Real-time containers for mixed-criticality cyber-physical cloud systems

Marcello Cinque

DIETI, Università degli Studi di Napoli Federico II, Italy

macinque@unina.it

DEpendable and Secure Software Engineering and Real-Time Systems

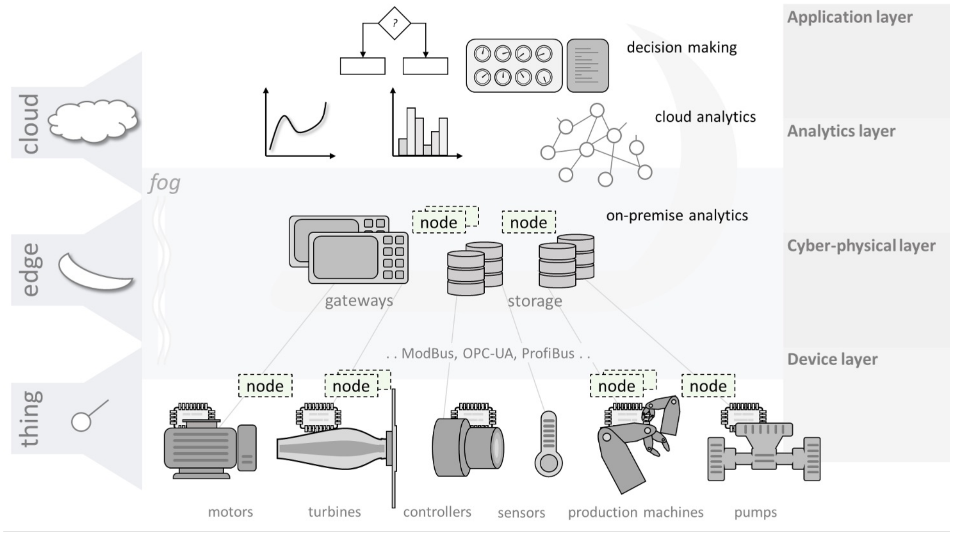
DESSERT

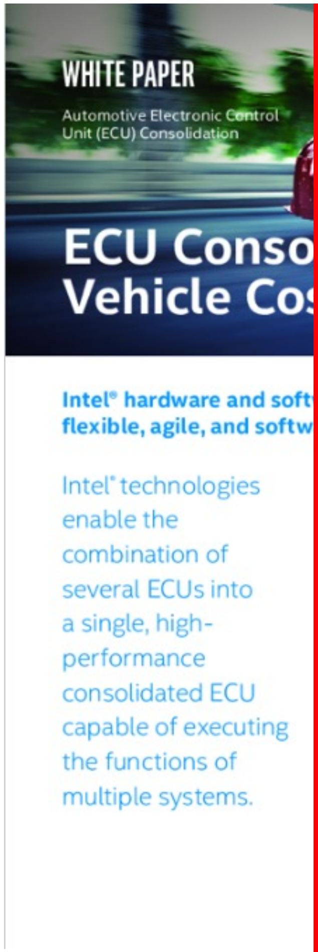
87th IFIP WG 10.4 Meeting – Ischia, June 29th 2025

Cyber-Physical Cloud

Recent spread of **cloud technologies** in industrial domains

- Use of **virtualization**, **VMs**, **containers** **hypervisors**, **orchestrators**, …
  … on cyber-physical systems
- With differentiated requirements
- Edge **devices** hosting different loads
  - real-time supervision and control
  - predictive maintenance
  - digital twins
- A multi-layered **Mixed-Criticality System**





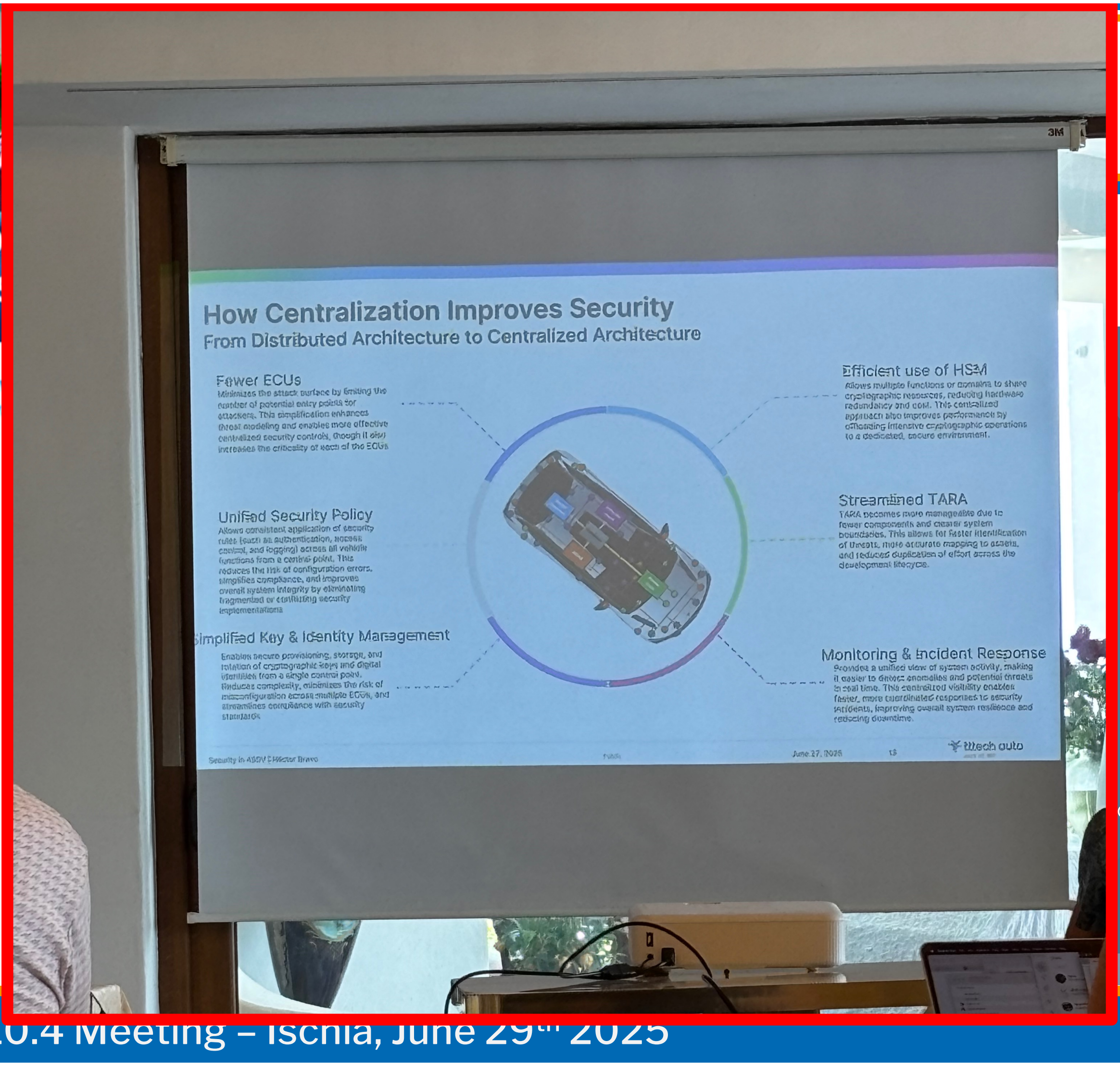
WHITE PAPER

Automotive Electronic Control Unit (ECU) Consolidation

ECU Conso
Vehicle Co

Intel® hardware and soft
flexible, agile, and softw

Intel® technologies enable the combination of several ECUs into a single, high-performance consolidated ECU capable of executing the functions of multiple systems.



