accelerat

Simplifying complexity

The Role of Virtualization at the Edge for Mixed-Criticality Applications

Who I am

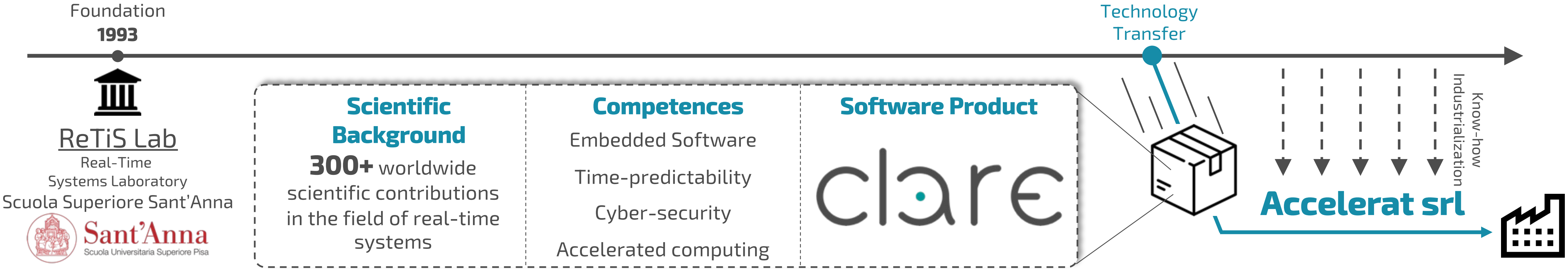
Eng. Giorgiomaria Cicero

- **CEO & Co-Founder of Accelerat S.r.l.**
- **Senior Research Fellow** at ReTiS Lab, Scuola Superiore Sant'Anna (Pisa, Italy)

Background: Embedded Software Engineer for Cyber-physical Systems

Research interests: Virtualization, system-level cyber-security, and time-predictability for embedded systems applied to safety-critical application domains (Automotive, Aerospace, Railway, Factory Automation, etc.)

An innovative Start-up and Spin-off company of Scuola Superiore Sant'Anna



Foundation
1993

ReTiS Lab
Real-Time
Systems Laboratory
Scuola Superiore Sant'Anna

Scientific Background
300+ worldwide scientific contributions in the field of real-time systems

Competences
Embedded Software
Time-predictability
Cyber-security
Accelerated computing

Software Product
clare

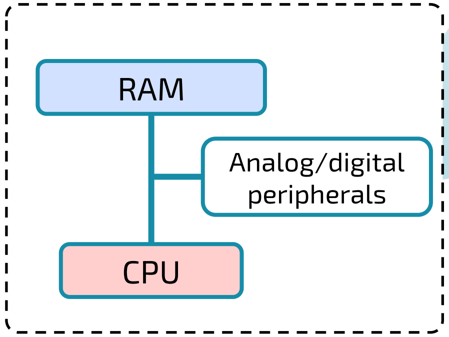
Technology Transfer

Know-how Industrialization

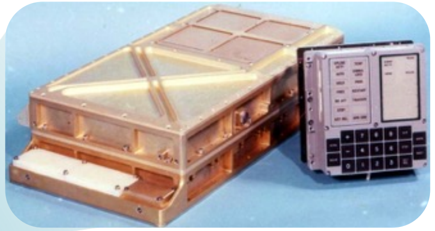
Accelerat srl

Evolution of embedded platforms

Single core with simple memory model

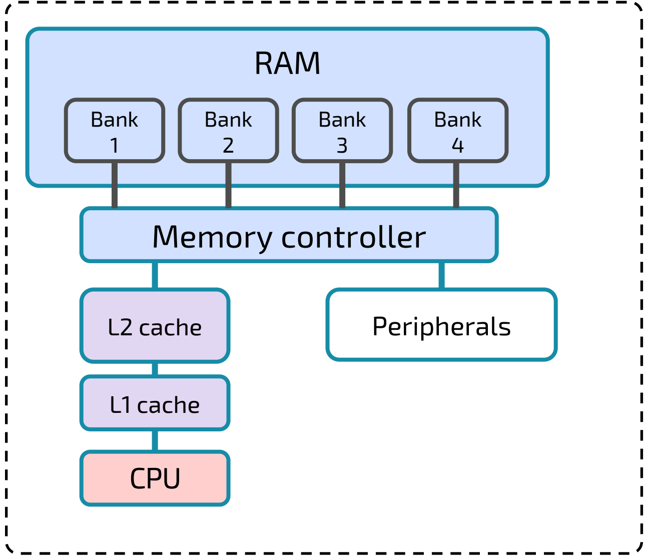


Apollo guidance computer (1960)

