CYBERSECURITY
SEMINAR
FRIBOURG

Fribourg Cybersecurity Seminar – HEIA-FR – 14.11.2024

Talk: The Road to Compliance: Cyber Regulations Shaping the Future of Connected Vehicles
Speaker: Kilian Marty, CEO | Cyber security consultant at CertX Solutions SA

Who we are

Kilian Marty

CEO | Cyber security consultant at CertX Solutions SA

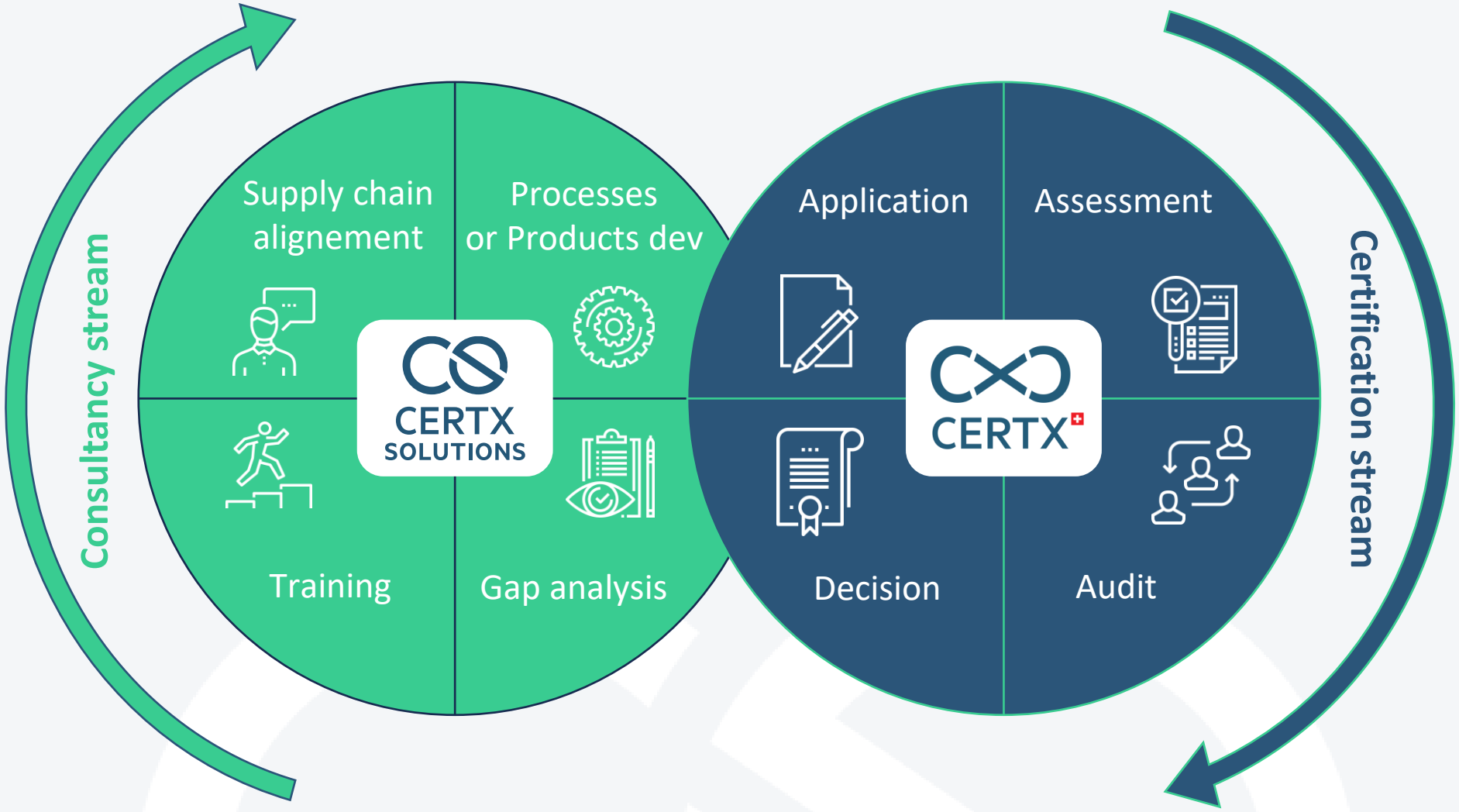
Kilian.marty@certx.com

Our ecosystem

CertX AG is the First Swiss Certification Body for Functional Safety, Cyber Security and AI accredited by Swiss Accreditation Service (SAS)

CertX Solutions is a consultancy company supporting customers to design, implement and maintain best security, safety and AI practices for reaching compliance with regulatory framework and State-of-the-Art references

