Secure Partition Manager Update Initial Investigation

An Implementation Update

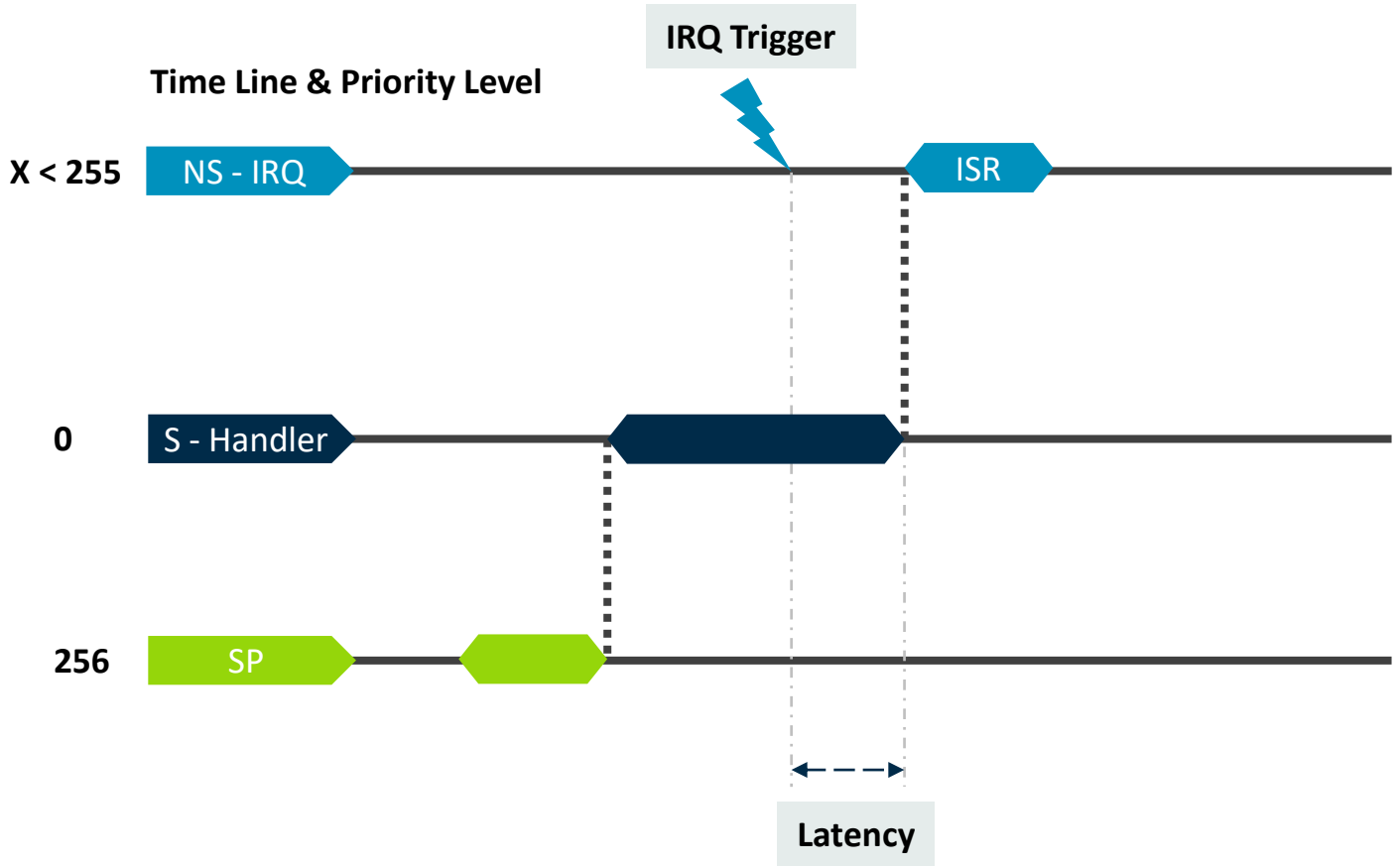
Ken Liu

Mar 18

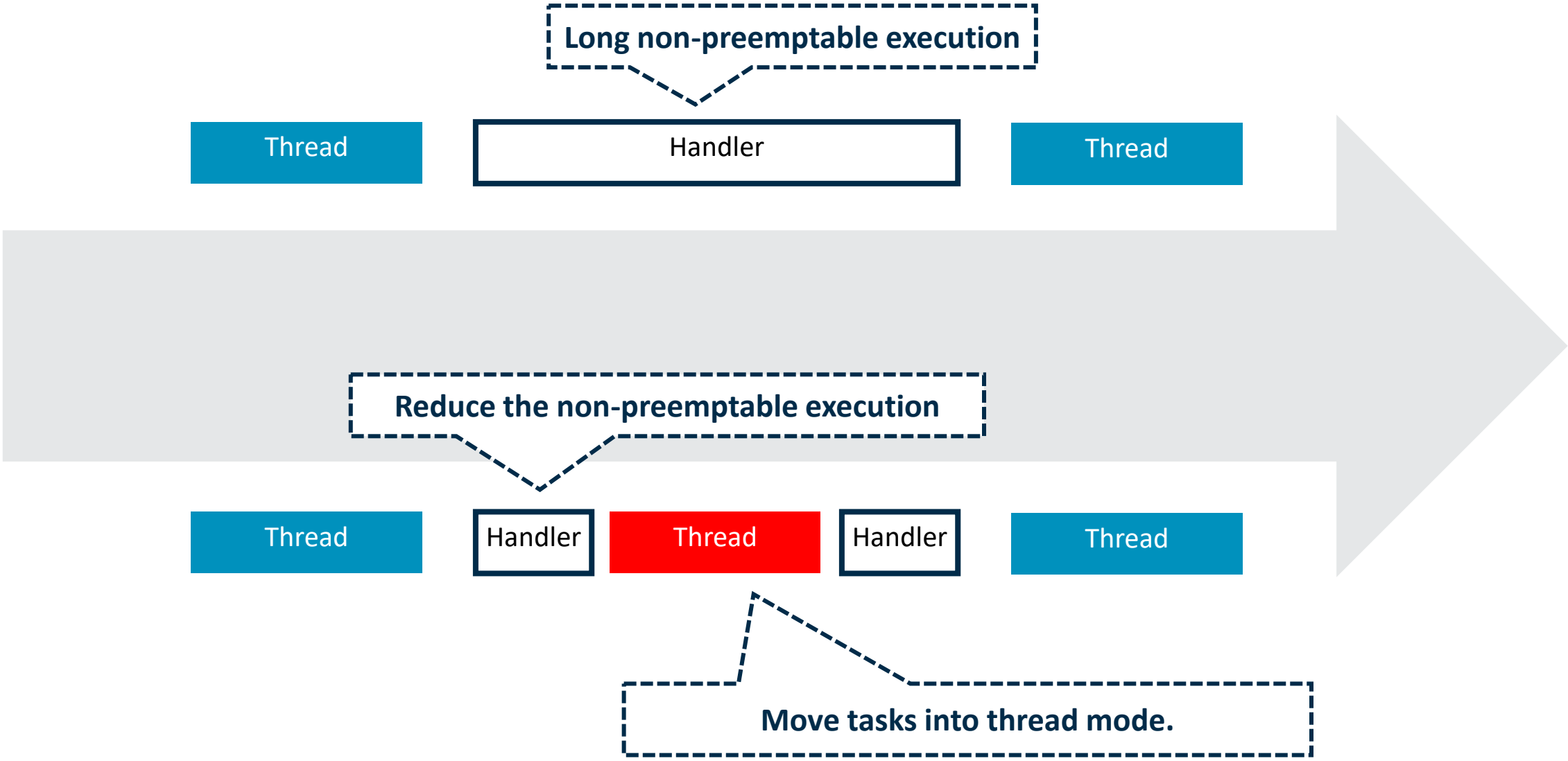
Backgrounds

- NS RTOS wants to reduce the impact on NS interrupt handling.
- The FF-M updated to 1.1 version supports simpler smaller system.
  - Secure Function Model (SFN).
- SPM needs to be updated to address the two main requirements above.

