<セッション4(16:55～17:35)>

OpenFogリファレンス・アーキテクチャ解説(詳細編)
OpenFog Reference Architecture (Part-2)

Security

高浦 則克 (Norikatsu Takaura)
OpenFog コンソーシアム 日本地区委員会
OpenFog Consortium Japan Regional Committee

株式会社 日立製作所
norikatsu.takaura.nd@hitachi.com

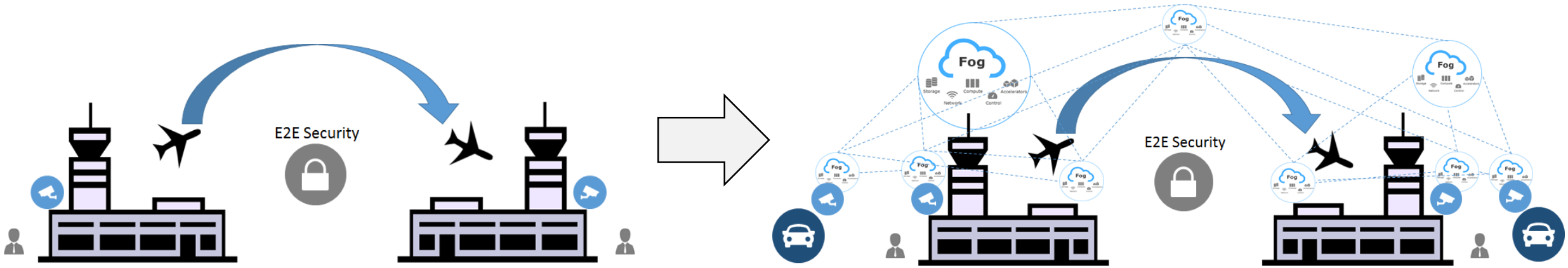
Index

1. Introduction

Applications where Fog security is required

(1) Autonomous driving in a situation where cloud communication is interrupted,
(2) Aset sharing in smart factory, (3) DDos attack against millions of sensors,
(4) Network drone cameras, (5) Power smart grid with overload,
(6) Smart car and traffic control system.

(7) End-to-end airport visual security



Before

After

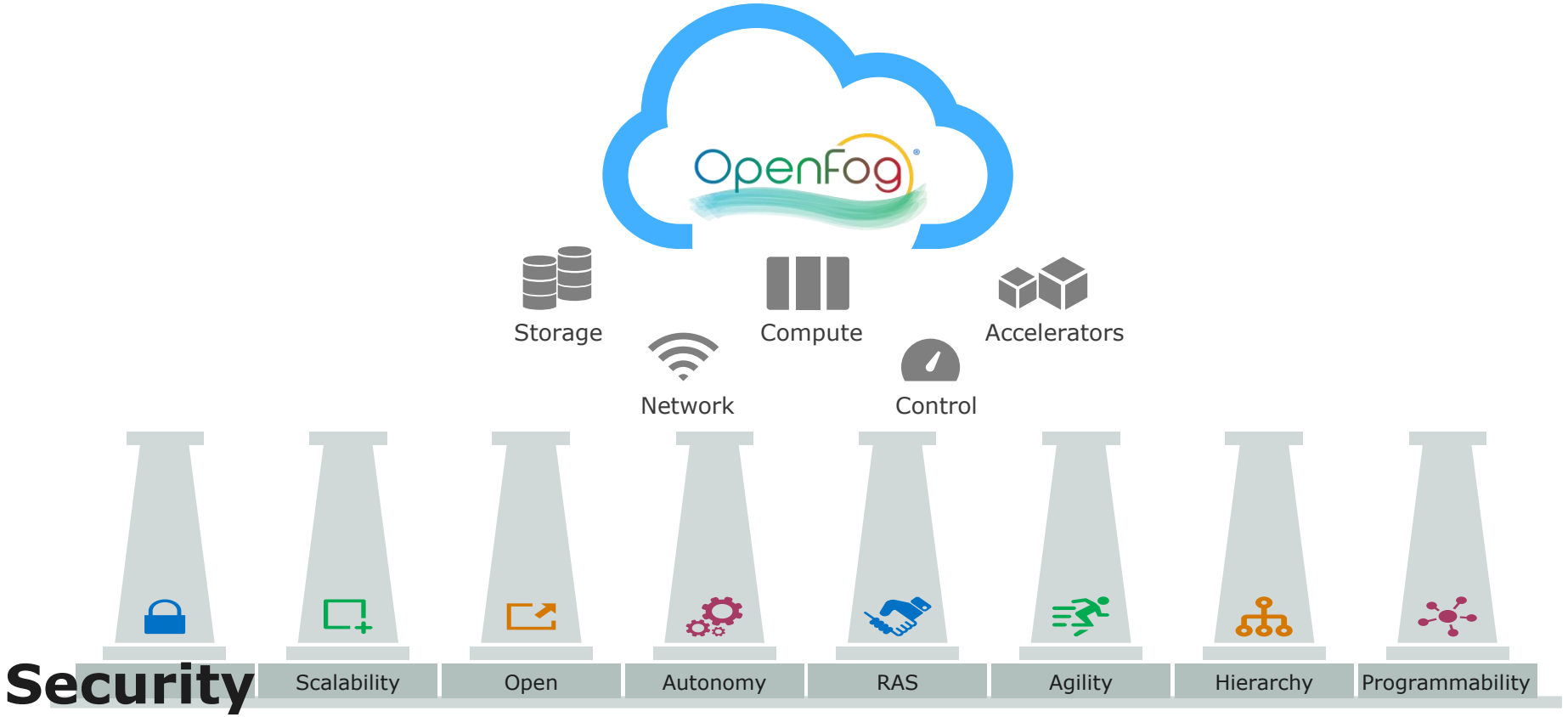
1.1 Threads and Assets in intended Use/ Location

