MAGNA

Forward. For all.

# Ensuring Automotive Cybersecurity in a Connected Car:

## Cybersecurity Challenges and Innovative Solutions in Compliance with UNECE 155 and ISO 21434

Dr. Klaus Kainrath

14.11.2025

# Overview




Disclosure or duplication without consent is prohibited

# Introduction

- Automotive industry is rapidly changing towards software-defined vehicle (SDV)
- Modern vehicle contain more software than a common aircraft
- Wireless Connectivity is becoming increasingly important
- Increasing safety and cybersecurity considerations
- Standards for Functional Safety, Safety of the Intended Functionality and Cybersecurity
  - ISO26262 (FuSa)
  - ISO21448 (SOTIF)
  - ISO21434 (Cybersecurity)
  - UNECE R155 and R156 regulations


Disclosure or duplication without consent is prohibited

# Evolution of Automotive Connectivity

GPS Navigation Systems (1990s): Enabled vehicles to use satellite technology for navigation.

Telematics (Early 2000s): Integration of telecommunications and informatics, e.g., driver assistance, navigation, and emergency services.

Internet Connectivity (2010s): Vehicles began featuring built-in internet access, allowing for services like live traffic updates, streaming media, and Wi-Fi hotspots.

| 1990s | 1996 | Early 2000s | 2000s | 2010s |
|---|---|---|---|---|

On-Board Diagnostics II (OBD-II) (1996): Standardized diagnostic system allowing real-time data reporting and diagnostics from the vehicle.

Bluetooth Integration (2000s): Enabled hands-free calling, audio streaming, and integration of mobile devices.


Disclosure or duplication without consent is prohibited

# Modern Vehicle Communication

- In-Vehicle Communication
- Vehicle-to-Cloud (V2C)
- Over-the-Air-Updates (OTA)
- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I)
- Vehicle-to-Network (V2N)
  Indirect via a network
- Vehicle-to-Everything (V2X or Car2x)
  → direct
- Key-to-Vehicle



Disclosure or duplication without consent is prohibited

# Connected Automotive Services

- Software Updates Over The Air (OTA)
- Navigation with Online Traffic Information
- Map Updates (Nav. and ISA)
- Music Streaming (even Video streaming for passengers)
- Hotspot for passengers
- Remote Functions (e.g., Preconditioning, un/locking, charging start/stop via App)
- Diagnostic Over The Air (EU7 compliance)
- Intrusion Detection System
- Key Management System
- And many more…

Source: Wireless Car


Disclosure or duplication without consent is prohibited

# Connectivity brings Vulnerability

Backend Vulnerabilities

Remote Functions Vulnerabilities

After Sales Vulnerabilities

Source: LinkedIn

Vulnerabilities in Communication Standards

Vulnerabilities in components

Implementation of vulnerable technologies


Disclosure or duplication without consent is prohibited

# Go Online – Connect everything

Connected Car:

- Hacker managed to fully take over the control of a Jeep Cherokee
- An online remote service “Uconnect” was exploited
- Tipp: Watch on YouTube:
  Jeep Cherokee Hack
  https://www.youtube.com/watch?v=MK0SrxBC1xs

https://www.wired.com/


Disclosure or duplication without consent is prohibited

# Go Online – Connect everything

- Everything, from small handheld devices up to facilities are nowadays „smart“
- „Smart“ means, everything is online, connected and…
  …not secure…
- So, what is secure then?
- Can it run DOOM?





Disclosure or duplication without consent is prohibited

# Cyber Incidents

- Only some examples…

2015

kaspersky daily

Products Renew Downloads Support Resource Center Blog Secure Futures

car hacking

Search blog posts

## Shock at the wheel: your Jeep can be hacked while driving down the road

Taking over a Jeep Cherokee driving at speed 70 mph at a remote highway is quite real.

Kate Kochetkova July 23, 2015

Oops, they've done it again: after two successful breaches into the systems of Toyota Prius and Ford Escape, security researchers Charlie Miller and Chris Valasek have recently hacked a Jeep Cherokee.

car hacking | Cars | connected devices | exploits | hackers

2017


2023


Tesla owner warning others after being locked out of car, account hacked

2022

Bloomberg

Europe Edition

Sign In

Live Now | Markets | Industries | Technology | Politics | Wealth | Pursuits | Opinion | Businessweek | Equality | Green | CityLab | Crypto | More

Technology
Cybersecurity

## Hacker Finds Way to Unlock Tesla Models, Start Cars

- Method to exploit smart technology tied to Bluetooth protocol
- No evidences of thieves using technique to access cars

Tesla Model S *Photographer: SeongJoon Cho/Bloomberg*

By Margi Murphy
16. Mai 2022 um 19:36 MESZ *Updated on 18. Mai 2022 um 15:59 MESZ*

Auto Recent

The leading source of breaking car news, reviews and more!

News | Industry | Europe | Reviews | Trucks | Electric | SUVs | Spy Photos | Sports Cars | More

Home » Industry 'ignoring' threats, hacker says


Industry

TEL AVIV, Israel — Automakers ought to cease treating cybersecurity researchers as adversaries and as an alternative contemplate them collaborators.

So says David Colombo, the teenage hacker who exploited flaws in third-party software program that allowed him

https://www.youtube.com/watch?v=MK0SrxBC1xs


Disclosure or duplication without consent is prohibited

# How can modern cars be protected?

- **The only truly secure system is one that is powered off**, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then, I have my doubts. *Gene Spafford - "Computer Recreations: Of Worms, Viruses and Core War" by A. K. Dewdney in Scientific American, March 1989, pp 110.*

- When there is **no secure system**, then OEMs shall **reduce any Cybersecurity risk for vehicles to a minimum!**

- And how?
  → **It needs a regulation and a standard!**


Disclosure or duplication without consent is prohibited

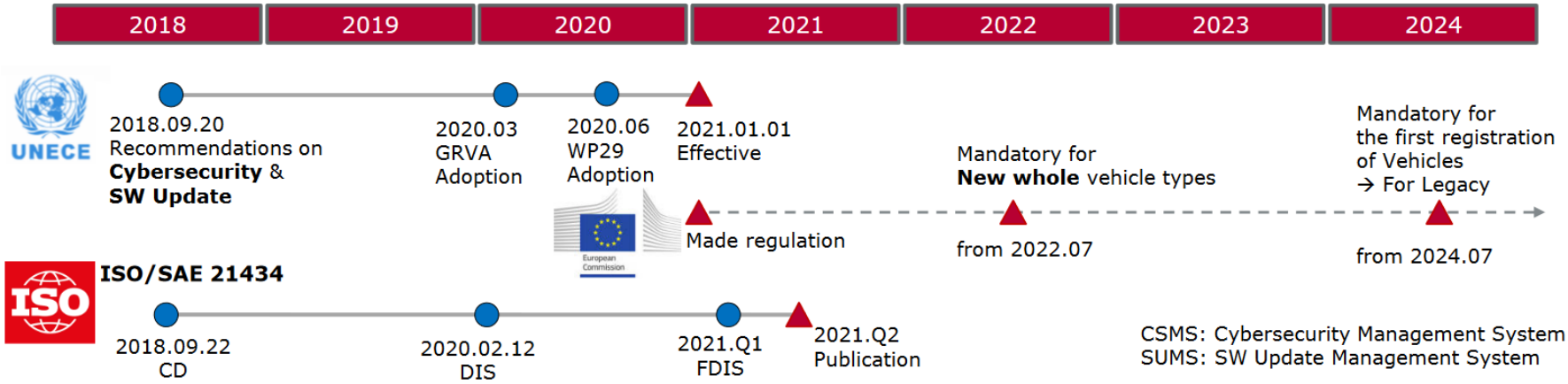
# Automotive Cybersecurity

- **UNECE R155 (**Cybersecurity Management System **– CSMS)** and **R156 (**Software Update Management System **– SUMS)** as regulations
- **ISO/SAE 21434** is the “tool” to implement a Cybersecurity Management system (CSMS).
- **ISO/SAE 21434** works to support the interest of UNECE WP.29 R155 and vice versa, protecting vehicles on a global scale.

Figure 1: Contracting Parties to the 1958 Agreement

Scope of application of the R155

Source: Upstream Report 2022




CSMS: Cybersecurity Management System
SUMS: SW Update Management System


Disclosure or duplication without consent is prohibited

# Automotive Cybersecurity

- Cybersecurity shall be implemented by design → starting in the **early dev. phase**
- Guidelines are stated within the ISO21434 → **CSMS**
- Must be assessed by an accredited testing institute → **MAGNA achieved it in 2023**
- Risk assessment shall help to identify possible CS threats → **TARA**
- CS Specifications are implemented to mitigate all CS risks → **CS Controls**
- Future SW updates shall help to maintain CS (e.g., Bug fixing) → **SUMS**