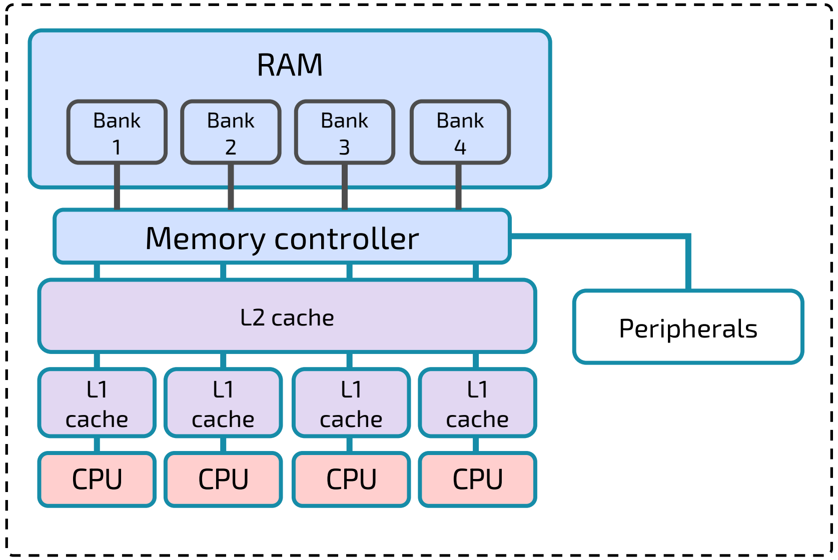


2 MHz of clock
36K-words ROM
2048 words RAM

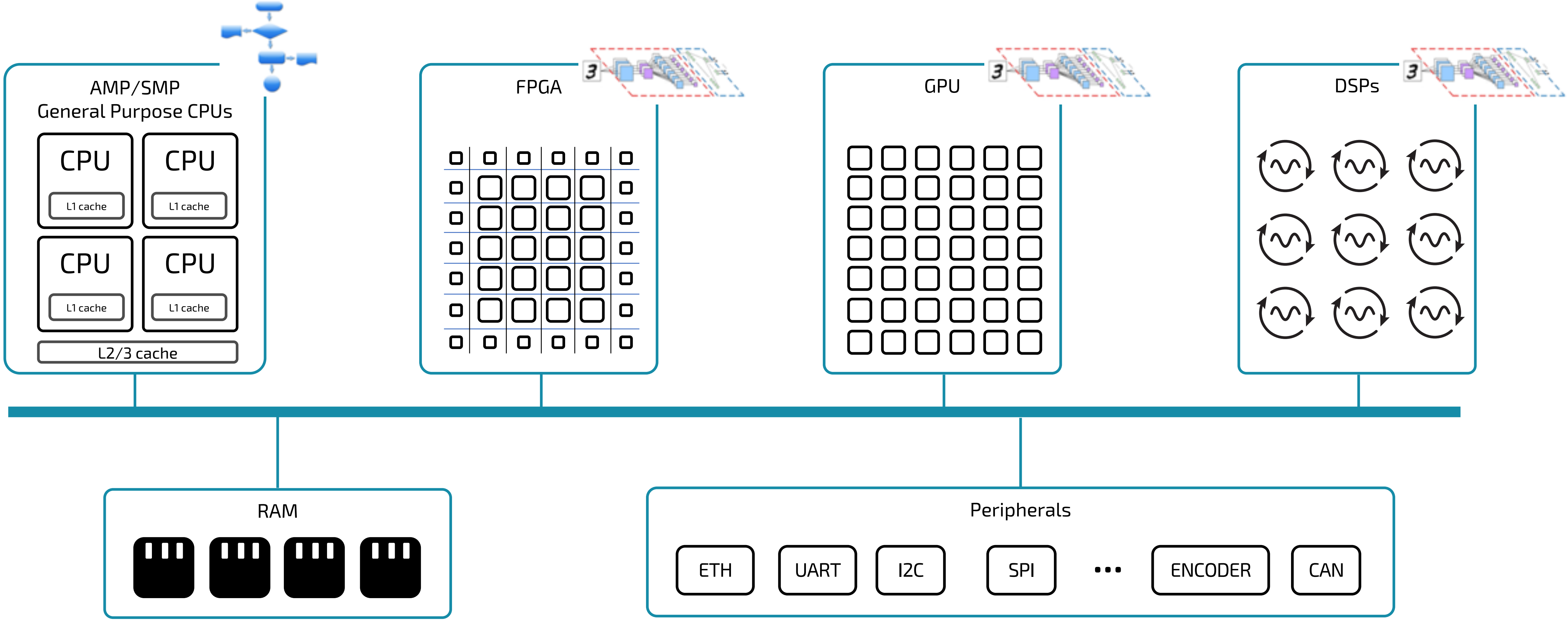
Single core with complex memory model



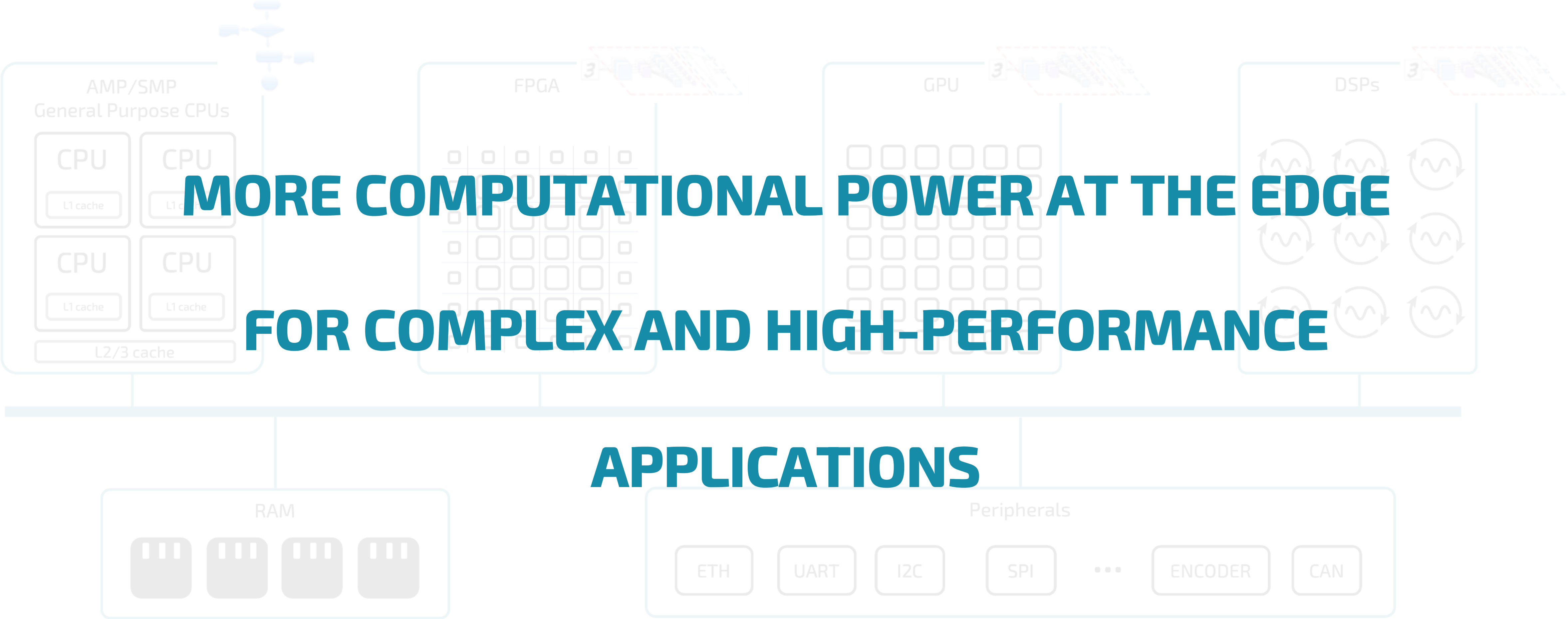
Multi core with complex memory model



Modern heterogeneous embedded platform



Modern heterogeneous embedded platform



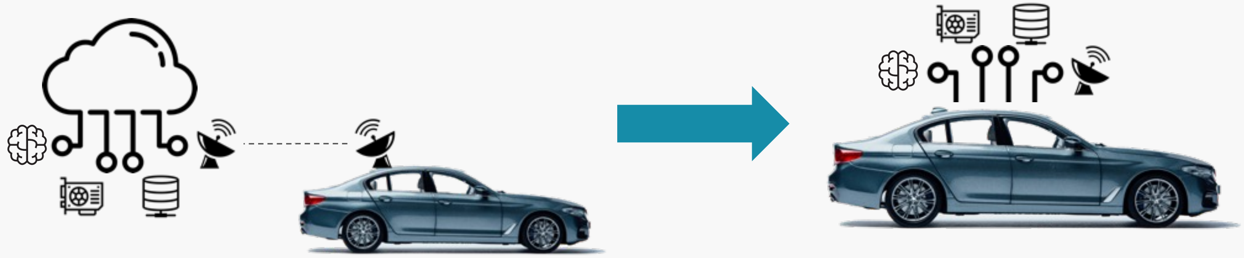
MORE COMPUTATIONAL POWER AT THE EDGE

FOR COMPLEX AND HIGH-PERFORMANCE

APPLICATIONS

Vision & Challenges of Edge Computing

Favoring the Edge-Computing



+ time-predictability

