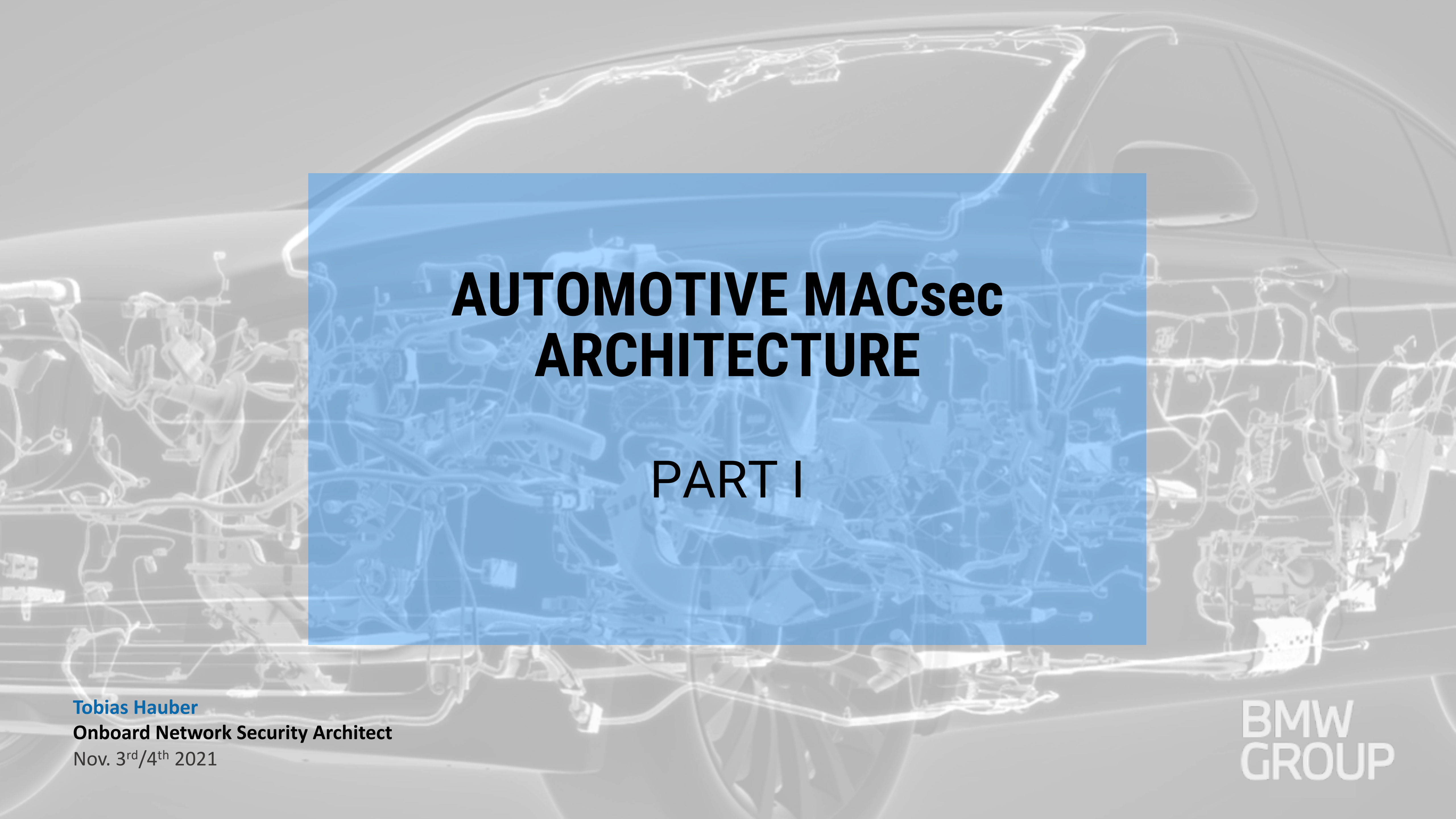
BMW GROUP technica engineering

AUTOMOTIVE MACSEC ARCHITECTURE

Tobias Hauber & Dr. Lars Völker

Nov. 3rd/4th 2021



AUTOMOTIVE MACsec ARCHITECTURE

PART I

Tobias Hauber
Onboard Network Security Architect
Nov. 3rd/4th 2021

BMW GROUP

INCREASING FUNCTIONAL DEMANDS…

Electronic Injection
Electronic Ignition
Check Control
Cruise Control
Central Locking
…

1970

Electronic Transmission Control
Electronic Climate Control
ASC Anti Slip Control
ABS Anti Lock Breaking System
Telephone
Seat Heating
Automated Mirror
…

1980

Navigation System
CD Changer
Bus Systems
ACC Active Cruise Control
Airbags
Dynamic Stability Control
Adaptive Transmission Control
Roll stabilization
Xenon Light
BMW Assist
RDS/TMC
Emergency Call
Servotronic
Electr. Dampener control
OBD
…

1990

Brake Force Displ
Adapt. Light Ctrl
Telematics
Online Services
Bluetooth
Car Office
Local Hazard Integrated Safety Systems
i-Drive
LH2
Personalization
SW-Bugfixing
AFS, Head Up Display,
Car Comm.Comp,
Efficient Dynamics
…

2000

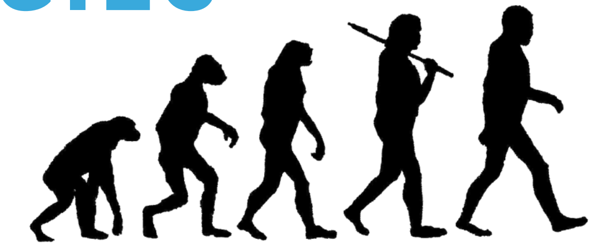
ACC Stop&Go
Internet Portal
Telematics
Online Services
Car Office.
Speed Limit Info
Sideview-Camera
Lane Assist
3D Navigation with variable POI
Infot. Features
Engine Start-Stop
Intelligent Generator Control
Diagnostics Strategy
New Logistics
…

2010

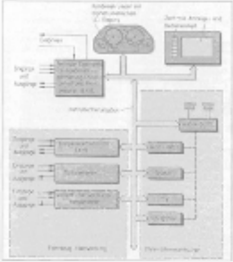
Electric Drivetrain
Automated Driving
Digitalization / Connectivity
Integration Customer Eco Systems
CarSharing
Remote-SW-Upgrade
Digital After Sales
Pay-per-use- systems
Online Services
Ad-hoc-Connecticity
LED-Light
Personal Radio
Preventive Diagnostics
Field Data
…

2020

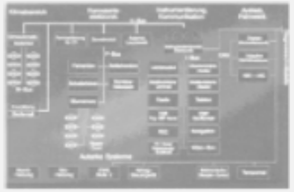
…LEAD TO A PROLIFERATION OF NETWORKING TECHNOLOGIES



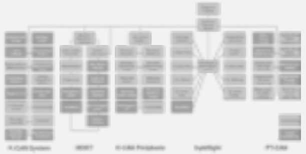
1986



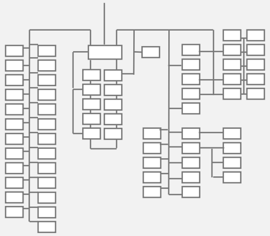
1994



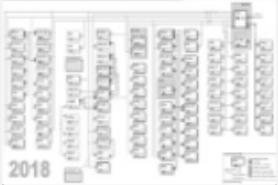
2000



2009



2018/2021



Next Gen

?

