THE STATE OF THE ART IN CYBER SECURITY, EU REGION

RICCARDO MARIANI | VICE PRESIDENT, INDUSTRY SAFETY, NVIDIA | IEEE CS FIRST VP
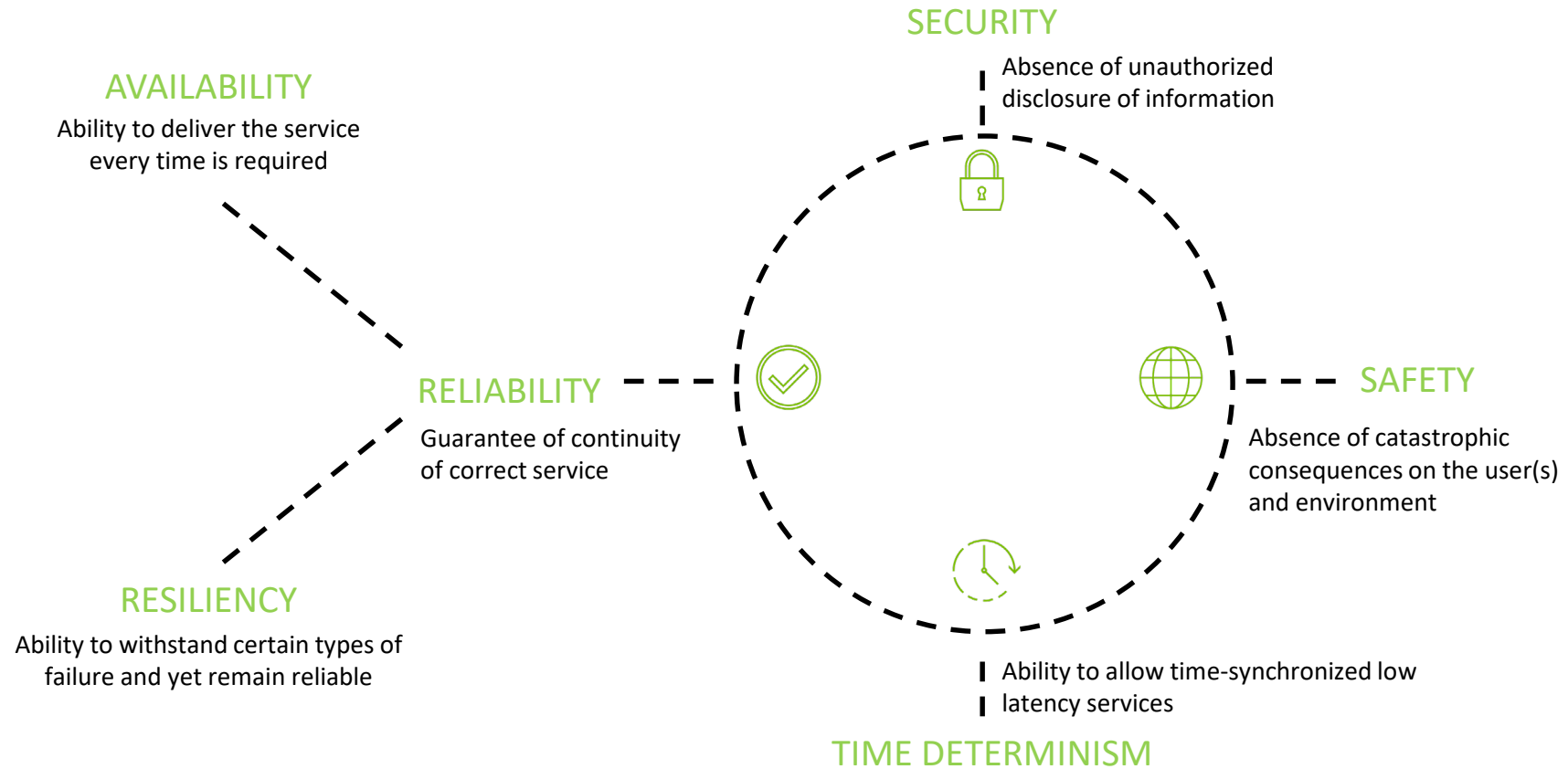BARNABY SIMKIN | MANAGER OF REGULATORY AFFAIRS, NVIDIA

