Technische Universität Braunschweig

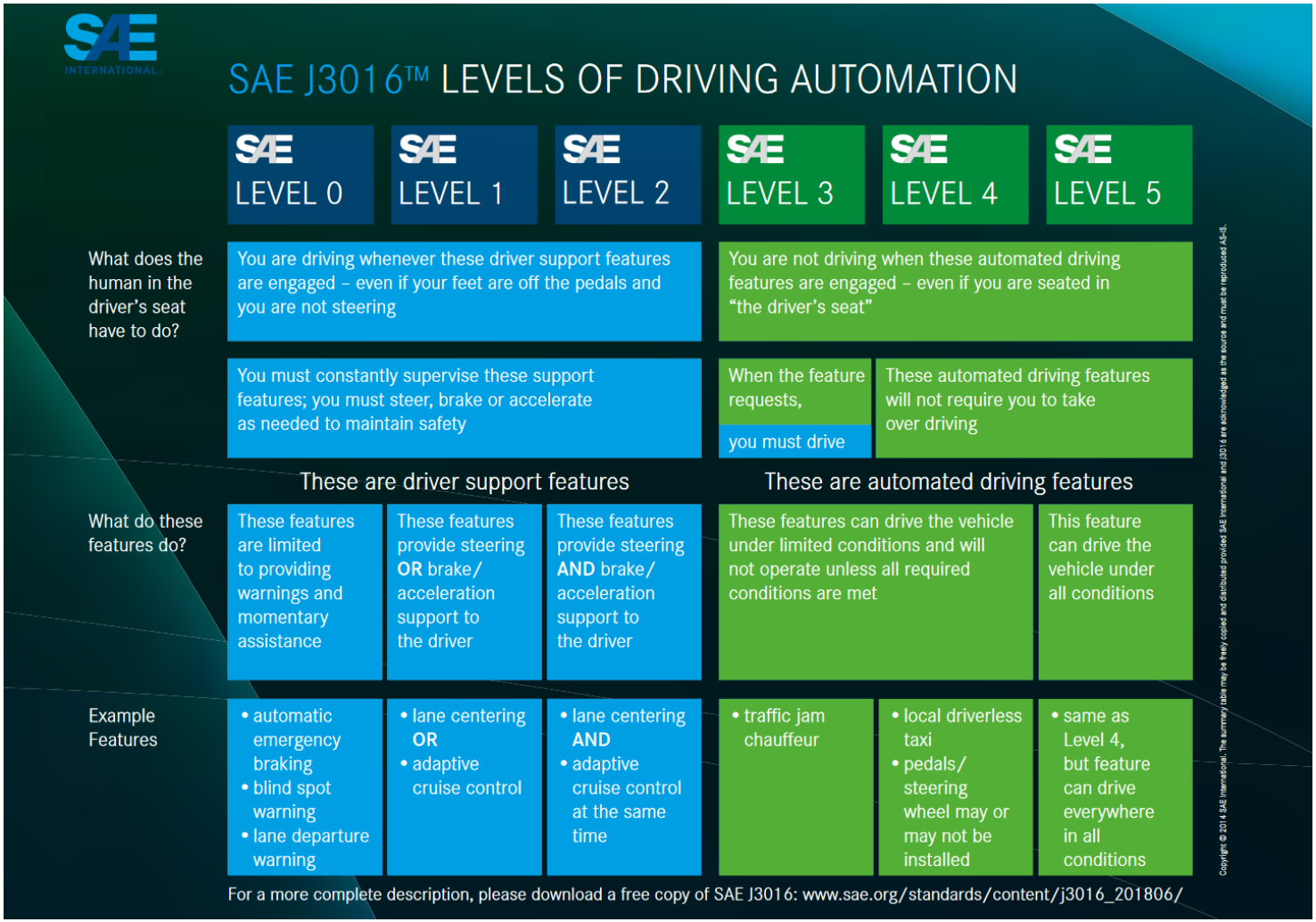
Safety and Security Aspects of Ethernet and TSN

Borislav Nikolić

Institut für Datentechnik und Kommunikationsnetze, TU Braunschweig, Germany

CERTS 2019 Workshop, Stuttgart, 9 July 2019

Focus on Automotive Domain



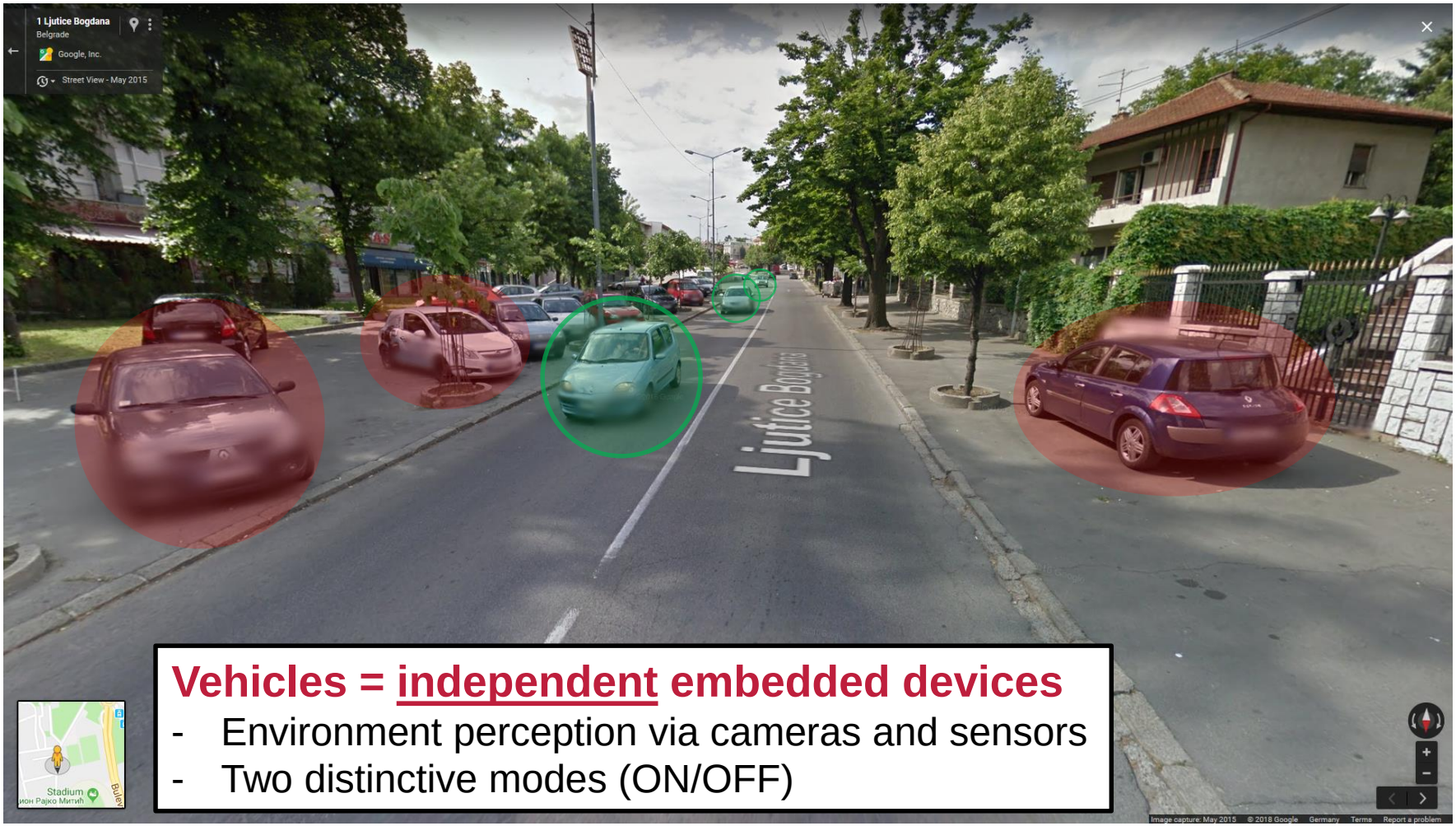
Outline

- **Automotive trends – Past, Present and Future**
- **Automotive Ethernet & TSN**
- **Safety Aspects**
- **Security Aspects**
- **Conclusions**

Outline

- **Automotive trends – Past, Present and Future**
- Automotive Ethernet & TSN
- Safety Aspects
- Security Aspects
- Conclusions

