ReTiS Lab Open Day
Research Activities on Hypervisors

Alessandro Biondi

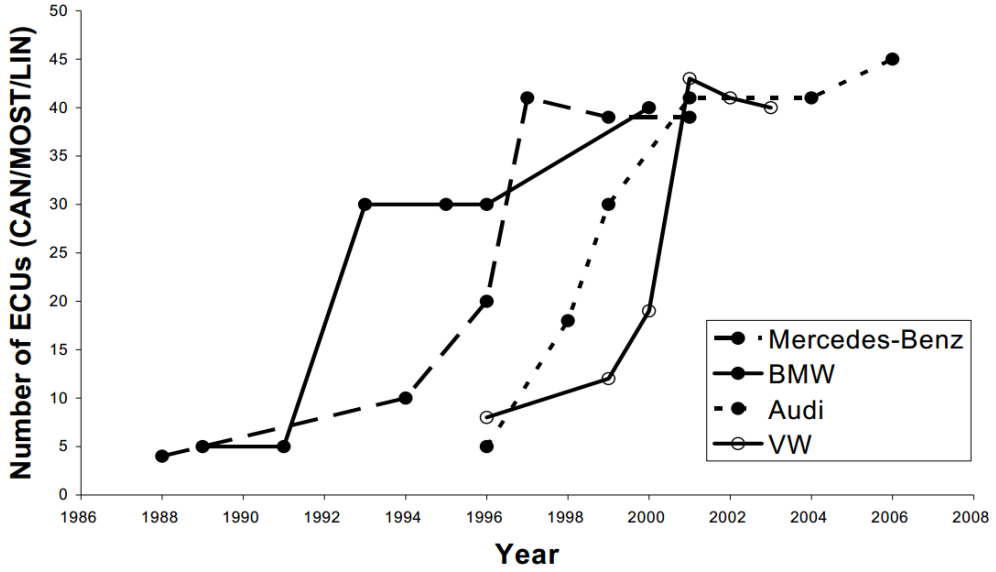
Scuola Superiore Sant'Anna, Pisa, Italy

Sant'Anna
Scuola Universitaria Superiore Pisa

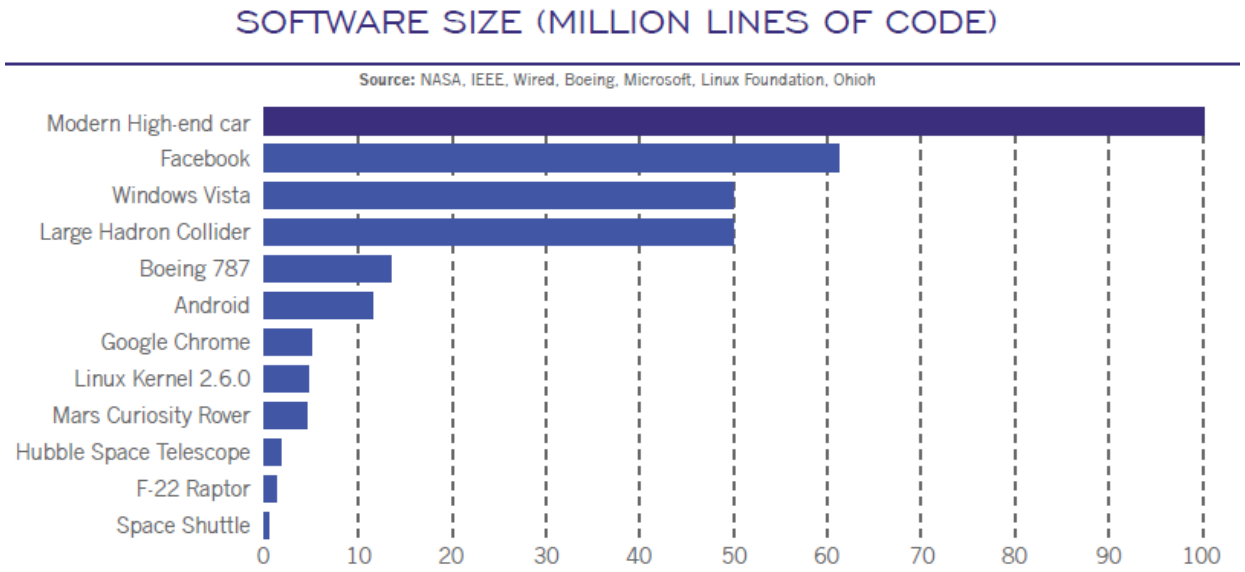
Real-Time Systems Laboratory

MILS Systems

- A story heard a thousand times: embedded SW complexity is tremendously increasing!
- Integration of multiple systems upon the same platform is not anymore an emerging trend, but rather a de-facto standard practice
  - Need to support different with multiple independent criticality and security levels (MILS)
  - Need to support multiple operating systems on the same platform



(the trend was clear even 10+ years ago)