JANUARY 27, 2021

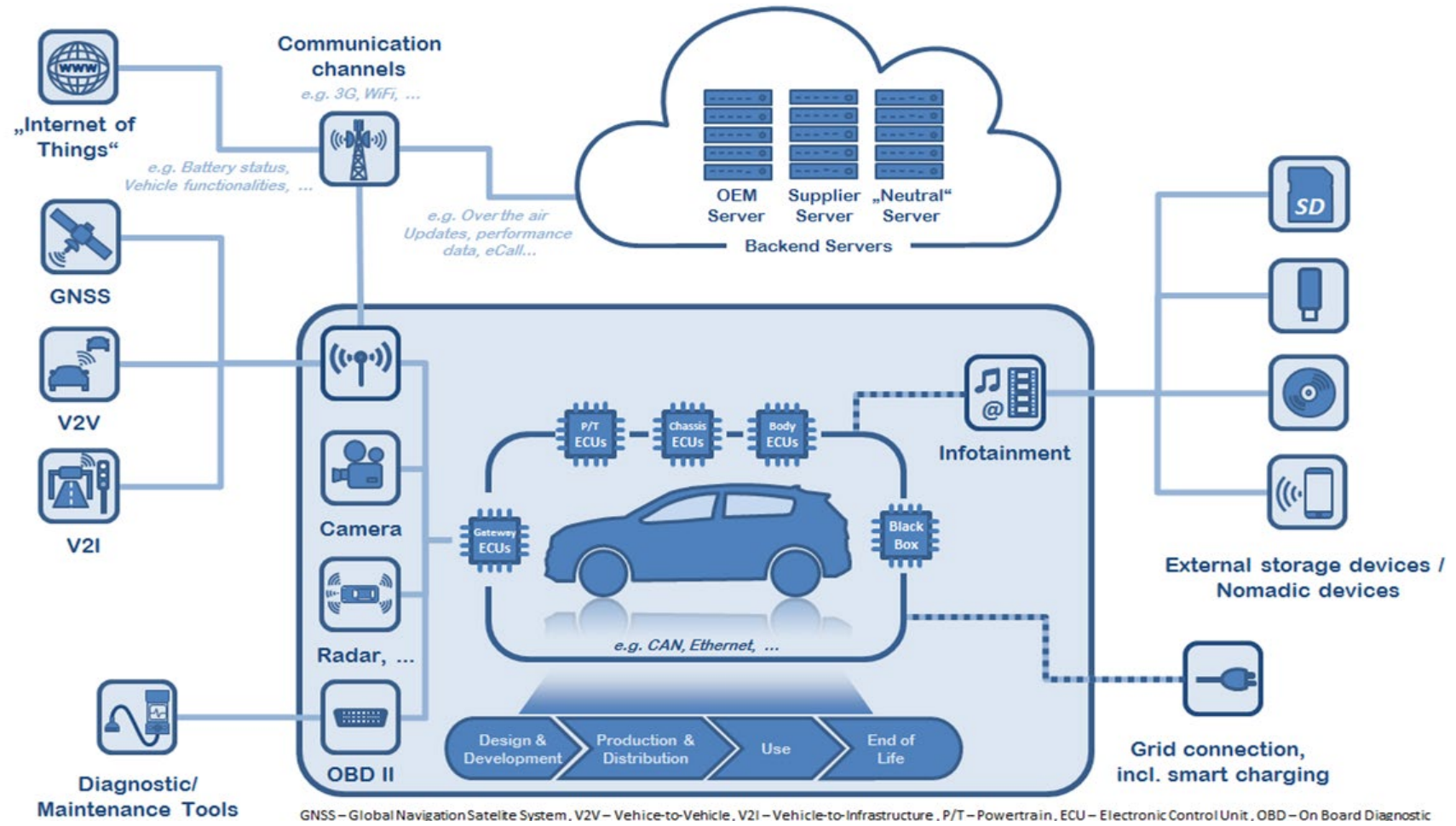# ABOUT TRUSTWORTHINESS

From VDE-AR-E 2842-61

ABOUT TRUSTWORTHINESS
Special Focus on Connected AVs

SECURITY

Absence of unauthorized disclosure of information

AVAILABILITY

Ability to deliver the service every time is required

RELIABILITY

