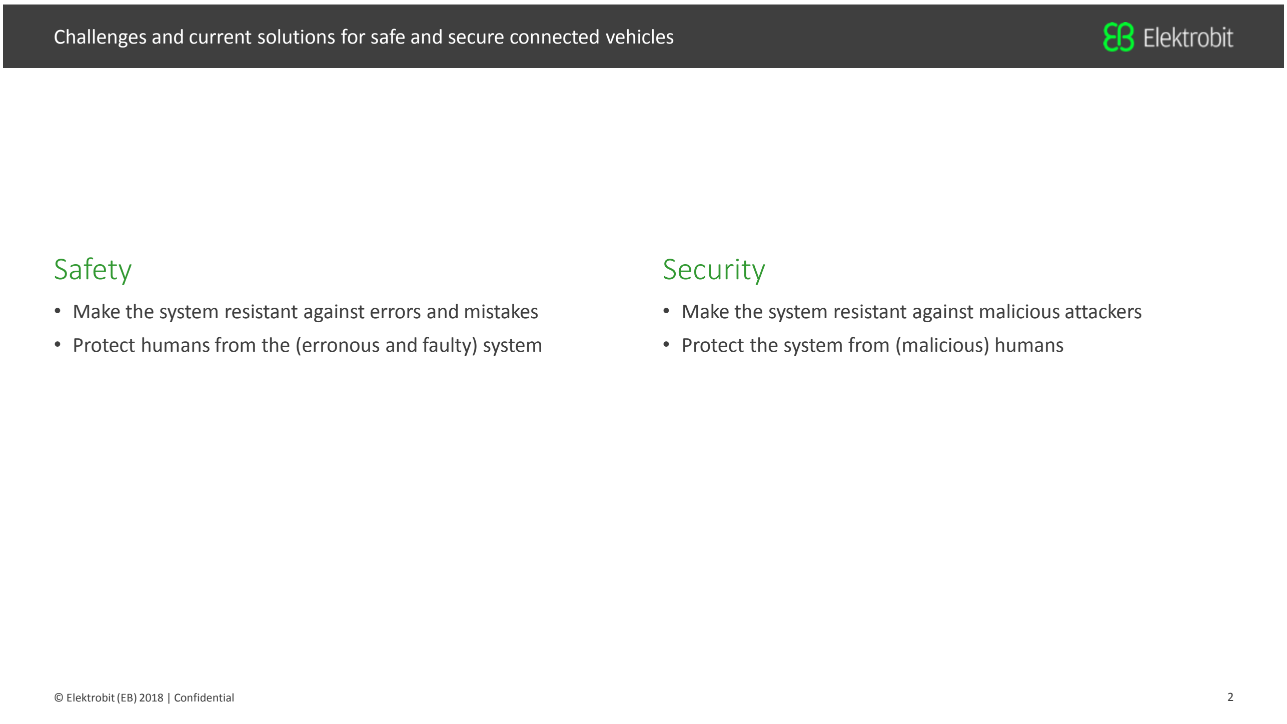
Challenges and current solutions for safe and secure connected vehicles

