Legal aspects of cybersecurity and data protection in mobility

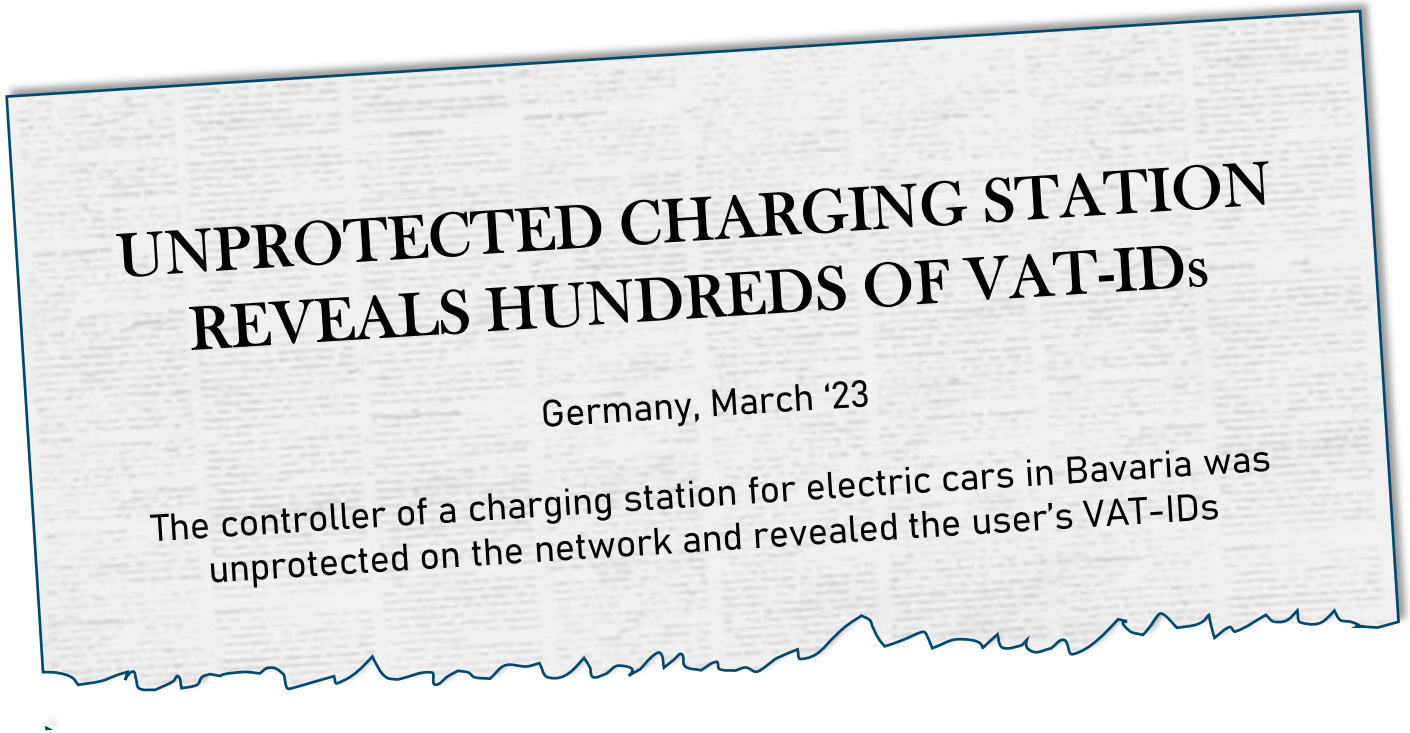
IKEM

Outline

- Overview of data protection law
- Introduction to cybersecurity law
- Implementation tips for the practice

Data Law

IKEM



UNPROTECTED CHARGING STATION REVEALS HUNDREDS OF VAT-IDs

Germany, March ‘23

The controller of a charging station for electric cars in Bavaria was unprotected on the network and revealed the user’s VAT-IDs

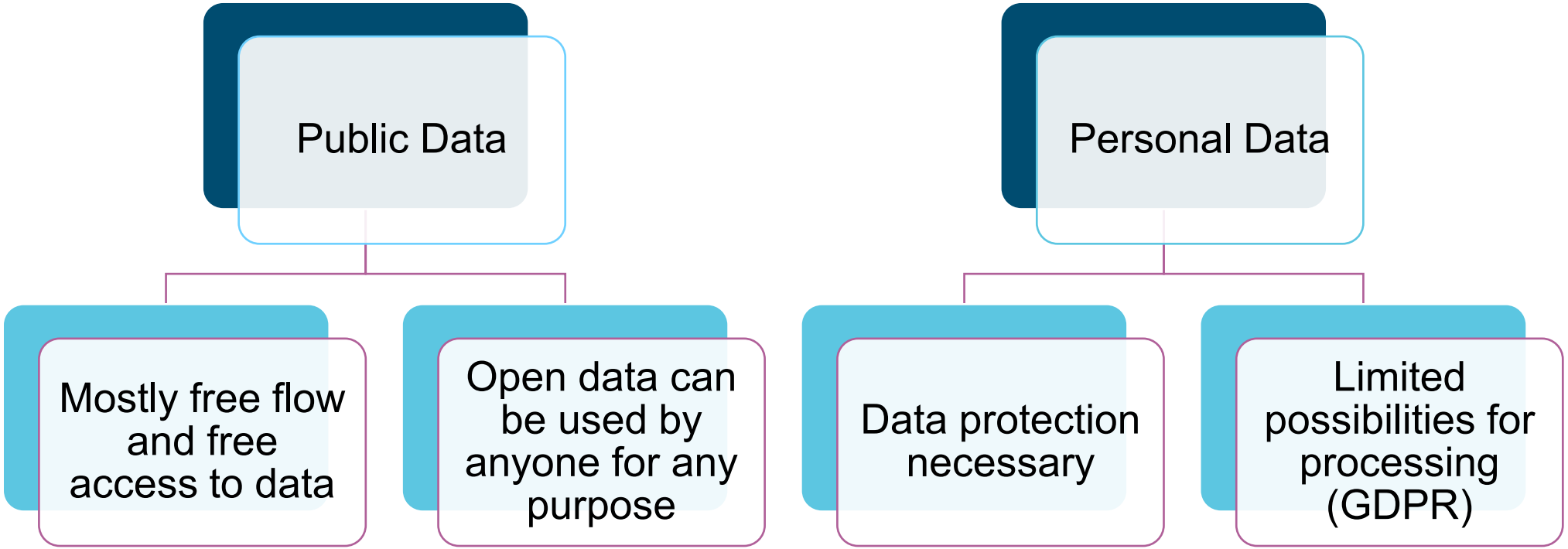
- Internet users could change various settings
- Personal data leaked:
  - Data could be used to clone charging cards and charge cars at the owner’s expense
  - Generation of user movement profiles possible

IKEM

Introduction to data law

- Definition: *Data means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording* (Art. 2 Nr. EU-Data-Act)
- Task of data law: promoting potential for progress while preserving people‘s interest in data protection
- Comprehensive cross-sector regulations on European and national level

Distinguishing the nature of the data



Personal data is any information relating to an identified or identifiable natural person

IKEM

Personal Data in mobility

- Geolocation data
- Real-time traffic and public transport data
- Personal data from linking the charging station and measurement data with the customer ID
- Charging data as personal data according to Art. 4 No. 1 GDPR
- Actors involved as responsible parties according to Art. 4 No. 7-10 GDPR

7 principles of Data Protection (Art. 5 GDPR)

IKEM

Legal bases for processing (Art. 6 GDPR)

Personal Data can only be processed:

- Consent
- Fulfilment of a contract
- Compliance with legal obligation
- Vital Interests
- Public Interest
- Legitimate interest