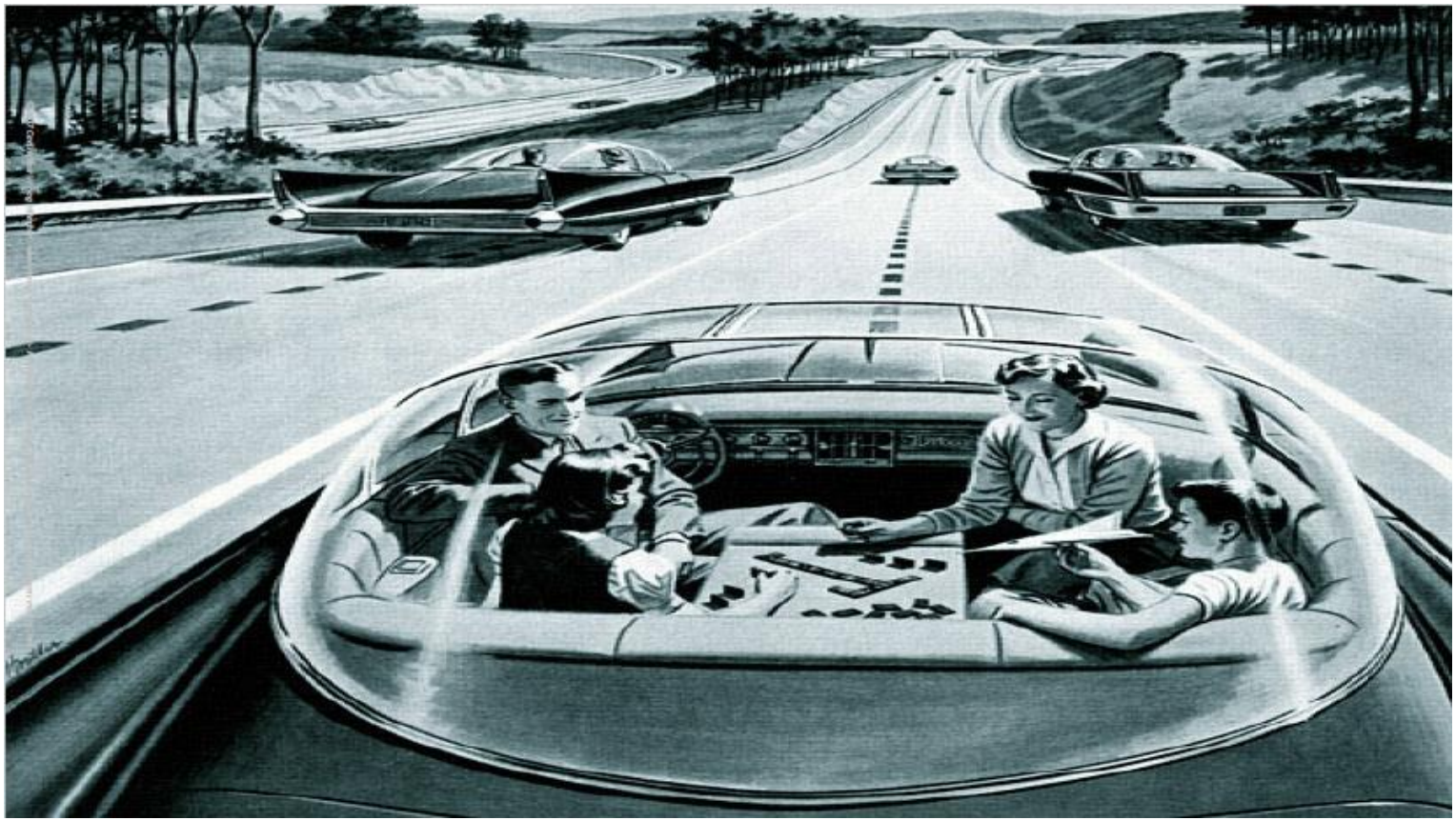
Automotive trends – Past & Present



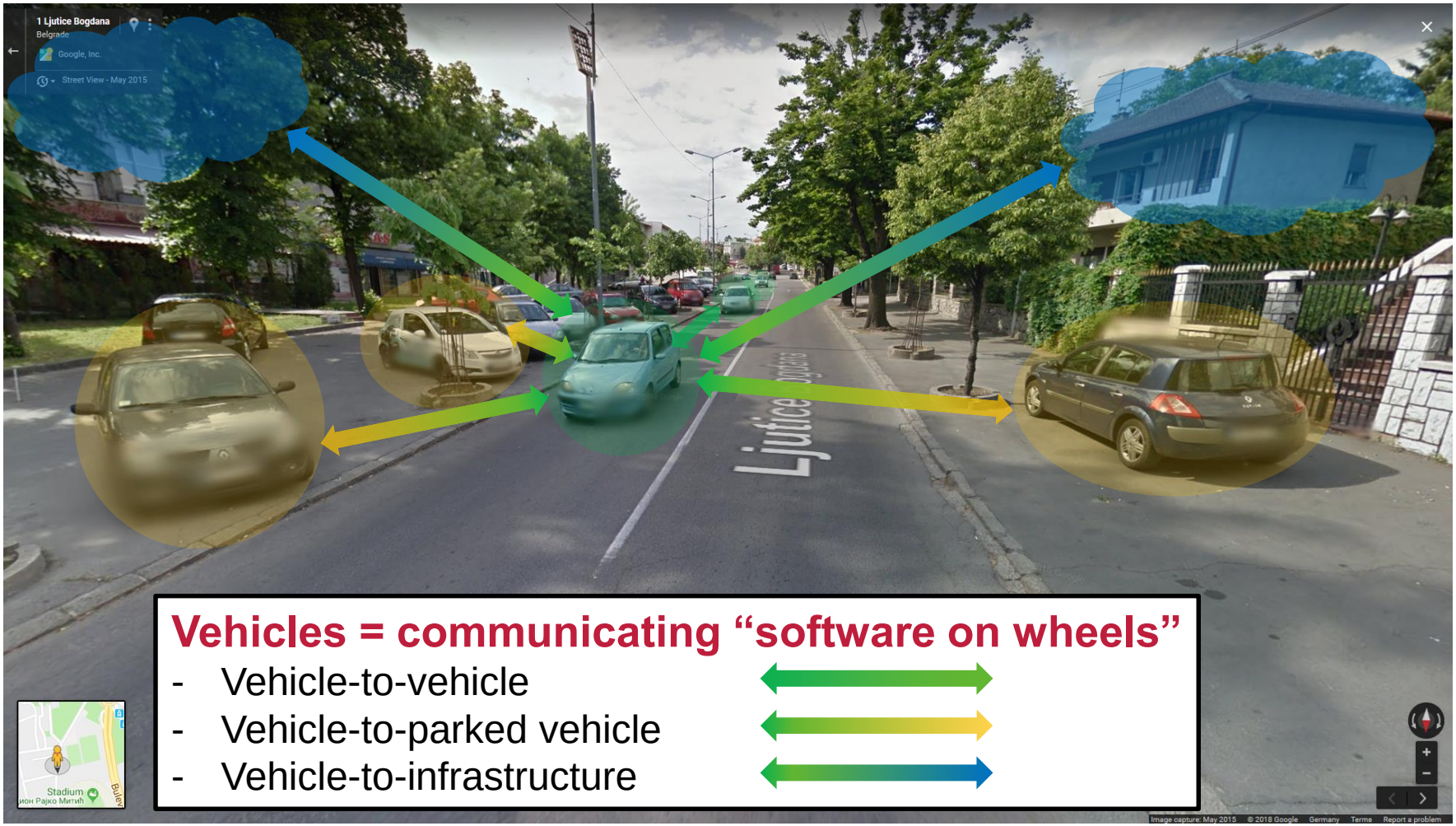
Vehicles = <u>independent</u> embedded devices

- Environment perception via cameras and sensors
- Two distinctive modes (ON/OFF)

Envisioned 21st Century Vehicles (1950s perspective)



Automotive trends – Future



Outline

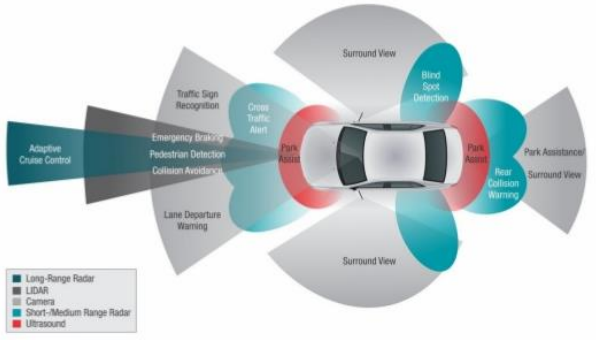
- Automotive trends – Past, Present and Future
- **Automotive Ethernet & TSN**
- Safety Aspects
- Security Aspects
- Conclusions

Why Ethernet in the Automotive Domain?

- **Ever-increasing requirements of current and future functionalities:**
  - High throughput - **infotainment**
  - Low (guaranteed) latencies
  - Fault-tolerance

  } **Sensor fusion**
  Real-time object detection

- **Ethernet benefits:**
  - **Bandwidth**: 100Mb/s → 1Gb/s → 10Gb/s → …
  - Open network capabilities
  - Shared technology cost (no ownership issues)
  - Huge engineering experience (avionics, industry)

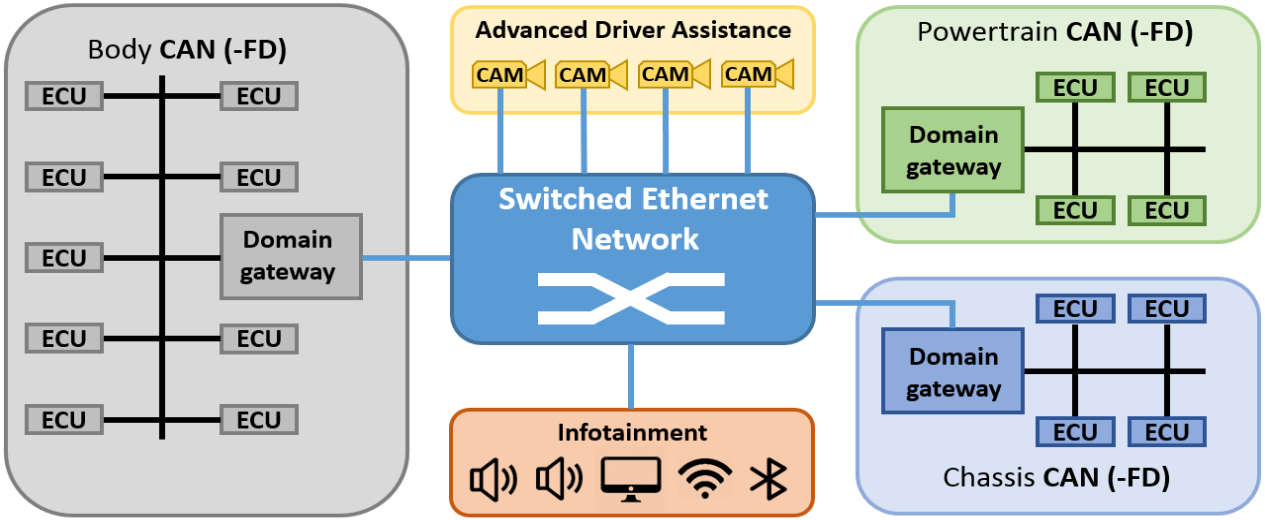


Sensors distribution, Image by http://www.engineering.com

- **Ethernet → communication backbone**
- **Ethernet is a very promising automotive technology**
  - Common view: Ethernet most likely candidate for mono-technological network

Ethernet in the Automotive Domain

- **Envisioned heterogeneous automotive architecture**



- **frame preemption** (IEEE 802.1Qbu)
- **stream filtering** (IEEE 802.1Qci)
- **time triggering** (IEEE 802.1Qbv)
- **frame replication & elimination** (IEEE 802.1CB)
- **...**

Ethernet TSN

- **Frame Preemption** (**IEEE 802.1Qbu**)
  - Reduces blocking time of lower-priority frames
  - Allows preemptions of lower-priority frames (at certain points)
- **Per-Stream Filtering and Policing** (**IEEE 802.1Qci**)
  - Ensure that streams stay within pre-defined bounds (fault containment)
- **Timing and Synchronisation** (**IEEE 802.1AS-rev***)
  - Extensions to 802.1AS: redundancy, multiple time domains
- **Time Triggering** (**IEEE 802.1Qbv**)
  - Time-aware shaper for low latency
  - Time slots protected by guard bands
- **Frame Replication and Elimination** (**IEEE 802.1CB**)
  - Increased network resilience to transmission faults via redundancy

