Technische Universität Braunschweig

Smart Network Control in Automotive Systems

Adam Kostrzewa and Rolf Ernst
TU Braunschweig, Germany
IEEE SAC 4-6 September 2019

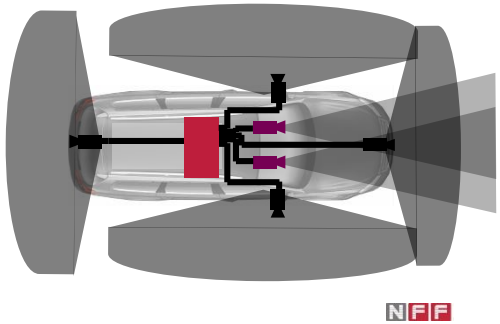
Outline

- **Automotive trends – Present and Future**
- **Automotive Ethernet – the safety perspective**
- **Automotive Networks – other challenges**
- **SDN – Promising Preliminary Solution**
- **Conclusions**

Automotive Systems - New Challenges

Trend 1: New applications

- networks with IP traffic via car-to-X communication
- *primarily best effort*



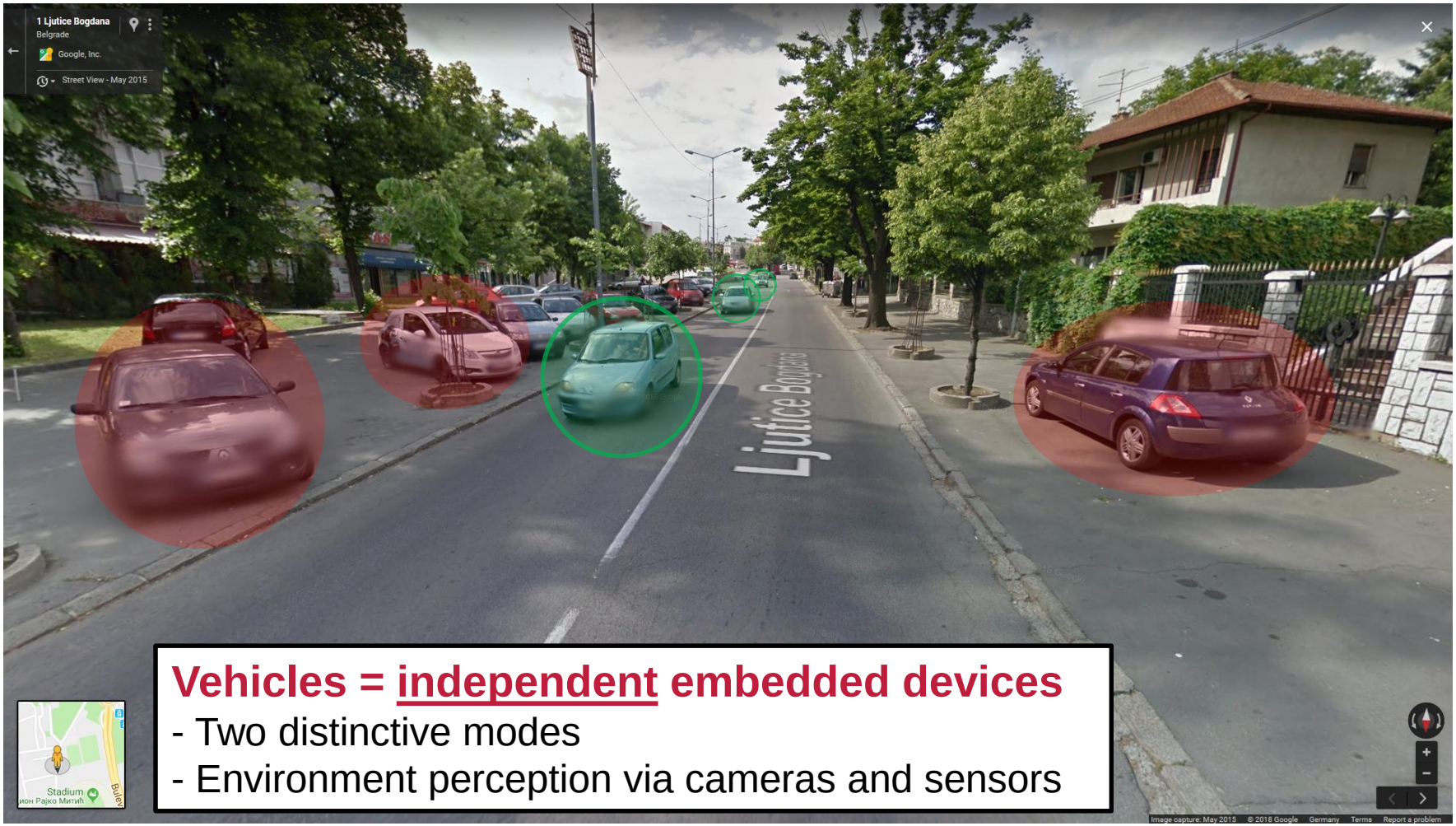
Trend 2: Quickly growing sensor traffic

- high resolution sensors for autonomous driving (e.g. LIDAR, radars)
- which are redundant
- in consequence high bandwidth communication and limited network latency (system response times)

Trend 3: Complex low latency traffic

- backbone function: legacy, future drives, highly interactive functions, ...
- low to medium volume, low latency traffic

Automotive trends – Present



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

- Two distinctive modes
- Environment perception via cameras and sensors

Example – ApolloScape from Baidu

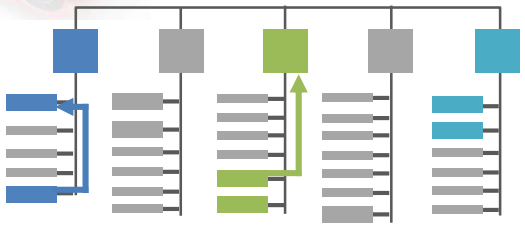
Sensor data:

- Two LIDARS (VMX-1HA modules)
  - 10Hz, avg. 1,6MB per frame
  - **16 MBps == 128 Mbps per lidar**
- Six video cameras (VMX-CS6 systems)
  - 30fps, 3384×2710 pixel resolution
  - avg, 2MB per frame, JPG 100% 24bit/pixel
  - **60 MBps = 480 Mbps per camera**
- Measuring head with IMU/GNSS
  - **below 1 Mbps**
- ***Additional radar data***
  - ***not included in the dataset but still necessary***

Source: **Baidu**, P. Wang, X. Huang, X. Cheng, D. Zhou, Q. Geng and R. Yang, "The ApolloScape Open Dataset for Autonomous Driving and its Application," in IEEE Transactions on Pattern Analysis and Machine Intelligence.

Bus-based communication

Quelle VW



- Straightforward support of **publisher-subscriber** mechanism
  - e.g. CAN msg. received by all nodes, sender is not aware of the readers
- Several application specific standards, CAN, FlexRay, LIN, ...
  - **relatively low data rates** < 100kbit ... 10Mbit (FlexRay, CAN FD)
- Predictable scheduling: **fixed priority** or **TDMA** or **slotted ring** (MOST)
- Routing by dedicated gateway (GW)
  - low speed allows SW implementation
- Majority of **communication constrained to a single domain** e.g. chassis, powertrain etc.

Are Bus-Based Architecture Sufficient?

		CAN	CAN-FD	FlexRay
Sensors	Req. \ Avail.	1 Mbps	10 Mbps	10 Mbps
1 Lidar	128 Mbps	✖	✖	✖
1 Camera	480 Mbps	✖	✖	✖

This is an entirely new world!

Reminder, bandwidth requirements per sensor

6 cameras and 2 lidars in Baidu ApolloScape dataset

Challenges:

- How can we increase the capacity of the automotive network?
- Without jeopardizing safety? (e.g. ISO26262)
- And rising design costs?

Why Ethernet in the Automotive Domain?

- **Bandwidth Promise**
  - **bandwidth, bandwidth, bandwidth …..**
  - 100Mb/s → 1Gb/s → 10Gb/s → …

- **Other benefits:**
  - open network capabilities
    - open protocols, IP protocols
  - shared technology cost
    - standard with high volume across industries
      - no headaches with next generation MOST, FlexRay, ...
    - huge engineering platform experience
      - avionics, industry ….