Data Subjects Rights Art. 15ff. GDPR

01

Right of access to their own data

02

Right to data portability

03

Right of erasure

04

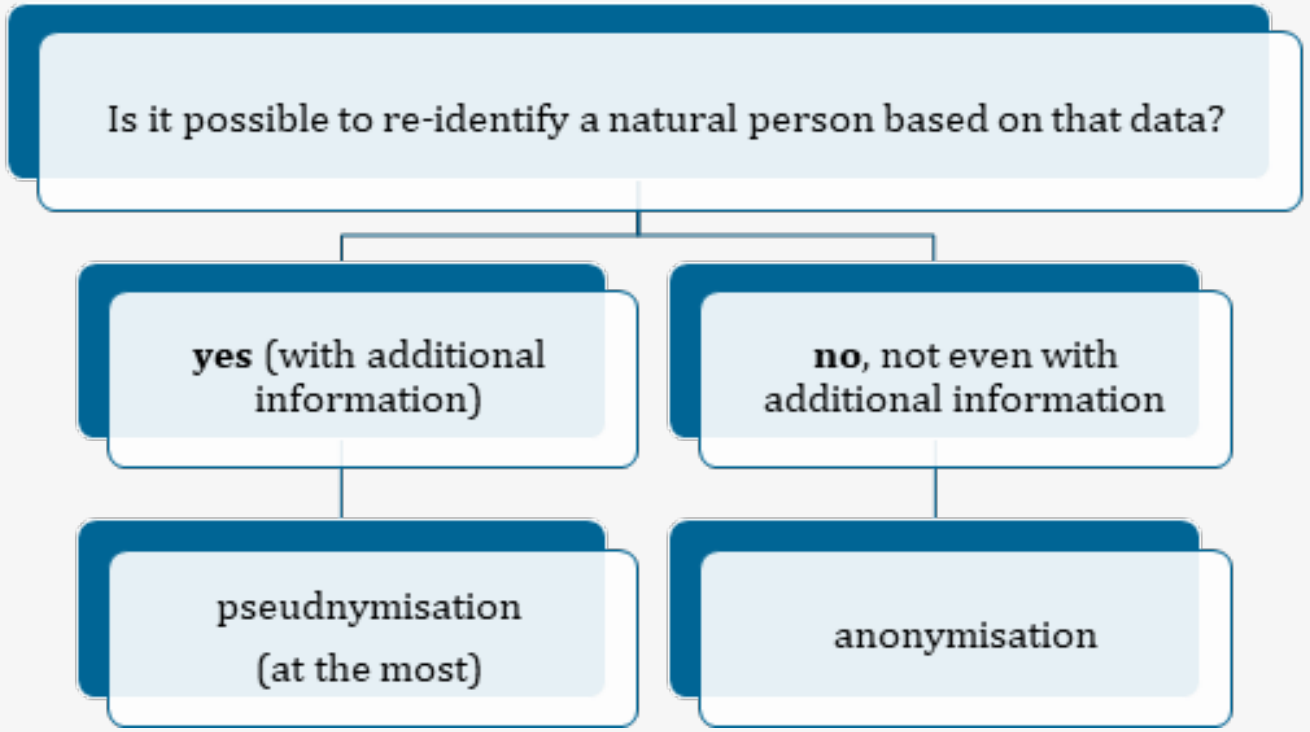
Right to rectification if incorrect

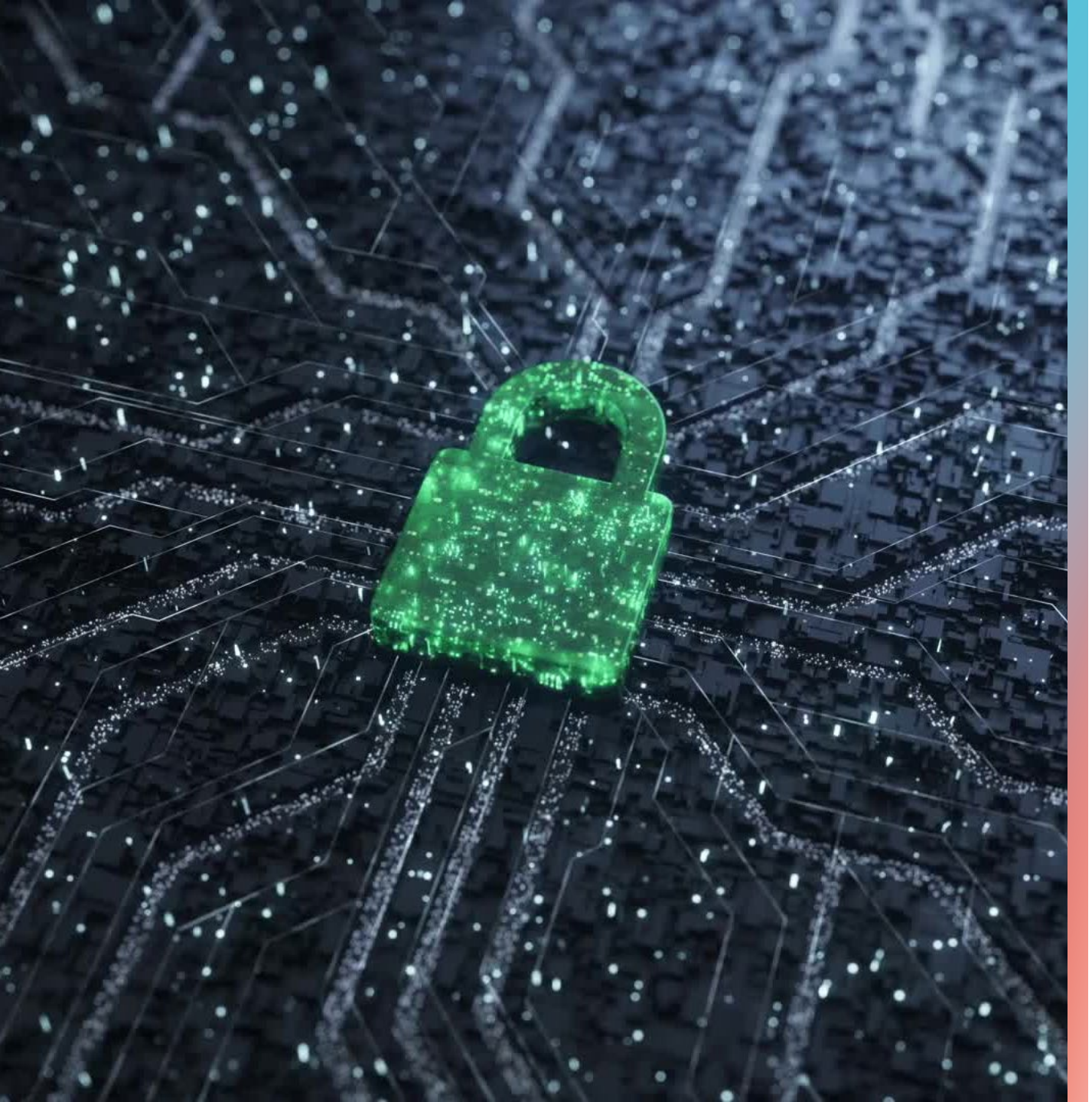
05

Right to object to processing

IKEM

Anonymisation in the GDPR for mobility data





Cybersecurity

IKEM

Cybersecurity

- Cybersecurity law refers to the legal framework that addresses the protection of digital infrastructure (information systems, networks and data) from cyber threats.
- encompasses laws, regulations, and policies designed to safeguard individuals, organizations, and governments from cyberattacks
- Also matter of national security: defending critical infrastructure and national interests
    - far-reaching short-term changes on European level

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

- Provides legal measures to boost the overall cybersecurity in the EU
- Expanding the scope of the prior NIS1 Directive to new sectors and entities
- Entry into force in 2023 - national implementation until 17 October 2024
- By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services.

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

Critical infrastructure under NIS2

- Entities operating in the subsectors and types of services listed in the annexes and of a certain size

Essential Entities

- Digital Infrastructure
- Public Administration
- Institutions designated by Member States
- Critical Entities (according to CER)

Important Entities

contain e.g. energy, transport

- Operators of end user charging ports, Provider of energy storage services and electricity producer

+

Size Cap

- 50 employees or
- annual turnover > € 10 million

IKEM

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

Obligations for operators under NIS2

- Art. 20 f.: Regulated Minimum standards of Cybersecurity have to be met
  - appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems
  - management bodies must approve cybersecurity, oversee its implementation and can be held liable for infringements
  - members of the management bodies of essential and important entities are required to follow training
- Art. 23: Reporting obligations in the event of significant disruptions
- Art. 25: Obligation to register

General Tips for the implementation of data protection and cyber security

- Be aware of the types of data handled by you and your unit
- When personal data is processed, the strict stipulations of the GDPR have to be met
    - notification, limitations, autohrizations
- Where your unit uses an external party for data processing it must have an agreement in place
- Determine which cybersecurity duties apply to you
- take general measures to avoid data breaches (encrypt documents containing personal data)

Simon Großmann, LL.M.
Tel +49 (0) 30 408 18 70 – 10
simon.grossmann@ikem.de

USER-CHI
CHARGING YOUR E-MOBILITY FUTURE

CARAMEL

Jordi Guijarro
Cyber Security Innovation Director at
i2CAT Foundation / Master Course In...

