The Practical Use Cases of the RISC-V IOPMP – Andes SoC's Rapid-k Model

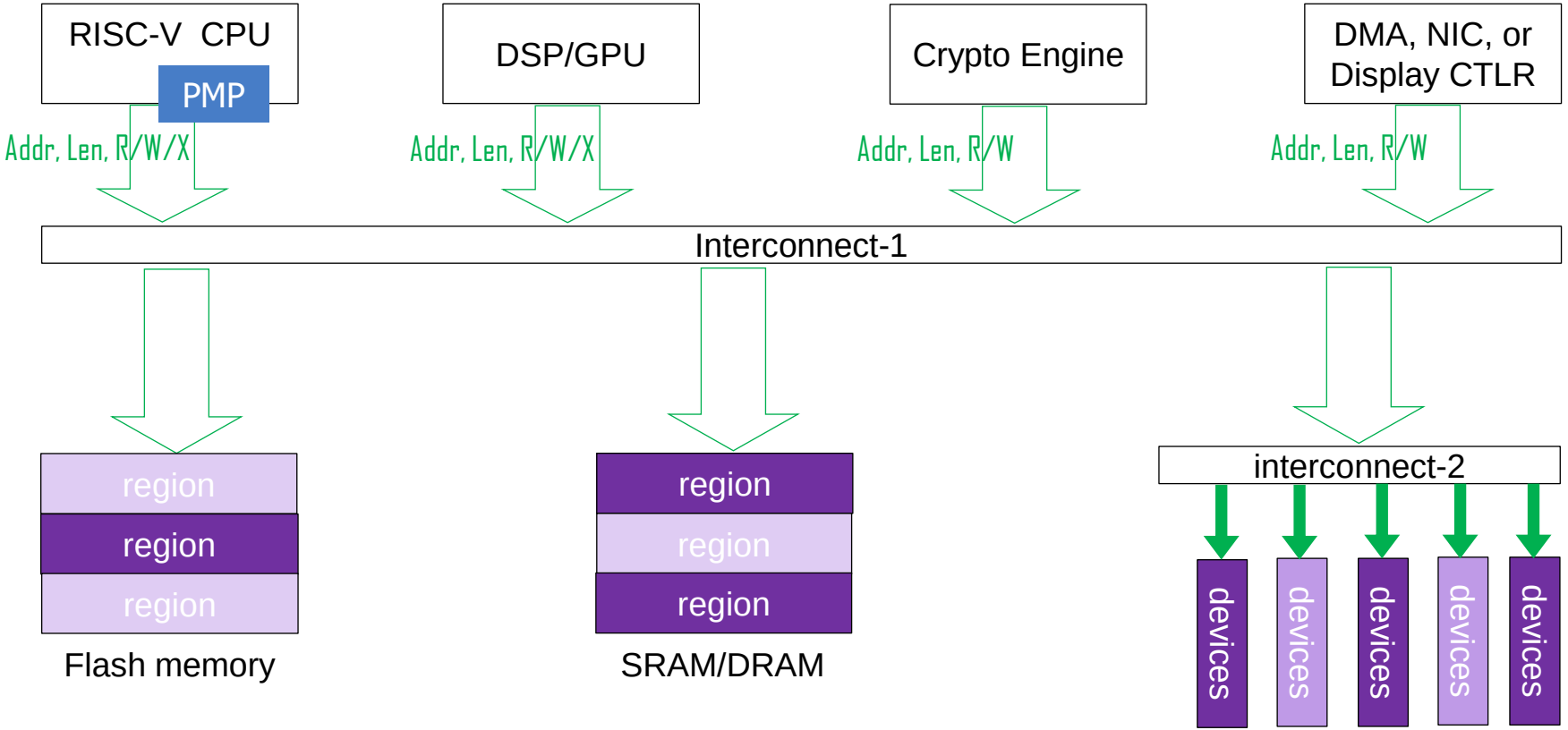
August 24, 2023
Dr. Paul Shan-Chyun Ku
Andes Technology

Speaker: Dr. Paul Shan-Chyun Ku

Experience:

- The Chair of IOPMP Task Group (2022-)
- The Vice-chair of TEE TG (2021-2022)
- Deputy Technical Director, Andes Tech