Landscape of Heterogeneous Platforms

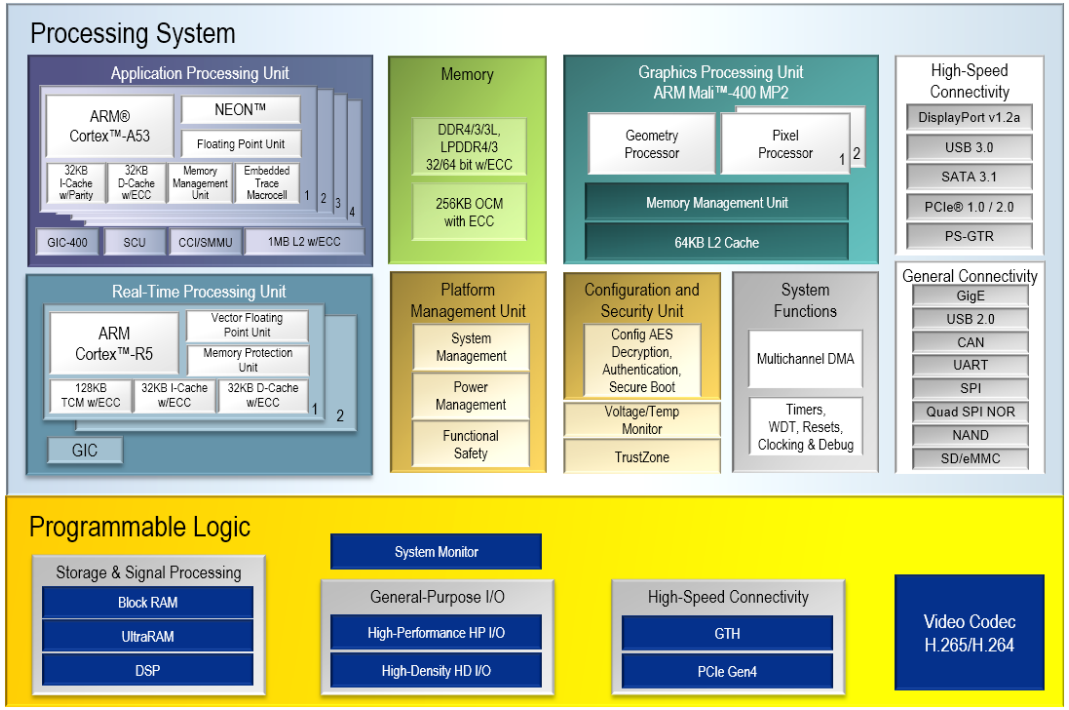
XILINX

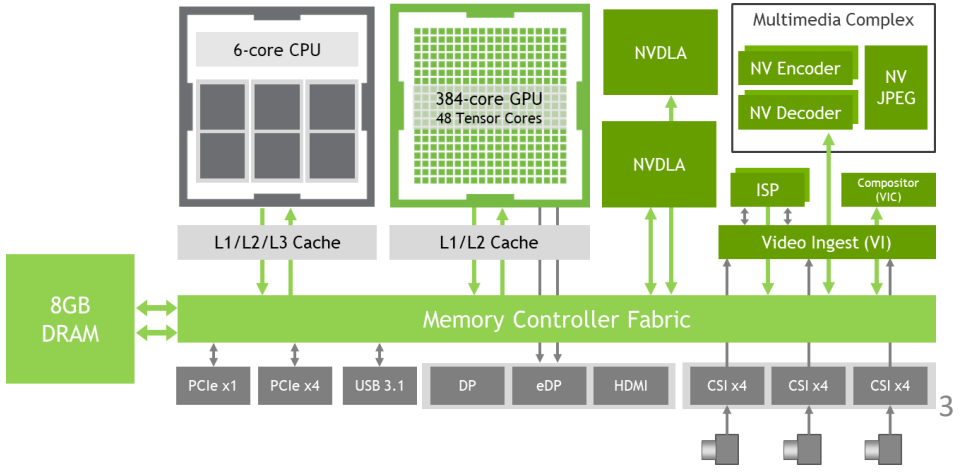
TEXAS INSTRUMENTS

life.augmented

QUALCOMM®

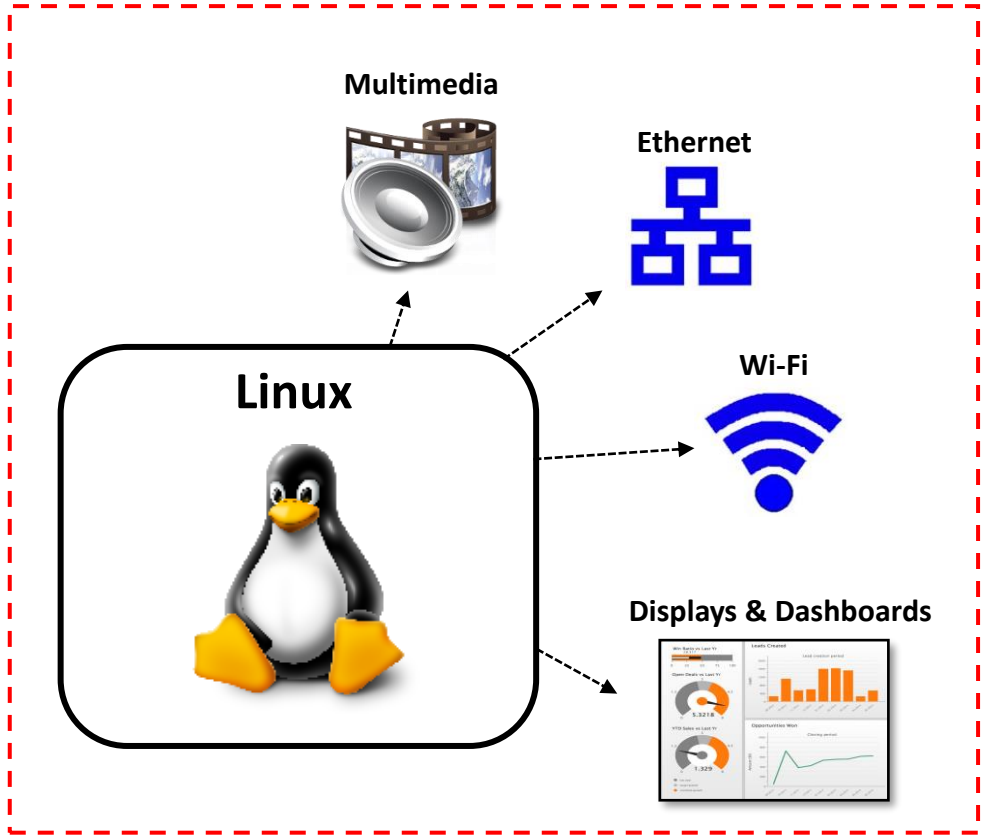
KALRAY

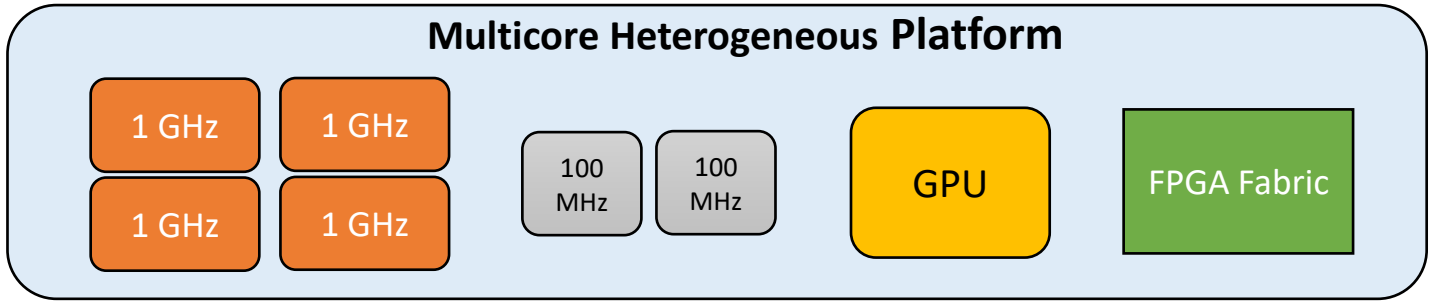




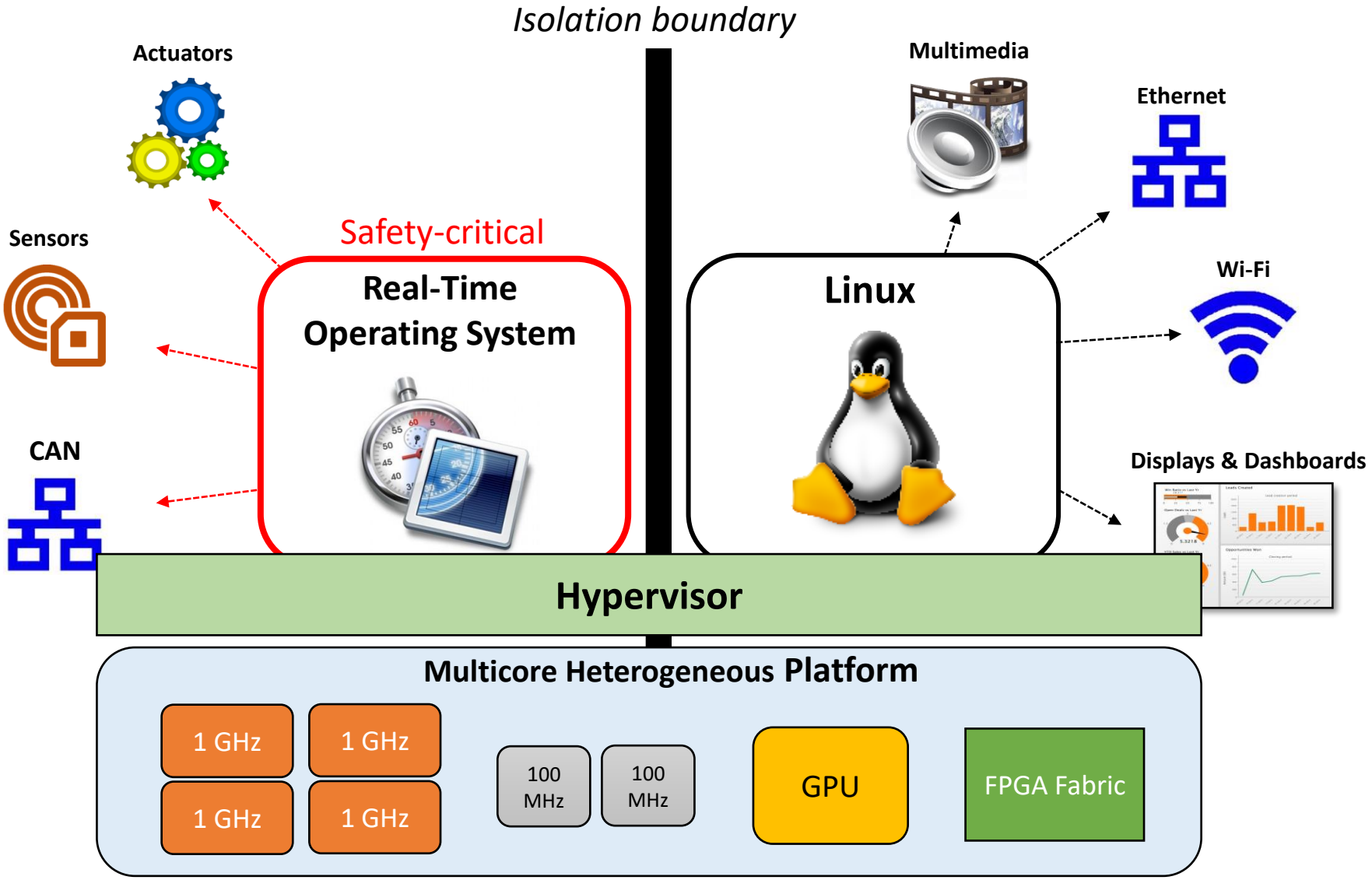