Guarantee of continuity of correct service

SAFETY

Absence of catastrophic consequences on the user(s) and environment

RESILIENCY

Ability to withstand certain types of failure and yet remain reliable

Ability to allow time-synchronized low latency services
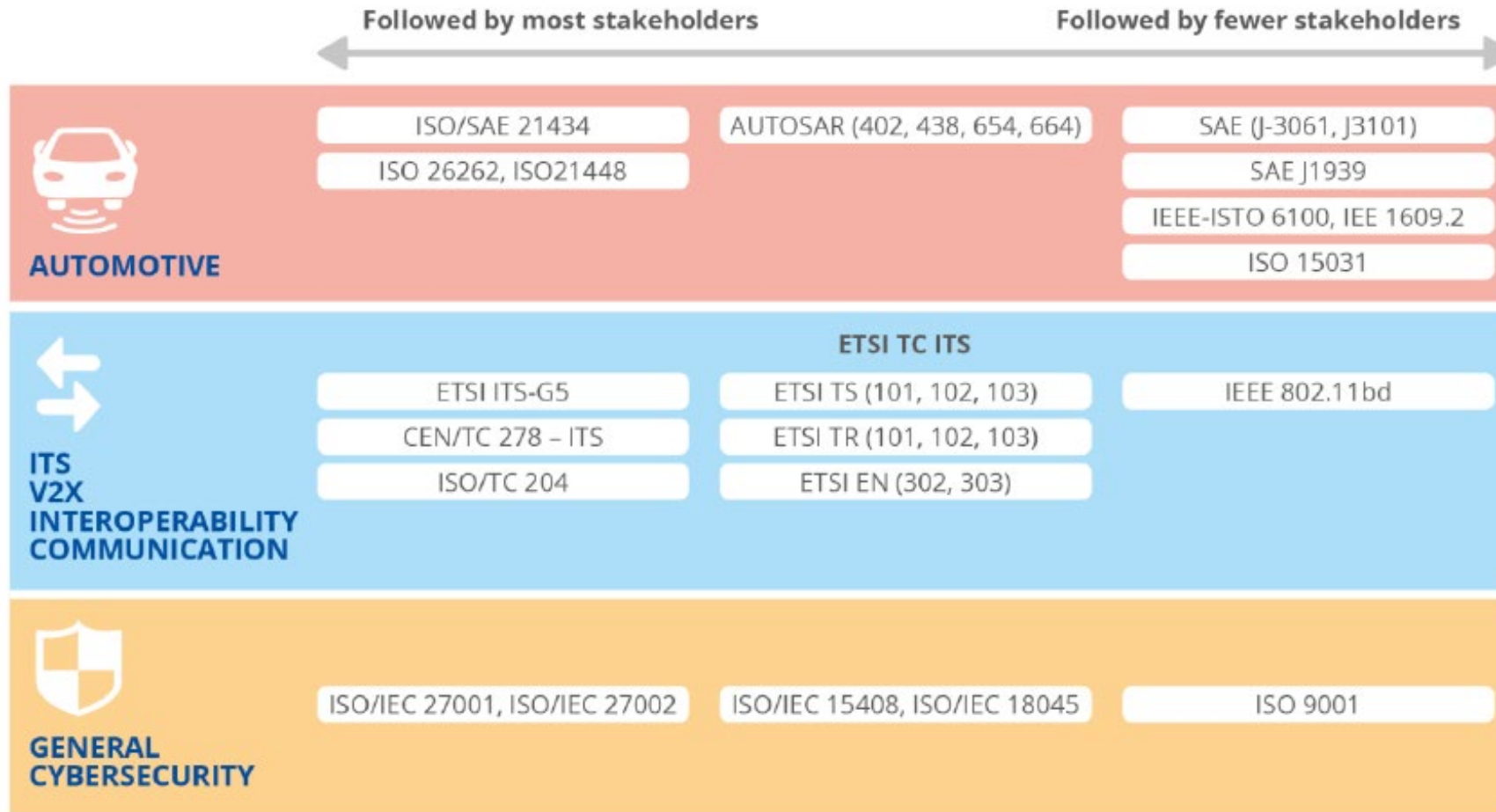
TIME DETERMINISM

