Andes and PUFsecurity Webinar

24 Feb 2022

Today's Speakers

- **John Min** is Director of Field Application Engineering at Andes USA. He has extensive background in Processing – CPU, DSP and ASIC. Prior to Andes, John spent last 20 years in Processor companies like SiFive, MIPS and ARC in various technical roles. Prior to that, he worked in consumer electronics at LG and HP. John has multiple degrees from University of Southern California.

Andrew Intro

- **Andrew Irvin,** Chairman's office of eMemory and PUFsecurity

15+ years experience across three continents in Sales, Marketing, and Project Management. Originally from the United Kingdom and is a graduate from Edinburgh University. He is also licensed Architect and oversaw the design and construction of serval large building projects in China and Europe prior to moving into the semiconductor industry.

Andes Technology Corporation

Who We Are

Pure-play CPU IP Vendor

RISC-V Founding Premier Member

Major Open-Source Contributor/ Maintainer

16-year-old Public Company

RISC-V Ambassador
Running Task Groups
Technical Steering Committee
Board of Directors

Quick Facts

100+ years
CPU Experience in Silicon Valley

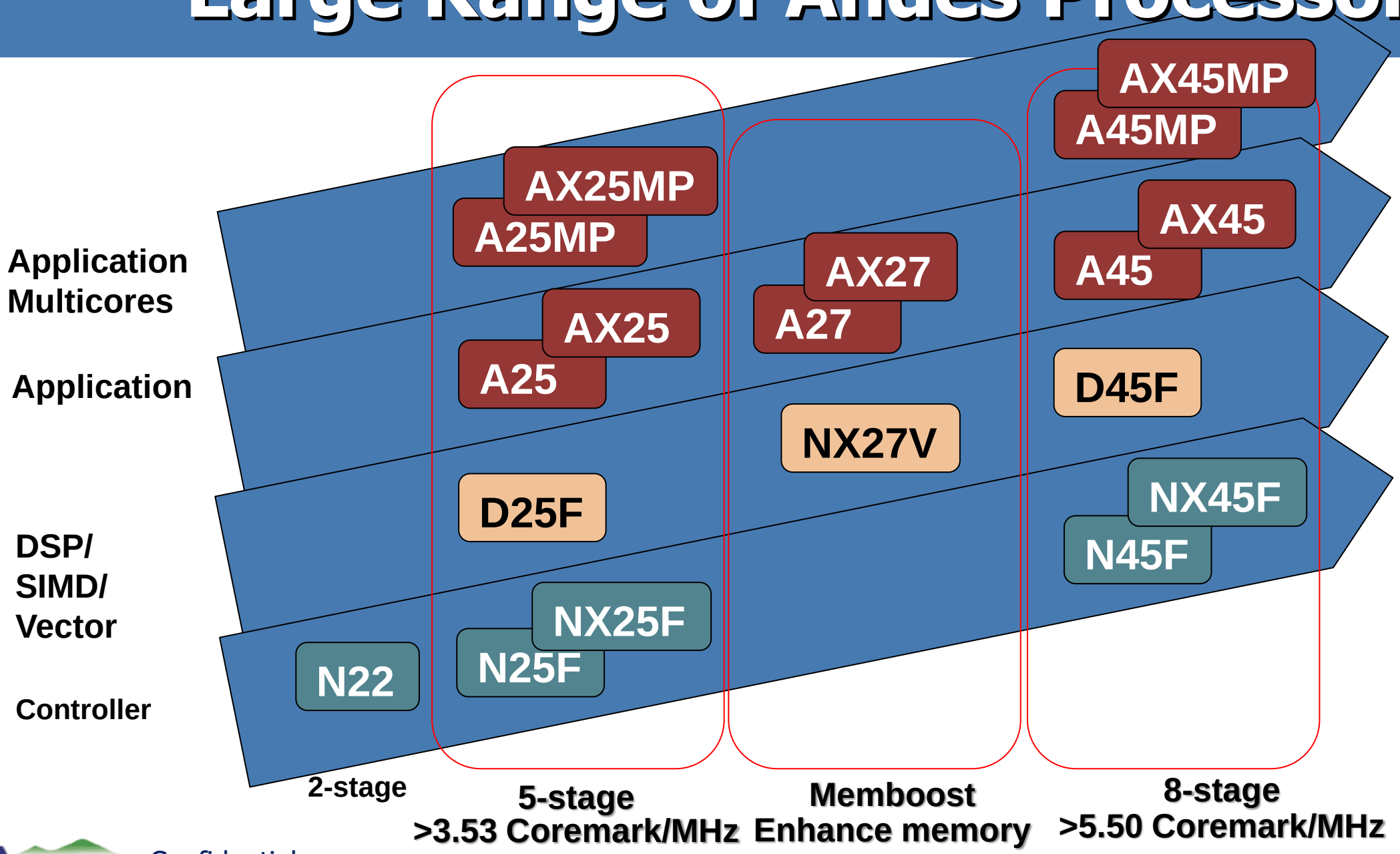
80+%
Engineers

250+
Licensees

20K+
AndeSight IDE installations

~10B (Q4/21)
Total shipment of Andes-Embedded™ SoC

Large Range of Andes Processors

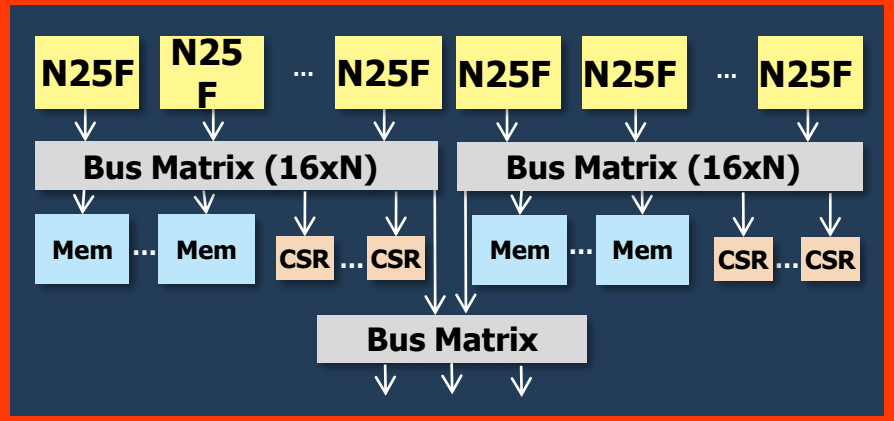


Andes RISC-V Adoption

Renesas: ASSP MCU with configurable V5 cores

- Scalable/configurable performance
- Selectable safety features
- Customization options
- Feature-rich AndeSight I

Picocom: 5G Open RAN small cells



Telink: IoT and Wireless Audio with D25F embedded

- Strong integer/DSP performan
- Efficient small data processing
- Good development tools

IAR SYSTEMS

AI Accelerators for Servers with >10 NX27V Cores

- RVV with 512-bit VLEN/SIMD
- Custom instructions
- LLVM compiler

Securing Andes RISC-V with PUFsecurity.

2022 February 24

PUFsecurity
AN eMemory COMPANY

Agenda

1. Company Profile
2. Securing the Future of Computing
3. The Four Fundamentals of Chip Security
4. PUF-based Solutions with Andes RISC-V

World's Largest
Pure-Play eNVM Provider

ememory

Subsidiary Dedicated to
PUF-based Security IP

PUFsecurity

22 Years
In the IP business
Based in Taiwan

990+
International
Patents Issued

300+
Employee Pure IP Company

70%
IP Developers

17 Years
Consecutive Growth

$84M+
Annual Revenue

5,850+
Customer
Tape-Outs

1.8M+
Wafers shipped quarterly

40M+
Wafers shipped to date

12 Years
Consecutive TSMC IP
Partner Award

Unique Contribution to the Industry .

Invention of
Logic Non-volatile
OTP Memory

Neo Fuse

Invention of
Logic Non-volatile
MTP Memory

Neo MTP

Invention of
Logic Chip Fingerprint
Quantum Tunneling PUF

Neo PUF

Logic Non-Volatile Memory

Provides embedded logic NVM solutions, including both OTP and MTP to Improves
yield, performance, and flexibility in product development and production.

