Automotive Cybersecurity

Information and Communication Security - Guest Lecture

Dr. Markus Tschersich

www.continental-automotive.com

Continental

Leading the Way for Your Mobility

Leading technology provider and systems integrator of choice for the **software-defined** vehicle

Material expertise for **industry solutions**

Industry-benchmark in **tires**

~200,000 **talented** and **dedicated employees**

Continental Group
Our Structure

Continental

Group Sectors	Automotive	Tires	ContiTech
			
Business Areas	› Safety and Motion › Autonomous Mobility › User Experience › Architecture and Network Solutions	› Original Equipment › Replacement APAC › Replacement EMEA › Replacement The Americas › Specialty Tires	› Industrial Solutions Americas › Industrial Solutions APAC › Industrial Solutions EMEA › Original Equipment Solutions › Surface Solutions

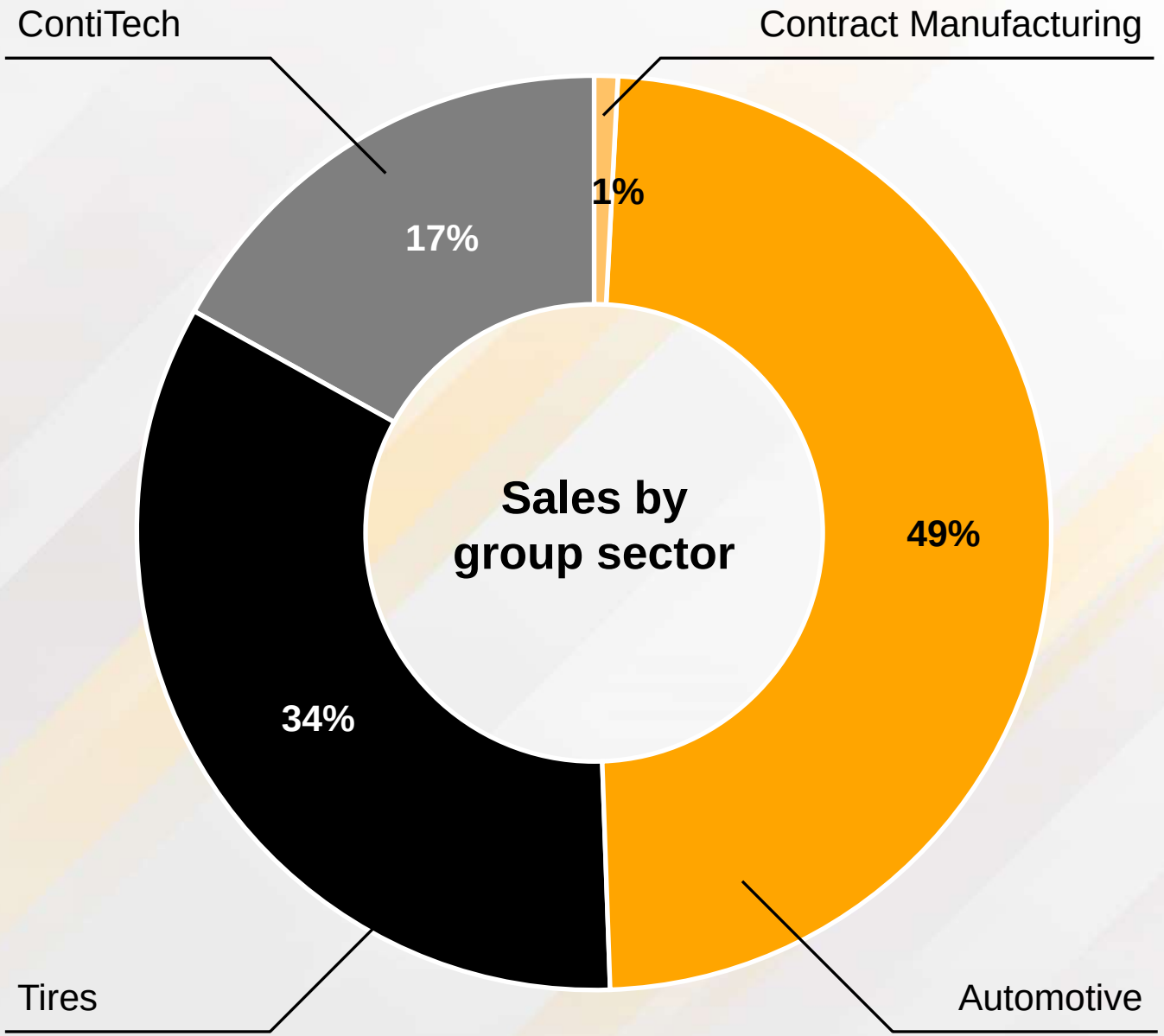
As of November 2024

Continental Group
Overview 2023

€ 41.4 billion
sales

~200,000
employees

505 locations
in **56 countries and markets**



As of Dec. 31, 2023

Automotive Group Sector

The Future of Mobility Solutions

- In the Automotive group sector, we have created dynamic, powerful and flexible business areas that consistently take their bearings from our strategic action fields and the development of the global automotive market. Together with Software and Central Technologies (SCT) they unite products and technologies that belong together from the perspective of the market.
- The business areas and SCT work together across the organization to push forward the implementation of our strategy.

User Experience

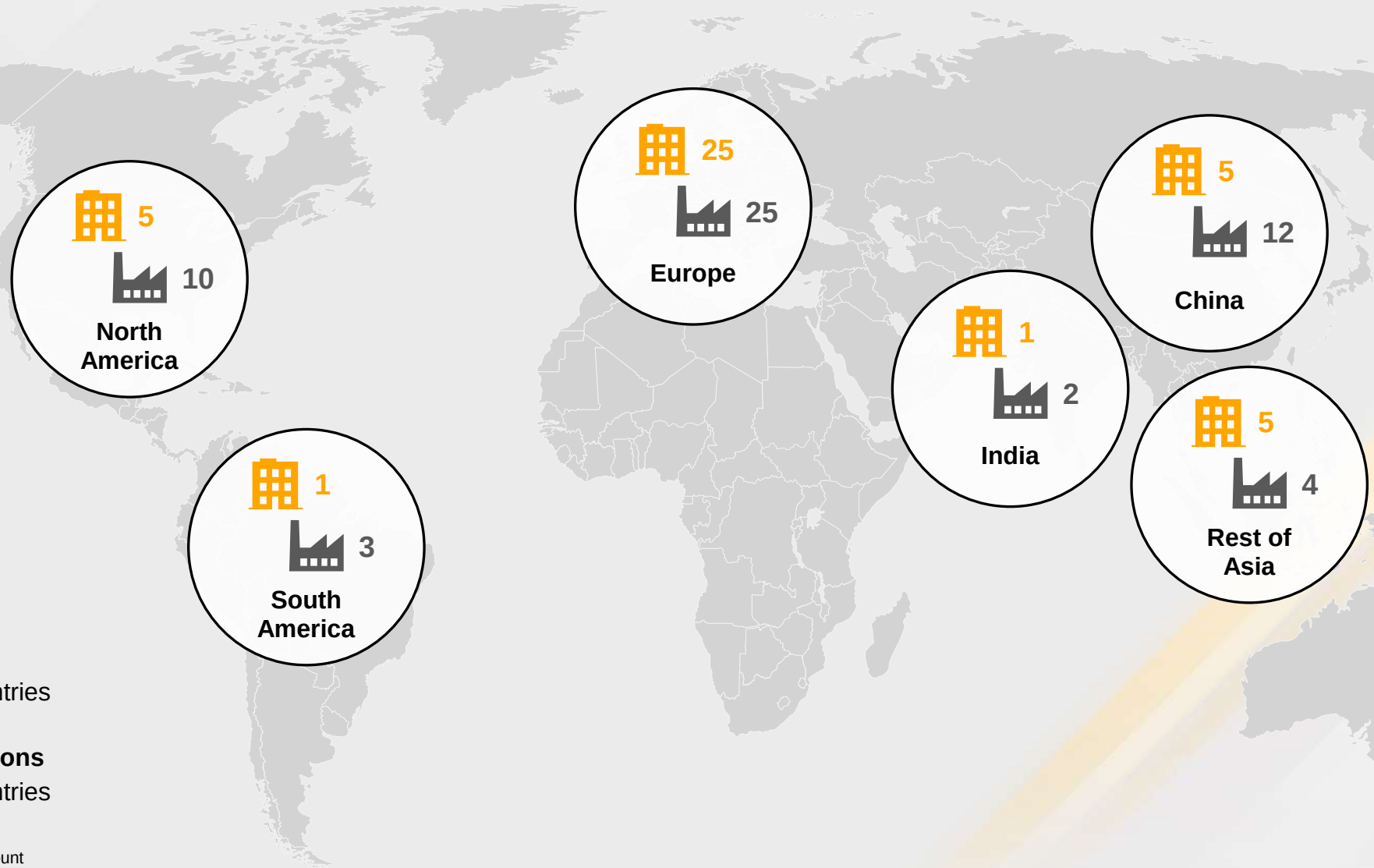
Architecture and Networking Systems

Autonomous Mobility

Safety and Motion

Technology Organization

Our R&D and Production Locations



R&D* locations
42 sites in 16 countries

Production locations
56 sites in 21 countries

* Research and Development, > 50 head count
w/o Continental Engineering Services, Elektrobit und PlaxidityX
Locations offering both R&D and Production are counted separately in each category

As of November 2024

Continental Automotive Group Sector

Our Structure

Safety and Motion

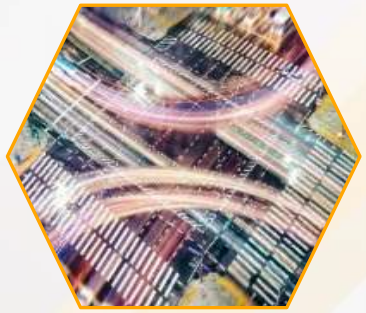
Architecture and Network Solutions

Autonomous Mobility

User Experience

Technology Organization

6 Megatrends
Shaping Our Future

MEGATRENDS	Demographic Shifts	Sustainability Transition	Empowered Society	Next-Gen Mobility	Exponential Innovation	Fracturing World
						
MACROTRENDS	› Population Growth › Urbanization › Aging Society › Global Migration	› Green Business Models › Sustainable Resources › Decarbonization › Circular Economy	› Individualization › Rising Consciousness › New Work › Digital Lifestyle › Rise of Education	› Mobility as a Service › Autonomous Mobility › Green Mobility › Software-defined Vehicle	› Computing Power & Connectivity › Artificial Intelligence › Automation & Robotics › Virtualization › Evolution of Science	› Geopolitical Hotspots › Populism & Neo-Nationalism › Economic Power Shift › Regulatory Complexity

Next-Gen Mobility

Motivation and Challenges

- Digitalization
- Differentiation
- Sustainability
- Lifestyle
- Reliable & Save

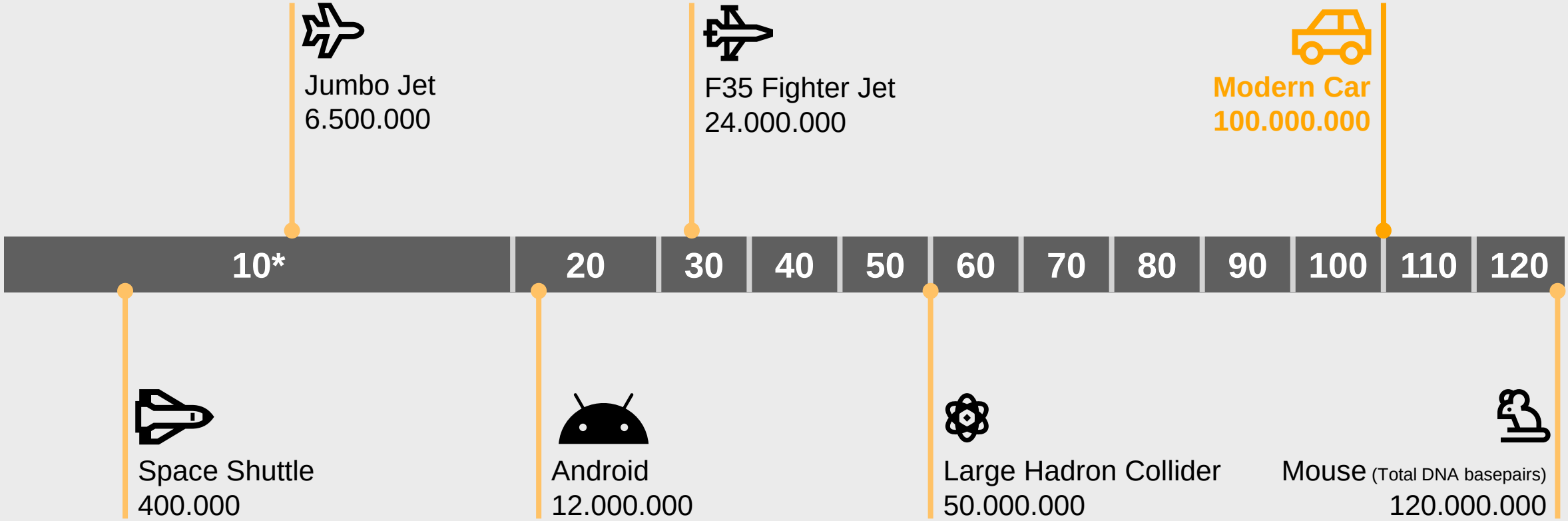
The vehicle is no longer a closed system but a part of a much bigger ecosystem – the Internet of Things

- Short time to market
- Increasing Complexity
- Lifetime Updates
- Software-defined (Hardware independent)
- Artificial Intelligence

Software-defined Vehicle (SDV)

Codebases of High Complexity

Software is of Increasing Complexity



| ***:** in million lines of code | **Source:** Million Lines of Code — Information is Beautiful |

Importance of Cybersecurity in the Automotive Industry

Safety of Drivers and Passengers

Modern vehicles are equipped with numerous electronic control units (ECUs) that manage critical functions such as braking, steering, and acceleration. A cyber attack could compromise these systems, leading to potentially dangerous situations.