Ethernet → communication backbone

Outline

- Automotive trends – Present and Future
- **Automotive Ethernet – the safety perspective**
- **Automotive Networks – other challenges**
- **SDN – Promising Preliminary Solution**
- **Conclusions**

Future Networks in the Automotive Domain

- Heterogenous network architecture
  - switched networks + legacy bus-based interconnects
- Switched network instead of the bus
  - point-to-point connections with dynamic address handling
- Many configuration parameters
  - higher overhead than CAN
- ***Consequence for network properties and design?***
  - ***we solve one problem and encounter new ones!***

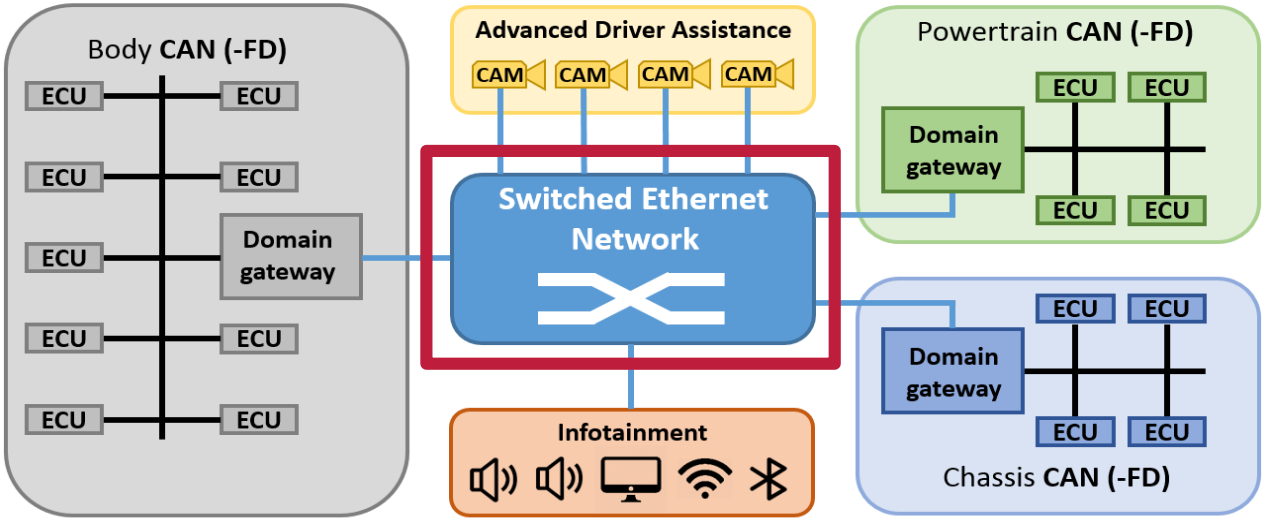
Automotive Ethernet Challenges

- **Lost inherent support for pub/sub mechanism** (switch-based)
  - need to use higher-level protocols
- **Routing necessary**
  - different routing mechanisms, flow control
  - *note: Ethernet-bus not suitable*
- **Different communication schemes**
  - unicast, multicast, broadcast
- **Freedom from interference?**
  - switches (forwarding table eviction example)
  - gateway (packaging example)

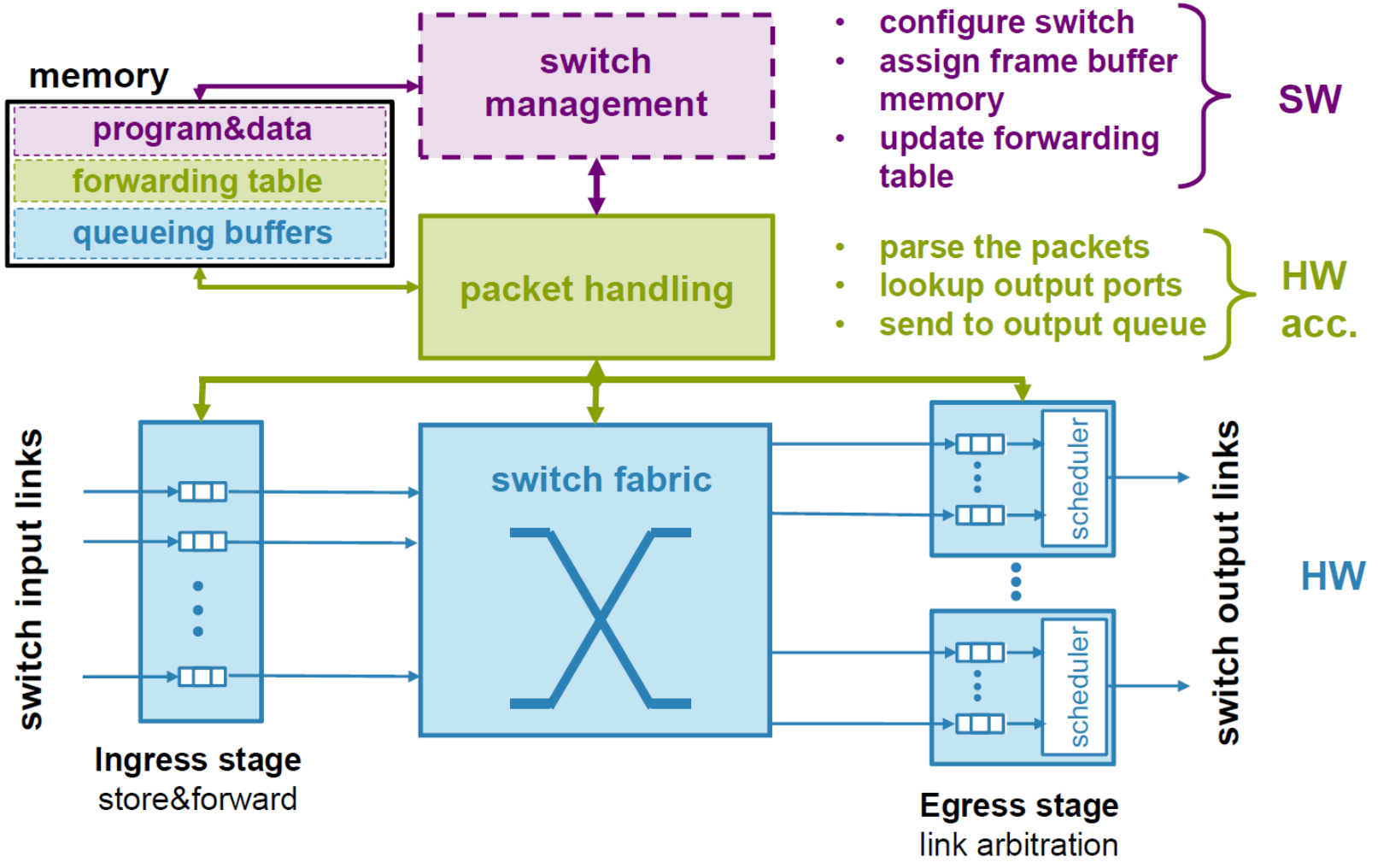
Ethernet was not designed for safety!

Ethernet in the Automotive Domain

- **Envisioned heterogeneous automotive architecture**
  - Note: Ethernet is a promising candidate for (future) monotechnological networks

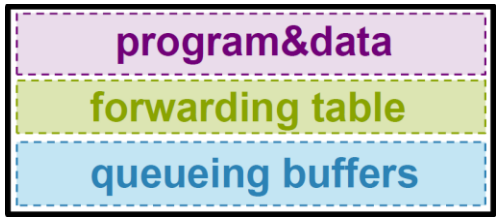


Ethernet Switch Structure

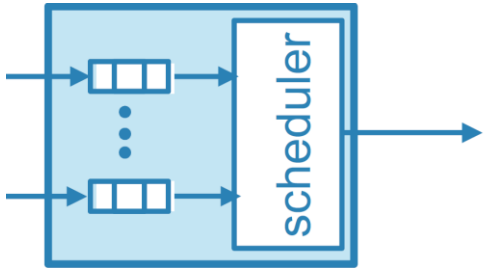


Ethernet Switch Challenges

- **Forwarding table**
  - **limited index space** leads to indexing conflicts
    - loss of timing → **interference**
  - thoughtful MAC address management required



- **Queuing buffers**
  - limited buffer space
    - message 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**

