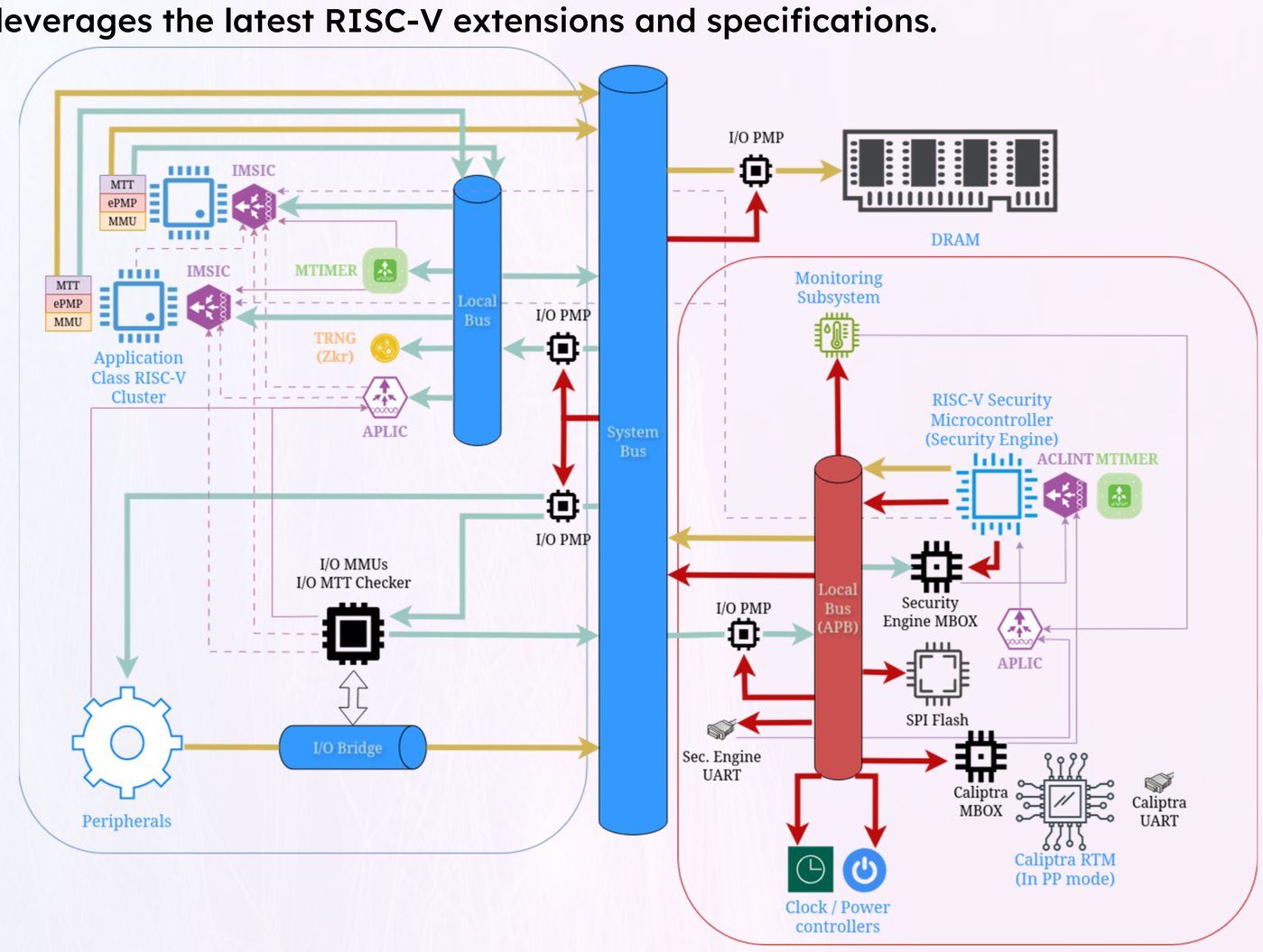
Designing a RISC-V Platform for the HIGHER Project Based on Current and Upcoming Extensions

Manolis Marazakis and Nick Kossifidis

Institute of Computer Science, Foundation for Research and Technology – Hellas (FORTH)

Outline

With the increasing demand for open-source and sovereign computing solutions, the HIGHER project is developing a server platform based on RISC-V and Open Compute Project (OCP) standards. Our reference design encompasses two distinct security domains that enforce strong system integrity and workload isolation. These domains work in concert to provide a secure, modular, and efficient server architecture that leverages the latest RISC-V extensions and specifications.



Main CPU Cluster (Compute Domain)

The Main CPU Cluster subsystem serves as the high-performance compute domain, built around a RISC-V CPU cluster compliant with the RVA23 profile for both user-mode and supervisor-mode operations. Key features include:

- **Multiple Supervisor Domains**: Secure virtualization through RISC-V Hypervisor extension
- **Advanced Interrupt Architecture (AIA)**: Efficient interrupt handling across domains
- **I/O MMU Integration**: Secure I/O operations for virtualized environments
- **Confidential Virtualization Extensions (CoVE and CoVE I/O)**: Hardware-enforced confidential computing
- **QoS Management**: Utilizing RISC-V Capacity and Bandwidth QoS Register Interface (CBQRI)

System Security Domain

At the core of the system, the System Management Domain integrates the Caliptra Root of Trust for Measurement module (RTM), defined as part of OCP Security WG specifications, alongside a dedicated RISC-V security processor. This domain provides:

- **Secure Boot Process**: Ensuring system integrity from power-on
- **Attestation Services**: Runtime verification of system authenticity
- **Power and Clock Control**: Dynamic power scaling, frequency throttling, and clock gating
- **System Monitoring**: Continuous monitoring through sensors and anti-tampering mechanisms
- **Error Detection and Reporting**: Via RISC-V RAS Error-record Register Interface (RERI)
- **Security Updates**: Enforced through signature verification and secure boot image updates
- **Memory Initialization and Isolation**: Leveraging RISC-V I/O Physical Memory Protection (I/O PMP)

RISC-V Non-ISA standards	
Category	**Standard**
System-level Services	MTIMER, CBQRI, RERI
Interrupt Control	IMSIC, ACLINT, APLIC
Platform-level memory isolation	I/O PMP/MTT/MMU
Confidential Computing	CoVE, CoVE IO

RISC-V ISA Extensions	
Category	**Extensions**
Base ISA	RV64GCHBV (RVA23)
Crypto extensions	Zkr (Entropy source), Zvkng (Vector crypto, NIST suite), Zkt, Svukte (Data independent latency)
MMU addressing mode	Sv48
Vector register length	256 bits
Physical memory isolation	ePMP, MTT

Conclusion & Outlook

By leveraging open-standard security mechanisms and a modular architecture, this server platform design directly contributes to HIGHER's mission of fostering European digital autonomy and providing a viable alternative to proprietary cloud infrastructure with hidden management engines and undocumented sub-zero privilege rings. The use of RISC-V and OCP standards ensures a transparent, auditable, and interoperable solution for next-generation cloud and edge computing.

European Commission

higher

www.higher-project.eu

HIGHER: European Heterogeneous Cloud/Edge Infrastructures for Next Generation Hybrid Services
Grant Agreement: 101189612, DG/Agency: HaDEA
Start/end date: 01.01.2025 - 31.12.2027