Integrated FDF and DbD Demo
Converged Communication and Computation

Arjan Geven, TTTech Computertechnik AG

Iñigo Odriozola, Ikerlan

Maryam Pahlevan, University Siegen

CONNECTA has received funding from the European Union’s Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

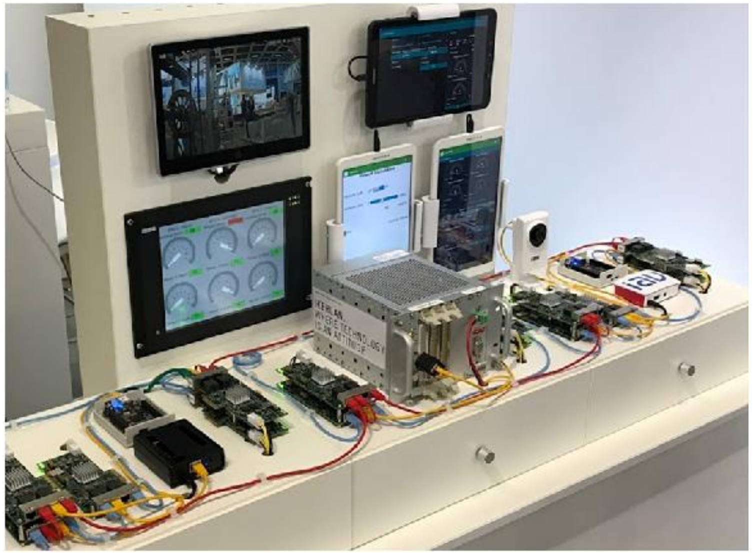
CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

Demonstrator Overview

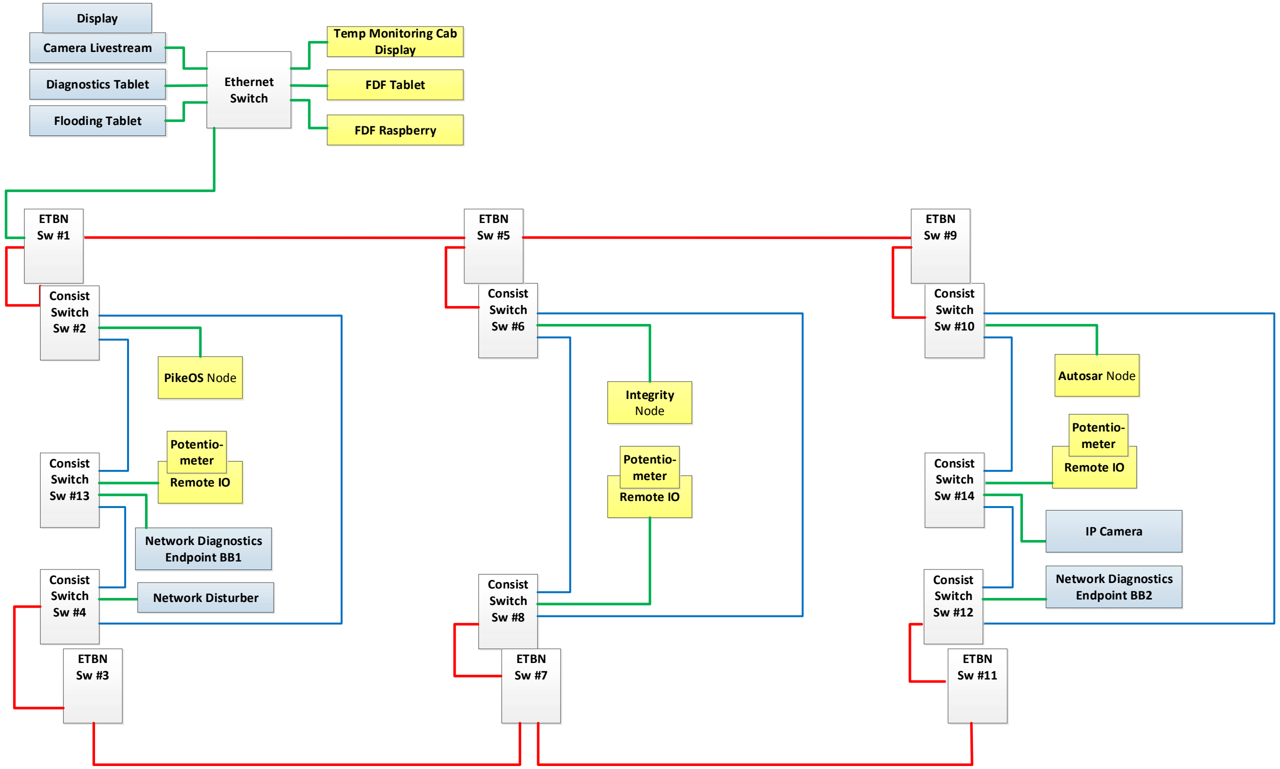
- Converged Communication (DbD)
  - Deterministic Communication
  - Full Network Isolation
  - Robust Topology
- Converged Computation (FDF)
  - Deterministic Computation
  - Full Partition Isolation
  - Spatial Separation
  - Access control for shared memory
  - Monitoring and error-prevention

Demonstrator Contents

- Network
  - Three consist networks + Backbone network
  - IP Camera
  - Network Diagnostics Application
  - Network Disturbance Control
- Computation platform
  - Three instantiations
  - Bogie Monitoring (BMS) Display
  - BMS Diagnostics and Control Terminal

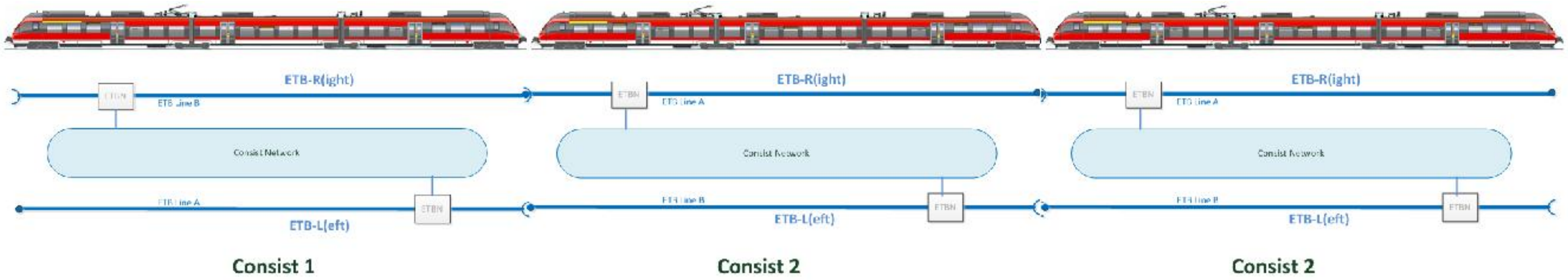


Demonstrator Layout



Robust Redundancy

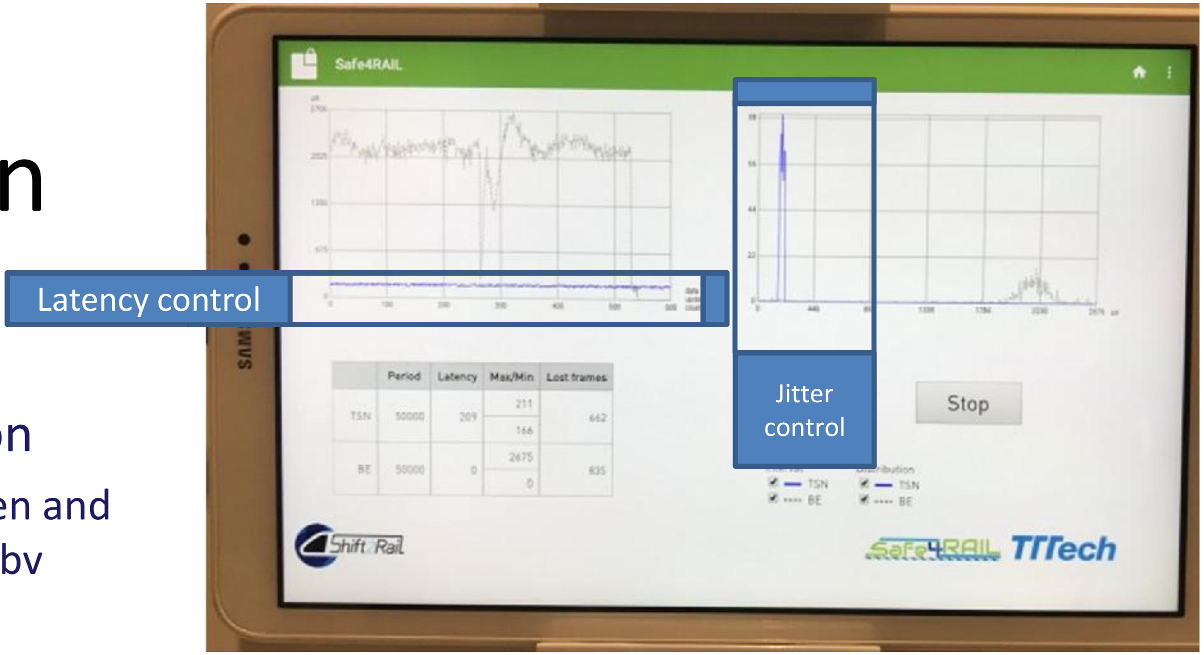
- Use two separated Ethernet lines along the train: ETB-L(eft) and ETB-R(ight).
- ECN ring topology
- Three consists connected



Converged Communication

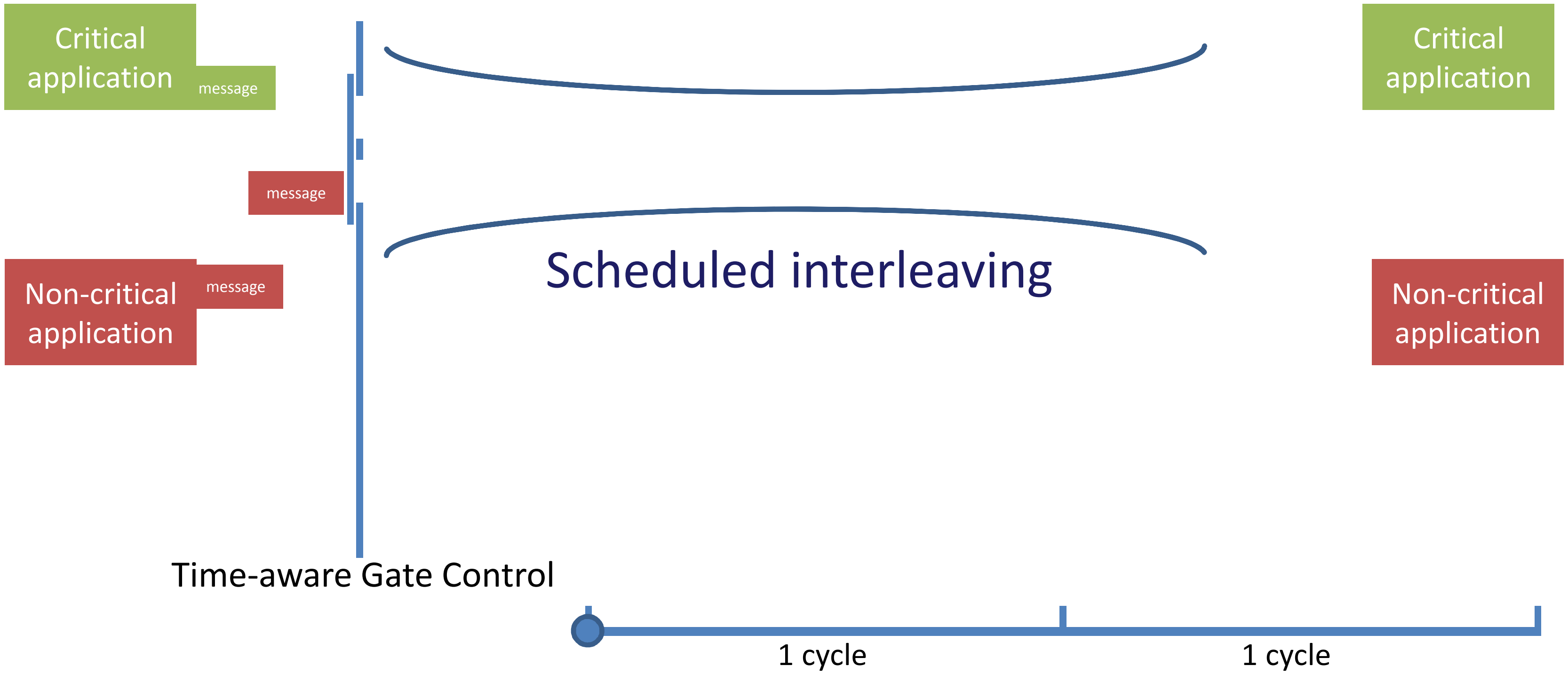
Deterministic Communication

- Synchronized clocks
  - according to 802.1AS-rev
- Scheduled Communication
  - Priority queue gates are open and closed according to 802.1Qbv

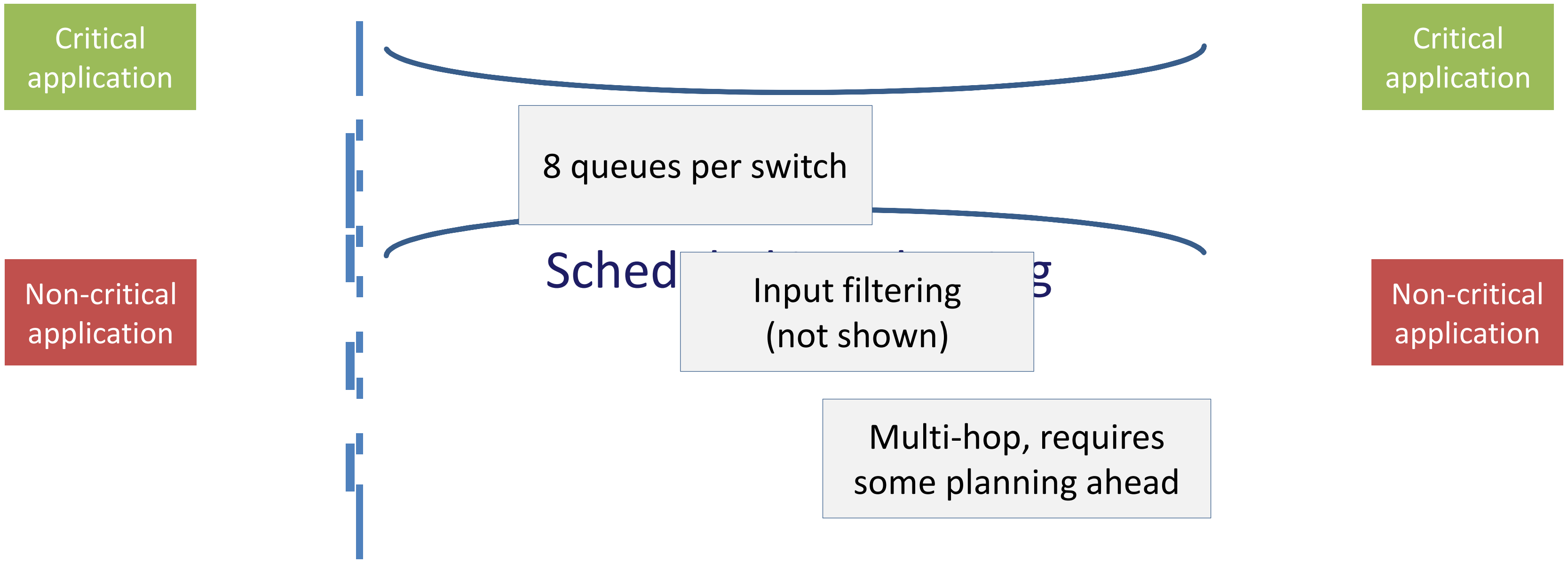


	Period	Latency	Max/Min	Lost frames
TSN	50000	209	211 166	642
BE	50000	0	2675 0	835

Gate Schedule



Gate Schedule



8 queues per switch

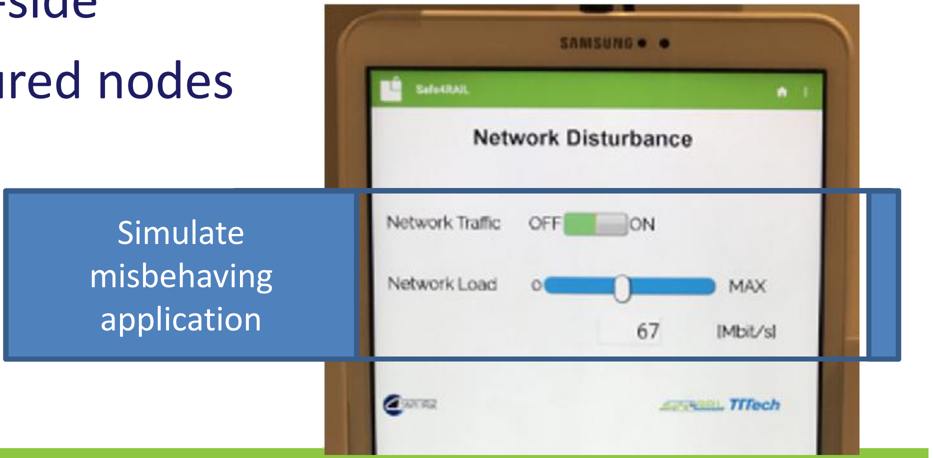
Input filtering (not shown)

Multi-hop, requires some planning ahead

Converged Communication

Full Network Isolation

- Full network virtualization
- Safety and non-safety streams side-by-side
- Misbehaving nodes or wrongly configured nodes can do no harm
- Incoming traffic controlled through 802.1Qci ingress policing
- Not affected by high traffic load



Network Disturbance

Network Traffic OFF ON

Network Load 0 MAX

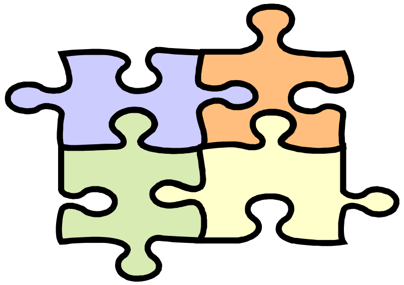
67 [Mbit/s]

Simulate misbehaving application

Live view

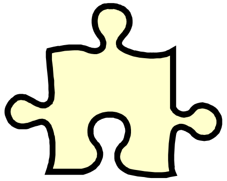
- Follow the camera!

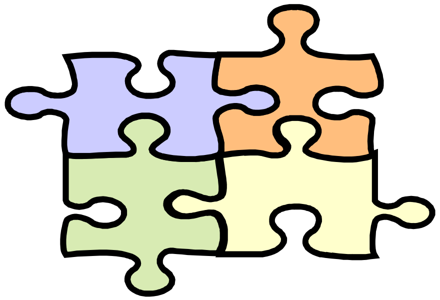
Modular integration concept



AUTOSAR FDF

HW A





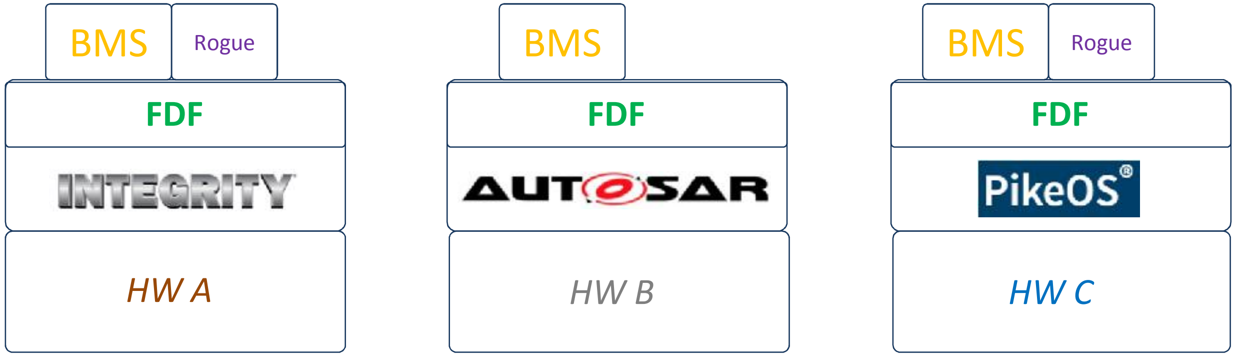
Integrity FDF

HW B

Safety-critical and non-critical application side-by-side on the same platform =>

- Non-interference guaranteed
- HW and communication abstraction

Interoperability



BMS | Rogue

FDF

INTEGRITY

HW A

BMS

FDF

AUTOSAR

HW B

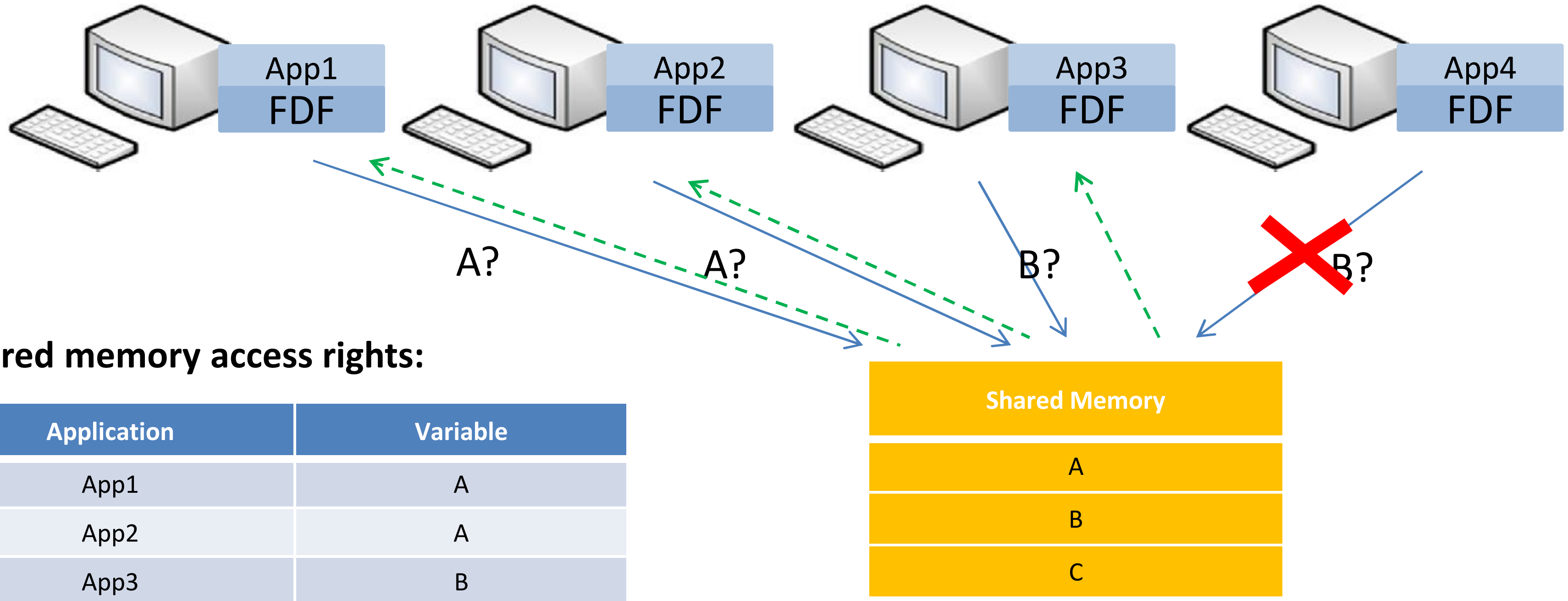
BMS | Rogue

FDF

PikeOS®

HW C

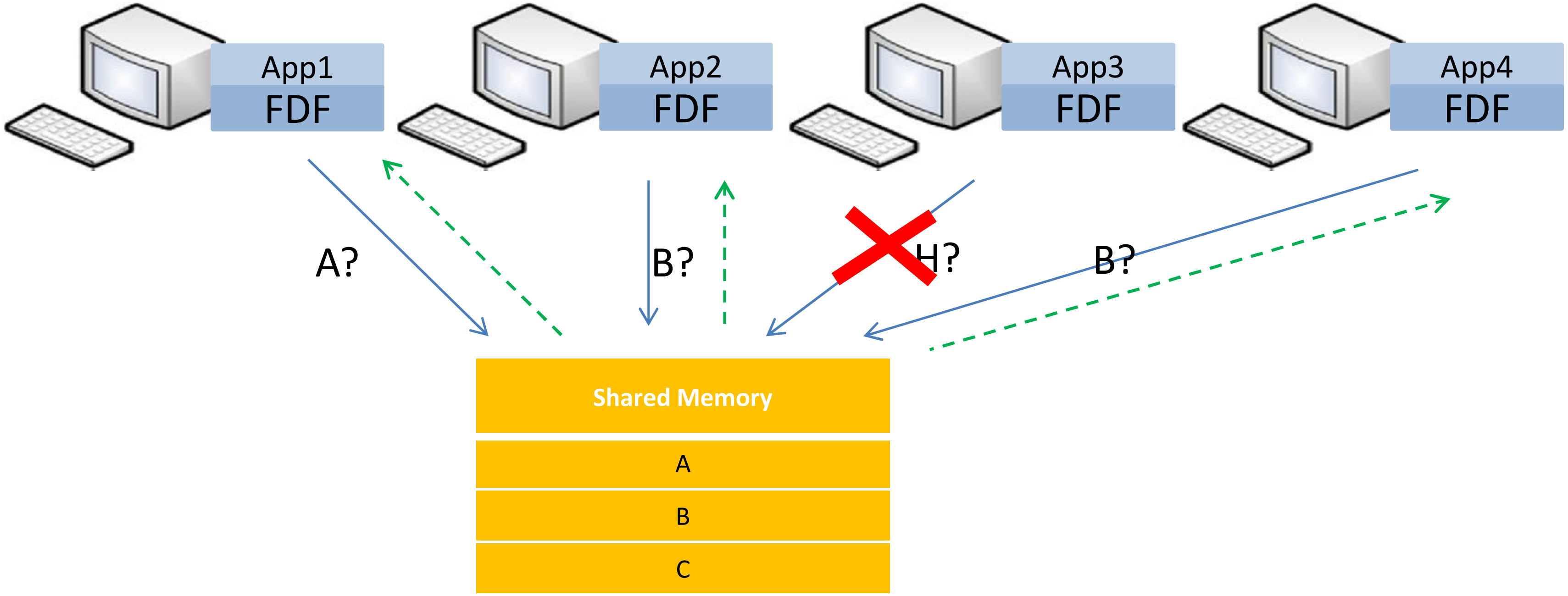
Spatial separation



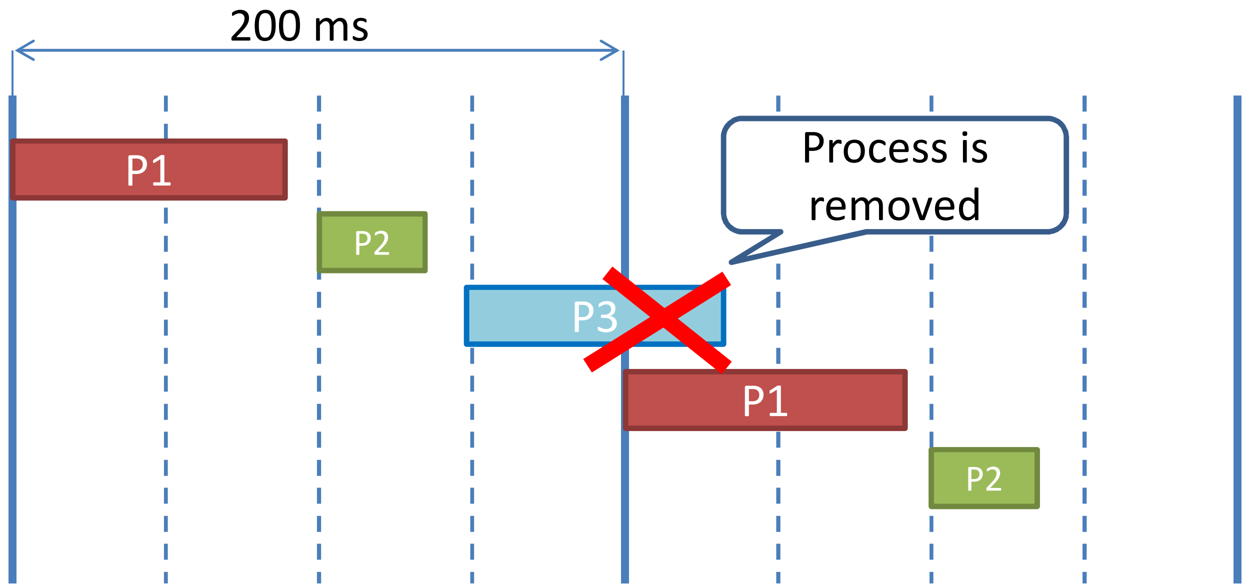
Shared memory access rights:

Application	Variable
App1	A
App2	A
App3	B

Protection & Isolation



Temporal separation



P1: SIL (Safety Integrity Level) 4

P2: SIL 2

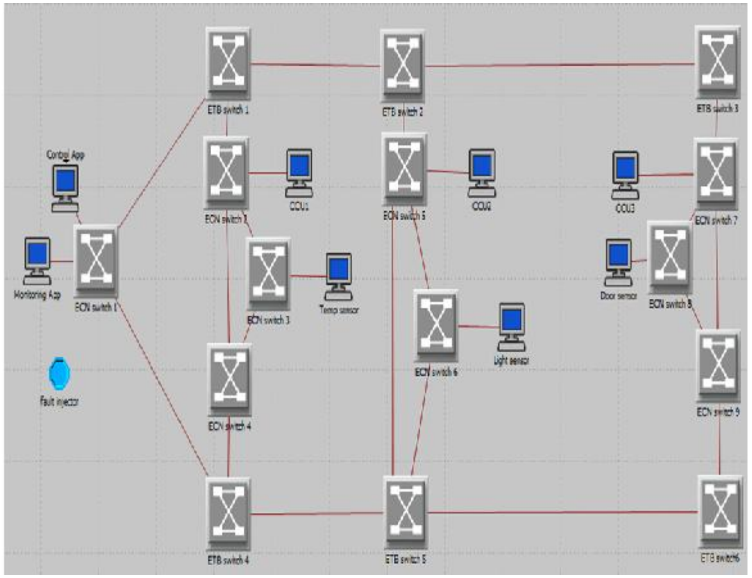
P3: SIL 0 tries to use more than the assigned slot!

Live view

- Follow the camera!

DbD Simulation Framework

- Evaluate and validate the applicability of TSN solutions for DbD concepts
  - The V/V processes of train components compliant to TSN protocols are expensive and timely
  - The simulation tools are time and cost efficient alternative for analyzing the temporal and non-temporal attributes of TSN-capable components
- DbD simulation components
  - Configuration Manager
    - Heuristic TT scheduler
    - Network Generator
  - TSN-capable Switches and End-system
    - Time-Aware Shaper (IEEE 802.1Qbv)
    - Ingress Time-based Filtering (IEEE 802.1Qci)
    - Frame Replication and Elimination for Reliability (IEEE 802.1CB)



Configuring the DbD Simulator

- Set up the example TCN layout taken from the proof-of-concept implementation of the demonstrator with minor adaptations
  - Run the heuristic TT scheduler to compute the global TT transmission schedule
  - Run configuration management to generate device-specific GCLs and the network layout XML file
  - Import the network topology XML file and create the demonstrator network
  - Set up statistics parameters of end-systems and switches
  - Run the simulation and examine the simulation results
  - Set the fault injector to inject different faults into the simulation network
  - Evaluate the impact of every faults on different streams in the simulated network