Artificial Intelligence based cybersecurity for connected and automated vehicles

Jordi Guijarro (i2CAT)

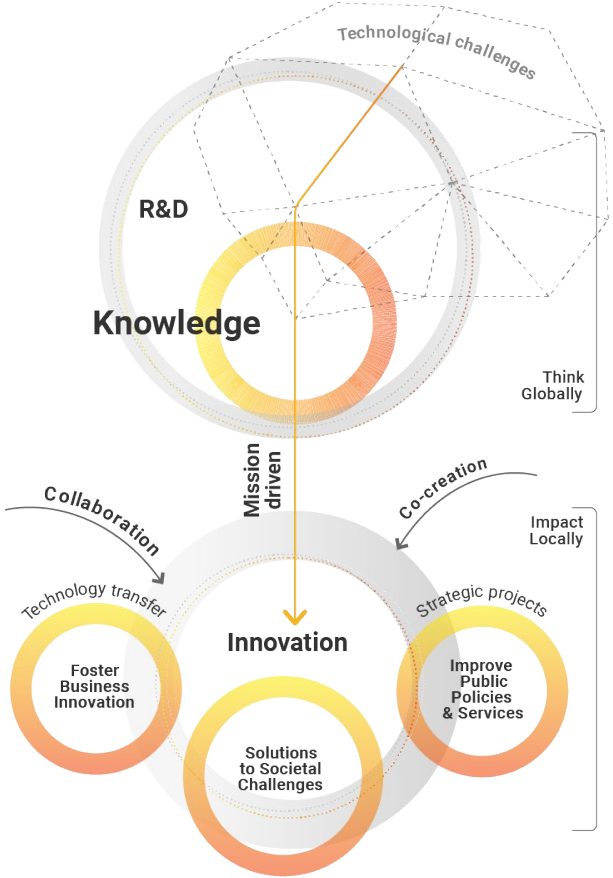
Jan 18 2024

i2CAT in a nutshell

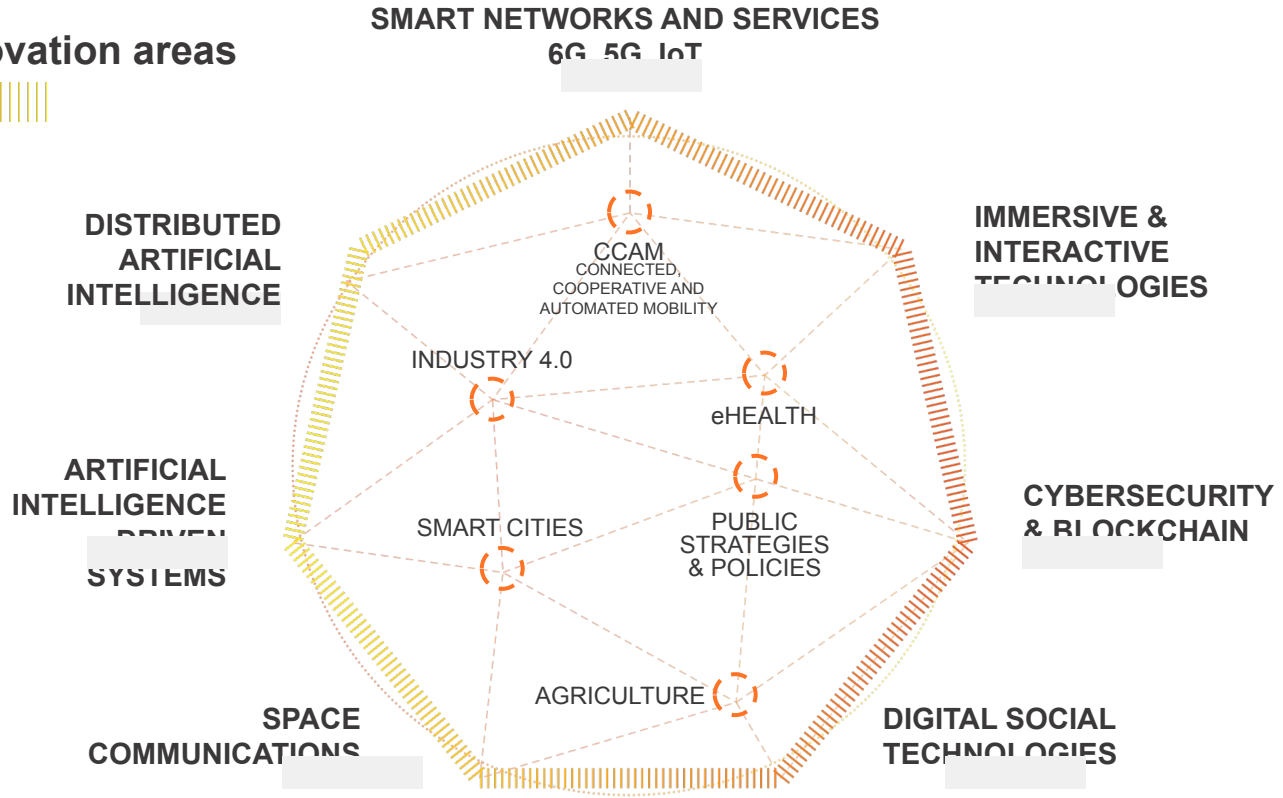
Never stop designing the digital future

Vision

i2CAT wants to lead the challenge of designing the digital society of the future based on research and innovation in advanced digital technologies.



Research and Innovation areas



European Commission

Horizon 2020
European Union funding
for Research & Innovation

CARAMEL

H2020 CARAMEL Project

i2CAT strategic R&D initiatives


CARAMEL

Agenda

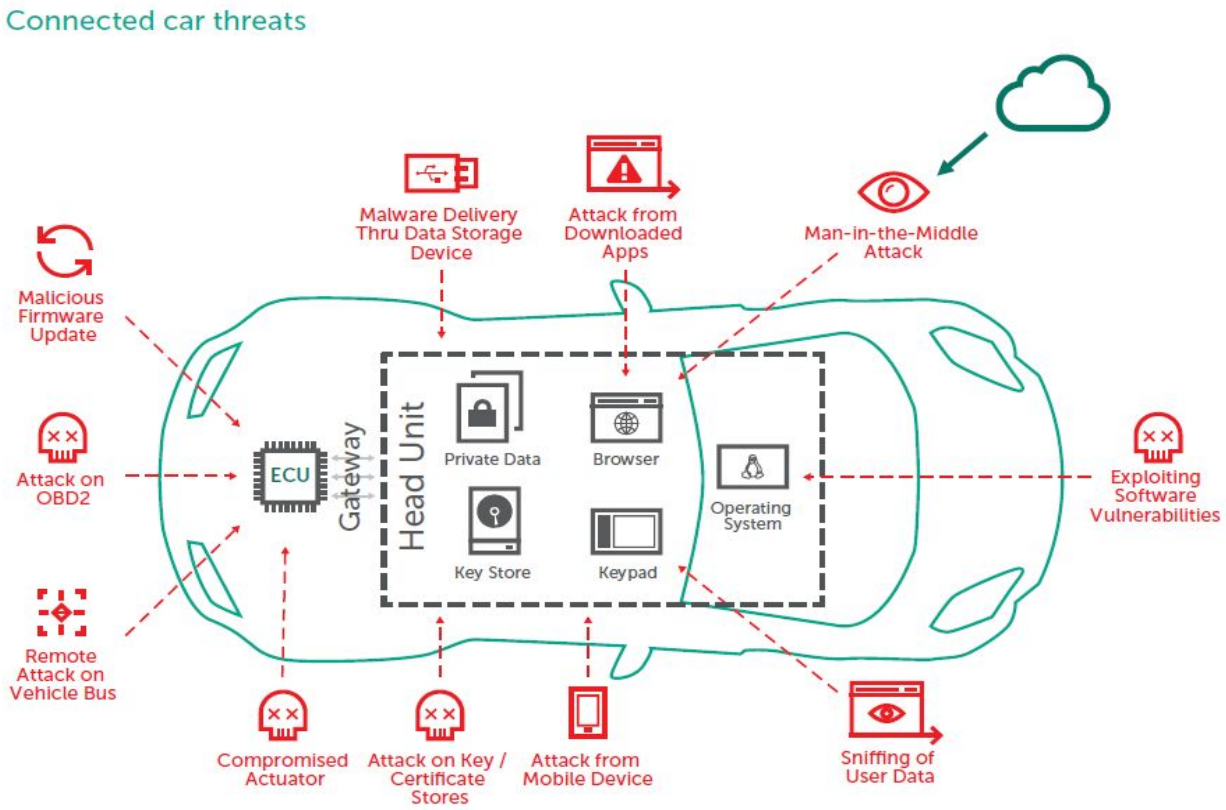
- Motivation – threats to connected vehicles
- CARAMEL project overview
- Pillar3 : eCharging manipulation Smart Charging Abuse & EV Scheduling Abuse
- Final demo execution
- Follow-up activities

Motivation

Attack surfaces

A modern car is a data center on wheels with a multitude of attack surfaces:

- Entertainment system
- Internal buses
- Sensors
- Cloud interfaces
- Interfaces to other vehicles and the road-side infrastructure (V2X)



