The RISC-V Isolation Toolbox

Andy Dellow
Director, Technical Standards
Qualcomm

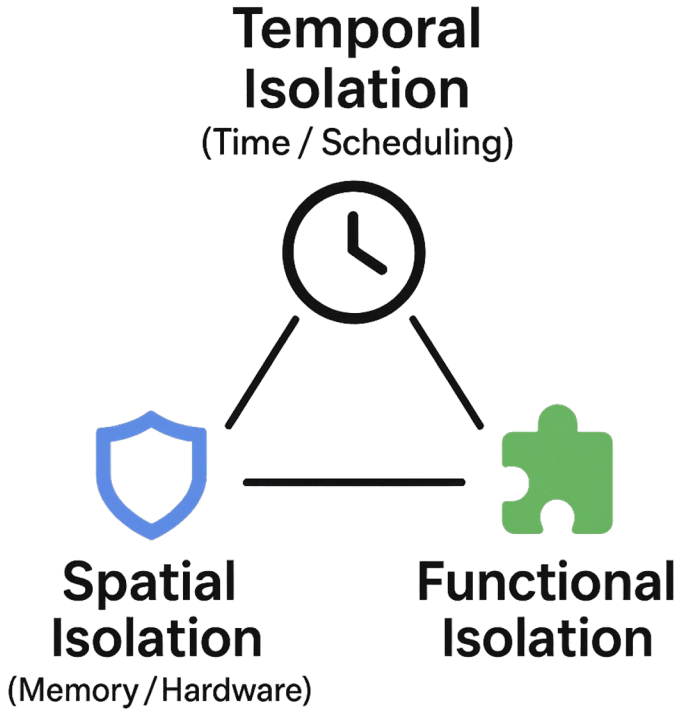
RISC-V®

From Privilege Levels to Composable Domains

- Why isolation?

Isolation

- What do we mean by Isolation ?



MCU → AP → Server

RISC-V®

Historical Foundations

- From temporal beginnings..
- Privilege Rings
  - Hardware enforced isolation
- M/S/U
- ePMP

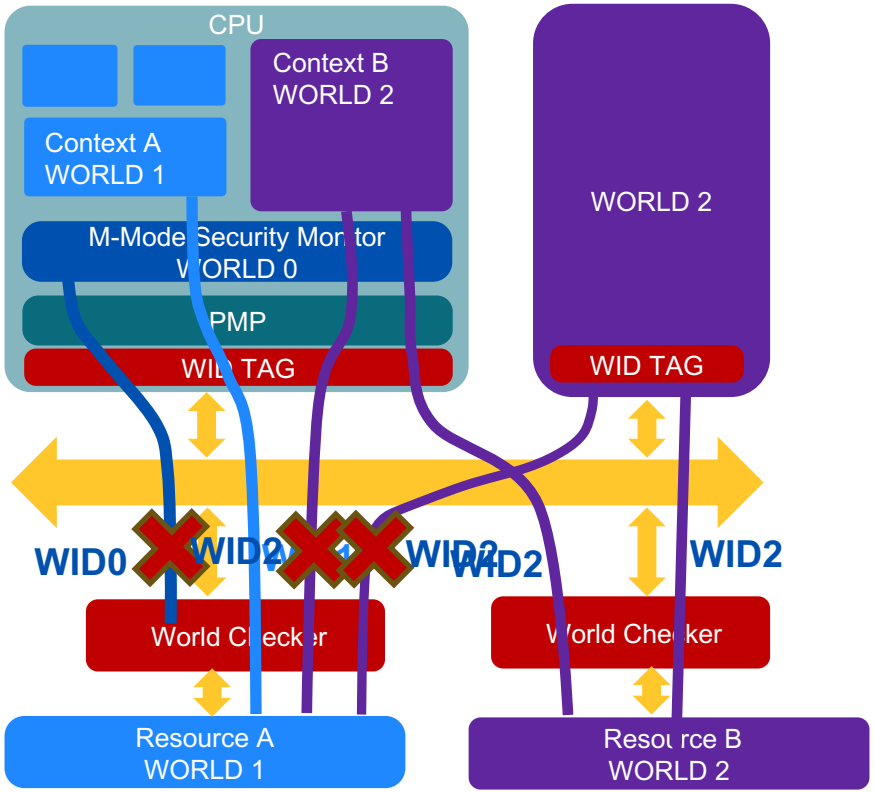
Scaling with Virtual Memory

- Add Address Translation
  - Every page has access permissions
  - Strong spatial isolation
  - Fast and permission checks are free
- Address spaces as isolation units

