CROSSCON Novel TEE for Next Generation RISC-V MCUs

Matjaž Breskvar, Beyond Semiconductor
Sandro Pinto, University of Minho

CROSSCON & (secure) Friends
RSC-V Summit EU 2024 - Side Event 1

RISC-V Summit EU 2024
24-28, June 2024, Munich, Germany

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537

Agenda

01 **Introduction**
Security, TEEs, and RISC-V MCU Gap

02 **Use Cases Motivation**
Secure AI at the Edge and Domain/Zonal Controllers

03 **Design & Implementation**
Background, Spike, BA51-H, and Bao

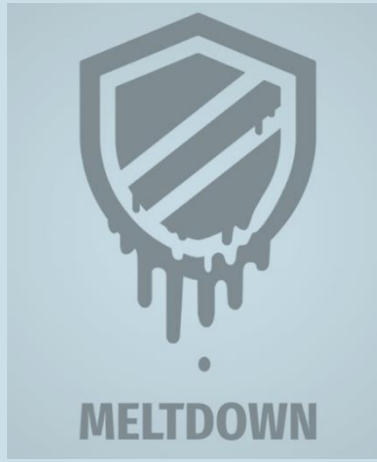
04 **Validation and Evaluation**
Hardware Resources and TCB Size

05 **Conclusion**
Roadmap and Next steps

Introduction

Security, TEEs, and RISC-V MCU Gap

Security is paramount
for the
Internet of Things (IoT)



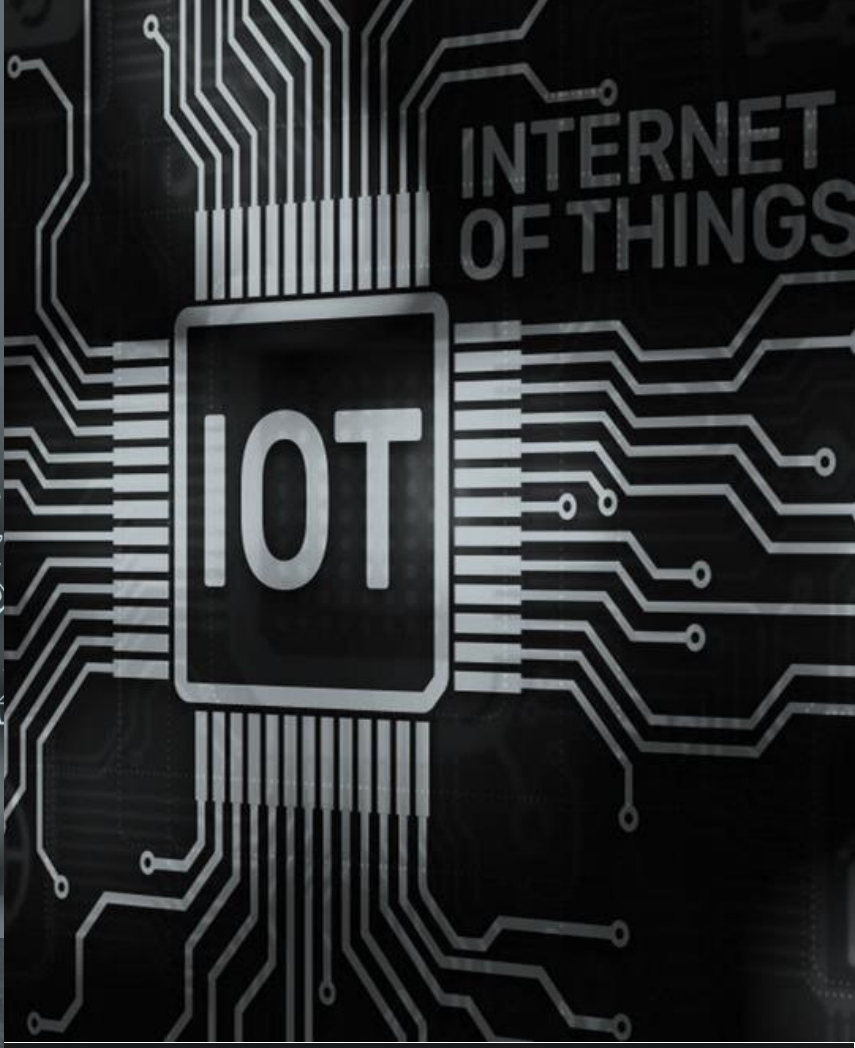
“We are witnessing cyberattacks on **critical** infrastructure, health services systems captured and **held to ransom** and home electronics devices used as **internet gateways** by **hackers**.”

arm, in Security Manifesto, 2017.

arm

TECHNOLOGIES

TRUSTZONE FOR CORTEX-A



intel

SGX

Tool

arm

TECHNOLOGIES

TRUSTZONE FOR CORTEX-M


RISC-V

RISC-V MCU TEE

IoT-based devices requirements

- Connectivity (e.g WiFi, Bluetooh, ZigBee)
- Upgradability (e.g. firmware, features, security)
- Sensitive information (e.g. keys, certificates)

RISC-V TEE for MCU

- No RISC-V TEE MCU related spec
- Existing solutions have limitations (performance & power)
- Evolving ecosystem

