Technische Universität Braunschweig

Advanced Resource Management in Automotive Networks

Adam Kostrzewa, TU Braunschweig, Germany
Email : kostrzewa@ida.ing.tu-bs.de

DIVERSE: 2nd Workshop on Advanced Technologies in Vehicular Systems @ IEEE ETFA 2020

Automotive Networks - New Trends

Trend 1: New applications

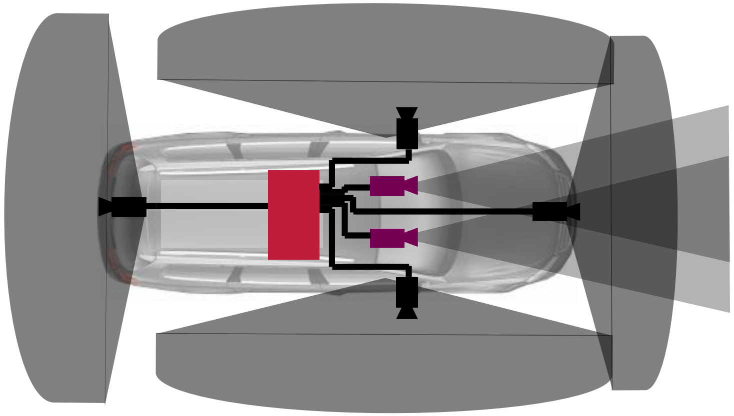
- networks with IP traffic via car-to-X communication
- communication with a cloud
- *primarily best effort*

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

Trend 3: Complex low latency traffic

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



Requirements for In-Vehicle Network

- vehicle is a mixed criticality system
  - design and operation governed by functional safety standard ISO26262
    - classifies functions in criticalities ASIL D to ASIL A and non classified QM
    - all computing and communication involved in an ASIL A to D function must adhere to a highly structured and constrained design process

  - network focus shifts towards critical network traffic
    - traditional vehicles: little critical communication, most communication volume QM
      - including advanced driver assistance: control is driver responsibility
    - future vehicles: higher automation levels lead to critical high-bandwidth traffic

→ most future vehicle network traffic regulated by safety standard requirements

- currently only manageable with static network configuration
  - safety concern!

Outline

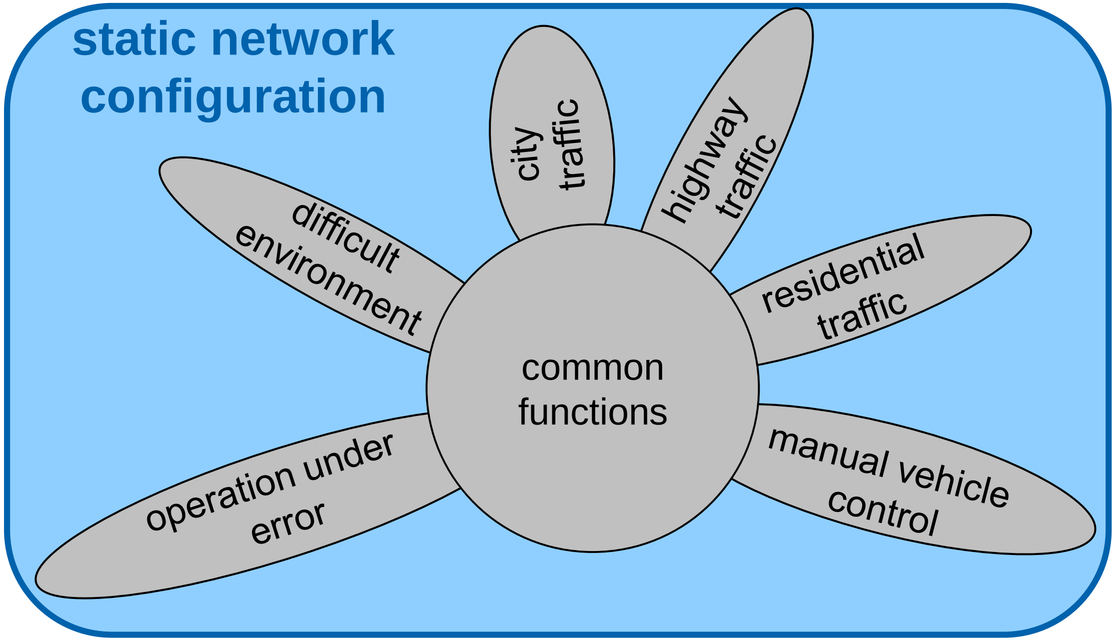
- Motivation
- Static Network Configuration
- Towards Network Dynamics
  - Fast and Safe Failover in the Network
- Exploiting Re-configuration
  - Car-2-X Communication
- Conclusions

Work partially sponsored by Huawei

Static Configuration - Dilemma

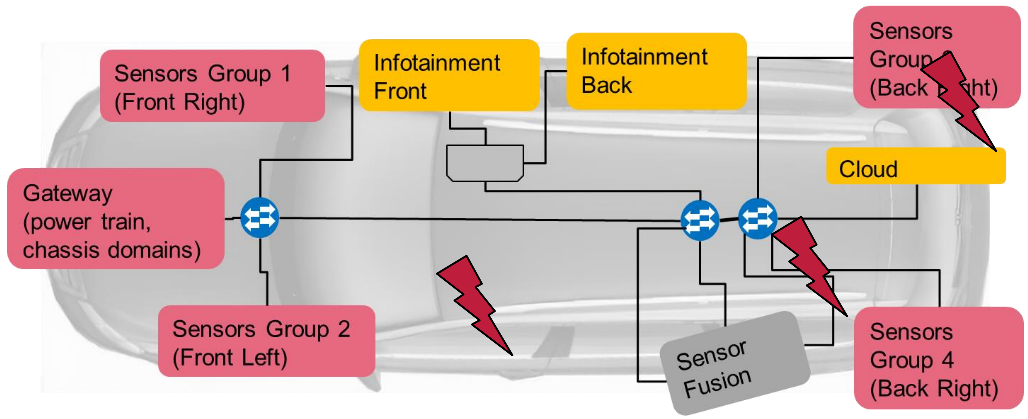
- static configurations must be designed for the worst case
  - of all driving and operating modes
  - of all traffic combinations under real-time constraints
  - of all transient and some static network errors
- leads to redundancy under almost all conditions
  - hardly exploitable under static TSN configuration