- Hypervisor Extension
  - HS/VS modes and second-stage translation
  - Isolation between guest Oses

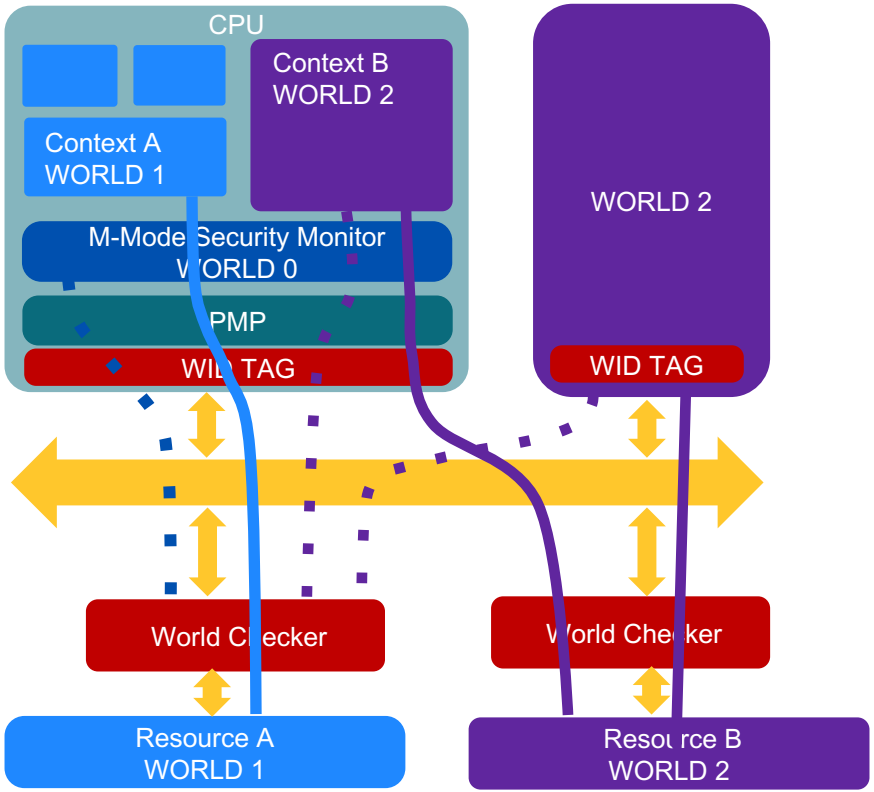
RISC-V Worlds

- Hardware-Enforced Compartmentalization
- World ID
  - Carried with transactions
  - Device Side or Interconnect Filtering
- Notionally static resource allocation



RISC-V Worlds

- Hardware-Enforced Compartmentalization
- World ID
  - Carried with transactions
  - Device Side or Interconnect Filtering
- Notionally static resource allocation



