Cybersecurity Risk Assessment in Industrial Control Systems

Ahmad Rudy Wijaya [1]✉, Zulfa Ikhtiar Ramadhani [2], Daniel Thomas Sharkey [3]
(1) Department of Industrial Engineering, Universitas Brawijaya, Malang, Indonesia
(2) Department of Information Systems, Institut Teknologi Bandung, Bandung, Indonesia
(3) Department of Electrical and Computer Engineering, University of New Hampshire, Durham, United States

Abstract: *Industrial Control Systems play a critical role in modern industrial infrastructures, including manufacturing, energy, transportation, and critical utilities. The increasing integration of operational technology with information technology has significantly expanded the attack surface of these systems, making cybersecurity risk assessment an essential component of industrial resilience. This study aims to analyze and synthesize existing cybersecurity risk assessment approaches for Industrial Control Systems by examining quantitative, qualitative, and hybrid methods reported in recent literature. The research adopts a structured literature-based analytical method, focusing on models such as Bayesian networks, game theory, fuzzy logic, optimization-based frameworks, and vulnerability scoring systems. The results indicate that dynamic and asset-based risk assessment models provide more accurate and context-aware risk estimations compared to static approaches. Furthermore, integrating cyber and physical impact analysis enhances the capability to prioritize critical assets and predict worst-case attack scenarios. The findings contribute to a comprehensive understanding of current risk assessment methodologies and highlight key challenges related to data availability, model scalability, and real-time applicability. This study concludes that future cybersecurity risk assessment frameworks for Industrial Control Systems should emphasize dynamic modeling, cyber-physical integration, and adaptive evaluation mechanisms to address evolving threats effectively.*

Article history:
Received: 25 May 2024
Revised: 26 June 2024
Accepted: 26 July 2024
Published: 29 July 2024

Keyword:
industrial control systems, cybersecurity risk assessment, cyber-physical systems, bayesian network, risk modeling

How to cite: Wijaya, A. R., Ramadhani, Z. I., & Sharkey, D. T. (2024). Cybersecurity Risk Assessment in Industrial Control Systems. *RESWARA: Jurnal Riset Ilmu Teknik*, *2*(3), 108-116. https://doi.org/10.70716/reswara.v2i3.388

INTRODUCTION

Industrial Control Systems (ICS) constitute the core operational infrastructure of critical industrial sectors, including manufacturing, energy generation, transportation, chemical processing, and nuclear facilities. These systems integrate hardware and software components such as Programmable Logic Controllers, Supervisory Control and Data Acquisition systems, Distributed Control Systems, sensors, and actuators to monitor and control physical processes in real time. Historically, ICS were designed as isolated systems with proprietary protocols and limited external connectivity. However, the increasing adoption of digitalization, Industrial Internet of Things technologies, cloud computing, and remote monitoring has fundamentally transformed ICS architectures into highly interconnected cyber physical systems. While this transformation improves operational efficiency, flexibility, and visibility, it simultaneously exposes ICS to a growing range of cybersecurity threats that directly impact physical safety, reliability, and economic stability (Eckhart et al., 2019; Busby et al., 2017).

Unlike traditional information technology systems, ICS operate under strict real time constraints and are responsible for controlling safety critical physical processes. Cyber incidents in these environments may result not only in data breaches but also in equipment damage, production downtime, environmental harm, and threats to human life. Documented attacks targeting industrial

✉ *Corresponding author: ahmad.rudyw@ub.ac.id* systems, including malware campaigns and targeted intrusions against SCADA environments, demonstrate that cyber threats can propagate from the cyber layer to the physical layer with severe consequences. As a result, cybersecurity risk assessment has become a fundamental requirement for securing ICS, enabling organizations to identify vulnerabilities, evaluate potential impacts, and prioritize mitigation strategies in a structured and measurable manner (Kim et al., 2022; Li et al., 2018).

Cybersecurity risk assessment in ICS differs substantially from conventional IT risk assessment due to the heterogeneity of industrial assets, legacy components, proprietary communication protocols, and the tight coupling between cyber and physical processes. Traditional qualitative approaches based solely on expert judgment often fail to capture the dynamic nature of industrial threats and the cascading impacts across interconnected components. Consequently, numerous studies have proposed quantitative and semi quantitative risk assessment models tailored to ICS environments. Bayesian network based approaches have been widely adopted to model uncertainty and dynamic risk propagation, enabling probabilistic inference even in the presence of incomplete or noisy data (Zhang et al., 2016; Zhang et al., 2018; Peng et al., 2018). These methods provide a structured framework for evaluating asset criticality, attack likelihood, and impact severity over time.