Dr. Simone Böttger
10. Juli 2018



Challenges and current solutions for safe and secure connected vehicles

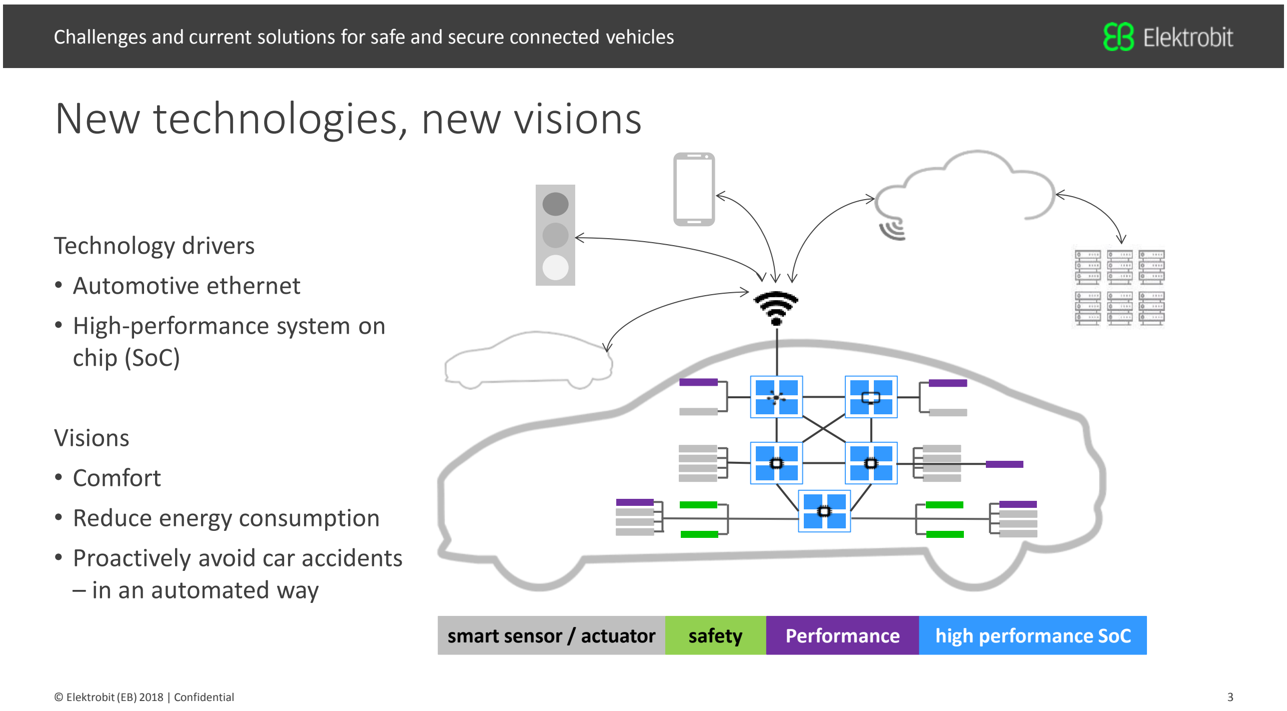
Elektrobit

Safety

- Make the system resistant against errors and mistakes
- Protect humans from the (erronous and faulty) system

Security

- Make the system resistant against malicious attackers
- Protect the system from (malicious) humans



Challenges and current solutions for safe and secure connected vehicles

Elektrobit

New technologies, new visions

Technology drivers

- Automotive ethernet
- High-performance system on chip (SoC)

Visions

- Comfort
- Reduce energy consumption
- Proactively avoid car accidents – in an automated way

smart sensor / actuator	safety	Performance	high performance SoC

© Elektrobit (EB) 2018 | Confidential

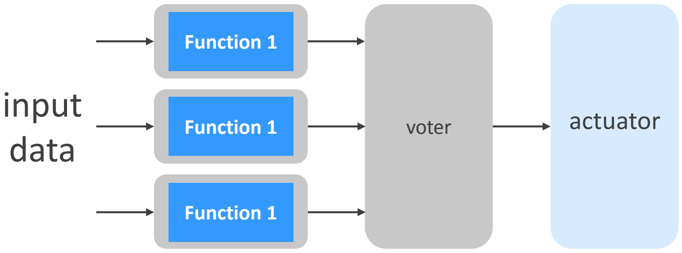
3

Safety

2oo3 architecture

2 out of 3 architecture

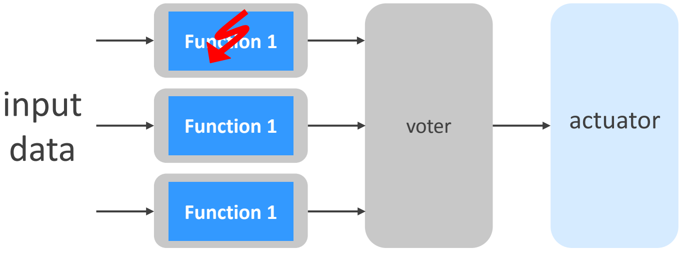
- Triple modular redundancy
- Diversity
- Lower safety requirements on each of the three