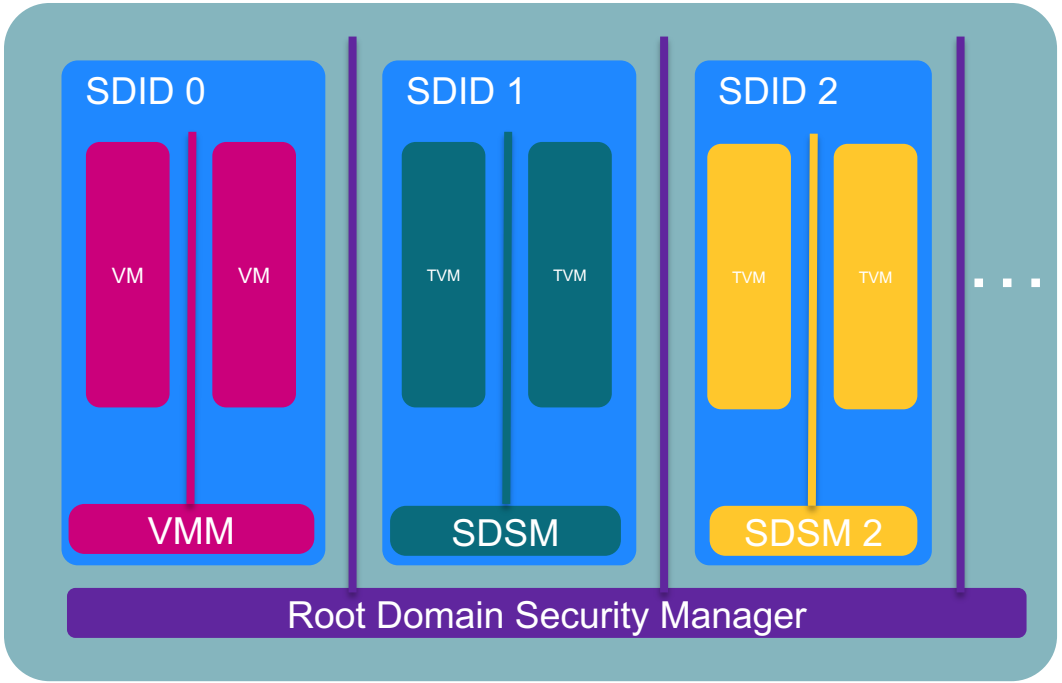
Worlds+

- Watch this space….

Fast Domain Switch – IRQ / Function Call
Lockable Domains – Certified TCB

Supervisor Domains

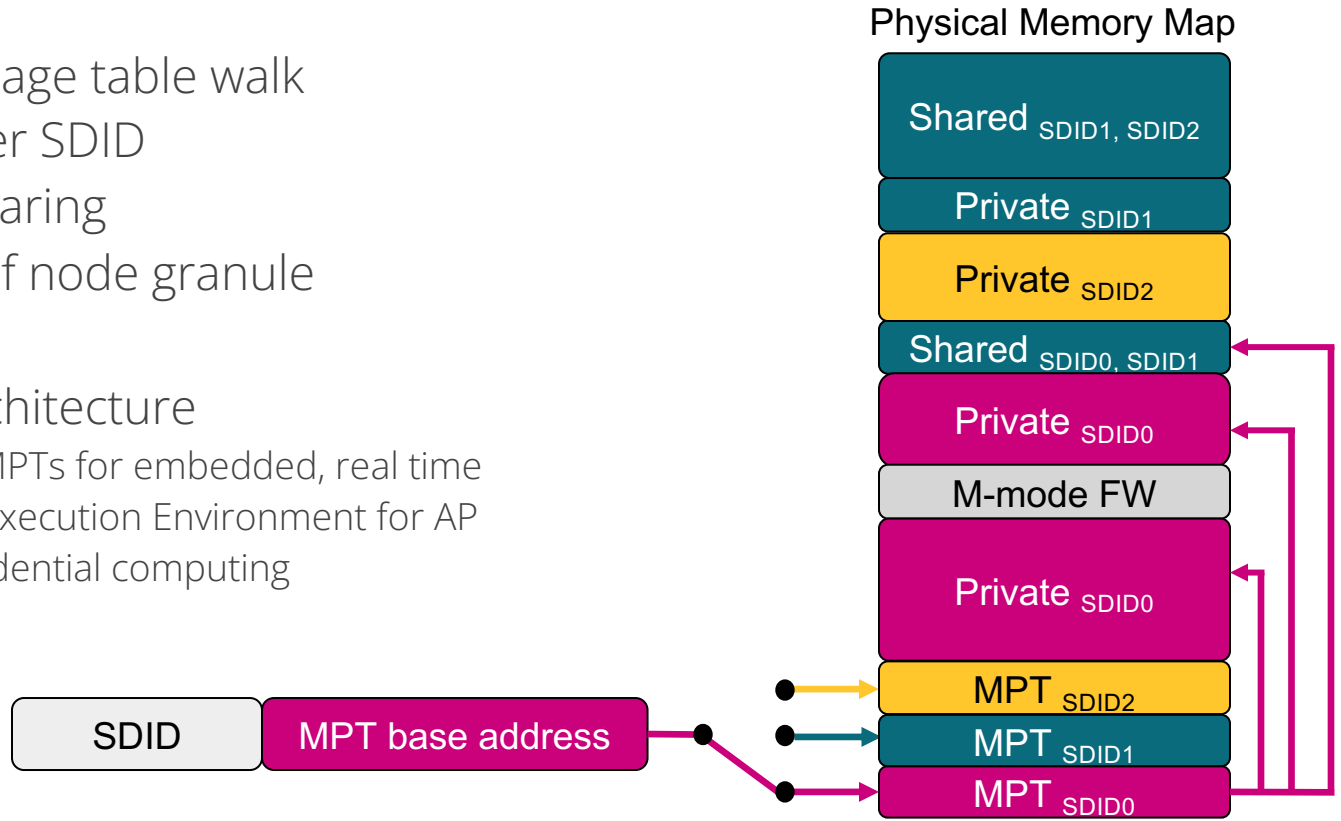
- Scalable Isolated Domains
  - VMM, CC, TEE etc
- Confidential Computing
- Trusted Execution Domains
- Memory Encryption Contexts
- Remote Attestation
- Sealing



