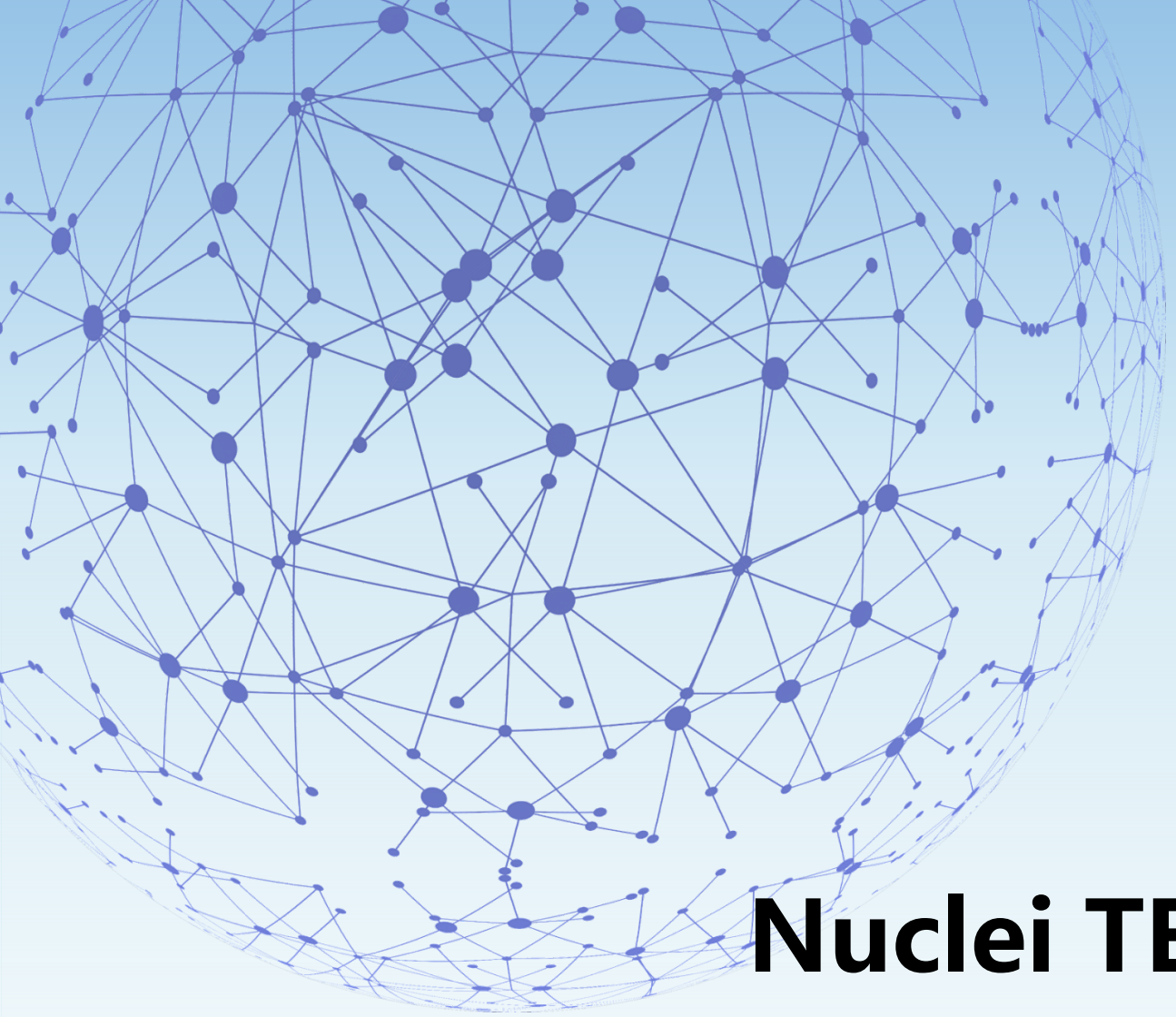


芯来科技 NUCLEI

Nuclei TEE: RISC-V 安全系统实践

桂兵 芯来科技

芯来科技简介

芯来科技
NUCLEI

- 芯来科技成立于2018年，是中国大陆本土专业的**RISC-V IP、子系统IP及SoC解决方案**提供商，赋能下游各类应用场景

5G通信　工业控制
AI　汽车电子
物联网　存储
MCU　网络安全

- 总部位于**上海**，在**华北、华东、华中及华南**均能够提供本地技术支持

- 从0到1自主研发**全系列RISC-V CPU IP**，拥有一流的特性和优势

丰富的可配置性
稳健的编码格式
完整的信息安全方案
良好的扩展性
健全的功能安全方案
灵活的商业模式及技术支持

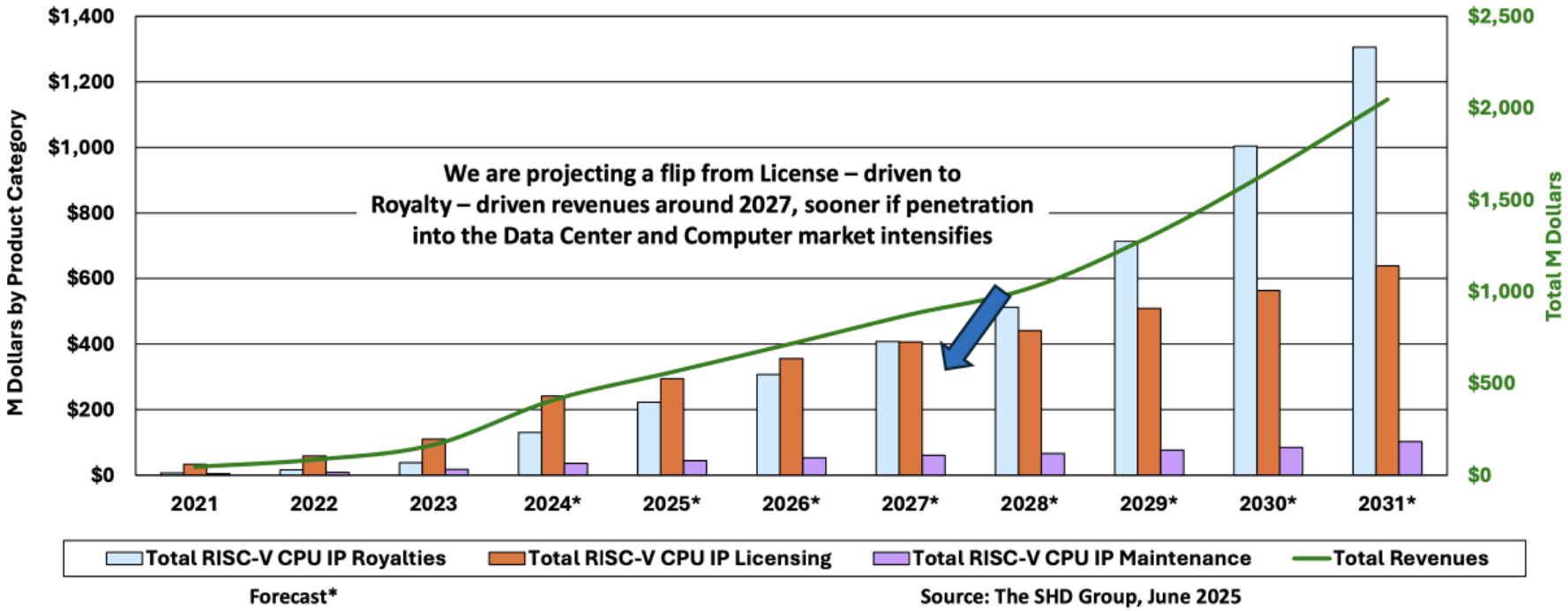
- **累计出货量达数亿颗**,是国内本土RISC-V IP领军企业

>300家正式授权客户

芯来科技，从本土创业，从零开始，跻身行业第一梯队

芯来科技 NUCLEI

RISC-V IP Market Will Continue Accelerating



RISC-V IP Market Leaders (alphabetical order)

- Andes – Worldwide market share leader based on current estimates
- Codasip
- DIY (home-grown RISC-V)
- MIPS
- Nuclei Systems -– **China Market Share Leader based on current estimates**
- SiFive

Newer entrants into RISC-V IP (alphabetical order)

- Akeana
- Condor Computing
- Synopsys
- Tenstorrent
- Ventana

the SHDgroup

中国地区Market Share Leader

芯来科技RISC-V处理器IP产品图

芯来科技 NUCLEI

通用处理器产品线

N 级别
32位架构
MCU, AIoT, 安全

U 级别
32位架构+MMU
Linux, 边缘计算

NX 级别
64位架构
存储, AR/VR

UX 级别
64位架构+MMU
Linux, 数据中心, 网络

专用处理器产品线

NS 级别
高安全性场景, 金融支付
