Sant'Anna
Scuola Universitaria Superiore Pisa

Retis
Real-Time Systems Laboratory

A Dual-Hypervisor for supporting multiple Trusted Execution Environments on Arm TrustZone

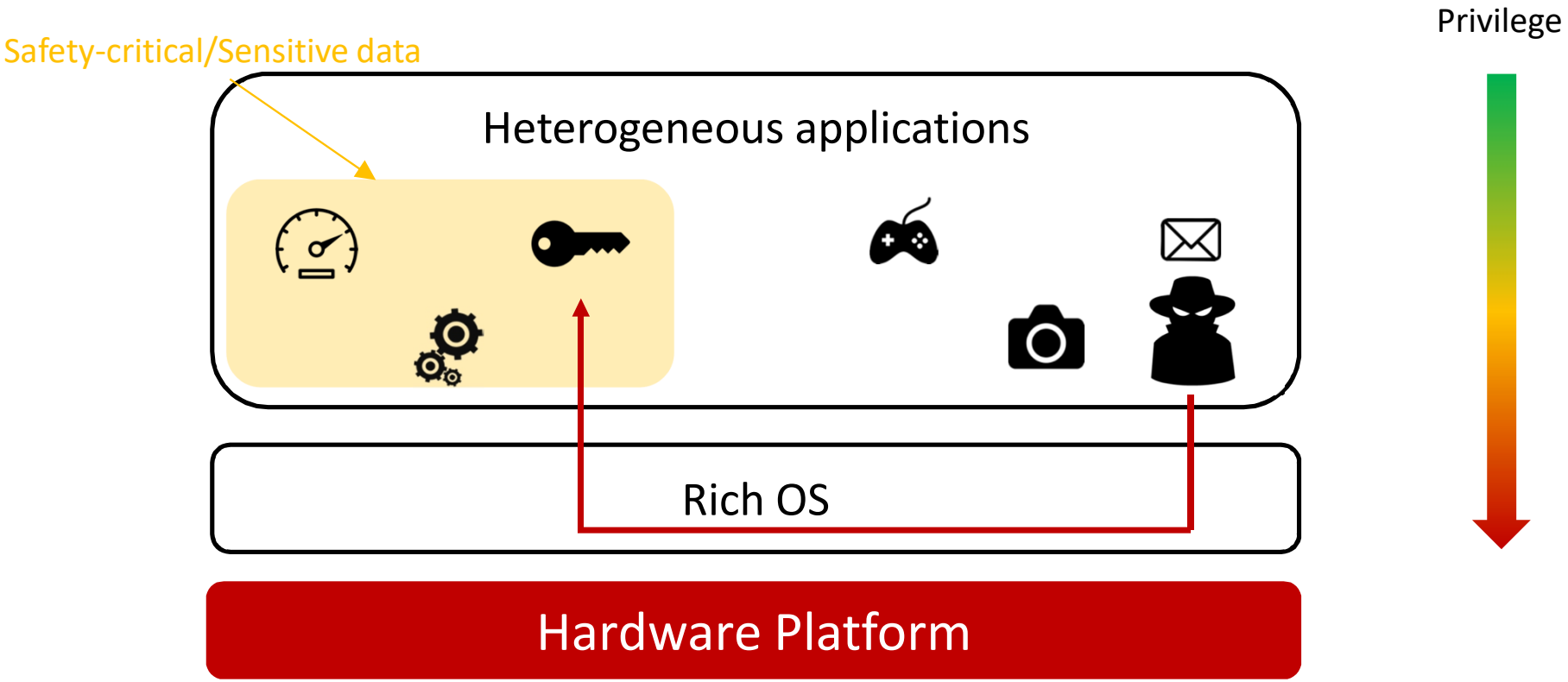
Giorgiomaria Cicero
Alessandro Biondi
Giorgio Buttazzo