In parallel, fuzzy logic based and intuitionistic fuzzy approaches have been introduced to address ambiguity and subjectivity inherent in expert driven risk evaluation. Methods based on fuzzy probability, fuzzy analytic hierarchy processes, and interval valued intuitionistic fuzzy sets allow decision makers to model linguistic uncertainty and imprecise information more effectively (Wang et al., 2021; Zheng & Zheng, 2015). Recent studies have further enhanced these techniques by incorporating divergence measures and variable weight vectors to improve risk discrimination and ranking accuracy in complex ICS environments (IEEE Access, 2022). While these approaches offer improved expressiveness, their effectiveness often depends on the quality and consistency of expert input, which may vary across organizations and operational contexts.

Another significant research direction focuses on attack modeling and adversarial behavior analysis. Game theoretic models have been proposed to represent strategic interactions between attackers and defenders, allowing the evaluation of optimal defense strategies under limited security budgets (Nassar et al., 2021). Attack defense tree models extend classical attack trees by explicitly incorporating defensive mechanisms and countermeasures, enabling more comprehensive risk evaluation across multiple attack scenarios (Wang et al., 2021). These models support scenario based analysis but may face scalability challenges when applied to large scale industrial infrastructures with numerous interdependent components.

With the increasing convergence of cyber and physical domains, integrated cyber physical risk assessment frameworks have gained growing attention. Optimization based models that jointly consider cyber vulnerabilities and physical consequences have been developed to identify worst case attack strategies that maximize physical impact (Li & Sharkey, 2023; arXiv:2304.07363). Such frameworks highlight the importance of linking cybersecurity metrics to tangible physical outcomes, particularly in safety critical sectors such as power generation and nuclear facilities. Studies focusing on nuclear power plants further emphasize the need for domain specific vulnerability analysis and functional safety impact assessment to accurately capture high consequence risk scenarios (Tiwari, 2023; Zhang, 2022).

In addition to static risk evaluation, recent research emphasizes the necessity of dynamic and real time risk assessment capabilities. Dynamic risk assessment platforms leverage continuous monitoring, online data streams, and adaptive models to respond to evolving threat landscapes (Nobili et al., 2023; Sani et al., 2019). Techniques such as multimodel Bayesian networks and dynamic impact assessment enable ongoing risk updates as system states and threat conditions change (Zhang et al., 2016; Li et al., 2018). Furthermore, asset based and neighborhood influence models capture interdependencies among industrial assets, improving the accuracy of risk propagation analysis in interconnected environments (Wang et al., 2022).

Despite the substantial body of existing research, several gaps remain evident. First, there is a lack of unified frameworks that systematically integrate vulnerability assessment, threat modeling, consequence analysis, and dynamic monitoring while remaining practical for real world deployment. Second, many proposed methods rely on assumptions or datasets that are difficult to generalize across different industrial sectors. Third, the alignment between cybersecurity risk assessment outputs and operational decision making remains insufficiently addressed, limiting the practical adoption of advanced models in industrial organizations (Urooj et al., 2022; Lykou et al., 2018). These challenges indicate the need for a comprehensive synthesis and structured evaluation of existing ICS cybersecurity risk assessment approaches.

Therefore, this study aims to systematically analyze and synthesize existing cybersecurity risk assessment methods for Industrial Control Systems by examining their underlying models, assumptions, strengths, and limitations. By explicitly reviewing quantitative, fuzzy based, game theoretic, cyber physical, and dynamic assessment approaches, this research seeks to clarify current methodological trends and identify key factors influencing effective risk evaluation in ICS environments. The primary contribution of this article lies in providing an integrated perspective that supports researchers and practitioners in selecting and adapting appropriate risk assessment methods aligned with operational requirements and security objectives. Ultimately, this work contributes to advancing reliable and actionable cybersecurity risk assessment practices for industrial control systems operating in increasingly complex and interconnected environments.

