IOPMP Proposal

joxie, andym @nvidia

RISCV TEE task group

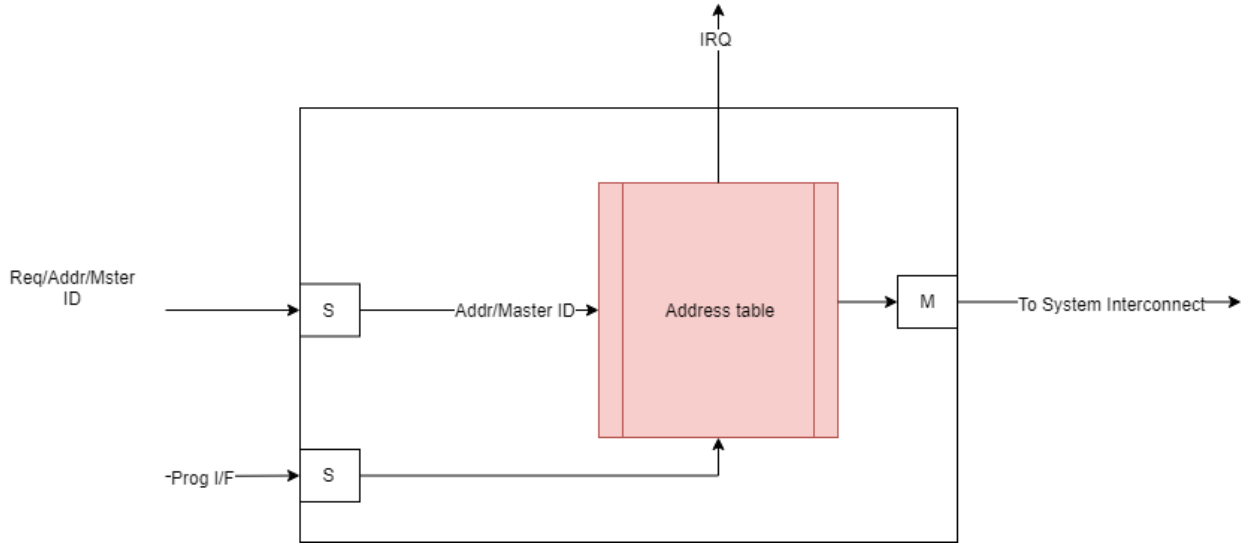
Revision – 0.5.1 candidate

IOPMP – Design Goals

- Protect physical memory from all memory masters in system
- Support systems with both single core and multi-cores
- Support error reporting
- Support 32bit and 64bit implementations
- Support *unlimited* number of entries
- Support *unlimited* memory masters sharing one IOPMP
- Unified programming model
- Scalability