How Centralization Improves Security

From Distributed Architecture to Centralized Architecture

Fewer ECUs
Minimizes the attack surface by limiting the number of potential entry points for attackers. This simplification enhances threat modeling and enables more effective centralized security controls, though it also increases the criticality of each of the ECUs

Unified Security Policy
Allows consistent application of security rules (such as authentication, access control, and logging) across all vehicle functions from a central point. This reduces the risk of configuration errors, simplifies compliance, and improves overall system integrity by eliminating fragmented or conflicting security implementations

Simplified Key & Identity Management
Enables secure provisioning, storage, and rotation of cryptographic keys and digital identities from a single control point. Reduces complexity, minimizes the risk of misconfiguration across multiple ECUs, and streamlines compliance with security standards

Efficient use of HSM
Allows multiple functions or domains to share cryptographic resources, reducing hardware redundancy and cost. This centralized approach also improves performance by offloading intensive cryptographic operations to a dedicated, secure environment.

Streamlined TARA
TARA becomes more manageable due to fewer components and clearer system boundaries. This allows for faster identification of threats, more accurate mapping to assets, and reduced duplication of effort across the development lifecycle.

Monitoring & Incident Response
Provides a unified view of system activity, making it easier to detect anomalies and potential threats in real time. This centralized visibility enables faster, more coordinated responses to security incidents, improving overall system resilience and reducing downtime.

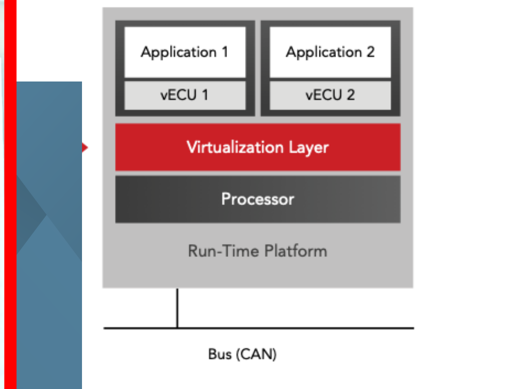
Security in ASDV [illegible] Hector Bravo

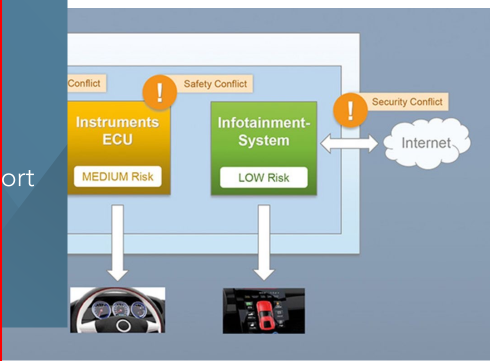
June 27, 2025

13

itech auto

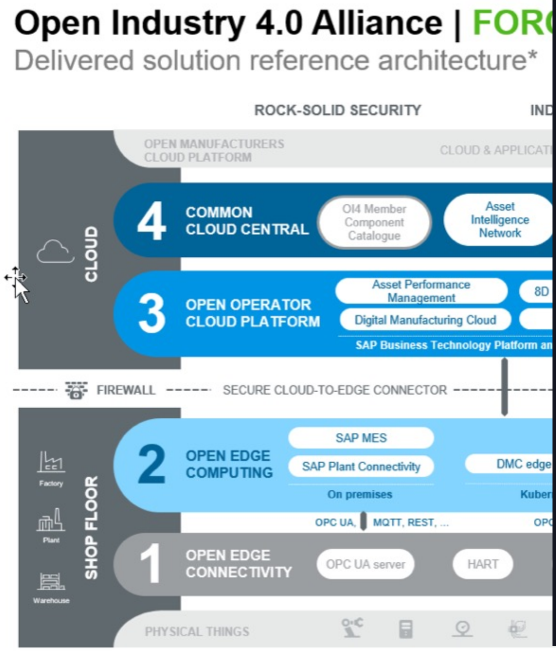
DESSERT

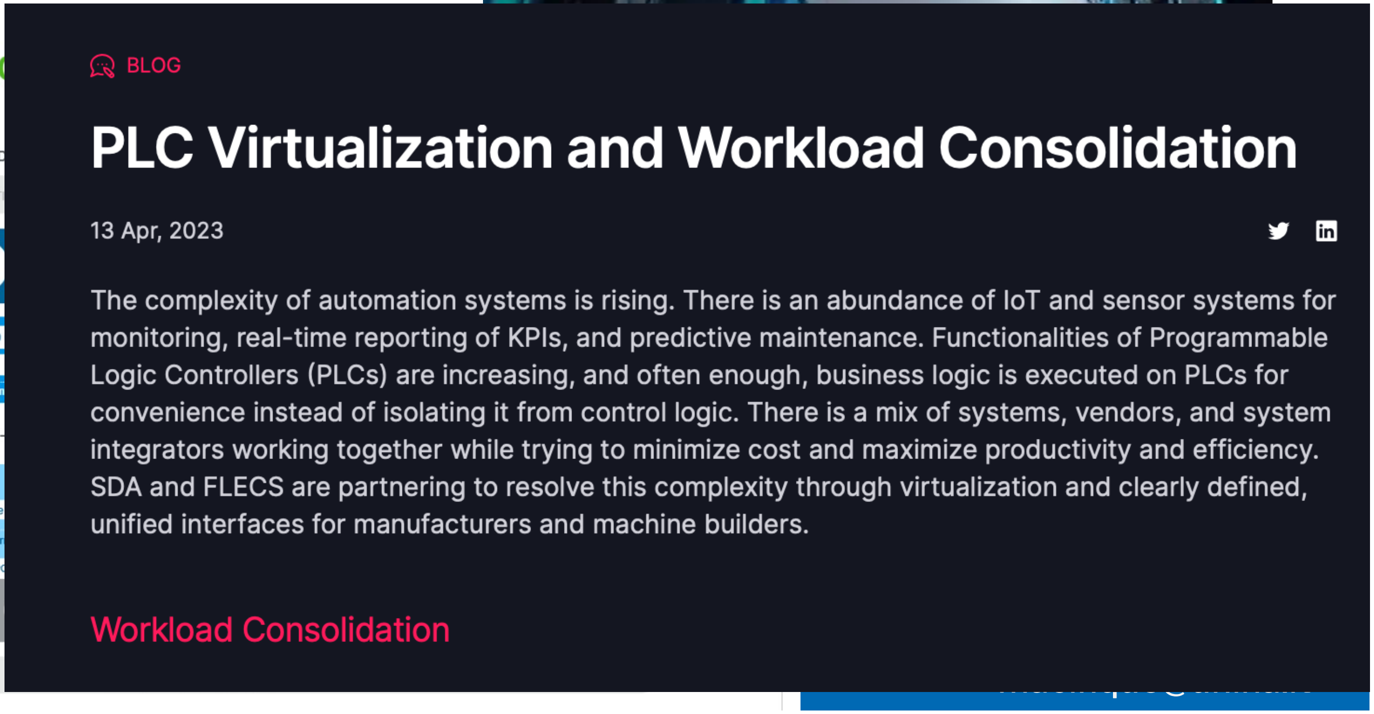




Similar trends in the factory

Programmable factory floor
Industry “*softwarization*”