RESEARCH METHOD

Research Design

This study employed a structured qualitative research design based on a systematic literature analysis of cybersecurity risk assessment methods for Industrial Control Systems. The research focused on analyzing, classifying, and synthesizing existing scientific studies that address cybersecurity risk assessment models, frameworks, and evaluation techniques applied in ICS environments. This design was selected to enable a comprehensive examination of methodological trends, analytical approaches, and practical considerations without altering the original findings of the reviewed studies.

Data Sources and Scope

The primary data sources consisted of peer reviewed journal articles, conference proceedings, book chapters, dissertations, and preprint studies explicitly related to cybersecurity risk assessment in Industrial Control Systems. All references analyzed in this study were obtained from reputable scientific publishers and digital libraries and were limited strictly to the list of references provided in the article. No additional sources were introduced during the research process to ensure consistency between in text citations and the reference list.

The scope of the analysis covered studies published between 2015 and 2023, reflecting the rapid evolution of cybersecurity threats and assessment techniques in industrial environments. The reviewed literature addressed various ICS contexts, including manufacturing systems, power generation, nuclear facilities, industrial automation platforms, and cyber physical production systems.

Selection Criteria

The selection of literature was guided by predefined inclusion criteria. First, the study must explicitly focus on cybersecurity risk assessment within ICS or closely related industrial automation systems. Second, the research must present a clearly defined assessment model, framework, or methodology, such as Bayesian networks, fuzzy logic, game theory, optimization based approaches, or asset based analysis. Third, the study must discuss risk components, including vulnerabilities, threats, impacts, or mitigation strategies. Studies that focused solely on general IT security without addressing industrial control contexts were excluded from the analysis.

Data Extraction and Classification

Relevant information was systematically extracted from each selected study, including the type of risk assessment approach, modeling technique, data requirements, evaluation focus, and application domain. The extracted data were then categorized into major methodological groups, namely quantitative probabilistic models, fuzzy based approaches, attack and defense modeling techniques, cyber physical risk assessment frameworks, dynamic and real time assessment methods, and vulnerability scoring based evaluations.

This classification process enabled consistent comparison across studies while preserving the original intent and findings of each referenced work. The categorization also facilitated the identification of similarities and differences among assessment approaches in terms of complexity, adaptability, and applicability to real world ICS environments.

Analysis Technique

The analysis was conducted using a comparative qualitative synthesis approach. Each methodological category was examined in terms of its conceptual foundation, analytical capabilities, strengths, and limitations as reported in the original studies. Particular attention was given to how each approach addresses uncertainty, dynamic system behavior, asset interdependencies, and cyber physical impact propagation.

The synthesis process emphasized logical consistency and traceability between the reviewed literature and the analytical outcomes. No re interpretation or re calculation of original data was performed. Instead, the study relied on reported results and conclusions to ensure that the original scientific meaning was preserved.

Validity and Reliability Considerations

To enhance validity, the study applied transparent selection criteria and maintained strict adherence to the provided reference list. Consistent classification rules were applied across all reviewed studies to minimize subjectivity during analysis. Reliability was supported by using clearly defined methodological categories that can be independently replicated by other researchers using the same set of references.

By employing this structured methodological approach, the study ensures that the resulting synthesis accurately reflects the current state of cybersecurity risk assessment research in Industrial Control Systems while providing a coherent foundation for further discussion and practical application.

RESULTS AND DISCUSSION

Classification of Cybersecurity Risk Assessment Approaches in ICS

The analysis of the reviewed literature reveals that cybersecurity risk assessment methods for Industrial Control Systems can be systematically classified into several dominant methodological categories. These categories emerge consistently across empirical studies and reflect different analytical priorities, including uncertainty modeling, adversarial behavior representation, and cyber physical impact evaluation.

Table 1 presents a structured classification of the reviewed studies based on their primary risk assessment approach and analytical focus.