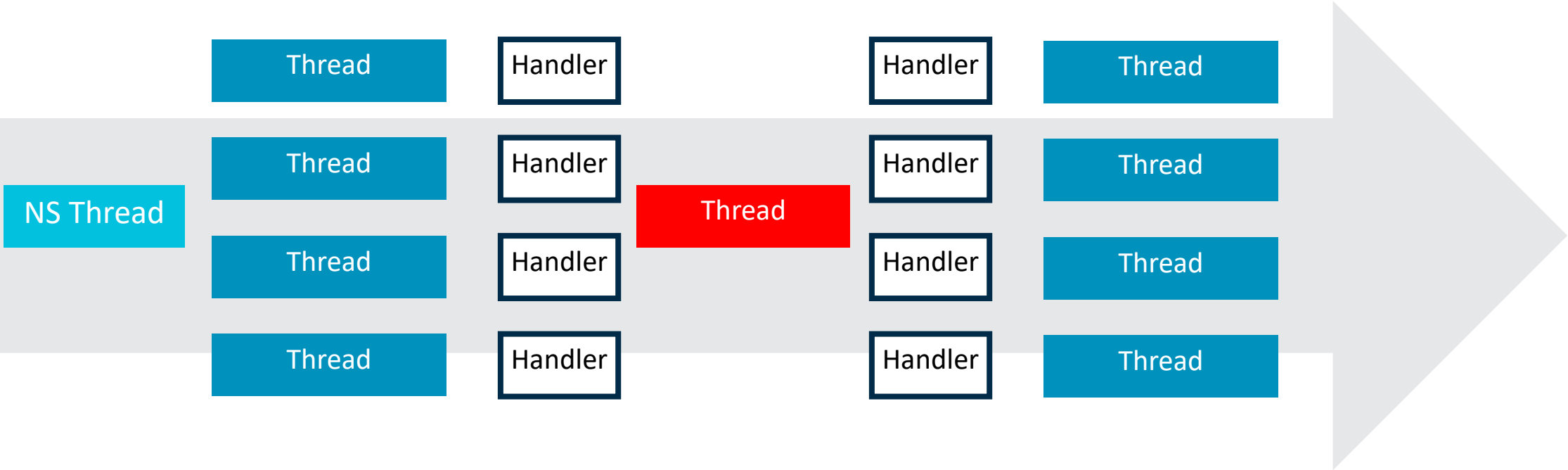
The NS Interrupt Handling Latency



Existing Execution Timeline and Expected Timeline



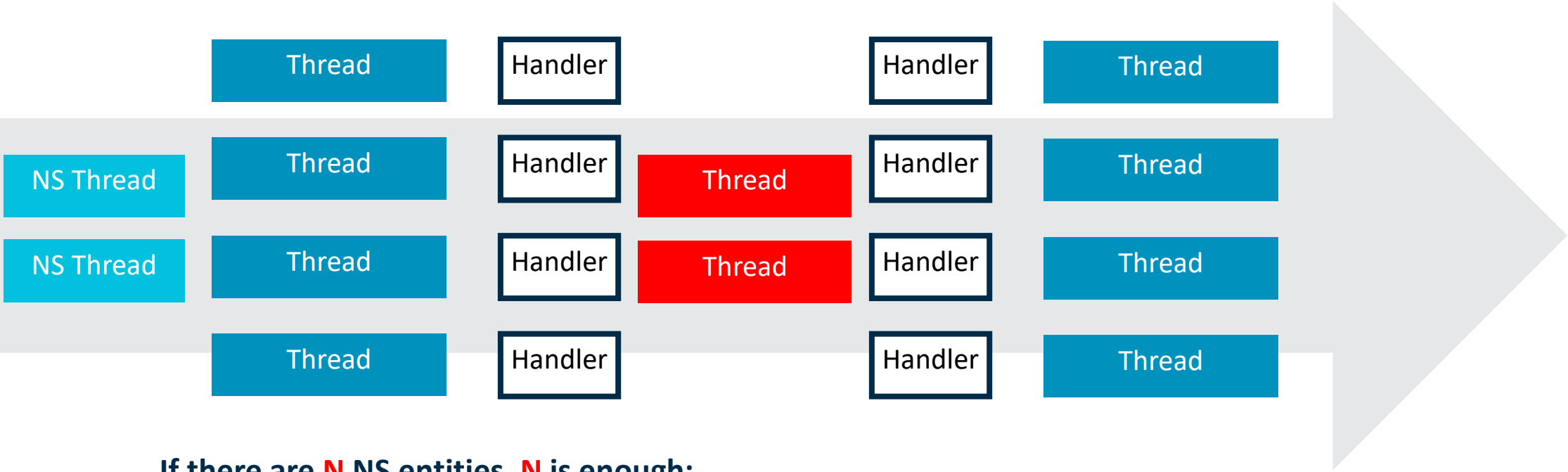
How many privileged thread instance are needed?



If there is ONE NS thread is supported, only ONE is enough:

- **Privileged thread has highest software priority (it would get run first if it is there).**
- **HW priority is still 256 to be preempted by interrupt routine.**

How many privileged thread instance are needed?



If there are N NS entities, N is enough:

- **Privileged thread has highest software priority (it would get run first if it is there).**
- **HW priority is still 256 to be preempted by interrupt routine.**

Reason:

- **Secure firmware execution is typically triggered by NS (NS is the initial user!).**

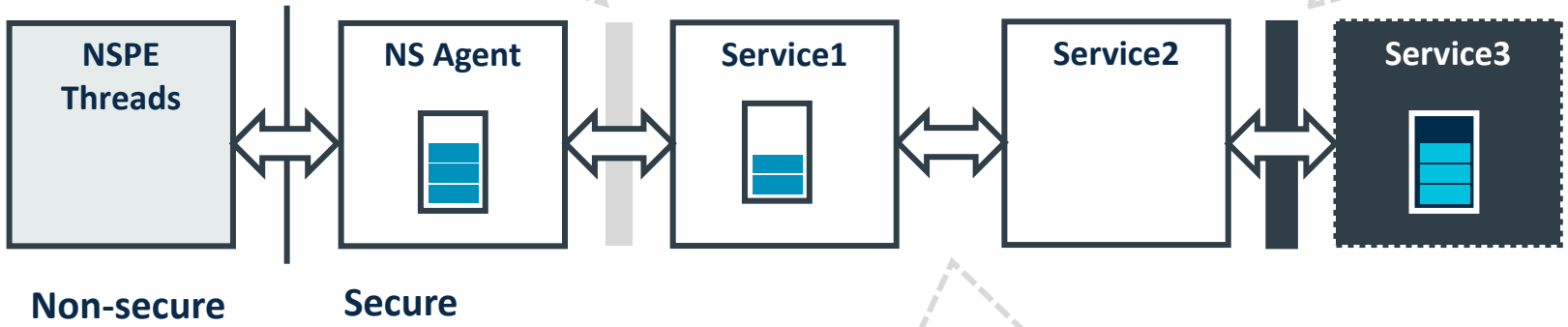
Still want to remove the reset 'Handler' execution? Check Secure Function Model.