Open Industry 4.0 Alliance | FORC
Delivered solution reference architecture*


BLOG

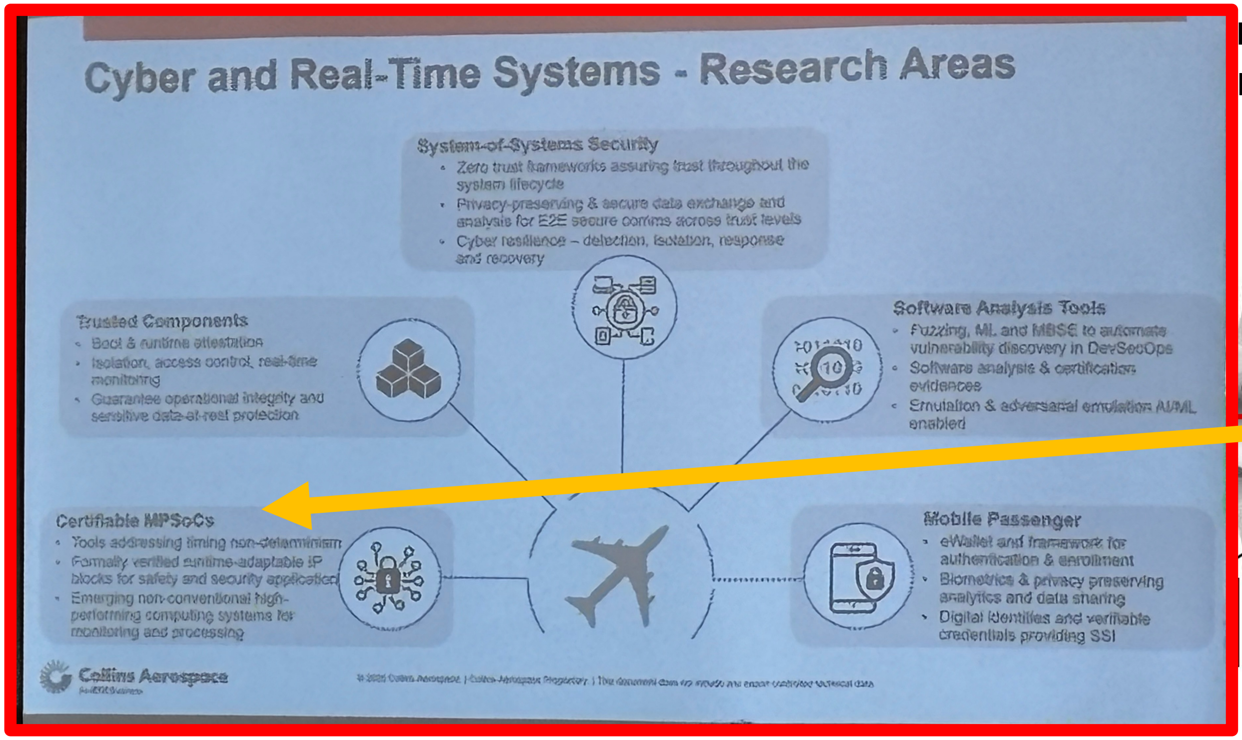
PLC Virtualization and Workload Consolidation

13 Apr, 2023

The complexity of automation systems is rising. There is an abundance of IoT and sensor systems for monitoring, real-time reporting of KPIs, and predictive maintenance. Functionalities of Programmable Logic Controllers (PLCs) are increasing, and often enough, business logic is executed on PLCs for convenience instead of isolating it from control logic. There is a mix of systems, vendors, and system integrators working together while trying to minimize cost and maximize productivity and efficiency. SDA and FLECS are partnering to resolve this complexity through virtualization and clearly defined, unified interfaces for manufacturers and machine builders.

Workload Consolidation

A consolidate trend in avionics



Cyber and Real-Time Systems - Research Areas

System-of-Systems Security
- Zero trust frameworks assuring trust throughout the system lifecycle
- Privacy-preserving & secure data exchange and analysis for E2E secure comms across trust levels
- Cyber resilience – detection, isolation, response and recovery

Trusted Components
- Boot & runtime attestation
- Isolation, access control, real-time monitoring
- Guarantee operational integrity and sensitive data-at-rest protection

Software Analysis Tools
- Fuzzing, ML and MBSE to automate vulnerability discovery in DevSecOps
- Software analysis & certification evidences
- Emulation & adversarial emulation AI/ML enabled

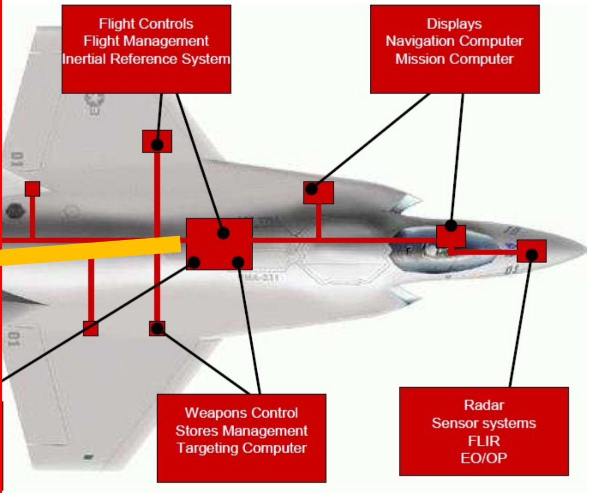
Certifiable MPSoCs
- Tools addressing timing non-determinism
- Formally verified runtime-adaptable IP blocks for safety and security application
- Emerging non-conventional high-performing computing systems for monitoring and processing

Mobile Passenger
- eWallet and framework for authentication & enrollment
- Biometrics & privacy preserving analytics and data sharing
- Digital Identities and verifiable credentials providing SSI

Collins Aerospace
An RTX Business

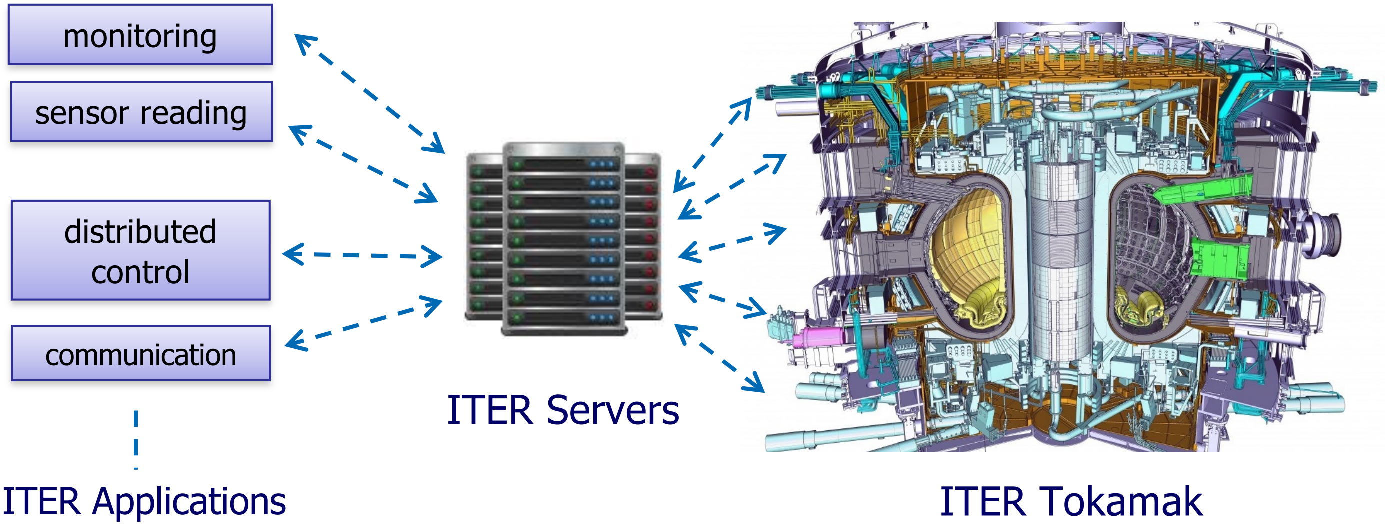
© 2025 Collins Aerospace | Collins Aerospace Proprietary | This document does not contain any export controlled technical data

rated Modular
rchitecture (IMA)