ReTiS Lab – Tecip Institute
Scuola Superiore Sant'Anna

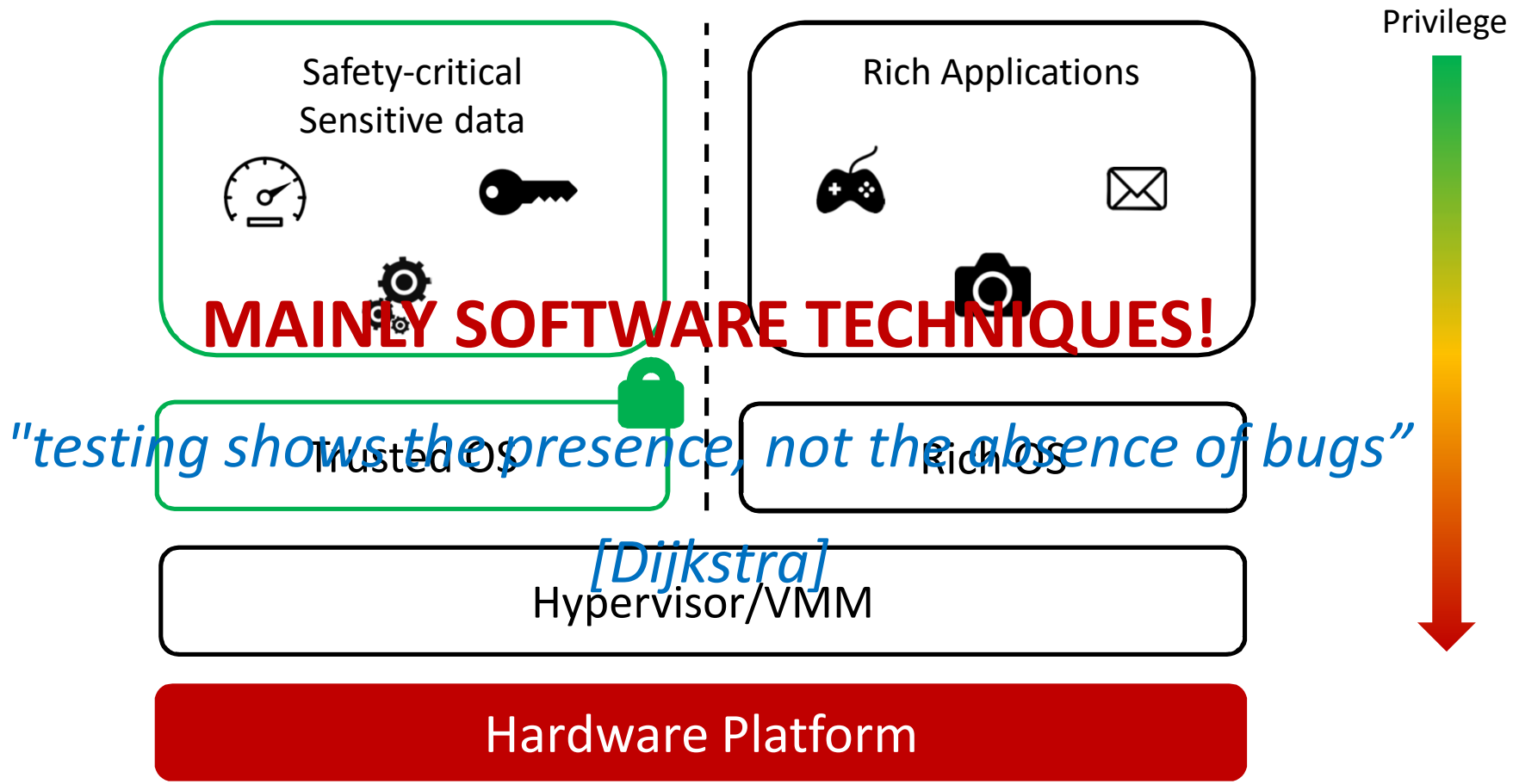
AGENDA

1. **Isolation for multiple domains with Trusted Execution Environments (TEEs)**
   - The need for reconciling virtualization with hardware-based security capabilities
2. **A Dual-Hypervisor design for ARM TrustZone**
   - Achieving virtualization of both secure and non-secure worlds with jointly-configured hypervisors with a limited overhead, small memory footprint and high predictability
3. **A Safe, Secure and Hard Real-time software stack**
   - A solution for next-generation autonomous systems