Protection of Personal Data

Vehicles today collect and store a significant amount of personal data, including location, driving habits, and even biometric information. Ensuring this data is secure is essential to protect the privacy of vehicle owners.

Preventing Unauthorized Access

Hackers gaining access to a vehicle's systems can manipulate its functions, such as unlocking doors or starting the engine, leading to theft or unauthorized use.

Compliance with Regulations

Various global regulations, such as UNECE WP.29 and ISO/SAE 21434, mandate stringent cybersecurity measures for automotive manufacturers. Compliance with these regulations is necessary to avoid legal repercussions and ensure market access.

Maintaining Consumer Trust

As vehicles become more connected and autonomous, consumers need to trust that their vehicles are secure from cyber threats. A breach can significantly damage a brand's reputation and consumer confidence.

Economic Impact

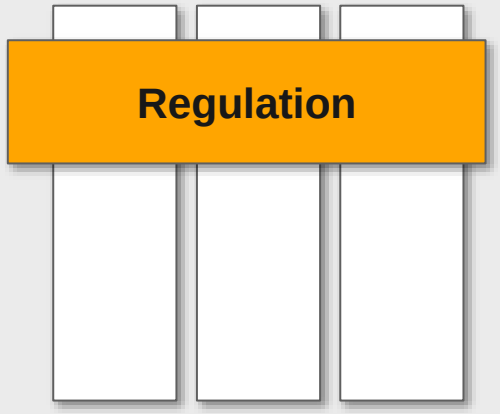
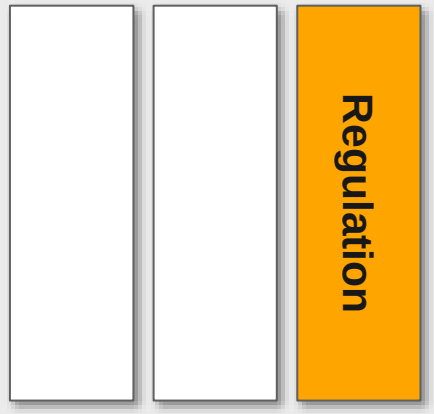
Cyber attacks can lead to significant financial losses due to recalls, legal liabilities, and damage to brand reputation. Investing in robust cybersecurity measures helps mitigate these risks.

Conclusion

By addressing these aspects, the automotive industry can ensure the safety, privacy, and trust of its consumers while complying with regulatory requirements and protecting its economic interests.

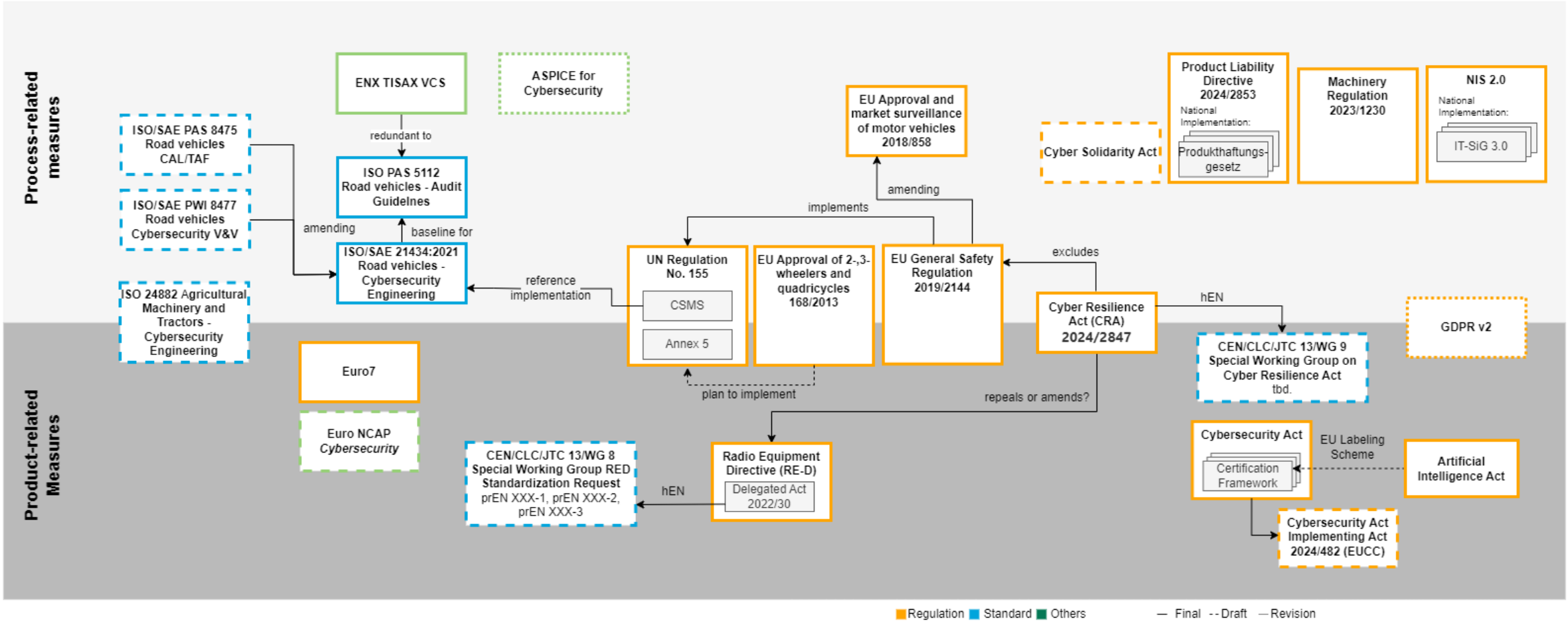
Horizontal and Industry-specific Regulations

Ensure to meet all necessary Compliance Requirements

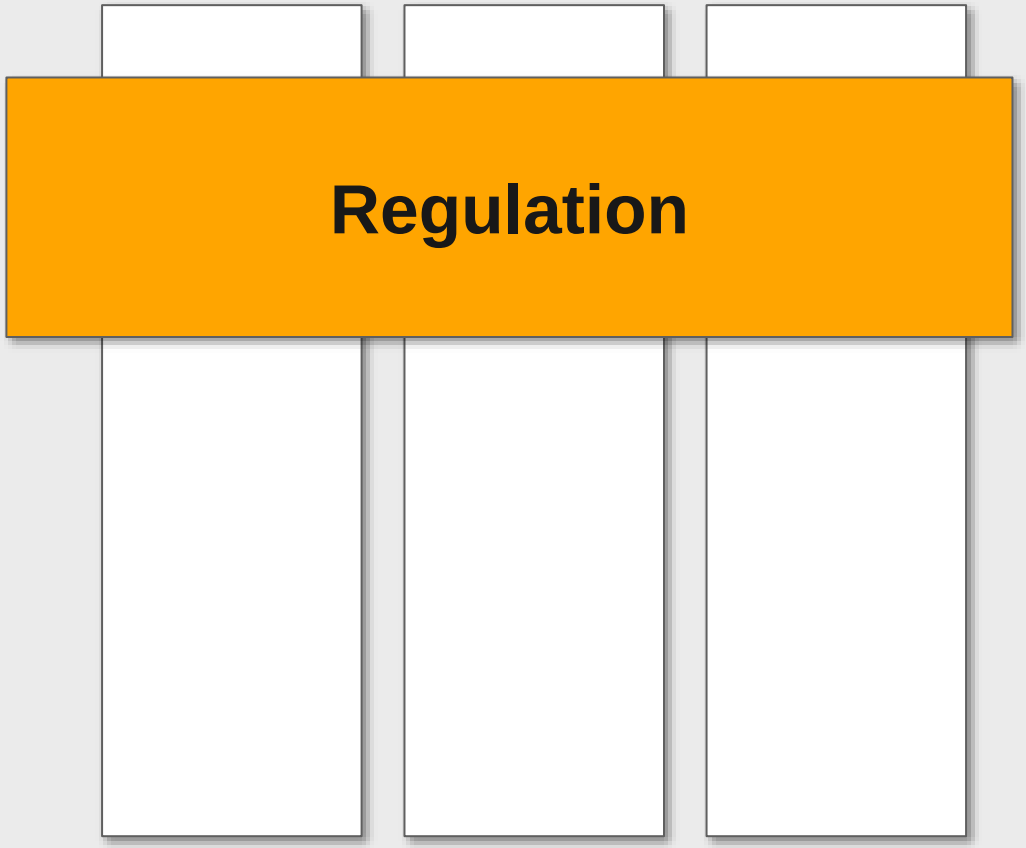
	Horizontal Regulations	Vertical Regulations
Scope	Broad scope and apply to multiple industry	Narrow and tailored to particular sectors
Focus	Address common issues like data protection and workplace safety	Focus on unique risks and requirements of specific industries
Implementation	Compliance is required across all sectors	Require specialized knowledge and practices relevant to the particular industry
		

Regulations and Standards Impacting European Market

Requirements are Process- and Product-related



Horizontal Regulations



General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679

Overview

- **Purpose:** Protects personal data of EU citizens and regulates data processing activities.
- **Scope:** Applies to all organizations handling EU citizens' data, regardless of location.

Key Requirements

- **Consent:** Explicit consent required for data collection and processing.
- **Data Subject Rights:** Includes right to access, rectify, and erase personal data.
- **Data Protection Officer (DPO):** Mandatory for certain organizations to oversee compliance.
- **Penalties:** Fines up to €20 million or 4% of global turnover for non-compliance.

Impact on Automotive Industry

- **Data Collection:** Vehicles collect extensive personal data (e.g., location, driving habits).
- **Compliance:** Automotive companies must ensure data protection measures are in place.
- **Consumer Trust:** Enhances trust by safeguarding personal data and ensuring transparency.
- **Operational Changes:** Requires updates to data management systems and processes.

EU Cybersecurity Act (CSA)
Regulation (EU) 2019/881

Overview

- **Purpose:** Establishes a framework for cybersecurity certification of ICT products, services, and processes across the EU.
- **Scope:** Applies to manufacturers, developers, and distributors of digital products and services.

Key Requirements

- **Certification Schemes:** Development of EU-wide certification schemes to ensure consistent cybersecurity standards.
- **Security by Design:** Integration of cybersecurity measures throughout the product lifecycle.
- **Market Surveillance:** Enhanced monitoring and enforcement of compliance.

Impact on Automotive Industry

- **Increased Certification:** Ensures vehicles and components meet high cybersecurity standards.

EU Network Information Security Directive (NIS 2)

Regulation (EU) 2022/2555

Overview

- **Purpose:** Enhance cybersecurity resilience across the EU.
- **Scope:** Applies to essential and important entities, including the automotive sector.

Key Requirements

- **Risk Management:** Implement measures to manage cybersecurity risks.
- **Incident Reporting:** Mandatory reporting of significant incidents within 24 hours.
- **Supply Chain Security:** Ensure cybersecurity throughout the supply chain.
- **Penalties:** Fines for non-compliance, up to €10 million or 2% of global turnover.

Impact on Automotive Industry

- **Enhanced Cyber Resilience:** Strengthens defenses against cyber threats.
- **Compliance Obligations:** Requires automotive companies to adopt robust cybersecurity practices.
- **Supply Chain Security:** Ensures end-to-end security in the automotive supply chain.
- **Operational Changes:** Necessitates updates to cybersecurity policies and incident response plans.

EU Cyber Resilience Act (CRA)

Regulation (EU) 2024/2847

Overview

- **Purpose:** Enhance cybersecurity for products with digital elements across the EU.
- **Scope:** Applies to manufacturers, developers, and distributors of digital products.

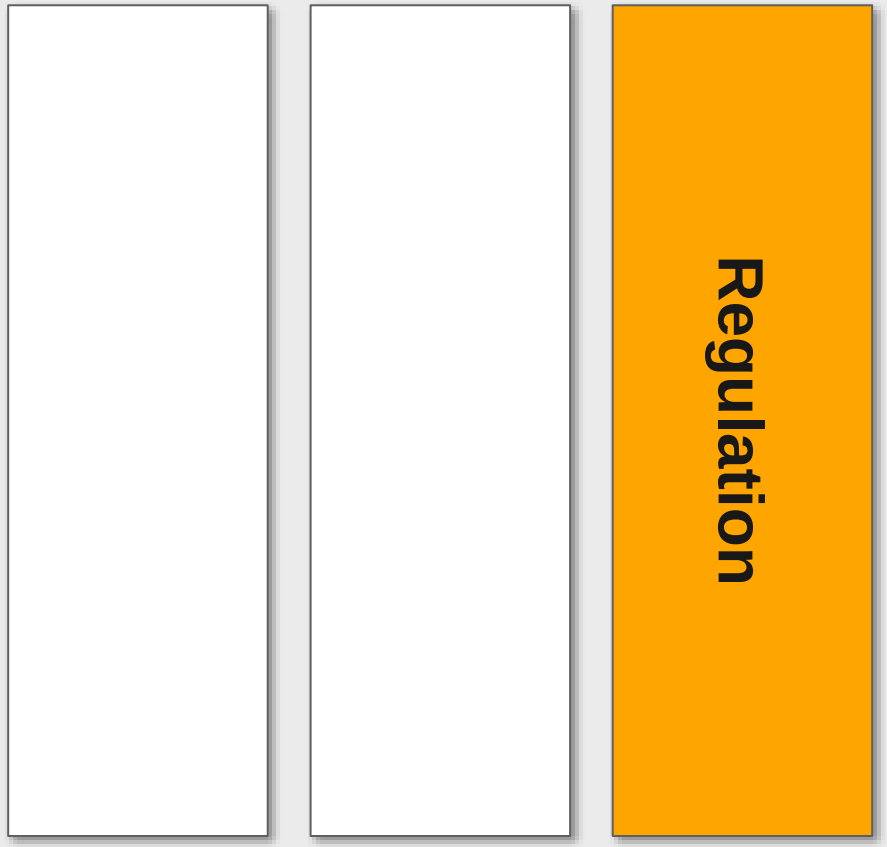
Key Requirements

- **Security by Design:** Cybersecurity must be integrated into the design, production, and lifecycle management of products.
- **Compliance Demonstration:** Products must meet stringent cybersecurity standards.
- **Penalties:** Fines up to €15 million for non-compliance.