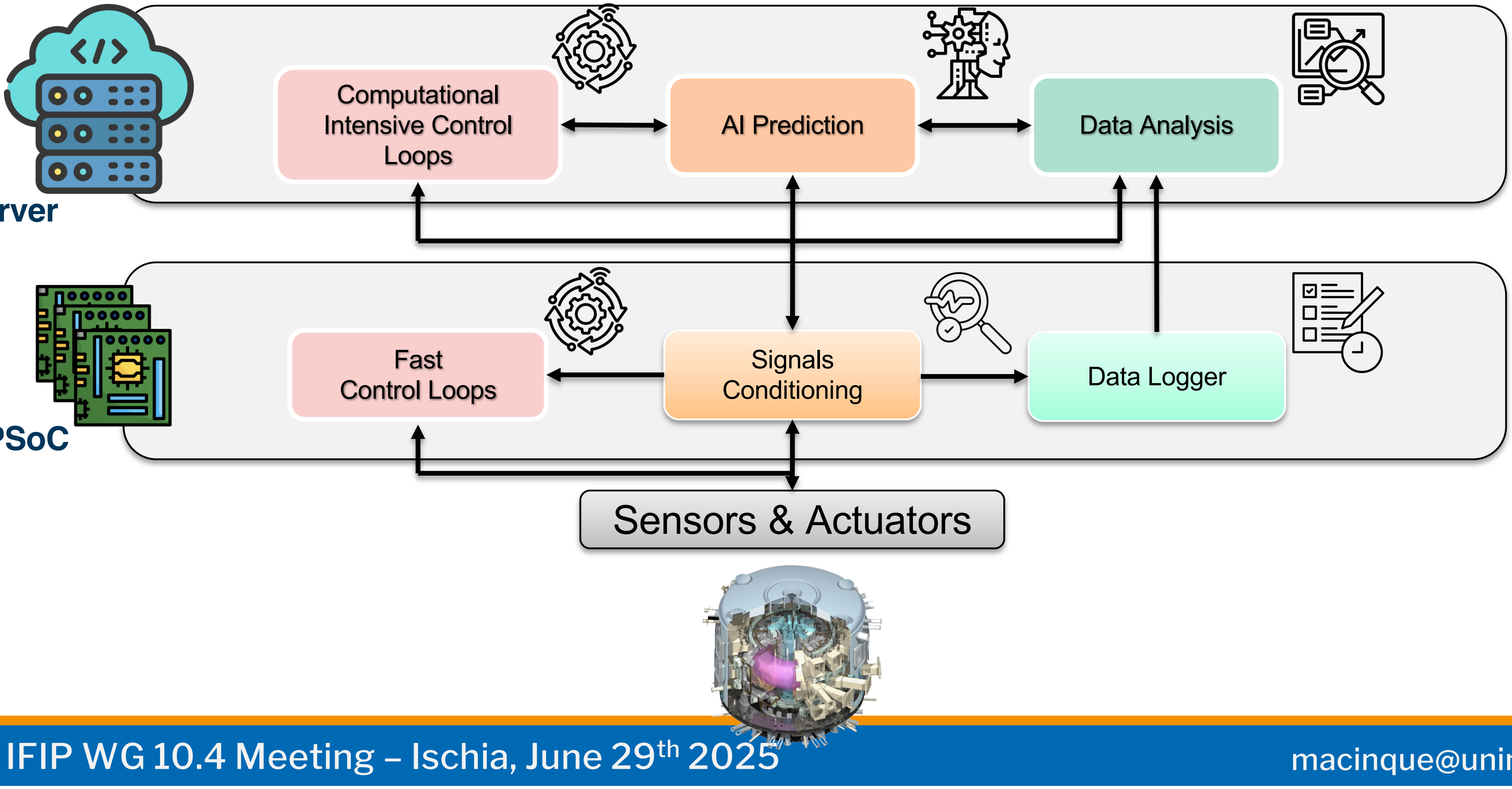


A peculiar case: the ITER fusion reactor

ITER real-time control and monitoring infrastructure



ITER CODAC Software Architecture



Server

Computational Intensive Control Loops

AI Prediction

Data Analysis

MPSoC

Fast Control Loops

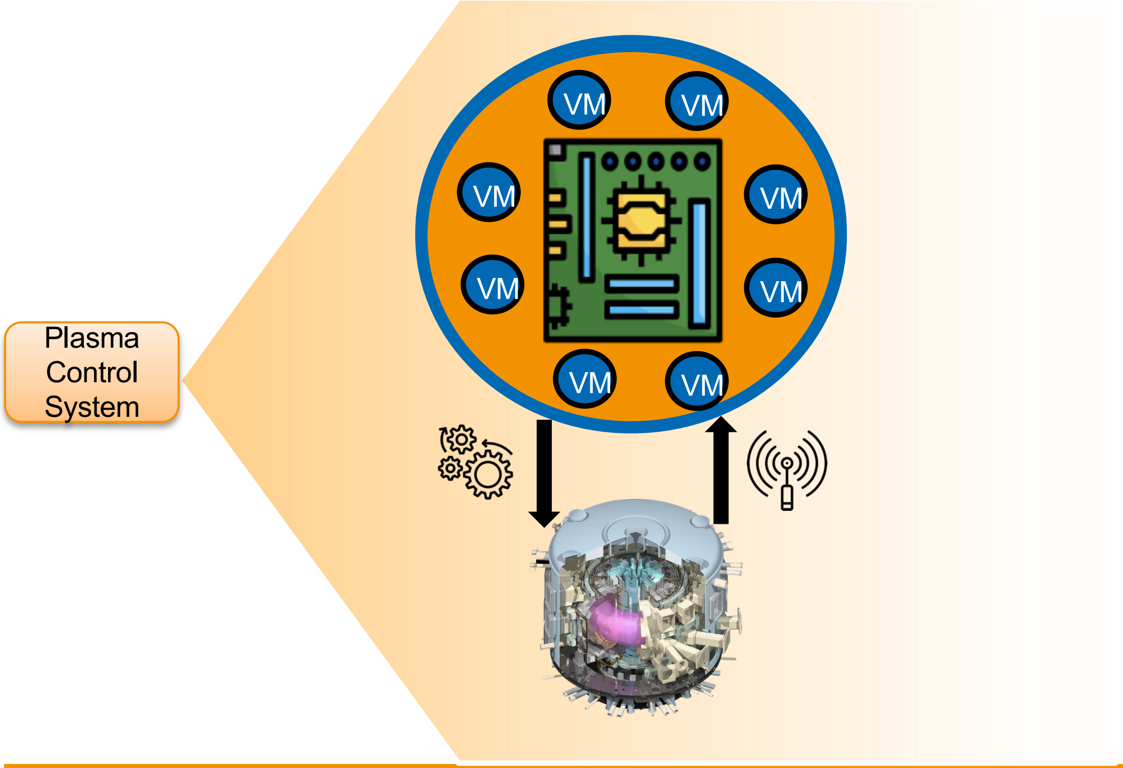
Signals Conditioning

Data Logger

Sensors & Actuators

Towards Integrated Systems

- Towards an **integrated development** model rather than a federated one



Why To Integrate?

