DAFTAR PUSTAKA

Abdo, H., Kaouk, M., Flaus, J. and Masse, F., 2017. A safety / security risk analysis approach of Industrial Control Systems : A cyber bowtie - combining new version of attack tree with bowtie analysis. *Computers & Security*, 72, pp.175-195. Available at: https://doi.org/10.1016/j.cose.2017.09.004.

Ahn, W., Chung, M., Min, B.G. and Seo, J., 2015. Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs. *International Journal of Distributed Sensor Networks*, 2015.

Alcaraz, C. and Zeadally, S., 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, pp.53–66.

Ali, S., 2021. Cybersecurity management for distributed control system : systematic approach. *Journal of Ambient Intelligence and Humanized Computing*, (0123456789). Available at: https://doi.org/10.1007/s12652-020-02775-5.

Ashibani, Y. and Mahmoud, Q.H., 2017. Cyber physical systems security : Analysis , challenges and solutions. *Computers & Security*, 68, pp.81–97. Available at: http://dx.doi.org/10.1016/j.cose.2017.04.005.

Aven, T., 2013. Practical implications of the new risk perspectives. *Reliability Engineering and System Safety*, 115, pp.136–145.

BAPETEN, N.E.R.A., 2012. BAPETEN Chairman Regulation No.6/2012 (Peraturan Kepala BAPETEN No.6/2012 tentang Desain Sistem Yang Penting Untuk Keselamatan Berbasis Komputer Pada Reaktor Daya).

BAPETEN, N.E.R.A., 2012. BAPETEN Government Regulation No.54/2012 (Peraturan Pemerintah No.54/2012 tentang Keselamatan dan Keamanan Instalasi Nuklir)

Bou-harb, E., 2016. A Brief Survey of Security Approaches For Cyber-Physical Systems.

Bou-Harb, E., Debbabi, M. and Assi, C., 2014. Cyber scanning: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 16(3), pp.1496–1519.

Cho, H.S. and Woo, T.H., 2017. Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs). *Annals of Nuclear Energy*, 99, pp.47–53.

Daria, G. and Massel, A., 2018. Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility. *IEEE Explore*.

El-genk, M.S., Altamimi, R. and Schriener, T.M., 2021. Annals of Nuclear Energy Pressurizer dynamic model and emulated programmable logic controllers for nuclear power plants cybersecurity investigations. *Annals of Nuclear Energy*, 154, p.108121. Available at: https://doi.org/10.1016/j.anucene.2020.108121.

Fan, X., Fan, K., Wang, Y. and Zhou, R., 2015. Overview of cyber-security of industrial control system. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings*.

FTA(Federal Transit Administration), 2004. Risk Analysis Methodologies and Procedures, *United States Department of Transportation, Washington DC*

Hahndel, StefanDraeger, J., 2019. Simulation-based Unified Risk Assessment for Safety and Security. , (September 2017).

Hashim, N.A., Abidin, Z.Z., Zakaria, N.A. and Ahmad, R., 2018. Risk Assessment Method for Insider Threats in Cyber Security : A Review. *IJACSA International Journal of Advanced Computer Science and Applications*, 9(11), pp.126–130.

Henshel, D., Alexeev, A., Cains, M., Rowe, J., Cam, H., Hoffman, B. and Neamtiu, I., 2016. Modeling cybersecurity risks: Proof of concept of a holistic approach for integrated risk quantification. *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*.

Holm, H., Shahzad, K., Buschle, M. and Ekstedt, M., 2015. P 2 CySeMoL : Predictive , Probabilistic Cyber Security Modeling Language. *IEEE Transactions on Dependable and Secure Computing*, 12(6), pp.626–639.

IAEA, 2016. IAEA SAFETY GLOSSARY. *International Atomic Energy Agency, Vienna*, p.219.

IAEA, I.A.E.A., 2011. IAEA Nuclear Security Series No. 17 Computer Security at Nuclear Facilities. *IAEA Nuclear Security Series*, (17).

IAEA, I.A.E.A., 2015. IAEA Nuclear Security Series No. 23-G Security of Nuclear

Information. IAEA Nuclear Security Series, (23).

