AVL SecGuard

Get Ready for Automotive Cyber Security

Securing a Safe Future Together

ENSURING SECURITY AND SAFETY IN THE EVOLVING AUTOMOTIVE INDUSTRY

In recent years the automotive industry has experienced the increasing incidence of cyber security attacks and related cyber security regulations. With vehicles transforming into more software-defined, fully connected products, the probability and vulnerability to cyber-attacks have increased considerably. Also, the development of autonomous or semi-autonomous vehicles and other safety systems introduces additional cyber security challenges. Thus, a secure vehicle lifecycle starting with a „secure-by-design" mindset has become a paramount concern for automakers, regulators, and consumers alike.

Governments and regulatory bodies are increasingly recognizing the importance of cyber security in the automotive industry and constantly implementing new standards and legal regulations to ensure the security of connected vehicles. Cyber security now forms an integrational component of vehicle homologation, rendering it mandatory for OEMs to furnish evidence of compliance. The OEMs and Tiers must implement cyber security-by-design to become compliant and pass the type approval.

PIONEERING CYBER SECURITY SOLUTIONS FOR THE FUTURE OF CONNECTED VEHICLES

Committed to innovating and shaping the future of safe and secure vehicles, AVL has developed a comprehensive software suite, AVL SecGuard. The software-suite accompanies you into the future of cyber security in the automotive industry from identifying potential threats and assessing their impact (TARA) to the definition of robust security requirements for building future-proof concepts that encompass the whole vehicle with all its components.

Increased automation in testing, along with the integration of CI/CD for continuous automotive testing, is crucial. This approach allows for exceptional cyber security testing benefits.

However, AVL's offering doesn't stop there. To maintain cyber security, vehicles must be constantly assessed and tested and kept up-to-date with the latest security patches and updates. Therefore, AVL's comprehensive solution extends beyond the start of production, providing a reliable long-term solution for security, compliance and certification.

> "Simplifying everything from threat identification to continuous testing is an integrational part to ensure vehicles stay secure and compliant throughout their lifecycle. Leveraging our expertise to bring more standardization and automation to automotive cyber security is what AVL stands for.

From Code to Road: Safe and Secure Over The Whole Vehicle Lifecycle

A structured cyber security approach is crucial to ensure the safety and security of modern vehicles. A systematic and continuous process must be followed throughout the entire vehicle lifecycle to ensure cyber security for manufacturers, suppliers, and end consumers. AVL supports these efforts throughout the complete process with the AVL SecGuard software suite:

1. Project Planning
The first step is to define the project scope and ensure compliance with cyber security regulations, such as UNECE R155 and ISO 21434 or China GB and GB/Ts. Companies must identify the legal requirements for each market where the vehicle will be sold.

AVL's ComplyGuard provides predefined process models and templates that enable companies to rapidly set up their development projects, including managing workproducts across the supply chain, ensuring compliance.

2. Threat Analysis & Risk Assessment
A comprehensive Threat Analysis and Risk Assessment (TARA) must be performed to identify potential threats and attack paths, as well as their impact and likelihood in relevant vehicle systems and assets. This helps to determine which systems are at risk, how to protect them and to allocate resources efficiently.

AVL ThreatGuard supports TARA with a model-based and highly automated approach, enabling efficient identification and assessment of threats. This speeds up risk assessments, ensuring that security is embedded early in the development process and maintained throughout the vehicle's life.

3. Cyber Security Concept Development
After the TARA, a cyber security concept is developed to outline the necessary security measures for mitigating identified threats. This concept should cover all critical vehicle components, specifying security requirements for both hardware and software.

4. Implementation
The next step involves the implementation of the defined security controls, including e.g. firewalls, encryption, and secure boot mechanisms to protect against cyber-attacks.

5. Testing
Once security controls are implemented, extensive testing of both software and hardware is necessary to validate their robustness and ensure thorough coverage of the identification of potential vulnerabilities.

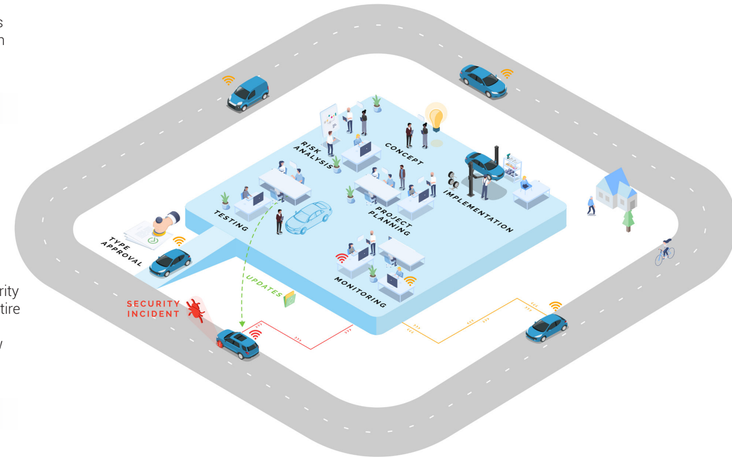
AVL TestGuard enables automated security testing with customizable test plans for functional, fuzz, and penetration testing, helping validate the security of the vehicle's systems and ensuring compliance with regulations and standards (e.g. China GB and GB/Ts).

