

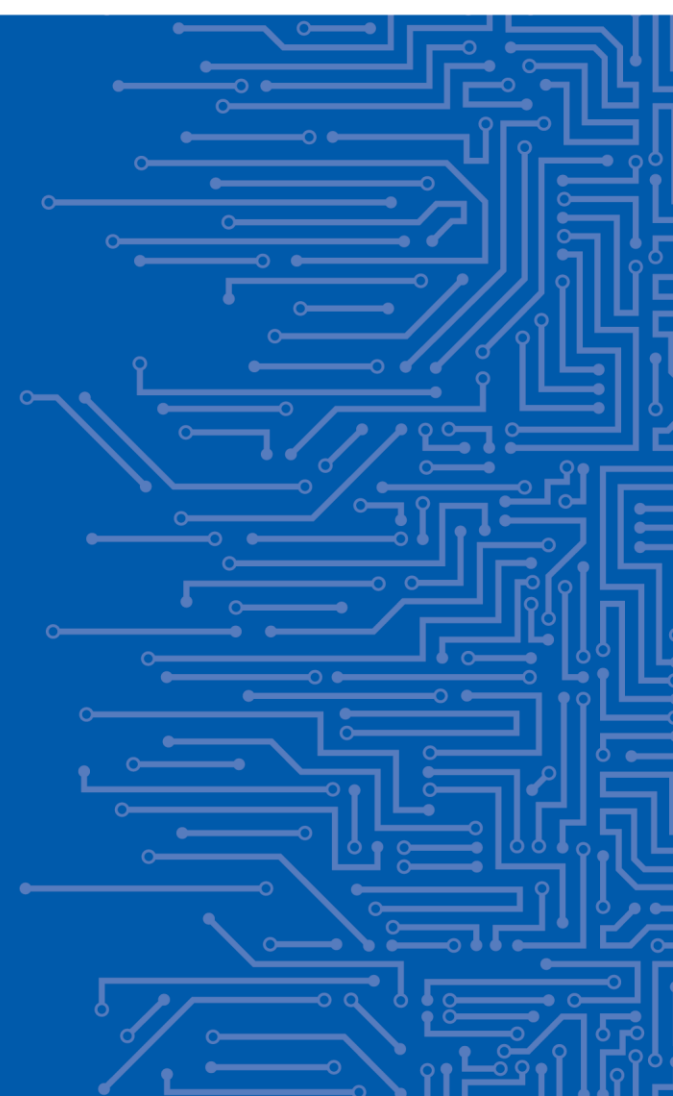


EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# CYBERSECURITY IN THE CONNECTED AND AUTOMATED MOBILITY WORLD

Rossen Naydenov  
Officer in Network and Information Security, ENISA

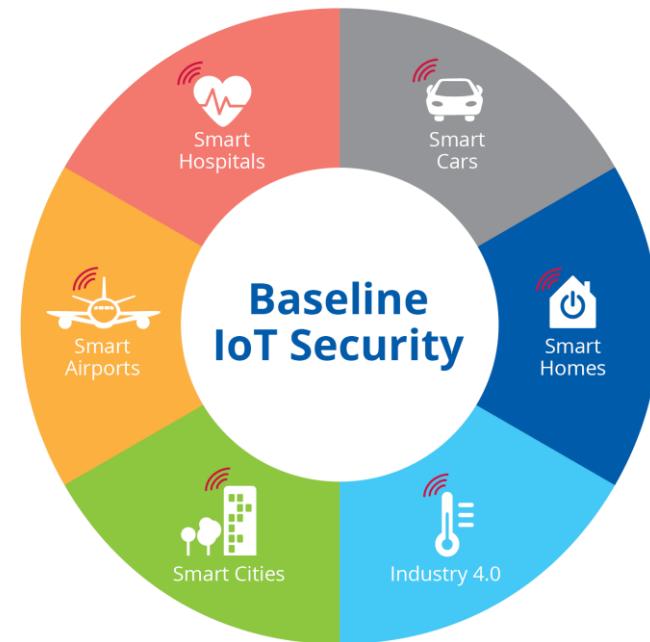
08 | 09 | 2020



# EVERYTHING IS CONNECTED

## Automated mobility is IoT for mobility

- Wide ecosystem
  - OEMs
  - Intelligent transport systems
  - Suppliers
  - Third party services, e.g. ride share, different modes of transport (scooter, bike, bus)
- Advanced connectivity
- Adaptive behavior
- Artificial Intelligence
- Numerous sensors and actuators
- Real-time analytics





