DAFTAR PUSTAKA

Adepu, S., Mathur, A., 2016, An Investigation into The Response of a Water Treatment System to Cyber-Attacks, In Proceedings of the 17th IEEE High Assurance Systems Engineering Symposium, Orlando, FL, USA, pp. 141-148.

Ahmed, C. M., Murguia, C., dan Ruths, J., 2017, Model-based Attack Detection Scheme for Smart Water Distribution Networks, *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security - ASIA CCS '17*, 2-6 April 2017, 101–113.

Alcaraz, C., Cazorla, L., dan Fernandez, G., 2014, Context-awareness using anomaly-based detectors for smart grid domains, *International Conference on Risks and Security of Internet and Systems*, 27-29 Agustus 2014, 17–34.

Anstrom, K. J. dan Murray, R. M., 2008, *Feedback Systems*, Princeton University Pers, Princeton.

Aung, K.M., 2015, Secure Water Treatment Testbed (SWaT): An Overview, Technical Report, Singapore University of Technology and Design, Singapore.

Athalye, S., Ahmed, C.M., dan, Zhou, J., 2020, A Tale of Two Testbeds: A Comparative Study of Attack Detection Techniques in CPS, dalam Rashid, A., Popov, P. (eds) Critical Information Infrastructures Security, CRITIS, Lecture Notes in Computer Science, vol 12332.

Balakumaran, S. dan Manathar, J.G., 2022, Application of Dynamic Mode Decomposition with Control (DMDc) for Aircraft Parameter Estimation, *IFAC PapersOnline, 55-1, 789-794.*

Byres, E., 2012, *7 Steps to ICS and SCADA Security*, Tofino Security.

Bhamare, D.Zolanvari, M., Erbad, A. , Jain, R., Khan, K., Meskin, N, 2020, Cybersecurity for Industrial Control Systems: A Survey, Computers & Security, Vol. 89, February 2020.

Caselli, M., Zambon, E., dan Kargl, F., 2015, Sequence-aware intrusion detection in industrial control systems, *Proceedings of the 1st ACM Workshop on Cyber-physical System Security*, 14 April 2015.

Chakraborti, S. dan Graham, M.A., 2019, Nonparametric Statistical Process Control, Wiley, New York, NY.

Goh, J., Adepu, S., Junejo, K. N., dan Mathur, A., 2017, A Dataset to Support Research in the Design of Secure Water Treatment Systems, *International Conference on Critical Information Infrastructures Security*, 10-12 Oktober 2016, 88–99.

Graham, M.A., S. Chakraborti, and Human, S.W., 2011, Nonparametric EWMA Sign Chart for Location Based on Individual Measurements, Quality Engineering, Vol. 23, Issue 3, pp 227-241.

Hadˇziosmanovi´c, D., R. Sommer, E. Zambon, and P. H. Hartel., 2014, Through the eye of the PLC: semantic security monitoring for industrial processes, *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 126–13.

Hu, Y., Yang, A., Li, H., Sun, Y., dan Sun, L., 2018, A survey of intrusion detection on industrial control systems, *International Journal of Distributed Sensor Networks*, vol. 14, No. 8

Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M., dan Sun, J., 2017, Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning, *2017 IEEE International Conference on Data Mining Workshop (ICDMW)*, 18-21 Nopember 2017, 1058-1065.

Khan, R., Maynard, P., Mclaughlin, K., et al., Laverty, D., Sezer, S., Threat Analysis of Blackenergy Malware for Synchrophasor Based Real-Time Control and Monitoring in Smart Grid, *Proceedings of the International Symposium for ICS & SCADA Cyber Security Research. Swindon: BCS Learning & Development L td, 2016:1-11.*

Kleinmann A., Amichay O., Wool A., Tenenbaum D., Bar O., Lev L., 2017, Stealthy Deception Attacks Against SCADA Systems, *International Workshop on the Security of Industrial Control Systems and Cyber-physical Systems,* 15 September 2017, 93-109.

Knapp, E.D., dan Langill, J.T., 2015, *Industrial Network Security*, Elsevier.

Katayama, T., 2005, *Subspace Methods for Systems Identification*, Springer-Verlag.

