AVL Software and Functions GmbH

Challenges of automotive cybersecurity in automated and autonomous vehicles

Kaspersky Industrial Cybersecurity Conference Sochi 2019

Public

AVL- Enterprise Development Automotive

AVL

RESEARCH 10%
of turnover in-house R&D

INNOVATION 1500
granted patents

STAFF
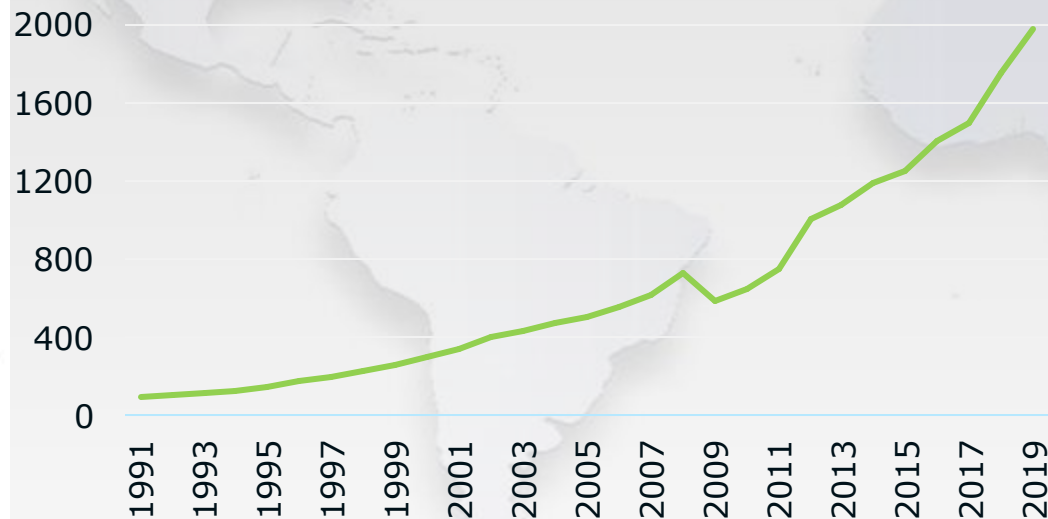
10.400 employees

65% engineers and scientists

GLOBAL FOOTPRINT

45 Affiliates
40 Tech & Engineering Centers
Global customer support network

GROWTH

SALES

1995:
0.15 billion €

2018:
1.75 billion €

Plan 2019:
1.98 billion €

EXPERIENCE
70 years !

5 powertrain elements

ONE
PARTNER

Benefits of the connected car

Autonomous Driving

Remote Diagnostics

Over-the-Air Software Updates

Insurance

V2X Communication

Proactive Service and Maintenance

Remote Driver Assistance

Fleet Management

Example Connected Powertrain
SMART ENERGY MANAGEMENT

CONNECTED POWERTRAINS WITH POWER BRAINS

PREDICTIVE ADAPTIVE CRUISE CONTROL

PREDICTIVE HEV ENERGYMANAGMENT

PREDICTIVE THERMAL MANAGEMENT

PREDICTIVE SHIFTING

COASTING ASSISTENT

ECO ROUTING

TRAFFIC LIGHT ASSISTENT

ADAS/AD HMI

ADAS and AD – a must have in automotive

- **Accident free driving**
active safety functions e.g. emergency braking, lane keeping assistant

- **Driver relief and comfort functions**
e.g. parking assistant, adaptive cruise control

- **Connectivity**
e.g. smart phone interaction, real time traffic information, car2x, cloud computing

- **Fuel/energy efficiency**
e.g. EV driving range, predictive fuel saving

- **Operating cost:** Driver substitution as TCO argument at mainly transport & shared mobility business

high importance

Safety and Security – Common, yet Different

SECURITY
Protect the system against human beings

SAFETY
Protect human beings against the system

Both Safety and Security are companions in the automotive world!