Threat Categories / Intents / Attack Venues	Confidentiality Violation	Integrity Violation	Authentication Violation	Availability Violation	Privacy Violation
	Leaking information through overt/covert channels	Modifying data/code without proper authorization	Masquerading one entity as another entity	Rendering resources unreach-able/unavail-able	Leaking sensitive information of an entity (incl. identity)
Insider Attacks	Data Leaks	Data Alteration	Identity/Password/Key Leaks	Equipment Sabotage	Data/Identity Leaks
Hardware Attacks	Hardware Trojans, Side Channel Attacks	Hardware Trojans	Hardware Trojans	Radio Jamming, Bandwidth Exhaustion	Hardware Trojans, Side Channel Attacks
Software Attacks	Malware	Malware	Malware	DoS/DDoS, Resource Depletion	Malware, Social Network Analyses
Network Based Attacks	Eavesdropping	Message/Transaction Replay	Spoofing, Man-in-Middle Attacks	DoS/DDoS, Subnet Flooding	Traffic Pattern Analyses

Assets may include:

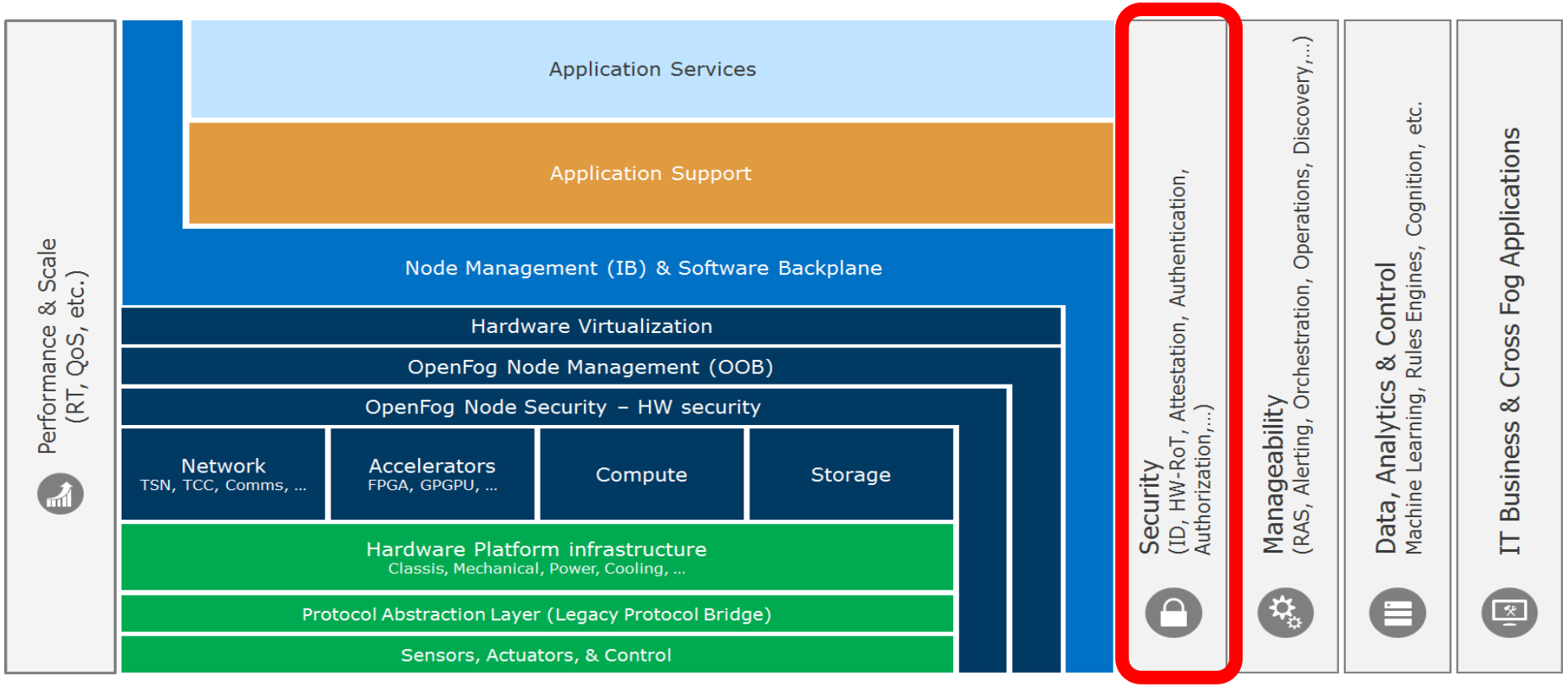
- Information Technology
- Infrastructure
- Critical infrastructure
- Intellectual property
- Financial data
- Service availability
- Productivity
- Sensitive information
- Personal information

2. Security Pillar



- **Trustworthy** fog depends on using **trusted** elements.
- **Attestation** is the ability to provide some evidence to a third-party verifier.
- **Privacy** attributes of the data must be allowed to be specified by users.

