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 1, September 2024

Advancing Threat and Risk Analysis with a Combined Approach: Asset Container Method and CWSS Integration

Mr. Mounesh A, Ms. Shikha Shetty, Ms. Shilpa, Ms. Shilpa A, Mr. Showrya Shetty
Department of CSE (IoT, Cyber Security including BlockChain)
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India
mouneshstjit25@gmail.com , shikashetty2013@gmail.com , shilpashettigar102@gmail.com ,
mail2shilpa.ajeru@gmail.com, showryashetty20112004@gmail.com

Abstract: *In recent years, the development of cybersecurity standards for cyber-physical systems, such as automotive systems, has seen significant progress. One key development is ISO/SAE 21434, released in 2021, which provides a framework for managing and analyzing cybersecurity in the electrical systems of road vehicles. This standard also introduces methods for the Threat Analysis and Risk Assessment (TARA) process. However, current security analysis techniques face two notable challenges: first, the conventional CVSS-based approach is inadequate for assessing attack feasibility in cyber-physical systems. Second, the relationship between damage factors and their impact on assets remains unclear. This paper addresses these issues by enhancing the TARA process through the use of the "asset container" method for threat classification, as proposed at DECSoS 2017, alongside a CWSS-based risk quantification approach. Furthermore, the paper suggests improvements to risk evaluation methods specifically tailored for automotive systems, focusing on direct access attacks on in-vehicle networks.*

Keywords: Risk quantification and cognitive bias reduction in automotive cybersecurity

DOI: 10.48175/IJARSCT-19513