IAEA, I.A.E.A., 2009. Development , Use and Maintenance of the Design Basis Threat. , *IAEA Nuclear Security Series No.10*

IAEA, I.A.E.A., 2008. Preventive and Protective Measures against Insider Threat., *IAEA Implementing Guide Nuclear Security Series No.8*

IAEA, I.A.E.A., 2021. National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements. *IAEA Nuclear Security Series No 10-G*, (Rev-1).

IAEA, I.A.E.A., 2008. IAEA Nuclear Security Series No.7 Nuclear Security Culture. *IAEA Nuclear Security Series*, (7).

IAEA, I.A.E.A., 1994. Nuclear Non-Proliferation Treaty and Global Non-Proliferation Regime: A US Policy Agenda, The. *BU Int'l LJ*, 12(April), p.407.

ISO/IEC, 2005. INTERNATIONAL STANDARD ISO / IEC 27001 Information Security Management System. *Information Systems*, 2005.

Ivanchenko, O., Kharchenko, V., Moroz, B., Kabak, L. and Konovalenko, S., 2018. Risk Assessment of Critical Energy Infrastructure Considering Physical and Cyber Assets : Methodology and Models. In *IEEE International Symposium on Wireless Systems*. IEEE, pp. 225–228.

Karabacak, B., Yildirim, S.O. and Baykal, N., 2016. A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, 15, pp.47–59.

Kim, D.-Y., 2014. Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy*, 65, pp.141–143.

Kim, H.E., Son, H.S., Kim, J. and Kang, H.G., 2017. Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants. *Reliability Engineering and System Safety*, 167(August 2016), pp.290–301. Available at: http://dx.doi.org/10.1016/j.ress.2017.05.046.

Kim, Sangwoo, Kim, Seung-min, Nam, K., Kim, Seonuk and Kwon, K., 2021. Security Information and Event Management Model Based on Defense-in-Depth Strategy for Vital Digital Assets in Nuclear Facilities. *Advances in Computer Science and Ubiquitous Computing*, pp.331–339. Available at: http://dx.doi.org/10.1007/978-981-15-9343-7_46.

Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K., 2015. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, pp.52–80.

Kumar, D. and Ghosh, R., 2018. Journal of Information Security and Applications Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security. *Journal of Information Security and Applications*, 40, pp.173–182. Available at: https://doi.org/10.1016/j.jisa.2018.04.002.

Lallie, H.S., Debattista, K. and Bal, J., 2018. Evaluating practitioner cyber-security attack graph configuration preferences. *Computers & Security*, 79, pp.117–131. Available at: https://doi.org/10.1016/j.cose.2018.08.005.

Lee, C., 2013. *Introduction of a Cyber Security Risk Analysis and Assessment System for Digital I & C Systems in Nuclear Power Plants*, IFAC. Available at: http://dx.doi.org/10.3182/20130619-3-RU-3018.00311.

Lee, C., Bin, H. and Hyun, P., 2018. Annals of Nuclear Energy Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept. *Annals of Nuclear Energy*, 112, pp.646–654.

Lee, C., Chae, Y.H. and Seong, P.H., 2021. Annals of Nuclear Energy Development of a method for estimating security state : Supporting integrated response to cyber-attacks in NPPs. *Annals of Nuclear Energy*, 158, p.108287. Available at: https://doi.org/10.1016/j.anucene.2021.108287.

Lee, C., Han, S.M. and Seong, P.H., 2020. Annals of Nuclear Energy Development of a quantitative method for identifying fault-prone cyber security controls in NPP digital I & C systems. *Annals of Nuclear Energy*, 142, p.107398. Available at: https://doi.org/10.1016/j.anucene.2020.107398.

Leszczyna, R., 2018. Computer Standards & Interfaces Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Computer Standards & Interfaces*, 56(April 2017), pp.62–73. Available at: https://doi.org/10.1016/j.csi.2017.09.005.

Leuprecht, C., Skillicorn, D.B. and Tait, V.E., 2016. Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, 33(2), pp.250–257. Available at: http://dx.doi.org/10.1016/j.giq.2016.01.012.

Mandelli, D., Yilmaz, A., Aldemir, T., Metzroth, K. and Denning, R., 2013. Scenario clustering and dynamic probabilistic risk assessment. *Reliability*

Engineering and System Safety, 115, pp.146–160.