AUTOMOTIVE ETHERNET IS WELL-SUITED FOR ALMOST ALL ONBOARD USE CASES: “THE IP FAMILY IS GROWING”

Security is an expected quality for customers and of central importance to (emerging) legal regulation.

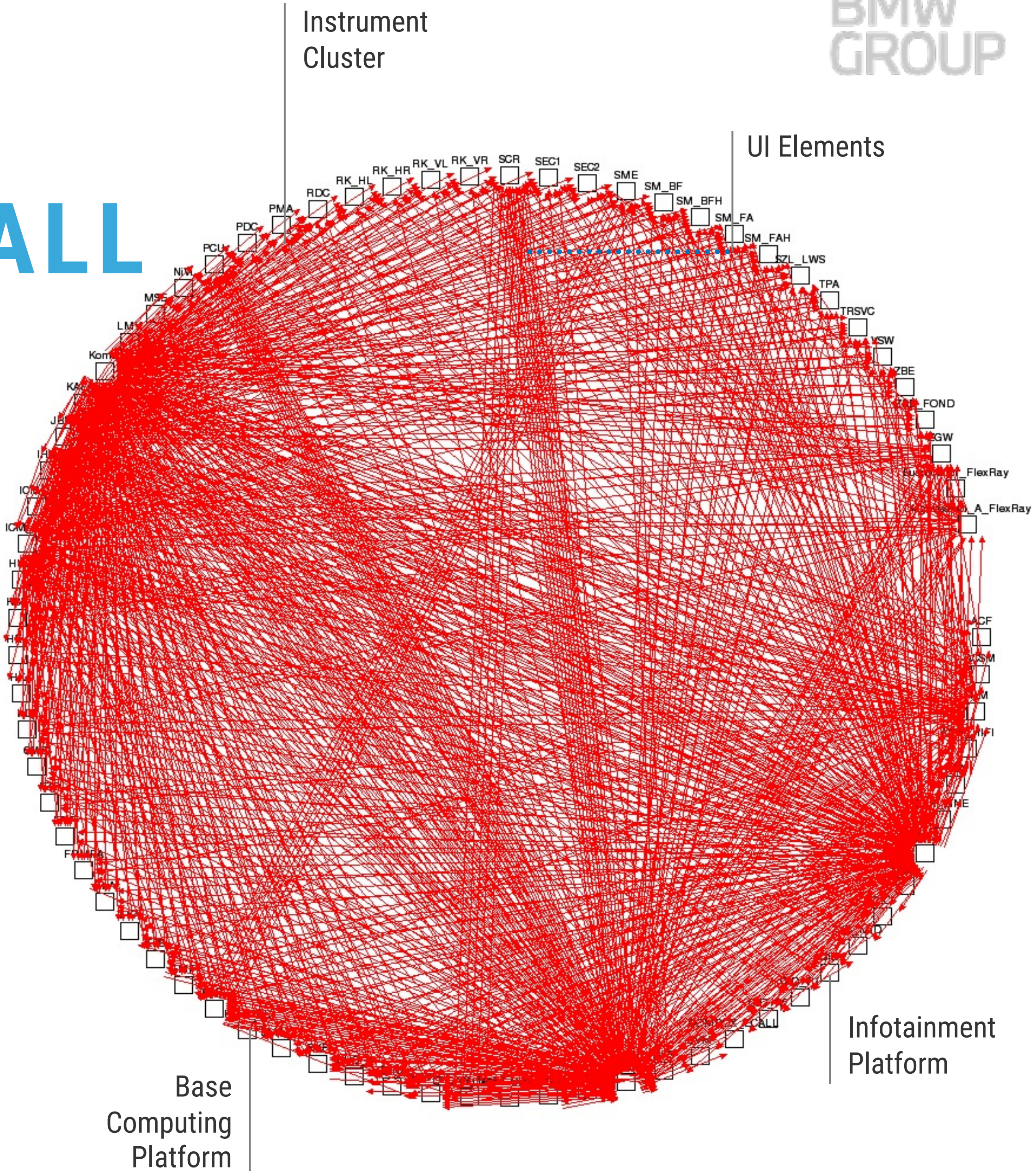
Infotainment

Driver Assistance / Autonomous Driving

Service- and Network-oriented Architecture

Traditional Onboard Communication

END-2-END SECURITY MECHANISMS HIT A WALL



Scalability problems exist in particular for complex communication patterns and higher layers.

Function-oriented Security mechanisms are where we came from:

- Every individual risk analysis leads to individual mitigations
- SecOC, (D)TLS, and IPsec all offer dedicated protection

Is it time to push security to the „expected quality“ of protecting **all** onboard communication?

NEXT GENERATION ARCHITECTURE (1)

BMW components with competitive advantages

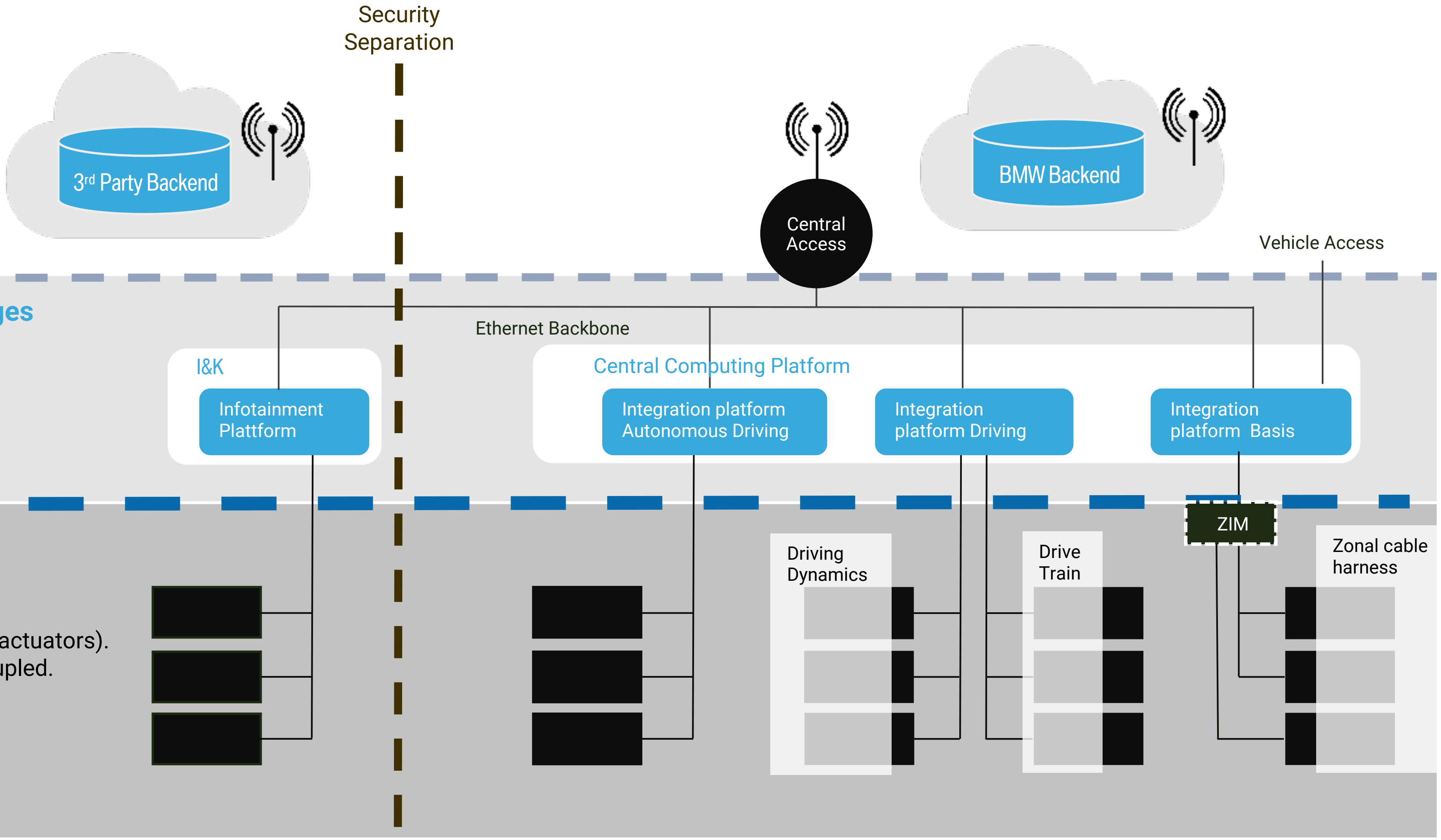
High performance compute with Ethernet backbone:

- Functionality with global knowledge
- Fast updates, updates over long time
- Software driven
- “Fast” changing

Rolling Chassis

Commodity ECUs with clear function domain architecture and service architecture.

- Functionality with local knowledge (smart sensors, actuators).
- Vehicle architecture specifics / mechatronically coupled.
- Specific solutions (cost and function).
- Less or different need for updateability.
- “Slow” changing.
- High validation effort.
- Zonal and modular physical cable hardness.



NEXT GENERATION ARCHITECTURE (2)

Let‘s protect 100% of
traffic in here!

BMW components with competitive advantages

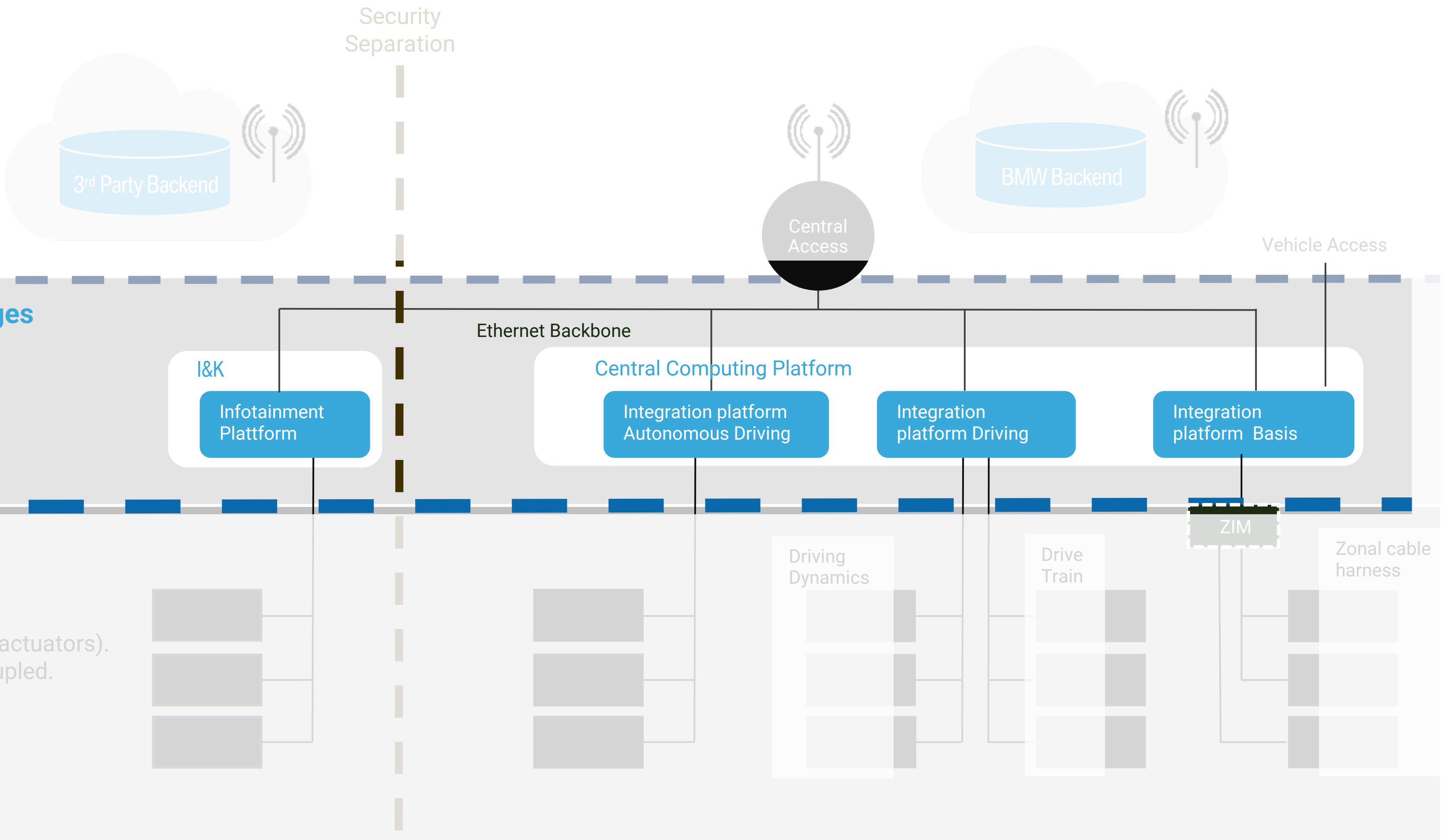
High performance compute with Ethernet backbone:

- Functionality with global knowledge
- Fast updates, updates over long time
- Software driven
- “Fast” changing

Rolling Chassis

Commodity ECUs with clear function domain architecture and service architecture.

- Functionality with local knowledge (smart sensors, actuators).
- Vehicle architecture specifics / mechatronically coupled.
- Specific solutions (cost and function).
- Less or different need for updateability.
- “Slow” changing.
- High validation effort.
- Zonal and modular physical cable hardness.



