DAFTAR PUSTAKA

[1] L. S. Dalenogare, G. B. Benitez, N. F. Ayala, and A. G. Frank, "The expected contribution of Industry 4.0 technologies for industrial performance," *Int J Prod Econ*, vol. 204, pp. 383–394, Oct. 2018, doi: 10.1016/j.ijpe.2018.08.019.

[2] S. Mantravadi, R. Schnyder, C. Møller, and T. D. Brunoe, "Securing IT/oT links for low power IIoT devices: Design considerations for industry 4.0," *IEEE Access*, vol. 8, pp. 200305–200321, 2020, doi: 10.1109/ACCESS.2020.3035963.

[3] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2020, pp. 1537–1543. doi: 10.1109/ETFA46521.2020.9212128.

[4] M. Pollard, "Pepperdine Policy Review Pepperdine Policy Review A Case Study of Russian Cyber-Attacks on the Ukrainian Power A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States Grid: Implications and Best Practices for the United States," *Pepperdine Policy Review*, vol. 16, pp. 4–23.

[5] S. Khan and S. Madnick, "Protecting Chiller Systems from Cyberattack Using a Systems Thinking Approach," *Network*, vol. 2, no. 4, pp. 606–627, Dec. 2022, doi: 10.3390/network2040035.

[6] P. Celeda, J. Vykopal, V. Svabensky, and K. Slavicek, "KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems," in *SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, Feb. 2020, pp. 1026–1032. doi: 10.1145/3328778.3366908.

[7] Wm. A. Conklin, "IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilienc," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 2642–2647. doi: 10.1109/HICSS.2016.331.

[8] A. Ocaka, D. Ó Briain, and K. Barrett, "Evaluating the Impact of Cyberattacks on PLC Performance: A Systematic Implementation and Empirical Investigation," in *IFAC-PapersOnLine*, Elsevier B.V., Jun. 2024, pp. 387–392. doi: 10.1016/j.ifacol.2024.07.182.

[9] W. B. W Mariam and Y. Negash, "Performance evaluation of machine learning algorithms for detection of SYN Flood Attack," in *IEEE AFRICON Conference*, Institute of Electrical and Electronics Engineers Inc., Sep. 2021. doi: 10.1109/AFRICON51333.2021.9570968.

[10] P. D. Bojovic, I. Basicevic, S. Ocovaj, and M. Popovic, "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method," Nov. 2018, doi: 10.1016/j.compeleceng.2018.11.004.

[11] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," Feb. 01, 2020, *Elsevier Ltd*. doi: 10.1016/j.cose.2019.101677.

[12] R. Paes, D. C. Mazur, B. K. Venne, and J. Ostrzenski, "A Guide to Securing Industrial Control Networks: Integrating IT and OT Systems," *IEEE Industry Applications Magazine*, vol. 26, no. 2, pp. 47–53, Mar. 2020, doi: 10.1109/MIAS.2019.2943630.

[13] P. K. Garimella, "IT-OT Integration Challenges in Utilities," in *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, 2018, pp. 199–204. doi: 10.1109/CCCS.2018.8586807.

[14] K. H. John and M. Tiegelkamp, *IEC 61131-3: Programming industrial automation systems: Concepts and programming languages, requirements for programming systems, decision-making aids*. Springer Berlin Heidelberg, 2010. doi: 10.1007/978-3-642-12015-2.

[15] A. Kumar Dubey and R. P. Chauhan, "Effective Boiler Automation using PLC and SCADA," *REFERENCE HANDBOOK ON POWER, CONTROL 4 COMMUNICATION SYSTEMS*, 2016.

[16] W. Bolton, *Programmable Logic Controllers W. Bolton*. Newnes/Elsevier, 2016.

[17] A. Moftah, S. I. Almoshity, A. Majeed, and A. Ghafeer, "Design of Control System for Concrete Machine based on PLC and HMI," *African Journal of Advanced Pure and Applied Sciences (AJAPAS)*, pp. 489–496, 2024.