3. Reference Architecture



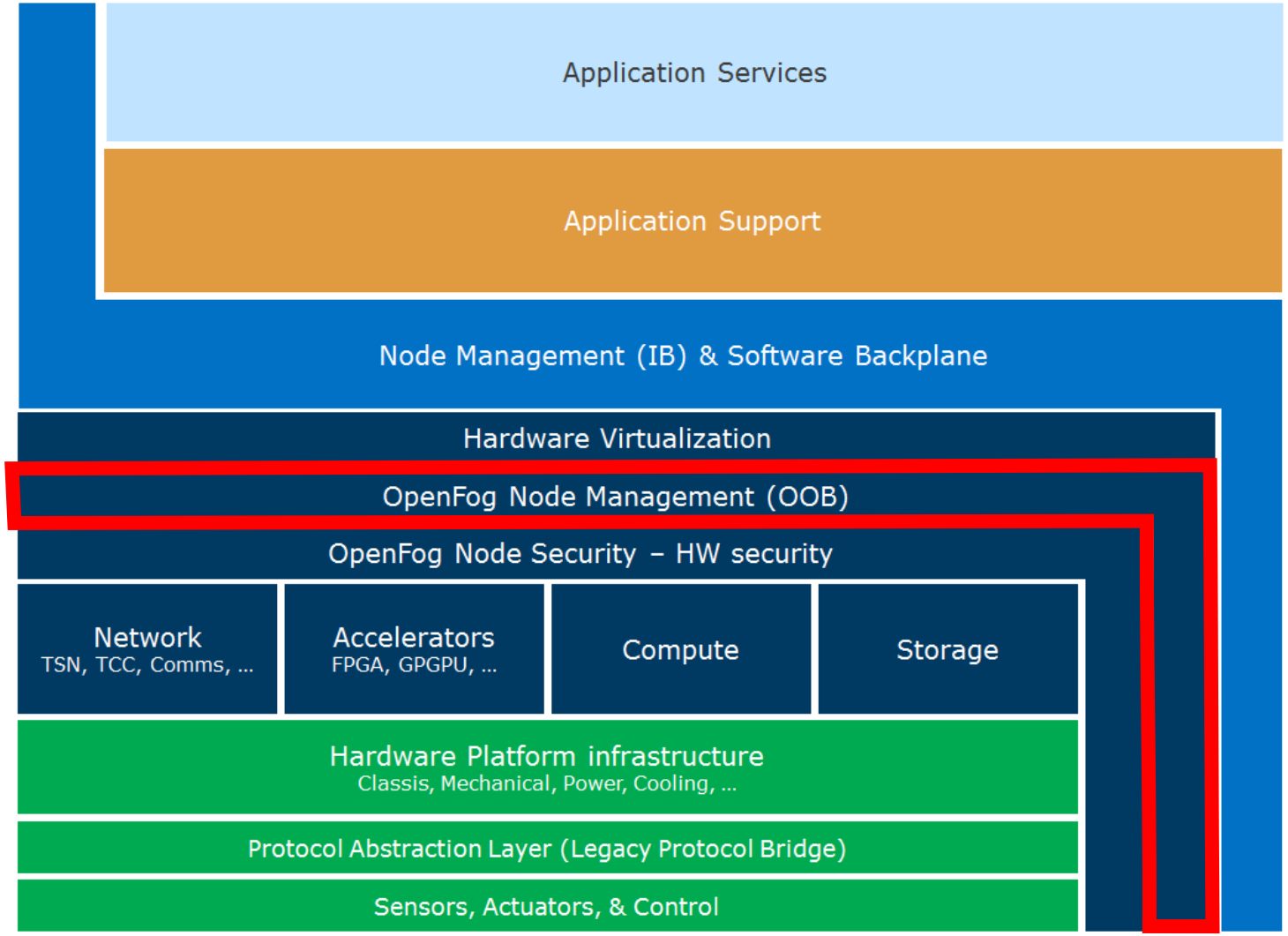
One Aspect of Security Perspective

Fog must be able to identify itself to other entities within the network.

It enables to attest to credentials of a given system while preserving privacy.

3.1 OpenFog Node View

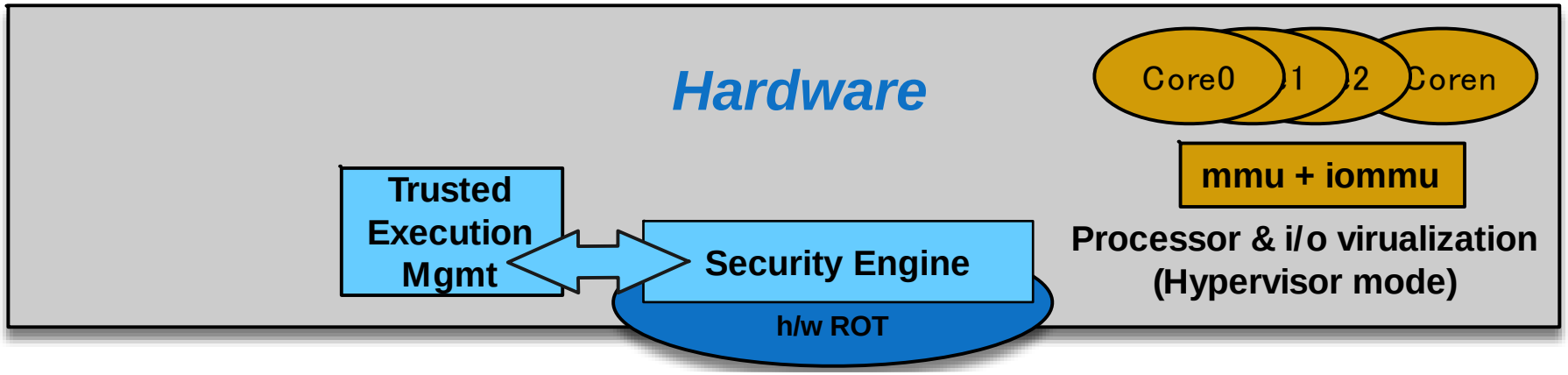
A node can act as a security gateway for sensors, etc. If it is not secure, no amount of network security or encryption will make it secure



4. Deeper Node Security Aspect

Hardware Root-of-Trust

- Starts with a Trusted hardware component receiving control at power-on.
- Uses h/w-based virtualization as a security mechanism.
- Security Engine instantiates a Trusted Execution Environment(TEE).