arm

Secure Functions

service1() { return CALL_WITH_SP(psa_call, sp1); }

service1() { return SVCALL_WITH_SP(psa_call, sp3); }

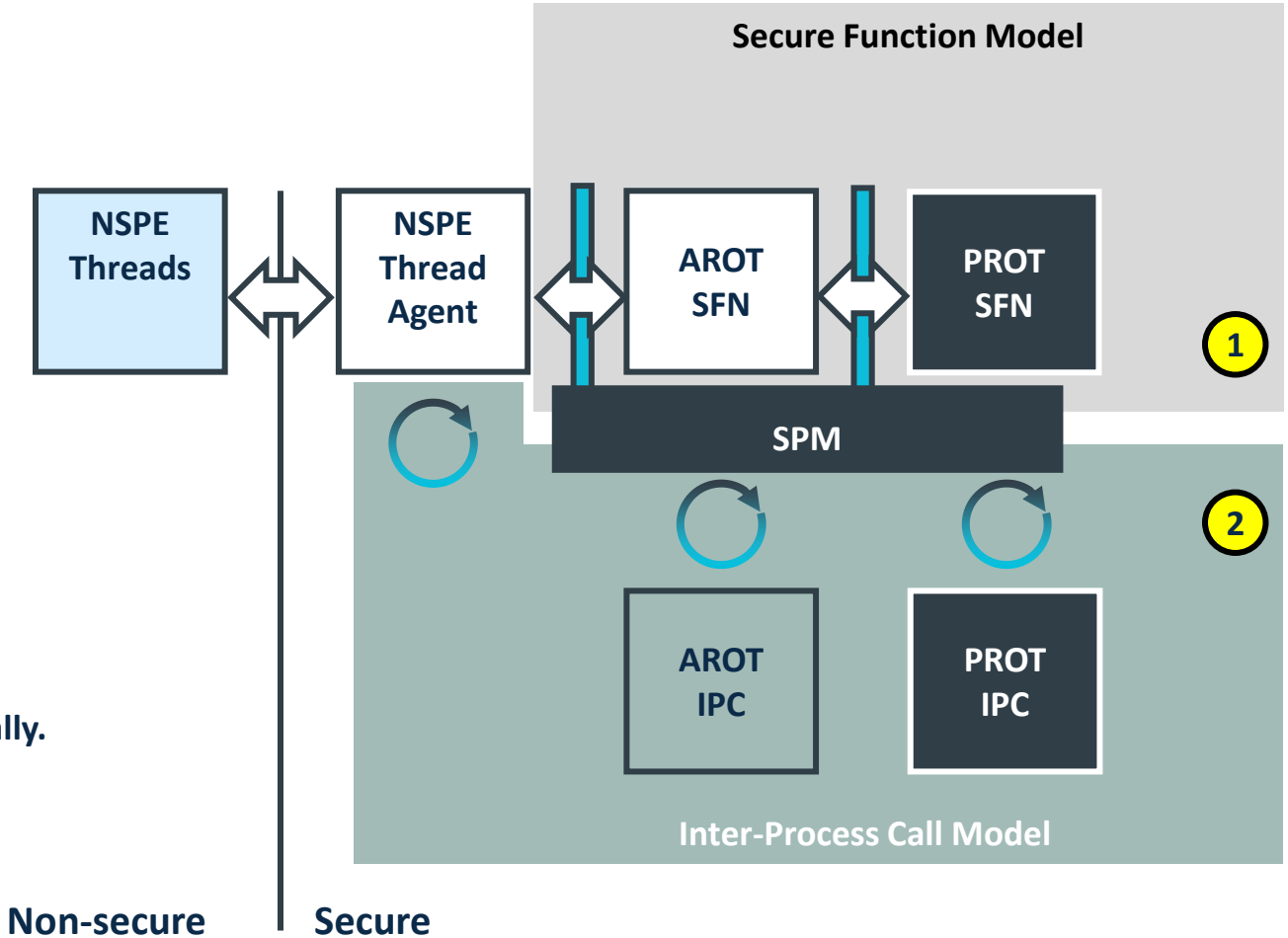


service2() { /* Use caller stack. */ }

Stack

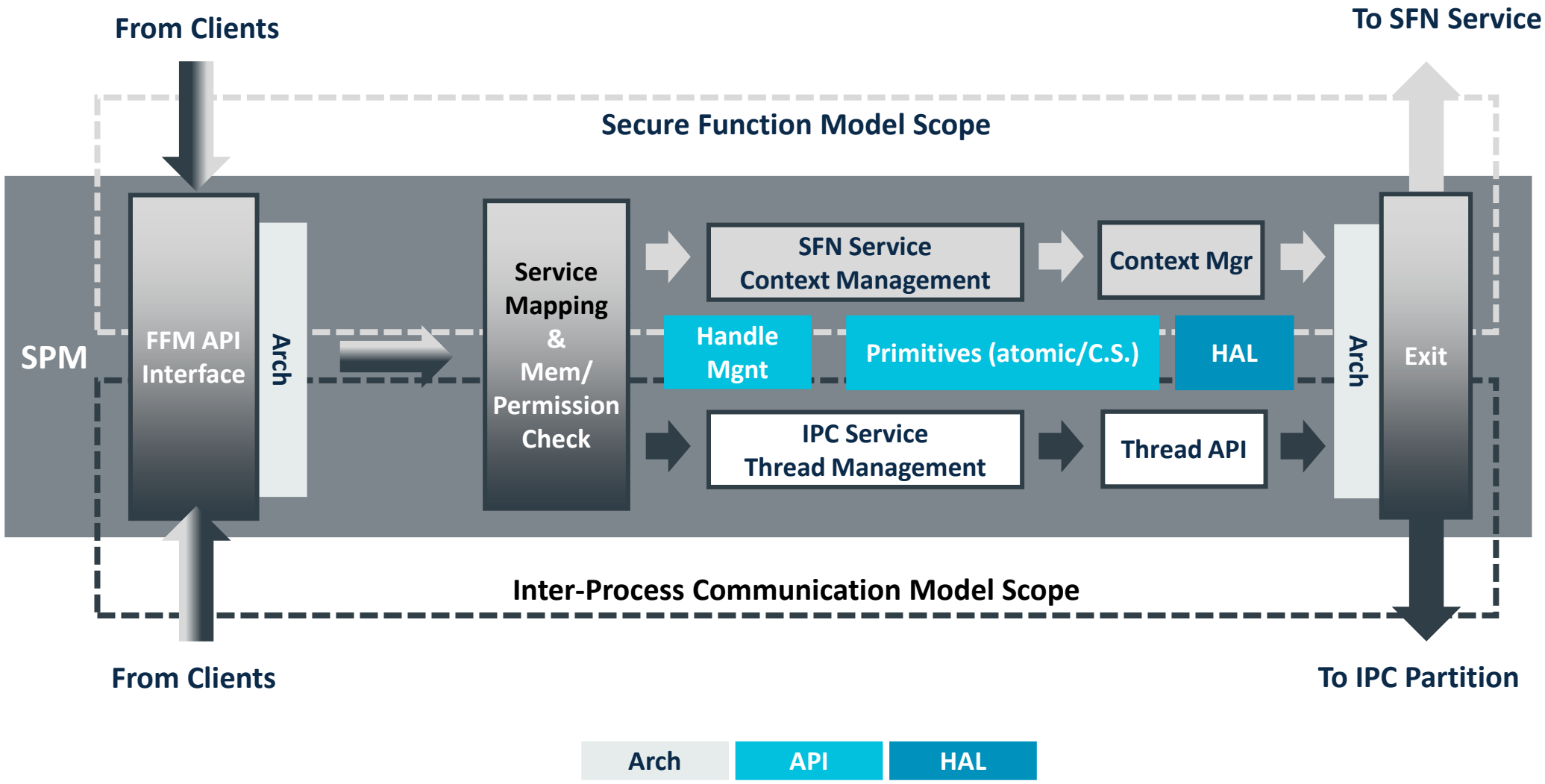
arm