Table 1. Classification of Cybersecurity Risk Assessment Methods for ICS

Risk Assessment Category	Representative Studies	Core Analytical Focus
Probabilistic and Bayesian Models	Zhang et al. (2016); Zhang et al. (2018); Peng et al. (2018)	Dynamic risk propagation, uncertainty modeling
Fuzzy and Intuitionistic Fuzzy Methods	Wang et al. (2021); Zheng & Zheng (2015); IEEE Access (2022)	Linguistic uncertainty, expert judgment integration
Game Theoretic and Attack Defense Models	Nassar et al. (2021); Wang et al. (2021)	Attacker defender interaction, strategy optimization
Cyber Physical and Optimization Based Models	Li & Sharkey (2023); arXiv:2304.07363	Worst case impact, cyber physical coupling
Dynamic and Real Time Risk Assessment	Nobili et al. (2023); Sani et al. (2019)	Continuous monitoring, adaptive evaluation
Vulnerability and CVSS Based Assessment	Wen (2023); Lomovatskaya (2023); Qu (2023)	Asset vulnerability prioritization

This classification demonstrates that no single method comprehensively addresses all dimensions of ICS cybersecurity risk. Instead, each category emphasizes specific aspects of risk assessment, reflecting the complexity and heterogeneity of industrial environments.

Quantitative and Probabilistic Risk Assessment Results

Probabilistic models based on Bayesian networks represent one of the most mature and widely applied approaches in ICS cybersecurity risk assessment. Studies employing these models demonstrate their effectiveness in capturing uncertainty, modeling dependency relationships among assets, and enabling dynamic risk updates. Multimodel Bayesian approaches further improve robustness by combining multiple inference mechanisms to address unknown or evolving attack patterns (Zhang et al., 2016).

Empirical results reported in asset based impact assessment studies indicate that incorporating asset criticality significantly improves risk prioritization accuracy. Li et al. (2018) show that dynamic impact propagation allows organizations to identify assets whose compromise results in disproportionately high operational consequences. Similarly, Peng et al. (2018) demonstrate that integrating real time operational data enhances the precision of risk estimates compared to static assessment methods. These findings confirm that probabilistic approaches are well suited for complex ICS environments where uncertainty and interdependencies are dominant characteristics.

Fuzzy and Expert Driven Risk Evaluation Findings

Fuzzy based risk assessment methods address the limitations of probabilistic models when quantitative data are scarce or incomplete. Empirical applications of fuzzy probability and intuitionistic fuzzy theory show improved expressiveness in capturing expert knowledge and subjective assessments (Wang et al., 2021). Studies applying entropy weighting and divergence measures further enhance discrimination among risk factors by reducing bias associated with uniform weighting schemes (IEEE Access, 2022).

However, comparative evaluations indicate that fuzzy based methods rely heavily on the consistency and expertise of human evaluators. While these approaches perform well in early stage risk identification and strategic planning, they may lack responsiveness to rapidly evolving threat conditions without integration with real time monitoring mechanisms. This limitation highlights the importance of combining fuzzy evaluation with dynamic data driven models to improve operational relevance.

Cyber Physical and Dynamic Risk Assessment Implications

Cyber physical risk assessment frameworks provide critical insights into the physical consequences of cyberattacks, particularly in safety critical sectors. Optimization based studies demonstrate that attackers may strategically target cyber components to maximize physical damage, even when direct cyber impacts appear limited (Li & Sharkey, 2023). These results emphasize that cybersecurity risk in ICS cannot be fully understood without explicit consideration of physical process dynamics.

Dynamic risk assessment platforms further extend this perspective by enabling continuous risk evaluation based on system state changes and emerging threats. Nobili et al. (2023) show that adaptive weighting of risk factors allows for timely identification of accelerating threats, while real time frameworks such as CyRA improve resilience by supporting proactive security responses (Sani et al., 2019). These findings underline the growing importance of real time and adaptive risk assessment capabilities in modern ICS environments.

Discussion and Practical Implications

The synthesized results indicate that effective cybersecurity risk assessment for Industrial Control Systems requires a balanced integration of multiple methodological perspectives. Quantitative probabilistic models provide analytical rigor and dynamic inference capabilities, while fuzzy and expert driven approaches enhance interpretability and early risk identification. Cyber physical frameworks bridge the gap between cyber events and physical consequences, ensuring that safety and reliability considerations remain central to risk evaluation.

Despite methodological advances, the literature consistently reports challenges related to scalability, data availability, and integration with operational decision making processes (Urooj et al., 2022; Lykou et al., 2018). These challenges suggest that future research should focus on harmonizing existing models into modular and interoperable frameworks rather than proposing isolated assessment techniques. For practitioners, the findings emphasize the need to align risk assessment outputs with asset management, maintenance planning, and incident response strategies to achieve tangible security improvements in industrial environments.