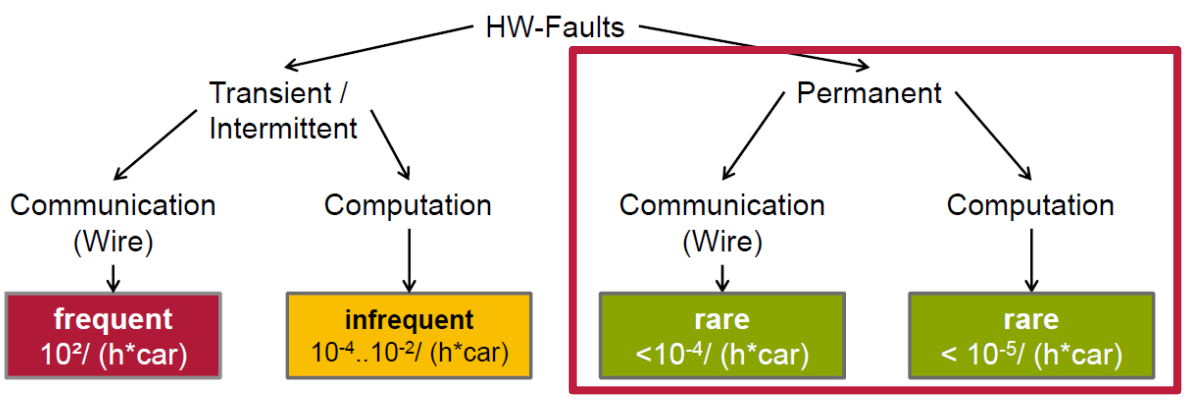
→ expensive overprovisioning



Example – Permanent faults!

- an automotive system must be able to handle permanent faults
  - fail-safe behaviour may not be enough for higher ASILs
  - **fail-operational behaviour**
    - it may not be possible to bring the driver back into the control loop!
- fortunately one failure at a time e.g. BroadR-Reach standard

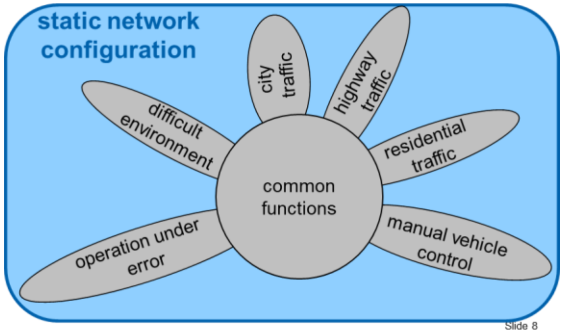




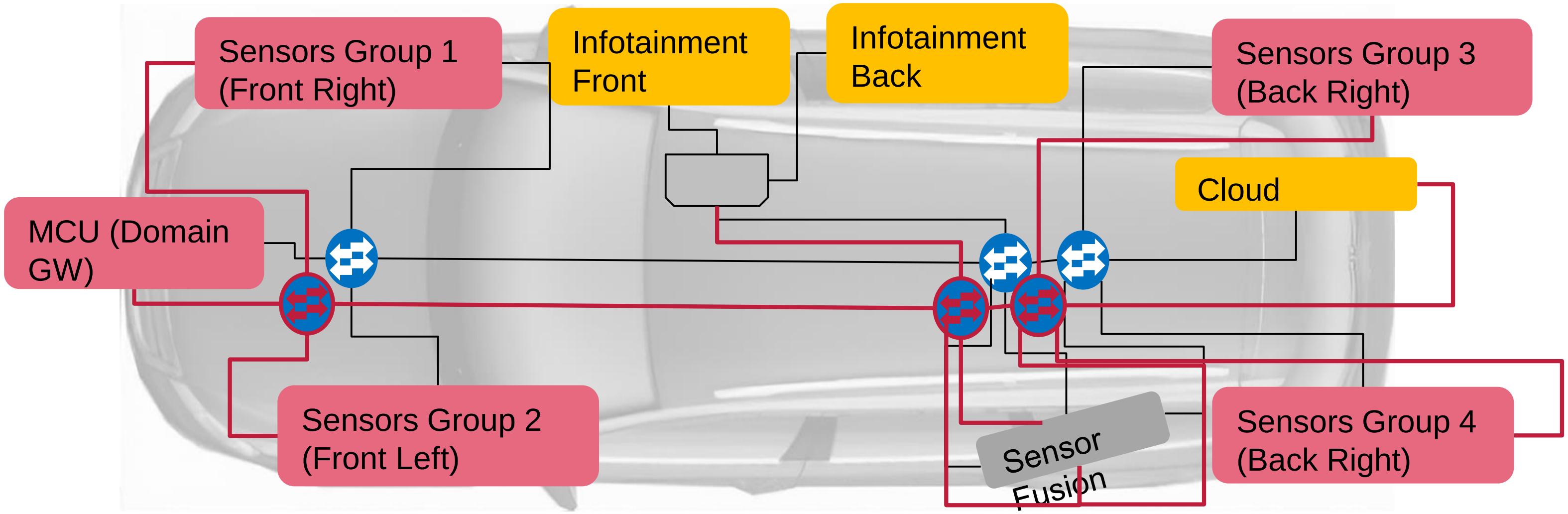
note: resulting computation errors strongly depend on state protection (memory)

Naïve approach – let's duplicate!

- introduce full hardware redundancy – duplicate whole network
  - example: 3 new switches, 12 new cables, 10 new ports
- immediate recovery at a high cost
  - overprovisioning in error-free case
  - including cost of maintenance, weight and power consumption



Overprovisioning

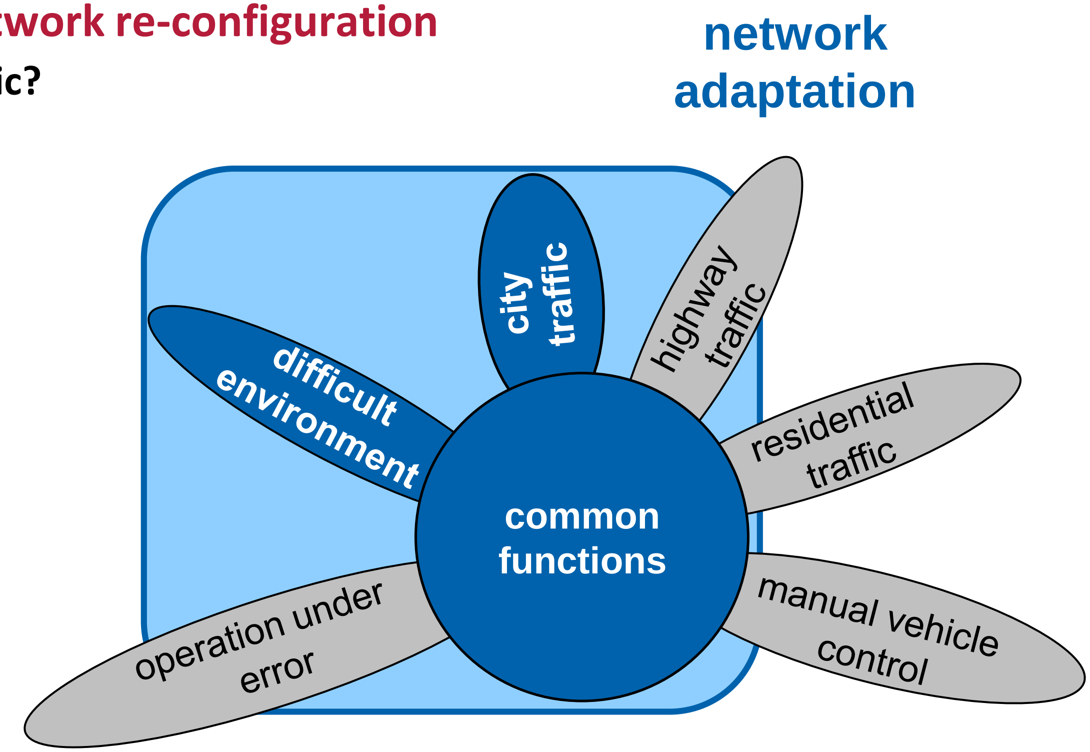


Towards Network Dynamics

- reduce redundancy by adaption to current communication requirements
  - great opportunity for vehicle cost and performance optimization
  - but must guarantee real-time, safety, and network standard compatibility