Integrating multiple software components

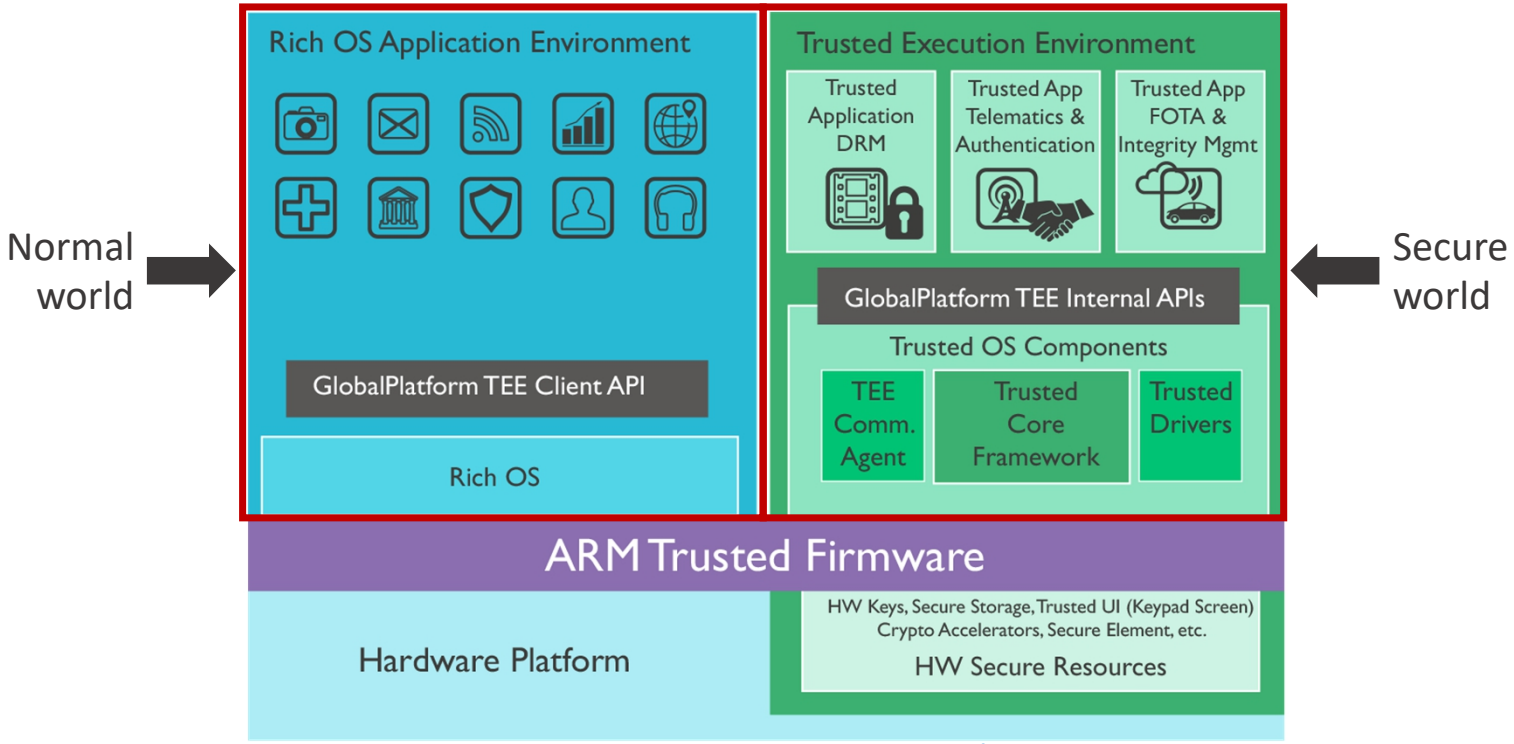


Multi-OS solution through virtualization



Proposed HW solution – ARM TrustZone

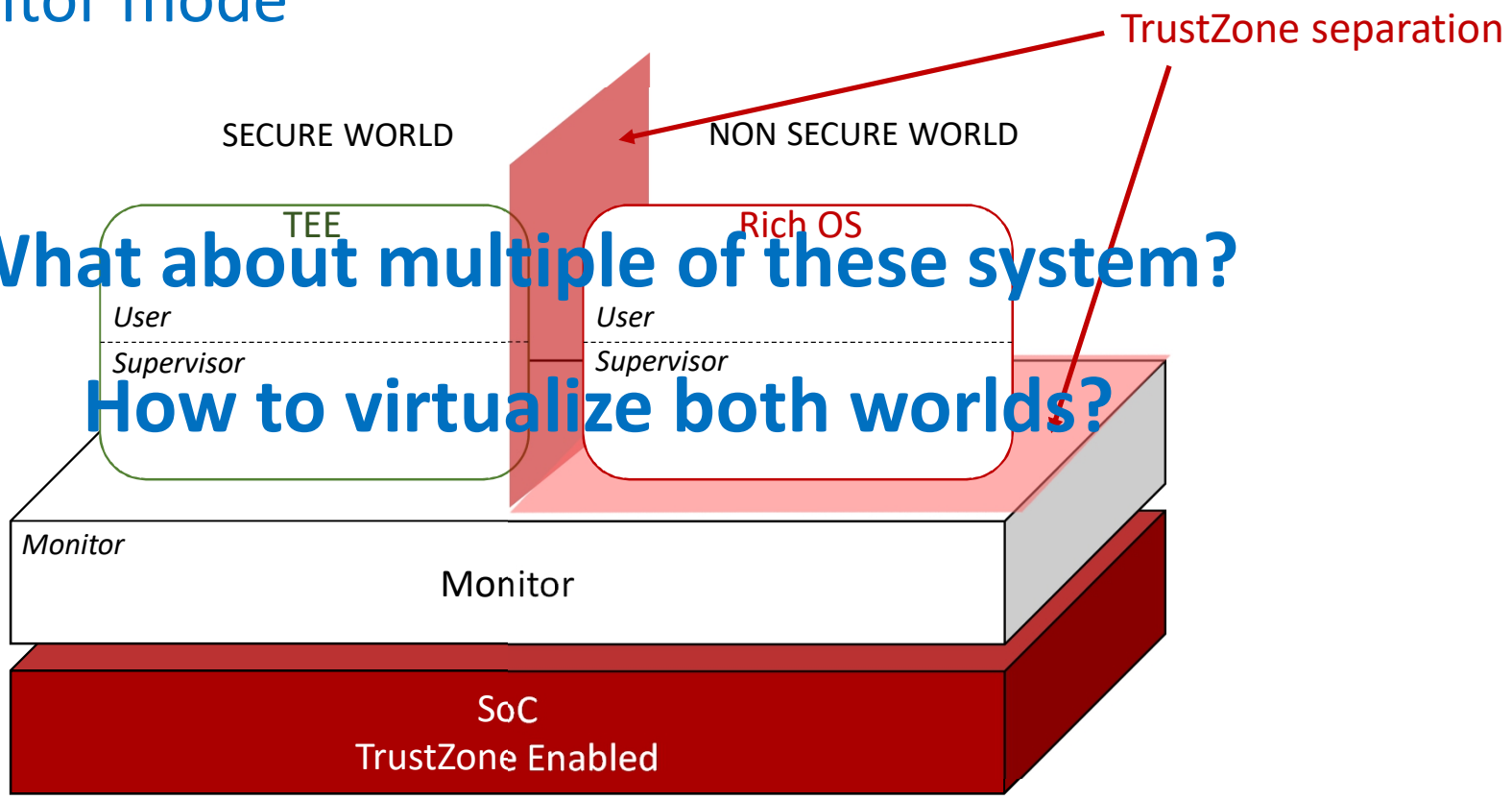
TrustZone provides support for a hardware-based TEE by splitting computer resources between two execution worlds



