# Secure RISC-V

# A FIPS140-2 Compliant Trust Module for Quad 64-bit RISC-V Core Complex

Shumpei Kawasaki, Murthy Vedula, Software Hardware Consulting Group

Kesami Hagiwara, Cong-Kha Pham, University of Electro-Communications



# SHC Products

Secure OS

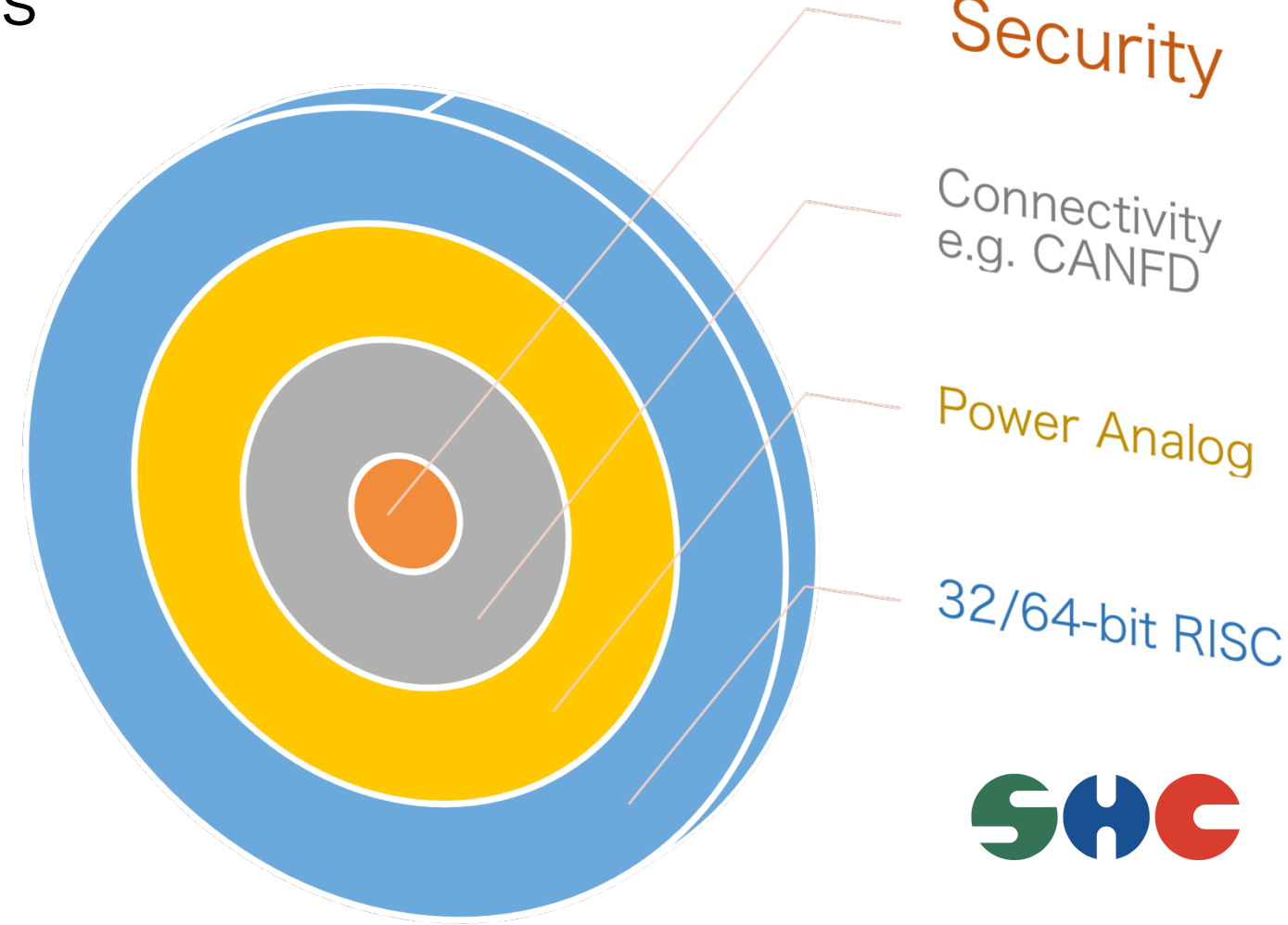
Crypto API

Connectivity
e.g. Lora, BTLE

BSP

Compiler

OS Internals



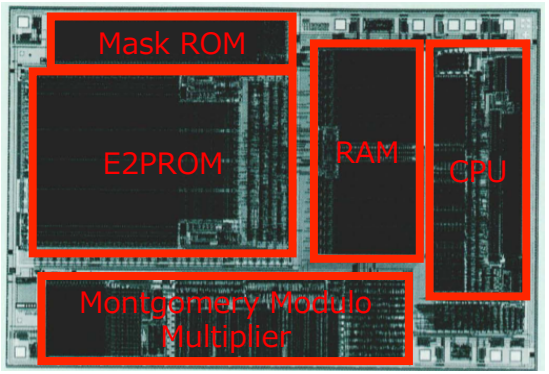
# 30+ Years Security Hardware

1986 IC card

1991 GSM SIM card

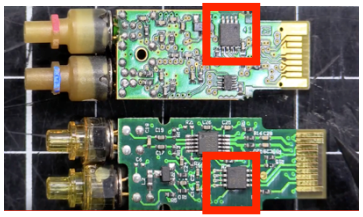


1995 Modulo Exponentiation Coprocessor



