

DAFTAR PUSTAKA

- [1] N. Sekonya dan S. Sithungu, “An Analysis of Critical Cybersecurity Controls for Industrial Control Systems,” *eccws*, vol. 22, no. 1, Art. no. 1, Jun 2023, doi: 10.34190/eccws.22.1.1157.
- [2] E. D. Emake, I. A. Adeyanju, dan G. O. Uzedhe, “Industrial Control Systems (ICS): Cyber-attacks & Security Optimization,” *International Journal of Computer Engineering and Information Technology*, vol. 12, no. 5, hlm. 31–41, Mei 2020, doi: 10.47277/IJCEIT/12(5)1.
- [3] J.-M. Flaus, *Cybersecurity of Industrial Systems*. John Wiley & Sons, 2019.
- [4] D. K V, J. S N, G. B, D. G. Chandu, dan A. Dinesh, “Security of Cyber Physical Systems,” dalam *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Mar 2023, hlm. 170–174. doi: 10.1109/ICACCS57279.2023.10112935.
- [5] W. L. Luyben, “Design and Control of a Modified Vinyl Acetate Monomer Process,” *Ind. Eng. Chem. Res.*, vol. 50, no. 17, hlm. 10136–10147, Sep 2011, doi: 10.1021/ie201131m.
- [6] M. Krotofil, “Security of cyber-physical systems: process-aware approach,” 2023, doi: 10.15480/882.4913.
- [7] “Distributor Bahan Kimia | PT. Graha Jaya Pratama Kinerja.” Diakses: 27 April 2025. [Daring]. Tersedia pada: <http://www.gratamachemical.com/info>
- [8] A. Psaltis, I. K. Kookos, dan C. Kravaris, “Plantwide control structure selection methodology for the benchmark vinyl acetate monomer plant,” *Computers & Chemical Engineering*, vol. 62, hlm. 108–116, Mar 2014, doi: 10.1016/j.compchemeng.2013.12.003.
- [9] D. M. Soares, H. A. M. Calil, dan R. M. Stephan, “Cascade Control vs Full-State Feedback,” dalam *2019 IEEE 15th Brazilian Power Electronics Conference and 5th IEEE Southern Power Electronics Conference (COBEP/SPEC)*, Des 2019, hlm. 1–6. doi: 10.1109/COBEP/SPEC44138.2019.9065696.
- [10] L. Maccarone, M. Rowland, R. Brulles, dan A. Hahn, “Design of Defensive Cybersecurity Architectures for High Temperature, Gas-Cooled Reactors,” SAND--2024-11449R, 2463004, Agu 2024. doi: 10.2172/2463004.
- [11] A. Nourian dan S. Madnick, “A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet,” *IEEE Transactions*





- on Dependable and Secure Computing*, vol. 15, no. 1, hlm. 2–13, Jan 2018, doi: 10.1109/TDSC.2015.2509994.
- [12] R. P. Griffin, U. Tatar, dan B. Yankson, *ICCWS 2022 17th International Conference on Cyber Warfare and Security*. Academic Conferences and Publishing Limited, 2022.
- [13] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, dan S. Sezer, “Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid,” dipresentasikan pada 4th International Symposium for ICS & SCADA Cyber Security Research 2016, BCS Learning & Development, Okt 2016. doi: 10.14236/ewic/ICS2016.7.
- [14] M. L. Luyben dan B. D. Tyr us, “An industrial design/control study for the vinyl acetate monomer process,” *Computers & Chemical Engineering*, vol. 22, no. 7, hlm. 867–877, Jul 1998, doi: 10.1016/S0098-1354(98)00030-1.
- [15] R. Chen, K. Dave, T. J. McAvoy, dan M. Luyben, “A Nonlinear Dynamic Model of a Vinyl Acetate Process,” *Ind. Eng. Chem. Res.*, vol. 42, no. 20, hlm. 4478–4487, Okt 2003, doi: 10.1021/ie020859k.
- [16] D. Gollmann, P. Gurikov, A. Isakov, M. Krotofil, J. Larsen, dan A. Winnicki, “Cyber-Physical Systems Security: Experimental Analysis of a Vinyl Acetate Monomer Plant,” dalam *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, dalam CPSS ’15. New York, NY, USA: Association for Computing Machinery, Apr 2015, hlm. 1–12. doi: 10.1145/2732198.2732208.
- [17] Y. Machida *dkk.*, “Vinyl Acetate Monomer (VAM) Plant Model: A New Benchmark Problem for Control and Operation Study,” *IFAC-PapersOnLine*, vol. 49, no. 7, hlm. 533–538, Jan 2016, doi: 10.1016/j.ifacol.2016.07.397.
- [18] V. Tiwari, V. Bhagat, Z. Hodekar, dan R. Rasal, “Design and Engineering of Two Phase Separator,” *ResearchGate*, Okt 2024, doi: 10.48175/IJARSCT-18854.
- [19] N. Pc dan N. Ko, “Efficient Model for Estimation of Dew Point Pressure in Gas Condensate Systems,” *PPEJ*, vol. 8, no. 4, hlm. 1–8, Des 2024, doi: 10.23880/ppej-16000397.
- [20] J. Gmehling dan M. Kleiber, “Chapter 2 - Vapor–Liquid Equilibrium and Physical Properties for Distillation,” dalam *Distillation*, A. G rak dan E. Sorensen, Ed., Boston: Academic Press, 2014, hlm. 45–95. doi: 10.1016/B978-0-12-386547-2.00002-8.