SIM卡，物联网安全

NA 级别
ISO26262功能安全
汽车电子

NI 级别
人工智能，自动驾驶
通信计算，视频处理

1000 系列 Out-of-Order 3/4/6-Wide Decode				UX1000 (SMP)		NA1000	NI1000
900 系列 9-Stage Pipeline Dual-Issue	N900 (SMP)	U900 (SMP)	NX900 (SMP)	UX900 (SMP)		NA900	NI900
600 系列 6-Stage Pipeline Single-Issue	N600 (SMP)	U600 (SMP)	NX600 (SMP)	UX600 (SMP)	NS600		
300 系列 3-Stage Pipeline Single/Dual-Issue	N300				NS300	NA300	
200 系列 2-Stage Pipeline Single-Issue	N200						
100 系列 2-Stage Pipeline Single-Issue	N100				NS100		

提纲

芯来科技
NUCLEI

- TEE 背景介绍
- Nuclei AP OP-TEE 方案
- Nuclei MCU TEE 方案
- Demo 展示

TEE 背景介绍

芯来科技 NUCLEI

TEE(Trusted Execution Environment):

2006 OMTP双系统安全解决方案 → 2008 ARM TrustZone → 2010 GP 制定TEE规范标准

现有**TEE**情况:

CPU 架构	支持TEE的硬件	支持TEE的软件
ARM	TrustZone	QTEE/TEEgris/ITrustee/ Trustonic/OP-TEE/TF-M
RISC-V	PMP，Worldguard，IOPMP，SMMTT	Keystone/PengLai/ MutilZone

TEE 背景介绍

芯来科技 NUCLEI

ARM Cortex-A Trustzone

- Processor Architecture
  - Monitor Mode
- System Architecture
  - AXI/AXI2AHB/AXI2APB
- Debug Architecture
  - Secure privileged/user invasive (JTAG)/non-invasive(Trace) debug
- Hardware Lib
  - TZASC/TZPC/GIC