CARAMEL on one page

Project goals

- Automotive Security: Detection and mitigation of threats against connected cars using ML techniques:
  - Pillar 1: Attacks on (semi-)autonomous driving
  - Pillar 2: Attacks on communication links and systems (GPS spoofing, V2X attacks, OBU attacks)
  - Pillar 3: Attack on eCharging infrastructure
  - Pillar 4: Remote controlled vehicle

Results

- Demonstrators: Detection of defaced traffic signs, attacks on V2X communication, GPS spoofing, attack on eCharging grid
- Anti-hacking device: Highly secure on-board intrusion detection system with ML capabilities
- Integration with backend systems (Automotive SOC)

Project information

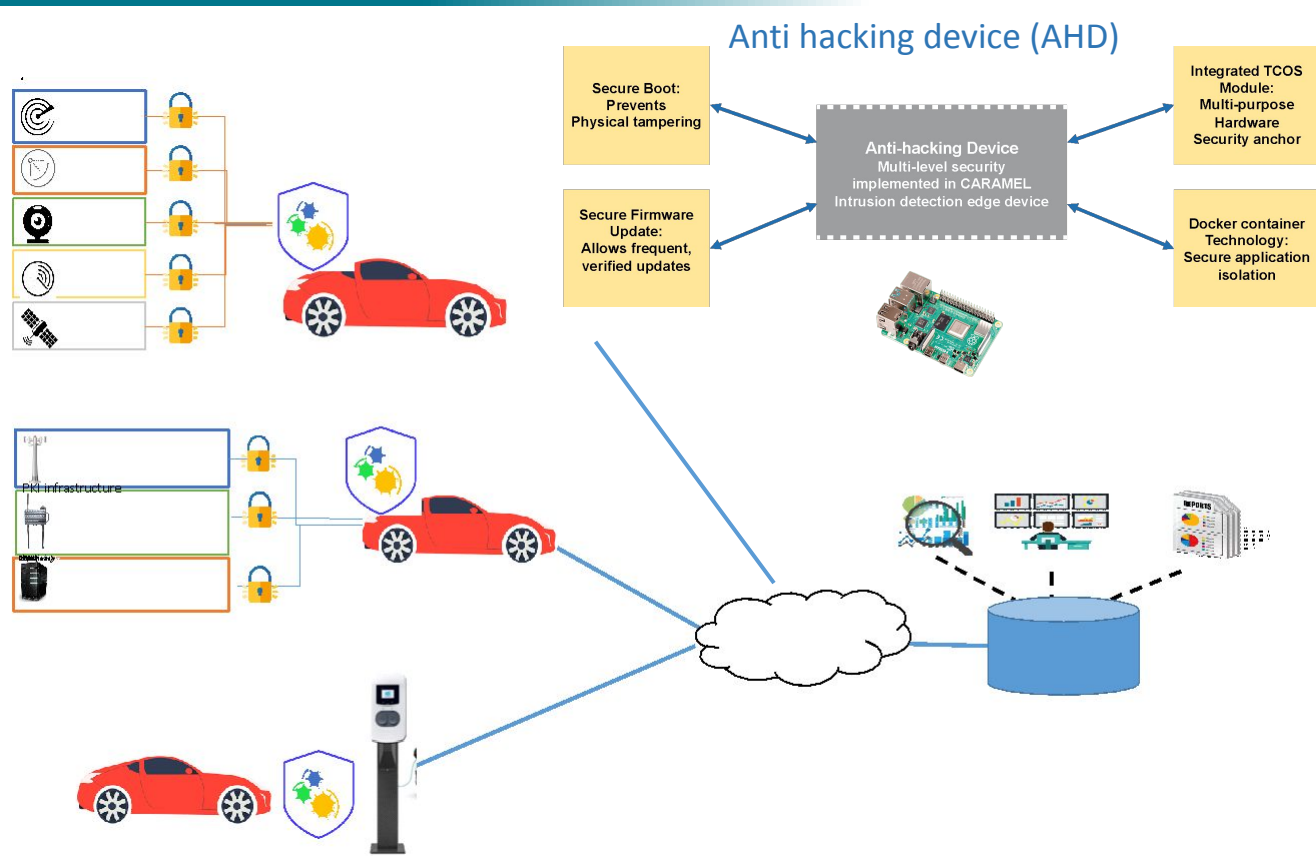
- 15 academic and commercial partners across Europe
- Affiliation with Korean partner project (funded by KR)
- Project runtime: 33 month, 10/2019-06/2022
- Horizon 2020 project 70 % funded by EU (100 % for academic partners)

CARAMEL Project

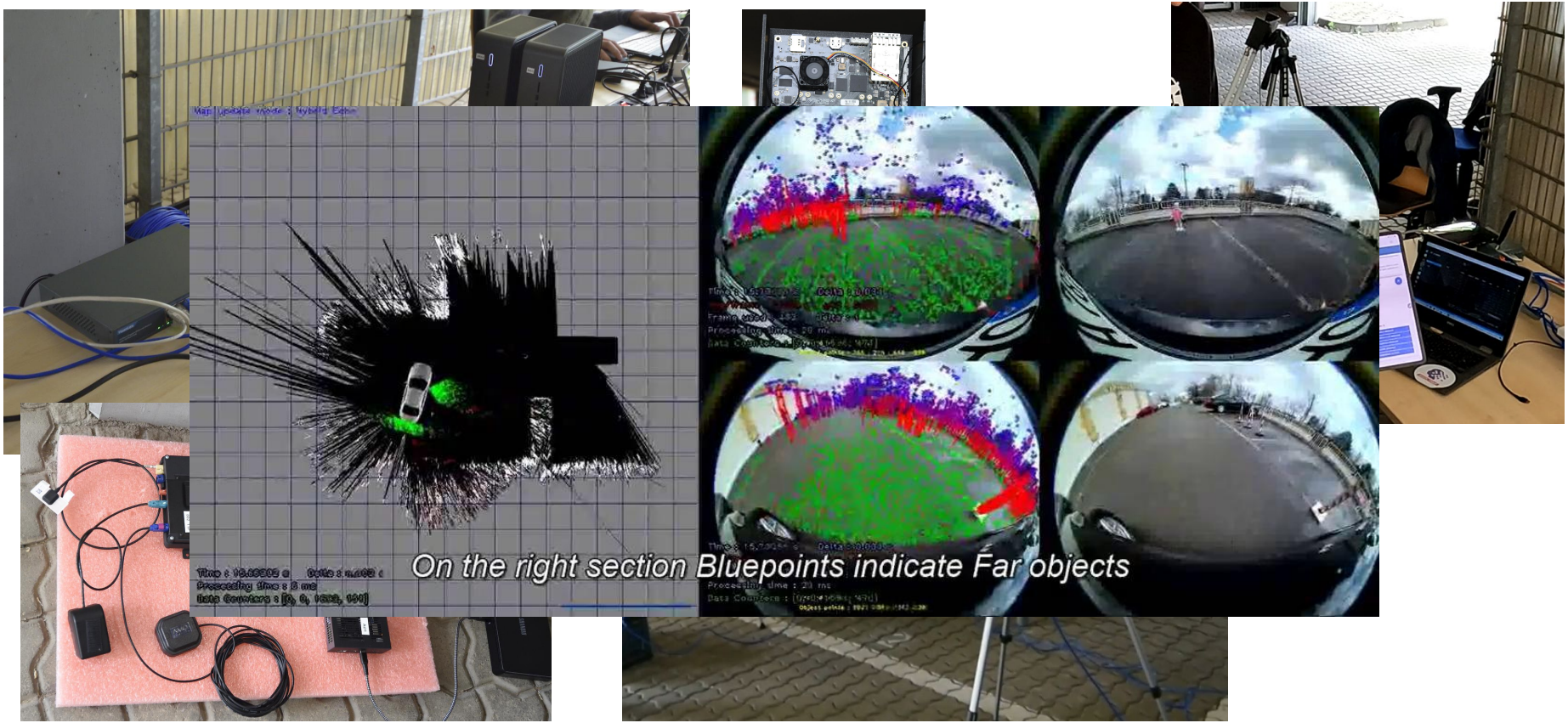
High-level overview

CARAMEL pillars

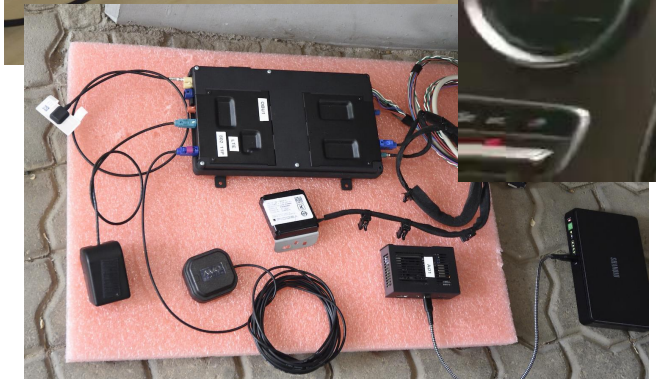
- Pillar 1
  - Attacks against sensors
- Pillar 2
  - Attacks against V2X infrastructure (forging of messages, vehicle track)
  - GPS spoofing
  - OBU compromise
- Pillar 3
  - eCharging manipulation
- Pillar 4: KR partners
- Common elements:
  - Anti-hacking device
  - Backend