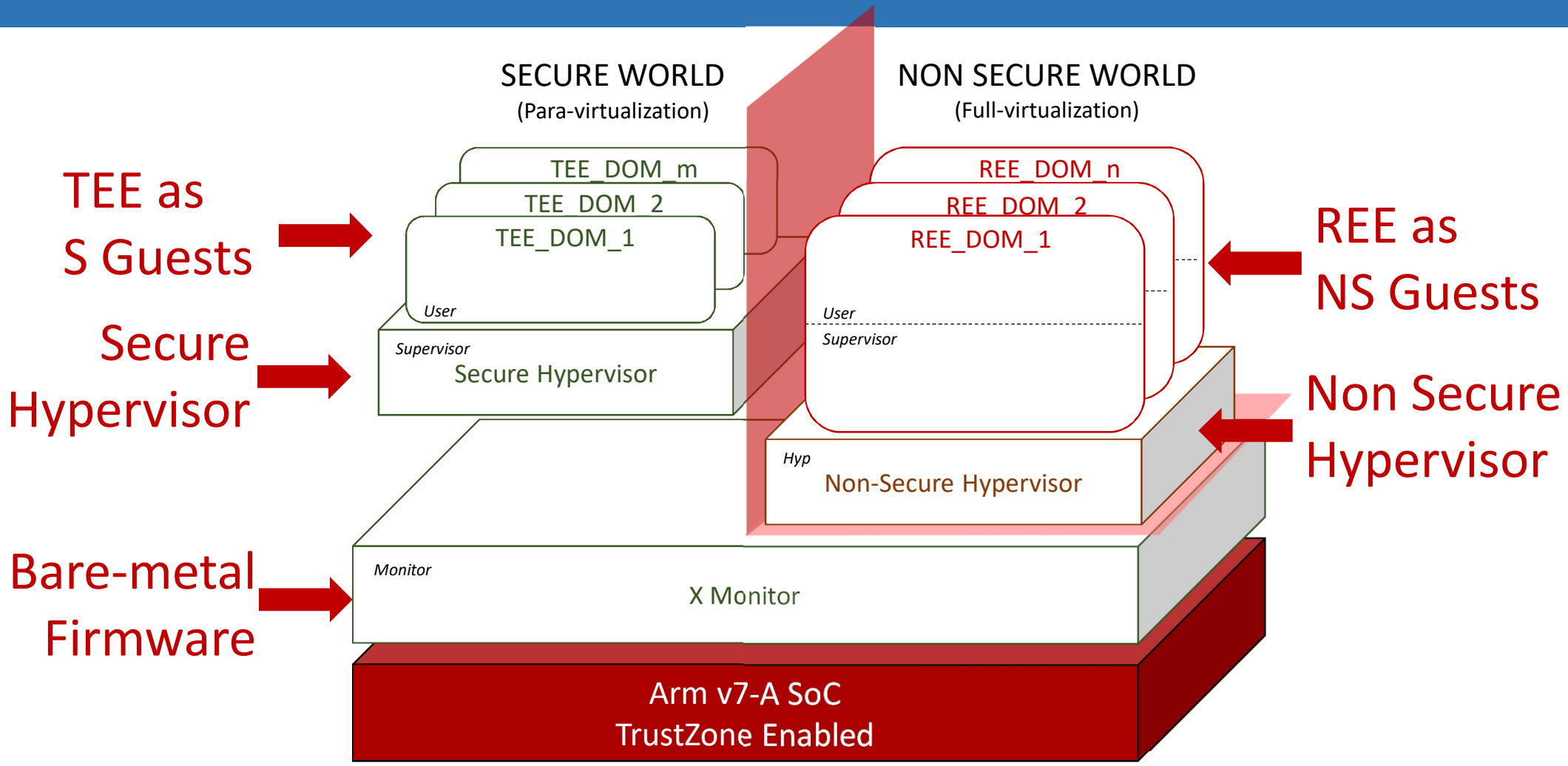
Picture from www.developer.arm.com

ARM TrustZone for ARMv7-A/R processor

Classical processor modes split into normal and secure plus a super privileged monitor mode

