Contact: idiada@idiada.com

Cybersecurity

The automotive industry has been under constant evolution during recent years with the introduction of connectivity, ADAS, and autonomous driving functionalities. The inclusion of these new features in current vehicles increases the cybersecurity threats and vulnerabilities that can affect the security and safety of vehicles and users. To minimize the impact of possible cyberattacks, industry stakeholders shall develop, produce, and maintain their vehicles considering cybersecurity throughout the whole lifecycle of the vehicle.

Applus+ IDIADA offers different cybersecurity solutions, enabling OEMs and suppliers to develop their vehicles and products in compliance with industry regulations and standards. Our extensive experience in the cybersecurity field and demonstrated success of our customers **obtaining UN R155 certification** ensures customer satisfaction.

Cybersecurity compliance

Our team of experts in automotive cybersecurity supports our customers throughout the entire development phase related to cybersecurity. We provide expertise in the following areas:

- Cybersecurity Development according to **ISO/SAE 21434** aiming for UN R155 compliance
  - Threat Analysis and Risk Assessment (TARA)
  - Cybersecurity Goals definition
  - Requirements for cybersecurity mitigations
  - Cybersecurity validation to confirm the goals have been achieved
  - Assistance with supplier management and development of Cybersecurity Interface Agreements to ensure supply chain security

- Gap analysis and support for compliance with UN R155 and UN R156

Secure architecture design

In coordination with different departments inside the organization, IDIADA supports customers in the secure architecture design of the vehicle. The architecture of current vehicles shall consider aspects like cybersecurity, EMC, wiring harness, power management, and functional safety from the design phase. Integrating these aspects from the start of the design results in a robust and reliable vehicle architecture.

Automotive cybersecurity trainings

IDIADA has designed a set of trainings to support manufacturer employees in understanding cybersecurity regulations and good practices to improve the cybersecurity culture of the organization. IDIADA offers trainings in accordance with:

- UN R155 compliance training
- UN R156 compliance training
- ISO 21434 training
- Training in good cybersecurity practices

IDIADA offers tailored trainings to cover any lack of knowledge in specific automotive cybersecurity aspects.

Penetration testing activities: The Cyberbox tool

IDIADA has internally developed a validation system that enables testing of the security of a vehicle's connectivity vectors.

The **Cyberbox tool** is designed to guarantee that any test is conducted automatically following the same process, enabling the repeatability of the test under the same conditions to ensure the validity of the obtained result.

This repeatability guarantees that the test results can be used as evidence of validation activities under UN R155, and can also be used to compare performance between different vehicles or configurations.

The tests can be conducted to validate Wi-Fi, Bluetooth, TPMS, USB, GPS, OBD, and CAN security at the vehicle level. IDIADA is constantly updating and upgrading the test capabilities, including secure EV charging process testing.

Cybersecurity facilities in Europe, North America and China

IDIADA has extended its cybersecurity services with local support to our customers in Europe, North America, and Asia.

- **Applus+ IDIADA Headquarters and Technical Centre** – Pol. Industrial L'Albornar, 43710 Santa Oliva, Tarragona, Spain
- **Applus+ IDIADA North America** – 100 West Big Beaver Road Suite 200, Troy, Michigan, United States
- **Applus+ IDIADA China** – Hucheng Pioneer Park, Building 23, 3999 Xiupu Road, Kangqiao Town, Pudong District, 201315 Shanghai, China