Impact on Automotive Industry

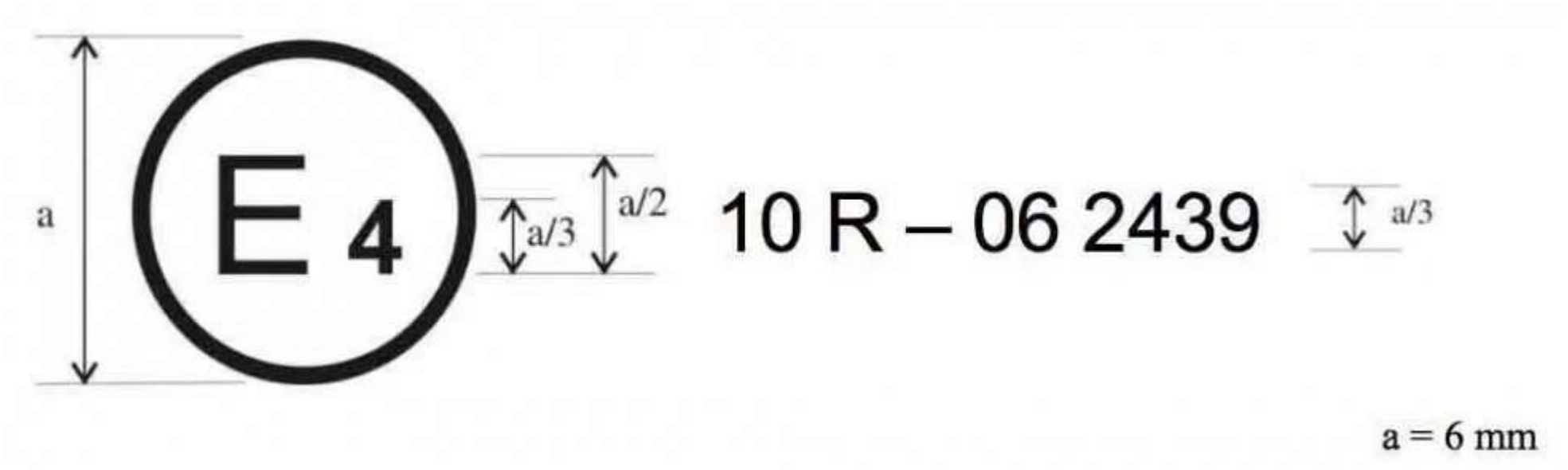
- **Enhanced Product Security:** Ensures vehicles and components meet high cybersecurity standards.
- **Supply Chain Security:** Mandates cybersecurity measures throughout the automotive supply chain.
- **Operational Changes:** Requires updates to design, production, and maintenance processes to comply with the Act.

Industry-specific Regulations and Standards



UNECE Vehicle Type Approval

Have you seen this sign?



Introduction to UNECE

United Nations Economical Commission of Europe

Structure

ITC
Inland Transport Committee

WP.29
World Forum for Harmonization of Vehicle Regulations

GRSP | GRSG | GRPE | GRBP | GRVA | GRE

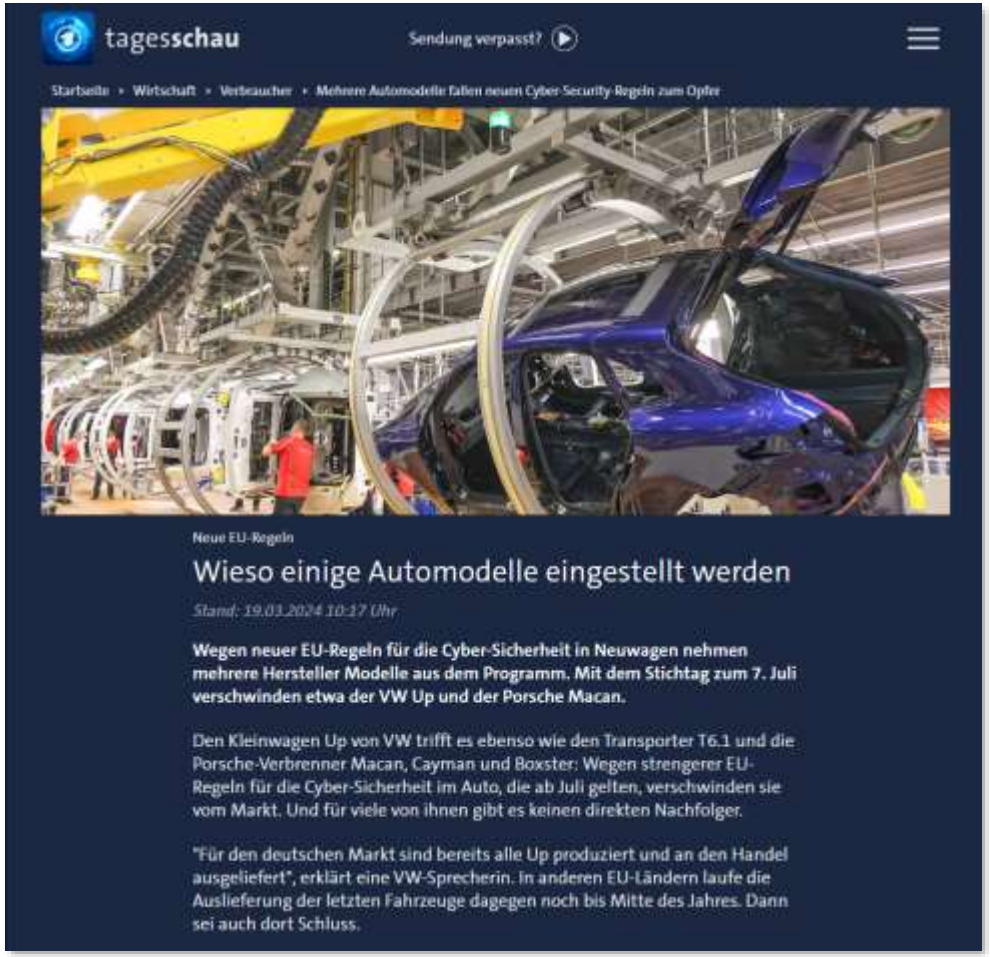
Legal Framework

UN Regulations – 1958 Agreement
Provisions related to safety and environmental aspects for vehicles, their systems, parts and equipement.

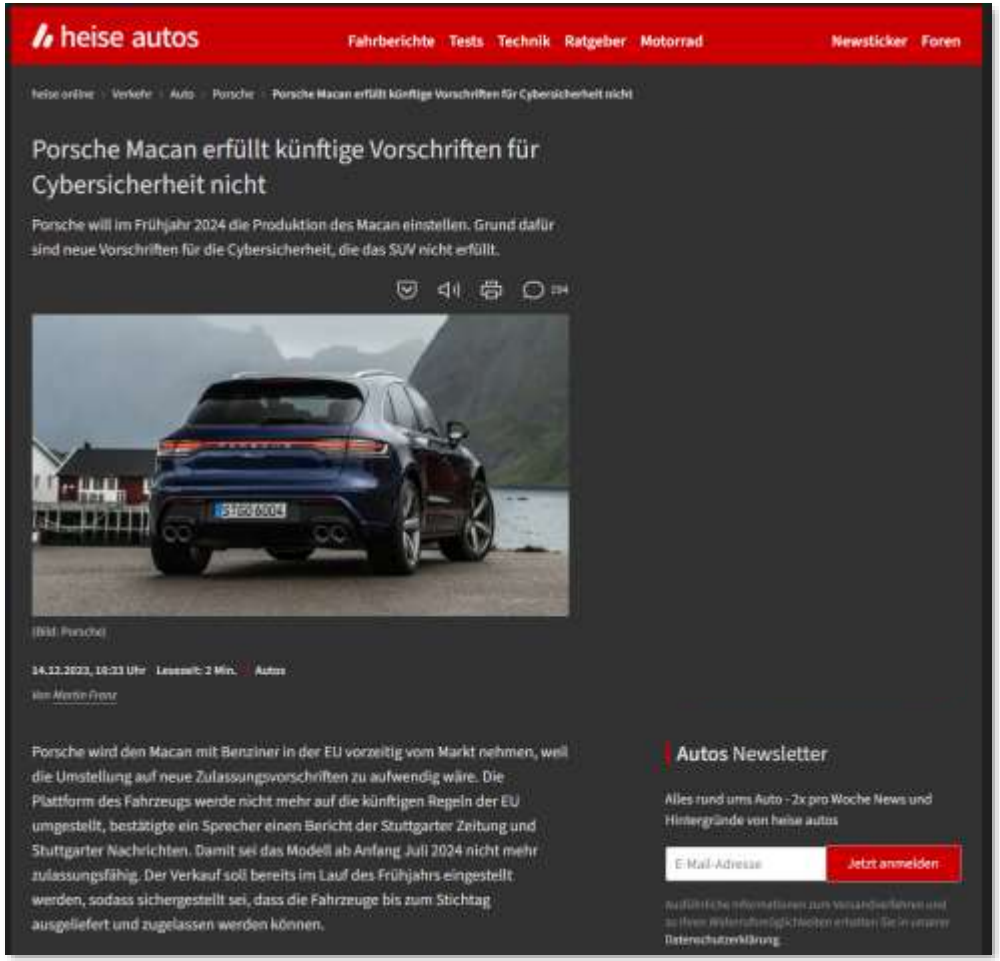
UN GTRs – 1998 Agreement
Globally harmonized performance-related requirements and test procedures for predictable regulatory framework