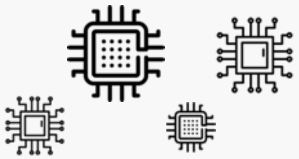
+ privacy & security

- cost of infrastructure

BUT

SWaP-C

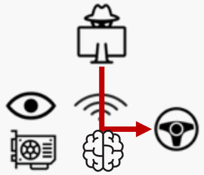
(Size, Weight, Power, and Costs)



Today's cars have 200+ Processors

+ functionalities
+ electronic boards & wires

Mixed-criticality



Presence of tasks with mixed independent levels of criticality

Low-critical tasks may harm high-critical tasks

Certification issue

Not certified functionalities | Certified functionalities

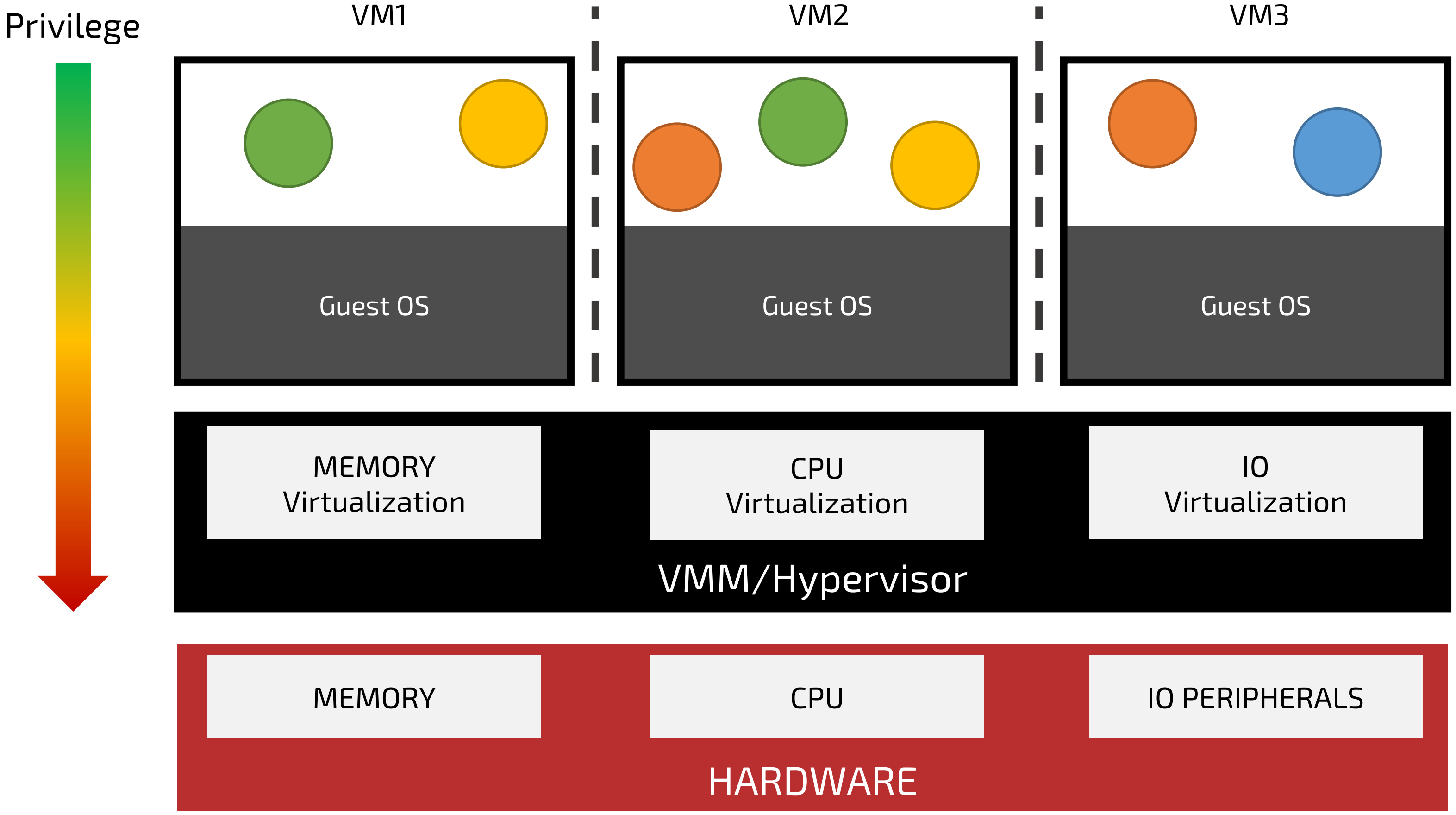
How to certify portions of the application with different SIL

