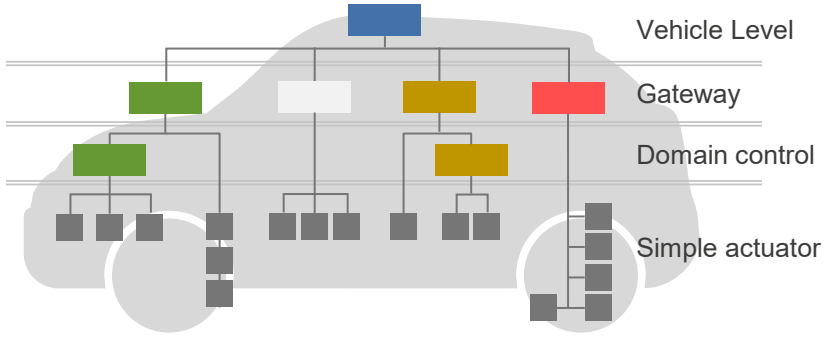
Automotive Trends in MCU/SoC Features: Opportunities for Work in GlobalPlatform

2025-05-22

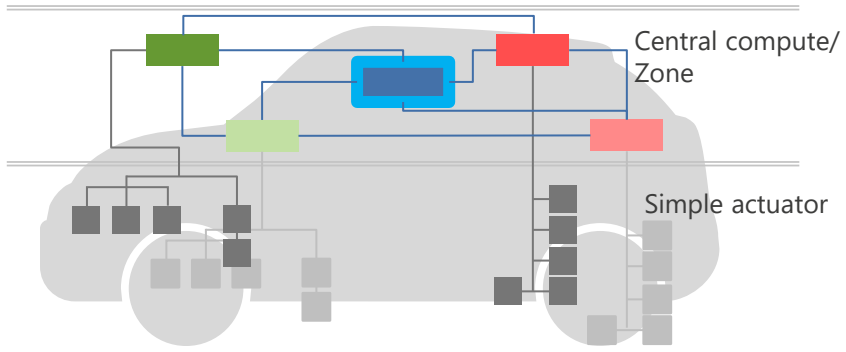
DAISUKE MORIYAMA
PRINCIPAL ENGINEER
RENESAS ELECTRONICS CORPORATION

AUTOMOTIVE IN-VEHICLE ARCHITECTURE

Today - Centralized architecture



Tomorrow - Zone architecture



- Scalable & Easy to plug-in hardware
- Upgradable & Reusable software
- Safe, redundant and streamlined network

AUTOMOTIVE MCU/SOC SECURITY DEVELOPMENT

Automotive OEM and Tier1 companies

Request for Quotation

Develop and supply MCU/SoC

Semiconductor vendors

?

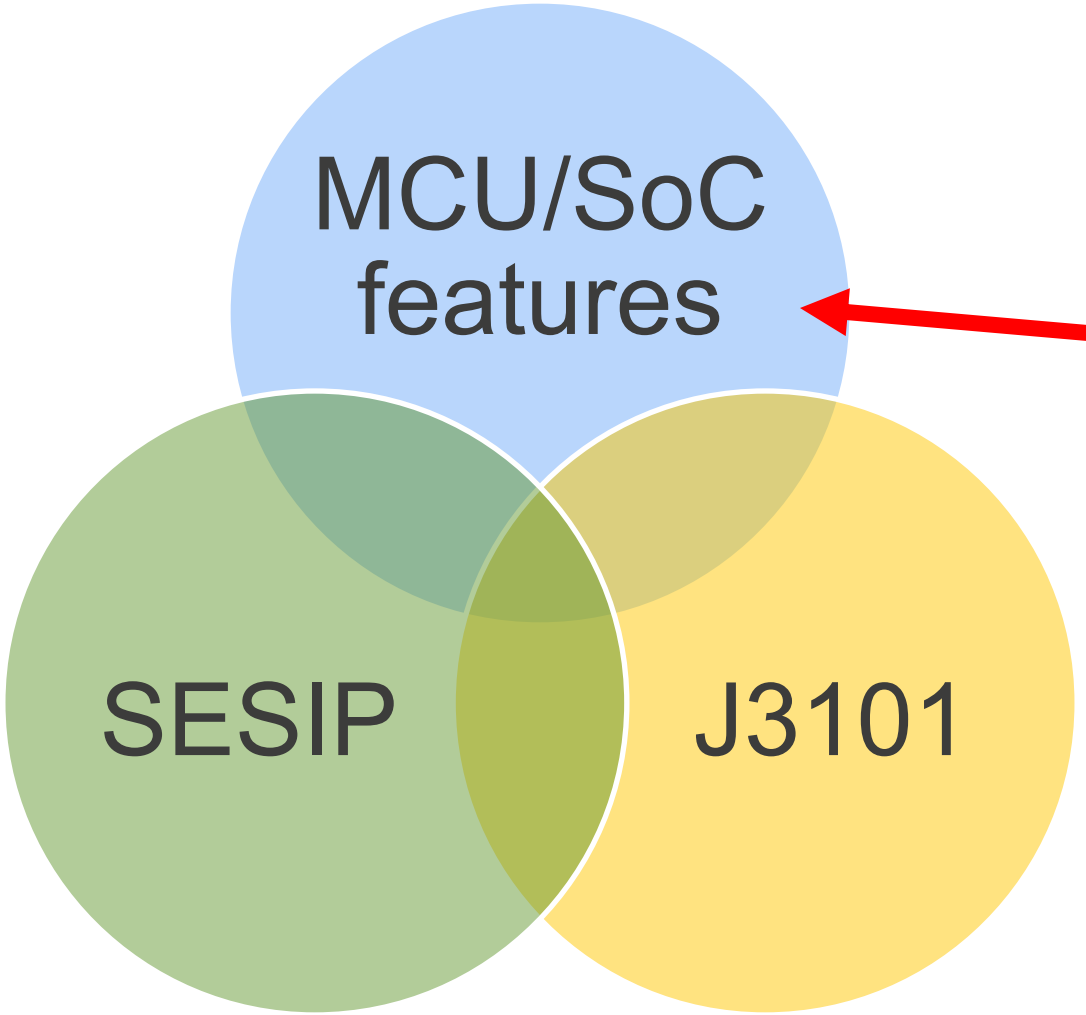
?

SESIP security functional requirements

GP_FST_070

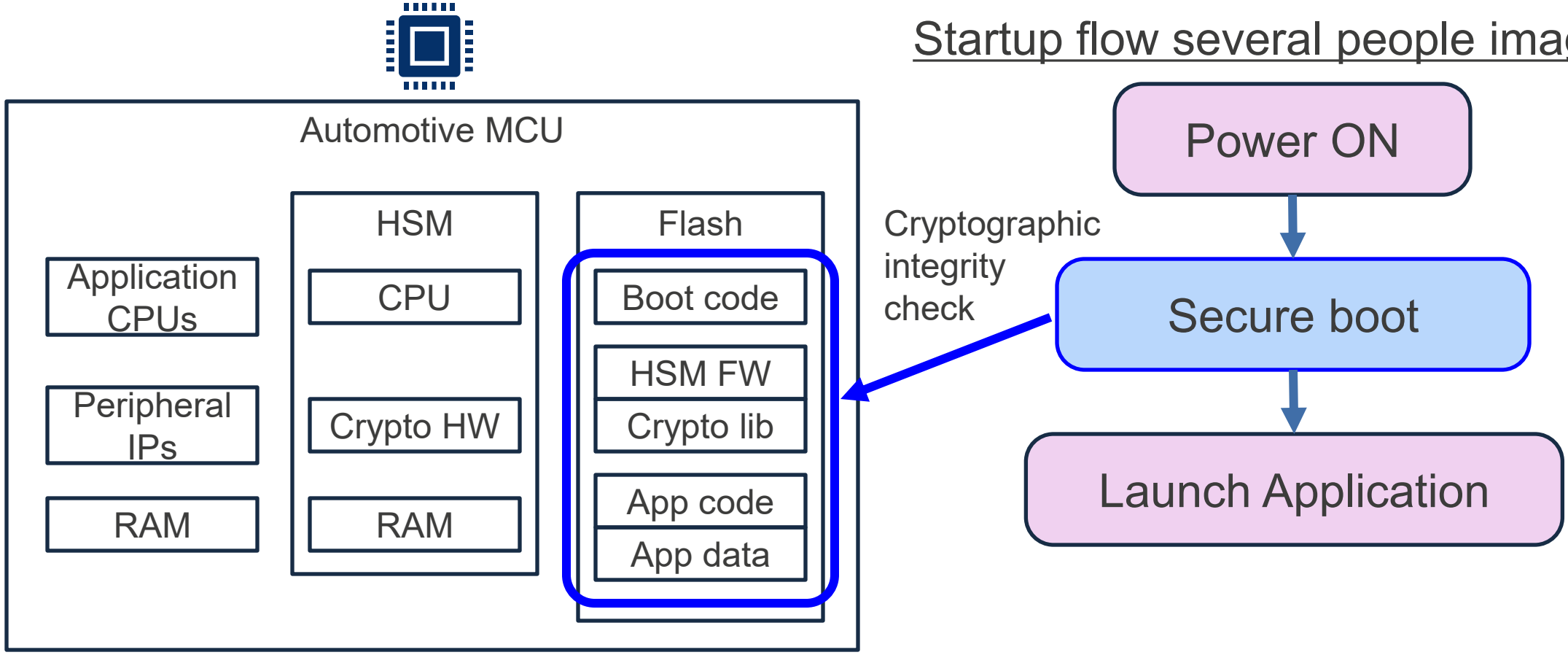
Original J3101
SESIP PP for J3101? (future)

