Real-Time Ethernet in the Automotive Systems

Robin Hofmann, *Borislav Nikolic, Rolf Ernst*
TUBS
SAFURE WORKSHOP
22nd January 2018
Manchester, UK

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

SAFURE

SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems

Standard Ethernet Summary

- State of the art
  - Standard Ethernet, IEEE802.1
    - Weighted Round Robin: alternating transmission
  - Ethernet Quality of Service (QoS), IEEE802.1Q
    - Static priority non-preemptive: priority based transmission
  - Audio/Video Bridgeing, IEEE802.1Qas
    - Credit based shaper: bandwidth guarantees for traffic classes
- Mixed critical traffic → provide isolation between streams
- Desired improvements
  - Isolation / freedom from interference
  - Low and bounded latencies
  - Simple verification
  - Handling of transmission errors

Real-time Ethernet – TSN

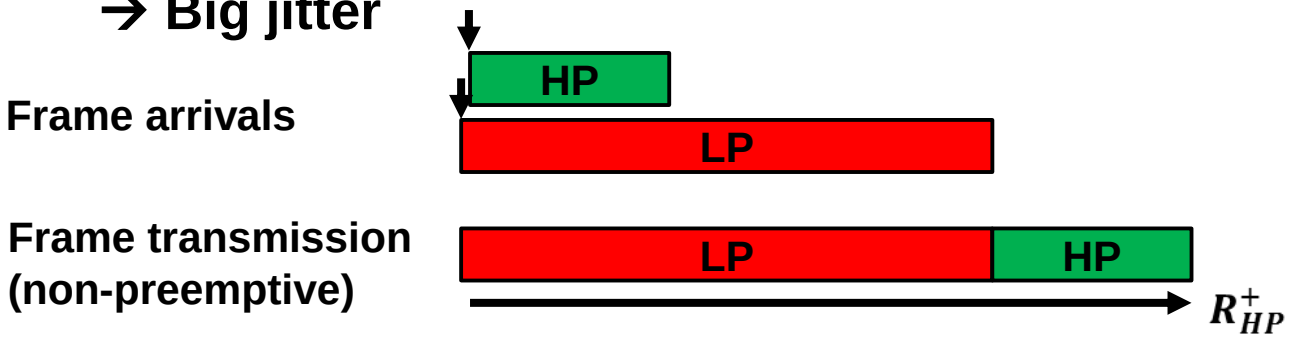
- Ethernet TSN (Time-Sensitive Networks)
  - Continuation of the AVB group
  - Set of standards (partially and fully completed)
  - Accurate time synchronisation
  - QoS (bounded latency, improved reliability)
  - Protection (against derouted and rogue traffic)
  - Scheduled traffic

- SAFURE relevant TSN efforts:
  - Traffic shapers, IEEE802.1Qbv
    - Burst limiting shaper
    - Time aware shaper
    - Peristaltic shaper
  - Frame preemption, IEEE802.1Qbu
  - Frame replication, IEEE802.1CB
  - Stream filtering, IEEE802.1Qci

Limitations of non-preemptive transmission schemes

- **Standard Ethernet:** Non-preemptive transmissions
  - Lower priority (LP) blocking
  - Longest Ethernet frame: 1500 Byte
  - Long blocking times: **120µs** @ 100Mbit/s per switch

