

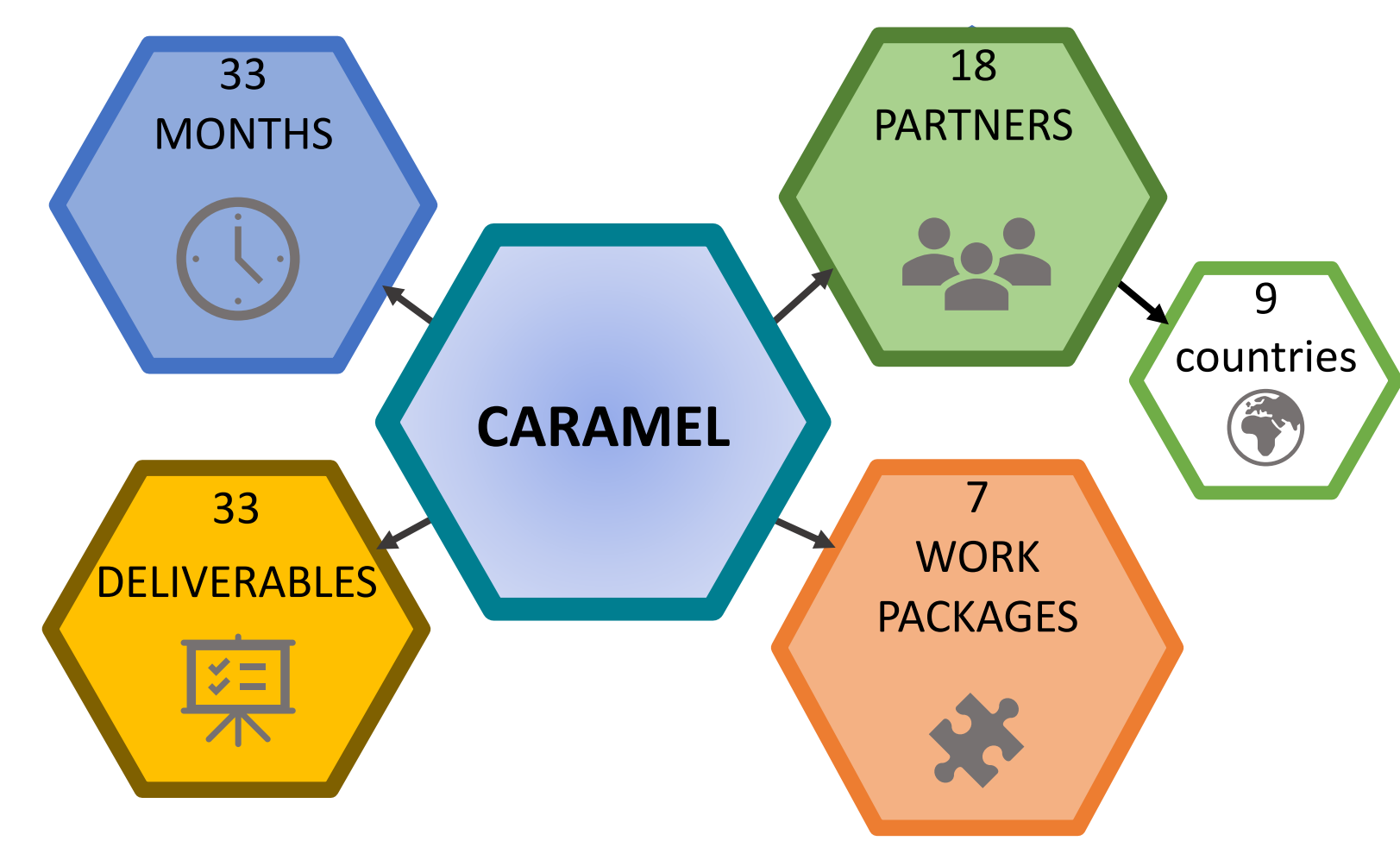
Artificial intelligence based cybersecurity for connected and automated vehicles



Abstract

Car safety has come a long way. From the first padded dashboard to seat belts and from rear-view cameras to active safety measures such as autonomous emergency braking (AEB), technological advances are picking up speed. Nowadays, cars are becoming smarter and “greener” through connectivity and artificial intelligence, and cybersecurity is emerging as a new concern able to stop such huge potential for more sustainable safer roads with zero fatality. The EU-funded CAMEL project is developing cybersecurity solutions for the new generation of cars: i) autonomous cars, ii) 5G connected vehicles, and iii) electromobility. The project applies a proactive method based on artificial intelligence and machine learning techniques to mitigate cybersecurity-originated safety risks on roads. Considering the entire supply chain, CAMEL aims to introduce innovative anti-hacking intrusion detection/prevention systems for the European automotive industry.

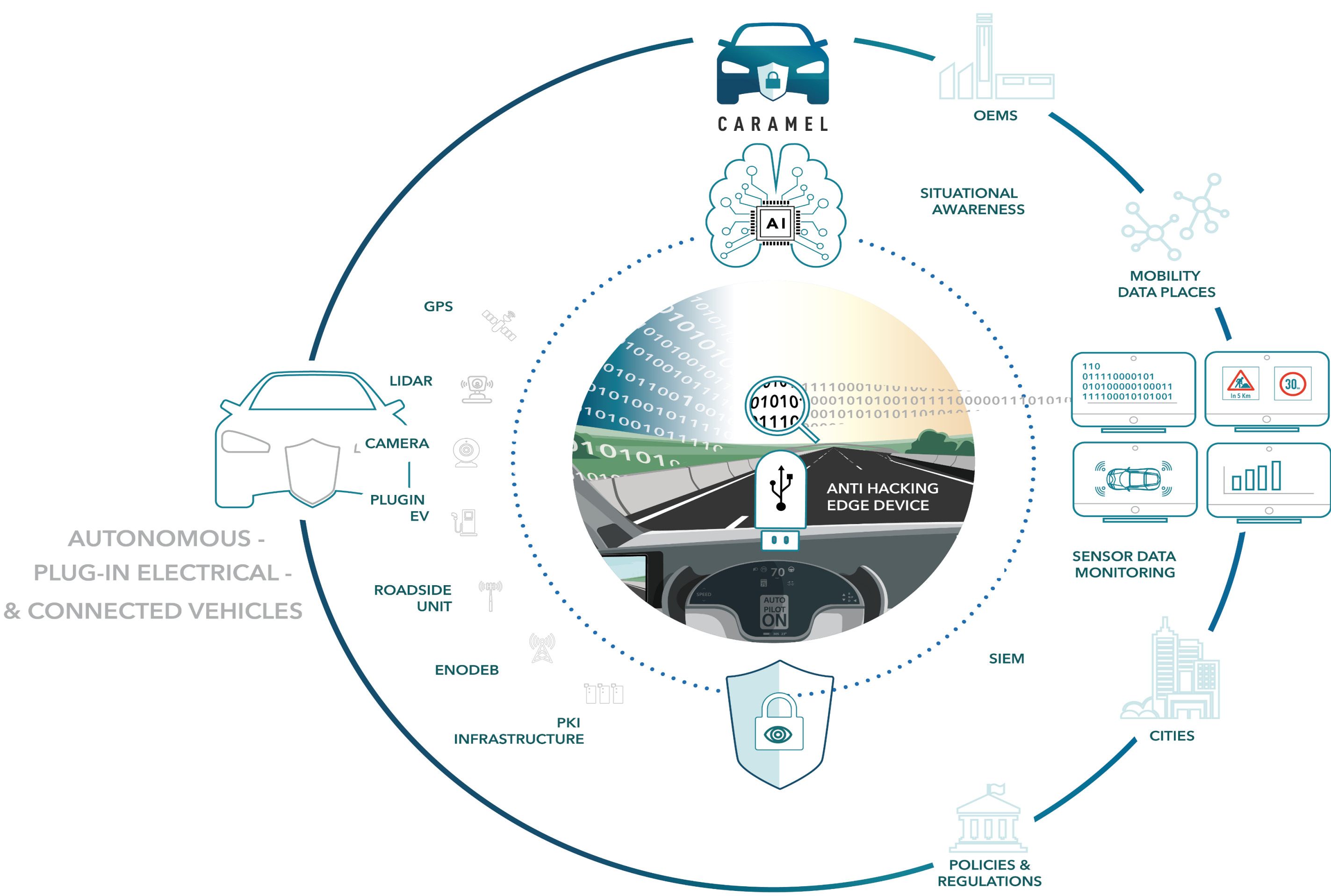
CAMEL in numbers



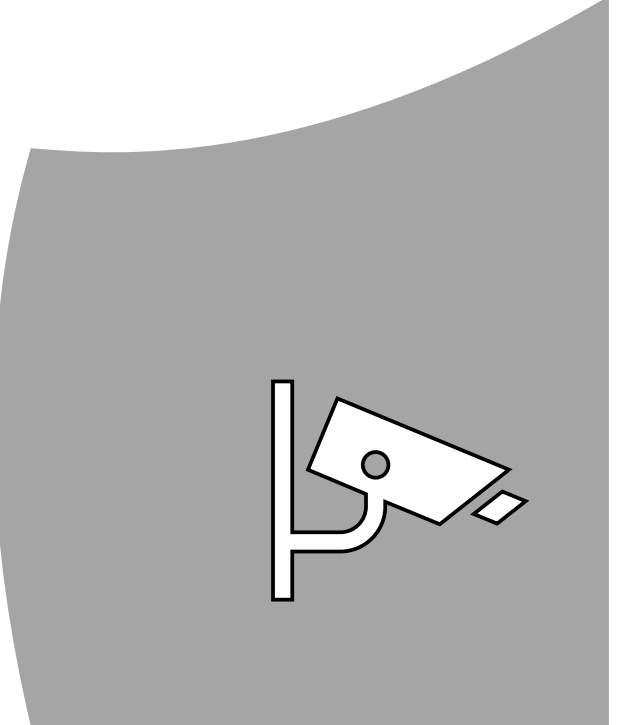
Objectives

- To identify cybersecurity threats and vulnerabilities in the context of cooperative, connected and automated mobility vehicles (including electrical plug-in vehicles).
- To design and develop a successful extensible, scalable and market-oriented cybersecurity architecture for the provisioning of situational awareness in CCAM vehicles
- To model cyberthreats, detect cyberattacks and to identify appropriate responses for each modern vehicle category considered in CAMEL.
- To consider and fuse different data sources of information in order to achieve contextual and situational awareness and to facilitate the decision-making process.
- To create an anti-hacking device that will be able to disable higher level functions in case of a cyberattack.
- To perform penetration testing, validate and demonstrate the CAMEL solution.
- To ensure the long-term success of the project through standardisation and dissemination in commercial and industrial fora and by exploring synergies with other EU initiatives and projects.
- To design and develop a successful market-oriented, AI-driven and extensible cybersecurity framework for modern vehicles / Business Models to exploit findings in partners’ future product/service portfolios.


High-level architecture



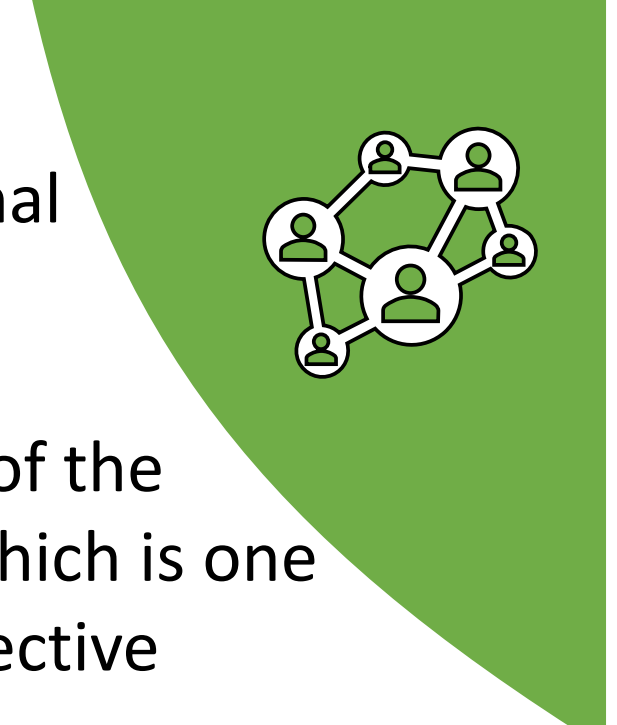
Impact



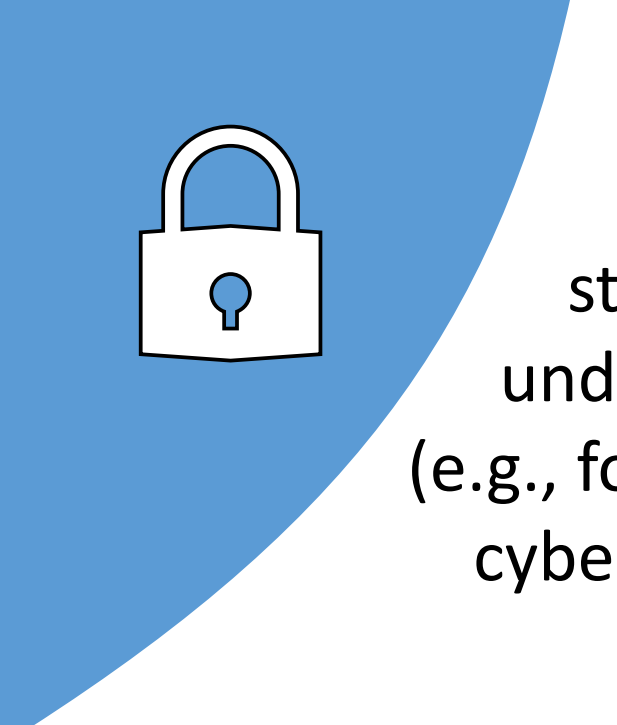
Enhanced protection against novel advanced threats.



Advanced technologies and services to manage complex cyber-attacks and to reduce the impact of breaches.



The technological and operational enablers of co-operation in response and recovery will contribute to the development of the CSIRT Network across the EU, which is one of the key targets of the NIS Directive



Robust, transversal and scalable ICT infrastructures resilient to cyber-attacks that can underpin relevant domain specific ICT systems (e.g., for energy) providing them with sustainable cybersecurity, digital privacy and accountability

Innovation pillars

Autonomous Mobility

Electromobility

Connected mobility

Remote Control Vehicle (RCV)



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 833611