Functional Safety

The Big Picture of Safety

Safety Domains

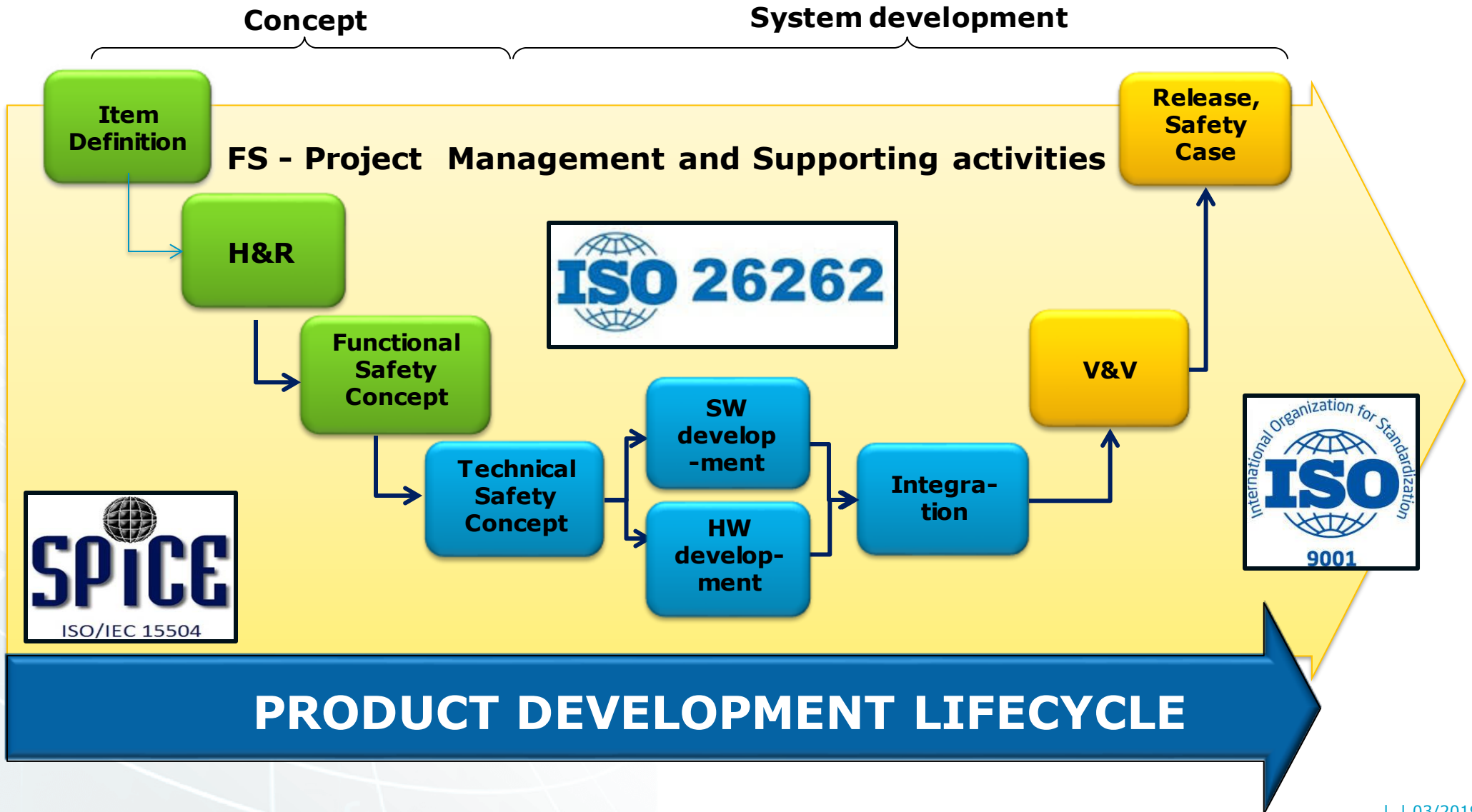| Vehicle safety	Functional Safety	High Voltage (HV)	Safety of Use	Component Safety
Safety shortly before, during and after a crash	**Safety through reliable functions in SW and electronic HW**	**Safety by protecting against high voltage**	**Safety in customer use** (intended / foreseeable abuse)	**Safety by design (mechanical, electrical, chemical,...)**
Turn off the HV-system when it recognizes the crash Airbag protects occupants in case of an crash.	Measures for monitoring and plausibility check of the driver demand against the wheel torque	Avoiding contact with voltage leading parts Measures for monitoring the HV system	Instructions for use and cautionary concepts (engine sign on dashboard. Measures to protect unintended engine starts (Start-Stop)	The mechanism assembly is designed so that the parking pawl tooth collides and overrides the parking gear teeth (ratchets) until a safe engagement speed for the vehicle is reached