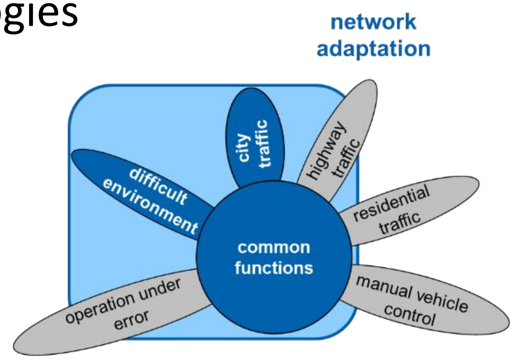
- adaptation requires dynamic network re-configuration
  - is dynamic re-configuration realistic?

- And most of all is it safe?

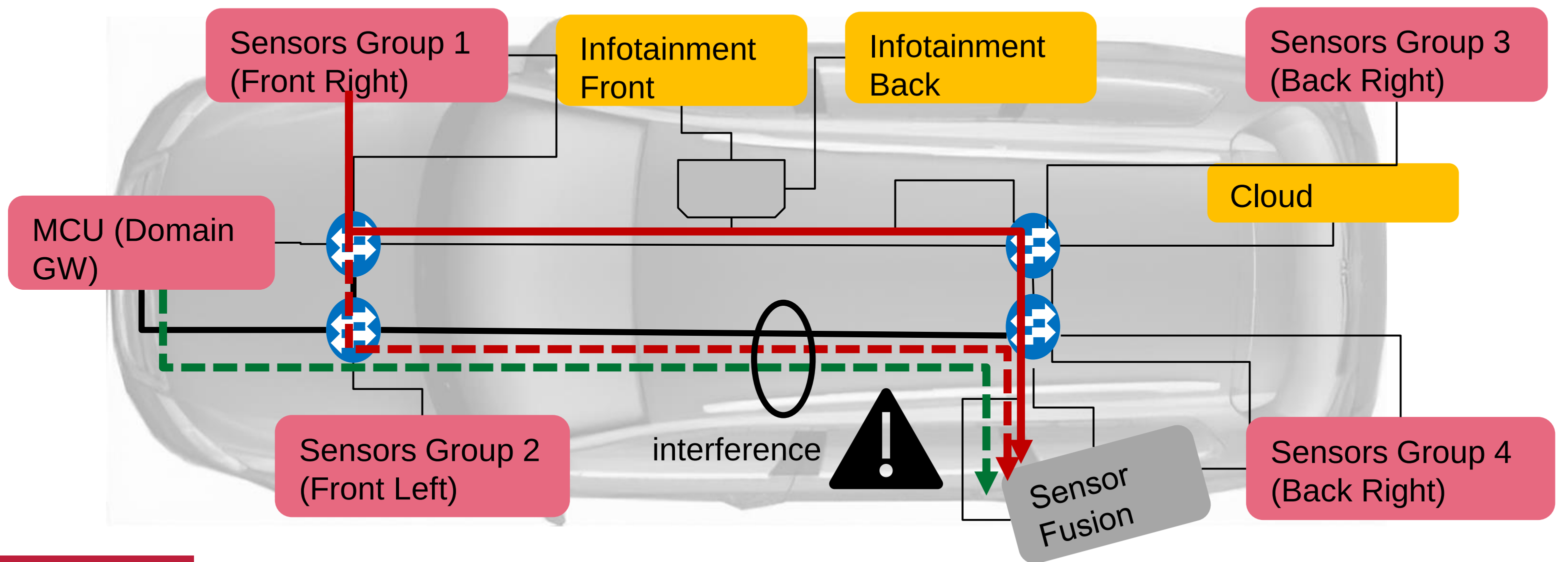


Alternative – Limited Redundancy

- redundant paths through the network such as ring- based topologies
  - example : 1 new switch, 3 links, 1 port
- redundant transmissions e.g. TSN FRER (IEEE 802.1CB)
  - zero extra delay but permanent overhead
- automated path detection and routing
  - may endanger safety or high permanent overhead



Uncoordinated reallocation



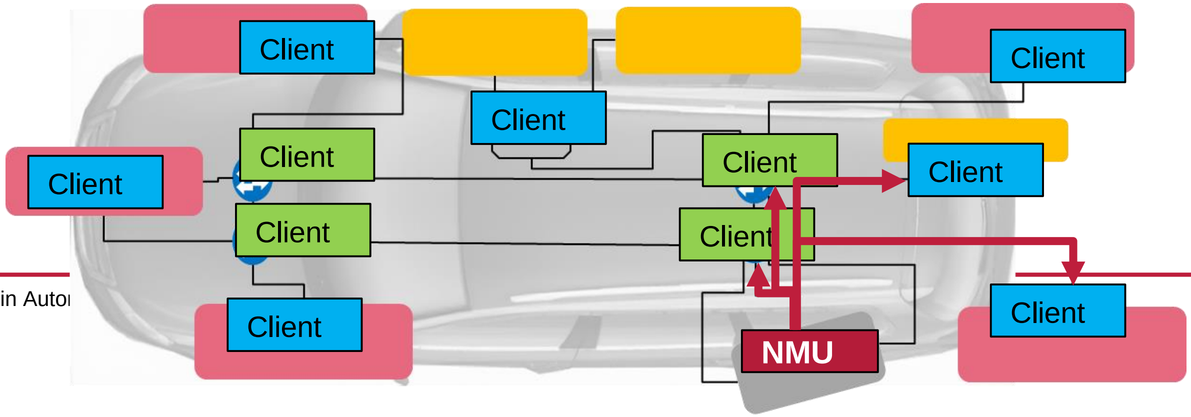
Managing Dynamic Re-configuration

- our alternative solution uses overlay network for controlled loss-free re-configuration in real-time
  - key challenge : preserving safety during mode-changes

- automotive TSN networks use many parameters for adaptation and optimization
  - TSN standard offers interfaces to configure switches and network interfaces
  - may use IEEE 802.1Qcc protocols for network parameter distribution
  - but currently no run-time configuration due to missing transition guarantees