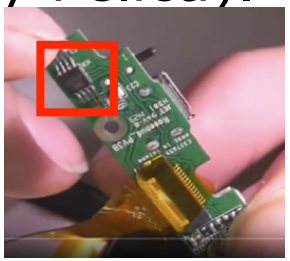

1996 Java Card™ MULTOS

2003 C-Callable Crypto Library for Routers



2004 Contactless eMoney “Suica” (Sony Felica).

2008 Secure OS for Smart Phone.



2018 Apple Secure Enclave.

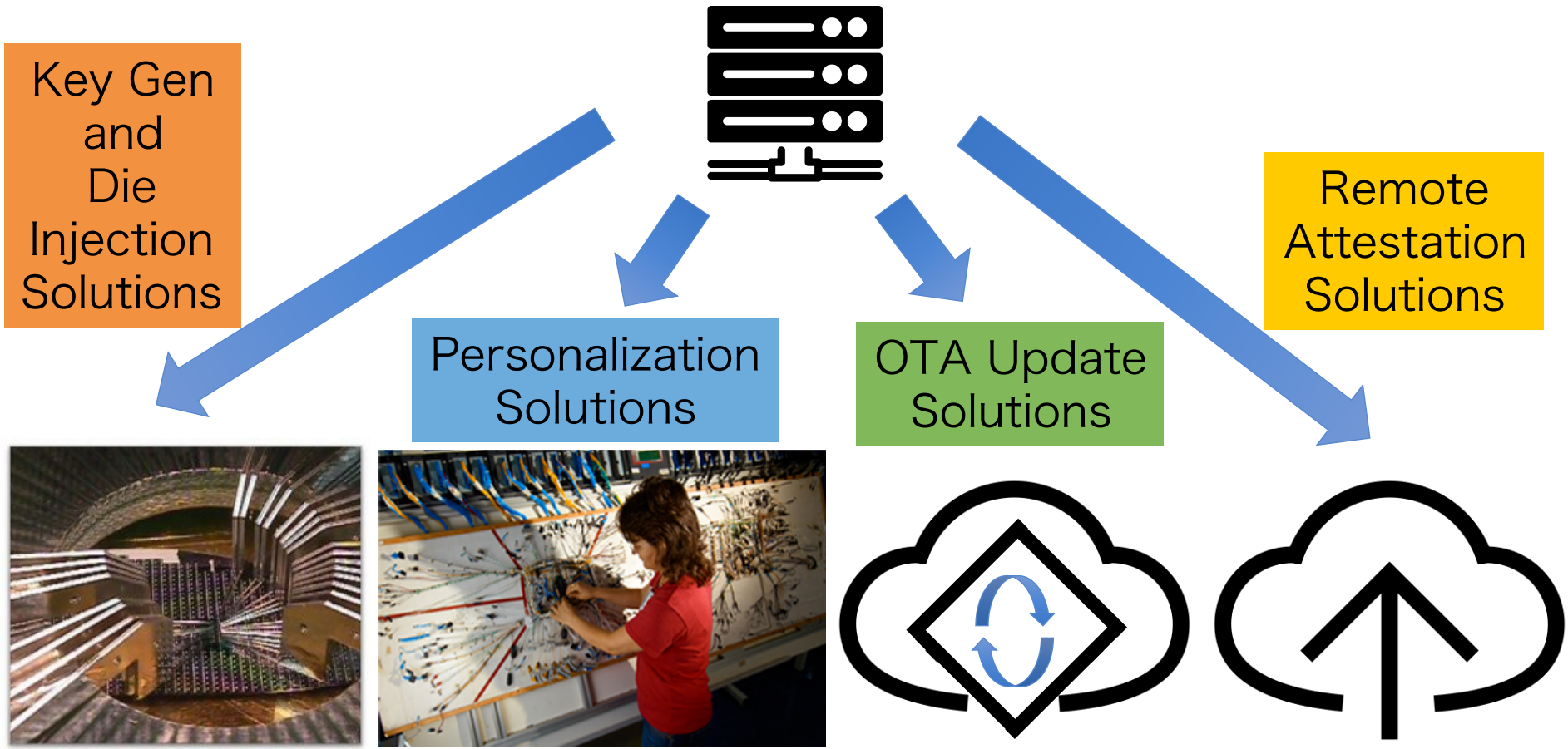
# Open Sourcing Security

- Proprietary CPUs designs are not disclosed (e.g. meltdown / spectrum).
- Third-party can confirm vulnerability for white box security functions (source code release).
- Open source security IPs will lowers barriers to secure systems and nurture future exciting application products (e.g. AI, cyber-physical systems, and robotics).