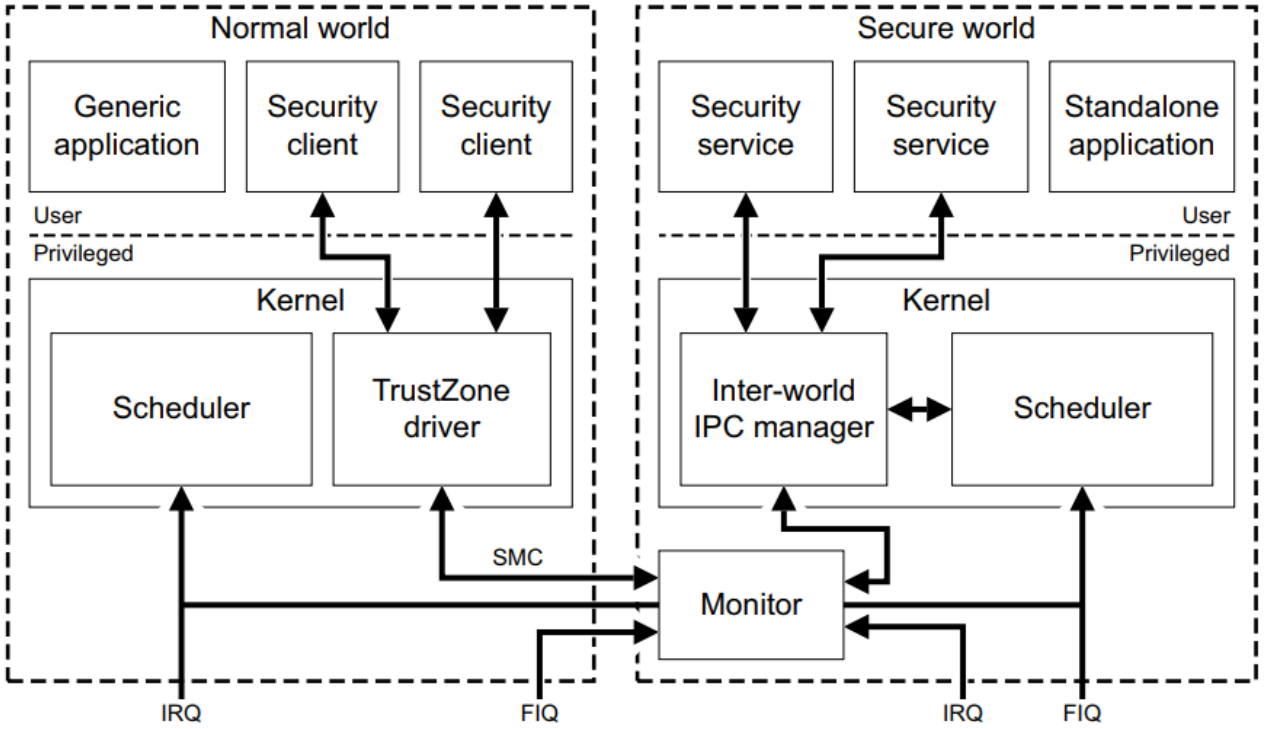


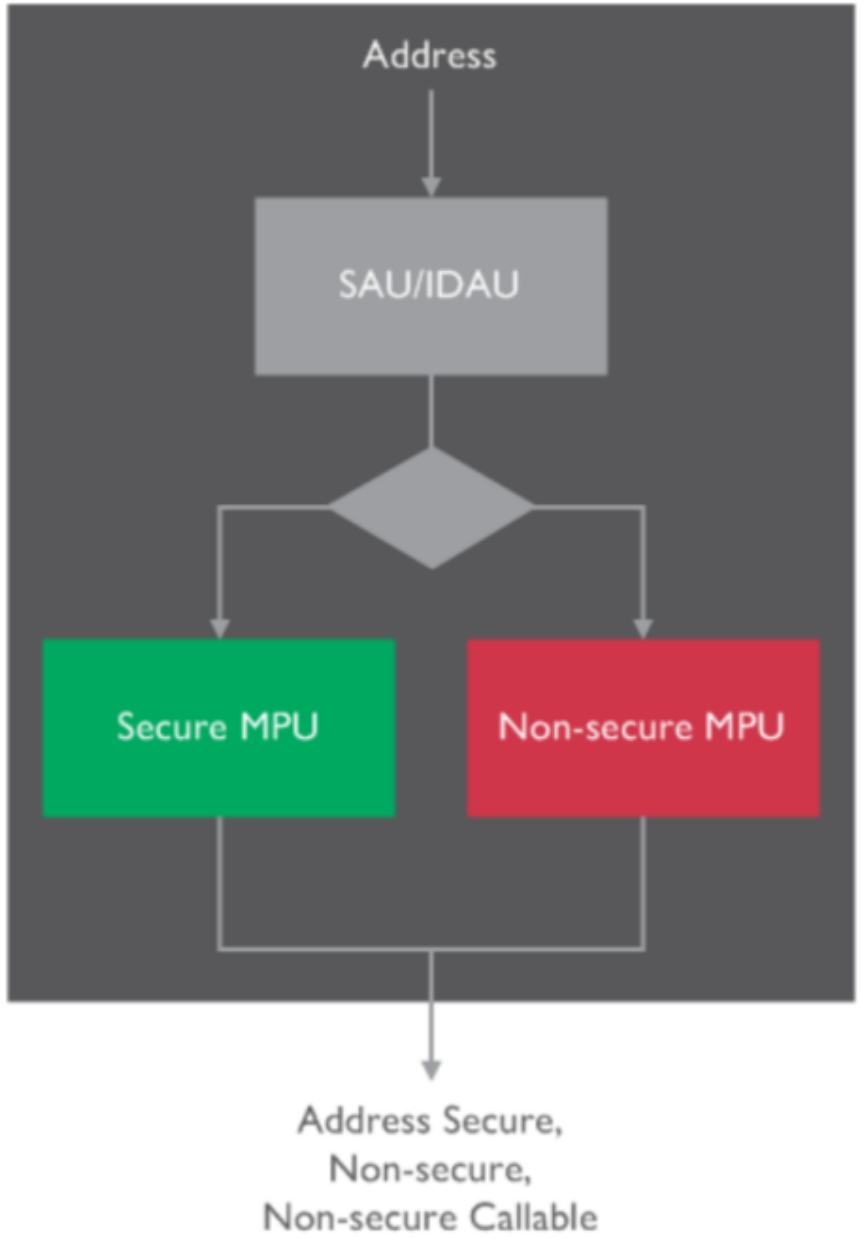
Figure 5-1 : A possible architecture with an independent Secure world OS