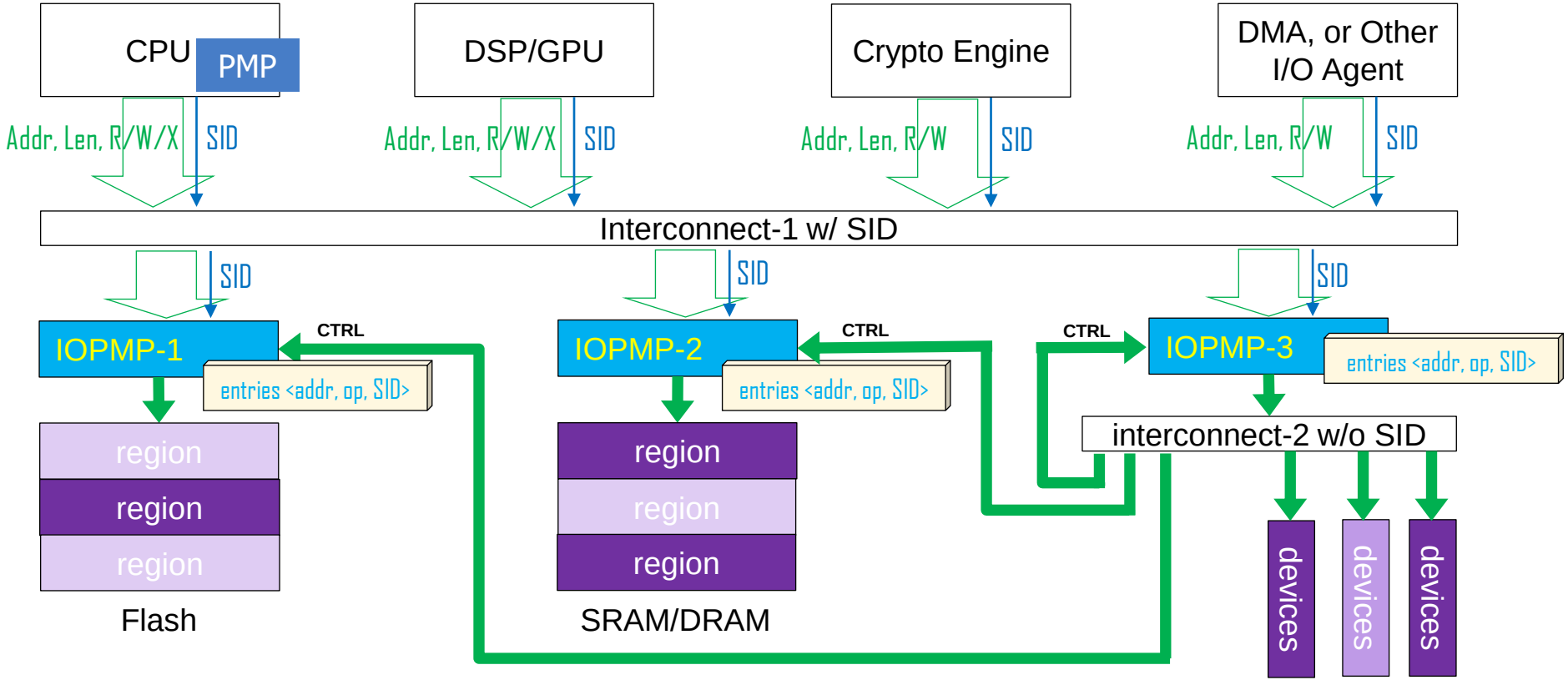
A Typical Platform



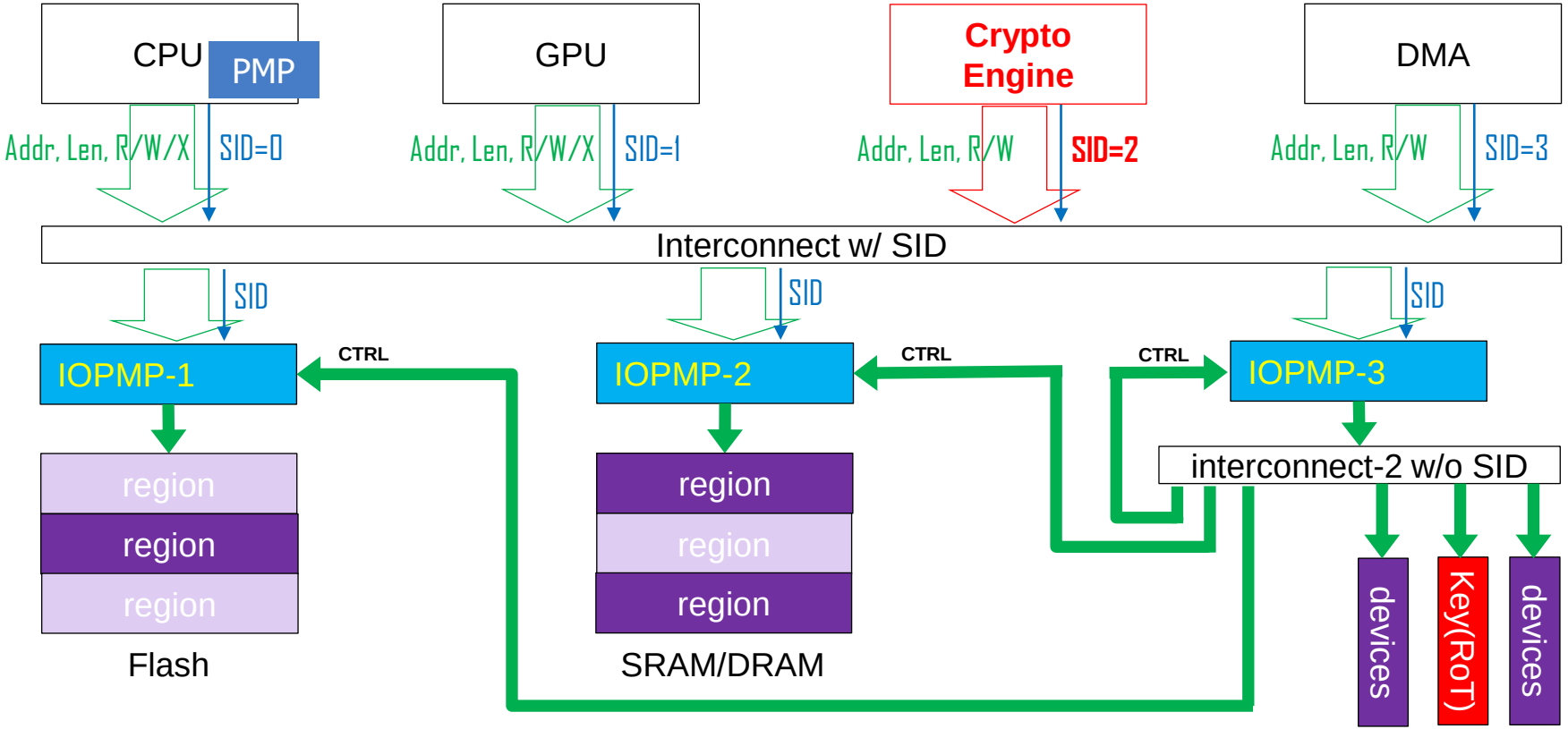
Vulnerability and Threat

- RISC-V CPU's transactions are checked by PMP/ePMP:
  - By Where, How, and Which to access
- The other I/O agents: DSP, GPU, DMA, NIC, LCDC…
  - Transactions from them are NOT CHECKED ➔ vulnerability!
  - A malicious SW that can control the I/O agents to access anywhere becomes the threat.
  - EX: an attack asks the I/O agent to read the sensitive asset without PMP/ePMP's check and store it to its own legal space.
- IOPMP is the tool to mitigate the such a threat.
  - The IOPMP task group under the RISC-V international is working on the architecture spec.