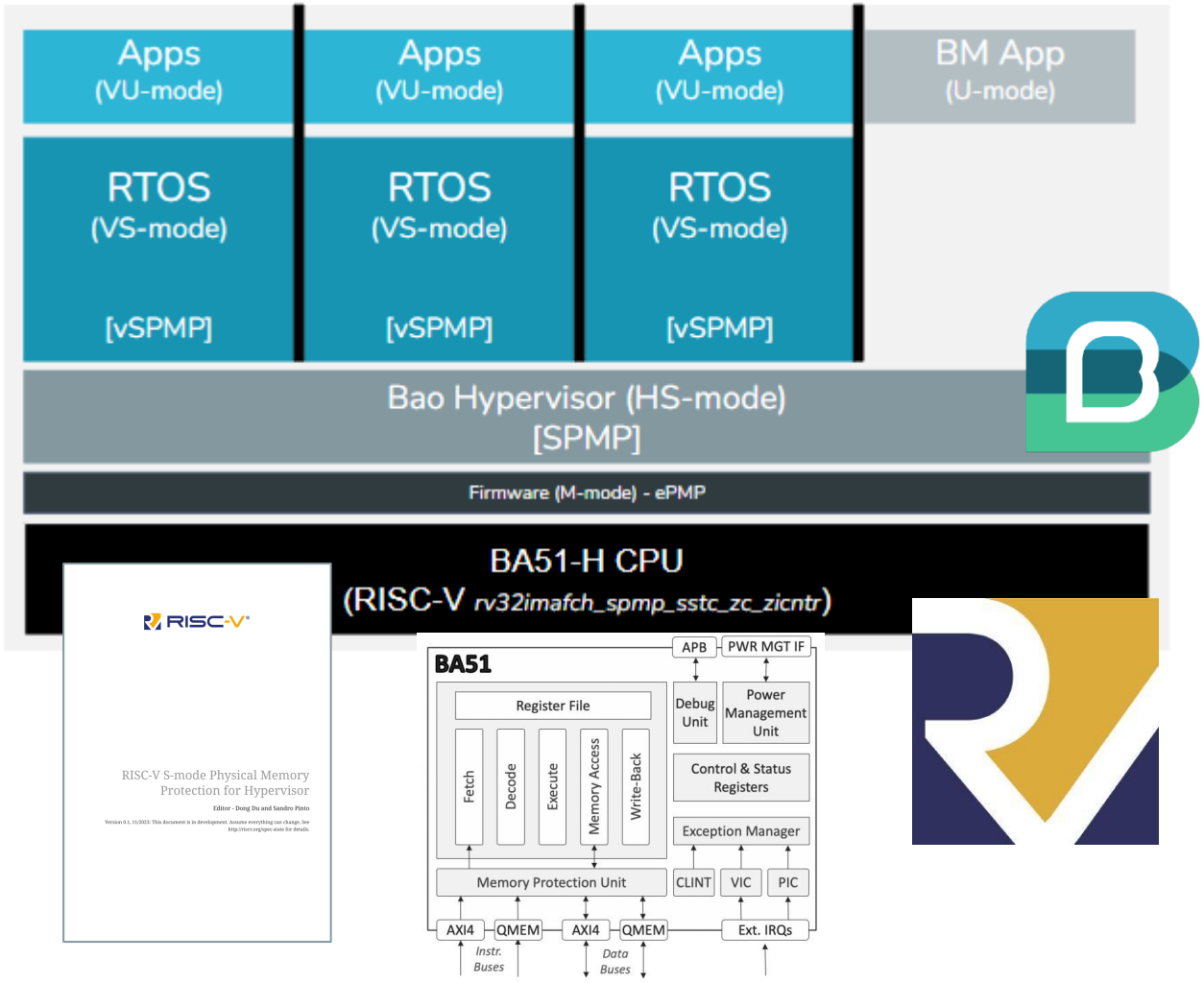
Isolate! TEE to the rescue

- Hardware-enforced Isolation
- Separate execution environment
- Multiple protection models

Can devs do something?

Contribution: Novel TEE for RISC-V MCU

- **Central Novelty**
  - Virtualization-based TEE
  - SPMP with Hypervisor support
- **Implementation and Artifacts**
  - SPMP for Hypervisor Spec
  - Spike (SPMP for Hypervisor) Model
  - BA51-H MCU
  - Bao SPMP-H port