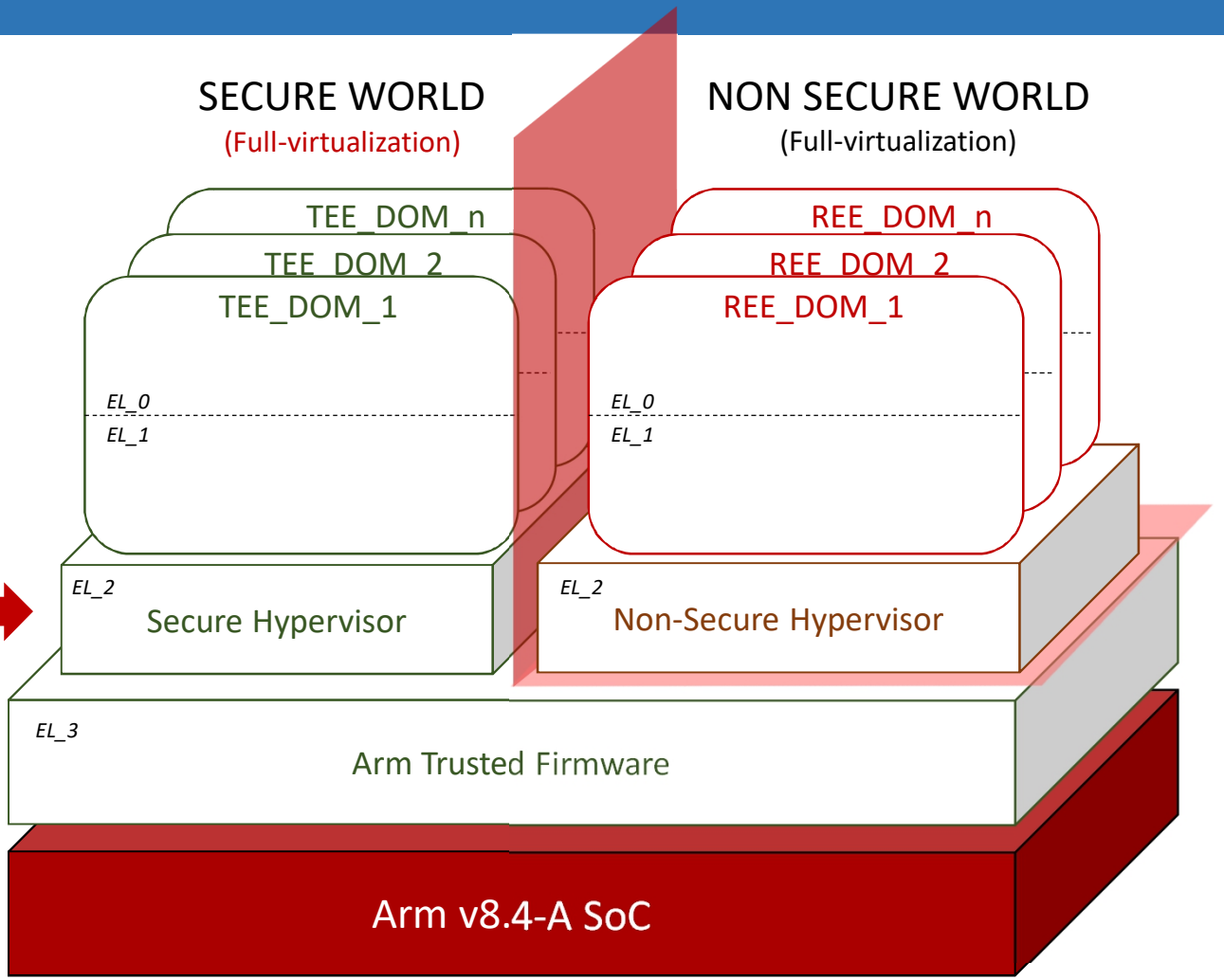


The Dual-Hypervisor Design

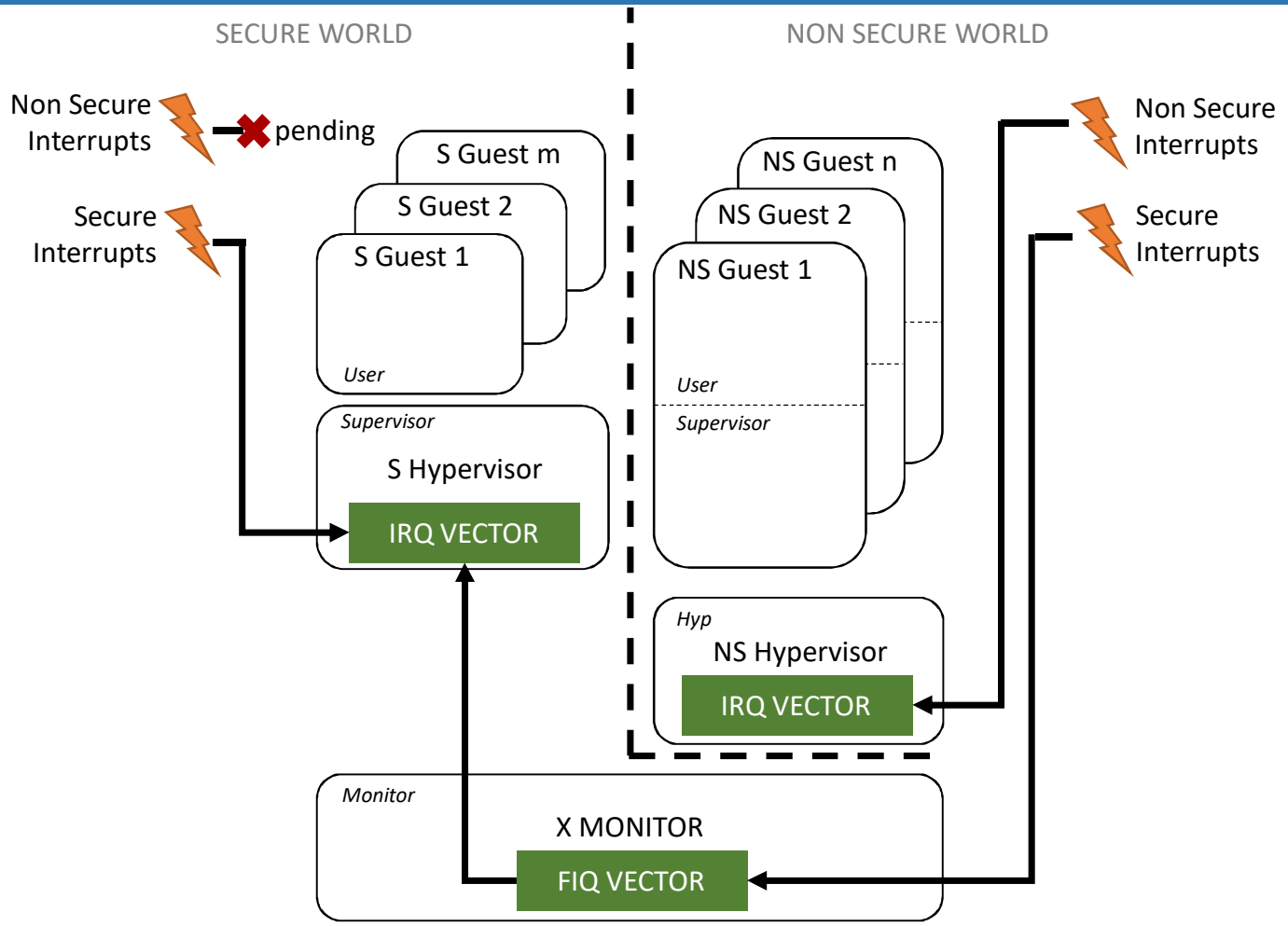


The Future Dual-Hypervisor Design

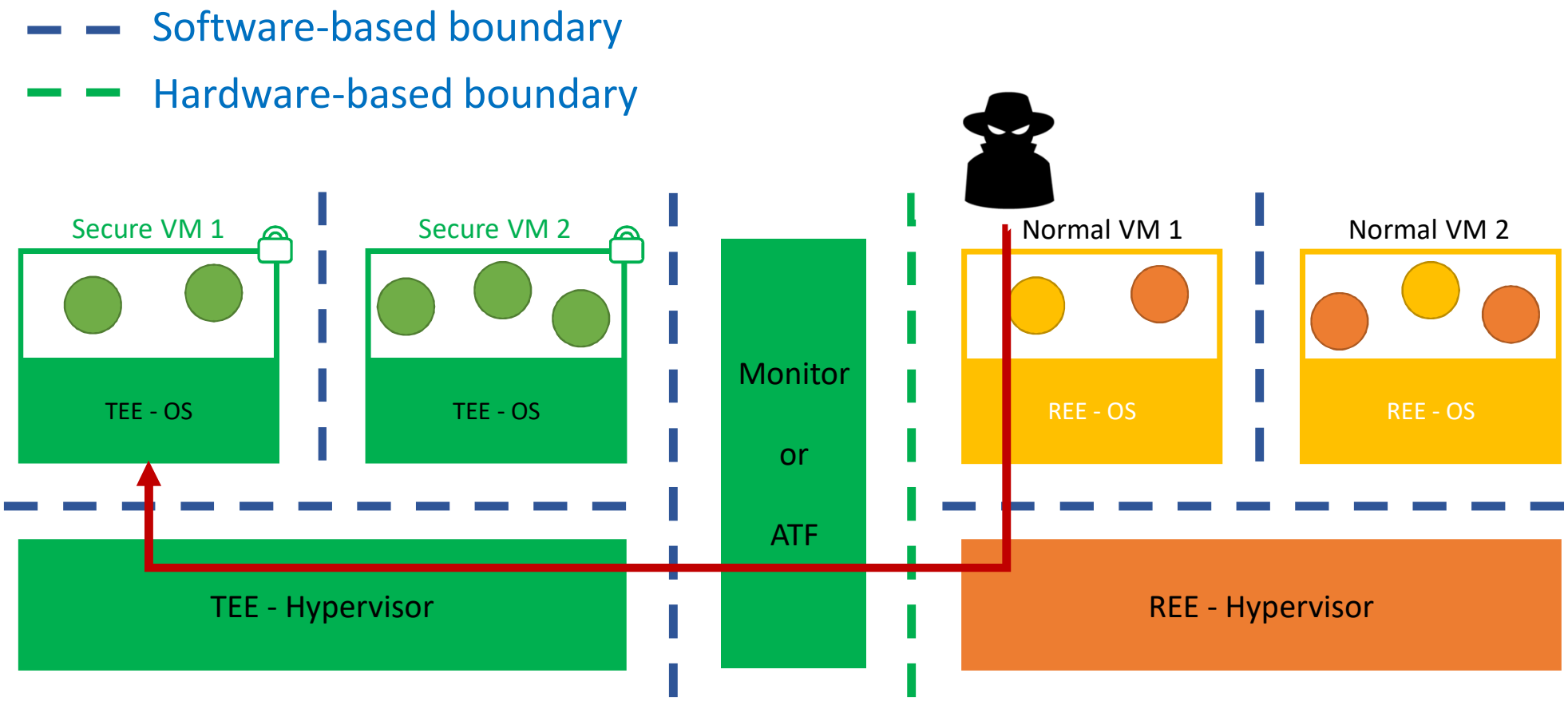
Secure Hyp mode



Secure world is highly predictable

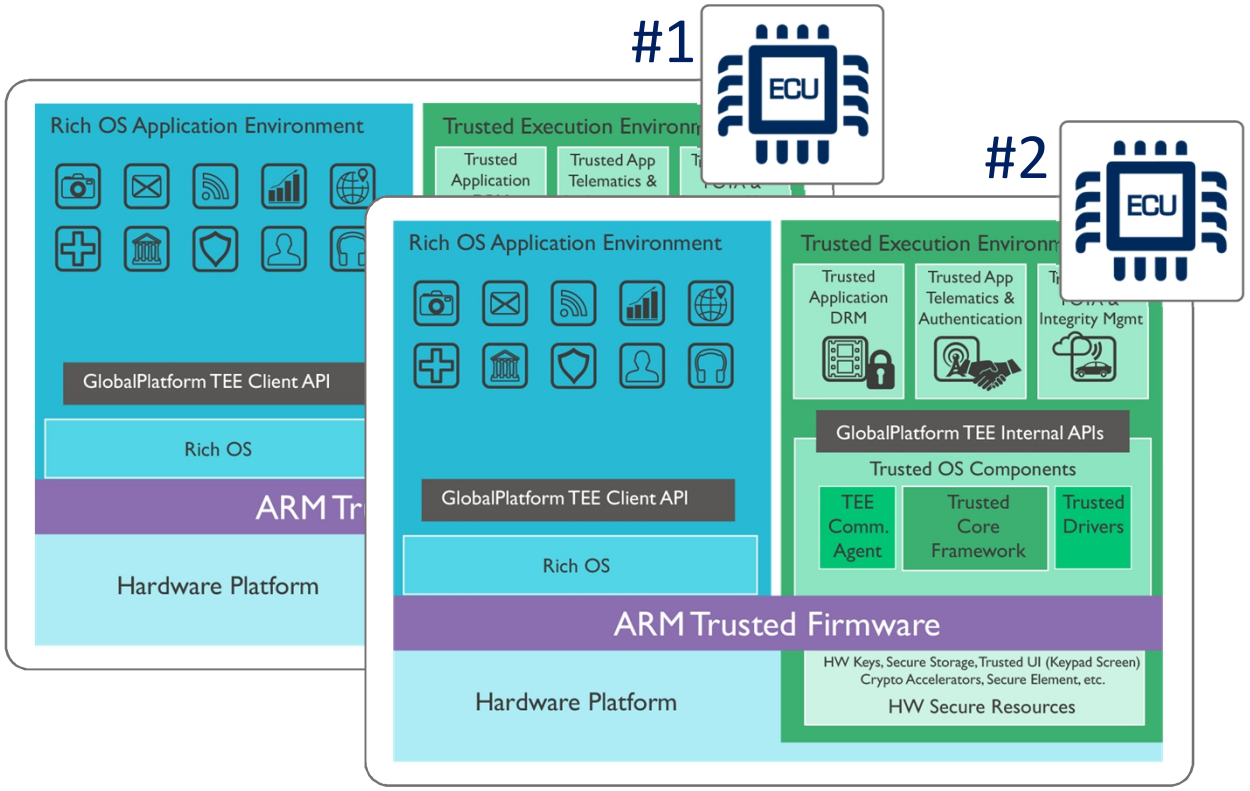