Quantum Tunneling PUF

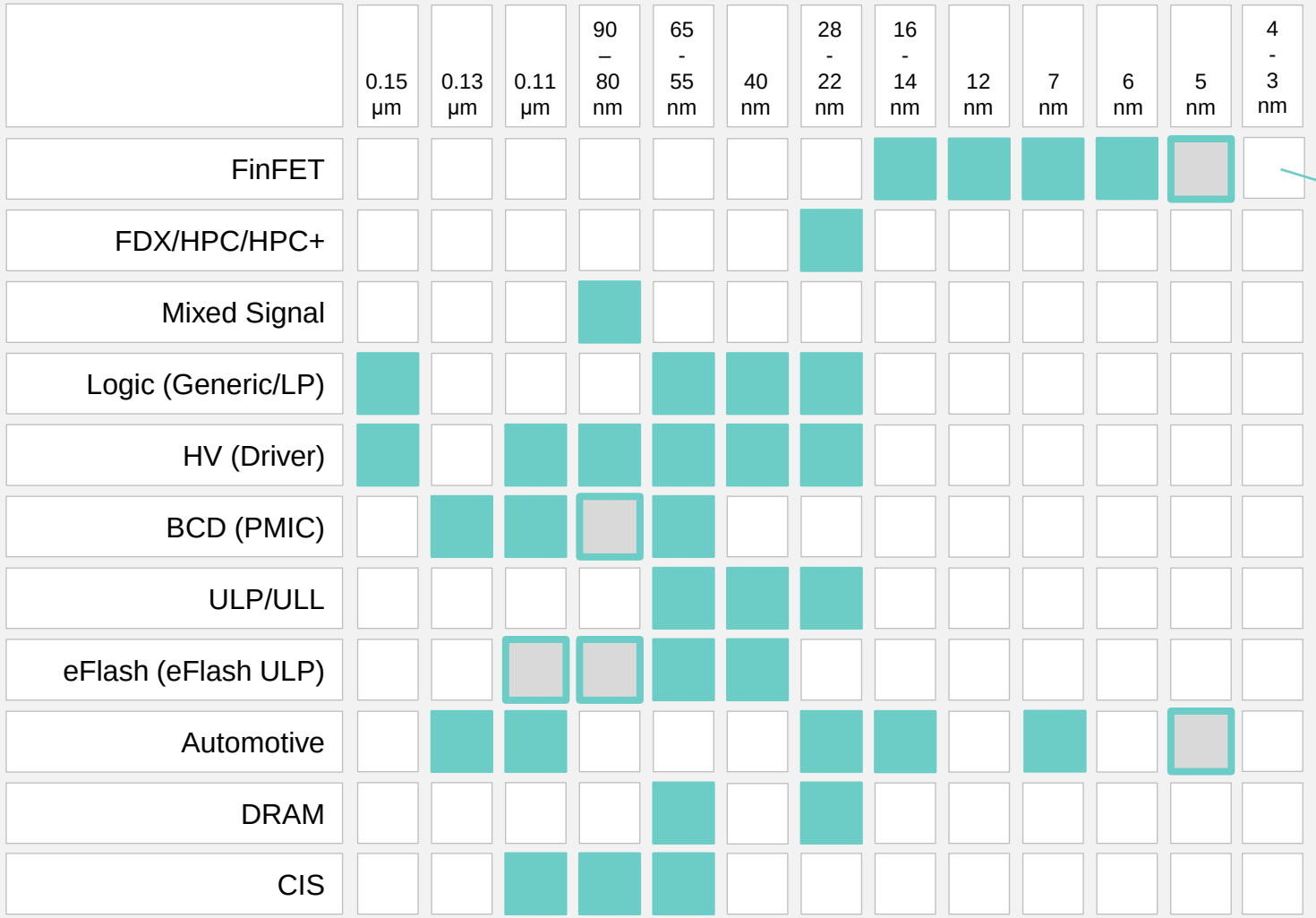
Provides unique ID for each chip and the necessary hardware ‘Root of Trust’ to achieve high security solutions whilst also eliminating the need for additional processes.

PUF

Physically
Unclonable
Function

A chip fingerprint for silicon

Widely Available Security IPs



Qualified/Production

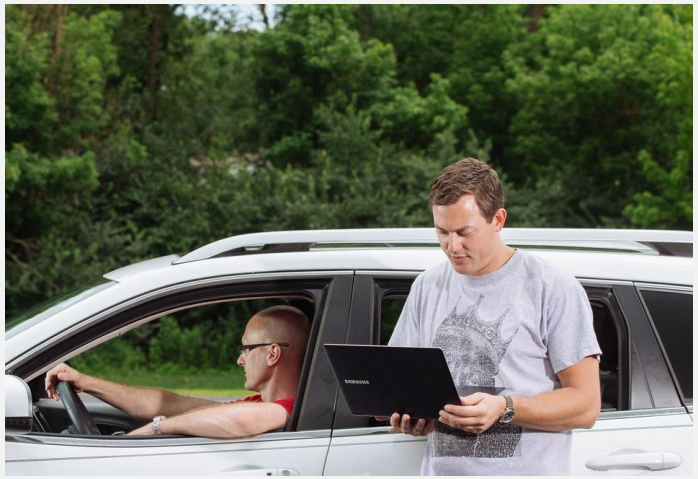
Verified/Developing

Kickoff in 2022

- NeoPUF adopts the same technology, programming mechanism, and bit cell as NeoFuse
- Qualified NeoFuse stands for NeoPUF and PUF-based IPs readiness

Hacking is Everywhere .

Threat to **Life**



Hackers Remotely Kill a Jeep on the Highway

Sparking a 1.4 million vehicle recall by Chrysler, marking the start of the age of hackable vehicles.

Link

Threat to **Privacy**

IoT Security Camera hacking demonstration on YouTube

Step by step guides for hacking IoT devices are widely available online.

Link

Threat to **Assets**

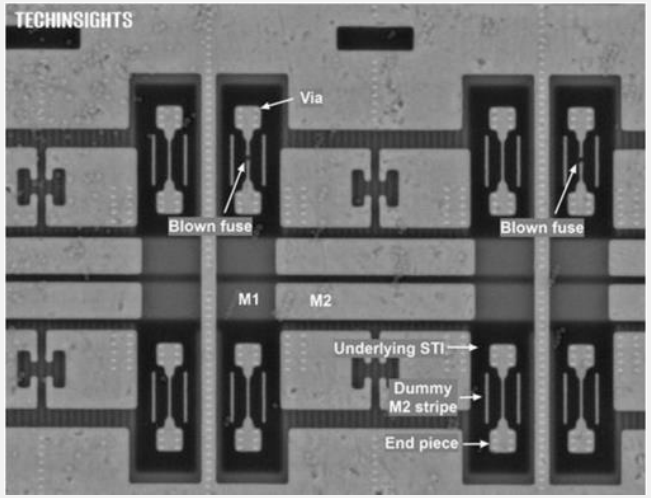
Colonial Pipeline pay $4.4m to end ransomware attack

ending the massive shutdown of approximately half of the USA's East Coast fuel supply

Link

Hardware Attacks are Today Reality

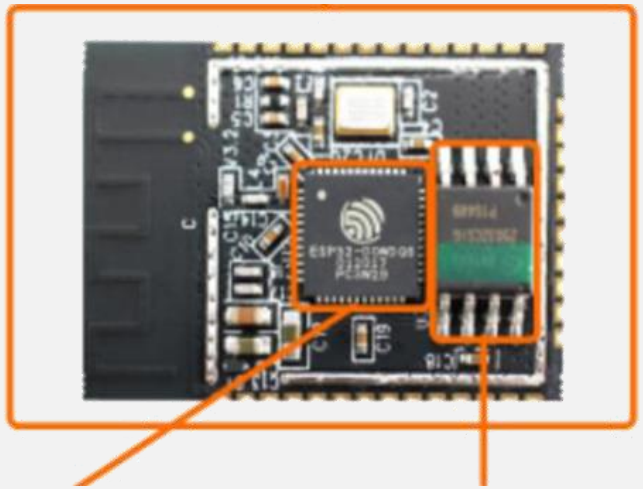
De-cap
E-fuse keys stolen



- Secure Storage needed

Invisible OTP

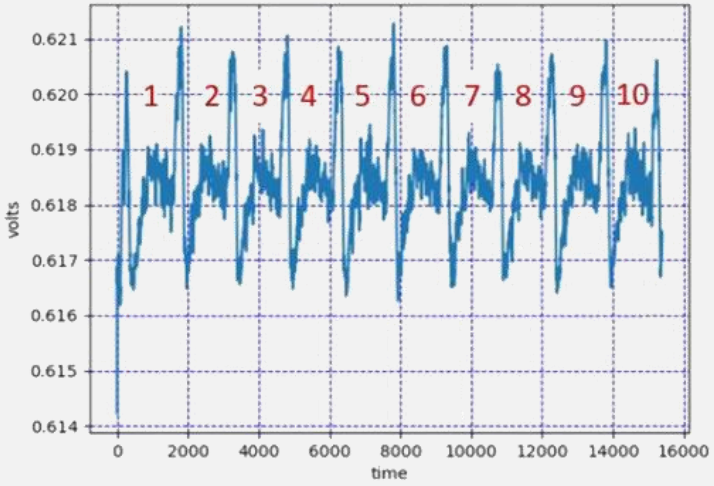
Fault Injection
Espressif WiFi-IoT Chip Hacked



ESP32 Flash Memory (SPI)

- ESP32-S2 will ECO soon

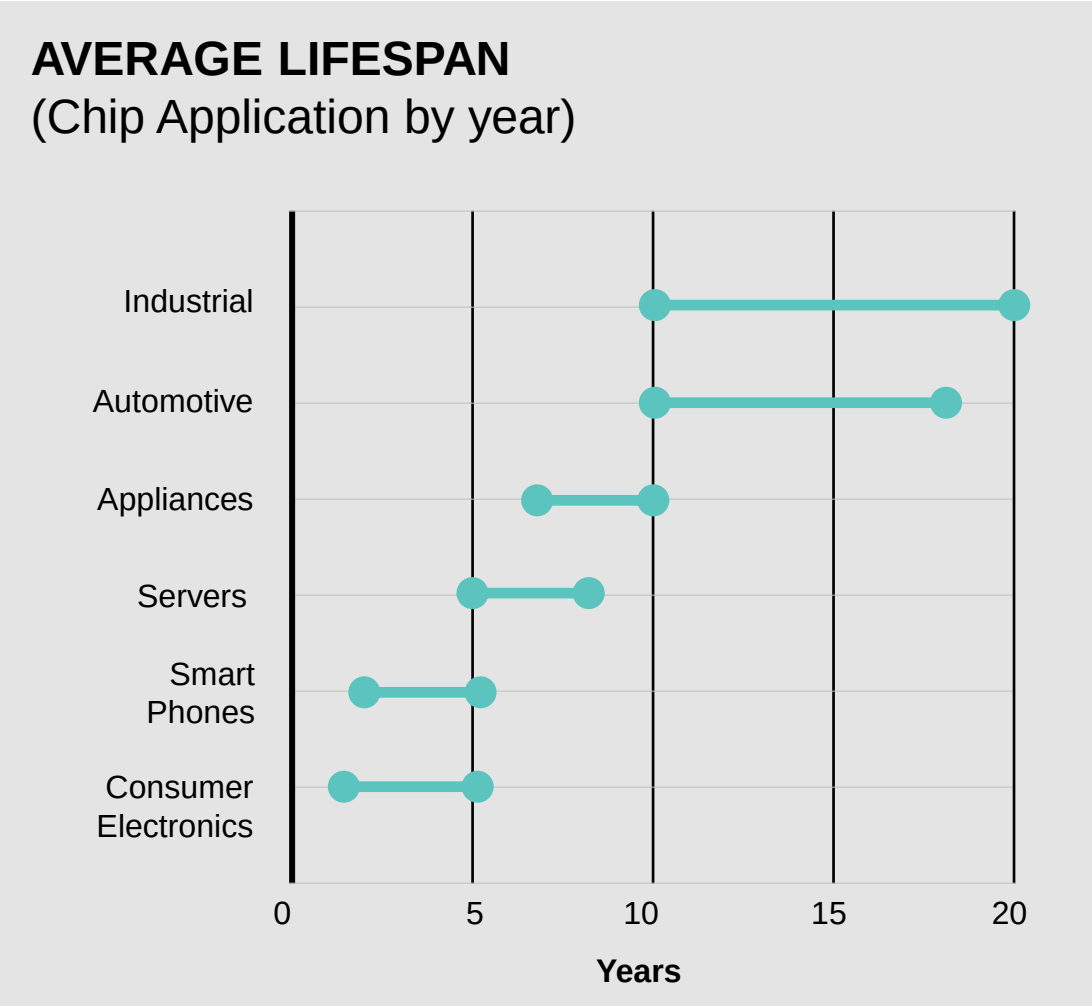
Differential Power Analysis
STM MCU AES key found



- Countermeasures needed

Side Channel Attack Protection / Anti-Tampering Design

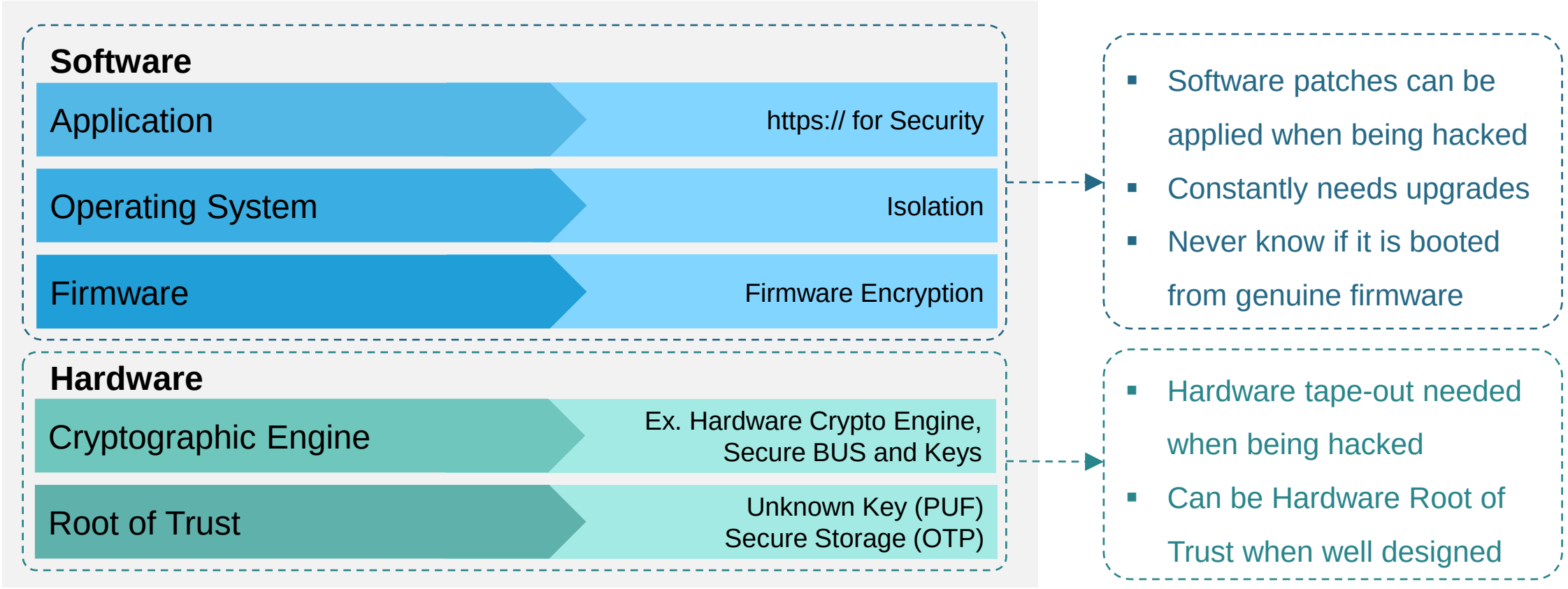
Securing the Future of Computing .



[1] Source: https://semiengineering.com/making-chips-to-last-their-lifetime/

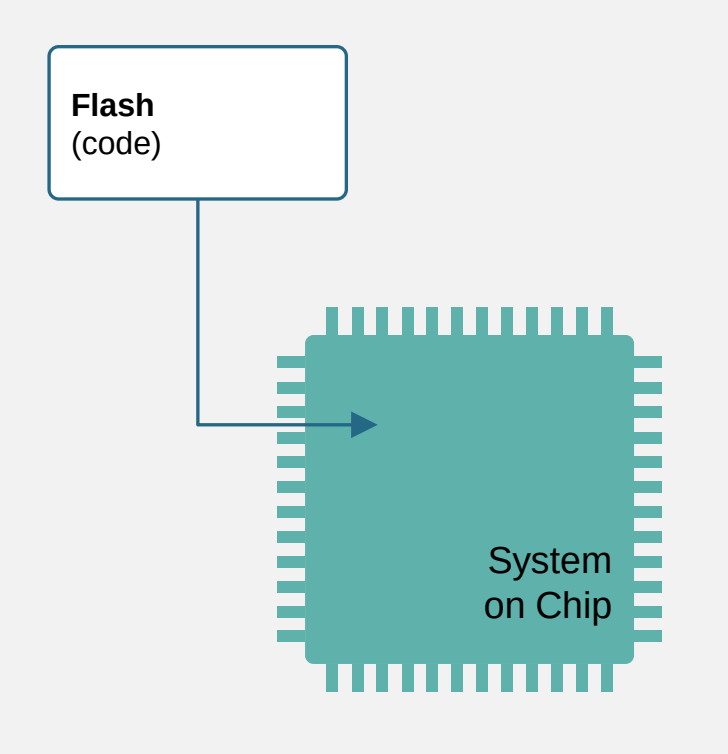
The Security Ecosystem's **Weakest Link**

SECURITY SYSTEM BY COMPUTING LAYER
(and Example Protection Approach)

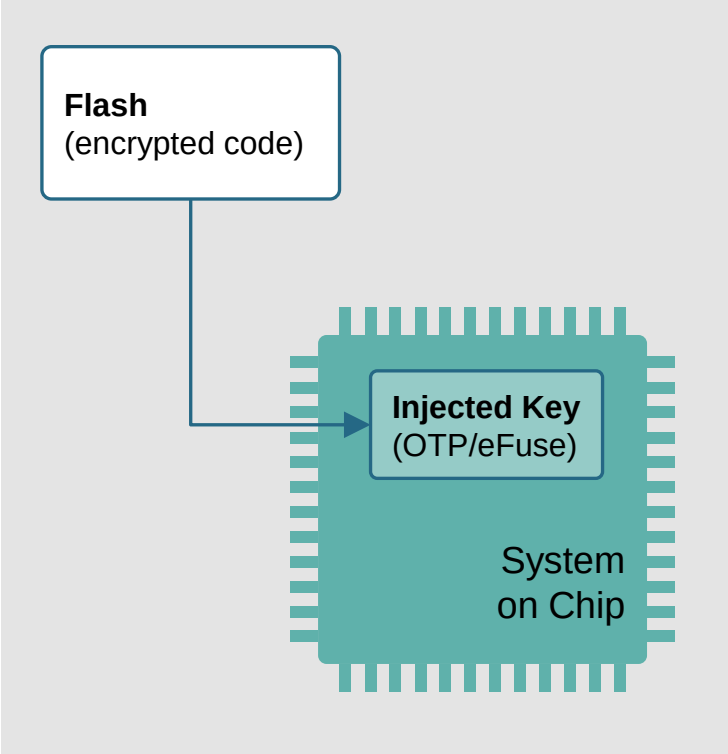


How **Chips Boot Up** is Key to Security

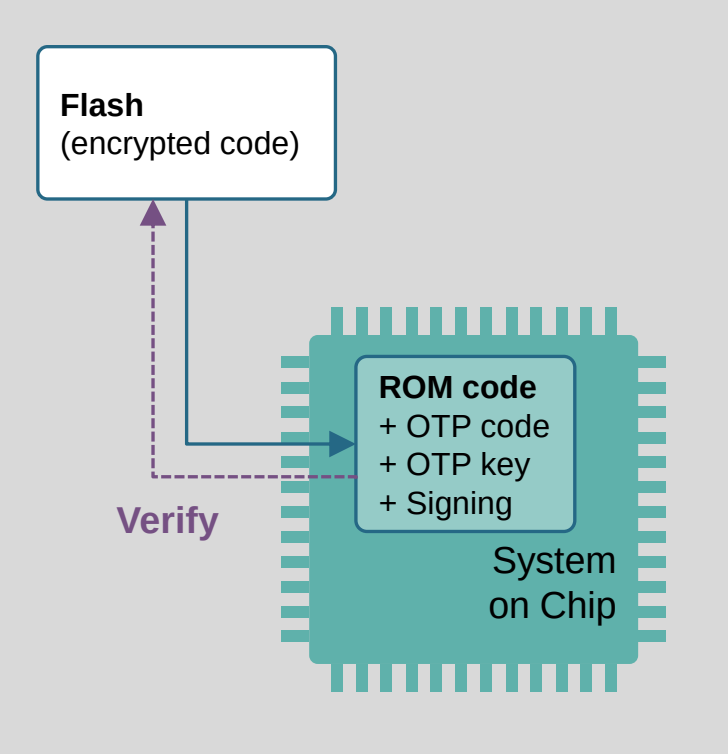
1st Generation
Conventional Booting



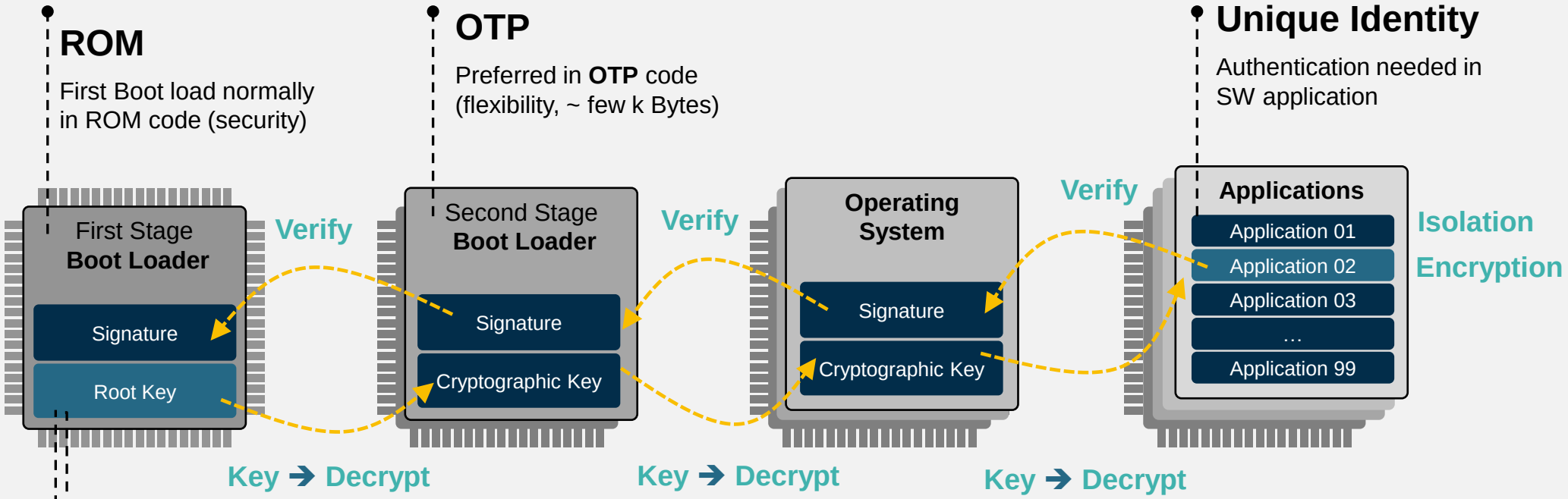
2nd Generation
Improved Booting



3rd Generation
Secure Booting

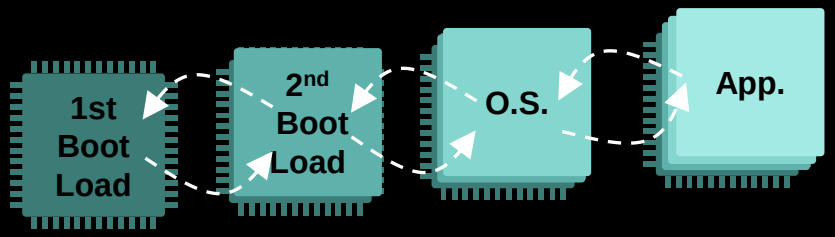


Secure Boot Flow (Hardware and Software)



The **Four Fundamentals** of Chip Security .

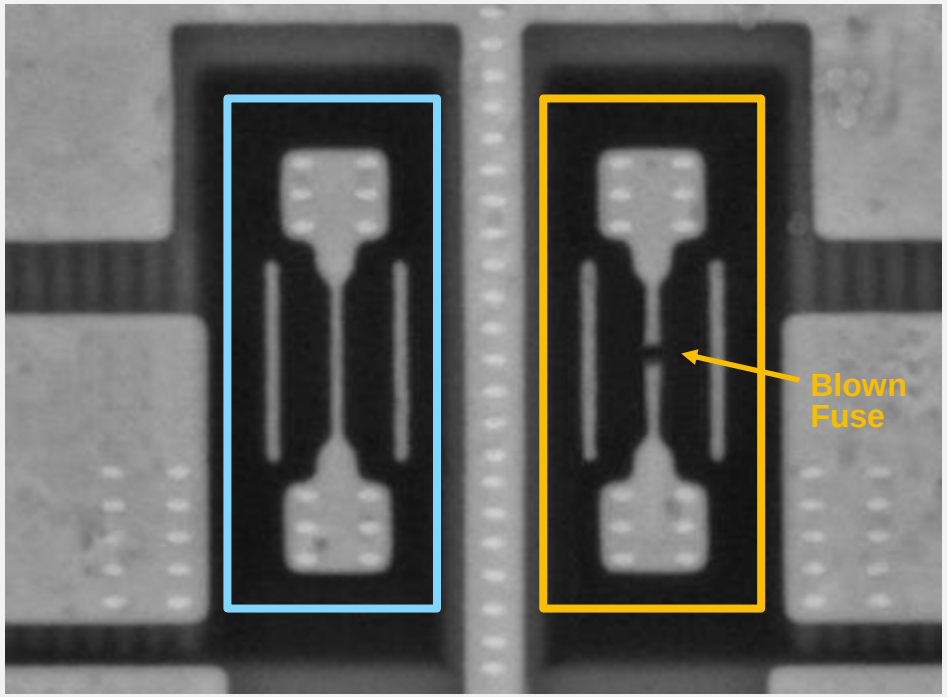
1. OTP for Boot Code
2. Root Key Storage
3. Root Key Generation
4. Unique Unclonable Identification



Physical Invisibility Top View via SEM

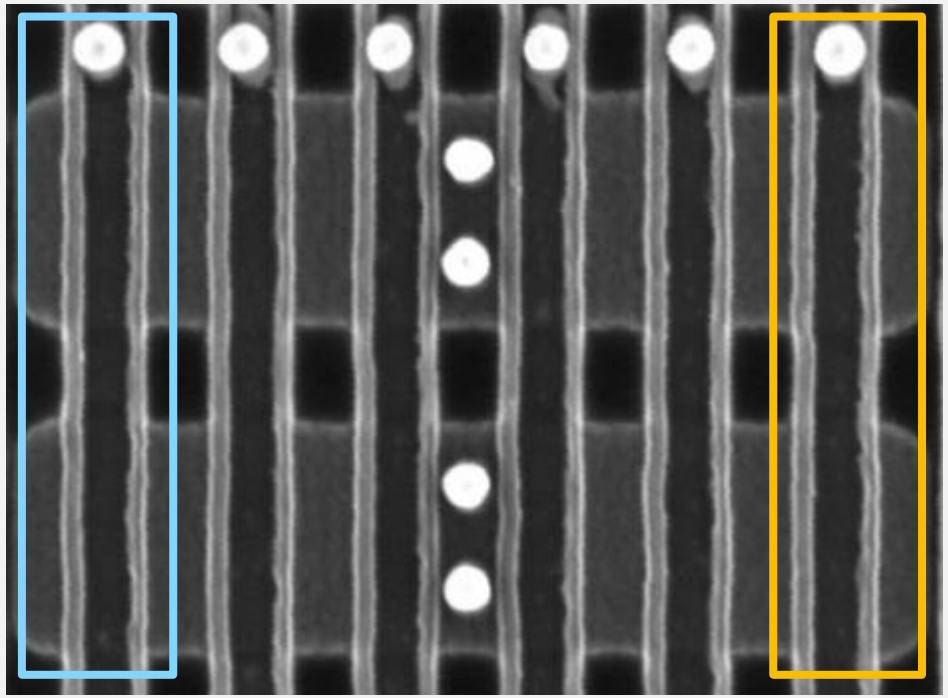
e-Fuse (Electrical Fuse)

UN-PROGRAMMED PROGRAMMED



anti-Fuse (NeoFuse/NeoPUF)

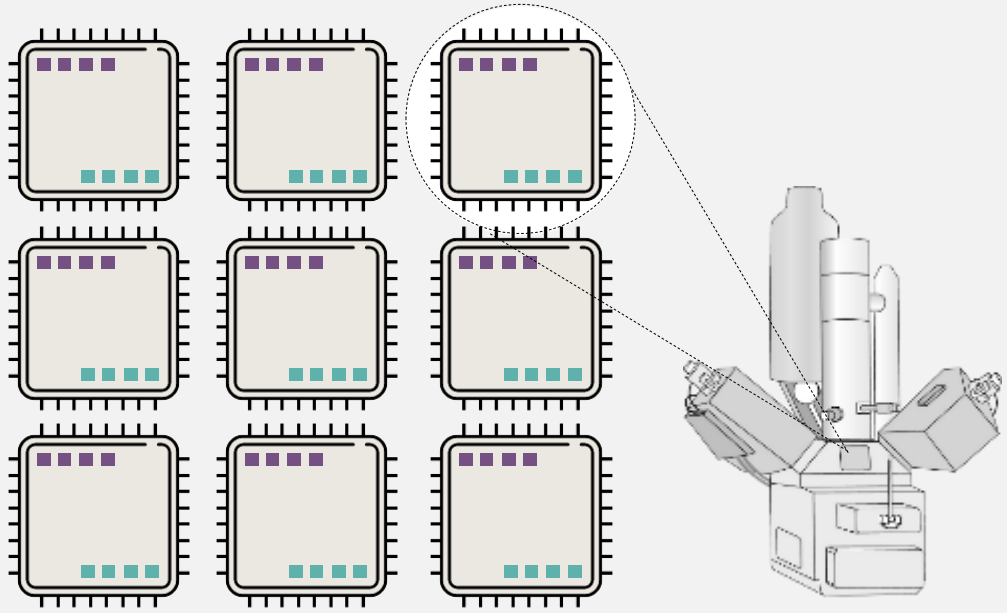
UN-PROGRAMMED PROGRAMMED



[1] Source: https://www.eetimes.com/a-look-at-metal-efuses/

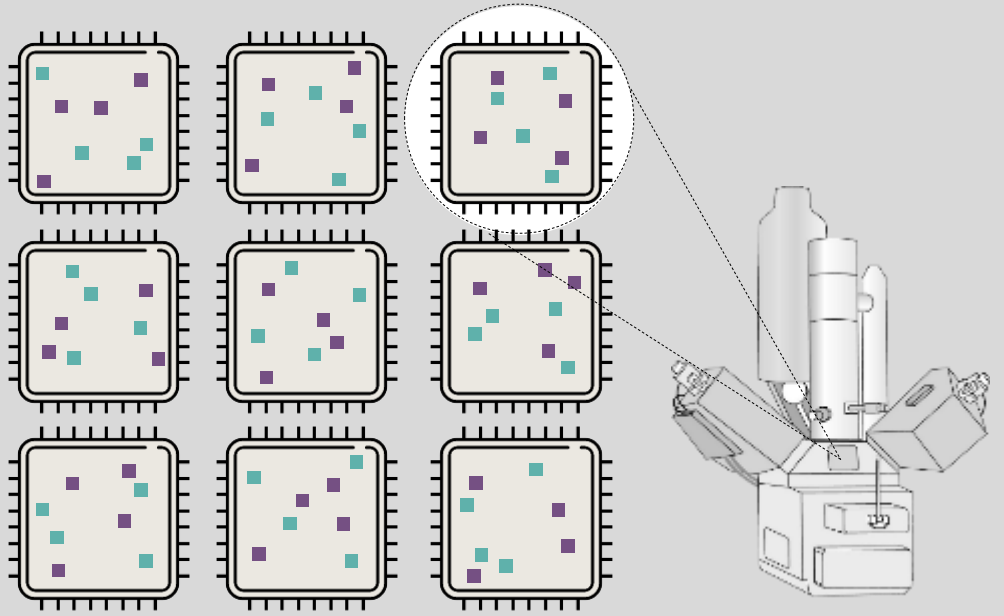
Hardware RoT Root Key Storage

eFuse OTP
No PUF-based Storage



- OTP address can be easily located

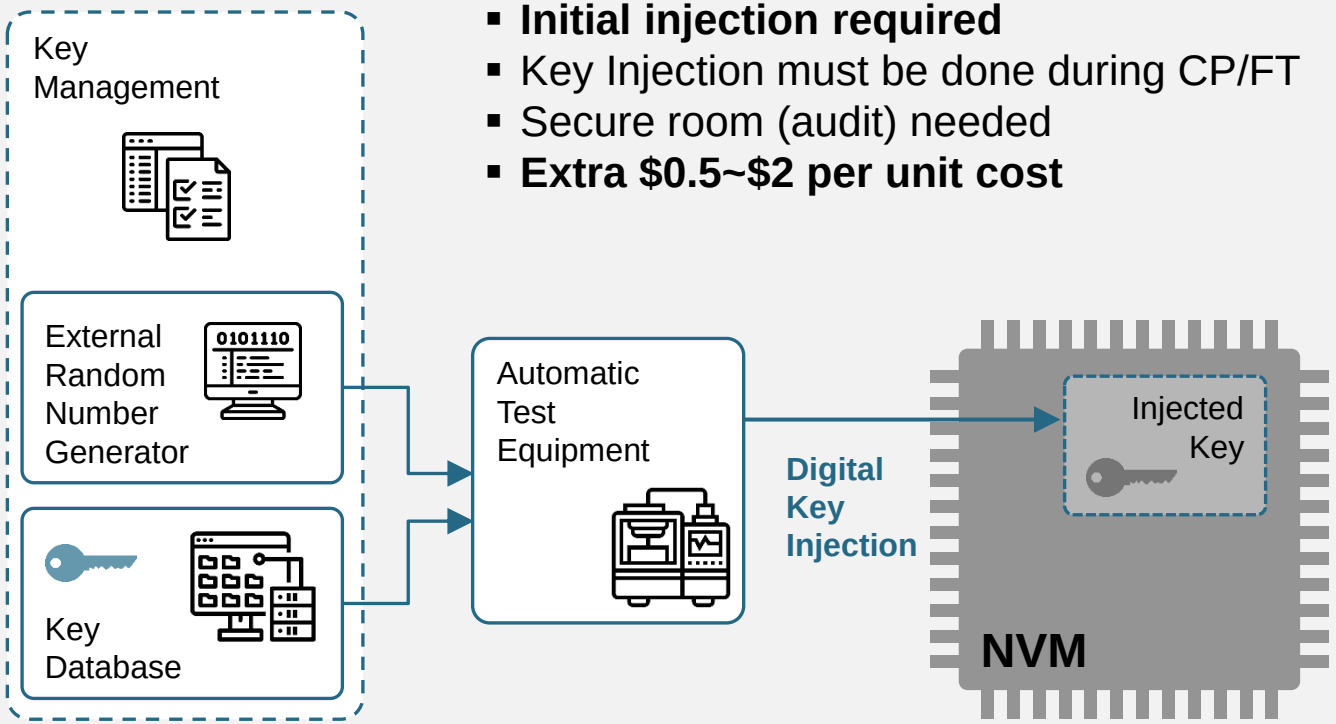
Secure OTP
With NeoPUF Protection



- Different Physical location for each chip

Root Key Generation

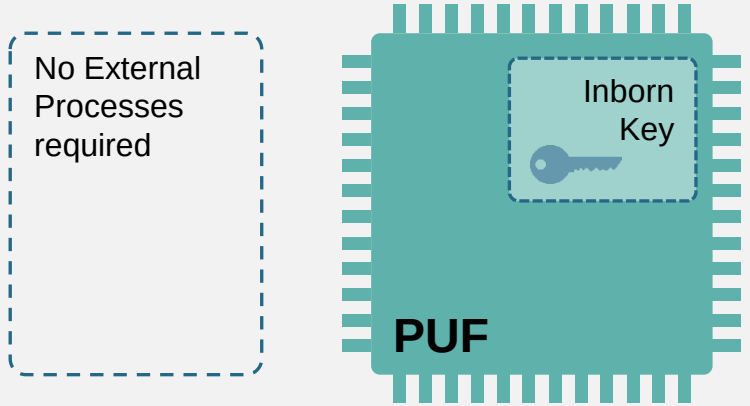
Injected Root Key
(Serial Identification)



- **Initial injection required**
- Key Injection must be done during CP/FT
- Secure room (audit) needed
- **Extra $0.5~$2 per unit cost**

Inborn Root Key
(PUF-based Identification)

- **Inborn,** unique, unclonable ID
- Provides **zero-touch / zero-trust**
- **Private key** from PUF **never exposed** outside SOC



Combining Digital and Analog IPs

Security Subsystem

Analog Macro
(process dependent)

- Anti-Tamper Design
- **TRNG** (entropy)
- **OTP** (Secure Storage)
- **PUF** (Chip Fingerprint)

Digital IP
(process independent)

- Secure CPU
- HASH Crypto
- Symmetric Crypto
- Asymmetric Crypto

Security systems rely on OTP Memory

Secure OTP is replacing eFuse

Crypto engines require TRNG

TRNG is digital + analog

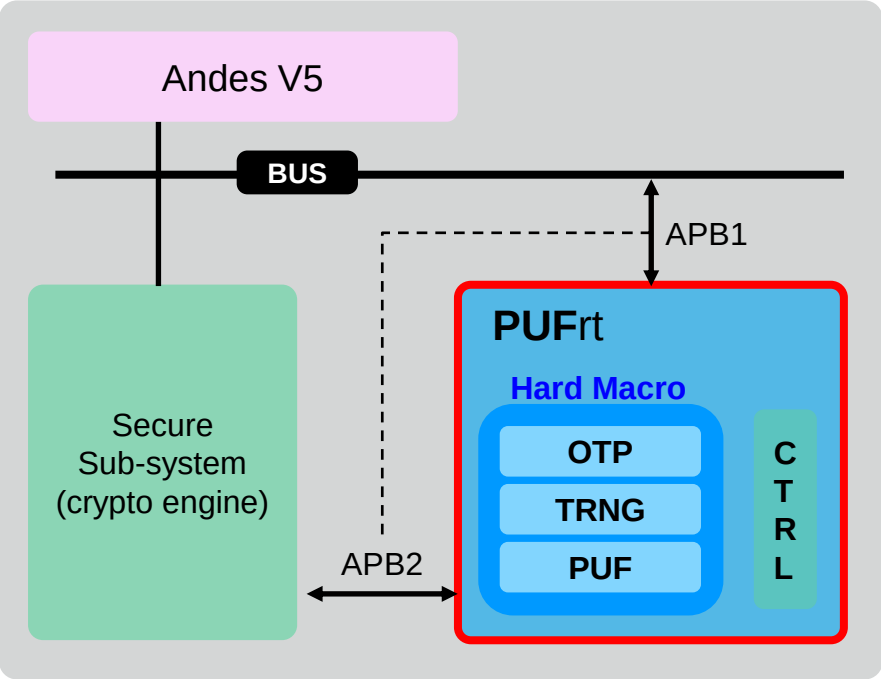
External Key injection is expensive

PUF has zero-touch provisioning

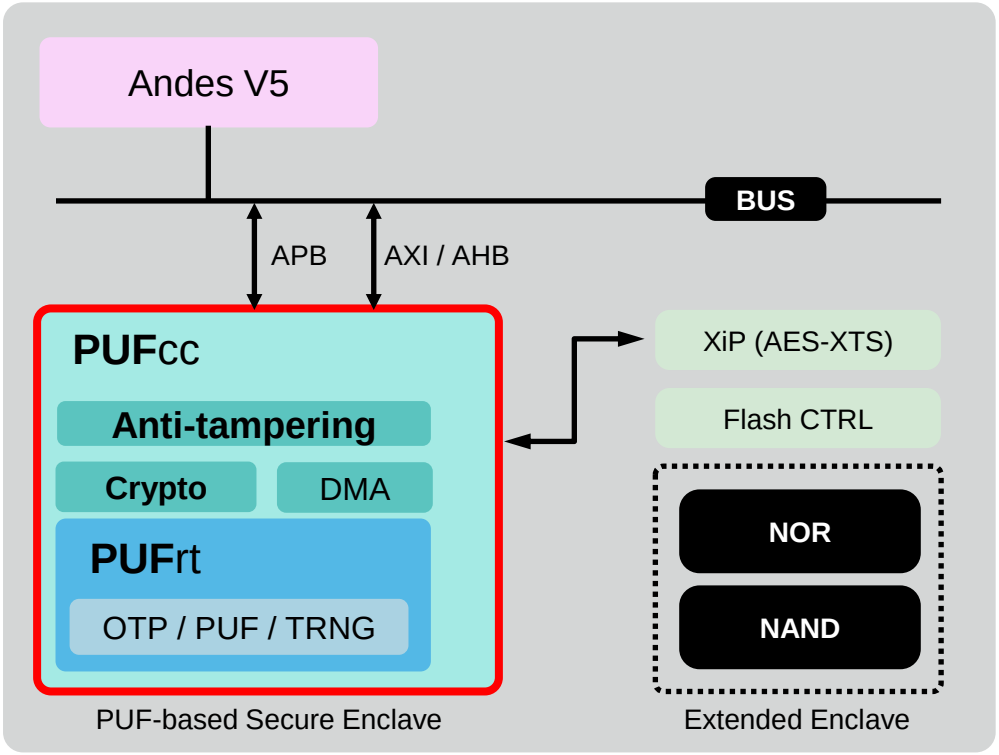
PUF / OTP / TRNG / Anti-tampering combined into one single **Hardware Root of Trust IP** is Ideal

PUF-based Security Solutions for RISC-V

PUFrt : Secure Storage (OTP) + Inborn ID / Key (PUF) + Randomness (TRNG) + Anti-Tampering + 3rd party security lab certification



PUFcc : **PUFrt** + Anti-tampering & NIST-certified Crypto Coprocessor + Secure Enclave (Boundary)



RISC-V Platform Demonstration

FPGA Demonstration

by integrating RISC-V (ANDES) and PUFcc (PUFsecurity)

- **On-chip Inborn HUK**: Saving provisioning cost
- **Secure boot using PUFcc**: Paired SoC and FW to protect from HW/SW counterfeiting

Total Solutions
for Hardware Security .

