

WFCS 2026

Foundational Security From Car to Factory

Friedrich Wiemer
Robert Bosch GmbH
April 23rd, 2026

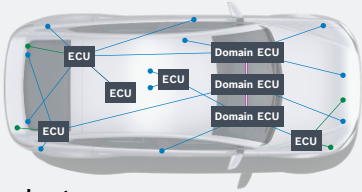
NextCarNet BOSCH

1

Automotive Mega Trends
In-Vehicle Architectures – Decoupling Hardware from Functions

Domain-based Architecture

Ethernet CAN LIN

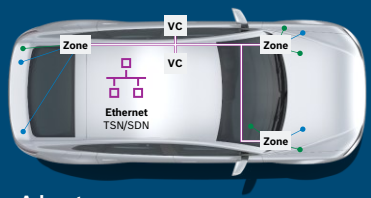


Disadvantages

- Vehicle consists of weakly coupled subsystems (domains)
- Deterministic communications between systems only exceptional with extra effort
- Specific individual solutions and software partitioning
- Limited systematic communication network design

Zonal-based Architecture

Ethernet TSN/SDN CAN LIN



Advantages

- One unified network with common time zone
- Synchronous actions in multiple ECUs with accuracy < 200 ns at vehicle level
- Systematic communication network design with simulation and validation

TSN Time Sensitive Network, **SDN** Software Defined Network, **VC** Vehicle Computer

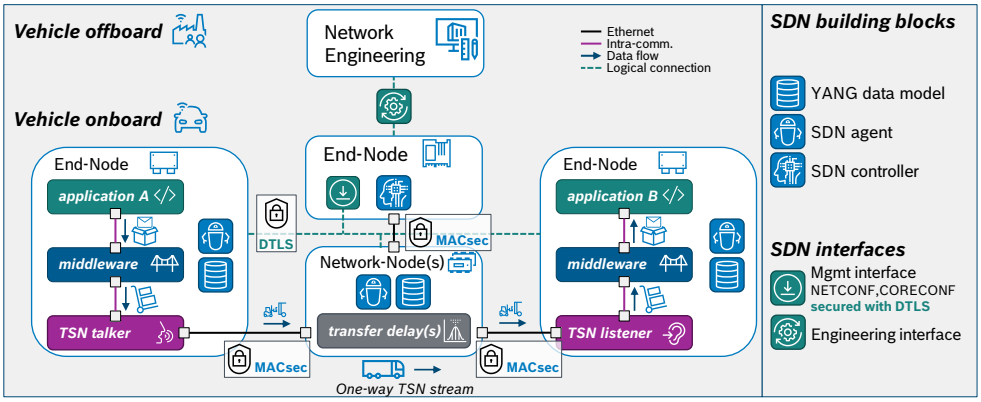
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

2

SDV to SDN: Connecting the dots
Automotive SDN Interfaces

SDN: Software Defined Network
SDV: Software Defined Vehicle
TSN: Time Sensitive Networks
YANG: YANG Data Modeling Language



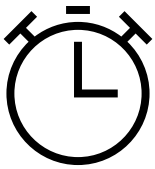
SDV decouples functions from ECU – SDN decouples communication from wiring.

XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

3

Introduction
Foundational requirements



Hard real-time behavior



Safety critical



Immediate start up



Updateability

... and Security:

UNECE r155

ISO/SAE 21434

IEC 62443

Cyber Resilience Act



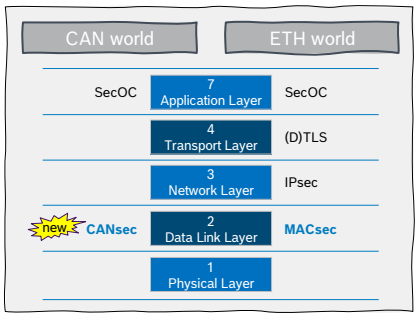
XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

4

Introduction
How to protect communication

Communication and security protocols

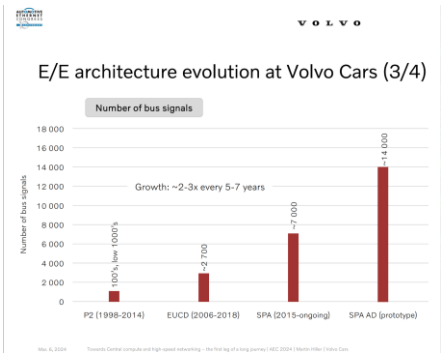


Typical Automotive Protocols

Signal PDUs, DoIP, XCP, ...