International Functional Safety Standards

Development can be safety-related in several industries...

[railway]
EN 5012x
EN 50128

[aerospace]
DO-254
DO-178B

[medical equipment]
IEC 60601

[furnace power plant]
IEC 50156

[process plant]
IEC 61511

[nuclear power]
IEC 60880 - 2

[agriculture earth moving]
ISO 25119
ISO 15998

Functional safety of electrical / electronic / programmable electronic safety-related systems

[automotive]
ISO 26262 1-9

IEC/DIN EN 61508
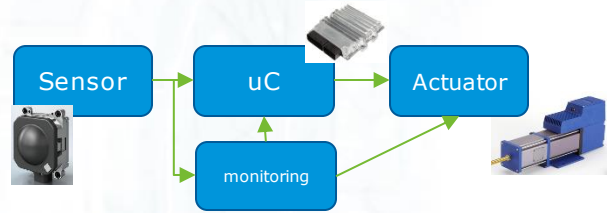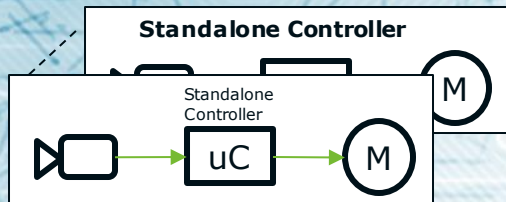
Functional Safety Development Lifecycle

Functional Safety for ADAS/AD systems

Increased system complexity (hardware / intended functionality) & interaction with external environment

Increased number of driving scenarios and hazardous events

Changes in system design due to fallback-strategies & redundancy concepts
FAIL SAFE VS. FAIL OPERATIONAL
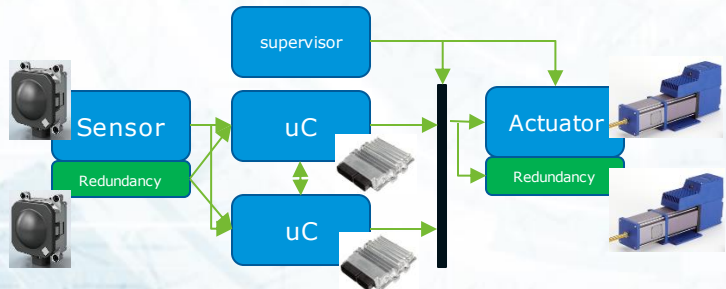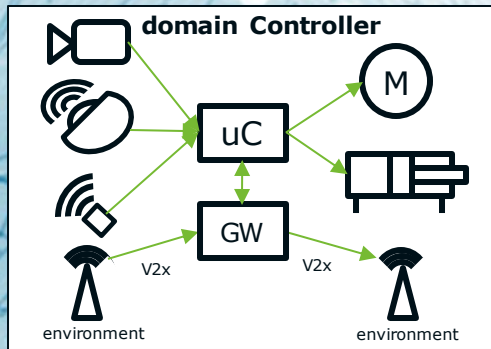
Safety engineering up to ASIL D through the whole development process to meet current & future ADAS/AD requirements

Automotive CyberSecurity

Why Automotive Security?

