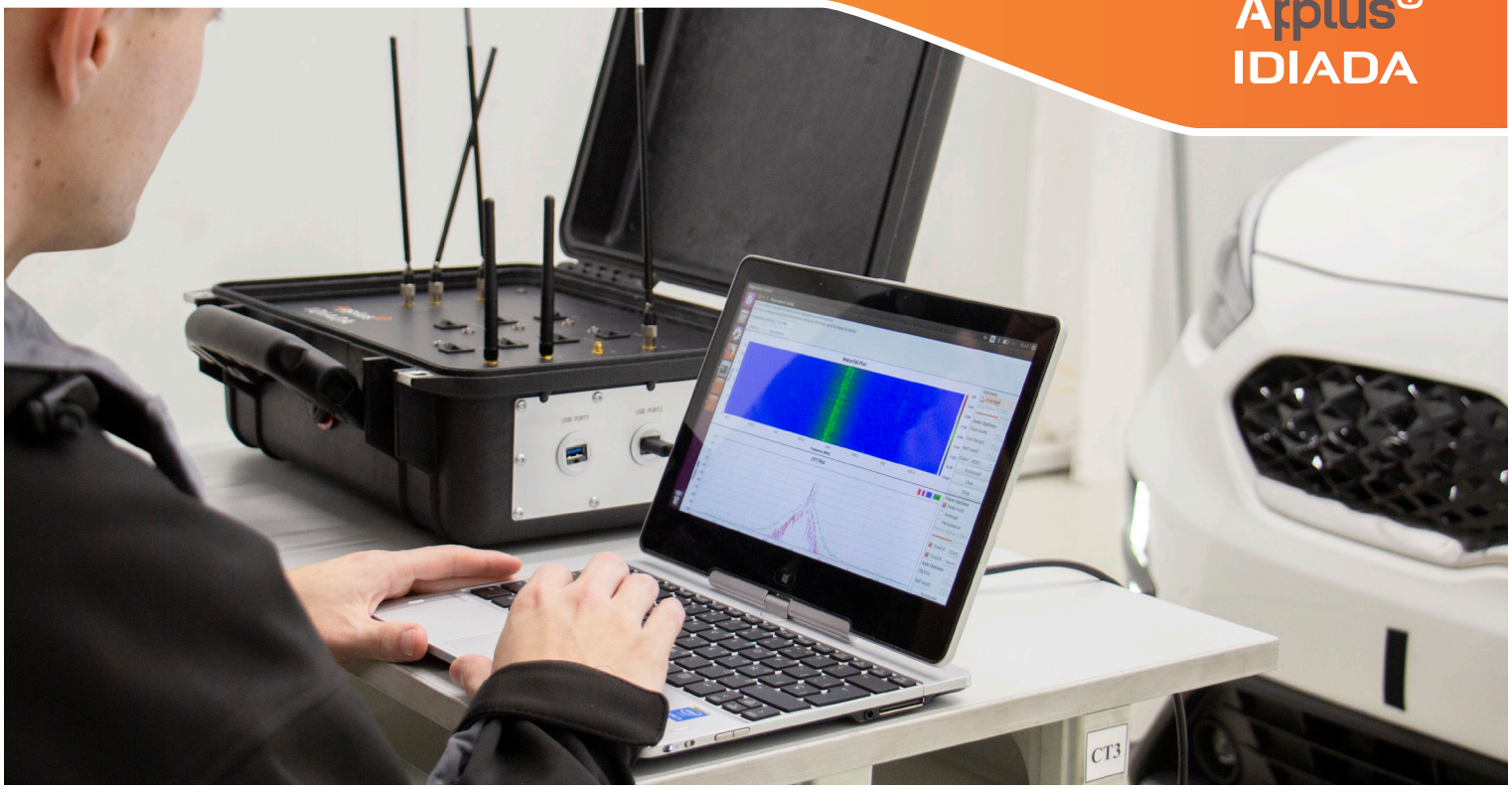

Automotive cybersecurity services

Cybersecurity incidents in vehicles are currently a real threat to the safety of road users, both in terms of their physical safety and their data and privacy. In addition, cybersecurity is a "hidden" quality of a vehicle and is only perceived by the user after an event (as with passive safety). In order to ensure the protection of users and vehicle systems, **cybersecurity has been introduced in the automotive industry**; in fact, new standards and regulations have been released in recent years to meet the growing demand for standardized guidelines. IDIADA has a dedicated team of automotive cybersecurity experts to provide multiple services to support manufacturers and stakeholders in developing and validating their cybersecurity systems.

VEHICLE DEVELOPMENT PROJECTS

IDIADA has the capability to lead and/or support the development activities that are required, considering the development of new cybersecurity processes inside organizations or specific activities. IDIADA performs the following activities always **based on ISO/SAE 21434 and UN ECE R-155**.

- Development of cybersecurity management systems (CSMS)
- Cybersecurity by design: architecture, network, methods, guidelines
- Over-the-air (OTA) security and implementation procedures
- Cybersecurity interface agreements management
- Threat analysis and Risk Assessment (TARA) execution
- Cybersecurity concept and requirements definition
- Incident and process development monitoring

COMPLIANCE WITH REGULATIONS AND STANDARDS

IDIADA is a Technical Service (TS) designated by the Spanish Type Approval Authority (TAA) for the homologation/certification of **R-155** (Cybersecurity) and **R-156** (Software Updates). IDIADA is also able to audit and certify compliance with **ISO/SAE 21434** and **ISO 24089**.

IDIADA can support the interpretation and understanding of **UNECE R-155** and **R-156** regulations performing pre-assessment activities to identify deviations and proposing roadmaps to solve issues on compliances according to the requirements defined in the regulations. These regulations consider two different assessments, on the one hand the requirements linked to the organization processes to cover cybersecurity and software updates requirements, the cybersecurity management systems and software update management systems (CSMS and SUMS); and on the other hand, the vehicle type approval, that includes requirements to verify the execution and implementation of TARAs, cybersecurity measures, testing activities and monitoring activities, among others.

TESTING AND VALIDATION

IDIADA has developed **a tool to evaluate cybersecurity on connected vehicles (CyberBox)**. The tool tests the connectivity vectors on vehicles: Wi-Fi, Bluetooth, RKE, TPMS, OBDII, GPS, APPs. The software developed allows our tool to automatize the penetration tests performed, optimizing the time required to evaluate the vehicles in a pre-defined and controlled scenario that guarantees valid results in each execution also permitting the comparison of the level of security among all the tested vehicles.

The penetration tests include various techniques to assess vehicle systems, such as spoofing signals, scan ports, replay RF, fuzz testing, etc.

CONSULTANCY AND TRAINING

In addition to audit and certification, IDIADA can support the **understanding of ISO/SAE 21434 and ISO 24089 and automotive cybersecurity topics**, through consultancy activities and/or tailored training.

CONTACT INFORMATION

Headquarters & Technical Centre • *L'Albornar - PO Box 20* • *E-43710 Santa Oliva (Tarragona) Spain*

For further details, please contact: *info@idiada.com* *T +34 977 189 360*