TEE 背景介绍

芯来科技

ARM Cortex-M Trustzone

- memory partition
  - SAU/IDAU configure S/NSC/NS memory region
  - secure MPU/non-secure MPU（optional）

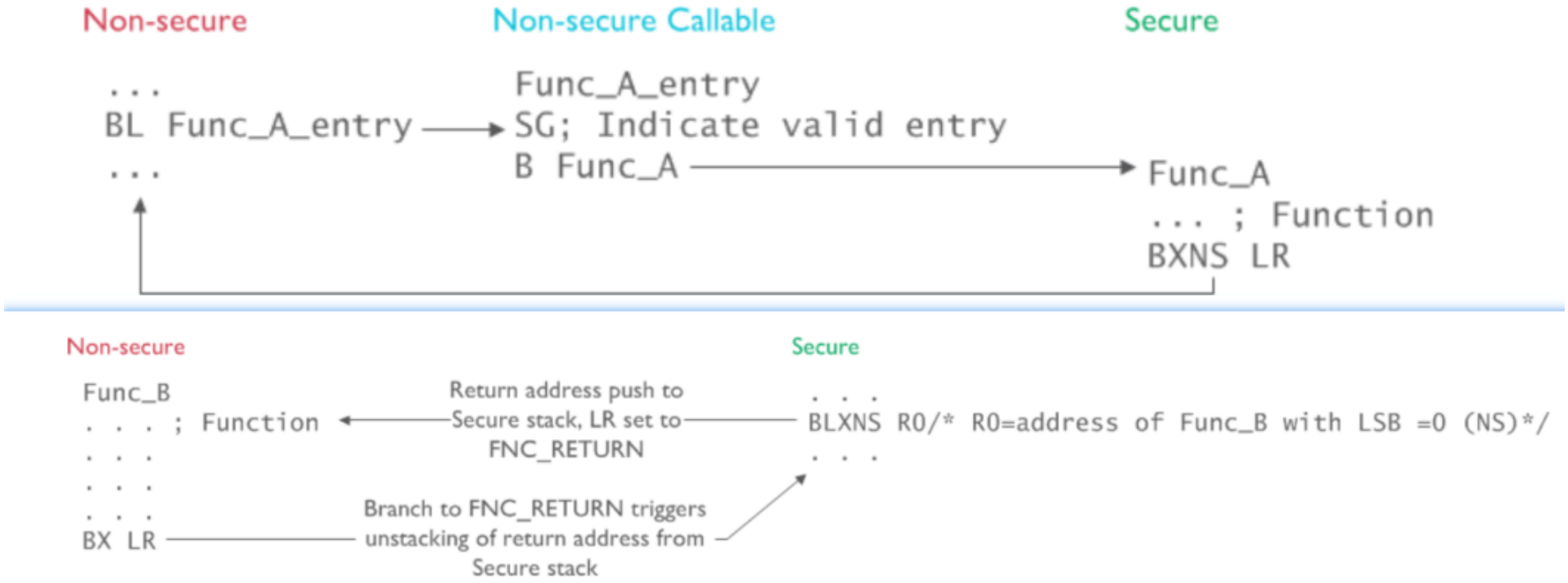


TEE 背景介绍

芯来科技 NUCLEI

ARM Cortex-M Trustzone

- State transitions
  - the system starts up in Secure state
  - function call across secure state： SG/BXNS/BLXNS



TEE 背景介绍

芯来科技 NUCLEI

RISC-V Security Mechanisms

- Privilege Levels(M/H/S/U)
- Physical Memory Protection (PMP)