Use Cases Motivation

Secure AI at the Edge and Domain/Zonal Controllers

WHITE PAPER

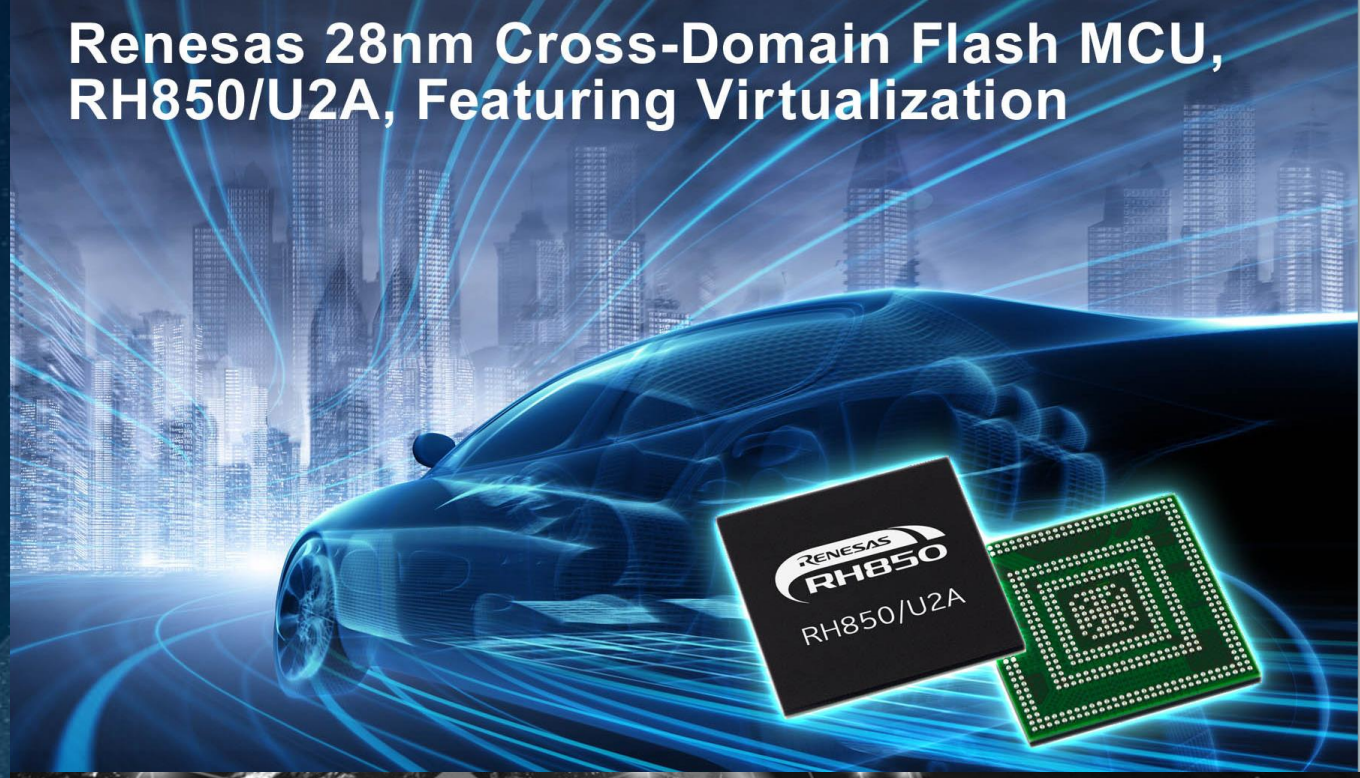
arm

ETAS

Best Practices for Armv8-R Cortex-R52+ Software Consolidation

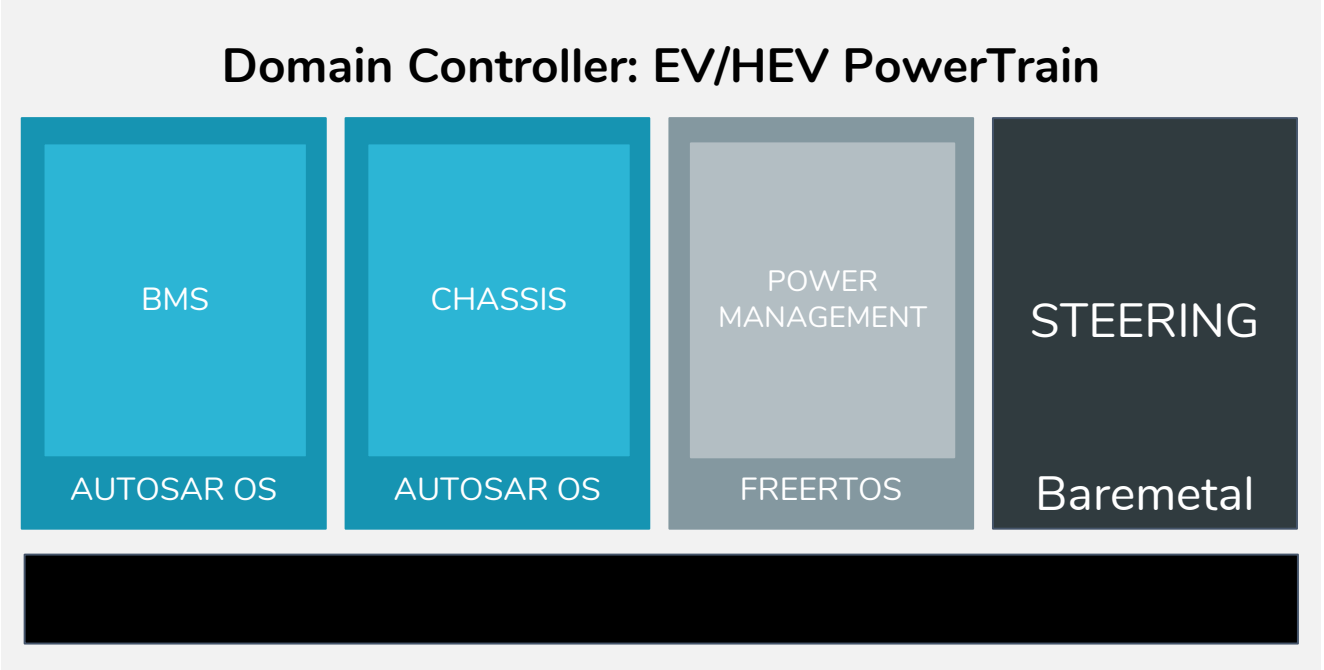
Dr Paul Austin, Principal Software Engineer, ETAS
Dr Andrew Coombes, Senior Product Manager, ETAS
Paul Hughes, Lead System Architect and Distinguished Engineer ATG, Arm
James Scobie, Director Automotive Product Management, Arm
Bernhard Rill, Director Automotive Partnerships EMEA, Arm

Renesas 28nm Cross-Domain Flash MCU, RH850/U2A, Featuring Virtualization



Use Cases: Automotive Domain/Zonal Controllers

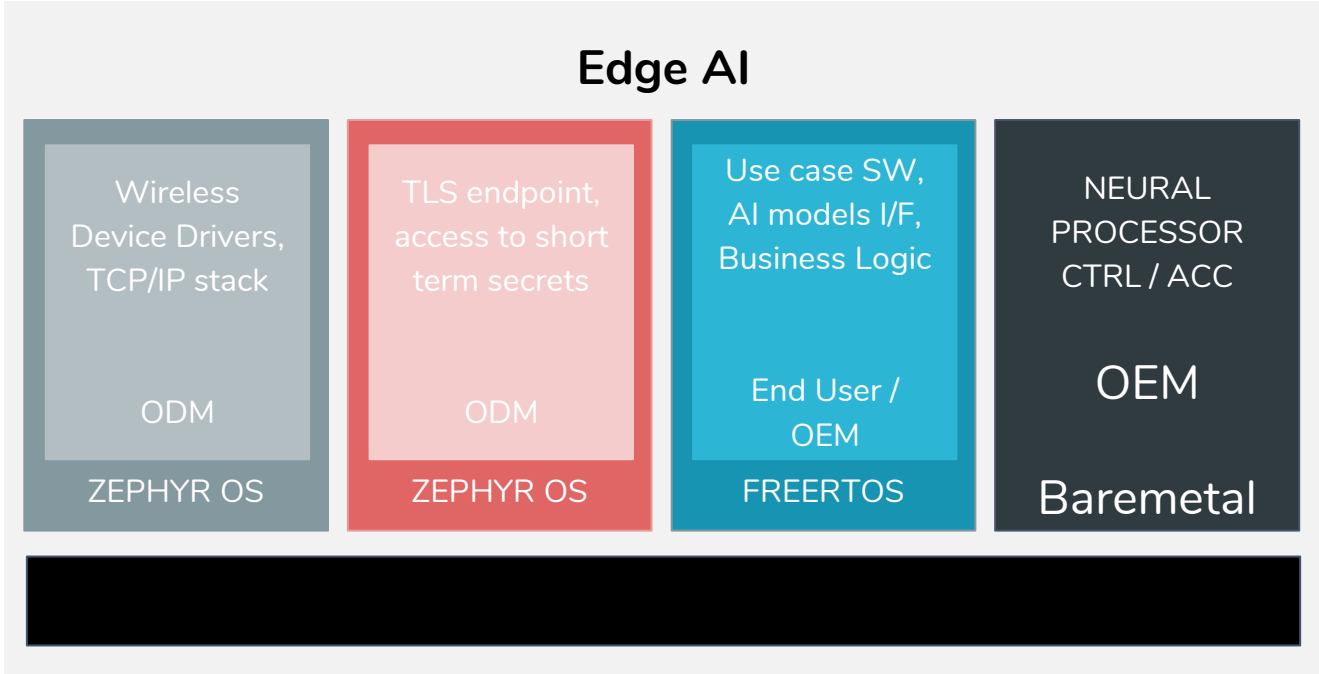
- **ECU consolidation:**
  - Reduce complexity and cost
  - Safety - ISO26262 (FFI)
  - High-performance
  - Real-time (Predictability)
- **EV/HEV PowerTrain*:**
  - ***Battery Management System (BMS)***
  - ***Chassis Control***
  - ***Power Management (DC/DC Inverter)***
  - ***Steering Control***
  - Model Predictive Control (MPC)
  - Thermal Monitoring
  - …



* Inspired from: https://community.nxp.com/t5/Blog/GreenBox-3-Safe-Multi-ECU-Consolidation-Demo/ba-p/1580941

Use Cases: Secure AI at the edge

- **Separation for Security/Resilience:**
  - Reduce complexity and cost
  - Consolidation while avoiding Security issues
  - End-User SW support
  - Real-time Operation
- **End User / OEM:**
  - ***Simple use of ODM maintained on-chip services (e.g. Secure Channel to cloud)***
  - ***Transparent software sandbox with software adjustable/assignable resources***
  - ***Control / acceleration of on-chip AI (pre)processing, offload to cloud***



