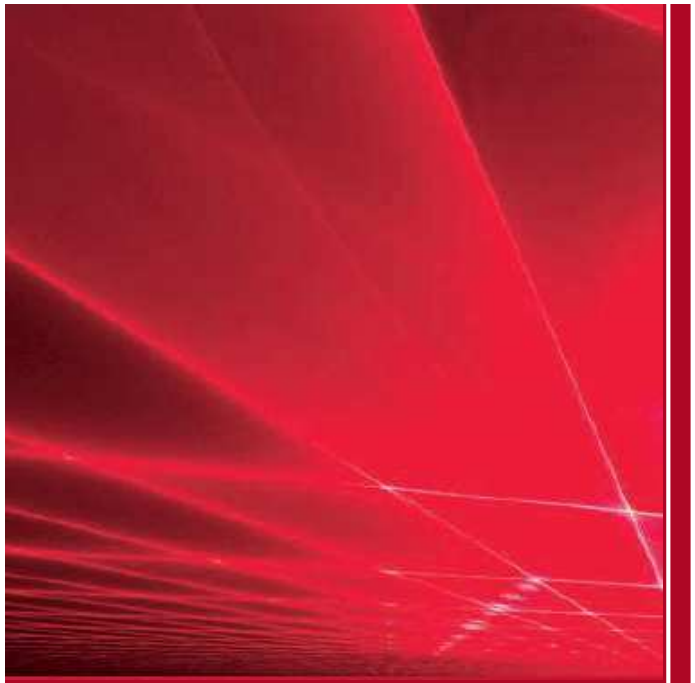


SAFety and secURity by dEsign for interconnected mixed-critical CPS

Carolina Reyes, TTTech Computertechnik AG

ARTEMIS Spring Event
14th April 2016
Vienna, Austria

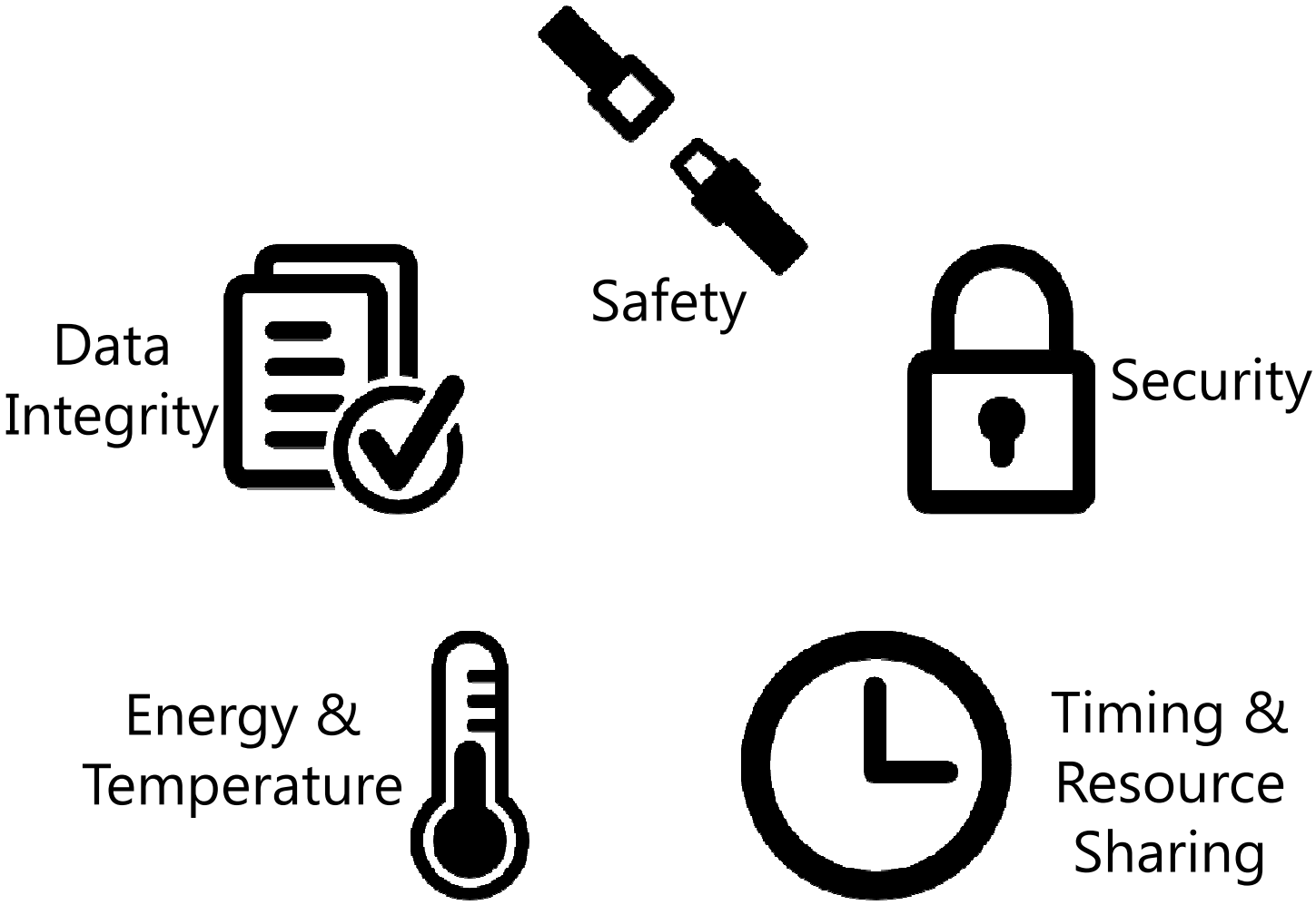
SAFURE

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

Introduction