Multi-OS Solutions

- ✓ Rich availability of libraries, drivers, and network stacks
- ✓ Widespread and free
- ✗ Large code base
- ✗ Prone to **bugs** and **cyber attacks**
- ✗ Hard (if not *impossible*) to **certify**





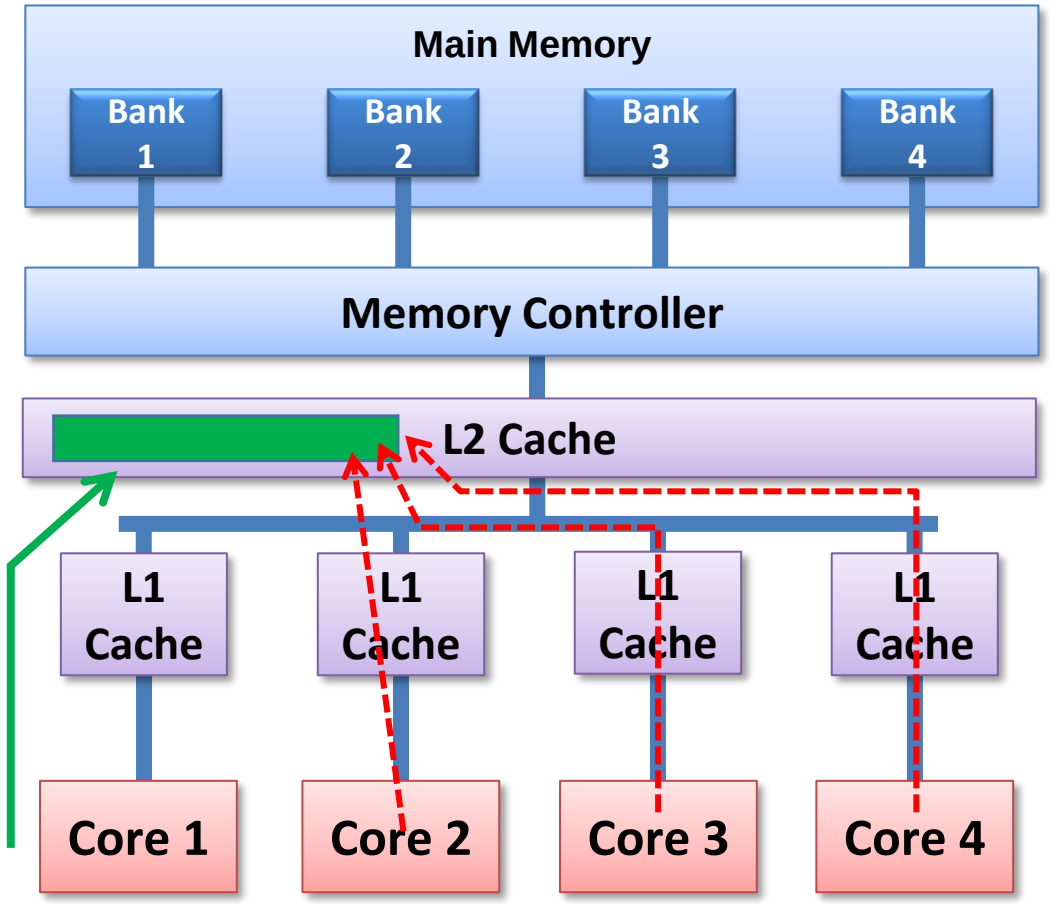
Multi-OS Solutions



Cache and Memory Contention

- Applications running in parallel on different cores can incur in highly-unpredictable interference due to cache and memory bandwidth contention
- Key issue to achieve **strong isolation** among domains and time-predictability on multicores