CYBERSECURITY CHALLENGES

Potential Cyber/Physical Interfaces into a CAV

STANDARDS

ENISA Publication on Connected and Automated Mobility (CAM)

Followed by most stakeholders ◄──────► Followed by fewer stakeholders

AUTOMOTIVE
- ISO/SAE 21434
- ISO 26262, ISO21448
- AUTOSAR (402, 438, 654, 664)
- SAE (J-3061, J3101)
- SAE J1939
- IEEE-ISTO 6100, IEE 1609.2
- ISO 15031

**ITS
V2X
INTEROPERABILITY
COMMUNICATION**

ETSI TC ITS
- ETSI ITS-G5
- CEN/TC 278 – ITS
- ISO/TC 204
- ETSI TS (101, 102, 103)
- ETSI TR (101, 102, 103)
- ETSI EN (302, 303)
- IEEE 802.11bd

**GENERAL
CYBERSECURITY**
- ISO/IEC 27001, ISO/IEC 27002
- ISO/IEC 15408, ISO/IEC 18045
- ISO 9001

REGULATIONS
Going Beyond the Standards

UN / WP.29 – World Forum for Harmonization of Vehicle Regulations
› Draft Proposal to introduce a Regulation on Cyber Security and Software Updates

ISO TC22/SC32/WG11 - Cybersecurity
› ISO/SAE 21434 Road vehicles – Cybersecurity Engineering
› ISO 24089 on Software Updates Engineering

National Discussions
› (D) VDA QMC
› (UK) BSI PAS 1885:2018
› …

European Union
› Cybersecurity Act
› General Data Protection Regulation
› NIST Directive
› C-ITS Delegated Act

China
› Cybersecurity Law
› Draft Encryption Law
› SAC/TC 114/SC 34/WG Cyber

Regulation American Market
› NHTSA Cybersecurity Guidelines
› Draft SELF DRIVE Act
› Draft AV START Act

REGULATIONS
Existing EU Requirements

UN Regulation Automotive Cybersecurity

- Mandatory cybersecurity requirements as precondition for vehicle registration

- Certification is based on type approval by an authority which designated a technical service

- Objective: Impose minimum regulatory cybersecurity requirements to assure safety and data protection of the consumer in the vehicle and its infrastructure

EU Cybersecurity Act

- Voluntary certification of products with regard to cybersecurity (not yet specific to the automotive sector) -- certification could become mandatory in a later step

- Certification is based on self-certification for lower assurance levels or external certification for the highest assurance level

- Objective: Permit the consumer to identify products with a good level of cybersecurity (market transparency and security awareness)