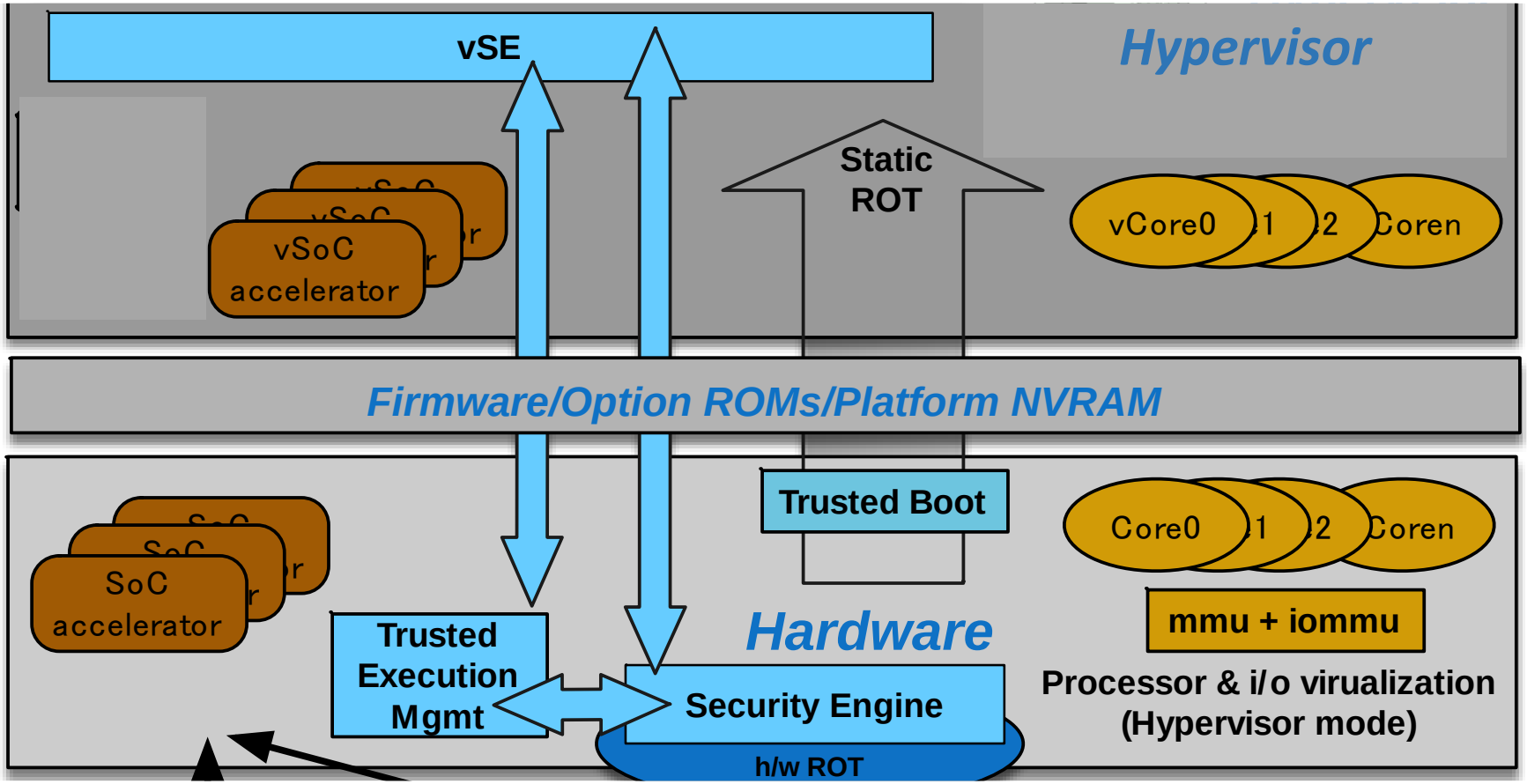


mmu: memory management unit

4.1 Secure(Verified)/Trusted (Measured) Boot

Trusted hardware executes immutable firmware.

