Constructing Trusted Execution Environments Using RISC-V

Andes Technology Marketing Division

Senior Technical Manager

Warren Chen

Andes at A Glance

Who We Are

CPU

Pure-play
CPU IP Vendor

Active Open-Source
Contributor/Maintainer

RISC-V Founding
Premier Member

Stock Exchange Listed

RVI board: Frankwell Lin
RVI TSC: Charlie Su
RVI RVP TG chair: Rich Fuhler
RVI IOPMP TG chair: Paul Ku
RVI Marketing Events Committee Chair: Hsiao-Ling Lin
RVI Fast interrupt vice-chair: Kevin Chen
RISE board: Charlie Su, Rich Chuang
RISE TSC: Simon Wang, Tim Ouyang
RISE System Library WG Lead: Ruinland Tsai
CIP TSC: Simon Wang, Tim Ouyang

Quick Facts

20
Years Old
Public Company

80%
R&D
Employees

16B+
Total Shipment of
Andes-embedded SoCs

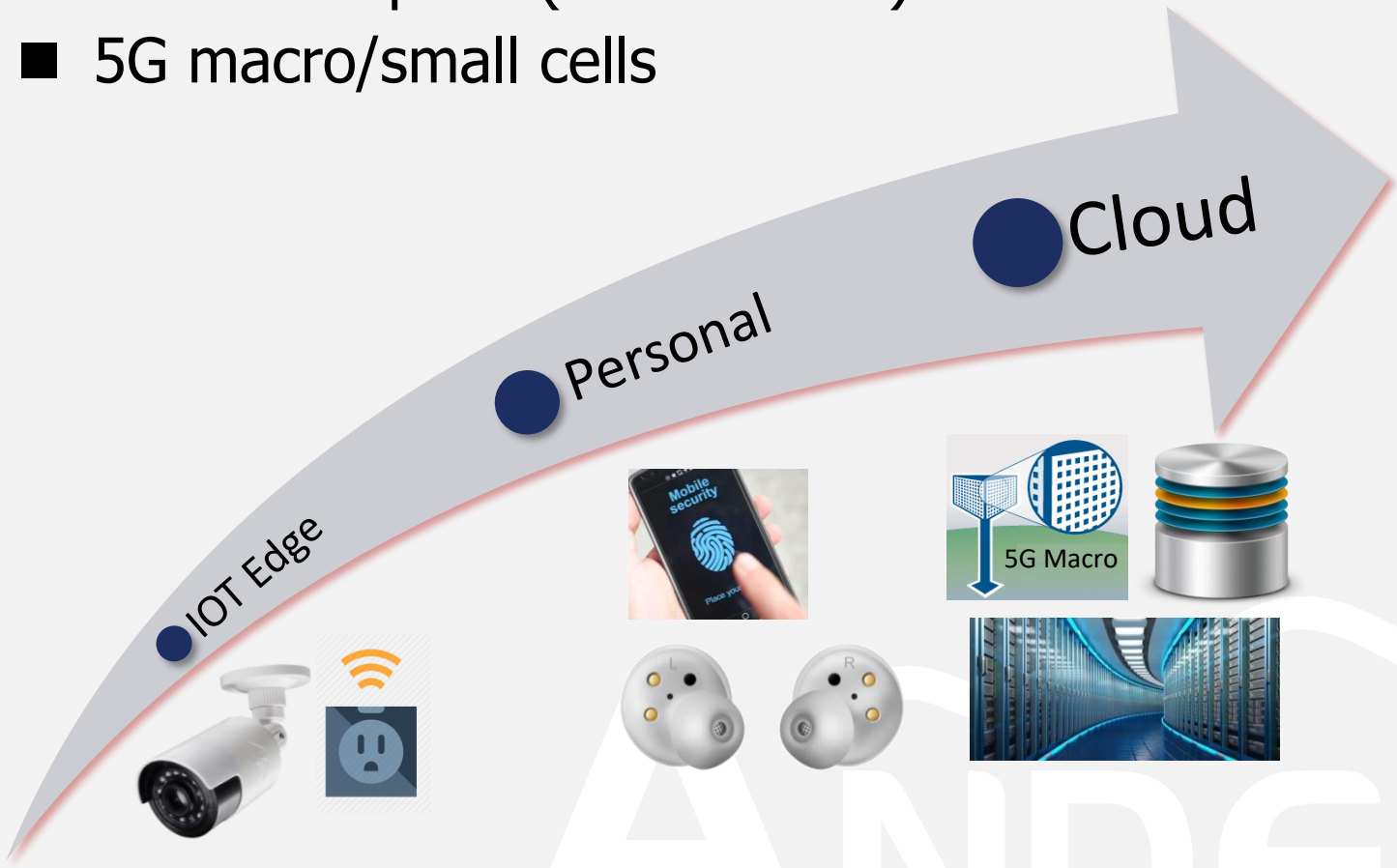
400+
Worldwide
Licensees

100K+
AndeSight IDE
Effective Users

Taking RISC-V® Mainstream

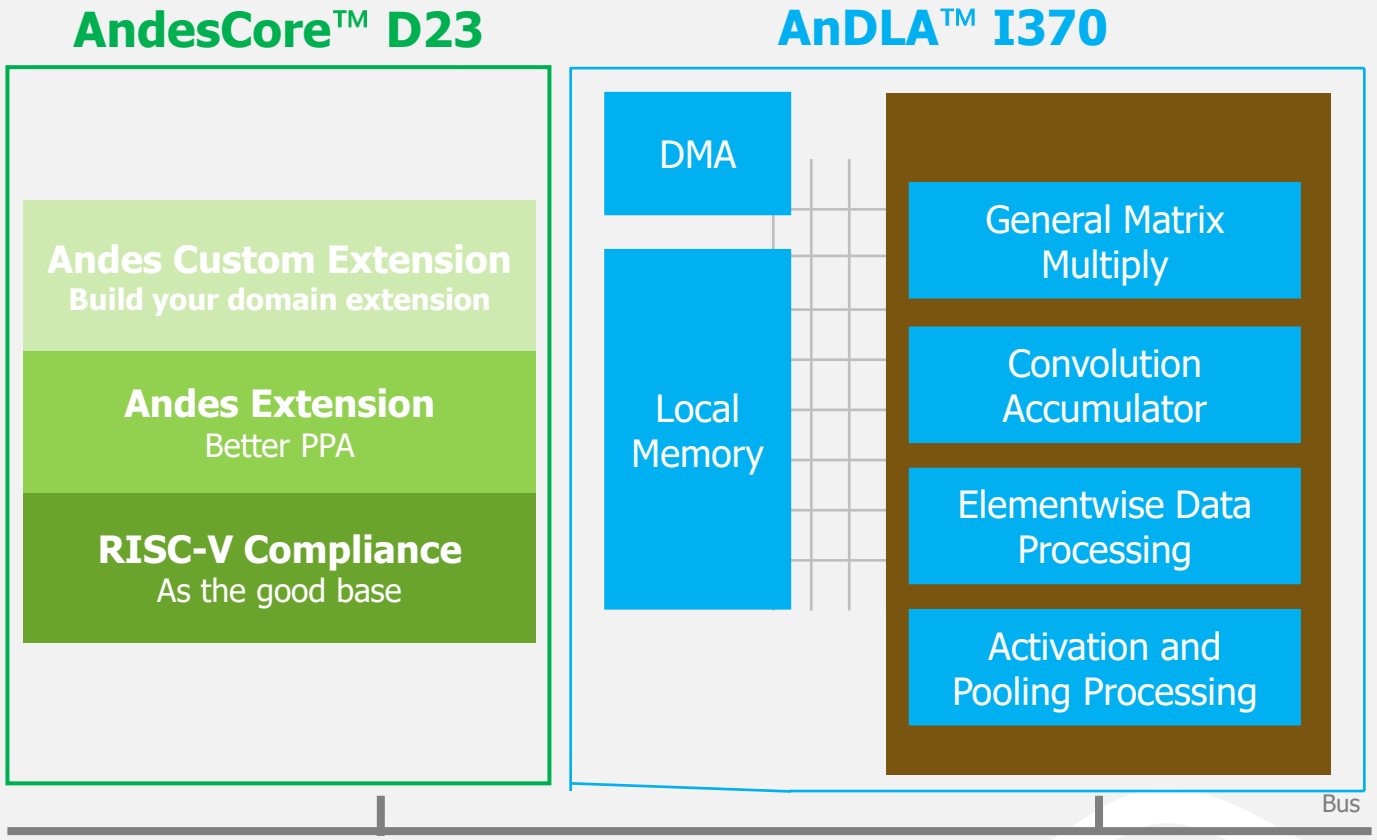
V5 Adoptions: From MCU to Datacenters

- Edge to Cloud:
  - ADAS
  - AIoT
  - Blockchain
  - FPGA
  - MCU
  - Multimedia
  - Security
  - Wireless (BT/WiFi)
- 1 to 1000+ core
- 40nm to 7nm
- **Many in AI**
  - Datacenter AI accelerators
  - SSD: enterprise (& consumer)
  - 5G macro/small cells



Edge AI Subsystem: D23 + I370