2oo3 architecture

2 out of 3 architecture

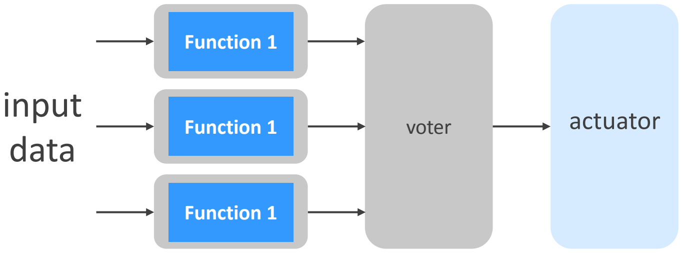
- Triple modular redundancy
- Diversity
- Lower safety requirements on each of the three
- If one of the ECUs fails, the system can still continue with the remaining ECUs
- High safety requirements on the voter



2oo3 architecture

Suboptimal for automotive due to

- More ECUs
- More wiring
- More weight
- More power consumption
- More complexity
- More costs



input data

Function 1

Function 1

Function 1

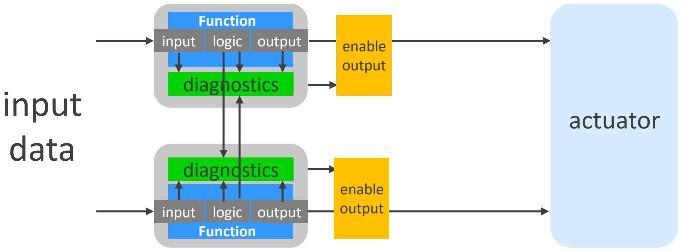
voter

actuator

1oo2D architecture

1 out of 2 with diagnostics

- High diagnostic coverage needed to detect a failure in one channel



input data

Function

input logic output

diagnostics

enable output

diagnostics

input logic output

Function

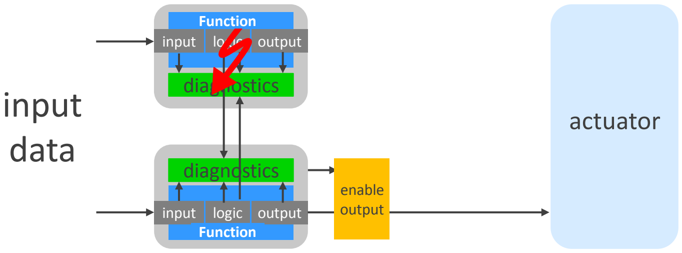
enable output

actuator

1oo2D architecture

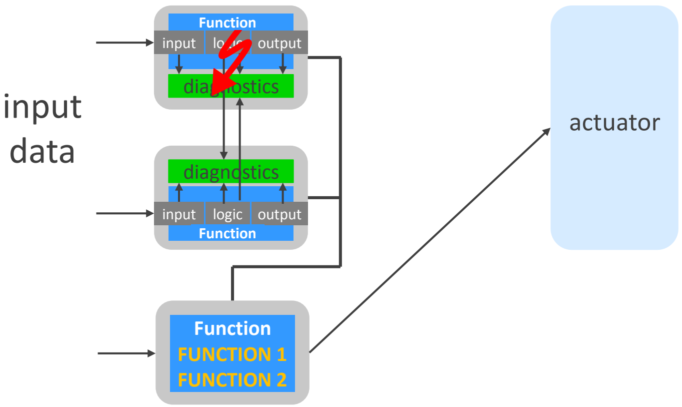
1 out of 2 with diagnostics

- High diagnostic coverage needed to detect a failure in one channel
- If one channel fails in the system, the system continues to operate with the other channel
- Sufficient for a certain period of time



