

SPMP for All Layers: A RISC-V Full-Stack PoC

Manuel Rodríguez ⁽¹⁾

Luís Cunha ⁽¹⁾

José Martins ⁽²⁾

Sandro Pinto ⁽¹⁾

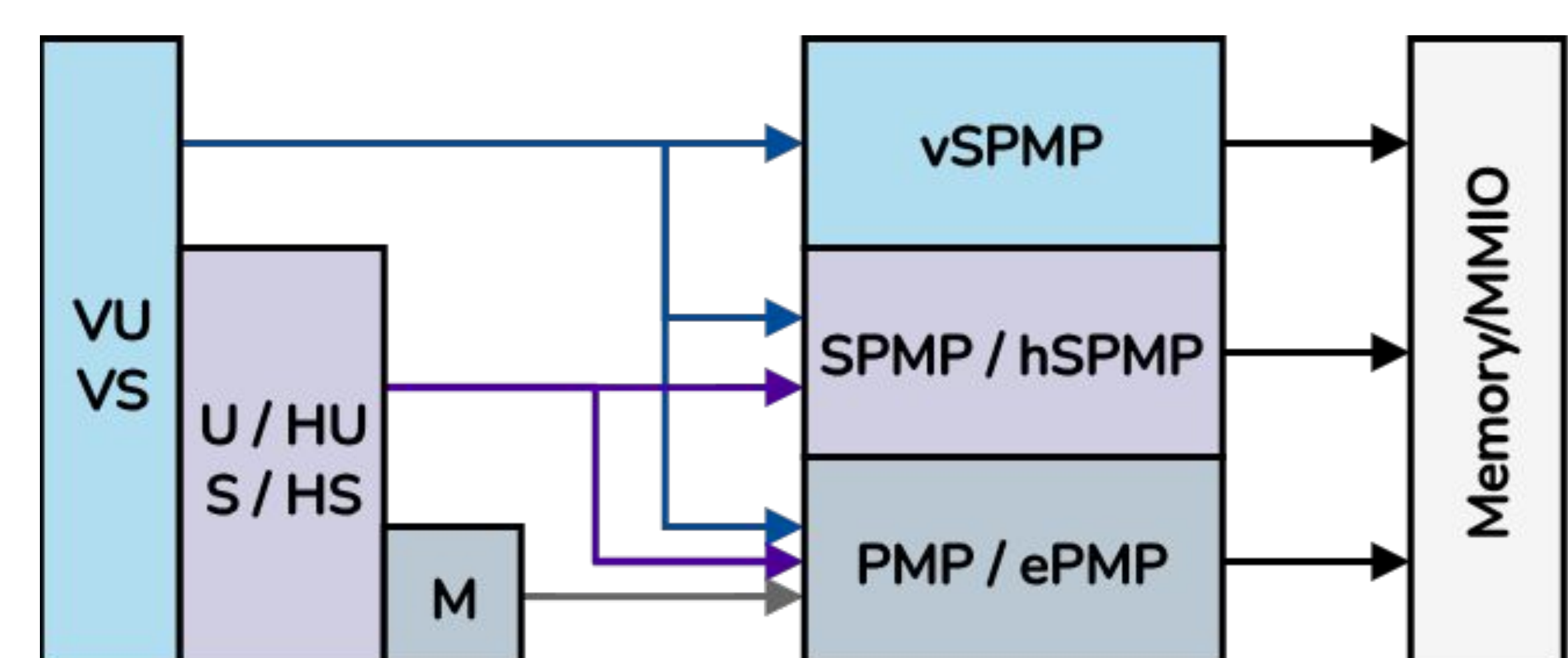
⁽¹⁾ Centro ALGORITMI/LASI - Universidade do Minho; ⁽²⁾ OSYX Technologies

Abstract

Memory protection is critical for secure and predictable computing, especially in real-time systems. While RISC-V offers isolation through PMP and MMU-based mechanisms, the undeterminism introduced by virtual memory makes MMUs unsuitable for time-sensitive applications. To address this, the RISC-V community is ratifying the Supervisor-mode PMP (SPMP) as a lightweight, PMP-like mechanism for S-mode, along with a dual-stage SPMP version to enable virtualization in MMU-less systems. In this work, we present a comprehensive set of proof-of-concept (PoC) artifacts spanning the hardware, emulation, and software layers, demonstrating how the SPMP can enable secure, MMU-less isolation across the RISC-V stack. These contributions aim to support the ongoing ratification process, and will be open-sourced to benefit the broader RISC-V ecosystem.