CRITICAL RUNTIME REQUIREMENTS

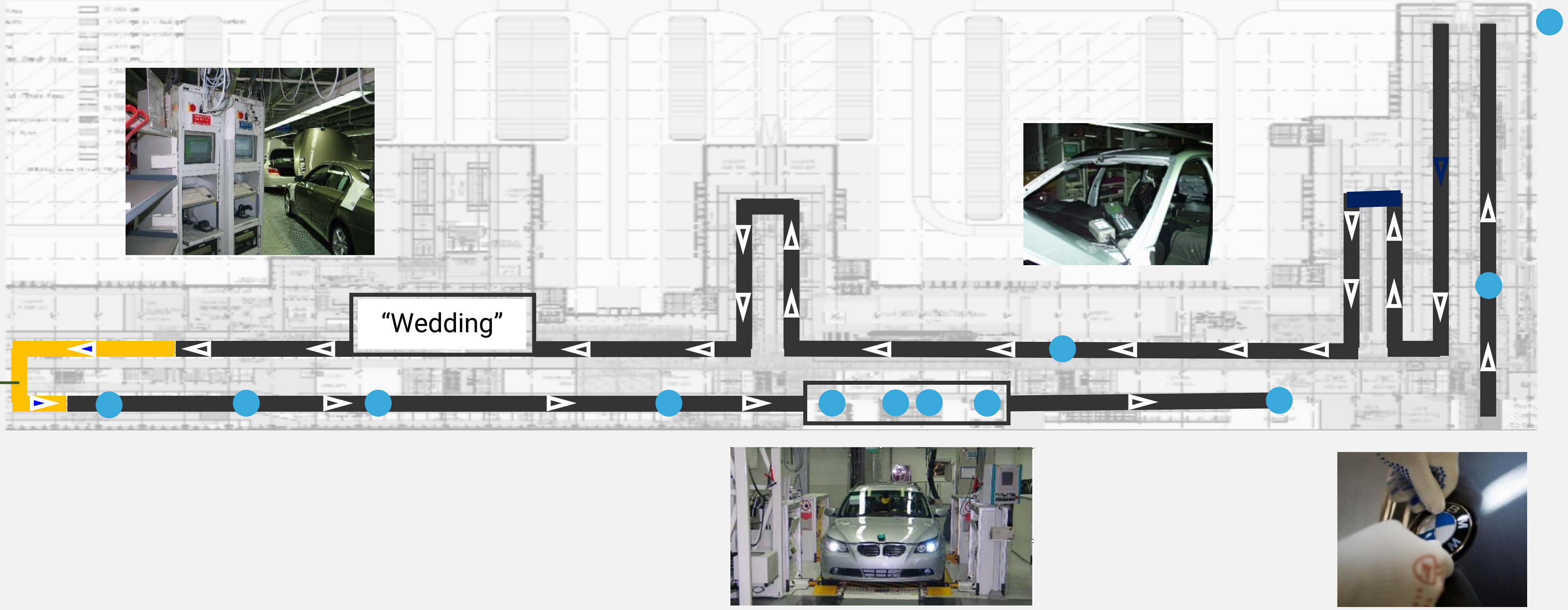
Go for the fastest possible startup times (e.g., < 100ms)!

Plan for the car electronics to constantly going to sleep and to wake up!

Make your solution scale for large networks with high connectivity!

BUT WAIT! MANUFACTURING IS INCREASINGLY BECOMING ONLINE: A “NETWORK INSTALLATION AND CONFIGURATION” CHALLENGE ON THE CLOCK

ECUs are powered on for < 10 minutes, do your thing here!



REQUIREMENTS TO SUPPORT PRODUCTION AND SERVICE

Build the secure networks fully automated!

Have processes and systems robust and distributed!

Design for an untrusted production environment!