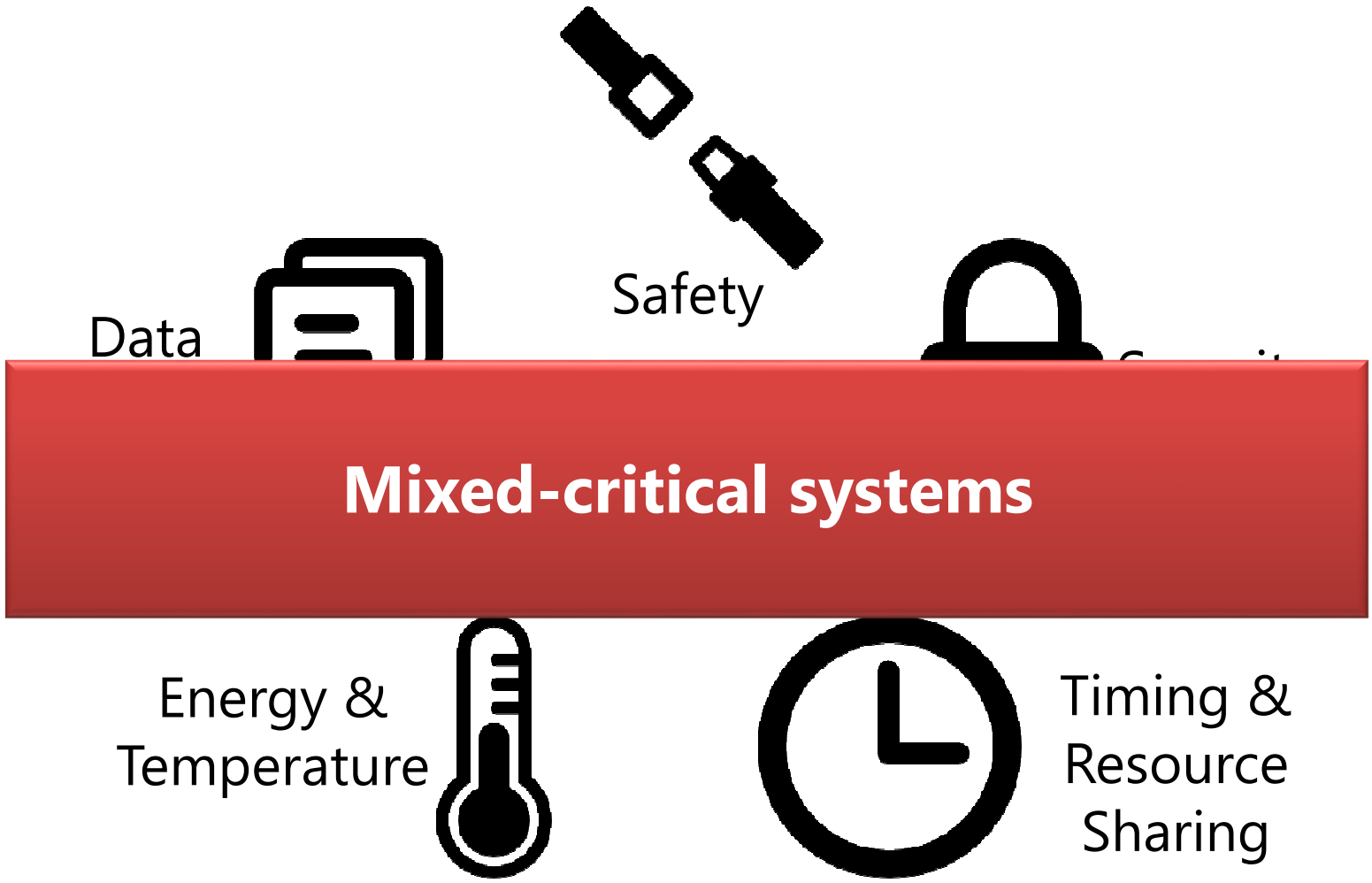
- Current trends in embedded systems:
  - **Multi-core** architectures
    - Energy efficiency
  - **Networking**
    - TTEthernet, WiFi, Bluetooth LE
  - **Real-time** response
  - **Safety-critical** functions
    - Medical devices (insulin pumps)
    - Automotive (crash avoidance, driver assistance)