Secure OTP

for Key Storage & Boot code

PUF

inborn identity & saving key management flow

TRNG

SP800-90B compliant random number

NIST certified Crypto Engines

With encryption and anti-tamper

Thank You .

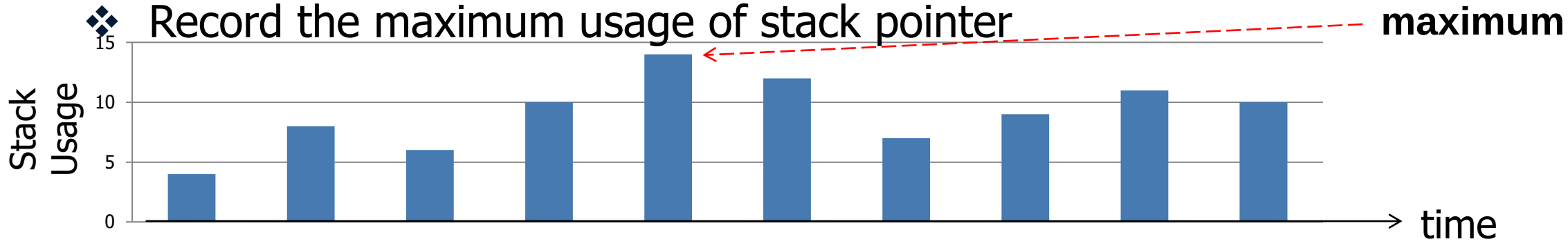
PUFsecurity
AN eMemory COMPANY

Andes Advantage

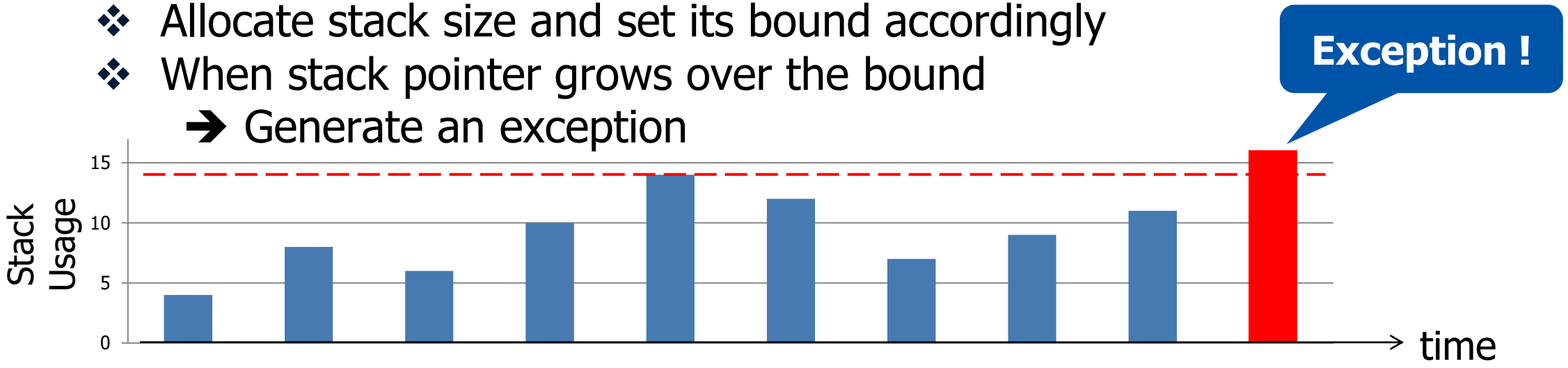
- Standard RISC-V ISA with Andes Extensions
- AndeStar V5 ISA - Extensions to accelerate and secure computing
  - **StackSafe**™: HW supported stack protection
  - **PowerBrake** : Stalling pipeline to save powe
  - **QuickNap**™ : Fast power-down/wake-up support for caches
- **ACE -** Andes Custom Extensions
  - **Custom Instructions –** Accelerate Instruction
  - **Custom Memories –** Fast and local operands
  - **Custom Ports –** Accelerate, move, and secure – predictable bus

StackSafe™: Protect Stack Usage

- Recording mode:
  - Record the maximum usage of stack pointer

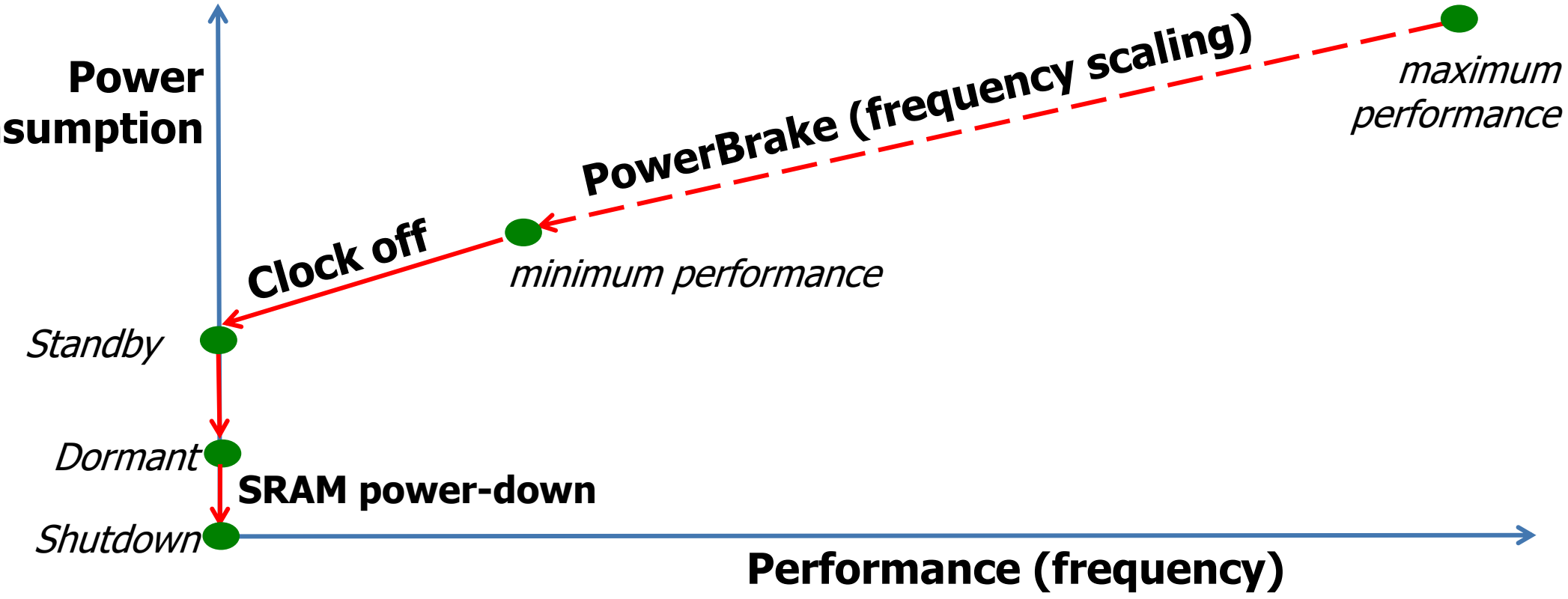


- Protection mode:
  - Allocate stack size and set its bound accordingly
  - When stack pointer grows over the bound
    - ➔ Generate an exception