- This help transition from security based on “obscurity” to one based on “let enemy know”.

# cryptospec

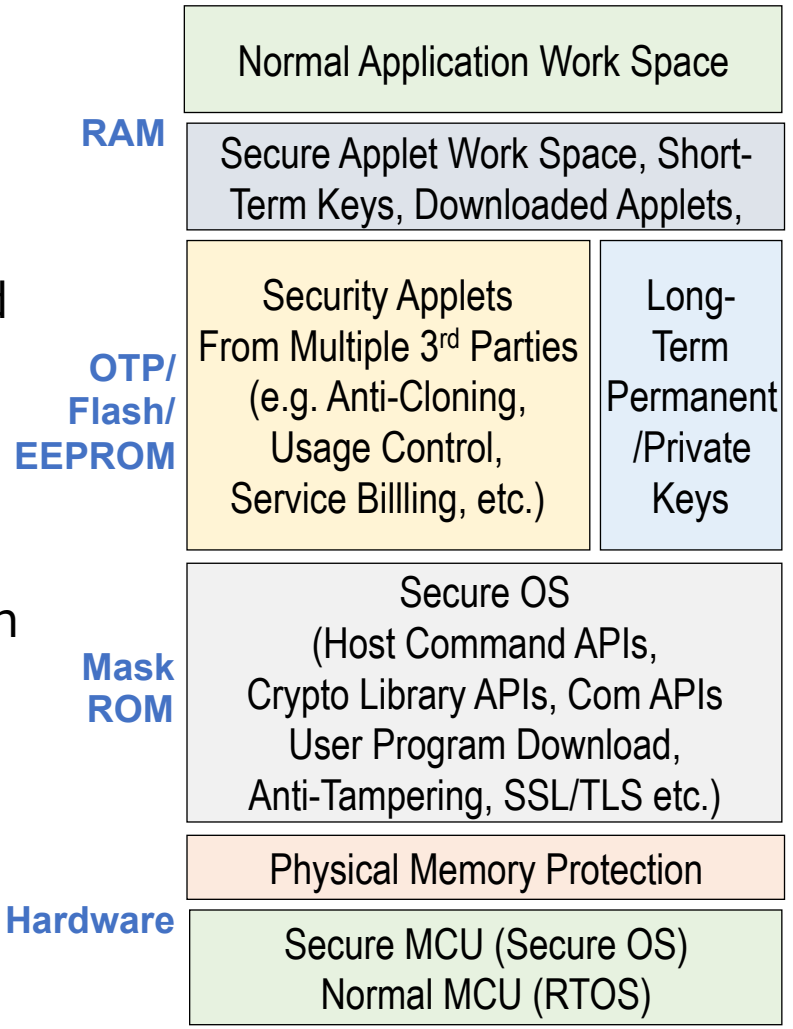
- cryptospec macro cell IP protects system and user secrets from unauthorized access.
- cryptospec is deeply embedded in 64-bit RISC-V system to prevent the main CPUs running unauthorized software. Makes go-or-no-go decision based on trust measure of the instructions/data.
- Has its own TLS software to establish its own secure connection with the server.