Design Goal

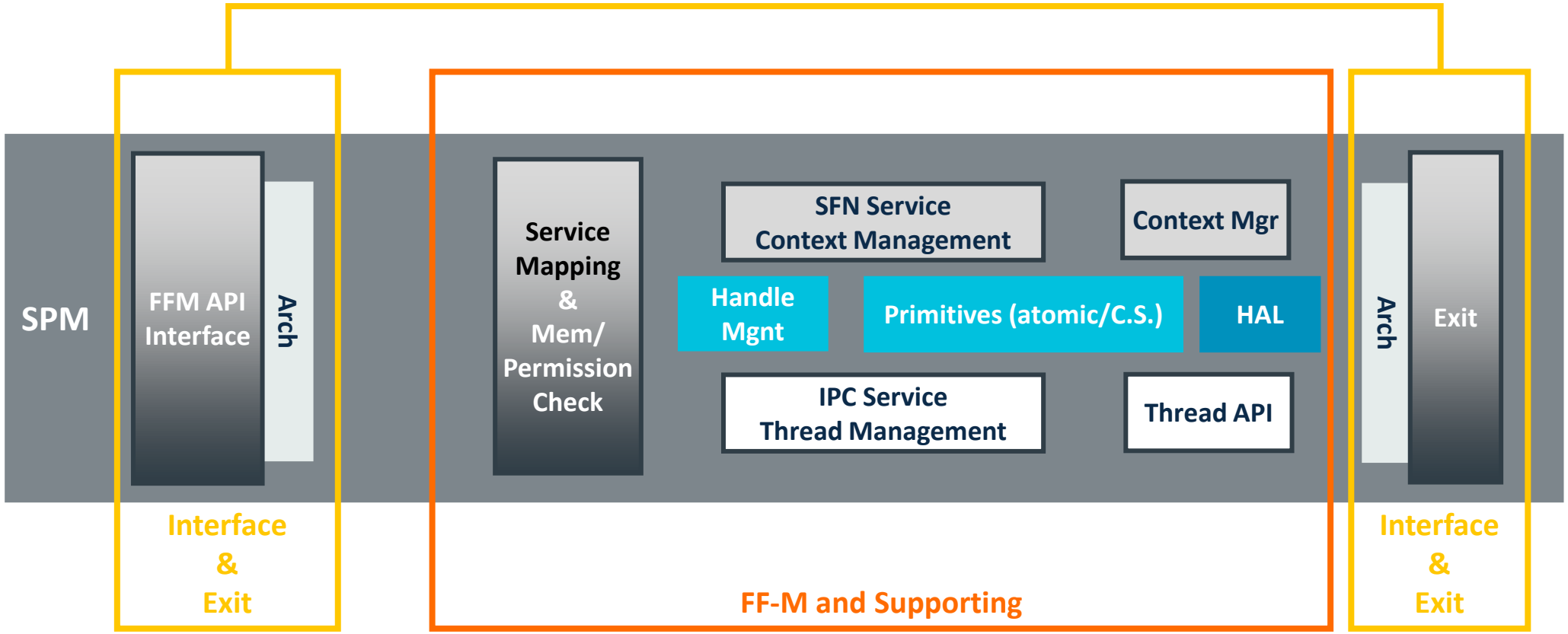


1 and 2 can be provided by the implementation individually.

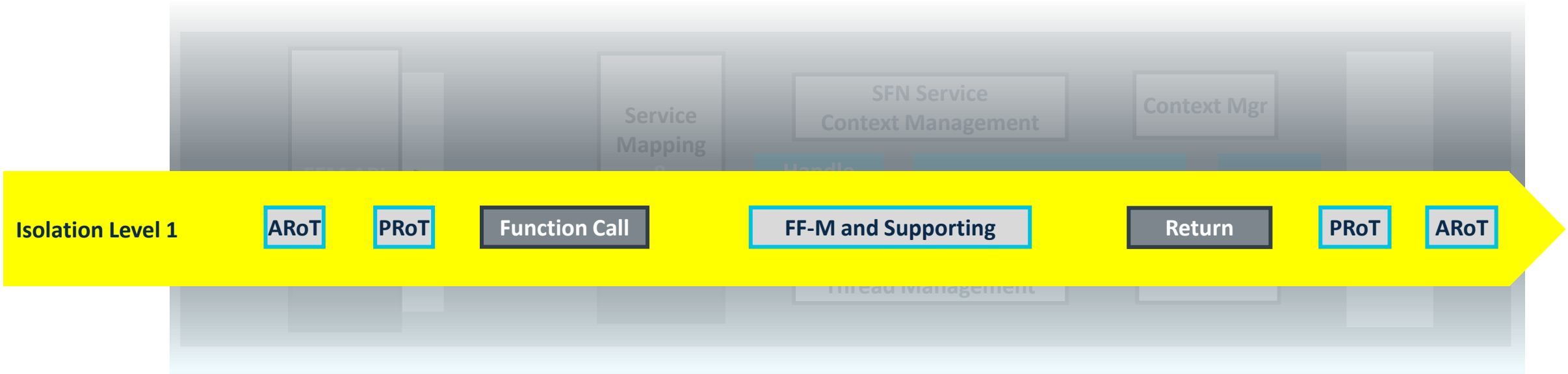
SPM Internal Modules – Call Routine



SPM Internal Modules – Software Modulization

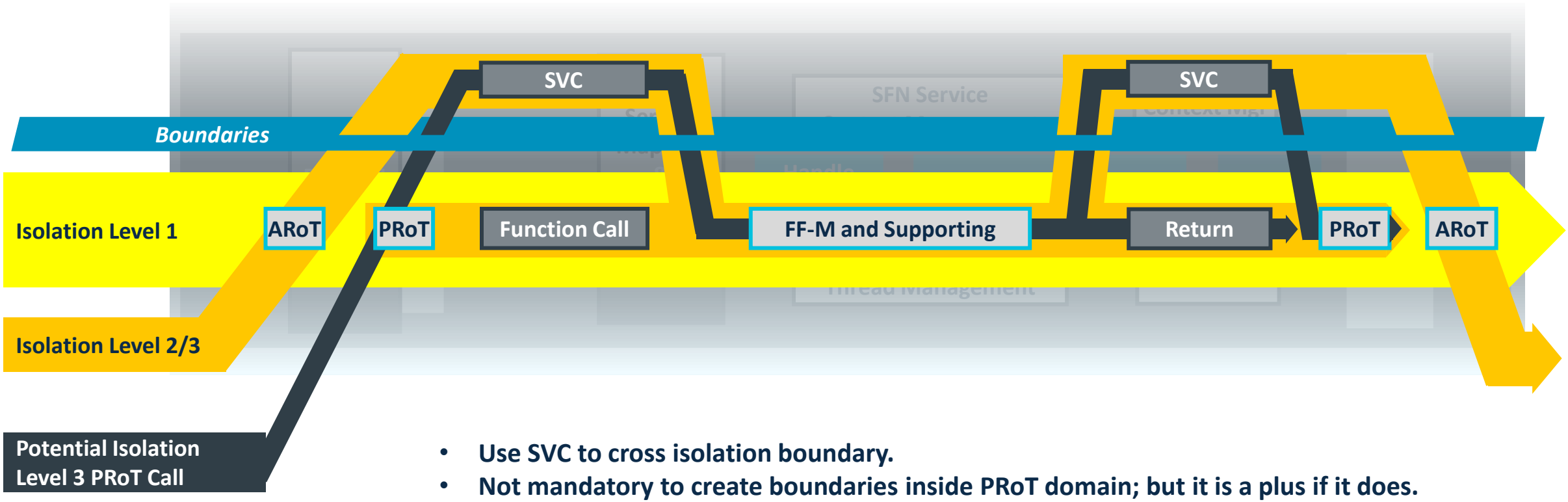


SPM Internal Modules – Simplest Case



- There is no secure boundaries under Isolation Level 1, so all plain function call is possible.
- This is for SFN model. IPC model scheduling needs to deal with interrupt cases, which means PendSV can't be avoided.