How we are supporting our customers

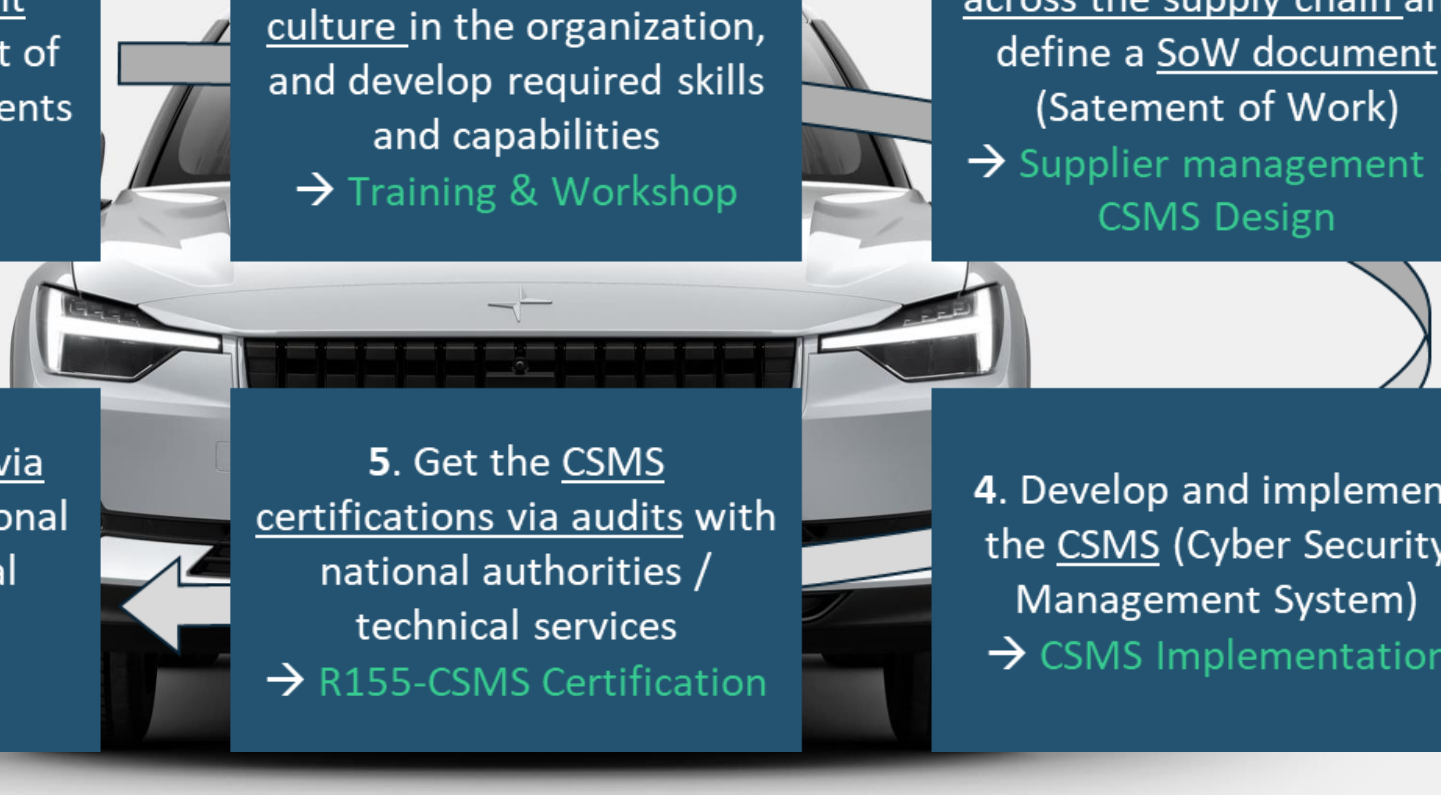


Successful customer case

1. Evaluate the current posture against new set of cyber security requirements
→ Gap Analysis

2. Establish a cyber security culture in the organization, and develop required skills and capabilities
→ Training & Workshop

3. Establish agreements across the supply chain and define a SoW document (Satement of Work)
→ Supplier management & CSMS Design



6. Get type approvals via assessements with national authorities / technical services
→ Type approval

5. Get the CSMS certifications via audits with national authorities / technical services
→ R155-CSMS Certification

4. Develop and implement the CSMS (Cyber Security Management System)
→ CSMS Implementation

CERTX SOLUTIONS

Automotive threat landscape – WHAT

Hackers Found Millions of Kias Could Be Tracked, Controlled With Just a Plate Number

Kia updated its web portal after the hackers informed them of the security issue, which was similar to a past vulnerability with Lexus and Toyota vehicles.

AR BACKCHANNEL BUSINESS SCIENCE CULTURE

URITY AUG 4, 2016 9:00 AM

IOT SECURITY

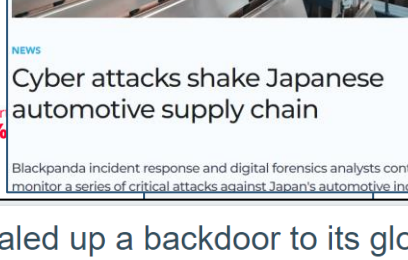
16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure

A group of seven security researchers have discovered numerous vulnerabilities in vehicles from 16 car makers, including bugs that allowed them to control car functions and start or stop the engine.

MAGAZINE TRANSPORTATION MATERIAL HANDLING TECHN

Report: hackers target third-party suppliers automakers' supply chains

90% of cyberattacks in the sector are aimed at "less vigilant firms protected OEMs



NEWS

Cyber attacks shake Japanese automotive supply chain

Blackpanda incident response and digital forensics analysts continue to monitor a series of critical attacks against Japan's automotive industry.

Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles

Researchers try out methods of jamming and spoofing the car's radar, ultrasonic sensors, and cameras---with disturbing results.