UN Rules – 1997 Agreement
Periodical technical inspections of vehicles in use

Setup of Working Groups



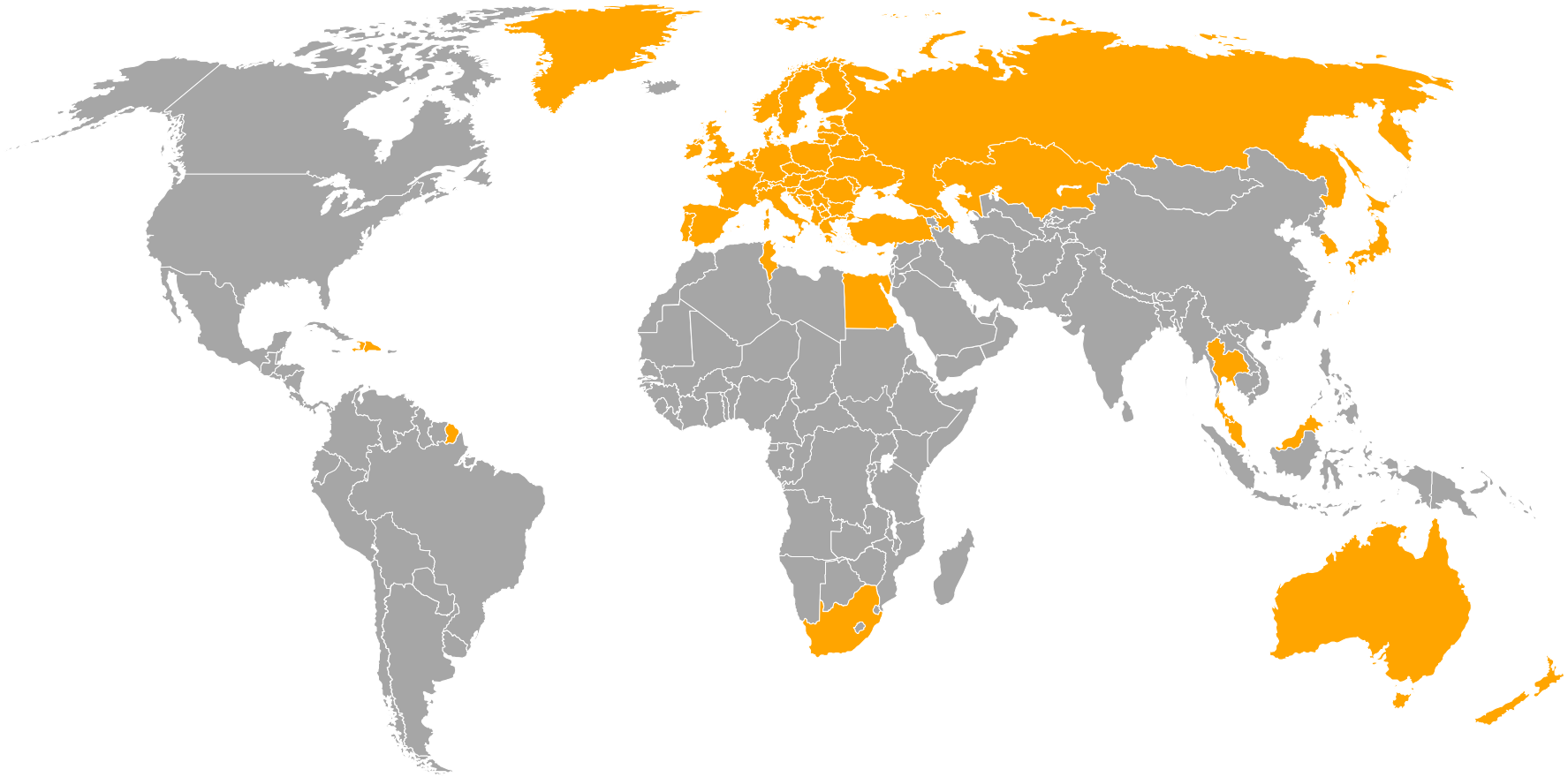
Source



Source

UN Regulation on Type Approval for Cybersecurity

Potential Affected Markets of UNECE 1958 Agreement



UN Regulation on Type Approval

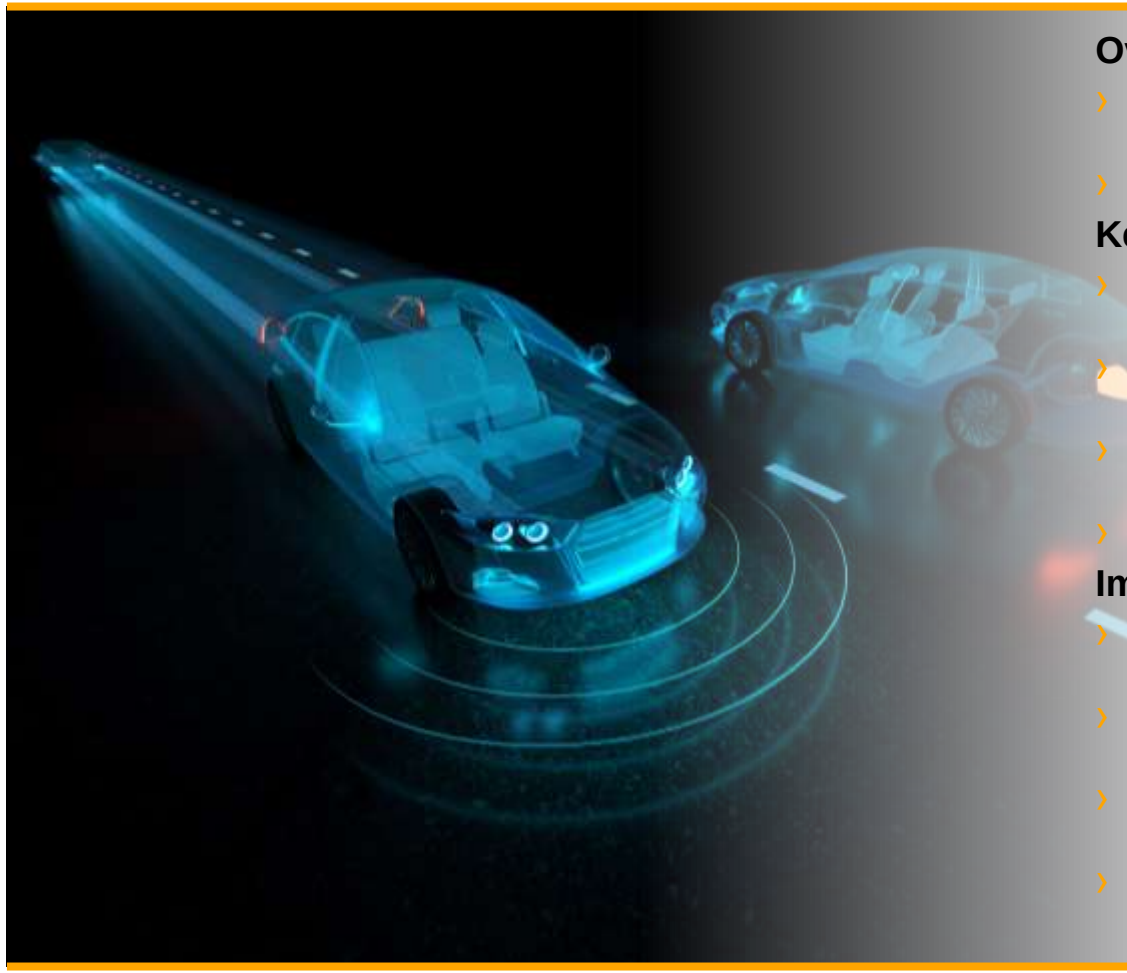
Affected Vehicle Categories

			CS	SU
	**M_1**	Passenger vehicles	X	X
	**$M_{2,3}$**	Busses	X	X
	**$N_{1,2,3}$**	Light and heavy duty trucks	X	X
	**$L_{6,7}$**	Light and heavy quadricycles If equipped with automated describing functionalities from level 3 onwards as defined in ECE/TRANS/WP.29/1140	X	
	**O**	Trailers If fitted with at least one electronic control unit	X	X
	**R**	Agricultural Trailers		X
	**S**	Interchangeable towed equipment		X
	**T**	Agricultural and Forestry tractory		X

Based on: TRANS/WP.29/1045

UNECE Regulation No. 155

Vehicle Type Approval with regards to Cybersecurity



Overview

- **Purpose:** Establishes cybersecurity requirements for vehicles to protect against cyber threats.
- **Scope:** Applies to all new vehicle types and models in UNECE member countries.

Key Requirements

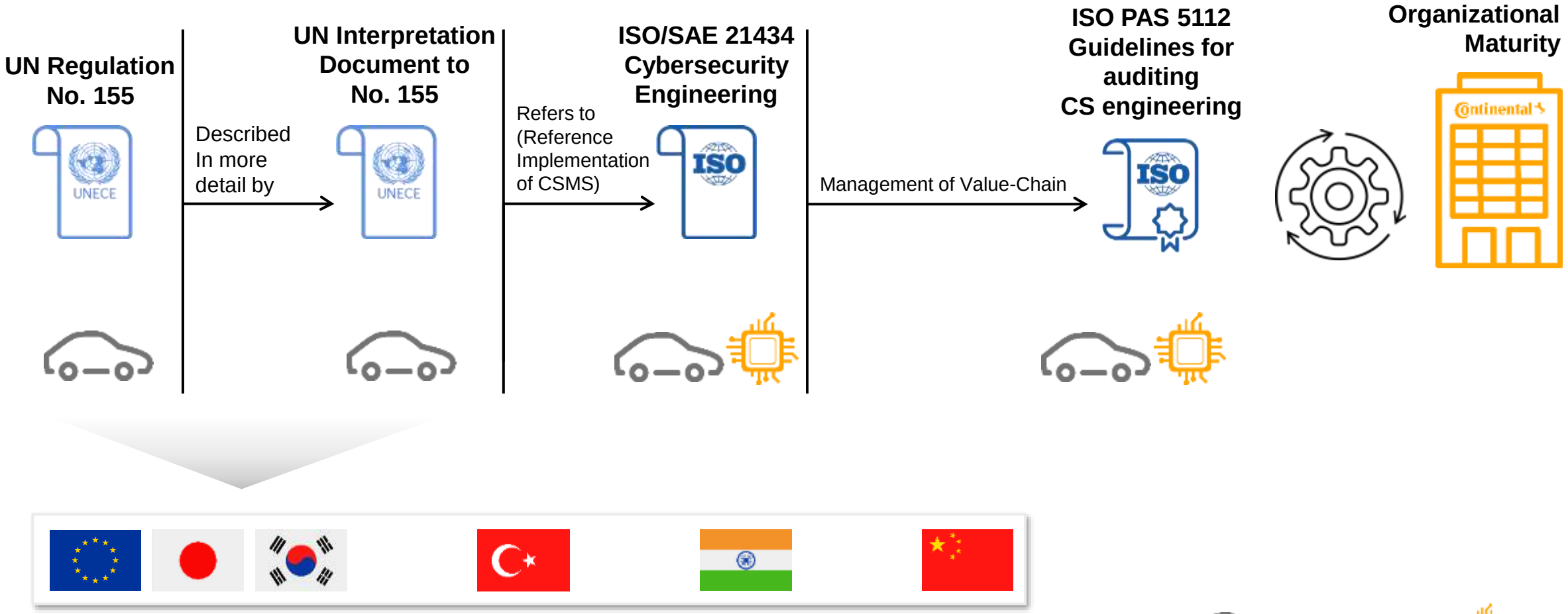
- **Cybersecurity Management System (CSMS):** Manufacturers must implement a CSMS to manage cybersecurity risks throughout the vehicle lifecycle.
- **Risk Assessment:** Continuous identification, assessment, and mitigation of cybersecurity risks.
- **Incident Response:** Procedures for detecting, reporting, and responding to cybersecurity incidents.
- **Certification:** Vehicles must be certified for compliance with the regulation.

Impact on Automotive Industry

- **Enhanced Vehicle Security:** Ensures vehicles are protected against cyber threats, enhancing overall safety.
- **Compliance Obligations:** Requires manufacturers to adopt comprehensive cybersecurity practices and obtain certification.
- **Operational Changes:** Necessitates updates to design, production, and maintenance processes to integrate cybersecurity measures.
- **Consumer Trust:** Builds consumer confidence in the security of automotive products, improving brand reputation.

Process-Related Requirements for Automotive

Solid Baseline for different Obligations



ISO/SAE 21434 Road vehicles–Cybersecurity Engineering

Involved Organizations

OEM

Tier-1

Sub-Supplier

Cert. Body

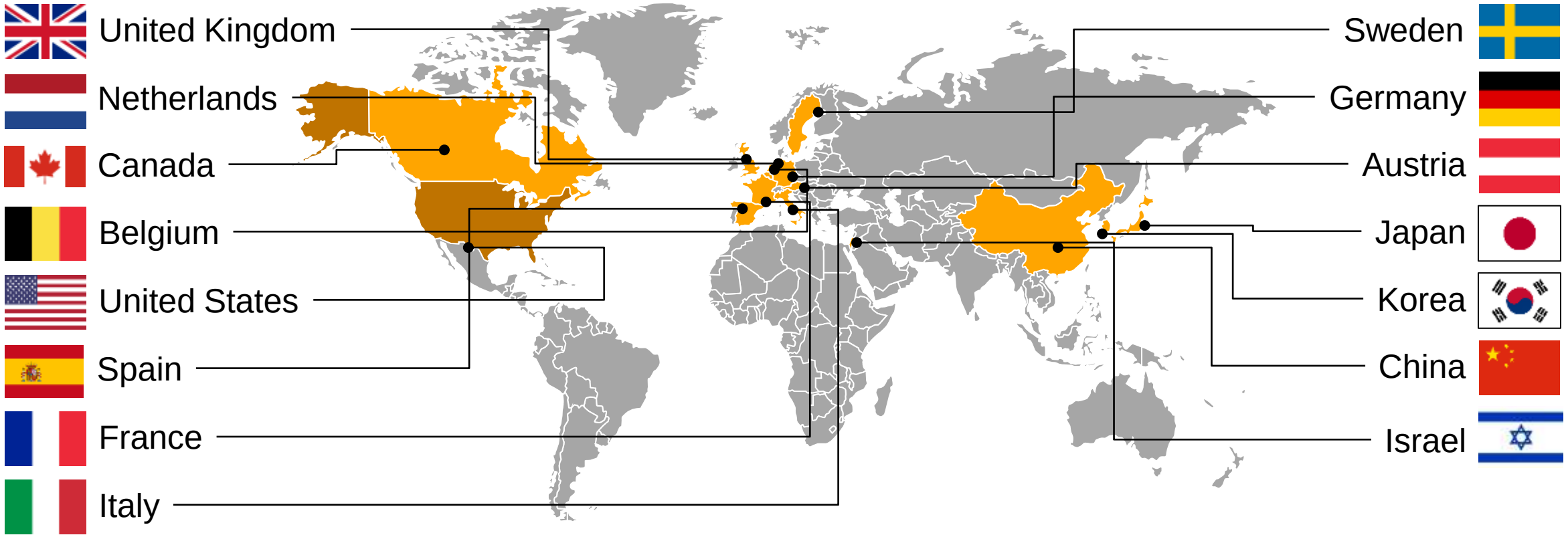
Regul. Body

Consulting

Accademia

ISO/SAE 21434 Road vehicles–Cybersecurity Engineering

National Delegations



ISO/SAE 21434 Road Vehicles-Cybersecurity Engineering

Baseline for the Supply-Chain

Regulation

Overview

- **Purpose:** Provides a comprehensive framework for managing cybersecurity risks in the automotive industry.
- **Scope:** Applies to all stages of the vehicle lifecycle, from design and development to decommissioning.

Key Requirements

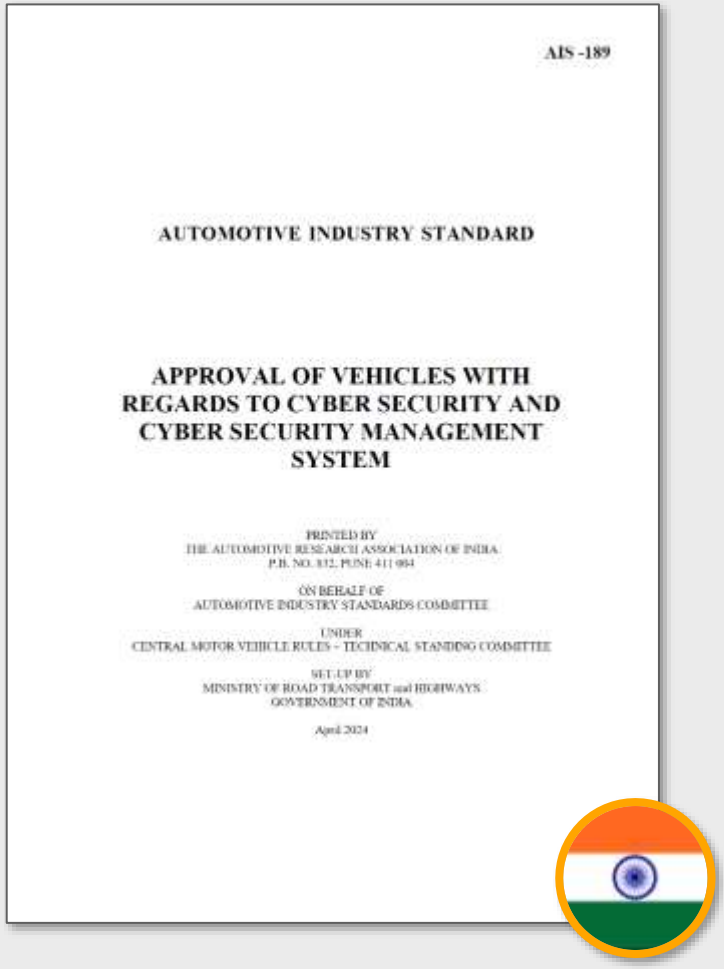
- **Cybersecurity Management:** Establishes a dedicated cybersecurity management plan within organizations.
- **Risk Assessment:** Identifies and evaluates potential cybersecurity risks specific to vehicles and their components.
- **Security by Design:** Integrates cybersecurity measures from the early stages of vehicle development.
- **Incident Response:** Implements protocols for effectively responding to cybersecurity incidents.

Impact on Automotive Industry

- **Supply Chain:** Baseline for certification in the supply-chain to increase trust.
- **Compliance Obligations:** Supports manufacturers to demonstrate cybersecurity practices along the supply chain.