Design & Implementation

Background, Spike, BA51-H, and Bao

MMU

Memory Management Unit

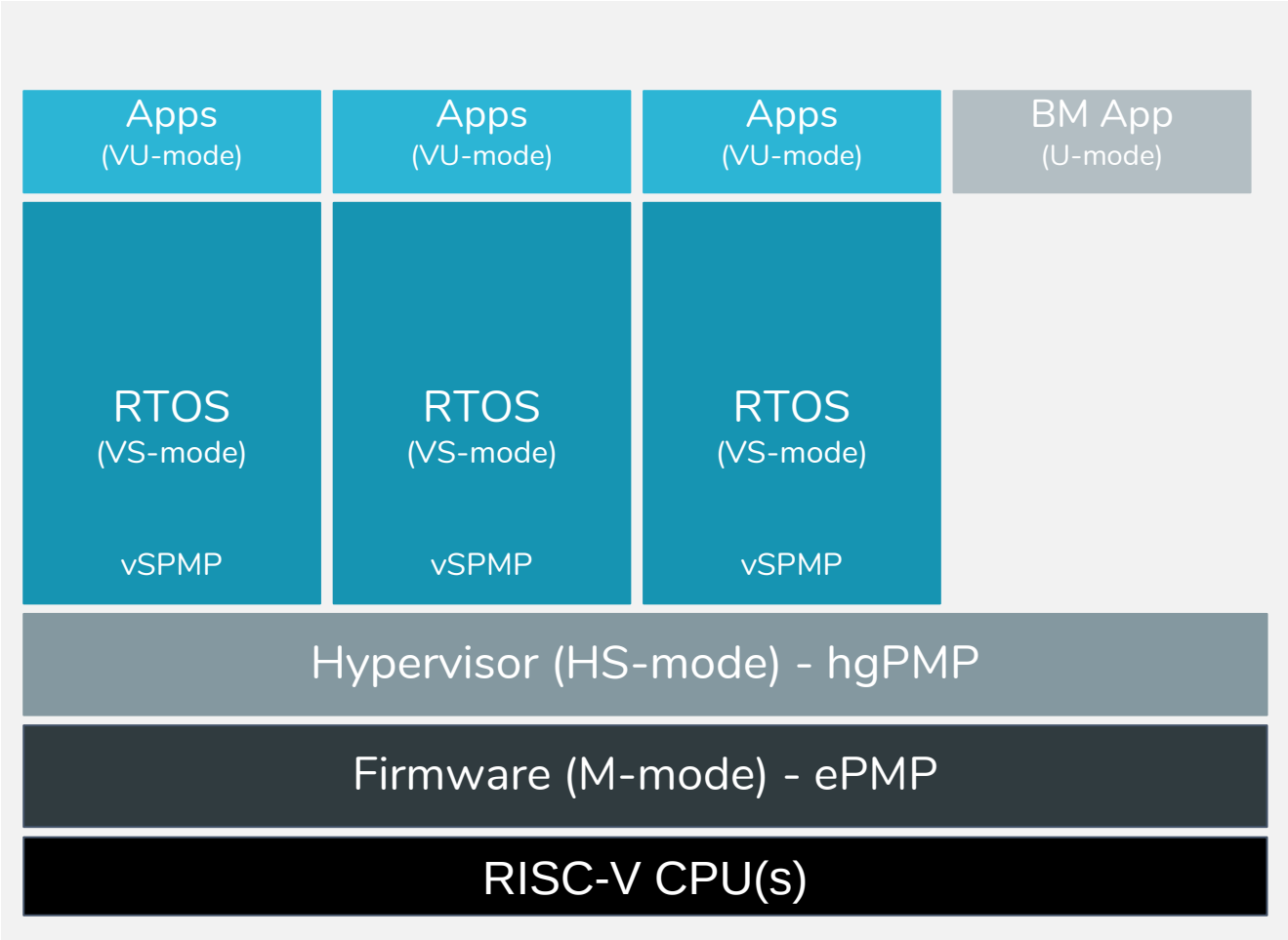
- Translation
- Protection
- Flexibility

