Trusted Execution Environments

Introduction & Current focus

Richard Hayton
- Trustonic Ltd
- Chair Automotive Task Force, GlobalPlatform
- Chair TES Committee, GlobalPlatform

TRUSTONIC

Global Platform™

Protecting a modern operating system

Modern operating systems such as Linux and Android are extremely complex

They are use *everywhere* from Phones to Computers, and increasingly within larger ECUs in vehicles

Think of the Operating System as a city, with many different activities going on at once

Protecting a modern operating system

Modern operating systems such as Linux and Android are extremely complex

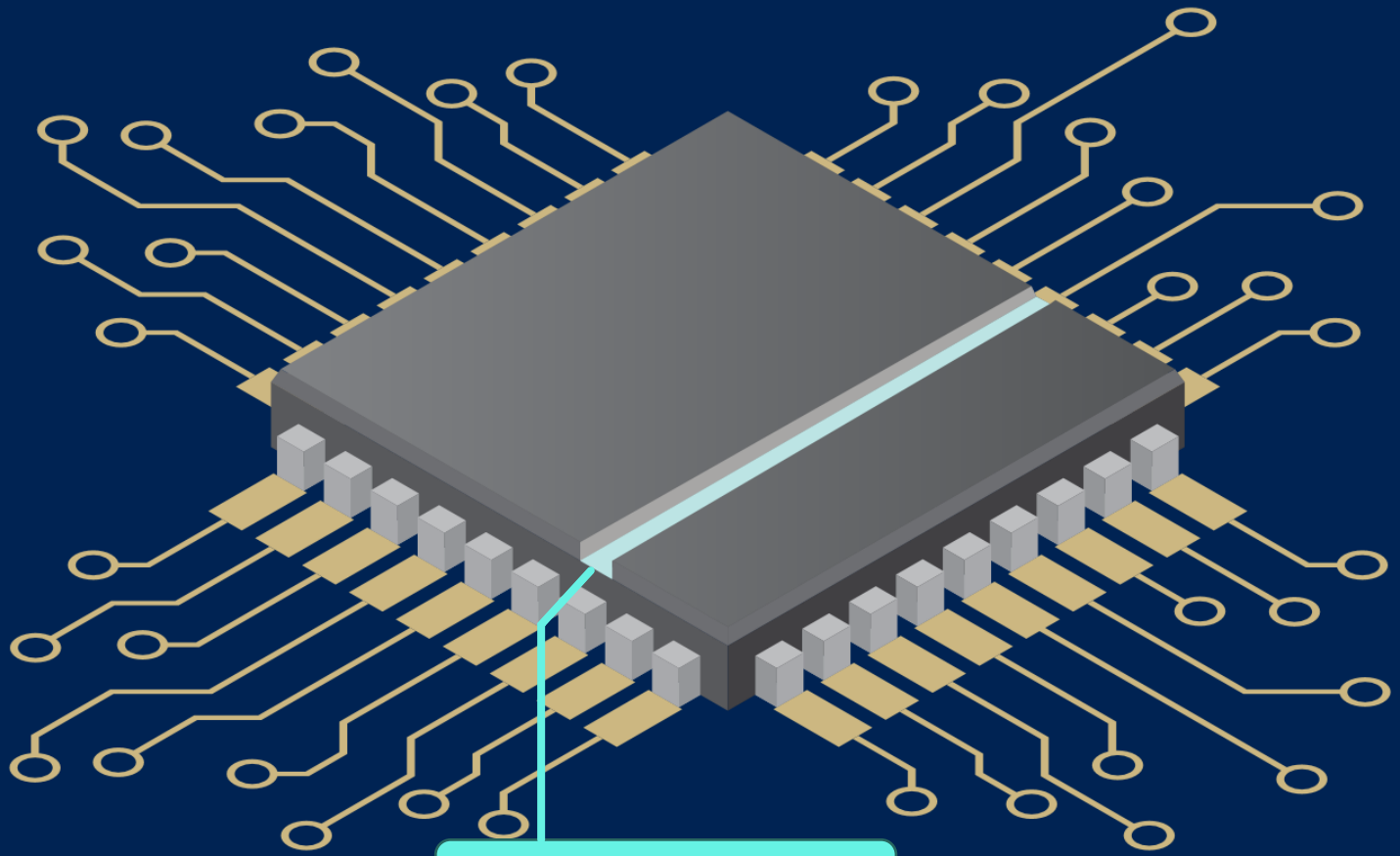
They are use *everywhere* from Phones to Computers, and increasingly within larger ECUs in vehicles

Think of the Operating System as a city, with many different activities going on at once

Attacks can start in one building and then spread to another. The complexity of the operating system makes it inherently hard to protect.