Criticalities



Icons designed by Freepik

Criticalities



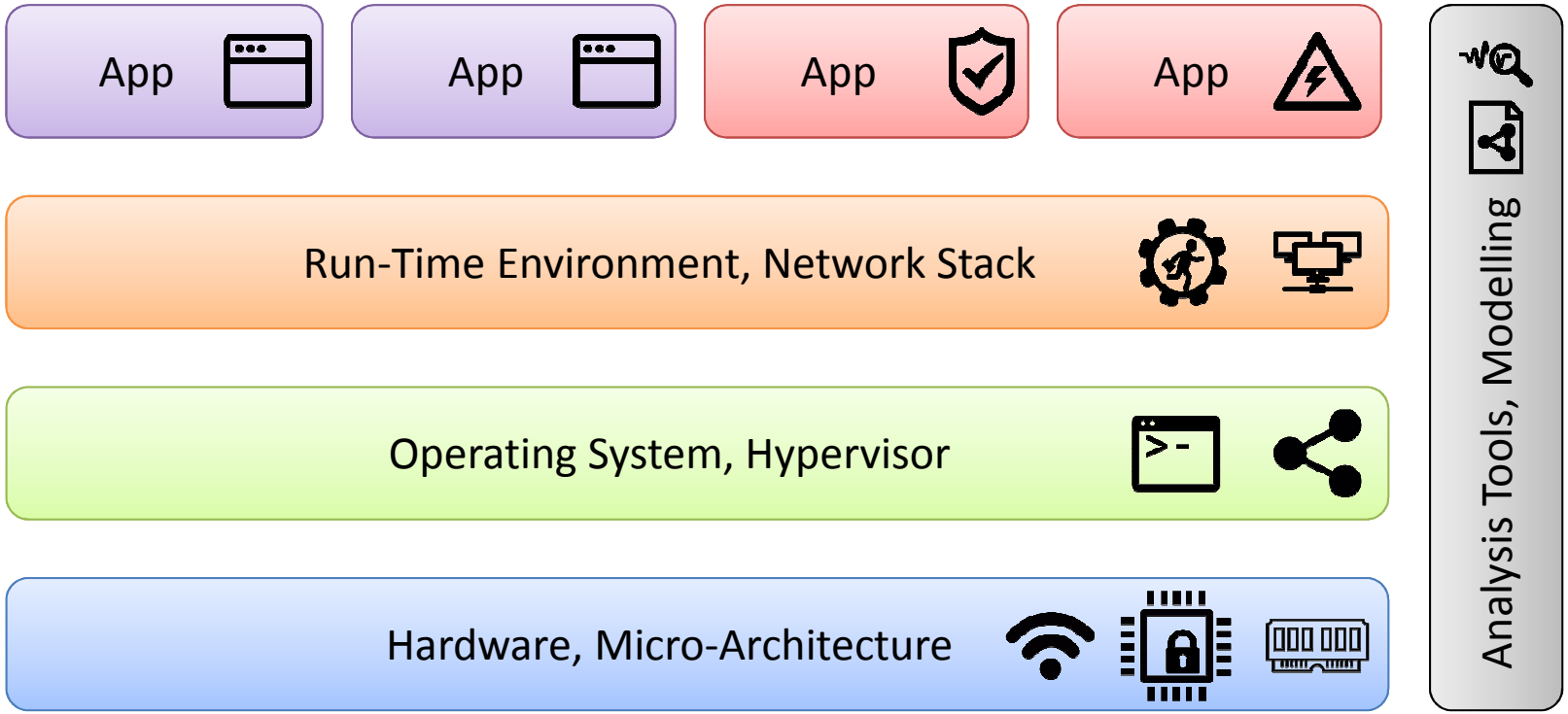
Icons designed by Freepik

SAFURE Project

- 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

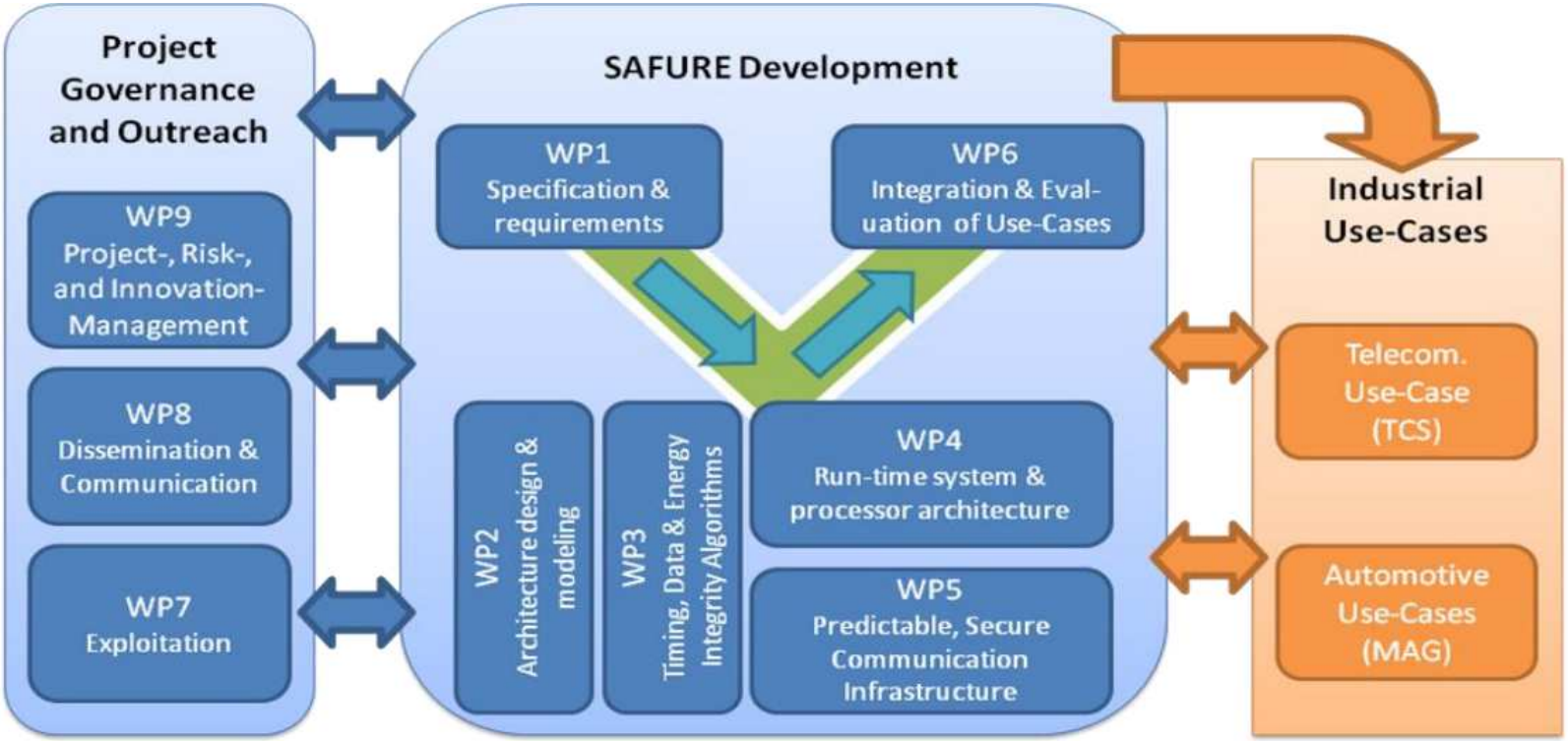