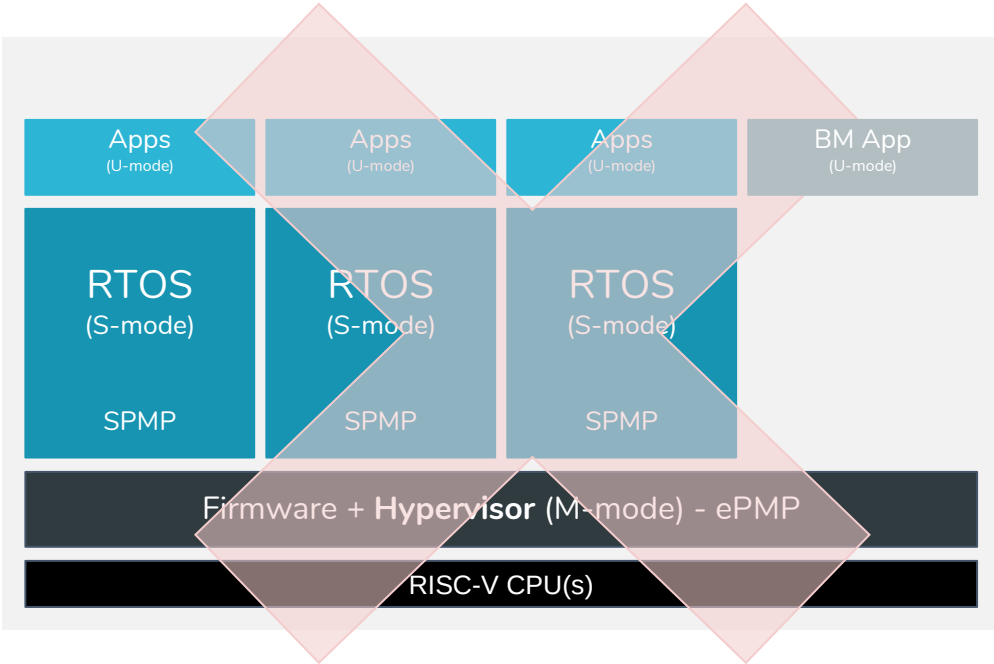
PMP

Physical Memory Protection

- Protection
- Predictability
- Simplicity

RISC-V TEE MCU-H Architecture

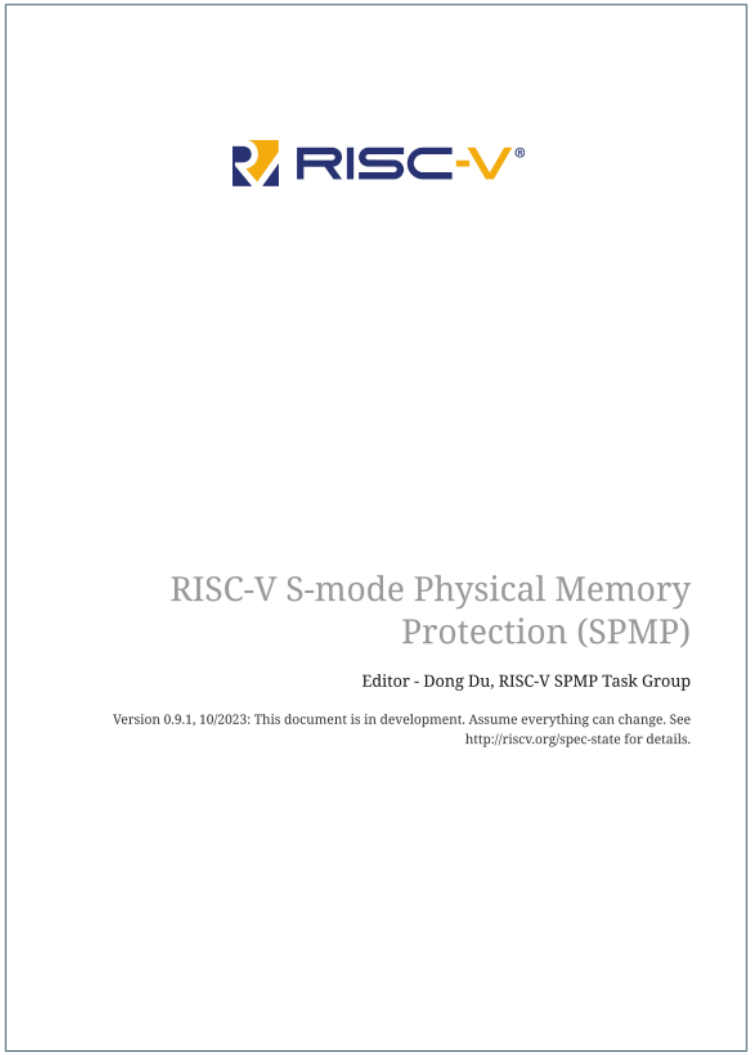




Disadvantages:

- Hypervisor portability
- Firmware Reuse
- No platform-level domains

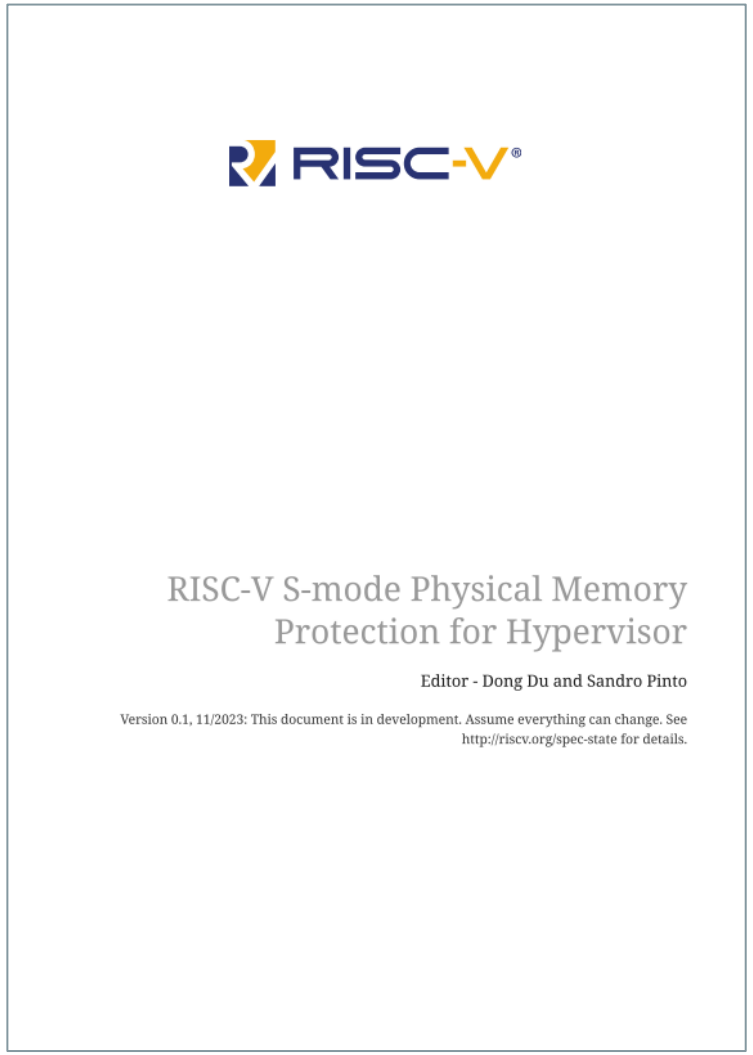
RISC-V SPMP (for Hypervisor)



RISC-V S-mode Physical Memory Protection (SPMP)

Editor - Dong Du, RISC-V SPMP Task Group

Version 0.9.1, 10/2023: This document is in development. Assume everything can change. See http://riscv.org/spec-state for details.

