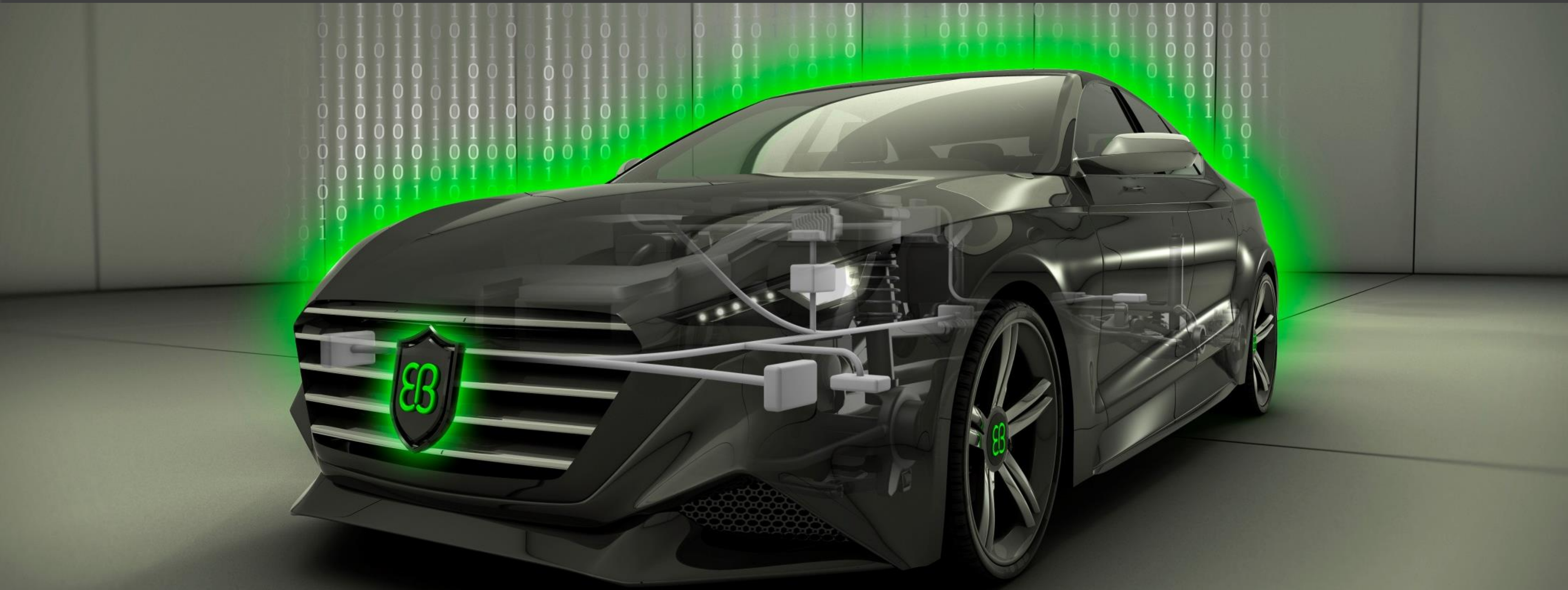
Secure Ethernet Communication for Autonomous Driving

Elektrobit

Dr. Roman Pallierer, Dr. Michael Ziehensack
Automotive Ethernet Congress
2016, February 3-4, Munich



Motivation

Advanced driver assistance systems (ADAS) are evolving towards autonomous driving

- From alert & assist…
  e.g. lane departure warning, lane keeping assist
- … to features taking more control
  e.g. highway chauffeur, valet parking

Automotive Ethernet is a key enabler for autonomous driving.
Secure Ethernet Communication is required to ensure:

Availability

- Sensor data is available on time to create an environment model of the vehicle
- Actuator commands are sent correctly to control the vehicle