Ethernet IEEE 802.1Q – Standardization

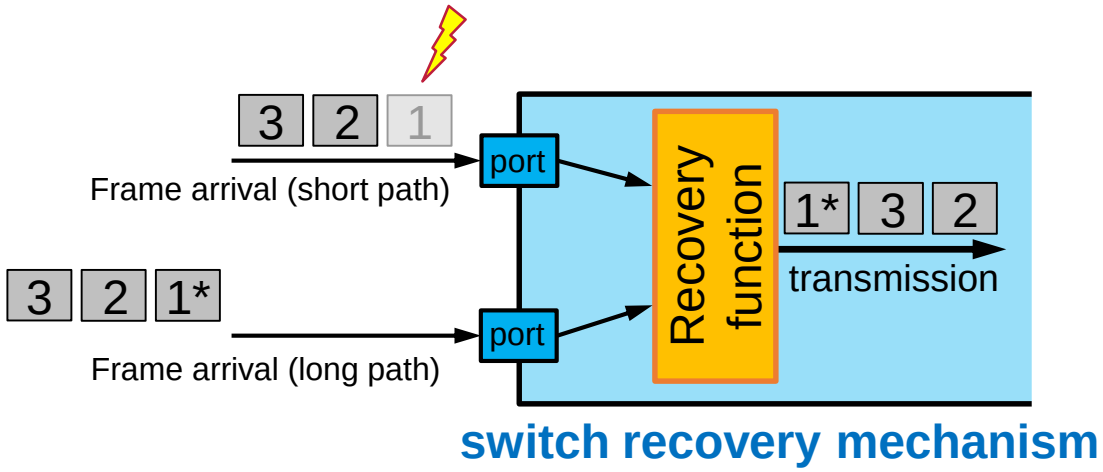
- **Standard Ethernet (IEEE 802.1Q)**
  - priority based
  - up to 8 priorities and 4096 VLANs
  - static priority scheduling
- **Ethernet AVB (IEEE 802.1Qav)**
  - originally defined for streaming applications
  - adds standardized traffic shaping to IEEE 802.1Q
  - 802.1AS: clock synchronization
- **Time-Sensitive Networking – TSN**
  - set of (draft) Ethernet standards addressing real-time requirements

TSN Arbitration and Shaping

- **Frame preemption** (IEEE 802.1Qbu)
  - reduce blocking time by lower-priority fames
  - allow preemption of lower-priority frames (at certain points)
- **Ingress filtering** (IEEE 802.1Qci)
  - ensure that traffic streams stay within predefined bounds (fault containm.)
- **Timing and synchronization**(IEEE 802.1ASbt)
  - extensions to 802.1AS: redundant masters, multiple time domains
- **Time triggering**(IEEE 802.1Qbv)
  - time aware shaper for low latency, time sensitive traffic
  - more shapers: burst limited,
- **Asynchronous traffic shaper**(IEEE 802.1Qcr)
- And many more … (e.g. IEEE 802.1CB FRER)

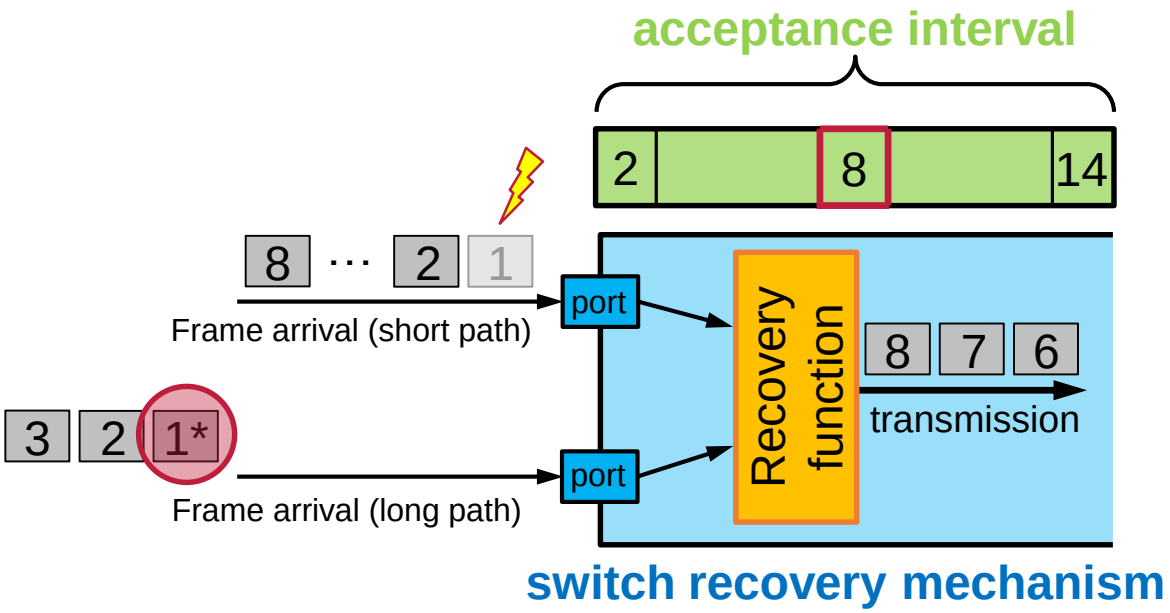
IEEE 802.1CB (out of order example)

- **Standard does not prevent out of order transmission of frames**
  - key “unlock – lock” commands
  - order preservation must be manually implemented



IEEE 802.1CB (out of order example)

- **Standard does not prevent acceptance interval misconfiguration**
  - possible dropping of valid frames

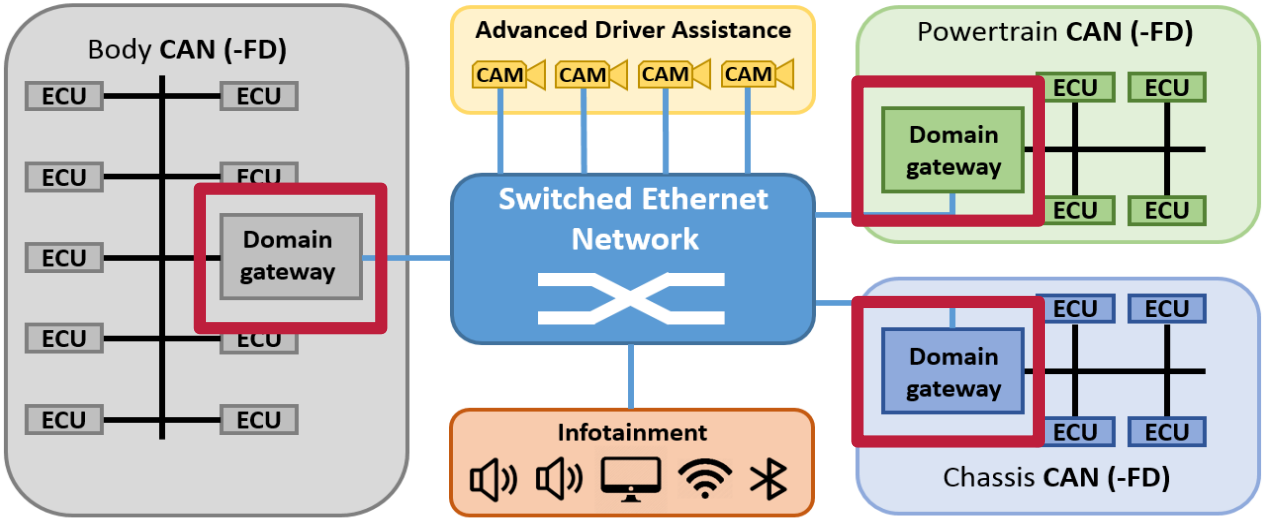


Automotive Ethernet Challenges

- **Plethora of configuration and misconfiguration opportunities**
  - MAC address management
  - switch management
  - protocol selection
- **TSN increases the feature set**
  - standardisation addresses compatibility, does **not** limit variety
  - some additions seem redundant to AVB
  - **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"**
  - IEEE 802.1CB (out of order example, acceptance interval example)
  - **thoughtful application required!**

Ethernet in the Automotive Domain

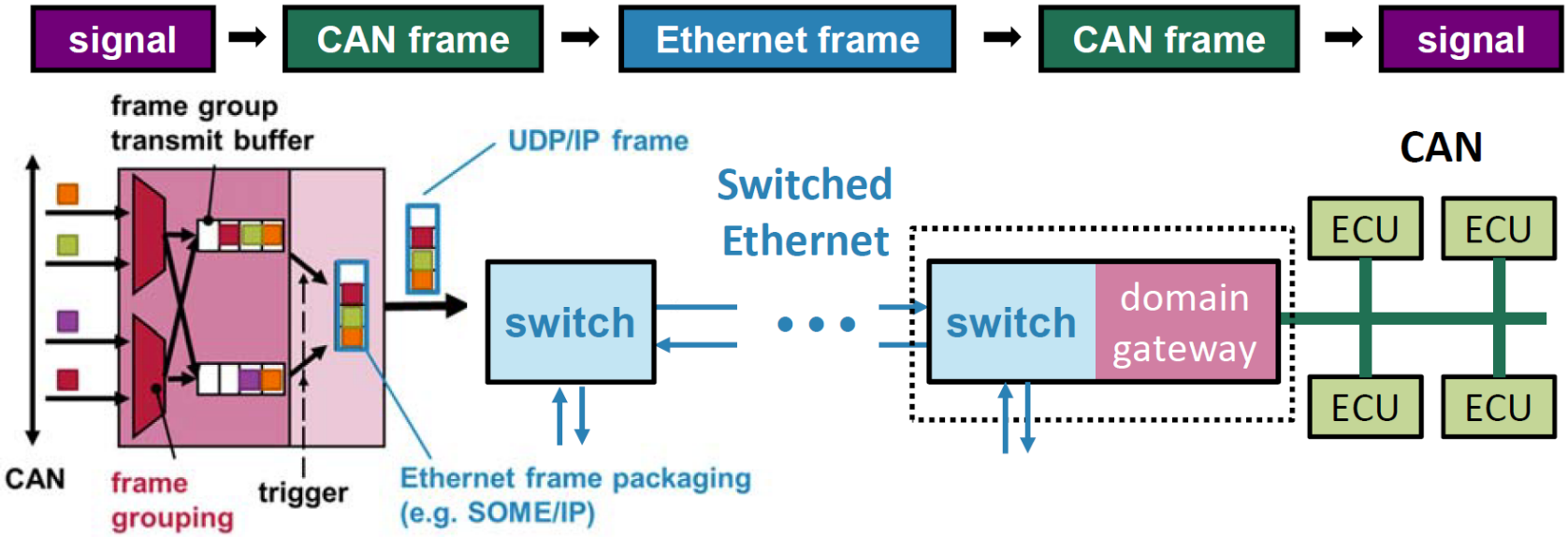
- **Envisioned heterogeneous automotive architecture**
  - Note: Ethernet is a promising candidate for (future) monotechnological networks