# ENISA ACTIVITIES ON MOBILITY

- **Support the implementation of the NISD in the Road Transport sector**
- **Recommendations for CAM**
  - Builds on the good practices for smart cars from 2019
- **Collaboration with DG MOVE, RTD, GROW & CONNECT via CCAM Platform**
- **Engagement with industrial stakeholders, e.g. OEMs, Tier 1 and Tier 2 suppliers, wider ecosystem stakeholders**



# HARMONIZATION EFFORTS IN AUTOMOTIVE TRANSPORT

- **Mapping to existing automotive cybersecurity initiatives**
  - UNECE, ISO, SAE, ETSI, ...
- **Engaging and validating findings with the community**
  - Manufacturers
  - Tier 1, Tier 2 suppliers
  - Relevant EC DGs and MS cybersecurity agencies
- **Threat model of ENISA 2016 was used for UNECE threat model**
- **2019 study maps to UNECE regulation**
  - Extra security measures for semi-autonomous and autonomous vehicles
  - Wider view of automotive ecosystem



# CONNECTED AND AUTOMATED MOBILITY ECOSYSTEM

- **Stakeholders**

- Connected vehicles,
- Connected infrastructure (e.g. traffic management, etc. )
- Suppliers – both to the vehicles and the infrastructure
- Third party services (e.g. intelligent transport, bikes, scooters, parkings, etc.)

- **Critical services**

- Connected to the user
- Between stakeholders in the ecosystem

- **Critical information infrastructure**

- Vehicle systems
- Systems with direct or no direct vehicle interaction

# CAM SERVICES (PREVIEW)

## User services

### Driving Enhancement

- Driving optimization
- Autonomous driving
- Navigation
- EV services
- Parking & Toll services

### Infotainment

- Music / Audio
- In vehicle Payment
- Information apps
- Games

### Safety Management

- ADAS (Emergency functions, collision protection, hazard warnings, etc.)
- Roadside assistance
- Environmental protection

### MaaS

- Car sharing
- Car rental
- Co-riding
- Public / shared transport
- Bike sharing services
- Free floating services
- Soft mobility navigation and optimization
- Multimodality optimization

### Home Management

- Appliances management
- Automated features when approaching home

### Remote services

- Vehicle data collection (performance, use, etc.)
- Remote control

### Insurance Management

- Pay as you drive/use
- Incident investigation

### Security systems

- Video protection
- Anti-theft
- Tracking

### Vehicle interaction (V2X)

- C-ITS services
- C-CAM services
- C2C services

### Advertising

- In-vehicle advertising
- Promotional offer
- Suggestion

## B2B Services (OEM, suppliers, operators, tiers)

### Fleet Management

- Localization
- Data collection
- Fleet optimization
- Rental Management

### Maintenance

- Diagnosis & prognosis
- Over The Air update & repair
- Data collection

### Road Infrastructures Management

- Route and priority optimization
- Traffic signal management
- Road analysis and management
- Road infrastructures analysis and management
- Traffic analysis and management
- Data braking

# SYSTEMS AND INFRASTRUCTURES

Vehicle systems

Systems with direct vehicle interaction

Systems without direct vehicle interaction

Conception and Manufacturing

**Conception & Development**

Design and Development of CAM systems (CAO, Coding, etc.)

Configuration management systems

Supplier management systems

**Vehicle, components and systems Manufacturing**

Onboard electronic initialization systems

Asset inventory & procurement systems

Industrial control systems

Cybersecurity tools and back-ends

Detection and reaction systems (VSOC)

Vulnerability Management systems

Risk Management systems

Infrastructure protection systems (IPS, etc.)

Administration systems

Secured archiving systems

Back-ends

Manufacturer, Suppliers and Service providers Operations

**Connected Services Management & Upgrades**

Connected Vehicles Platforms

Customers applications

Connected services

Over the Air Systems

**Dealer Network – Sales, Distribution and Customer relations**

Marketing systems

Sales and After-sales systems

**Maintenance**

Asset inventory & procurement systems

Diagnostic systems

Road Vehicles & Micro mobility

Onboard cybersecurity systems

Onboard E/E systems & (ECUs, sensors, etc.)

Onboard Infotainment systems and services

Telematic systems

Short range communication network

Long range communication network

User devices

Smartphone and other portable devices

Smart Home building integration

Interactions, interoperability and 3rd Parties

V2X communication systems (C-ITS, C2C, etc.)

3rd Parties systems and platforms

Data exchange and collaboration systems and platforms

MaaS systems and platforms

Tiers and Road Infrastructures

Communication systems for ecosystems (police, rescue, etc.)