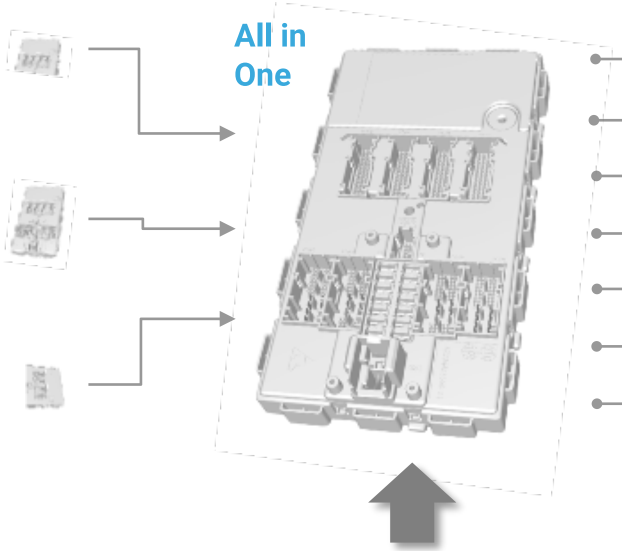
DEFENSE IN DEPTH IS NEEDED AGAINST ALL POSSIBLE ATTACK VECTORS

3000 Coding parameters

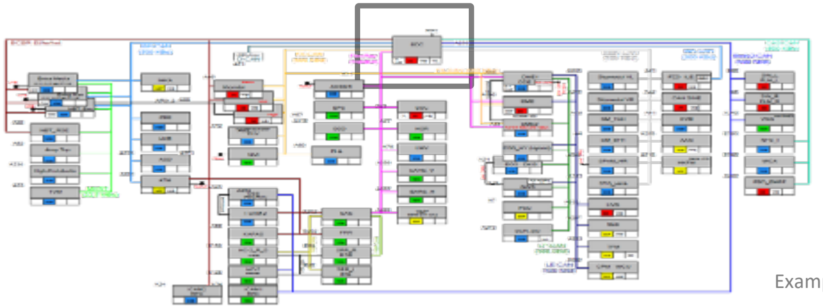
2,4 Mio. Lines of Code

310 Pins to harness

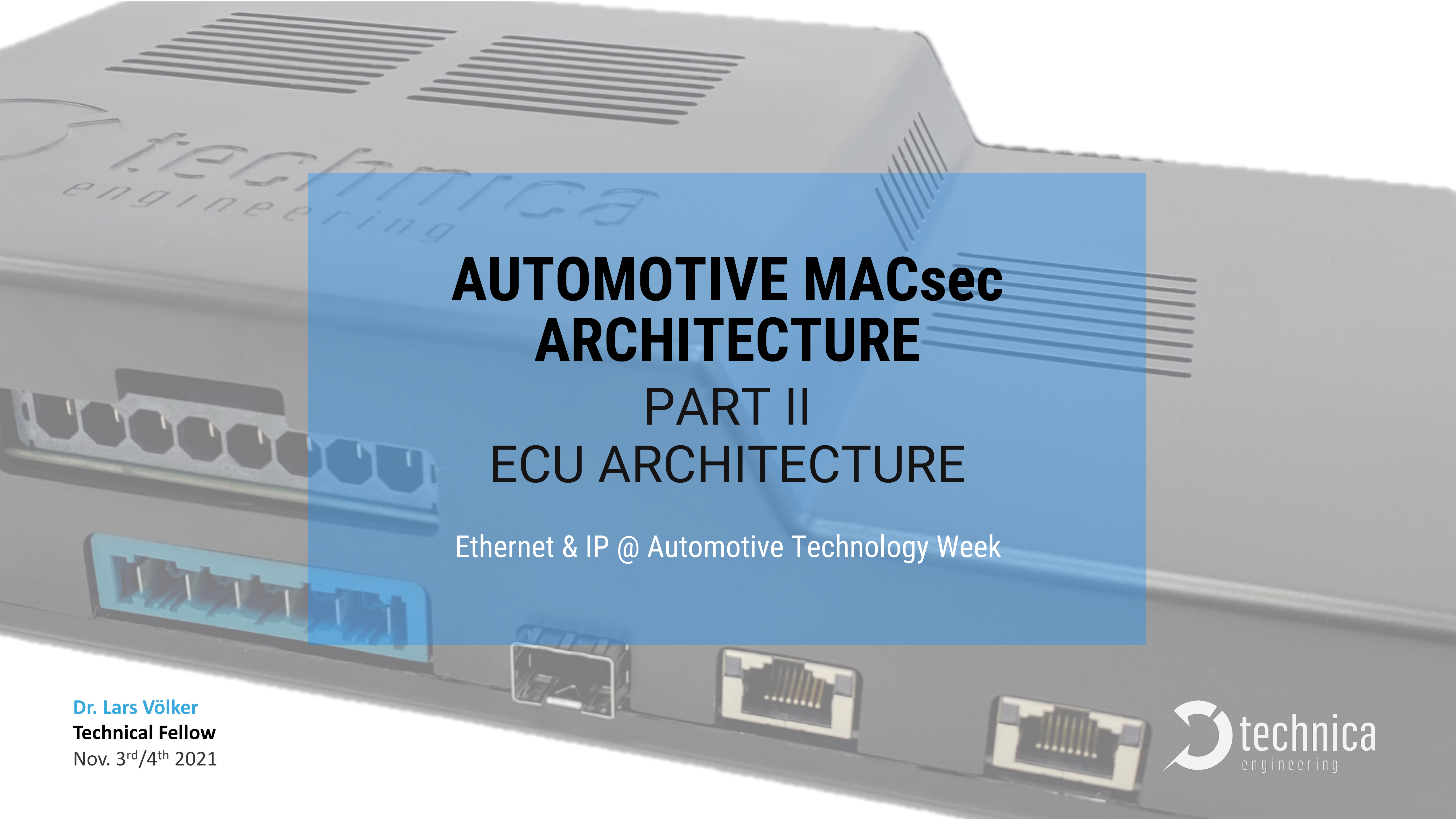
Master of 130 LIN nodes



- Clamp and power management
- Gateway (LIN, CAN, FlexRay, Ethernet)
- Access and Car Immobilizer
- Interior and exterior lighting
- Window control
- Wiper control
- Diverse sensors and switches



Example: Central ECU (2015)



AUTOMOTIVE MACsec ARCHITECTURE

PART II
ECU ARCHITECTURE

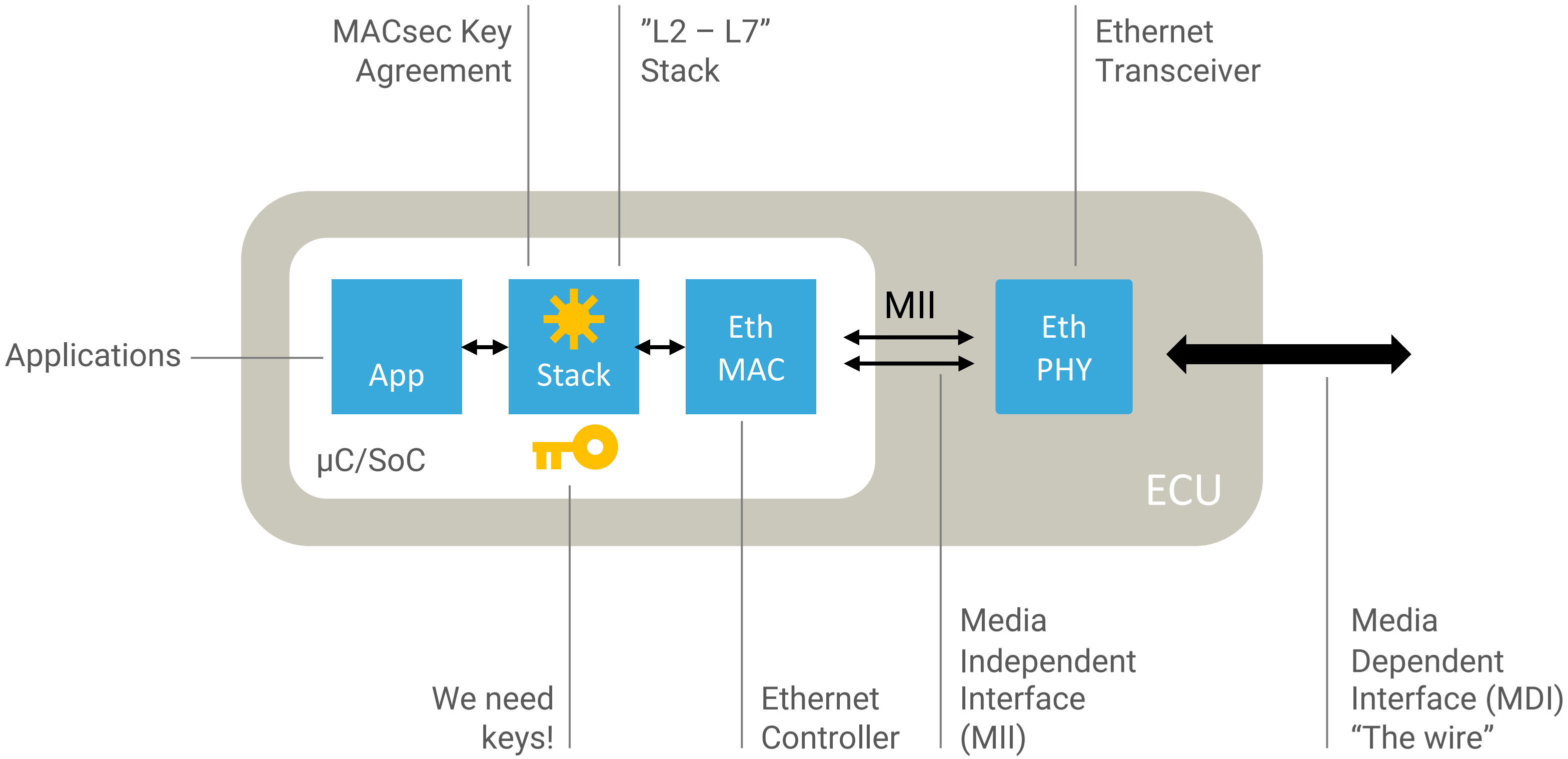
Ethernet & IP @ Automotive Technology Week

Dr. Lars Völker
Technical Fellow

Nov. 3rd/4th 2021

technica
engineering

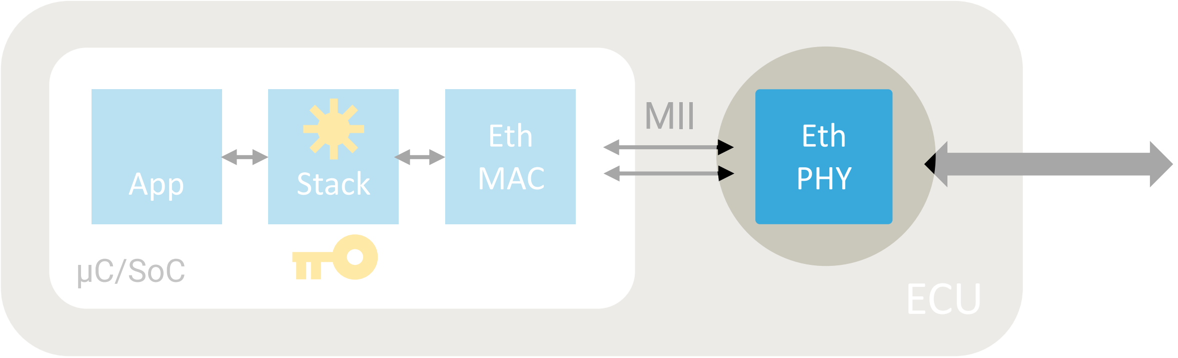
ECU ARCHITECTURE (1)



✳ MACsec Key Agreement (MKA)

ECU ARCHITECTURE (2)

MACsec Placement



Option “MACsec in the Ethernet PHY”

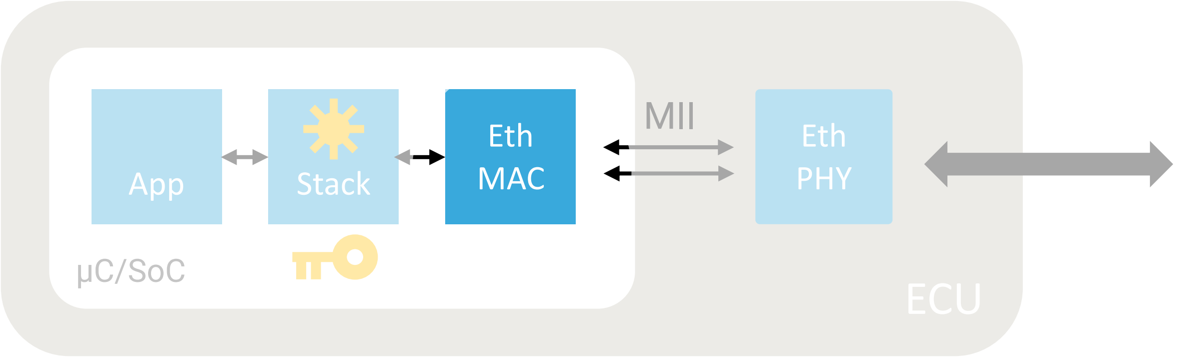
Available now.