Contention at shared caches

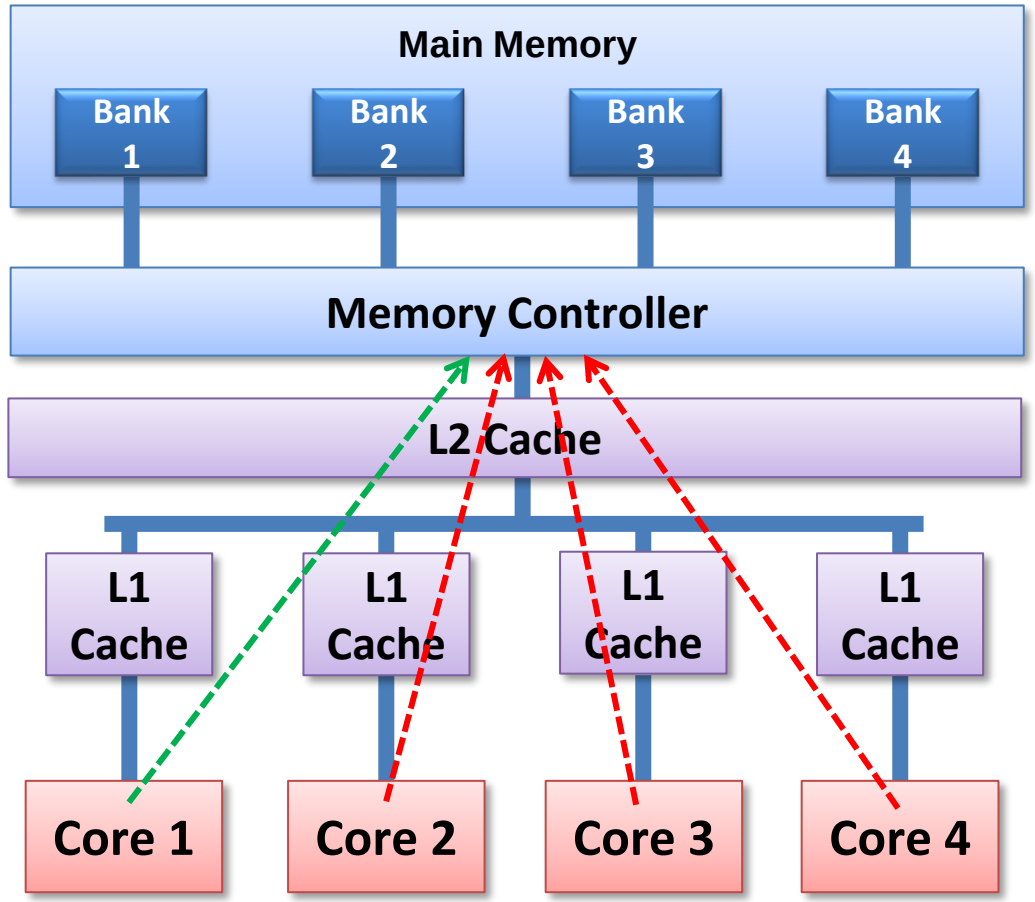


Cache and Memory Contention

- Applications running in parallel on different cores can incur in highly-unpredictable interference due to cache and memory bandwidth contention
- Key issue to achieve **strong isolation** among domains and time-predictability on multicores