TCP, UDP

IP, 1722, gPTP



Secure the layer, not the signal.

XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

5

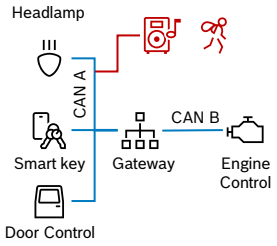
Secure Communication for In-Vehicle Networks
Real World Benefits





https://kentindell.github.io/2023/04/03/can-injection/

What went wrong?



Tindell: "The proper solution to a CAN Injection attack is to adopt a *Zero Trust* approach to CAN."

XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

6

02

01 Software Defined Vehicles and Networks
02 Foundational Security: MACsec
03 Shared Medium Key Agreements
04 Foundational Security Beyond Ethernet
05 Summary and Conclusion

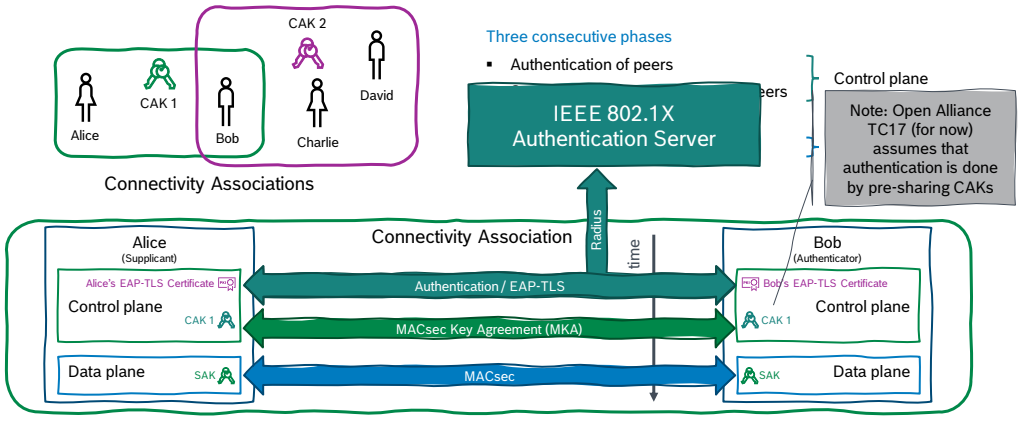
A Foundational Security Layer:
MACsec

... Ethernet's answer to CAN injections since 2006

NextCarNet BOSCH

7

A Foundational Security Layer
MACsec's Communication Architecture

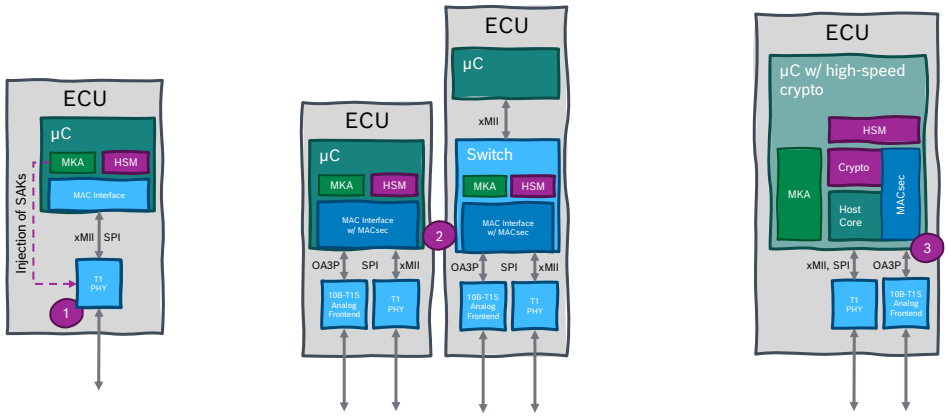


XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

8

A Foundational Security Layer
MACsec in Electronic Control Units



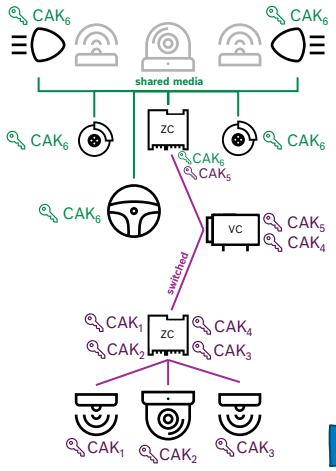
XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