Final Demonstration I

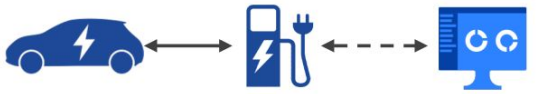


Final Demonstration II



Smart Charging Abuse & EV Scheduling Abuse

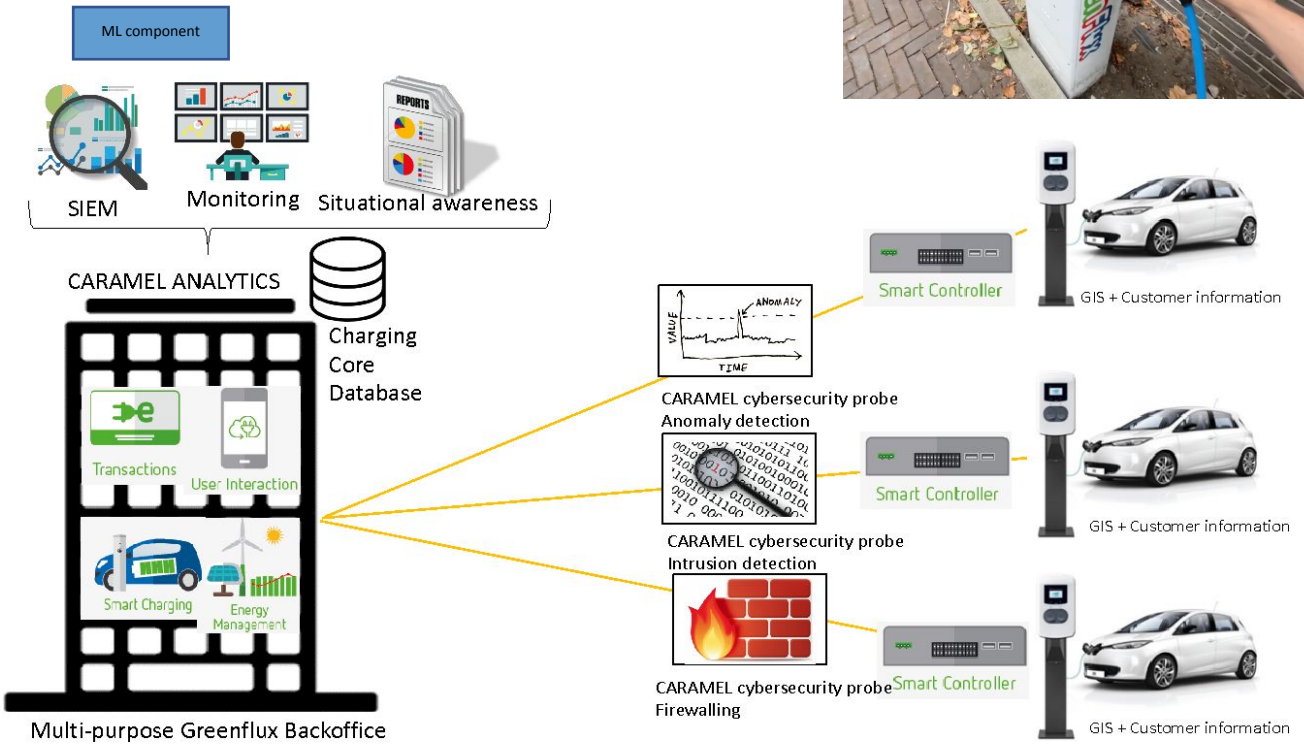
Use Case 3 : Electromobility



- Scenario
  - Smart Charging Abuse
  - The attacker(s) occupy (physically or remotely) the available charging stations and proceed timely in connection/disconnection actions creating an enormous load to the electric grid.
- Novelty
  - This is a scenario combining physical attack on a smart vehicle with anomaly detection algorithms.
- Evaluation Criteria
  - The GFX/SID software detects the attack and forward the alert on the CARAMEL back-end