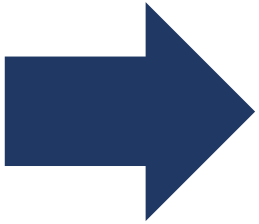
Isolation boundaries of the Dual-Hypervisor design

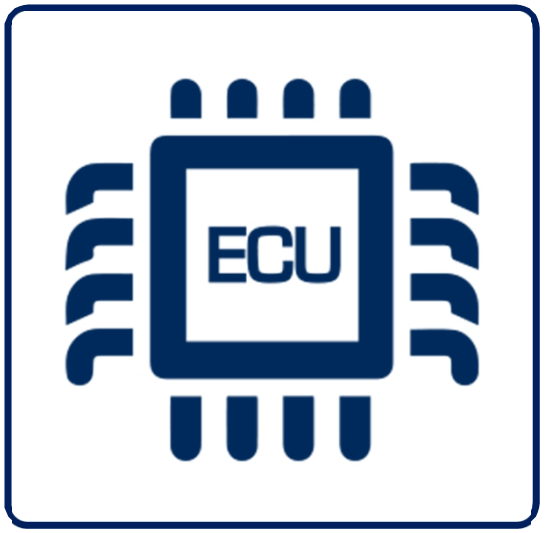


Potential application in the automotive field

Towards reducing #ECUs, integrating multiple ECU functionalities (i.e. software) within the same platform can be very challenging