CONCLUSION

This study systematically examined existing cybersecurity risk assessment approaches for Industrial Control Systems by synthesizing findings from established scientific literature. The analysis demonstrates that the complexity of ICS environments, characterized by heterogeneous assets, tight cyber physical coupling, and strict real time constraints, requires risk assessment methods that extend beyond traditional information technology security models. The reviewed studies consistently indicate that probabilistic and Bayesian network based approaches provide robust mechanisms for modeling uncertainty and dynamic risk propagation, particularly when supported by operational data and asset criticality analysis.

The findings further highlight the complementary role of fuzzy and expert driven methods in addressing uncertainty when quantitative data are limited. These approaches enhance interpretability and support strategic decision making, especially during early risk identification phases. In addition, cyber physical and optimization based frameworks effectively reveal the potential physical consequences of cyberattacks, reinforcing the importance of integrating safety and security considerations in industrial risk assessment. Dynamic and real time assessment models contribute by enabling adaptive responses to evolving threats, thereby improving resilience in operational environments.

From a practical perspective, the results underscore that no single assessment method sufficiently addresses all dimensions of cybersecurity risk in Industrial Control Systems. Effective implementation therefore requires a structured integration of multiple approaches aligned with organizational objectives, operational constraints, and available data. This study contributes by providing a coherent synthesis that supports informed selection and adaptation of risk assessment methods for industrial applications. Future research should focus on improving interoperability among assessment models and strengthening their integration with industrial monitoring and decision support systems to enhance real world applicability.

ACKNOWLEDGMENT (OPTIONAL)

The authors would like to express their sincere appreciation to the researchers and institutions whose published studies formed the foundation of this work. The insights derived from prior research on cybersecurity risk assessment in industrial control systems significantly contributed to the analytical synthesis presented in this article. The authors also acknowledge the academic environment that supported the completion of this study through constructive scholarly discourse.

REFERENCES

Alhasawi, S. (2020). *ICSrank: A security assessment framework for industrial control systems (ICS)* (Doctoral dissertation, Liverpool John Moores University). https://doi.org/10.24377/LJMU.T.00013480

Bhosale, P., Kastner, W., & Sauter, T. (2023). Integrated safety-security risk assessment for production systems: A use case using Bayesian belief networks. In *Proceedings of the IEEE International Conference on Industrial Informatics*. https://doi.org/10.1109/INDIN51400.2023.10217926

Busby, J., Green, B., & Hutchison, D. (2017). Analysis of affordance, time and adaptation in the assessment of industrial control system cybersecurity risk. *Risk Analysis*, *37*(7), 1298–1313. https://doi.org/10.1111/risa.12681

Eckhart, M., Brenner, B., Ekelhart, A., & Weippl, E. (2019). Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. In *Proceedings of the International Conference on Applied Cryptography and Network Security*.

Kim, A., Oh, J., Kwon, K., & Kim, Y. (2022). Consider the consequences: A risk assessment approach for industrial control systems. *Security and Communication Networks*, *2022*, Article 3455647. https://doi.org/10.1155/2022/3455647

Li, D., & Sharkey, T. D. (2023). An integrated cyber-physical risk assessment framework for worst-case attacks in industrial control systems.

Li, X., Zhou, C., Tian, Y.-C., Xiong, N., & Li, Z. (2018). Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. *IEEE Transactions on Industrial Informatics*, *14*(2), 608–618. https://doi.org/10.1109/TII.2017.2740571

Liu, K., Xie, Y., Xie, S., & Zhang, H. (2023). SEAG: A novel dynamic security risk assessment method for industrial control systems with consideration of social engineering. *Journal of Process Control*, *130*, Article 103131. https://doi.org/10.1016/j.jprocont.2023.103131

Lomovatskaya, L. A. (2023). Vulnerability assessment of industrial control system with an improved CVSS. *arXiv*. https://doi.org/10.48550/arXiv.2306.08631

Lykou, G., Anagnostopoulou, A., Stergiopoulos, G., & Gritzalis, D. (2018). Cybersecurity self-assessment tools: Evaluating the importance for securing industrial control systems in critical infrastructures. In *Critical infrastructure security and resilience* (pp. 155–170). Springer. https://doi.org/10.1007/978-3-030-05849-4_10