# Supply Chain Key Solutions

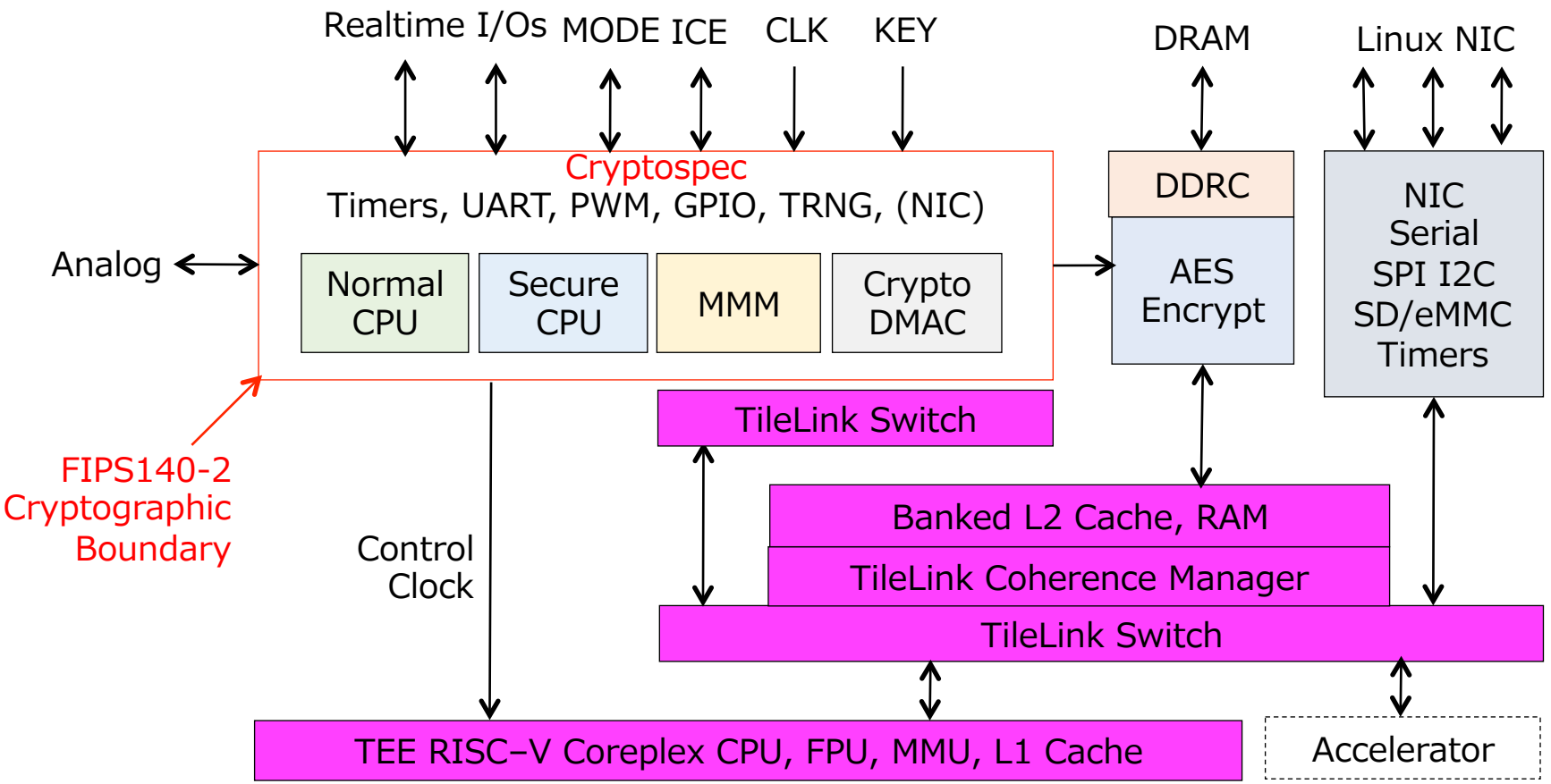


# Cryptospec Secure OS

- EEPROM/Flash/OTP stores long-term, permanent keys (e.g. RSA/DSA/ECDSA) and private keys (e.g. 3DES/AES/HMAC).
- RAM stores short-term (e.g. TLS session keys (e.g. 3DES/AES/HMAC).
- Privacy information is stored in on-chip Flash or external Flash encrypted.
- Own SSL/TLS separate from Linux SSL/TLS.
- Callback, Integrity check, Caller address list.