- RISC-V ISA related
  - SMMTT
  - WorldGuard

- RISC-V Non-ISA related
  - AP-TEE
  - IOPMP

Nuclei TEE 介绍

芯来科技
NUCLEI

Nuclei AP TEE 硬件（UX900系列）

- M/S/U
- MMU
- PMP
- Nuclei 增强的PLIC

Nuclei MCU TEE 硬件（N300系列）

- M/S
- PMP
- Nuclei ECLIC

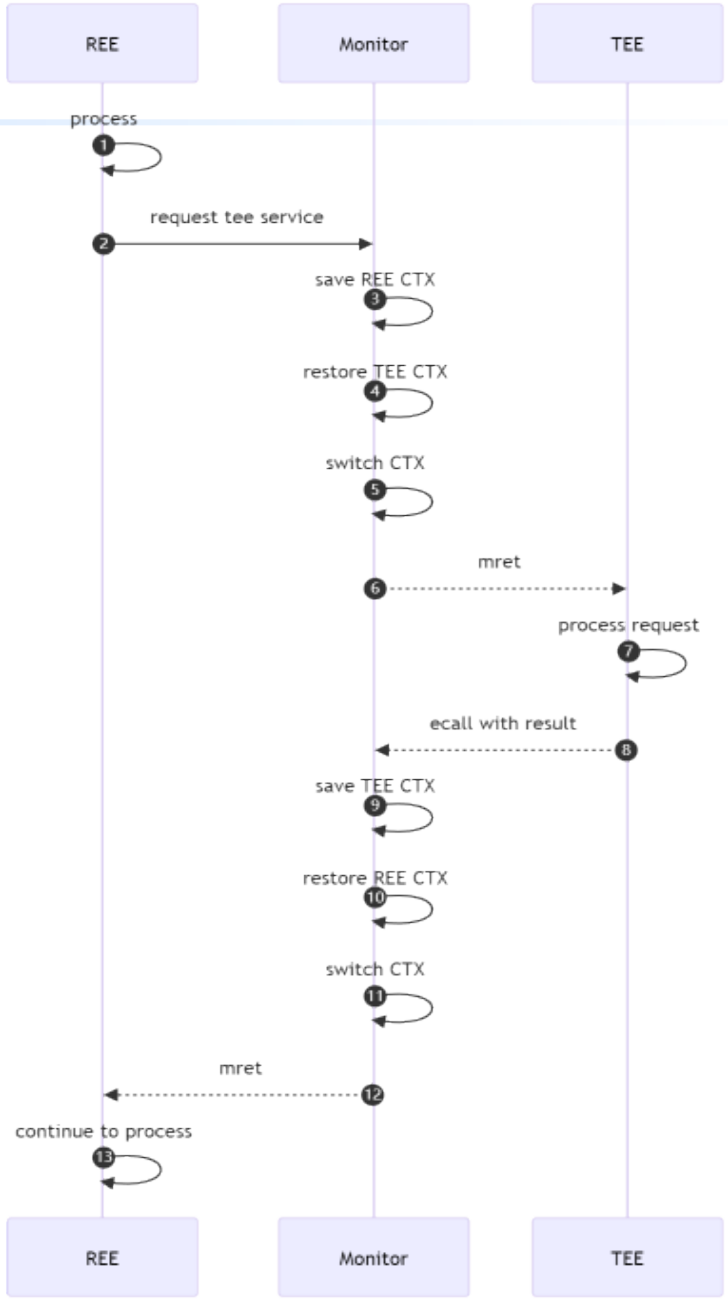
Nuclei AP OP-TEE 方案

芯来科技 NUCLEI

架构图及流程

- HW：M/S/U特权模式，PMP，PLIC
- SW：
  - Monitor[M]：管理安全状态上下文，负责处理REE的请求，TEE的执行结果处理，PMP内存划分，中断配置。
  - REE-OS/TEE-OS[S]: 操作系统
  - CA/TA[U]：用户程序

Client APP[U]	Trusted APP[U]
Linux[S]	OP-TEE[S]
Monitor[M] Hart CTX Manage/PMP memory Manage	