Trial Architecture

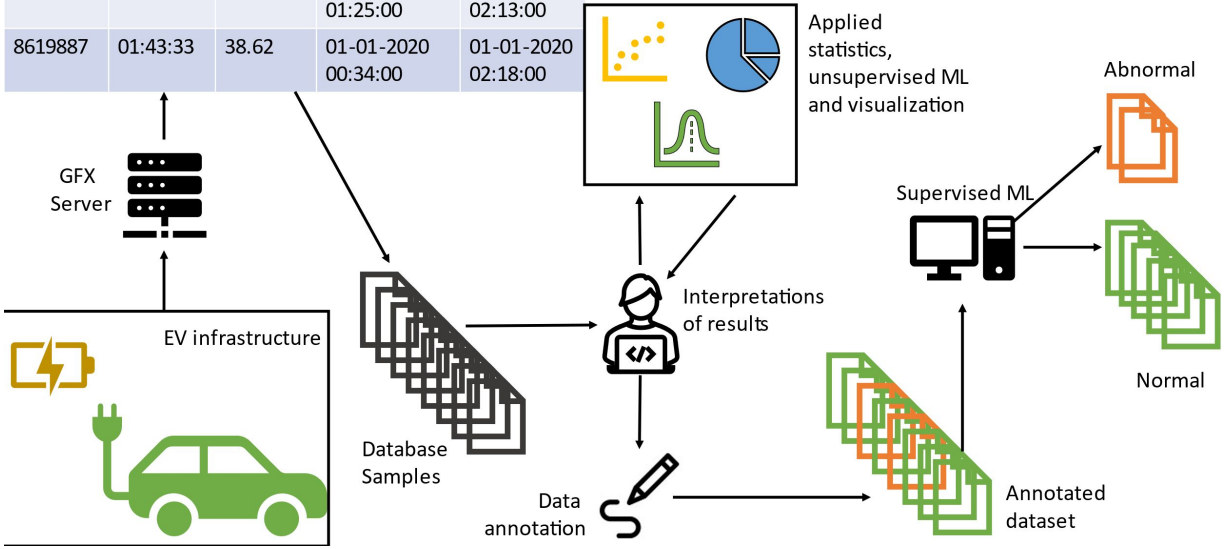
A look on GreenFluX's back-end



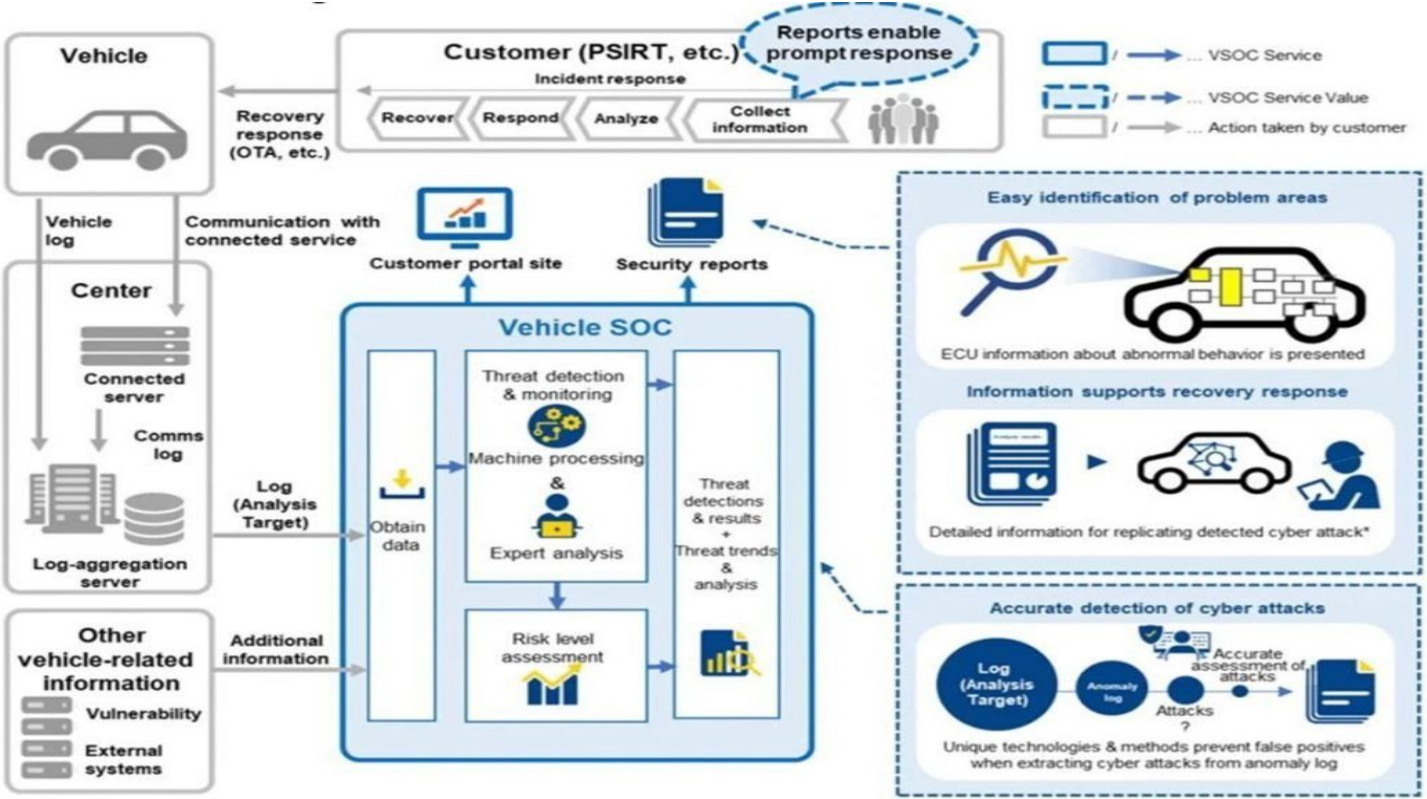
Development of anomaly detection

ID	Duration	Volume	dStart	dEnd
8619630	01:10:51	19.33	01-01-2020 00:21:00	01-01-2020 01:32:00
8619849	00:48:14	39.97	01-01-2020 01:25:00	01-01-2020 02:13:00
8619887	01:43:33	38.62	01-01-2020 00:34:00	01-01-2020 02:18:00

Snippet of database



VSOC Vision: Data Protection Challenges



CARAMEL in action

CARAMEL CHANNEL

https://www.youtube.com/channel/UCX9JMlToA5U1CRWwNMnwTYQ

Bonus slide: Threat modelling tutorial

https://www.h2020caramel.eu/2021/08/16/automotive-threat-modelling-tutorial/

Bonus slide: Caramel Project Book

https://nowpublishers.com/article/BookDetails/9781638280606

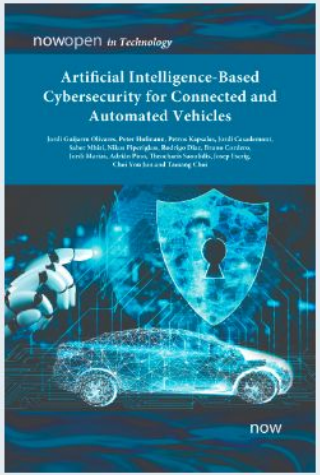
Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles

nowopen

Edited by **Jordi Guijarro Olivares**, i2CAT, Spain, jordi.guijarro@i2cat.net | **Peter Hofmann**, Deutsche Telekom Security, Germany | **Petros Kapsalas**, Panasonic Automotive Systems Europe, Greece | **Jordi Casademont**, Universitat Politècnica de Catalunya, Spain | **Saber Mhiri**, i2CAT, Spain | **Nikos Piperigkos**, University of Patras, Greece | **Rodrigo Diaz**, ATOS, Spain | **Bruno Cordero**, i2CAT, Spain | **Jordi Marias**, i2CAT, Spain | **Adrián Pino**, i2CAT, Spain | **Theocharis Saoulidis**, SIDROCO, Cyprus | **Josep Escrig**, i2CAT, Spain | **Choi You Jun**, KATECH, South Korea | **Taesang Choi**, ETRI, South Korea

Publication Date: 29 Dec 2022

Suggested Citation: Jordi Guijarro Olivares (ed.), Peter Hofmann (ed.), Petros Kapsalas (ed.), Jordi Casademont (ed.), Saber Mhiri (ed.), Nikos Piperigkos (ed.), Rodrigo Diaz (ed.), Bruno Cordero (ed.), Jordi Marias (ed.), Adrián Pino (ed.), Theocharis Saoulidis (ed.), Josep Escrig (ed.), Choi You Jun (ed.), Taesang Choi (ed.) (2022), "Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781638280613



ISBN: 978-1-63828-060-6
166 pp. Price: $125.00

Buy Book (hb)

ISBN: 978-1-63828-061-3
166 pp.

Open Access (.pdf)

Jordi Guijarro

Cyber Security Innovation Director at i2CAT Foundation / Master Course In...

CARAMEL

USER-CHI

CHARGING YOUR E-MOBILITY FUTURE

Thank you for your attention!