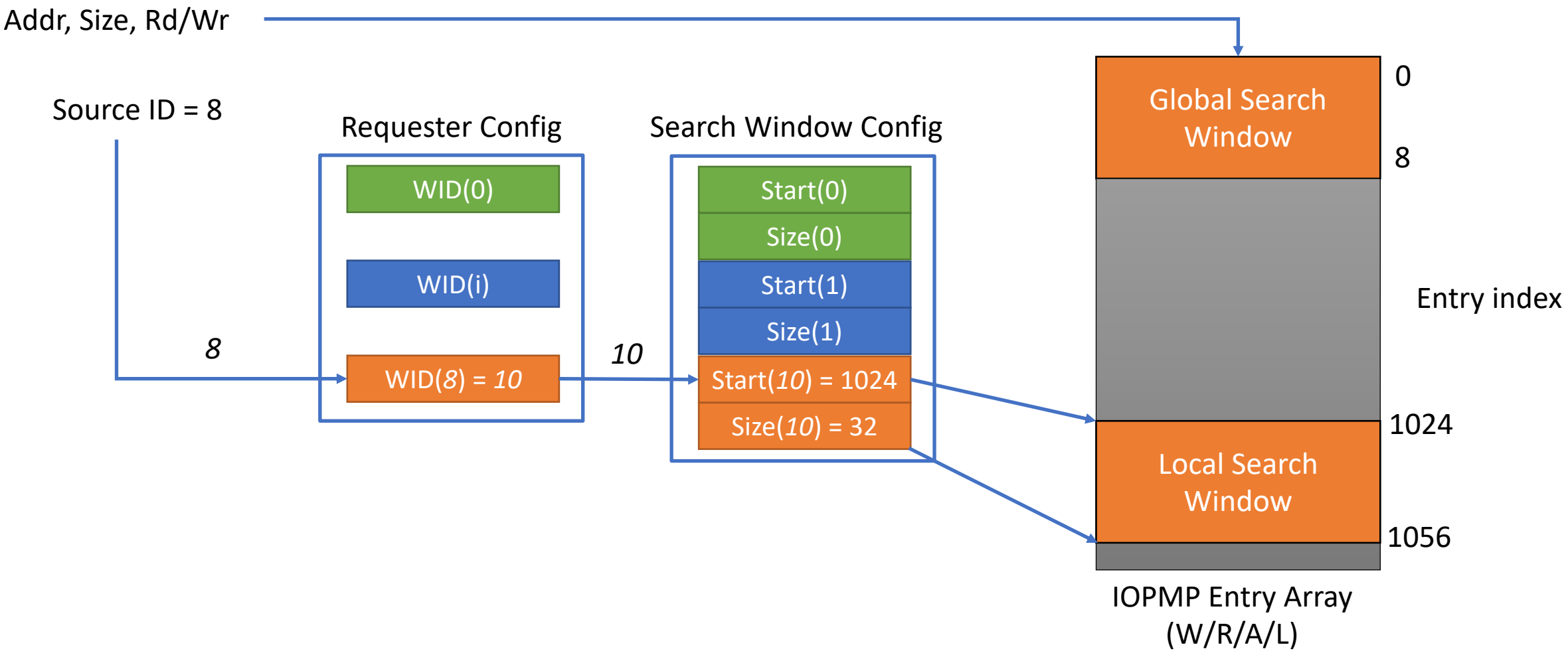
IOPMP Arch Proposal – 0.1

- Not scalable
  - Area cost for MSID bitmap in every entry
- Low performance
  - Time to search many entries
  - Context switch



N	1bit	2bit	1bit	1bit	XLEN
MSID[N:0]	L	A	W	R	Address[`XLEN-1:0]