International Regulations

UN Regulation and Standard is accepted on global Level



Implementation of a Robost CSMS at a Supplier

Actions to take to ensure Compliance and Conformity

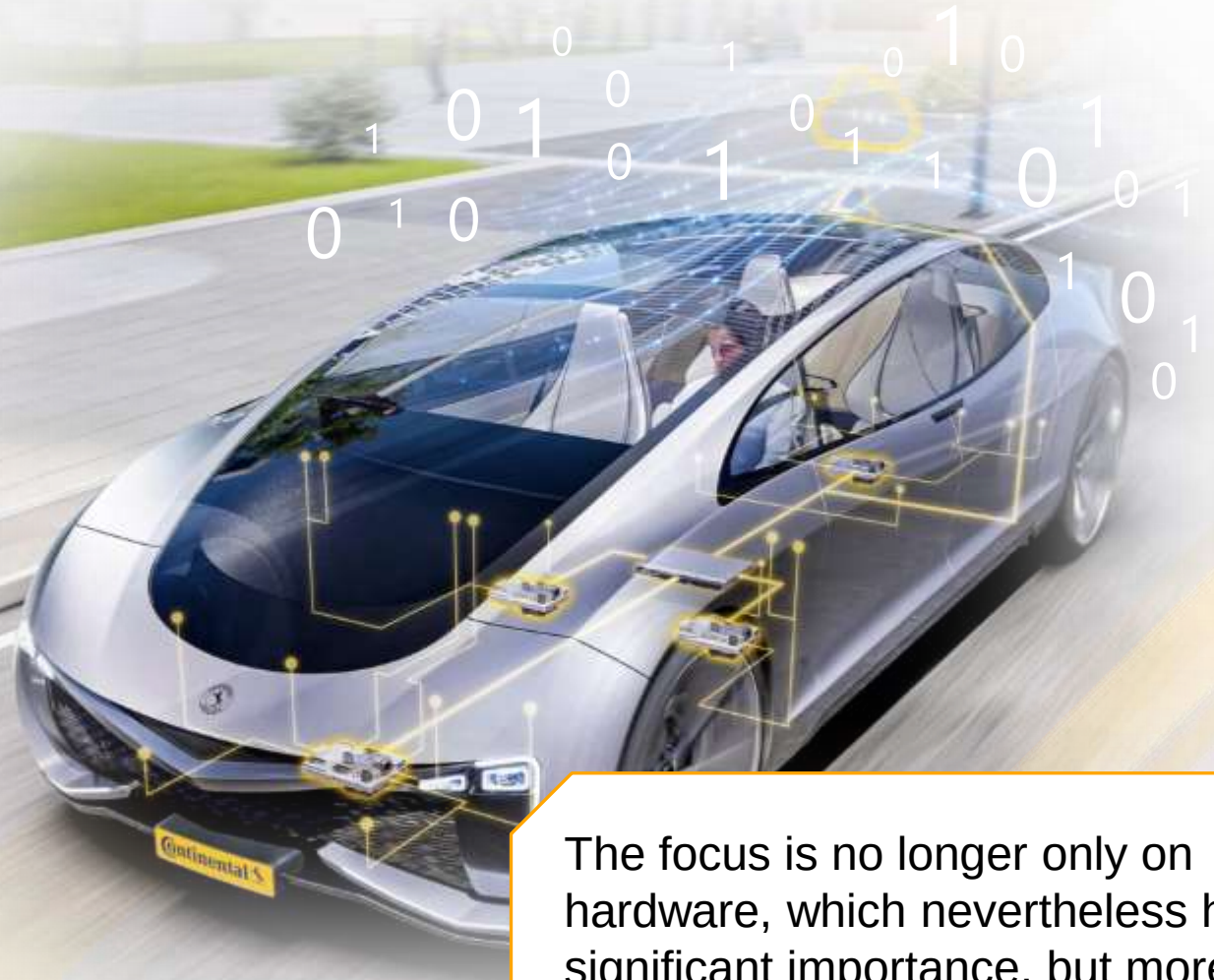
The Future of Mobility

Software-defined Vehicle

In a Software-defined Vehicle, functions are enabled by software.

Decoupling software from hardware enables swift and continuous development & implementation of new functions and software updates throughout vehicle lifetime.

This results in new requirements regarding – products, collaboration, development, system integration and ecosystem.



The focus is no longer only on hardware, which nevertheless has a significant importance, but more and more on all relevant building blocks of the Software-defined Vehicle.

Continental Automotive

Software-defined Vehicle – What Does That Really Mean?

Characteristics of a Software-defined Vehicle:

Decoupling software from hardware development

Software and hardware evolve independently from each other. Updating software doesn't necessarily mean upgrading hardware – the hardware can remain the same throughout the entire product life cycle.

Deliver new or additional software features

Software-defined Vehicles are providing new functions and services to existing devices as well as easing maintenance.

Software can be reused across devices and vehicles.

Capture value with software solutions

When software updates provide new value cross-domain independent of hardware sales, Software-defined Vehicles can enable the monetization of the software value.

Hardware and system knowledge as well as our software know-how are key success factors for our customers.

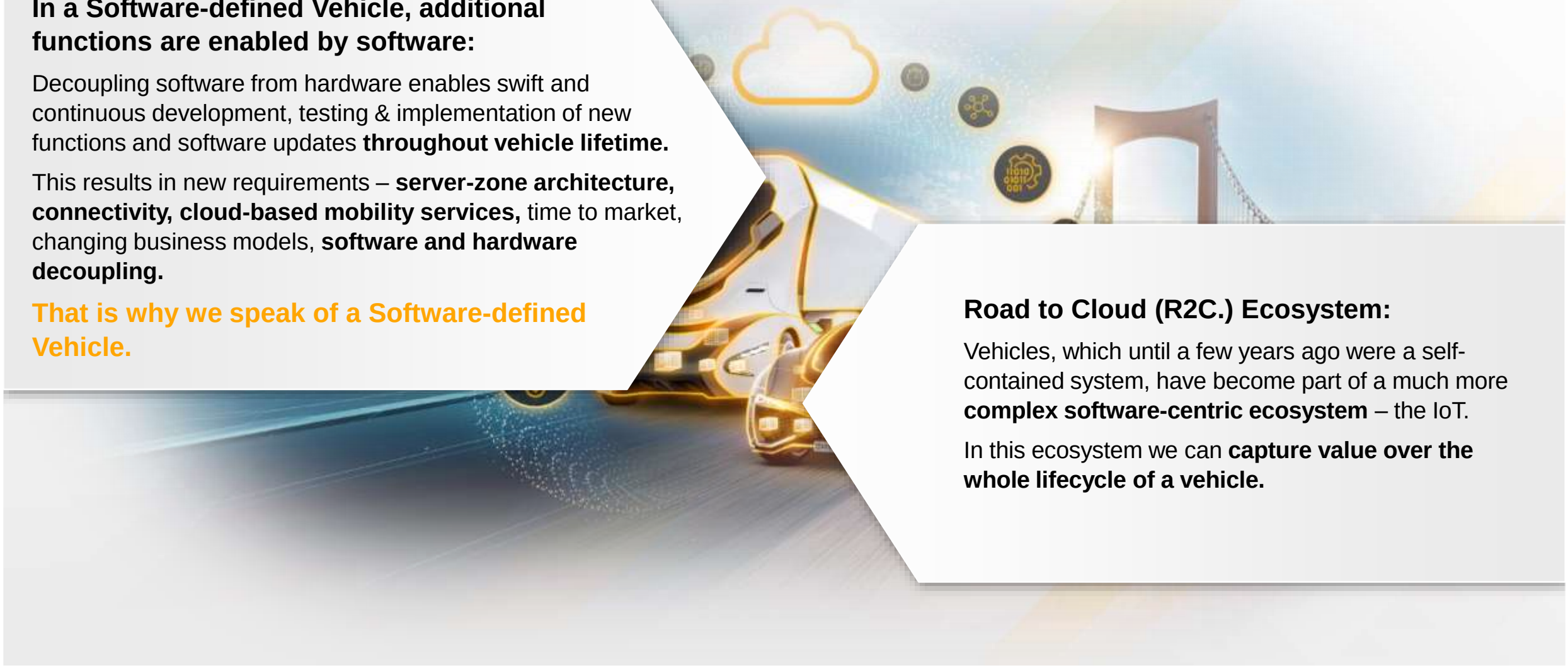
Software-defined Vehicle and Road to Cloud Ecosystem

In a Software-defined Vehicle, additional functions are enabled by software:

Decoupling software from hardware enables swift and continuous development, testing & implementation of new functions and software updates **throughout vehicle lifetime.**

This results in new requirements – **server-zone architecture, connectivity, cloud-based mobility services,** time to market, changing business models, **software and hardware decoupling.**

That is why we speak of a Software-defined Vehicle.



Road to Cloud (R2C.) Ecosystem:

Vehicles, which until a few years ago were a self-contained system, have become part of a much more **complex software-centric ecosystem** – the IoT.

In this ecosystem we can **capture value over the whole lifecycle of a vehicle.**

Road to Cloud Ecosystem

Solutions for the Software-defined Vehicle

R2C. Services
. Engineering
. Manufacturing

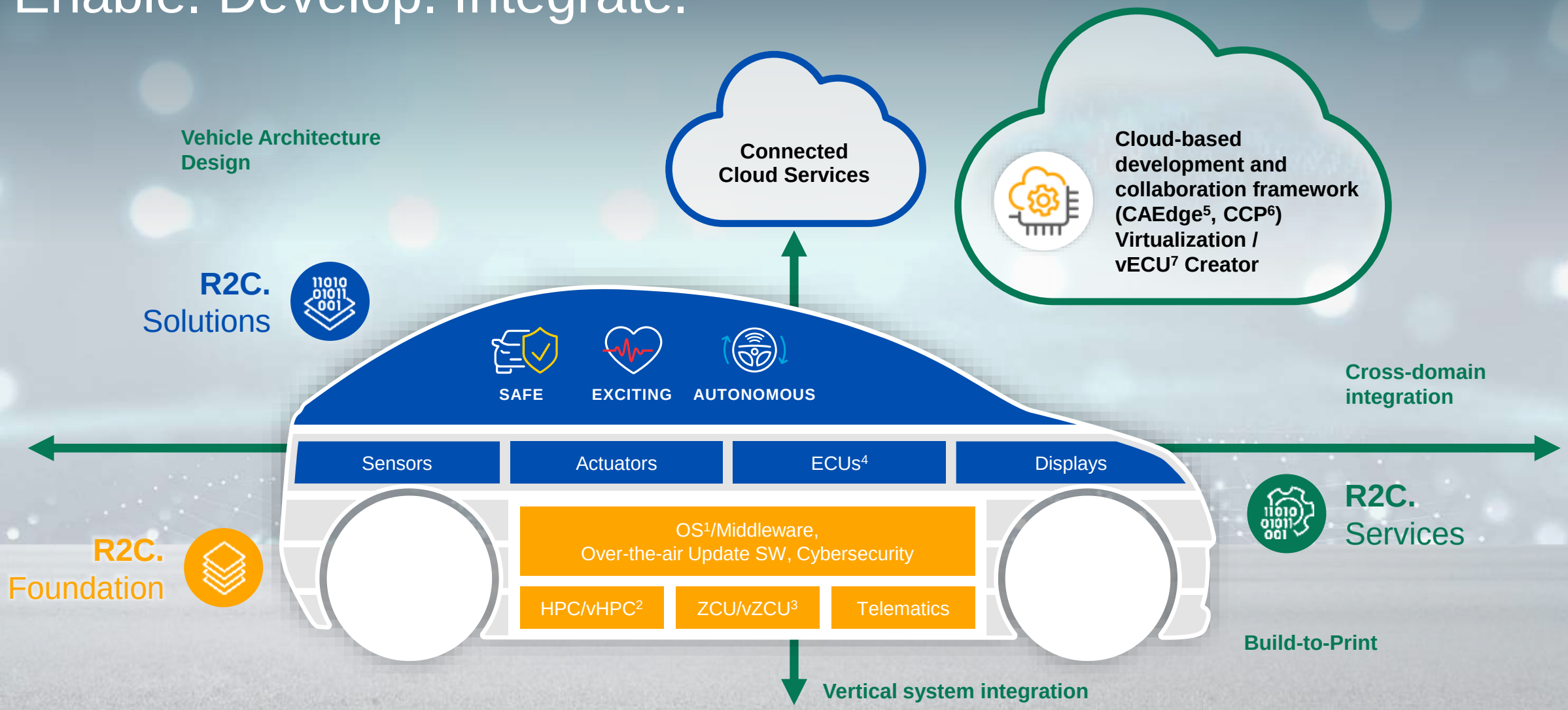
R2C. Solutions
. Software
. Hardware

R2C. Foundation
. Software
. Hardware
. Tooling

[1] ZCU: Zone Control Unit, [2] HPC: High-Performance Computer, [3] OS: Operating System, [4] CAEdge: Continental Automotive Edge Framework, [5] vECU: virtual Electronic Control Unit, [6] ECU: virtual Electronic Control Unit, [7] SW: Software, [8] B2P: Build-to-Print

Road to Cloud (R2C.) Ecosystem

Enable. Develop. Integrate.