SAFURE Project – Approach

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

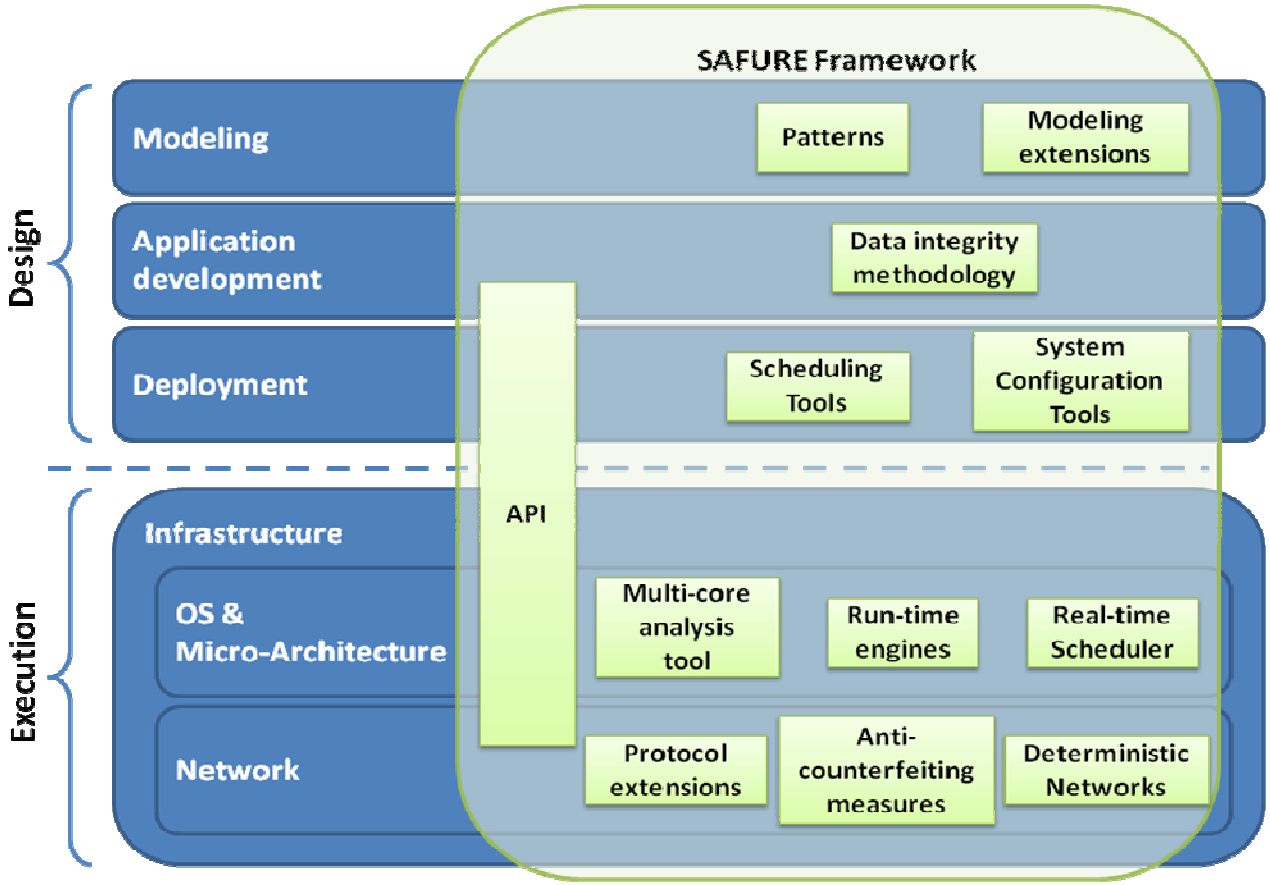


Icons designed by Freepik

SAFURE Project – WP Structure

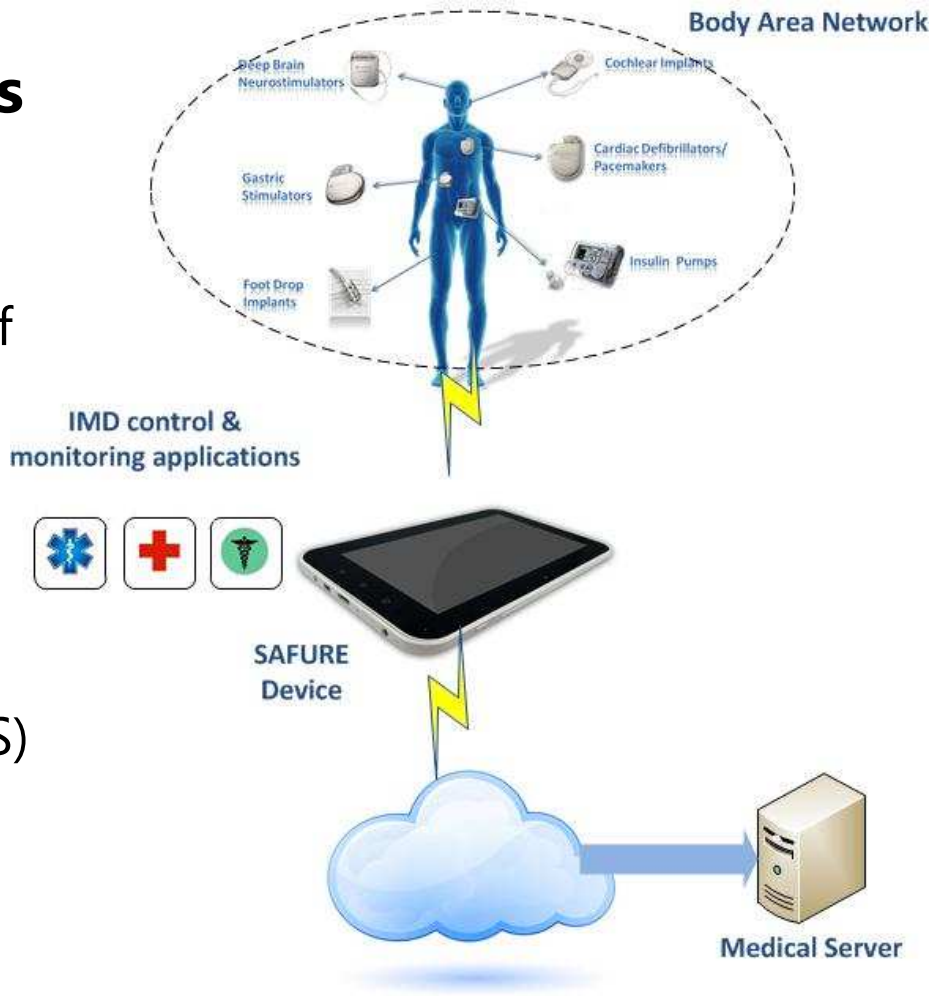


SAFURE Framework