- **D23:** AI Control & future-proof
  - RISC-V compliant extensions
    - 32-bit 3-stage pipeline & partial dual-issue
    - IMAFD, **C/Zc (16-bit),** B (bit-manipulation), K (scalar crypto), CMO (cache management)
  - AndeStar™ V5 extensions
    - Performance (15% Coremark/Dhrystone gain)
    - CoDense™ (12% code size reduction)
    - StackSafe™ (stack protection)
    - PowerBrake (power throttling)
    - WFI/WFE (quick to sleep)
  - Andes Custom Extension™
- **AnDLA I370:** AI computation
  - CNN/RNN, INT8/IN16
  - Image/video & speech/voice
  - up to 2 TOPS (INT8 @1GHz)
  - 900MHz @28nm
  - Power efficiency ~5 TOPS/W (@28nm logic only)



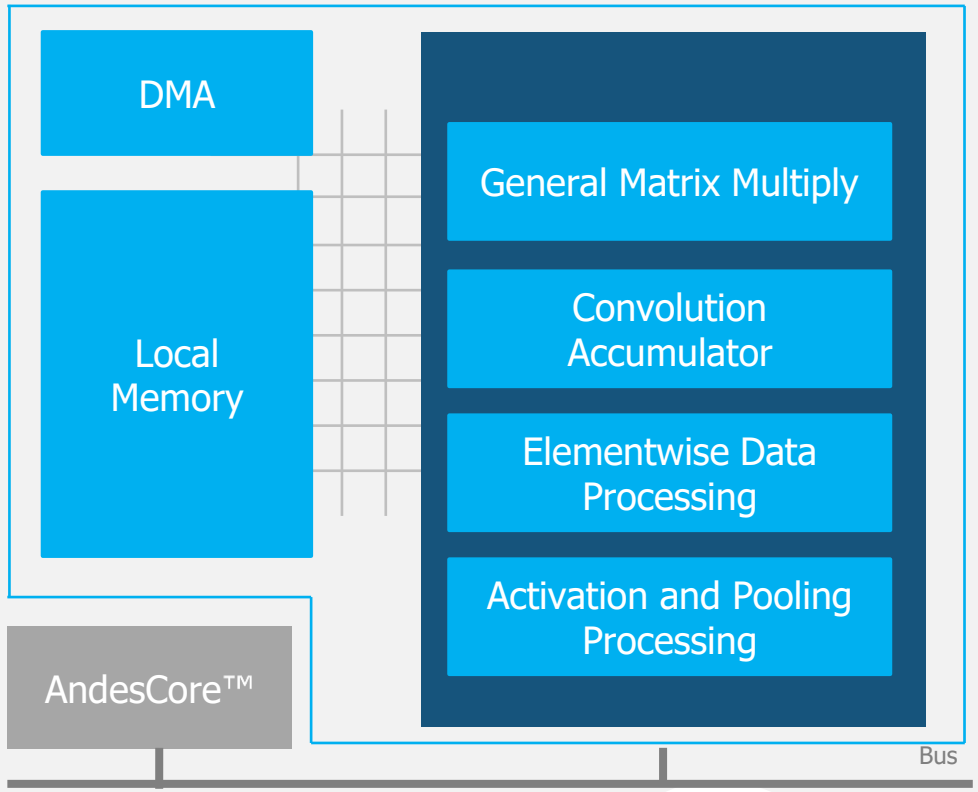
Taking RISC-V® Mainstream

AndesAIRE™ AnDLA™ I370

PPA-optimized Andes DLA (AnDLA) for edge and end-point inference

- Target NN applications
  - Image and video
  - Speech/voice and audio
- Target performance
  - Configurable MACs: **64, 256, 1024** (INT8)
  - Performance: **up to 2 TOPS** (INT8 @1GHz)
  - Datatype: **INT8, INT16**
  - Configurable local memory: **16KB to 4MB**
  - Power efficiency ~5 TOPS/W (@28nm logic only)
  - Can use with any AndesCore™
- Integrated DMA and local memory
- Multi-bank memory and crossbar
- Operator fusion for reducing memory access

