 (Industrial CyberSecurity 4.0) project, which aims to develop open-source educational materials for training industrial production technicians in cybersecurity by conducting field research to identify industry needs and tailor the training content accordingly
2018	(Lees, Crawford, and Jansen 2018)	NA	Risk Assessment & Mitigation	This paper examines cybersecurity resilience in multinational corporations, focusing on the need for senior management leadership, effective internal procedures, and robust OT infrastructure to mitigate cyber threats and ensure business continuity.
2013	(Piggin 2013)	NA	Standards and Frameworks	This paper reviews existing standards for ICS and SCADA security, discusses current best practices, and explores the future direction of these standards.
2007	(Creery, Eng, and Member 2007)	NA	Risk Assessment & Mitigation	This paper presents a methodology for assessing and mitigating cybersecurity risks in networked control systems by identifying vulnerabilities, implementing technical and procedural countermeasures

Table 1 summarises industrial cybersecurity research trends, categorised by theme. Risk Assessment & Mitigation studies focus on robust IIoT strategies using layered defenses & threat intelligence, and OT threat analysis. Education and Training research explores diverse methods, including serious games, eye-tracking for code review improvement, blockchain in Industry 4.0, gamified learning for human error reduction, and hands-on training platforms. Industrial Cloud Security research investigates machine learning for enhanced cloud protection. Standards and Frameworks studies analyse overlaps between existing standards and review best practices for ICS and SCADA security. Several studies across themes, particularly risk assessment and mitigation, examine risk assessment methodologies and emphasise the importance of leadership and robust procedures for OT infrastructure resilience.

3.2. Challenges in Industrial Cybersecurity

3.2.1. Lack of training material

Currently, there is a lack of published cybersecurity training material or courses that

focus on Industrial Control Systems (ICS) (Tharot et al. 2023; Prada et al. 2023). Some of the researchers are taking the initiative to create a training platform to supplement the theoretical aspects of through a Master's degree course in industrial cybersecurity (Prada et al. 2023). As a result, over 70% of participants in this course found that this system engagement improved their learning, motivation, and theoretical understanding. In this case, more comprehensive training material or programmes are needed for working in the industry 5.0 environment.

3.2.2. Lack of skill

There is a huge shortage of cybersecurity workforce in OT environments (Bhole, Sauter, and Kastner 2025; Prada et al. 2023). To enhance cybersecurity skills and defences against cyber threats, there is a need for training, certifications, research, and resources that can be provided through firms like ISA.org (International Society of Automation) and SANS Institute. Additionally, (Kuchar, Blazek, and Fujdiak 2023) are educating the pupils/students/employees about cybersecurity challenges caused by the convergence of IT and OT through training platform. Next, (Sell and Dupuis 2023) implements an industrial cybersecurity program for a manufacturing firm and (Domínguez et al. 2022) presents a Critical Infrastructure Cybersecurity Laboratory (CICLab) for the OT environment. Further, InCyS 4.0 (Industrial CyberSecurity 4.0) project aims to develop open-source educational materials for training industrial production technicians in cybersecurity (Karampidis 2019).

3.2.3. Resistance to change

It has been noticed that people are resistant to adopting new practices and technologies, hindering the implementation of robust cybersecurity measures (Bhole, Sauter, and Kastner 2025). Effective change management strategies are essential to overcome this resistance. Some motivation programmes can be built to help the workforce with this new change and its benefits.

3.2.4. Legacy technology

Many industrial systems rely on legacy technologies that lack built-in security features, making them vulnerable to cyberattacks (Bhole, Sauter, and Kastner 2025). Upgrading or retrofitting these systems can be expensive and time-consuming, creating a significant challenge.

3.2.5. Convergence of IT and OT technology

The increasing convergence of Information Technology (IT) and Operational Technology (OT) creates new attack vectors. Traditional IT security solutions may not be adequate for OT environments, requiring specialised approaches to secure industrial systems.