Gateway (CAN → Ethernet scenario)

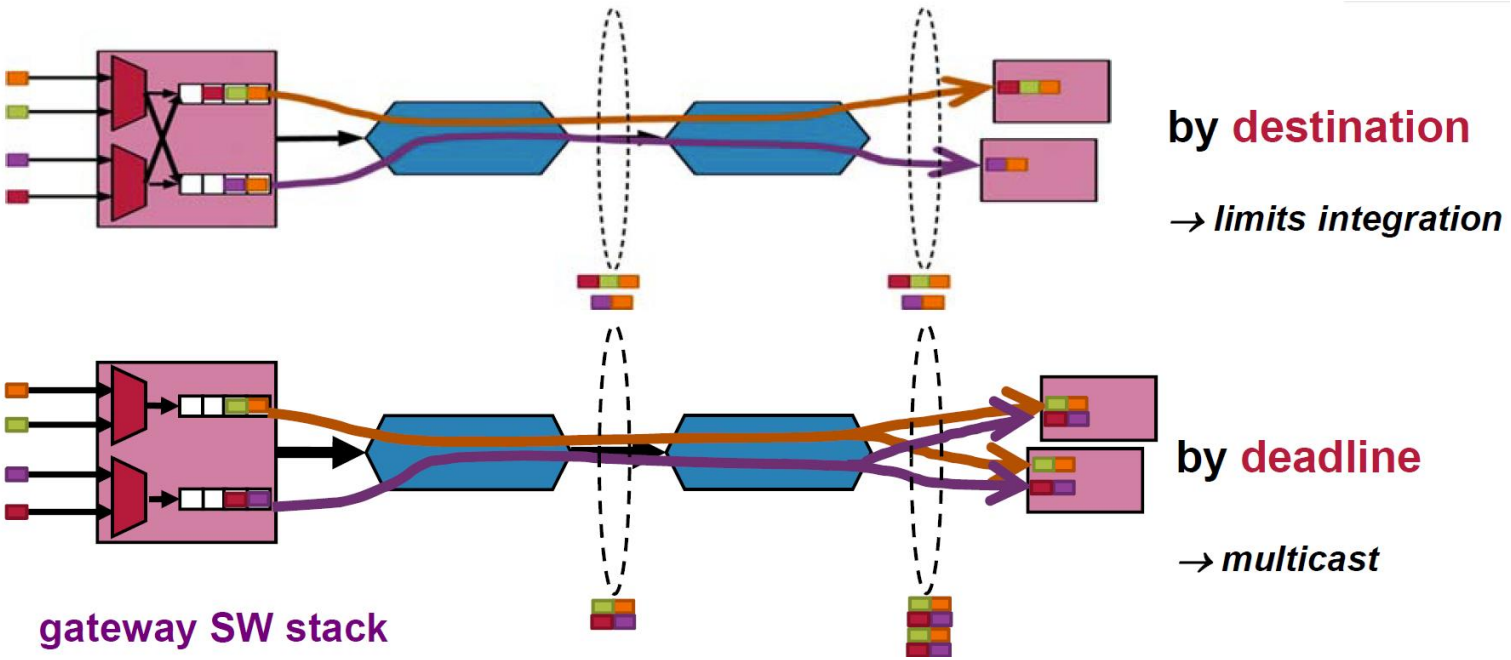
- **Complex protocol choices**
  - SOME/IP – UDP – IP – MAC
  - TCP – IP – MAC

- **Packaging** is additional **source of interference**



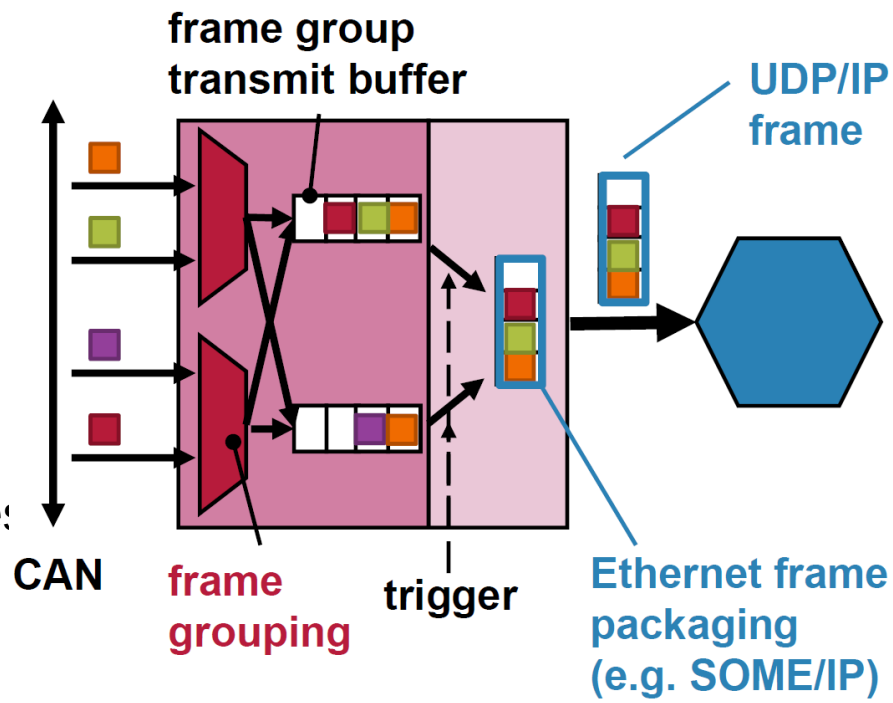
Gateway (CAN → Ethernet scenario)

- **Frame 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 (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



Automotive Ethernet Summary

- **Ethernet** – **promising** technology for **future automotive** networks
  - @AN'17: >50% participants foresee fully Ethernet-based in-vehicle networks

- Abundance of standards → **growing** protocol & circuit **complexity** and **cost**
  - **quantity ≠ quality**
  - lots of configuration and misconfiguration opportunities
- Application requires **systematic approach** and **thoughtful consideration**

- How far can TSN take us down the automation path?
  - TSN = **T**owards **S**tatic **N**etworking?
  - *Conditional automation* (level 3) seems achievable

Automotive trends – Present

***Conditional automation* seems achievable**

- Requires certain conditions
- Driver must be ready to take control

Automotive Ethernet Summary

- **Ethernet** – **promising** technology for **future automotive** networks
  - @AN'17: >50% participants foresee fully Ethernet-based in-vehicle networks

- Abundance of standards → **growing** protocol & circuit **complexity** and **cost**
  - **quantity ≠ quality**
  - lots of configuration and misconfiguration opportunities
- Application requires **systematic approach** and **thoughtful consideration**

- How far can TSN take us down the automation path?
  - TSN = **T**owards **S**tatic **N**etworking?
  - *Conditional automation* (level 3) seems achievable

- **What about *High automation* (level 4) and *Complete automation* (level 5)?**