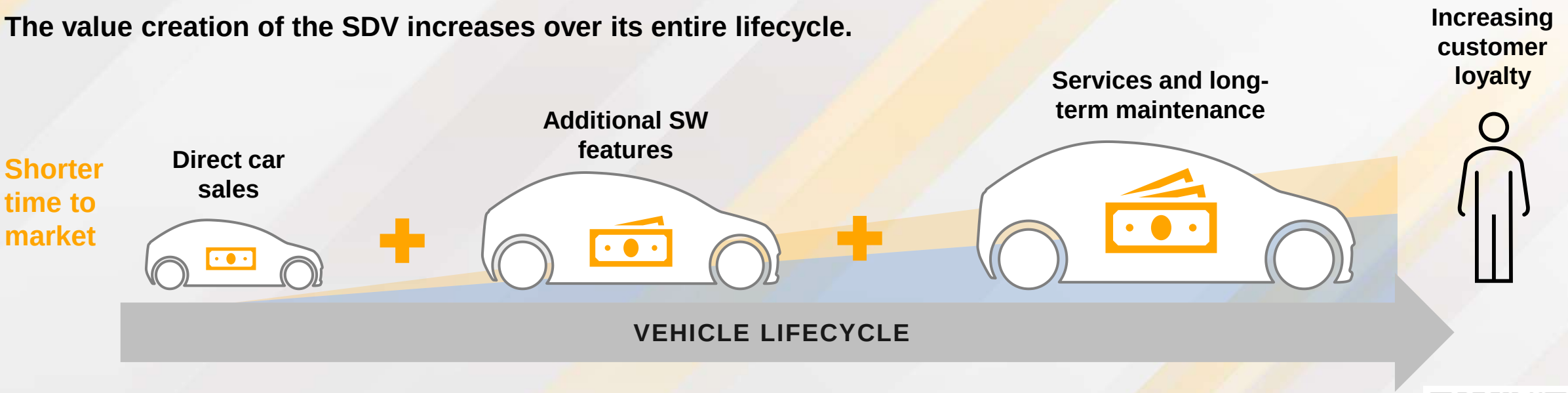
[1] OS: Operating System, [2] HPC: High-Performance Computer / vHPC: virtual High-Performance Computer,
[3] ZCU: Zone Control Unit / vZCU: virtual Zone Control Unit, [4] ECU: Electronic Control Unit, [5] CAEdge: Continental Automotive Edge Framework, [6] CCP: Continental Cooperation Portal, [7] vECU: virtual Electronic Control Unit

The Software-defined Vehicle

What Is the Value of a SDV for the OEM?

The Software-defined Vehicle (SDV) enables OEMs to create additional value by facilitating over-the-air updates, allowing continuous improvement and feature enhancements without requiring physical recalls.

The value creation of the SDV increases over its entire lifecycle.



Increasing direct and indirect revenue and customer loyalty

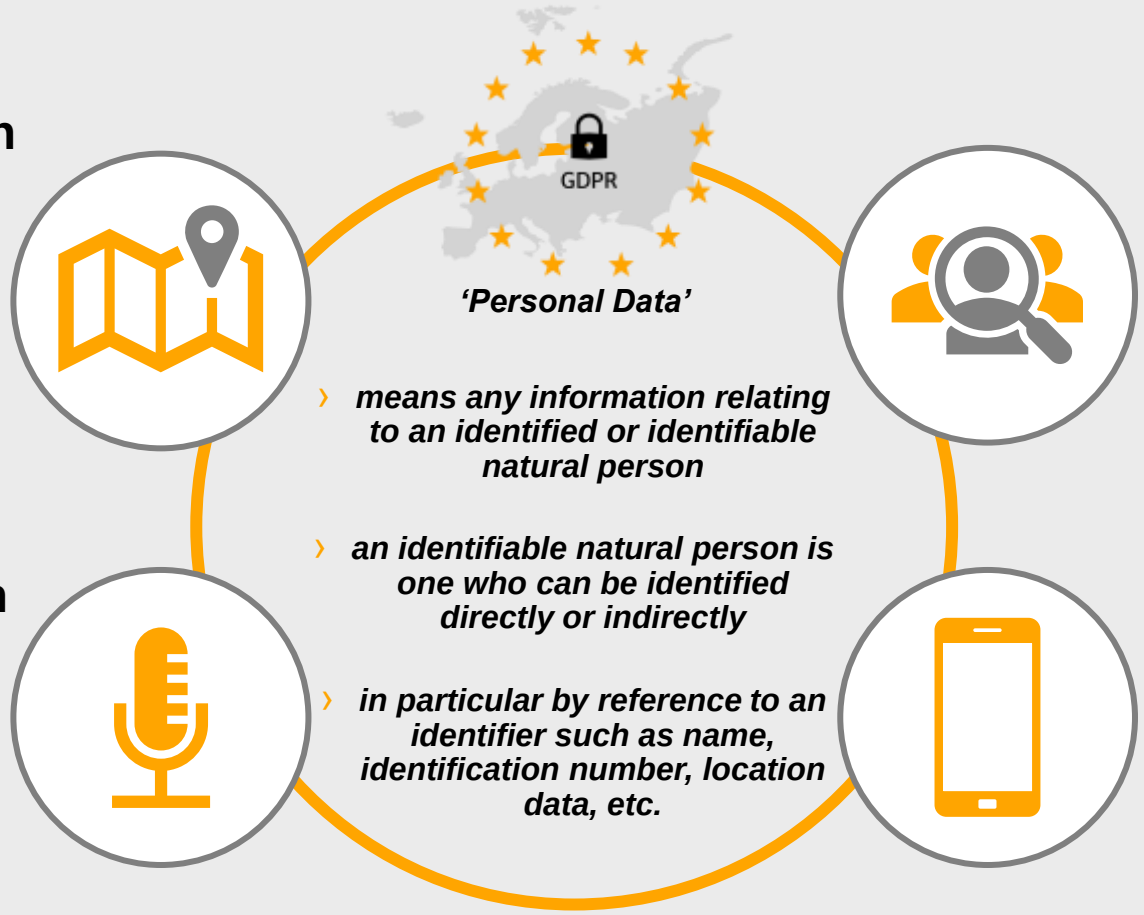
More information here or scan

Data Protection and Privacy

Examples for Data Collection in Smart Vehicles

- **Location Information**
  - Starting position
  - Destination
  - Route
  - Time
  - Speed

- **In-Cabin Information**
  - Microphone
  - Camera
  - Infotainment
  - Vehicle Occupants



- **User Recognition**
  - Physical/ Biometrics
  - Fingerprint
  - Face
  - Eye movement
  - Seat Configuration

- **Applications**
  - Contacts
  - Call logs & Messages
  - Payment
  - Subscriptions

| **Source:** PERSONAL DATA IN YOUR CAR, National Automobile Dealers Association and the Future of Privacy Forum |

Data Protection and Privacy

Increasing Global Relevance by Local Regulations

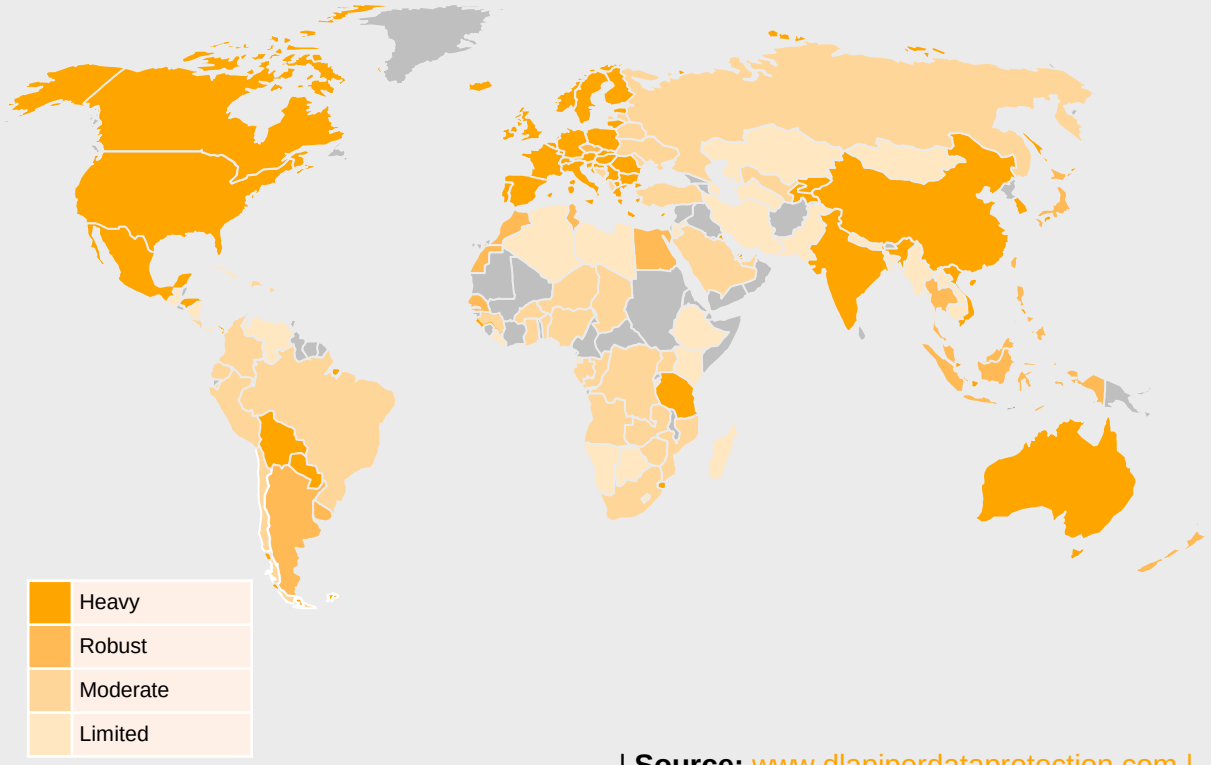
All Automotive Products and Mobility Services need to meet Data Protection Regulations

Data Protection laws worldwide are legally binding and **punishable with high sanctions** (Automotive GDPR violation with 1,2 Mio€ penalty)

Privacy Enhancing Technologies **are enablers** for future personalized Mobility Services and Automotive Products

Investing in privacy-friendly technologies can **increase business opportunities** and **build customer trust** relationships

Data Protection Laws Worldwide



| **Source:** www.dlapiperdataprotection.com |

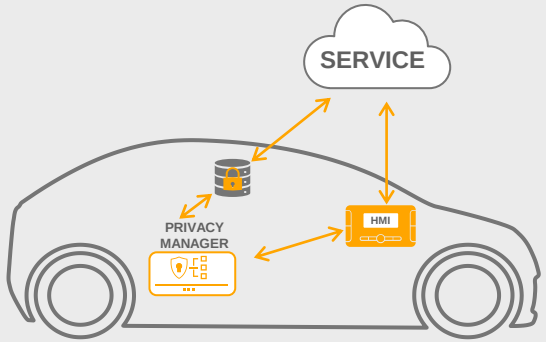
Innovation: Data Protection and Privacy

Automotive Privacy at Continental

METHODOLOGIES

Privacy Impact Analysis

GENERIC SOLUTIONS



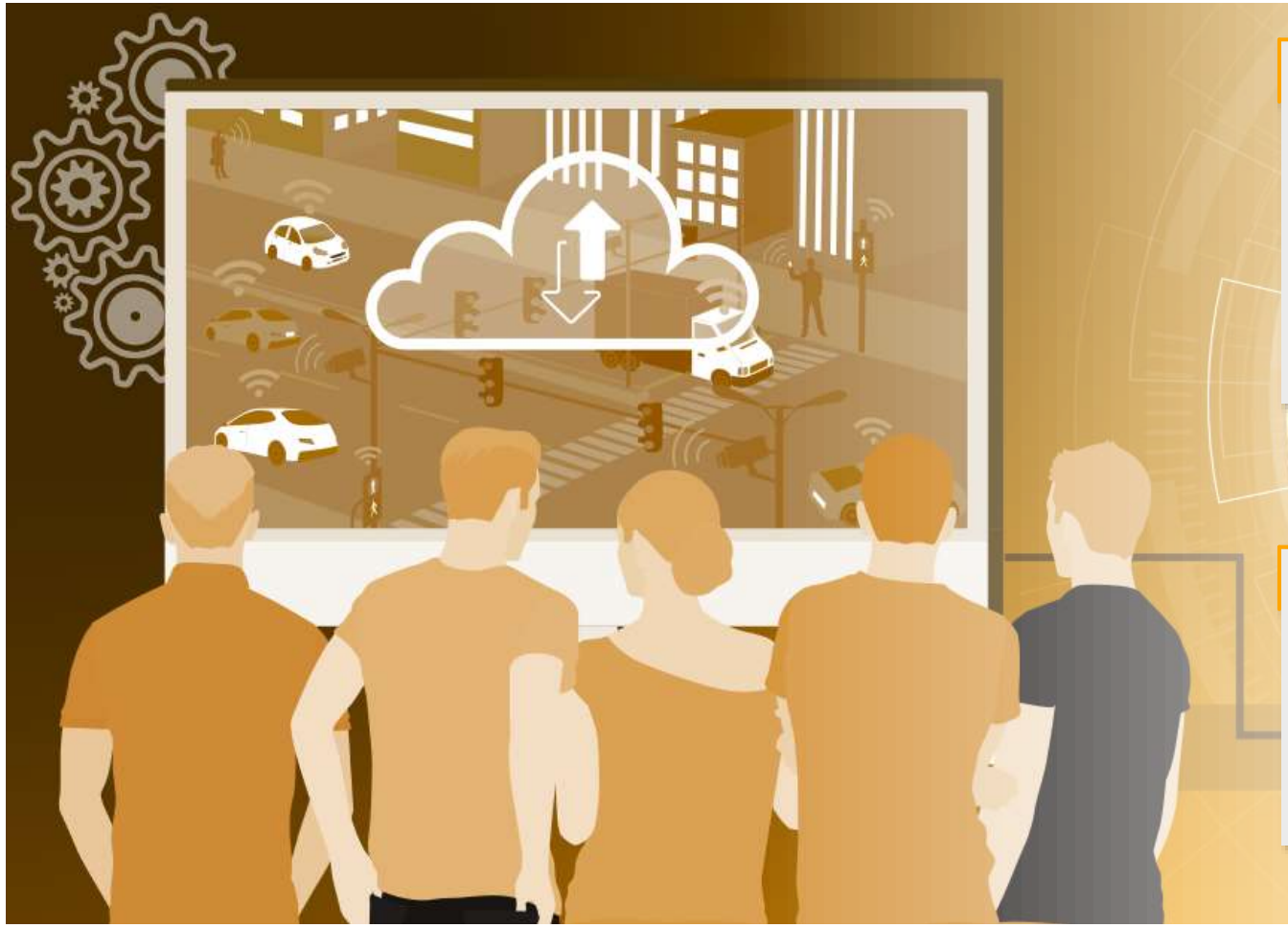
Privacy Oriented-System Model

SPECIFIC SOLUTIONS

Privacy HMI

AUTOPSY Research Project

Automotive Data-Tainting for Privacy Assurance System



Goals

- Create better understanding of Data flows in Automotive environments
- Create Privacy-Aware System Model for an Automotive Use-Case in specific technical design