- Flexibility

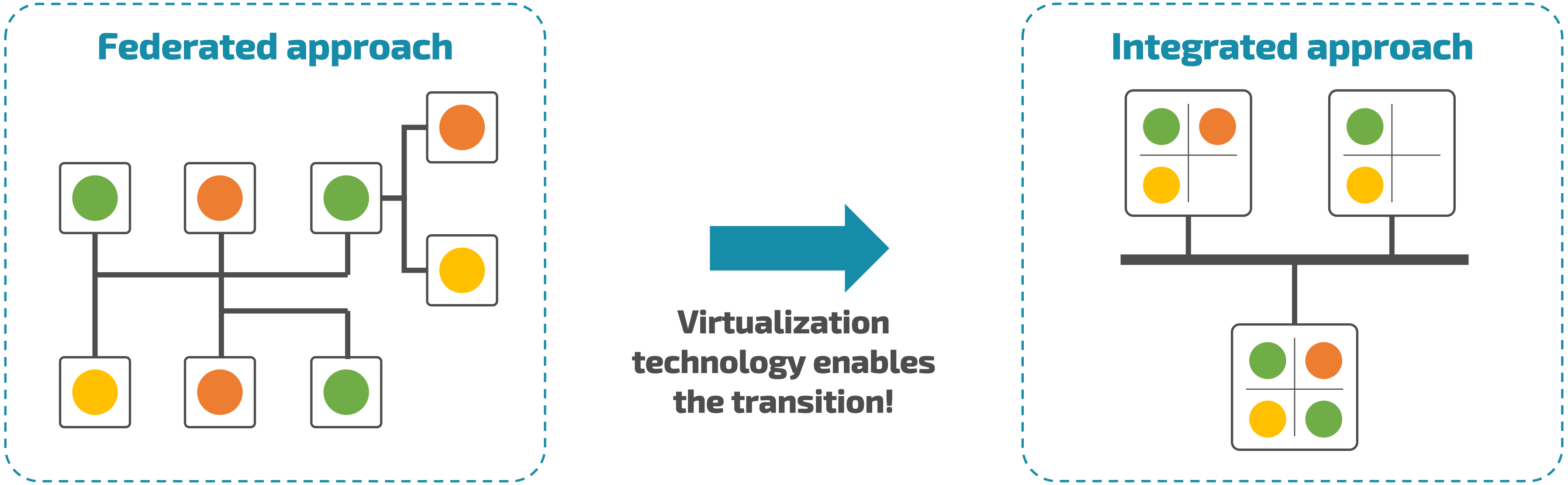
Virtualization

Hypervisor technology

- CPU virtualization
- Interrupts virtualization
- Memory virtualization
- Devices virtualization/emulation
- Spatial and temporal isolation
- …



SWaP-C Reduction

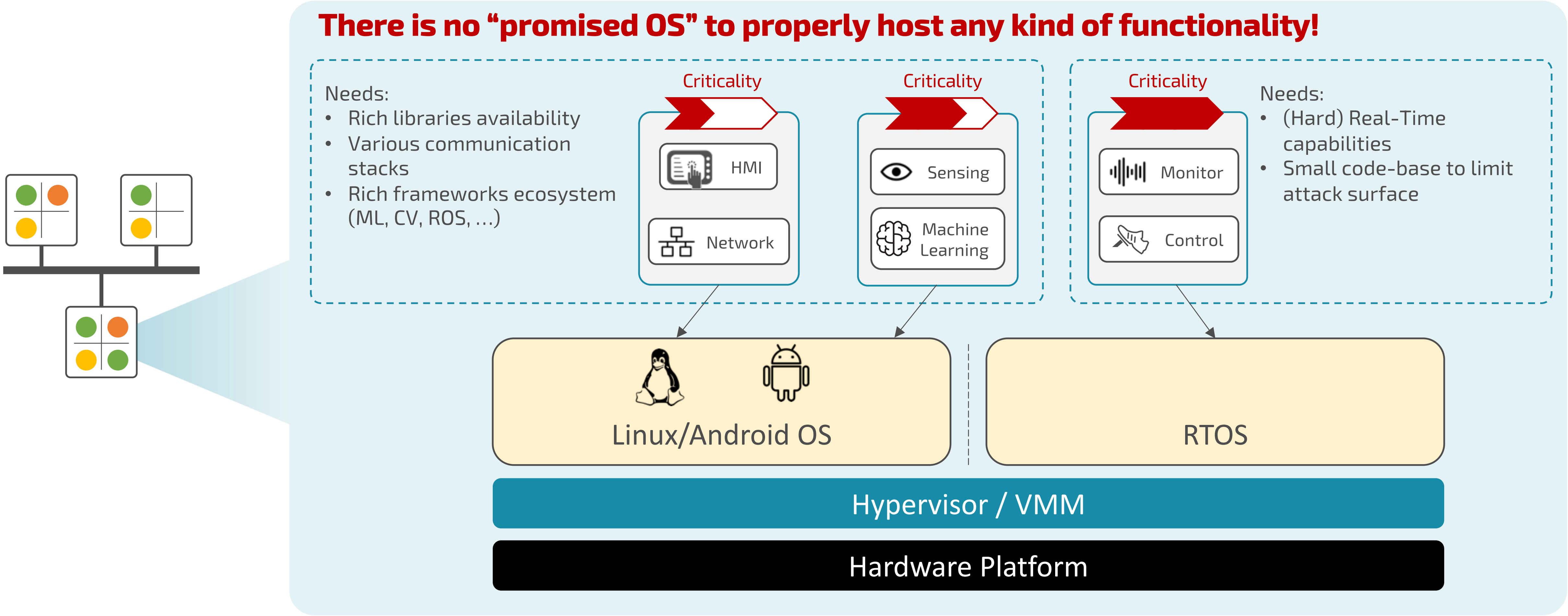


- ☹ Indefinitely increasing of #ECUs and #wires
- ☹ High communication latency
- ☹ High costs of production and maintenance
- ☹ High power consumption

