ICT4CART

ICT Infrastructure for Connected and Automated Road Transport

A connected future for automated driving

- ICT4CART aims to combine, adapt and improve technological advances from the **telecommunication, automotive and IT industries**
- In order to design, implement and test an Information and Communications Technology (ICT) infrastructure in real life conditions to enable the transition towards road transport automation

Objectives

1. **Identify** the most reliable and effective functional and technical connectivity requirements for higher levels of automation
2. **Implement and test** a standards-based distributed IT environment for data aggregation
3. **Implement** cyber security, data protection and privacy mechanisms according to EU policy
4. **Improve** localisation by combining information from different sources and adapting existing tools and algorithms for data fusion
5. **Validate and demonstrate** the ICT infrastructure architecture through use cases and test sites
6. **Create** new business models and market services for the innovative use of cross-sector data

Project scope

- **High-value use-cases**, demonstrated and validated under real-life conditions
- **Hybrid communication approach** where all the major wireless technologies are integrated under a flexible “sliced” network architecture
- **Distributed IT environment for data aggregation and analytics** that offers seamless integration and exchange of data between actors from 3 different industries: telecom, automotive, IT

Our main role in ICT4CART is to:

Develop cyber security and data privacy solutions for connected automated vehicles with a high level of automation (up to 4). The proposed solutions **comply with existing EU standards and regulations to be adopted by most of car manufacturers**.

- Provide privacy and access control in the connected and automated driving environment, we develop a **role-based identity and access manager** ensuring the secure communication of Intelligent Transport Systems and authorised as well as legitimate access to cloud services and road-side units.

- Bring **cyber security situational awareness** on deployed systems through a supervision centre:
  - It assesses and reports vulnerabilities of large vehicle fleets and smart objects.
  - It monitors anomalies at the level of the authentication layer by collecting and correlating logs from the identity and access manager and the intelligent transport systems.

These two solutions will be demonstrated in **real life conditions** on German and Italian test sites through use-cases such as smart parking and lane merging.

HORIZON 2020: ec.europa.eu/programmes/horizon2020
ICT4CART: https://www.ict4cart.eu/
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 768953.

Programme co-funded by the EUROPEAN UNION

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com