Access to MII traces may be critical for high security use cases.

✷ MACsec Key Agreement (MKA)

ECU ARCHITECTURE (2)

MACsec Placement



Option “MACsec in the Ethernet MAC”

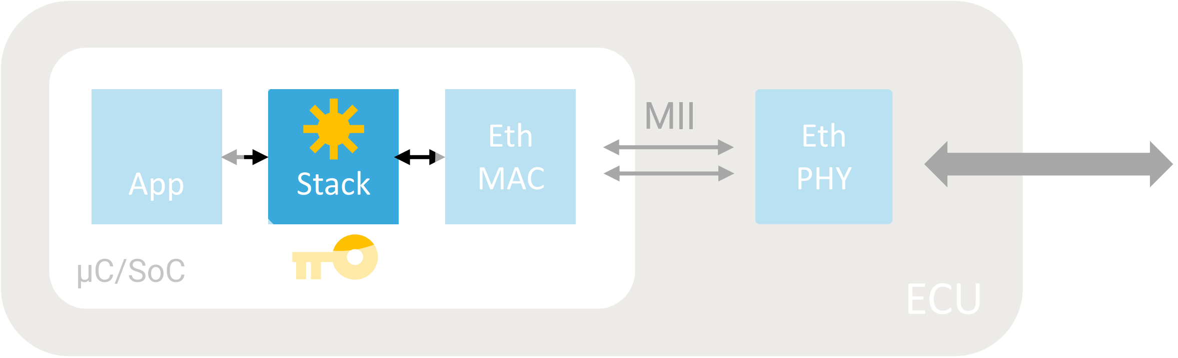
Best solution for ease and security.

Long adoption time for all µC/SoCs.

✱ MACsec Key Agreement (MKA)

ECU ARCHITECTURE (2)

MACsec Placement



Option "MACsec in Software"

Cost effective solution with hardware crypto.
Performance of hardware crypto very critical.

✹ MACsec Key Agreement (MKA)

ECU ARCHITECTURE (3)

Each MACsec port needs a CAK

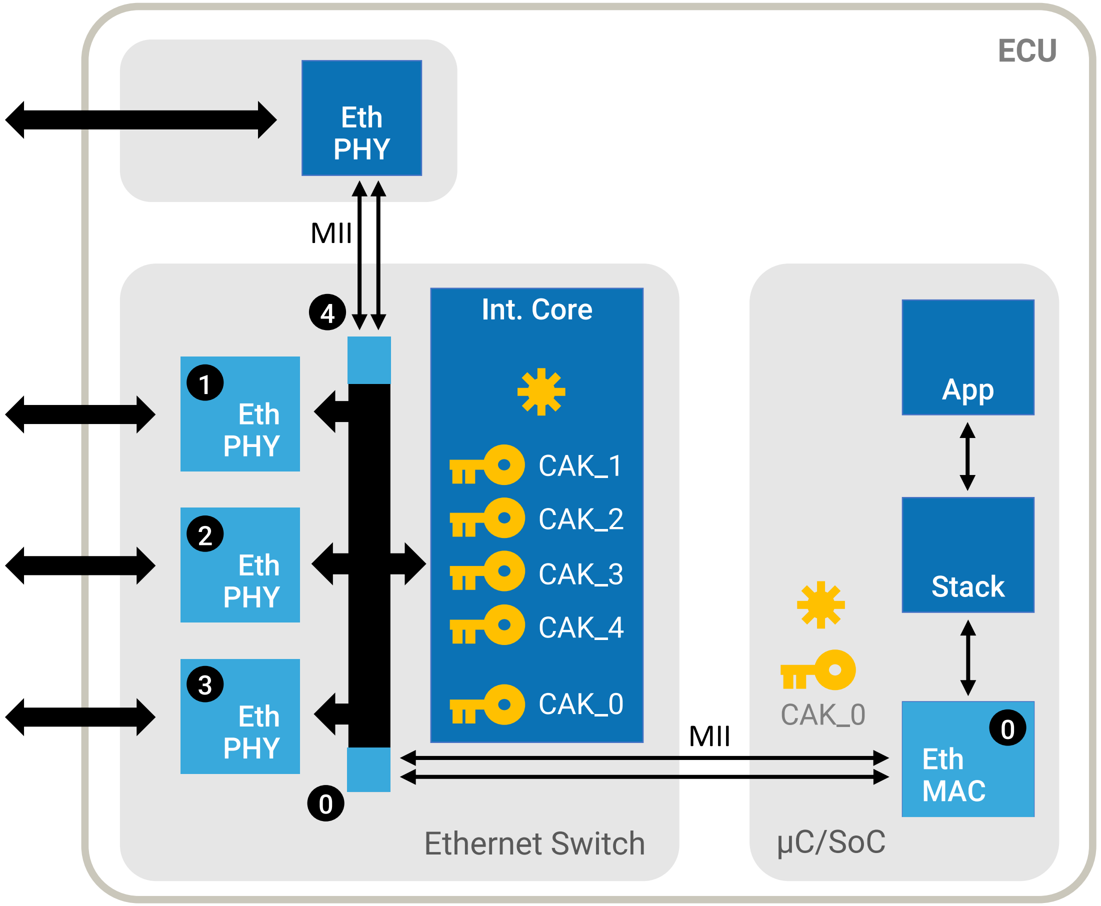
Where to place MKA in Switch ECUs?

- On the Switch (integrated core)
- µC/SoC (transport keys into switch)
- both

More options

❶ MACsec between Switch and µC/SoC?

❹ MACsec and External PHYs?



MACsec placement ✷ MACsec Key Agreement (MKA) 🔑 CAK: Connectivity Association Key (symmetric long-term secret)

DEFENSE IN DEPTH

Important complementary solutions

! Address Filtering on Switches

Since switch ports are authenticated, strong address and VLAN filtering (layer 2 and 3) is possible and highly recommended. This stops address spoofing and unauthorized VLAN access.