Contention at shared caches

Contention at the memory controller



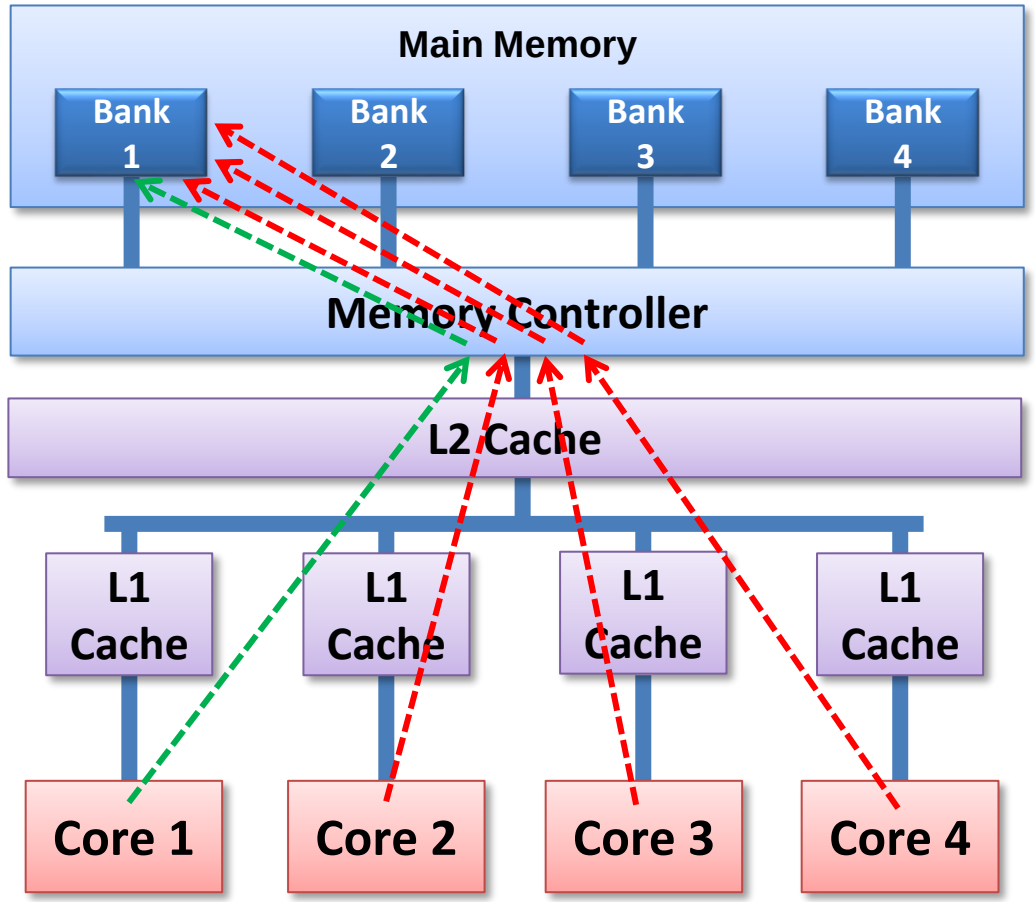
Cache and Memory Contention

- Applications running in parallel on different cores can incur in highly-unpredictable interference due to cache and memory bandwidth contention
- Key issue to achieve **strong isolation** among domains and time-predictability on multicores