    → **Big jitter**

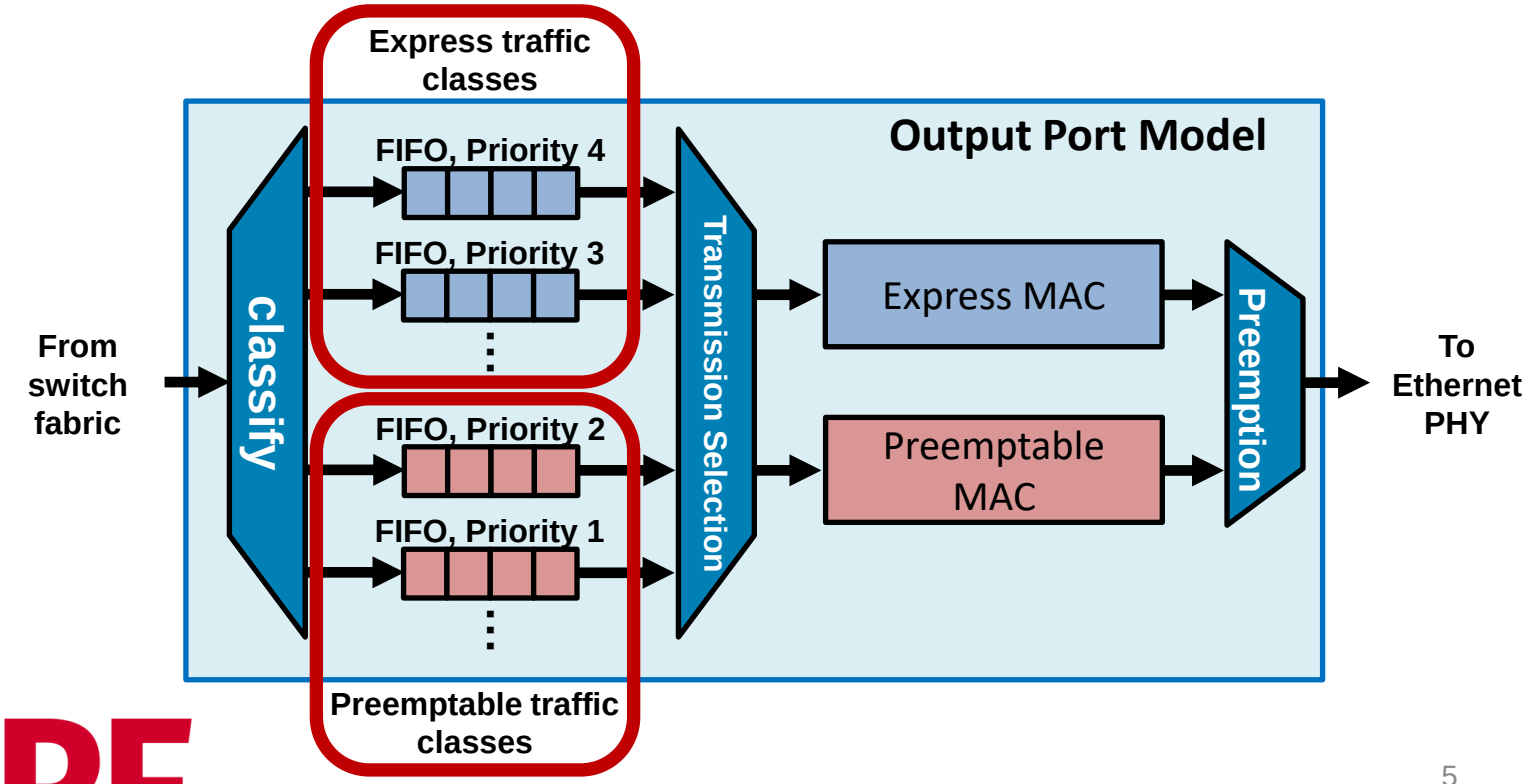


Solution:
Allow preemption of low priority frames

Frame preemption 1/2

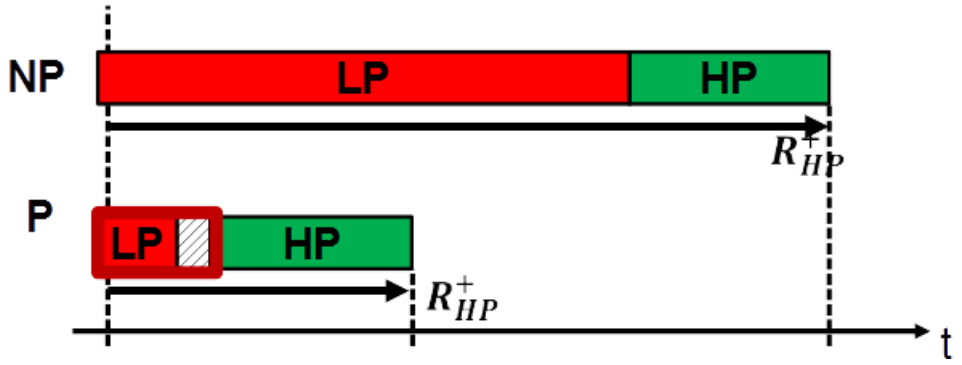
IEEE 802.3br and IEEE 802.1Qbu introduce frame preemption to Ethernet

- Two MAC interfaces Express and preemptable
- Only one level of preemption



Frame preemption 2/2

- Priority based transmission (IEEE802.1Q)



Performance gain due to frame preemption*

12µs vs 120µs @ 100Mbit/s per switch

→ Factor 10 improvement

* Thiele and Ernst. "Formal Worst-Case Performance Analysis of Time-Sensitive Ethernet with Frame Preemption". *ETFA 2016*

Ethernet TSN – Time-Aware Shaper (TSN/TAS)

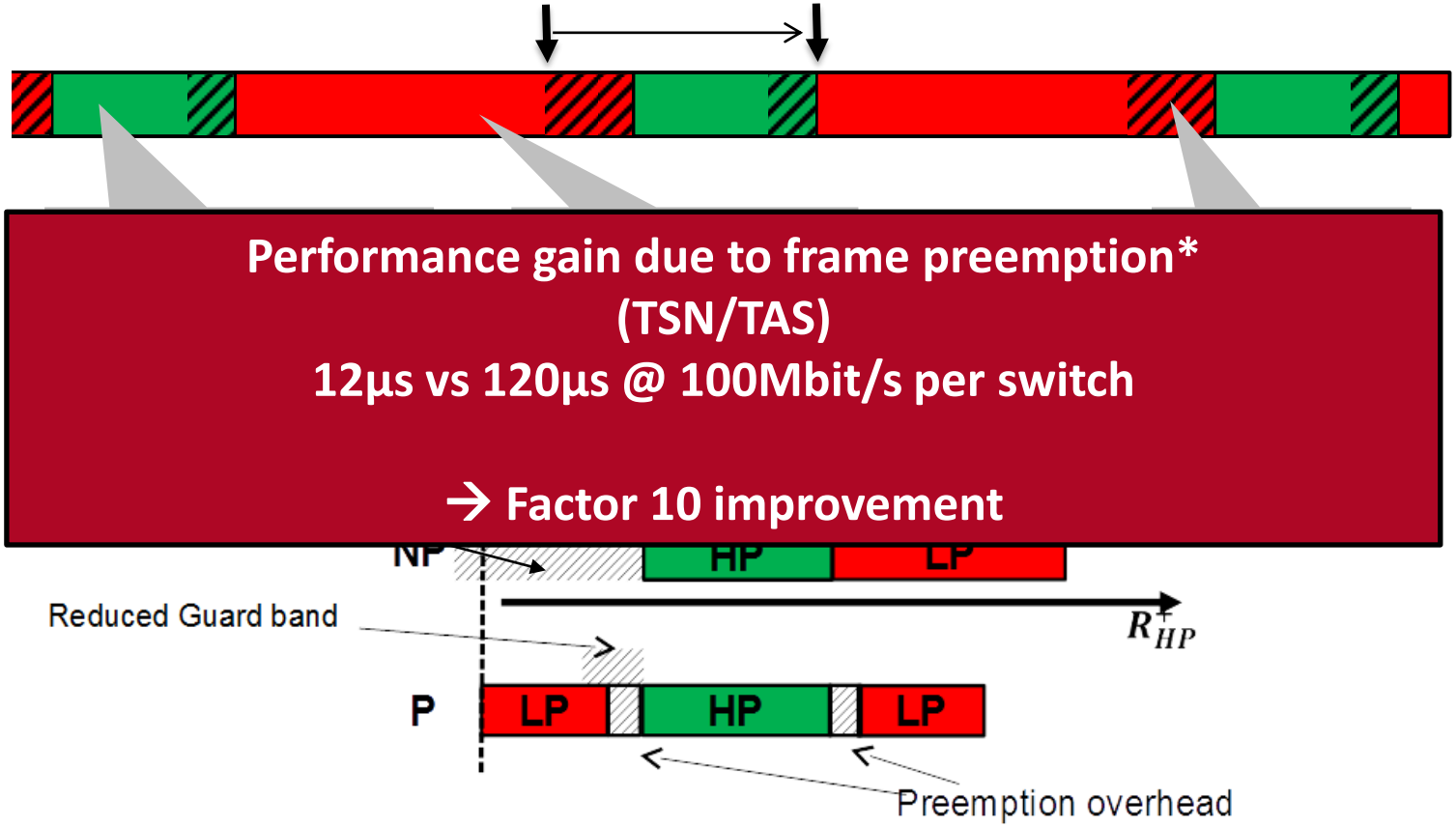
Temporal isolation of two traffic classes via time segments

