RISC-V-based Automotive Secure Framework

July 18, 2025

Paul Shan-Chyun Ku, Ph.D.
Andes Technology

Speaker: 辜善群 博士， Paul Ku, Ph. D.

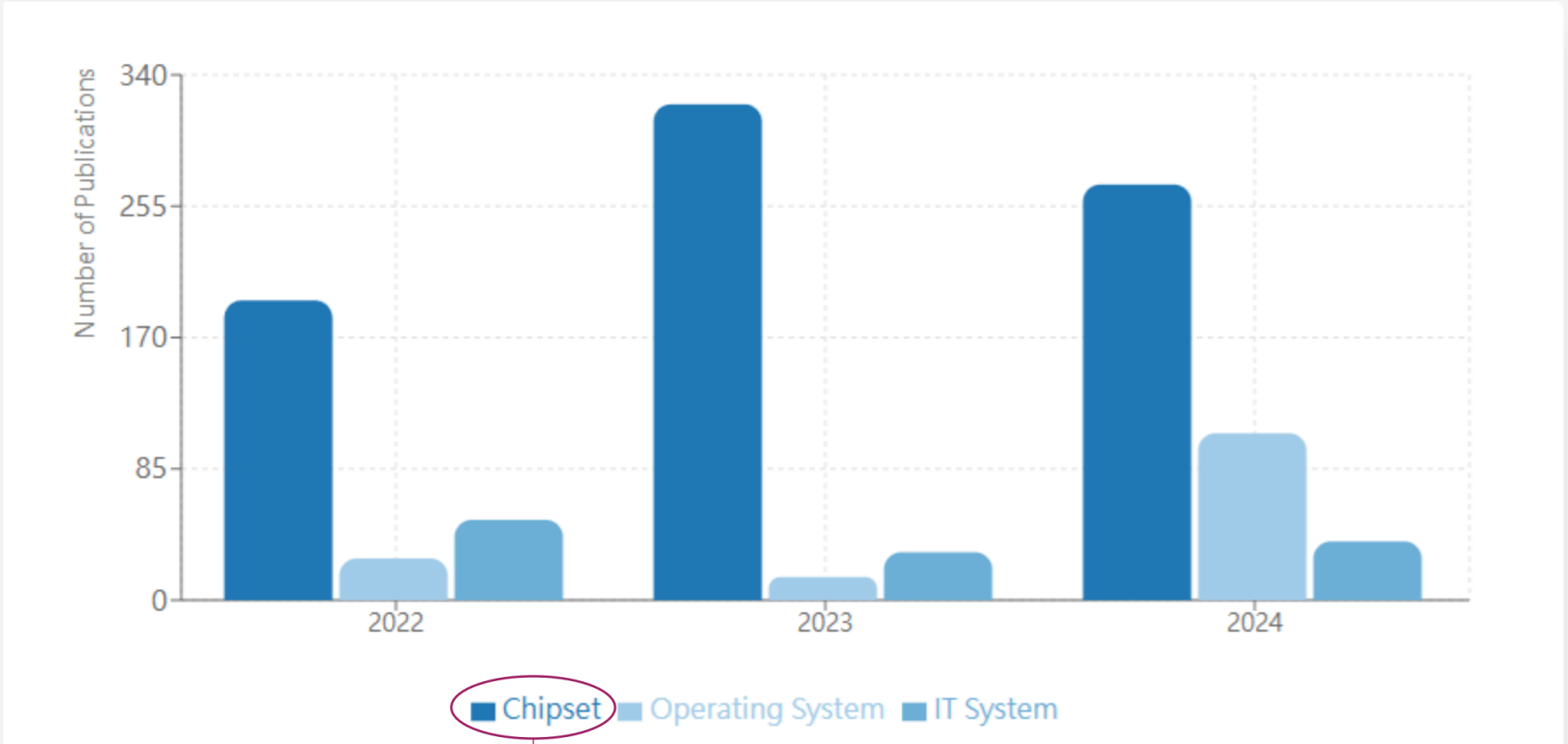
Experience:

- The Chair of IOPMP Task Group (2022-)
- The Vice-chair of TEE TG (2021-2022)
- Deputy Director, Andes Technology (2019-)

Outline

- The landscape of automotive vulnerabilities
- Real-time requirements of automotive requirement
- Explore RISC-V security components from real-time:
  - Memory isolations
  - Interrupts isolations
- AndeSentry automotive secure framework

Distribution of Automotive Major Vulnerabilities Published



Shifting Gears VicOne 2025 Automotive Cybersecurity Report

backdoors, microarchitectural attacks, and side-channel exploits

Taking RISC-V® Mainstream

Estimated Cost of Cyberattacks

Cost Category	2022	2023	2024
Data Leakage	$4.0M	$9.7B	$20.0B
System Downtime	$802.7M	$2.5B	$1.9B
Ransomware Damage	$242.8M	$523.6M	$538.2M
Total	**$1.0B**	**$12.8B**	**$22.5B**

Note: M = Million, B = Billion.

Shifting Gears VicOne 2025 Automotive Cybersecurity Report

Taking RISC-V® Mainstream

Smart Devices Regulatory Landscape

European Union

- GDPR
- Cybersecurity Act
- Cyber Resilience Act (CRA)
- NIS2 Directive

United States

- NIST Cybersecurity Framework 2.0
- SEC Reporting Requirements
- Cyber Trust Mark Labeling

United Kingdom

- Product Security & Telecommunications Infrastructure (PSTI) Bill

2025 Global Automotive and Smart Mobility Cybersecurity Report (Upstream)

ASIL and Real-time Response

- What is ASIL?
  - Automotive Safety Integrity Levels classify the safety requirements of vehicle systems.
  - Levels range from ASIL-A (lowest risk) to ASIL-D (highest risk).
- Why Real-Time Response Matters?
  - Predictability & Reliability: Automotive systems must operate within defined timeframes.
  - Error Detection & Recovery: Quick responses help identify and correct faults before they escalate.
  - Driver Assistance: Functions like Lane Departure Warning (LDW) and Adaptive Cruise Control (ACC) rely on real-time data.
  - System Coordination: Real-time communication ensures different vehicle components work in sync.

RISC-V Security Components

- For virtualization, the most important items:
  - Memory isolation:
    - Page-based/TLB-based: MMU, xMPT, IOMMU
    - Register-based: ePMP, sPMP, IOPMP
  - Interrupt isolation:
    - PLIC, AIA

Page-based Memory Isolation

- MMU:
  - First-stage address translation:
    - Used by OS → isolate OS and its user applications
  - Second-stage address translation:
    - Used by Hypervisor → isolate Hypervisor and its Oses
  - TLB is cache of tree-structured page tables
    - A TLB miss could cause multiple TLB misses in worst case, and these TLB missies could cause more.

    ➢Such a large uncertainty is not preferred over a stringent real-time requirement.
- xMPT:
  - A page table based physical memory protection, that is, it is also TLB-based.

Register-based Memory Isolation

- PMP/ePMP:
  - Control access permissions for different memory regions, ensuring protection against unauthorized reads, writes, and executions by the access from M-mode or the rest modes.
- sPMP/xsPMP:
  - Control access from S, U, HS, VS, and VU-mode
- IOPMP:
  - Control access from individual I/O agents, identified by their RRIDs, Requestor Role ID.