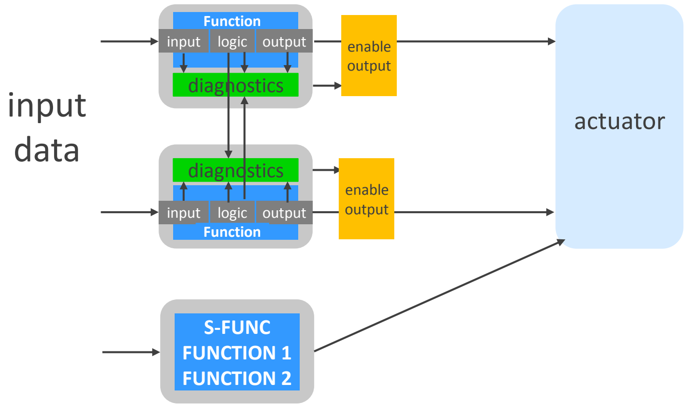
1oo2D architecture with reallocation

- One 1oo2 architecture; both controller running the function
- One controller with same function on “hot-standby” (disabled)
- If one channel fails in the system, the function is dynamically allocated



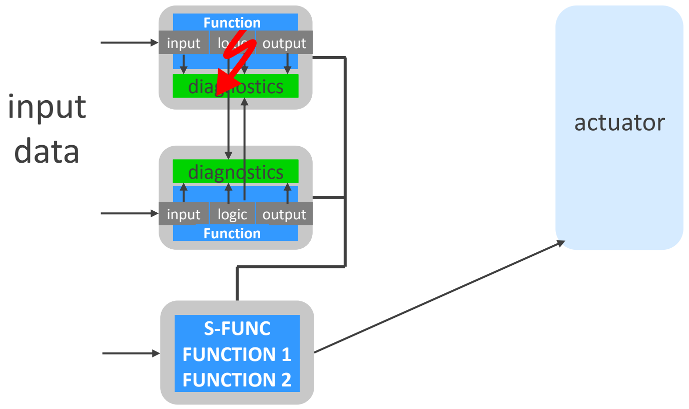
1oo2D architecture with turn to minimum risk maneuver

- One 1oo2 architecture; both controller running the function
- One controller with “minimum risk maneuver” function (S-FUNC) active
- Input of S-FUNC is ignored by the actuator as long as there is no other input



1oo2D architecture with turn to minimum risk maneuver

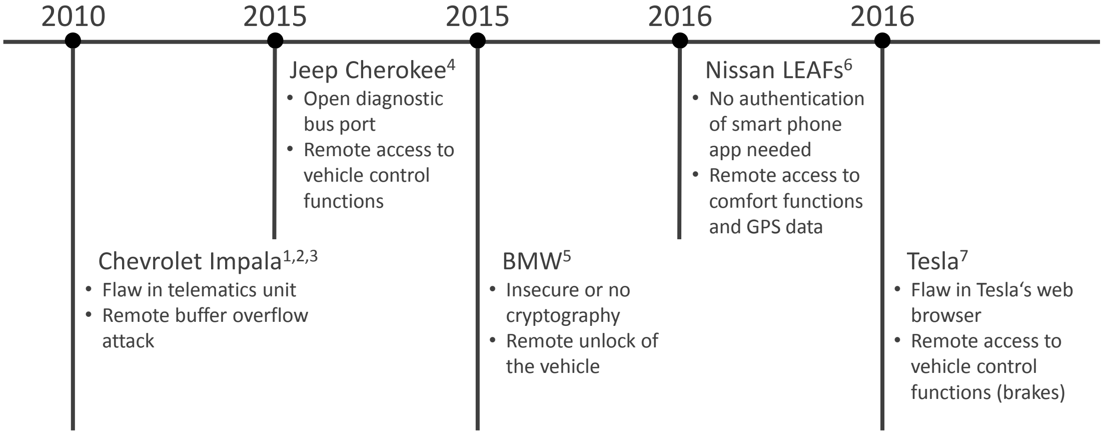
- One 1oo2 architecture; both controller running the function
- One controller with “minimum risk maneuver” function (S-FUNC) active
- Input of S-FUNC is ignored by the actuator as long as there is no other input