A New Wireless Hack Can Unlock 100 Million Volkswagens

team of researchers has found that Volkswagen stores secret keys in car components that leave almost all its vehicles since 1995 vulnerable to theft.

Android Phone Hacks Could Unlock Millions of Cars

Kaspersky security researchers find missing security safeguards in nine different connected car apps.

Toyota sealed up a backdoor to its global supplier management network

Adam Bannister 07 February 2023 at 17:34 UTC

A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features

new wrinkle in auto-hacking research points to a fundamental vulnerability in the CAN protocol cars' innards use to communicate.

Volkswagen vehicles hacked via WiFi hotspot feature

Jessica Haworth 04 May 2018 at 11:14 UTC
Updated: 08 November 2018 at 15:43 UTC

A Remote-Start App Exposed Thousands of Cars to Hackers

The bugs could have let an industrious hacker locate cars, unlock them, and start them up from anywhere with an internet connection.

Thieves Use CAN Injection Hack to Steal Cars

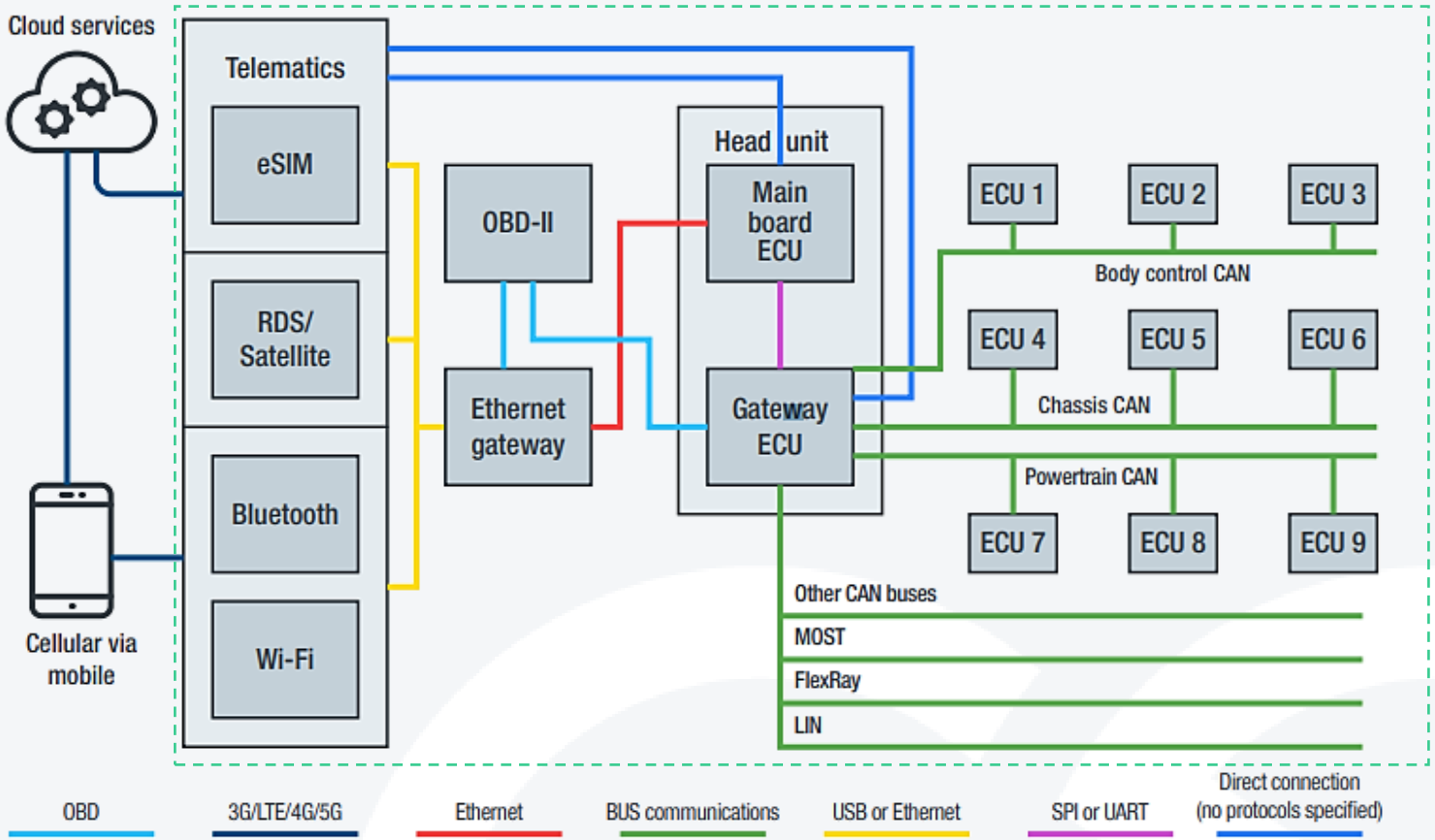
An innocent-looking portable speaker can hide a hacking device that launches CAN injection attacks, which have been used to steal cars.

Hackers Can Clone Millions of Toyota, Hyundai, and Kia Keys

Encryption flaws in a common anti-theft feature expose vehicles from major manufacturers.