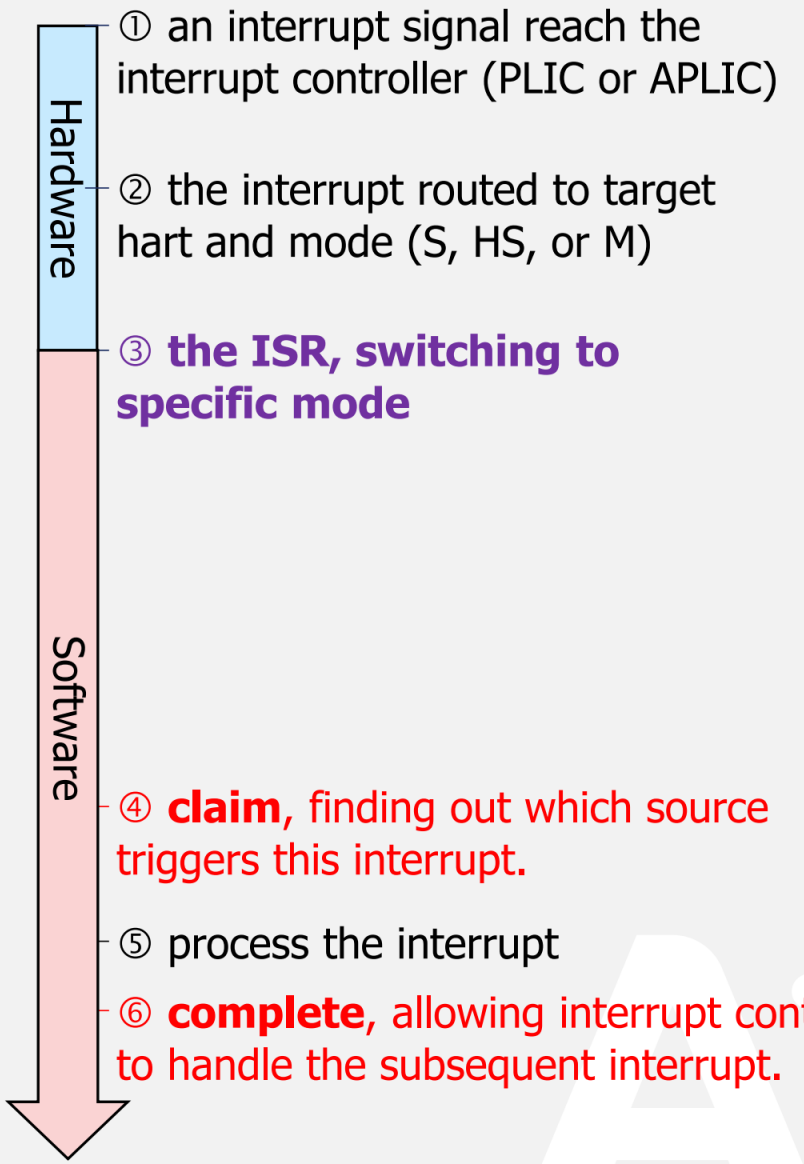
➢Their check latency can be easily implemented as a fixed time.

Taking RISC-V® Mainstream

Interrupt Latency Analysis

Multiple OSes can share a hart:

A hart dedicate for an OS:



③ ISR must enter M-mode:
3.1: save the context of previous OS,
3.2: clean all REGs/CSRs,
3.3: restore all REGs/CSRs of target OS, and
3.4: jump to target OS

3.5: target OS's preamble

③ ISR directly enters S/HS-mode:

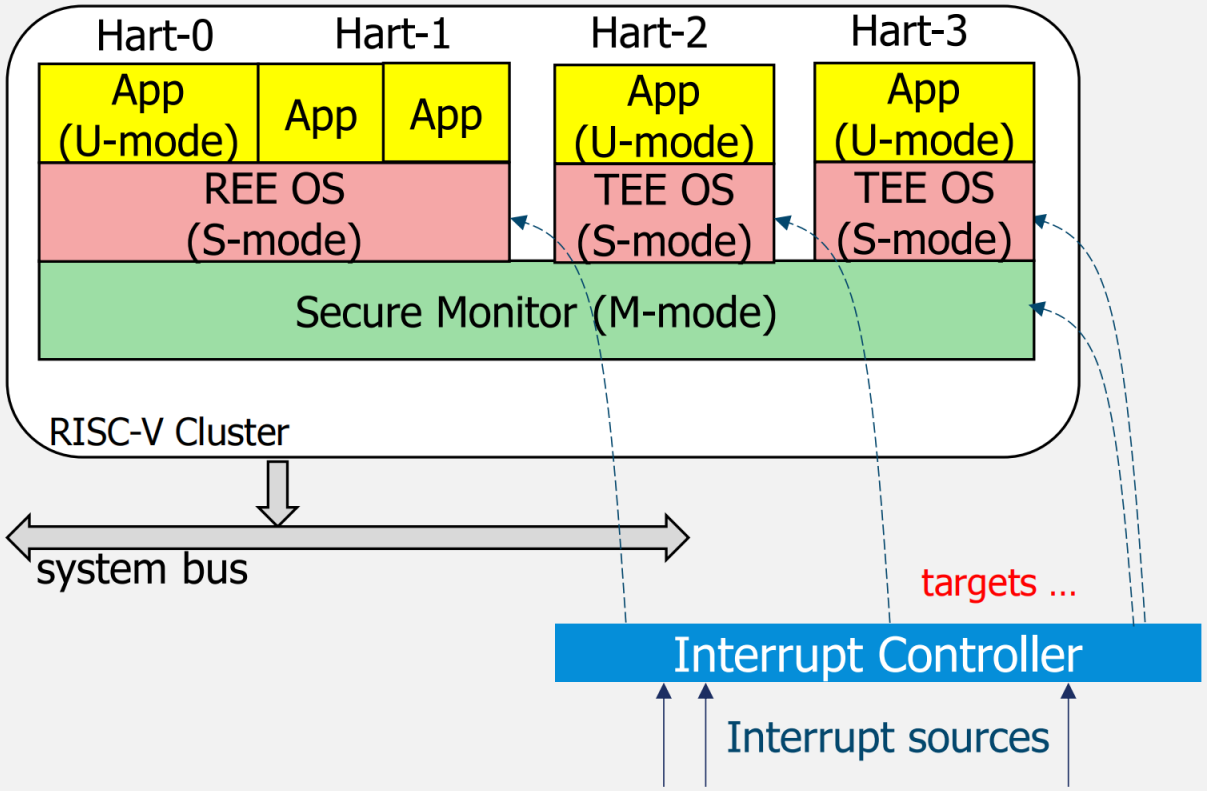
3.5: target OS's preamble

Sharing a Hart not a Favorite for Real-time

- Step 3.1 ~ 3.4 take cycles: hundreds to thousands
  - CSRs and registers
    - General purpose
    - Floating point
    - Memory isolation: ePMP, sPMP, and/or satp
    - Other machine status
  - Memory write and read

- For stringent real-time demands, multiple OSes should not share a hart.