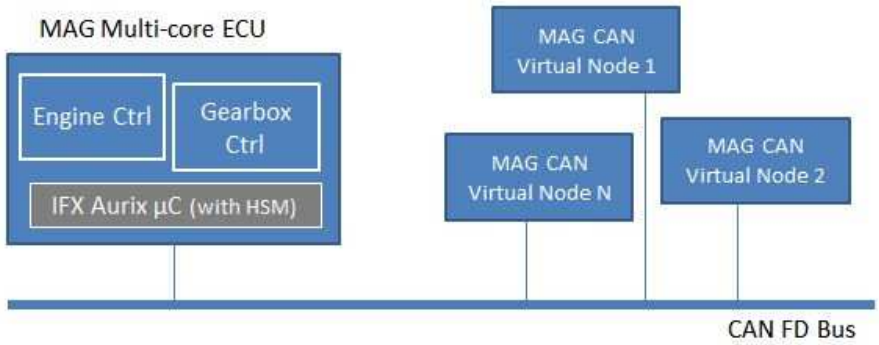
SAFURE Industrial Use Cases (I)

- **Telecommunications Use Case**
  - Body Area Network
  - Remote monitoring of a patient's health status
  - Device: Qualcomm Dragonboard 810
  - 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 (incl. HSM)
  - ErikaOS (real-time, AUTOSAR-compliant OS)

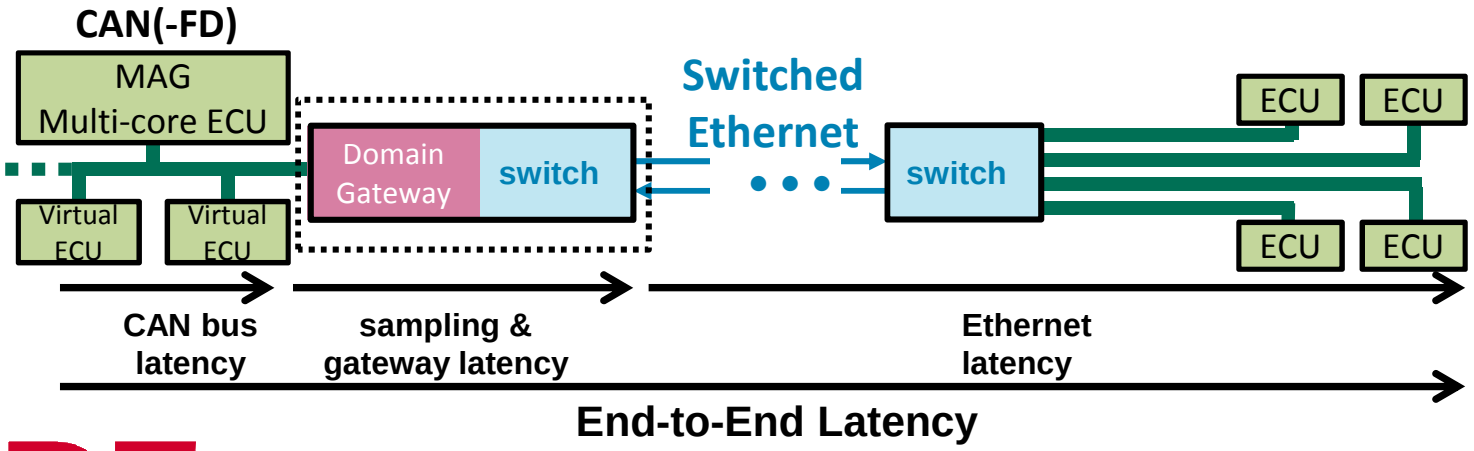


SAFURE Industrial Use Cases (III)

- **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
  - Real demonstrator
    - Time-Triggered Ethernet (TTEthernet)
  - Virtual demonstrator
    - Based on software simulation

SAFURE Industrial Use Cases (IV)

- **Use Case Combination**
  - Demonstrate 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

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