Resource **Utilization**

System **Scalability**

Reliable **Communication**

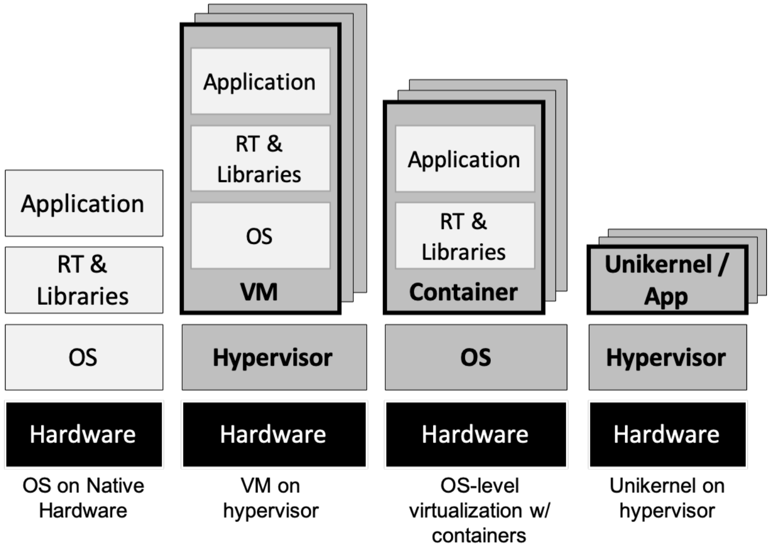
Main Challenges

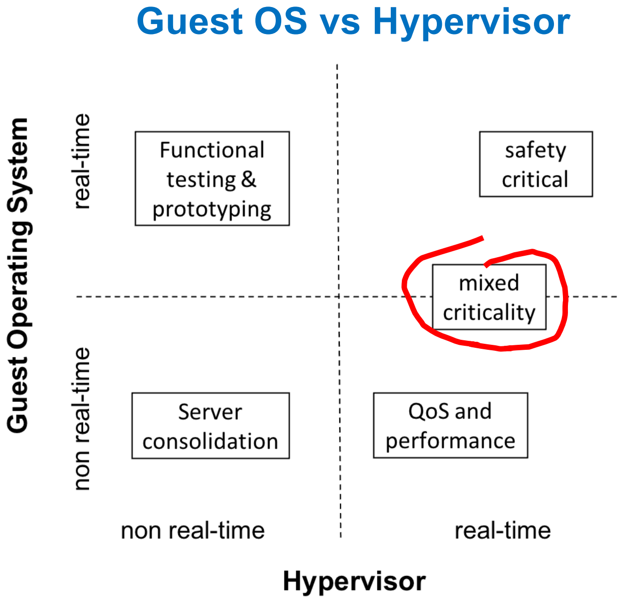
Applications **Isolation & Consolidation**

Hardware/Software **Heterogeneity**

How to isolate real-time workloads?

A plethora of approaches available





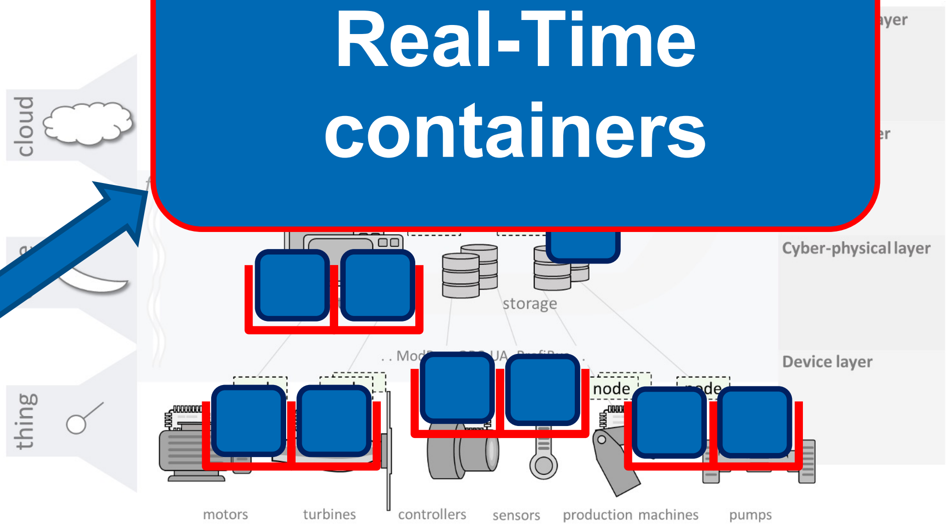
M. Cinque et al., “Virtualizing Mixed-Criticality Systems: A Survey of Industrial Trends and Issues” Future Generation Computer Systems, Volume 129, 2022

Cyber-Physical Cloud

Our vision

Containers everywhere!

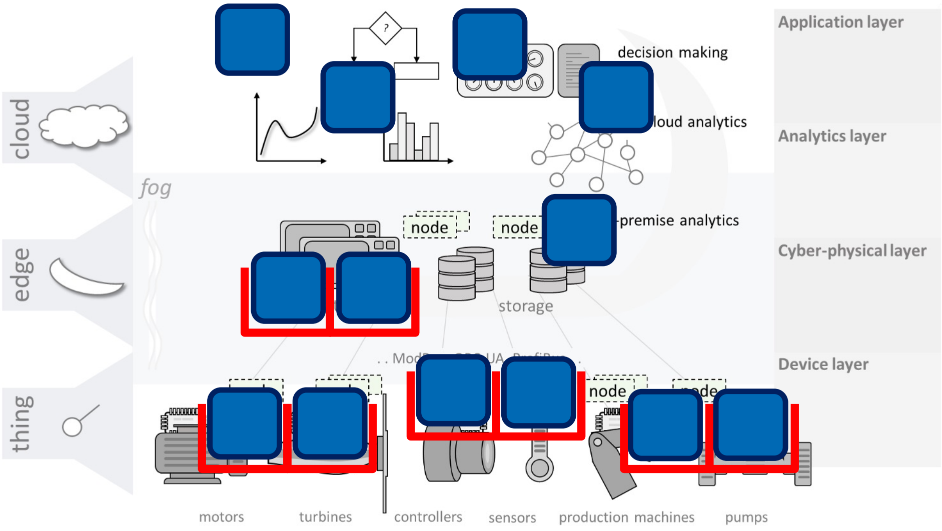
Real-Time containers



Assure isolation at edge/things layer by <u>running containers in isolation</u>

Real-Time containers

- Key **benefits**
  - **Same abstraction** from the cloud to the edge and things
  - Integration with **DevOps**
  - Integration with **Orchestrators**
  - **Lightweight** solution, compared to VMs
  - Fit the **Real-Time FaaS**[1] model



[1] M. Cinque. Real-Time FaaS: serverless computing for Industry 4.0. Service Oriented Computing and Applications 17(2), 2023

Challenges of real-time containers

1. How to achieve isolation with containers?
   - Need to go beyond OS-level virtualization
2. Ho to deal with heterogenous hardware?
3. How to orchestrate considering mixed-criticality?

Many proposals for real-time containers!