9

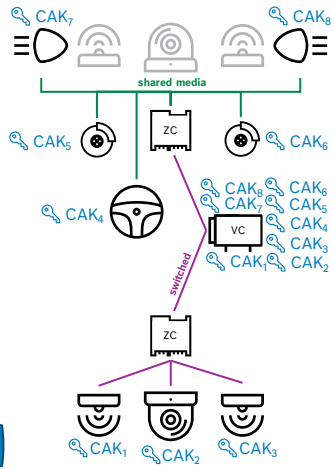
CAK Secure Connectivity Association Key

A Foundational Security Layer
MACsec in the Vehicle – Hop-to-Hop vs. End-to-End



- Keys are all symmetric
- Increasing the number of communication relationships thus increases the number of to be handled keys drastically
- As the keys have to be handled in HW implementation of MACsec, this gets expensive quite fast

Preferred deployment: Hop-to-Hop



XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

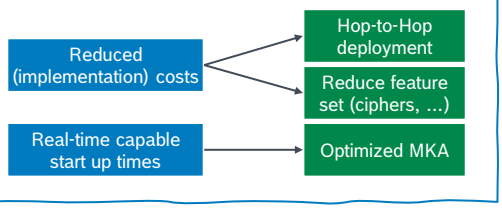
NextCarNet BOSCH

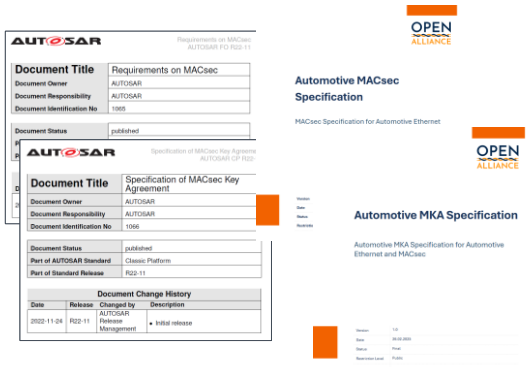
10

A Foundational Security Layer
Open Alliance TC17: Automotive Profile for MACsec

- Automotive relevant MACsec specifications
  - IEEE 802.1AE-2018
  - IEEE 802.1X-2020
  - OPEN Alliance TC17 profile specifications
  - AUTOSAR MACsec concept

Main Challenges in Automotive Adoption





https://www.autosar.org/fileadmin/standards/R22-11/FO/AUTOSAR_RS_MACsec.pdf
https://www.autosar.org/fileadmin/standards/R22-11/CP/AUTOSAR_SWS_MACsecKeyAgreement.pdf
https://opensig.org/wp-content/uploads/2025/05/Automotive-MACsec-Specification-v1.0.pdf
https://opensig.org/wp-content/uploads/2025/03/OA_MACsec_Automotive-MKA-v1.pdf

XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

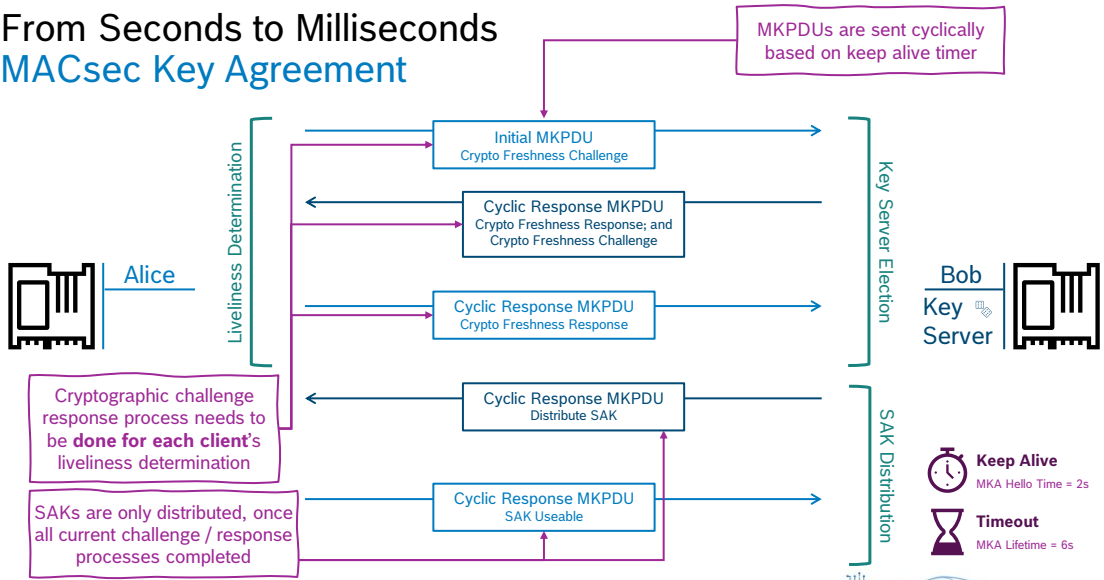
03

01 Software Defined Vehicles and Networks
02 Foundational Security: MACsec
03 Shared Medium Key Agreements
04 Foundational Security Beyond Ethernet
05 Summary and Conclusion

From Seconds down to Milliseconds
Automotive MACsec Key Agreement
... on all the links!

NextCarNet BOSCH

From Seconds to Milliseconds
MACsec Key Agreement



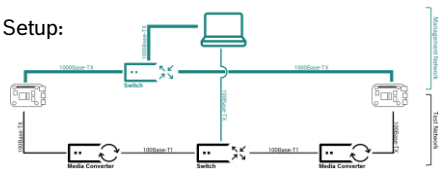
XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

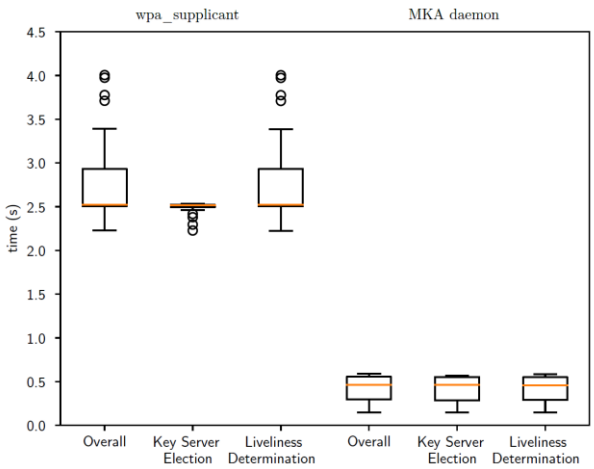
NextCarNet BOSCH

13

From Seconds down to Milliseconds
Raspberry Pi Measurements – Linux MKA implementation

- wpa_supplicant:
  - https://w1.fi/wpa_supplicant/
  - Implements IEEE 802.1X MKA and more
- MKA daemon:
  - https://github.com/Technica-Engineering/MKAdaemon
  - Open-Source implementation of Open Alliance AutoMKA v1 optimizations
- Setup:



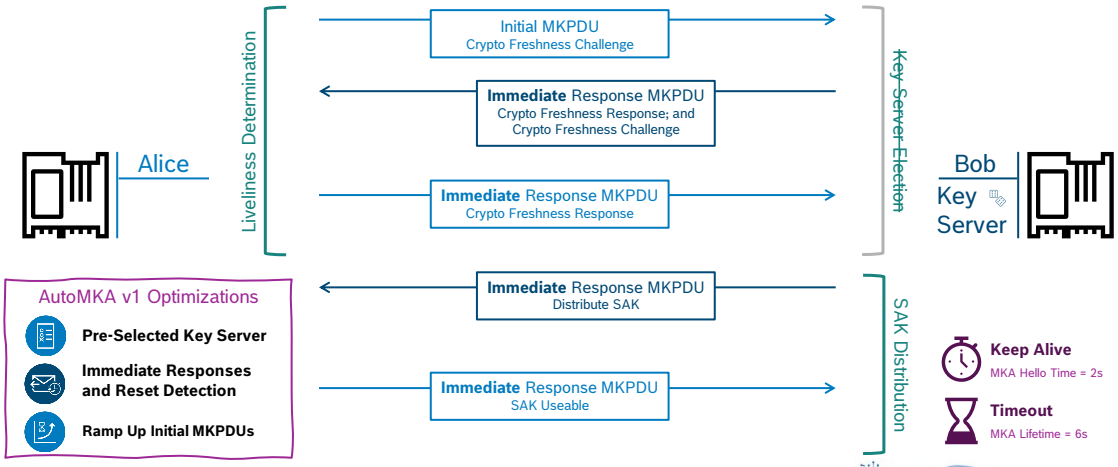


XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

14

From Seconds to Milliseconds
MACsec Key Agreement



© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

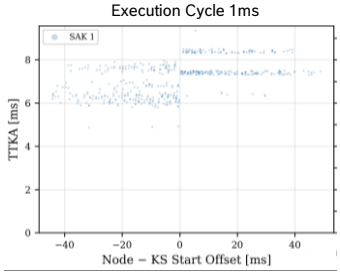
NextCarNet BOSCH

15

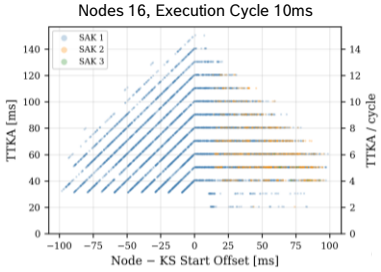
From Seconds to Milliseconds
Simulations for two peers and shared medium

Extensive simulations in RTaW's PEGaSE with varying parameters for Time-To-Key-Agreement

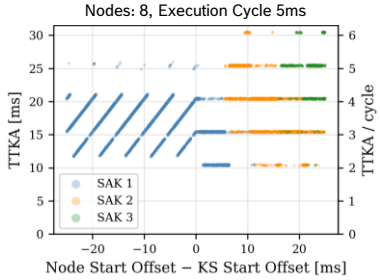
Hop-2-Hop
Execution Cycle 1ms



Shared Medium (AutoMKA v1)
Nodes 16, Execution Cycle 10ms



Shared Medium (new optimizations)
Nodes: 8, Execution Cycle 5ms



In switched hop-to-hop configurations: TTKAs < 10ms are achievable.

TTKA depends on no. of nodes, execution cycle and start offset distribution.

TTKAs for AutoMKA v2 below 100ms should be realistic.

© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

16

04

01 Software Defined Vehicles and Networks
02 Foundational Security: MACsec
03 Shared Medium Key Agreements
04 Foundational Security Beyond Ethernet
05 Summary and Conclusion

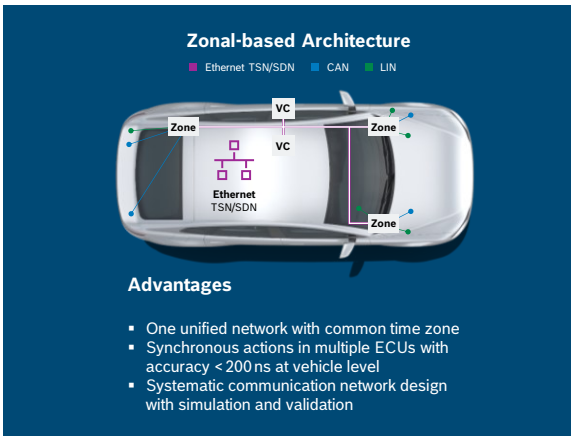
Foundational Security Beyond Ethernet
CANsec and FDAL

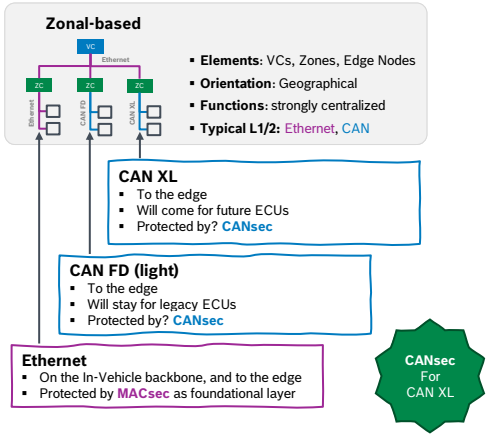
... CAN's answer to CAN injections since 2026

BOSCH

17

Foundational Security Beyond Ethernet
Future E/E Architecture's Communication Network





XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

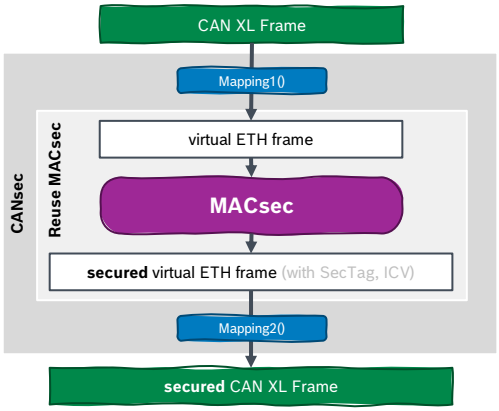
18

Foundational Security Beyond Ethernet
CANsec Strategy

Strategy

Reuse MACsec

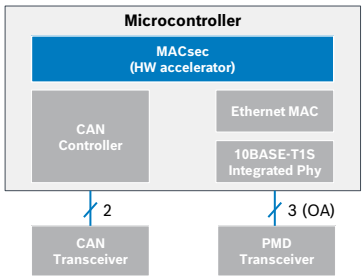
Reuse MKA



© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
BOSCH

Foundational Security Beyond Ethernet
Reuse MACsec – Advantages

- **No discussion needed**
  whether ETH or CAN security is better ➔ it is the same!
- **Mature**
  because MACsec is mature
- **Short time to market**
  MACsec implementations need to be only slightly extended
- **Share implementation between CAN and ETH,**
  CAN & ETH can use the same hardware accelerator on MCU



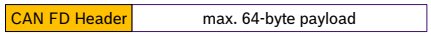
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
OA: Open Alliance
BOSCH

Foundational Security Beyond Ethernet
CANsec for CAN FD

What about CAN FD – CAN it use CANsec, too?

CAN FD Protocol Limitations Today

- Payload length max. 64 byte



- Indication, if CANsec was applied to the frame (yes/no) (= no EtherType)

Strategy

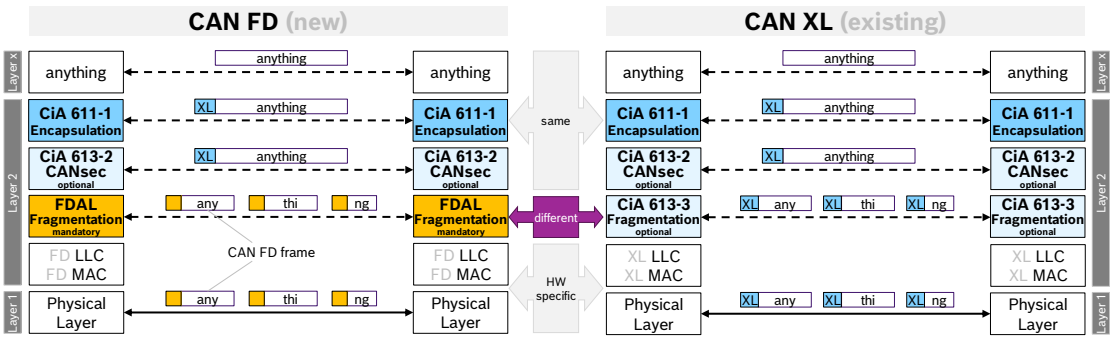
A) Overcome payload limitations with FDAL

B) Reuse existing CANsec for CAN XL

© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
FDAL: CAN FD Adaptation Layer
BOSCH

21

Foundational Security Beyond Ethernet
Protocol Stack CAN FD vs. CAN XL



Key property: Similar stack in FD and XL!

© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
FDAL: CAN FD Adaptation Layer
BOSCH

22

05

01 Software Defined Vehicles and Networks
02 Foundational Security: MACsec
03 Shared Medium Key Agreements
04 Foundational Security Beyond Ethernet
05 Summary and Conclusion

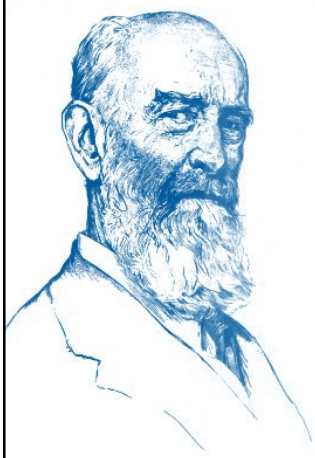
One Layer, Every Wire

... from car to factory

NextCarNet BOSCH

23

One Layer, Every Wire
Questions? Feedback?



