DAFTAR PUSTAKA

[1] M. Boeding, K. Boswell, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, "Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid †," *Energies (Basel)*, vol. 15, no. 22, 2022, doi: 10.3390/en15228692.

[2] D. Jung, J. Shin, C. Lee, K. Kwon, and J. T. Seo, "Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology," *IEEE Access*, vol. 11, pp. 15229–15241, 2023, doi: 10.1109/ACCESS.2023.3244991.

[3] D. Berardi, F. Callegati, A. Giovine, A. Melis, M. Prandini, and L. Rinieri, "When Operation Technology Meets Information Technology: Challenges and Opportunities," *Future Internet*, vol. 15, no. 3, 2023, doi: 10.3390/fi15030095.

[4] L. Patera, A. Garbugli, A. Bujari, D. Scotece, and A. Corradi, "A layered middleware for ot/it convergence to empower industry 5.0 applications," *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010190.

[5] G. Sitorus, G. Sitorus, R. Fauzi, R. Fauzi, R. A. Nugraha, and R. A. Nugraha, "ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO PADA DINAS KOMUNIKASI DAN INFORMATIKA JAWA BARAT," 2020, [Online]. Available: https://www.semanticscholar.org/paper/baf617f0dba4dcf8ce58a7c730ce085b79f3fcb4

[6] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi*, 2022, doi: 10.34010/jati.v12i2.6829.

[7] R. A. F. Hamzah *et al.*, "Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X," 2020, doi: 10.19109/jusifo.v6i1.5880.

[8] S. Alfarisi and N. Surantha, "Risk assessment in fleet management system using OCTAVE allegro," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 530–540, Feb. 2022, doi: 10.11591/eei.v11i1.3241.

[9] M. Wiboonrat, "Cybersecurity of Industrial Automation and Control System (IACS) Networks in Biomass Power Plants," in *IEEE International Symposium on Industrial Electronics*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ISIE51358.2023.10228108.

[10] A. I. Awad, M. Shokry, A. A. M. Khalaf, and M. K. Abd-Ellah, "Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach," *Computers and Electrical Engineering*, vol. 108, May 2023, doi: 10.1016/j.compeleceng.2023.108667.

[11] V. Gerardo and A. N. Fajar, "Academic IS Risk Management using OCTAVE Allegro in Educational Institution," *Journal of Information Systems and Informatics*, vol. 4, no. 3, pp. 687–708, 2022, doi: 10.51519/journalisi.v4i3.319.

[12] I. Zografopoulos, C. Konstantinou, N. G. Tsoutsos, D. Zhu, and R.

Broadwater, “Security assessment and impact analysis of cyberattacks in integrated T&D power systems,” in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, New York, NY, USA: ACM, 2021, pp. 1–7. doi: 10.1145/3470481.3472706.

[13] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” 2007. [Online]. Available: http://www.sei.cmu.edu/publications/pubweb.html

[14] “CIA Triad.” Accessed: Dec. 10, 2025. [Online]. Available: https://www.researchgate.net/publication/346192126/figure/fig1/AS%3A961506053197825%401606252315731/The-Confidentiality-Integrity-Availability-CIA-triad.png

[15] “IT/OT Diagram.” Accessed: Dec. 10, 2025. [Online]. Available: https://www.rtautomation.com/wp-content/uploads/2023/06/it-ot-diagram.jpg

[16] “Architecture-of-industrial-control-system.” Accessed: Dec. 10, 2025. [Online]. Available: https://www.researchgate.net/publication/327073518/figure/fig1/AS%3A660600527015936%401534510847055/Architecture-of-industrial-control-system.png

[17] International Organization for Standardization, “ISO/IEC 27005:2018 Information Security Risk Management,” 2018. Accessed: Dec. 10, 2025. [Online]. Available: https://www.iso.org/standard/75281.html

[18] International Organization for Standardization, “ISO 31000:2018 Risk Management — Guidelines,” 2018.

[19] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[20] K. Stouffer and S. Katzke, “Industrial Control System Security and NIST SP 800-53,” 2008. Accessed: Jul. 21, 2025. [Online]. Available: https://csrc.nist.rip/CSRC/media/Presentations/Industrial-Control-System-Security-and-NIST-SP-800/images-media/ICSS_SP800-5307-02-2008.pdf

[21] International Electrotechnical Commission, “IEC 62443 Industrial Communication Networks — Network and System Security,” 2018.

[22] K. Stouffer *et al.*, “Guide to Operational Technology (OT) security,” Sep. 2023. doi: 10.6028/NIST.SP.800-82r3.

[23] “STRATEGI RISIKO DAN PROFIL RISIKO,” 2025.

[24] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, “Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies,” *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[25] R. Alajlan, M. M. Hafizur Rahman, M. Alnaeem, and M. Almaiah, “A Literature Review on Cybersecurity Risks and Challenges Assessments in Virtual Power Plants: Current Landscape and Future Research Directions,” 2024, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2024.3515635.