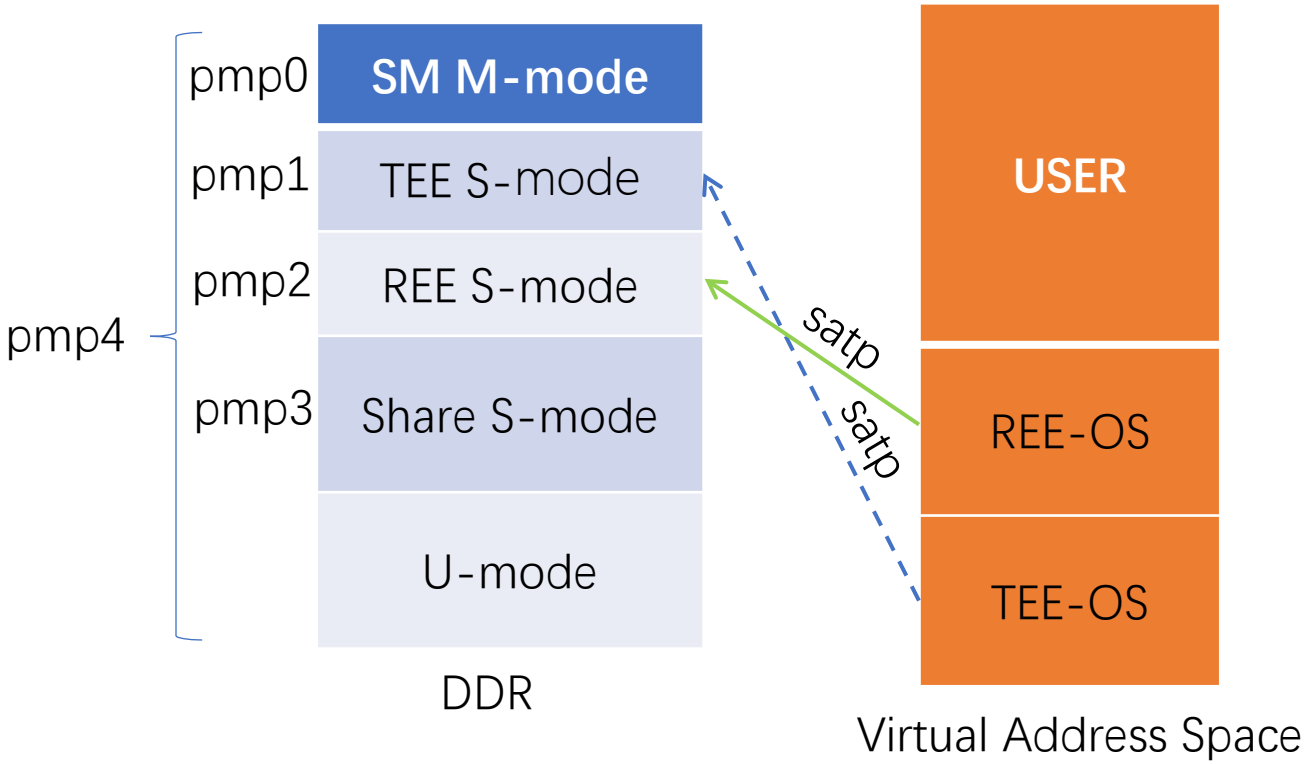
Nuclei AP OP-TEE 方案

芯来科技 NUCLEI

隔离机制-内存隔离，CPU安全状态隔离

- PMP实现内存隔离：区分安全系统与非安全系统的内存地址空间
- M模式Monitor：管理CPU安全状态上下文，负责CPU安全状态上下文切换，执行地址空间切换
- PMP配置以编号小的优先级高

- 结合Nuclei Secure特性，CPU安全状态有硬件支持，BUS/Cache/TLB也区分硬件安全状态



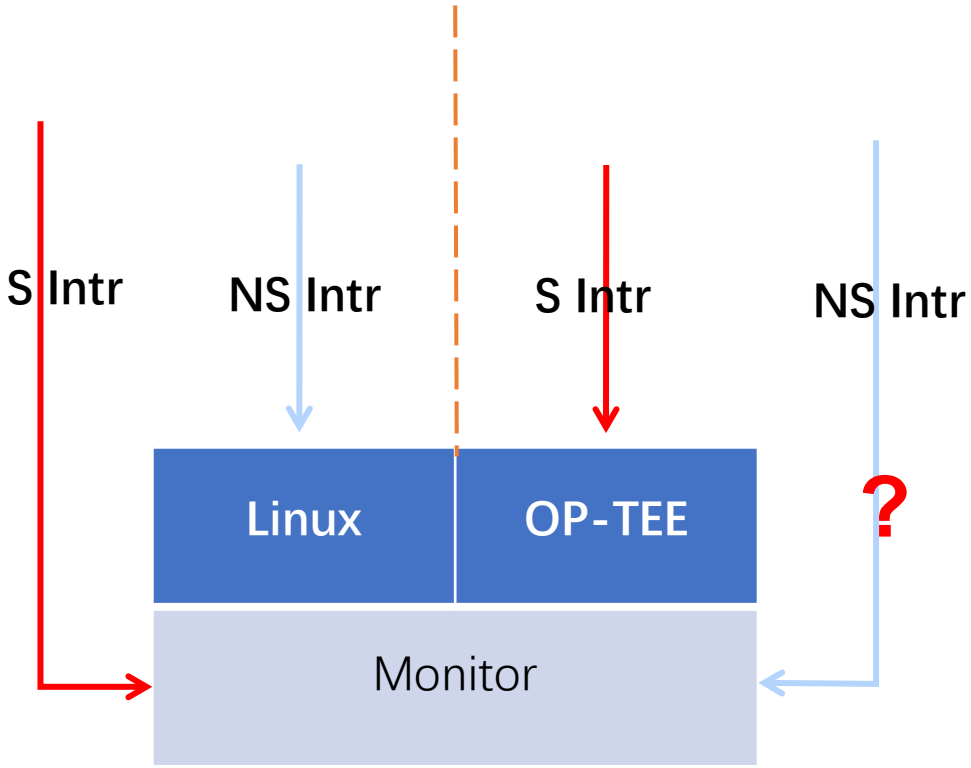
Nuclei AP OP-TEE 方案

芯来科技 NUCLEI

隔离机制-中断隔离

- 代理所有中断到S模式
- 对PLIC 中断使能模式分类：
  - M模式使能的中断：非本世界处理
  - S模式使能的中断：本世界处理
- Monitor 管理中断使能模式，比如进入非安全世界前，设置安全外设中断到M模式使能，非安全外设中断到S模式使能
- 为避免竞态，规定进入安全世界后，不响应非安全世界中断，但安全中断能打断非安全世界执行

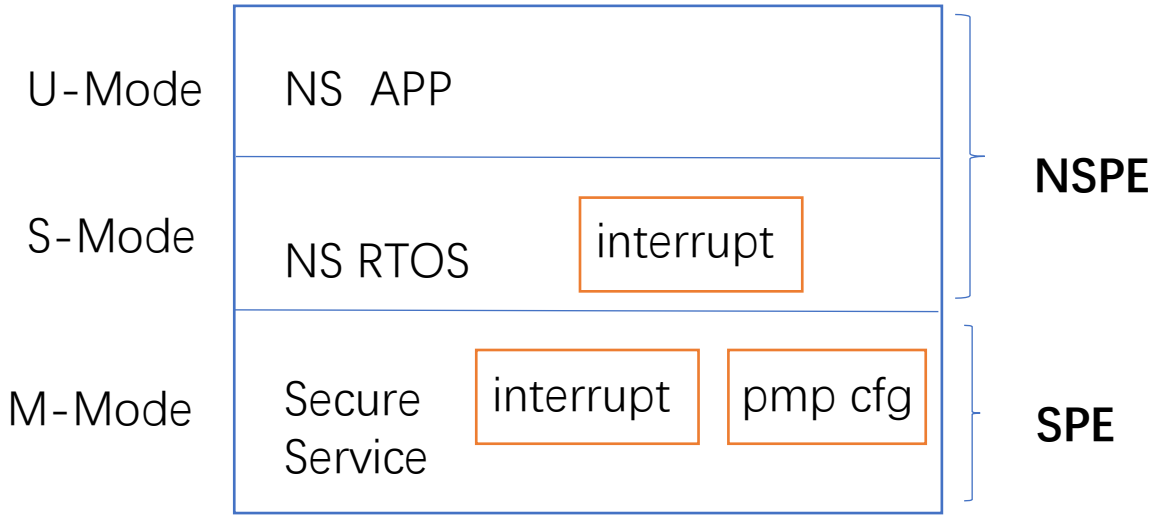
- Nuclei PLIC硬件处理
  - M模式使能的中断，S模式不能修改中断相关寄存器
  - CPU在M模式下可修改PLIC 中断pending



Nuclei MCU TEE 方案

芯来科技 NUCLEI

- **内存隔离**
  - PMP 划分出安全世界与非安全世界的地址空间
- **cpu安全状态隔离**
  - M-mode 是安全世界，提供安全服务，处理安全中断
  - S-mode 为非安全世界，处理非安全中断
  - U-mode 为非安全应用
  - 只实现了SPE与NSPE的隔离，SPE内部暂时没有硬件隔离



Based on Trusted Firmware-M (TF-M)

Nuclei MCU TEE 方案

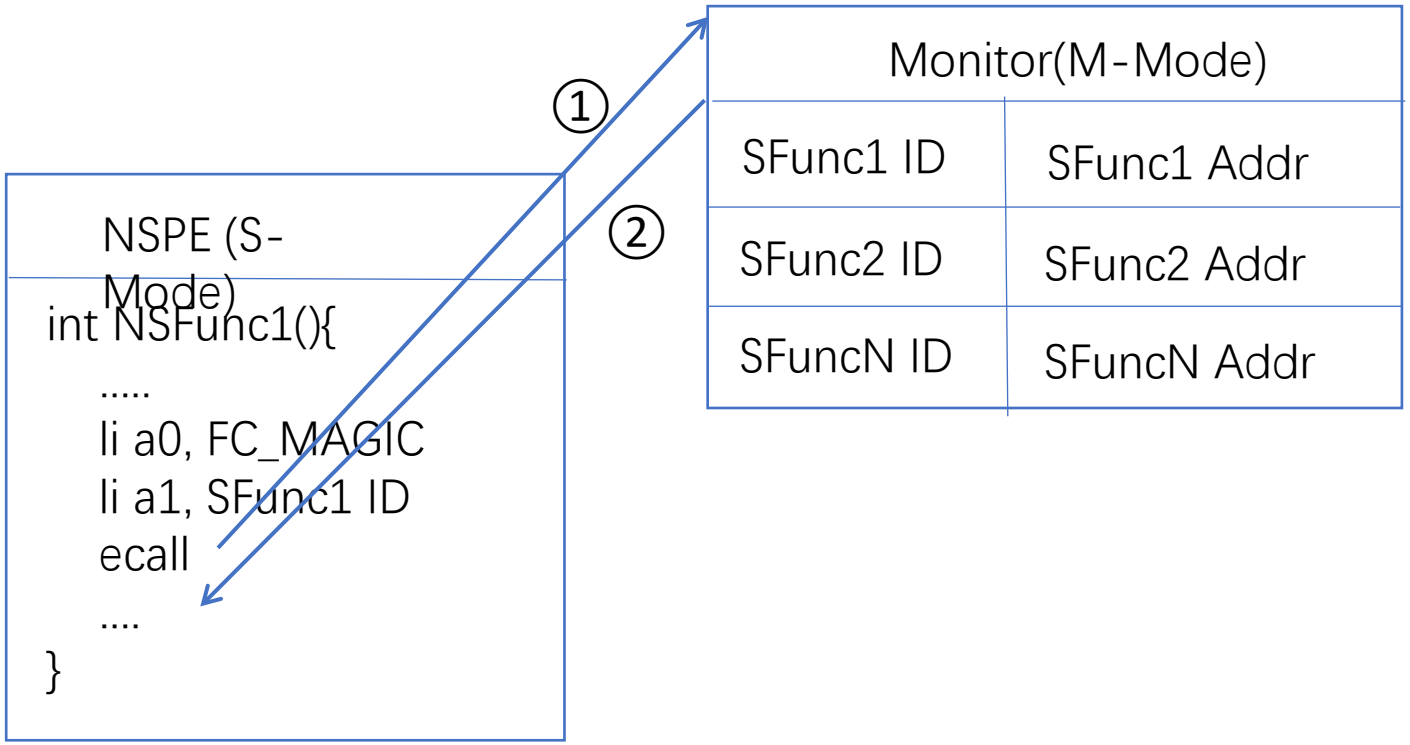
芯来科技 NUCLEI

- **中断隔离**
  - 非安全中断，设置为S模式使能，在非安全世界处理
  - 安全中断， 设置为M模式使能，在安全世界处理
  - M模式SPE，间接响应非安全中断(M模式执行安全服务时，mtimer超时则切换到S模式，处理可能的pending中断)
  - S模式NSPE，响应安全中断