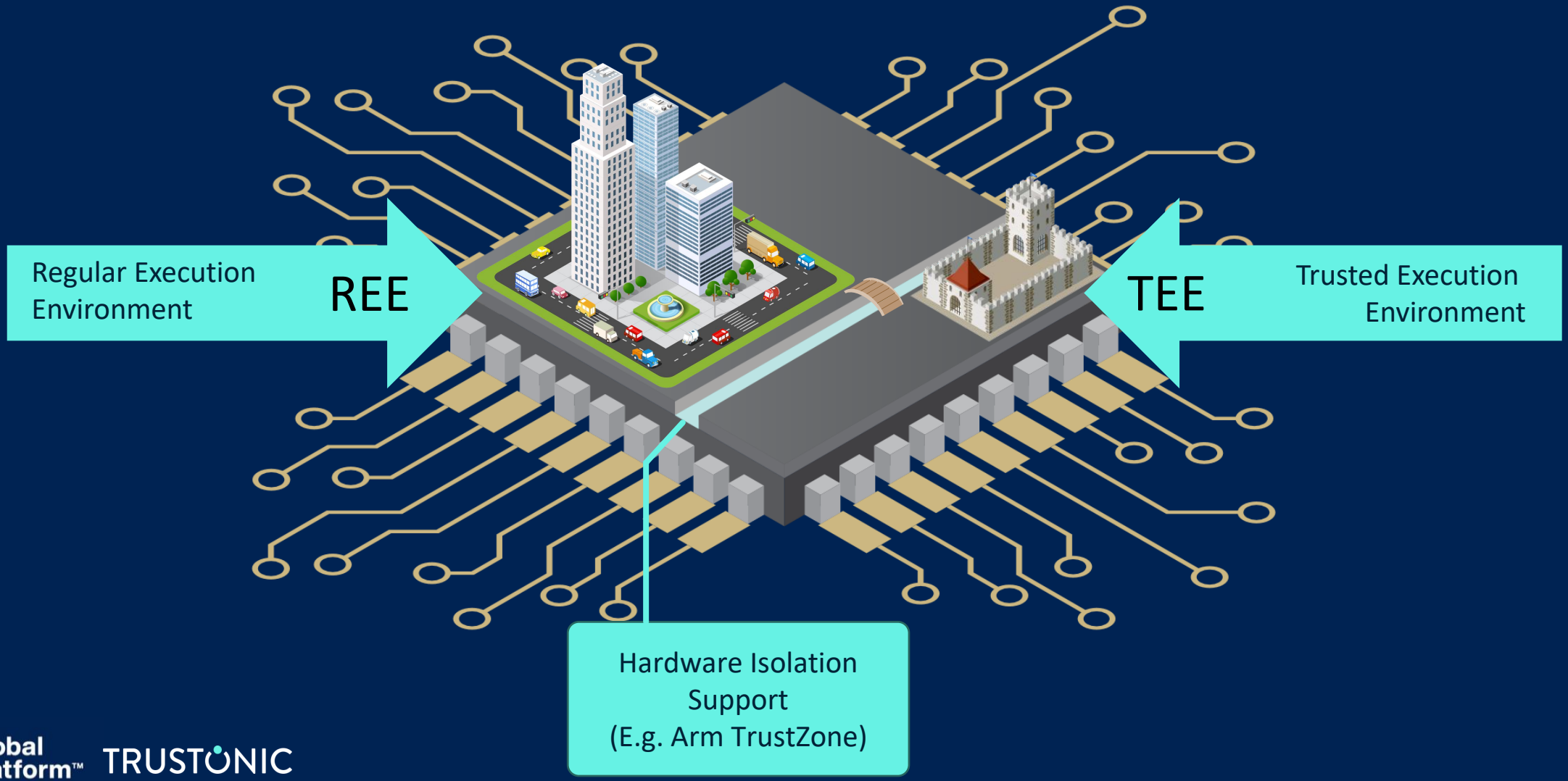
Trusted Execution Environments

Based on hardware capabilities that provide isolation



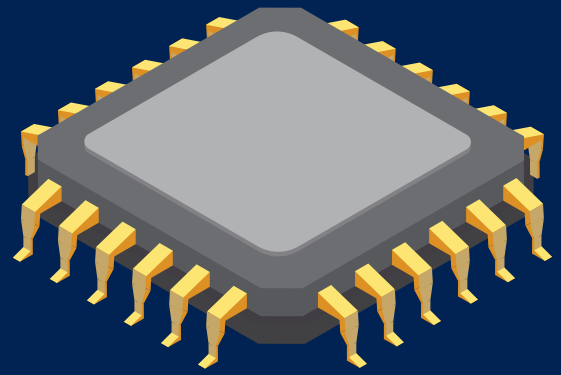
Trusted Execution Environments

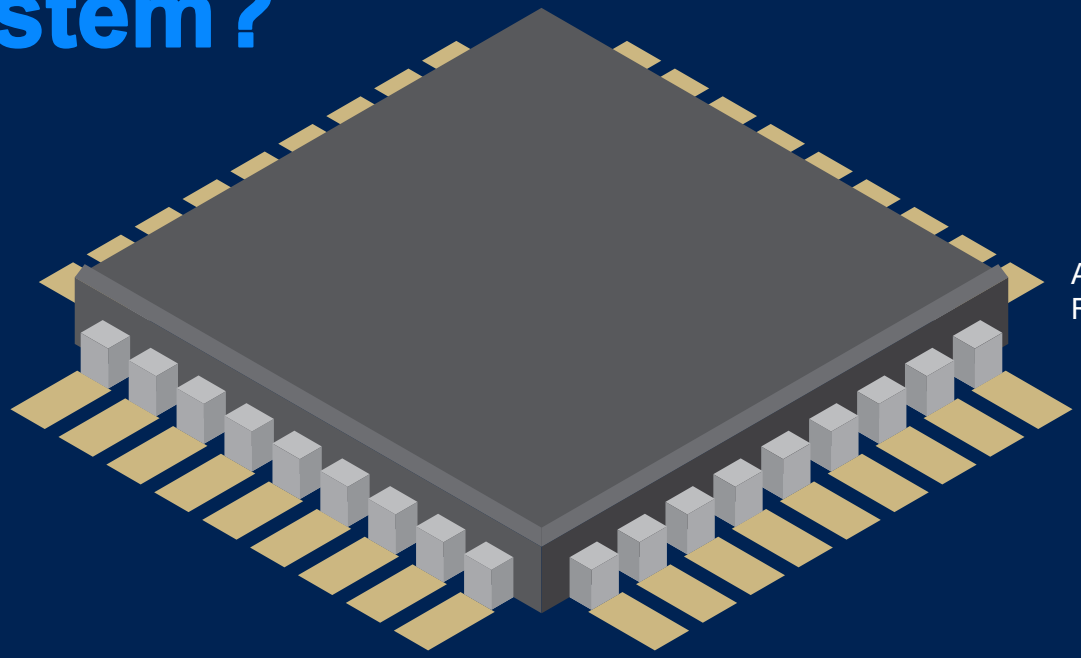
GlobalPlatform defined a TEE Operating System that leverages this hardware capability to provide security functions



Is there a TEE on my system?

Arm Cortex-M
Risc-V embedded





Arm Cortex-A
Risc-V (soon)

Smaller “microcontrollers” commonly used in single-purpose ECUs typically do not have a TEE OS

Modern MCUs, such as Arm Cortex-M V8 have the necessary hardware capabilities, and some vendors provide TEE-like solutions

Use of a hardware keystore is much more common in automotive.

Larger “microprocessors” used in larger ECUs and domain, or zonal, controllers typically DO have the hardware capabilities for a TEE and TEE Operating Systems are common.

TEEs are *required* for Android deployments, and are commonly used for Linux, QNX and other embedded operating systems.