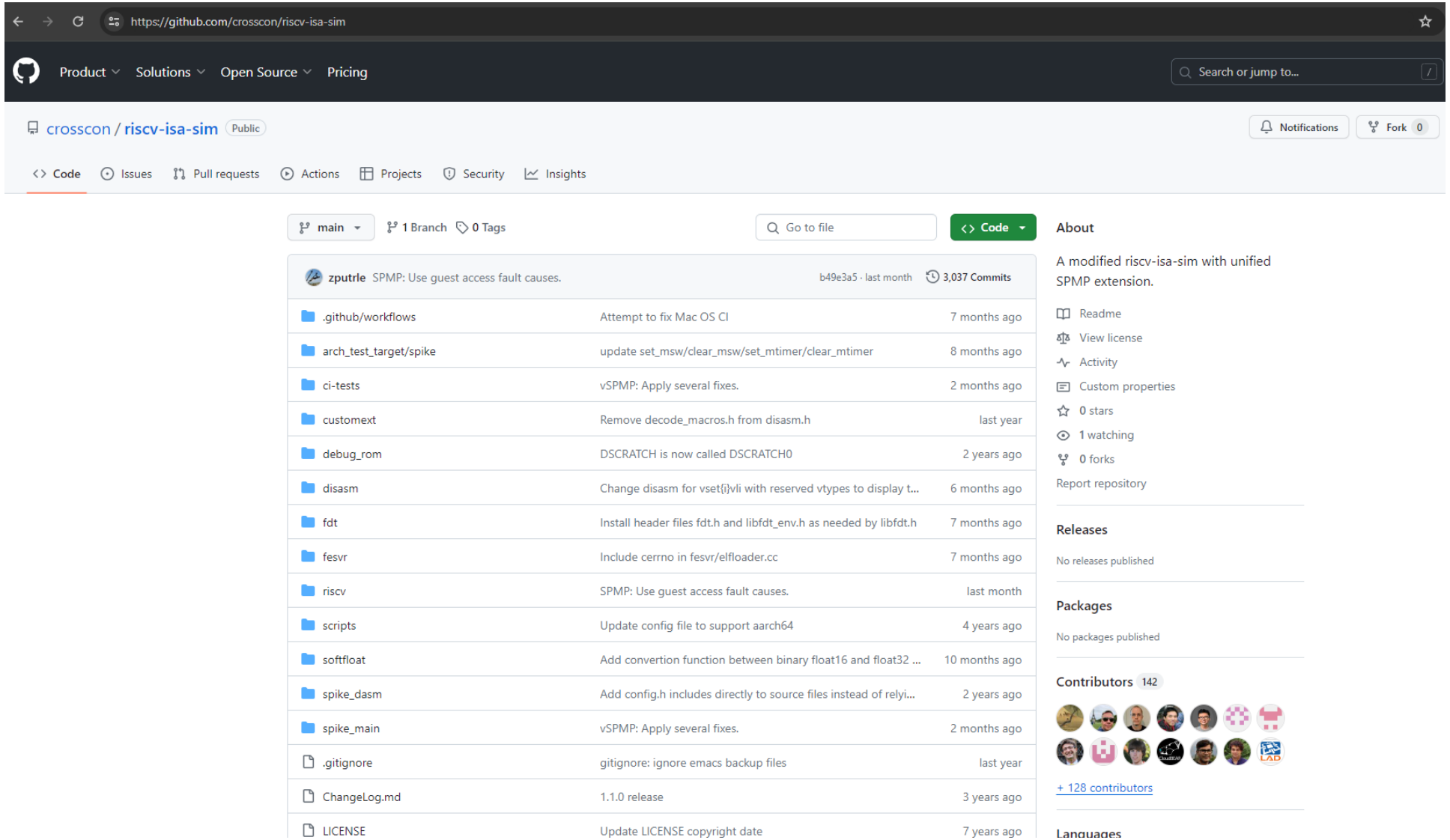


RISC-V S-mode Physical Memory Protection for Hypervisor

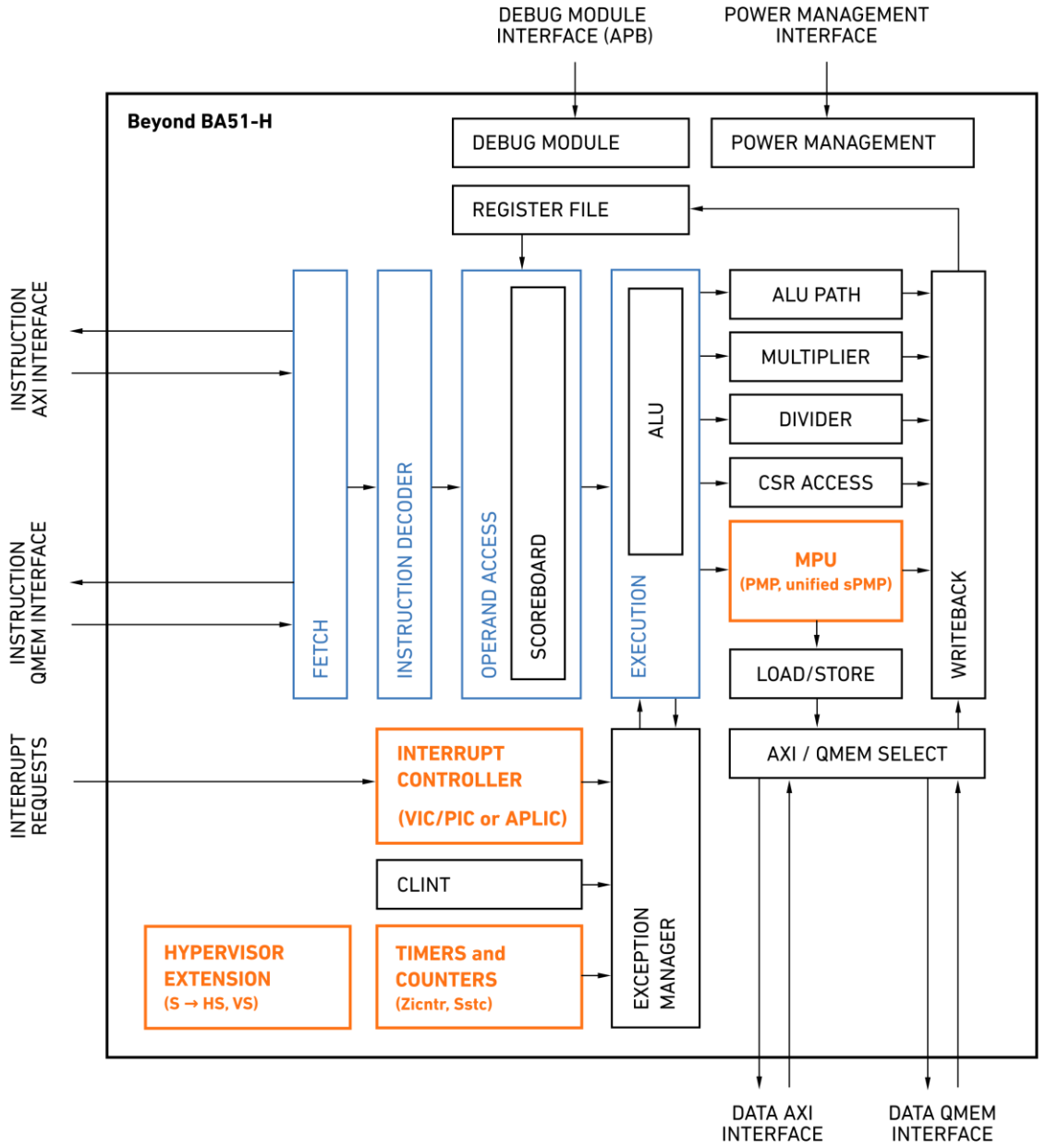
Editor - Dong Du and Sandro Pinto

Version 0.1, 11/2023: This document is in development. Assume everything can change. See http://riscv.org/spec-state for details.