Memory Protection Tables

- Additional page table walk
- One MPT per SDID
- Arbitrary Sharing
- RWX per leaf node granule

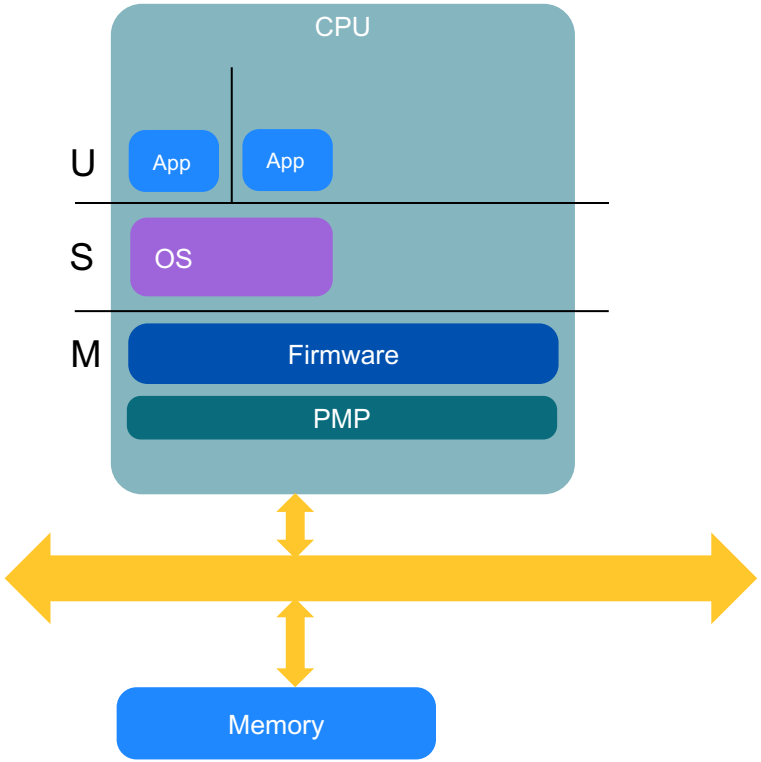
- Scalable Architecture
  - Cached MPTs for embedded, real time
  - Trusted Execution Environment for AP
  - Full confidential computing



RISC-V®

Layering Isolation Mechanisms

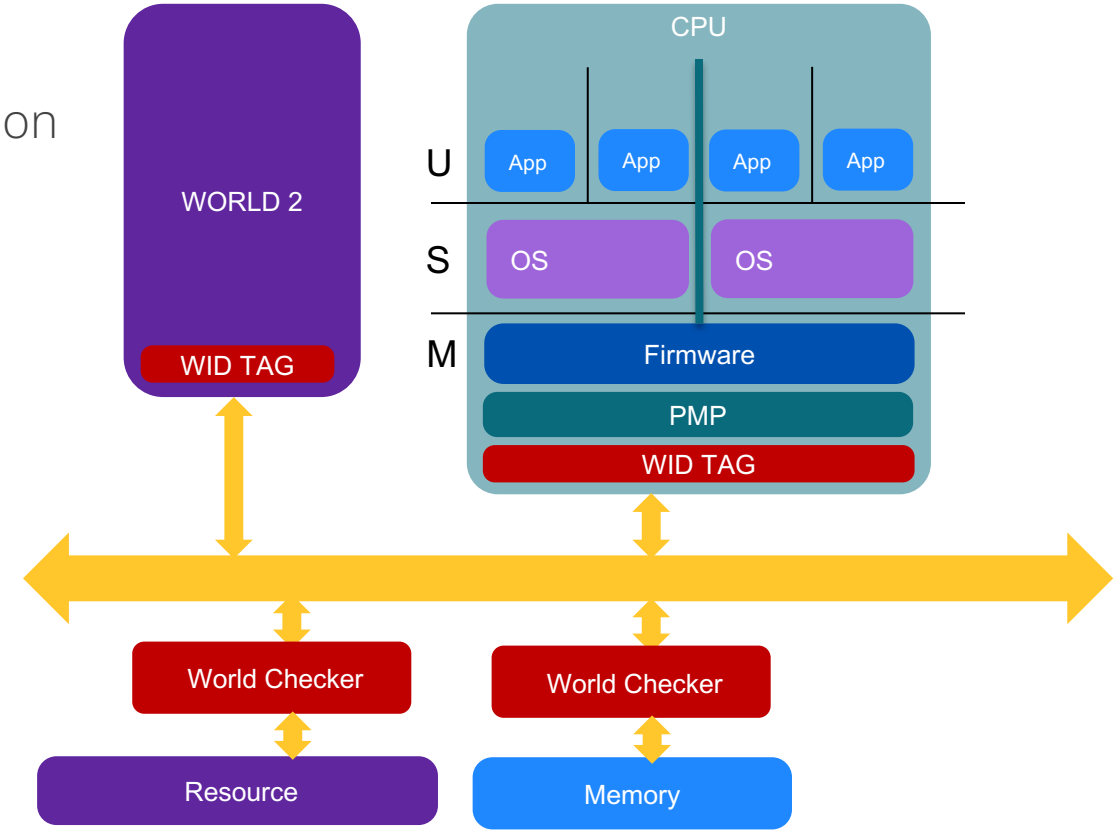
- Basic Privilege
- Physical Memory Protection
- Supervisor Mode
- Virtual Memory