Overlay Network for Real-time Loss-free Re-configuration

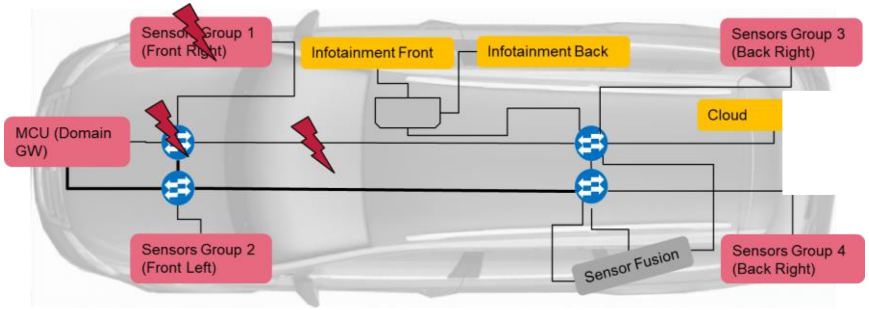
- Decouple flow and network management
  - data layer – low-level flow-control method in automotive network responsible for switching packets/frames
  - control layer – global and dynamic arbitration
    - clients in switches – like SDN
    - clients in end nodes – unlike SDN
- Network Management Unit (NMU)
    - central scheduling function with guaranteed timing – unlike SDN
- Protocol based synchronization
    - protocol for safe mode changes at runtime!
    - key enabling feature of the technology!

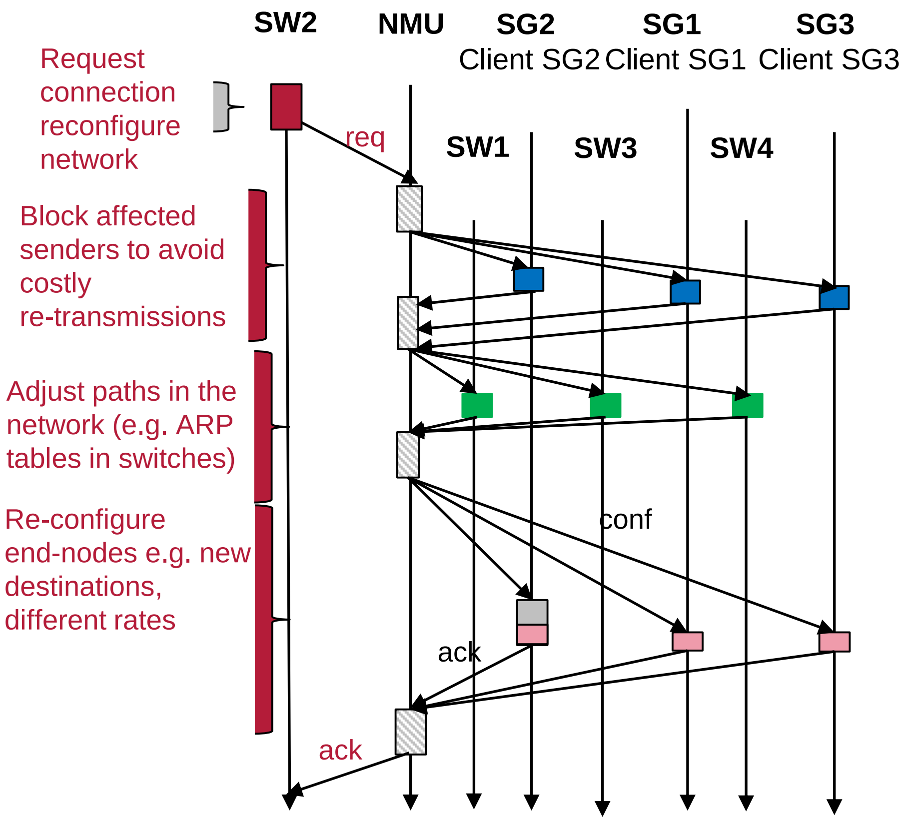


Overlay Protocol Requirements

- not that easy to make the re-configuration safe
  - protocol itself must be resilient to transient errors
  - order of re-configuration must avoid QoS violation
  - re-configuration timing must be bounded

Fast and Safe Mode-Change in the Network





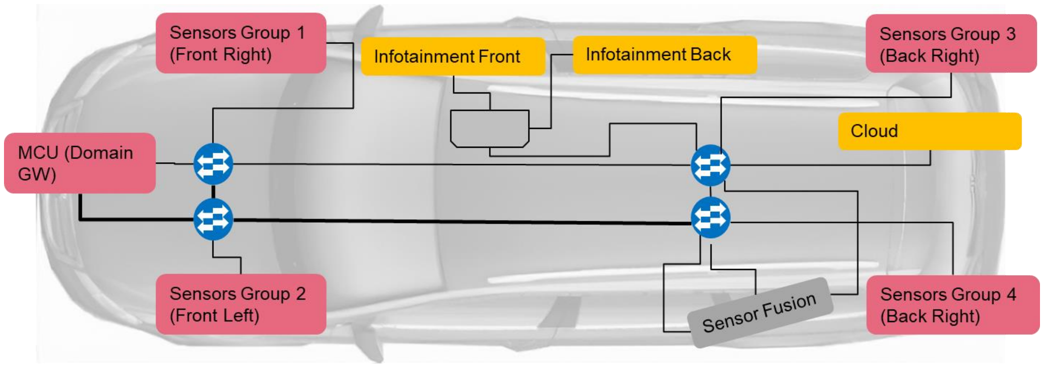
- block senders to avoid dropped packets
- load pre-configured router settings
- changed destination (IP)
- re-configure senors (switch off radars, adjust cameras)

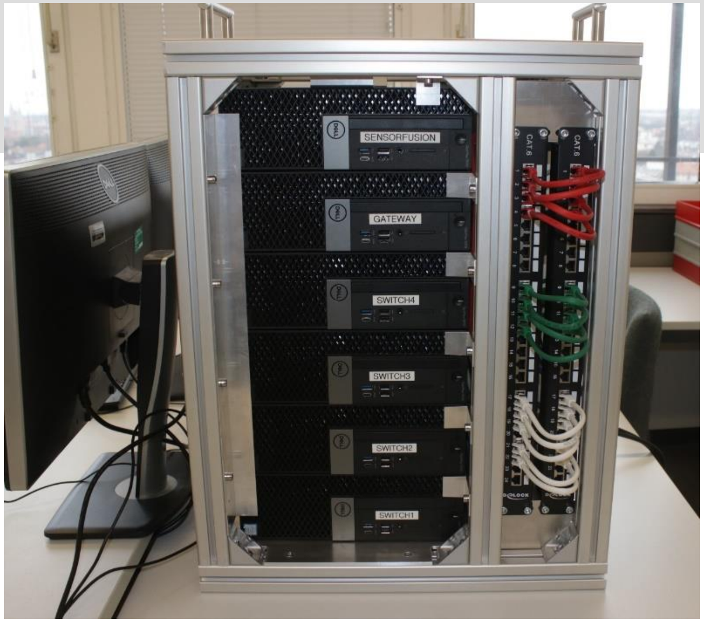
And restart transmissions

Timing must allow rollback at any moment to the safe state!