[26] A. H. Maulana, I. G. P. Ari Suyasa, and E. Kurniawan, "Analysis of the Demilitarized Zone Implementation in Java Madura Bali Electrical Systems to Increase the Level of IT/OT Cyber Security With the Dual DMZ Firewall Architecture Method," in *2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/SmartNets58706.2023.10215960.

[27] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, Sep. 2022, doi: 10.1016/j.eij.2022.03.001.

[28] M. Shilenge and A. Telukdarie, "4IR integration of information technology best practice framework in operational technology," *Journal of Industrial Engineering and Management*, vol. 14, no. 3, pp. 457–476, 2021, doi: 10.3926/jiem.3429.

[29] M. Bhole, W. Kastner, and T. Sauter, "IT Security Solutions for IT/OT Integration: Identifying Gaps and Opportunities," in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ETFA61755.2024.10710968.

[30] A. Amiri, G. Steindl, and S. Hollerer, "Integrated Safety and Security by Design in the IT/OT Convergence of Industrial Cyber-Physical Systems," in *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems, ICPS 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICPS59941.2024.10640023.

[31] V. Gerardo and A. N. Fajar, "Academic IS Risk Management using OCTAVE Allegro in Educational Institution," *Journal of Information Systems and Informatics*, vol. 4, no. 3, 2022, [Online]. Available: http://journal-isi.org/index.php/isiPublishedByDRPM-UBD

[32] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method," *Sustainability (Switzerland)*, vol. 15, no. 12, Jun. 2023, doi: 10.3390/su15129812.

[33] H. Kanamaru, *The Extended Risk Assessment Form for IT/OT Convergence in IACS Security*. IEEE, 2021.

[34] B. Zahran and F. Abu Zahra, "IT/OT Convergence Protocols: MQTT, OPC, and REST," in *Proceedings - 2023 Congress in Computer Science, Computer Engineering, and Applied Computing, CSCE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1732–1737. doi: 10.1109/CSCE60160.2023.00285.

[35] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry," *Sustainability*, vol. 14, no. 3, p. 1269, Jan. 2022, doi: 10.3390/su14031269.

[36] J. Reyes, W. Fuertes, P. Arévalo, and M. Macas, "An Environment-Specific Prioritization Model for Information-Security Vulnerabilities Based on Risk

Factor Analysis," *Electronics (Basel)*, vol. 11, no. 9, p. 1334, Apr. 2022, doi: 10.3390/electronics11091334.

[37] R. Kumar, I. Rai, K. Vora, and M. Shah, "Realistic Attacks with Realistic Attackers: An Information-Security Risk Analysis of an Automatic Metering Infrastructure," in *IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/IECON51785.2023.10312002.

[38] F. Panjaitan, F. Panjaitan, A. Aprilo, and A. Aprilo, "ANALISIS MANAJEMEN RISIKO KEAMANAN JARINGAN MENGGUNAKAN FRAMEWORK NIST," *Jurnal ilmiah matrik*, 2022, doi: 10.33557/jurnalmatrik.v24i1.1682.

[39] K. N. Isnaini, G. J. N. Sari, and A. P. Kuncoro, "Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa," *Jurnal Eksplora Informatika*, 2023, doi: 10.30864/eksplora.v13i1.696.

[40] M. S. A. Setiawan, E. M. Safitri, M. A. T. Taufiqurahman, and M. A. Pratama, "Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic.id menggunakan Metode OCTAVE dan FMEA," *Jurnal Sistem dan Teknologi Informasi (JustIN)*, 2023, doi: 10.26418/justin.v11i3.66628.

[41] Ryan Dsouza, "Assessing OT and IIoT cybersecurity risk," https://aws.amazon.com/blogs/iot/assessing-ot-and-iiot-cybersecurity-risk/.

[42] Stephen J. Bigelow, "What is IT/OT convergence? Everything you need to know," https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence.

[43] The Claroty Team, "IT vs OT Security: Key Differences In Cybersecurity," https://claroty.com/blog/it-and-ot-cybersecurity-key-differences.

[44] R. Ganesen, A. A. Bakar, R. Ramli, F. A. Rahim, and M. N. A. Zawawi, "Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, 2022, doi: 10.14569/IJACSA.2022.0130843.

[45] R. A. Herdianto, K. Ramli, and Y. Suryanto, "Risk Assessment of Electronic Archive Services using Octave Allegro Method (Case Study: SIKN JIKN)," *IOP Conf Ser Mater Sci Eng*, vol. 1232, no. 1, p. 012007, Mar. 2022, doi: 10.1088/1757-899X/1232/1/012007.

[46] V. R. Putri and A. F. Wijaya, "Information Technology Risk Management Analysis Using ISO: 31000 at PT. XYZ," *Journal of Information Systems and Informatics*, vol. 4, no. 3, pp. 574–588, 2022, doi: 10.51519/journalisi.v4i3.288.

[47] M. A. Rivai, J. S. Suroso, and F. Pangemanan, "Review of the risk analysis using MEHARI model: The guideline to analyze risk for startup educational platform," in *Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020*, 2020. doi: 10.1109/ICIMTech50083.2020.9211204.