Outline

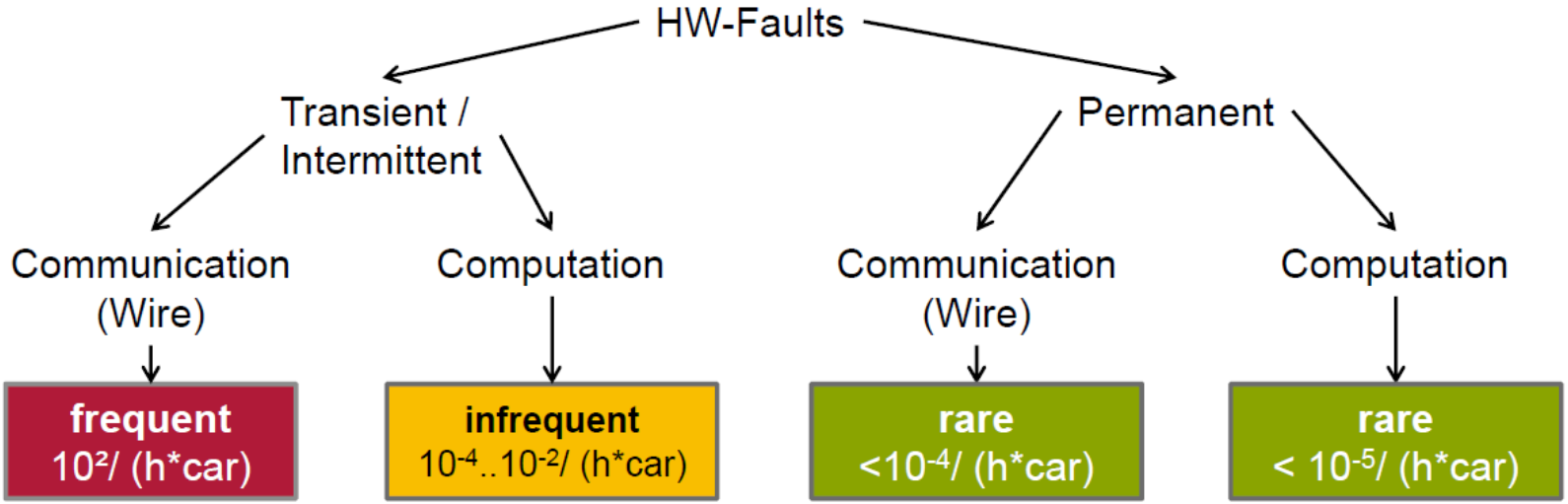
- Automotive trends – Present and Future
- Automotive Ethernet – the safety perspective
- **Automotive Networks – other challenges**
- **SDN – Promising Preliminary Solution**
- **Conclusions**

Ethernet – The safety perspective

- **Isolation**
  - how well does Ethernet isolate critical from other traffic?
  - „freedom from interference“
- **Delivery under transmission errors**
  - what timing guarantees are possible under errors?

Fault Tolerance

- A system must be able to handle transient/permanent faults
  - fail-safe behaviour
  - **fail-operational behaviour**

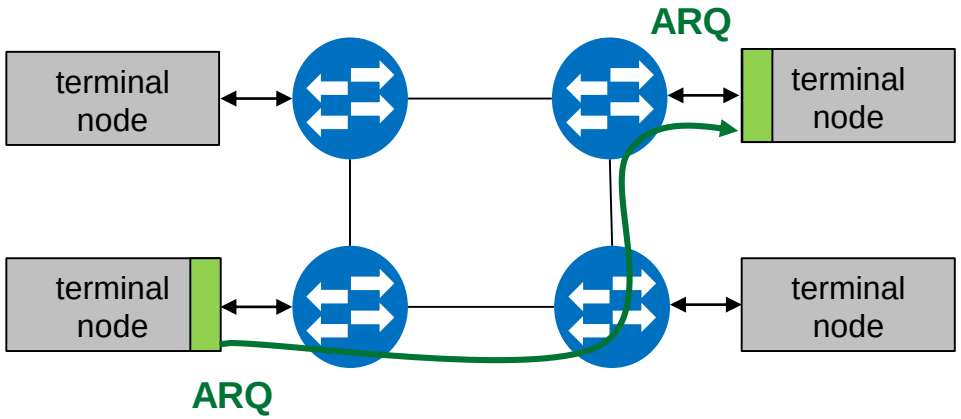


note: resulting computation errors strongly depend on state protection (memory)

- Transient transmission errors dominate
  - **transient error handling must be part of regular communication!**

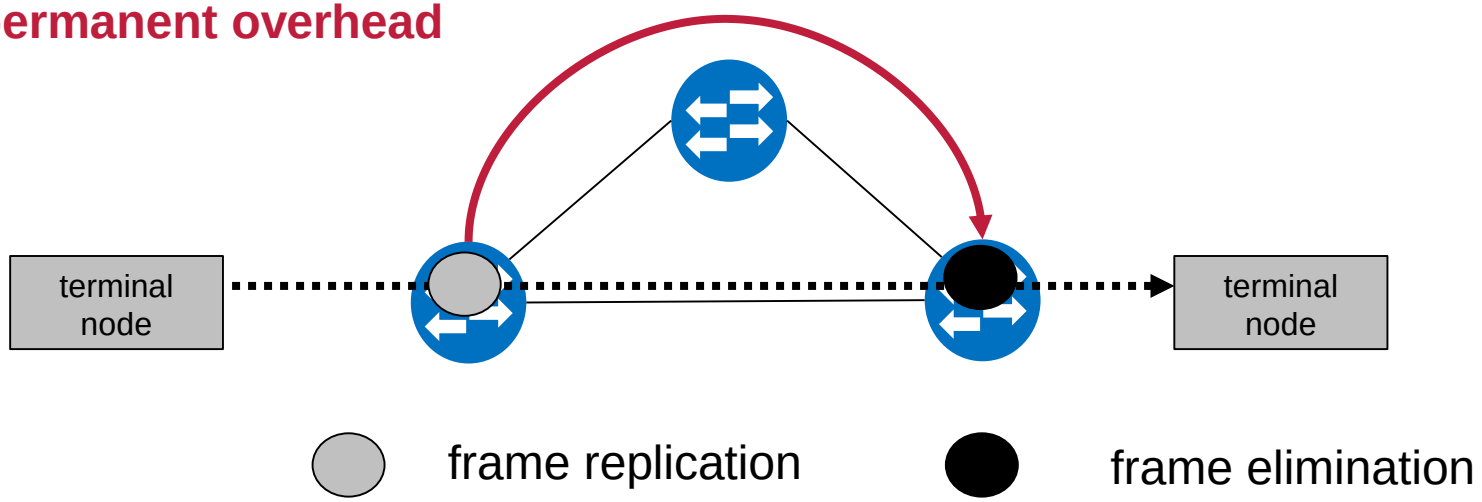
Communication under transient faults

- System must be capable of real-time operation
  - even under occasional transmission errors (cp. CAN, FlexRay, ...)
- **Suggest end-to-end error control**
  - overhead can be limited to critical messages
  - covers all error types (link, tail-drop, ...)



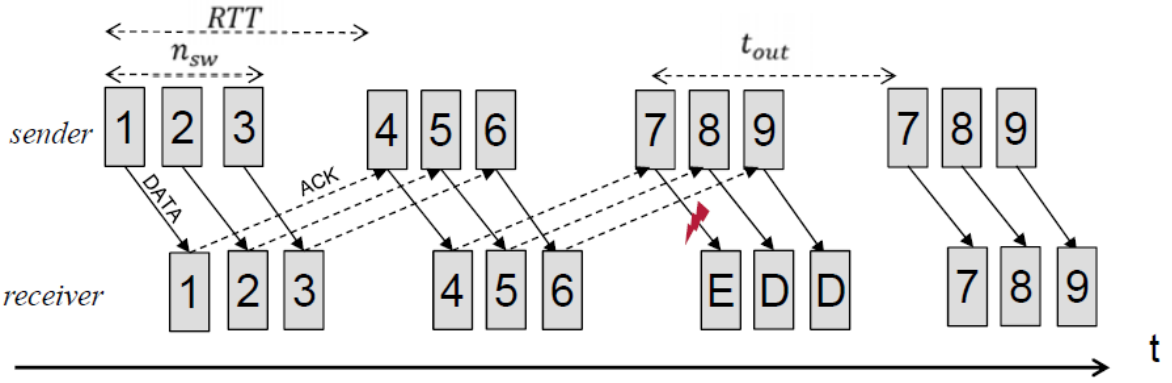
Fault Tolerance

- **FRER** (IEEE 802.1CB) one viable approach
  - frame copies via redundant paths (Spatial FRER)
  - alternatively, frame copies via same paths (Temporal FRER)
  - **proactive** mechanism, **requires** path **redundancy**
  - applicable to both **transient and permanent** faults
  - in case of fault → **negligible** additional **delay**
  - **permanent overhead**



Fault Tolerance

- **Automatic Repeat Request (ACK N)**
  - Stop and Wait (explicit acknowledgement)
  - Go back N (pipeline N transmissions)
  - **reactive** mechanism
  - **transient** faults **only**
  - fault → latency increase
  - multicast?