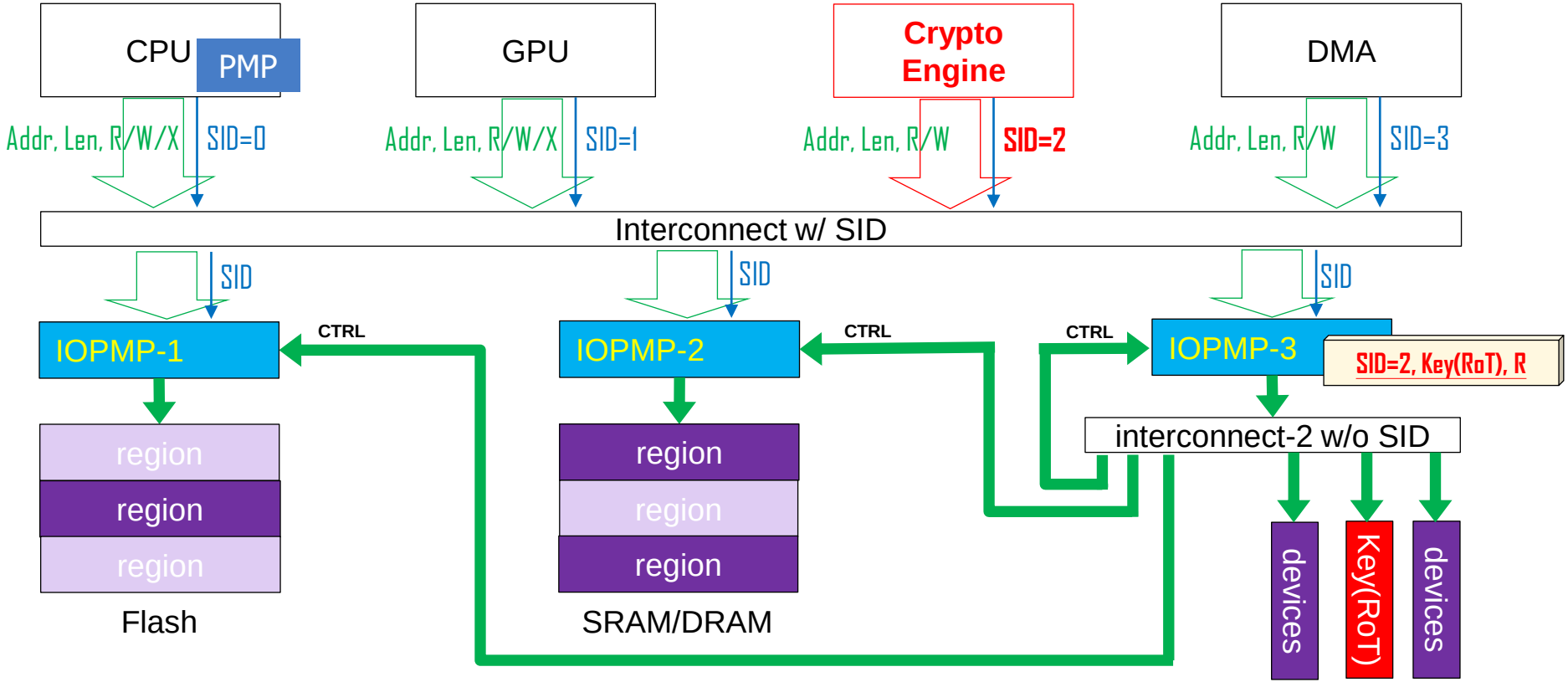
A Platform with IOPMPs



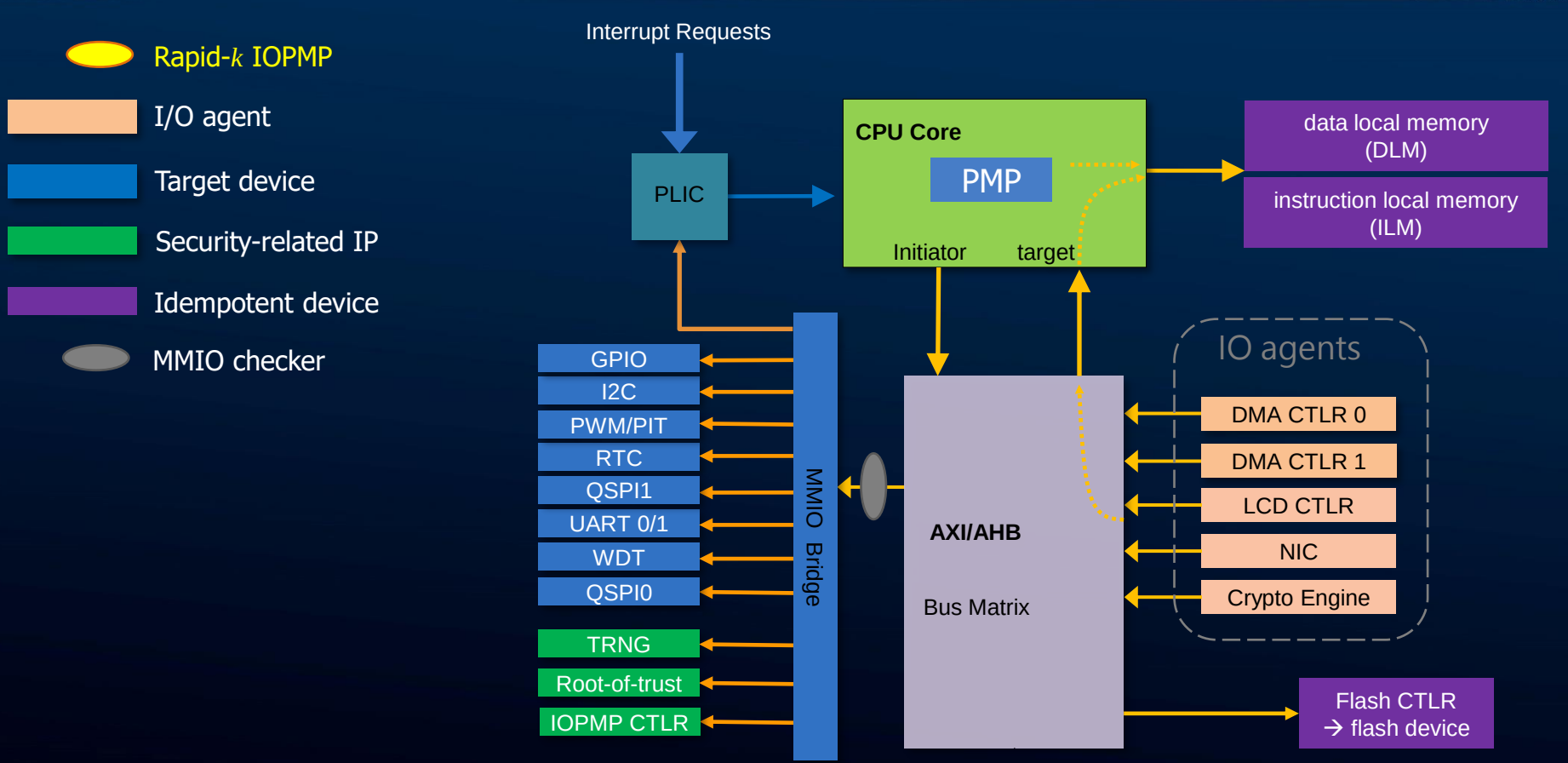
Crypto Engine Read Privat Key



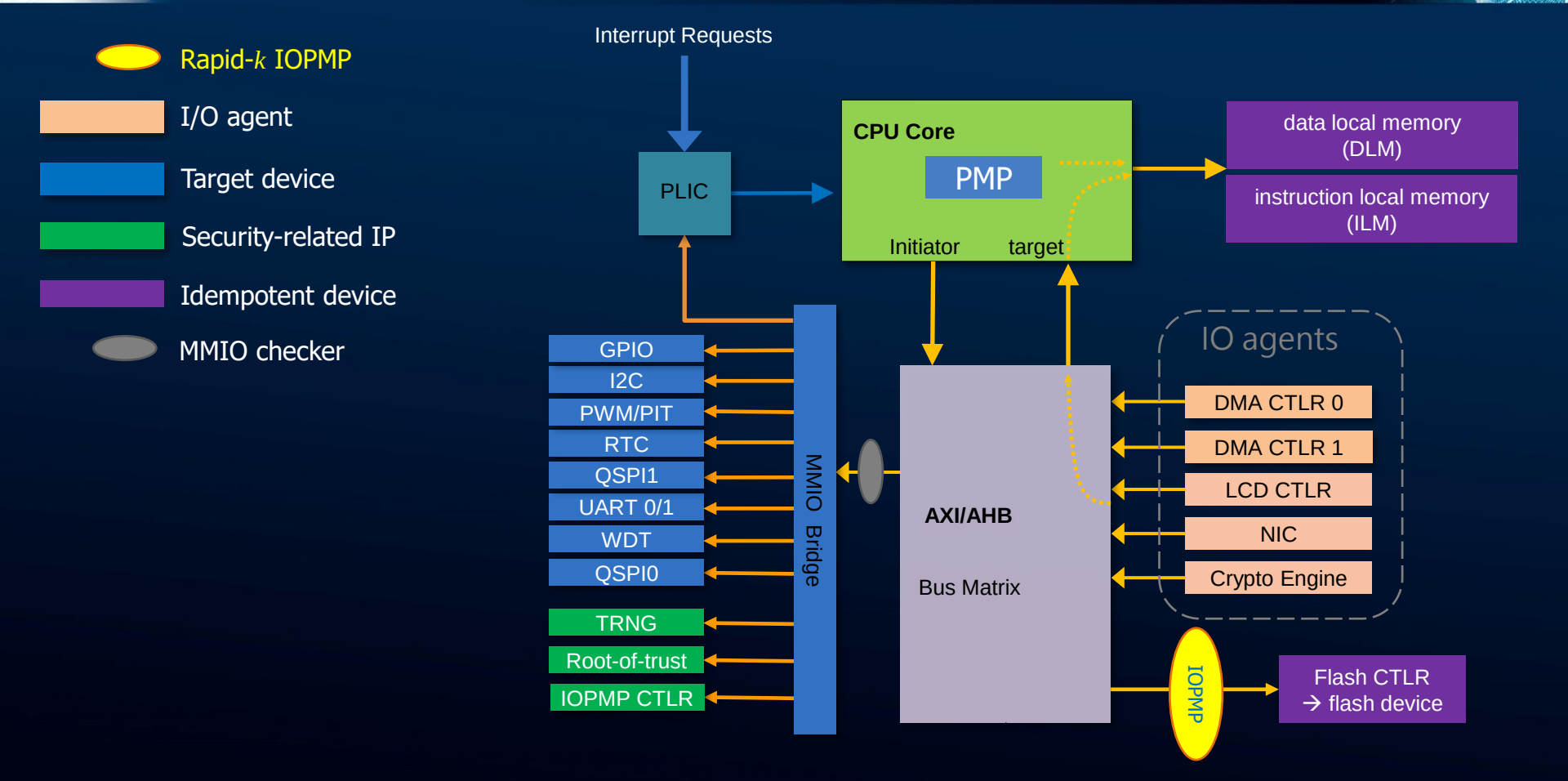
Crypto Engine Read Privat Key



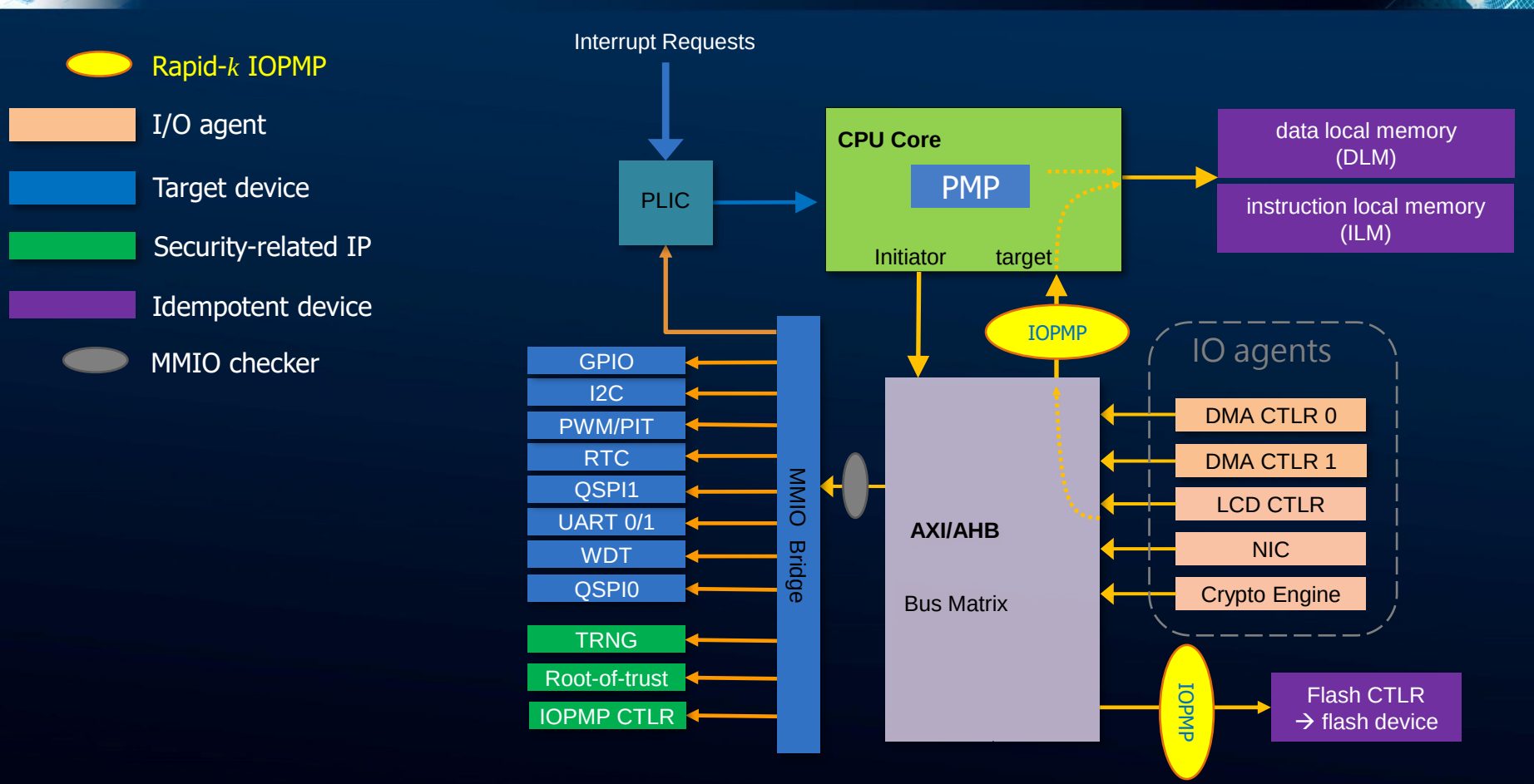
Andes IoT Platform with IOPMP



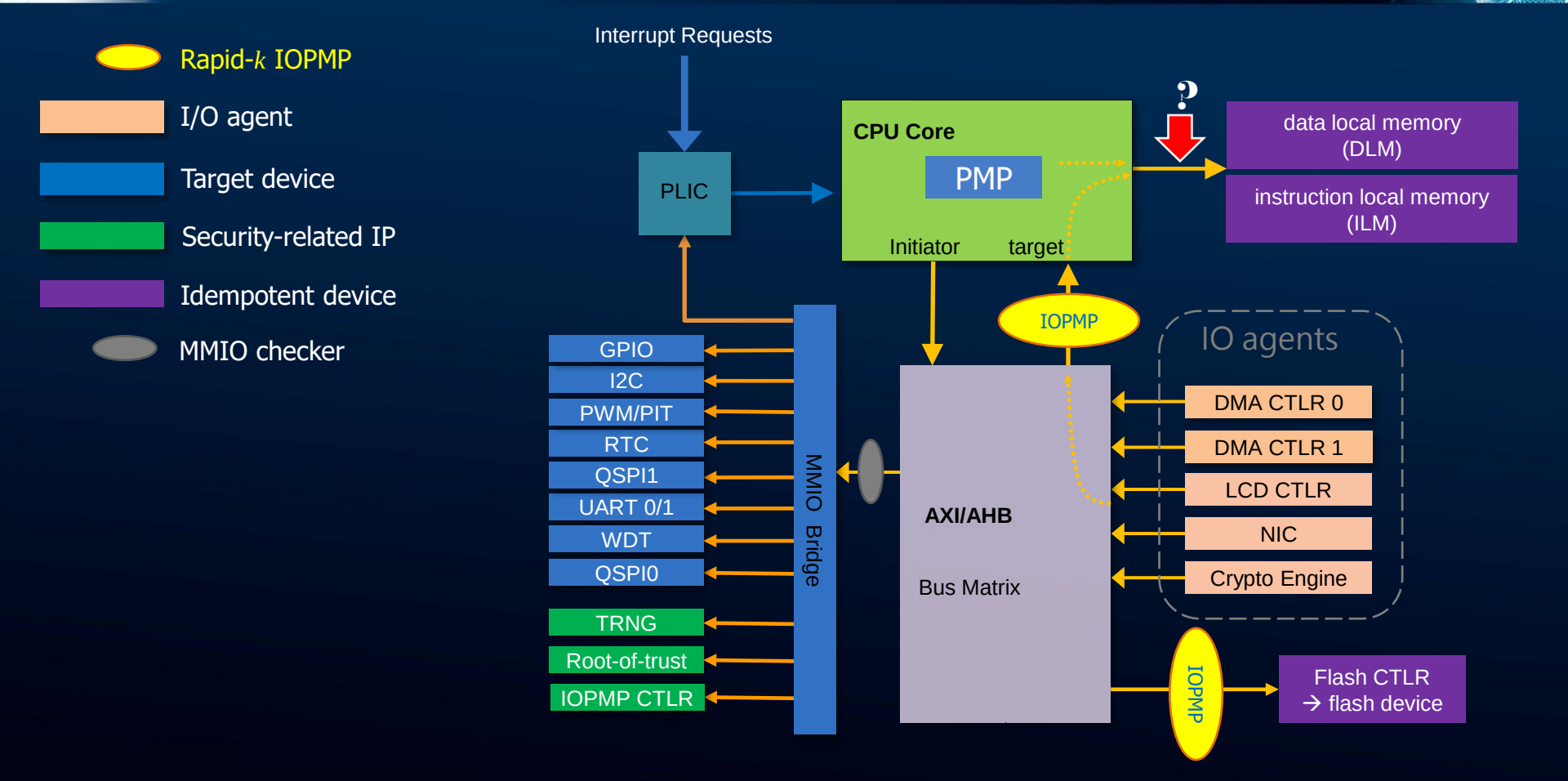
Andes IoT Platform with IOPMP



Andes IoT Platform with IOPMP

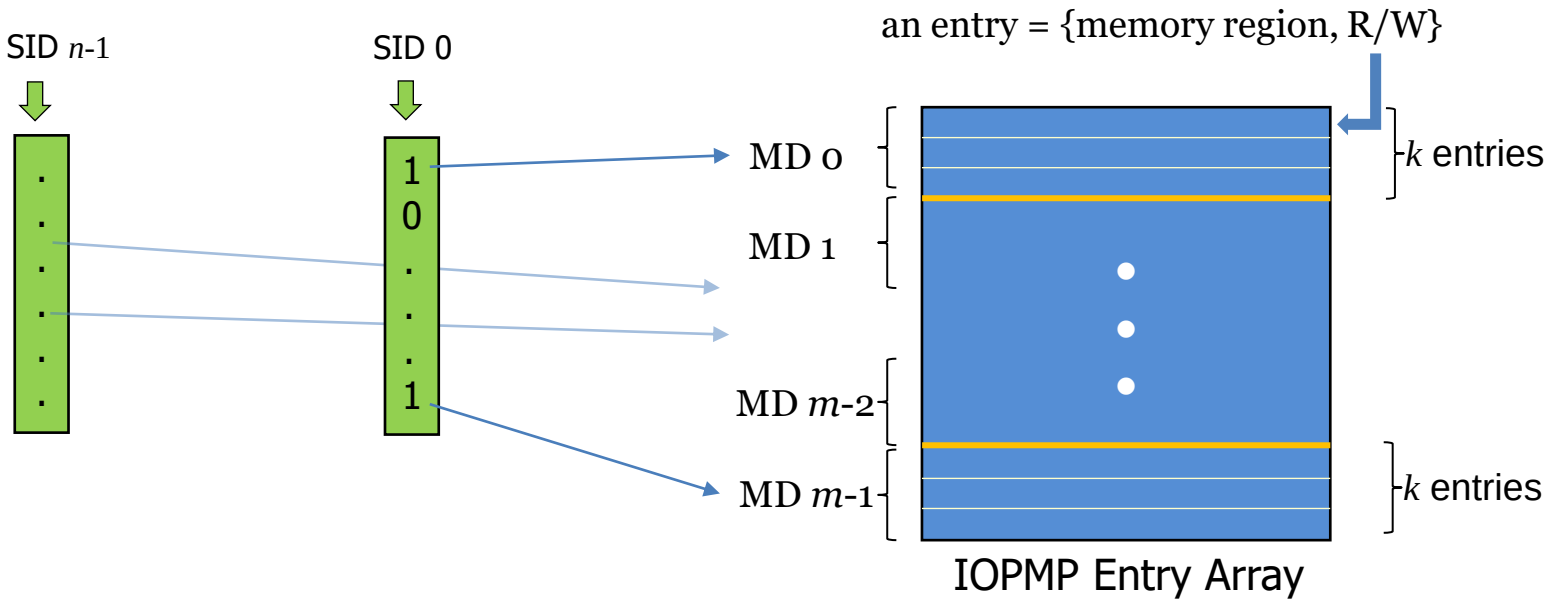


Andes IoT Platform with IOPMP



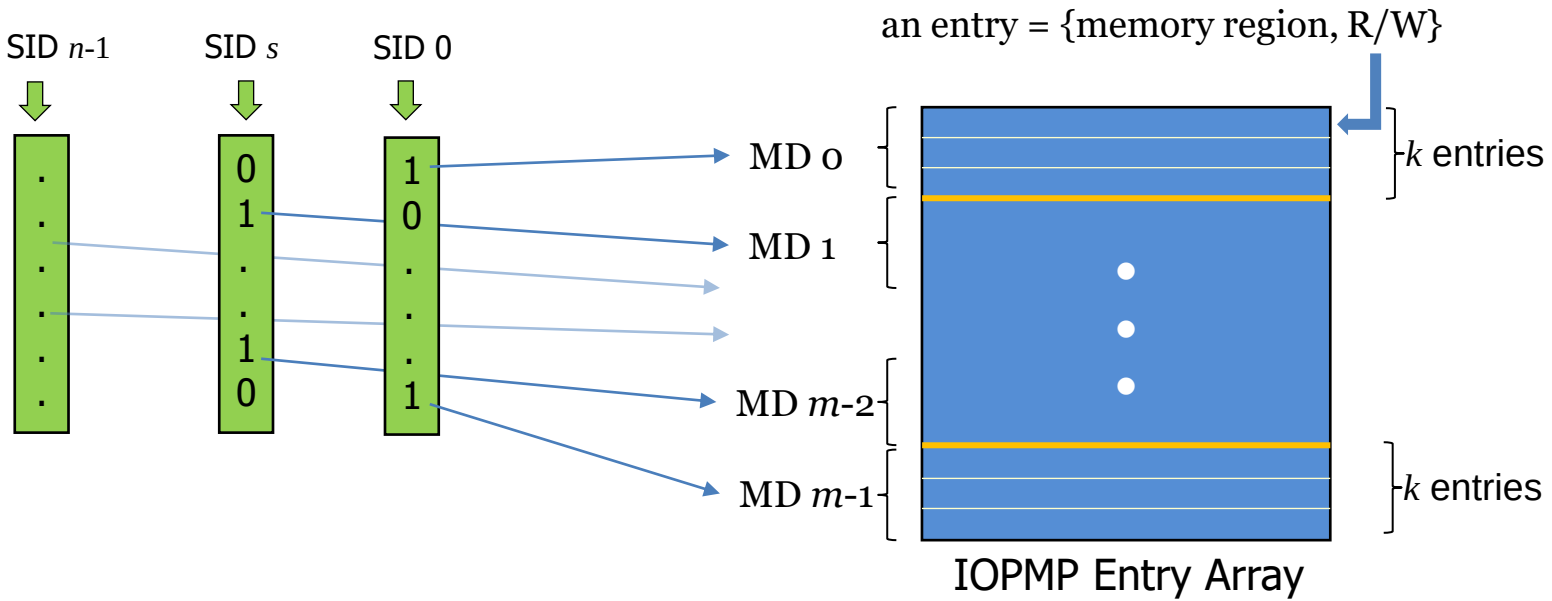
IOPMP Rapid-k Model

- Prioritized PMP-like entries
- m MD → (m x k) entries



IOPMP Rapid-k Model

- Prioritized PMP-like entries
- m MD → (m x k) entries



Why Rapid-k Model

- Why the rapid-k model?