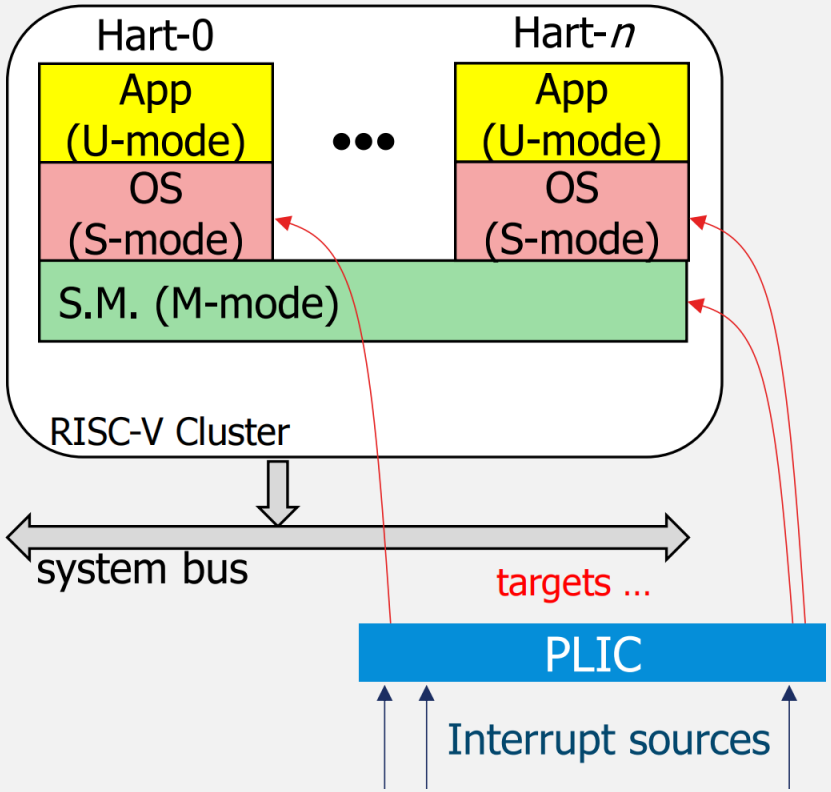
Execution Environment Arrangement



- A hart is dedicated for an OS.
- An OS can have multiple harts

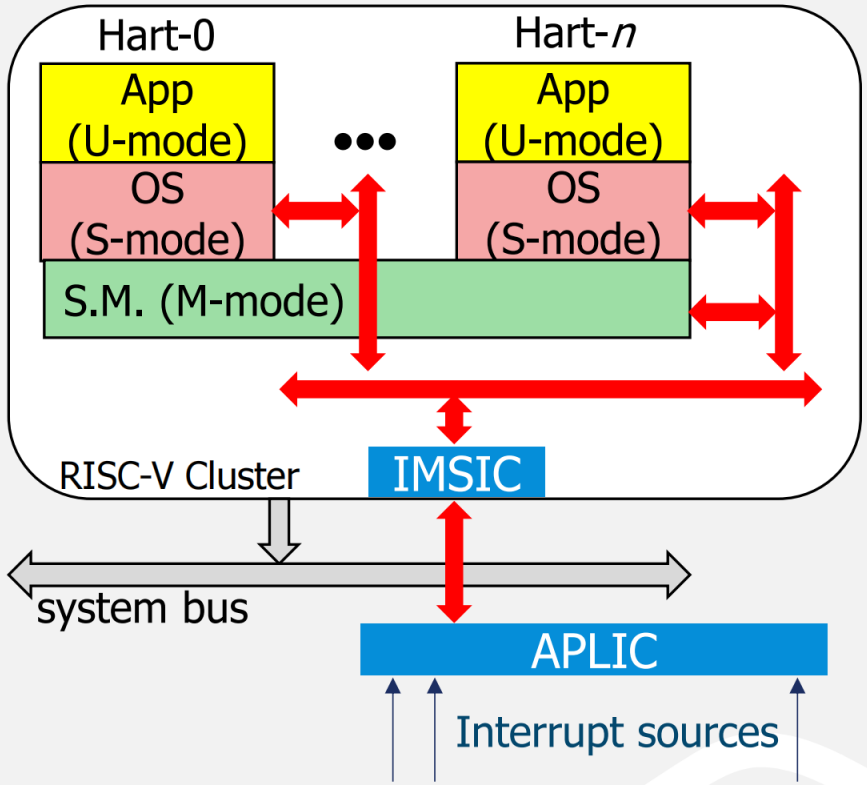
Interrupt Latency of PLIC and AIA

- Interrupt Routing



dedicated wires to specific **targets**:
e.g., hart0.M, hart0.S, hart1.M, hart1.S, ...