AnDLA™ I370



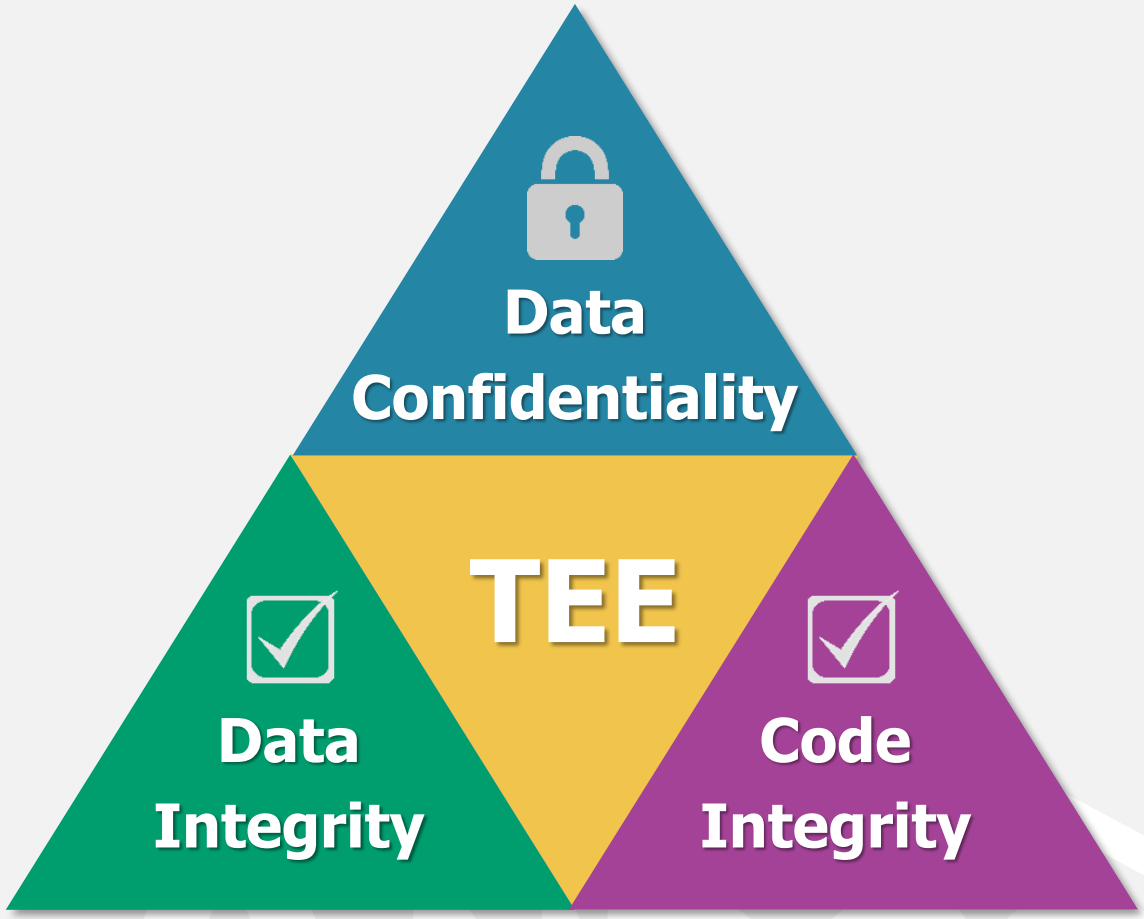
Security from SoC Point of View

- Secure Boot
  - Ensure first-stage bootloader (FSBL) integrity
- Secure Firmware Update
  - Upgrade new FW and anti-rollback
- Trust Execution Environment
  - Create a Secure Enclave for security-critical application
- Encryption
  - Protect Data (at Rest, in Motion, in Transmit)
- Secure Storage
  - Data at Rest protection
- Physical Attack Defense
- Confidential Computing

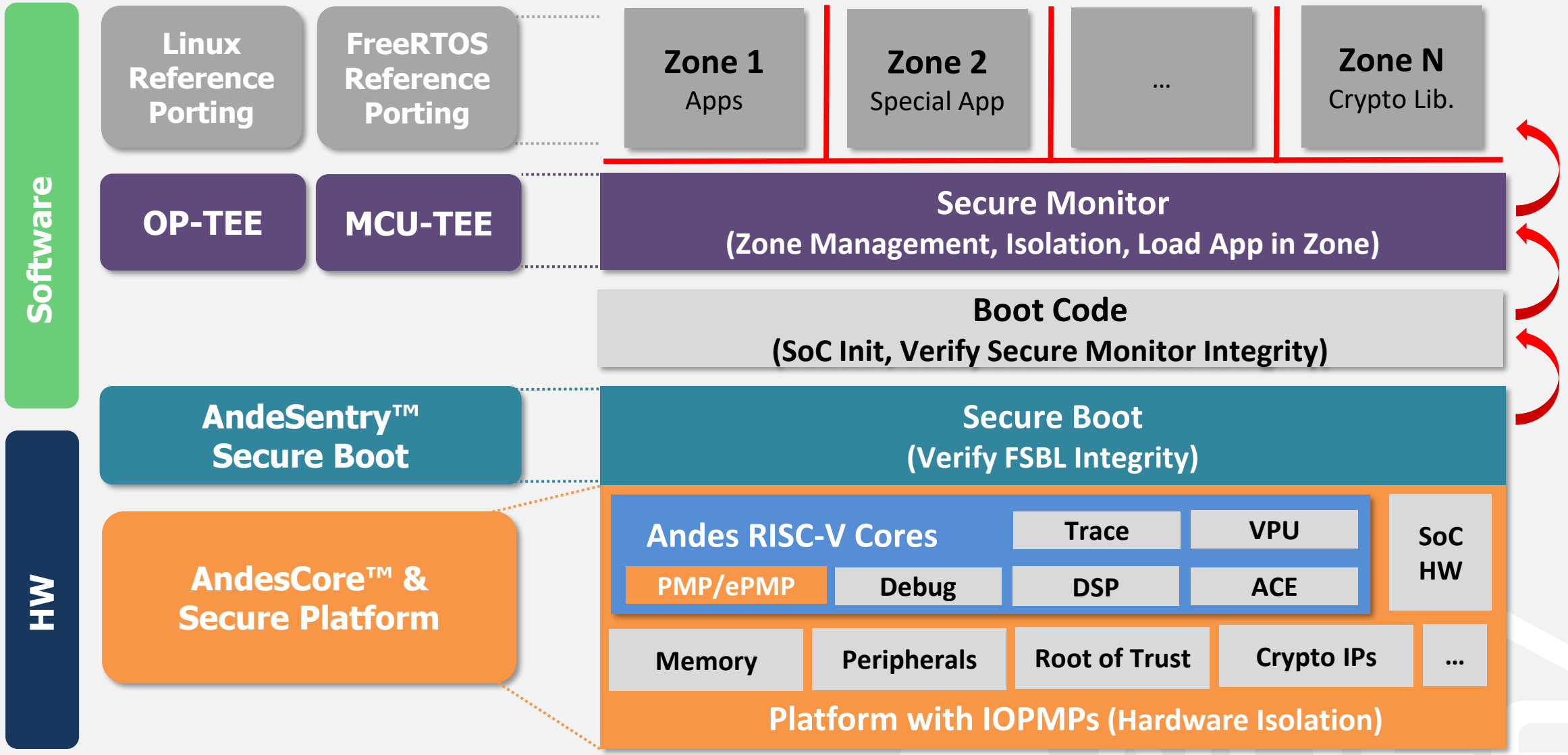
Trusted Execution Environment

- Isolated secure area within the processor
  - Secure Execution
  - Data Confidentiality
  - Security Domain Isolation
  - Integrity Protection

- Isolated execution environment
  - Hardware isolation mechanism
  - Software helps manage isolated zones

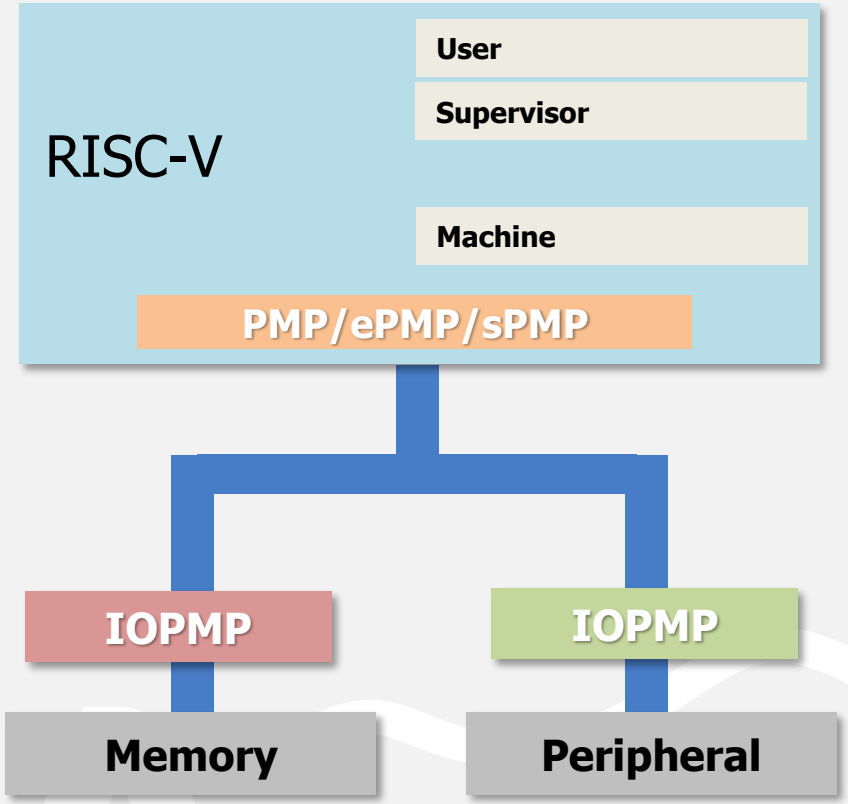


Andes TEE Solutions



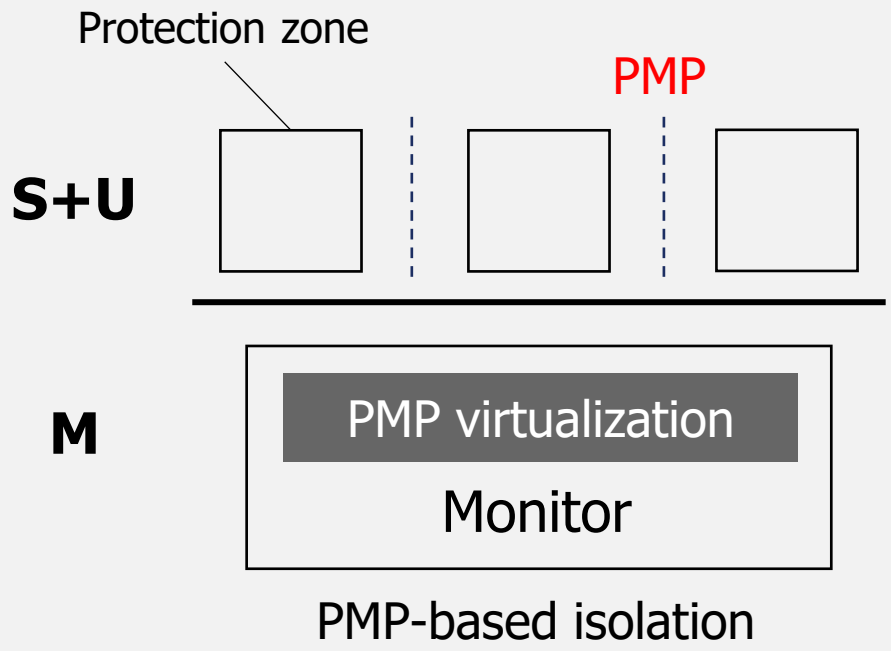
Construct Hardware Isolation in RISC-V

- RISC-V PMP
  - Memory Access Privilege
- RISC-V IOPMP & IOMMU
  - Memory Access Control
  - Peripheral Access Control
- RISC-V AIA
  - Interrupt Isolation
- RISC-V provides flexibility due to multiple zone support



RISC-V PMP/ePMP (Enhanced) Physical Memory Protection

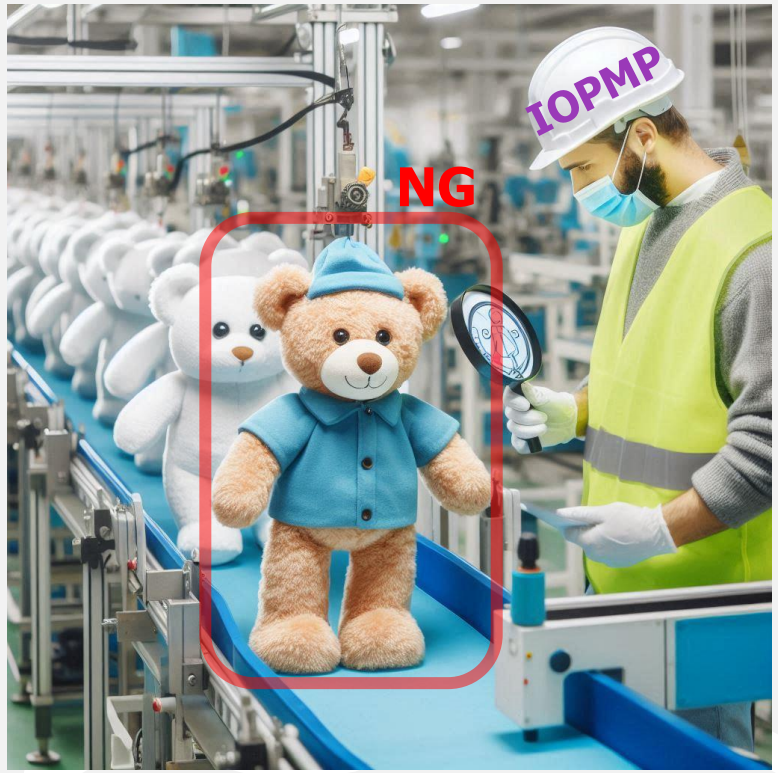
- PMP controls **physical address accesses** in RISC-V cores according to **privilege modes**
  - S/U-mode or M-mode
  - Read/Write/Executable
  - Specific entries can be locked down
- ePMP (An Enhancement of PMP)
  - Prevent high-privileged processes to
    - Use the data of the less-privileged process
      - Supervisor Memory Access Prevention (SMAP)
    - Execute code of the less-privileged process
      - Supervisor Memory Execution Prevention (SMEP)
  - Block unallocated regions by default
  - Restrictions of shared memory regions



PMP-based isolation

RISC-V IOPMP Overview

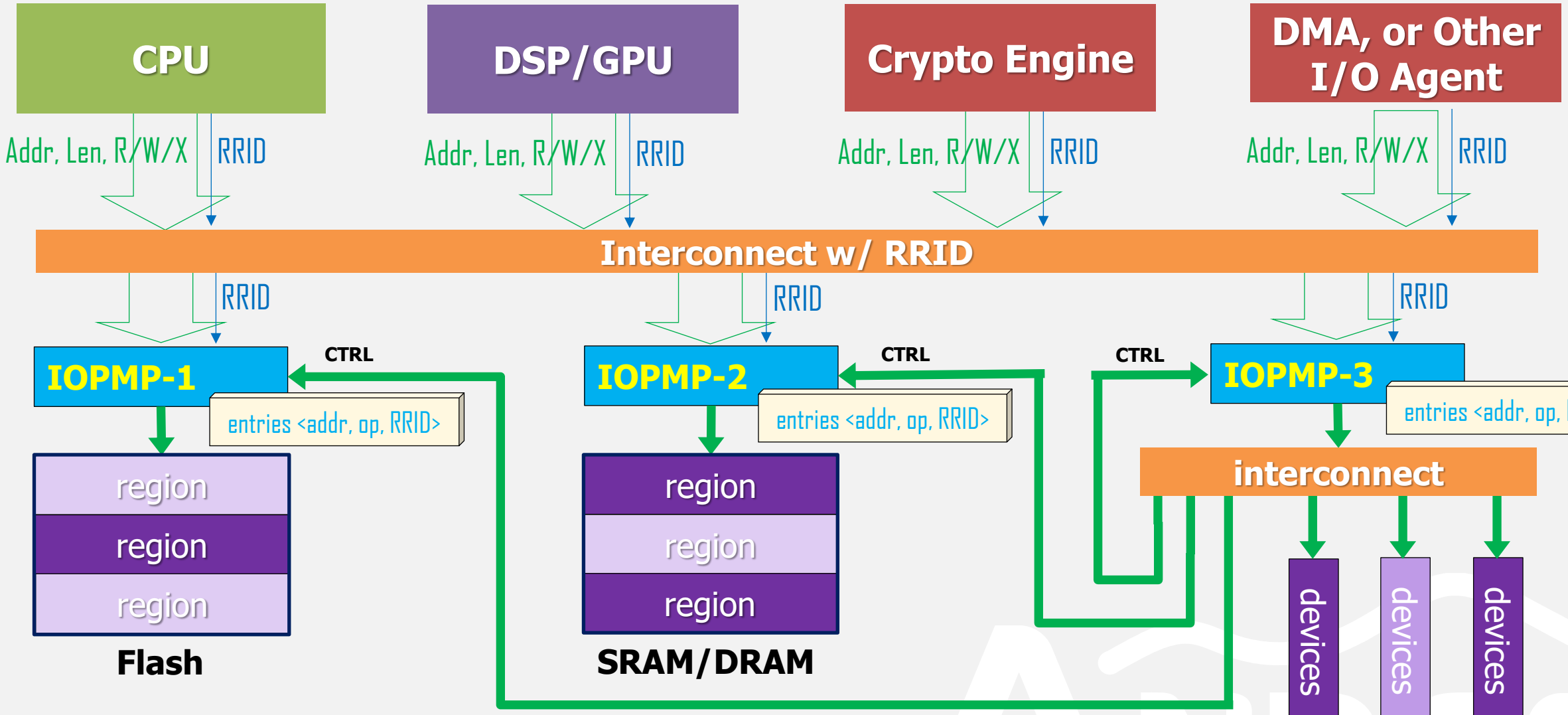
- Andes/nVidia Chair/Co-chair of RISC-V IOPMP Task Group
- Checker with a set of ordered entries
  - lower order entry with higher priority
- Check a transaction by
  - Address/Length
  - Operation (R/W/X)
  - Initiator (RRID)
- Provide mechanisms to react to violations



RISC-V®

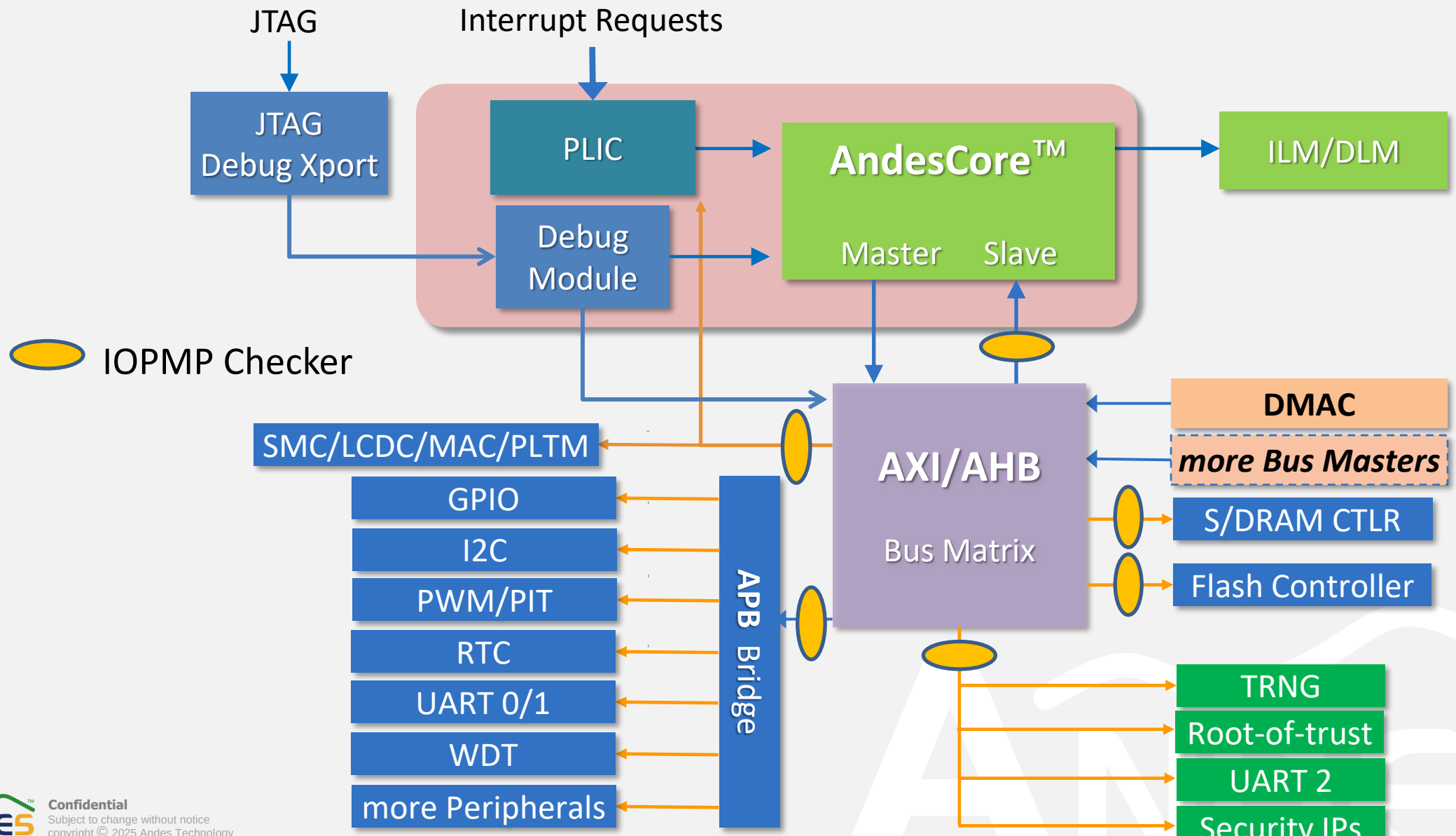
Taking RISC-V® Mainstream

Platform with IOPMPs



RRID: Requester Role ID

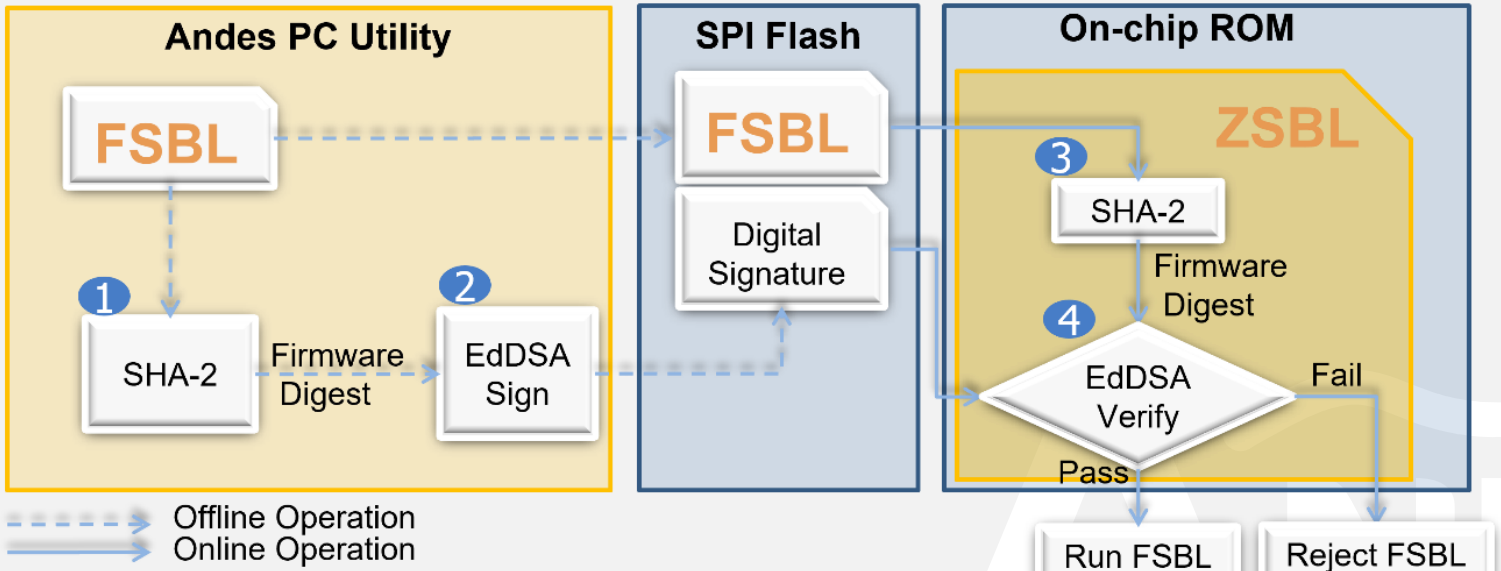
AndeSentry™ Secure Platform Framework



Taking RISC-V® Mainstream

AndeSentry™ Secure Boot Mechanism

- Pure software solution and support RISC-V scalar/vector crypto
- Secure Boot is a verification mechanism to ensure FSBL integrity
  - Manufacturing (Step1 & Step2)
    - PC utility signing (EdDSA/RSA2048) the first stage bootloader (FSBL) and writing to storage
  - Boot
    - (Step3) ZSBL with Andes software library to get the digest of the FSBL image
    - (Step4) Verify the integrity of the FSBL to determine whether to run or reject



Secure Firmware Update

- Ensure that **authentic**, **verified**, and **tamper-proof firmware** is installed on a device
- Key Features
  - Cryptographic Signing
  - Secure Boot Integration
  - Rollback Protection
  - Integrity Checks before update

Secure Boot

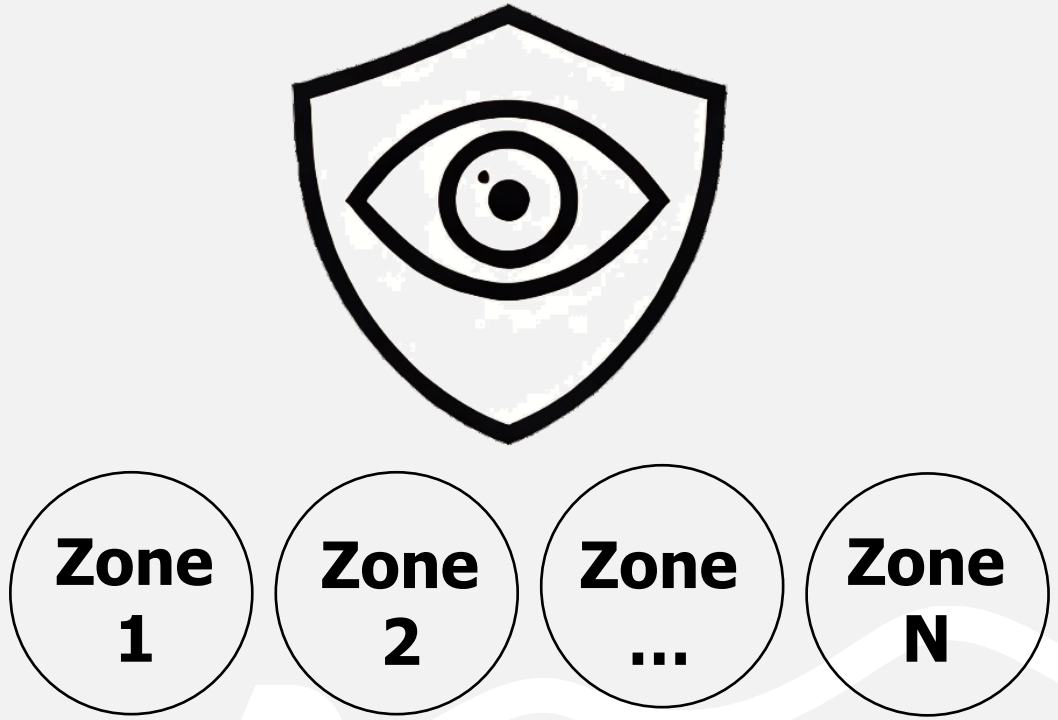
Signature

Anti-Rollback

Taking RISC-V® Mainstream

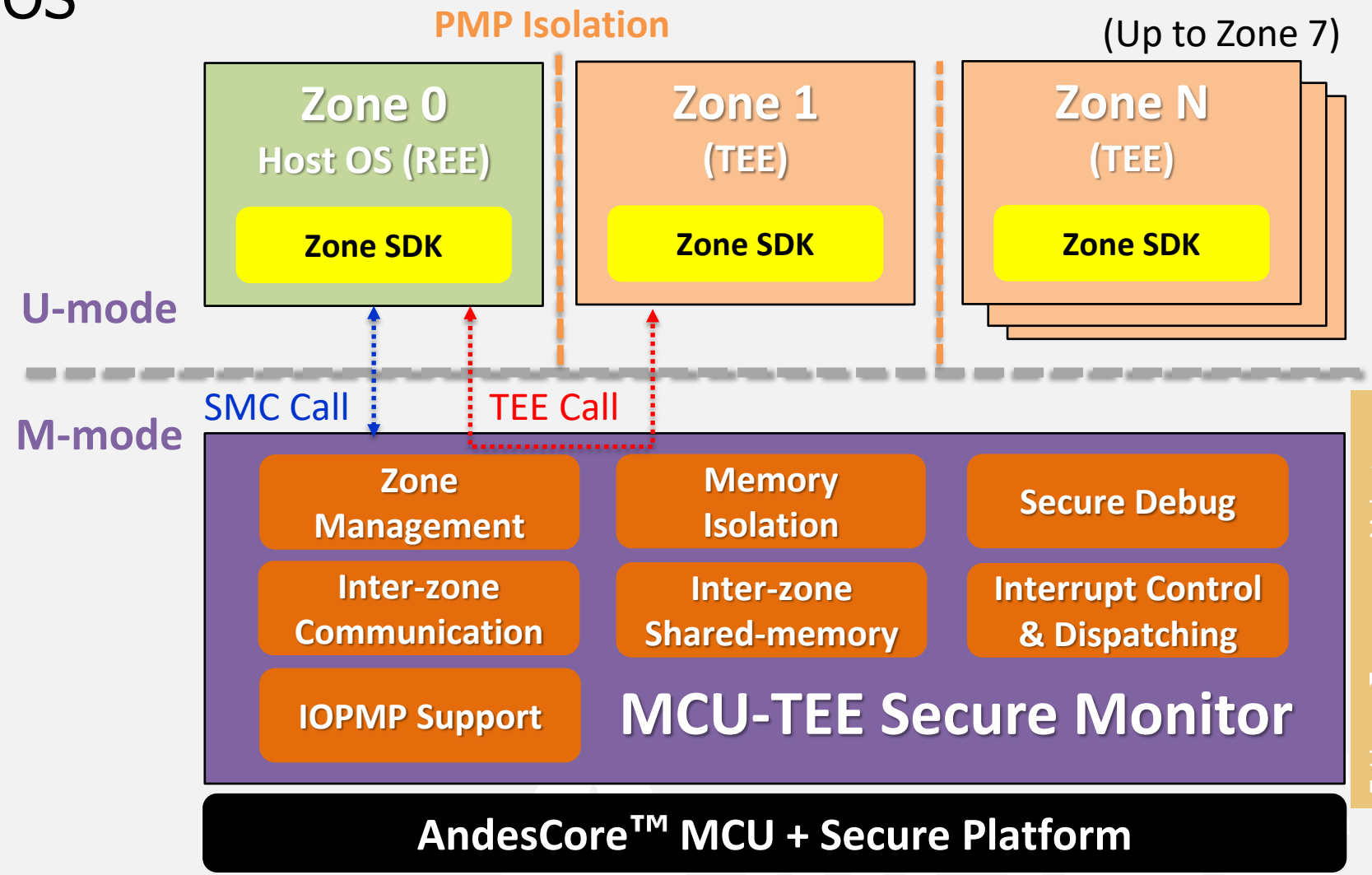
Secure Monitor

- A privileged software manages the transition between
  - Secure zones
  - Non-Secure zones
- Key Features
  - Context Switching
  - Memory Isolation
  - Exception Handling
  - Secure System Calls (SMC)
  - Enforcement of Security Policies



AndeSentry™ MCU-TEE Secure Monitor

- For single hart and RTOS
- Target Environment
  - Work with M+U mode
  - BareMetal/FreeRTOS
  - MCU single hart
  - PLIC
  - 16+ PMP/ePMP entries[1]
  - Support Secure Platform

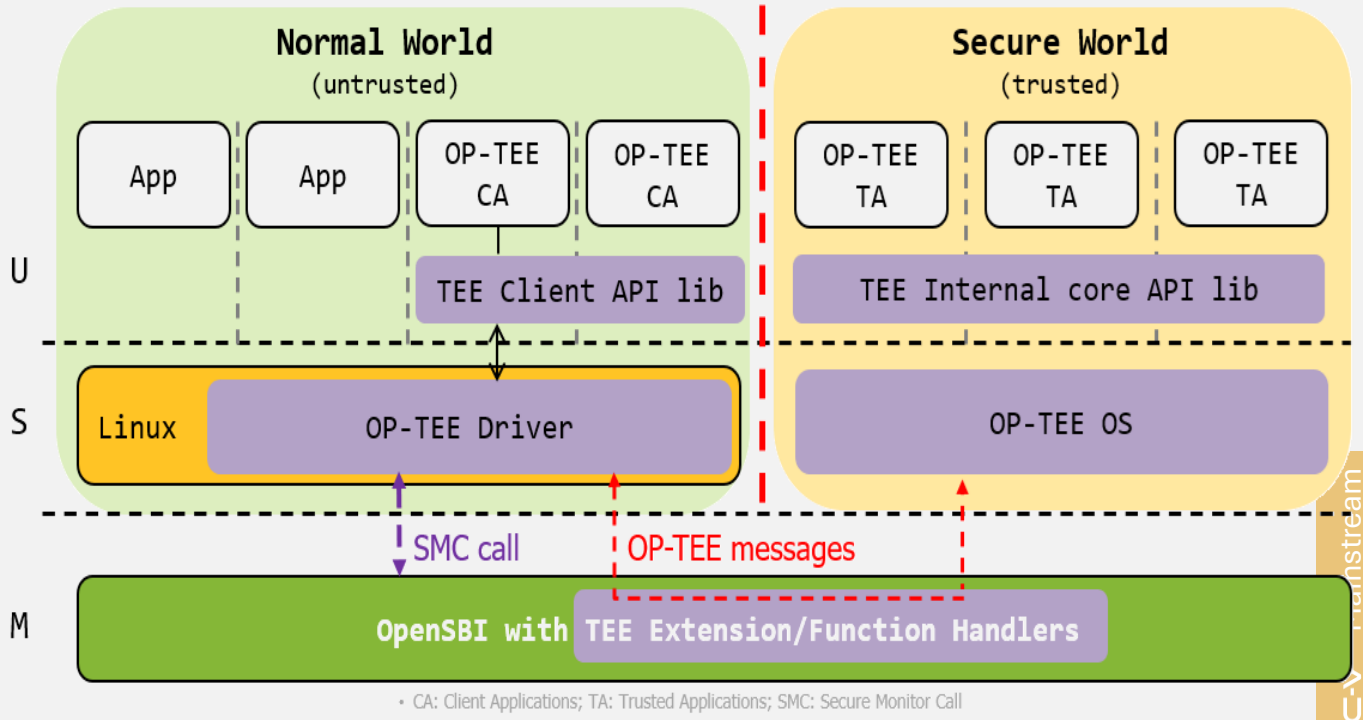


1: Full function of MCU-TEE could be enabled with 16 PMP entries

SMC: Secure Monitor Call

OP-TEE Secure Monitor

- A popular open-source secure monitor project
- OP-TEE design goals
  - Isolation
  - Small footprint
  - Portability
- Support GlobalPlatform TEE API[1]
- A RISE project owned by the Andes
  - Bring OP-TEE to the RISC-V Ecosystem
  - Support UP/SMP RISC-V cores, and IOPMP



RISC-V Software Ecosystem

Taking RISC-V Mainstream

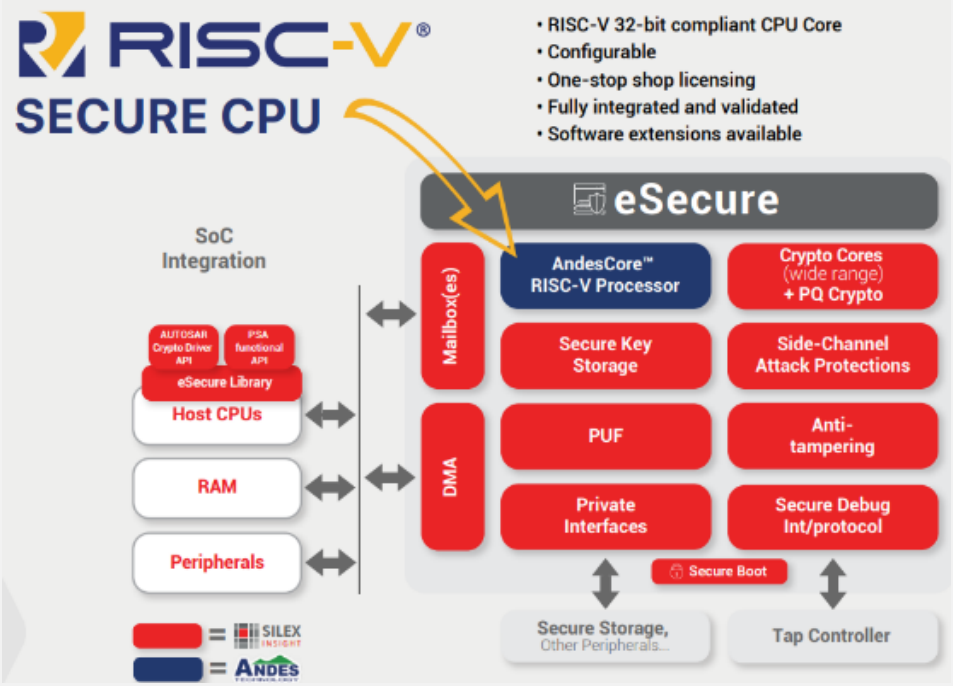
1: OP-TEE has support for GlobalPlatform TEE Client API Specification v1.0 (GPD_SPE_007) plus Errata and Precisions 2.0 (GPD_EPR_028) and TEE Internal Core API Specification v1.3.1 (GPD_SPE_010).

Partners for Security IPs

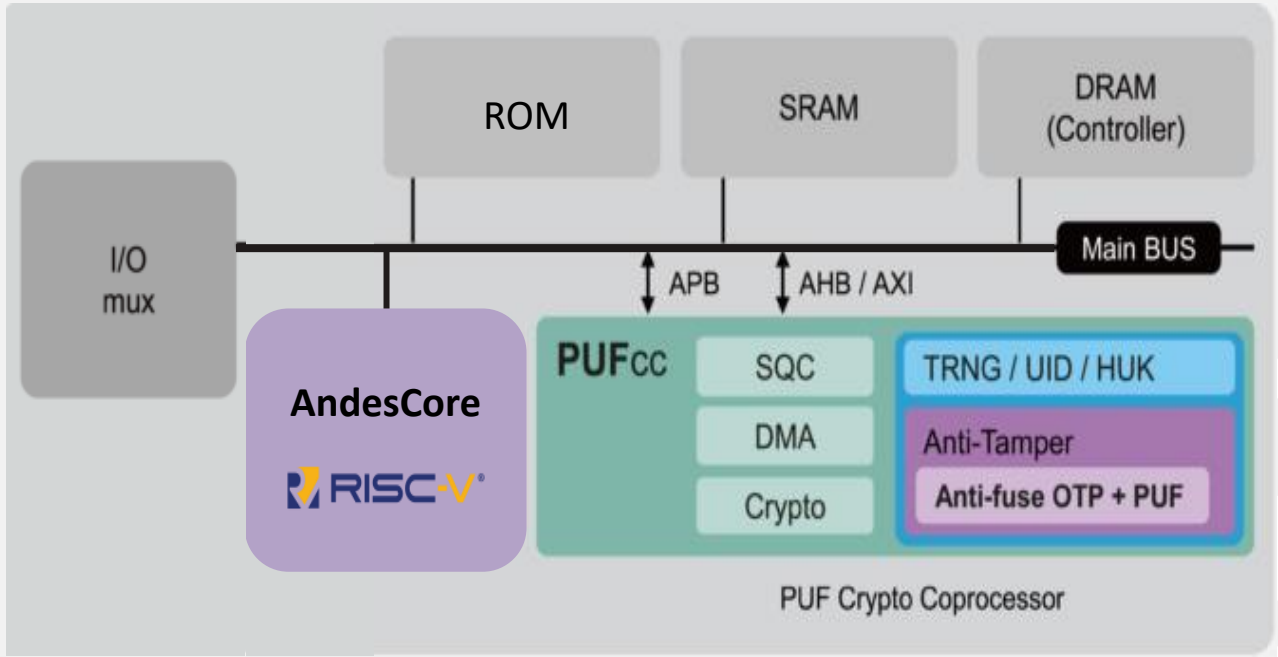
- AndesCore as part of the Secure Element: Secure-IC
- AndesCore as the host: PUFsecurity, Rambus, Secure-IC
- AndesCore enhanced with cyber-attack protection: Secure-IC
- AndesCore enhanced with data in motion protection: Rambus

Rambus
Data · Faster · Safer

SECURE-IC
THE SECURITY SCIENCE COMPANY



PUFsecurity



Taking RISC-V® Mainstream

AndeSentry™ Security Partners

深圳市新芯矽创电子科技有限公司
Shenzhen Xinxin Si Chuang Electronic Technology Co., Ltd.

Taking RISC-V® Mainstream

Andes RISC-V Boost Security Applications

- Performance
  - RISC-V vector processor
  - Andes Custom Extension
  - AnDLA accelerator, NN software stacks, and NN libs
- Security
  - Continuous specification improvement from RISC-V Foundation
  - RISC-V PMP + IOPMP + IOMMU + AIA provide a hardware isolation mechanism
  - Secure Boot and Secure Monitor solutions
  - AndeSentry™ collaborative framework provides comprehensive solutions

Taking RISC-V® Mainstream

Thank you!!

Taking RISC-V® Mainstream