Automotive threat landscape – WHY

Simplified onboard architecture

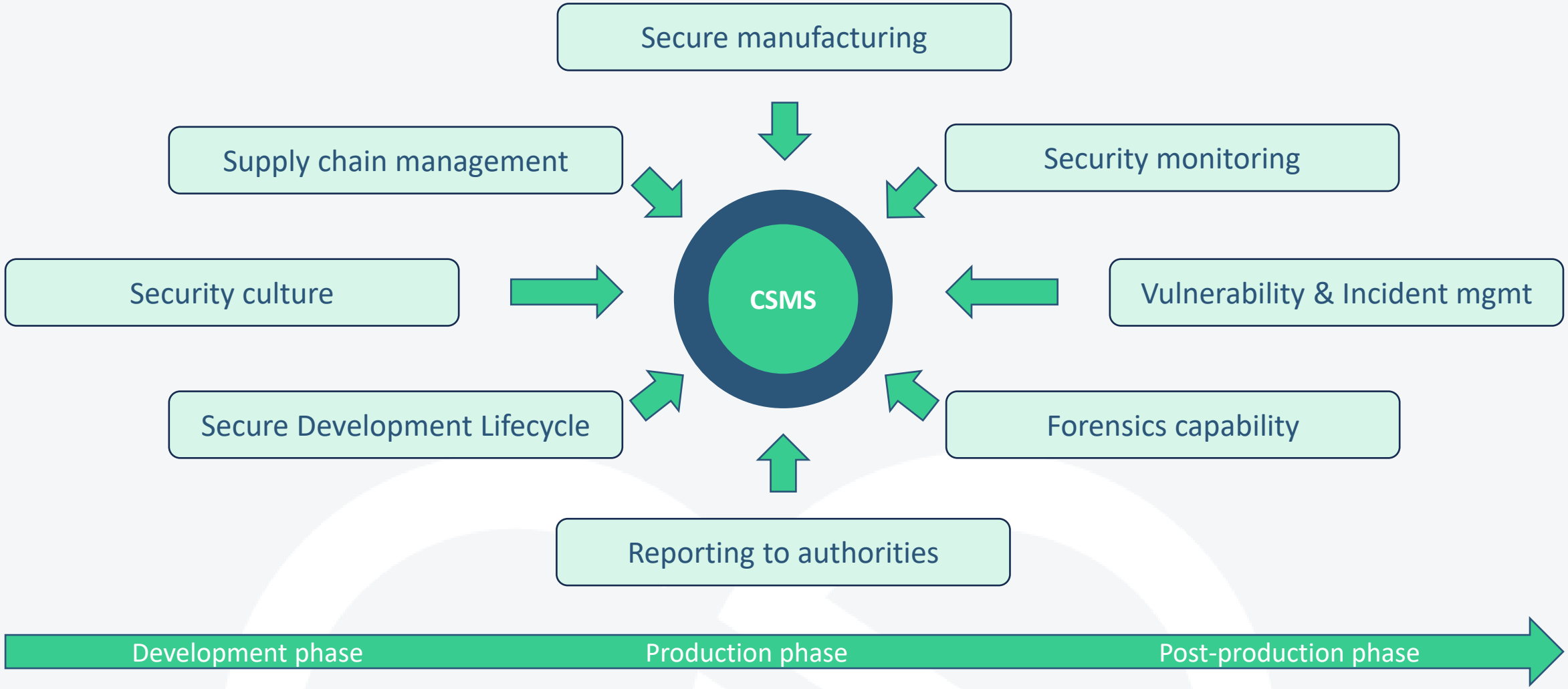


- COMPLEXITY – Modern cars feature around **150 million lines of code**, which is expected to triple by 2030, In comparison, a passenger aircraft contains about 15 million lines of code *[src: McKinsey & Co]*
- CONNECTIVITY – A connected vehicle would generate and consume up to 40 terabytes of data every eight hours of driving
- VEHICLE ENVIRONMENT – Today' vehicles are computer-based systems vulnerable to cyber attacks… and not only targeting vehicle itself !
- ATTACKER INTEREST – Cybercrime, including automotive-targeted initiatives, is more "profitable" than global illegal drug trade, with a projection of ≈ $10 trillion for 2024 versus $600 billion *[src: UNODC & Forbes]*

Automotive cyber security compliance – HOW

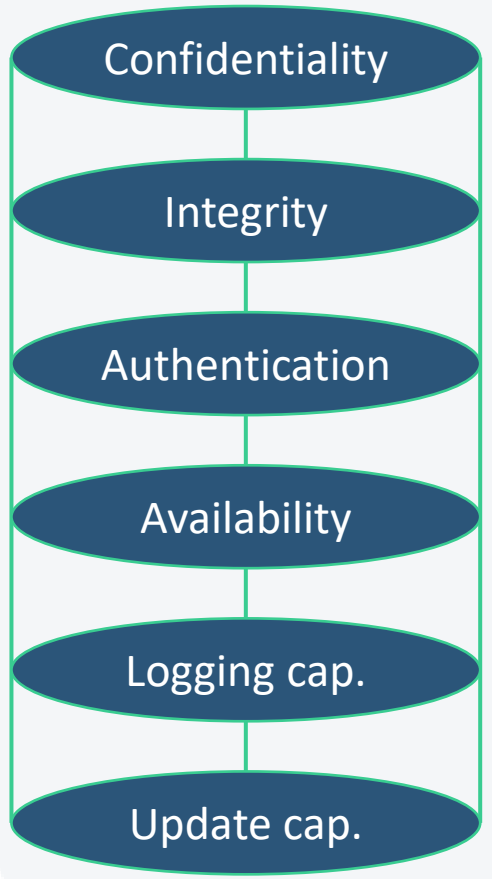
- **UN ECE R155 – Enforcement timeline**
  - *Official release: June 25, 2020*
  - *Applicable to all new type-approved vehicle: July 1, 2022*
  - *Applicable to all type-approved vehicle: July 1, 2024*
- **Requirements related to CSMS** (Cyber Security Management System) - to be considered as a foundation / prerequisite for VTA (Vehicle Type Approval) applications
- **Requirements related to Vehicle Types** – to be considered per project / program / model
- **Approval methods** – documentation assessment & security testing or witnessing (using risk based sampling)
- Parallel stream specifying legally binding requirements for Software Update Management System (SUMS) under UN ECE R156