- TEE provides services to the hypervisor, and it virtualizes Security Engine, vSE.
- Trusted Boot verify/measure each subsequent load of firmware or software.

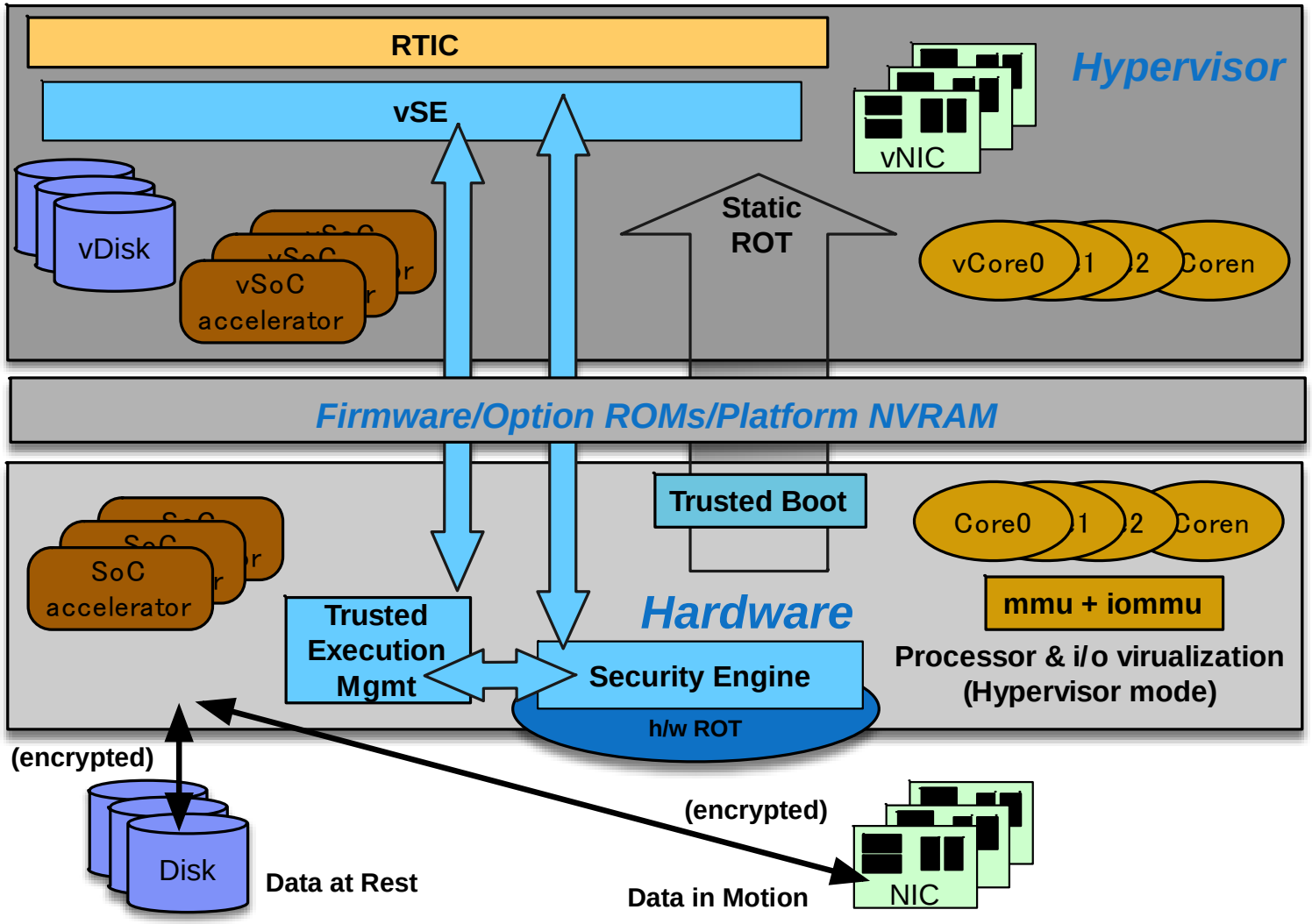


SE: Security Engine

SoC: System on Chip