PLIC-based Intr Routing



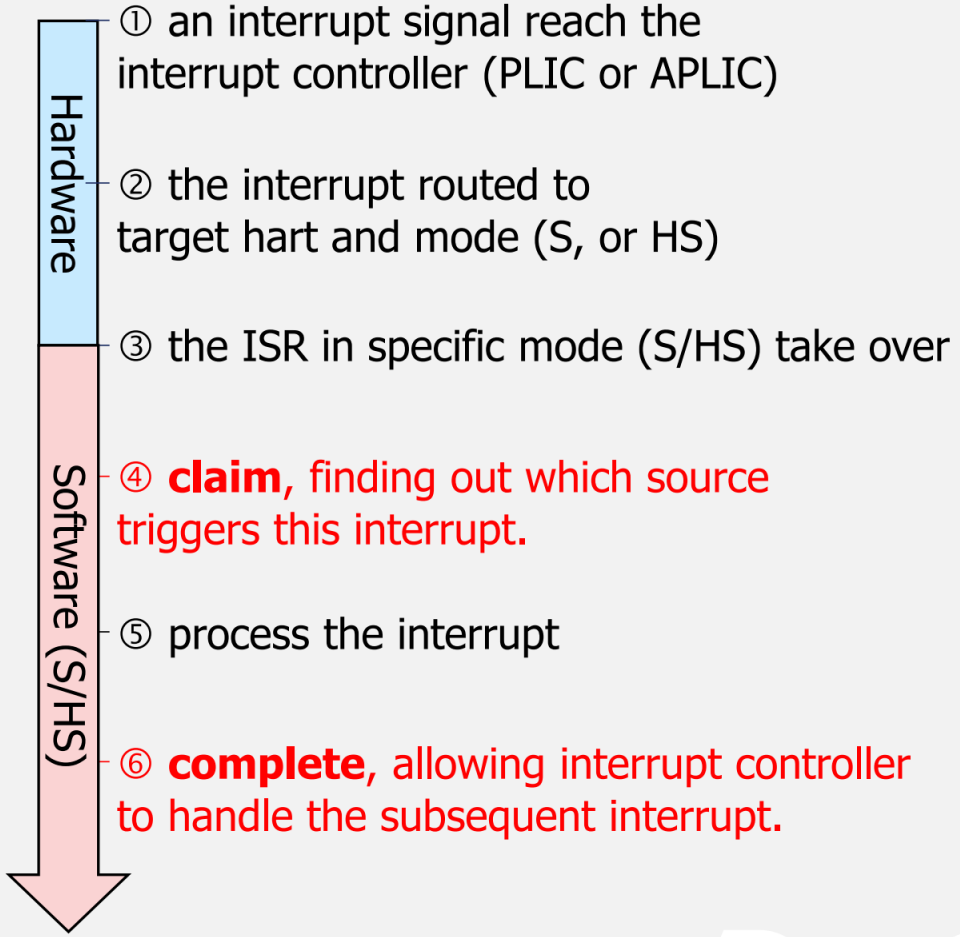
An MSI bus to all **targets**, routing by MSI-address
hart0.M, hart0.S, hart1.M, hart1.S, ...

AIA-based Intr Routing

Interrupt Timing Diagram

PLIC:

AIA:



④: a MMIO read if every OS has a target.