RISC-V Supervisor Physical Memory Protection (SPMP)

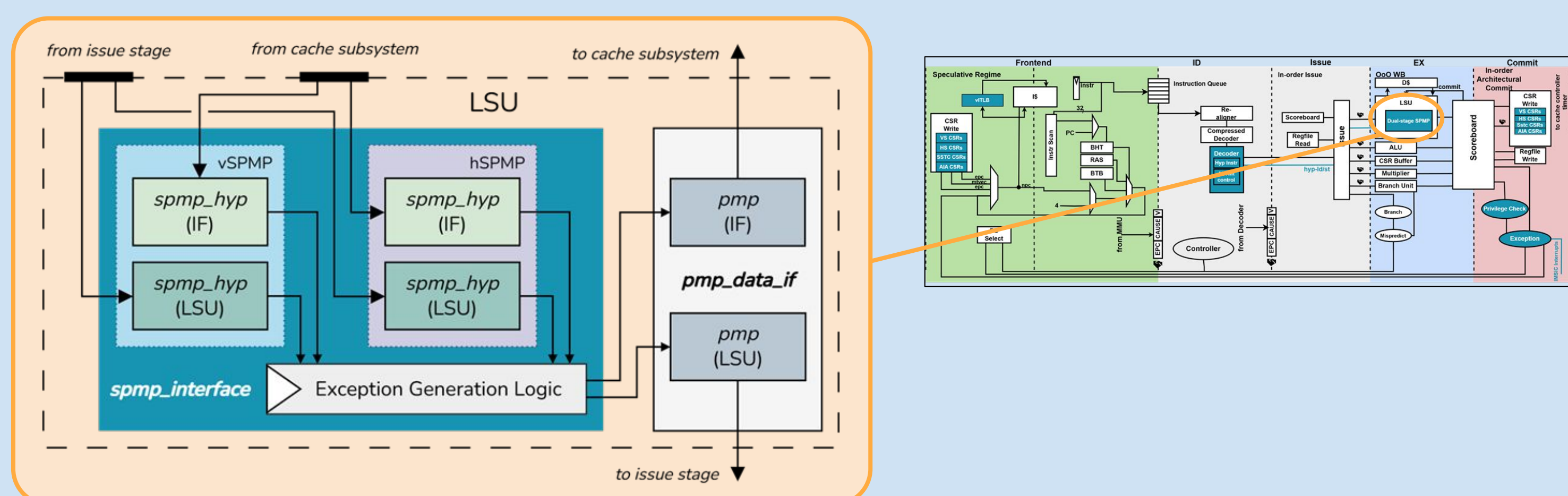
- **SPMP** → Isolates **S-mode** Oses (e.g., RTOS) and **U-mode** apps
 - Similar to M-mode PMP, but with **S-mode** and **U-mode** rules
- **SPMP for Hypervisor** → Dual-stage SPMP
 - Single **unified** SPMP controlled by **HS-mode**: **hSPMP**
 - Isolates hypervisor (**HS-mode**) accesses from VM accesses (**VS/VU**)
 - Virtual SPMP controlled by **VS-mode**: **vSPMP**
 - Isolates guest Oses (**VS-mode**) from **VU-mode** apps