- [21] T. L. See, T. W. Horng, K. K. Lau, dan M. S. Azmi, “Modelling of High Pressure, High Concentration Carbon Dioxide Capture in Absorption Column,” *Applied Mechanics and Materials*, vol. 773–774, hlm. 1138–1142, 2015, doi: 10.4028/www.scientific.net/AMM.773-774.1138.
- [22] C. Zunino, R. Obermaisser, dan S. Petersen, “Guest Editorial Special Section on Industrial Communication Technologies and Systems,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, hlm. 2062–2065, Mei 2018, doi: 10.1109/TII.2018.2816933.
- [23] M. Gaiceanu, M. Stanculescu, P. C. Andrei, V. Solcanu, T. Gaiceanu, dan H. Andrei, “Intrusion Detection on ICS and SCADA Networks,” dalam *Recent Developments on Industrial Control Systems Resilience*, E. Pricop, J. Fattahi, N. Dutta, dan M. Ibrahim, Ed., Cham: Springer International Publishing, 2020, hlm. 197–262. doi: 10.1007/978-3-030-31328-9_10.
- [24] D. E. Seborg, D. A. Mellichamp, T. F. Edgar, dan F. J. D. III, *Process Dynamics and Control*. John Wiley & Sons, 2010.
- [25] W. L. Luyben, *Chemical Reactor Design and Control*. John Wiley & Sons, 2007.
- [26] F. Hagen, *PID Control*. Tapir Academic Press, 2004.
- [27] N. S. Nise, *Control Systems Engineering*. John Wiley & Sons, 2020.
- [28] P. J. Woolf, *Chemical Process Dynamics and Controls*. University of Michigan Engineering Controls Group, 2009.
- [29] G. Loukas, *Cyber-physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann, 2015.
- [30] K. Hemsley dan R. Fisher, “A History of Cyber Incidents and Threats Involving Industrial Control Systems,” dalam *Critical Infrastructure Protection XII*, J. Staggs dan S. Sheno, Ed., Cham: Springer International Publishing, 2018, hlm. 215–242. doi: 10.1007/978-3-030-04537-1_12.
- [31] Q. S. Qassim, N. Jamil, M. Daud, N. Ja’affar, W. A. W. Kamarulzaman, dan M. N. Mahdi, “Compromising the Data Integrity of an Electrical Power Grid SCADA System,” dalam *Advances in Cyber Security*, M. Anbar, N. Abdullah, dan S. Manickam, Ed., Singapore: Springer, 2021, hlm. 604–626. doi: 10.1007/978-981-33-6835-4_40.
- [32] S. Sridhar dan G. Manimaran, “Data integrity attacks and their impacts on SCADA control system,” dalam *IEEE PES General Meeting*, Jul 2010, hlm. 1–6. doi: 10.1109/PES.2010.5590115.





- [33] G. Y. S. Varshini dan S. Latha, "Detection of Data Integrity Attack Using Model and Data-Driven-Based Approach in CPPS," *International Transactions on Electrical Energy Systems*, vol. 2023, no. 1, hlm. 6098519, 2023, doi: 10.1155/2023/6098519.
- [34] A. Hassanzadeh *dkk.*, "A Review of Cybersecurity Incidents in the Water Sector," *Journal of Environmental Engineering*, vol. 146, no. 5, hlm. 03120003, Mei 2020, doi: 10.1061/(ASCE)EE.1943-7870.0001686.
- [35] M. M. Aslam, A. Tufail, K.-H. Kim, R. A. A. H. M. Apong, dan M. T. Raza, "A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects," *Sensors*, vol. 23, no. 18, Art. no. 18, Jan 2023, doi: 10.3390/s23187999.