- **Critical traffic** scheduled in time-triggered segments
  - FIFO order
  - Guard bands prevent segment violations
    - Guard band length equal to longest possible frame size
- **Non-critical traffic** scheduled during remaining time
  - Fixed-priority based and FIFO within same priority class
- Switch synchronization necessary for good performance
- Formal worst-case timing analysis performed*

* Thiele et al., "Formal Worst-Case Timing Analysis of Ethernet TSN's Time-Aware and Peristaltic Shapers". *VNC 2015*

TSN/TAS – Frame Preemption

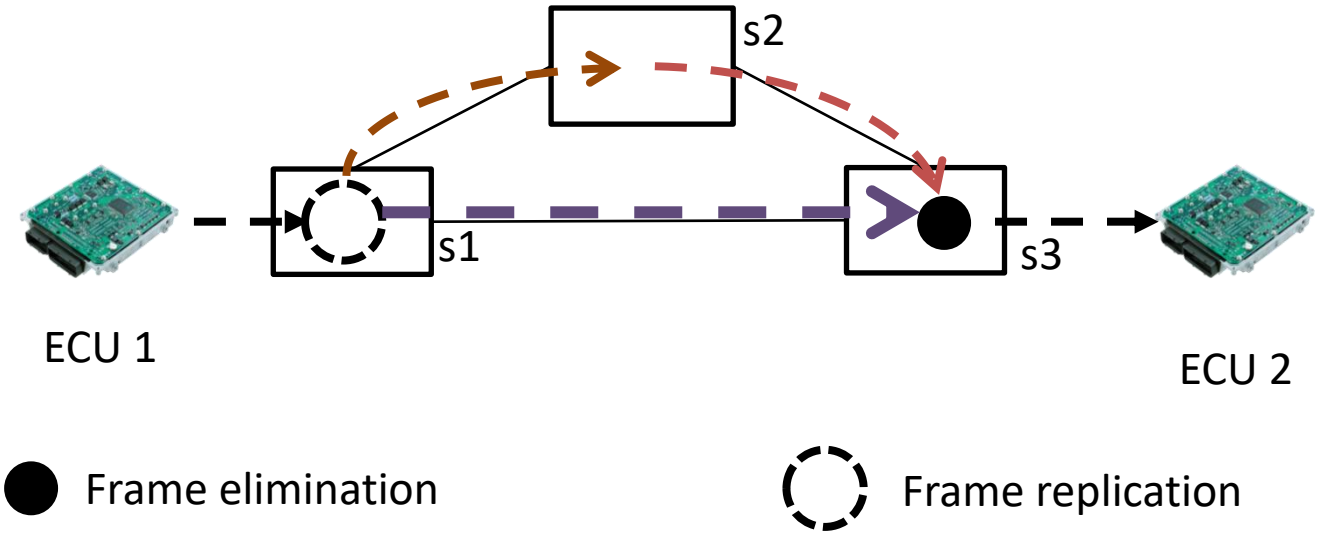
- TAS/TSN (IEEE802.1Qbv)



* Thiele and Ernst, "Formal Worst-Case Performance Analysis of Time-Sensitive Ethernet with Frame Preemption". *ETFA 2016*

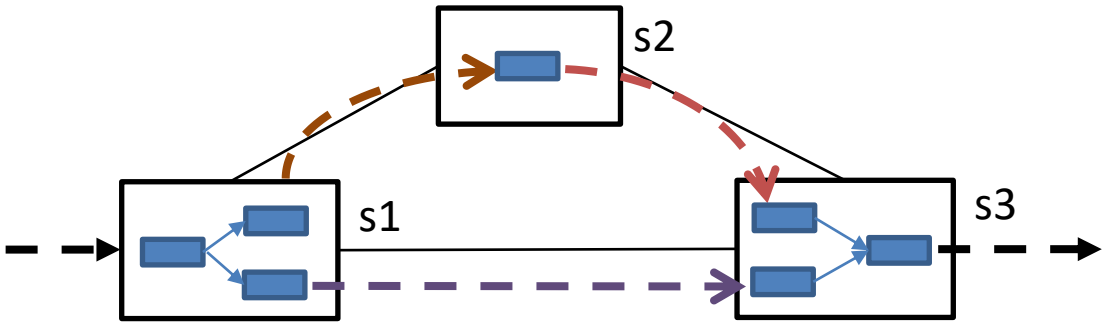
FRER

- Frame replication and elimination for increased reliablity (FRER)
- TSN standard under IEEE802.1CB
- Increased reliablity and reduced packet loss rate under transmission errors



FRER principle

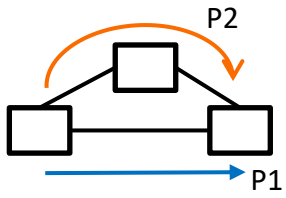
1. Network element receives FRER-proctected stream
2. Replication of stream in traversed element
3. Sending frame copies via redundant paths
4. Merge streams / Elimination of copies
5. Forwarding a single frame