Contention at shared caches

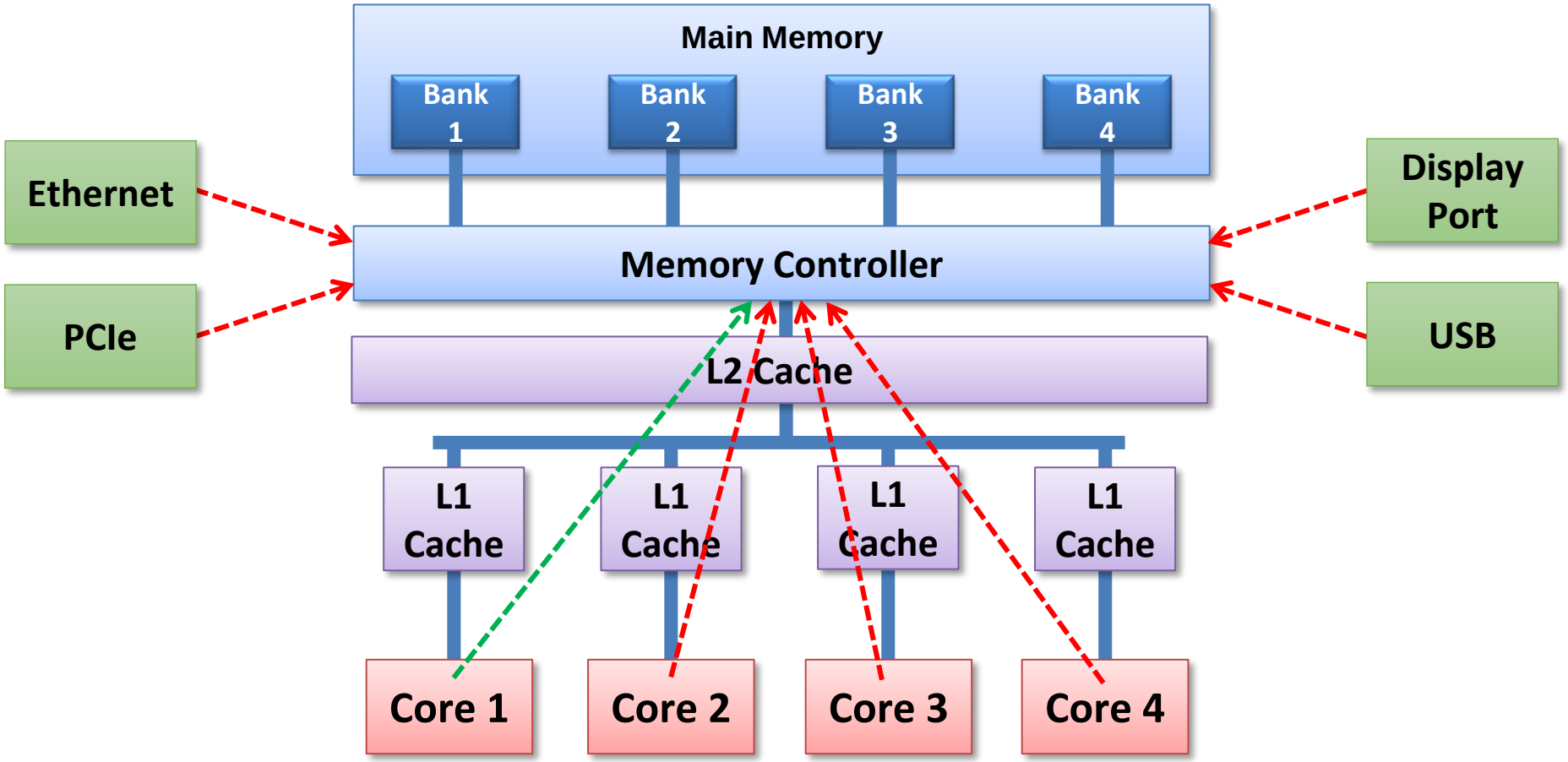
Contention at the memory controller

Contention at memory banks



I/O-Related Memory Contention

- Several I/O peripherals include a DMA engine to directly move I/O data from and to memory
- They constitute other bus masters that contribute to the overall memory contention in the platform



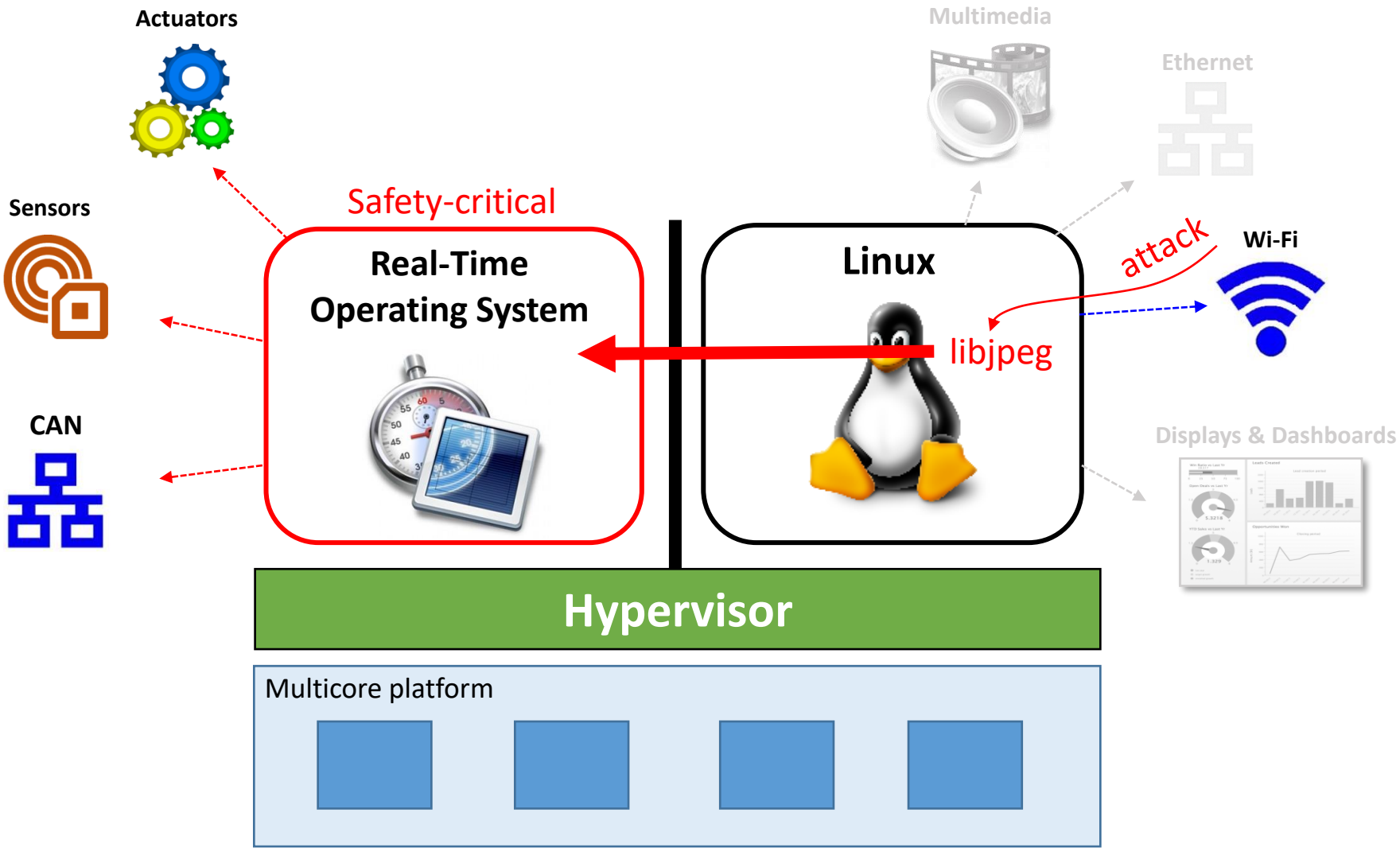
Safety and Security

- **Uncontrolled contention** of microarchitectural resources is both a safety and security problem