Why Automotive Security?

Manipulation without direct physical access

Manipulation over direct physical interaction

Loss of Confidentiality

Loss of Integrity

Loss of Availability

Financial Damage

Reputation Damage

Causing Safety Hazards

In addition to the threats in IT Security,

Automotive Cyber Security also has the goal of avoiding safety hazards.

Commonly Used Attack Points

AVL

USB

Mobile Device

Charging Interface

OBD-II

Bluetooth

NFC

Remote Key

WiFi

INTERNAL

EXTERNAL
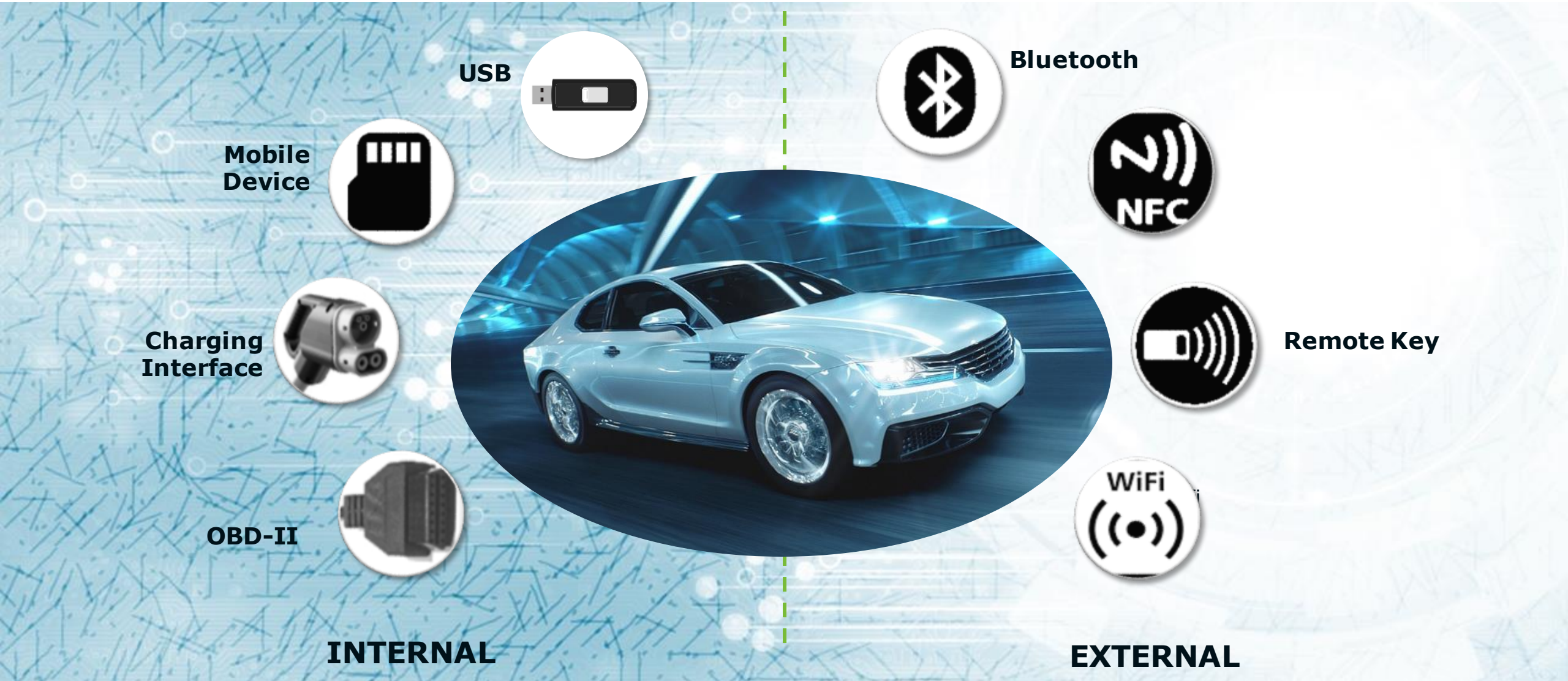
Security threats as subject on safety requirements 1/3