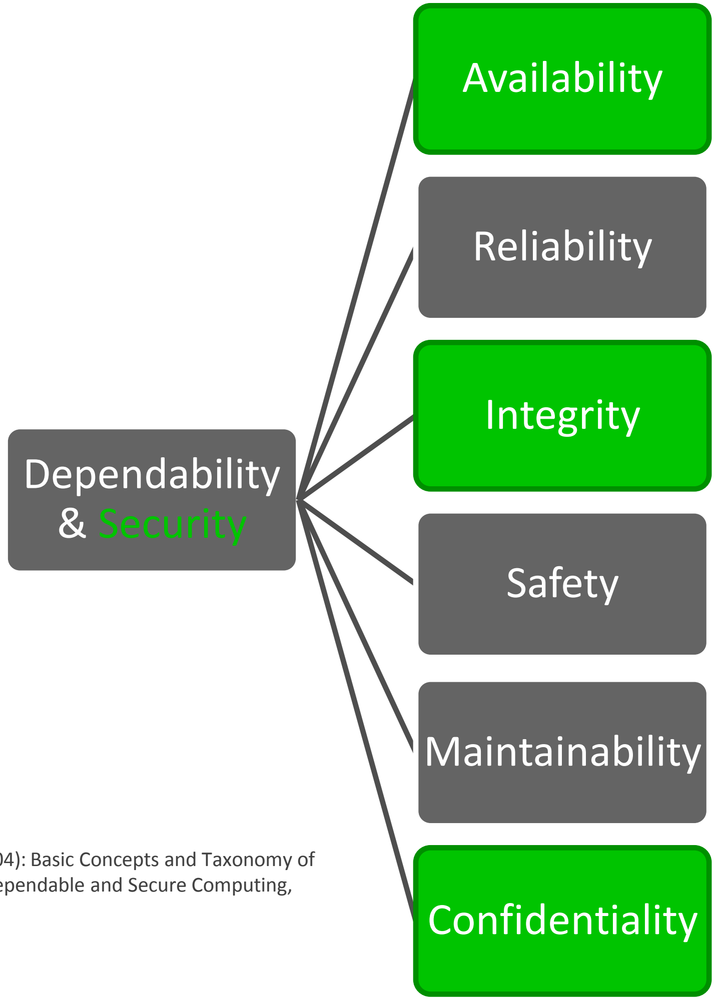
Integrity

- Sensor and actuator data are sent by authorized parties only to avoid manipulation
- Sensor and actuator data is not altered, removed or delayed to avoid manipulation

Confidentiality

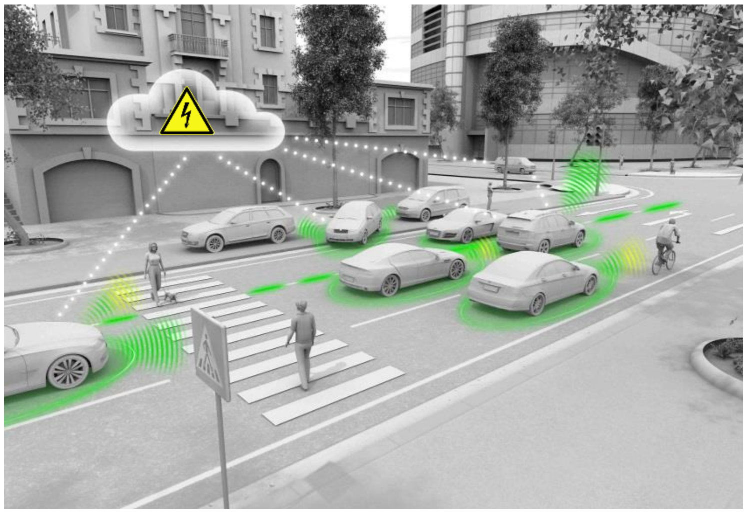
- Sensor and actuator data are not monitored by unauthorized 3rd parties to protect driver's privacy

Dependability & Security



Source: A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr (2004): Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, Vol. 1, N. 1

Security issues in a safety environment



- **Safety:** Protection against **non-malicious** faults, e.g. EMV
- **Security:** Protection against **malicious** faults, e.g. intended attacks

Security protects Safety

There is no safety without security

Secure communication

Protection against effects of malicious faults on the communication link

- **Types of Attack**:
  - injection of malicious control commands
  - prevention of correct system function (insertion, deletion, manipulation, replay and delay of messages)
- **Points of Attack**:
  - additional nodes (e.g. via OBD connector or wireless access)
  - corrupted and misused existing nodes (e.g. root access to infotainment system via cellular network)
  - nodes replaced by manipulated ones

- New threats can emerge during system operation
- Threats are attacks (malicious, human made, external)
- Goal: Protect assets (property, environment and human life)

Solution: Multi-Level Security Architecture

Enhanced connectivity and the dynamics of the security threats demand to establish several security barriers in order to avoid a full exposure in case a security mechanism is bypassed.

Approach: establish security mechanisms on four levels:

Level 1: restrict access to the network

Level 2: secure onboard communication

Level 3: apply data usage policies

Level 4: detect anomalies and defend

Goal:

Protect against attacks violating the **availability**, **integrity** and **confidentiality**.