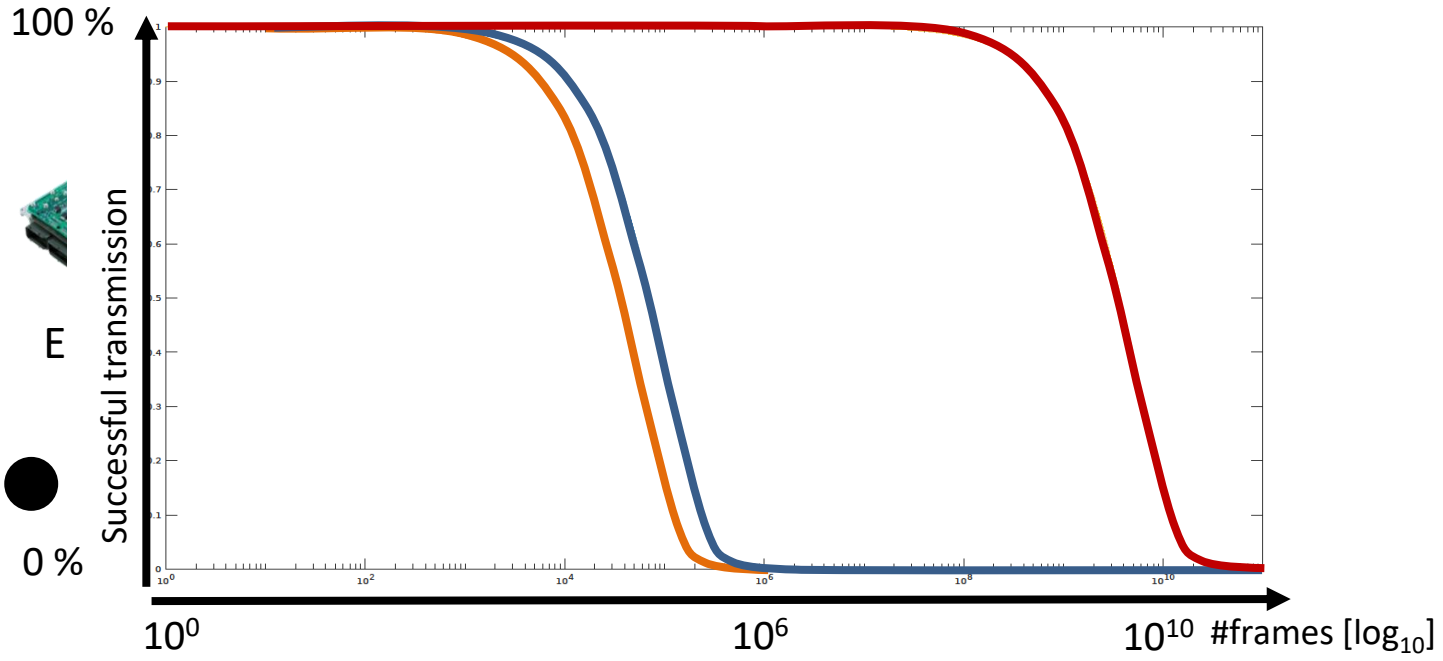


Hofmann et al. „Formal Worst-case Analysis of TSN Ethernet Frame Replication and Elimination for Reliabilty", *Under submission*

FRER – benefits

- Error rate: 10e-10 BER
- Transmission speed: 100Mb/s
- Frame size: 1200 Byte

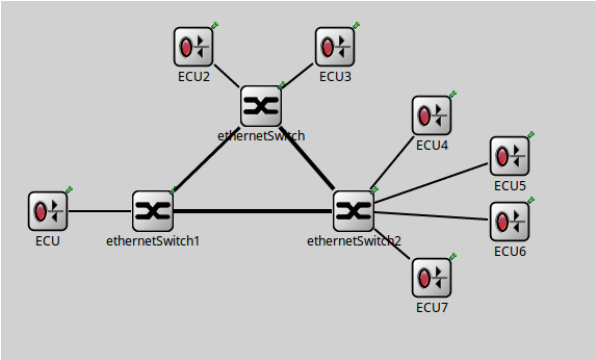


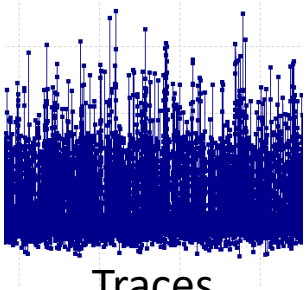


Analysis and simulation tools

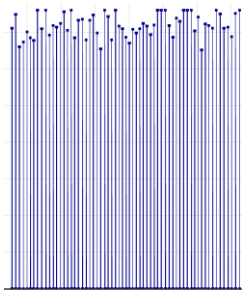
- Formal worst-case timing analysis: pyCPA
- Simulation environment: OMNeT++

- All features implemented in either pyCPA or OMNET.
  - Some in both

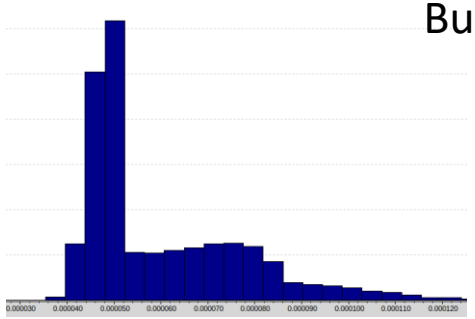




Traces



Buffer levels



End-to-end delay distributions

Future work

- Desired features for next-generation networks
  - Dynamic behaviour
  - Improved safety (resilience to failures)
  - Improved security (intrusion detection)
- TSN lacks solutions to handle dynamics
- Software defined networking (SDN) a promising approach
  - Centralalised network runtime management
  - Already successfully applied in other domains (e.g. OpenFlow)
- Ongoing research topic*
- Future research directions
  - Intrusion detection / run-time admission control
  - Fail-operational behaviour
  - Bootstrapping procedures

* Thiele and Ernst, “Formal Analysis Based Evaluation of Software Defined Networking for Time-Sensitive Ethernet”. *DATE 2016*

SAFURE Grant Agreement No. 644080

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

"This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government."

If you need further information, please contact the coordinator:

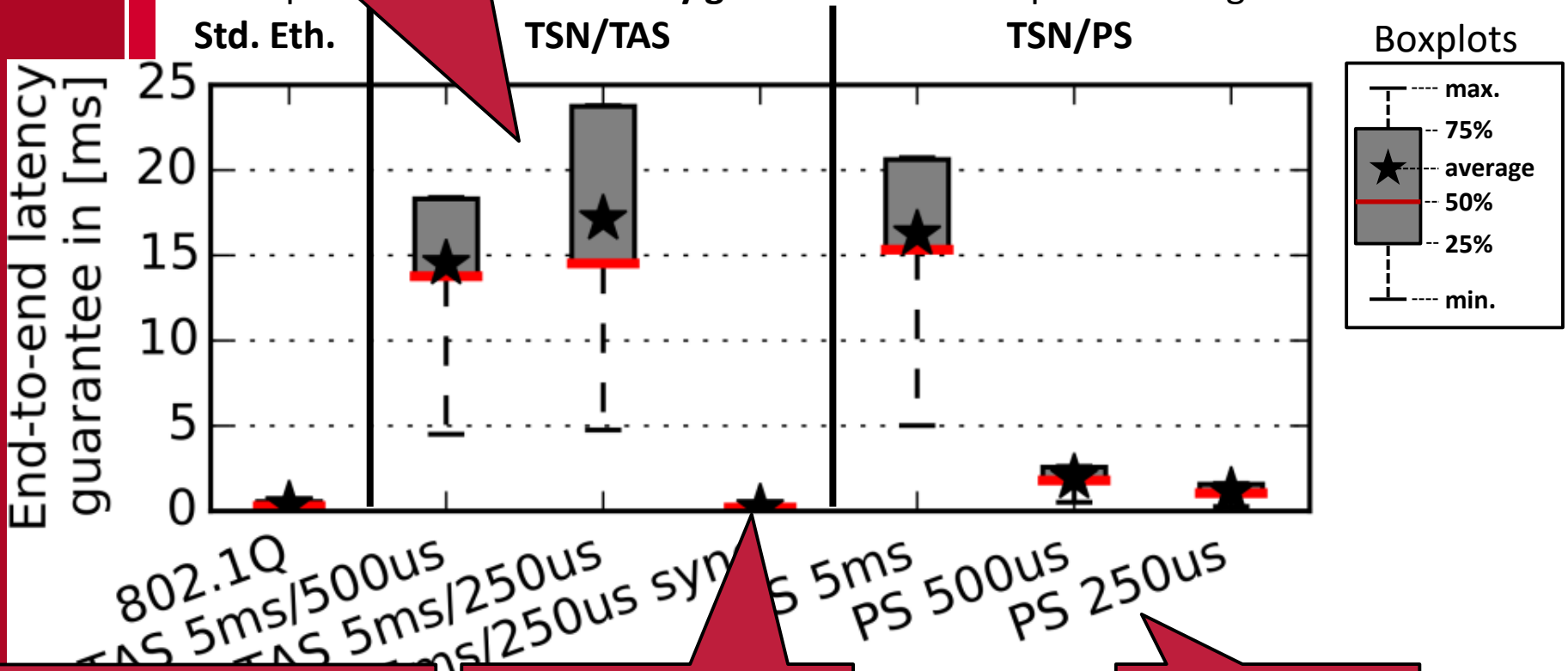
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@safure.eu

Back up slides

Back up slides – TSN/TAS

Evaluation of the Quad Star Topology – N-Shaped Traffic

- Compar[illegible] **end latency guarantees** on 121 paths through the network



TSN/TAS: significantly worse than std. Eth., if unsynchronized

Only use TSN/TAS with synchronization!

TSN/TAS: very low latencies, if synchronized

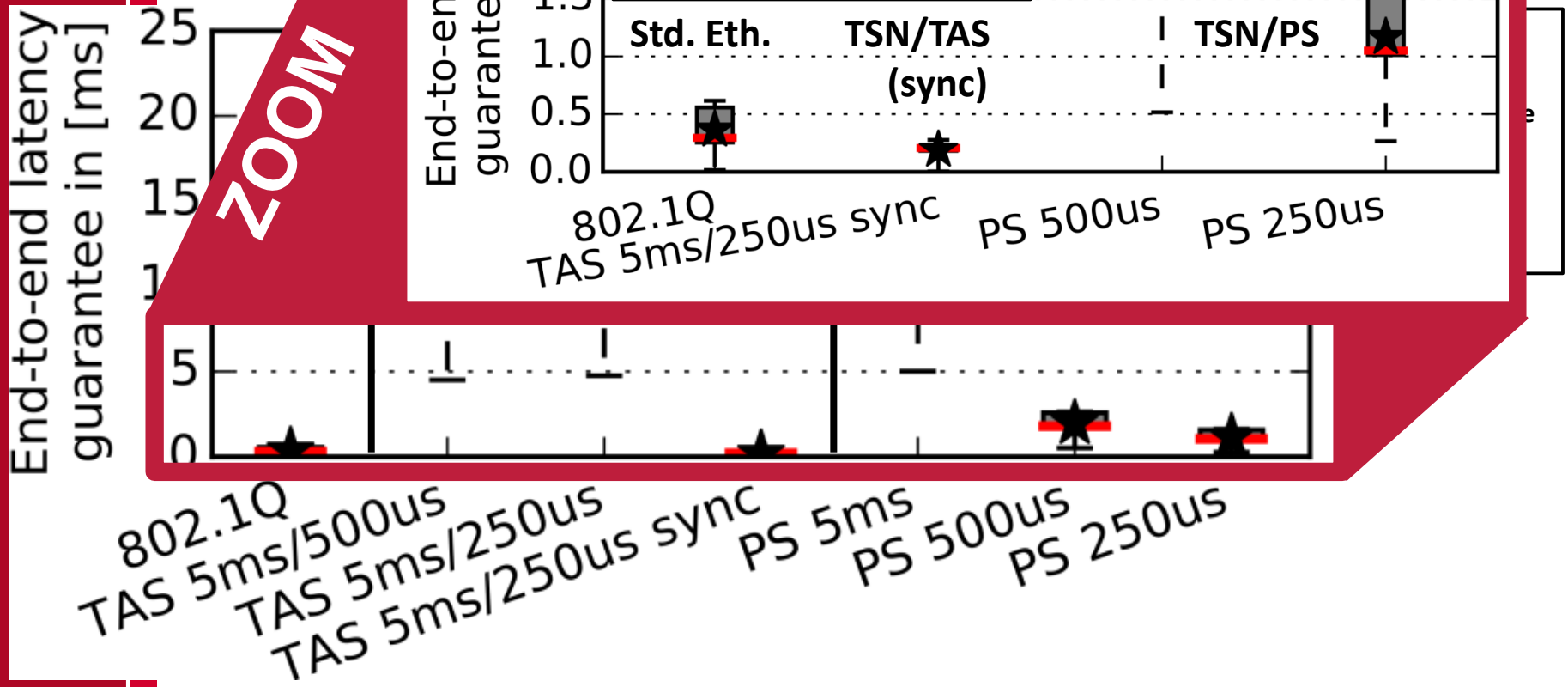
TSN/PS: always worse than std. Eth.