🚫 Access Control Lists (ACLs) on ECUs

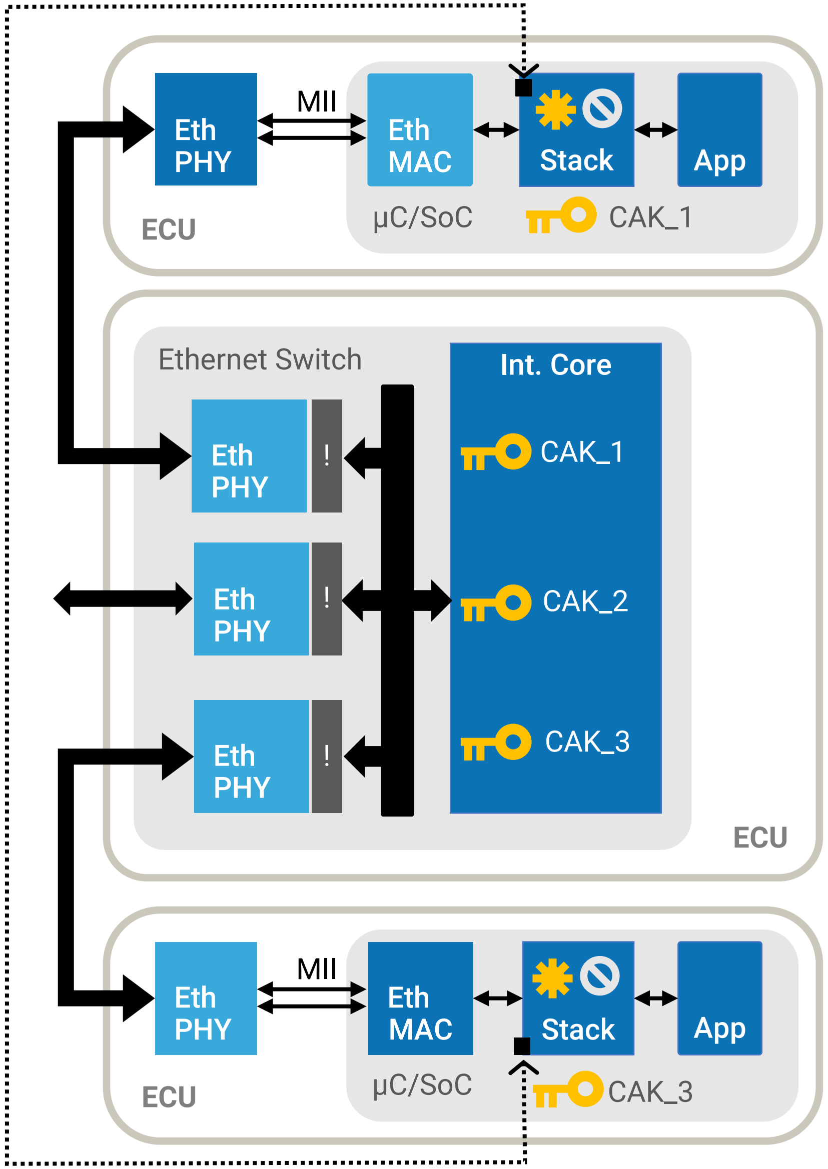
Without address spoofing, access control can be based on addresses.

For example, SOME/IP ACLs or regular packet filters in ECUs.

⋯› SecOC for selected communication

Legacy to Ethernet, Secure Element to Application, etc.

Highly critical use cases (e.g., vehicle immobilizer).



MACsec placement ✸ MACsec Key Agreement (MKA) CAK: Connectivity Association Key

KEY INSTALLATION (1)

Challenge: Tester needs to install long term pairwise secret keys, here CAK_1.

For security reasons, keys need to be vehicle individual.

This means that keys need to be installed after assembly.

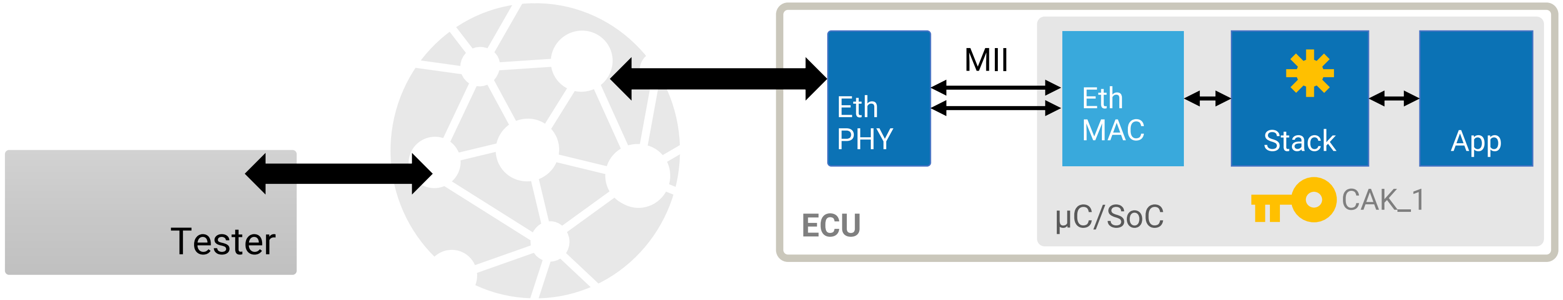
For this installation, diagnostics need to work for setting up MACsec keys.

Recommended solution:

Create bypass in MACsec implementation for certain bring up communication (e.g., via VLAN).

Allow needed diagnostic jobs for bring up here.

After key installation, MACsec can allow other communication.



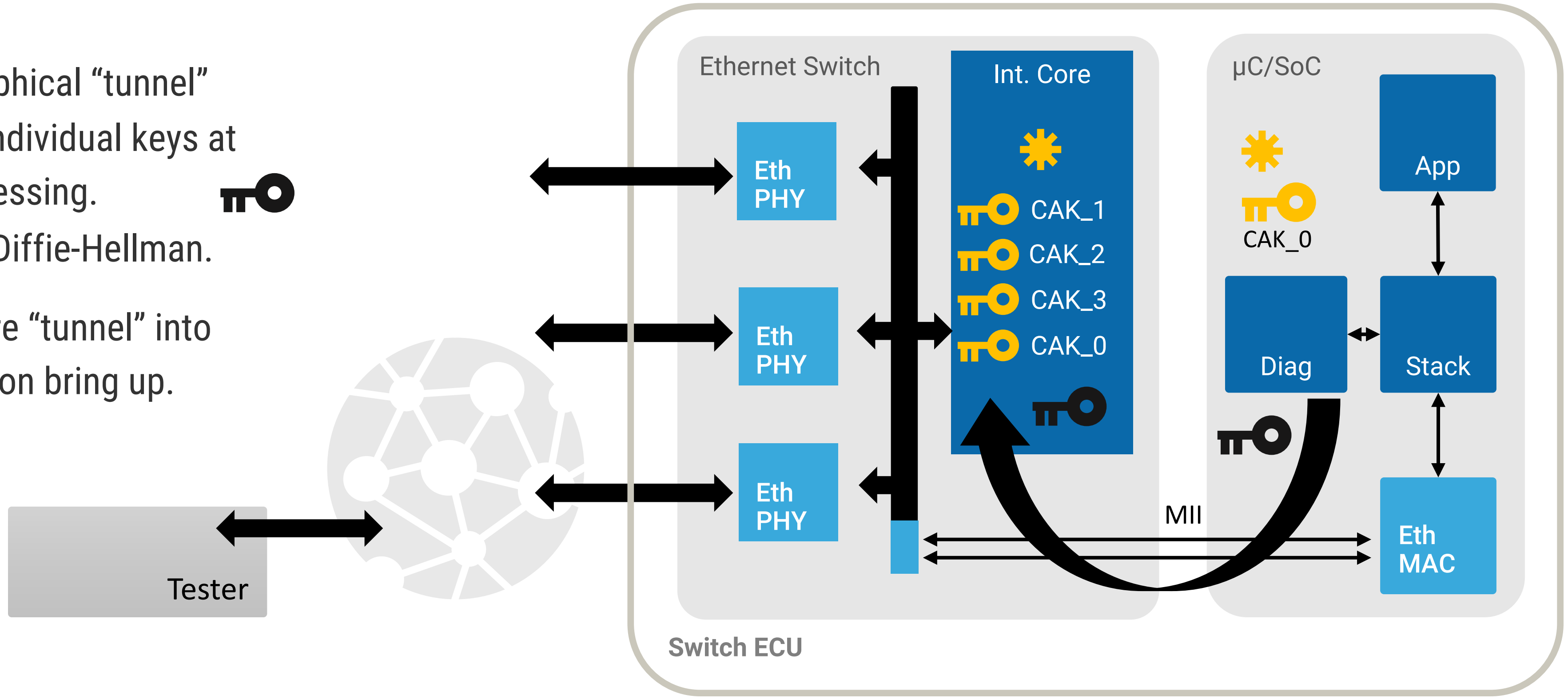
MACsec placement ✹ MACsec Key Agreement (MKA) 🔑 CAK: Connectivity Association Key