Example 1 – the cooperative highway assistant (vehicle level):

Information about position and speed of vehicle in front/ hijacked V2V message:

Hazard and Risk Analysis must consider:

- unintended loss of braking function

- unintended strong braking without real cause in high speed

Functional and Technical Safety Concepts shall contain measures and mechanisms for detection / avoidance of intrused „faults"

Safety analyses must prove effectiveness of safety concepts including security mechanisms
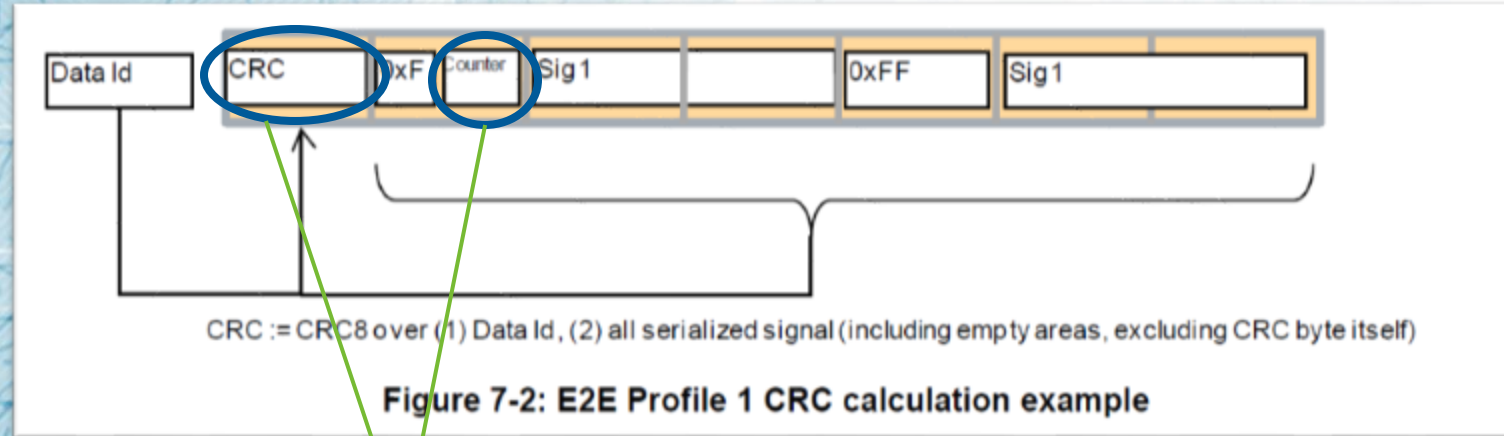

Photo Source: USDOT

Example 2 – the communication monitoring (control system level):

Input variable too low / too high / wrong (COM fault **/ hijacked CAN message:**

| Data Id | CRC | 0xF | Counter | Sig 1 | | 0xFF | Sig 1 | |

CRC := CRC8 over (1) Data Id , (2) all serialized signal (including empty areas, excluding CRC byte itself)

**Figure 7-2: E2E Profile 1 CRC calculation example**

Knowledge about message structure allows to insert corrupted messages (override)

Structure for safety suitable up to ASIL D (DC 99%), but very weak for security

Enhancement to lightweight anomaly detection needed (frequency- /sequency based)

Confidential handling of information about signal structures

Example 3 – the safety monitoring functions (control component level):