Security

Elektrobit

Remote attacks



2010

Chevrolet Impala[1,2,3]

- Flaw in telematics unit
- Remote buffer overflow attack

2015

Jeep Cherokee[4]

- Open diagnostic bus port
- Remote access to vehicle control functions

2015

BMW[5]

- Insecure or no cryptography
- Remote unlock of the vehicle

2016

Nissan LEAFs[6]

- No authentication of smart phone app needed
- Remote access to comfort functions and GPS data

2016

Tesla[7]

- Flaw in Tesla's web browser
- Remote access to vehicle control functions (brakes)

Hardending high performance SoCs

Analyze the system

- Evaluate assets
- Identify threats, risks, and security measures

Limit impact

- Use multiple independent security layers
- Harden each SW layer
- Individualize ECUs – restrict attacks to single ECUs

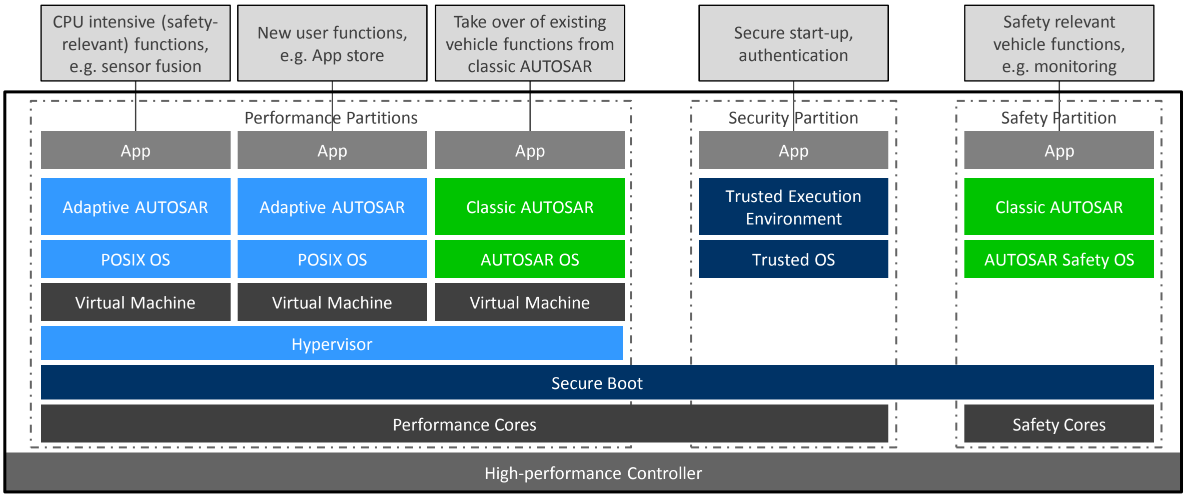
Ensure authenticity

- Use secure boot for all software
- Restrict the users of the signing toolchain

Updating

- Known vulnerabilities will be exploited
- Updates protect against it

High performance SoC architecture



CPU intensive (safety-relevant) functions, e.g. sensor fusion