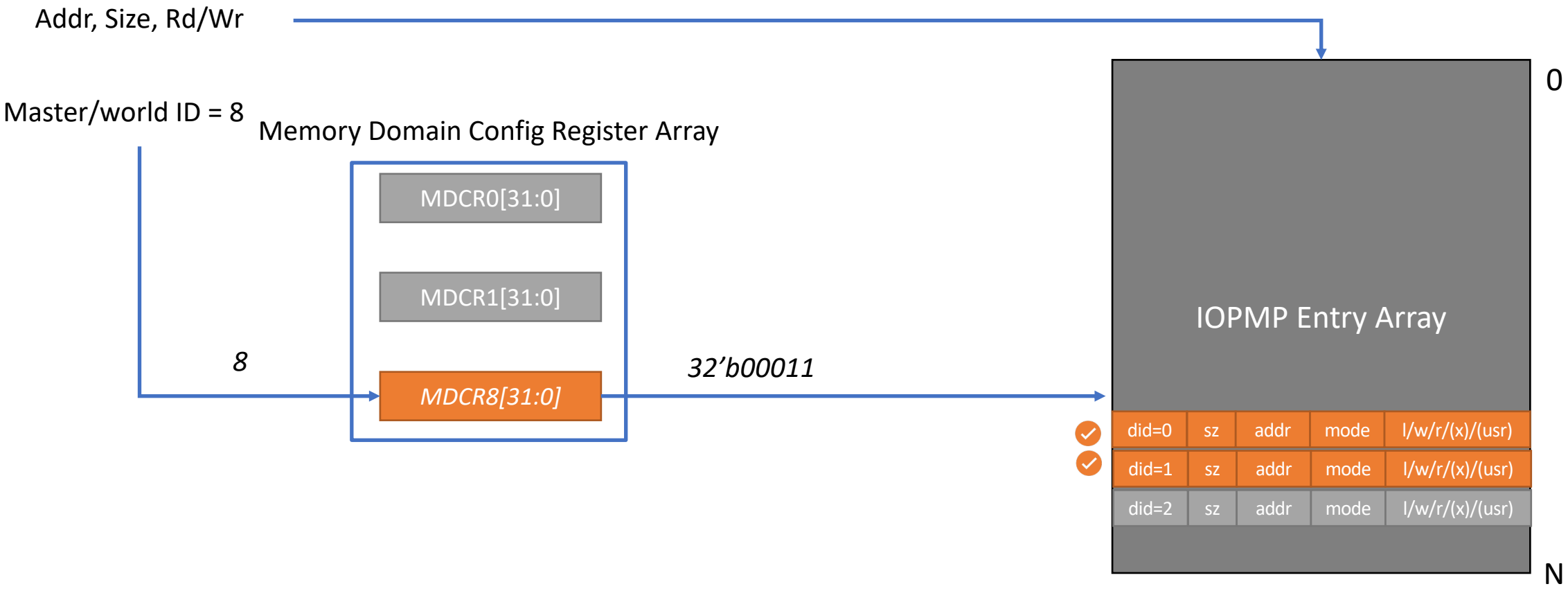
IOPMP Arch Proposal – 0.5



Rationale - v0.5.1

- Area is important, especially for IoT
  - Window selection overkill to IoT systems (extra area cost)
  - Entry duplication (extra area cost) for IoT systems

IOPMP Arch Proposal 0.5.1



IOPMP Arch Proposal 0.5.1 – Overview

- Every IOPMP entry is tagged with a memory domain ID field (DID)
- Every request is tagged with master/world ID
- Optionally, IOPMP has a memory domain configuration register array to map source/world ID to memory domain ID
- IOPMP checks entry DID vs request DID

Memory Domain Config Registers (MDCR)

- MDCR is XLEN bit register array
- MDCR(i) is a bitmap to map master/world ID *i* to memory domain ID
  - MDCR(8)=32’b000111 maps master/world ID = 8 to memory domain ID 0, 1 and 2
- Bit0 of MDCR(i) must be tied to 1
- MDCR is an optional feature, SW can use **IOPMPCFG** to discover its existence

Global Control and Status Register

- **IOPMPCFG** – IOPMP Hardware Config Register, used by software to determine hardware capacity.
  - Total number of IOPMP entries hardware support (read-only)
  - Total number of source IDs hardware support (read-only)
  - Total number of memory domains hardware support (read-only)

IOPMP Entry Configuration

XLEN	XLEN	1	2	1	1
DID	Addr	L	M	R	W
Domain ID	Address	Lock	Mode	Read	Write

- **DID** : Domain ID field
- **Addr**: Address field.
- **L** : Lock. When set, the entry is locked until next reset
- **A** : Mode. Inherit rules from PMP spec
- **R** : Read enable when set
- **W** : Write enable when set

IOPMP Entry Configuration

1	User defined
X	Attr
Execute	Attr

- **(Optional) X**: Executable-enable when set
- **(Optional) Attr**: Extra attributes. When present, IOPMP checks the extra attributes tagged in transaction against attr field, fault on mismatch