- Mutual interference between critical and non-critical software systems
- Poor time predictability
- Fault propagation

- Malicious software in a non-critical domain can intentionally delay critical software as much as possible, compromising its correctness if it is real time
- Room for side channel attacks

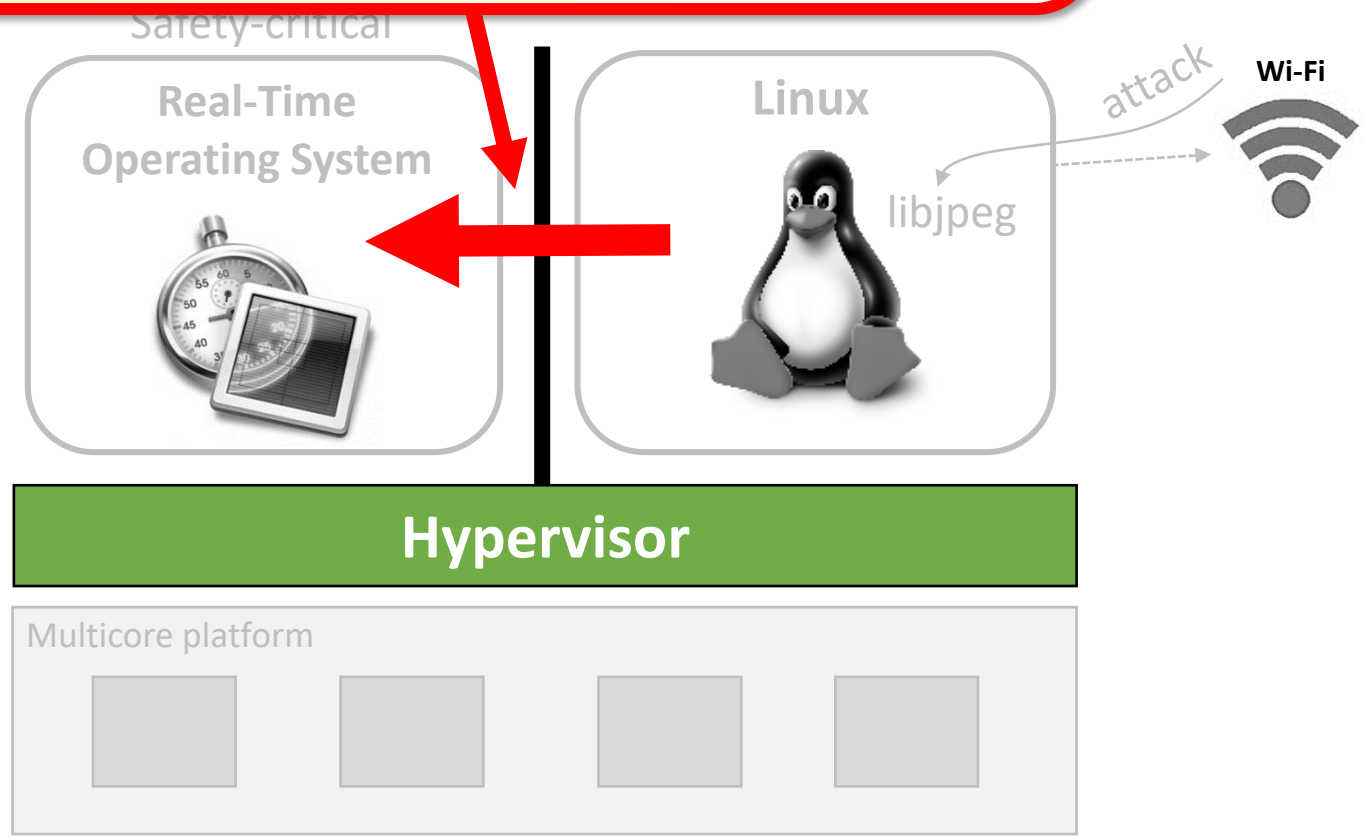
Cyber-attacks



Cyber-attacks

Compromised isolation boundaries

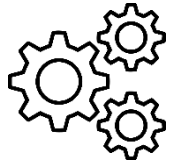
- Vulnerabilities in the hypervisor
- Wrong configuration/initialization
- Malicious exploitation of peripherals in the platform
- Side channels



Opportunities @ ReTiS

Real-Time Systems Laboratory

- The ReTiS Lab offers various opportunities to work on Hypervisor technology, both at the system and application level



Design and development of new **Hypervisor-level mechanisms** for safety, security and time predictability

Realization of **optimization algorithms** to allocate resources to domains

Virtualization support for **new heterogeneous platforms**

Application of Hypervisor technology to systems such as autonomous vehicles and robots

Research contracts sponsored by the **industry** (including our spin-off company *Accelerat*) are available!

Thank you!

Alessandro Biondi
alessandro.biondi@santannapisa.it

https://retis.sssup.it/~a.biondi/