# 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)

## Abstract

*The demand for secure and modular server architectures is driving interest in RISC-V as a foundation for scalable cloud and edge computing based on open standards. In the context of the HIGHER project, an initiative focused on developing open-source, high-density rack-scale systems for cloud and edge services, this presentation introduces a reference design for RISC-V-based server platforms designed for Open Compute Project (OCP) compatibility, structured around two distinct security domains to enforce strong system integrity and workload: System Management and Main CPU Cluster. By leveraging recently ratified RISC-V extensions, the Caliptra root-of-trust open-source module, and upcoming architectural advancements, we explore key security and system features, including memory isolation, confidential computing, and hardware-backed attestation, ensuring trustworthy functionality for managing, securing, and controlling modular server infrastructures. The isolation mechanisms recently introduced in RISC-V standards and incorporated in this reference design are of broad applicability, fitting also the automotive, mobile, and desktop environments.*

## Server Reference Design

With the increasing demand for open-source and sovereign computing solutions, the HIGHER project [1] is developing a server platform based on RISC-V and Open Compute Project (OCP) standards [2]. This poster outlines a reference design for a server platform structured around two distinct security domains to enforce strong system integrity and workload isolation : System Management and Compute (Main CPU Cluster). Figure 1 provides a visual overview of the reference design.

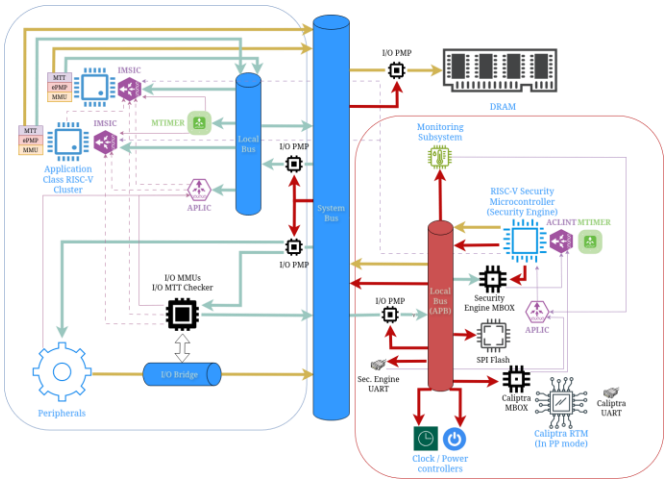


**Figure 1 : Overview of Reference Server Design.**

At the core of the system is the **System Management Domain**, which integrates the *Caliptra Root of Trust Module (RTM)* [3] alongside a dedicated RISC-V security processor. This security domain handles the secure boot process, and provides attestation services at runtime, ensuring the system's integrity and authenticity. It also manages power and clock control, enabling features such as dynamic power scaling, frequency throttling, and clock gating to optimize performance and efficiency. Moreover, it may potentially continuously monitor the system's physical integrity through various sensors and anti-tampering mechanisms, and also detect various errors and report them through the *RISC-V RAS Error-record Register Interface (RERI)*. Security updates are enforced through signature verification and a secure boot image update mechanism, guaranteeing that firmware modifications adhere to strict authenticity requirements. The System Management Domain also plays a crucial role in memory initialization and physical memory isolation enforcement, leveraging the upcoming *RISC-V I/O Physical Memory Protection (I/O PMP)* specification, to regulate hardware-level device access and protect critical system resources.

The **Main CPU Cluster** subsystem serves as the high-performance compute domain, built around a RISC-V CPU cluster compliant with the RVA23 profile, augmented with upcoming extensions to enhance system capabilities. This subsystem integrates high-speed peripherals, such as NVMe storage, networking and other PCIe devices, ensuring efficient data transfer and resource utilization. A key feature of this security domain is its ability to host multiple supervisor domains, allowing for the secure virtualization of workloads through the *RISC-V Hypervisor extension*, *Advanced Interrupt Architecture (AIA)*, and *I/O MMU*. To further strengthen system security, it incorporates *Confidential Virtualization Extensions (CoVE and CoVE I/O)* [4], which provide hardware-enforced guarantees of confidential computing and extend trust to both virtualized environments and connected peripherals. A

fundamental component of this design is the *Memory Tracking Table (MTT)*, which enforces physical memory isolation between supervisor domains. Much like an MMU isolates virtual memory between processes, MTT ensures that each supervisor domain can only access its allocated physical memory regions, with requests filtered accordingly. This mechanism extends beyond the CPU to peripherals through the *I/O MTT Checker*, which operates along the I/O MMU to further enforce fine-grained, scalable access control across virtualized domains. A software framework built on top of MTT and I/O MTT, provides confidential execution guarantees by ensuring that only authorized entities can access sensitive workloads and data. *CoVE I/O* plays a crucial role in verifying the authenticity of PCIe peripherals, ensuring that only trusted devices can interact with the system. This prevents attackers from introducing malicious peripherals, that could otherwise compromise system integrity.

Since this is a server platform aimed at cloud services, availability requirements are taken into account as well. For this purpose, the reference design leverages the recently ratified RISC-V Capacity and Bandwidth QoS Register Interface (CBQRI) specification.

Other extensions, both ISA and non-ISA (such as software-related specifications) have also been considered, although not covered in detail in this poster. The goal is to give an overview so that the audience understands the big picture on where we are in terms of feature maturity of RISC-V, and where we are headed, in the context of OCP server systems.

## Concluding Remarks

By leveraging open-standard security mechanisms and a modular architecture, this platform 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. Our team, with direct contributions to RISC-V security extensions, IOMMU specifications, and multiple SoC integration projects, will be sharing insights into developing a fully open, scalable, and secure RISC-V server platform, highlighting the benefits of open-source hardware and software in ensuring trust and long-term technological sovereignty.

## Acknowledgement

The HIGHER project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement Nr. 101189612.

## References

[1] The HIGHER Project: https://higher-project.eu
[2] The Open Compute Project: https://www.opencompute.org
[3] Caliptra Root of Trust Module: https://github.com/chipsalliance/Caliptra
[4] Ravi Sahita, Vedvyas Shanbhogue, Andrew Bresticker, Atul Khare, Atish Patra, Samuel Ortiz, Dylan Reid, and Rajnesh Kanwal. 2023. CoVE: Towards Confidential Computing on RISC-V Platforms. In Proceedings of the 20th ACM International Conference on Computing Frontiers (CF '23). Association for Computing Machinery, New York, NY, USA, 315–321. https://doi.org/10.1145/3587135.3592168