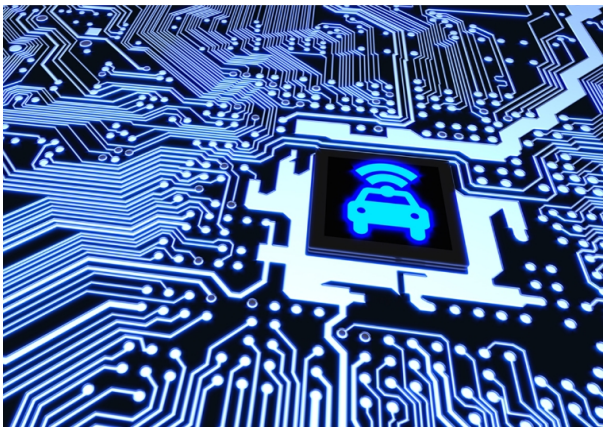
Contact us

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.



New vehicles are increasingly made up of a network of IT components that communicate internally, using wired and wireless interfaces (CAN, LIN or Auto Ethernet), and externally, with telematics services, EV charging systems, and intelligent driving systems.

Automotive Tier 1 suppliers are responsible for developing most of the cybersecurity-critical components embedded in a car. OEMs require guarantees that adequate protections and countermeasures are in place to ensure product resilience against potential attackers.

The automotive standards and regulations ecosystem for cybersecurity in vehicles and components is still under development. UNECE WP.29 is the only mandatory regulation in place, while OEMs have a myriad of sectoral standards and best practices available to set up the cybersecurity requirements passed by Tier 1s.

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 Evaluations 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.

Threat Analysis and Risk Assessment (TARA)

- Reviews of global, per-project, and continuous cybersecurity management and activities for the concept, development and post-development phases of the product life cycle, to reach the desired level of security guarantees
- TARA projects can be done following specific automotive standards, such as ISO /SAE DIS 21434 and less sectorial frameworks such as ISO/IEC 62443, even with custom TARA systems (such as in-house requirements)

Security evaluations tailored to the customer need

We can tailor the evaluation effort in accordance to the desired level of assurance (basic, moderate and complete assurance). Evaluation targets ranges from single components (SoC, HSM, PCB), to devices (ECU, TCU, OBC) to systems and networks (3GPP, Bluetooth, CAN, 100-BaseT1)

- 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.