"One layer to secure them all,
One profile to bind them"



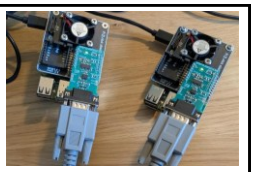
—Robert Bosch (probably)

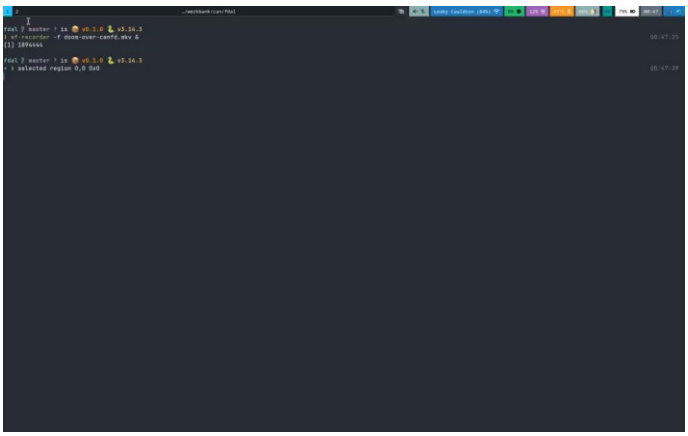
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

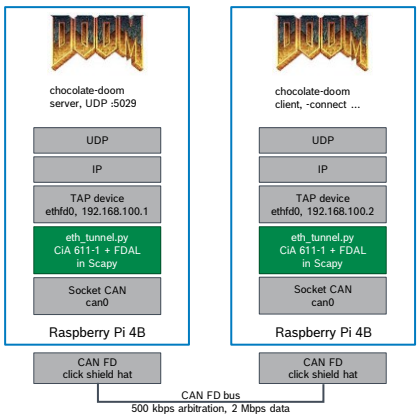
NextCarNet BOSCH

24

One Layer, Every Wire
… but does it run Doom?





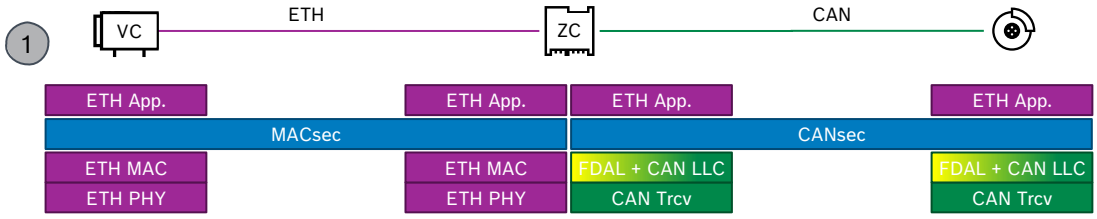


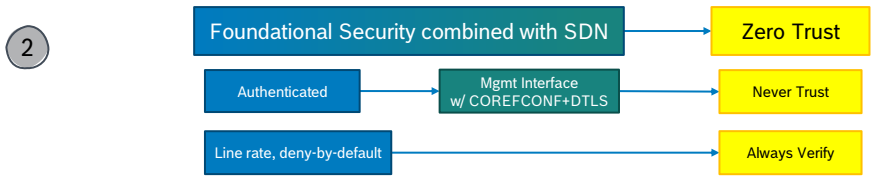
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

25

One Layer, Every Wire
A unified stack: strong foundational security and zero trust





© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH

26

Wrap up
Questions?

IPCEI Microelectronics and Communication Technologies



"One layer to secure them all,
One profile to bind them"

—Robert Bosch (probably)



Funded by the European Union NextGenerationEU

Supported by: Federal Ministry for Economic Affairs and Energy on the basis of a decision by the German Bundestag

Baden-Württemberg MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

SACHSEN

Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

The IPCEI ME/CT project is supported by the Federal Ministry for Economic Affairs and Energy on the basis of a decision by the German Parliament, by the Ministry for Economic Affairs, Labor and Tourism of Baden-Württemberg based on a decision of the State Parliament of Baden-Württemberg, the Free State of Saxony on the basis of the budget adopted by the Saxon State Parliament, the Bavarian State Ministry for Economic Affairs, Regional Development and Energy and financed by the European Union - NextGenerationEU.

XC-CE/ESS3 | 2026-04-23
© Robert Bosch GmbH 2025. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

NextCarNet BOSCH