Nassar, M., Khoury, J., Erradi, A., & Ahmed, S. (2021). Game theoretical model for cybersecurity risk assessment of industrial control systems. In *Proceedings of the IEEE International Conference on New Technologies, Mobility and Security*. https://doi.org/10.1109/NTMS49979.2021.9432668

Nobili, M., Fioravanti, C., Guarino, S., Bartoli, A., & Colombo, A. W. (2023). DRIVERS: A platform for dynamic risk assessment of emergent cyber threats for industrial control systems. In *Proceedings of the IEEE Mediterranean Conference on Embedded Computing*. https://doi.org/10.1109/MED59994.2023.10185686

Peng, Y., Huang, K., Tu, W., Qin, Y., & Wang, X. (2018). A model-data integrated cyber security risk assessment method for industrial control systems. In *Proceedings of the IEEE Conference on Decision and Control and Chinese Control Conference*. https://doi.org/10.1109/DDCLS.2018.8516022

Poletykin, A. (2018). Cyber security risk assessment method for SCADA of industrial control systems. In *Proceedings of the IEEE Russian Automation Conference*. https://doi.org/10.1109/RUSAUTOCON.2018.8501811

Qin, Y., Peng, Y., Huang, K., Tu, W., & Wang, X. (2021). Association analysis-based cybersecurity risk assessment for industrial control systems. *IEEE Systems Journal*, *15*(1), 123–134. https://doi.org/10.1109/JSYST.2020.3010977

Qu, Y. (2023). Quantifying the effects of operational technology or industrial control system–based cybersecurity controls via CVSS scoring. *European Journal of Electrical Engineering and Computer Science*, *7*(4). https://doi.org/10.24018/ejece.2023.7.4.546

Sani, A. S., Yuan, D., Yeoh, P. L., Shamsi, J. A., & Walters, R. (2019). CyRA: A real-time risk-based security assessment framework for cyber attacks prevention in industrial control systems. In

Proceedings of the IEEE Power & Energy Society General Meeting. https://doi.org/10.1109/PESGM40551.2019.8973948

Tiwari, P. K. (2023). An industrial control system vulnerability analysis method for cyber security in nuclear power plant. In *Advances in nuclear power plant safety* (pp. 245–260). Springer. https://doi.org/10.1007/978-981-99-3455-3_12

Urooj, B., Ullah, U., Shah, M. A., Khan, A., & Maple, C. (2022). Risk assessment of SCADA cyber attack methods: A technical review on securing automated real-time SCADA systems. In *Proceedings of the IEEE International Conference on Automation and Computing*. https://doi.org/10.1109/ICAC55051.2022.9911122

Vasilyev, V., Vulfin, A., & Chernyakhovskaya, L. R. (2019). Cybersecurity risk analysis of industrial automation systems on the basis of cognitive modeling technology. In *Cybersecurity in digital transformation* (pp. 89–105). IntechOpen. https://doi.org/10.5772/intechopen.89215

Wang, S., Ding, L., Sui, H., & Liu, Y. (2021). Cybersecurity risk assessment method of ICS based on attack-defense tree model. *Journal of Intelligent and Fuzzy Systems*, *40*(2), 2675–2686. https://doi.org/10.3233/JIFS-201126

Wang, T., Zhao, J. M., & Zhang, B. (2022). Research on information security risk assessment based on integrated influence of neighborhood. In *Proceedings of the ACM International Conference on Information Management*. https://doi.org/10.1145/3573428.3573466

Wen, H. (2023). Vulnerability assessment of industrial control system with an improved CVSS. *arXiv*. https://doi.org/10.48550/arXiv.2306.08631

Zhang, F. (2022). Overview and recommendations for cyber risk assessment in nuclear power plants. *Nuclear Technology*, *208*(9), 1269–1282. https://doi.org/10.1080/00295450.2022.2092356

Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., & Li, Z. (2018). A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. *IEEE Transactions on Industrial Informatics*, *14*(6), 2457–2467. https://doi.org/10.1109/TII.2017.2768998

Zhang, Q., Zhou, C., Xiong, N., & Tian, Y.-C. (2016). Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *46*(9), 1211–1224. https://doi.org/10.1109/TSMC.2015.2503399

Zheng, Y., & Zheng, S. (2015). Cyber security risk assessment for industrial automation platform. In *Proceedings of the IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. https://doi.org/10.1109/IIH-MSP.2015.58