RISC-V Spike SPMP for Hypervisor



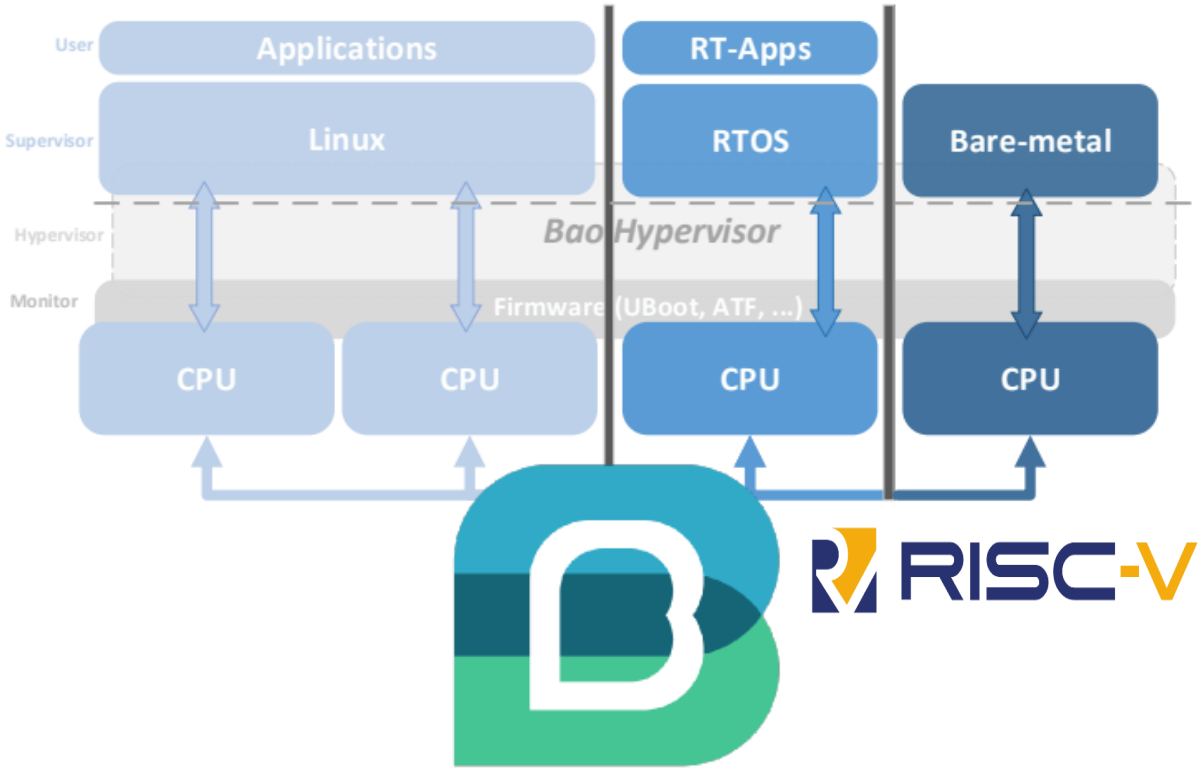
Beyond BA51-H



- **RISC-V RV32IMAFC**
- **Hypervisor Extension**
- **Unified SPMP extension:**
  - Adds support for the supervisor mode physical memory protection;
- **Zc Extension:**
  - Reduces the code size by adding to the 16-bit instruction set;
- **Sstc Extension:**
  - Timer services in supervisor mode;
- **Advanced Platform-Level Interrupt Controller (APLIC):**
  - Interrupt delegation;

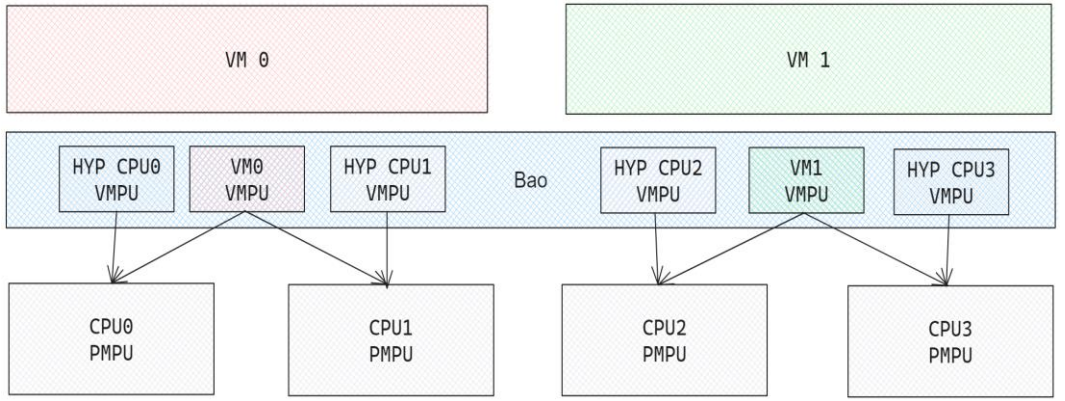
Bao Hypevisor

- **Type-1 / Bare-metal**
- **Static Partitioning Architecture:**
  - 1:1 vCPU-to-pCPU mapping
  - Static memory assignment
- **Hardware-assisted**
- **Inter-VM communication**
- **Real-Time & Predictability**
- **No Dependencies (libraries / OS)**
- **RISC-V and Armv8-A ISA**



Bao RISC-V: SPMP Hypervisor

- **Two-layer MPU/PMP Design**
  - Top Layer - Architecture-independent (VMPU)
  - Bottom Layer - Architecture-dependent (PMPU)
- **Advantages of such Design**
  - Agnostic memory management
  - Agnostic policy-checks
  - Optimized PMP entry management



- **RISC-V SPMP Limitation**
  - No shared regions between hypervisor and guest
  - Bao does not use shared permissions -> duplicated regions (flipped mode bit)

