IEEE SA
STANDARDS ASSOCIATION

THE GLOBAL CYBER SECURITY APPROACH (SUMMARY WEBINAR)

RICCARDO MARIANI | VICE PRESIDENT, INDUSTRY SAFETY, NVIDIA | IEEE CS FIRST VP

FEBRUARY 12, 2021

IEEE

WEBINAR CYBER SECURED AUTONOMOUS VEHICLES

The state of the art in Cyber Security,
EU region

Riccardo Mariani: VP Industry Safety NVIDIA
IEEE Computer Society 1st VP and VP of Standardization

Development status of China's connected vehicles cybersecurity industry,
CN region

Yanan Zhang: CATARC / Deputy Director Cyber Security

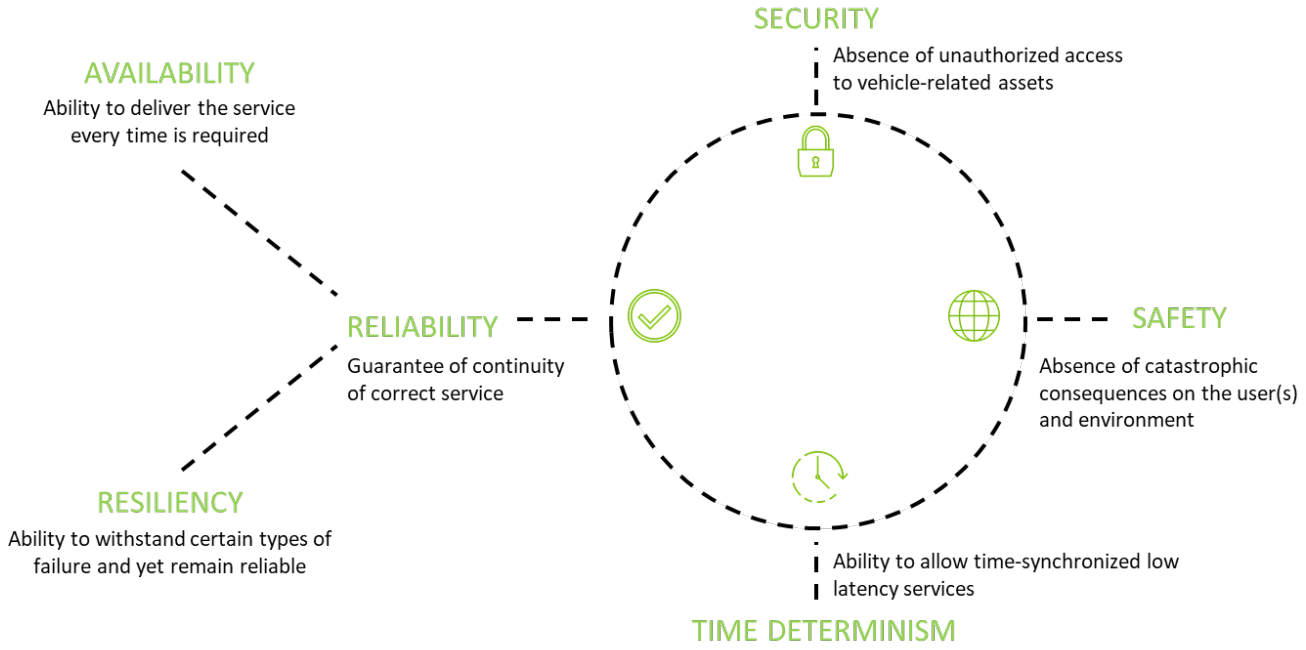
How to prepare the automotive V2X-ecosystem for the quantum age,
US region

Dr. Joachim Taiber: Chief Technical Officer
International Transportation Innovation Center

