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
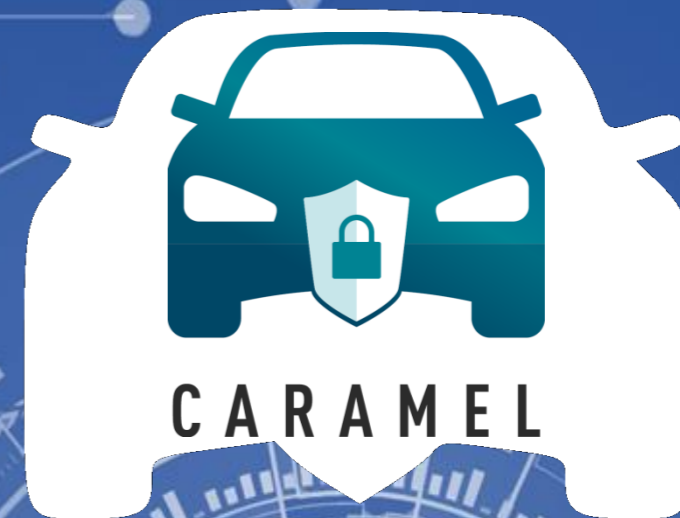
Twitter **@caramel_project**

LinkedIn **Caramel Project**

YouTube **Caramel Project**

www.h2020caramel.eu

CARAMEL

Project Partners

T·· · | 8 Bells | Atos | i2cat

ubiwhere | KATECH | S | UNIVERSITY OF PATRAS

GreenFlux | ETRI — Electronics and Telecommunications Research Institute | nextium by idneo

Panasonic AUTOMOTIVE | EXALENS | University of Cyprus | AVL

Capgemini engineering | mobigen — Make The Best For Smart Business

Project Funded

CARAMEL

Artificial Intelligence based Cybersecurity for Connected and Automated Vehicles

# 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

CARAMEL'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.
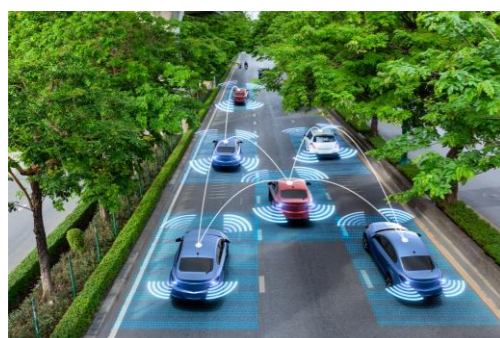
Challenges

The EU-funded CARAMEL project is developing cybersecurity solutions for the new generation of cars: i) Autonomous mobility, ii) Connected Mobility iii) Electromobility, iv) Remote Controlled Vehicles
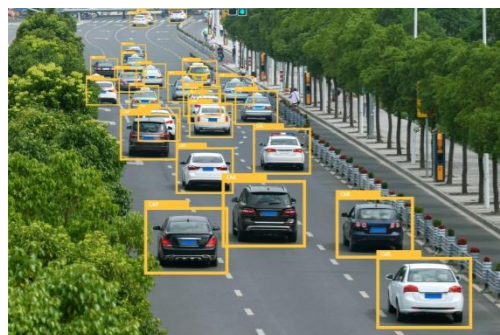
Autonomous mobility

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

Connected Mobility

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 Controlled Vehicles

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

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

Pilot demonstrations

CARAMEL pilot demonstrations will take place in two premises: at the Test Area in Hesen 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.

Download the Automotive Threat Modelling Tutorial

https://www.h2020caramel.eu/resources/tutorial/