

Product cybersecurity- Security testing methodologies for Earth Moving Machinery

Sheela Hariharan^{1,2}, Andreas Erséus², Thomas Nolte¹, and Alessandro V. Papadopoulos¹

¹ Mälardalen University, Västerås, Sweden {name.surname}@mdu.se

² Volvo Construction Equipment, Eskilstuna, Sweden {name.surname}@volvo.com

Abstract:

Modern connectivity and cyber-physical systems are becoming increasingly prominent in products such as earth-moving machinery. Safety-critical systems have become more complex as technology advances, with cybersecurity becoming more important. As a result of interdependencies and network connectivity, attack surfaces and vulnerabilities have grown significantly. To prevent cyberattacks on machinery segments, it is imperative to perform a risk assessment and implement robust security testing methods [1]. In the recent systematic mapping study, the importance of analyzing security testing in the development lifecycle and the use of automotive cybersecurity testbeds were discussed in detail [2].

Specifically, we study security testing methodologies to secure that earth-moving machinery meets security standards and regulations against cyber resilience. We plan to build the testing framework on top of penetration testing, fuzzing, and model-based testing. As part of this research, security requirements will be verified, and hidden vulnerabilities will be investigated in embedded system software as a black box method. Finally, the developed testing method will be tested on earth-moving machinery electronic units and digital construction sites connectivity solutions. Additionally, we discuss the standards, regulations, and challenges associated with implementing security testing in construction machinery. For our final work, we plan to implement most validation methods using hardware-in-loop systems, Linux-based penetration testing tools, and modeling tools to ease the tester's workload in evaluating machinery security. Since security compromises safety in many ways, this work also utilizes threat modeling tools and functional safety measures to identify the safety critical risks. The results of the tests will be used to develop a more secure system with better safety measures. This will help to ensure that the system is safe for use in industrial settings and will also help to identify and address any potential security issues.

Keywords: Security testing, Cybersecurity testbeds, Threat modeling, Earth moving machinery.

References:

- [1] D'Anna, G.: Cybersecurity for Commercial Vehicles book. SAE International (2018)
- [2] Luo, F.; Zhang, X.; Yang, Z.; Jiang, Y.; Wang, J.; Wu, M.; Feng, W. Cybersecurity Testing for Automotive Domain: A Survey. *Sensors* 2022, 22, 9211. <https://doi.org/10.3390/s22239211>