  - Moderately complex:
    - It has the bitmap mapping from a SID to its associated MDs, but
    - No table mapping from a MD to its entries.
  - Compare to the full model:
    - The full model is more flexible to manage MDs and their entries.
    - The rapid-k model has simpler design, shorter the latency and/or fewer cycles to fetch entries.
  - Compare to the compact and isolation model:
    - The two models do not support shared MD, so more entries would be needed.

Config the Rapid-k Model

- How many SID?
  - A SID per I/O agent and/or per channel?
- How to pick up k?
  - Strongly depends on your application; rule of thumb:
    - Average number of entries per MD: 6~12
    - k = 4~16
- How many MDs?
  - Total number of entries used by all SIDs in the runtime.
  - Any SID switch between different memory regions and permissions in a high frequency?
    - Switch SID-to-MD mapping instead of updating entries' contents

Concluding Remarks

- Introduced the IOPMP rapid-k model
- Explained why the rapid-k model in Andes' IoT Platform
- Analyzed the factors for configuring the rapid-k model

Thank You

The practical use cases of the RISC-V IOPMP

-- Exemplary Usage Model

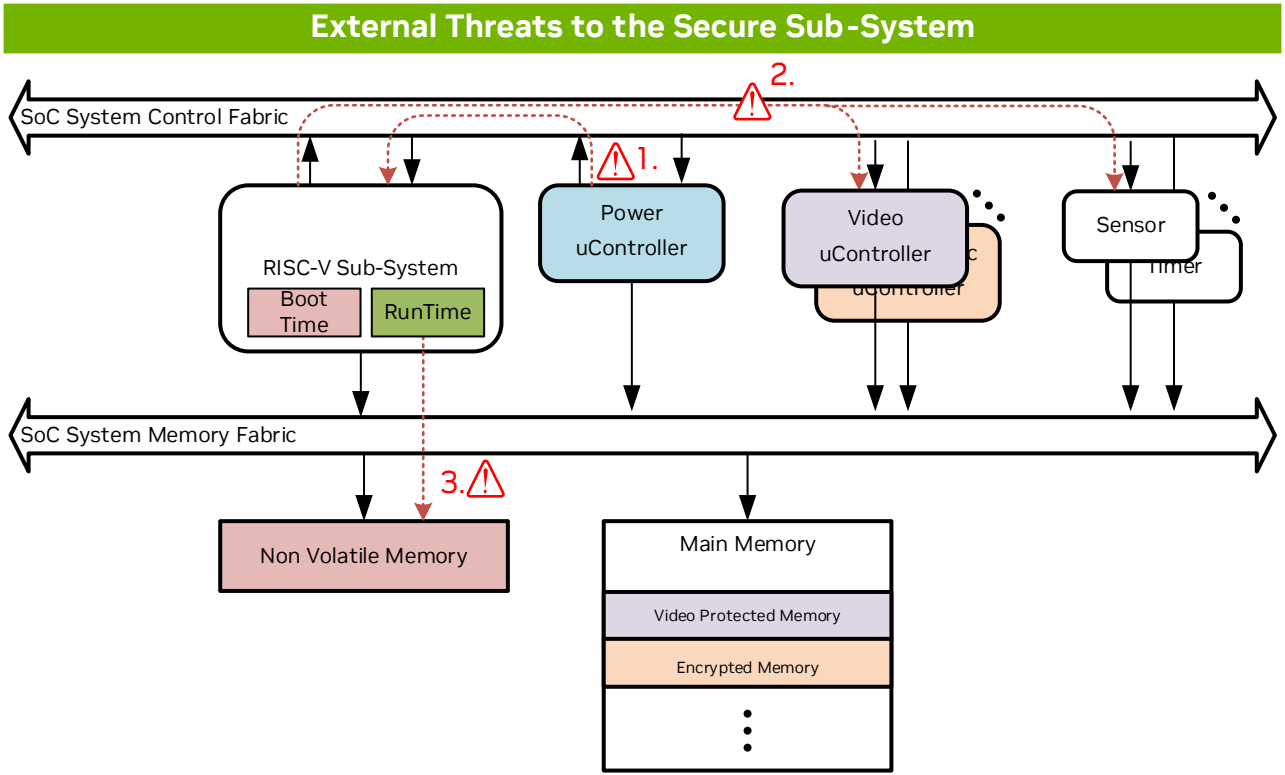
Channing Tang, Dr. | 2023 China RISC-V Summit/2023-08

Speaker: Dr. Channing Tang

- Vice chair of the RISC-V IOPMP TG.
- Senior HW Architect with Nvidia, she is focuses on the hardware architecture and design of security system.

Threat Modeling

What should be protected and Who wants to attack



- Threats from and to the SoC System

1. Unauthorized access from external initiators, e.g., power uController, to the RISC-V sub-system local IO devices

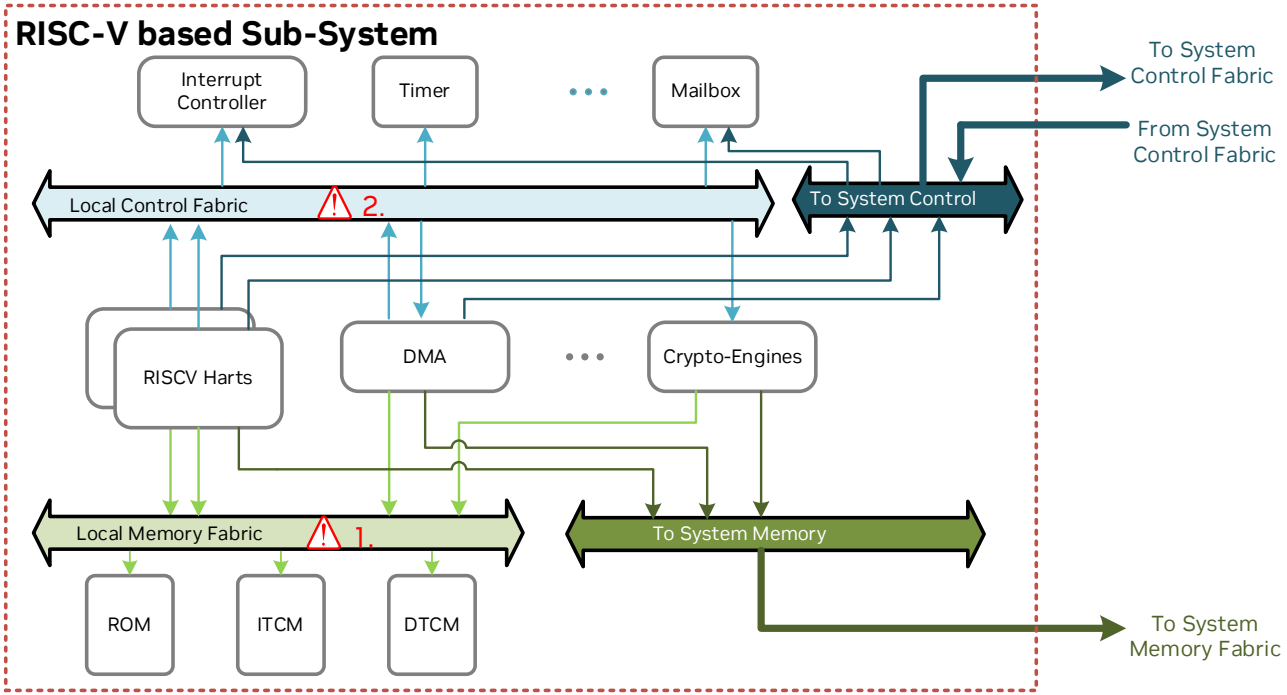
2. Unauthorized access from sub-system to SoC IO devices

3. Spoofing to the protected memory regions, e.g., boot time data v.s., runtime data

Threat Modeling

What should be protected and Who wants to attack

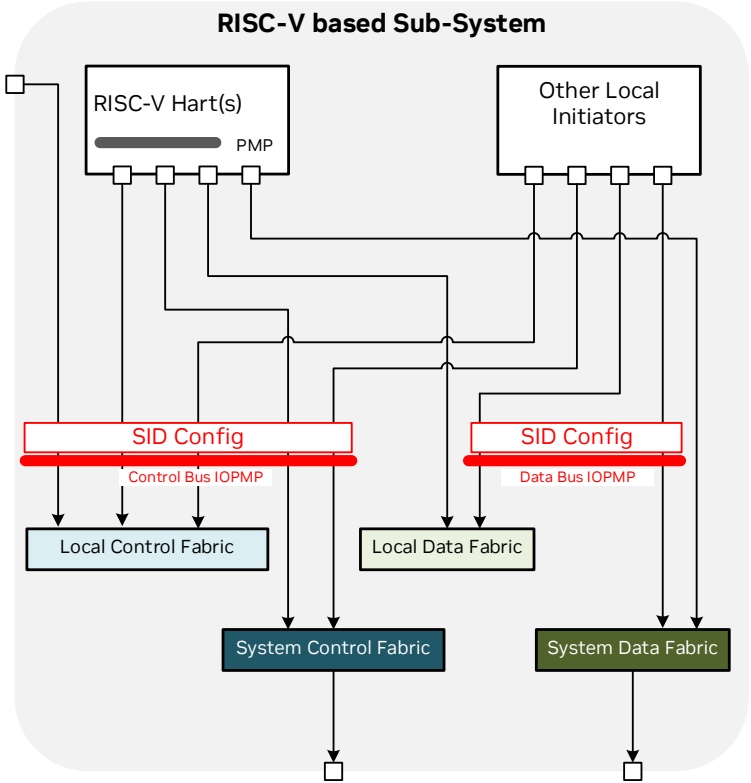
Internal Threat to the Secure Sub-System



- Threats Internally in the Sub-system
  1. Access Isolation to local memories among different devices
  2. Access Isolation to local devices among different runtimes

Position of the IOPMP in System

How to Integrate the IOPMP to the System



- Two IOPMP Instances for each RISC-V based Sub-System
- An IOPMP for Control Plane
  - Access controls for RISC-V harts to local and System IO devices
  - Access controls for local initiator peripherals, e.g., DMA, to local and system IO devices.
- An IOPMP for Data Plane
  - Access controls for local initiator peripherals to local memories
  - Access controls for local initiator peripherals to global memories
  - RISC-V harts accessing memories can be protected by PMPs.
- SID Config Registers

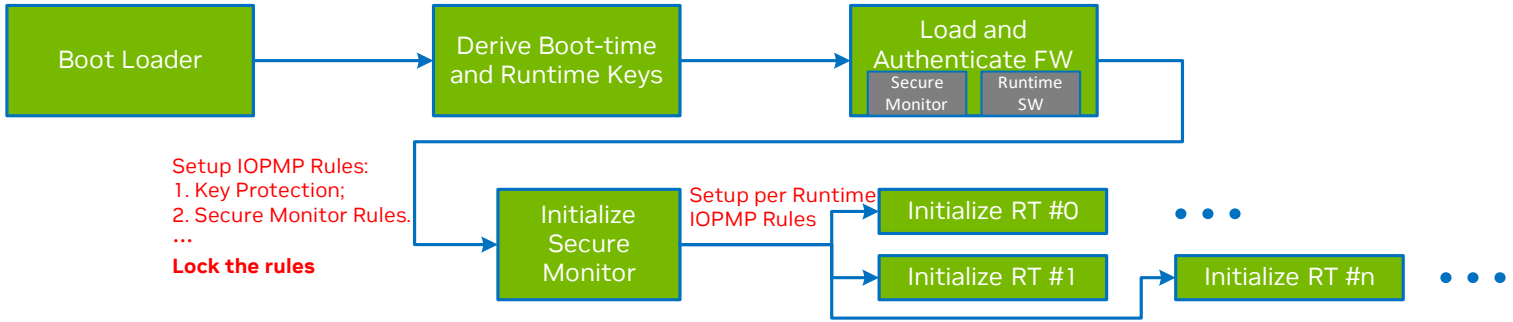
IOPMP Model and Parameters

- IOPMP Full Model is Adopted
  - Flexible – SW can determine the number of entries belongs to each MD.
  - Less fragmentation on IOPMP entries – Rapid-K or Dynamic-K model although is easier for HW implementation but may end up with entries not used or insufficient in certain MDs.
- Typical IOPMP Parameters Used in Different Sub-Systems
  - Security Critical Configuration:
    - Security critical requirement
    - Frequent SW context switch
    - 1~2 SID(s) per SW context: a SID can be assigned to multiple HW initiators.
  - Light Configuration:
    - Bare metal usage model
    - Limited access to system memory and system control fabric
    - HW initiator to SID mapping are semi-static (programmed once during boot time)

	# of SW contexts	# of HW initiators	# of SID(s)	# of MD(s)	# of entries
Security Critical Configuration	8~96	>= 64	16~32	16~32	128~256
Light Configuration	1~2	4~8	4~8	16	16

IOPMP Usage Model

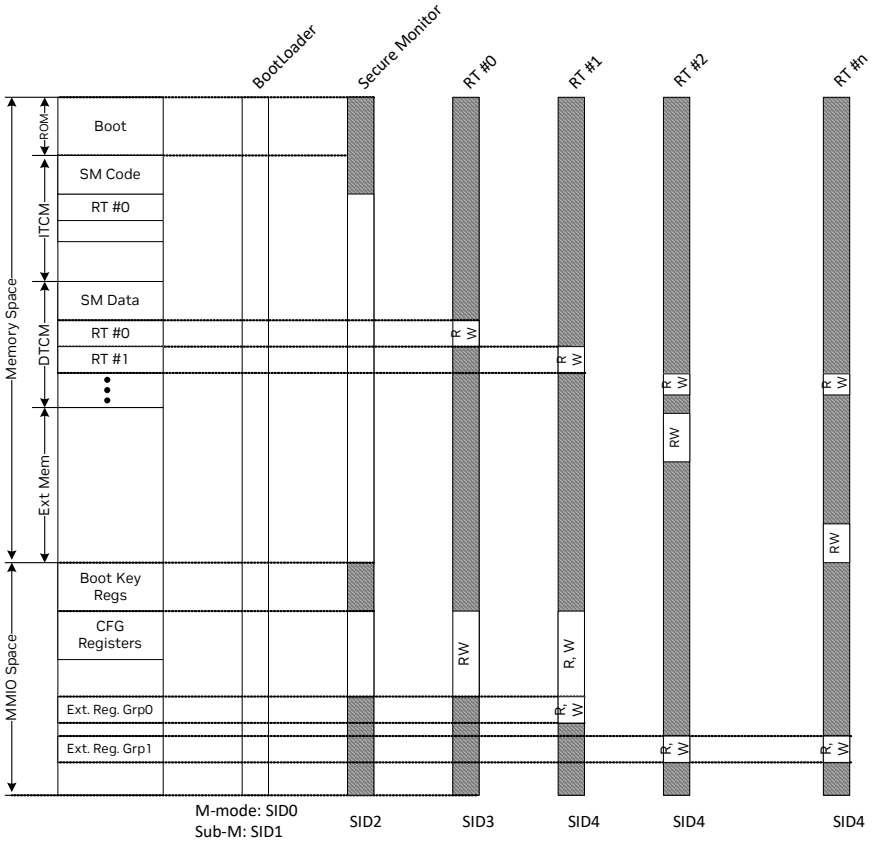
Example for Security Critical Configurations



- Setting up IOPMP rules stage by stage:
  - Boot Loader – Using highest prioritized entries and set lock
    - **Block any runtime** from accessing critical sections, e.g., key registers and ROM.
    - Minimal rules for Secure Monitor to run
  - Secure Monitor
    - Common IOPMP rules that needed for each RT

IOPMP Usage Model

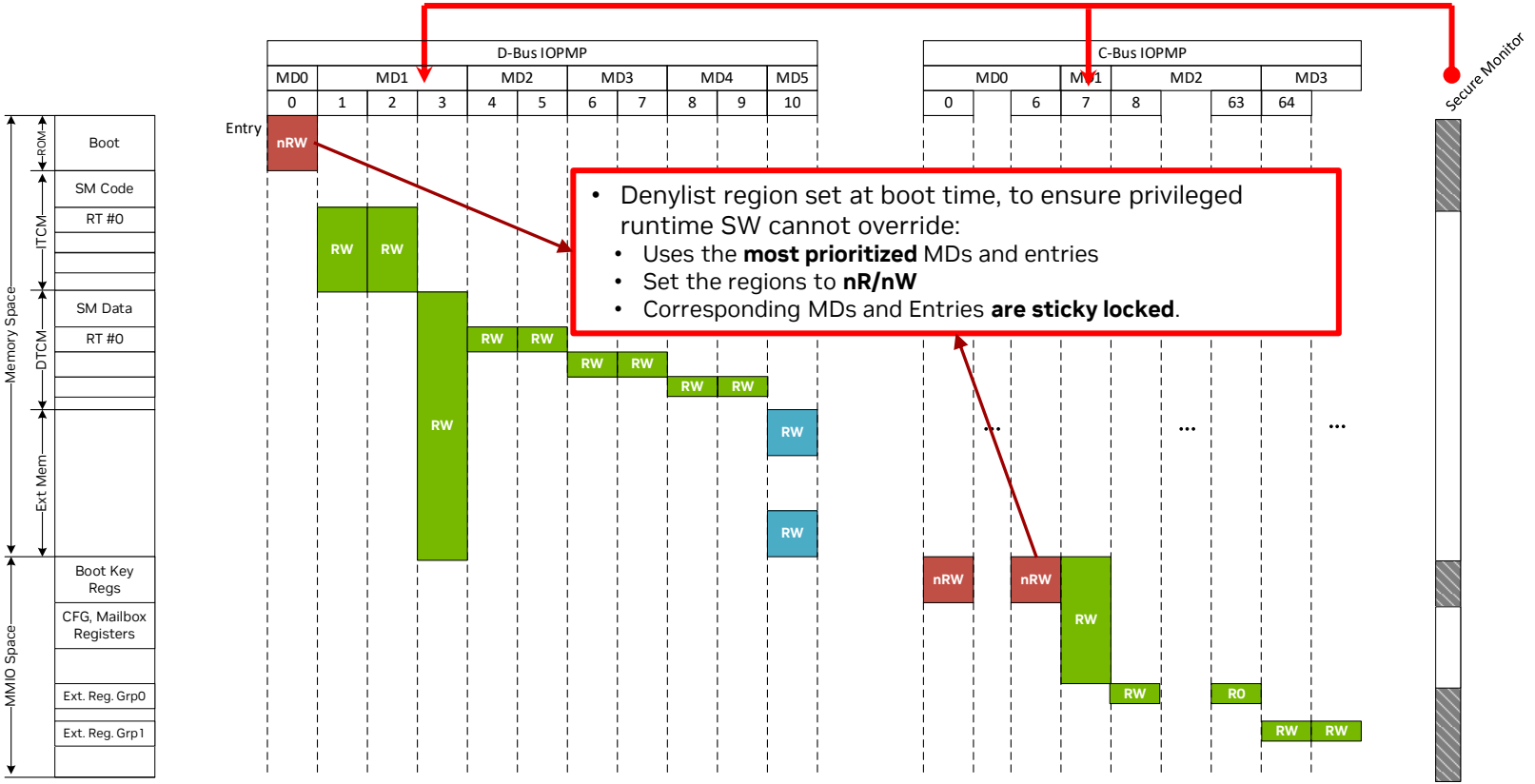
Example with Security Critical Configurations



- Sub-system Assumption:
  - Multi-hart RISC-V sub-system
  - Multiple RunTimes (RT)
  - Each RT is allocated with 1~2 SIDs
  - Security critical
- Boot Loader
  - Can access the entire address space
- Secure Monitor
  - Has no access to the Boot protected space and TCM region containing SM code.
  - Has r/w access to the rest of the address space.
- RTs
  - Only has access to each own memory region
  - Only has access to limit IO space