Multi-Level Security Architecture

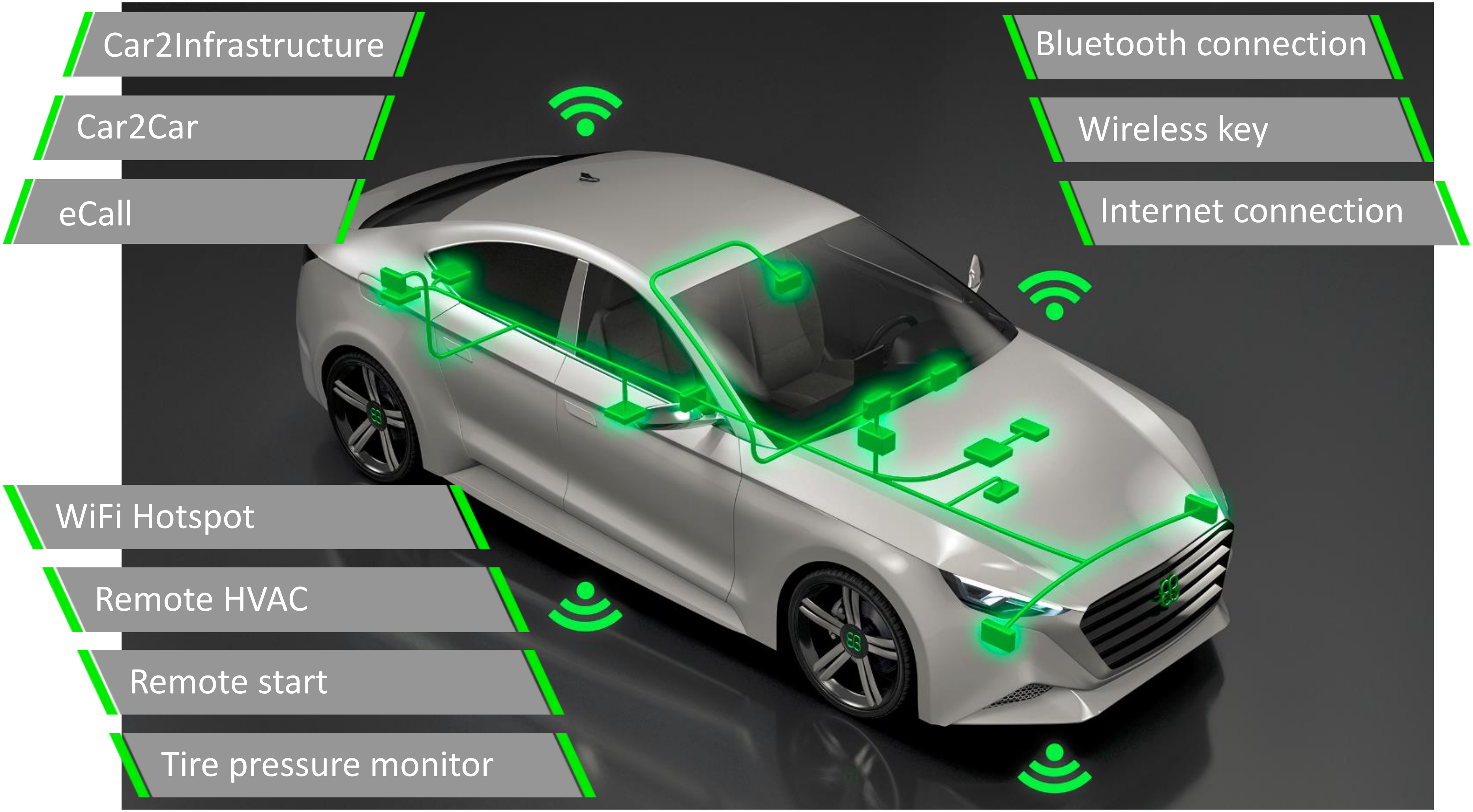
Level 1: Restrict access to the network

Level 2: Secure onboard communication

Level 3: Apply data usage policies

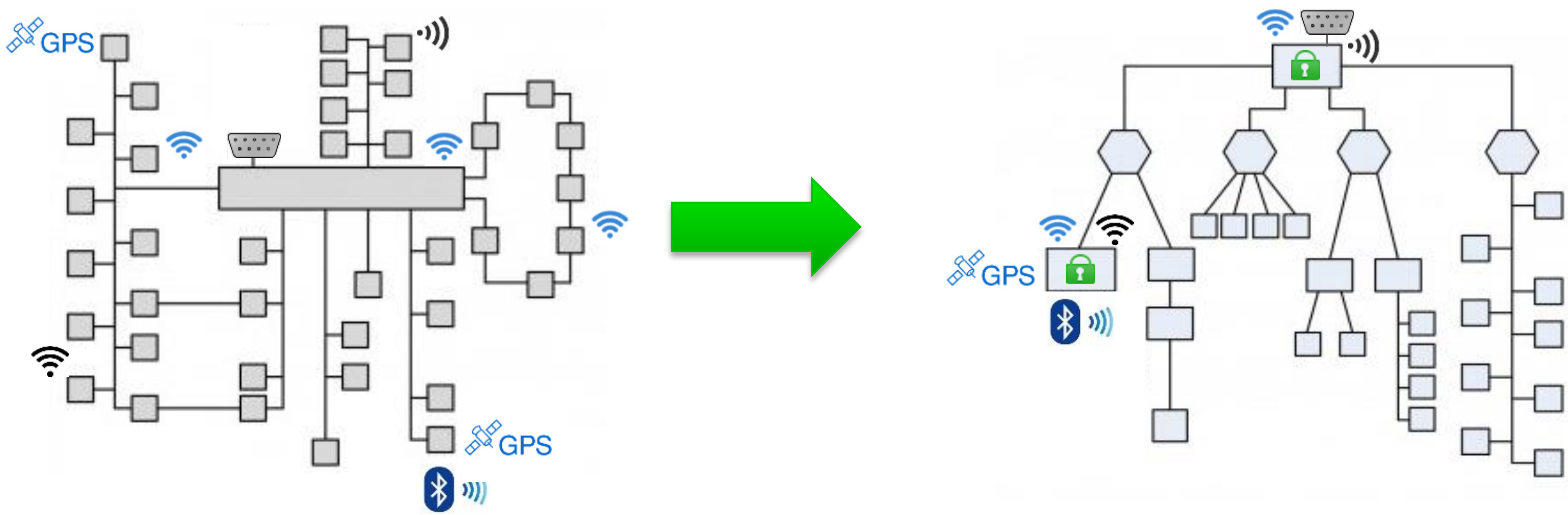
Level 4: Detect anomalies and defend

Various access points to the network



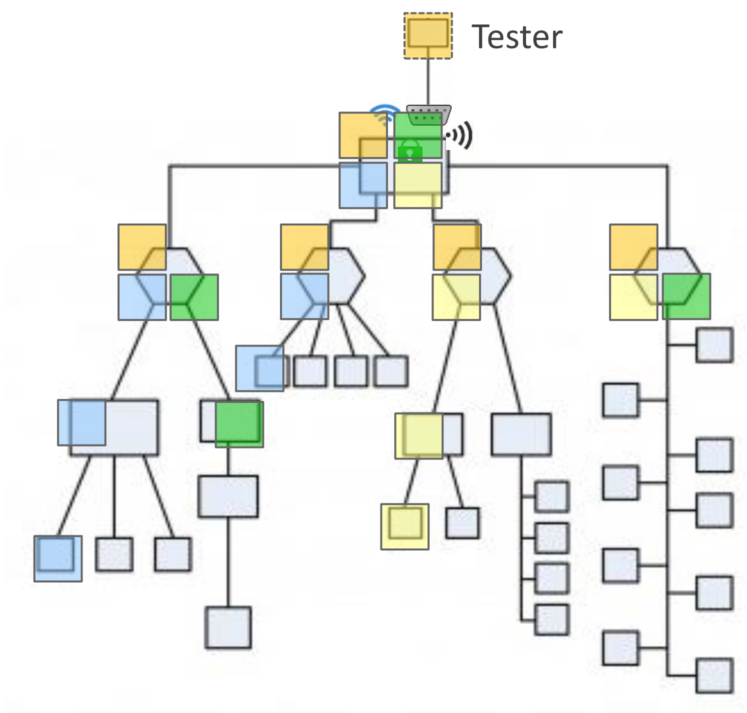
Level 1: Restrict access to the network (I)

- **Limit the number** of ECUs with **off-board connections** (WLAN, bluetooth, cellular, wireless key, DAB, OBD plug, PLC), e.g. via
  - central network access point with stateful firewall
  - diagnostic communication from external tester to ECUs via central gateway (communication between tester and central gateway via TLS)