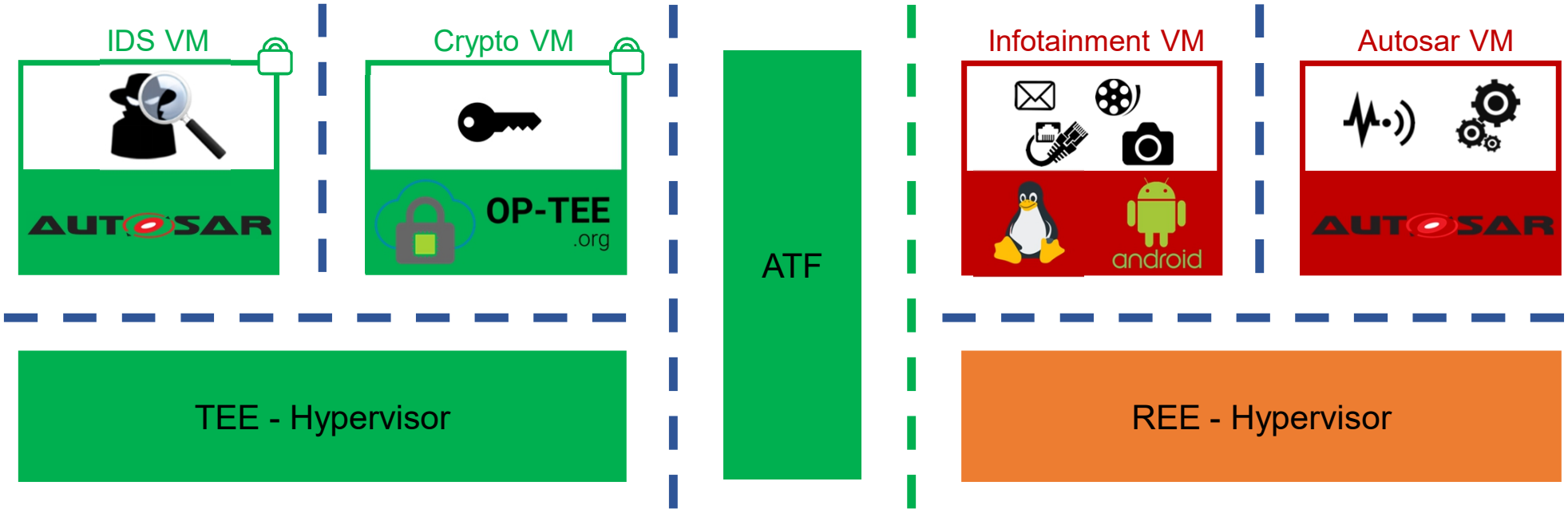




SINGLE ECU

Potential application in the automotive field (2)

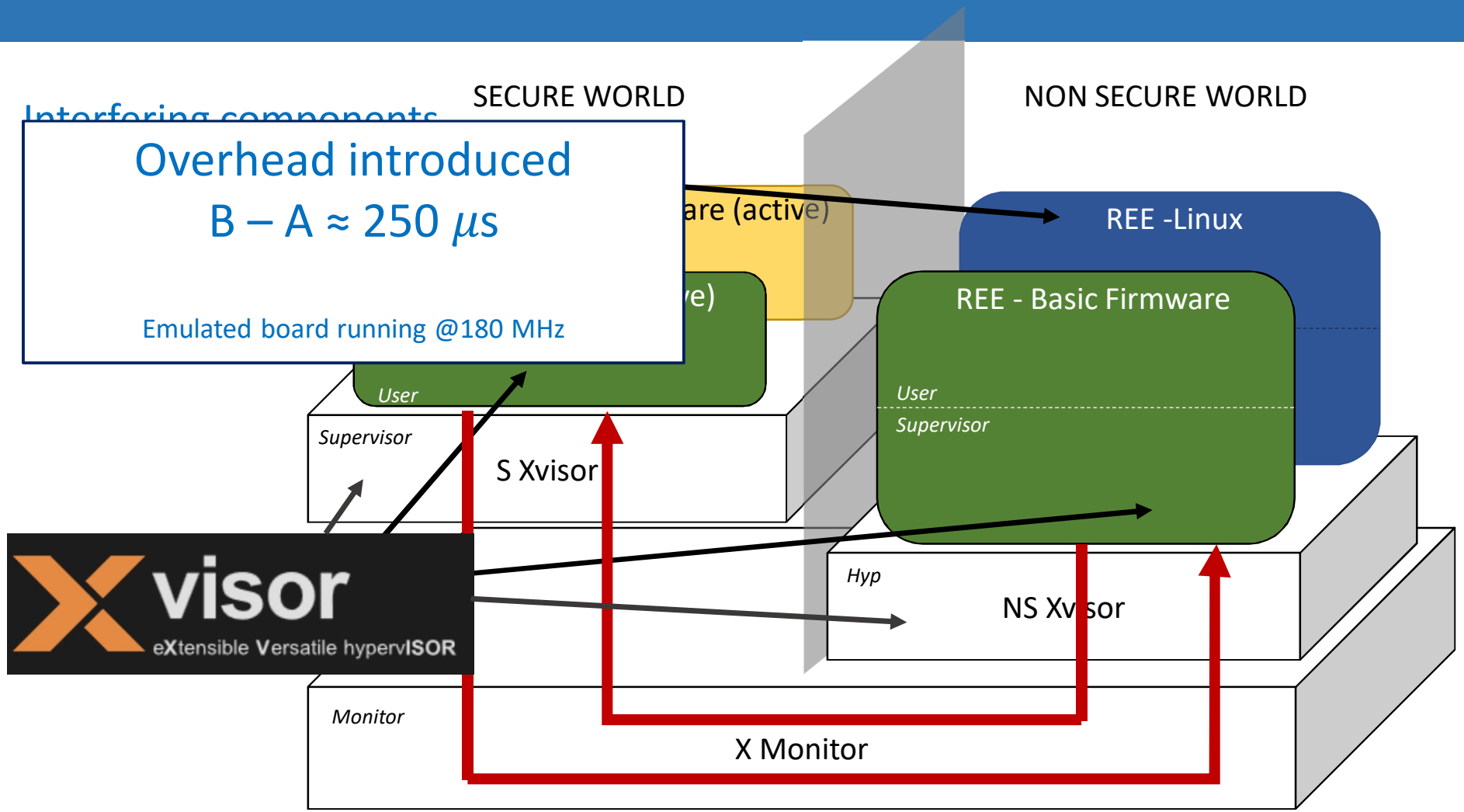
Combining infotainment system with Autosar systems



- - - - Hardware-based boundary (e.g. Arm TrustZone)