Validation and Evaluation

Hardware Resources and TCB Size

Bao @ Spike Validation

```
OpenSBI v1.4-31-g322b598

Platform Name             : ucbbar,spike-bare
Platform Features         : medeleg
Platform HART Count       : 1
Platform IPI Device       : aclint-mswi
Platform Timer Device     : aclint-mtimer @ 10000000Hz
Platform Console Device   : uart8250
Platform HSM Device       : ---
Platform PMU Device       : ---
Platform Reboot Device    : htif
Platform Shutdown Device  : htif
Platform Suspend Device   : ---
Platform CPPC Device      : ---
Firmware Base             : 0x80000000
Firmware Size             : 315 KB
Firmware RW Offset        : 0x40000
Firmware RW Size          : 59 KB
Firmware Heap Offset      : 0x46000
Firmware Heap Size        : 35 KB (total), 2 KB (reserved), 9 KB (used), 23 KB (
free)
Firmware Scratch Size     : 4096 B (total), 188 B (used), 3908 B (free)
Runtime SBI Version       : 2.0

Domain0 Name              : root
Domain0 Boot HART         : 0
Domain0 HARTs             : 0*
Domain0 Region00          : 0x10000000-0x10000fff M: (I,R,W) S/U: (R,W)
Domain0 Region01          : 0x80040000-0x8004ffff M: (R,W) S/U: ()
Domain0 Region02          : 0x02080000-0x020bffff M: (I,R,W) S/U: ()
Domain0 Region03          : 0x80000000-0x8003ffff M: (R,X) S/U: ()
Domain0 Region04          : 0x02000000-0x0207ffff M: (I,R,W) S/U: ()
Domain0 Region05          : 0x0c000000-0x0cffffff M: (I,R,W) S/U: (R,W)
Domain0 Region06          : 0x00000000-0xffffffff M: () S/U: (R,W,X)
Domain0 Next Address      : 0x80400000
Domain0 Next Arg1         : 0x82200000
Domain0 Next Mode         : S-mode
Domain0 SysReset          : yes

Boot HART ID              : 0
Boot HART Domain          : root
Boot HART Priv Version    : v1.12
Boot HART Base ISA        : rv32imafdch
Boot HART ISA Extensions  : sstc,zicntr,zihpm,sdtrig
Boot HART PMP Count       : 16
Boot HART PMP Granularity : 2 bits
Boot HART PMP Address Bits: 32
Boot HART MHPM Info       : 0 (0x00000000)
Boot HART Debug Triggers  : 4 triggers
Boot HART MIDELEG         : 0x00001666
Boot HART MEDELEG         : 0x00f0b509
Bao Hypervisor
BAO WARNING: trying to flush caches but the operation is not defined for this p
latform
BAO WARNING: trying to flush caches but the operation is not defined for this p
latform
[guest 0] Bao bare-metal test guest
[guest 0] cpu 0 up
[guest 1] Bao bare-metal test guest
[guest 1] cpu 0 up
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
[guest 0] cpu0: timer_handler
[guest 1] cpu0: timer_handler
```


```
Boot HART ID              : 0
Boot HART Domain          : root
Boot HART Priv Version    : v1.12
Boot HART Base ISA        : rv32imafdch
Boot HART ISA Extensions  : sstc,zicntr,zihpm,sdtrig
Boot HART PMP Count       : 16
Boot HART PMP Granularity : 2 bits
Boot HART PMP Address Bits: 32
Boot HART MHPM Info       : 0 (0x00000000)
Boot HART Debug Triggers  : 4 triggers
Boot HART MIDELEG         : 0x00001666
Boot HART MEDELEG         : 0x00f0b509
Bao Hypervisor
BAO WARNING: trying to flush caches but the operation is not defined for this pl
atform
BAO WARNING: trying to flush caches but the operation is not defined for this pl
atform
[guest 0] Bao bare-metal test guest
[guest 0] cpu 0 up
[guest 1] Bao bare-metal test guest
[guest 1] cpu 0 up
[guest 0] cpu0: timer_handler
```

BA51-H HW Resources

	Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1)	BA51 CC	25,239	100%	5%	12%	3%
(#2)	BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3)	BA51 FRC	206,430	818%	38%	100%	28%
(#4)	BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
	Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
	PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
	PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
	APLIC	1,403	5.6%	0.3%	0.7%	0.2%
	Sstc	904	3.6%	0.2%	0.4%	0.1%
	Zc	1,287	5.1%	0.2%	0.6%	0.2%

8x Area difference between **compact** and **feature rich configuration** of the processor

BA51-H HW Resources

	Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1)	BA51 CC	25,239	100%	5%	12%	3%
(#2)	BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3)	BA51 FRC	206,430	818%	38%	100%	28%
(#4)	BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
	Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
	PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
	PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
	APLIC	1,403	5.6%	0.3%	0.7%	0.2%
	Sstc	904	3.6%	0.2%	0.4%	0.1%
	Zc	1,287	5.1%	0.2%	0.6%	0.2%

SRAM Area dominates

BA51-H HW Resources

	Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1)	BA51 CC	25,239	100%	5%	12%	3%
(#2)	BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3)	BA51 FRC	206,430	818%	38%	100%	28%
(#4)	BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
	Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
	PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
	PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
	APLIC	1,403	5.6%	0.3%	0.7%	0.2%
	Sstc	904	3.6%	0.2%	0.4%	0.1%
	Zc	1,287	5.1%	0.2%	0.6%	0.2%

- PMP is the main area contributor
- 1600 gates per entry for (S)PMP

BA51-H HW Resources

	Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1)	BA51 CC	25,239	100%	5%	12%	3%
(#2)	BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3)	BA51 FRC	206,430	818%	38%	100%	28%
(#4)	BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
	Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
	PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
	PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
	APLIC	1,403	5.6%	0.3%	0.7%	0.2%
	Sstc	904	3.6%	0.2%	0.4%	0.1%
	Zc	1,287	5.1%	0.2%	0.6%	0.2%

S → HS + VS is important area contributor

BA51-H HW Resources

	Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1)	BA51 CC	25,239	100%	5%	12%	3%
(#2)	BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3)	BA51 FRC	206,430	818%	38%	100%	28%
(#4)	BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
	Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
	PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
	PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
	APLIC	1,403	5.6%	0.3%	0.7%	0.2%
	Sstc	904	3.6%	0.2%	0.4%	0.1%
	Zc	1,287	5.1%	0.2%	0.6%	0.2%

Delegation & Zc instructions are **net area gain** due to code size savings

BA51-H HW Resources

	Hardware Logic Functionality	Gates	% of (#1)	% of (#2)	% of (#3)	% of (#4)
(#1)	BA51 CC	25,239	100%	5%	12%	3%
(#2)	BA51 CC + 64 KiB SRAM	549,527	2177%	100%	266%	75%
(#3)	BA51 FRC	206,430	818%	38%	100%	28%
(#4)	BA51 FRC + 64 KiB SRAM	730,718	2895%	133%	354%	100%
	Hypervisor extension	7,685	30.4%	1.4%	3.7%	1.1%
	PMP (16e) + unified SPMP (16e)	51,223	203.0%	9.3%	24.8%	7.0%
	PMP (32e)	50,733	201.0%	9.2%	24.6%	6.9%
	APLIC	1,403	5.6%	0.3%	0.7%	0.2%
	Sstc	904	3.6%	0.2%	0.4%	0.1%
	Zc	1,287	5.1%	0.2%	0.6%	0.2%

Virtualization and Physical Memory Protection hardware (area) cost is easily offset by reduced SRAM overprovisioning and flexibility improvements

Bao RV64 (Application)

Trusted Computing Base

- 6.9 K SLoC
- 31 KiB (.text)

Bao SPMP Hypervisor

Trusted Computing Base

- 6.4 K SLoC
- 29.5 KiB (.text)
- WiP Optimizations

Conclusion

Roadmap and Next steps

Status, Road Ahead

- **Spike reference implementation**
  - unified SPMP and hypervisor extensions
  - available from CROSSCON github
- **Bao initial version**
  - validated in Spike
- **BA51-H implementation**
  - includes all virtualization relevant extensions (for MMU-less processor)
  - unified SPMP and hypervisor extensions
- **RISC-V standardization activities**
  - finalize ongoing standardization efforts
  - memory address translation
- **Bao memory footprint reduction**
  - free unused memory after init,…
- **BA51-H optimizations**
  - hardware support for inter VM communication
  - optimized PMP implementation

THANK YOU!

<matjaz.breskvar@beyondsemi.com>

<sandro.pinto@dei.uminho.pt>

Q&A