Matching Rules with DID

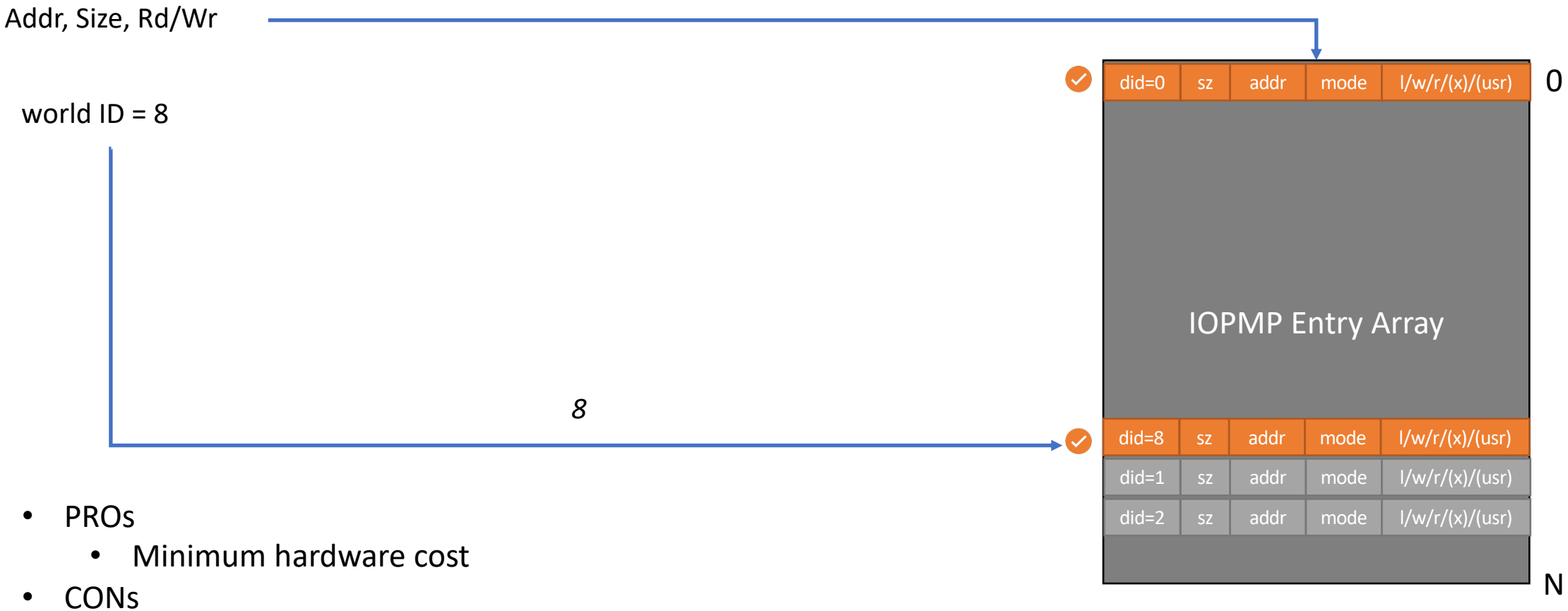
- IOPMP address mapping rule is inherited from RISC-V PMP spec

- In addition to address mapping rule, IOPMP hardware checks memory domain ID (DID) field against incoming DID
  - When entry DID field = 0, always report DID match
  - When entry DID field != 0, report DID match when entry DID == incoming DID