Intelligent Transport systems (intelligent warehouses, parking lots, etc.)

Traffic management & signaling systems

EV charging infrastructures

Road Infrastructures Systems (highway toll, parking meter, etc.)

Micro mobility systems (bikes, e-scooters, stations, etc.)

Monitoring & Surveillance systems (CCTV, etc.)



# CHALLENGES AND RECOMMENDATIONS FOR CYBERSECURITY OF CAM

- **Objective**

- Identify which are the challenges the stakeholders have in implementing cybersecurity in the CAM ecosystem
- Propose recommendations to overcome the challenges

- **Target audience**

- Policy makers - European Commission, National Authorities
- OEMs
- Suppliers
- Third Party Service providers
- Road Equipment Manufacturers



# CHALLENGES IN CAM (TOP 3)

- **Governance**

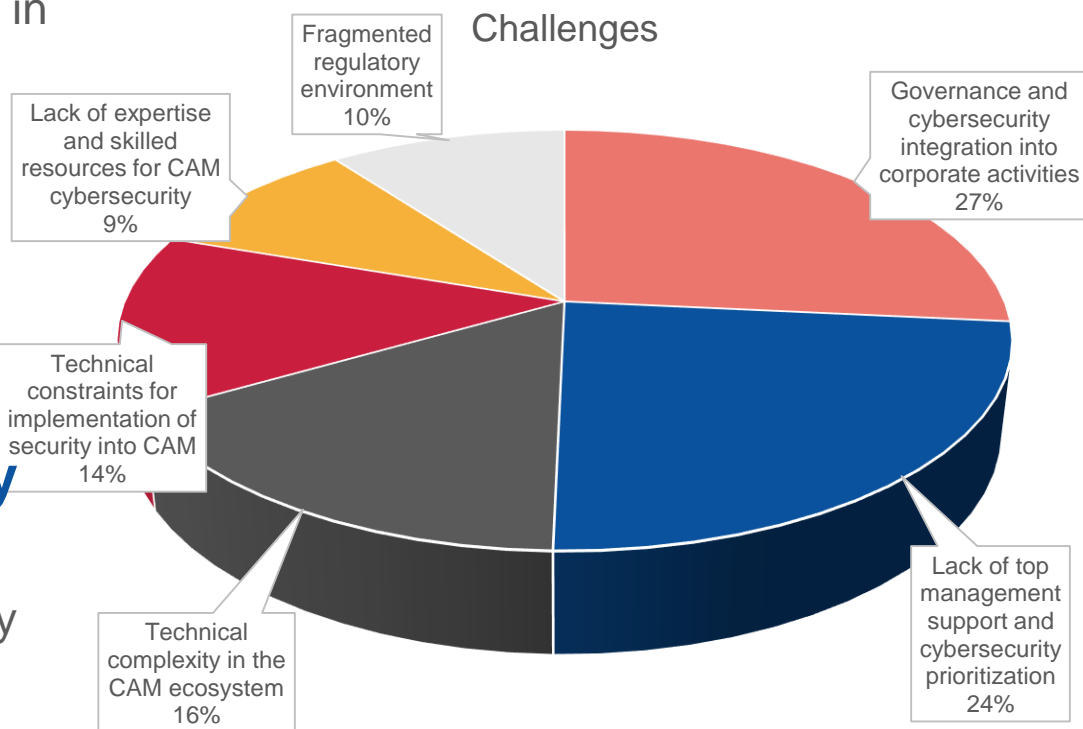
- integration of cybersecurity in the corporate activities

- **Top Management support**

- Cybersecurity not a priority

- **Technical Complexity**

- Multiple stakeholders with different or even no security requirements





# PREVIEW OF RECOMMENDATIONS FOR CYBERSECURITY OF CAM

- **Establish administrative structures for top-level management to discuss and exchange views with cybersecurity experts and CISOs.**
- **Incentivize innovation and R&D activities for securing IT and CAM environments, components, systems and services.**
- **Promote the use of standardized components to homogenize the systems in order to simplify, and make possible the understanding of the ecosystem interaction.**



# CONCLUSIONS

- **Mobility industry is having similar cybersecurity issues as many other industries, e.g. Rail, Energy**
- **Encourage cross-functional security and safety knowledge exchange between IT and mobility experts respectively**
- **Raise awareness to the board level of the organization about the impact of cybersecurity and technology on the CAM ecosystem lifecycle**

# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**  
Vasilissis Sofias Str 1, Maroussi 151 24  
Attiki, Greece

 +30 28 14 40 9711

 [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