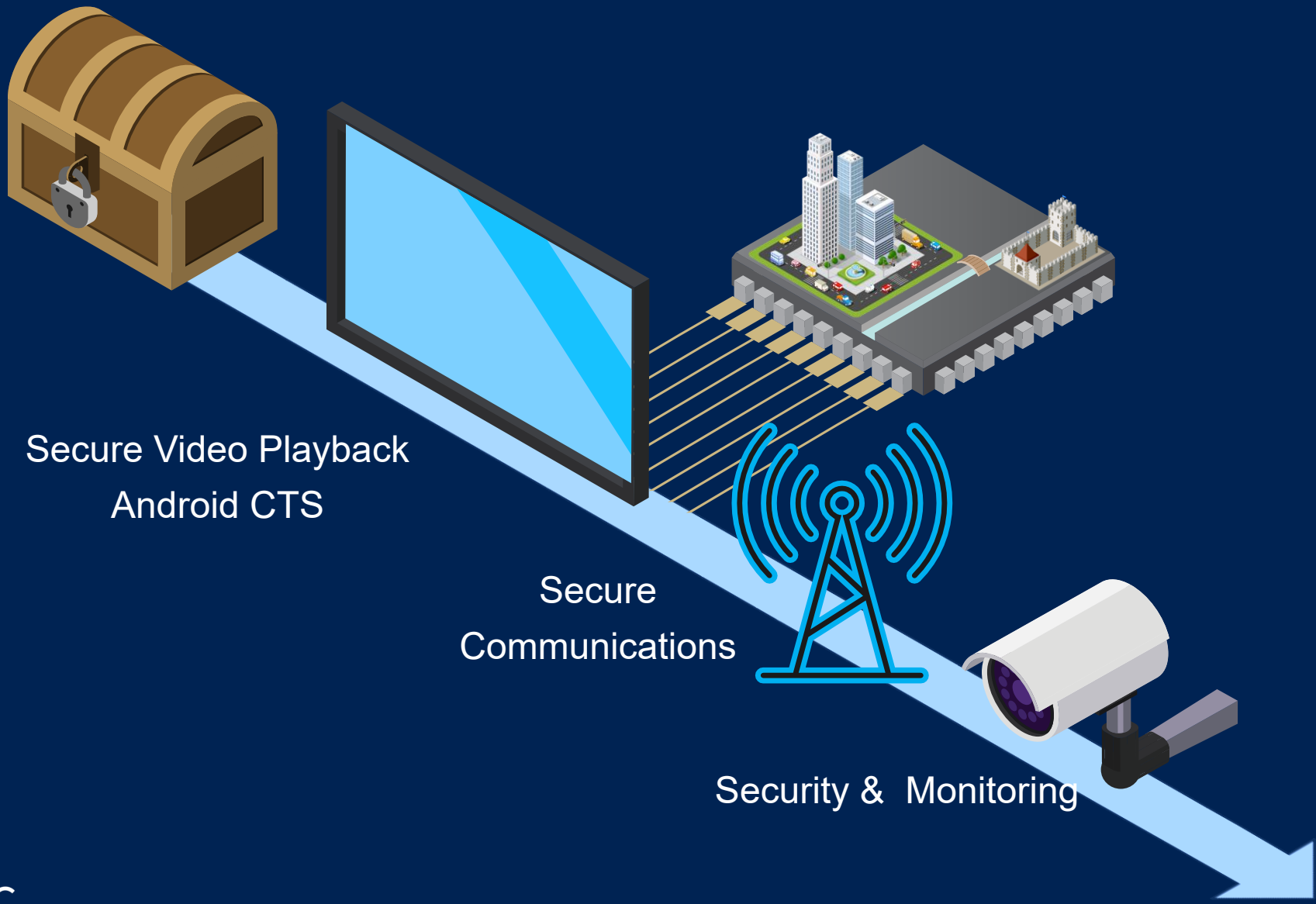
TEEs have evolved

TEEs were first standardized over 15 years ago

Whilst the security promise made by TEEs have not changed, the functional capabilities of TEEs have increased significantly

- Single Threaded → Symmetric Multi-Processing
- Small Memory → Effectively unlimited memory
- Limited Storage → Effectively unlimited storage
- Limited Function → Peripheral & Network access
- Single Client OS → Hypervisor Support

Use Case Evolution in Automotive



Trends

Data Collection and Storage

- Diagnostic and Performance Data
- Personal / Driver Data (Privacy)
- Data collection for AI training

Secure & Robust Supply Chain

- Secure Manufacture & Attestation
- OTA Update
- Silicon / SW Vendor independency

Future & Regulation Readiness

- Post Quantum Cryptography
- Defensible design choices
- Global .v. Local designs

Data

Unlike HSMs that have a small and fixed amount of storage for keys, TEEs support effectively unlimited storage

GlobalPlatform standardized a simple flat file system, original used mainly for configuration and keys

Increasingly customers are asking for more

- Large files, such as biometric models
- Large numbers of files, such as to support user profiles and applications such as messaging and media
- Structured data storage, for on-device analysis of datasets

Example, recording actual .v. posted speed in a database table in order to detect errors in mapping data.