TODAY'S TALK

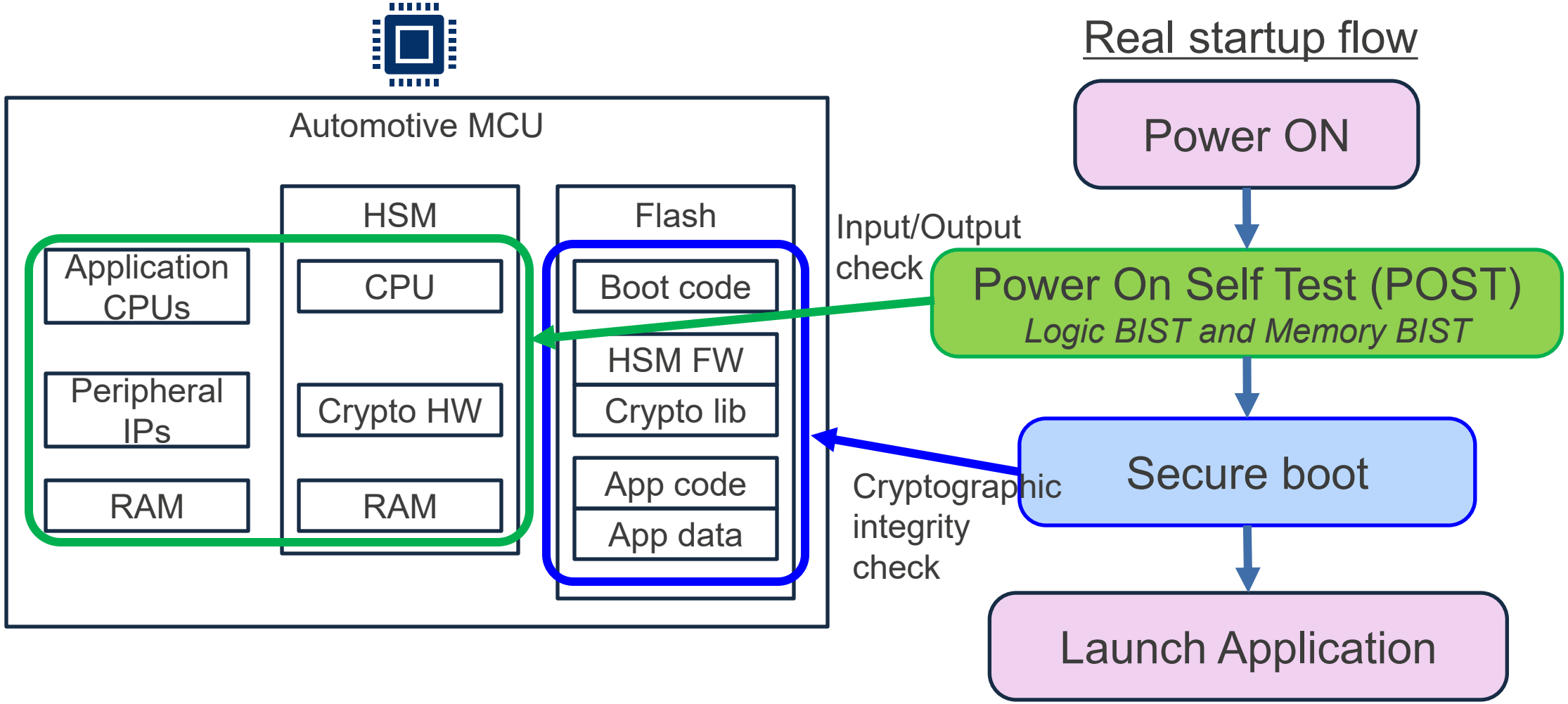


Today I focus on several **gaps** from viewpoint of one automotive MCU/SoC vendor