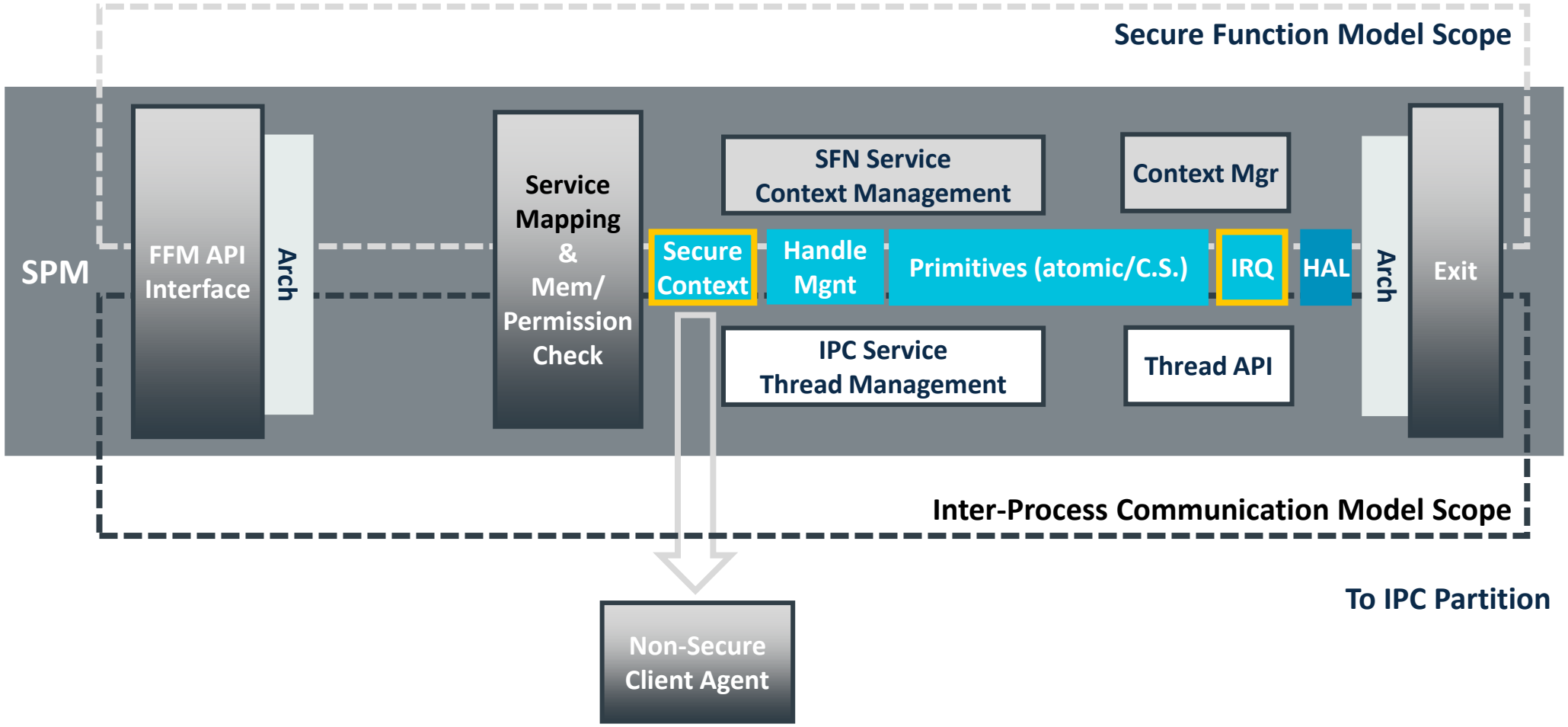
SPM Internal Modules – Interfaces



- Use SVC to cross isolation boundary.
- Not mandatory to create boundaries inside PRoT domain; but it is a plus if it does.