Error Config and Info Registers

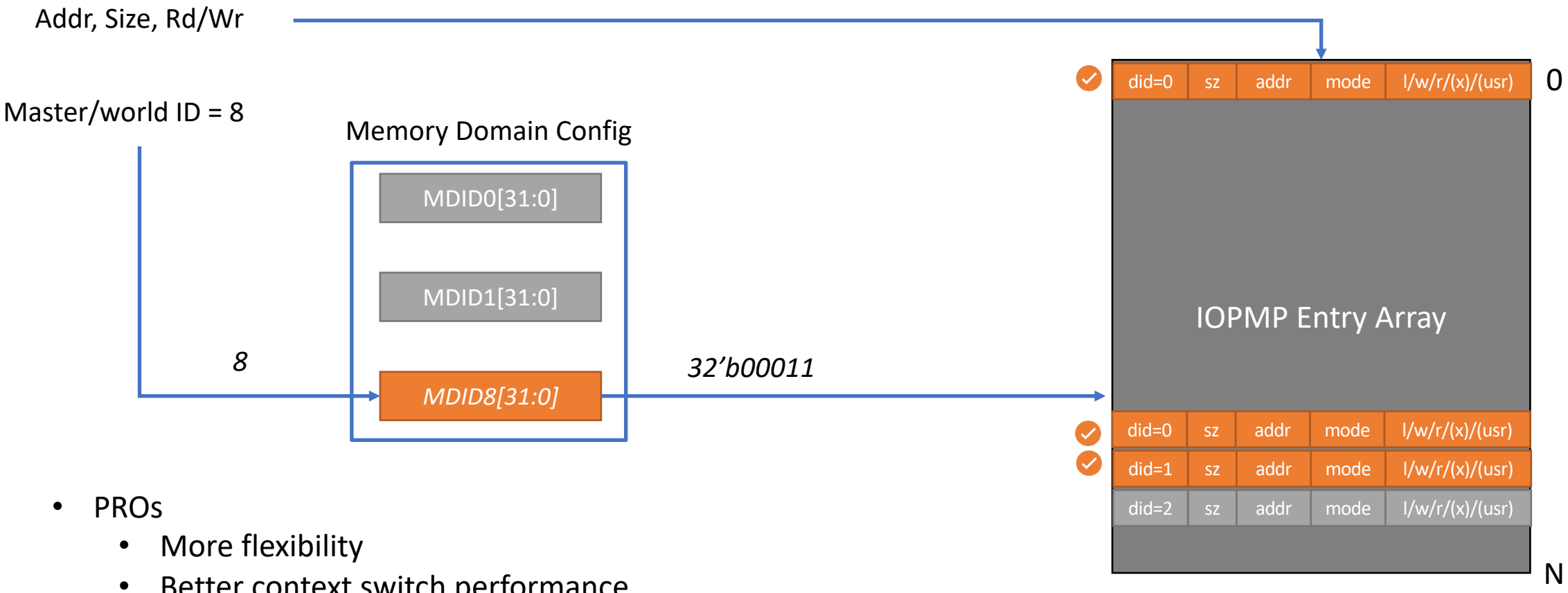
- **ERRADDR** : Error Address
- **ERRREQID** : Error Source ID
- **ERRREQINFO** : Error Request Info
  - Request Size/Error_is_RD/WID/EntryID
- **ERRIRQ :** Error Interrupt Register
  - Clear error interrupt
- **ERRCFG(i)** : Error Config for master/world ID *i*
  - Record-and-forget / Record-and-Interrupt
  - Record-first-error / Record-last-error

IOPMP Implementation Variant 1



- PROs
  - Minimum hardware cost
- CONs
  - Duplicate entry for shared memory regions
  - Low context switch performance

IOPMP Implementation Variant 2



- PROs
  - More flexibility
  - Better context switch performance
  - No entry duplication to support shared regions
- CONs
  - Extra hardware cost to add MDCR registers

IOPMP Config Example

Memory Domain Config Registers

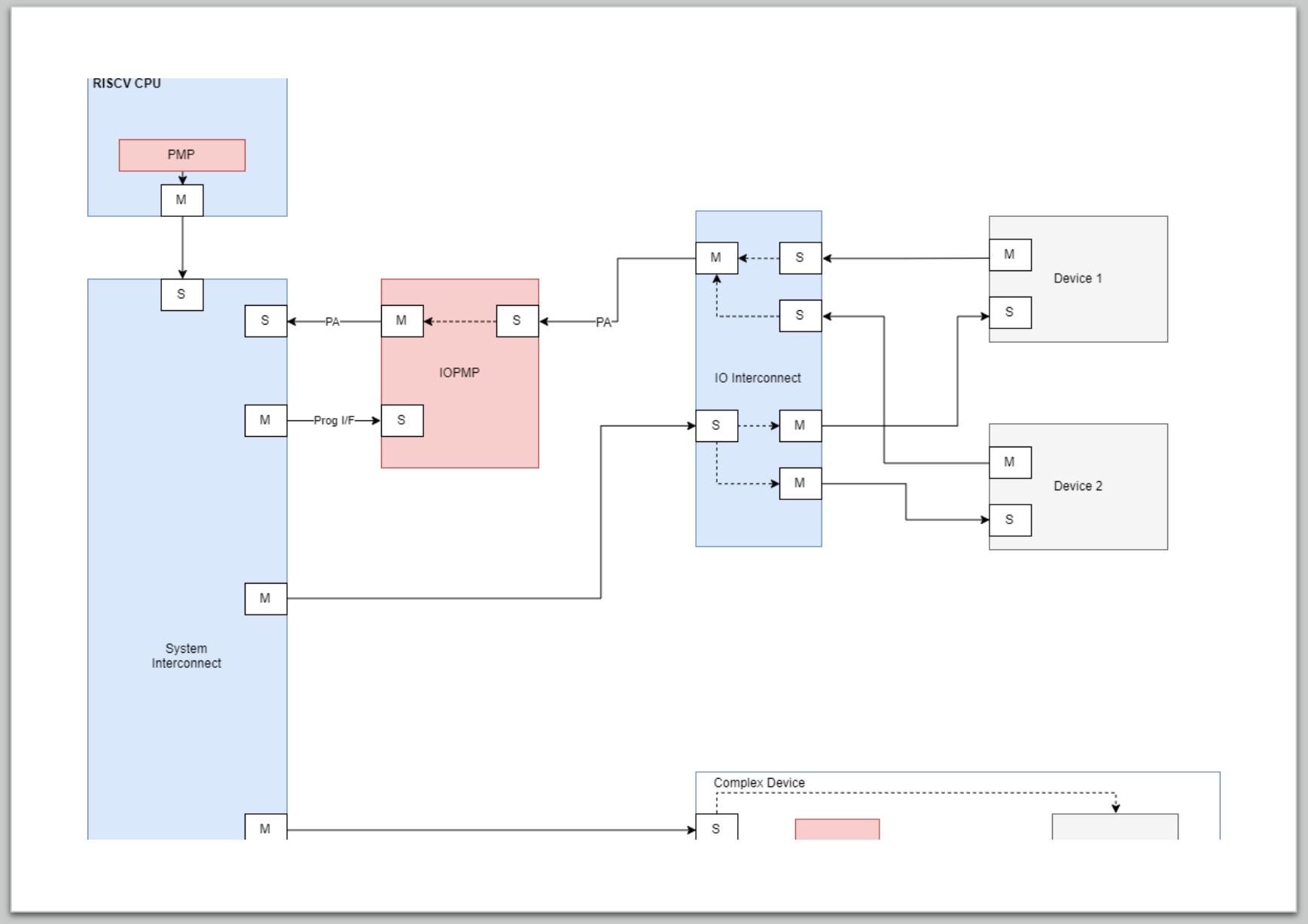
Master ID	MDCR(i)
0	32’b01011
1	32’b01011
2	32’b01011
3	32’b01101
4	32’b01101
5	32’b10001

IOPMP Entry Array
(Intentionally hide addr field for simplification)

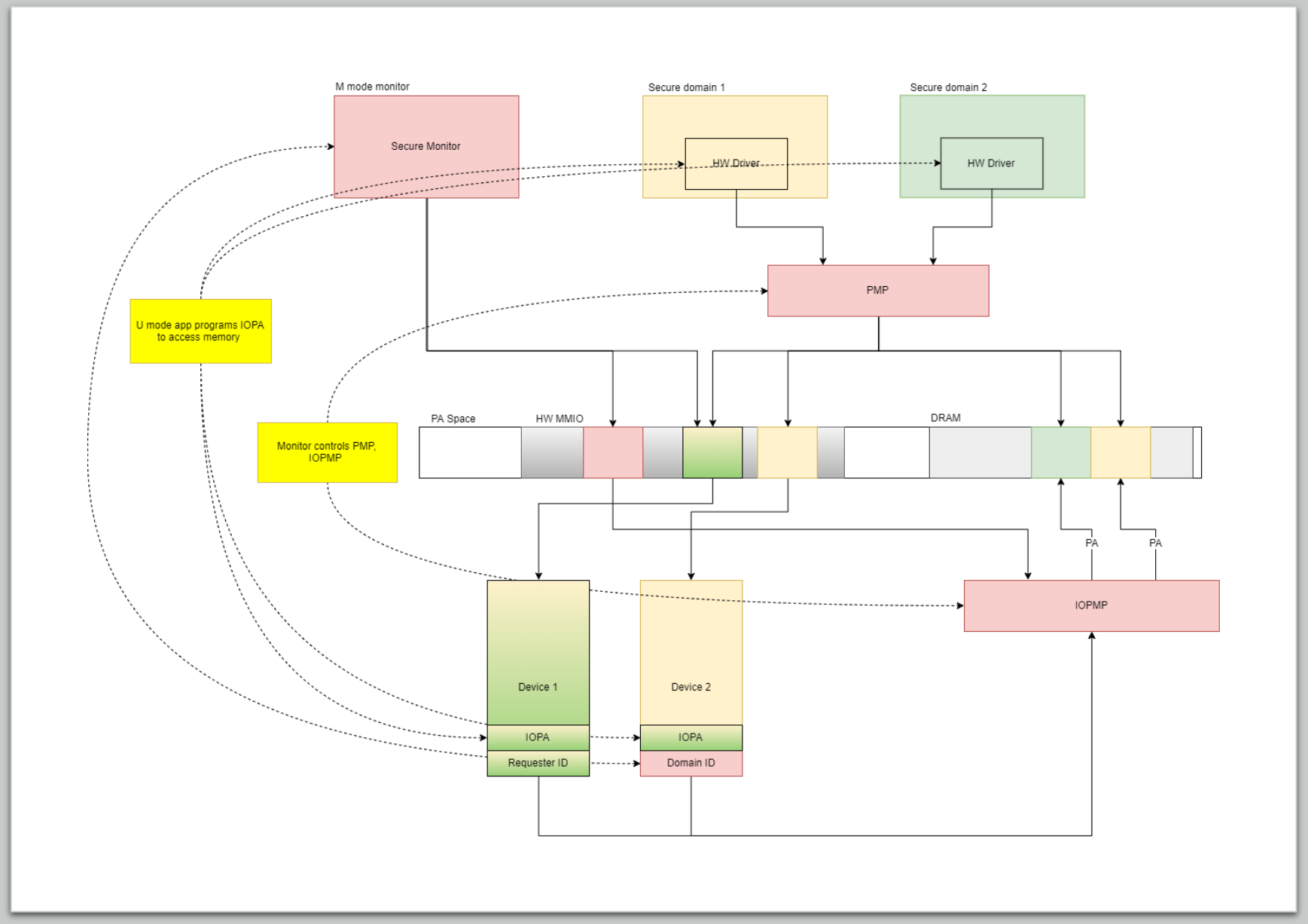
Entry Index	DID	W	R	L	Comment
0	0	0	0	1	Secure Monitor's code, black-out, locked
1	4	0	1	1	Secure monitor’s data, RO to devices, locked
2	1	1	1	0	Secure domain 1's private data
3	2	1	1	0	Secure domain 2's private data
4	3	1	1	0	Shared data region for domain 1 and 2

- This example shows IOPMP configuration for 3 secure domains (secure monitor, domain 1 and 2) for 5 different masters
- Master ID 0~2 owned by secure domain 1, they can access domain 1’s private data region and shared data
- Master ID 3~4 owned by secure domain 2, they can access domain 2’s private data region and shared data region
- Master ID 5 owned by secure monitor, it can access monitor’s data but cannot access secure domains’ data
- Secure monitor’s code is blacked out and not accessible to all masters (Prevents a buggy secure monitor cannot modify its own code via DMA)

System Instantiation Example



Programming Model Example



Backup