IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

Cyber Resilience Approaches for Cyber Physical Systems

Manjunath D[1] and Dr. M. N. Nachappa[2]
PG Student, Department of MSc CS-IT[1]
Professor, School of CS & IT[2]
Jain (Deemed-to-be University), Bangalore, India
1manjunathmanju200129@gmail.com

Abstract: *Cyber-physical systems (CPS) integrate physical processes with computing, communication, and control systems to increase efficiency, reliability, and safety. However, these systems are also vulnerable to cyber attacks, which could have severe consequences, such as loss of life, property damage, and economic disruption. To ensure the safety and security of modern society, it is crucial to ensure that CPS are cyber-resilient, meaning they can continue to function and recover from cyber attacks. This requires a multi-faceted approach that includes secure design, risk assessment, monitoring and response, redundancy and backup, and training and education. By implementing these strategies, organizations can improve the cyber resilience of theirCPS, reducing the risk of cyber attacks and promoting the safety and security of modern society.*

Keywords: Cyber Attacks, CPS, Physical Components, Risk Assessment

REFERENCES

[1] X. Ge, F. Yang, and Q. Han. Distributed networked control systems: A brief overview. Information Sciences, 380:117–131, February 2017.
[2] X. M. Zhang, Q. L. Han, and X. Yu. Survey on Recent Advances in Networked Control Systems. IEEE Transactions onIndustrial Informatics, 12(5):1740–1752, October 2016.
[3] L. Zhang, H. Gao, and O. Kaynak. Network-induced constraints in networked control systems — a survey. IEEE Transactions on Industrial Informatics, 9(1):403–416, 2013.
[4] Y. Z. Lun, A. D'Innocenzo, I. Malavolta, and M. D. Di Benedetto. Cyber-Physical Systems Security: a Systematic Mapping Study. Journal of Systems and Software, 149:174–216, March 2019. arXiv: 1605.09641.
[5] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson. Attack Models and Scenarios for Networked Control Systems.In Proceedings of the 1st International Conference on High Confidence Networked Systems, HiCoNS '12, pages 55–64, New York,NY, USA, 2012. ACM.
[6] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. A secure control framework for resource- limited adversaries.Automatica, 51:135–148, 2015.
[7] L. Fillatre, I. Nikiforov, P. Willett, et al. Security of scada systems against cyber–physical attacks. IEEE Aerospace andElectronic Systems Magazine, 32(5):28–45, 2017.
[8] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat. Cyber-physical systems and their security issues. Computers inIndustry, 100:212–223, 2018.
[9] N. Falliere, L. O. Murchu, and E. Chien. W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5:6,2011.
[10] D. Corman, V. Pillitteri, S. Tousley, M. Tehranipoor, and U. Lindqvist. NITRD Cyber-Physical Security Panel. 35th IEEE Symposium on Security and Privacy, IEEE S&P 2014, San Jose, CA, USA, May 18-21.
[11] D. U. Case. Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and AnalysisCenter (E-ISAC), 2016.
[12] J. Slay and M. Miller. Lessons learned from the maroochy water breach. In Critical Infrastructure Protection, pages73–82, Boston, MA, 2008. Springer US.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

[13] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo. Bibliographical review on cyber attacks from acontrol oriented perspective. Annual Reviews in Control, 48:103–128, 2019.
[14] Y. L. Huang, A. A. Cárdenas, S. Amin, Z. S. Lin, H. Y. Tsai, and S. Sastry. Understanding the physical and economicconsequences of attacks on control systems. International Journal of Critical Infrastructure Protection, 2(3):73 – 83, 2009.