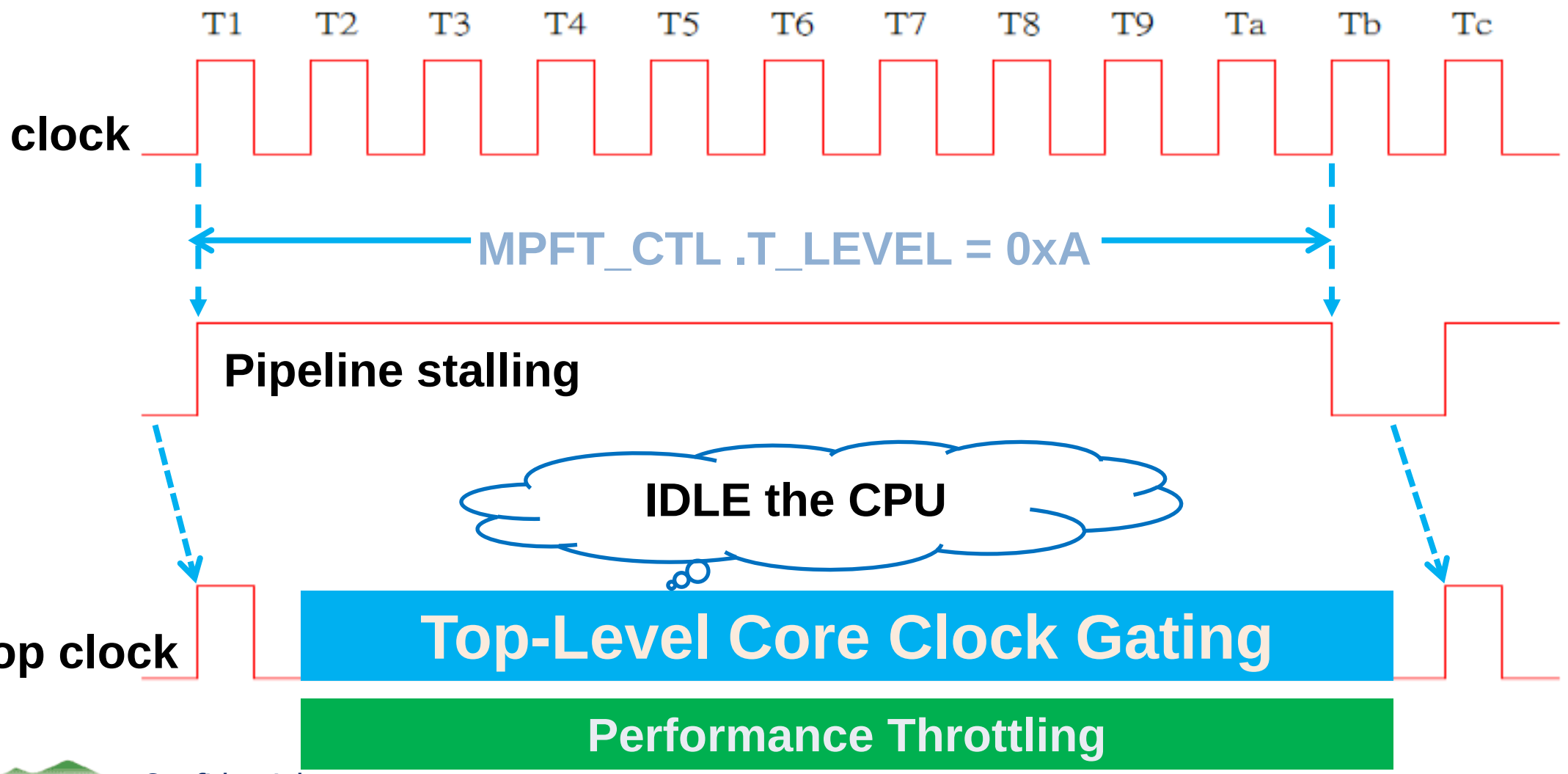


PowerBrake & QuickNap™: Power Management

- **PowerBrake** to digitally adjust power (via stalling pipeline)
- **QuickNap™**: logic power-down and SRAM in retention
  - Put dirty bits in tag SRAM instead of flops
  - Eliminate the need to flush data cache



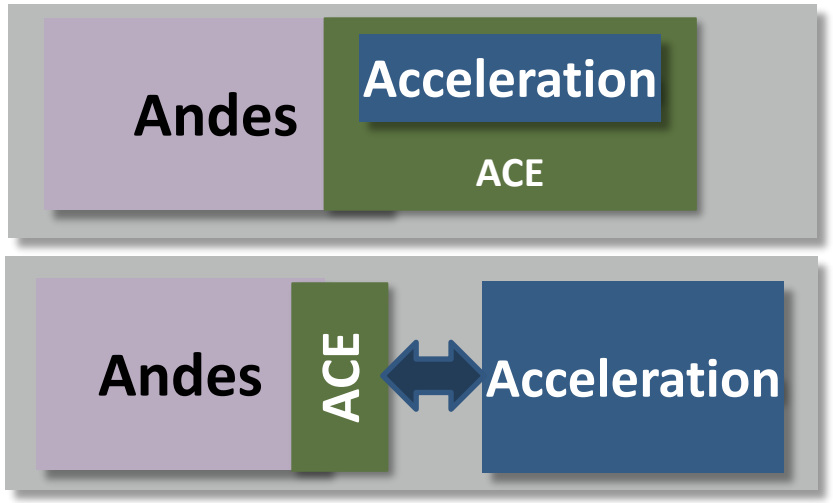
PowerBrake


T1
T2
T3
T4
T5
T6
T7
T8
T9
Ta
Tb
Tc
clock
MPFT_CTL .T_LEVEL = 0xA
Pipeline stalling
IDLE the CPU
Top clock
Top-Level Core Clock Gating
Performance Throttling

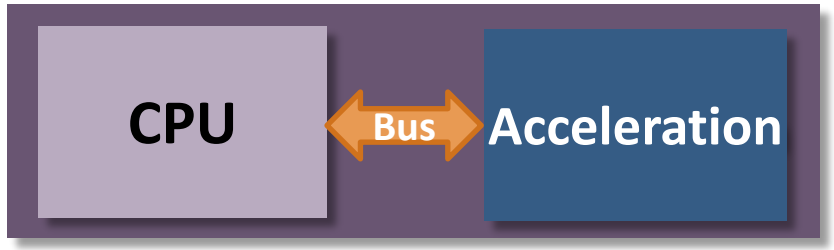

ACE
Andes Custom Extensions

ACE for Performance and Security

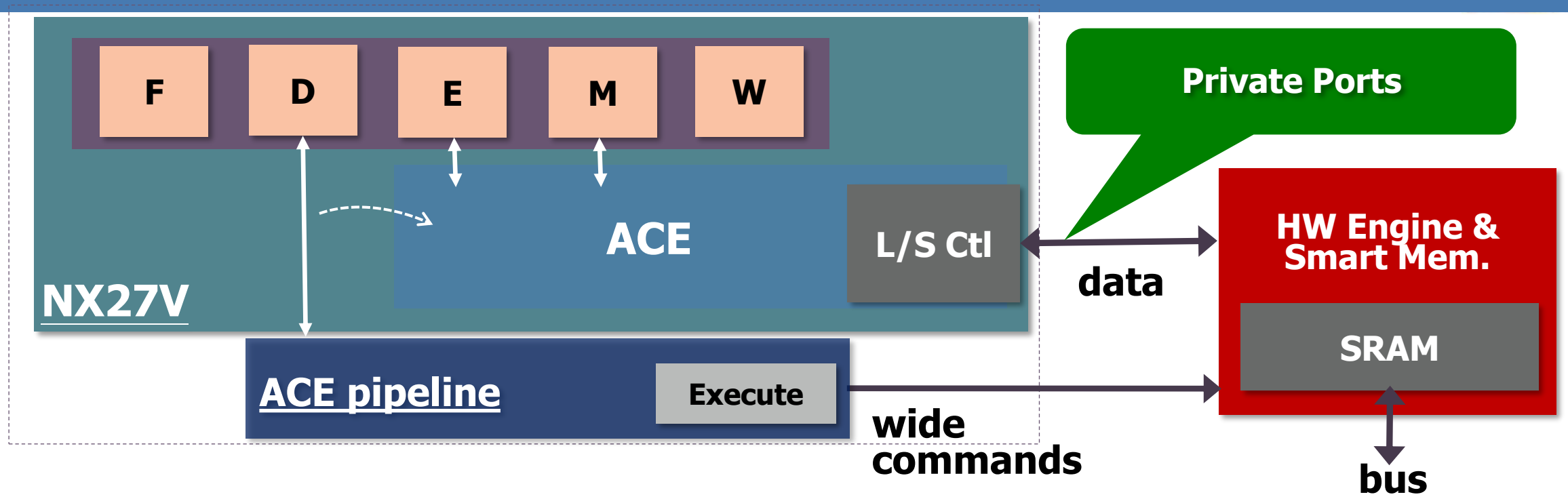
- RISC-V ISA extension enables
  - New instructions
  - New coprocessors
  - New memory locations
- Andes eases extension with
  - ACE key words in System C framework
  - Rich semantics for new instructions
  - Fully automated COPILOT generator
    - Integrating acceleration & RISC-V core
    - Resource & data hazard protection
    - Simulator, compiler, assembler, etc.
    - Test vectors for verification



Vs Traditional Architecture.



Private Port for Data Isolation



- A usage example
  - HW engine: application-specific DMA and structured computations (e.g. CNN)
  - ACE instructions: control HW engine, and load/store data to/from VRF

- **Advantages:**
  - **HW engine is tightly-coupled**
  - **Data accesses are more efficient**
  - **Data accesses are isolated**

Q&A

Thank you!