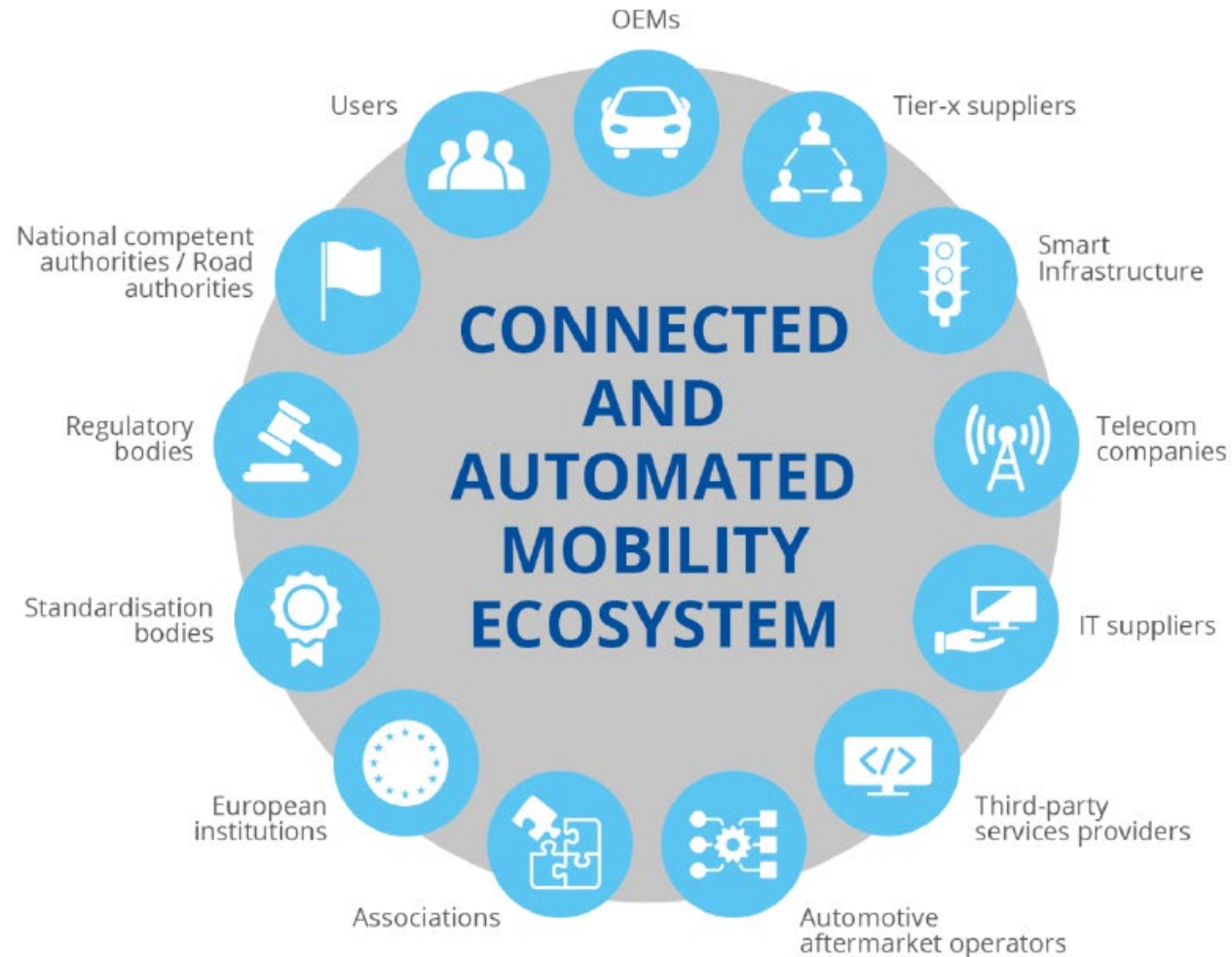# REGULATION – EU DEVELOPMENT
EU Directive

EU NIST 2.0 Directive

• Member States shall adopt a national cybersecurity strategy, designate competent national authorities, single points of contact and Computer Security Incident Response Team (CSIRT)s

• Member States shall lay down cybersecurity risk management and reporting obligations for essential entities and important entities (most micro and small entities are exempt)

- • Management bodies of all entities shall take specific cybersecurity-related training.