Evaluation of the Quad Star Topology –

Hig

- Compa

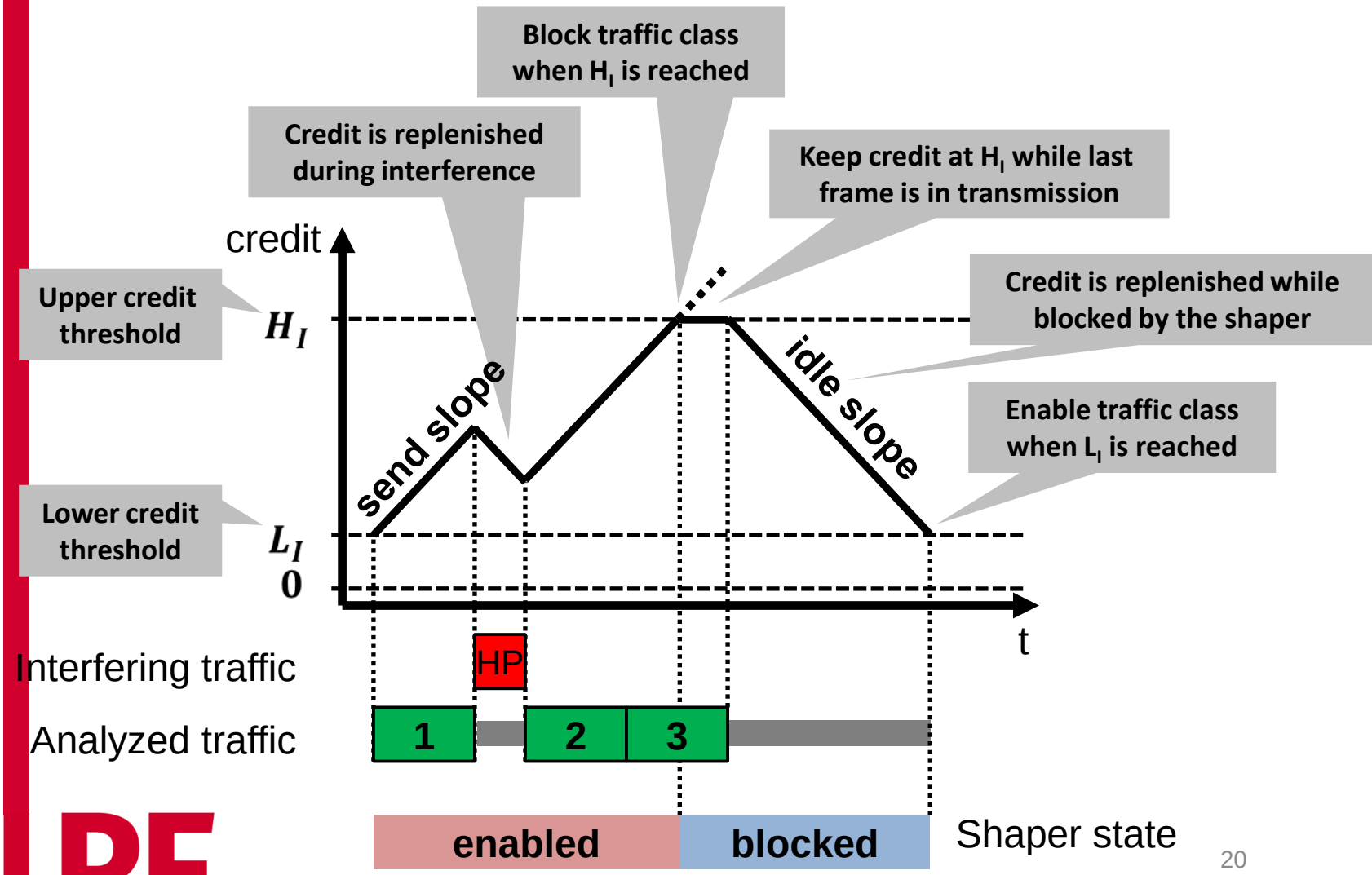
Std. Et



SAFURE

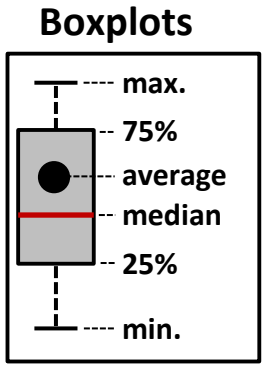
Back up BLS Shaper

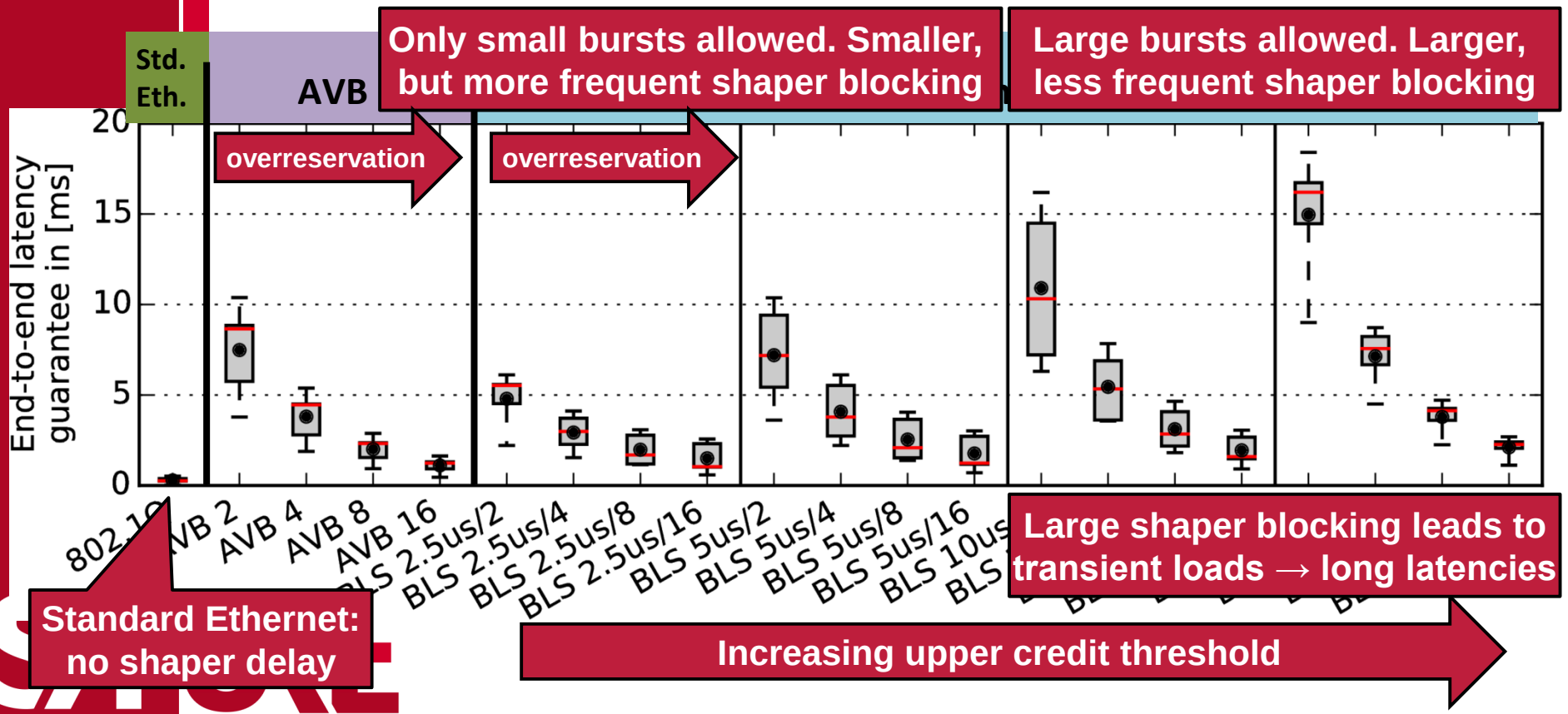
The Burst-Limiting Shaper 1/3



BLS 2/3

- Compare **worst-case end-to-end latency guarantees** of (all) 5 **latency-critical traffic streams**
  - TSN/BLS can give comparable worst-case guarantees as AVB
  - Allowing large bursts in TSN/BLS → large replenishment intervals → longer shaper blocking





BLS 3/3

- Ethernet TSN's burst-limiting shaper
  - **Enforce bandwidth** limits
  - **Allow bursts** of certain size