Automotive cyber security – Key domains



Automotive cyber security – Key principles

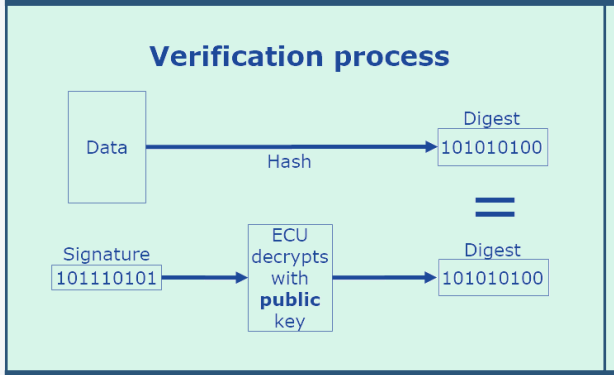
- **Holistic approach** – Technology, Process and People
- **Risk-based approach** – Target a reasonably secure posture
- **Defense in depth** – Multiply your protection barriers
- **Security-by-design** – Integrate cyber security as a foundational pillar of your organization and services/products
- **Be proactive AND reactive** – Assess and design, then monitor, reassess and react
- **Think "collaboratively"** – Information sharing is key



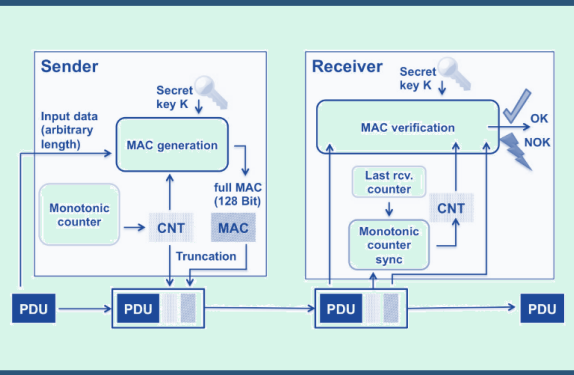
Automotive cyber security – Key measures

Using risk-based argumentations, secure technologies, components and architecture are implemented, incl.

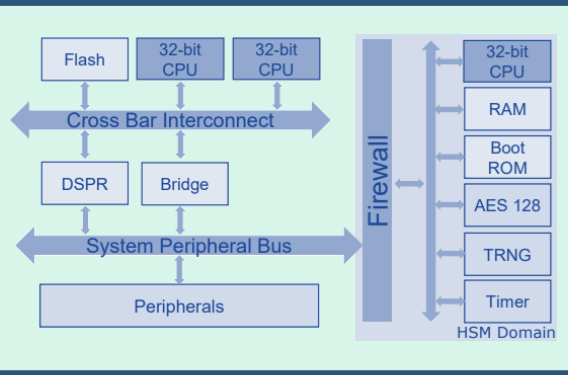
Secure boot & Firmware integrity



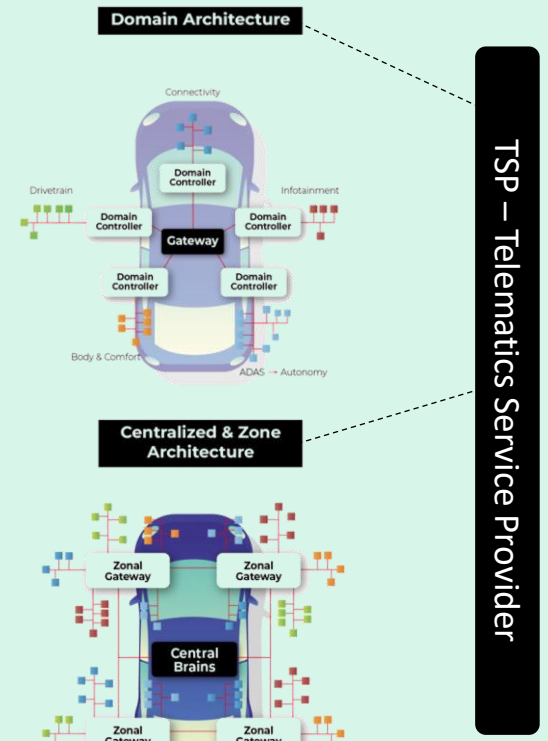
Secure in-vehicle communication



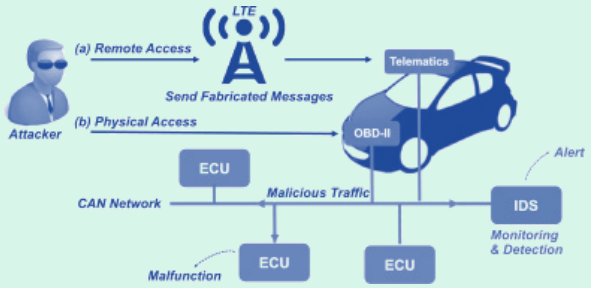
HSM – Hardware Security Module



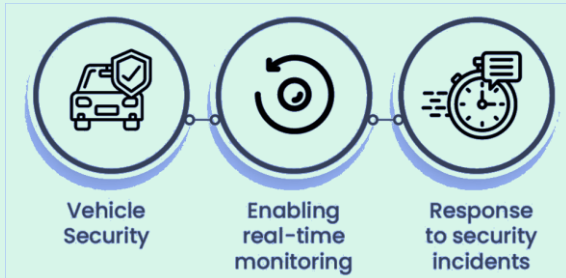
Secure E/E architecture & beyond



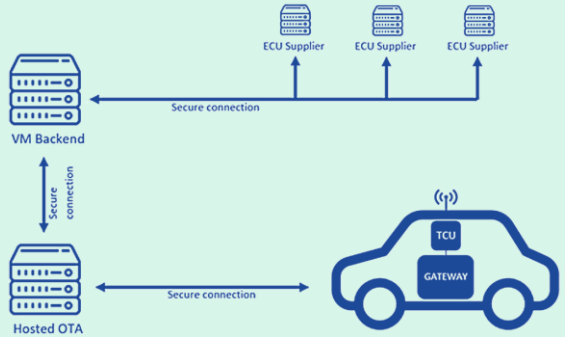
IDPS – Intrusion Detect./Prevent. System



VSOC – Vehicle Security Operation Center



OTA Update – Over-The-Air Update



UN ECE R155 – What is «good enough» ?

UN ECE R155 [Annex 5] is giving a mandatory baseline of threats to be considered, and risks to be minimized

Threats regarding **back-end servers** related to vehicles in the field

Backend servers weaknesses, connected services disruptions, cloud data breach…

Threats to vehicles regarding their **communication channels**

Vehicle interface / communication spoofing, tampering, injections, MitM, replay, DoS…

Threats to vehicles regarding their **external connectivity and connections**

Compromised hosted 3rd party SW, Exploit on diag or using infected media…

Threats to vehicles regarding their **update procedures**

Update procedure compromission, Update package alteration, DoS...

Threats to **vehicle data/code**

In-vehicle compromissions incl. PII, Identity fraud, integrity compromissions, unauthorized data modification / deletion…

Threats to vehicles regarding **unintended human actions** facilitating a cyber attack

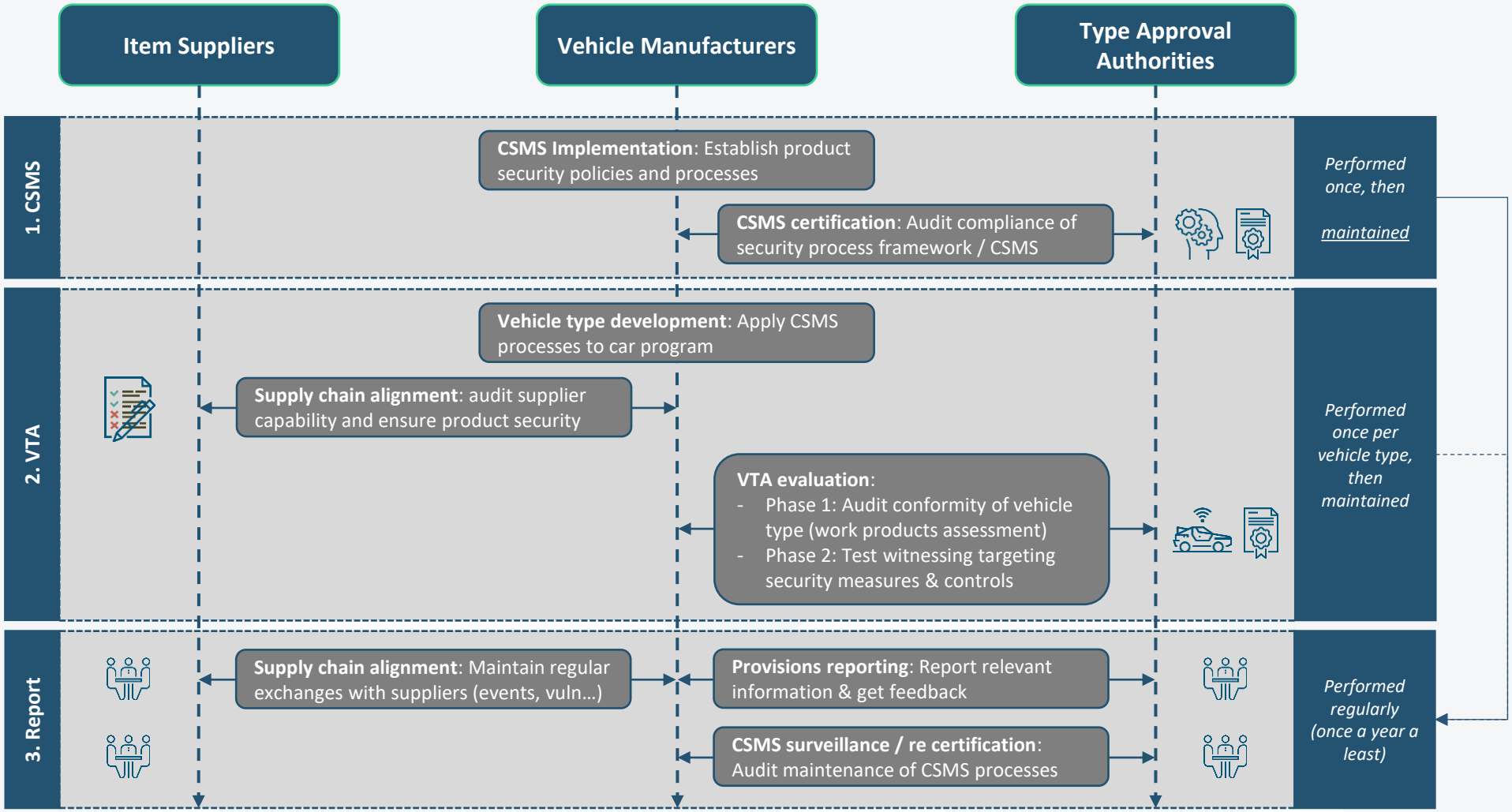
Social engineering practices, security procedure not followed by operators/users…