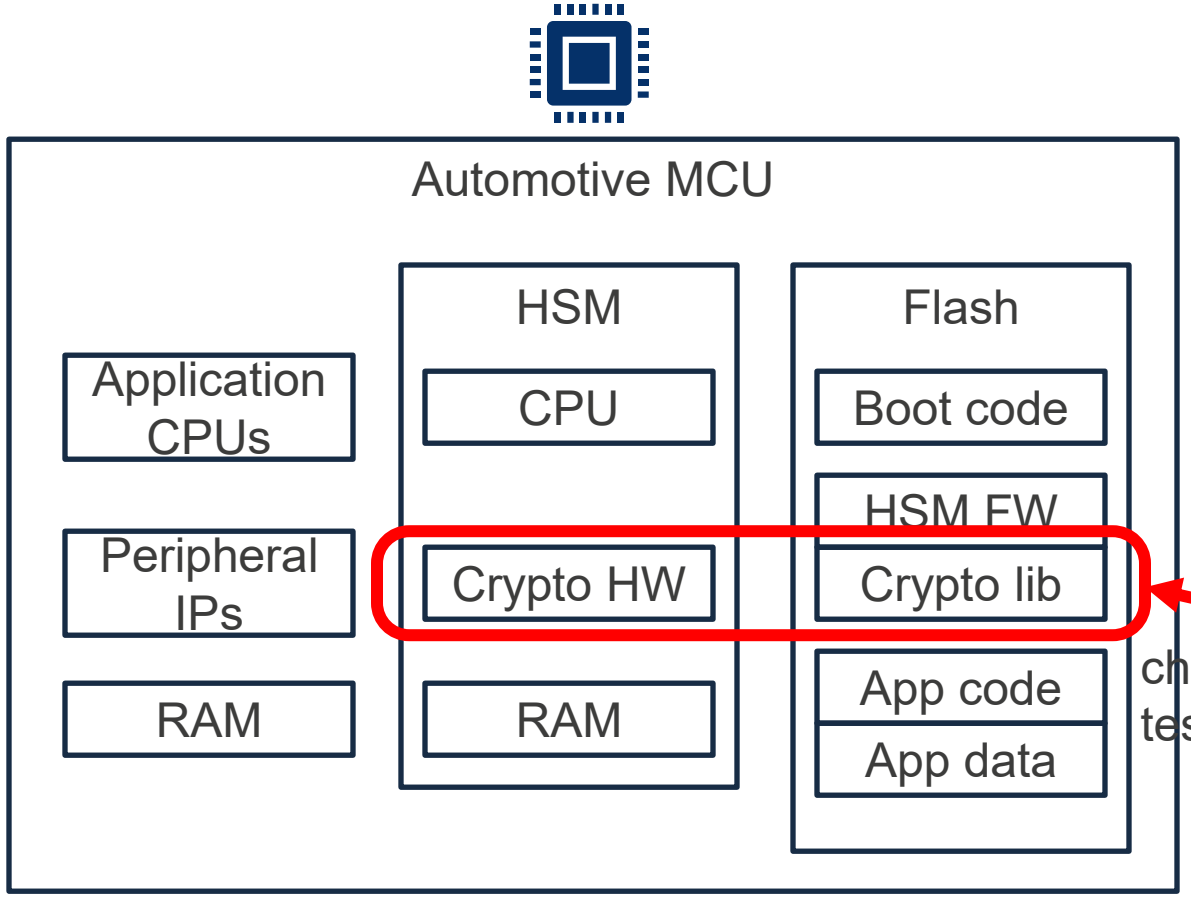
GAP 1: CRYPTO HW/SW TEST AFTER POWER-ON



GAP 1: CRYPTO HW/SW TEST AFTER POWER-ON



GAP 1: CRYPTO HW/SW TEST AFTER POWER-ON

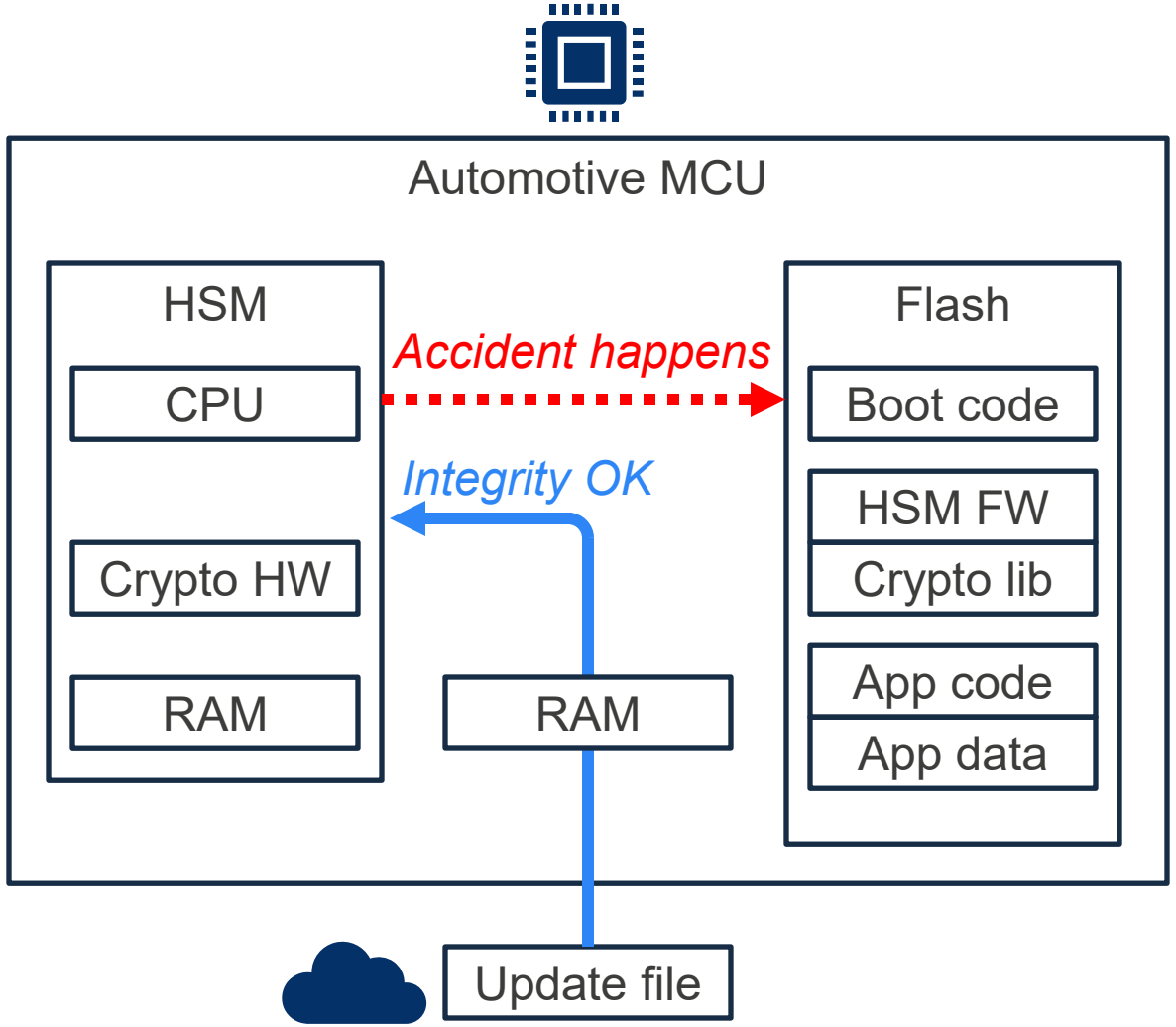


SESIP:
Only focus secure boot

J3101:
Require cryptographic algorithm self-test before secure boot

Its motivation will be to check crypto operation

GAP 2: (ACCIDENTAL) FW UPDATE FAILURE



If integrity check & update are successfully finished

➡ No trouble

If integrity check is failed

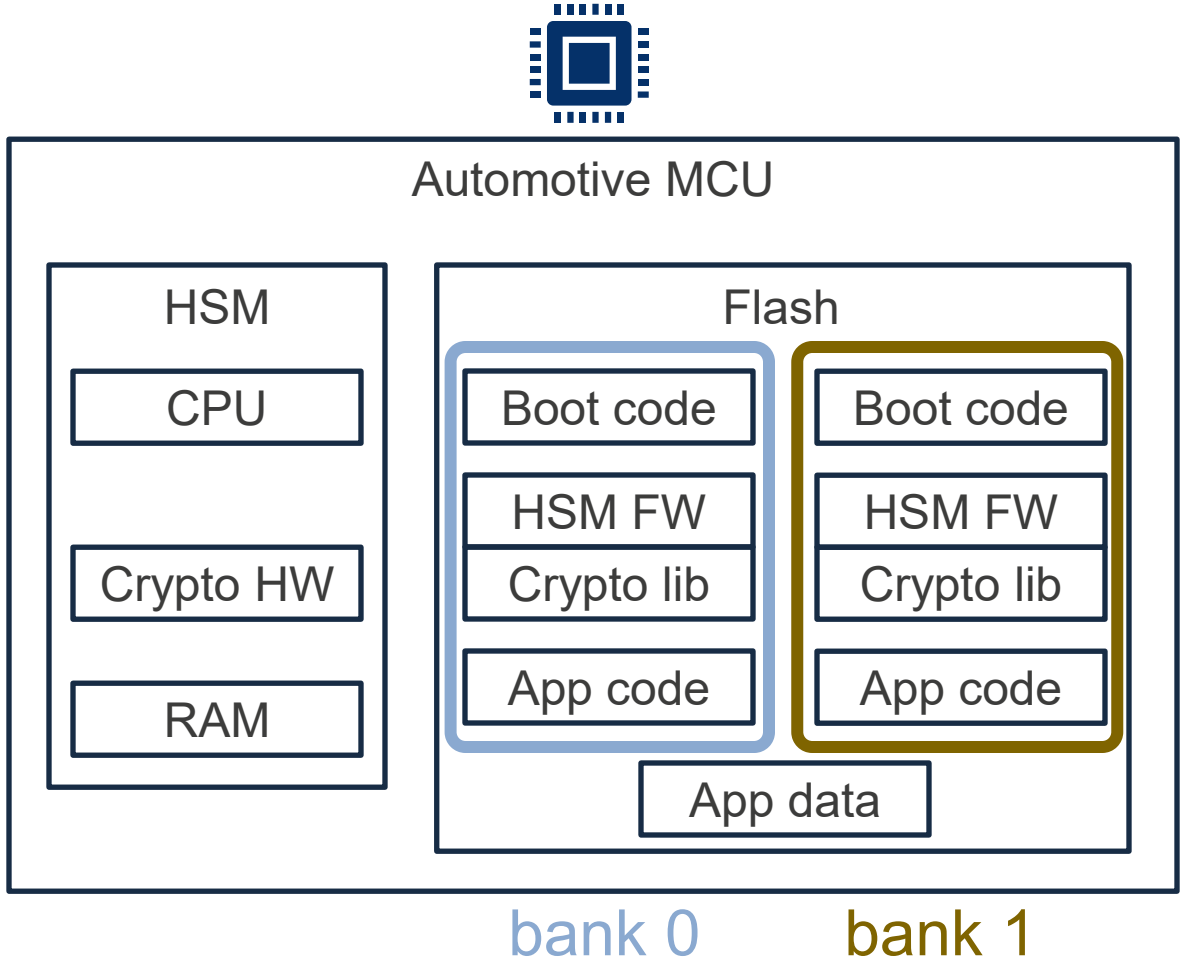
➡ No trouble

If integrity check is passed but overwrite process is incidentally failed

➡ **Problematic**

(car becomes scrap!)

