FIRST SWISS

Functional Safety and Cyber Security Certification Body

Functional Safety

OT & IT Cyber Security

Artificial Intelligence

CERTX ✛

Cyber security: How to build secure automated vehicles?

"The critical path to introduce autonomous driving vehicles will not be the technology but the development of a metric which empowers for an approval"
Prof. Dr. rer. nat. H. Winner, November 2013

We Are:

First Swiss Certification Body for Functional Safety and Cyber Security accredited by Swiss Accreditation Service (SAS) with international validity
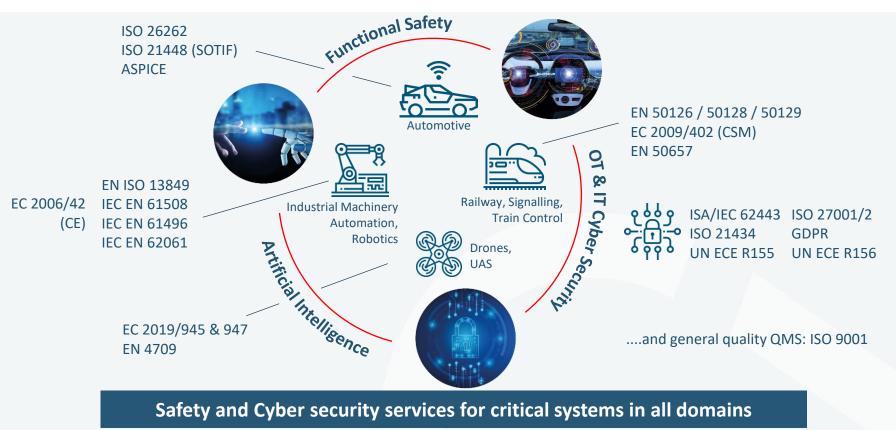
Experts in Functional Safety and Cybersecurity with Swiss DNA and Quality. Innovations at heart, pragmatic in style.
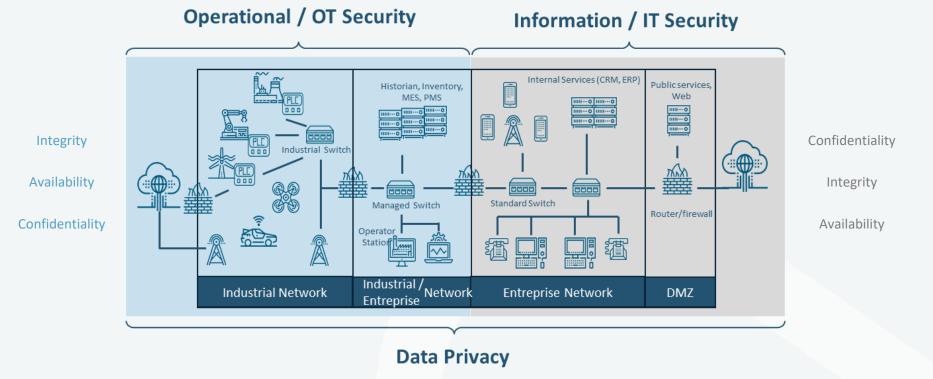
We co-write the standards for future automated systems, autonomous mobility and cyber security

Expertise Across All Safety Critical Domains

Functional Safety

ISO 26262
ISO 21448 (SOTIF)
ASPICE

Automotive

EN 50126 / 50128 / 50129
EC 2009/402 (CSM)
EN 50657

OT & IT Cyber Security

EN ISO 13849
IEC EN 61508
IEC EN 61496
IEC EN 62061

EC 2006/42
(CE)

Industrial Machinery
Automation,
Robotics

Railway, Signalling,
Train Control

ISA/IEC 62443   ISO 27001/2
ISO 21434   GDPR
UN ECE R155   UN ECE R156

Artificial Intelligence

Drones,
UAS

EC 2019/945 & 947
EN 4709

....and general quality QMS: ISO 9001

Safety and Cyber security services for critical systems in all domains

Cyber Security Domains

Operational / OT Security

Information / IT Security

Integrity

Availability

Confidentiality

Historian, Inventory, MES, PMS

Internal Services (CRM, ERP)

Public services, Web

Industrial Switch

Managed Switch

Standard Switch

Operator Station

Router/firewall

Confidentiality

Integrity

Availability

Industrial Network

Industrial / Entreprise Network

Entreprise Network

DMZ

Data Privacy

Cars are Vulnerable

Attacks on Connected & IoT Devices

OTA Updates

Engine Control Units

Attacks on the Cloud
Automotive Service Providers

DDoS

Remote Hijacking or Vehicle Theft

Ransomware

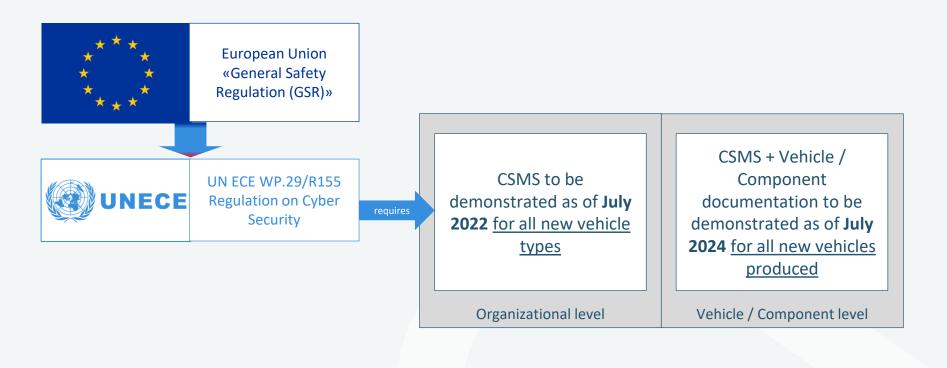# Cyberthreats are Real

Source: Wired

Chrysler had to recall 1.4 million
vehicles after (ethical)
hackers could remotely hijack a
Jeep's over the Internet.

…. apart from the commercial damage
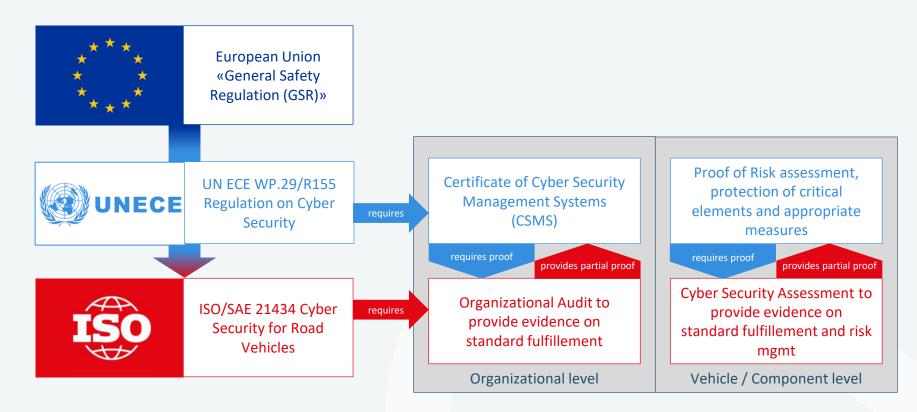a large loss in reputation and public acceptance

… will become mandatory for critical infrastructure but concerns all connected systems

Secure Road Vehicles – A Challenging Schedule

European Union
«General Safety
Regulation (GSR)»

UN ECE WP.29/R155
Regulation on Cyber
Security

requires

CSMS to be demonstrated as of July 2022 for all new vehicle types

Organizational level

CSMS + Vehicle / Component documentation to be demonstrated as of July 2024 for all new vehicles produced

Vehicle / Component level

Approach for Compliance

European Union «General Safety Regulation (GSR)»

UN ECE WP.29/R155 Regulation on Cyber Security

ISO/SAE 21434 Cyber Security for Road Vehicles

requires → Certificate of Cyber Security Management Systems (CSMS)

requires → Organizational Audit to provide evidence on standard fulfillment

Proof of Risk assessment, protection of critical elements and appropriate measures

requires proof / provides partial proof

Cyber Security Assessment to provide evidence on standard fulfillement and risk mgmt

requires proof / provides partial proof

Organizational level

Vehicle / Component level
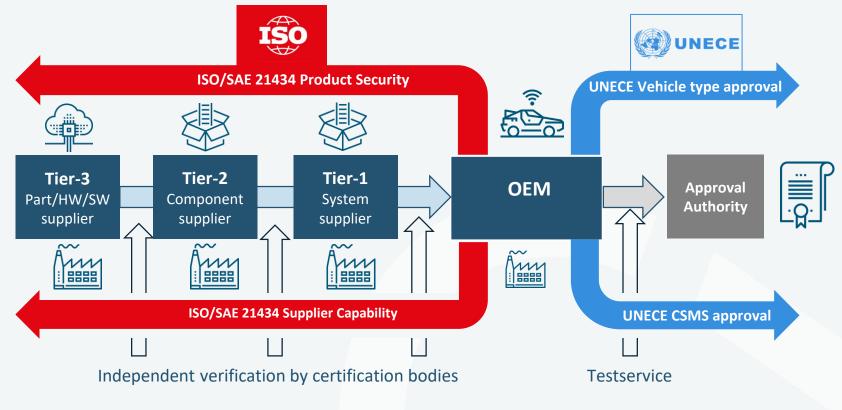
On project level:

- Vehicle / Component-specific work product and records
- **Independent** Cyber Security Assessment Report **required** (= evaluation of the evidence of security measures on product / vehicle level)

4. General considerations						
5. Organizational cybersecurity management						
5.4.1 Cybersecurity governance	5.4.2 Cybersecurity culture	5.4.3 Information sharing	5.4.4 Management systems	5.4.5 Tool management	5.4.6 Information security management	5.4.7 Organizational cybersecurity audit
6. Project dependent cybersecurity management						
6.4.1 Cybersecurity responsibi-lities	6.4.2 Cybersecurity planning	6.4.3 Tailoring	6.4.4 Reuse	6.4.5 Component out-of-context	6.4.6 Off-the-shelf component	6.4.7 Cybersecurity case / 6.4.8 Cybersecurity assessment / 6.4.9 Release for post-development
7. Distributed cybersecurity activities						
7.4.1 Supplier capability		7.4.2 Request for quotation		7.4.3 Alignment of responsibilities		
8. Continual cybersecurity activities						

On organizational level

- Cyber Security Management System (CSMS)
- **Independent** Cyber Security Audit Report **required**

Coordination across the Entire Supply Chain

ISO/SAE 21434 Product Security

UNECE Vehicle type approval

| Tier-3 Part/HW/SW supplier | Tier-2 Component supplier | Tier-1 System supplier | OEM | Approval Authority |

ISO/SAE 21434 Supplier Capability

UNECE CSMS approval

Independent verification by certification bodies

Testservice

Typical Approach Adopted by OEM's

1. Evaluate the <u>current posture</u> against new set of cyber security requirements
→ **Gap Analysis**

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

3. Establish <u>agreements across the supply chain</u> and define a statement of work
→ **Supplier management & CSMS Design**

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

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

4. Develop and implement the <u>CSMS</u> (Cyber Security Management System)
→ **CSMS Implementation**

Support for Compliance

Education

- **Awareness sessions for managers and engineers** on best security practices (e.g. threat modelling, penetration tests…)

- **Certifiable trainings** on key standards (e.g. ISO/SAE 21434 Automotive Security Red Belt)

Gap Analysis

- **Identification of relevant references** for different customer sectors

- **Third-party compliance checks on product**

- **Third-party compliance checks on processes**

Certifications

- **Certification of products**

- **Certification of processes**

- **Certification of management systems**

Specific support

- process design and implementation

- best practices implementation

- discussion with authorities

Further questions ?

Kilian Marty
Head of Cybersecurity Department
T +41 26 309 29 94
kilian.marty@certx.com

CertX AG
Route de l'Ancienne Papeterie 106
1723 Marly, Switzerland

www.certx.com

The information contained in this presentation is the property of CertX AG.

This presentation and extracts thereof may only be duplicated or forwarded to third parties following explicit written approval by CertX AG.

All product names used in this documentation are trademarks or otherwise protected by law, even if not specifically indicated.