Use Cases

- Silent Testing
- Platooning
- Pay as you Drive

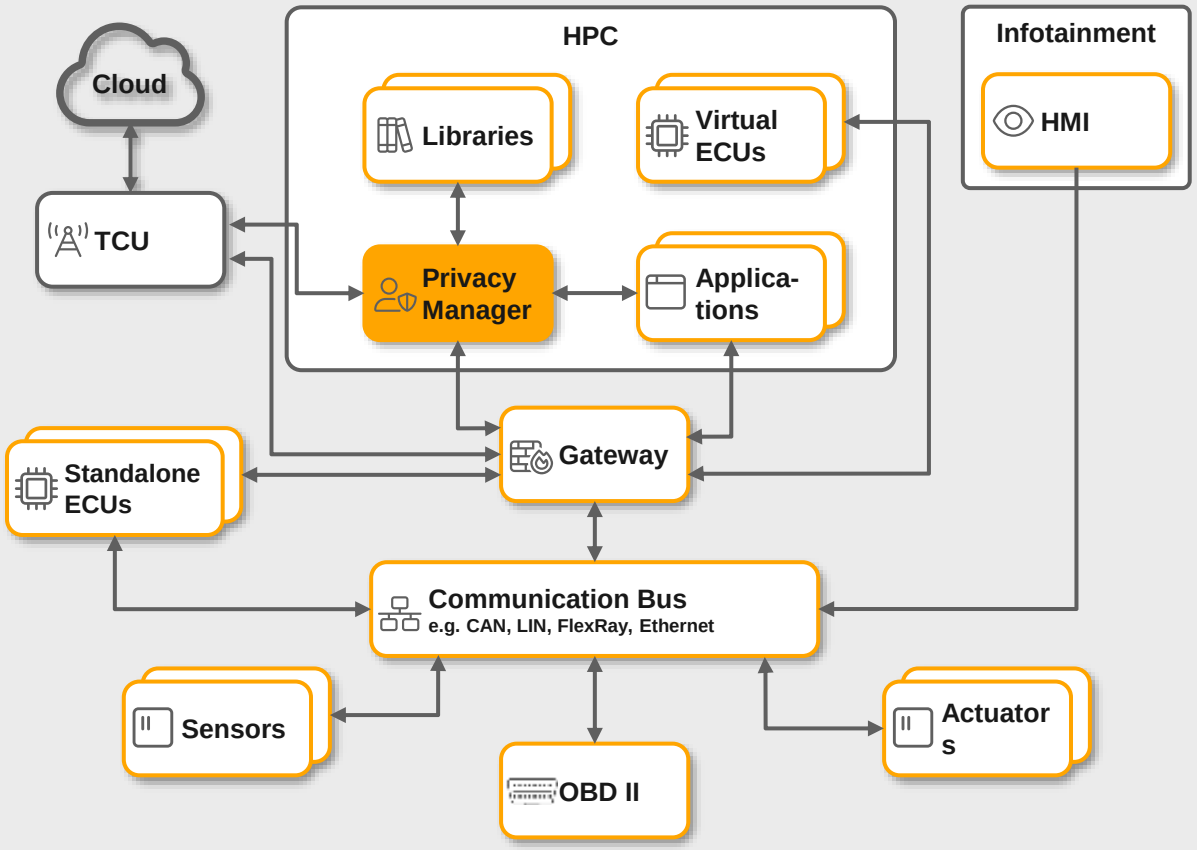
AUTOPSY Research Project

Application to Silent Testing Scenario

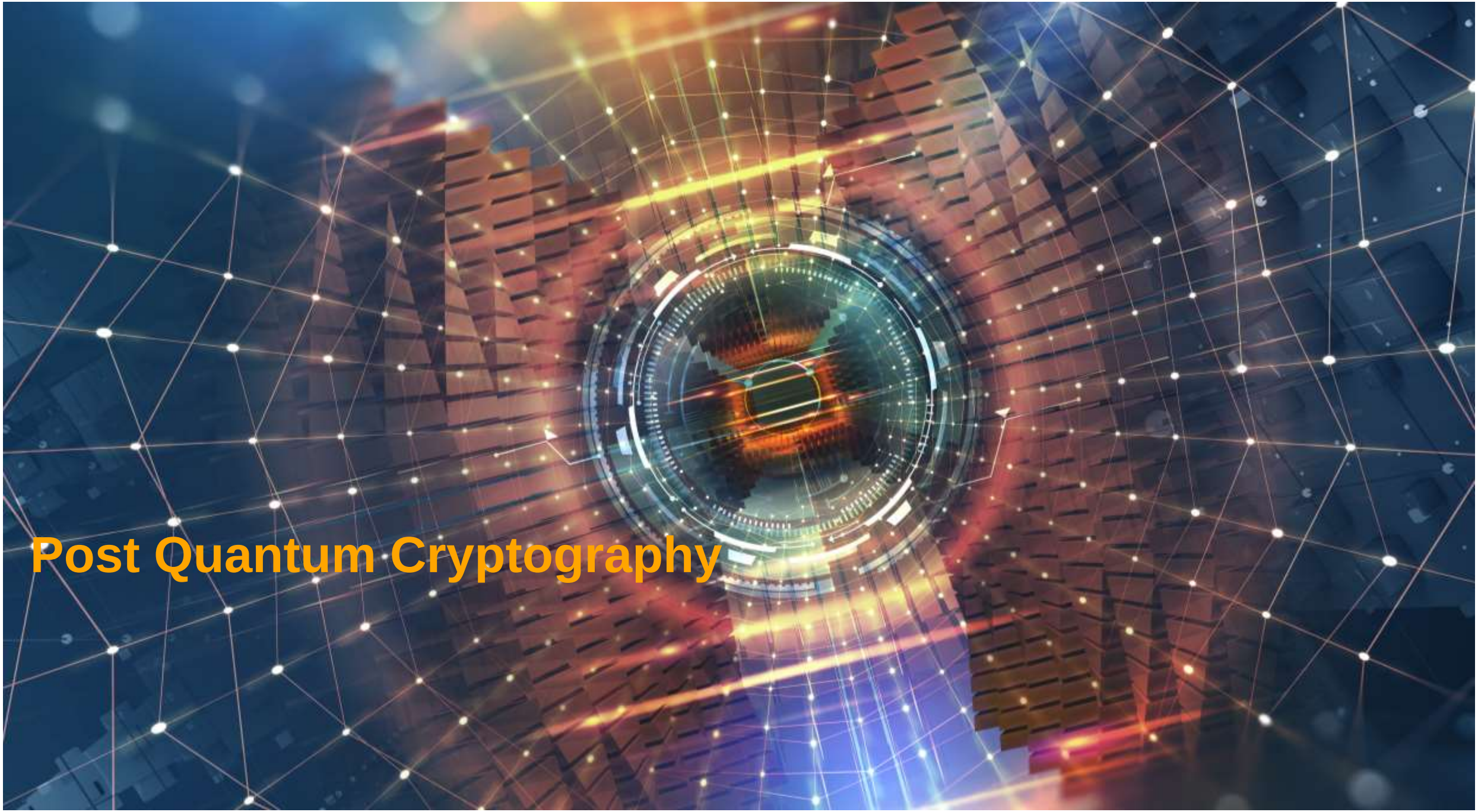
- Purpose: Test method **leveraging data on AVs**
- In real-world conditions on public roads,
  - **without control** of the vehicle
  - already released software version is running in parallel
  - driver and passengers do not actively participate
- **Safety validation** of an AV as main use case
- Data collections vary highly with the specific monitoring and development goals.
- Transfer of the data to the Silent Testing cloud backend

Privacy Manager

- Application depends on target function
- PETs: Add noise, encrypt, apply MPC
- Separation of raw data most likely not applicable due to debug limitations



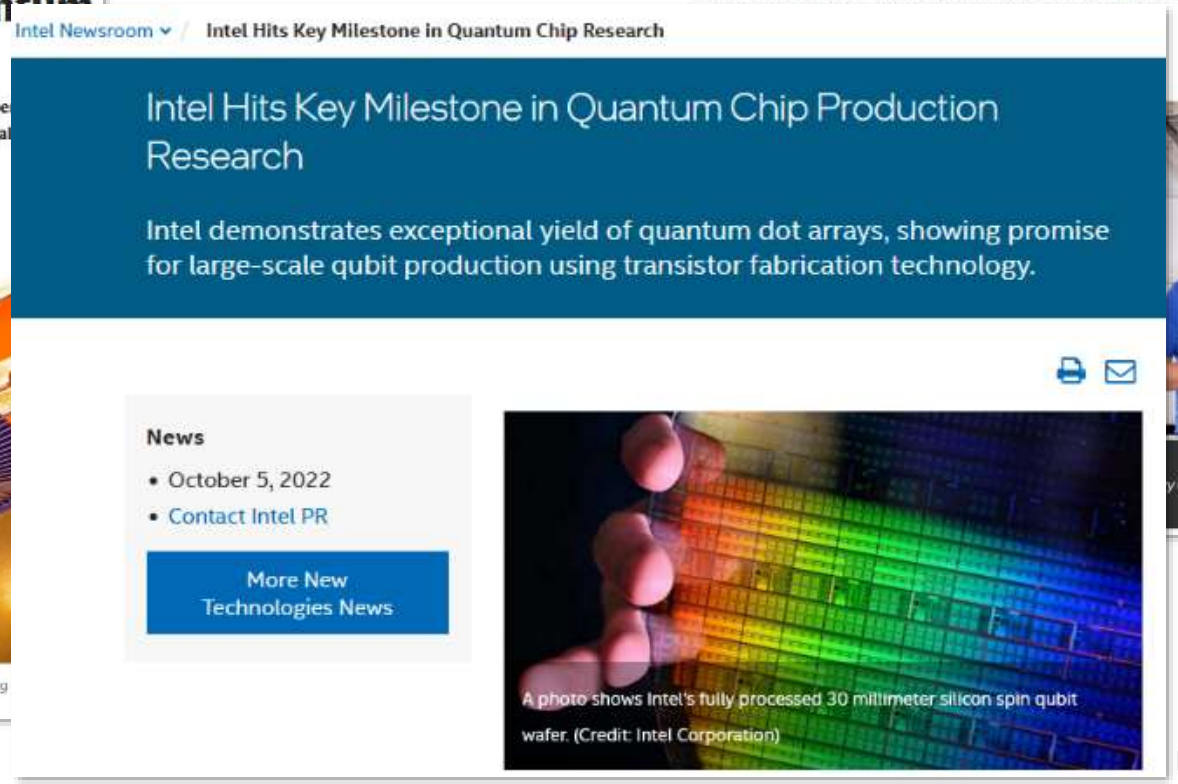
| **AV:** Automated Vehicle | **MPC:** Multi-Party Computation | **PET:** Privacy-Enhancing Technology |



Post Quantum Cryptography

Active Research on Quantum Computers Ongoing

[1]



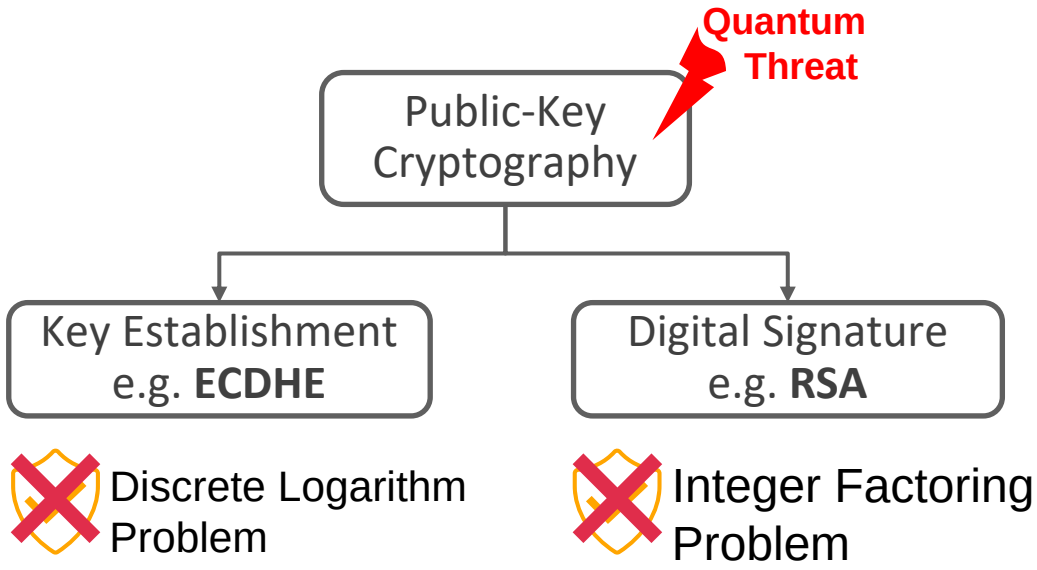
[2]

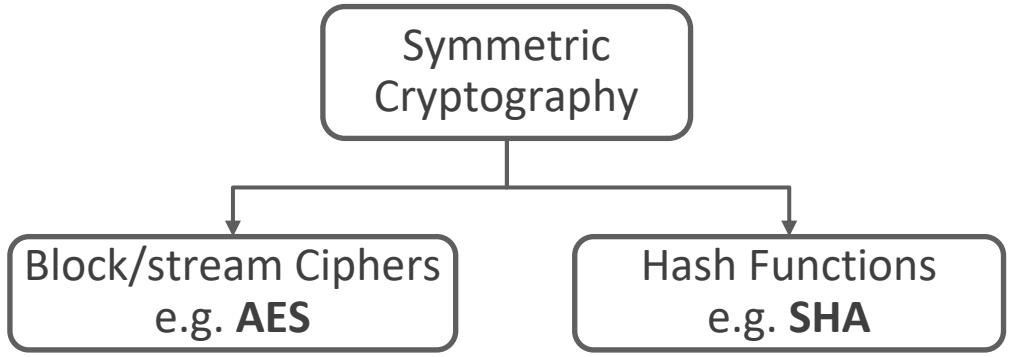
[3]

| **1:** https://www.nature.com/articles/d41586-019-03213-z/ | **2:** Intel Hits Key Milestone in Quantum Chip Production Research | **3:** IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two |