***ISO/SAE 21434***
***Security by design***

Engineering requirements for each step of product development

***R155***
***Cybersecurity Management System***

Cybersecurity monitoring throughout vehicle lifecycle

***R155***
***Threat Analysis & Risk Assessment***

Risk assessment and risk score for vulnerabilities

***R155***
***Monitoring***

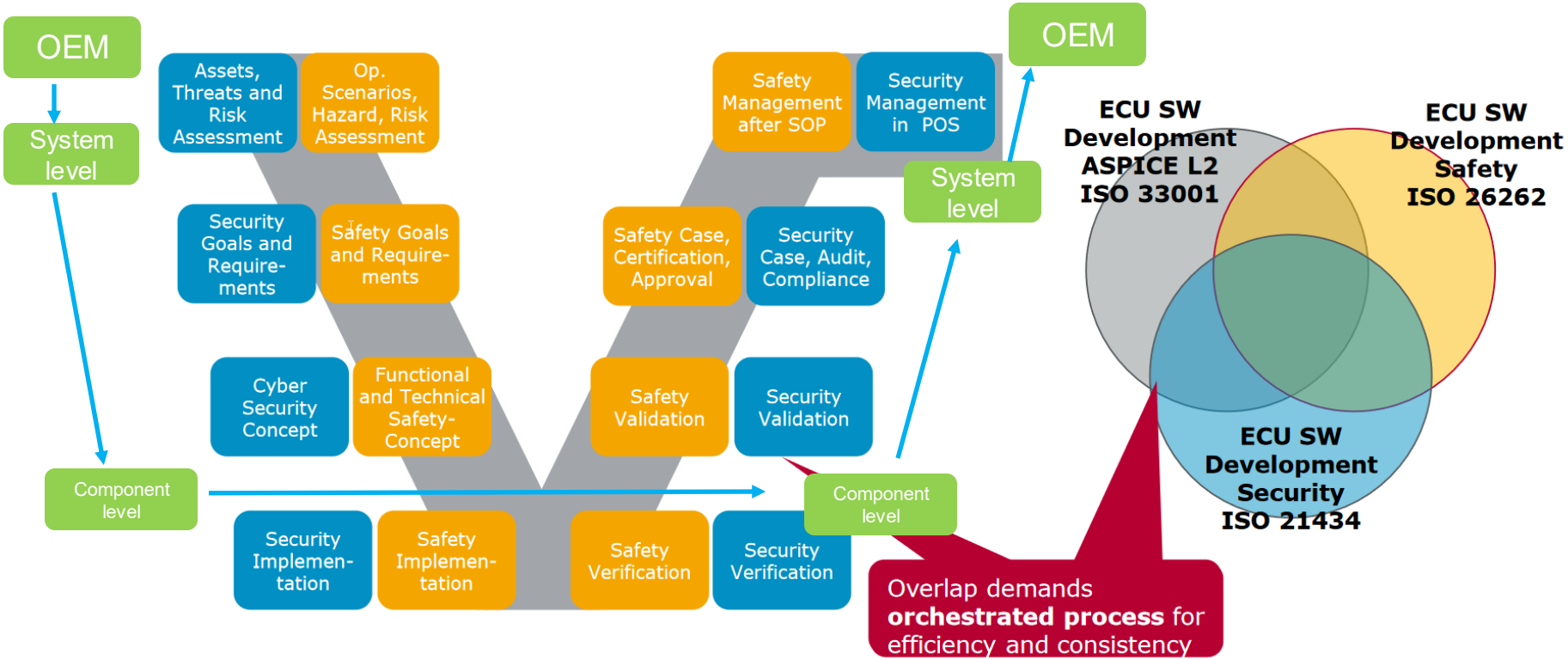
Early detection based on vehicle logs, and rapid response to incidents

***R156***
***Software Update Management System***

Continuous safe updates throughout the vehicle lifecycle


Disclosure or duplication without consent is prohibited

# Product development → Magna Scope




**Safety and Security must be an integrated part of the life-cycle**


Disclosure or duplication without consent is prohibited


Source: Gettyimages

# Summary and Outlook

- Modern vehicle are highly connected with **RF technologies** to communicate
  - V2X (V2V, V2I, V2C…)
  - Mobile Radio
  - Wi-Fi
  - Bluetooth
- **A highly interconnected car offers a wide cybersecurity attack surface**
  - Every **Interface** can have on or more **Vulnerabilities**
  - Remote Functions and many Backend services provide a large attack scale from the traditional **IT world**
  - One CS Incident might have a huge impact
- **Cybersecurity must be considered from the development phase throughout the whole lifespan of the vehicle**
  - UNECE **R155** and **R156** as regulation
  - **ISO21434 as tool to implement CS by design - CSMS**
  - **Continuous CS monitoring** and **SW updates** shall secure the vehicles


Disclosure or duplication without consent is prohibited


Forward.
For all.
MAGNA