latency <= 10 to 50 ms

Demo Setup





MCU (Domain GW)

Sensor Fusion

Intel Core i5-8400 CPU @ 2.8 GHz
x 6cores, 8192MB DDR4-2666 SDRAM
Intel I340-T4 Ethernet adapters 1Gbit

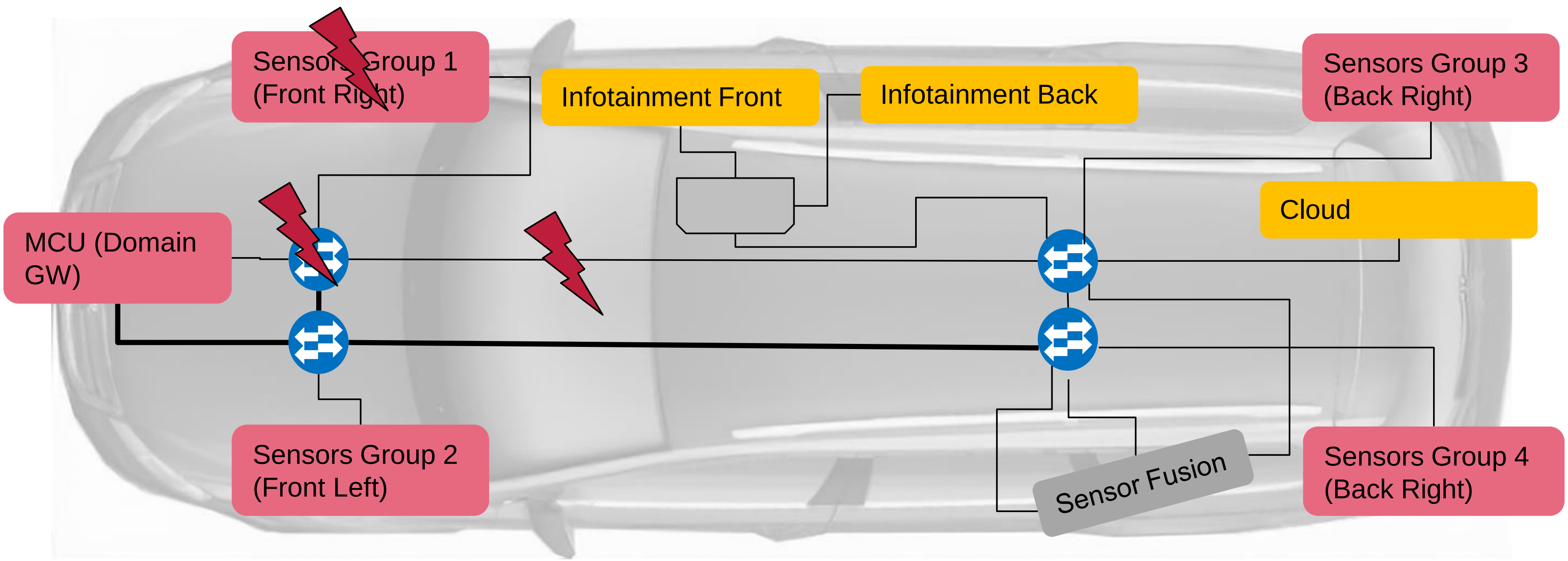
Sensors Groups

Alliwnner H3 SoCs
(1GHz Quad-Core ARM Cortex-A7 @ 1.296GHz,
1GB DDR3-1333 SDRAM)
Allwinner Ethernet Adapter 1Gbit

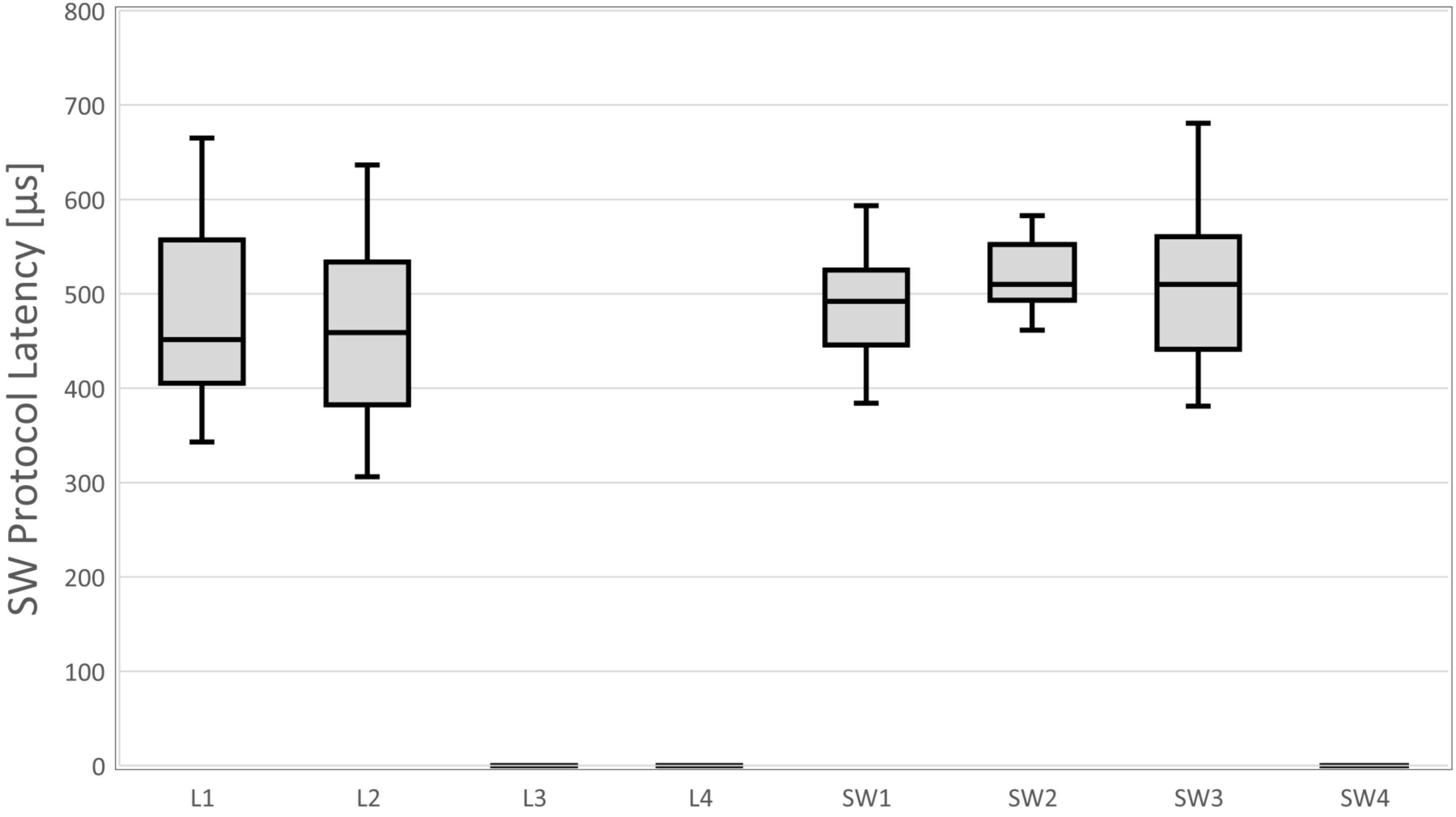
Linux network stack (5.0.0-38-generic x86-64)
Clients + NMU C-libraries running in user-space
AVB Ethernet schedulers according to the IEEE 802.1Qav, IEEE 802.1QAS standards.