- Presented **complete formal worst-case analysis** for Ethernet TSN/BLS
  - **End-to-end latencies,** buffer sizes (not part of this presentation)
- Key takeaways for TSN/BLS
  - TSN/BLS allows **better shaper control than AVB**
  - **No advantage of using TSN/BLS over AVB** from a worst-case perspective
    - Shaper delay proportional to the bandwidth limit
  - **Shaping has significant impact on worst-case guarantees**

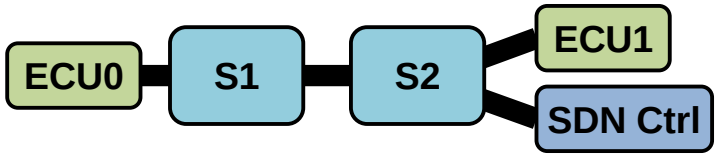
SAFURE

Back up Slides - SDN

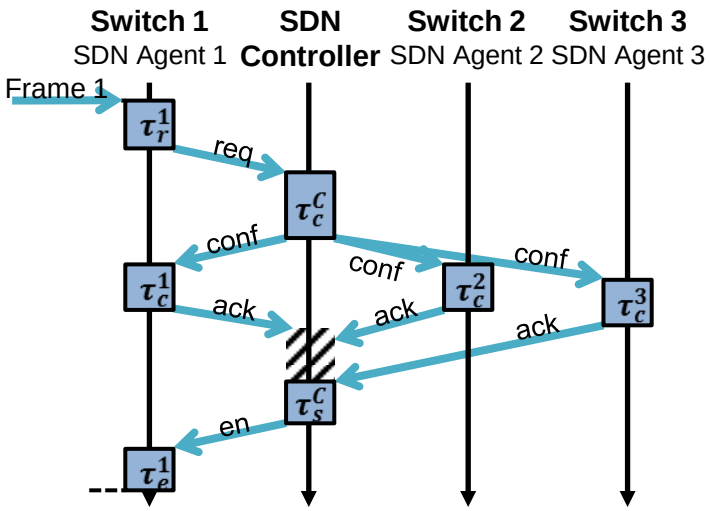
SDN 1/4

- Goal: derive timing guarantees
- Model SDN in **compositional performance analysis** framework [Henia2005]