Level 1: Restrict access to the network (II)

- Divide network into **security zones**, e.g. extern, “demilitarized”, internal. And restrict traffic between zones: Physical split or separation via VLANs
- Not only extern-intern, but also intern-intern, e.g. infotainment to powertrain



VLAN Tagging to separate external – internal

- All frames from the external tester are tagged with an orange VLAN tag at the switch located at the GW
- Thus only nodes assigned to the orange VLAN can receive frames from the external tester
- Frames to be sent to external tester, are sent via the orange VLAN – the switch at the gateway removes the orange VLAN tags before forwarding it to the tester

VLAN Tagging to separate internal networks

- ECUs from Infotainment (blue VLAN), chassis (green VLAN) and powertrain (yellow VLAN) can be separated, i.e. will only see frames from the assigned VLANs
- Traffic between VLANs require a switch or Gateway

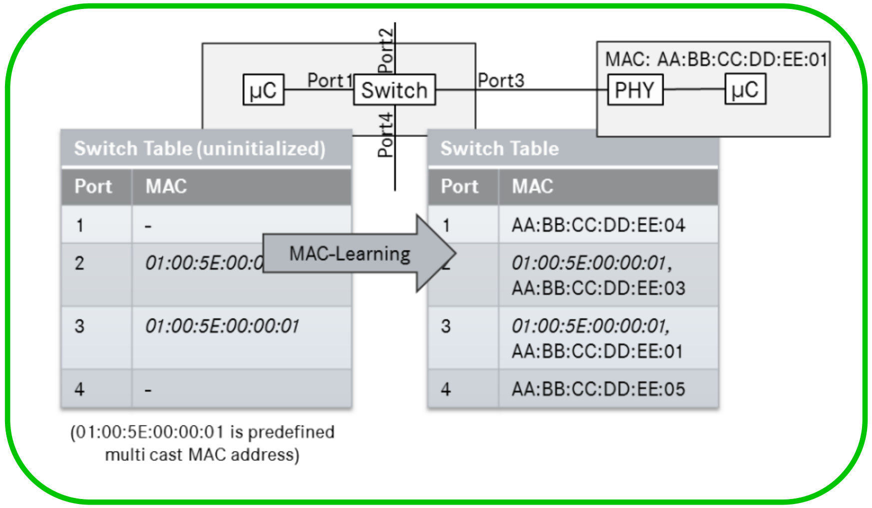
Level 1: Restrict access to the network (III)

- static **Ethernet Switch** Forwarding tables OR MAC learning only during learning mode (e.g. end-of-line)

- static ARP tables **at nodes** OR Address Resolution Protocol only during learning mode (e.g. end-of-line)

- **device authentication/authorization**

- **deactivation** of unused (non authorized) ports



Source: AUTOSAR 4.2 EthSwt SWS

Multi-Level Security Architecture

Level 1: Restrict access to the network

Level 2: Secure onboard communication

Level 3: Apply data usage policies

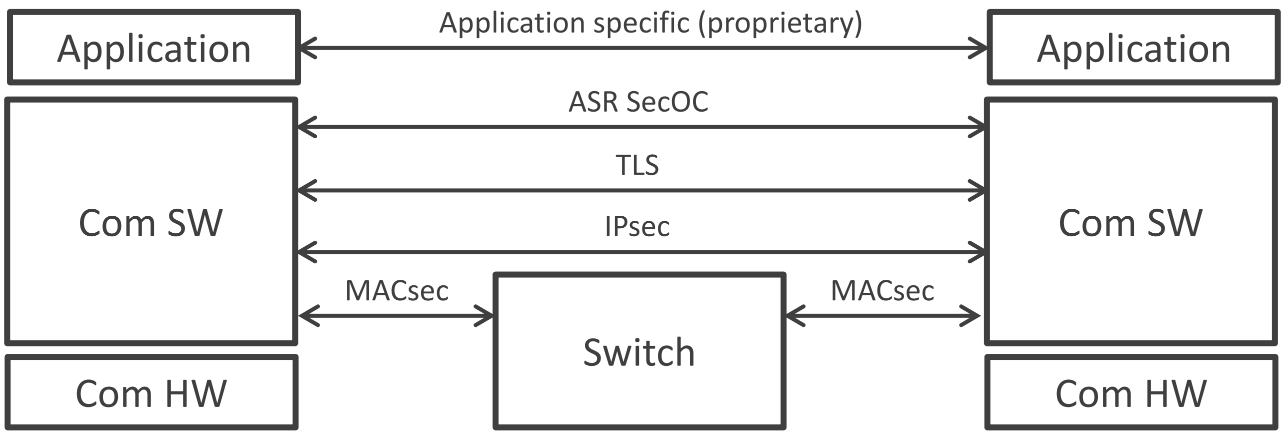
Level 4: Detect anomalies and defend

Level 2: Secure onboard communication (I)

Data integrity, authentication, encryption

- Authentication and integrity of critical frames
- Symmetric key because of calculation effort (and required bandwidth)
- Encryption for exchange of session keys

- Choice of protection layer and protocol:



Level 2: Secure onboard communication (II)

Data integrity, authentication, encryption - Protocols

Protocol	Standard	Type/Layer	Authent.	Encryption	Comment
MACsec	IEEE 802.1AE	Hop-by-hop Data-Link	X	X	Requires crypto/keys at each network node
IPsec AH (Authentication Header)	IETF RfC 4302	End-to-End IP	X	-	
IPsec ESP (Encapsulating Security Payload)	IETF RfC 4303	End-to-End IP	X	X	
TLS 1.2 (Transport Layer Security)	IETF RfC 5246	End-to-End TCP	X	X	Does not work with UDP
SecOC	AUTOSAR	End-to-End PDUs	X	-	supports MACtruncation (works also with CAN / FlexRay)

Level 2: Secure onboard communication (III)

Data integrity, authentication using AUTOSAR SecOC

- Authentication and integrity of critical frames based on Message Authentication Code (MAC, i.e. usage of symmetric key) and freshness value (counter or timestamp)
- Symmetric key because of calculation effort (and required bandwidth)
- Sender **generates** MAC based on DataId, data, freshness value and secret key.
  MAC and freshness value are transmitted together with PDU data.
- Receiver **verifies** MAC based on received data and freshness value as well as locally stored secrete key, DataId
- CNT/MAC truncation can be used if message length is very limited.

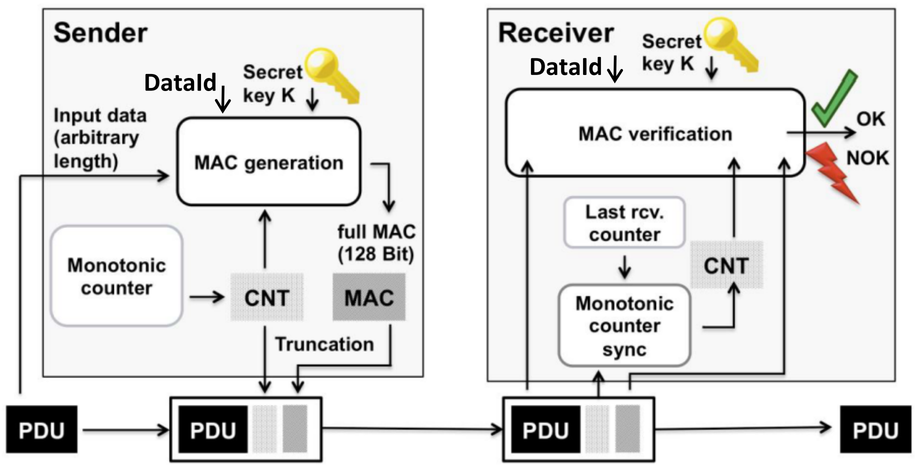


Figure 3: Message Authentication and Freshness Verification

Source: AUTOSAR 4.2 SecOC SWS

Level 2: Secure onboard communication (IV)

Design principles for key usage (for encryption and authentication)