Considered Scenarios

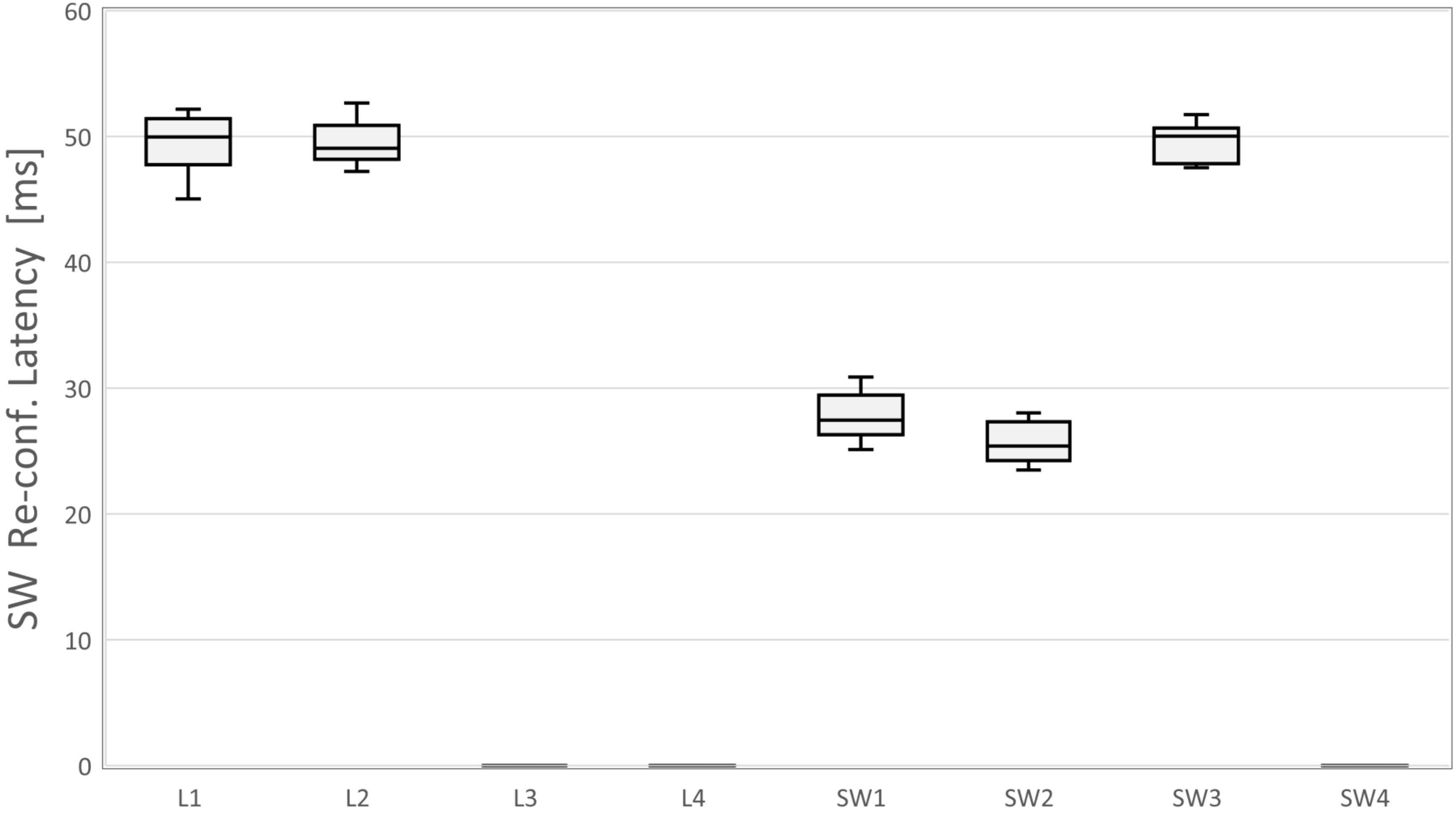
- Scenario 1 – SG unit is down
- Scenario 2 – Backbone link is down
- Scenario 3 – Switch is down



Demo Results – Protocol Overhead



Demo Results with NIC Re-conf. Latency



Comparison with Other Solutions

Protocol	Vendor	Topology	Failover time (max. 10 switches)
STP	IEEE Standard	Any	>30 s
RSTP (802.1w)	IEEE Standard	Any	Several Seconds
HiPER Ring	Hirshmann	Ring	200-500 ms
Turbo Ring	Hirshmann	Ring	<200ms
S-Ring	GarrettCom	Ring	<250 ms
RS-Ring	GarrettCom	Ring	<100 ms
RapidRing	Contemporary Controls	Ring	<300 ms
eRSTP	Siemens	Any	<50 ms (ring only
RSTP (802.1D-2004)	IEEE Standard	Any	<50 ms (ring only)
Fast Protocol-based Reconfiguration		**Any**	**<1 ms protocol overhead ~ 50ms linux-based**