RISC-V®

Layering Isolation Mechanisms

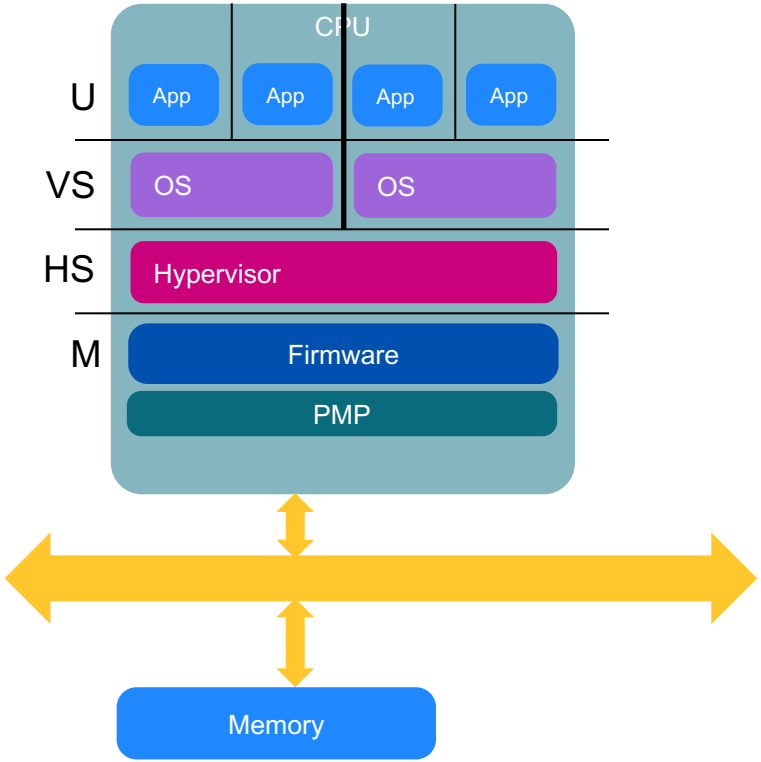
- Basic Privilege
- Physical Memory Protection
- Supervisor Mode
- Virtual Memory
- World IDs



RISC-V®

Layering Isolation Mechanisms

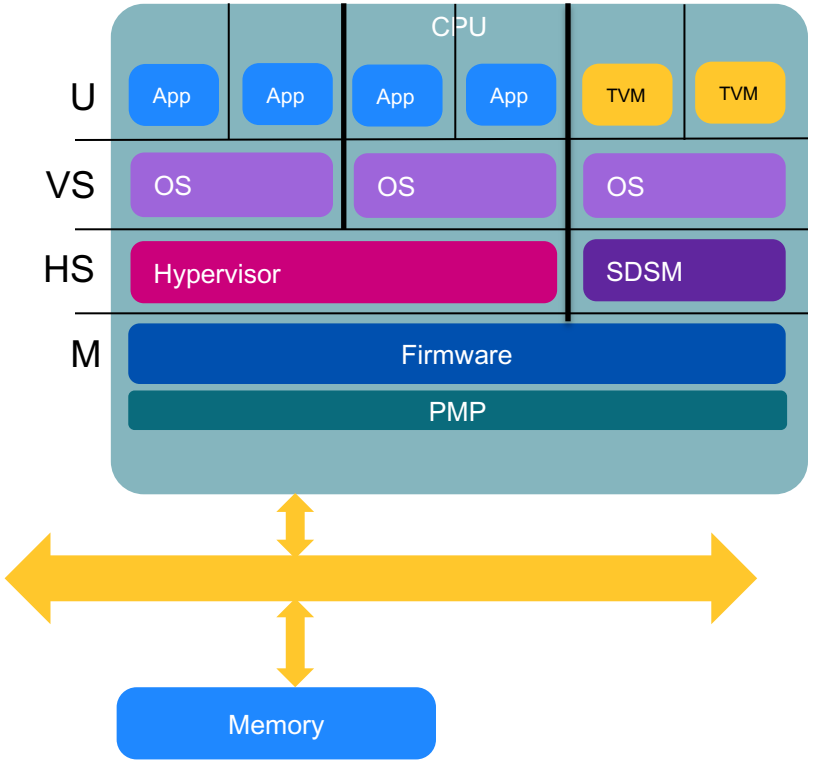
- Basic Privilege
- Physical Memory Protection
- Supervisor Mode
- Virtual Memory
- World IDs
- Hypervisor Extension



RISC-V®

Layering Isolation Mechanisms

- Basic Privilege
- Physical Memory Protection
- Supervisor Mode
- Virtual Memory
- World IDs
- Hypervisor Extension
- Supervisor Domains



RISC-V®

The Isolation Toolbox

- Modern systems require layered, composable isolation
- Risc-V Composability over single “golden” mechanism

- Supervisor Domains signal the next step beyond privilege hierarchies

- The future:
  - Worlds+
  - Flexible architectures
  - CHERI … ?

Thankyou

RISC-V®