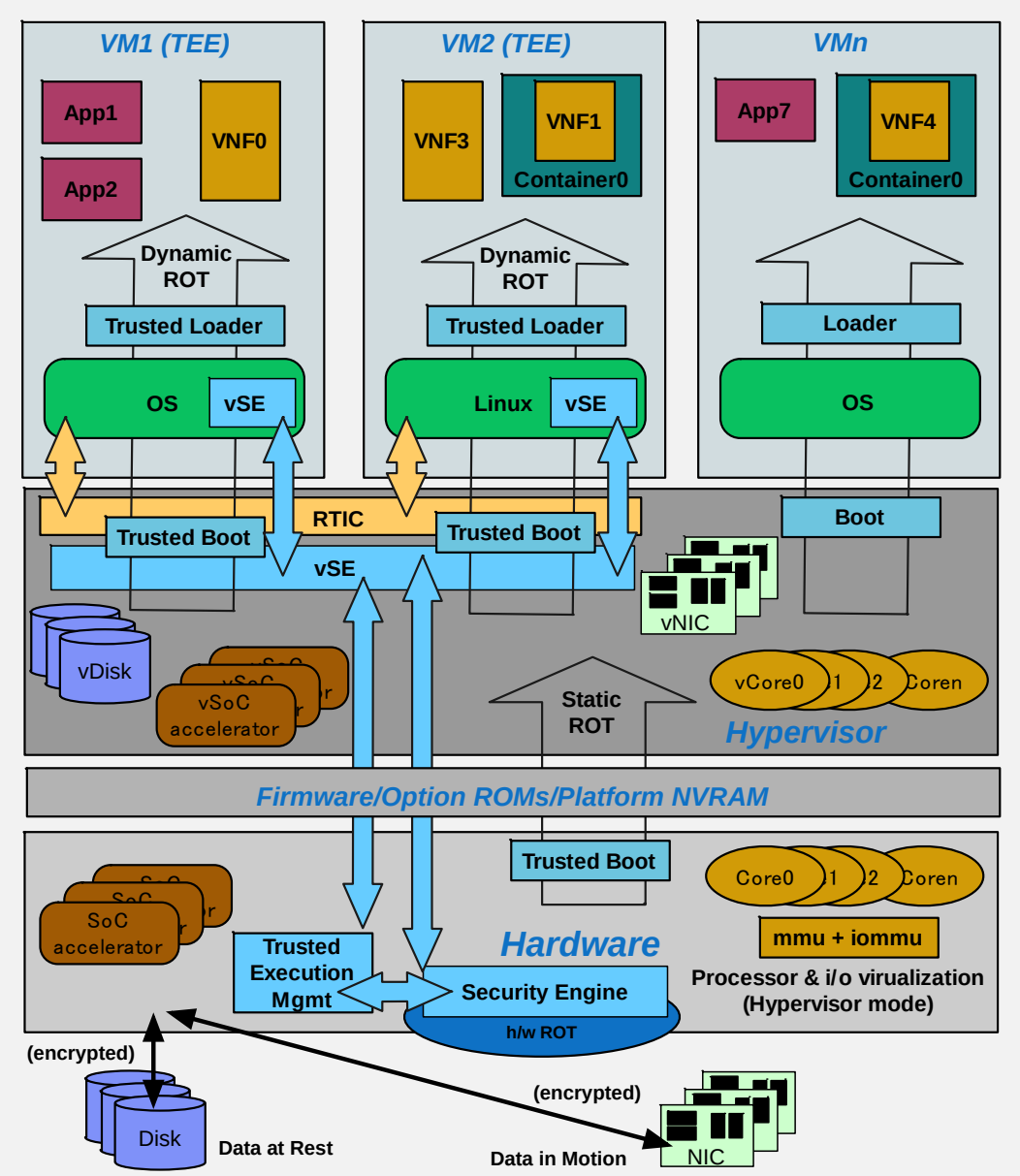
4.2 Extends the Chain-of-Trust

- The state of the areas of memory is modified during execution for Data in Use.
- Storage devices and NIC are encrypted for Data at Rest and Data in Motion.



