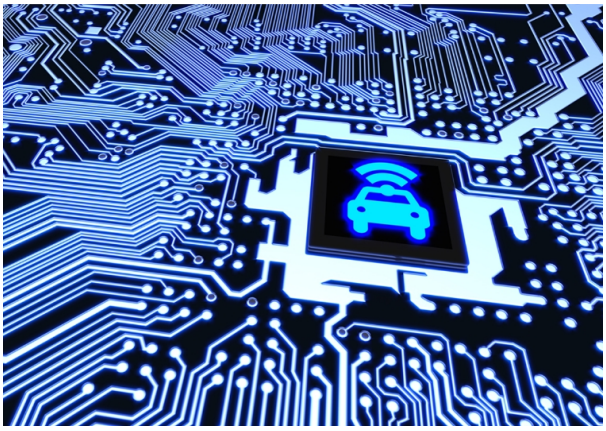
Contact us

Cybersecurity for Automotive

As an expert lab in embedded systems security evaluations and penetration testing, we support the automotive industry evaluating components and systems resilience against state-of-the-art cybersecurity attacks, at a hardware, software, communications and cryptographic level.



Modern vehicles are complex networks of IT components interconnected via wired and wireless interfaces such as CAN, LIN and Automotive Ethernet. Also, new vehicle generations can connect externally to telematics services, EV charging networks, and intelligent driving platforms, making them vulnerable to sophisticated cyber threats.

To address these risks, vehicle manufacturers must comply with evolving regulations and standards for managing cybersecurity in road vehicles. As the primary developers of cybersecurity-critical components, Tier 1 suppliers play a pivotal role in ensuring the safety and resilience of the automotive ecosystem.

Currently, UNECE R155 and R156, together with new local Chinese regulations GB44495 and GB44496 and the RED Directive in Europe, stand for the current state of the art on regulations that OEMs navigate to define cybersecurity requirements.

In order to demonstrate components' resilience against state-of-the-art attacks, OEMs and Tier 1 manufacturers can turn to specialized security laboratories to evaluate their products.

Cybersecurity Services for Automotive Components

Applus+ IT labs have a strong record of accomplishments evaluating embedded components' security at hardware, software, communications, and cryptographic level. We have expertise with the complete OSI stack, from system boot to intersystem

communications. This bird's eye view allows us to assess complex systems with a high level of assurance.

Certification of Conformity services for International Standards

Our team of cybersecurity experts and experienced auditors offers Certification of Conformity services for the following applicable international standards:

- ISO/SAE 21434: Establishes a framework at organization level for managing cybersecurity risks in road vehicles throughout their lifecycle, from concept and design to production, operation, and decommissioning.
- ISO 26262: Defines functional safety standards for road vehicles, focusing on the identification, assessment, and mitigation of risks associated with electronic and electrical systems to prevent hazardous failures.
- ISO 24089: Provides guidelines for software updates in road vehicles, ensuring secure, reliable, and efficient management of over-the-air updates and related cybersecurity measures.

The service includes the following activities and deliverables:

- **Gap Analysis**: Our cybersecurity experts conduct a preliminary gap analysis to identify deviations from ISO/SAE 21434 requirements and provide actionable recommendations to bridge compliance gaps effectively.
- **Audit Assessment**: Our certification service conducts a detailed audit of your cybersecurity management system, ensuring they align with the requirements of ISO/SAE 21434.
- **Detailed Audit Report**: Receive a comprehensive audit report outlining findings, strengths, and areas for improvement, offering a comprehensive third party evaluation criteria based on ISO/PAS 5112.
- **Certificate of Conformity**: Upon successful completion of the audit, we provide a certificate of conformity, demonstrating your compliance with ISO/SAE 21434 standards to partners, customers and the industry.

Security evaluations tailored to the customer need

Security evaluations encompass penetration testing activities for automotive electric /electronic components. We customize the evaluation effort to align precisely with your desired scope and requirements.

Target for these kind of evaluation includes a wide range of target components such as:

- **Electronic Components**: Foundational building blocks of automotive systems, including **System-on-Chip (SoC)** for processing, **Hardware Security Modules (HSM)** for encryption and secure data handling, and **Printed Circuit Boards (PCB)** that interconnect and support electronic components.
- **Devices**: Integrated units that perform specific functions within the vehicle, such as **Electronic Control Units (ECU)** for managing engine or braking systems, **Telematics Control Units (TCU)** for connectivity and communication, and **On-Board Chargers (OBC)** for managing electric vehicle charging.
- **Systems and Networks**: Infrastructure connecting components and devices, including communication protocols like **CAN (Controller Area Network)**, **Bluetooth,** and **100-BaseT1 Ethernet**, as well as external networks such as **3GPP** standards for cellular connectivity.

The main activities that we perform in our security evaluations are:

- Design Review, Source Code Review (SCR) and Vulnerability Analysis (VA).
- Full-stack penetration testing to evaluate the attack resistance and resilience of the device.
- Custom evaluations for custom OEM/Tier conformance requisites.

Security training and best practices (design and code)

Open cybersecurity training and courses aimed at roles like system engineers, cybersecurity managers or software architects. Some examples of our training:

- State-of-the-art secure coding principles and how they can be applied to day-to-day operations.
- Automotive solutions from an attacker's perspective and how the devices can be attacked, helping to identify ways to apply this knowledge to your product and make it more robust.

Why choose Applus+ as a cybersecurity partner?

- High assurance security evaluation laboratory with experience in several sectors: automotive, payments, telecom, industrial, mobile...
- State-of-the-art attack techniques and equipment to evaluate components and devices integrated in a vehicle, covering physical attacks, software attacks, and network and wireless attacks.

- Expertise to support the validation of a secure life cycle during product development.
- Cybersecurity footprint in Europe (3 labs in Spain), in North America (1 lab in Canada and 1 lab in the USA) and Asia (1 lab in Shanghai, China).
- Capability to cover several standards and regulations related to cybersecurity in the automotive sector.

Note: Because Applus+ Laboratories is accredited as a third-party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.