4. Conclusions

On the one hand, it has been identified that there is a lack of material for industrial cybersecurity, but on the other hand, it has been noticed that most of the research on this subject is about education and training. This paper concludes that there is a need for a comprehensive cybersecurity framework for industrial systems since, right now, there is scattered information. There are several initiatives, standards, guidelines, directives, and acts for industrial cybersecurity but those need to be integrated to provide a comprehensive framework for cybersecurity and AI governance.

References

Abbas, Zaheer, and Seunghwan Myeong. 2023. “Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in Cloud Computing Environment.” *Electronics (Switzerland)* 12 (12). https://doi.org/10.3390/electronics12122650.

Babić, Mladen, Miloš Stanojević, Gordana Ostojić, Srđan Tegeltija, and Stevan Stankovski. 2022. “Industrial Cyber Security Aspects in ICS Applications.” https://doi.org/10.2507/33rd.daaam.proceedings.xxx.

Bhole, Mukund, Thilo Sauter, and Wolfgang Kastner. 2025. “Enhancing Industrial Cybersecurity: Insights from Analyzing Threat Groups and Strategies in Operational Technology Environments.” *IEEE Open Journal of the Industrial Electronics Society*. https://doi.org/10.1109/OJIES.2025.3527585.

Breque, Maija., Lars. De Nul, and Athanasios. Petridis. 2021. *Industry 5.0 : Towards a Sustainable, Human-Centric and Resilient European Industry*. Publications Office of the European Union.

Cervini, James, Aviel Rubin, and Lanier Watkins. 2022. “Don’t Drink the Cyber: Extrapolating the Possibilities of Oldsmar’s Water Treatment

Cyberattack." In *International Conference on Cyber Warfare and Security*, 17:19–25.

Correia, Samuel Riegel, Maria Pinto-Albuquerque, Tiago Espinha Gasiba, and Andrei-Cristian Iosif. 2024. "Improving Industrial Cybersecurity Training: Insights into Code Reviews Using Eye-Tracking." https://doi.org/10.4230/OASIcs.ICPEC.2024.1.

Creery, A, P P E Eng, and Ieee Member. 2007. "Industrial Cybersecurity For Power System And SCADA Networks."

Djebbar, Fatiha, and Kim Nordstrom. 2023. "A Comparative Analysis of Industrial Cybersecurity Standards." *IEEE Access* 11:85315–32. https://doi.org/10.1109/ACCESS.2023.330320.

Domínguez, Manuel, Juan J. Fuertes, Miguel A. Prada, Serafín Alonso, Antonio Morán, and Daniel Pérez. 2022. "Design of Platforms for Experimentation in Industrial Cybersecurity." *Applied Sciences (Switzerland)* 12 (13). https://doi.org/10.3390/app12136520.

DORA. 2022. "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011."

EU. 2019. "High-Level Expert Group on Artificial Intelligence Set up by the European Commission Ethics Guidelines for Trustworthy AI." https://ec.europa.eu/digital-.

EU AI Act. 2023. "First Regulation on Artificial Intelligence." 2023. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Europa. 2022. "Cyber Resilience Act." 2022.

European Union. 2022. "NIS 2 Directive) (Text with EEA Relevance."

Iosif, Andrei-Cristian, Ulrike Lechner, Maria Pinto-Albuquerque, and Tiago Espinha Gasiba. 2024. "Serious Game for Industrial Cybersecurity: Experiential Learning Through Code Review." In , 1–6. Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/cseet62301.2024.10663058.

ISA/IEC. 2018. "62443 Series of Standards." 2018. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

ISO/IEC 27000:2018(en). 2018. "Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary." 2018. https://www.iso.org/standard/73906.html.

ISO/IEC 27032:2023. 2023. "Cybersecurity — Guidelines for Internet Security." 2023. https://www.iso.org/standard/76070.html.