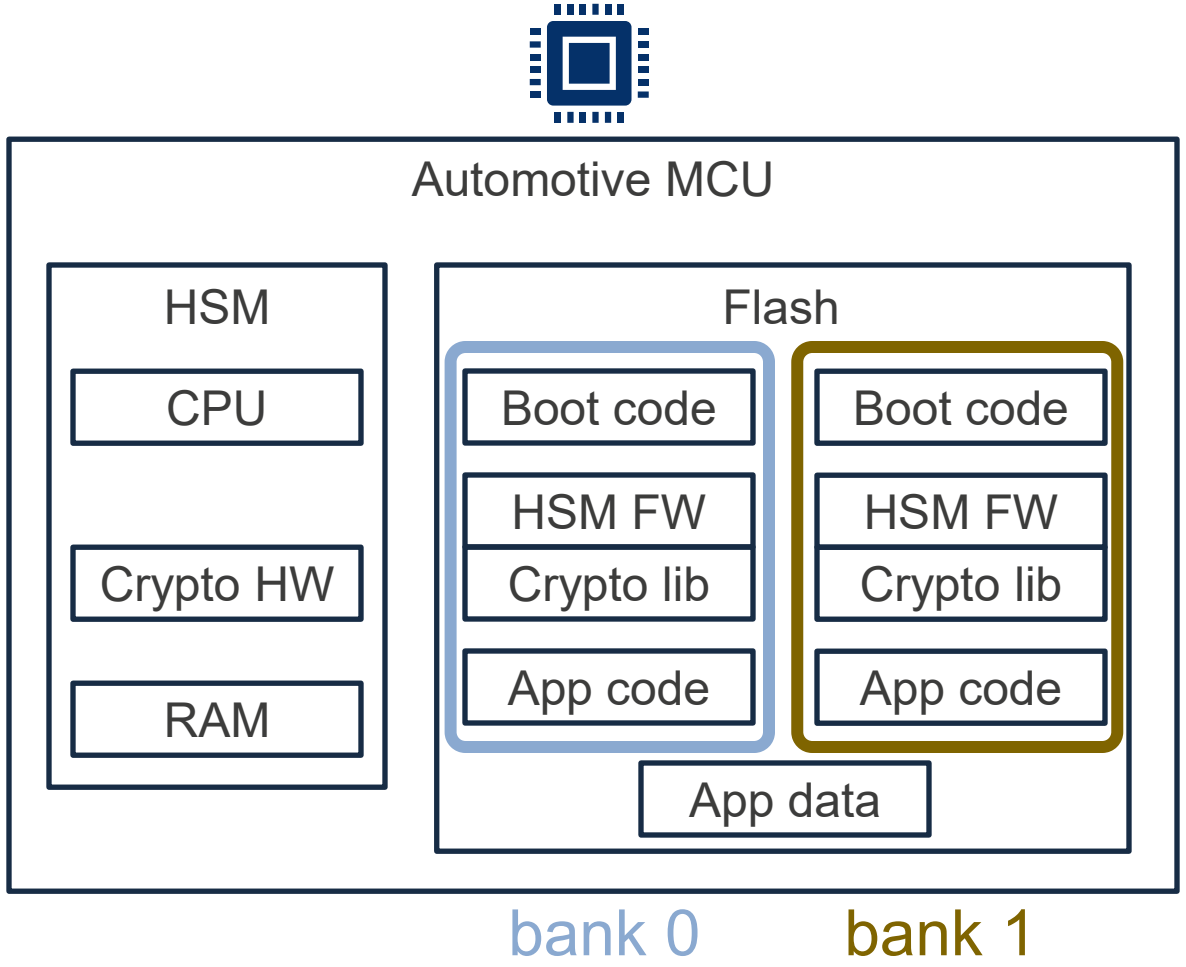
GAP 2: (ACCIDENTAL) FW UPDATE FAILURE



Double bank mechanism is adopted (to enhance both safety & security)

When a failure happens, next activation is proceeded from the other bank

GAP 2: (ACCIDENTAL) FW UPDATE FAILURE

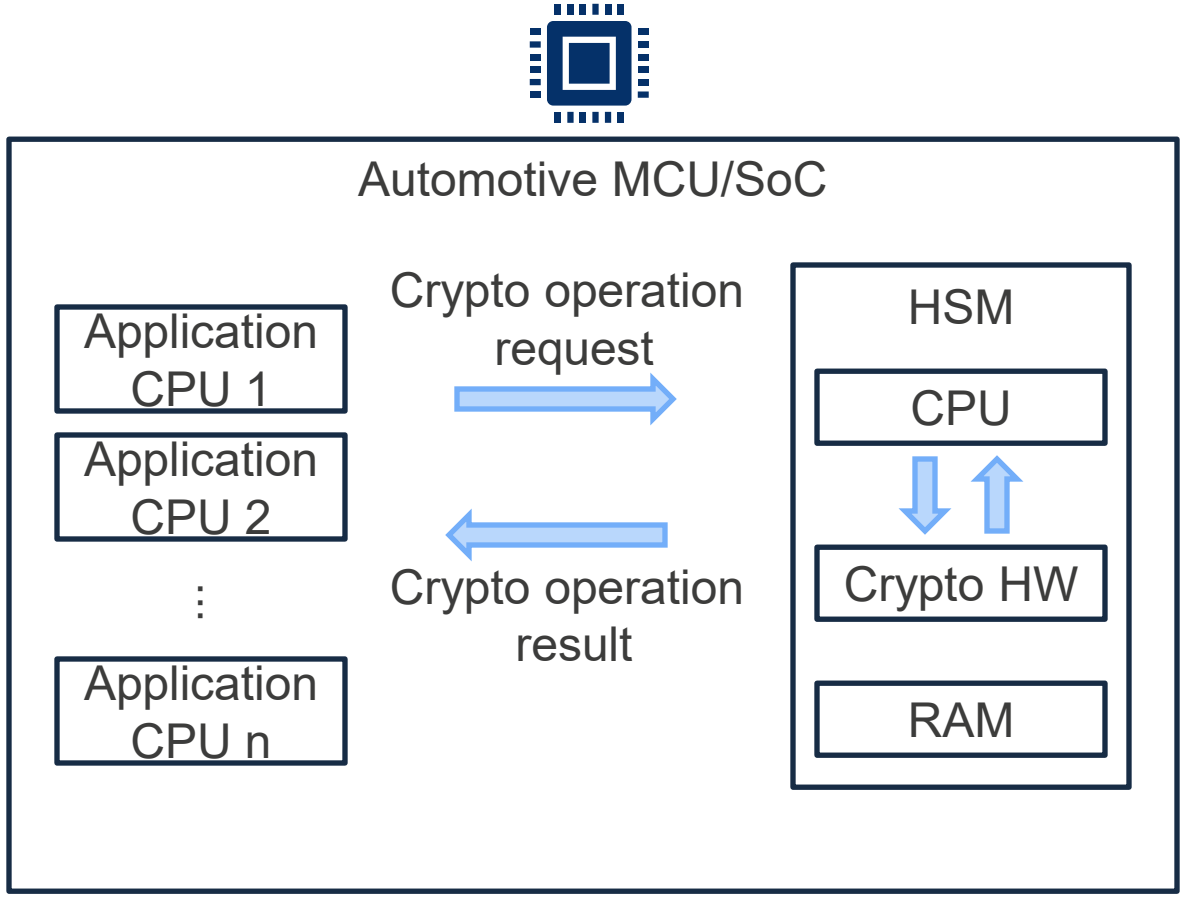


SESIP:
While FW update is required, no criteria to support double bank mechanism

J3101:
Require fallback to prevent system failure

Example includes “dual memory” architecture (as left figure)

