

### Coordinators

*Project Coordinator*

Jordi Guijarro  
Fundación i2CAT  
jordi.guijarro@i2cat.net

*Technical Coordinator*

Peter Hofmann  
Deutsche Telekom Security GmbH  
p.hofmann@t-systems.com

### Social media channels



@caramel\_project



Caramel Project



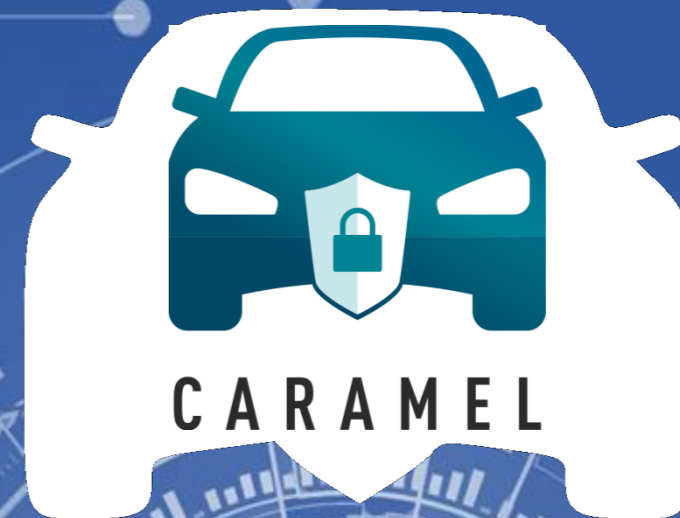
Caramel Project



CARAMEL

www.h2020caramel.eu

### Project Partners



Artificial Intelligence based  
Cybersecurity for Connected  
and Automated Vehicles

### Project Funded



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

## Artificial Intelligence based cybersecurity for connected and automated vehicles

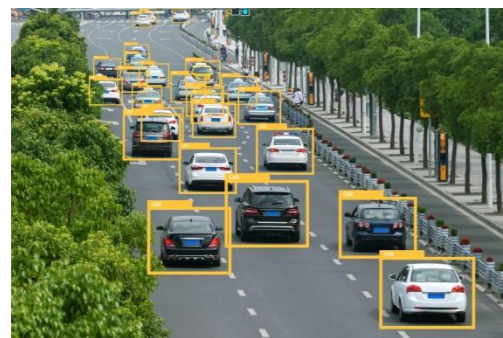
Vehicles are becoming smarter and “greener” through connectivity and artificial intelligence, and cybersecurity is emerging as a new concern able to stop such huge potential for more sustainable safer roads with zero fatality.

### Goal

CAMEL’s goal is to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques, and also to continuously seek methods to mitigate associated safety risks.

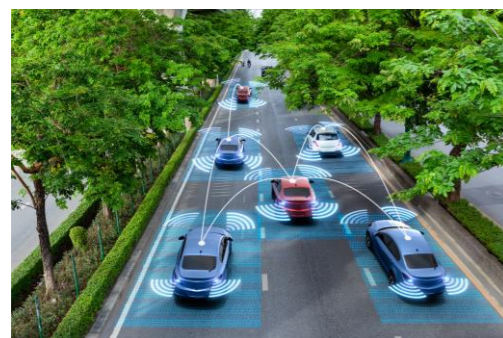
### Challenges

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.



#### Autonomous cars

Cyberattacks do not require physical access to the vehicle or tampering with the communication system.



#### 5G connected vehicles

V2X applications interconnect not only vehicles but also infrastructure and pedestrians, hence it is critical to protect V2X functions from a misuse of such technology.



#### Electromobility

Unauthorized access and control of EVSE stations and firmware modifications should be prevented.



#### Remote Control Vehicle

Intrusion detection and estimation algorithm in the Gateway & RCV controller is necessary to avoid misuse.

Considering the entire supply chain, CAMEL aims to introduce innovative anti-hacking intrusion detection/prevention systems for the European automotive industry.

#### Pilot demonstrations

CAMEL pilot demonstrations will take place in two premises: at the Test Area in Baden-Württemberg in Germany and at GreenFlux R&D laboratory in the Netherlands where real-world scenarios will be performed with prototype vehicles and smart chargers, under a controlled environment.



CAMEL workshop planned in November 2021.  
Please check the [‘Upcoming Events’](#) for more details.

Download the Automotive Threat Modelling Tutorial  
<https://www.h2020caramel.eu/resources/tutorial/>