Recent studies focused on containers for **real-time** environments, with:

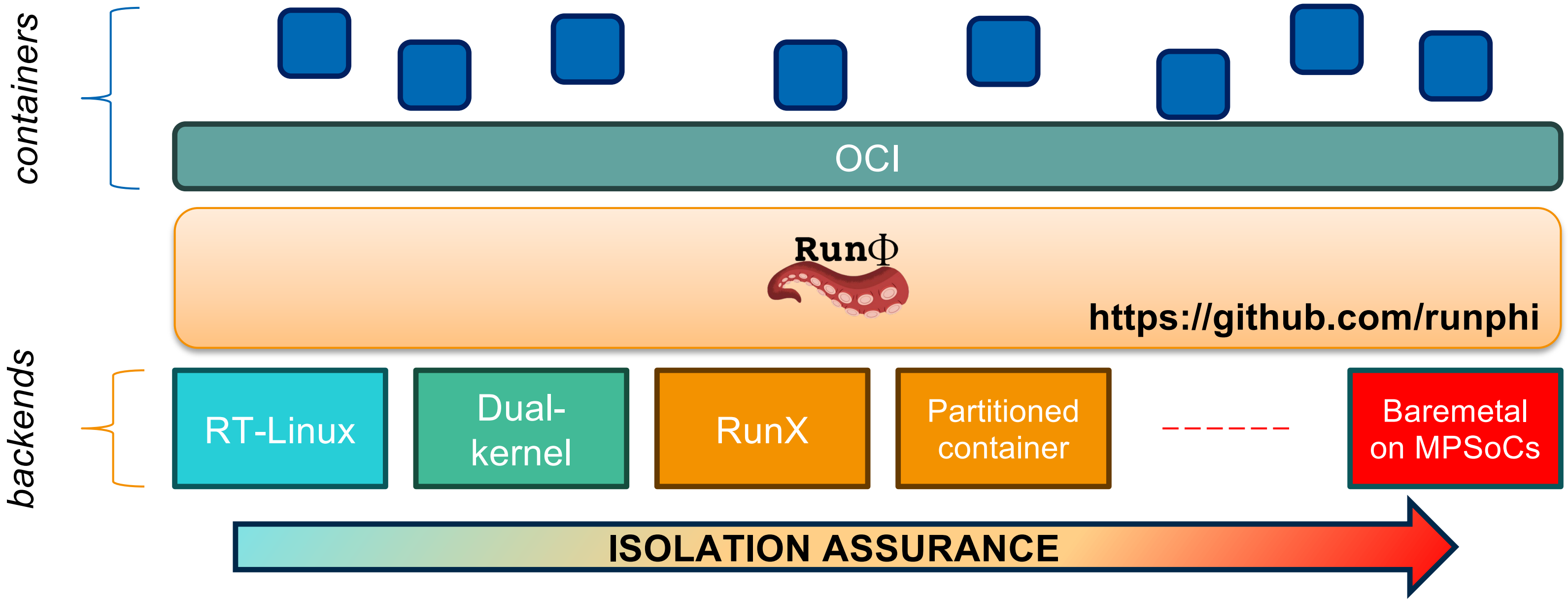
- **RT-Linux:** running containers on a **PREEMPT_RT** patched kernel with the **SCHED_DEADLINE** policy for group scheduling (rt-cgroups), affinity, isolcpu, …
- **Dual-kernels**: mapping containers on Xenomai or RTAI[1]
- **Sandboxes:** run as lightweight VMs (RunX, firecracker, gvisor, partitioned containers[2], …)
- **Baremetal**: run on accelerators (e.g., Zephyr app on an RPU)

Challenge

Can we **transparently map** a container on all this different "backends", based on criticality requirements?

Hardware

Mapping containers on backends



D. Ottaviano, M. Barletta, F. Boccola, Zero-Interference Containers: A Framework to Orchestrate Mixed-Criticality Applications, DSN 2025

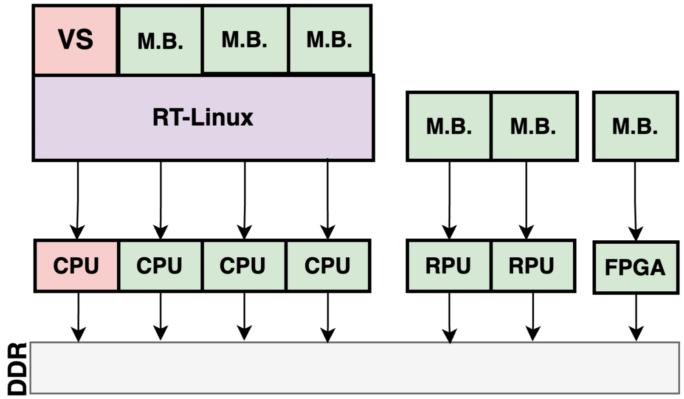
Benefits of RunPhi

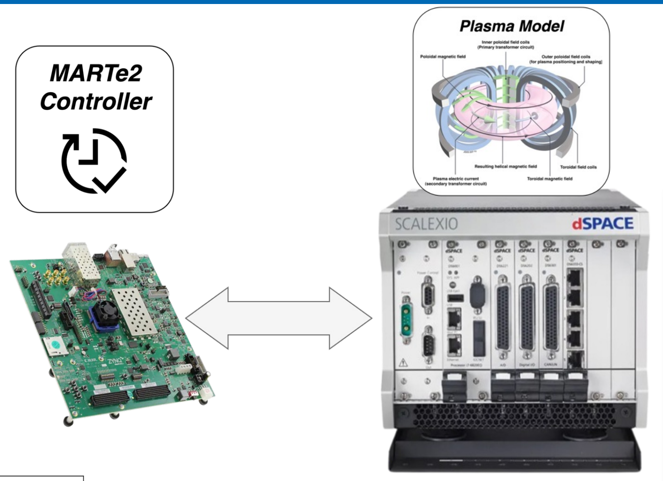
- Transparency
  - `docker run` works to run the same RT-POSIX container on Linux or on Zephyr on a Cortex-R co-processor
- Mixed-Criticality native
- Redundancy with diversity for free
- Seamless migration on different backends
- Diversified rolling upgrade

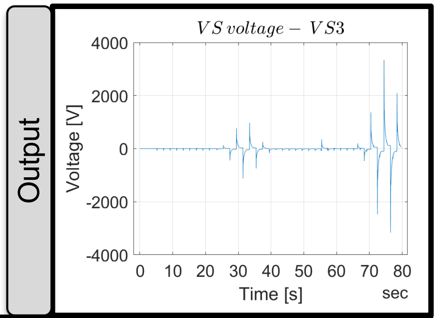
Challenges of real-time containers

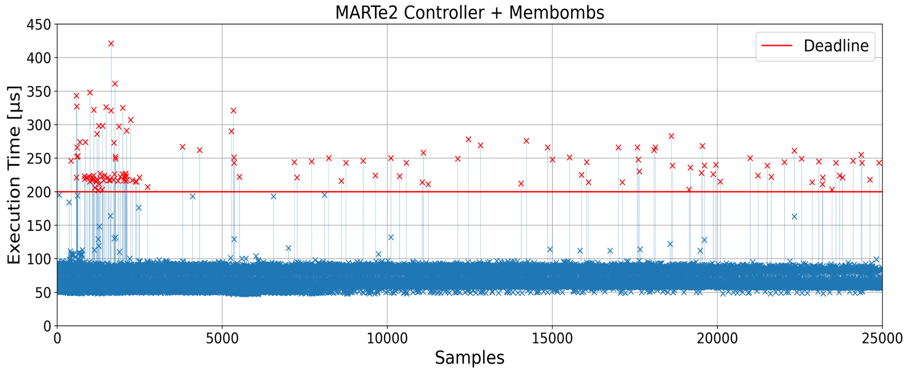
1. How to achieve isolation with containers?
   - Need to go beyond OS-level virtualization
2. **How to deal with heterogenous hardware?**
   - **How to extend isolation to MPSoCs?**
3. How to orchestrate considering mixed-criticality?