- • Entities shall take appropriate and proportionate technical and organizational measures to manage the cybersecurity risks

• A European Cyber Crises Liaison Organisation Network (EU - CyCLONe) shall be established to support the coordinated management of large-scale cybersecurity incidents

• Member States shall lay down obligations on cybersecurity information sharing

• ENISA is required to issue in cooperation with the Commission a biennial report on the state of cybersecurity in the Union

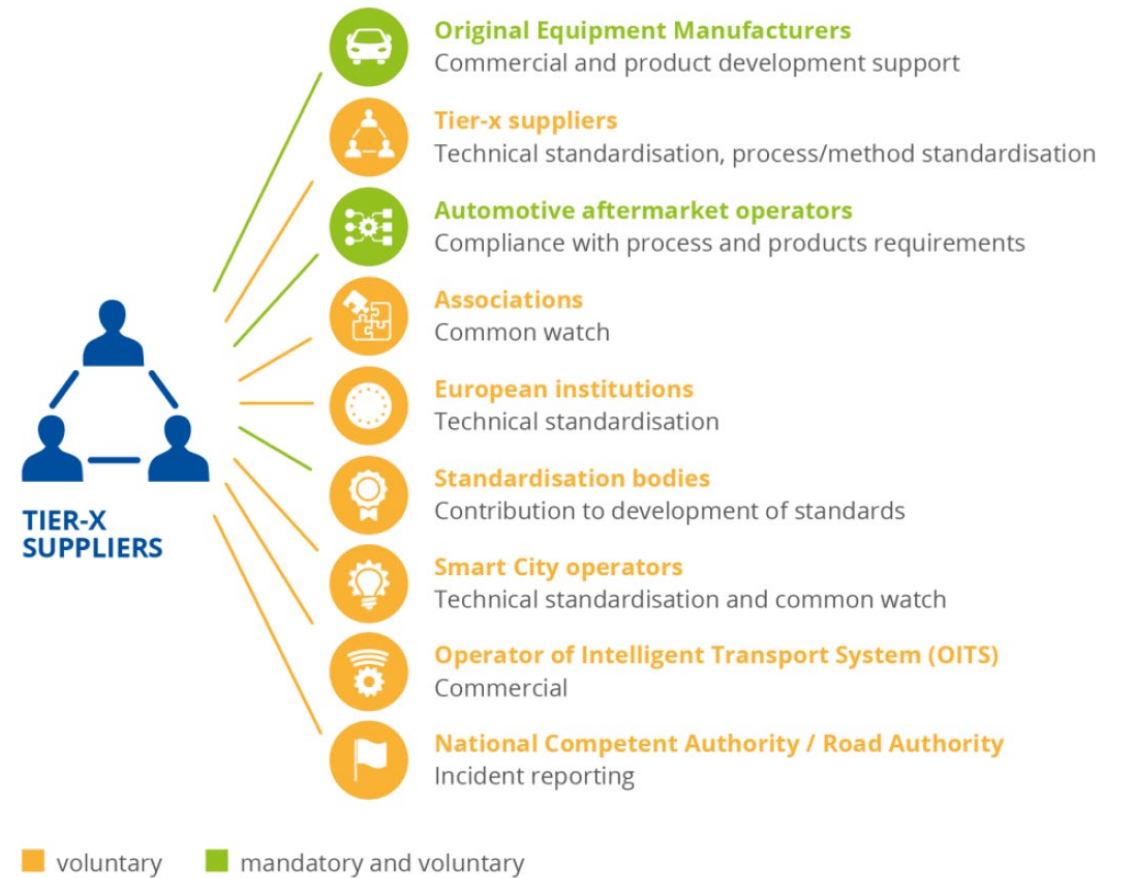## ENISA Publication on Connected and Automated Mobility (CAM)

Figures from "CYBERSECURITY STOCKTAKING IN THE CAM", ENISA, November 2020

Figures from "CYBERSECURITY STOCKTAKING IN THE CAM", ENISA, November 2020

ORIGINAL EQUIPMENT MANUFACTURERS (OEMS)

Tier-x suppliers
Technical standardisation, process/method standardisation

Automotive aftermarket operators
Compliance with process and products requirements

Associations
Common watch

European institutions
Technical standardisation, process/method standardisation, common watch

Standardisation bodies
Contribution to standards definition

National Competent Authority / Road Authority
Technical standardisation, common watch