KEY INSTALLATION (2)

On “Switch ECUs”, the diagnostics runs on the µC/SoC commonly, while the MKA could run on the switch.

Create a secure cryptographical “tunnel” between both chips with individual keys at the Tier-1 end of line processing.
For example: anonymous Diffie-Hellman.

Push CAKs over this secure “tunnel” into integrated core on Switch on bring up.



MACsec placement ✳ MACsec Key Agreement (MKA) CAK: Connectivity Association Key

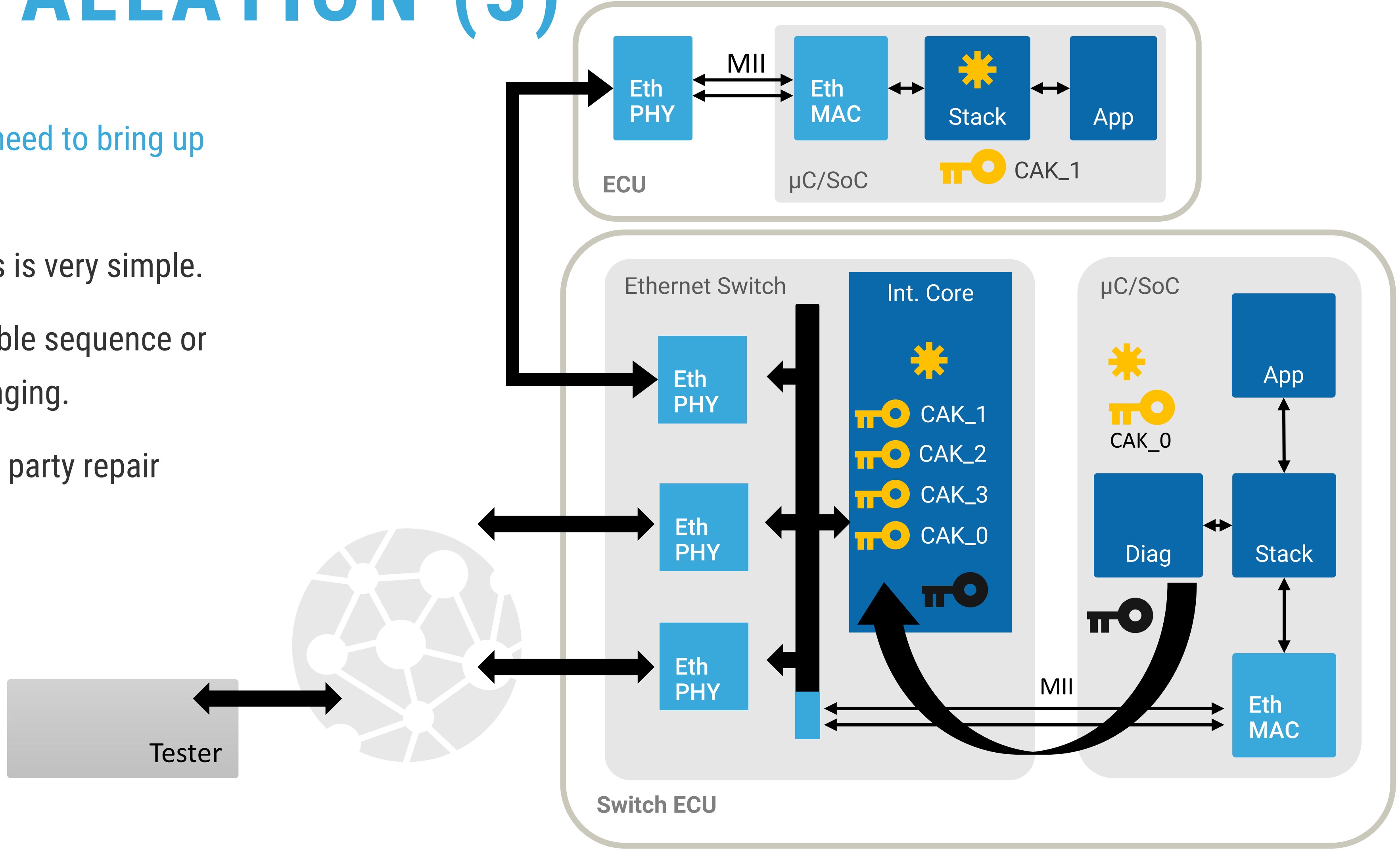
KEY INSTALLATION (3)

And don't forget that you need to bring up both ends of link!

With a "bypass VLAN", this is very simple.

With a secure enable/disable sequence or similar, this can be challenging.

How much do you trust 3rd party repair shops?



MACsec placement ✱ MACsec Key Agreement (MKA) CAK: Connectivity Association Key

TESTING AND INTEGRATION

Aspect 1: “Prototypes / A-samples”

Proof that MACsec fits your requirements!

Aspect 2: “Testing MACsec”

Test cases and test suites for MKA.

Test cases and test suites for MACsec.

Hardware tools to enable MACsec testing.

Aspect 3: “Trace analysis vs. MACsec”

Solution: “Authentication only MACsec”

Hardware tools to record communication.

Wireshark support since Wireshark 3.4.

https://automotive-macsec.com

SUMMARY

Automotive MACsec Architecture

Automotive MACsec is ready:

- E/E Architecture and ECU Architecture can clearly be envisioned.
- Bring up of MACsec can be engineered to be secure, fast, and robust.
- MACsec promises outstanding performance that scales with link speed by design!

- Automotive MACsec requires optimized MKA!
  - Find details of automotive MKA and more here: https://automotive-macsec.com
- Automotive MACsec has been proven in prototypes and A-Samples.
- Testing, integration, and tools are ready.

Outlook: Any interest in defining a “Automotive Profile for MACsec”?

Tobias Hauber

Onboard Network Security Architect
Tobias.Hauber@bmw.de
+49-151-60121917

BMW AG

80788 Munich
Germany

https://www.linkedin.com/in/tobias-hauber-04a903224/

Dr. Lars Völker

Technical Fellow
Lars.Voelker@technica-engineering.de
+49-175-1140982

Technica Engineering GmbH
Leopoldstraße 236
80807 Munich
Germany

https://www.linkedin.com/in/lars-v-761b629/