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E. K., & Papadourakis, G. 2019. "Industrial CyberSecurity 4.0 : Preparing the Operational Technicians for Industry 4.0." In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) : Proceedings : 11-13 September 2019, Limassol, Cyprus*. IEEE.

Kouari, Oumaima El, Saiida Lazaar, and Tarik Achoughi. 2025. "Fortifying Industrial Cybersecurity: A Novel Industrial Internet of Things Architecture Enhanced by Honeypot Integration." *International Journal of Electrical and Computer Engineering* 15 (1): 1089–98. https://doi.org/10.11591/ijece.v15i1.pp1089-1098.

Kour, Ravdeep, Ramin Karim, Pierre Dersin, and Naveen Venkatesh. 2024. "Cybersecurity for Industry 5.0: Trends and Gaps." *Frontiers in Computer Science*. Frontiers Media SA. https://doi.org/10.3389/fcomp.2024.1434436.

Kour, Ravdeep, Amit Patwardhan, Adithya Thaduri, and Ramin Karim. 2023. "A Review on Cybersecurity in Railways." *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit* 237 (1): 3–20. https://doi.org/10.1177/09544097221089389.

Kuchar, Karel, Petr Blazek, and Radek Fujdiak. 2023. "From Playground to Battleground: Cyber Range Training for Industrial Cybersecurity Education." In *ACM International Conference Proceeding Series*, 209–14. Association for Computing Machinery. https://doi.org/10.1145/3638782.3638814.

Langner, R. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Secur. Priv. 9 (3), 49–51 (2011)."

Lees, Michael J., Melissa Crawford, and Christoph Jansen. 2018. "Towards Industrial Cybersecurity Resilience of Multinational Corporations." In *IFAC-PapersOnLine*, 51:756–61. Elsevier B.V. https://doi.org/10.1016/j.ifacol.2018.11.201.

NIST. 2014. "Cybersecurity Framework." 2014. https://www.nist.gov/cyberframework.

Piggin, R S H. 2013. "Development of Industrial Cyber Security Standards: IEC 62443 for SCADA and Industrial Control System Security."

Prada, Miguel A., Juan J. Fuertes, José R. Rodríguez-Ossorio, Raúl González-Herbón, Guzmán González-Mateos, and Manuel Domínguez.

2023. "Hands-on Training in Industrial Cybersecurity for a Multidisciplinary Master's Degree." In *IFAC-PapersOnLine*, 56:11217–22. Elsevier B.V. https://doi.org/10.1016/j.ifacol.2023.10.850.

Regulation, Protection. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council." *Regulation (Eu)* 679:2016.

Sasikumar, R, P Karthikeyan, and Thangavel Murugan. 2023. "Privacy and Security Through Blockchain in Industry 4.0: An Industrial Cybersecurity Perspective." In *Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies*, 315–34. IGI Global.

Sell, Matthew, and Marc Dupuis. 2023. "Designing an Industrial Cybersecurity Program for an Operational Technology Group." In *SIGITE 2023 - Proceedings of the 24th Annual Conference on Information Technology Education*, 125–30. Association for Computing Machinery, Inc. https://doi.org/10.1145/3585059.3611438.

Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. 2023. "Guide to Operational Technology (OT) Security." https://doi.org/10.6028/NIST.SP.800-82r3.

Tharot, Kanthanet, Quoc Bao Duong, Andreas Riel, and Jean Marc Thiriet. 2023. "Industrial Cybersecurity Game-Scenarios Based on the MITRE ATT&CK Framework." In *Conference Proceedings - 2023 IEEE Asia Meeting on Environment and Electrical Engineering, EEE-AM 2023*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EEE-AM58328.2023.10395155.

Wan, Ming, Jiawei Li, Ying Liu, Jianming Zhao, and Jiushuang Wang. 2021. "Characteristic Insights on Industrial Cyber Security and Popular Defense Mechanisms."