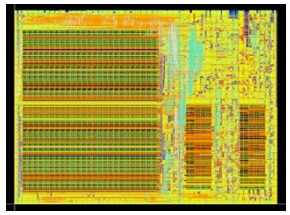


# System Block Diagram



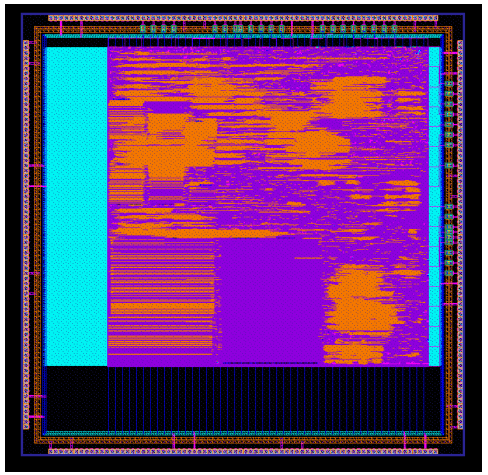
# Devkit Development

Open Secure MCU
Igloo2 25K FPGA



+

Open RISC-V Coreplex 180nm

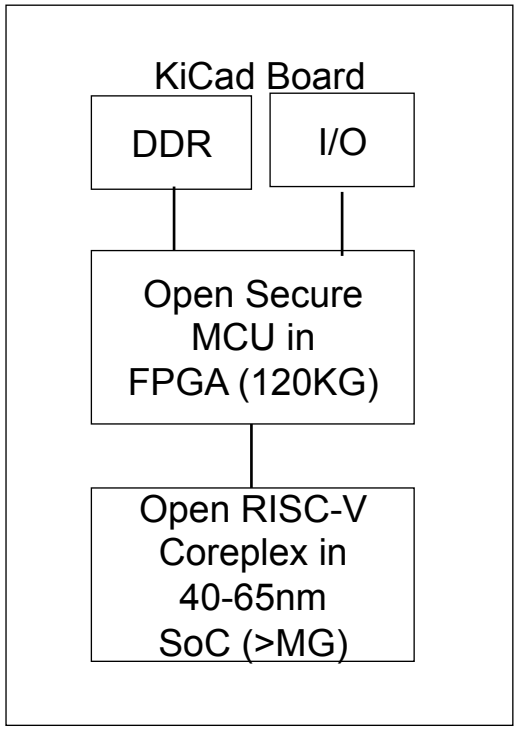



Open DevKit in Kicad

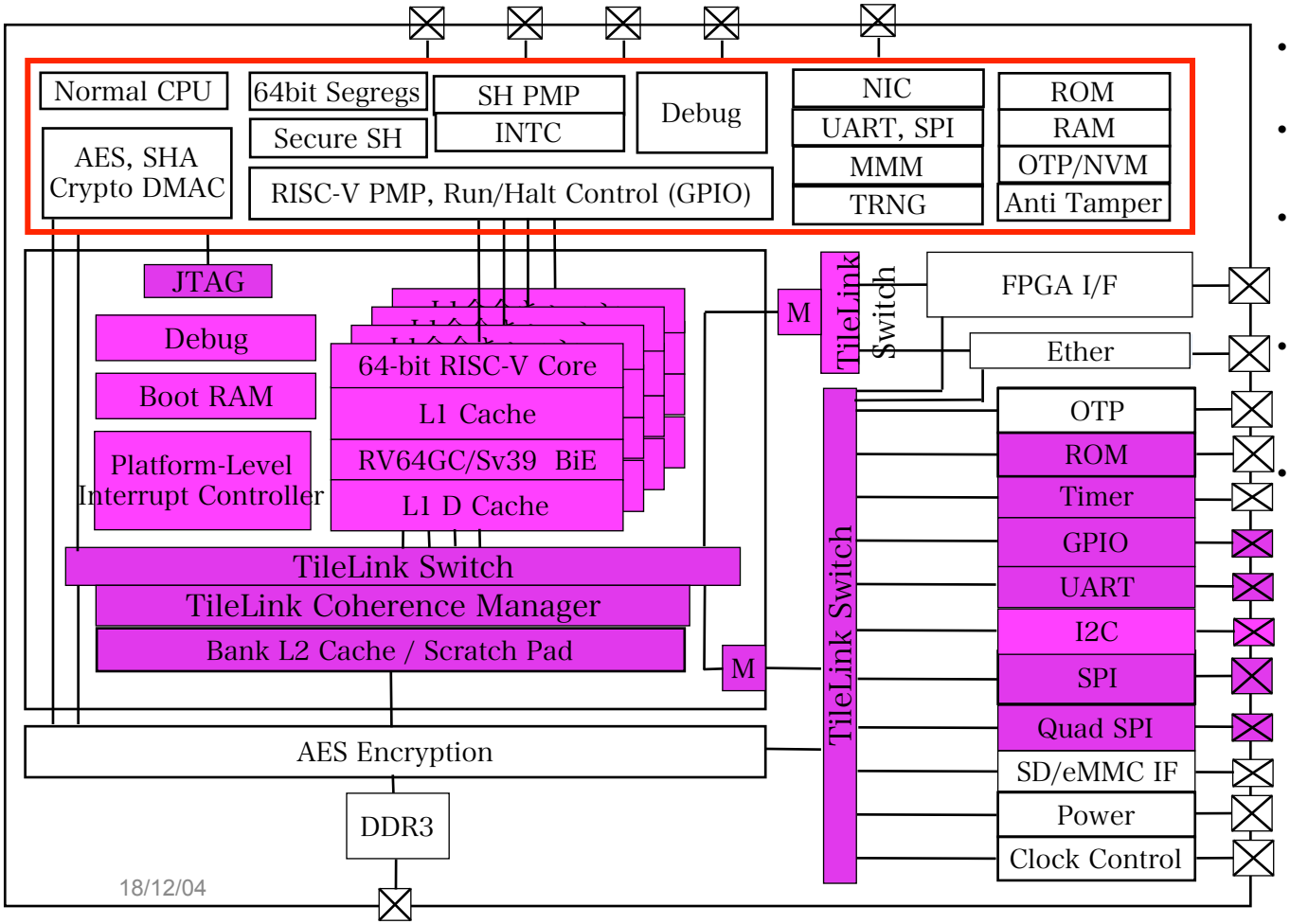
+

Open Dev Environment
OP-TEE = Trusted Execution Environment

Cyber-Physical System POC



# Secure RISC-V System




- TEE Implementation Going in Parallel
- 論理シミュレーション
  - ブートローダ動作確認
- RISC-VのTLBエント数
  - 命令：３２エントリ
  - データ：３２エントリ
- L1キャッシュ
  - 4KB (テストチップ)
  - 16KB（実チップ）
- L2キャッシュスクラッチパッド
  - L2 64KB RAM（テストチップ）
  - L2キャッシュ 256KB（実チップ）予