Krotofil, M., Kursawe, K., dan Gollmann, D., Securing Industrial Control Systems, dalam Alcaraz, C., *Security and Privacy Trends in the Industrial Internet of Things,* Springer, Switzerland, pp. 3-27, 2019.

Langill, J.T., 2014, *Defending Against the Dragonfly Cyber Security Attacks*, White Paper, Belden Inc.

Langner, R., 2013, *To kill a centrifuge*, Langner Communications.

Lee, R.M., Assante, M.J., Conway, T., 2016, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, SANS.

Li, L., Fu, Z., Zou, G., Mu, Z., Zhang, Q., Wang, G., Wang, P., 2020, *S*urvey on Methodology of Intrusion Detection in Industrial Control System Based on Artificial Intelligence, *International Conference on Computers and Artificial Intelligence Technologies, 94-103*

Lin, Q., Adepu, S., Verwer, S., dan Mathur, A., 2018, TABOR: A Graphical Model-based Approach for Anomaly Detection in Industrial Control Systems, *Proceedings of 2018 ACM Asia Conference on Computer and Communications Security,* 4-8 Juni 2018, 525-536.

Loukas, G., 2014, *Cyber-physical Attacks: A Growing Invisible Threat*, Elsevier.

Lun, Y., Innocenzo, Z., Malavolta, A.D., Domenica, I. Benedetto, D., dan May, S. Y., 2016, *Cyber-physical* Systems Security: a Systematic Mapping Study, *The Journal of Systems and Software 149 (2019) 174-216.*

Mashima D., Cárdenas A.A., 2012, Evaluating Electricity Theft Detectors in Smart Grid Networks, R*esearch in Attacks, Intrusions, and Defenses. RAID 2012*, Lecture Notes in Computer Science, vol 7462, 2010-229.

Mitchel, R. dan Chen, 2014, A Survey of Intrusion Detection Techniques for *Cyber-physical* Systems, *ACM Computing Surveys*, 46, 4, 55.1 -- 55.29.

Murguia, C. dan Ruths, J., 2016, Characterization of a Cusum Model-Based Sensor Attack Detector, *2016 IEEE 55th Conference on Decision and Control (CDC)*, 12-14 Desember 2016, 1303–1309.

Overschee, P.V., dan Moor, B.D., 1996, Subspace identication for linear systems: theory, implementation, applications, Boston: Kluwer Academic Publications.

Proctor, J. L., Brunton, S. L., dan Kutz, J. N., 2016, Dynamic Mode Decomposition with Control, *SIAM Jornal on Applied dynamic Systems*, 15, 1, 142–161.

Qadeer, R., Murguia, C., Ahmed, C. M., dan Ruths, J., 2017, Multistage Downstream Attack Detection in a Cyber Physical System, *Cyber ICPS Workshop 2017 in Conjunction with ESORICS 2017*, 14-15 Nopember 2017, 177-185.

Shoukry, Y., Martin, P., Yona, Y., Diggavi, S., dan Srivastava, S., 2015, PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks, *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security* (CCS), 1004–1015.

Urbina, D.I., Giraldo, J., Cardenas, A.A., Valente, J., Faisal, M., Tippenhauer, N.O., Ruths, J., Candell, R., dan Sandberg, H., 2016, *Survey and New Directions for Physics-Based Attack Detection in Control Systems*, National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

Winnicki, A., Krotofil, M., dan Gollman, D., 2017, Cyber-physical System Discovery – Reverse Engineering Physical Process, *Proceedings of the 3rd ACM Workshop on Cyber-physical System Security*, 2-6 April, 2017, 3-14

Yang, T., Murguia, C., Kuijper, M., dan Nešić, D., 2019, An Unknown Input Multi-Observer Approach for Estimation, Attack Isolation, and Control of LTI Systems under Actuator Attacks, *2019 18th European Control Conference (ECC)*, Naples, Italy, 4350-4355

Yusheng, W., Zenghui, L., Kefeng, F., Yinxiu, L., Ruikang, Z., dan Lin, L., 2017, Intrusion Detection of Industrial Control System based on Modbus TCP Protocol, *IEEE 13tth International Symposium on Autonomous Decentarlized Systems*, 22-24 Maret 2017, 156-162