Topology

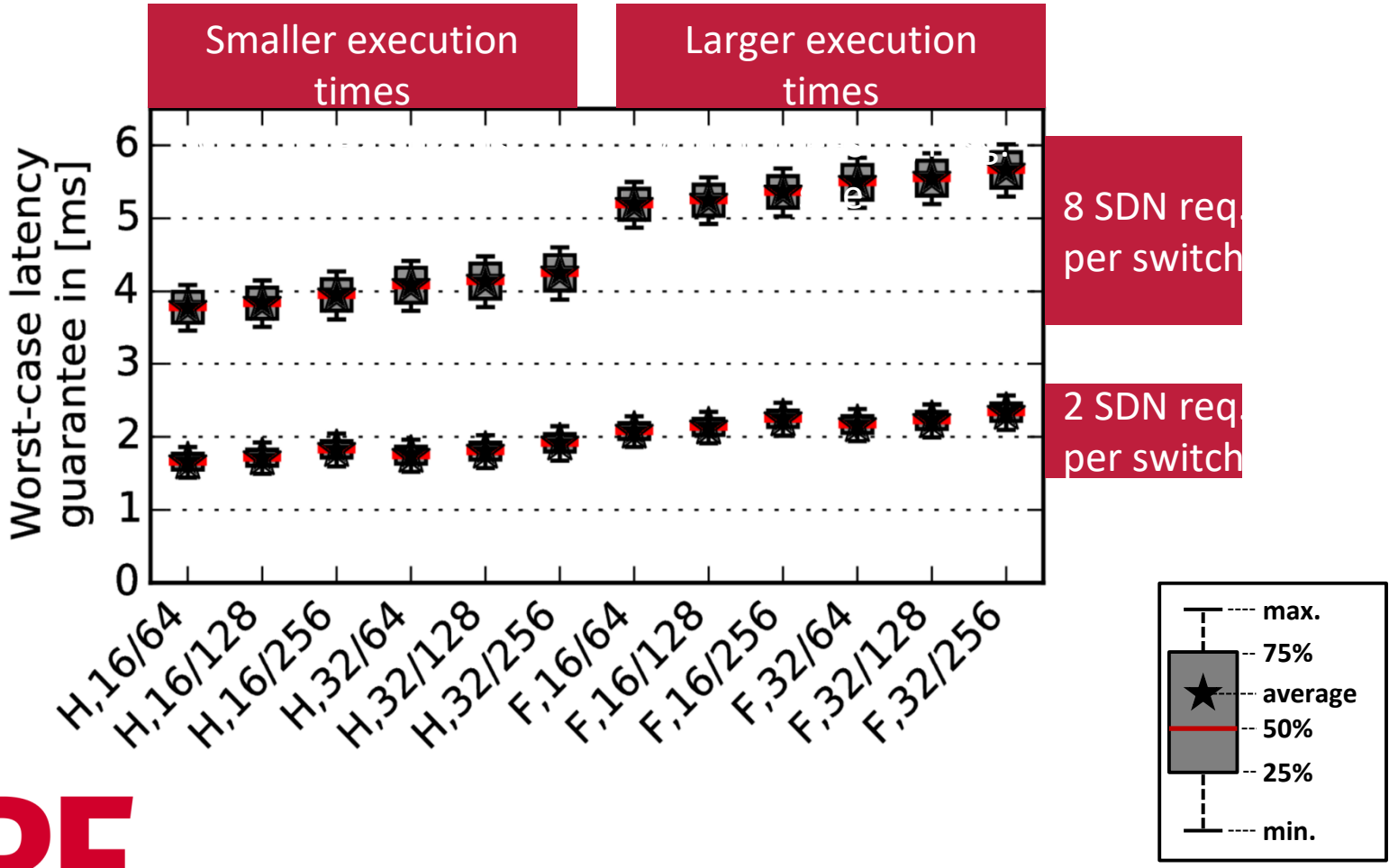


SDN Traffic



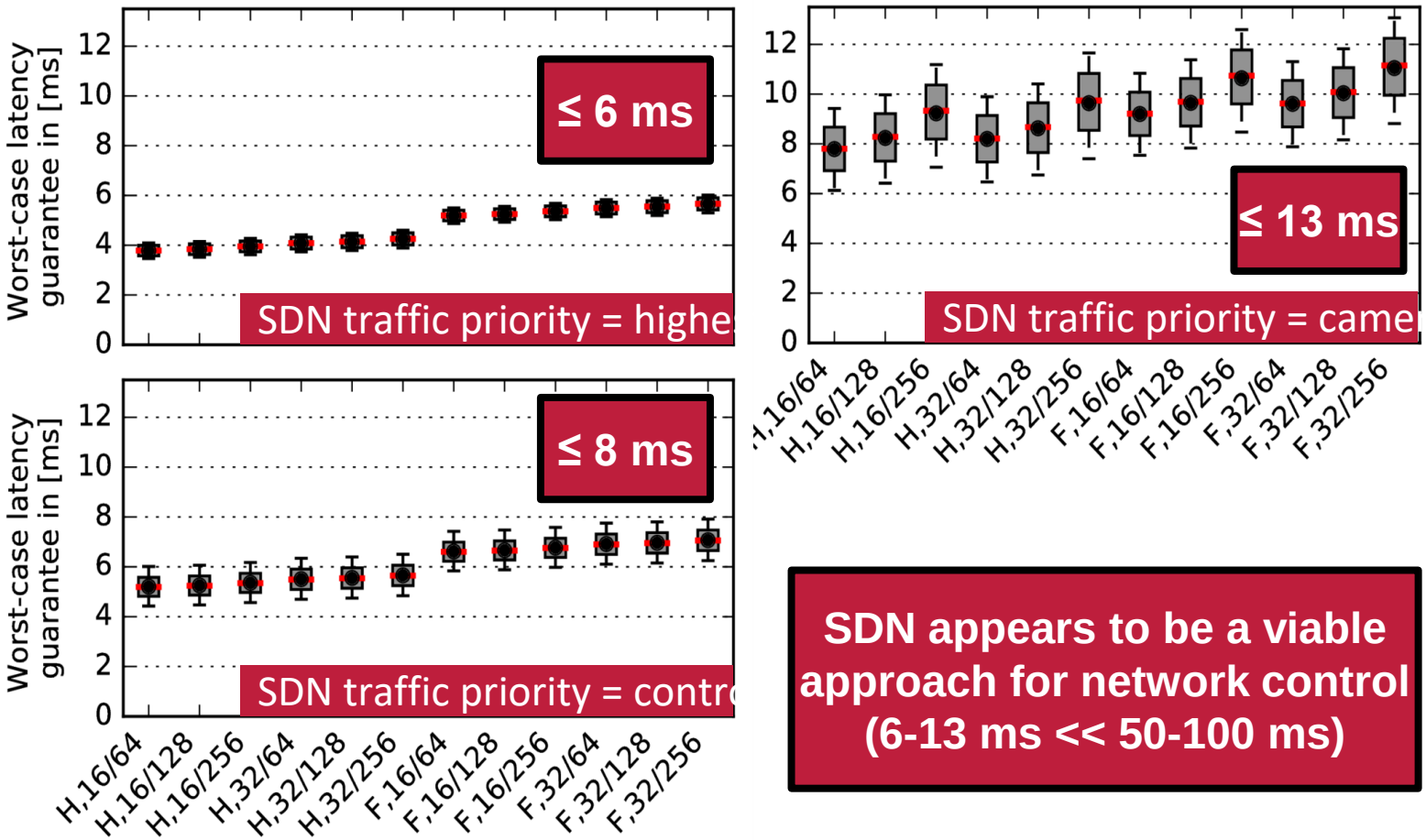
SDN 2/4

- Setup: SDN traffic on highest priority, **variable number SDN requests, request sizes, and execution times**



SDN 3/4

- Setup: **variable SDN traffic priority**, 8 SDN requests per switch, variable request sizes and execution times



SDN appears to be a viable approach for network control (6-13 ms << 50-100 ms)

SDN 4/4

- **Software Defined Networking** is an **interesting** approach to solve the **requirements of future automotive networks**
  - **Freedom from interference** (ISO 26262)
  - **Redundancy** control

- Evaluated the **general suitability of SDN for real-time applications**
  - Typical **automotive setup**
  - SDN **network reconfiguration** times are less than 13 ms
  - **Impact on normal traffic** latencies are less than 3 ms (not shown here)

- **Key takeaways**
  - **Formal timing analysis** of SDN is **possible**
  - **SDN is fast enough** for real-time networks

- Towards **SDN for automotive networks** (SAFURE project, www.safure.eu)
  - Protocol design
  - SDN controller is single point of failure
  - …

SAFURE