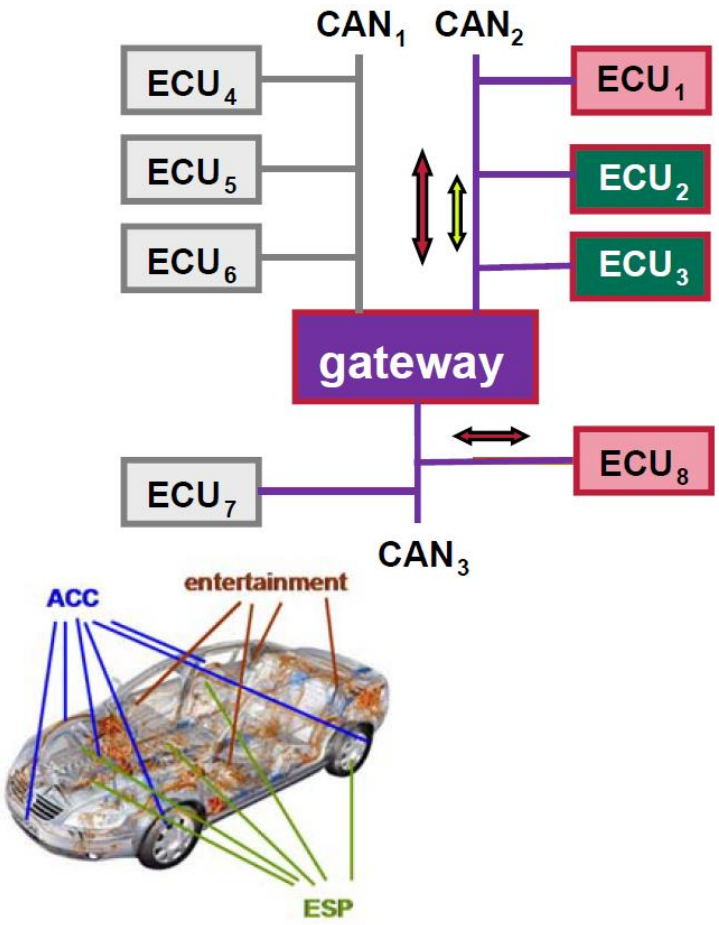
Outline

- Automotive trends – Past, Present and Future
- Automotive Ethernet & TSN
- **Safety Aspects**
- Security Aspects
- Conclusions

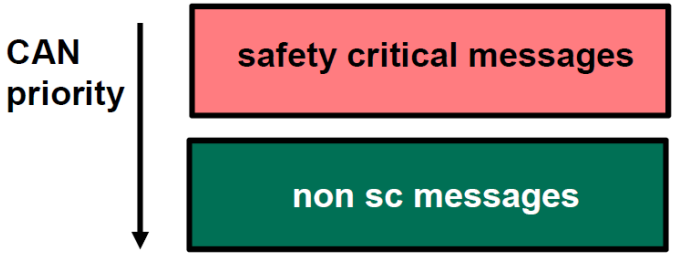
Automotive Ethernet Challenges

- **Lost inherent support for pub/sub mechanism** (switch-based)
  - Need to use higher-level protocols
- **Routing necessary**
  - Point-to-point communication with dynamic address handling
  - Different switch scheduling mechanisms, flow control
- **Different communication schemes**
  - Unicast, multicast, broadcast
- **Freedom from interference**
  - How does Ethernet achieve this goal?

Safety Aspects of Current Automotive Networks



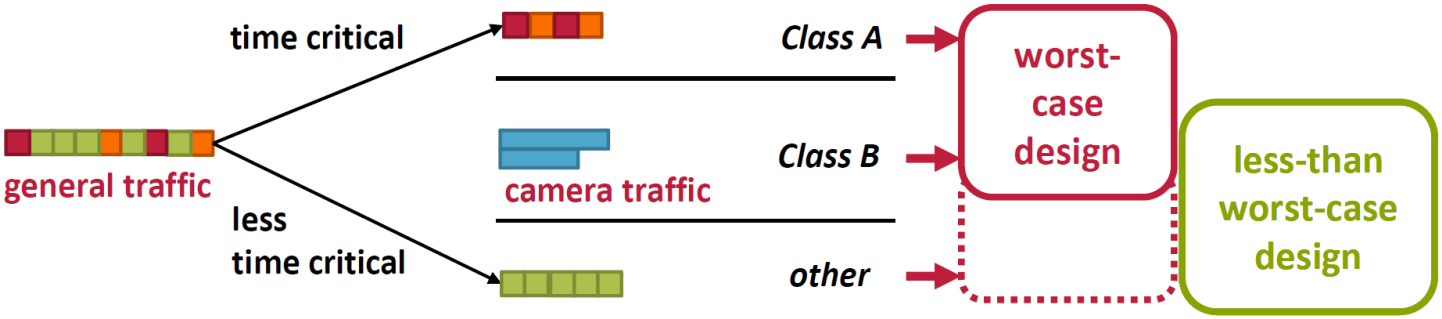
- **Application of safety standard ISO 26262 affects large part of the system**
  - "**Freedom from interference!**"
- **Isolation on mixed-critical busses**



- **Use priorities to separate criticalities**

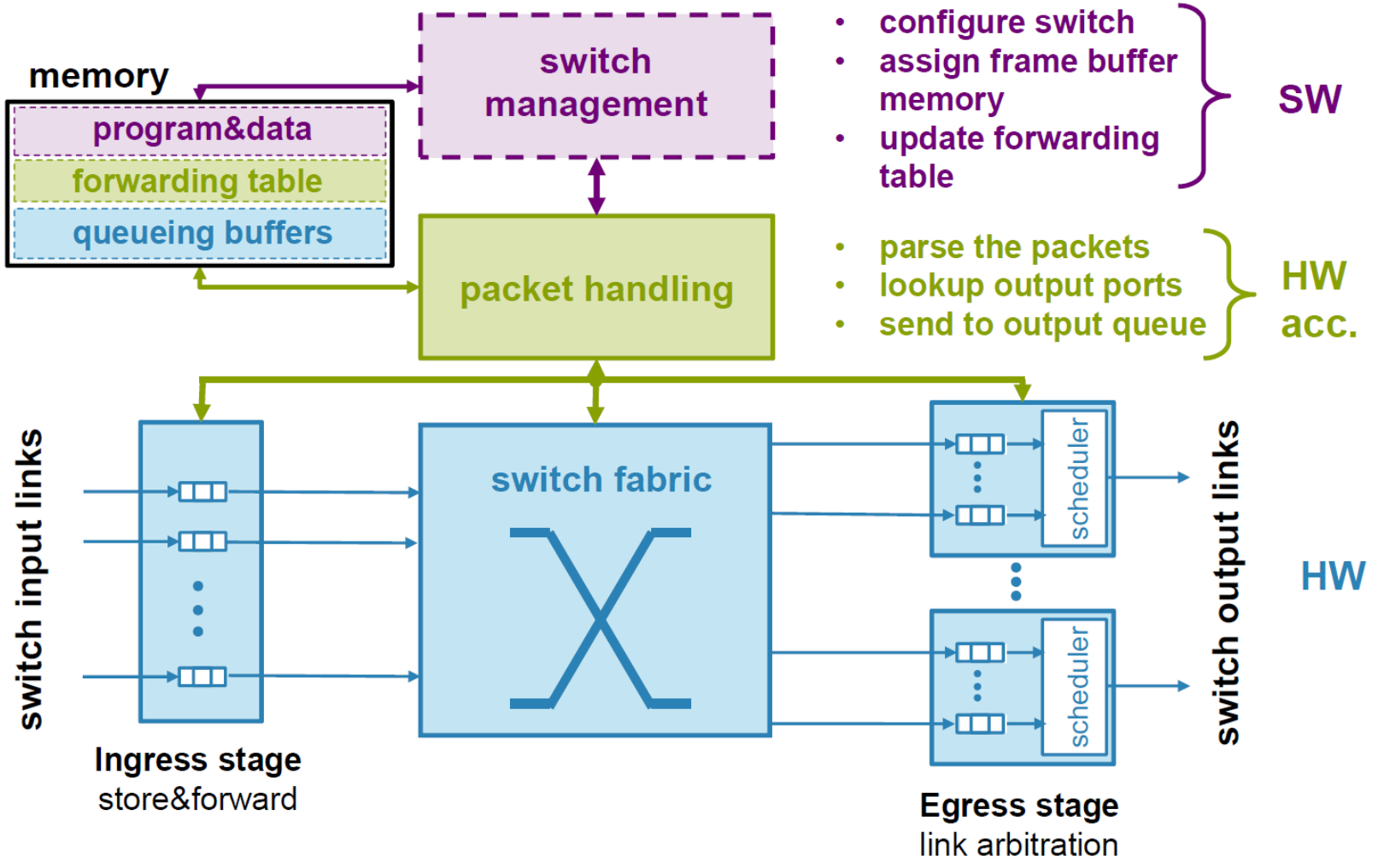
Safety Aspects of Ethernet and TSN

- **Apply similar techniques**
  - Assign priority/preemption classes according to criticality
  - Utilise shaping where necessary
  - Time-triggering
  - Support combinations



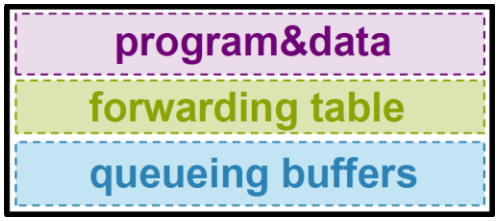
But is the isolation effective?