[18] D. F. Sea Cos-p, "S7-1500," 2013. [Online]. Available: https://www.siemens.com/industrialsecurity

[19] O. Eigner, P. Kreimel, and P. Tavolato, "Identifying S7comm Protocol Data Injection Attacks in Cyber-Physical Systems," BCS Learning & Development, 2018. doi: 10.14236/ewic/ics2018.6.

[20] H. Hui, K. McLaughlin, and S. Sezer, "Vulnerability analysis of S7 PLCs: Manipulating the security mechanism," *International Journal of Critical*

Infrastructure Protection, vol. 35, Dec. 2021, doi: 10.1016/j.ijcip.2021.100470.

[21] Saber Mhiri, "INPROSEC-AUTO 1 Analyzing an OT network, what to expect Saber Mhiri."

[22] W. B. W Mariam and Y. Negash, "Performance evaluation of machine learning algorithms for detection of SYN Flood Attack," in *IEEE AFRICON Conference*, Institute of Electrical and Electronics Engineers Inc., Sep. 2021. doi: 10.1109/AFRICON51333.2021.9570968.

[23] W. O. Nl and M. Joren, "Open Universiteit MASTER'S THESIS SIMATIC FUZZ: FUZZING THE S7 COMMUNICATION PROTOCOL." [Online]. Available: https://research.ou.nl/

[24] Geoffrey Alexander; Jedidiah R. Crandall, "2015 IEEE Conference on Computer Communications (INFOCOM)," *2015 IEEE Conference on Computer Communications (INFOCOM)*, 2015, doi: 10.1109/INFOCOM.2015.7218538.

[25] W. O. Nl and M. Joren, "Open Universiteit MASTER'S THESIS SIMATIC FUZZ: FUZZING THE S7 COMMUNICATION PROTOCOL." [Online]. Available: https://research.ou.nl/

[26] Q. Gu and P. Liu, *Denial of Service Attacks*. Handbook of Computer Network: Distributed Network, Network Planning, Control, Management, and New Trends and Applications.

[27] G. Sujatha, Y. Kanchal, and G. George, "An Advanced Approach for Detection of Distributed Denial of Service (DDoS) Attacks Using Machine Learning Techniques," in *3rd International Conference on Smart Electronics and Communication, ICOSEC 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 821–827. doi: 10.1109/ICOSEC54921.2022.9951944.

[28] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics. "cybernetics evolving to systems, humans, organizations, and their complex interactions" (cat. no.0*, 2000, pp. 2275–2280 vol.3. doi: 10.1109/ICSMC.2000.886455.

[29] A. Khamosh, M. A. Anwer, N. Nasrat, J. Hamdard, G. S. Gawhari, and A. R. Ahmadi, "Impact of Network QoS factors on QoE of IoT Services," in *2020 - 5th International Conference on Information Technology (InCIT)*, 2020, pp. 61–65. doi: 10.1109/InCIT50588.2020.9310969.

[30] Y. D. Lin, "Editorial: Third quarter 2018 IEEE communications surveys and tutorials," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 1607–1615, Jul. 2018, doi: 10.1109/COMST.2018.2862278.

[31] W. Sugeng, J. Eko Istiyanto, K. Mustofa, and A. Ashari, "The Impact of QoS Changes towards Network Performance," 2015. [Online]. Available: www.ijcncs.org

[32] R. Sharpe, E. Warnicke, and U. Lamping, "Wireshark User's Guide Preface Foreword." [Online]. Available: https://www.wireshark.org/docs/

[33] R. Christensen, *Analysis of Variance, Design, and Regression*, vol. 2. CRC Press, 2016. Accessed: Feb. 09, 2025. [Online]. Available: http://ndl.ethernet.edu.et/bitstream/123456789/33758/1/Ronald%20Christensen_2016.pdf

[34] K. Takeaways, "Lesson 1: Central Limit Theorem and Sampling Distribution of í µí±‹ ¯."

[35] MINITAB ASSISTANT WHITE PAPER, "One-Way ANOVA Overview." Accessed: Feb. 09, 2025. [Online]. Available: https://support.minitab.com/minitab/media/pdfs/translate/Assistant_One_Way_ANOVA.pdf

[36] NCSS and LLC, "NCSS Statistical Software Individuals and Moving Range Charts."