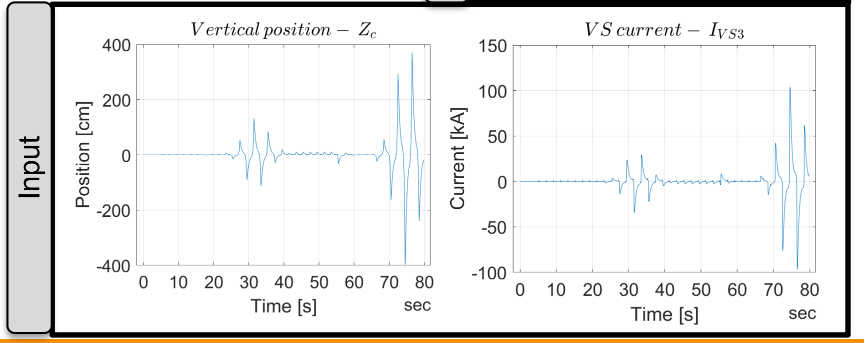
Still problems on MPSoCs!



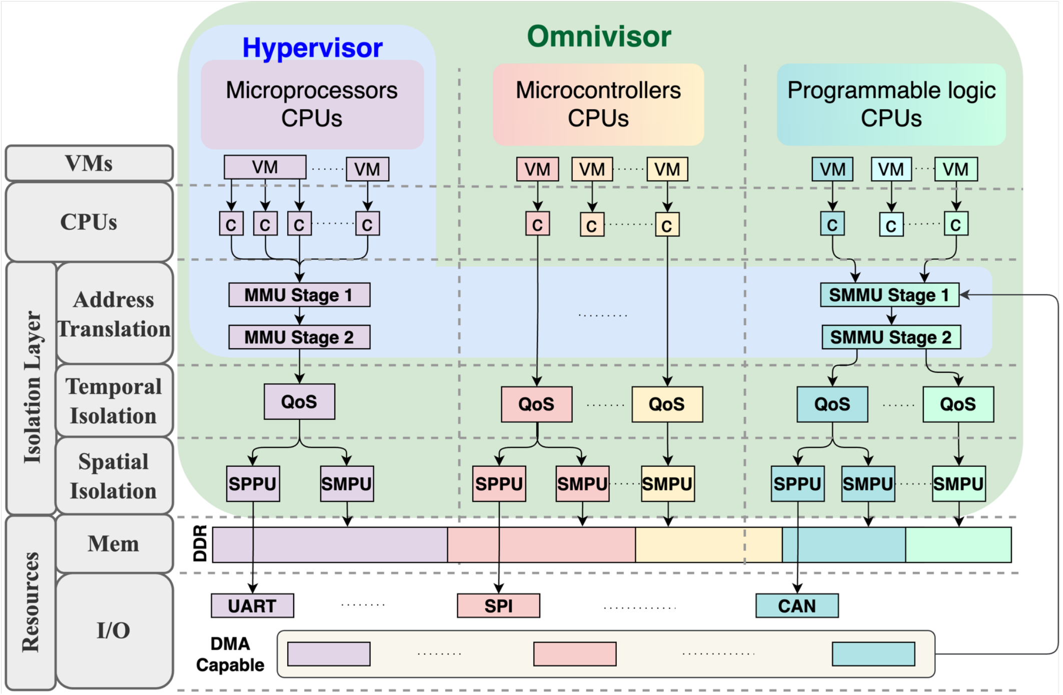








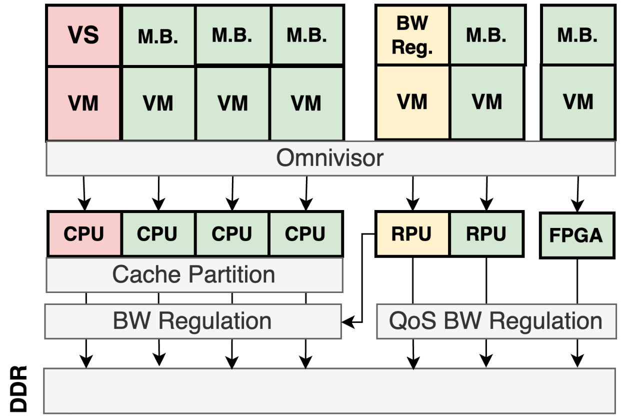
From Hypervisor to Omnivisor



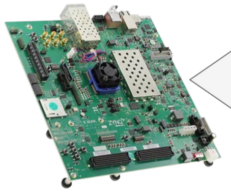
- ✓Spatial Isolation
- ✓Temporal Isolation

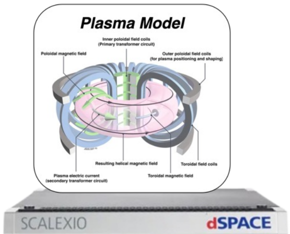
D. Ottaviano, F. Ciarolo, R. Mancuso, M. Cinque. The Omnivisor: A real-time static partitioning hypervisor extension for heterogeneous core virtualization over MPSoCs. ECRTS 2024