Ethernet Switch Structure

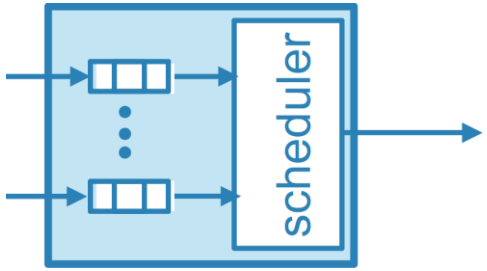


Ethernet Switch Challenges

- **Forwarding table**
  - **Limited index space** leads to indexing conflicts
    - Loss of timing → **interference**
  - Thoughtful MAC address management required



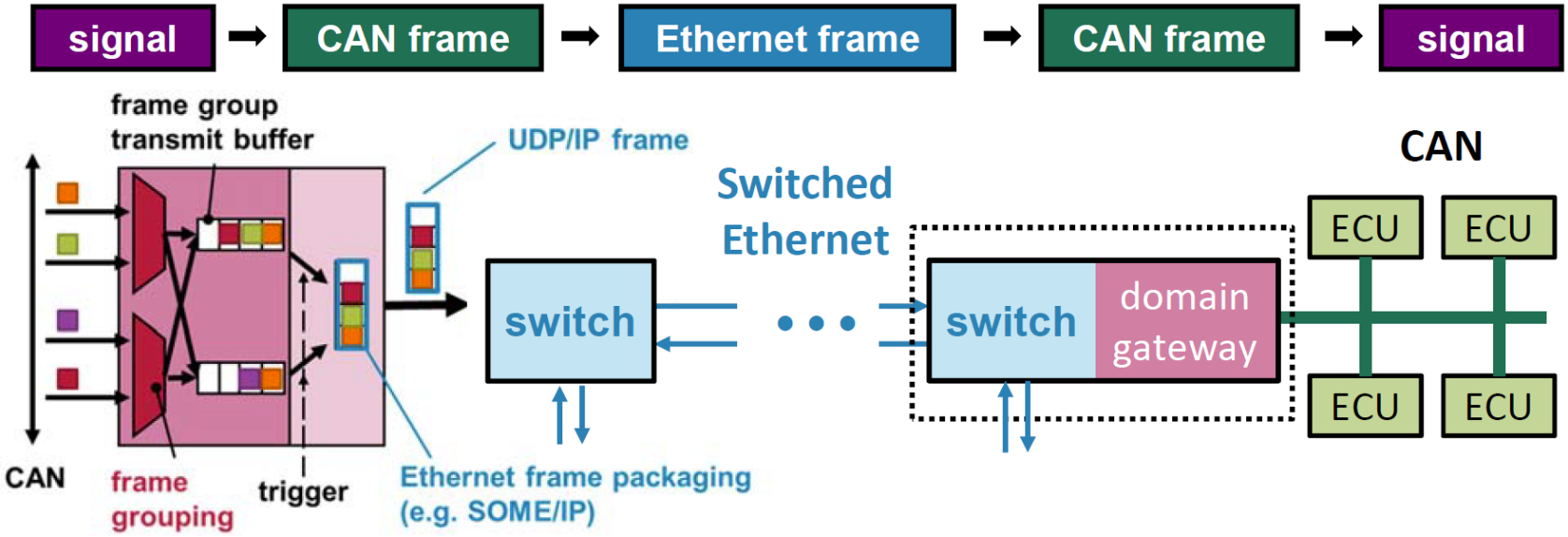
- **Queuing buffers**
  - **Limited buffer space**
    - Packet drop → **interference**
  - **Flow control**
    - Same-priority blocking, increased delay & buffer
  - **Few queues → few priorities**
    - Head of line blocking → **interference**



  - Queuing effects require **system-level end-to-end analysis**

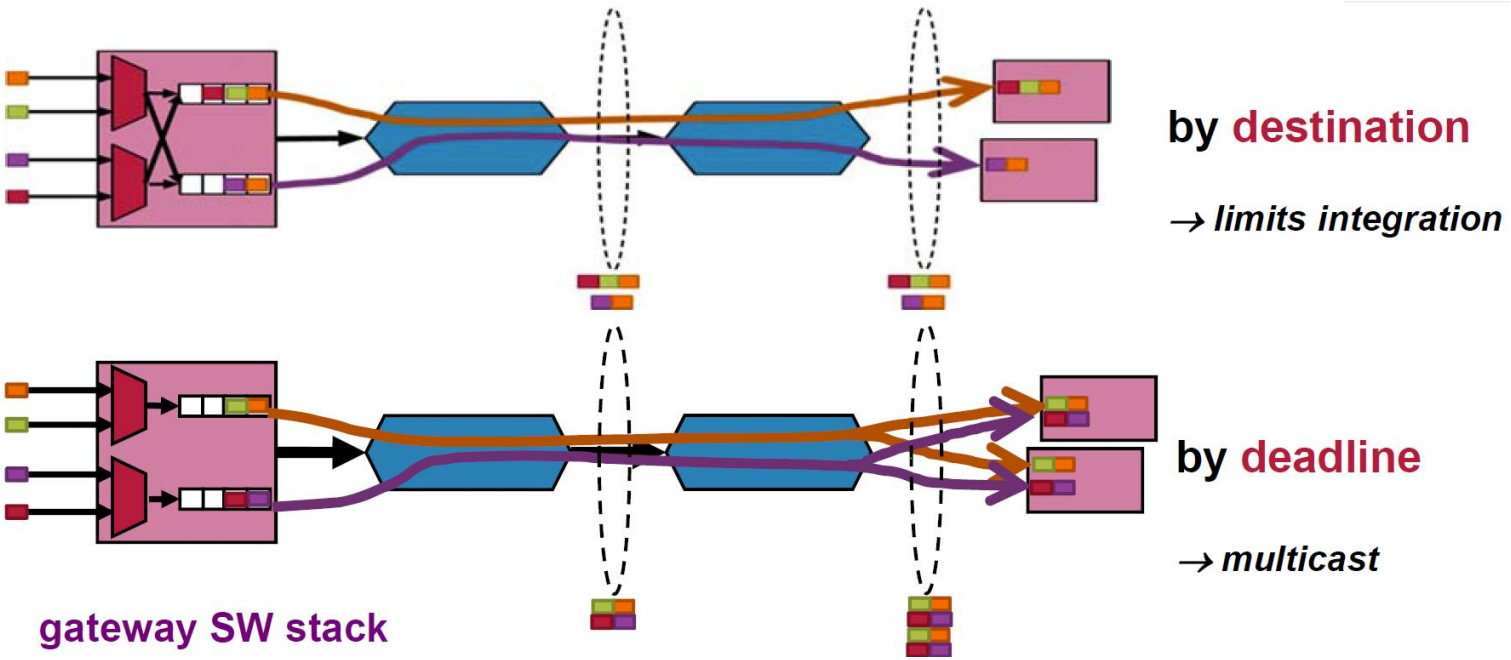
Gateway Safety Aspects (CAN → Ethernet scenario)

- **Complex protocol choices**
  - SOME/IP – UDP – IP – MAC
  - TCP – IP – MAC
- **Packaging** is additional **source of interference**



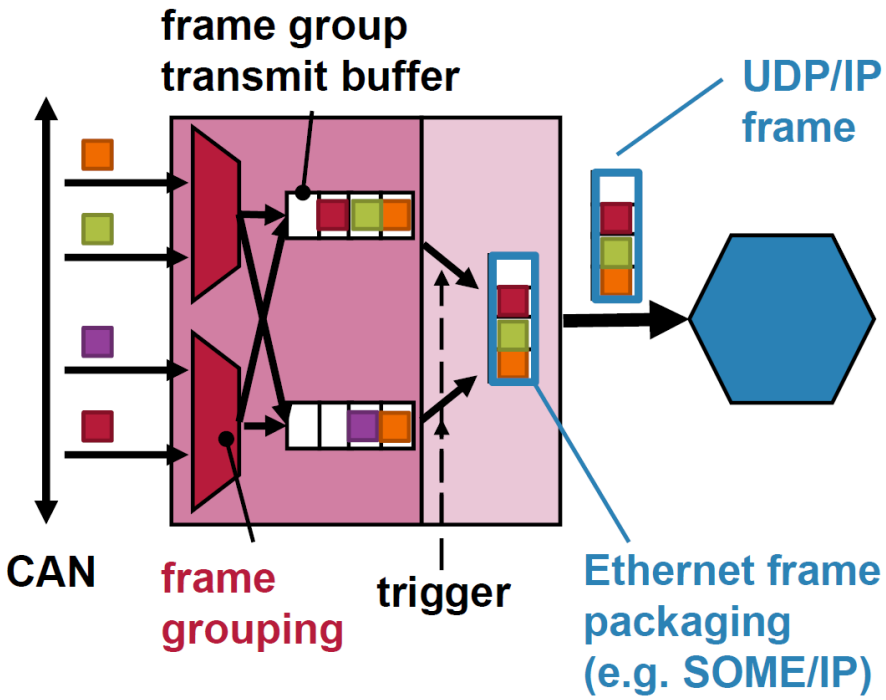
Gateway Safety Aspects (CAN → Ethernet scenario)

- **Signal grouping:**
  - By **destination** – minimise multicast overhead
  - By **priority** (e.g. CAN ID) – enable QoS for different traffic classes
  - By **period** or **deadline** – minimise sampling delay



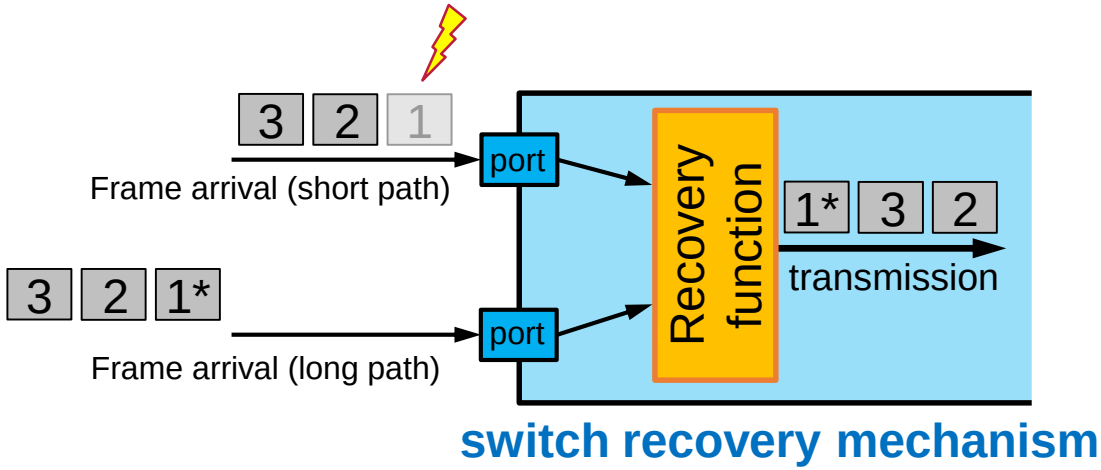
Gateway Safety Aspects (CAN → Ethernet scenario)

- **Transmission triggering:**
  - **Buffer timeout** (AUTOSAR)
    - Frame is sent periodically
    - **No interference**
  - **Buffer full event** (AUTOSAR)
    - Frame transmitted if buffer full
    - **Interference**
  - **Trigger frames** (AUTOSAR)
    - Immediate release of certain frames
    - **Interference**
  - **Per-frame timeout**
    - Send upon individual frame timeout



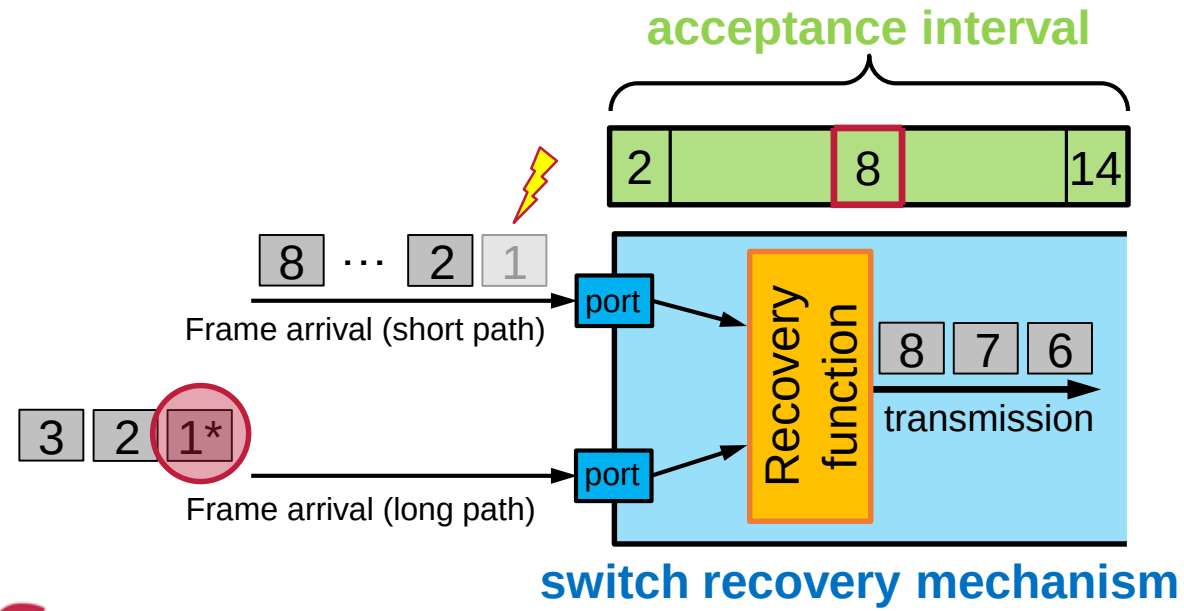
IEEE 802.1CB Safety Aspects

- **Standard does <u>not</u> prevent out of order transmission of frames**
  - Key “unlock – lock” commands, sensor inputs
  - Order preservation must be manually implemented → **interference**



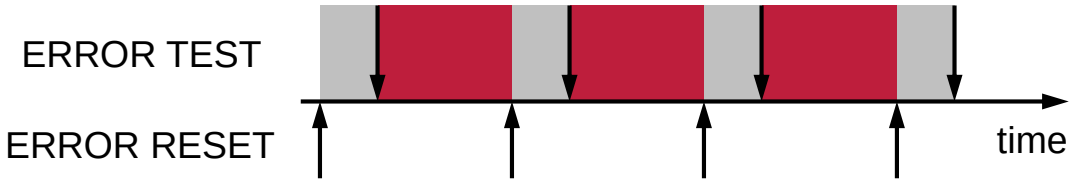
IEEE 802.1CB Safety Aspects

- **Standard does not prevent out of order transmission of frames**
  - Key “unlock – lock” commands, sensor inputs
  - Order preservation must be manually implemented → **interference**
- **Standard does not prevent acceptance interval misconfiguration**
  - Possible dropping of valid frames → **interference**



IEEE 802.1CB Safety Aspects

- **Standard does not prevent out of order transmission of frames**
  - Key “unlock – lock” commands, sensor inputs
  - Order preservation must be manually implemented → **interference**
- **Standard does not prevent acceptance interval misconfiguration**
  - Possible dropping of valid frames → **interference**
- **Standard does not provide rigorous fault detection mechanism**
  - Periodic latent fault test routine
  - Works on the level of estimates, “guesses”
  - Coverage issues



IEEE 802.1CB Safety Aspects

- **Standard does not prevent out of order transmission of frames**
  - Key “unlock – lock” commands, sensor inputs
  - Order preservation must be manually implemented → **interference**
- **Standard does not prevent acceptance interval misconfiguration**
  - Possible dropping of valid frames → **interference**
- **Standard does not provide rigorous fault detection mechanism**
  - Periodic latent fault test routine
  - Works on the level of estimates, “guesses”
  - Coverage issues
- **Propagation of fault information not addressed**
  - Mechanism needed to timely inform controlling entities about faults
  - Paramount for fail-operational behaviour

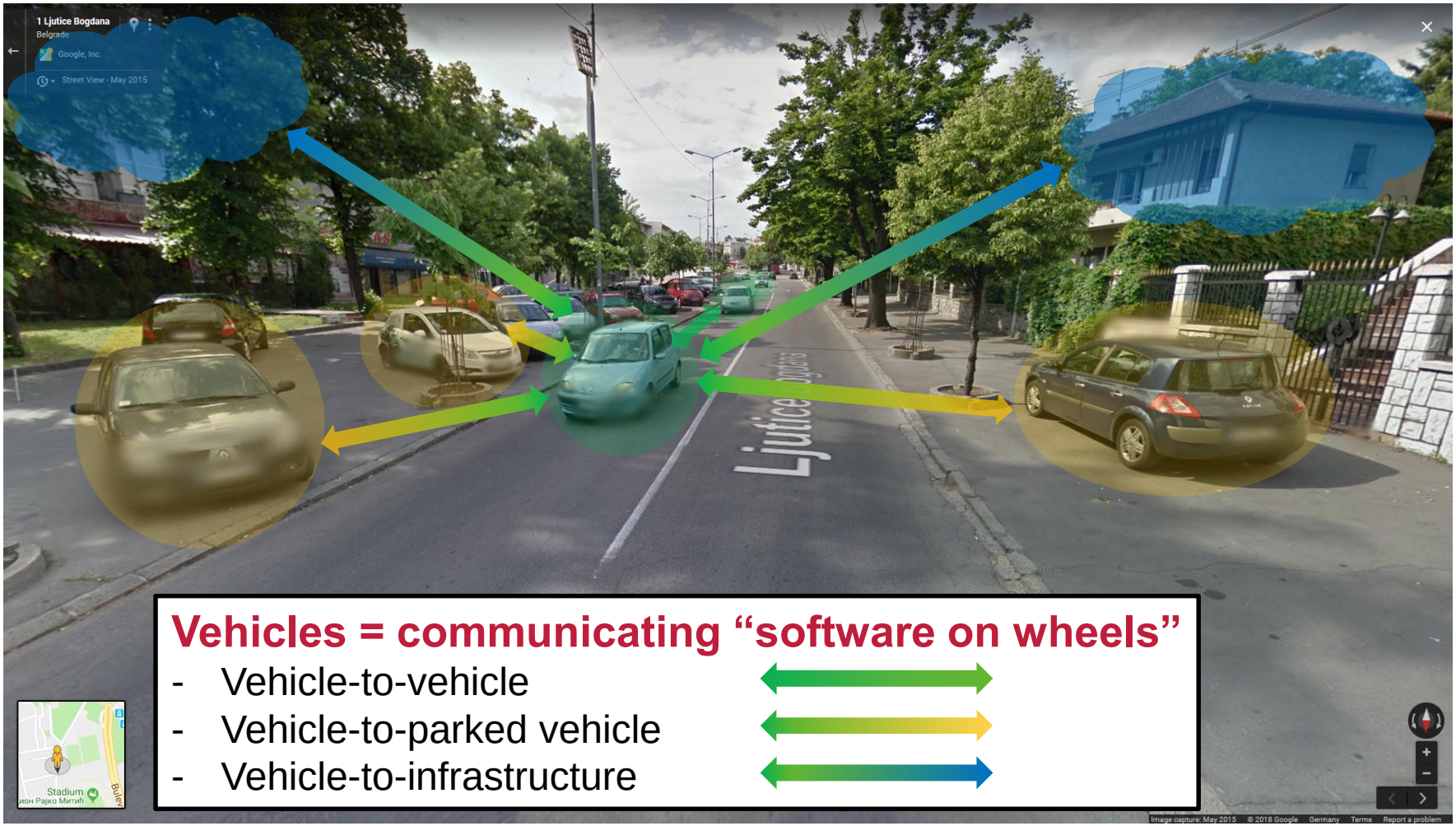
Safety Aspects of Ethernet and TSN

- **Plethora of configuration and misconfiguration opportunities**
  - MAC address management
  - Switch management
  - Protocol selection
  - Gateway packaging strategies
- **TSN increases the feature set**
  - Standardisation addresses compatibility, does **not** limit variety
  - Some additions seem similar to AVB (ATS former UBS)
  - **Increased** protocol and circuit **complexity** as well as **switch cost**
  - Are all TSN features useful?
- **Standardised does not necessarily mean safe "out of the box"**
- **Thoughtful application & systematic approaches required!**

Outline

- Automotive trends – Past, Present and Future
- Automotive Ethernet & TSN
- Safety Aspects
- **Security Aspects**
- Conclusions

Automotive trends – Future

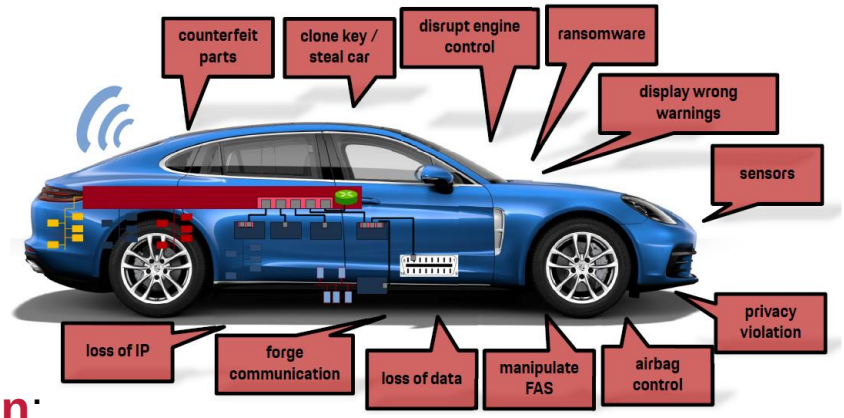


Security Aspects of Ethernet and TSN

- **Security** Goals:
  - **Confidentiality** – Protection against unauthorised access to functions and/or information
  - **Integrity** – Correctness of data and system functions
  - **Availability** – Functions and information are available whenever needed
- Properties:
  - Trade-off effort/cost vs level of achieved security level
  - Continuous activity, degrades over time, needs updates
  - Overheads of security measures
- Until few years ago, security not the main concern in Automotive domain
  - First and last talk at AN'17 about security
  - Still gaining increasing amount of attention

Security Aspects of Ethernet and TSN

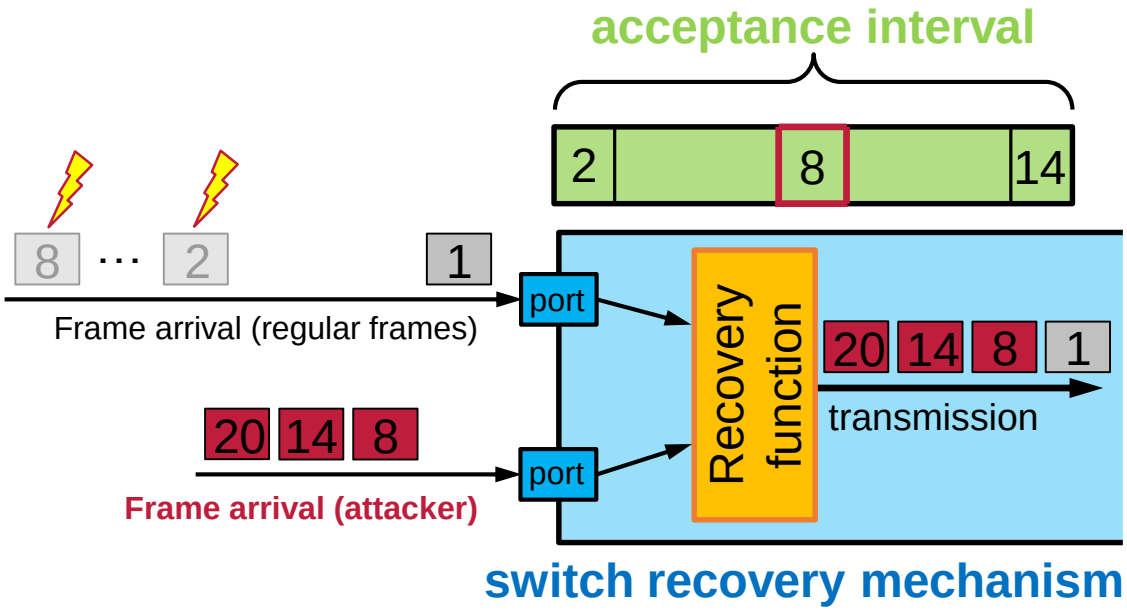
- Automotive vehicles = highly communicating “software on wheels”
- External systems and networks:
  - **Enable** sophisticated **functionalities**
  - But also **increase risk**!
- External threats:
  - **Attacks** and intrusions **via communication**:
    - WIFI, V2V, V2I, Charging stations, mobile device, app. centers
    - Cloud and Edge computing
- Internal threats:
  - Misbehaving & **malicious software**
    - Not all features thoroughly tested
- **Mechanisms** to protect **against both types** of threats **necessary**



Source: Dr. Christian Meineck @ AN’17

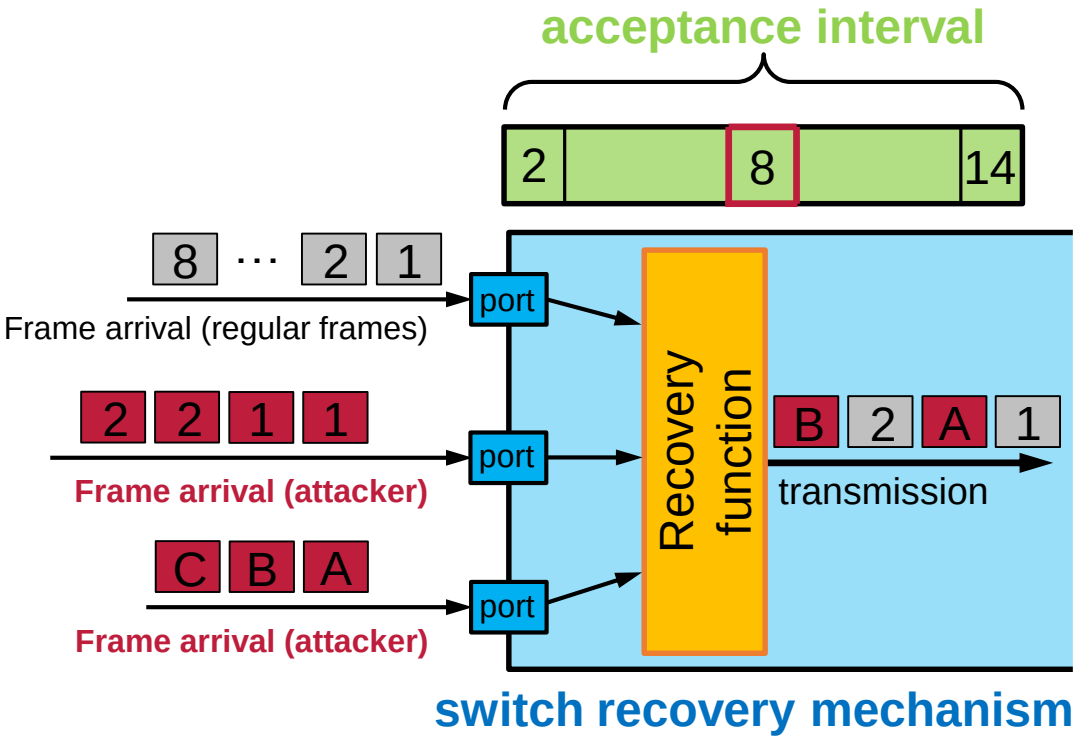
Security Aspects of Ethernet and TSN

- Attack Examples via 802.1CB:
  - Exploiting Acceptance Interval



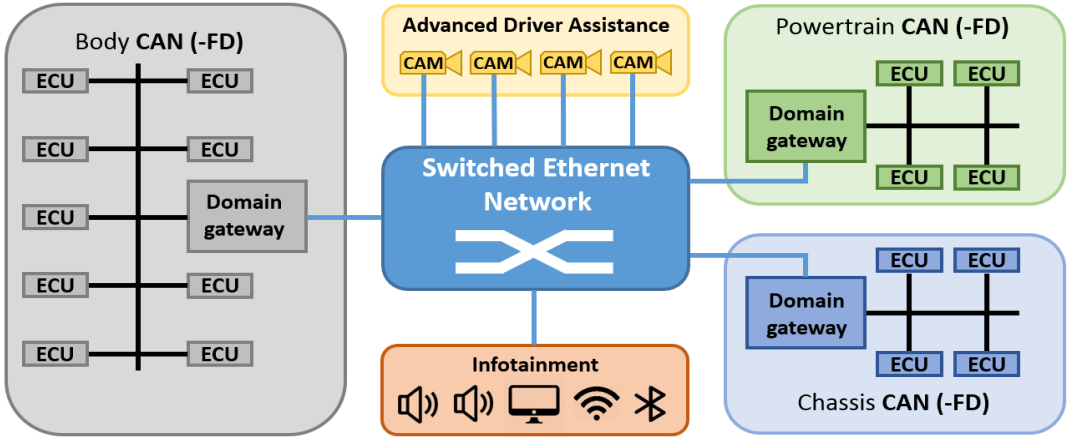
Security Aspects of Ethernet and TSN

- Attack Examples via 802.1CB:
  - Exploiting Acceptance Interval
  - Exploiting Elimination Mechanism



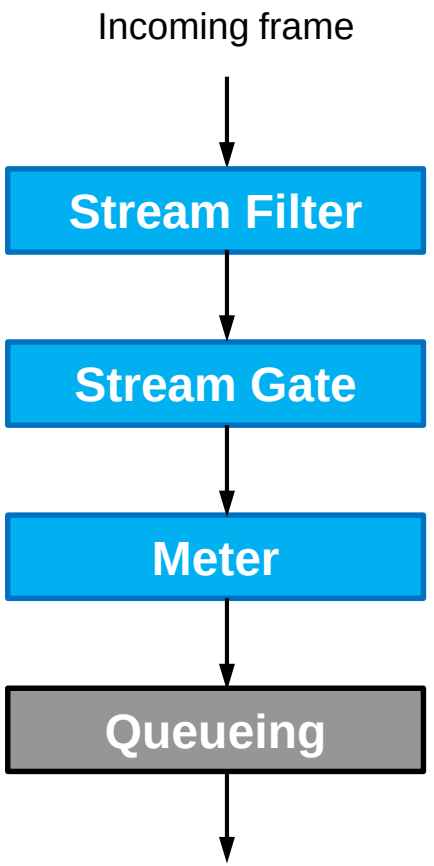
Security Aspects of Ethernet and TSN

- **Security Measures**:
  - **Separation**
    - Build internal security zones
    - Separate internal from external traffic
    - Minimise external connections
    - Use 802.1Q to classify traffic
    - Filtering



IEEE 802.1Qci Security Aspects

- Protection Against:
  - Bandwidth Violation
  - Malfunctioning
  - Malicious Attacks
- Decisions on a per-stream basis
- Stream Filter
  - Filters, Counters
- Stream Gate
  - **Open** or **Closed**
  - Can be time-scheduled
- Meter
  - Bandwidth Profile
  - **Red** / **Yellow** / **Green** Marking

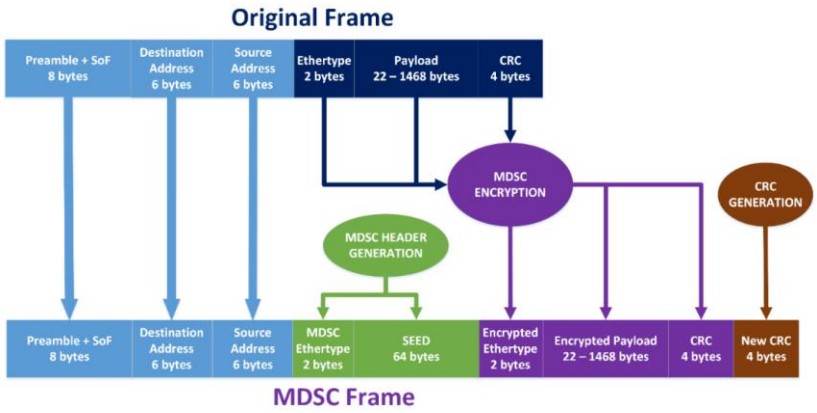


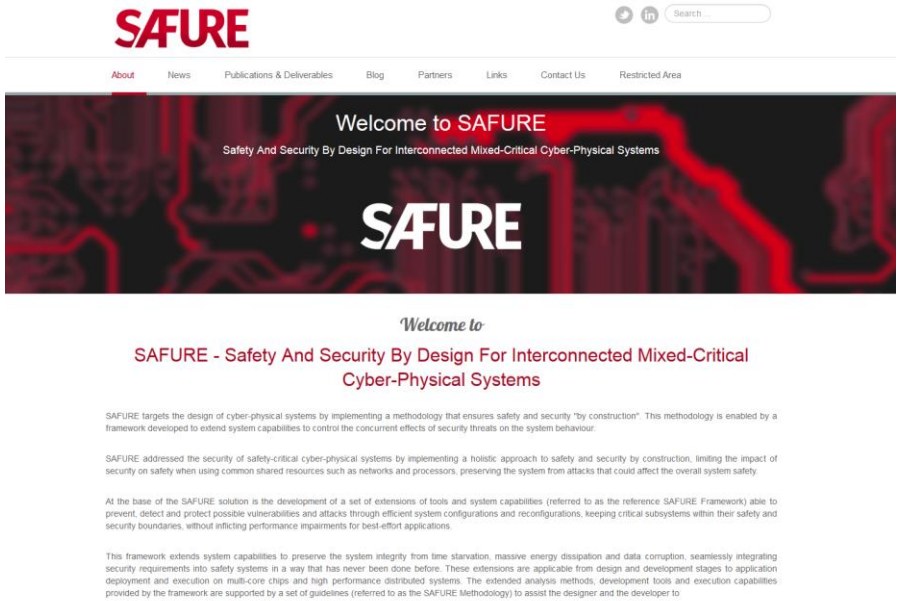
Security Aspects of Ethernet and TSN

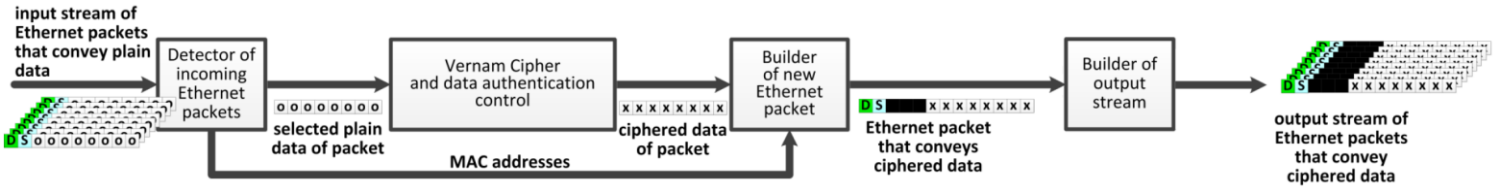
- **Security Measures**:
  - **Separation**
  - **Authentication, Encryption**
    - Hop-by-hop vs End-to-end
    - Encryption layer
    - Encrypted information
    - Encryption vs Integrity checks
    - Protection of all vs selected traffic

Security Aspects of Ethernet and TSN

- **MDSC** = Metadat Stream Cypher (TTTech)
  - SAFURE Project
  - End-to-end encryption
  - Applied on Layer 2
  - Compatible with TTEthernet

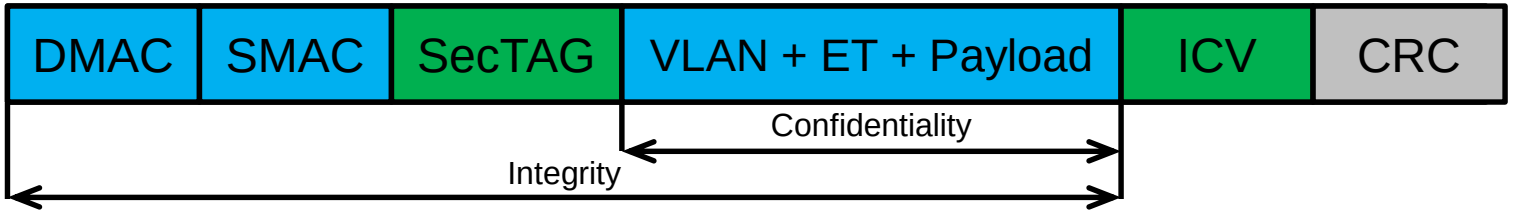






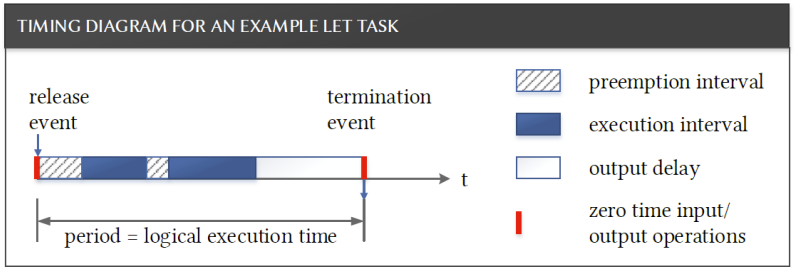
Security Aspects of Ethernet and TSN

- **MACsec (IEEE 802.1AE) applied on Layer 2**
  - "*... allows authorized systems that attach to an interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.*"
  - Compatible with other IEEE 802.1 standards
  - Hop-by-hop
  - Relatively simple to implement
  - Provides: source authentication, data integrity and data confidentiality
  - Protection against: Wiretapping, Impersonation, Masquerading, **Man-in-the-Middle**, Replay, Denial-of-Service



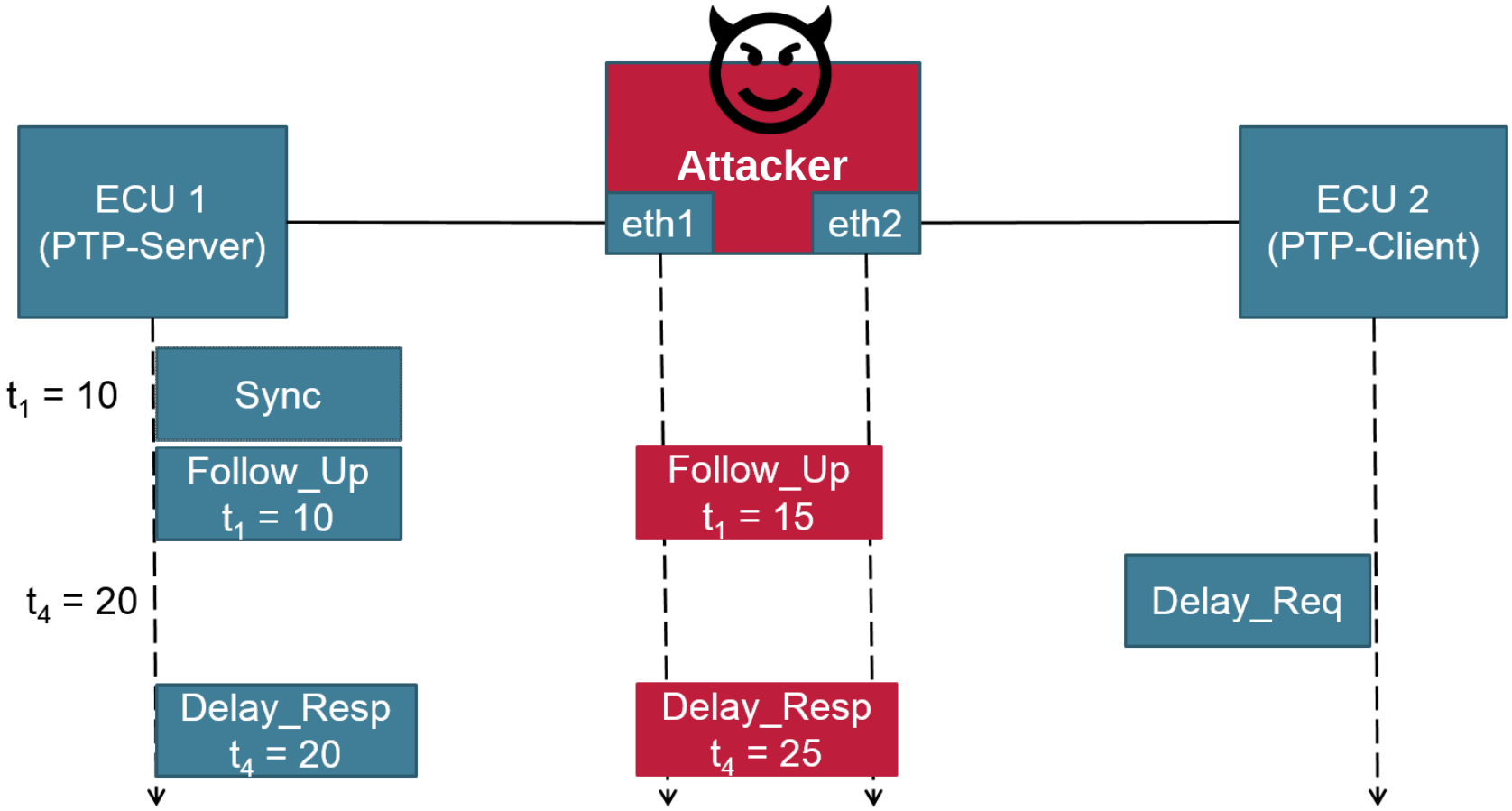
Security Aspects of Ethernet and TSN

- In Ethernet and TSN Networks **timing** very **important**
- Precision Time Protocol (**PTP**)
  - IEEE 1588 HW/SW
  - IEEE 802.1AS (-Rev*)
- Attacks on synchronisation may have catastrophic consequences
- Directly Affected Concepts
  - IEEE 802.1Qbv
  - LET (Logical Execution Time) Paradigm