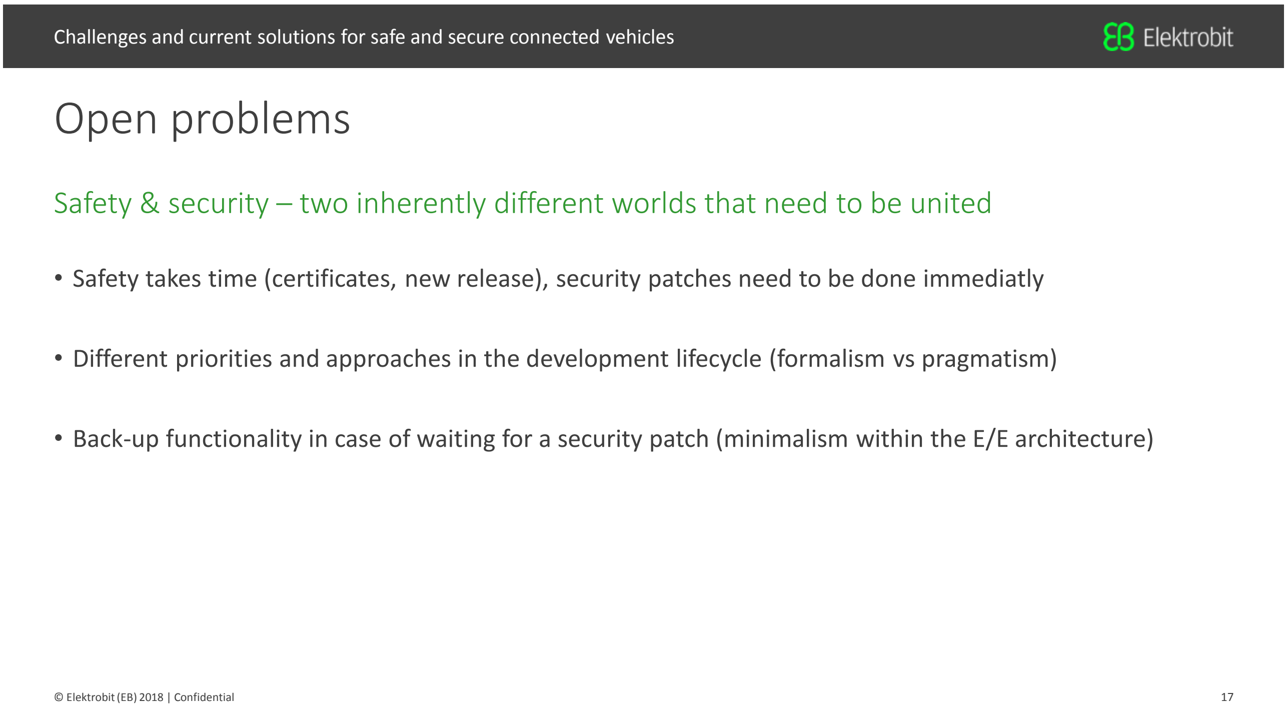
New user functions, e.g. App store

Take over of existing vehicle functions from classic AUTOSAR

Secure start-up, authentication

Safety relevant vehicle functions, e.g. monitoring

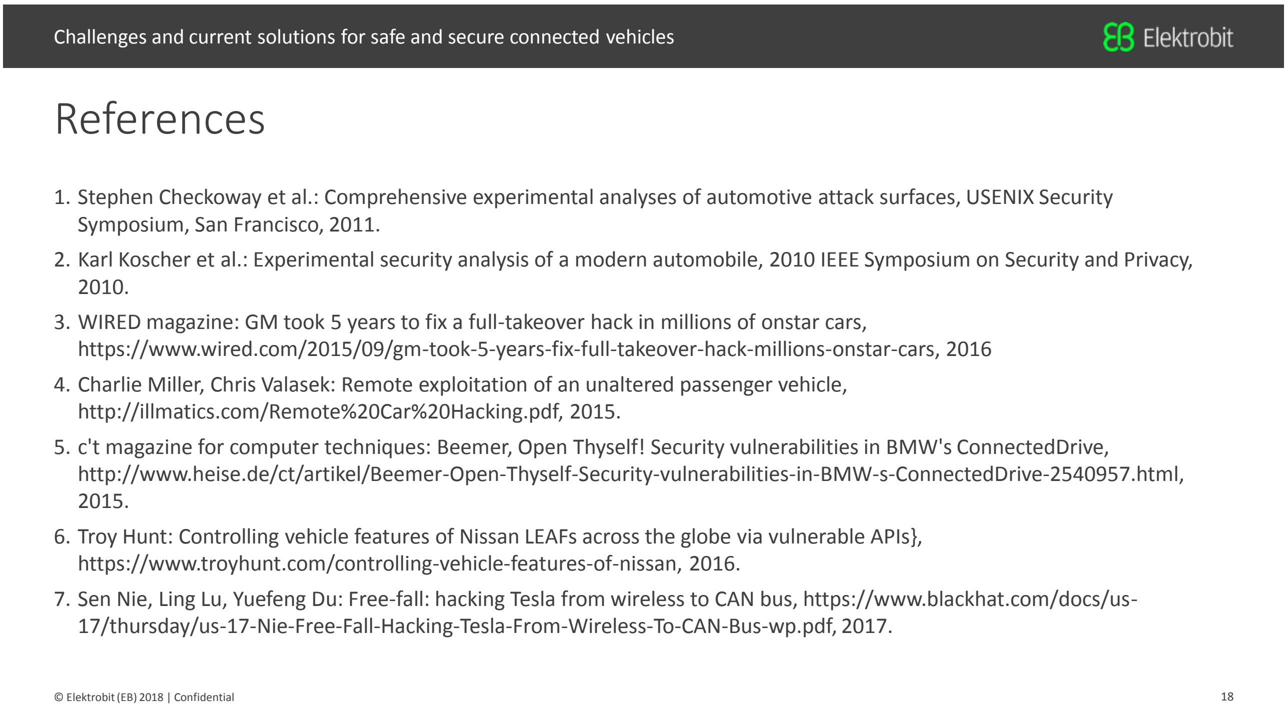
Performance Partitions			Security Partition	Safety Partition
App	App	App	App	App
Adaptive AUTOSAR	Adaptive AUTOSAR	Classic AUTOSAR	Trusted Execution Environment	Classic AUTOSAR
POSIX OS	POSIX OS	AUTOSAR OS	Trusted OS	AUTOSAR Safety OS
Virtual Machine	Virtual Machine	Virtual Machine		
Hypervisor				
Secure Boot				
Performance Cores				Safety Cores
High-performance Controller				



Open problems

Safety & security – two inherently different worlds that need to be united

- Safety takes time (certificates, new release), security patches need to be done immediatly
- Different priorities and approaches in the development lifecycle (formalism vs pragmatism)
- Back-up functionality in case of waiting for a security patch (minimalism within the E/E architecture)



References

1. Stephen Checkoway et al.: Comprehensive experimental analyses of automotive attack surfaces, USENIX Security Symposium, San Francisco, 2011.
2. Karl Koscher et al.: Experimental security analysis of a modern automobile, 2010 IEEE Symposium on Security and Privacy, 2010.
3. WIRED magazine: GM took 5 years to fix a full-takeover hack in millions of onstar cars, https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars, 2016
4. Charlie Miller, Chris Valasek: Remote exploitation of an unaltered passenger vehicle, http://illmatics.com/Remote%20Car%20Hacking.pdf, 2015.
5. c't magazine for computer techniques: Beemer, Open Thyself! Security vulnerabilities in BMW's ConnectedDrive, http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html, 2015.
6. Troy Hunt: Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs}, https://www.troyhunt.com/controlling-vehicle-features-of-nissan, 2016.
7. Sen Nie, Ling Lu, Yuefeng Du: Free-fall: hacking Tesla from wireless to CAN bus, https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf, 2017.

Get in touch!

Elektrobit

sales@elektrobit.com
www.elektrobit.com

Supported by BMWi

PASS

Grant 01MD16002G