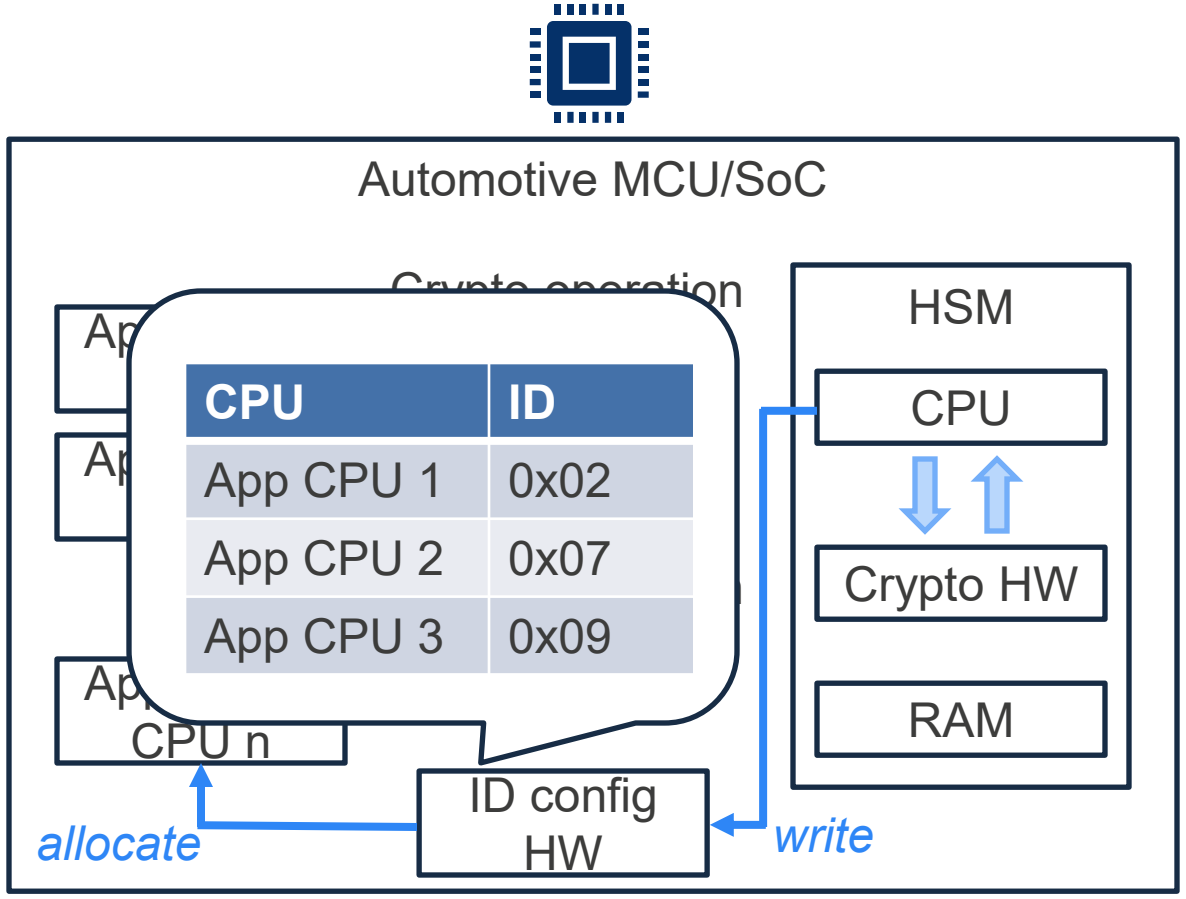
GAP 3: HOW TO CHECK APPLICATION CPU



HSM must securely manage secret keys for each application CPU

How does HSM identify application CPUs?

GAP 3: HOW TO CHECK APPLICATION CPU

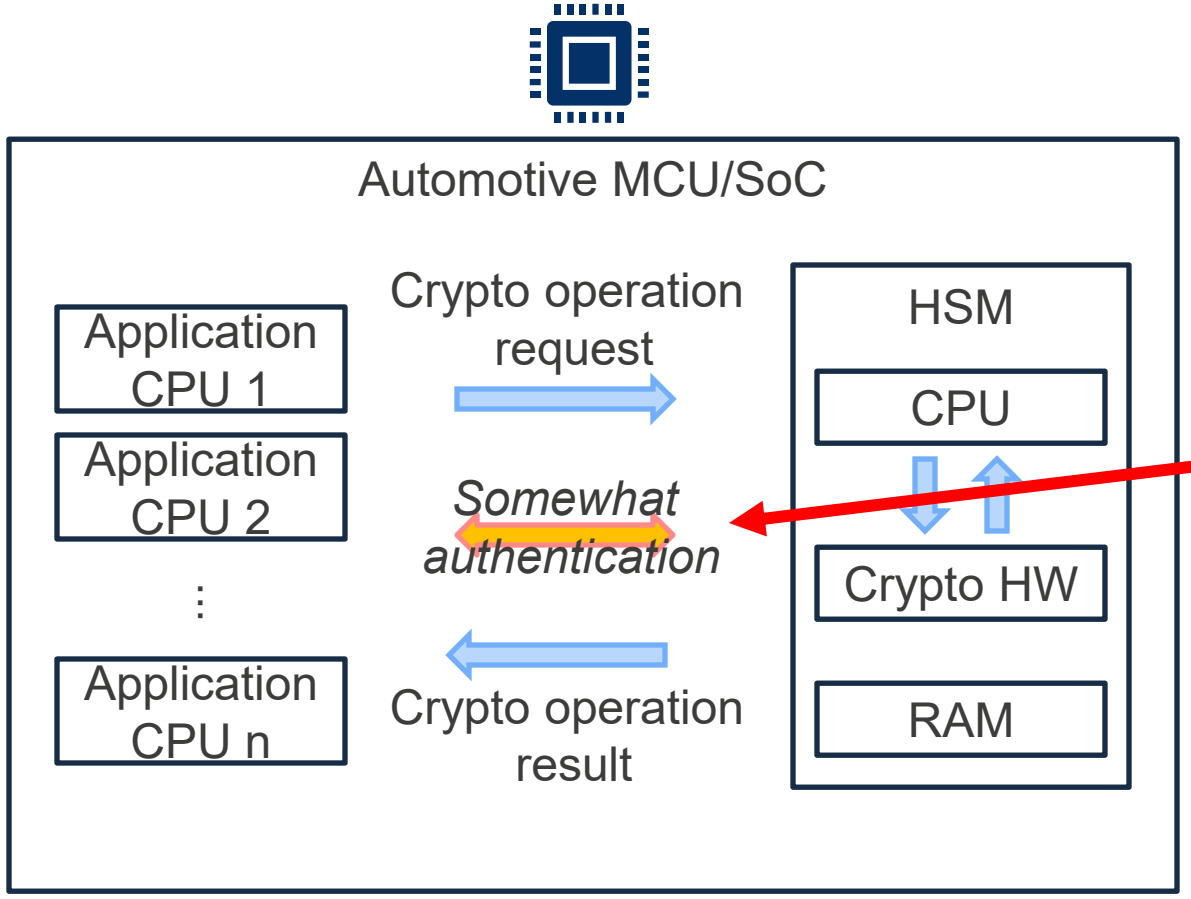


A simple solution: Assign static ID in HW or setup dedicated ID from HSM

The assigned ID can be transferred as a sideband information in the system bus

No application CPU/SW cannot cheat ID!

GAP 3: HOW TO CHECK APPLICATION CPU

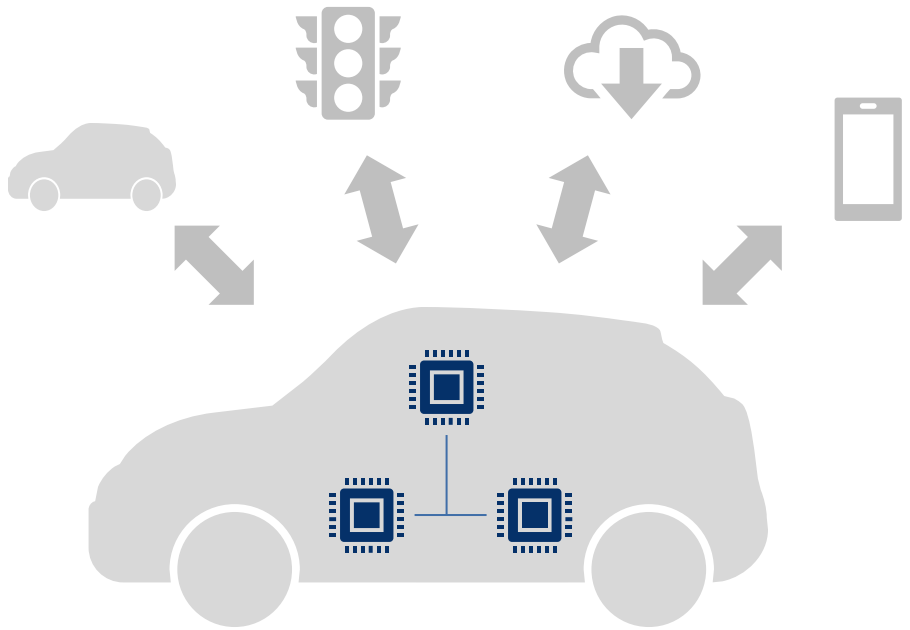


SESIP:
No focus on this issue

J3101:
Require prior authorization
before crypto operation

If J3101 follows FIPS140, this requires
- ID-password authentication or
- cryptographic authentication (MAC or signature)