Wrong algorithm including wrong calibration (design fault **/ malware flashing**)
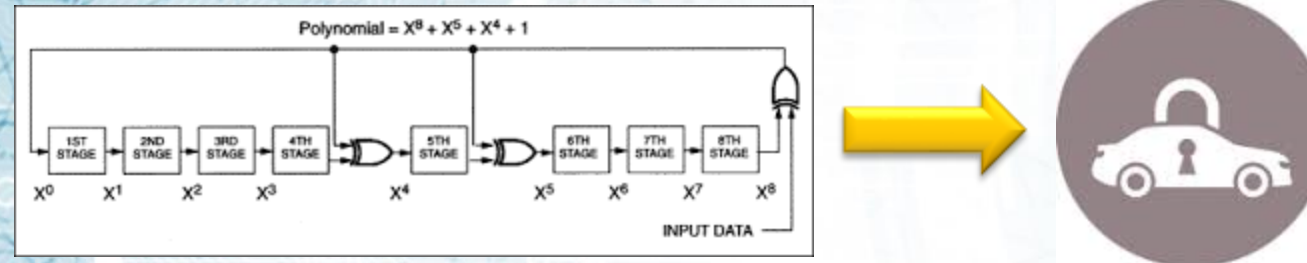
Knowledge about structure of flash integrity check opens the download of changed SW safety functions (e.g deactivated torque monitoring for power tuning)

Secured L2 – ROM key contains all setups of code, data and configuration of safety monitoring

Hamming distance defined in order to meet ROM integrity with ASIL D, but weak for security purposes (low „encription, standard algorithms for CRC)

Authentification and encryption methods needed

Automotive Security Engineering Steps

Security Risk Analyses	Architecture & Concept Development	Security Solutions, Operating Systems and Modules	Security Testing	Continuous System Care
▪ Attacker Models ▪ Threat Analysis ▪ Risk Assessment	▪ Requirements Engineering ▪ Functional Security Concept ▪ Technical Security Concept	▪ Secure Coding and HW Design ▪ Security Mechanisms ▪ Secure Operating Systems and Configurations	▪ Vulnerability Scan & Assessment ▪ Functional Security Testing ▪ Penetration Testing	▪ Vulnerability Database ▪ Variant Management ▪ Incident Response Management ▪ Security Updates

Security Organization, Processes & Risk Management

Partnership of AVL with Kaspersky Lab

AVL SOFTWARE AND FUNCTIONS

- Leading Company in automotive embedded SW
- Various SOP projects
- Deep Functional Safety and Diagnostics Know-how