- ☺ Reduced #ECUs and #wires
- ☺ Low communication latency
- ☺ High portability
- ☺ Reduced costs of production and maintenance
- ☺ Reduced power consumption

Mixed-criticality applications

Modern cyber-physical systems shall provide functionalities with different levels of criticality.



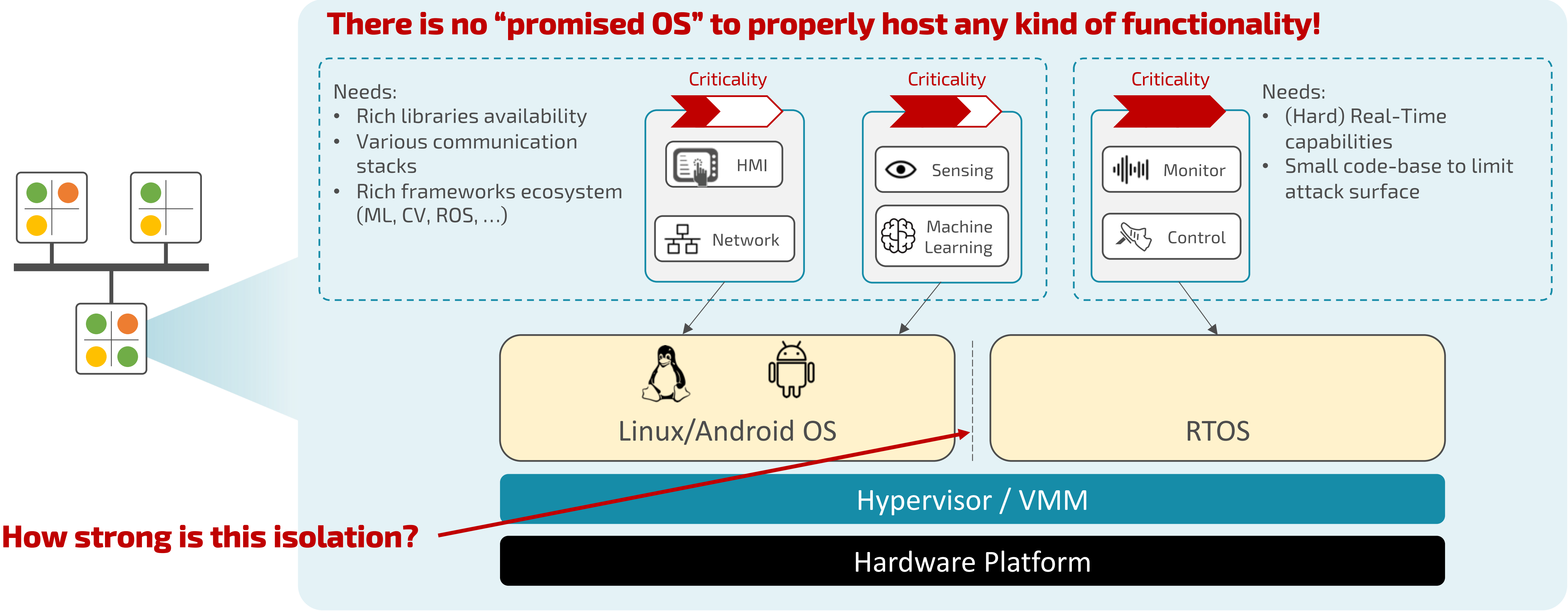
There is no "promised OS" to properly host any kind of functionality!

Needs:
- Rich libraries availability
- Various communication stacks
- Rich frameworks ecosystem (ML, CV, ROS, …)

Needs:
- (Hard) Real-Time capabilities
- Small code-base to limit attack surface

Mixed-criticality applications

Modern cyber-physical systems shall provide functionalities with different levels of criticality.



There is no “promised OS” to properly host any kind of functionality!

Needs:

- Rich libraries availability
- Various communication stacks
- Rich frameworks ecosystem (ML, CV, ROS, …)

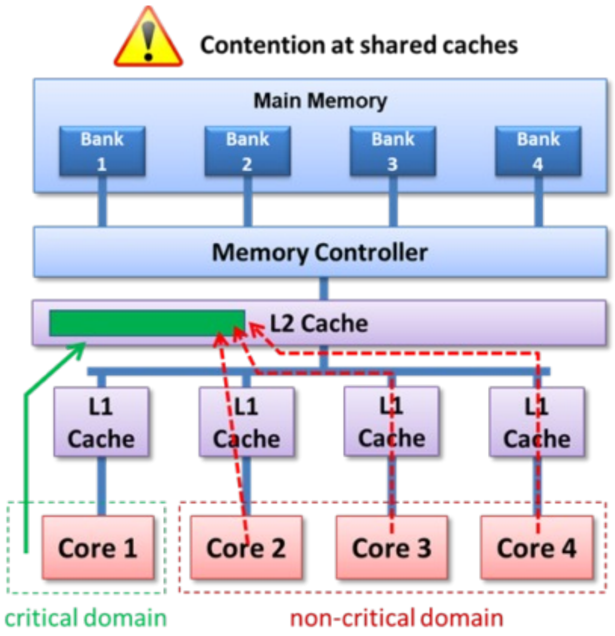
Needs:

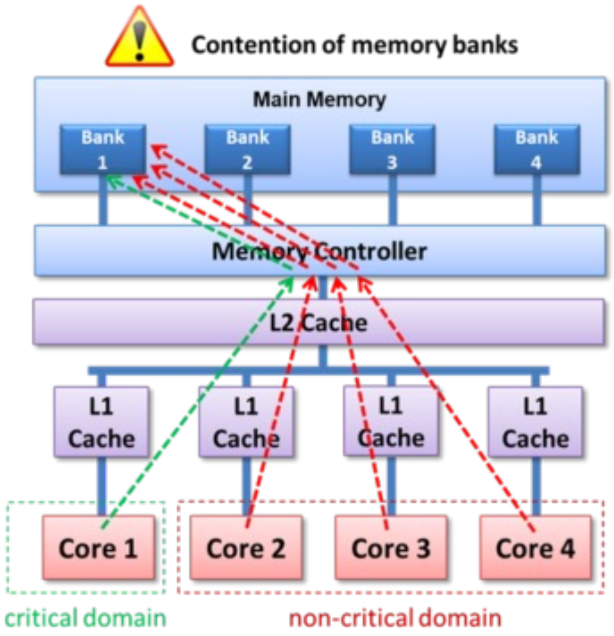
- (Hard) Real-Time capabilities
- Small code-base to limit attack surface

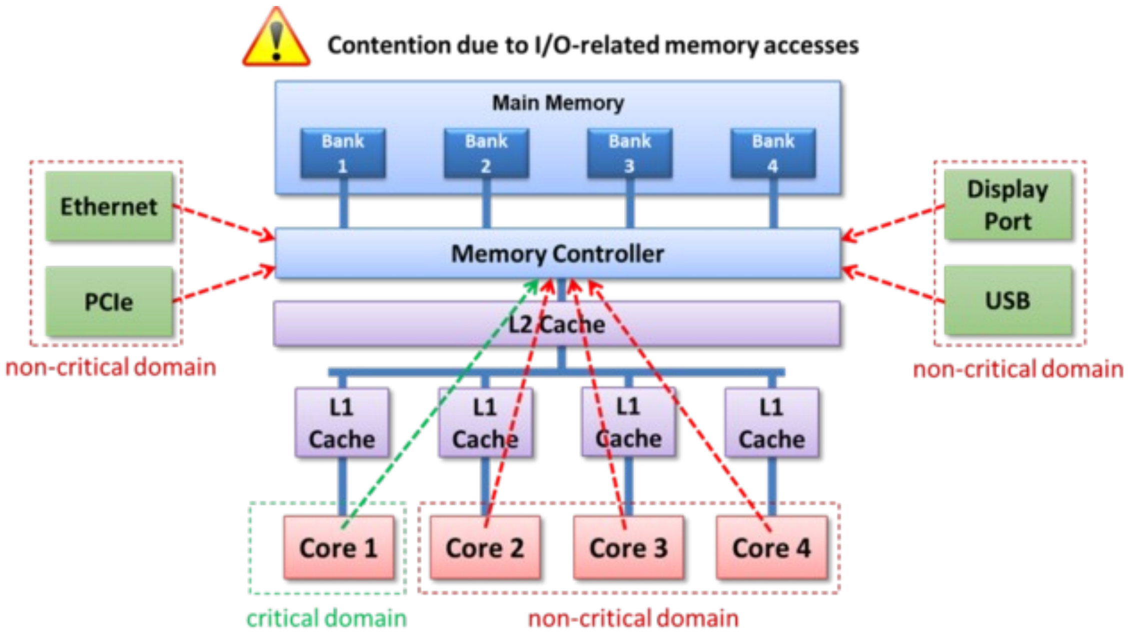
How strong is this isolation?

Points of interference of modern embedded platform

Running upon separated cores is not enough!


Contention at shared caches


Contention of memory banks

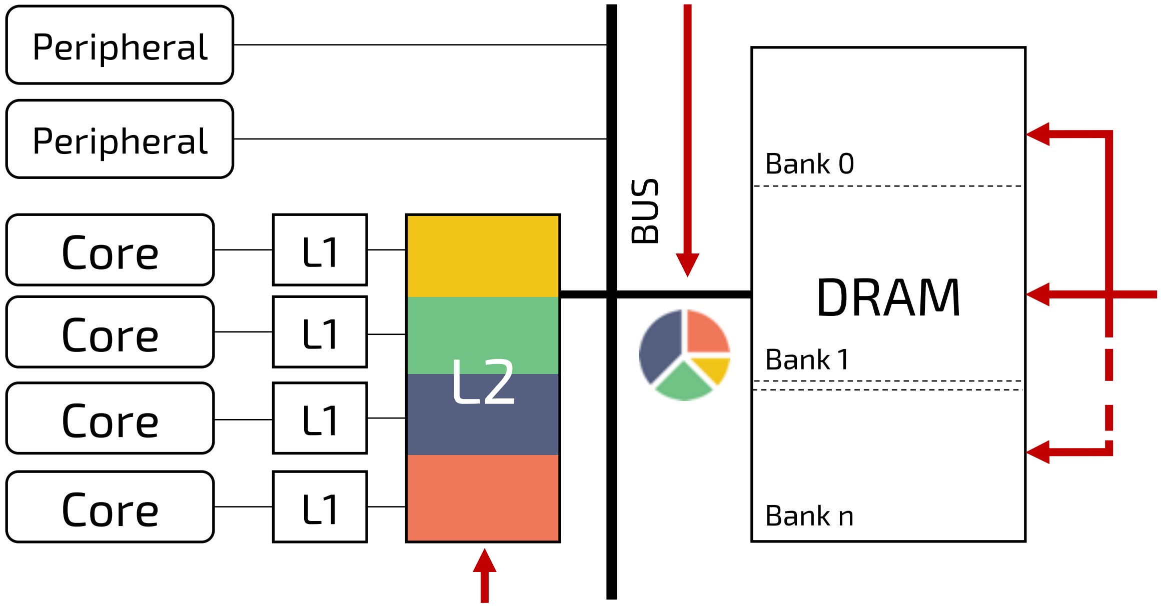

Contention due to I/O-related memory accesses

Strong isolation for modern embedded platforms

The Hypervisor can provide isolation mechanisms to control cache and memory bandwidth interference for multiprocessors