arm

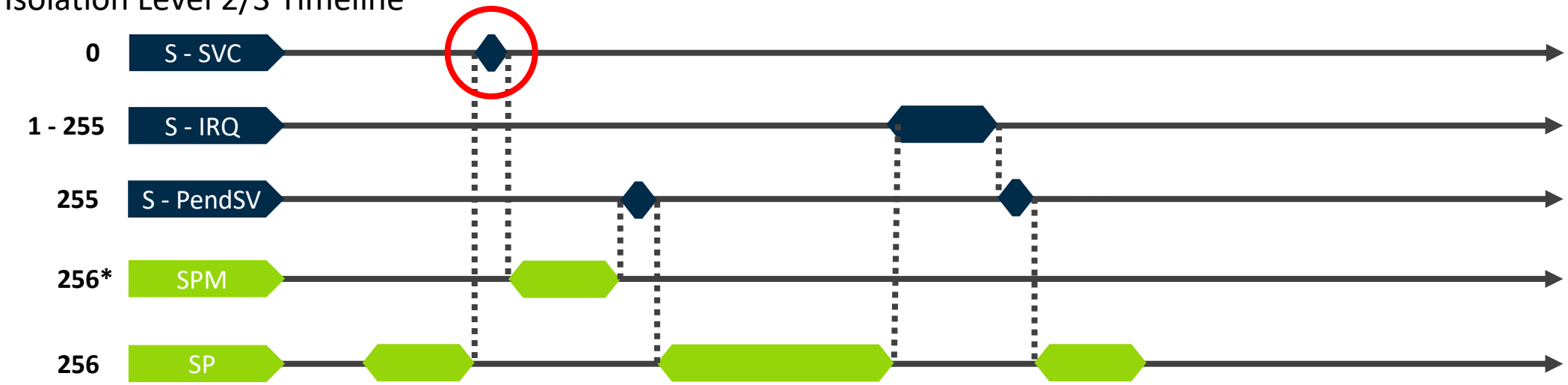
SPM Internal Modules – Extra Components



IPC Isolation Levels – Theoretic Timeline

Isolation Level 1 Timeline

Isolation Level 2/3 Timeline

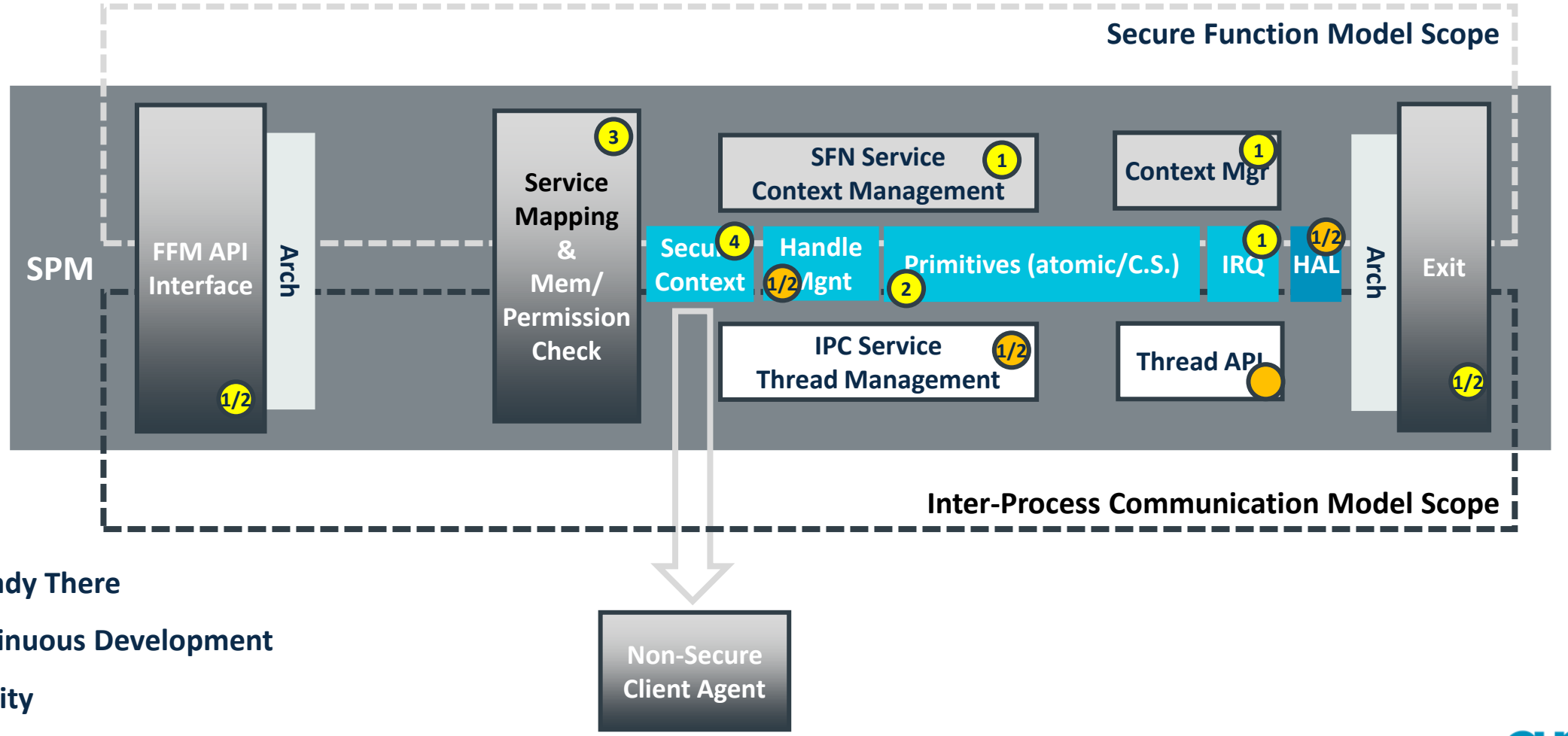


IPC vs SFN Theoretic Timeline

IPC Isolation Level 1

SFN Isolation Level 1

SPM Update – The Path



arm

Thank You
Danke
Gracias
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה