"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

Introduction to SAFURE

André Osterhues, ESCRYPT GmbH

HiPEAC
SAFURE Workshop
22th January 2018
Manchester, UK

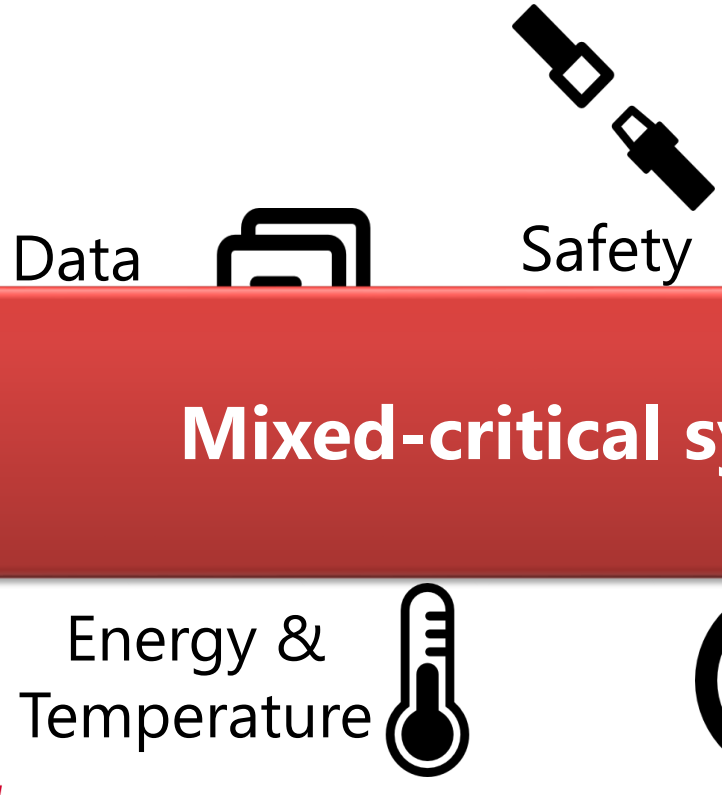
Agenda

- Introduction
- Criticalities
- SAFURE Project
- SAFURE Framework
- Security, Safety, and Integrity Aspects
- Mixed-critical Use Cases
- Industrial Use Cases
- Project Partners
- More Information

Introduction

- Current trends in embedded systems:
  - **Multi-core** architectures
    - Energy efficiency, temperature integrity
  - **Heterogeneous** solutions
    - CPUs, Networks
  - **Networking**
    - TTEthernet, WiFi, Bluetooth LE
  - **Real-time** response
  - **Safety-critical** functions
    - Medical devices
    - Automotive (crash avoidance, driver assistance)

Criticalities

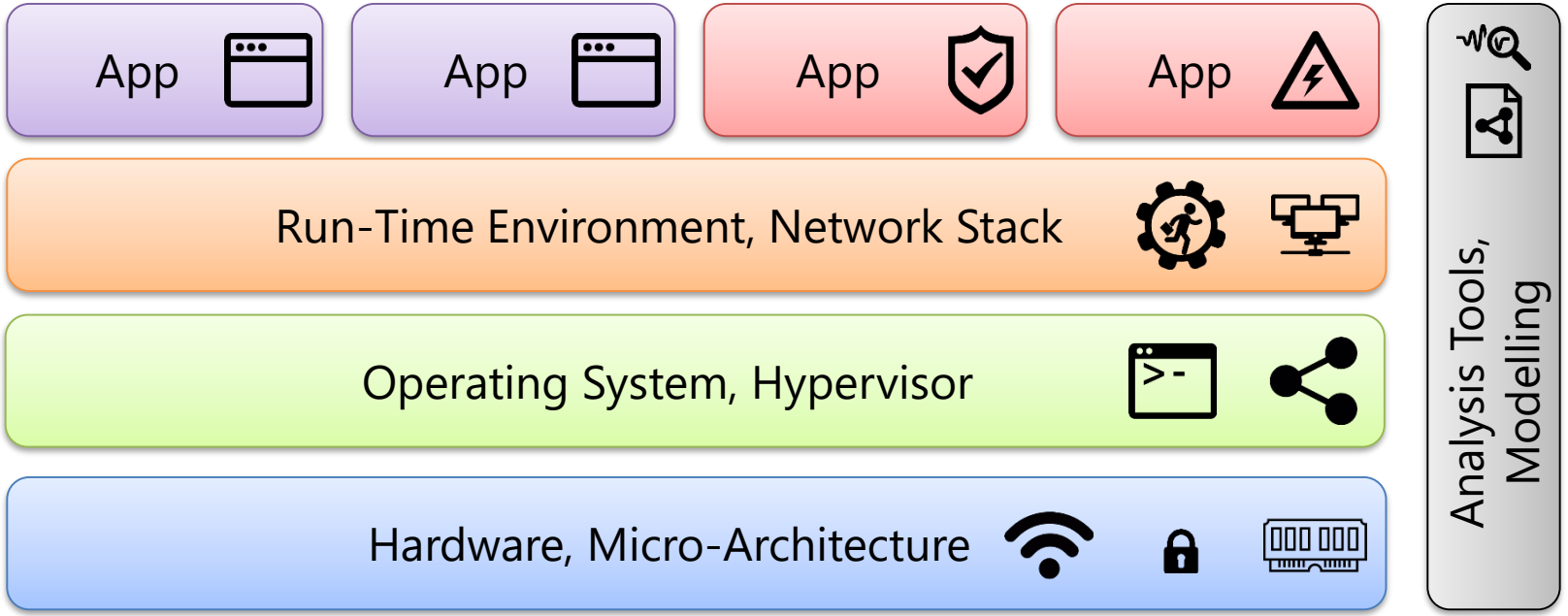


SAFURE Project – Ambition

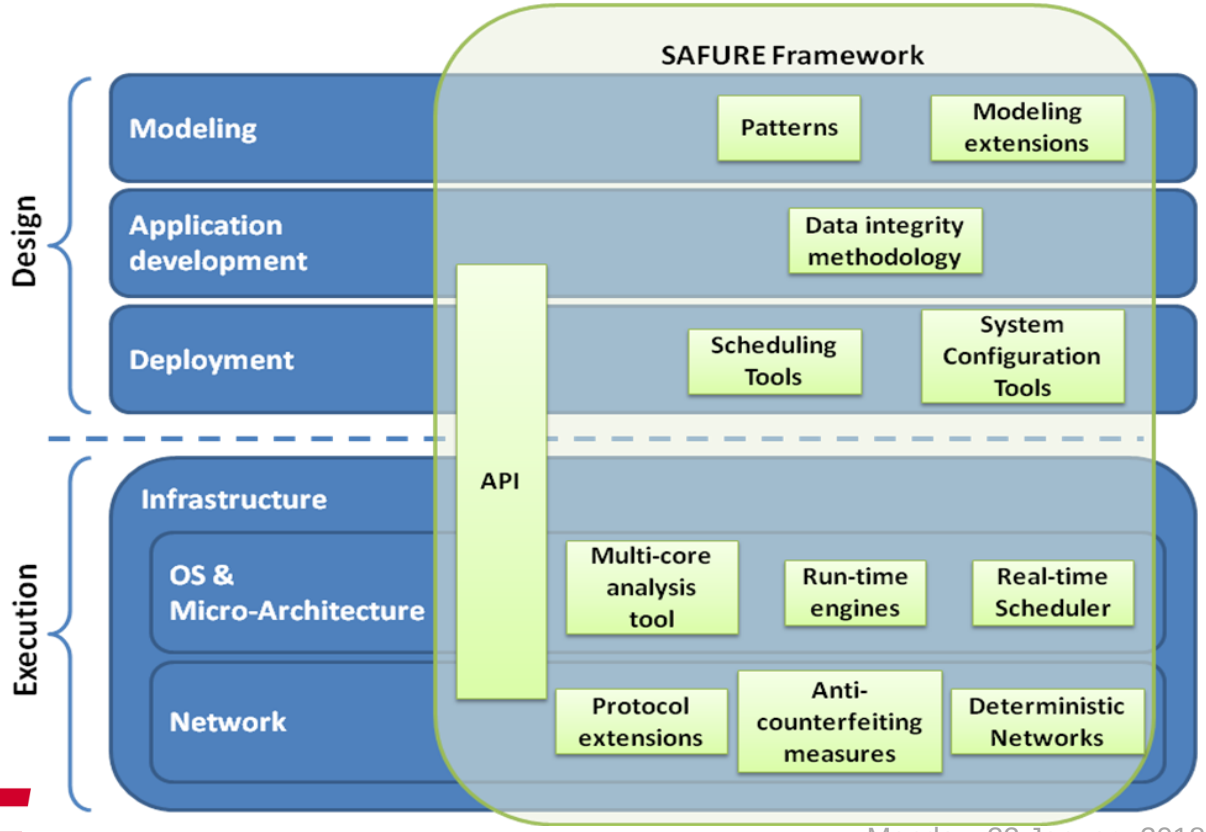
- Ambition:
  - Create & apply **methodology** to develop Cyber-Physical Systems
  - Consider mixed criticalities
- Problem:
  - Criticalities are often **not considered jointly**, or
  - applied **one on top of the other**
- Idea:
  - Integrate mixed criticalities **by design** into development process

SAFURE Project – Approach

- Enable criticalities **"by design"** across all levels



SAFURE Framework

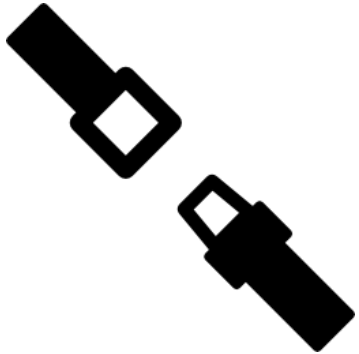


Security Aspects

- **Security Risks Analysis**
  - Threat identification
  - Risk Assessment
- **Secure Boot**
  - Ensure that system is not compromised
  - Guarantee authenticity and integrity of boot image
- **Secure Update**
  - Allow only authorized software/firmware to be flashed
- **Secure Communication**
  - Confidentiality: by encryption
  - Integrity and authenticity: by digital signatures or MACs
- **Secure Key Management**
  - Generation, Distribution, Storage, Deletion

Icons designed by Freepik

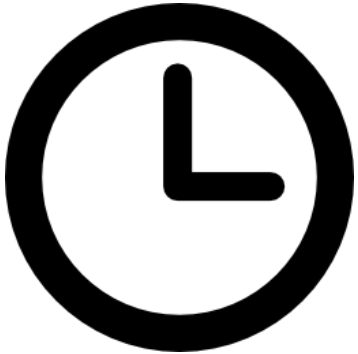
Safety Aspects



- Maintainability, reliability
  - Fault prevention
- Safety-aware Run-time Engines (RTE)
  - Distinguish critical and non-critical tasks
- RTE-level scheduling algorithms
  - Ensure that deadlines are met for critical tasks
- Real-time requirements
- Standards
  - ISO 26262: Road vehicles – Functional safety
  - Automotive safety integrity level (ASIL)

Icons designed by Freepik

Integrity Aspects



Timing

- Resource sharing
- QoS-enabled run-time engine
- Network scheduling

Energy & Temperature

- Power/temperature monitoring
- Thermal analysis and modelling (heat diffusion, cooling)

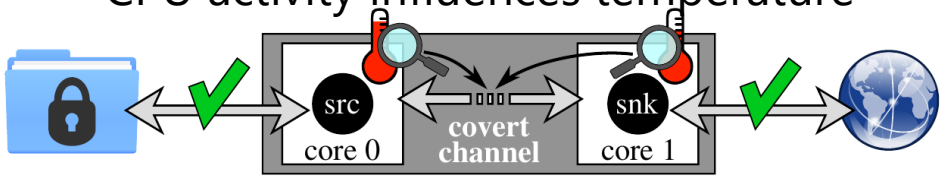
Data

- Anti-counterfeiting
- Digital signatures (RSA, ECC)
- MACs

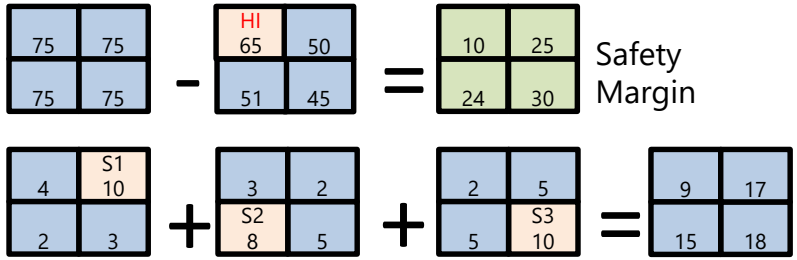
Icons designed by Freepik

Mixed-critical Use Cases (I)

- Thermal protection (security + energy)
  - Problem: Thermal side-channel attacks
    - CPU activity influences temperature



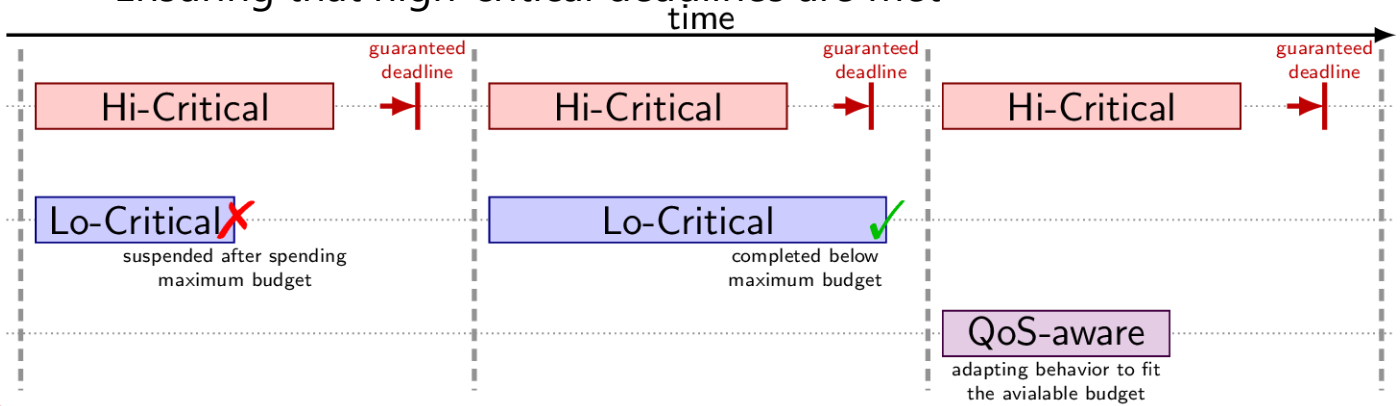
  - Solution: Temperature isolation servers
    - Bounds for allowed temperature increase



DTM triggered if any core is above 75

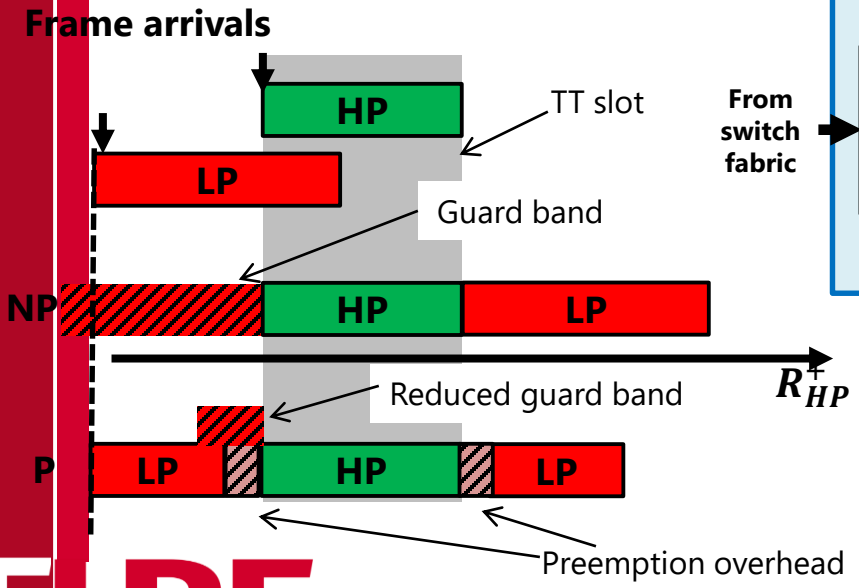
Mixed-critical Use Cases (II)

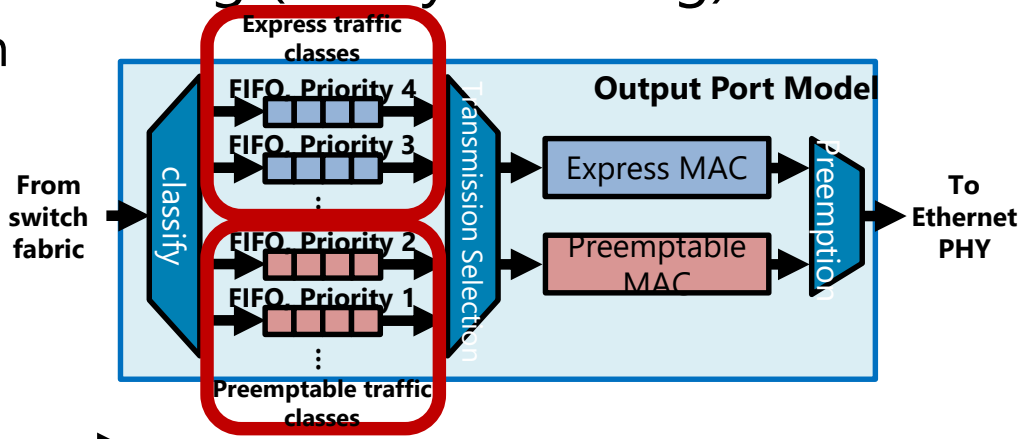
- Multi-core task scheduling (safety + timing)
  - Perform scheduling actions at runtime to avoid adverse effects by
    - Monitoring resource usage
    - Suspending low-critical tasks
    - Ensuring that high-critical deadlines are met



Mixed-critical Use Cases (III)

- Time-Sensitive Networking (safety + timing)
  - Frame preemption





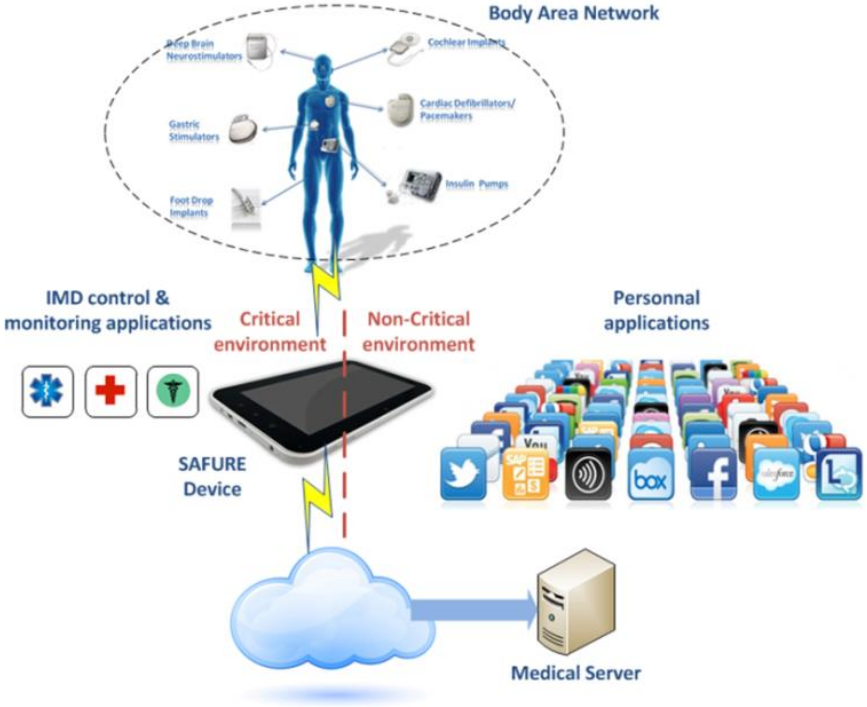
Performance gain due to frame preemption:
Ethernet: ~12us vs 120us
TSN: ~12us vs 120us
➔ Factor 10 improvement

Mixed-critical Use Cases (IV)

- Secure communication of patient data (security + safety)
  - Real-time, safety-critical data
  - Preserve confidentiality and integrity of data
    - AES in GCM mode of operation
  - Key management
    - Pre-shared symmetric keys
    - Public-Key Infrastructure (using RSA or EdDSA algorithms)

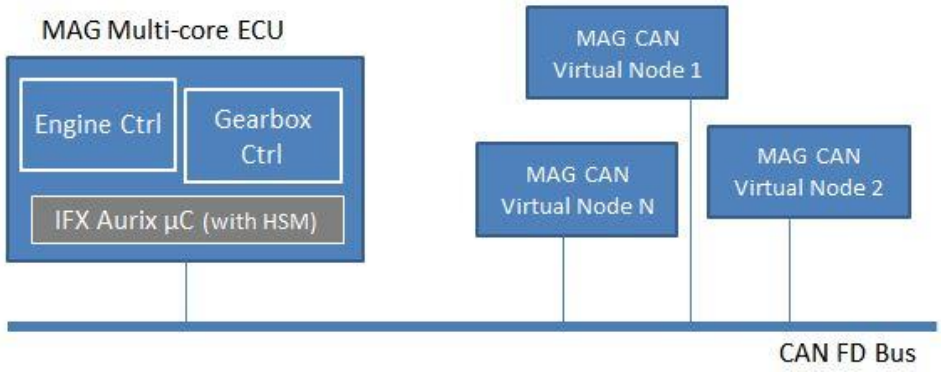
SAFURE Industrial Use Cases (I)

- **Telecommunications Use Case**
  - Body Area Network
  - Remote monitoring of a patient's health status
  - Device: Sony Xperia
  - PikeOS (real-time, microkernel-based OS)



SAFURE Industrial Use Cases (II)

- **Automotive Multi-Core Use Case**
  - Engine, valve and transmission control
  - Compliance with ISO-26262 (automotive safety)
  - Data integrity on Intra-ECU / Inter-ECU communications
  - Data protection
  - Timing analysis
  - Infineon Aurix
  - ErikaOS
    - Real-time
    - AUTOSAR-compliant

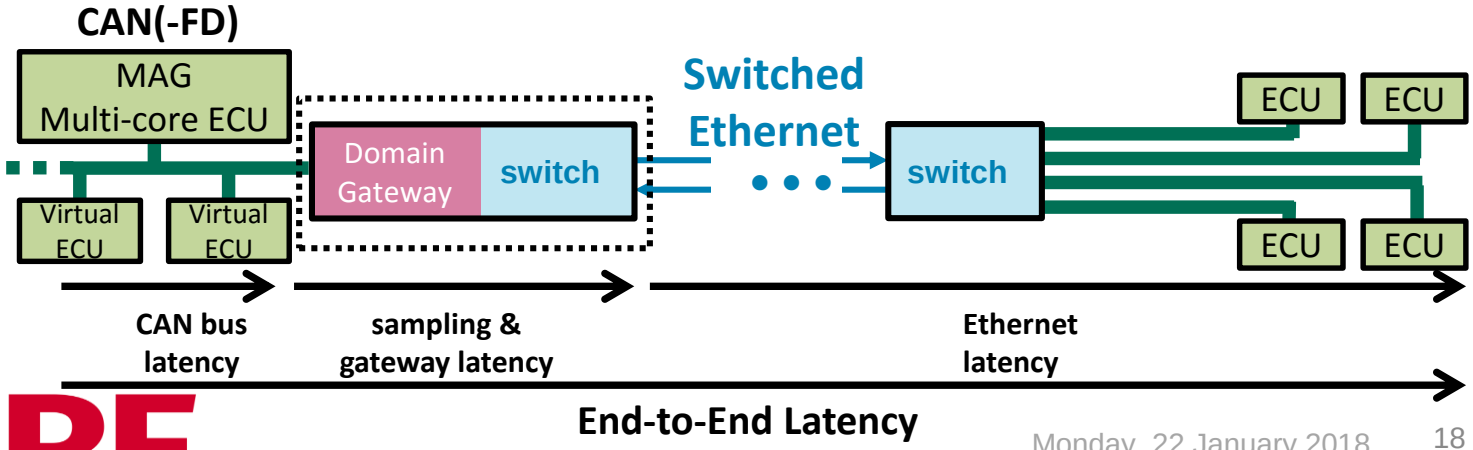


SAFURE Industrial Use Cases (III)

- **Automotive Network Use Case**
  - Ethernet will be the backbone network in future vehicles
  - Fail-operational communication required for highly-automated/autonomous driving
  - Connected vehicles require security to prevent attacks
  - Hardware-based demonstrator
    - Time-Triggered Ethernet (TTEthernet)
  - Virtual demonstrator
    - Based on software simulation

SAFURE Industrial Use Cases (IV)

- **Use Case Combination**
  - Combination of multi-core and network use cases
  - Inter-domain CAN(-FD) traffic from multi-core ECU to Ethernet and back
  - Ensure safety and security requirements by the SAFURE data, timing, and energy integrity solutions



SAFURE Project Partners

Barcelona Supercomputing Center
Centro Nacional de Supercomputación

escrypt
Embedded Security by ETAS

ETH zürich

MAGNETI MARELLI

INSTITUTE OF COMMUNICATION, INFORMATION AND PERCEPTION TECHNOLOGIES
Scuola Superiore Sant'Anna

SYMTA VISION

SYSGO
EMBEDDING INNOVATIONS

TECHNIKON

Technische Universität Braunschweig

THALES

TTTech
Ensuring Reliable Networks

More Information

- SAFURE website:
  - https://safure.eu/
- Blog:
  - https://safure.eu/blog
- Twitter:
  - https://twitter.com/SAFURE_H2020
- LinkedIn:
  - https://www.linkedin.com/grps/H2020-SAFURE-Friends-8284939/about

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