Sign of contract on 01.06.2017

kaspersky

- Leading Company for IT and Cyber Security
- 270.000 corporate clients worldwide
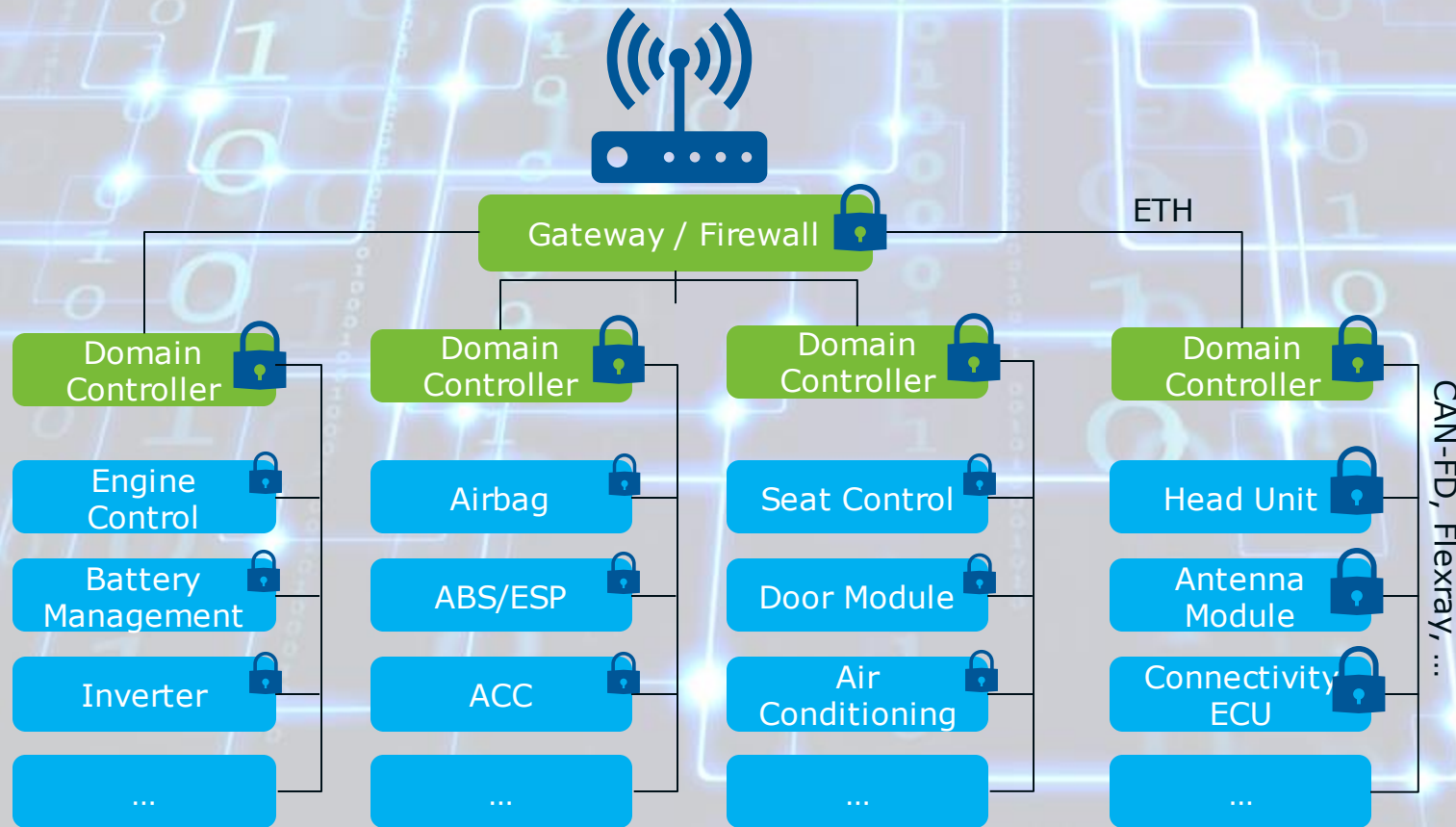- Defending against ~323.000 attacks daily