Potential vulnerabilities that could be exploited if **not sufficiently protected or hardened**

Lack of hardening…

CERTX SOLUTIONS

Automotive cyber security – compliance journey

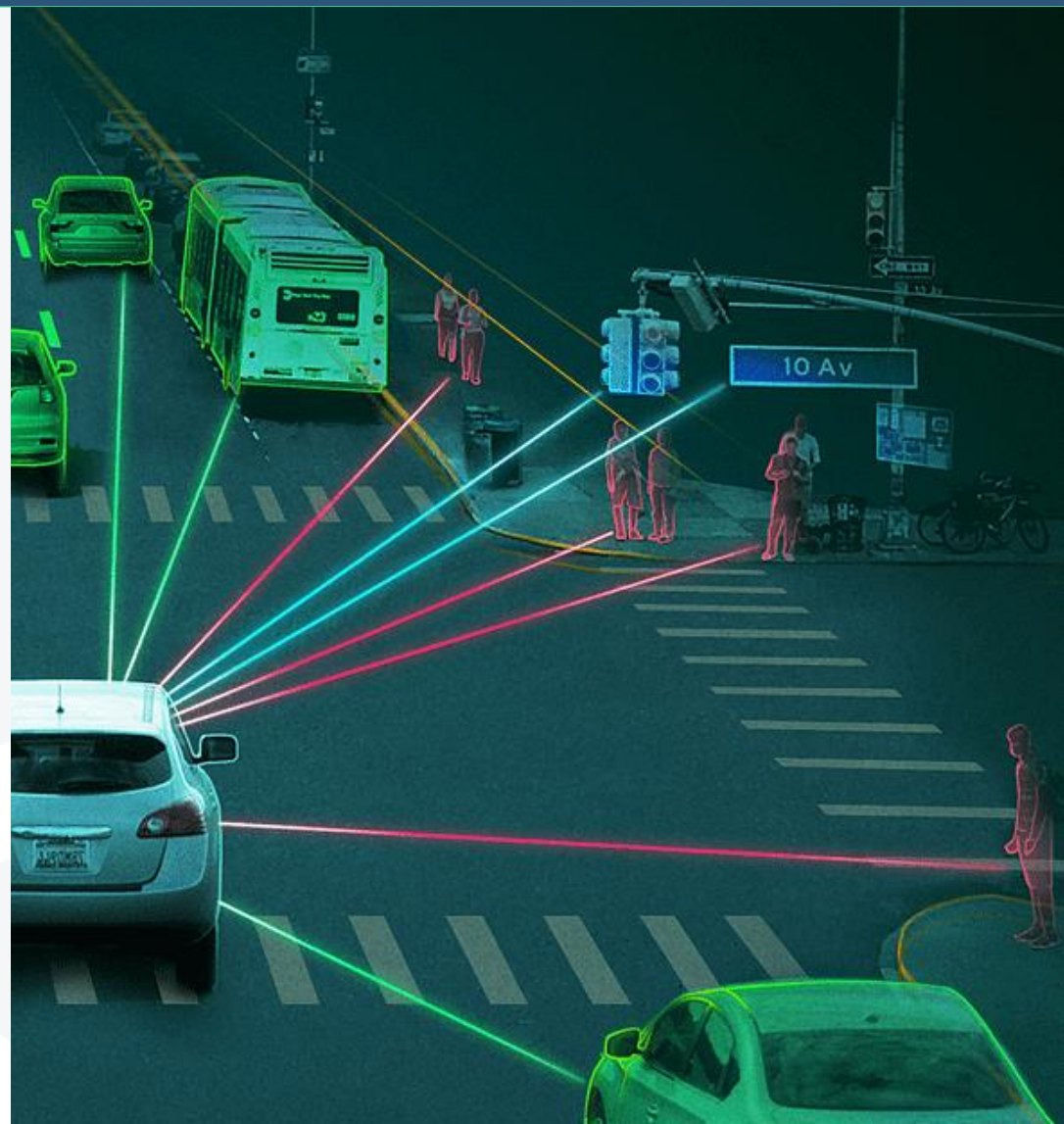


CERTX SOLUTIONS

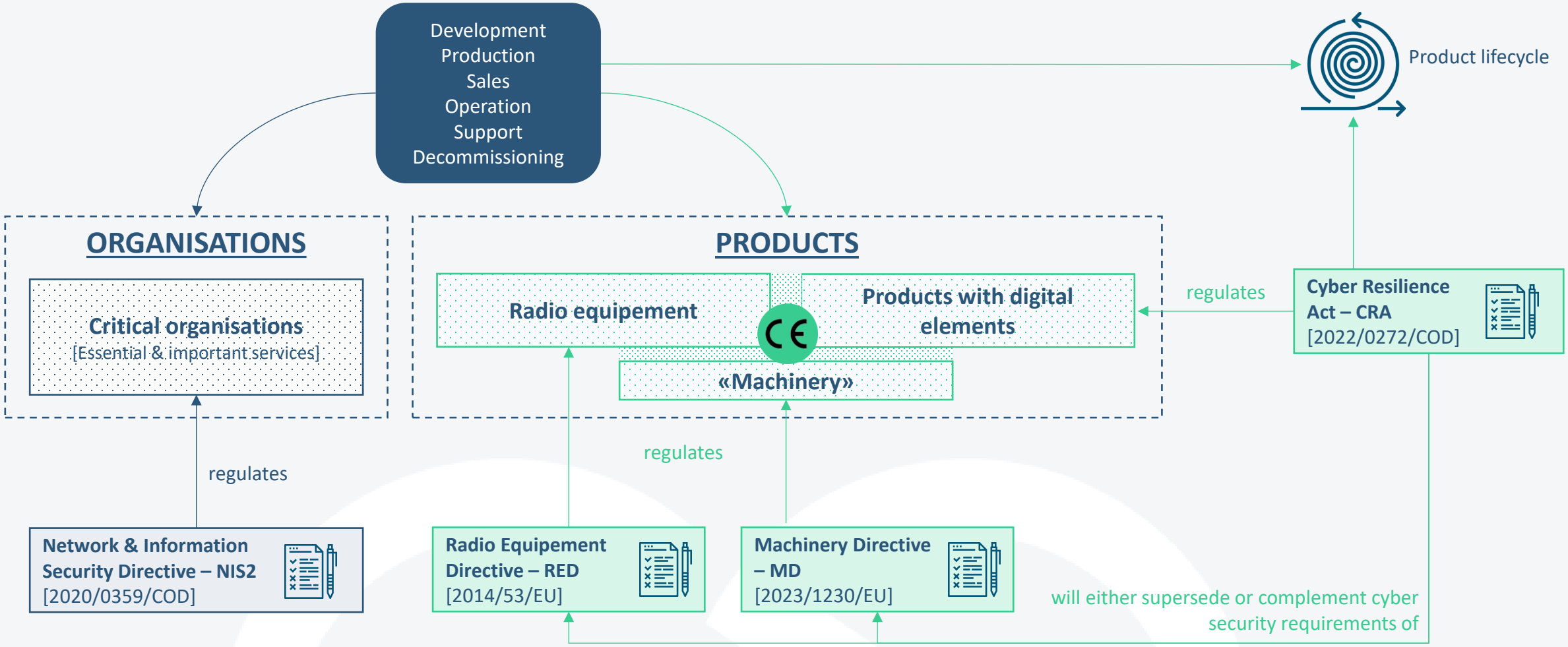
Automotive cyber security across supply chain

Connected mobility trends – C-ITS & automation

- Automated vehicles are coming, and with them stringent requirements and expectations about connected road infrastructure (C-ITS)
- Additional data are required to feed **detection**, localization and **path planning** algorithms
- New cyber security compliance scheme also exist on integrator and operator level
  - *NIS2 directive to be transposed by all EU countries*
- CERTX & are participating to Swiss founded research projects aiming to anticipate cyber risks raised by such upcoming mobility systems – **ASTRA-MB4**



And the same trend is going beyond roads !



Key takeaways

Rapidly evolving threat landscape

Spoofing
DoS
Tampering
Data breach
MitM
Ransomware
Rogue devices
Relay attack

Cyber security is a continuous process

Training & awareness
Market surveillance & response
Audit
Vuln. management
Continuous improvement
Threat intelligence

Product / Vehicle cyber security shall be considered «by-design»

Threat Analysis & Risk Assessment
Security testing
DevSecOps
Secure architecture
SBOM
Secure design practices
SDV

Newly established cyber security compliance scheme

UN ECE R155
UN ECE R156
NIS2
GDPR
CRA
AI Act
RED
MD
Data Act

Horizontal & industry-specific State-of-the-Art references

ISO/SAE 21434
ISO/IEC 27001
ISO 24089
ISO/IEC 27701
ISA/IEC 62443
ISO/PAS 5112
ISO/IEC 15408
SAE J3061

For any further advices, please do not hesitate to ping us

Thx, any questions ?

Kilian.marty@certx.com

CERTX
SOLUTIONS

Passage Du Cardinal 5
1700 Fribourg, Switzerland

www.certx-solutions.com