– – – – Software-based boundary (based on hardware-assisted virtualization)

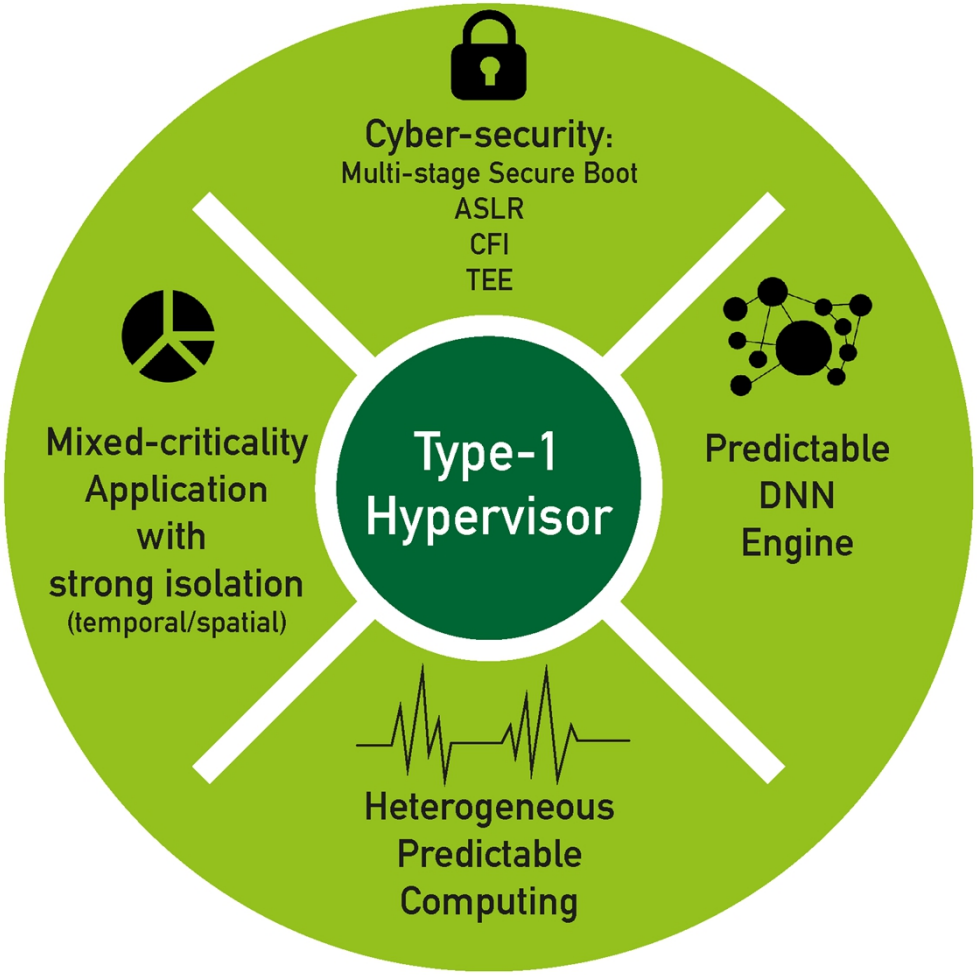
Test case


SECURE WORLD
NON SECURE WORLD
Overhead introduced
B – A ≈ 250 μs
Emulated board running @180 MHz
are (active)
ve)
REE -Linux
REE - Basic Firmware
User
Supervisor
User
Supervisor
S Xvisor
Hyp
NS Xvisor
Monitor
X Monitor
visor
eXtensible Versatile hypervISOR

Benefits

- A Dual-hypervisor design can support multiple TEEs
- Leveraging hardware-based isolation achieving robustness
- No single point of failure
- Limited overhead for NS Guests w.r.t. single-hypervisor designs
- More robustness with regard to hyperjacking
- High predictability on executing trusted code

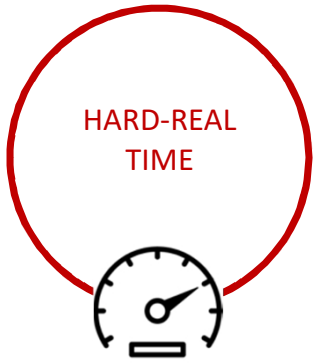
Current and future works



Working towards a Spin-Off!!

Hypervisor: main features

- Address-Space Randomization
- Control Flow Integrity (Armv-8.3 HW support)
- Stack overflow protection
- Secure boot for Virtual Machines
- Several side-channel attacks mitigations
- Dual-Hypervisor for strong MILS (see next slide)



- Cache-coloring
- Memory bandwidth
- Bank-aware memory allocation
- O(1) algorithm complexities (almost all)
- Fixed-priority (RM/DM) and EDF scheduling
- Resource reservation
- Very low boot latency

- Totally static
- Off-line auto-generated configuration
- MISRA-C 2012 compliant
- Code prone for SIL3/4 certification
- Safety guards for unpredictable SW
- Low memory-footprint

Current status

Xilinx Zynq Ultrascale+
(ZCU102 board)

CPU	Quad-core ARM Cortex-A53 Dual-core ARM Cortex-R5
GPU	ARM Mali-400 MP2
FPGA	Zynq Ultrascale FPGA XCZU9EG (600K logic cells, 32Mb mem, 2520 DSPs)
Memory	PS 4GB DDR4 64-bit SODIMM w/ ECC PL 512MB DDR4 at 1200MHz / 2400Mbps DDR

Targets
- ADAS
- Railway
- Industry 4.0

NVIDIA Jetson TX2

GPGPU	NVIDIA Pascal™, 256 NVIDIA CUDA® cores
CPU	HMP Dual Denver 2/2MB L2 + Quad ARM® A57/2MB L2
Memory	8 GB 128-bit LPDDR4 58.3 GB/s

Targets
- ADAS
- Autonomous driving
- Industry 4.0
- Robotics

Sant'Anna
Scuola Universitaria Superiore Pisa

Retis
Real-Time Systems Laboratory

THANKS FOR YOUR ATTENTION

Giorgiomaria Cicero
Research Fellow at Retis Lab
Scuola Superiore Sant'Anna
Pisa, Italy

g.cicero@sssup.it