Nuclei MCU TEE 方案

芯来科技 NUCLEI

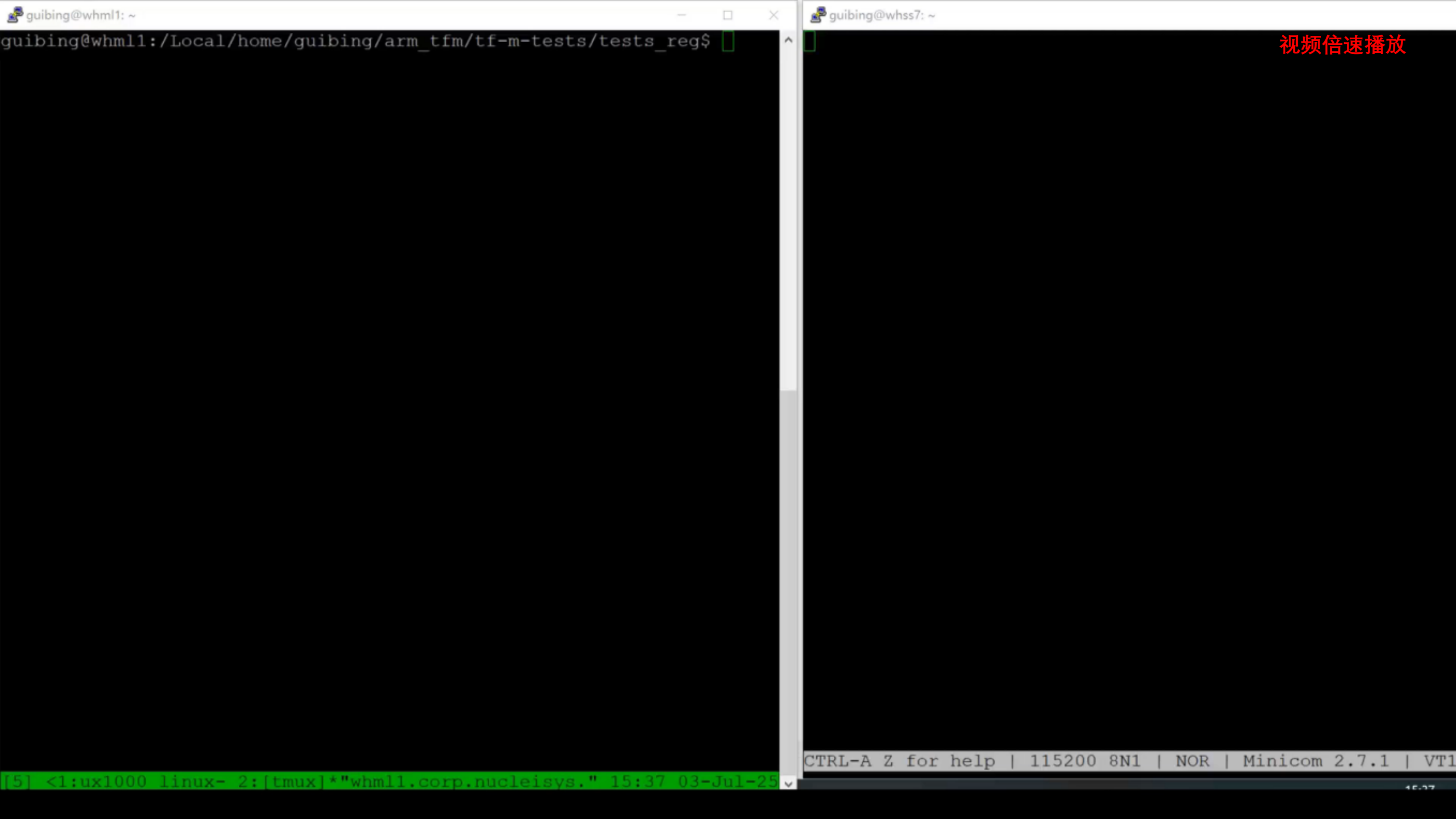
- **函数调用**
  - M模式SPE的API导出给S模式NSPE使用
  - M模式检查FunctionID 并执行对应的功能，对于无效ID则返回S模式ERROR



Nuclei TEE方案比较

芯来科技
NUCLEI

	Nuclei OP-TEE方案	Nuclei TEE方案
CPU安全状态隔离	M模式：安全状态 S模式：安全状态，也有非安全状态，具体由M模式控制	M模式：安全状态 S模式：非安全状态
内存隔离	PMP	PMP
中断隔离	增强的PLIC中断控制器	ECLIC中断控制器


guibing@whml1: ~
guibing@whml1:/Local/home/guibing/arm_tfm/tf-m-tests/tests_reg$
[5] <1:ux1000 linux- 2:[tmux]*"whml1.corp.nucleisys." 15:37 03-Jul-25
guibing@whss7: ~
视频倍速播放
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT1

芯来科技
NUCLEI

芯来科技公众号

芯来科技业务联络

欢迎大家来芯来展台-C18！　谢谢您！