ABOUT TRUSTWORTHINESS

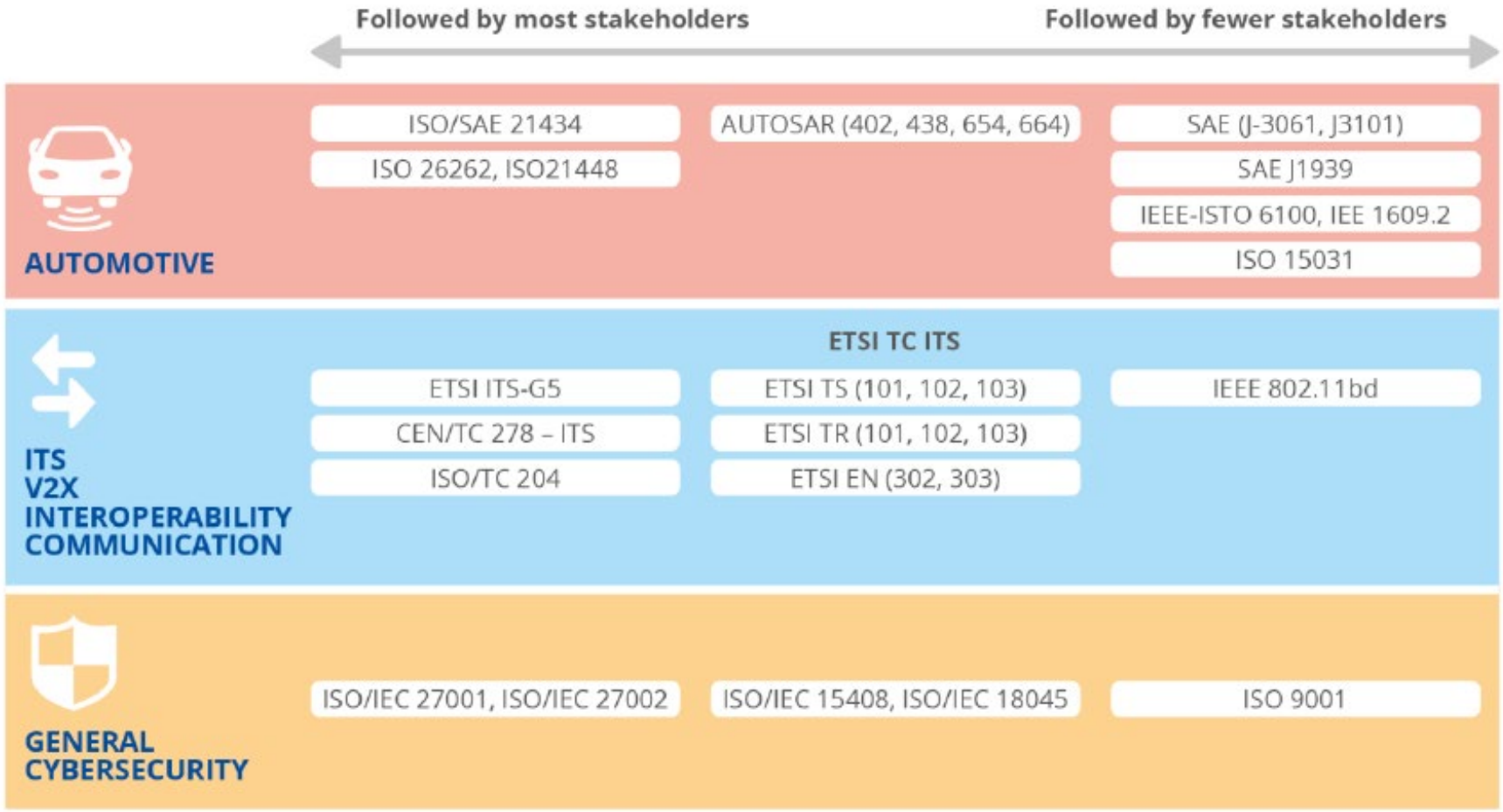
Introduction

From VDE-AR-E 2842-61



STANDARDS

ENISA Publication on Connected and Automated Mobility (CAM)



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

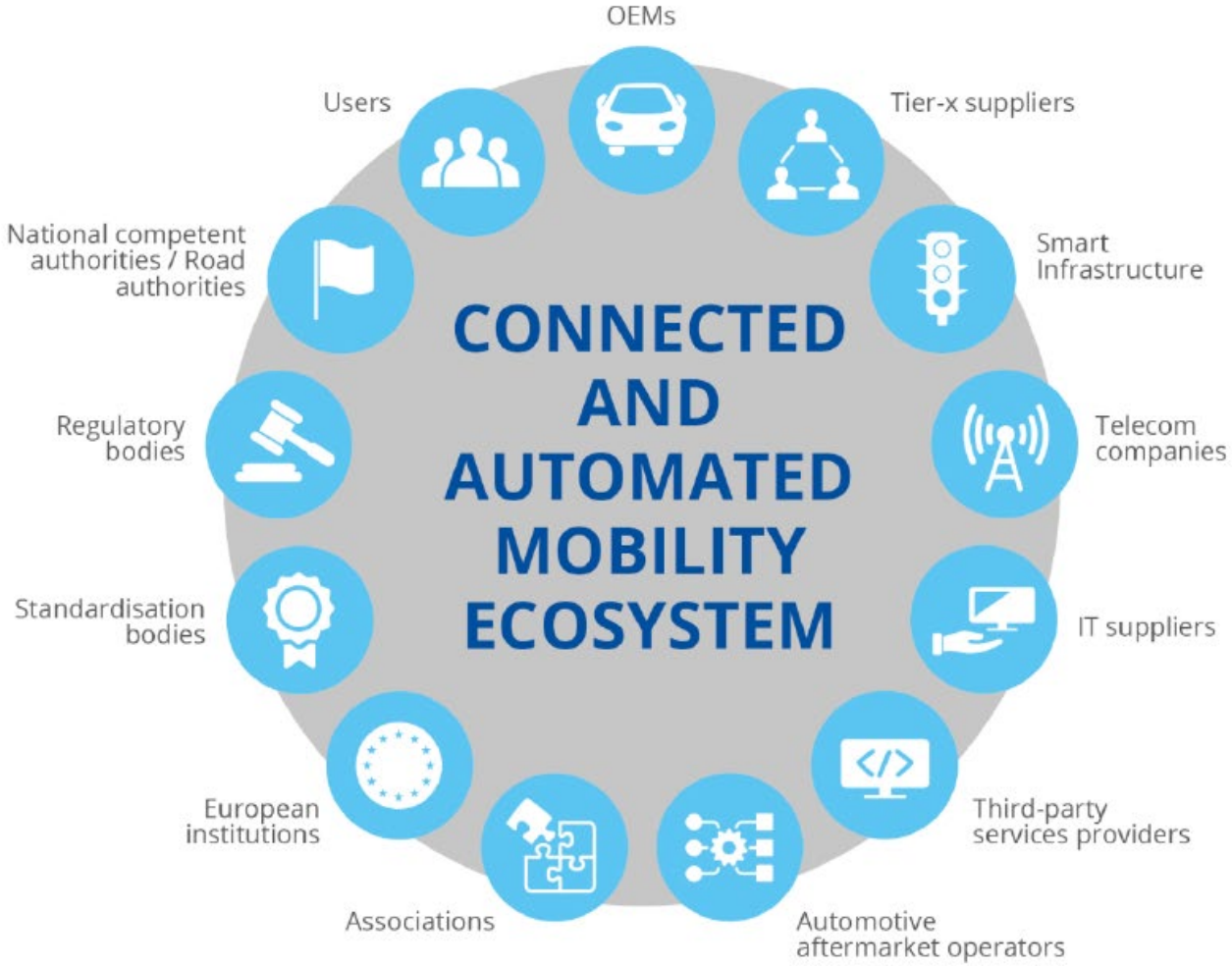
•Member States shall lay down obligations on cybersecurity information sharing

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

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

2.4 CAVD and C-Auto-ISAC

CAVD

Platform name

- China Automobile Vulnerability Database (CAVD)
- Platform address: https://cavd.org.cn

Platform purpose

- Information exchange of automotive and internet industry, including terminal users, white hats and security organizations.
- Collecting and verifying vulnerabilities to construct emergent incident response center of automotive industry.
- Establish a systematic database by statistical analysis, big data and other technical means.

Based on CAVD, a new cybersecurity related information sharing mechanism and analysis center is established: C-Auto-ISAC

3.2 Chinese local cybersecurity related standards

全国汽车标准化技术委员会
National Technical Committee of Auto Standardization

	Standard	Status
1	General technical requirements for vehicle cyber security	Approved
2	Technical requirements for cybersecurity of vehicle gateway	Approved
3	Technical Requirements for Cybersecurity of On-board Interactive System	Approved
4	Cybersecurity technical requirements for EV remote Service and Management system	Approved
5	Technical requirements for cybersecurity of EV charging system	Draft
6	Cybersecurity Risk Assessment Specification of vehicle	Project in discussion
7	Technical requirements for vehicle software update	Project in discussion
8	OBD interface cybersecurity technical requirements	Project in discussion
9	Cybersecurity emergency response management guide of vehicle	Project in discussion
10	Vehicle cybersecurity test method	Project in discussion
11	Road vehicles -Cybersecurity engineering (ISO/SAE21434 transform)	Project in discussion

- Recommended national standards
- Assist companies to produce cybersecurity ensured products
- References of mandatory type approval in the future
- Drafts of standard 1-5 are open on the Internet (Chinese version only)
- The approved standards will be released in 2nd quarter of 2021

4 Developing trend of China's automotive cybersecurity industry

01

Accelerate the establishment and implementation of cybersecurity related standards

02

Improve the approval management of cybersecurity related products, including vehicles and components

03

Improve the testing system and risk assessment system for intelligent connected vehicles

04

Establish national pilot areas for intelligent connected vehicles and smart traffic system

05

Improve the information sharing mechanism for the automotive industry

06

Accelerate the construction of testing and certification system for intelligent and connected vehicles

Potential application areas of quantum computing in Automotive

Automotive R&D

- Vehicle crash simulation
- Aerodynamic optimization
- Acoustic optimization
- Weight optimization
- Energy storage
- Supply chain optimization
- Embedded systems
- Data centers

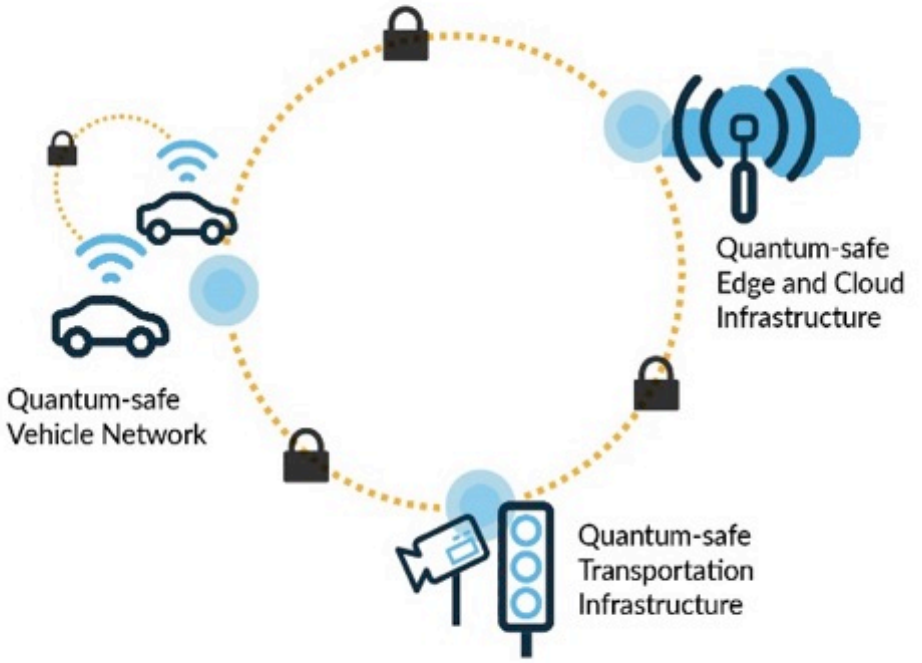
V2X

- Situational Awareness (crash avoidance)
- Cybersecurity threat prevention

Automotive fleet operation

- Traffic route optimization
- Energy use optimization
- Autonomous driving (co-simulation virtual and physical vehicles in real time)

A quantum-safe V2X ecosystem



Quantum Random Number Generation (QRNG)

- ✓ Instantly strengthen your network encryption key material
- ✓ Feed higher quality entropy into key generation servers, HSMs, Linux & crypto applications

State-of-the-art and Quantum-ready encryption

- ✓ Only go with AES-256 symmetric encryption and dedicated robust appliances
- ✓ Be **crypto-agile** & be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further

Quantum Key Distribution (QKD)

- ✓ Quantum-Safe Network Encryption or **Quantum Cryptography**
- ✓ Provide forward secrecy and anti-eavesdropping of the encryption keys
- ✓ Ensure sovereignty and data ownership for the next decade (Post-Quantum era)

Source: ID Quantique

How to apply a quantum risk assessment

First and foremost, it is essential to complete a thorough risk assessment across all system levels (end-to-end) to analyze where in the automotive ecosystem quantum technologies can pose a risk*.

There are five key steps to such a quantum risk assessment:

1. Analyse all assets and determine their cryptographic protection.

2. Map the technological progress in quantum technologies to the state-of-the-art technology being used in the target system.

3. Test and validate quantum-safe cryptography methods.

4. Identify potential threat actors and estimate the time until they could apply quantum technologies for attacks, which determines the timeline to make the target system quantum-safe.

5. Develop a plan to bring the target system into a quantum-safe system state and prioritize activities to anticipate the highest risks

*https://globalriskinstitute.org/publications/3423-2/

NIST working on post-quantum cryptography standard

After spending more than three years examining new approaches to encryption and data protection that could defeat an assault from a quantum computer, the National Institute of Standards and Technology (NIST) has winnowed the 69 submissions it initially received down to a final group of 15. NIST has now begun the third round of public review. This "selection round" will help the agency decide on the small subset of these algorithms that will form the core of the first post-quantum cryptography standard.

NIST plans to release the initial standard for quantum resistant cryptography in 2022.

Source: NIST

The implementation of quantum resistant cryptography will be a major challenge for the Automotive industry !

CONCLUSIONS

1. Experts from different regions are working together to shape the standardization and regulation framework. However, current fragmentation could create overlaps and contradictions between the different initiatives. IEEE can play a very important role to harmonize from the bottom.
2. Cybersecurity for CAV/CAM has a broad E2E scope, involving many technologies and stakeholders.
   It is paramount to create synergies and connections.
3. New technologies (AI, quantum computing etc) as also new business models (OTA updates, crowdsourced / cloud-based services etc.),are posing new challenges for cybersecurity but also new opportunities to solve those challenges. Connection between academic and industry experts is very important to expand the state of art.