RTIC: Runtime Integrity Checking
NIC: Network Interface Card

4.3 A Chain of Trust with VMs and apps/containers

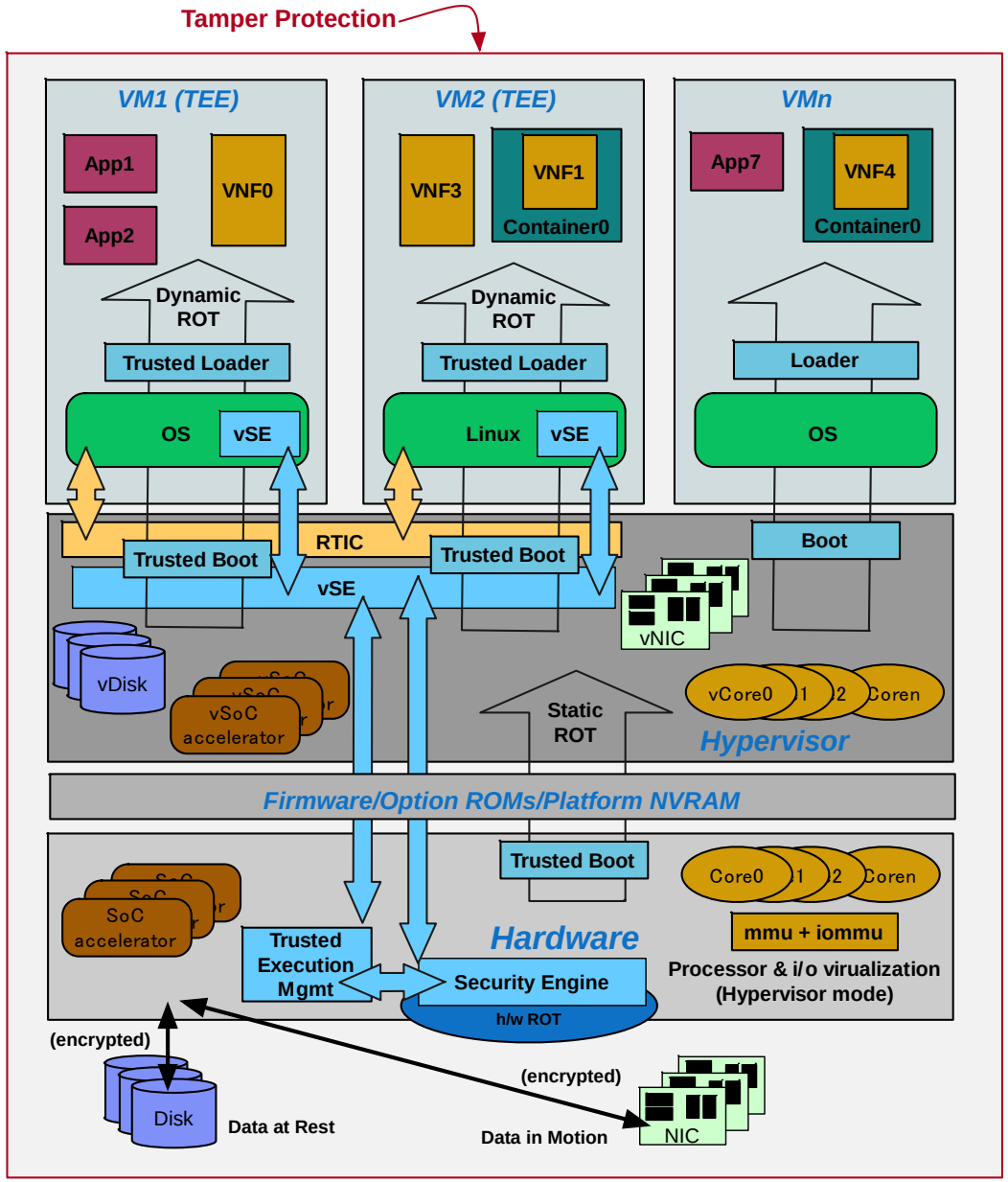


vSE with an agent in each trusted VM.

The OS in the VM manages to instantiate separate application address spaces or Linux containers.

TEE: Trusted Execution Environment
VM: Virtual Machine
VNF: Virtual Network function

4.4 Tamper Protection



Physical Security and Anti-tamper Mechanisms

Tamper Resistance/Evidence/Detection/Response

Thank You !