Automotive Cyber Security Portfolio

Secure and Compliant From Design to Post-Production

A wide variety of control units and software nodes are connected in the vehicle and the complexity will increase.

V2X, charging station and interconnectivity will provide more and more access points and so the development and the validation of the system must follow the complexity and the growing challenges to guarantee the system's integrity, security, and invulnerability to all the possible attacks that could be addressed to every port.

THE CHALLENGE

Compliance with new regulations, including UN R155 and UN R156 is now mandatory for car manufacturers to ensure the security of connected vehicles. To be compliant, carmakers should follow the guidelines provided by standards like ISO 21434 and ISO 24089. To secure communication, access control, and data privacy these regulations set standards to implement a CSMS as well as a Software Update Management System (SUMS) throughout the vehicle lifecycle. All stages of the development process, starting from the initial design and continuing through the entire product's lifespan, must adhere to ISO standards. Additionally, it's important to note that the upcoming requirements in July 2024 will demand even greater attention and effort within the automotive industry,

THE AVL SOLUTION

AVL's portfolio covers all the essential elements required for cybersecurity certification. This includes expertise in engineering to oversee and execute the necessary activities throughout the entire development cycle, as well as the use of tools that enhance quality, save time and resources, and optimize efficiency in both the development and testing phases.

Our tool portfolio and engineering services support you in conducting TARAs (Threat Analysis and Risk Assessment), analyzing the attack paths, generating the security concept, testing it and assuring the security of the system over its whole lifecycle by helping you setting up the Cyber Security Management System.

THE ADDED VALUE

AVL's distinctive value proposition in the market is the combination of its expertise and tools. We offer an easily accessible and interconnected set of tools that guide engineers through the entire process, encompassing secure-by-design principles, automated penetration testing, and an efficient management of vulnerabilities for all your software variants. This toolset is accessible to engineering teams globally, connecting them to the entire AVL group and providing a thorough grasp of the necessary legislative requirements.

Automotive Cybersecurity Portfolio

THREAT ANALYSIS & RISK ASSESSMENT (TARA)

This analysis is critical for the entire development process, starting at the project's outset. It shapes hardware design, software development, and remains relevant throughout the vehicle's lifecycle.

AVL FUSE™

Years of experience transformed into an ISO certified, understandable and integrable, ready-to-use process tool. One central place to manage all project activities internally & externally (suppliers, customers) according to standards & regulations. Continuously updated process models provide auto-generation of all kinds of reports for reviews, audits, and assessments.

CONCEPT DEVELOPMENT

Based on high-level security objectives out of TARA we carry out the development of secure-by-design architecture and allocation of security requirements to the components.

AVL THREATGET™

A tool aiming to a time reduction of up to 80% for TARA analysis compared to manual approach. Automated generation of threats, risks and attack tree based on an easily understandable system model. Continuously updated database of weaknesses, vulnerabilities, and attack patterns. Reusable and extendable set of elements with predefined security properties for system modeling.

IMPLEMENTATION

Consists of secure software implementation, hardware design and operating systems and their configurations with respect to valid security-oriented technical standards.

VULNERABILITY MANAGEMENT WITH AVL CRETA™

Automated vulnerability scanning triggered and managed in AVL CRETA, the leading software variant management tool used by 8 of the Top 10 global OEMs. Efficiently manage vulnerabilities of all your software variants by connecting AVL CRETA to the vulnerability scanner of your choice – enabled by AVL CRETA's powerful API.

VERIFICATION & VALIDATION

Vulnerability scan and assessment, functional security testing and penetration testing measures for verification and validation to proof the compliance of the technical solution.

AVL CYBERSECURITY TESTING

Modular testing platform combining well-known IT cybersecurity testing tools with tailored automotive testing modules. Seamless security tests from office to road by supporting all test environments (SiL to road). Automation of security process supporting the generation of test cases based on the security concept. High reproducibility due to standardized test modes.

CONTINUOUS SYSTEM CARE

Describes the Security Life Cycle Management by AVL. It monitors the used security mechanisms, hardware, and implementations from development until decommissioning and provides solutions and fixes if new vulnerabilities occur.

FIND OUT MORE

AVL List GmbH
Hans-List-Platz 1
8020 Graz

www.avl.com

June 2023, Classification Public