GAP 4: PERFORMANCE OF CRYPTO OPERATION

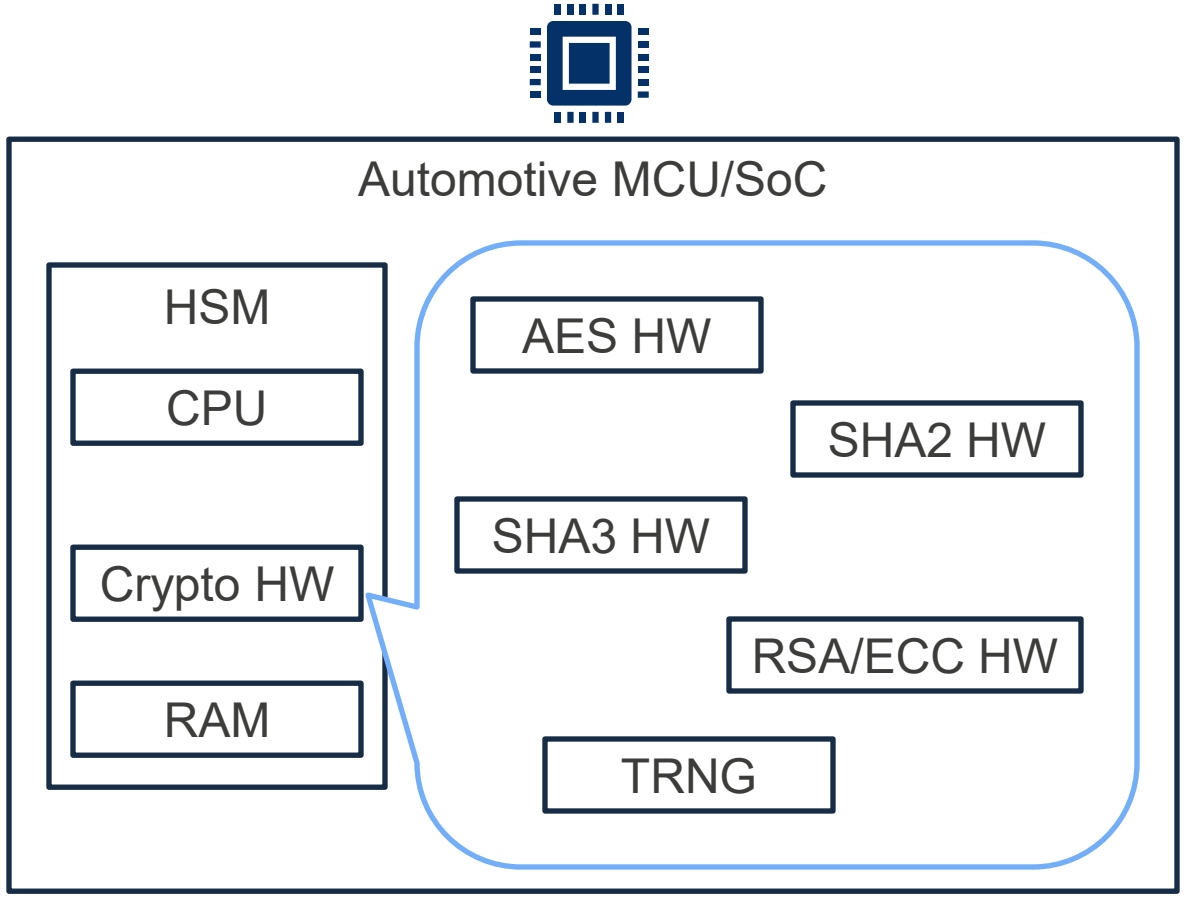


- V2x communication requires digital signature
  e.g., 1000 signatures per second
- Internet communication requires encrypted data transaction (with TLS)
  e.g., 10Gbps for 5G network

- Secure boot requires low-latency signature verification or MAC verification
  e.g., xxx ms until application OS starts
- In-vehicle communication requires low-latency CMAC
  e.g., 100 us for 1 AES block

