Inspiring excellence in worldwide technologies

Teoresi position paper concerning Cybersecurity and Privacy aspects on ADAS Systems in a C-ITS Scenario

ADAS implementation on vehicles is becoming increasingly useful for safety purposes in order to protect general users and vulnerable road users (VRU). Industry and computer technologies improve every day on the same direction of hardware computation power while the cost is decreasing. The use of complex algorithms with the extension of neural network and AI methodologies increase the power and the reliability.

Moreover, ADAS systems and vehicles in general, are more and more connection-oriented in a Collaborative Intelligent Transport System. This will improve efficiency and will make features more dynamic. On the other side, connected systems will affect privacy and security. New services like ISA (Intelligent Speed Adaptation), Platooning, GLOSA (Green Light Optimal Speed Advisory) require communication between vehicle and roadside equipment (RSE).

Wireless scenario implies increasing cybersecurity problems due to the interaction between systems. Basic concepts like **confidentiality, integrity, availability** (CIA triad), together with non-repudiation and authenticity must be guaranteed. Integrated scenario with cloud services, by the way, increase the attack surface and expose the whole infrastructure to hackers and attackers.

ADAS systems could access parameters that usually identify the vehicle and - in more advanced systems - can also monitor the **private drivers' attributes**. For example, monitoring the driver heartbeat or the driver drowsiness is usually done using standard sensors and camera. Even a simple system like TPMS (Tyre Pressure Monitoring Systems) can identify and reconstruct the movements of the drivers.

These technologies are invasive from a privacy point of view and these concepts always counter to the cybersecurity requirement of authenticity, confidentiality and non-repudiation. In these scenarios, it is important to have something more than best practices to assure that all the devices and the centralized cloud services follow type approval requirements to mitigate the risk and guarantee privacy for the users. A risk assessment must be analyzed to prevent different type of vulnerability.
It is urgent to define **type approval requirements** for devices and systems exchanging data to allow connected cars to implement new features in a safe way.

About Teoresi

TEORESI, founded in Turin in 1987, is nowadays an international Group, with offices in Europe and United States, who acts as a qualified partner to foster customers' product and process development. Backed up by a global expertise in engineering, Teoresi supports its customers by providing design, development and technology consulting services, with particular attention to innovation in every project challenge. Teoresi offering covers different industries such as: Aerospace and Defense, Automotive, Industrial, Railway, TLC & Media, Energy, Bioengineering, Financial Services, Public sector and University, HW & SW services, Home Appliances.

TEORESI S.P.A.
HEADQUARTERS ADDRESS Via Perugia, 24 10152 Torino (Italy) | **PHONE** +39 011 240.80.00 | **Fax** +39 011 240.80.24
WEB www.teoresigroup.com | **MAIL** info@teoresigroup.com
Cap. Soc. € 150.000 | **C.F. E P.IVA** 03037960014 | **REA** TO 700669 | **REP.** TO 2598/87

Sistema Qualità Certificato
UNI EN ISO 9001
Reg. N. 50 100 9752