- mandatory
- voluntary
- mandatory and voluntary

TIER-X SUPPLIERS

Original Equipment Manufacturers
Commercial and product development support

Tier-x suppliers
Technical standardisation, process/method standardisation

Automotive aftermarket operators
Compliance with process and products requirements

Associations
Common watch

European institutions
Technical standardisation

Standardisation bodies
Contribution to development of standards

Smart City operators
Technical standardisation and common watch

Operator of Intelligent Transport System (OITS)
Commercial

National Competent Authority / Road Authority
Incident reporting

- voluntary
- mandatory and voluntary

10

ENISA Publication on Connected and Automated Mobility (CAM)

Figures from "CYBERSECURITY STOCKTAKING IN THE CAM", ENISA, November 2020

CONCEPTION AND MANUFACTURING

Conception & Development systems

Design and Development of CAM systems (CAO, Coding, etc.) | Configuration management systems | Supplier management systems

Assets, components and systems Manufacturing

Onboard electronic initialisation systems | Asset inventory & procurement systems | Industrial control systems

CYBERSECURITY TOOLS AND BACK-ENDS

Detection and reaction systems (VSOC) | Vulnerability Management systems | Risk Management syste | Infrastructure protection systems (IPS, etc.)

Administration systems | Secured archiving systems | Back-ends

MANUFACTURERS, SUPPLIERS AND SERVICE PROVIDERS OPERATIONS

Connected Services Management & Upgrades systems

Connectivity gateways and platforms

Customers applications

Connected services

Over the Air Systems

Dealer Network – Sales, Distribution and Customer relations systems

Marketing systems

Sales and After-sales systems

Maintenance tools

Asset inventory & procurement systems

Diagnostic systems

RECENT DEVELOPMENTS IN THE EU
ENISA Publication on Connected and Automated Mobility (CAM)

Figures from "CYBERSECURITY STOCKTAKING IN THE CAM", ENISA, November 2020

RECENT DEVELOPMENTS IN THE EU
ENISA Publication on Connected and Automated Mobility (CAM)

Figures from "CYBERSECURITY STOCKTAKING IN THE CAM", ENISA, November 2020

GOVERNANCE
- Standards application
- Cybersecurity management system
- Cybersecurity management system audit
- Information system / product security policy
- Information system / product security indicators
- Human resource security

RISK & ECOSYSTEM MANAGEMENT
- Information system / product security risk analysis
- Information system / product security audit
- Information system / product security accreditation
- Ecosystem relations / suppliers risk management
- Ecosystem / suppliers mapping
- Communication with competent authorities and CSIRTs

DETECTION & REACTION
- Crisis management organisation
- Crisis management process
- Information system / product security incident detection
- Information system / product security incident response
- Information system / product security incident report
- Logging
- Logs correlation and analysis
- Business continuity management
- Disaster recovery management

MAINTENANCE IN SECURITY CONDITION
- Security maintenance procedure

IS/IT/OT
- Information security management
- Cryptography
- Access rights
- Identification
- Administration accounts
- Administration information systems
- System segregation
- Systems configuration
- Traffic filtering
- Industrial control systems
- Physical and environmental security

REFERENCES

[1] C. Schmittner, G. Macher, "Automotive Cybersecurity Standards – Relation and Overview", Oct. 2019

[2] Proposal For A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL On Measures For A High Common Level Of Cybersecurity Across The Union, December 2020

[3] Cybersecurity Stocktaking In The Cam, ENISA, November 2020

[4] IEEE Standards Activities in the Network and Information Security (NIS) Space

[5] How Can Autonomous Vehicles Be Protected Against Cyber Security Threats?, IEEE Innovation at work

[6] Automotive Cyber Security: Protecting the Vehicular Network, IEEE Innovation at work

[7] Automotive CyberSecurity, IEEE INFOSec

[8] Cybersecurity Best Practices for the Safety of Modern Vehicles, NHTSA, Draft 2020 update

[9] S. Parkinson et al, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges", March 2017

[10] Landini, "Ethical Issues, Cybersecurity And Automated Vehicles"