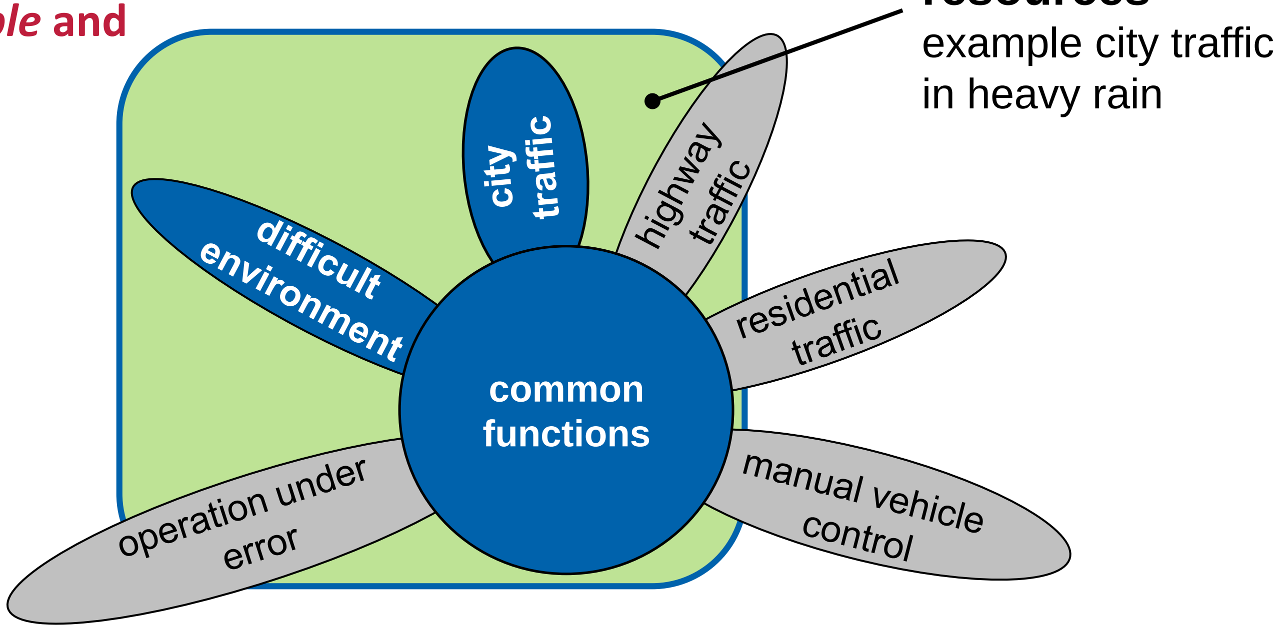
automotive network requirements: below 100 ms AVNu Alliance or even 50ms [2]

Comparison of ethernet-based network reconfiguration protocols based on [4] and [5].

Exploiting Re-configuration

- Dynamic re-configuration leaves **redundant resources** under almost all conditions
- Overlay network can make **redundancy available for predictable QM traffic**

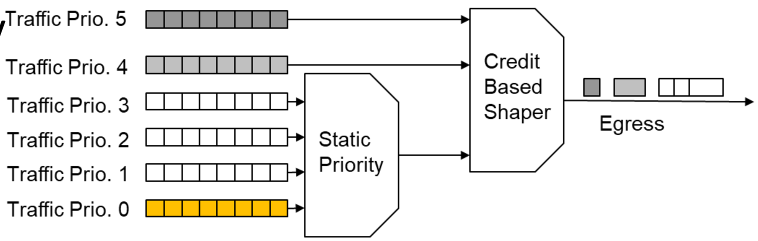
What if we could exploit network redundancy for *predictable* and *performant* dynamic communication?

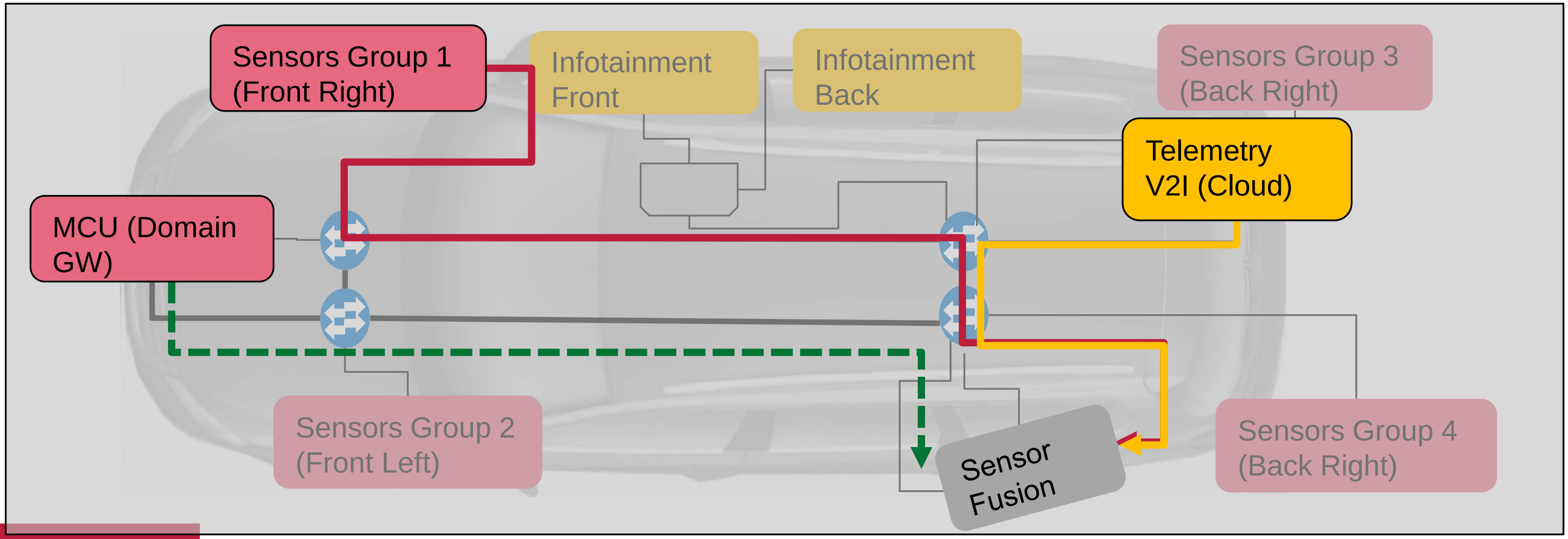


Example Cloud Integration

- **Redundant resources only partially utilized**
  - example: permanent faults are rare, e.g. once per component lifetime
- How to provide access to the Sensor Fusion?
- Right now cloud traffic is best effort with low priority
  - long latencies / low bandwidth
  - and/or dropped packets