FIPS-140-2 Cryptographic Boundary

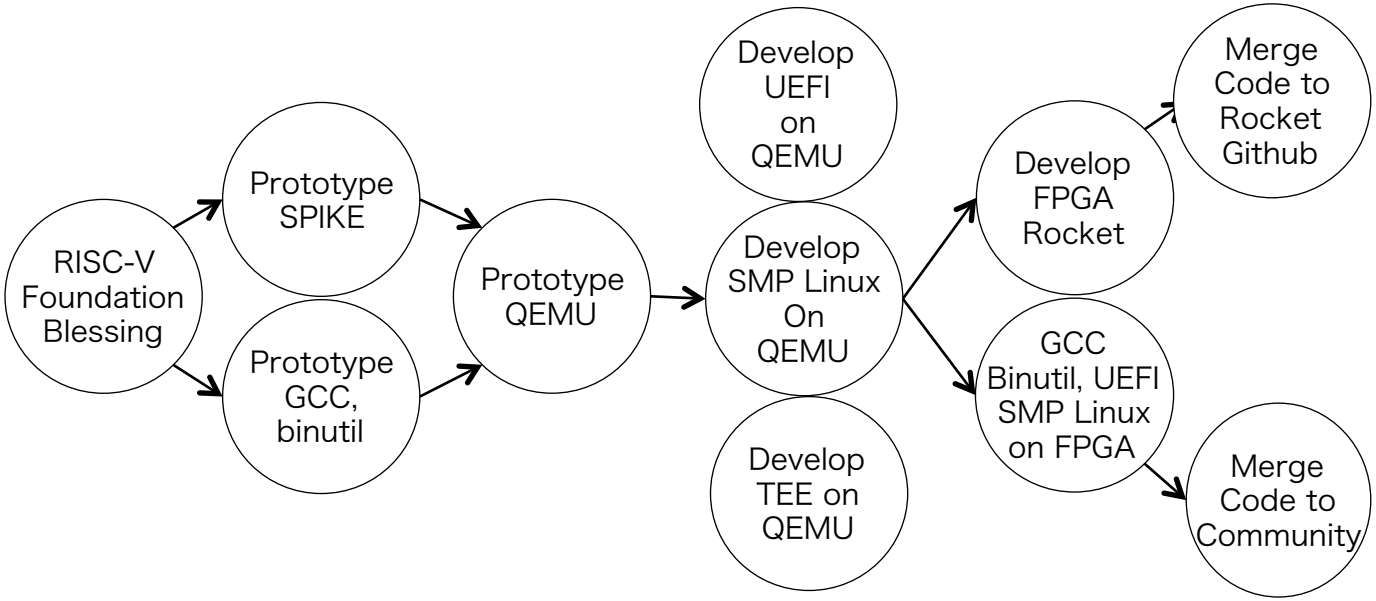
RISC-V Core Complex

# FIPS140-2 Certification

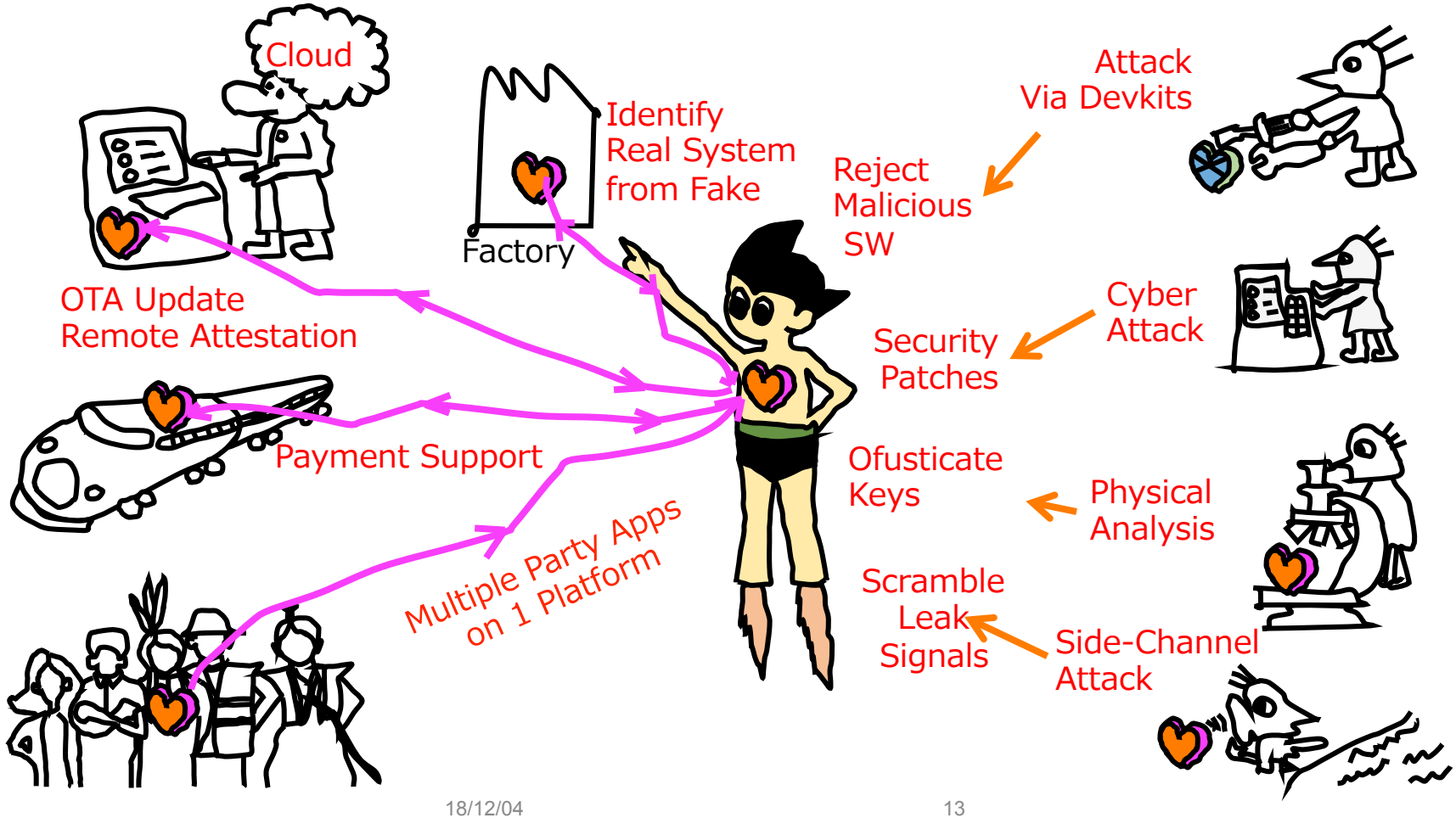
- Tamper-evident coatings or seals.
- Zeroization
- Methodically Tested and Checked: Design Assurance.
- Inputs: Security Architecture, Functional Tests, Developer Tests, Configuration Test and Developer Procedures.
- Vulnerability Analysis and Independent Testing.
- Previous Experience on FIPS140-2 Level 3 Certification.

# Bi-Endianness

- Many critical infrastructure (high-speed railroad, power plants, ) were constructed in big-endian. Despite secondary to little-endian, BIG-ENDIAN addition will be important for certain apps.
- We are ask OSS engineers in Japan in hope of making contribution to RISC-V.



# Security Needs for Society 5.0 Cyber-Physical Systems



# Conclusions



- We are planning to develop an open security system level platform with assistance from METI and NEDO.
- The benefit will be a broader reach of security technologies to IoTs without fragmenting RISC-V systems.
- The security architecture is orthogonal to the existent and future RISC-V hardware (e.g. TEE addition) and software (OP-TEE) activities also assisted by METI.
- Emphasis on Japanese cabinet's Society 5.0 infrastructure applications led us to bi-endian architecture extensions.
- We are working with AIST, Hitachi, SECOM, Keio University, University of Tokyo, NEDO and METI to make this into a reality.