⋮

GAP 4: PERFORMANCE OF CRYPTO OPERATION



Pure SW implementation

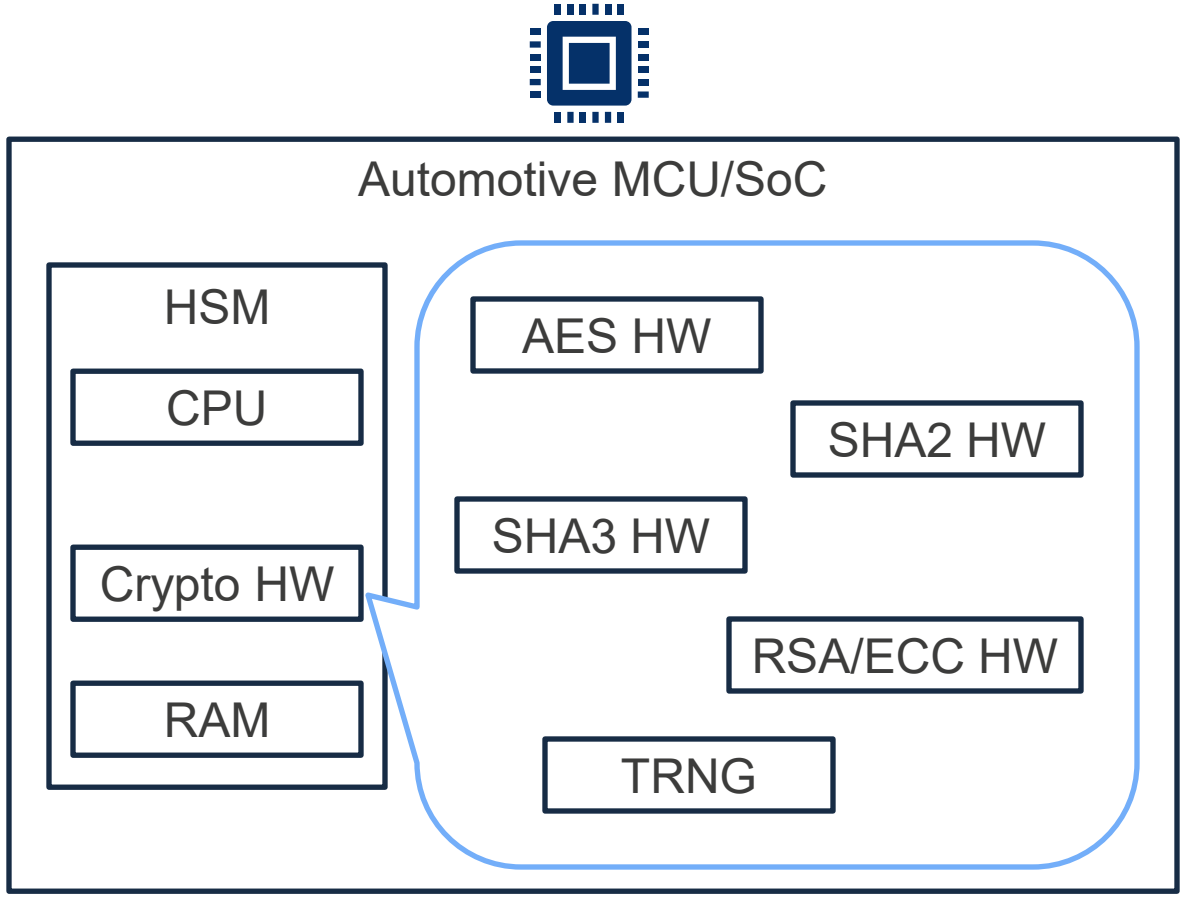
100x-1000x throughput

Crypto HW acceleration

Crypto HW support is natural to cover many scenarios

High-throughput and latency demands are higher than typical IoT devices

GAP 4: PERFORMANCE OF CRYPTO OPERATION

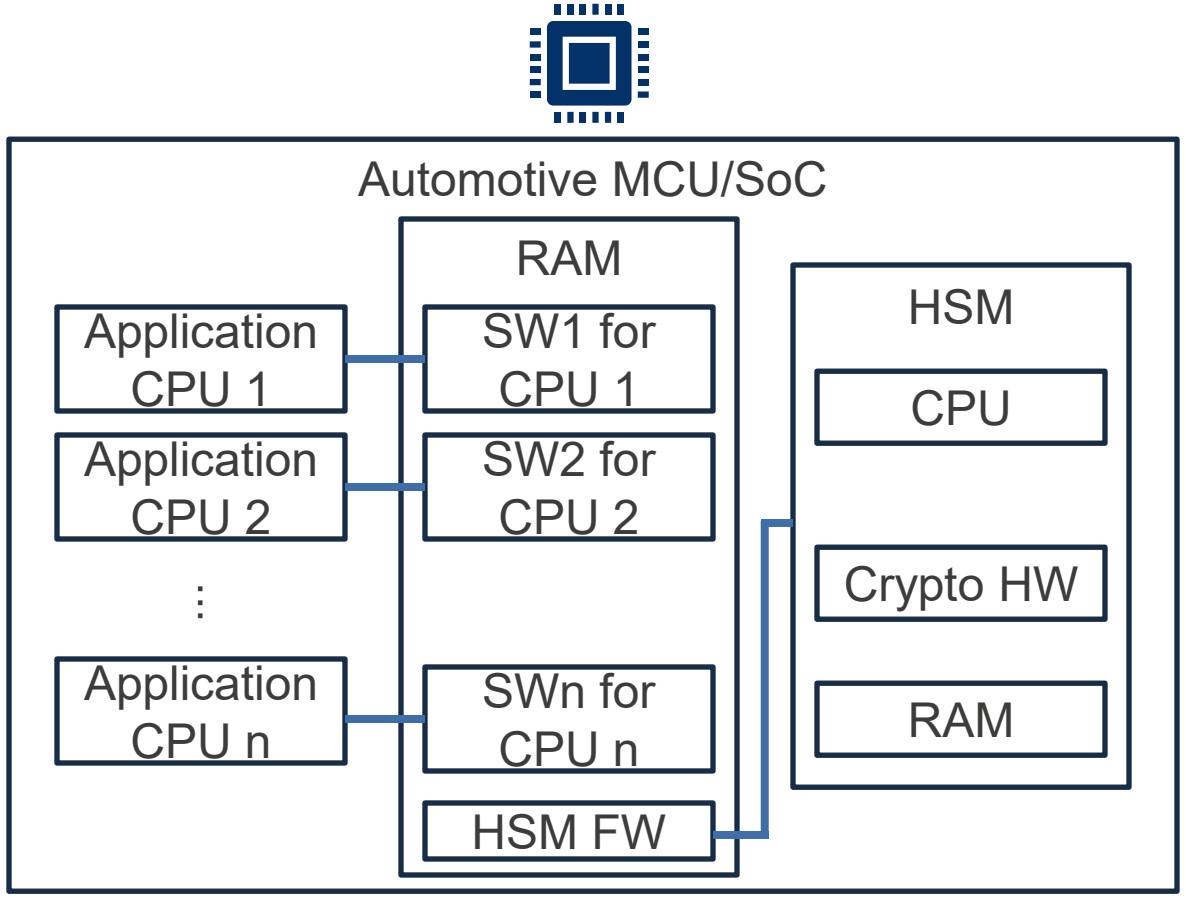


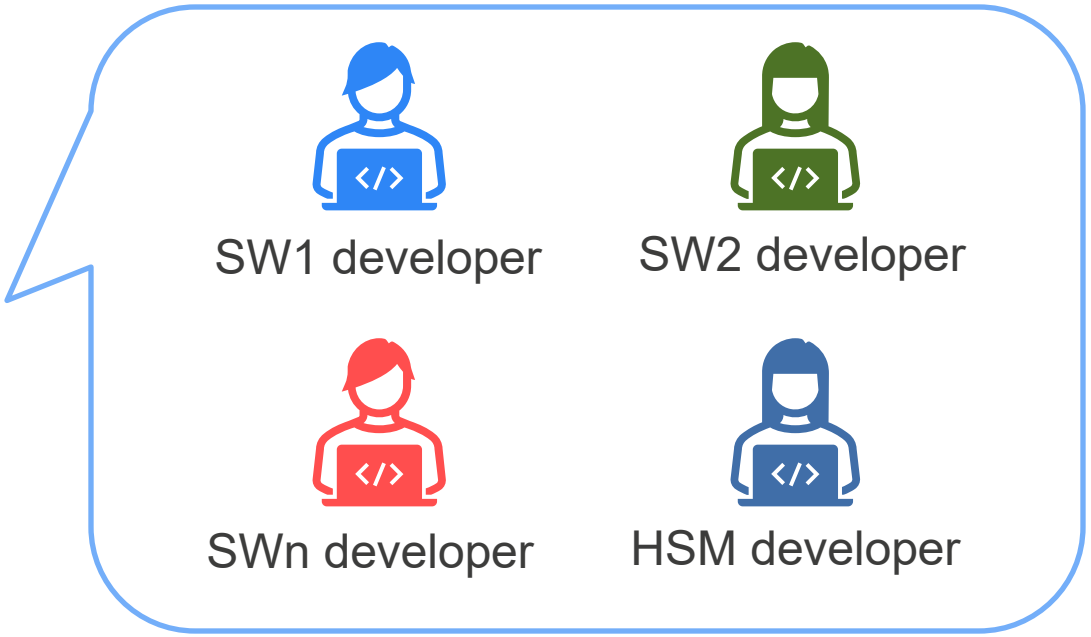
SESIP:
No throughput criteria for crypto operation