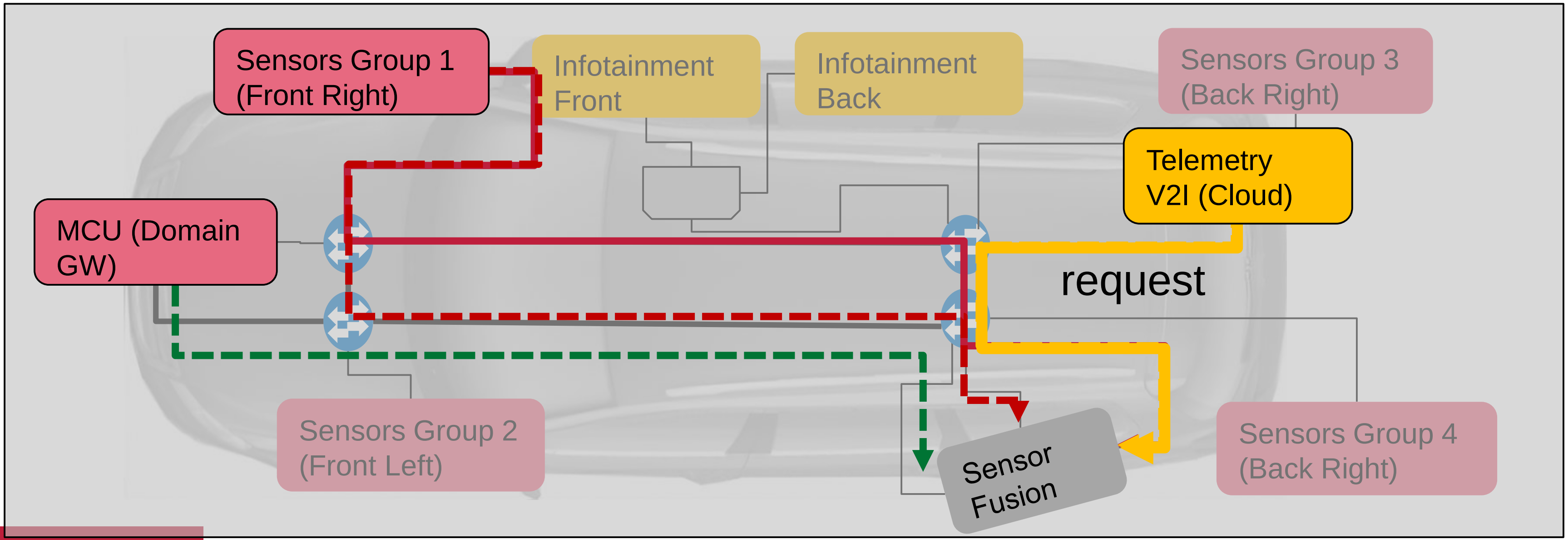
TSN Scheduler





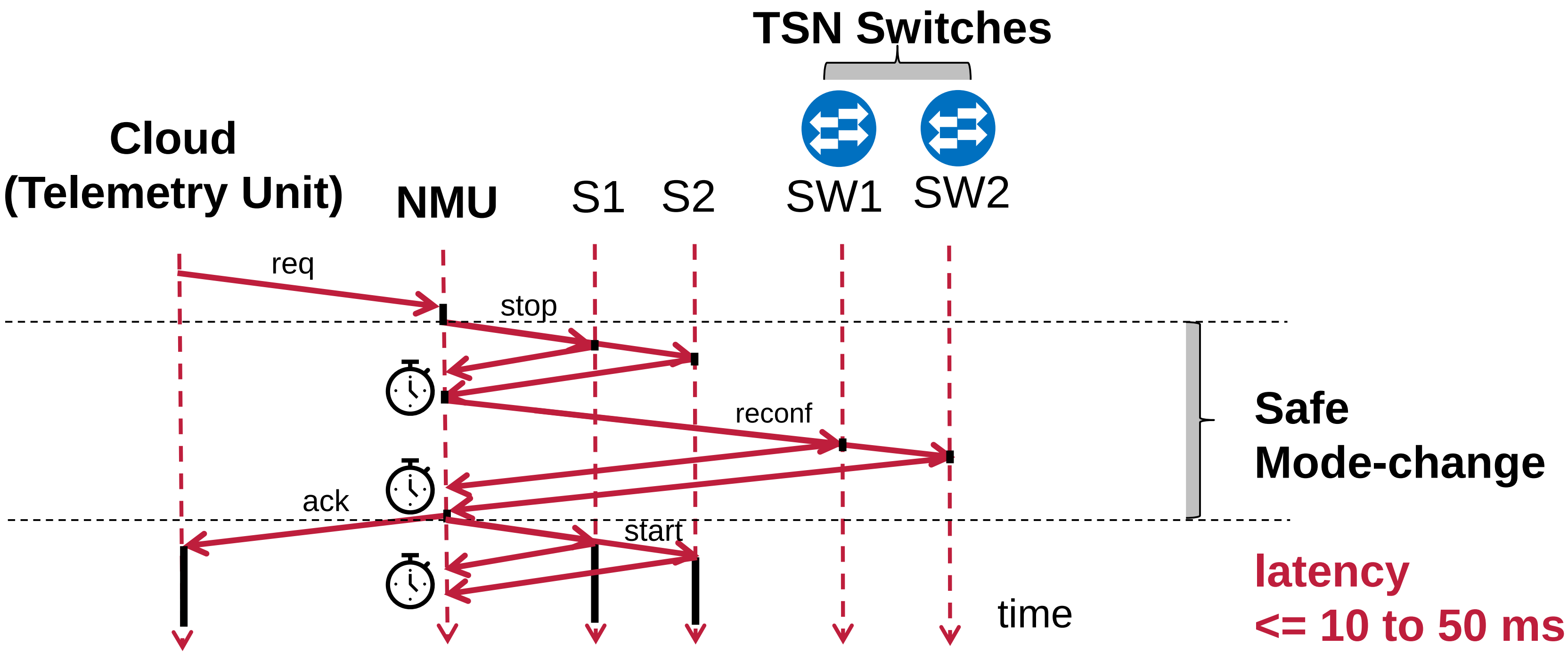
Cloud Integration - Example

- Cloud transmission wants **high-bandwidth real-time access** to “**Sensor Fusion**” unit
  - app1: **collaborative perception** with other vehicles and infrastructure;
  - app2: **data collection** for ML
- Safely re-configure the network without loss to assign redundant resources to cloud transmissions
- Cloud has **full access** as long as nothing “bad“ happens



Compatible, Safe, and Predictable Cloud Access

- partial dynamic re-configuration instead of complete network mode switch
- correct order and timing of actions!
- resilient rollback procedure e.g. ack msg + timeout



Example cloud access management

Benefits for Network Designer

- every vehicle has redundancy
  - cost can be minimized with dynamic re-configuration

- demo: huge benefits in cloud communication
  - efficient OTA communication almost for free!
  - the key enabling technology for efficient cloud communication
    - app1: collaborative perception with other vehicles and infrastructure;
      - 10x faster than SoA in demonstrator
    - app2: data collection for ML

- dynamic network management solves multiple problems with the same mechanism !

Conclusion

- ***does dynamic re-configuration und safety constraints really work?***
  - **yes, as proved by demonstrator**

- ***can we exploit re-configuration?***
  - **component cost saving via reduced network resources**
    - **for wiring harness, switch, energy @ high real-time & safety guarantees**
    - **for switches, smaller buffers and/or more workload!**

  - **multi-mode network functionality at low overhead**
    - **multi-mode systems with lower integration cost and higher performance**
    - **example fail operational network re-configuration**

  - **new system functions and improved user experience by dynamic OTA network operation**
    - **via exploitation of unused redundant resources and improved QM traffic management**
    - **app1: collaborative perception with other vehicles and infrastructure;**
    - **app2: data collection for ML**