DAFTAR PUSTAKA

[1] M. Bhole, W. Kastner, dan T. Sauter, "IT Security Solutions for IT/OT Integration: Identifying Gaps and Opportunities," dalam *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, Padova, Italy: IEEE, Sep 2024, hlm. 01–08. doi: 10.1109/ETFA61755.2024.10710968.

[2] R. Sangkhro dan A. K. Agrawal, "Cybersecurity in Industrial Control Systems: A Review of the Current Trends and Challenges".

[3] E. Sabev, G. Pavlova, R. Trifonov, K. Raynova, dan G. Tsochev, "Analysis of practical cyberattack scenarios for wind farm SCADA systems," dalam *2021 International Conference Automatics and Informatics (ICAI)*, Varna, Bulgaria: IEEE, Sep 2021, hlm. 420–424. doi: 10.1109/ICAI52893.2021.9639550.

[4] M. Krotofil, "Security of cyber-physical systems: process-aware approach," 2023, doi: 10.15480/882.4913.

[5] S. Yuan, G. Reniers, dan M. Yang, "Integrated management of safety and security barriers in chemical plants to cope with emerging cyber-physical attack risks under uncertainties," *Reliab. Eng. Syst. Saf.*, vol. 250, hlm. 110320, Okt 2024, doi: 10.1016/j.ress.2024.110320.

[6] C. Qin, X. Hu, C. Zhong, dan Y. Zeng, "Vulnerability analysis of power system under uncertain Cyber-physical attacks based on stochastic bi-level optimization," *Sustain. Energy Grids Netw.*, vol. 42, hlm. 101647, Jun 2025, doi: 10.1016/j.segan.2025.101647.

[7] Z. H. Pang, G. P. Liu, dan Z. Dong, "Secure Networked Control Systems under Denial of service Attacks*," *IFAC Proc. Vol.*, vol. 44, no. 1, hlm. 8908–8913, Jan 2011, doi: 10.3182/20110828-6-IT-1002.02862.

[8] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, dan S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 3, hlm. 73–83, Okt 2009, doi: 10.1016/j.ijcip.2009.06.001.

[9] D. Team, "Protect Against FrostyGoop ICS Malware Targeting Operational Technology," Dragos Blog. Diakses: 26 April 2025. [Daring]. Tersedia pada: https://www.dragos.com/blog/protect-against-frostygoop-ics-malware-targeting-operational-technology/

[10] J. J. Downs dan E. F. Vogel, "A Plant-Wide Industrial Process Control Problem," *Comput. Chem. Eng.*, vol. 17, no. 3, hlm. 245–255, 1993, doi: 10.1016/0098-1354(93)80018-I.

[11] V. Alves dan F. V. Lima, "On the selection of control structures using process operability analysis," *Control Eng. Pract.*, vol. 153, hlm. 106117, Des 2024, doi: 10.1016/j.conengprac.2024.106117.

[12] L. Ye, Y. Cao, X. Yuan, dan Z. Song, "Subset Measurement Selection for Globally Self-Optimizing Control of Tennessee Eastman Process**The author Lingjian Ye gratefully acknowledge the National Natural Science Foundation of China (NSFC) (61304081), Zhejiang Provincial Natural Science Foundation of China (LQ13F030007), National Project 973 (2012CB720500) and Ningbo Innovation Team (2012B82002).," *IFAC-Pap.*, vol. 49, no. 7, hlm. 121–126, 2016, doi: 10.1016/j.ifacol.2016.07.227.

[13] W. Li, L. Xie, Y. Rong, dan Z. Wang, "Greedy Modes of Data Integrity Attacks on Industrial Control Systems: A Case Study of Tennessee Eastman Process," *Int. J. Secur. Its Appl.*, vol. 11, no. 1, hlm. 135–148, Jan 2017, doi: 10.14257/ijsia.2017.11.1.12.

[14] M. Krotofil, A. Isakov, A. Winnicki, D. Gollmann, J. Larsen, dan P. Gurikov, "Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion," dalam *Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion*, Hamburg, Germany: Hamburg University of Technology (Self-published white paper for Black Hat), 2015, hlm. 1–52. [Daring]. Tersedia pada: https://github.com/satejnik/DVCP-VAC

[15] N. Lawrence Ricker, "Decentralized control of the Tennessee Eastman Challenge Process," *J. Process Control*, vol. 6, no. 4, hlm. 205–221, Agu 1996, doi: 10.1016/0959-1524(96)00031-5.

[16] T. Larsson, K. Hestetun, E. Hovland, dan S. Skogestad, "Self-Optimizing Control of a Large-Scale Plant: The Tennessee Eastman Process," *Ind. Eng. Chem. Res.*, vol. 40, no. 22, hlm. 4889–4901, Okt 2001, doi: 10.1021/ie000586y.

[17] H. Chavoshi, A. K. Sedgh, dan H. Khaloozadeh, "Resilient Control for Cyber-Physical Systems Against Denial-of-Service Cyber Attacks Using Kharitonov's Theorem," dalam *2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, Riga, Latvia: IEEE, Okt 2023, hlm. 1–6. doi: 10.1109/ITMS59786.2023.10317694.

[18] M. Daud, R. Rasiah, M. George, D. Asirvatham, A. F. A. Rahman, dan A. A. Halim, "Denial of service: (DoS) Impact on sensors," dalam *2018 4th International Conference on Information Management (ICIM)*, Oxford: IEEE, Mei 2018, hlm. 270–274. doi: 10.1109/INFOMAN.2018.8392848.

[19] J.-M. Lee dan S. Hong, "Keeping Host Sanity for Security of the SCADA Systems," *IEEE Access*, vol. 8, hlm. 62954–62968, 2020, doi: 10.1109/ACCESS.2020.2983179.

[20] S. Sridhar dan G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," dalam *IEEE PES General Meeting*, Minneapolis, MN: IEEE, Jul 2010, hlm. 1–6. doi: 10.1109/PES.2010.5590115.

[21] D. Mishchenko, I. Oleinikova, L. Erdődi, dan B. R. Pokhrel, "The Impact of Stealthy Data Integrity Attacks on Wide-Area Monitoring System Applications," dalam *2024 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, Dubrovnik, Croatia: IEEE, Okt 2024, hlm. 1–5. doi: 10.1109/ISGTEUROPE62998.2024.10863661.

[22] B. Jeffries, S. Saravia, C. Carter, dan Z. Ankuda, "Cyber Risk to Mission Case Study".