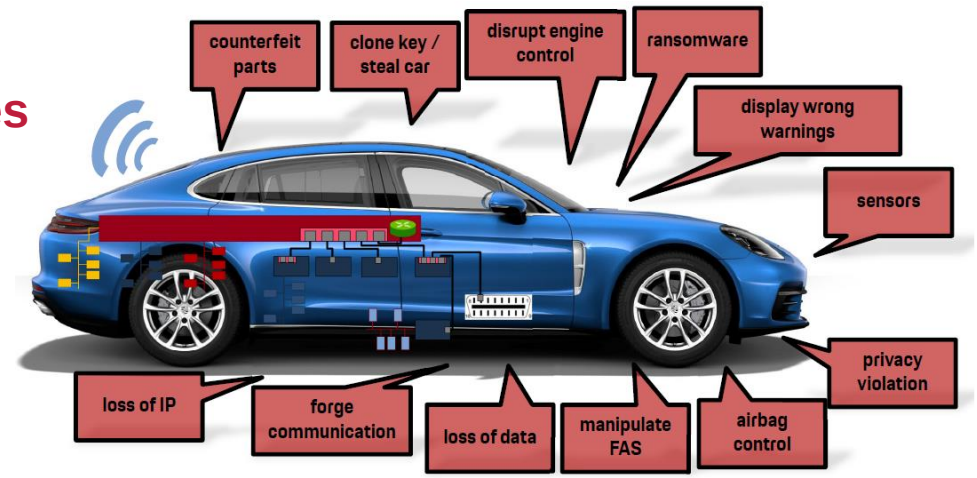


Ethernet – The safety perspective

- **Isolation**
  - how well does Ethernet isolate critical from other traffic?
  - „freedom from interference“
- **Delivery under transmission errors**
  - what timing guarantees are possible under errors?
- **Security**
  - how to enable complex functions without risk ?

Security

- Automotive vehicles = highly communicating “software on wheels”
- External systems and networks:
  - **enable** sophisticated **functionalities**
  - but also **increase risk**!
- Internal threats:
  - misbehaving & malicious software
    - not all features thoroughly tested



Source: Dr. Christian Meineck @ AN’17

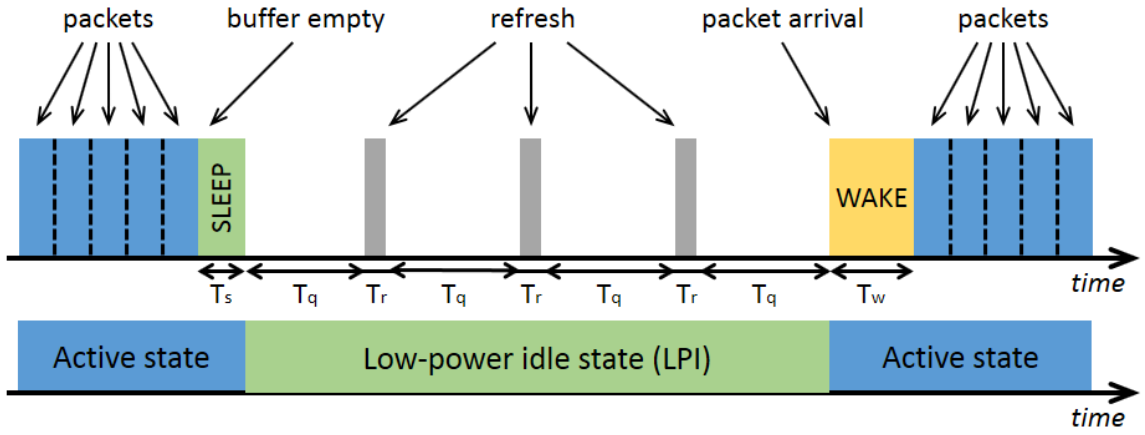
- External threats:
  - attacks and intrusions via communication:
    - WIFI, V2V, V2I, Charging stations, mobile device, application centers
- Intrusion detection mechanisms necessary, **verification?**
  - **adaptive** variant of per-**stream filtering** and **policing** (IEEE 802.1Qci)

Ethernet – The safety perspective

- **Isolation**
  - how well does Ethernet isolate critical from other traffic?
  - „freedom from interference“
- **Delivery under transmission errors**
  - what timing guarantees are possible under errors?
- **Security**
  - how to enable complex functions without risk?
- **Energy Efficiency**
  - how to decrease power consumption?

Energy Efficiency

- Energy efficiency considerations:
  - increasing numbers of **hybrid** and **electric vehicles**
  - functionality requirement: **substantial processing and networking power**
  - functionality requirement: **availability in all modes**
  - when **turned-off** all vehicles “live” on **limited battery capacity** (accumulator)
- Energy-Efficient Ethernet (EEE) – IEEE802.3az
  - so far considered for data centers and home networks, not automotive



Ethernet – The safety perspective

- **Isolation**
  - how well does Ethernet isolate critical from other traffic?
  - „freedom from interference“
- **Delivery under transmission errors**
  - what timing guarantees are possible under errors?
- **Security**
  - how to enable complex functions without risk?
- **Energy Efficiency**
  - how to decrease power consumption?

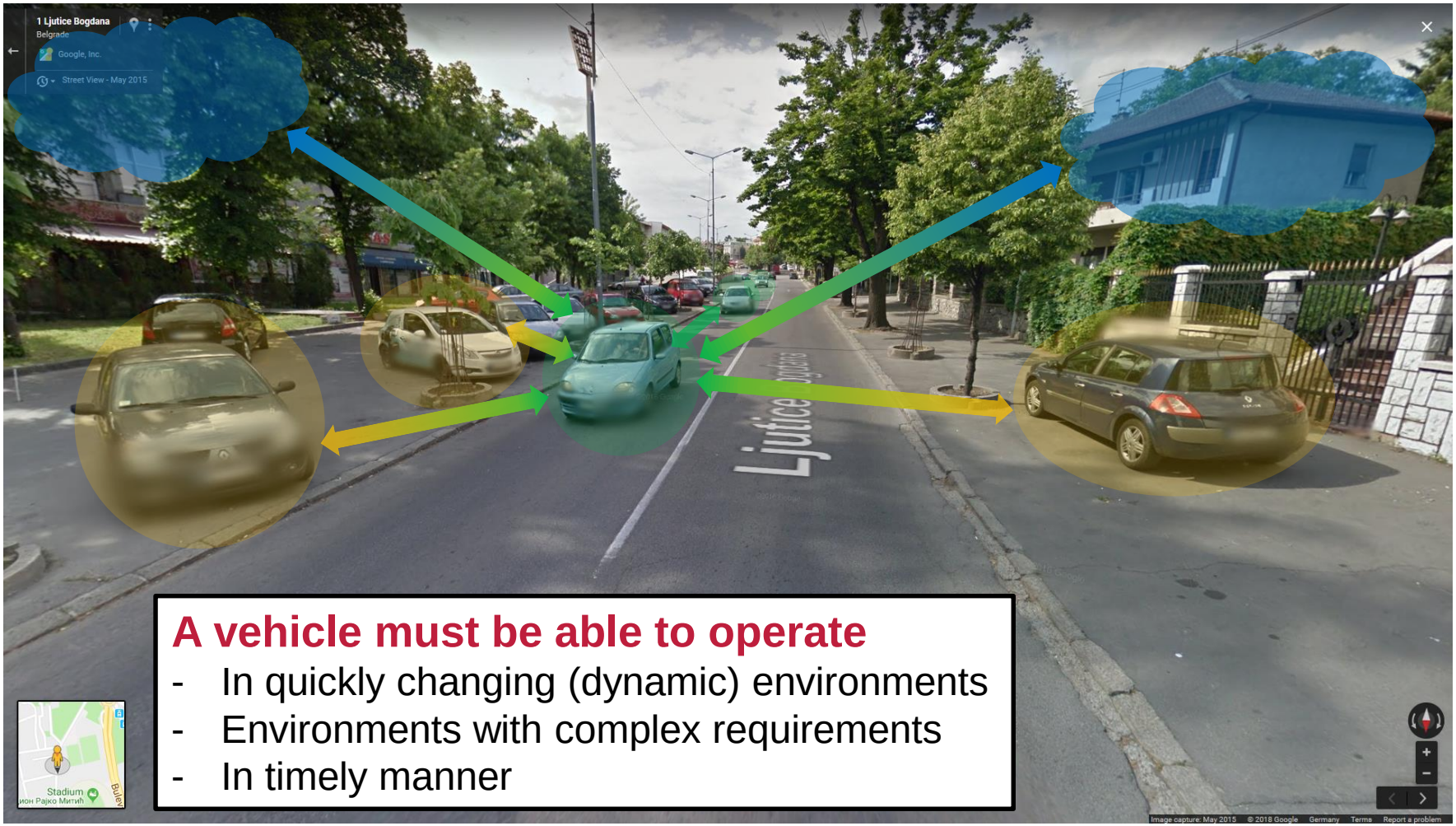
Now we have solved the problem?