J3101:
No throughput criteria for crypto operation

Performance criteria depends on each use-case and OEM

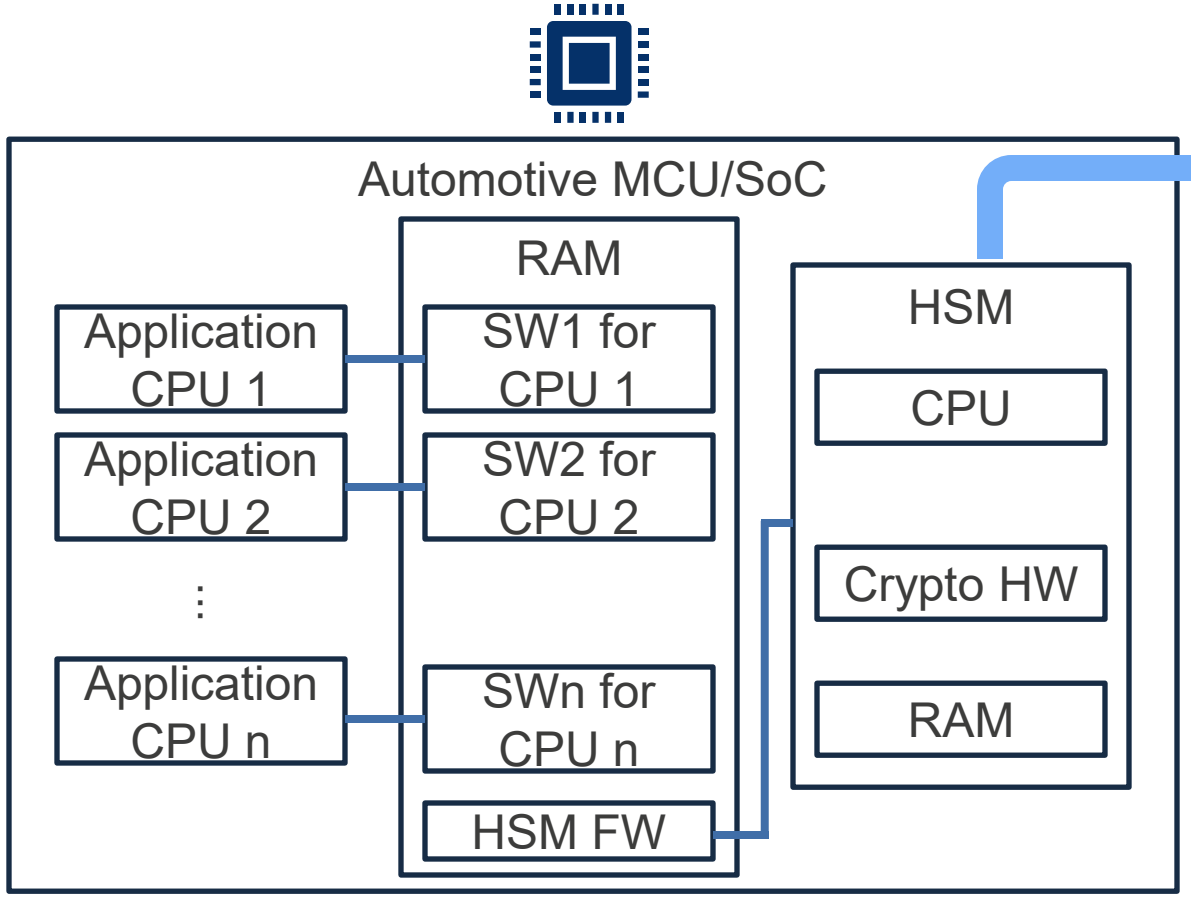
GAP 5: DEBUG ISOLATION





Many companies involve automotive software development

GAP 5: DEBUG ISOLATION

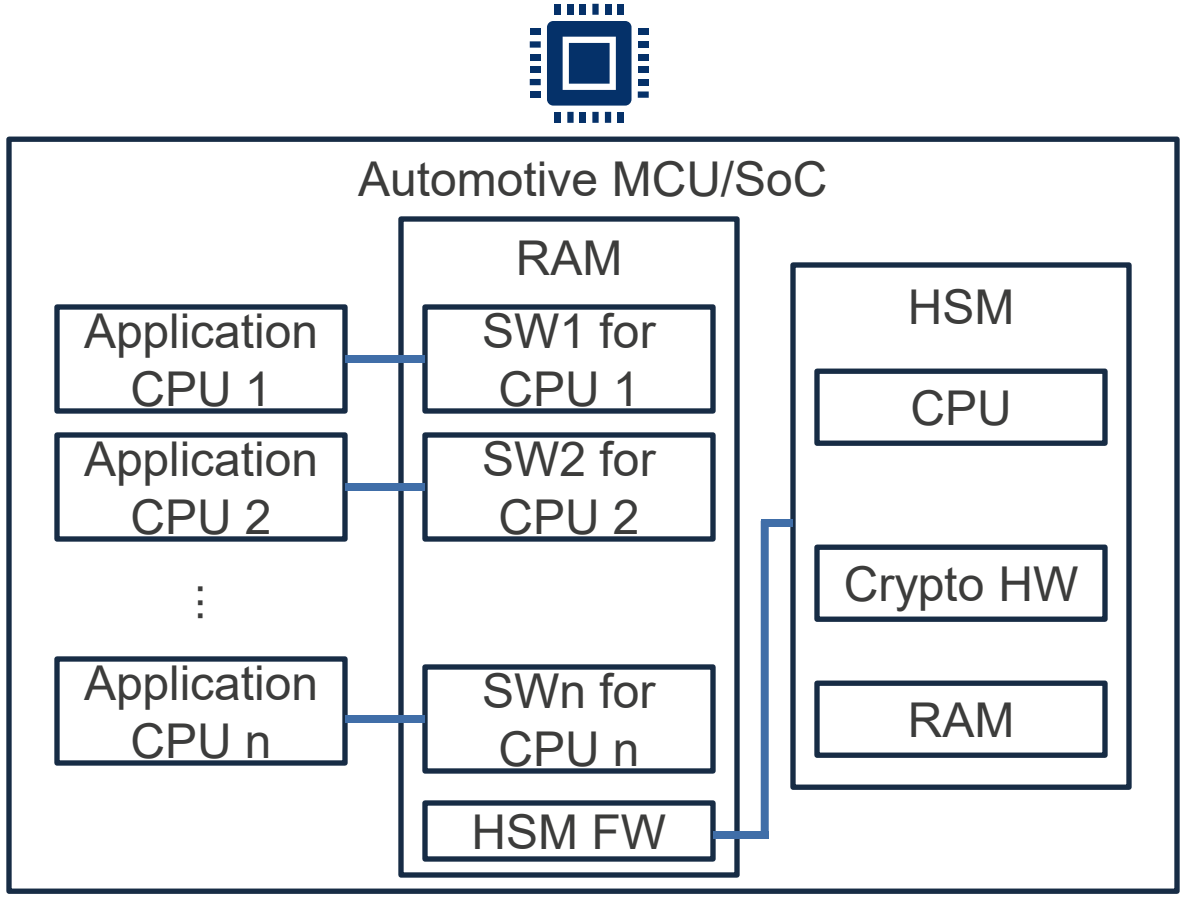


ID	Area 1	Area 2	HSM Area
ID A	OK (after auth)	NG	NG
ID B	NG	OK (after auth)	NG
ID C	NG	NG	OK (after auth)

Many companies involve automotive software development

Debug access area should be isolated even in application area

GAP 5: DEBUG ISOLATION



SESIP:
Multiple developers are not so focused in secure debug

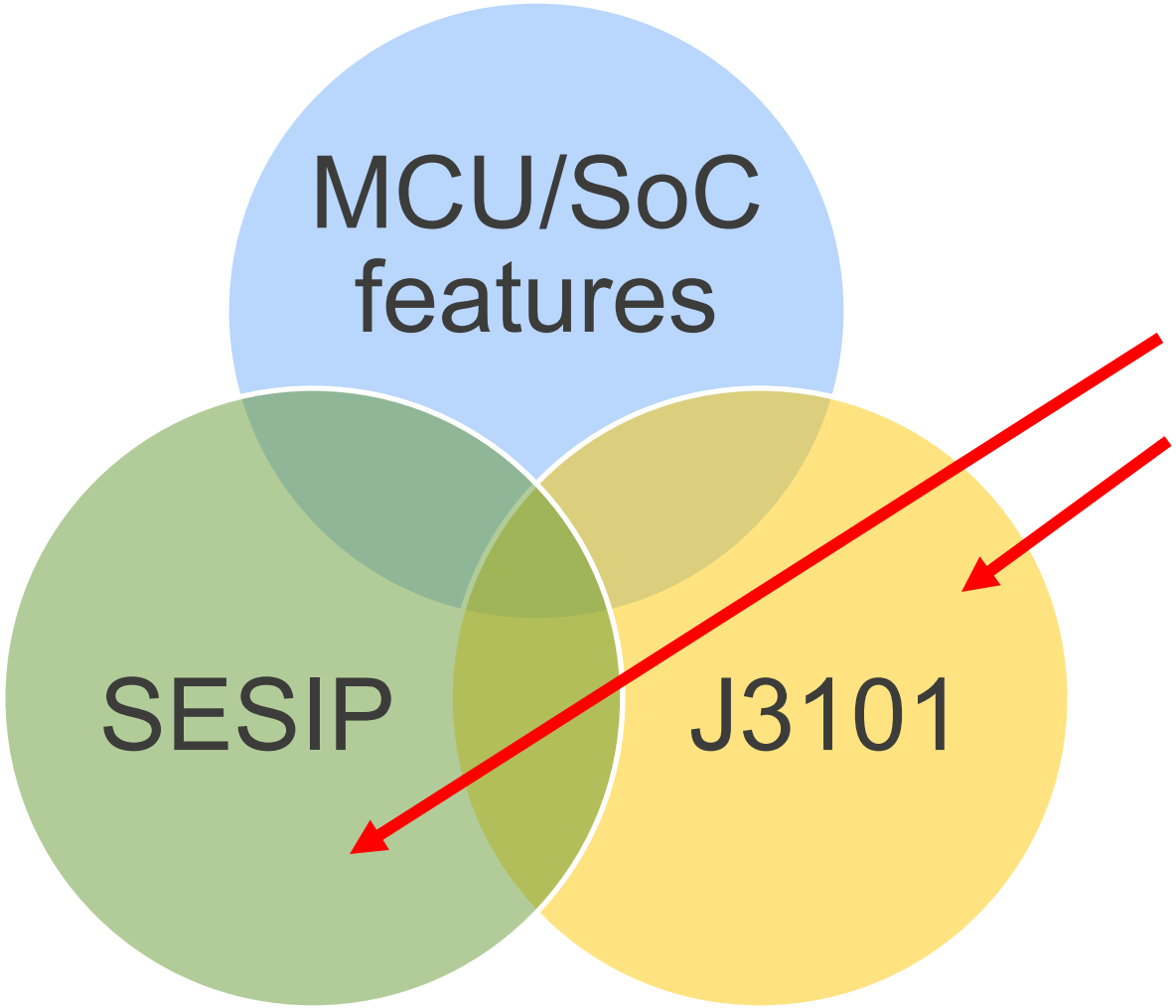
For in-field operation (not debug), SESIP defines several isolations

Application	⟺	HSM
HSM1	⟺	HSM2
Application1	⟺	Application2

J3101:
Require HSM/normal debug isolation only

Application	⟺	HSM

FUTURE ARGUMENT



Several SESIP and J3101 requirements are related to application layer security and operational issues

How to find the gap in them may be provided by OEM/Tier1

SUMMARY

- Automotive MCU/SoC include practical security features
  - Other semiconductor vendors may provide additional security features... please share!

- I wish GlobalPlatform extracts real demands from automotive OEM/Tier1/chip vendors to establish usable certification and standardization

Renesas.com