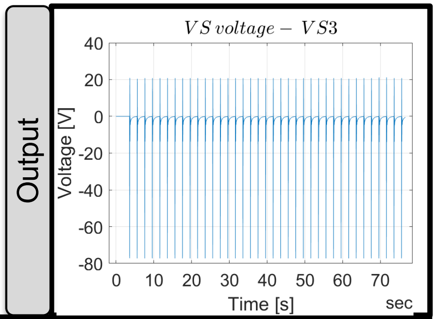
Same workload with the Omnivisor

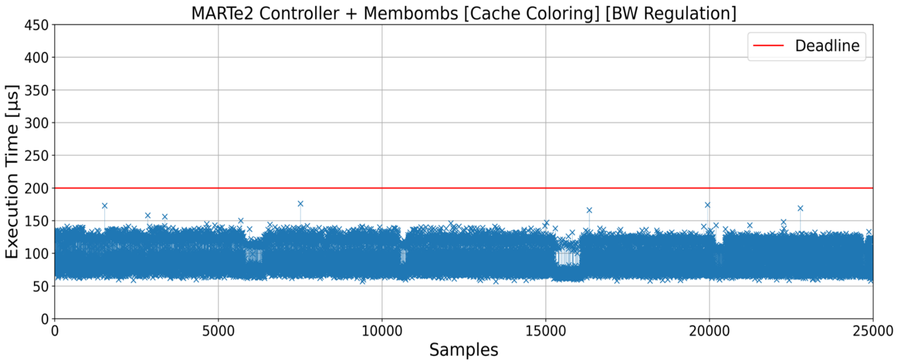


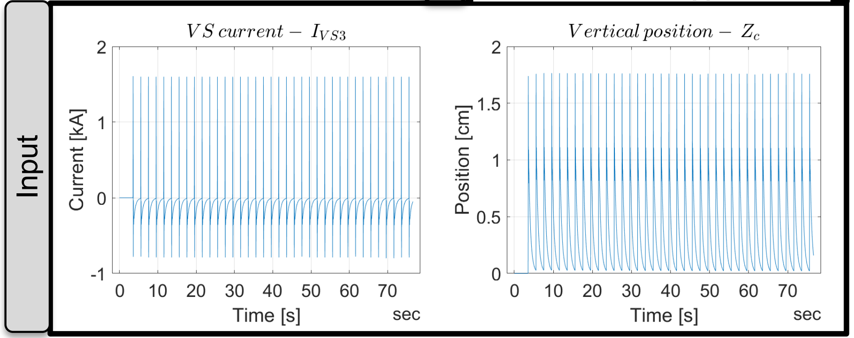
MARTe2 Controller











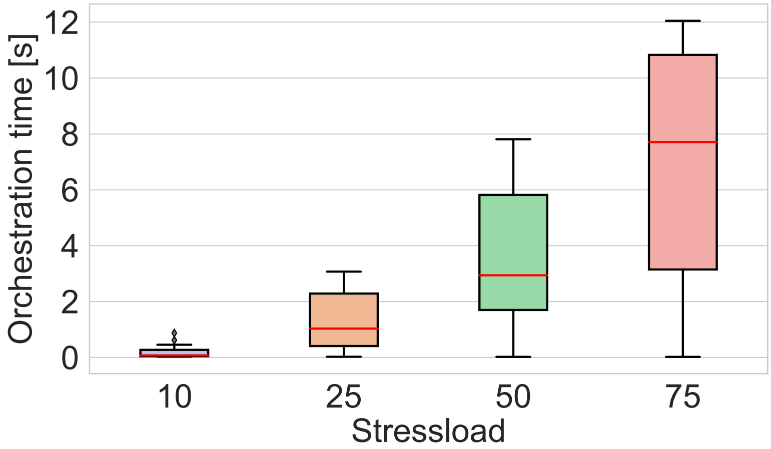
Challenges of real-time containers

1. How to achieve isolation with containers?
   - Need to go beyond OS-level virtualization
2. How to deal with heterogenous hardware?
   - How to extend isolation to MPSoCs?
3. **How to orchestrate considering mixed-criticality?**
   - **How to map containers on nodes**
     - **Considering their criticality**
     - **With bounded time**

Orchestration issues

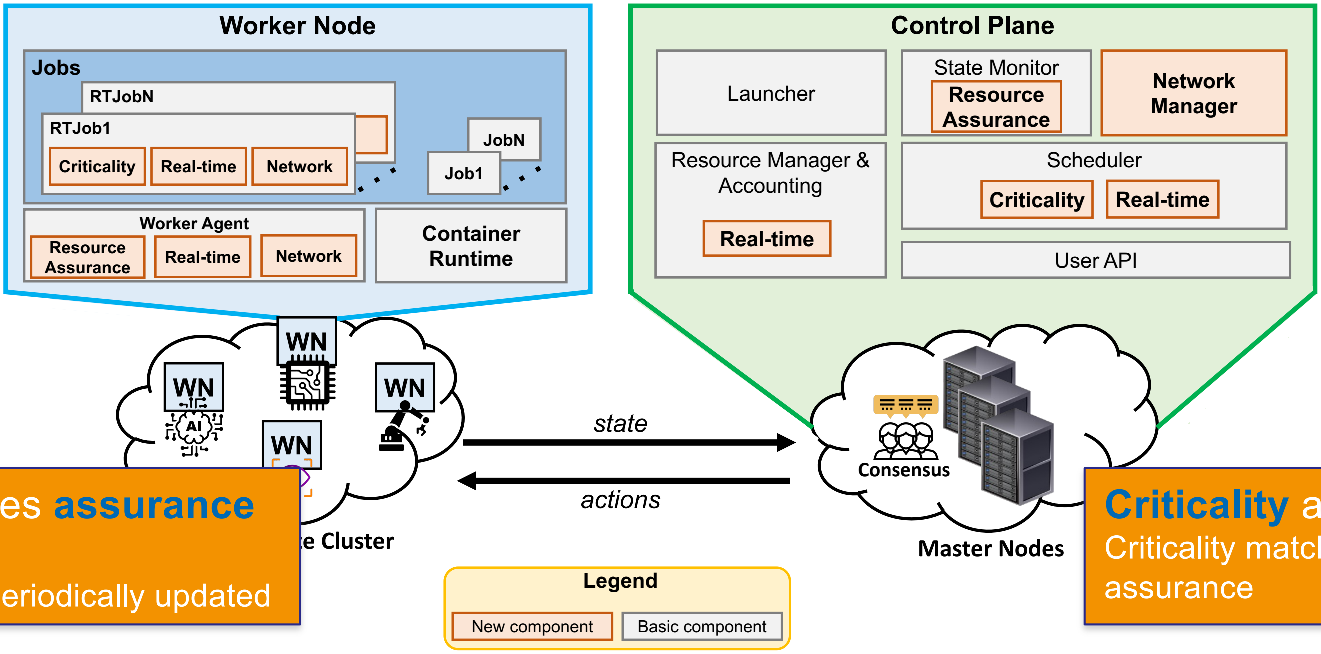
- Orchestrators map containers on nodes only considering CPU/memory/storage requirements
- They are not able to prioritize service requests[1]

Time for K8S to start a high-priority container while applying an increasing number of interfering requests



[1] M. Barletta, M. Cinque, L. De Simone, S. Toscano. PREEMPT-K8S: Pod Prioritization for Mixed-Criticality Edge-Cloud Services, DSD 2025

k4.0s: an orchestrator for I4.0



Worker nodes **assurance** monitoring
Assurance is periodically updated

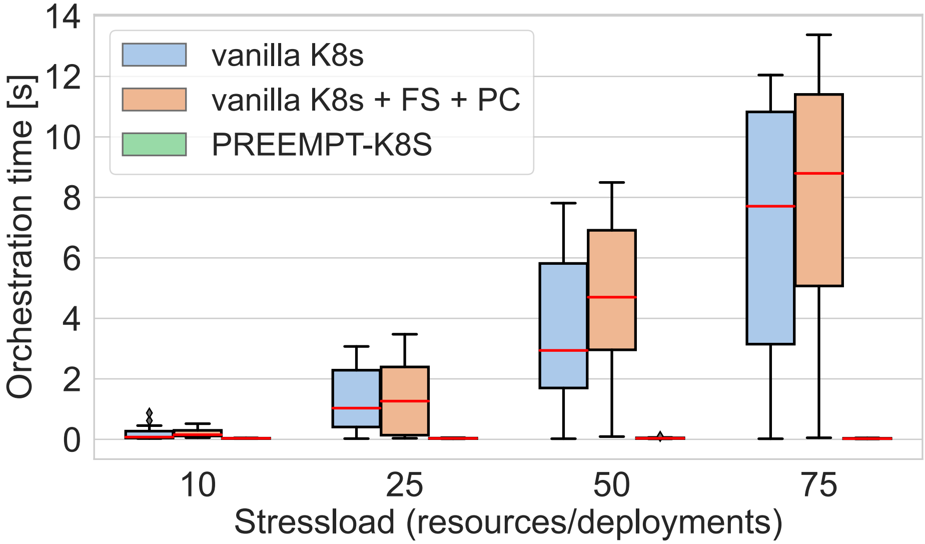
Criticality aware
Criticality matches the node assurance

M. Barletta, M. Cinque, R. Della Corte, L. De Simone. Criticality-Aware Monitoring and Orchestration for Containerized Industry 4.0 Environments. ACM Transactions on Embedded Computing Systems.. 2023

PREEMPT-K8S

- A preemptable Kubernetes controller able to fully prioritize critical requests[1]

Time for K8s, K8s + FlowSchema (FS) + Priority Class (PC), and PREEMPT-K8S to start a high-priority container while applying an increasing number of interfering requests



1. M. Barletta, M. Cinque, L. De Simone, S. Toscano. PREEMPT-K8S: Pod Prioritization for Mixed-Criticality Edge-Cloud Services, DSD 2025

CaPriC

PhD School on
Cyber-**P**hysical **C**loud

Anacapri, Capri Island, Italy
October 13-17, 2025
https://capric-school.github.io/

Thank you ! Questions ?