Now we have solved the problem?

***Conditional automation* seems achievable**

- Requires certain conditions
- Driver must be ready to take control

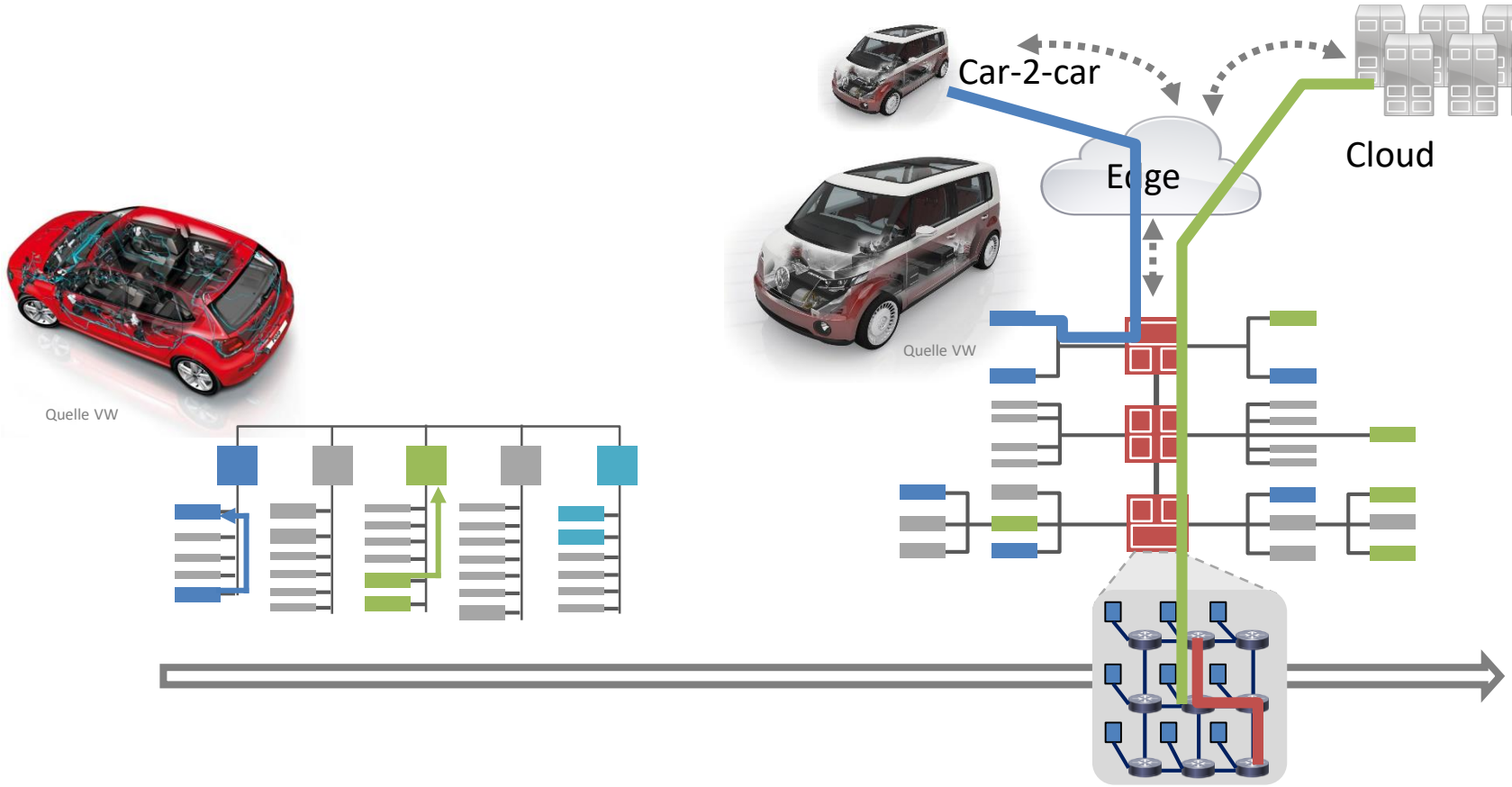
… or not???



A vehicle must be able to operate

- In quickly changing (dynamic) environments
- Environments with complex requirements
- In timely manner

But all that is still not enough ……



Adaptive Network Bahaviour

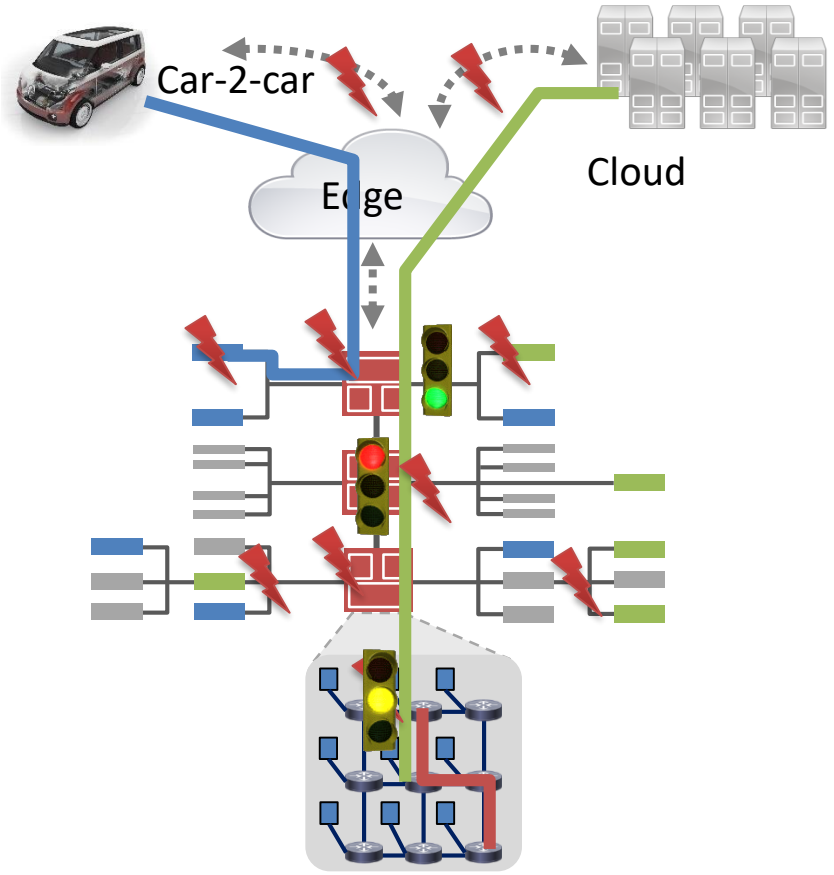
- **Dynamic workloads**
  - quickly changing (dynamic) environments e.g. weather, situation on the road …
  - new security threats and countermeasures!
  - … in a timely and safe fashion!
- **How to enable run-time adoption?**
  - adjust admission control, sys. reconfiguration & runtime diagnostics

- Hardware architectures and software platforms to accommodate:
  - AI applications
  - deep learning mechanisms

- **The goal : Eventually make human assistance for driving obsolete**

The New Challenges

- **End-to-end communication**
  - vast amounts of data
  - dynamic transfers
  - involved a wide range of parties
- **“On-the-fly” synchronization**
  - service discovery
- **Integration Challenges**
  - high costs
  - endangered safety



Service-Based Protocols

- To facilitate more convenient high-level communication
- AUTOSAR → **AUTOSAR AP** (since March 2017)
  - automotive software standard (has Ethernet socket adapter)
  - AUTOSAR AP Enables Adaptive Applications
  - allows **dynamic linking** of **services** and **clients** (runtime)

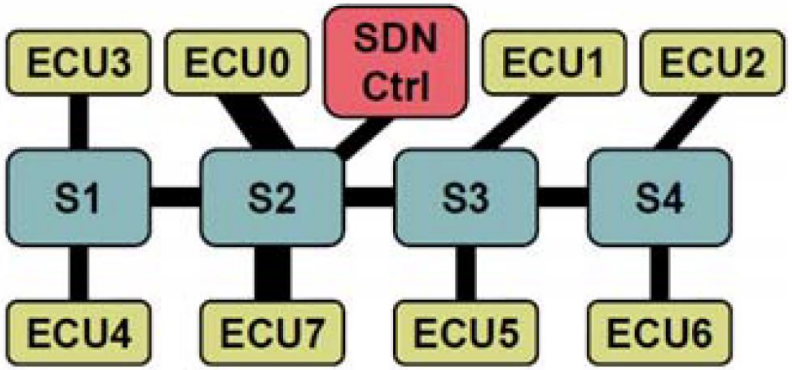
- SOME/IP
  - service-oriented middleware over IP
  - utilises both TCP and UDP
  - compatible with AUTOSAR
  - contains **service discovery** routine
- Other protocols: DDS, MQTT, 1722.1