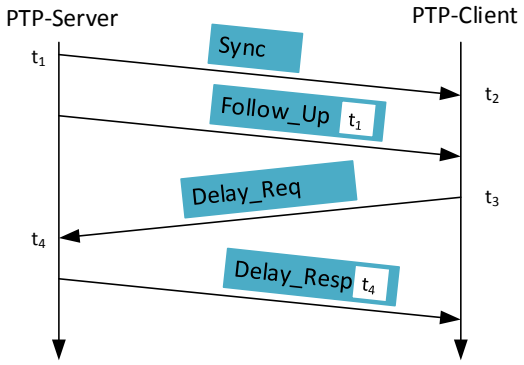


Security Aspects of Ethernet and TSN

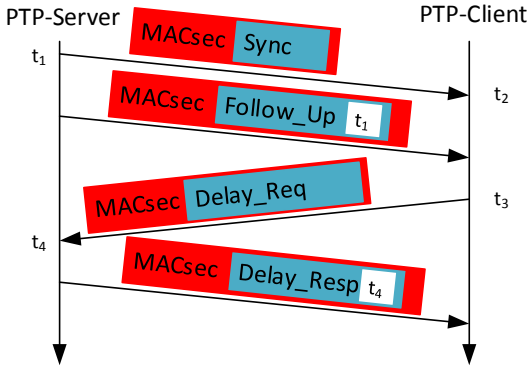
- Attack scenario (Man-in-the-Middle)



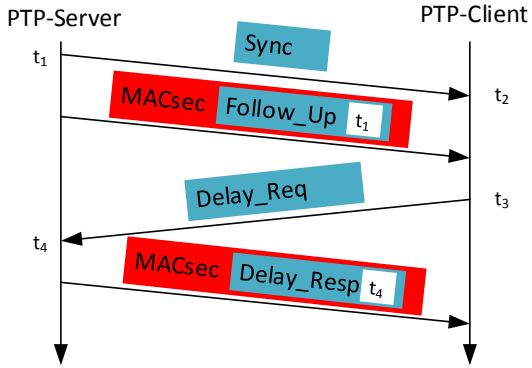
Security Aspects of Ethernet and TSN



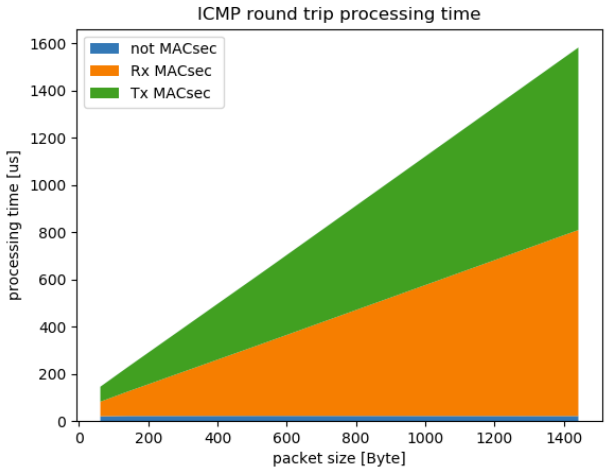
Unprotected PTP

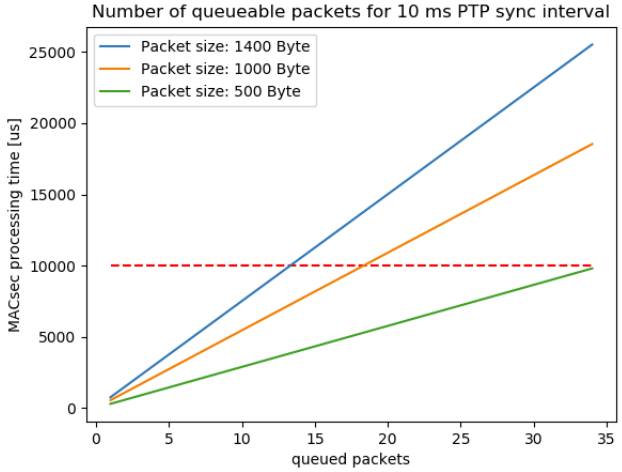


Full MACsec protection



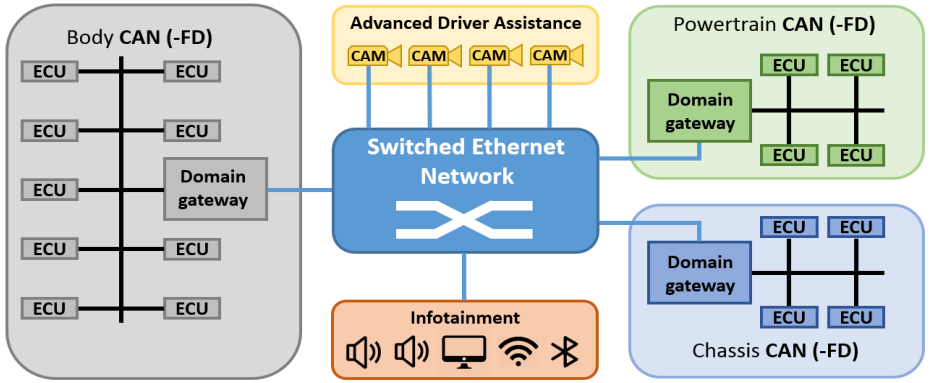
Partial MACsec protection





Security Aspects of Ethernet and TSN

- **Gateways are sensitive network points**
  - Single point of failure
  - Interfaces between domains, often traffic of diverse nature
  - More complex logic and functions than switches
  - Packing and triggering strategies particularly exploitable
  - Security aspects of GW = relevant topic, requires additional attention



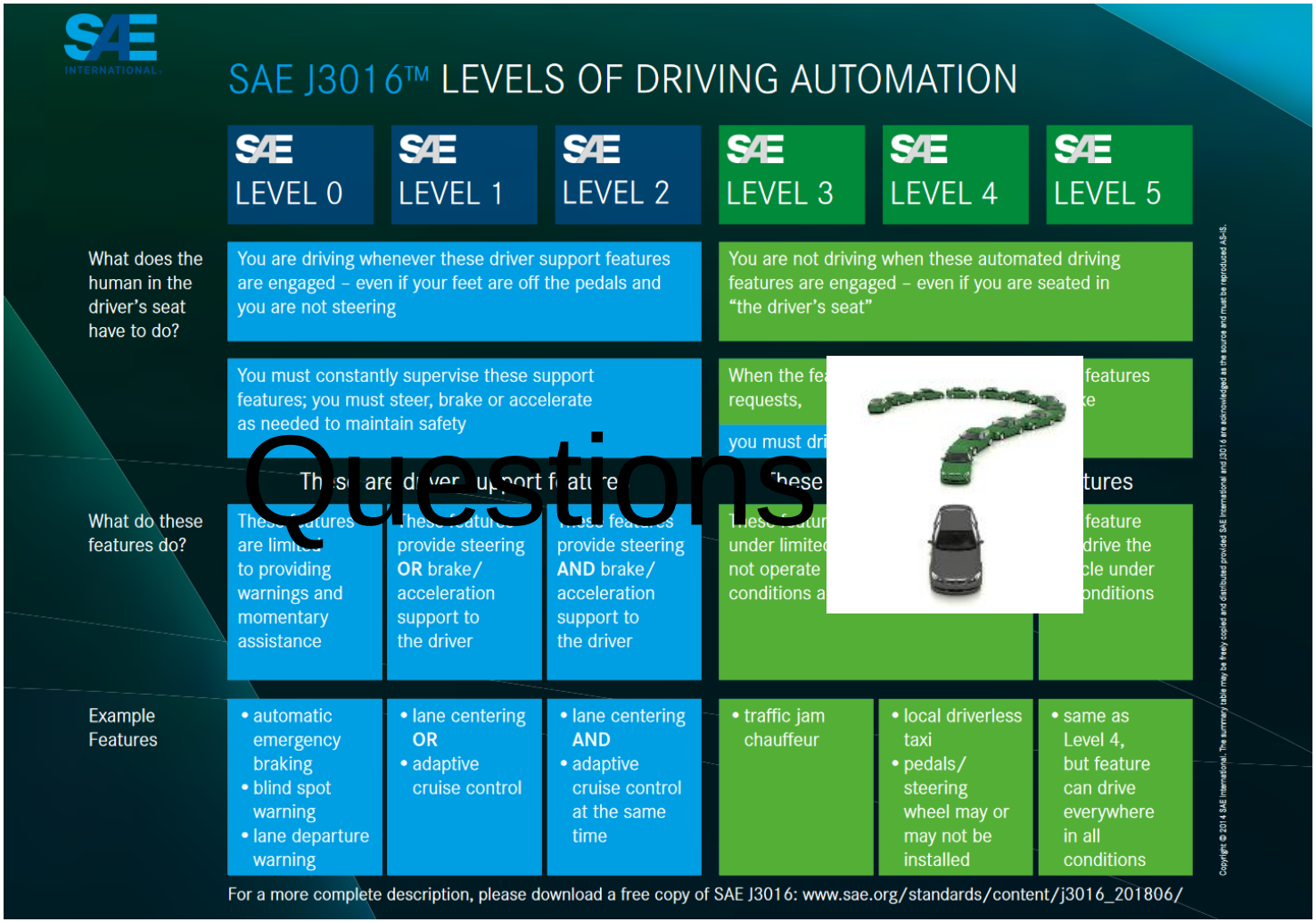
Outline

- Automotive trends – Past, Present and Future
- Automotive Ethernet & TSN
- Safety Aspects
- Security Aspects
- **Conclusions**

Conclusions

- **Ethernet and TSN** = **promising** automotive networking technologies
- Many **opportunities & pitfalls**, **careful application** necessary
- **TSN** beneficial but **not panacea**
- Applying **standards** “out-of-the-box” **not always safe**
  - Examples AUTOSAR, IEEE 802.1CB
- **Security** relatively new topic in Automotive domain:
  - Gains in importance due to the ***open-world* assumption**
  - Better understanding necessary (experience from other domains helpful)
  - **Integration** with existing and novel **technologies necessary**
  - **Trade-off** gains vs overheads
  - **Never settle**
- **Keep it simple**

Thank you for your attention!



Questions