Memory bandwidth reservation

Budgeting the number of transactions that can be issued by each core and each I/O peripheral over time



Bank-aware partitioning

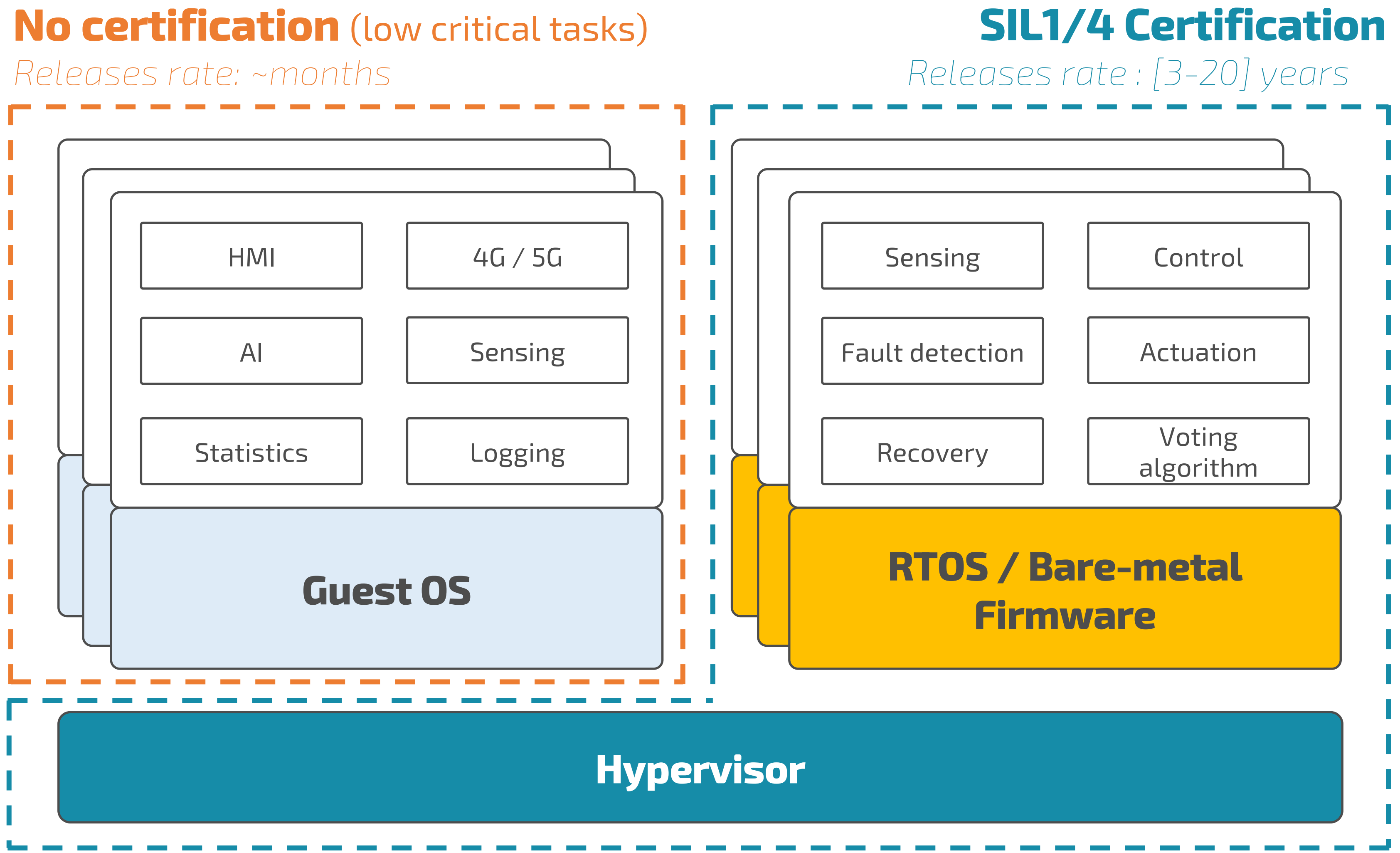
Allocating domains to different DRAM banks to control memory contention