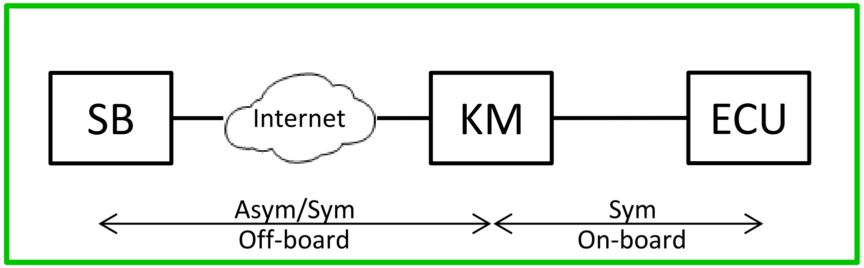
- **Distinct keys** for **different functions**, e.g.
  - Traffic Encryption Key (TEK): used for encryption/decryption of traffic
  - Key Encryption Key (KEK): unique for each ECU and used only for en/decryption of TEK
  - If TEK gets compromised, a new TEK can be distributed via KEK
  - If KEK of an ECU gets compromised, a new TEK can still be securely distributed to the other ECUs (as they are using all different KEKs)
- A **key** shall only be used for securing a **limited number of data**
  - TEK is only valid for a certain period to limit the exposure in case of compromise
  - Furthermore critical communication is clustered into secure communication groups, e.g. separate TEKs for ADAS sensors, chassis and powertrain communication.
- For efficient execution of cryptographic functions and secure key storage a **hardware security module (HSM)** is used in combination with software crypto libraries.

Elektrobit

Level 2: Secure onboard communication (V)

Design principle for Key Management (Generation, Distribution and Storage)

SB … Service Backend Server
KM … Key Master



Based on: The EVITA Project

- Service Backend (off-board) >> KeyMaster (on-board):
  - Communication between SB and KM is encrypted using asymmetric cryptography
  - SB configures and triggers key exchange at KM
- KeyMaster >> ECUs:
  - Communication between KM and ECUs is encrypted using symmetric cryptography
  - KM generates communication group session keys (TEK) if triggered, e.g. by the SB, a timeout or a diagnostic request
  - KM assigns TEKs to ECUs by using the related Key Encryption Key (KEK) of the ECU
  - ECU securely stores the keys in its HSM

Elektrobit

Multi-Level Security Architecture

Level 1: Restrict access to the network

Level 2: Secure onboard communication

Level 3: Apply data usage policies

Level 4: Detect anomalies and defend

Level 3: Apply data usage policies

Define data usage policies to limit the exposure

- Use service specific know how to implement policies in the application
  - Control Data: accept control commands only in specific application states, define priorities of requester
  - Sensor data: validate the contents of data (context, history, …)

Examples

- allow diagnostic messages only in specific vehicle state, e.g. speed is less than 5mph or drivers door open
- allow massive steering/braking/acceleration change only in certain vehicle state (e.g. crash indication, driver request in 'sport' mode, …)
- use more than one sensor (instance) to determine if the vehicle is not moving

Challenges

- Highly application dependent
- Side-effect must be considered

Multi-Level Security Architecture

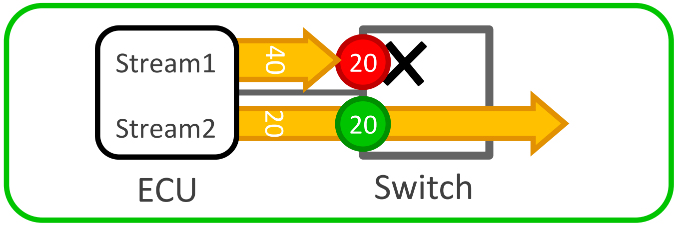
- Level 1: Restrict access to the network
- Level 2: Secure onboard communication
- Level 3: Apply data usage policies
- **Level 4: Detect anomalies and defend**

Level 4: Detect anomalies at the network and defend

- **Anomalies: deviations to specified communication matrices**
  e.g. cyclic message is received more often than defined, very high network load, 1:n message received with different source addresses, …

- **Detection:** via central device or at the receiver
  e.g. plausibility check based on diverse input data or data sequence, failed integrity checks

- **Defend:** report (e.g. DTC, involvement of driver, …) and start mitigation
  - mask (e.g. block messages from infotainment ECU, block messages from "babbling idiot" by enforcing bandwidth limitation at switches) or



  - reconfigure (e.g. deactivation of critical functions, initiate hand-over in case of autonomous driving, request change of session key …)

Summary: Protection by the security levels

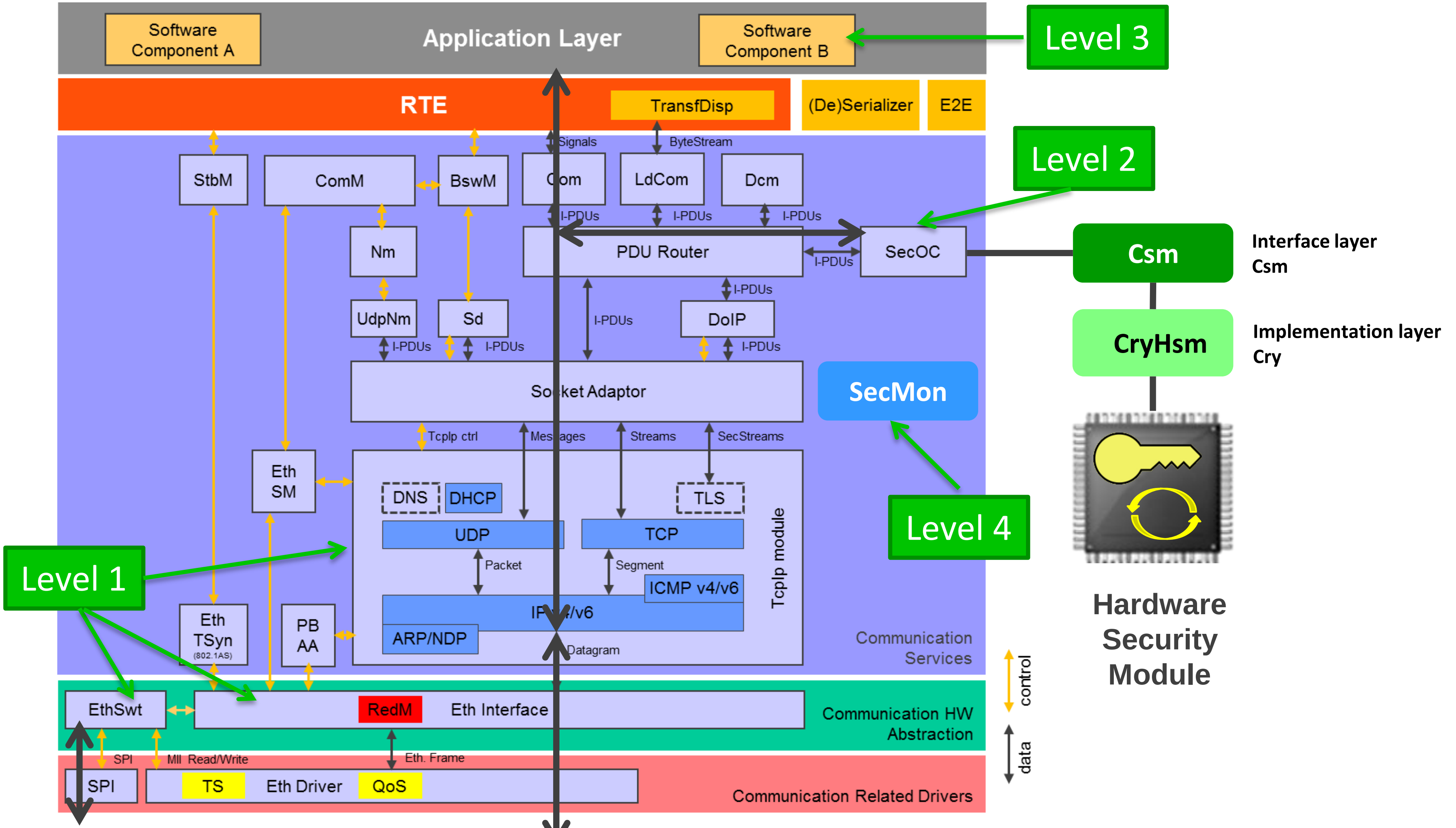
Levels protecting against attacks violating the **availability**, **integrity** and **confidentiality**:

Level	Availability	Integrity	Confidentiality
Level 1: restrict access to the network	**Yes**	**Yes**	**Yes**
Level 2: secure onboard communication	No (DoS attacks)	**Yes**	**Yes**
Level 3: apply data usage policies	No (DoS attacks)	**Yes**	No (eavesdropping)
Level 4: detect anomalies and defend	**Yes**	(Yes)	No (eavesdropping)

.

Elektrobit

Multi-level security architecture with AUTOSAR



Summary

- **Autonomous driving requires secure communication to protect against malicious attacks**

- **Multi-level security architecture**
  - ensures availability, integrity and confidentiality
- **Security mechanisms**
  - Lots of experience from IT industry
  - Adaptations for automotive necessary and implemented
  - First steps of standardization for security in automotive achieved, more needed.
- **Solutions are available, use them to secure Ethernet for autonomous driving.**

Thank you!

Elektrobit

automotive.elektrobit.com/ethernet

Roman.Pallierer@elektrobit.com
Michael.Ziehensack@elektrobit.com