Contemporary Cryptography

Asymmetric Cryptography is on Risk





Shor's Algorithm (1994)

- Quantum algorithm giving exponential speed-up over classical computers
- It can be used for Factoring large integers and Finding discrete logarithms

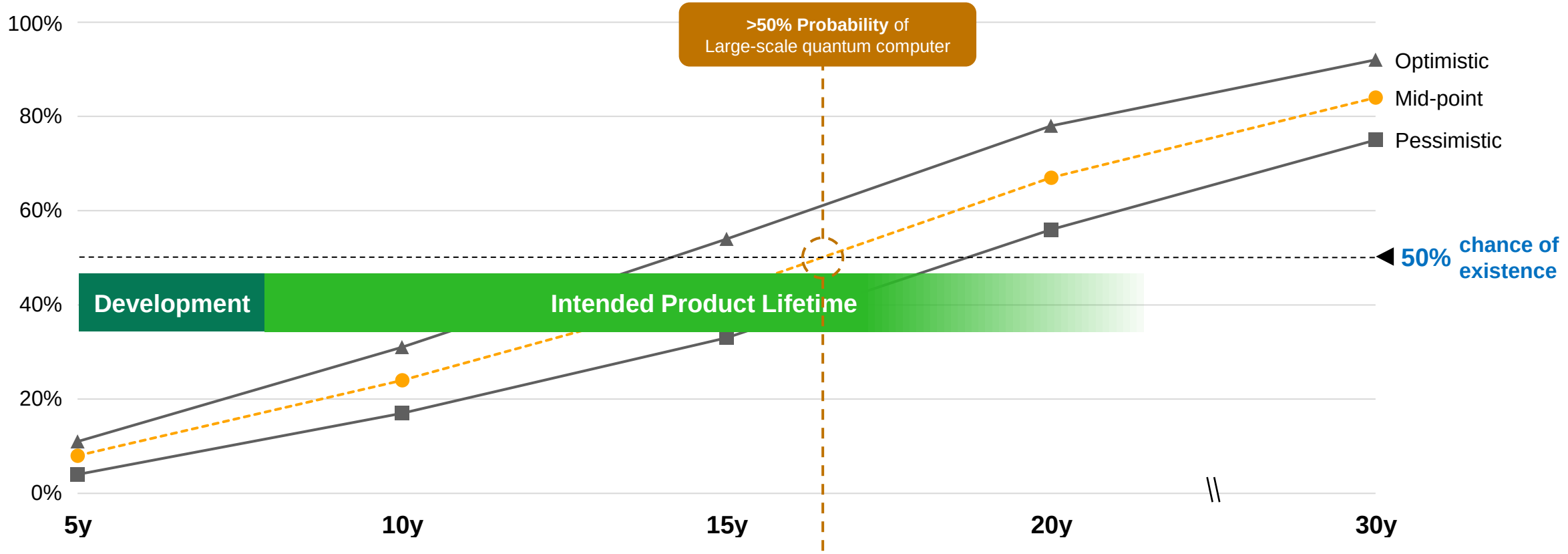
Grover's Algorithm (1996)

- Polynomial speed-up in unstructured search, from $O(N)$ to $O(\sqrt{N})$
- There is recent research to speed it up some more, but nothing feasible right now

Post Quantum Cryptography

The Status Quo will be on Risk

Opinion-based estimates of the cumulative probability of a digital quantum computer able to break RSA-2048 in 24 hours



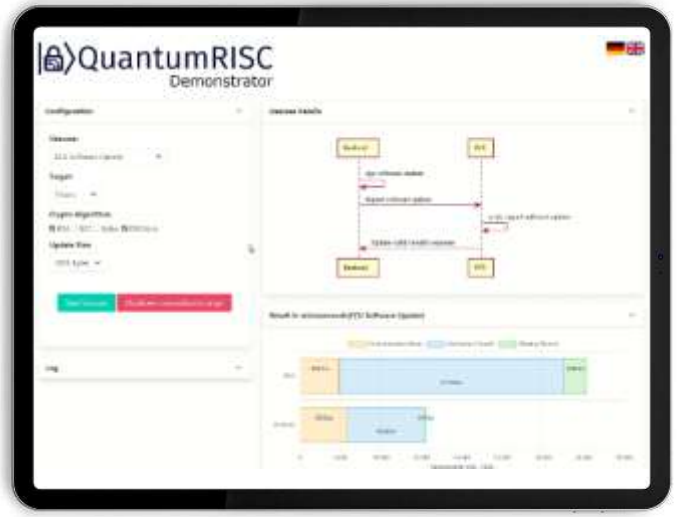
| **Adapted from** Mosca and Piani, Quantum Threat Timeline Report 2023 |

Post Quantum Cryptography

Working towards Solutions in QuantumRISC Project

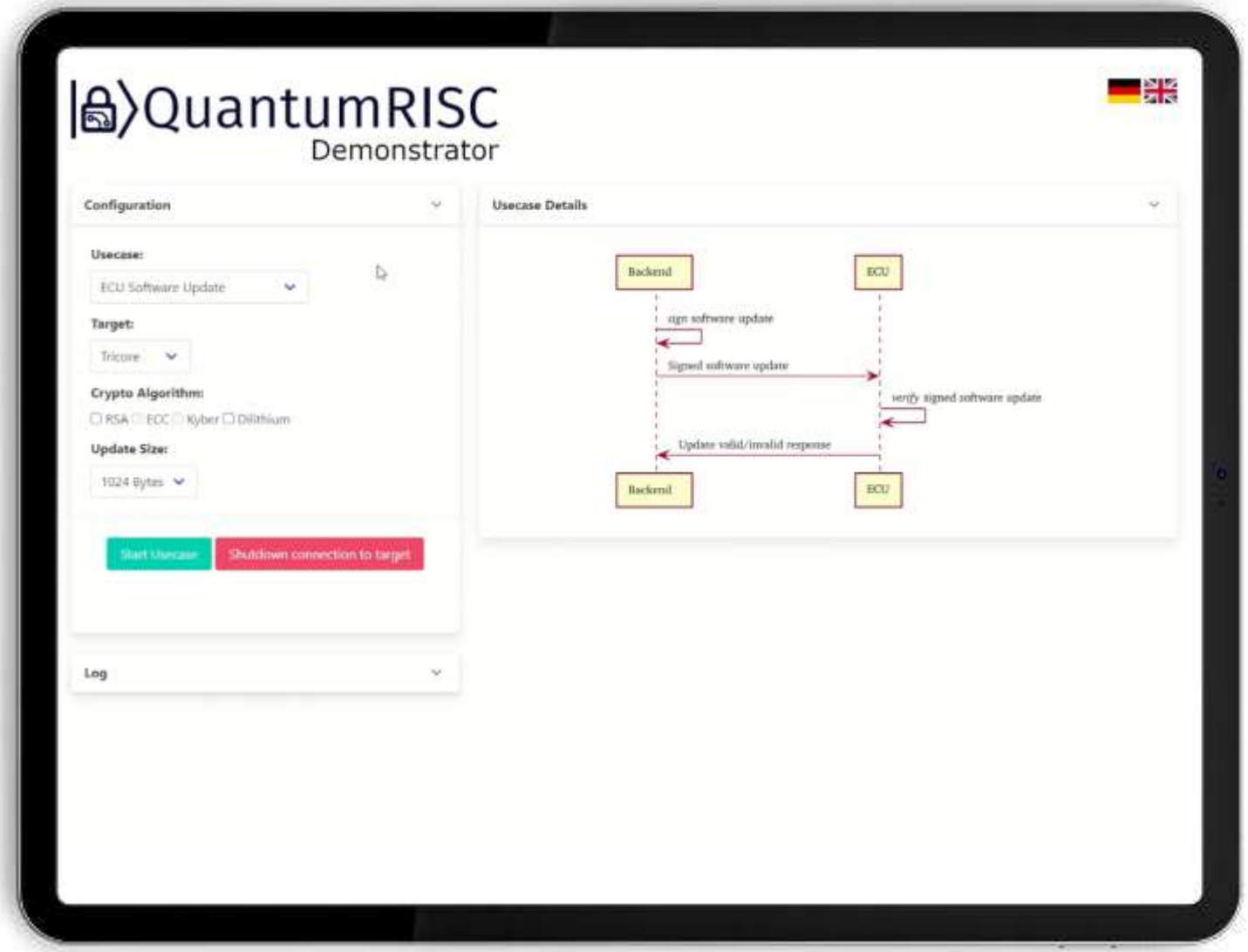
Goals of the Project

- Definition of **common Automotive Use-cases**
- Development of a **custom library** targeting embedded ECUs **containing post-quantum algorithms**
- Implementation of the Use-cases in a server-client architecture
- **Benchmarking** and **identification of requirements**



- Implemented the Use-cases in an **End-to-End demonstrator**
- End-to-End demonstrator based on **Elektrobit AUTOSAR Classic library** containing Kyber and Dilithium
- Integrated on 32-bit AURIX™ TriCore™ microcontroller from Infineon

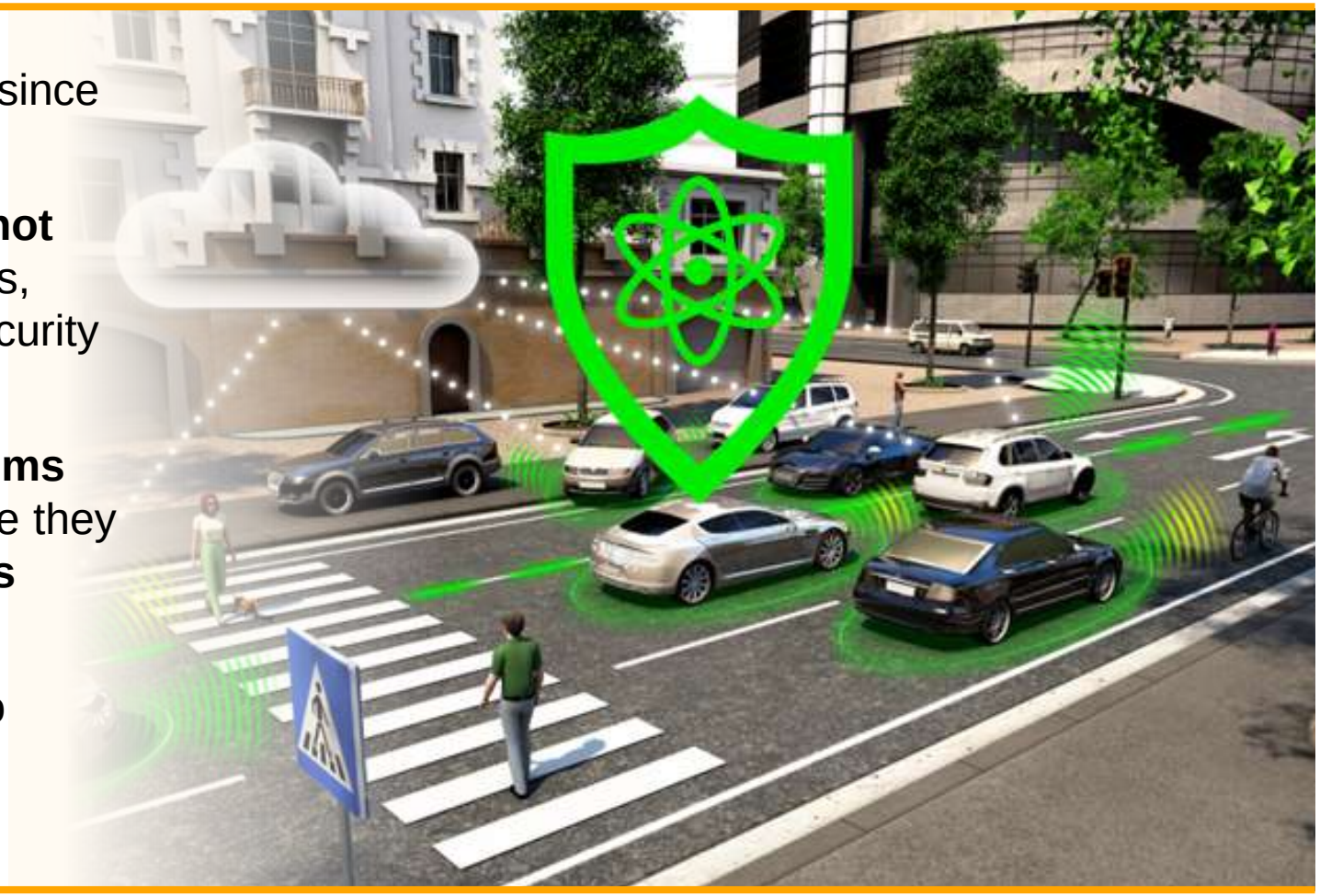
Post-Quantum Demonstrator



The numbers shown in this video are preliminary.

Post Quantum Cryptography Research
Conclusions

- **Migration** to PQC is **not straightforward** since no “one-size-fits-all” solution exists
- **Crypto-Agility** in the Automotive world is **not that easy** to achieve due to e.g., processes, hardware constraints, performance and security considerations
- Depending on the use-case, **PQC algorithms can be faster** than pre-quantum ones while they tend to **require more hardware resources** (ROM & RAM)
- We are working on **providing solutions** to support a **sustainable Cybersecurity** of Continental’s and our customer’s products.



Thanks for Listening
Any Questions?

Head of Security & Privacy Research and Governance

Dr. Markus Tschersich

Continental Automotive Technologies GmbH
Security & Privacy Competence Center
Guerickestraße 7
60488 Frankfurt am Main, Germany

Phone: **+49 69 7603-1832**

eMail: **markus.tschersich@continental.com**