Cache coloring

Partitioning the shared levels of cache to control inter-core interference

A New Certification Approach

Technology innovation run at different speeds

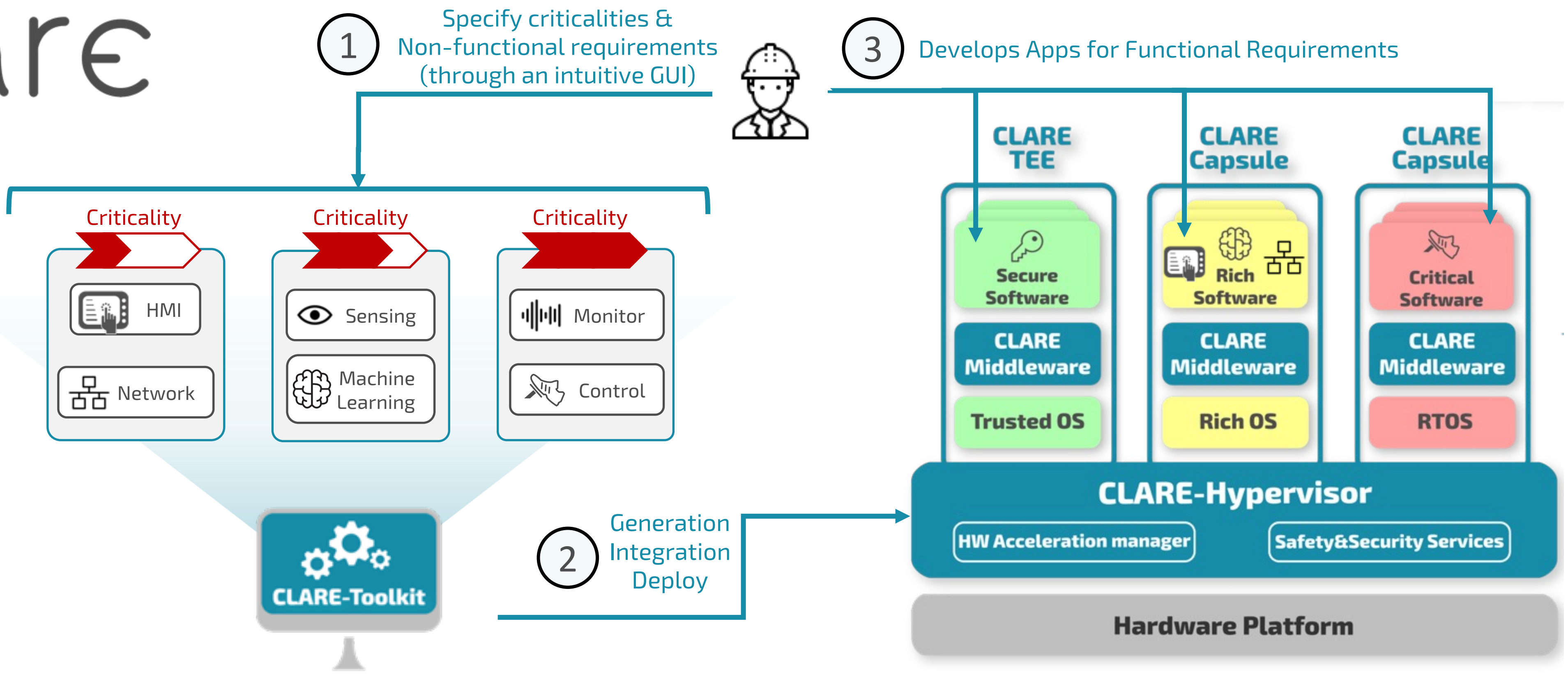


Updates without affecting certified part

(no need for re-certification)

Unchanged over time

The CLARE Software Stack



1 Specify criticalities & Non-functional requirements (through an intuitive GUI)

Criticality
HMI
Network

Criticality
Sensing
Machine Learning

Criticality
Monitor
Control

CLARE-Toolkit

2 Generation Integration Deploy

3 Develops Apps for Functional Requirements

CLARE TEE
Secure Software
CLARE Middleware
Trusted OS

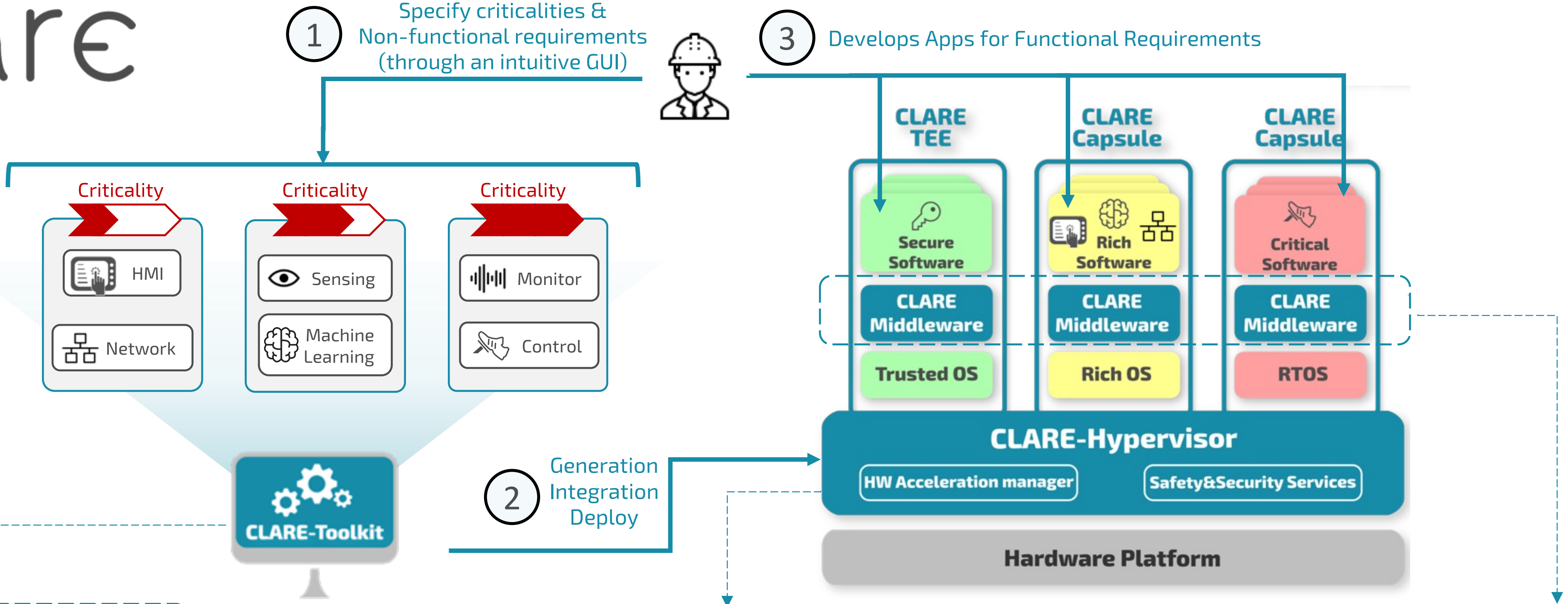
CLARE Capsule
Rich Software
CLARE Middleware
Rich OS

CLARE Capsule
Critical Software
CLARE Middleware
RTOS

CLARE-Hypervisor
HW Acceleration manager
Safety&Security Services

Hardware Platform

The CLARE Software Stack



Platform awareness
Optimized resource allocation
Final image generation
GUI-based

Hard Real-Time Resource Management
Strong temporal and spatial isolation
Cutting-edge system-level security mechanisms
Totally static with ~ 8K LoC

Safe & Secure Inter-domain communication
API for Services exposed by CLARE
Predictable usage of virtualized peripherals

accelerat

Simplifying complexity

See more at accelerat.eu

Contact us at info@accelerat.eu