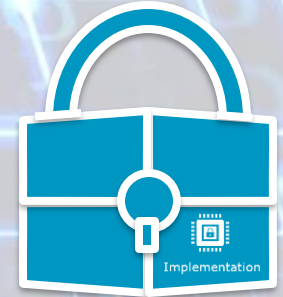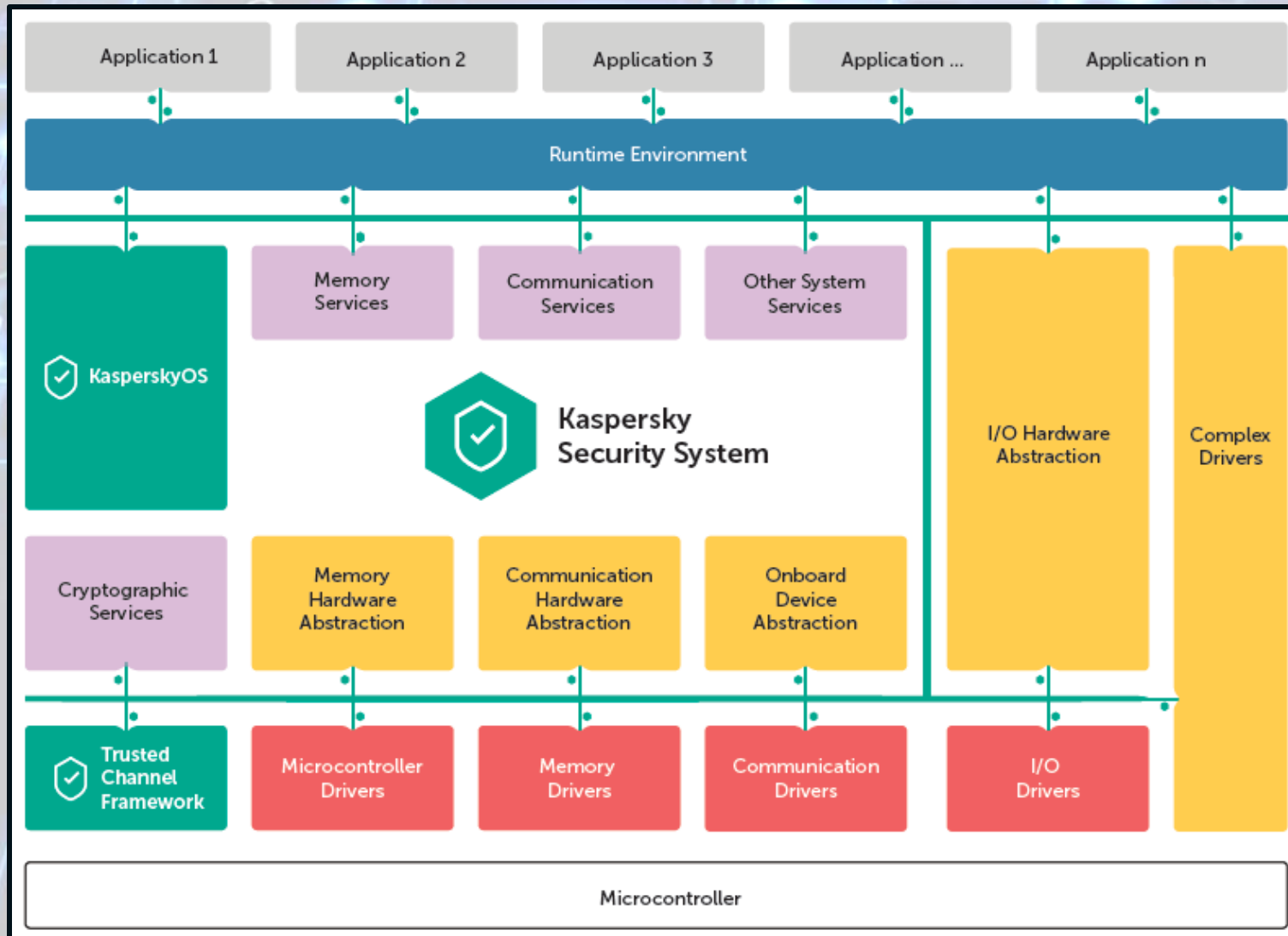| Organization	Detecting Intrusion	Avoiding Intrusion
Software & Security	Encryption	Malware Detection
Degradation / Reconfiguration	Authentication / Autorization	Link to Functional Safety

OEM

Tier 1

Cybersecurity on vehicle level

Development of security-related architecture and allocation of security requirements to the components:

Gateway / Firewall

ETH

Domain Controller

Domain Controller

Domain Controller

Domain Controller

Engine Control	Airbag	Seat Control	Head Unit
Battery Management	ABS/ESP	Door Module	Antenna Module
Inverter	ACC	Air Conditioning	Connectivity ECU
…	…	…	…

CAN-FD, Flexray, …

Security measures on level of operating system

Conclusion ?

- **Vehicle features require connectivity**

- **Vehicle features require safety**

- **Safety, availability and privacy require Security**

- **Security requires solutions**

- **Let's do it !**

Thank You

www.avl.com