Use case from RESPONSE H2020

Webinar – Cybersecurity and data protection in electric mobility

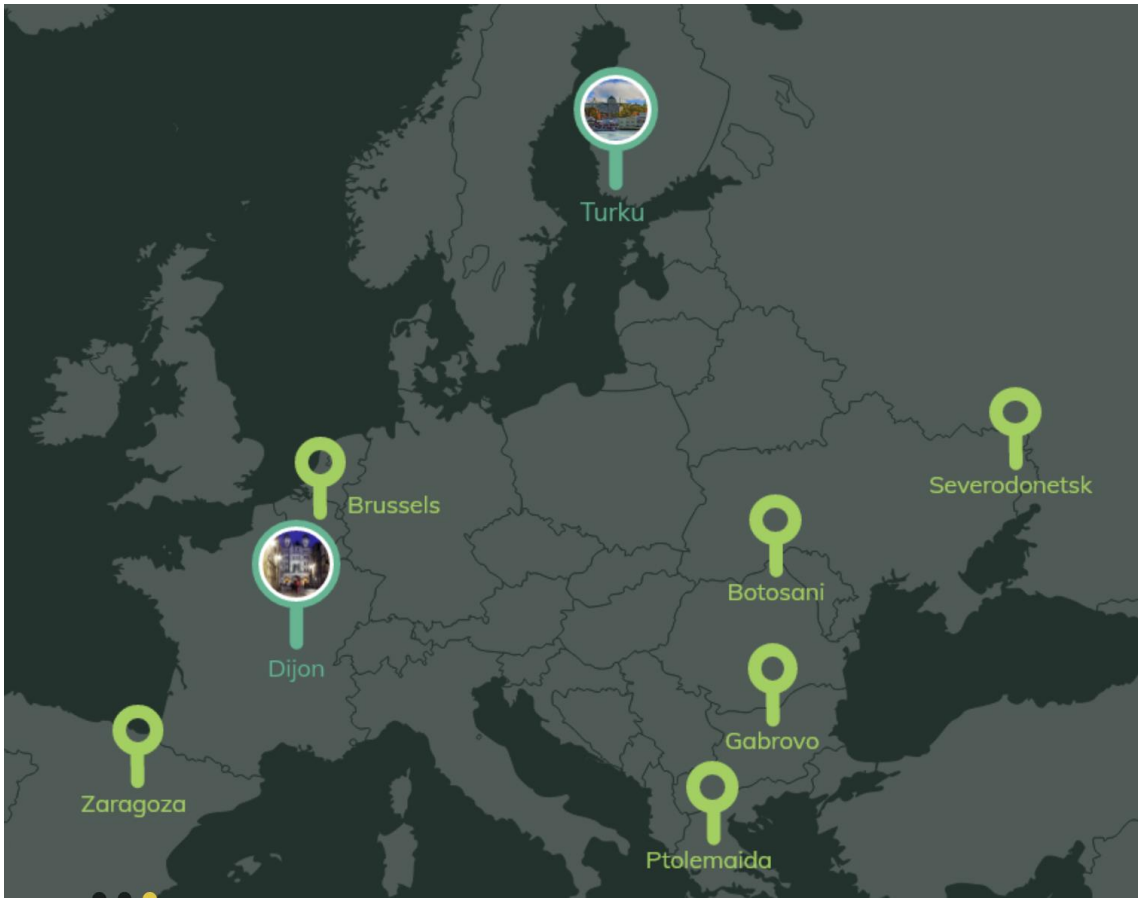
Inna Skarga-Bandurova

18 January 2024

2
Lighthouse Cities

6
Fellow Cities

13
European Countries



RESPONSE
Integrated Solutions for Positive Energy and Resilient Cities

54
Partners

54%
Industries and SMEs

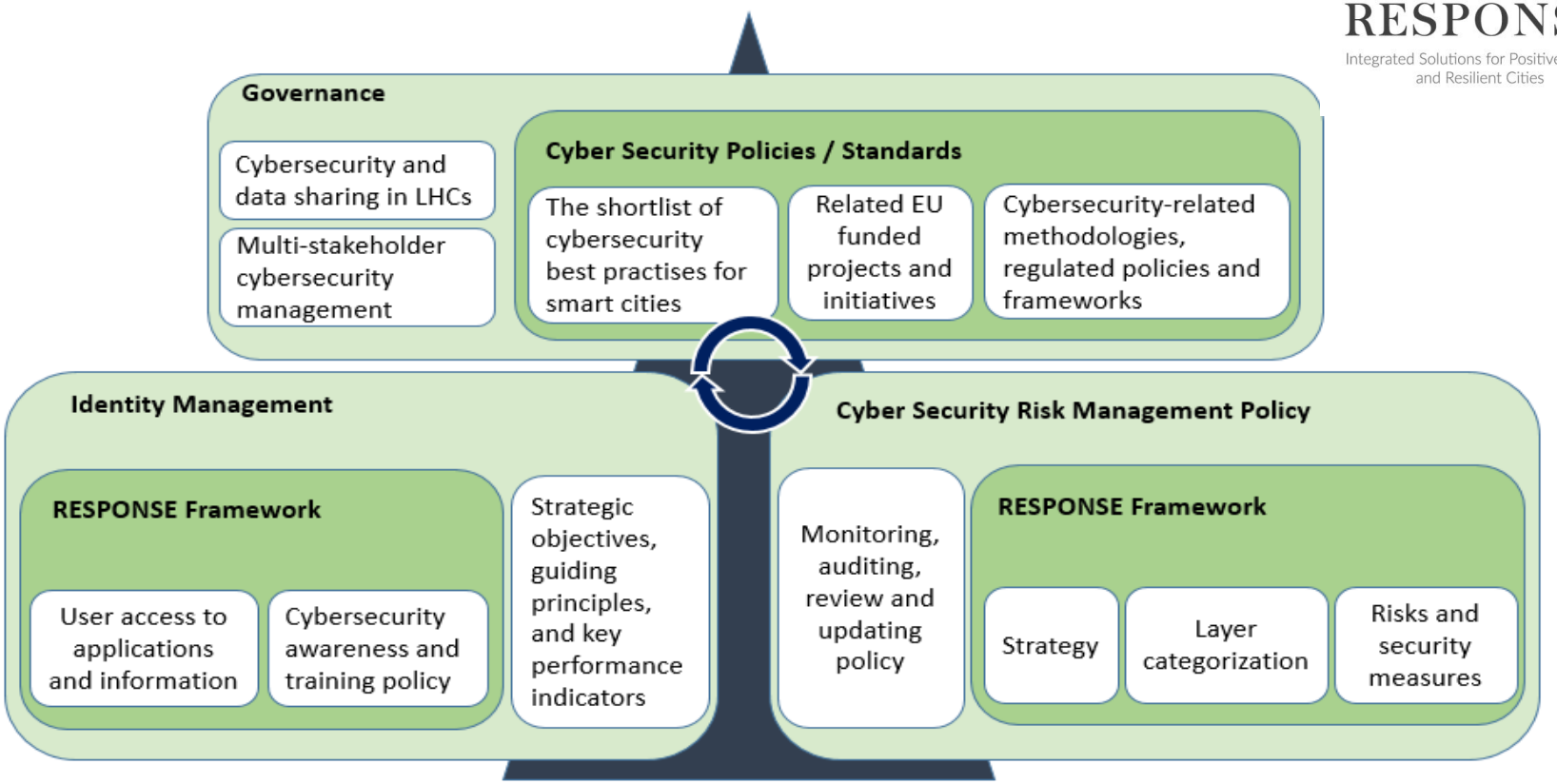
Lighthouse Cities

- Turku, Finland
- Dijon, France

Fellow Cities

- Brussels, Belgium
- Zaragoza, Spain
- Botosani, Romania
- Ptolemaida, Greece
- Gabrovo, Bulgaria
- Severodonetsk, Ukraine

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement nº 957751. The document represents the view of the author only and is his/her sole responsibility: it cannot be considered to reflect the views of the European Commission and/or the European Climate, Infrastructure and Environment Executive Agency (CINEA). The European Commission and the Agency do not accept responsibility for the use that may be made of the information it contains.



- Alignment with security policies, standards, plans and requirements of citizens and stakeholders.
- Support of the mission of the RESPONSE project.
- Strategic security and identity management plan unique to data sharing in smart cities
- Strategies to implement a layered data protection framework.

A Fragment of Innovative Elements in LHC

IE ID	IE Title	Planned/ Implemented		Level of impact	Potential cyber security threats
		Turku LHC	Dijon LHC		
4.1 City Information Platform-enabled Innovations					
4.1.1	Control command connections and security layer (GeneSys)		✳	city	✳✳✳
4.1.2	Shared data-lake		✳	city	✳✳✳
4.1.3	PEB Multi-Energy Dashboard		✳	PEB	✳
4.1.4	Automatic online energy and climate indicators computation		✳	city	✳
4.1.5	Energy-Climate Dashboard		✳	city	✳
4.1.6	Smart City Knowledge Graph AI	✳		city	✳
4.1.7	Air quality journey planner (app) for cyclists and pedestrians	✳		city	✳
4.1.8	District heating, cooling and flexibility control situational awareness and anomaly detection	✳		PED, city	✳
4.1.9	**Automated driving and Vehicle-to-vehicle communication of robot cars via 5G**	✳		PED	✳✳✳✳✳
4.1.10	5G Smart City Lighting Poles	✳		PED	✳✳✳✳
4.2 e-Mobility Grid Integration and City Planning					
4.2.1	Smart charging		✳	PED	✳✳✳✳✳
4.2.2	Smartcharging infrastructure deployment planning tool		✳	city	
4.2.3	3D visualization of enhanced decision-making		✳	city	
4.2.4	**Fast V2G Charging Station**	✳		PED	✳✳✳✳✳
4.2.5	Light Electric Vehicle Charging Hub	✳		PED	✳✳✳✳✳
4.2.6	**EV Sharing Scheme**	✳		PED	✳✳✳✳✳

Automated Driving and Vehicle-to-Vehicle Communication of Robot Cars via 5G

RESPONSE
Integrated Solutions for Positive Energy and Resilient Cities

- VTT's robot cars, demonstrate the benefits of a low-latency 5G network in Turku's PED area.
- Optimise energy use in electric vehicles by managing automation sensors based on redundant data from other sources, potentially extending their range in city areas.
- The vehicles act as data hubs, collecting and streaming information over the 5G network for route planning and Smart City Knowledge Graph interactions.
- Sensors include LiDAR, cameras, radars, and 5G communication units, with potential additions for air-quality and noise monitoring.