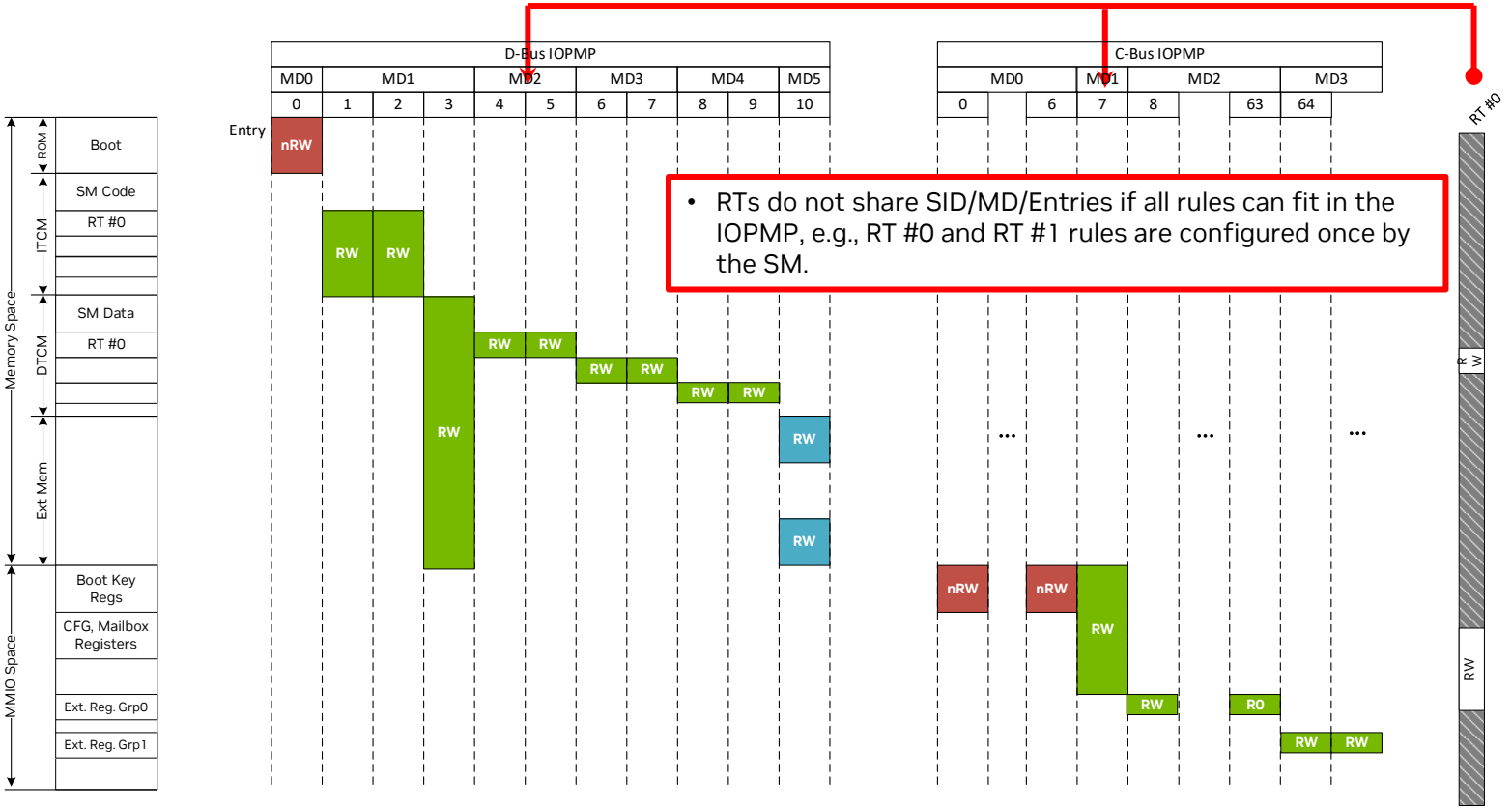
IOPMP Usage Model

Example with Security Critical Configurations



IOPMP Usage Model

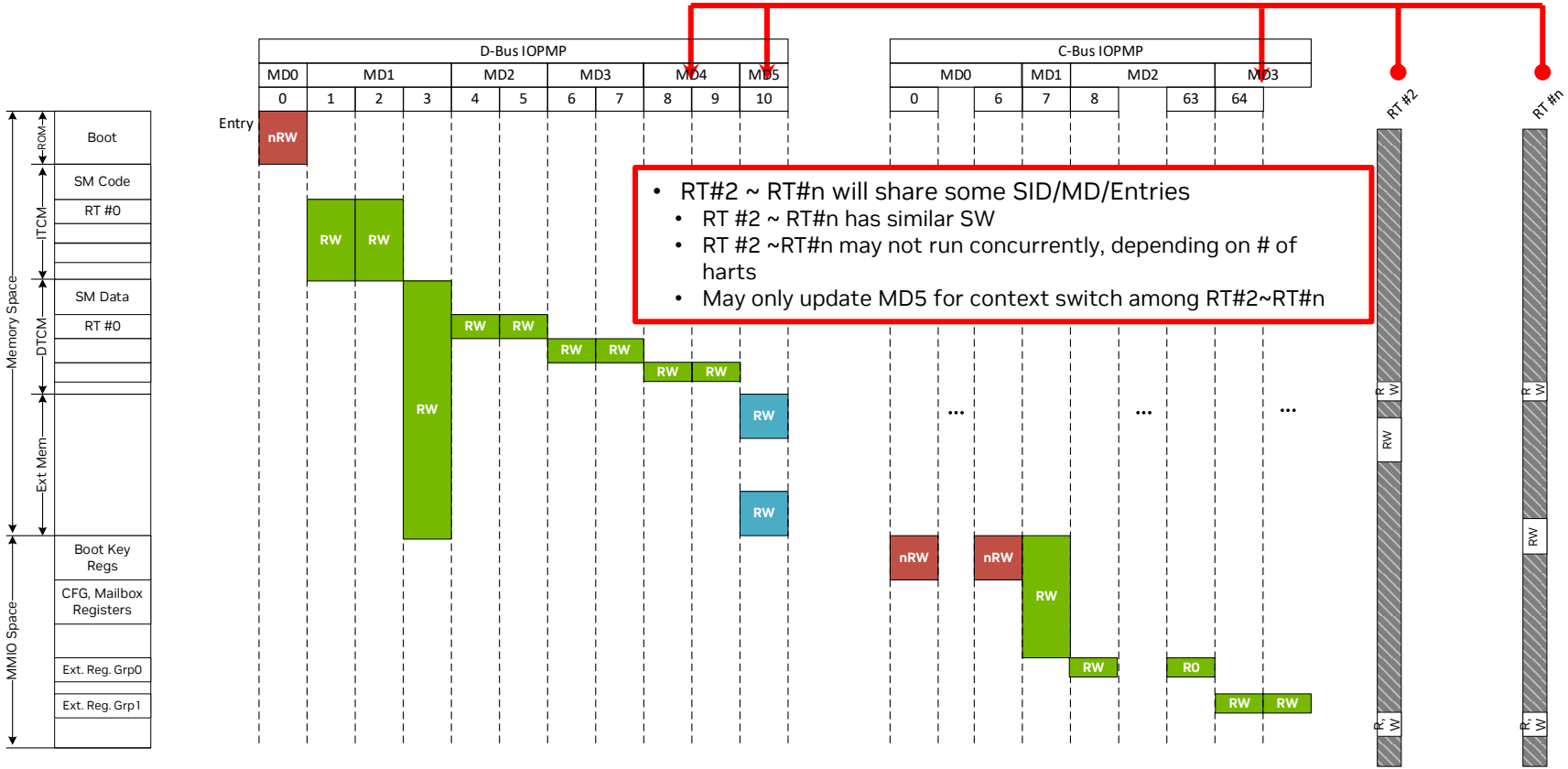
Example with Security Critical Configurations



- RTs do not share SID/MD/Entries if all rules can fit in the IOPMP, e.g., RT #0 and RT #1 rules are configured once by the SM.

IOPMP Usage Model

Example with Security Critical Configurations



Acknowledgement

I wish to acknowledge the contribution of colleagues from NVIDIA

- HW Team: Andy Ma, Howard Zhang, Xin Lv, Yudi Liu
- SW Team: Alon Shenfield, Marko Mitic, Yitian Chen