Outline

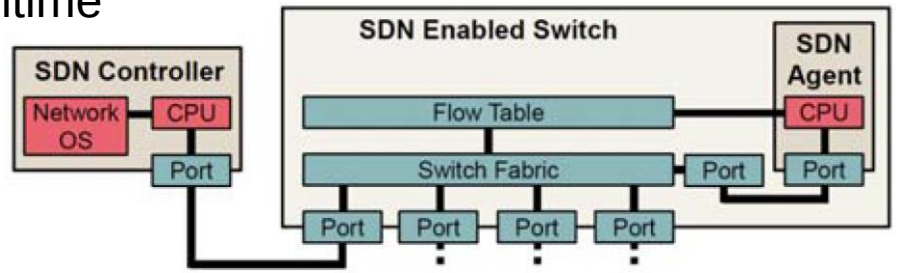
- Automotive trends – Present and Future
- Automotive Ethernet – the safety perspective
- Automotive Networks – other challenges
- **SDN – Promising Preliminary Solution**
- **Conclusions**

Software-Defined Networking (SDN)

- Initial approach centralised solution



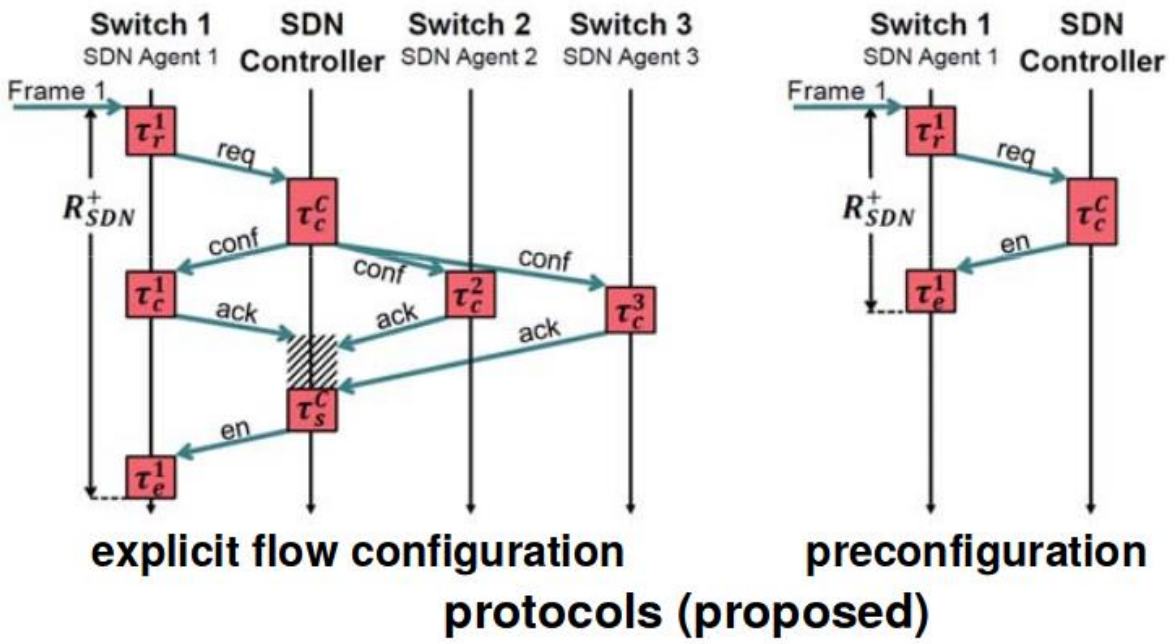
- Introduce a dedicated control plane
  - switch configs & reconfigs thereupon
  - Step 1: **Preconfigured**
    - configs for different modes @ design time
    - provision for safe transitions (mode changes)
  - Step 2: **Explicit**
    - plan & implement new configs @ runtime
    - fully adaptive behaviour
  - In future: **control redundancy**



SDN architecture

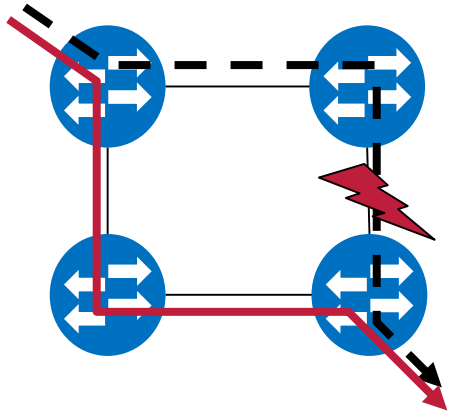
Software Defined Networking - Principle

- Uses network to communicate switch configuration
  - access control, reconfiguration, ...
  - explicit control or preconfigured
  - control redundancy must be added



Example - Handling permanent component failures

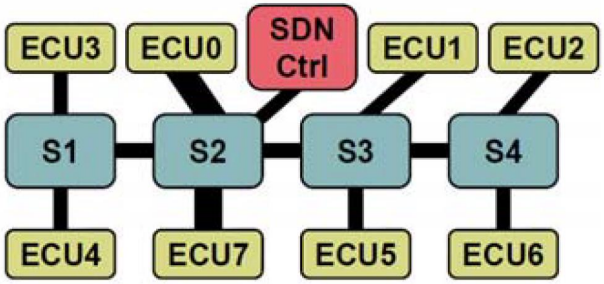
- **Introduction and control of component redundancy**
  - multipath routing – TSN
  - zero extra delay
  - permanent overhead

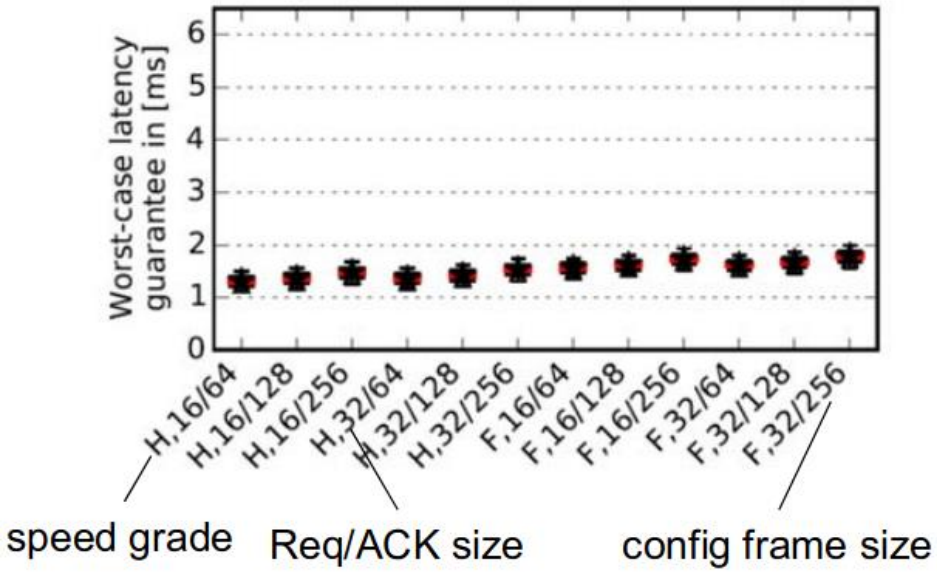


- **Automated path detection and routing**
  - standard approach
  - large and unpredictable delay
- **Alternative: centralized configuration**
  - possible solution: Software Defined Networking (SDN)
  - introduces control plane
  - fast enough?

Feasibility study for SDN [Thiele 2016]

- Protocol timing for access control
  - depends on load, number conf. requests
  - explicit configuration: 1ms ...6ms
  - preconf: < 1.3ms
  - feasible approach for automotive





Outline

- Automotive trends – Present and Future
- Automotive Ethernet – the safety perspective
- Automotive Networks – other challenges
- SDN – Promising Preliminary Solution
- **Conclusions**

Conclusions

- **Ethernet** = **promising** future automotive networking technology
- Many **opportunities & pitfalls**, **careful application** necessary
- **TSN** beneficial but **not panacea** (static)
- **Autonomous** vehicles: Lot of **work remaining**
  - especially for automation levels 4 (High) & 5 (Complete automation)
- Enabling **adaptive behaviour key** requirement for:
  - service-based communication
  - fault tolerance (e.g. fail-operational behaviour)
  - security
  - energy efficiency
- **SDN** = **favourable platform** for further investigations