Nagaraju, V., Fiondella, L. and Wandji, T., 2017. A Survey of Fault and Attack Tree Modeling and Analysis for Cyber Risk Management. *IEEE International Symposium on Technologies for Homeland Security (HST)*, pp.1–6.

Orojloo, H. and Azgomi, M.A., 2017. A method for evaluating the consequence propagation of security attacks in cyber – physical systems. *Future Generation Computer Systems*, 67, pp.57–71.

Oughton, E.J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., Dada, R., Ruffle, S., Tuveson, M. and Hall, J.W., 2019. Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. , 39(9).

Park, J. and Suh, Y., 2013. A Development Framework for Software Security in Nuclear Safety Systems: Integrating Secure Development and System Security Activities. *Nuclear Engineering and Technology*, 46(1), pp.47–54. Available at: http://dx.doi.org/10.5516/NET.04.2012.061.

Park, J., Suh, Y. and Park, C., 2016. Implementation of cyber security for safety systems of nuclear facilities. *Progress in Nuclear Energy*, 88, pp.88–94.

Park, J.W. and Lee, S.J., 2020. Annals of Nuclear Energy A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence. *Annals of Nuclear Energy*, 142, p.107432.

Park, Jaekwan, Park, Jeyun and Kim, Y., 2013. Progress in Nuclear Energy: A graded approach to cyber security in a research reactor facility. *Progress in Nuclear Energy*, 65, pp.81–87..

Peterson, J., Haney, M. and Borrelli, R.A., 2019. An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. *Nuclear Engineering and Design*, 346(February), pp.75–84. Available at: https://doi.org/10.1016/j.nucengdes.2019.02.025.

Porcedda, M.G., 2018. Patching the patchwork : appraising the EU regulatory framework on cyber security breaches. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 000, pp.1–22.

Ralston, P.A.S., Graham, J.H. and Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Transaction, 46, pp.583–594.

Saleh, Z.I., Refai, H. and Mashhour, A., 2011. Proposed Framework for Security

Risk Assessment. , 2011(April), pp.85–90.

Setianingsih, L.S., Pulungan, R, Putra, A.E., Wibowo, M.E., and Syarip, 2021. "Risk Assessment Methods for Cybersecurity in Nuclear Facilities: Compliance to Regulatory Requirements" International Journal of Advanced Computer Science and Applications(IJACSA), 12(9), 2021, pp.714-722.

Shabut, A.M., 2016. Cyber Attacks , Countermeasures , and Protection Schemes – A State of the Art Survey. *10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA) Cyber*, pp.37–44.

Shin, J., Son, H. and Heo, G., 2016. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nuclear Engineering and Technology*, (2016), pp.4–11.

Shin, J., Son, H., Khalil, R. and Heo, G., 2015. Development of a cyber security risk model using Bayesian networks. *Reliability Engineering and System Safety*, 134, pp.208–217.

Syed, R., 2020. Information & Management Cybersecurity vulnerability management : A conceptual ontology and cyber intelligence alert system. *Information & Management*, 57(6), p.103334.

USNRC, 1981. Fault Tree Handbook, *NUREG 0492*, (January), Washington D.C

USNRC, 2010. REGULATORY GUIDE 5.71 Cyber Security Programs for Nuclear Facilities, (January), pp.1–105.

US Department Homeland Security, 2010. The Design Basis Threat (U), *Interagency Security Committee Report*.

Vessels, L., Ph, D., Heffner, K. and Ph, D., 2019. Cybersecurity Risk Assessment for Space Systems. *IEEE Space Computing Conference*, pp.11–19.

Wang, Z., Zhu, H. and Sun, L., 2021. Social Engineering in Cybersecurity : Effect Mechanisms , Human Vulnerabilities and Attack Methods. *IEEE Access*, 9, pp.11895–11910.

Yang, S., Cao, Y., Wang, Y., Zhou, C. and Yue, L., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process Safety and Environmental Protection*, 148, pp.1279–1291.

Yousefnezhad, N., Malhi, A. and Främling, K., 2020. Journal of Network and Computer Applications Security in product lifecycle of IoT devices : A survey.

Journal of Network and Computer Applications, 171(January), p.102779.

Zio, E., 2018. The future of risk assessment. *Reliability Engineering and System Safety*, 177(June 2017), pp.176–190.