6. Type Approval & Certification
Before a vehicle enters the market, OEMs must demonstrate cyber security compliance as part of type approval. This includes providing documentation that proves the security measures align with the required standards and regulations.

AVL ComplyGuard supports built-in audit and assessment functionalities and simplifies the creation of homologation documents by offering automated compliance management, ensuring that OEMs meet regulatory requirements for various markets efficiently.

7. Lifecycle Management
Cyber security does not end at production – even more the security measures have to be maintained and updated throughout the entire lifecycle. After vehicles are on the road, continuous monitoring and software updates are necessary to identify and mitigate new vulnerabilities and threats that arise over time.

AVL TraceGuard helps OEMs to track and manage software updates, including RxSWIN numbers, ensuring compliance with the Software Update Management System (SUMS) and supporting long-term vulnerability management ensuring compliance with regulations like UNECE R156.



The Cyber Security Software-Suite at A Glance

AVL ThreatGuard - Mitigate Cyber Threats to a Minimum

Threat Analysis & Risk Assessment

AVL ThreatGuard is a solution for efficiently modeling security concepts for connected vehicle systems and their components. It stands out as the preferred choice for automated analysis and identification of cyber security threats. Employed from the earliest stages of design through development and into operation, ThreatGuard offers structured and timely detection of cyber-related security risks. Powered by its extensive, continuously updated threat catalog and high degree of automation, generating a security concept or identifying vulnerability impacts becomes effortless. Simply import or model your system and let AVL ThreatGuard fully automatically generate a first version of the Threat Analysis and Risk Assessment (TARA) including the potential Attack Paths for you.

- **Automated:** Automatically derive a first version of your TARA and attack trees and simply refine it instead of building everything up from scratch
- **Future-proof:** Reliable database of a myriad of Automotive Cyber Threats with constant threat intelligent updates
- **Reproducible:** Traceable and reproducible results thanks to a rule-based threat analysis and risk assessment based on imported or directly modeled components and systems

AVL TestGuard - Put Security First With Intelligent Verification and Validation

Cyber Security Testing

AVL TestGuard represents the all-in-one solution for cyber security testing in the automotive industry. Consisting of a tailored hardware, comprehensive test catalogs and a web-based software application TestGuard allows to efficiently determine whether or not your system is exposed to known vulnerabilities and complies to legal requirements. The robust dynamic security testing capabilities empower engineers to conduct comprehensive penetration, fuzz, and functional security tests, seamlessly transitioning from security concept design to real-world usage scenarios – on the component level but also across the entire system.

- **Efficient:** Just connect the TestGuard Agent device to your component, system or full vehicle and trigger and analyze your tests without leaving your office
- **Flexible:** the modular platform comes with continuously extended testing capabilities but also allows for easy extension with your own scripts or 3rd party modules
- **Compliant:** Dedicated test catalogs covering the requirements defined in the legislations and standards (UNR 155, China GB & GB/Ts…)

AVL ComplyGuard - Stay Ahead of Certification

Cyber Security Process

Ensuring certification without gaps - AVL ComplyGuard navigates the homologation process effortlessly and efficiently. AVL ComplyGuard is a Safety and Security Management Environment for the creation, maintenance and management of work products as defined in the ISO 26262 and ISO 21434 (incl. UNR 155). Ready-to-use process models based upon AVL's years of engineering expertise assure an efficient execution and management of any cyber security or safety project constantly aligning with the regulatory requirements. Benefit from automated document generation and an efficient and fully traceable process. Easily integrable with the existing IT infrastructure (ALM/PLM, engineering tools, requirements management tools, etc.).

- **Effortless:** Automated document generation (e.g. safety/security case, interface agreements (CIA/DIA), status reports)
- **Traceable:** Facilitated decision-making thanks to complete transparency, revision safety, and trackability of past and current projects in all stages of the development process
- **Consistent:** Coordinated development execution and enhanced and efficient collaboration across different team members
- **Audits and Assessments:** Benefit from built-in audit and assessment modules covering relevant standards and frameworks and directly linked to the respective ISO-work-product

AVL TraceGuard - Your Data Traced and Secure

Software Update Management

Based on AVL CRETA, the leading software variant management solution, AVL TraceGuard smooths the part to make it easy to track software versions, including regular analysis of relevant cyber security vulnerabilities according to regulation R156 (for Software Update Management System/ SUMS). TraceGuard streamlines the management of the intricate array of vehicle configurations and associated software versions, ensuring seamless and systematic vulnerability management becomes a norm. By identifying and tracking critical software updates, AVL TraceGuard makes sure that all changes of SUMS relevant parameters are treated and documented in a SUMS compliant way

- **Reliable:** Fleet-wide management of software updates according to regulations like UNECE R156
- **Seamless:** Easy integration with your preferred vulnerability scanner
- **Targeted security:** Strict review, software update and vulnerability scanning processes to assure safe and secure software updates

Complies with:

ISO/SAE 21434
UNECE WP.29 R155
China GB & GB/T standards for Cyber security
R156 for Software Update Management Systems (SUMS)

Reimagining Motion

For a greener, safer, better world of mobility.

AVL List GmbH
Hans-List-Platz 1
8020 Graz
Austria

Phone +43 316 787-0
E-mail info@avl.com
www.avl.com/avl-secguard

PA4110E V1, Classification Public