⑥: a MMIO write if every OS has a target

④: single S-mode CSR read

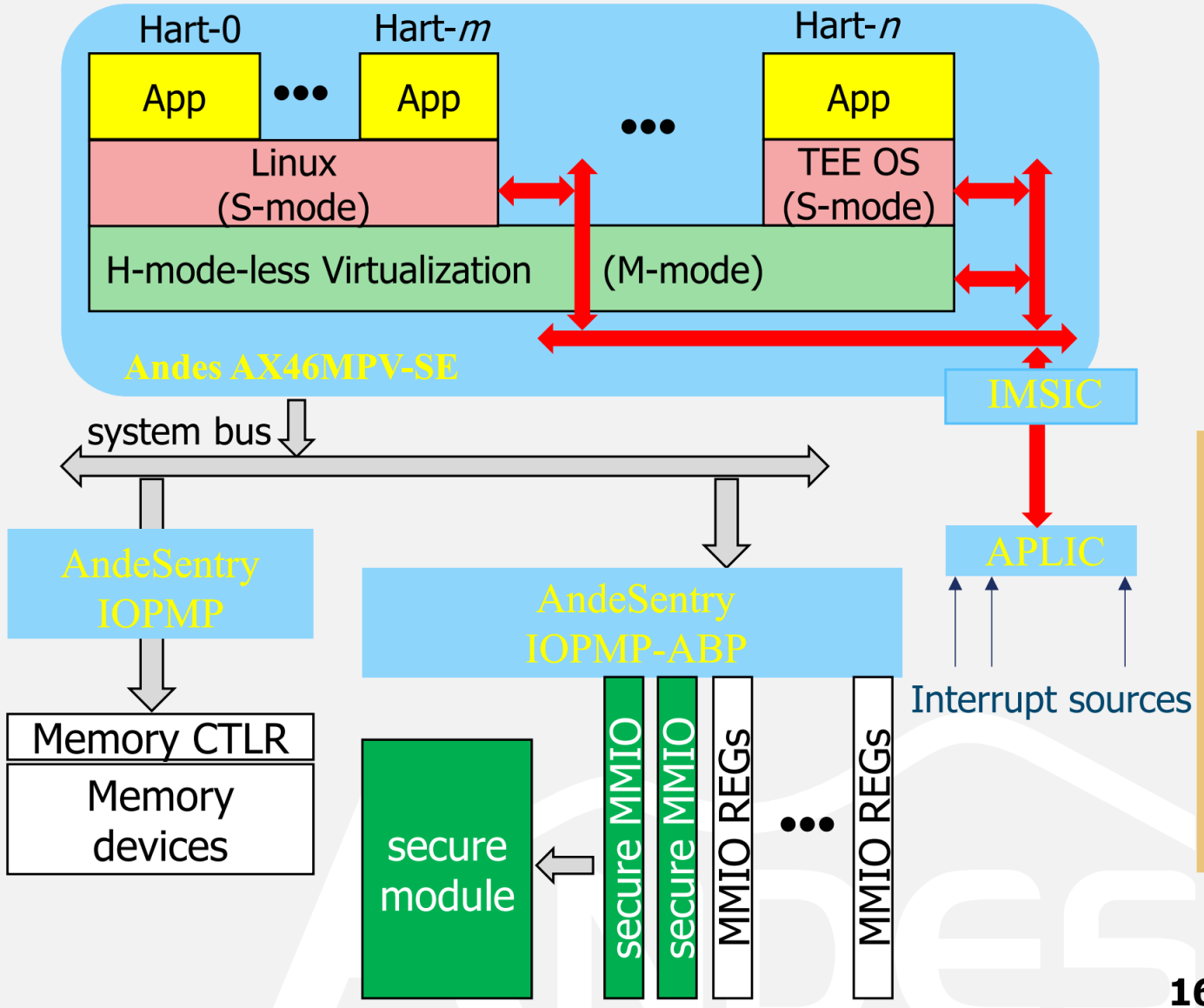
⑥: not needed

Taking RISC-V® Mainstream

AndeSentry Automotive Secure Collaboration Framework

Example AndeSentry Automotive Secure Platform Framework

- AX46MPV-SE:
  - Safety CPU + vector ISA
- IOPMP:
  - Device access isolation
- AIA: (IMSIC + APLIC)
- Secure Module (by partners):
  - TRNG, Crypto Eng
  - PUF, secure storage
- H-mode-less virtualization (partners):
  - Running on M-mode
  - ePMP-based isolation
  - sPMP used by TEE OSes
  - MMU used by Linux



Thank you!!

Andes in D25

Taking RISC-V® Mainstream