Towards SPMP Ratification: Proof-of-Concept Artifacts

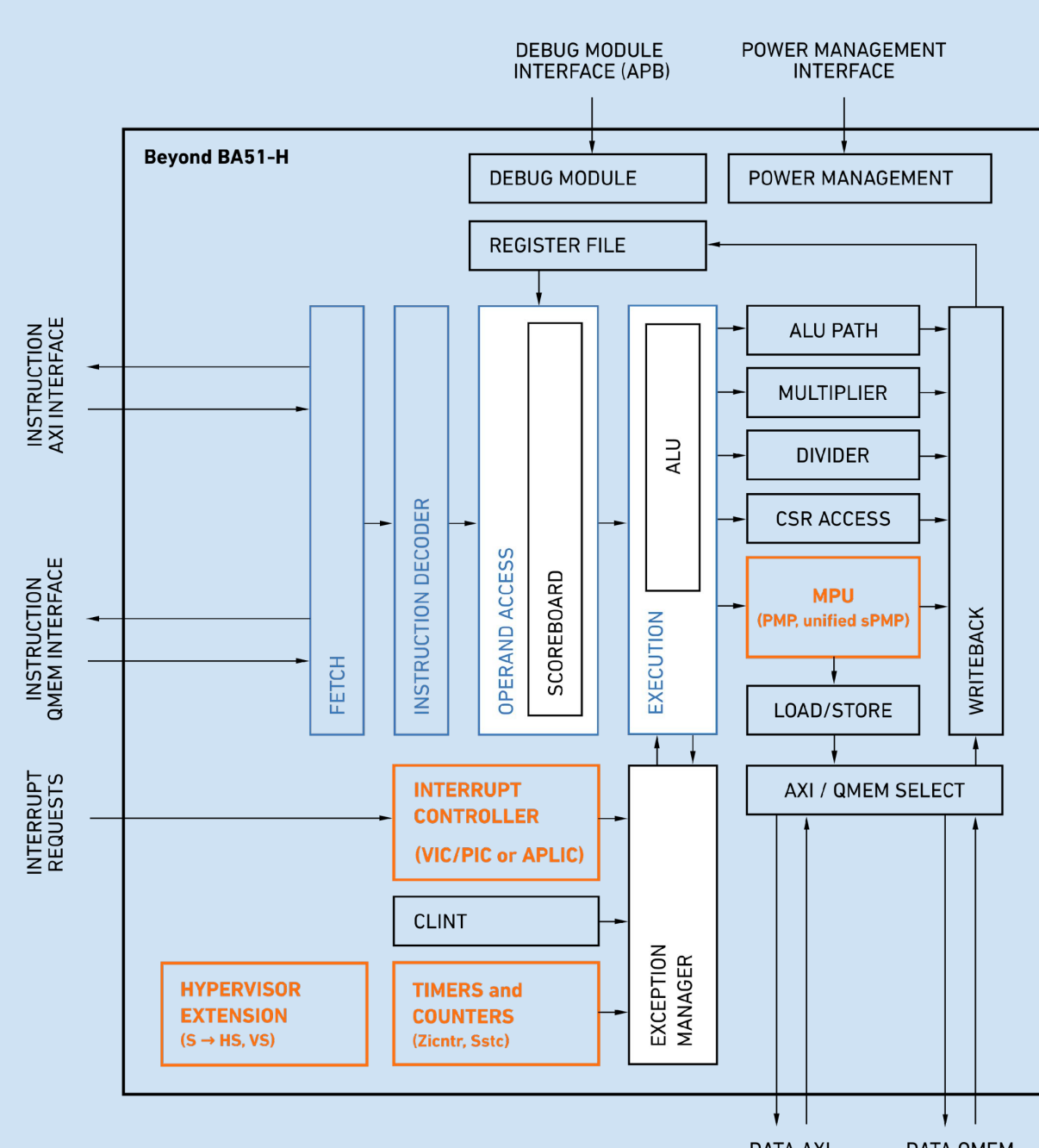
CVA6

- Hardware Baseline → CVA6 release 5.2.0
 - RV64IMAFDCH
- **SPMP + SPMP for Hypervisor** integrated within the LSU
 - Dedicated dual-stage SPMPs for IF and LS requests
 - **Parameterizable** SPMP/MMU instantiation and N of entries
 - Fully combinatorial **address matching logic**



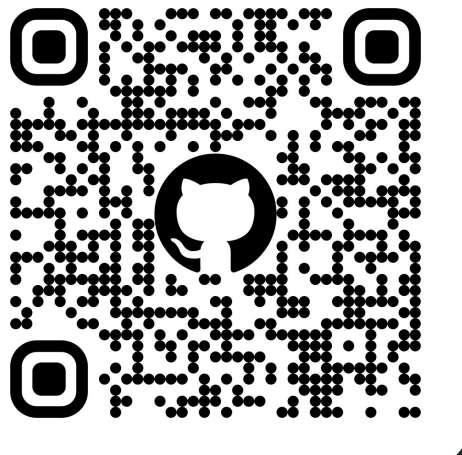
Beyond Semiconductor BA51-H

- First RISC-V MCU with Hypervisor + **Sspmp**
 - RV32IMAFCH
 - Sstc extension
 - APLIC
- Target **applications**
 - Secure AI
 - Automotive (e.g., zonal controllers)



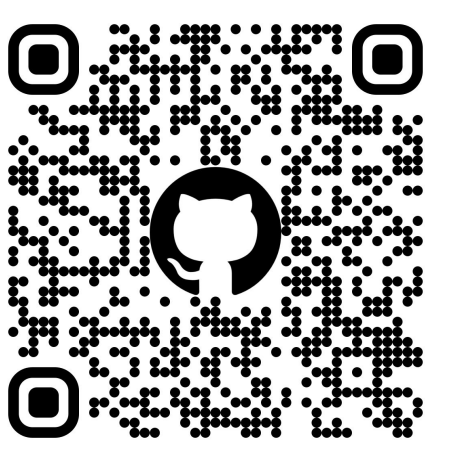
Spike

- Used as reference execution environment for BA51-H
 - rv32imafch_pmp_sstc_zc_zicntr
 - Extended to support SPMP for Hypervisor



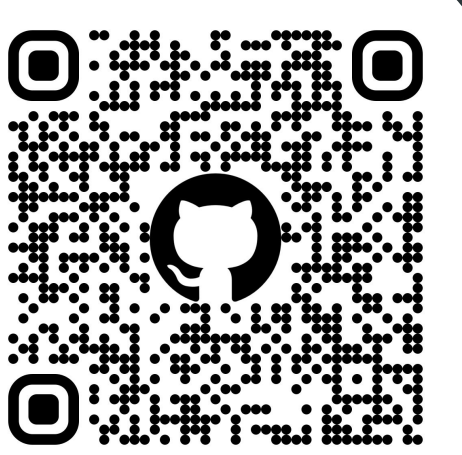
QEMU (10.0.0-rc4)

- Machine & userspace emulator and virtualizer
 - Extended with SPMP v0.9.10
 - Indirect CSR access support
 - Support for the SPMP for Hypervisor is WiP



Zephyr OS (v4.1)

- Lightweight RTOS designed for embedded platforms
 - Modified to run in S-mode, extended with SPMP
- Used to evaluate different SPMP CSR indirect access schemes when context-switching



Bao hypervisor

- Open-source hypervisor for mixed-criticality systems
 - Strong isolation, real-time guarantees
 - Reference in RISC-V
 - Extended to support SPMP for Hypervisor
- Two-layer MPU/PMP design (vMPU/pMPU)