VTT's electric robot car eLvira to be used in the project

Automated Driving and Vehicle-to-Vehicle Communication of Robot Cars via 5G

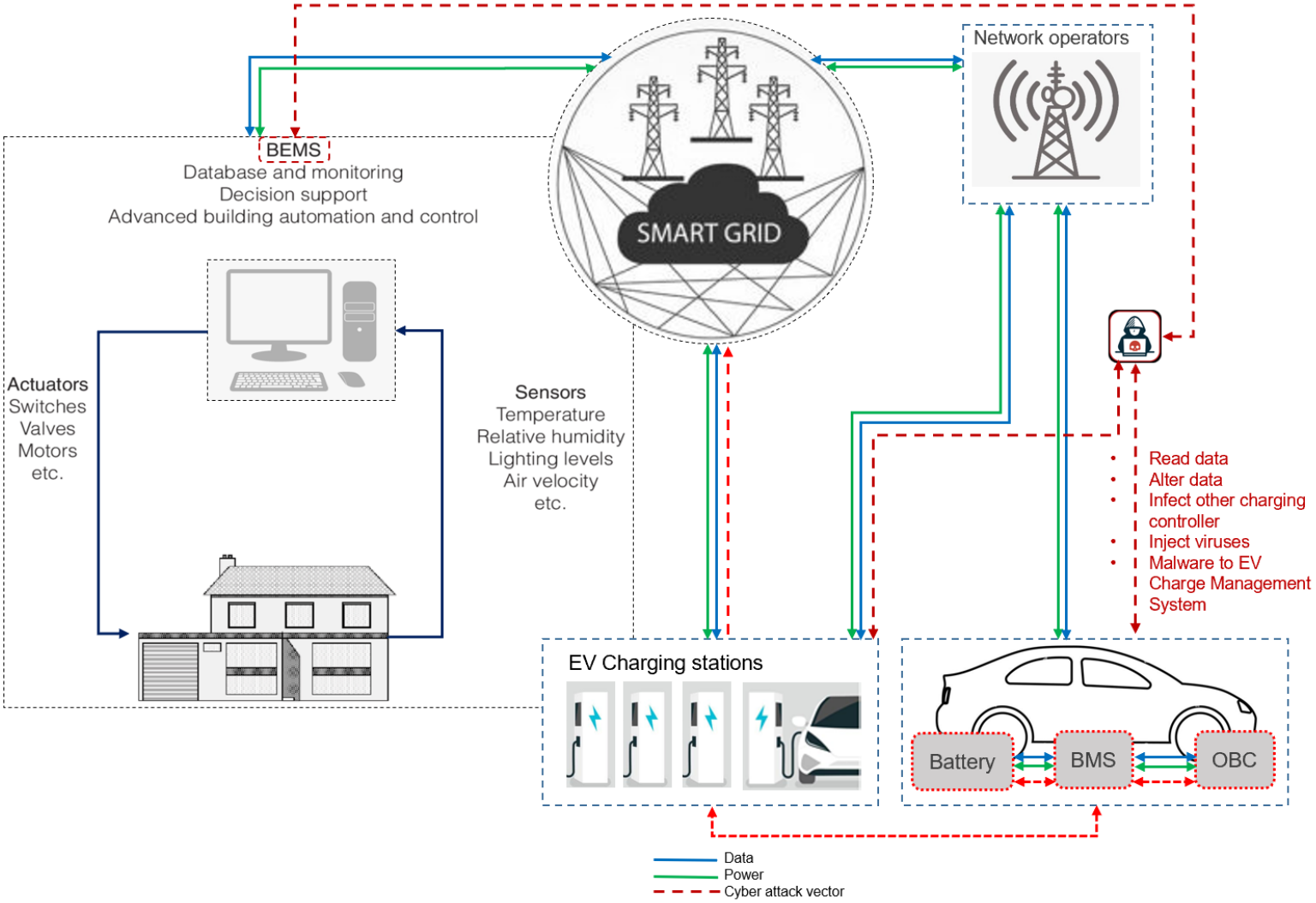
RESPONSE
Integrated Solutions for Positive Energy and Resilient Cities

Potential cyber threats:

- Data Interception
- Unauthorized Access to Vehicle Systems
- Denial of Service (DoS)
- Sensor Spoofing
- Vulnerabilities in Smart City Knowledge Graph
- Privacy Concerns

VTT's electric robot car eLvira to be used in the project

Typical Smart City Charging Infrastructure and Cyber Attack Vectors



Smart City Charging Infrastructure Security Issues

Charging attack surfaces:

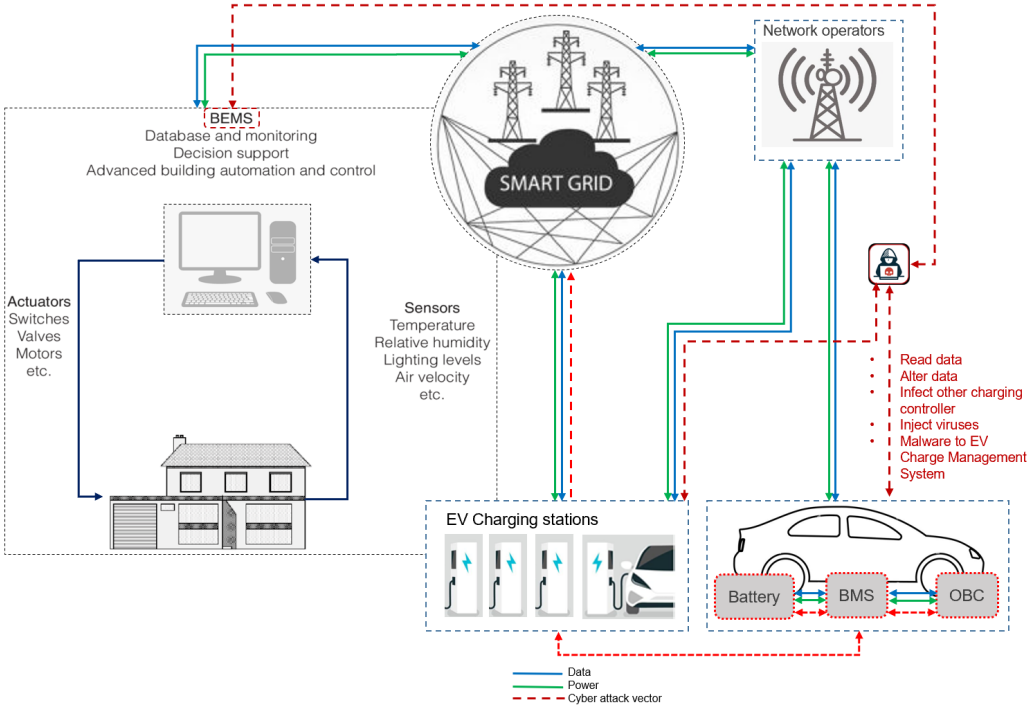
- EV-to-EVSE – charging fraud via vehicle impersonation.
- Grid to EV – attacks against charging networks could disrupt the ability to charge electric vehicles at scale.
- Grid to Fleet – charging stations attacking multiple vehicles.

Potential security issues in smart charging:

- MITM attacks
- DoS
- Denial-of-charge
- Malware (mostly used to penetrate a charging station network, targeting one OEM)
- Attack on two-way power flow

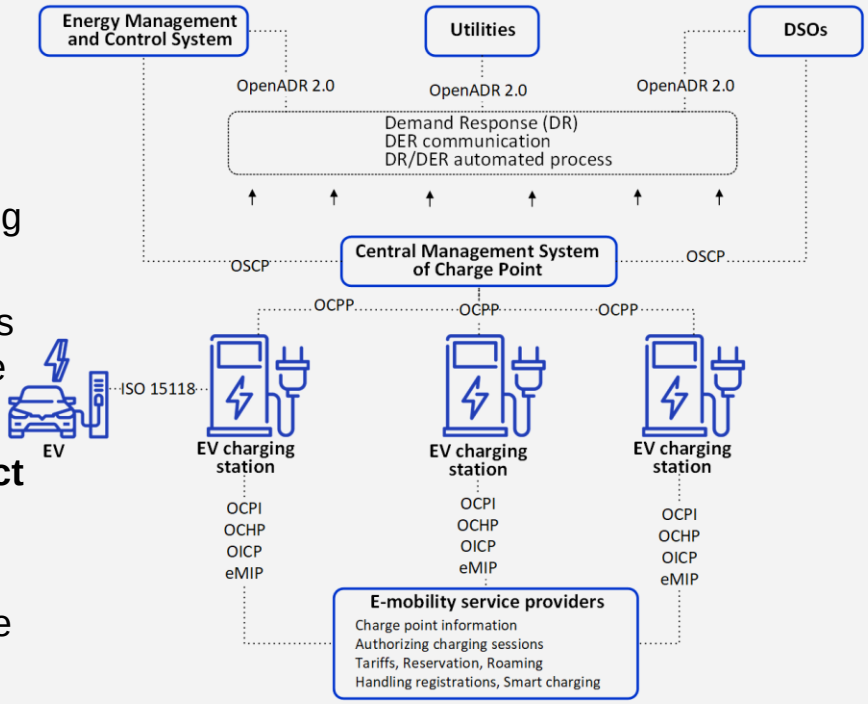
Potential security issues in fast chargers

- False Data Injection Attack (FDIA)
- MITM
- DoS
- Malware injections via EVs



Key Points on Cybersecurity Vulnerabilities in Electric Vehicle Charging Stations

- Electric vehicle (EV) charging stations face a **growing threat landscape**, with cybersecurity vulnerabilities posing risks to user data and system integrity.
- Vulnerabilities could allow hackers to access **vehicle data** or consumers' **credit card information**.
- Some chargers allowed hackers to **stop or start charging** at will, impacting frustrated drivers and posing potential risks to electricity networks.
- The **cumulative impact** of hackers affecting thousands or millions of chargers simultaneously could destabilize entire electricity networks.
- A top recommendation is for consumers **not to connect** their home **chargers to the internet** to prevent vulnerabilities.
- **Safeguards** against vulnerabilities must primarily come **from manufacturers**.
- **Regulation** is suggested as a means to drive the industry to improve baseline security standards.
- **Emerging EV charging technologies**, such as inductive charging and battery swapping, may offer superior cyber protection compared to traditional conductive charging methods.



Communication standards for the electric vehicle charging infrastructure

RESPONSE

Integrated Solutions for Positive Energy and Resilient Cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement nº 957751. The document represents the view of the author only and is his/her sole responsibility: it cannot be considered to reflect the views of the European Commission and/or the European Climate, Infrastructure and Environment Executive Agency (CINEA). The European Commission and the Agency do not accept responsibility for the use that may be made of the information it contains.