#	DriverId	Timestamp	RoadId	Start	Distance	PostedLimit	ActualSpeed	Discrepancy	ClearRoad
0	Driver1	1751130000	9000	4000	500	60	43	-17	true
1	Driver1	1839330000	9000	3800	700	60	40	-20	true
2	Driver1	1923510000	9000	3900	600	60	37	-23	false
3	Driver2	2154810000	9000	3900	600	60	39	-21	false
4	Driver2	2244810000	9000	3700	800	60	38	-22	true
5	Driver1	1717230000	9001	0	500	60	43	-17	true
6	Driver1	1803810000	9001	0	500	60	40	-20	true
7	Driver1	1887510000	9001	0	500	60	37	-23	false
8	Driver2	2148810000	9001	0	500	60	39	-21	false
9	Driver2	2237730000	9001	0	500	60	38	-22	true

Attestation & Secure Supply Chain

Supply chain integrity is gaining focus, as it is significant attack path.

There is also a desire from OEMs to use components from many manufacturers, especially to comply with regional needs, or handle shortages.

During vehicle lifetime, software may be modified or updated, and configuration changed.

Attestation is a means to enable devices to securely report on their current status, and for third parties to rely on this data to make key decisions – for example whether to enable autonomous functionality.

GlobalPlatform TES committee has recently created an Entity Attestation Protocol Specification which will be publicly available soon.

It is based on the IEFT EAT standard, which has just been formally published, but has been in used for a while.

Future work is turning to standarizing the processing of Attestation, for example the open source Veraison project.

Future Ready Crypto?

Looking to the future, much focus has been on Post Quantum Cryptography.

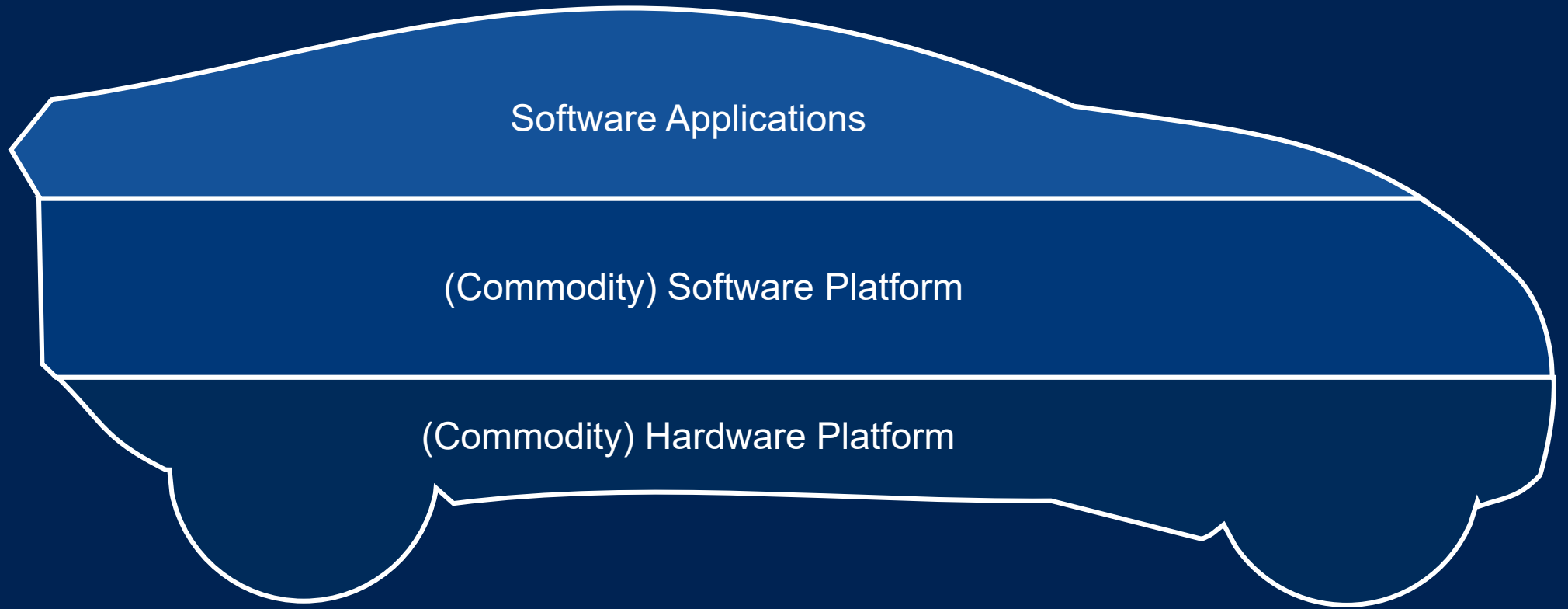
NIST has standardized a number of algorithms, and GP has added these to the TEE Core API

Some regions are adopting NIST recommendations, but it is unlikely we will get global standardization

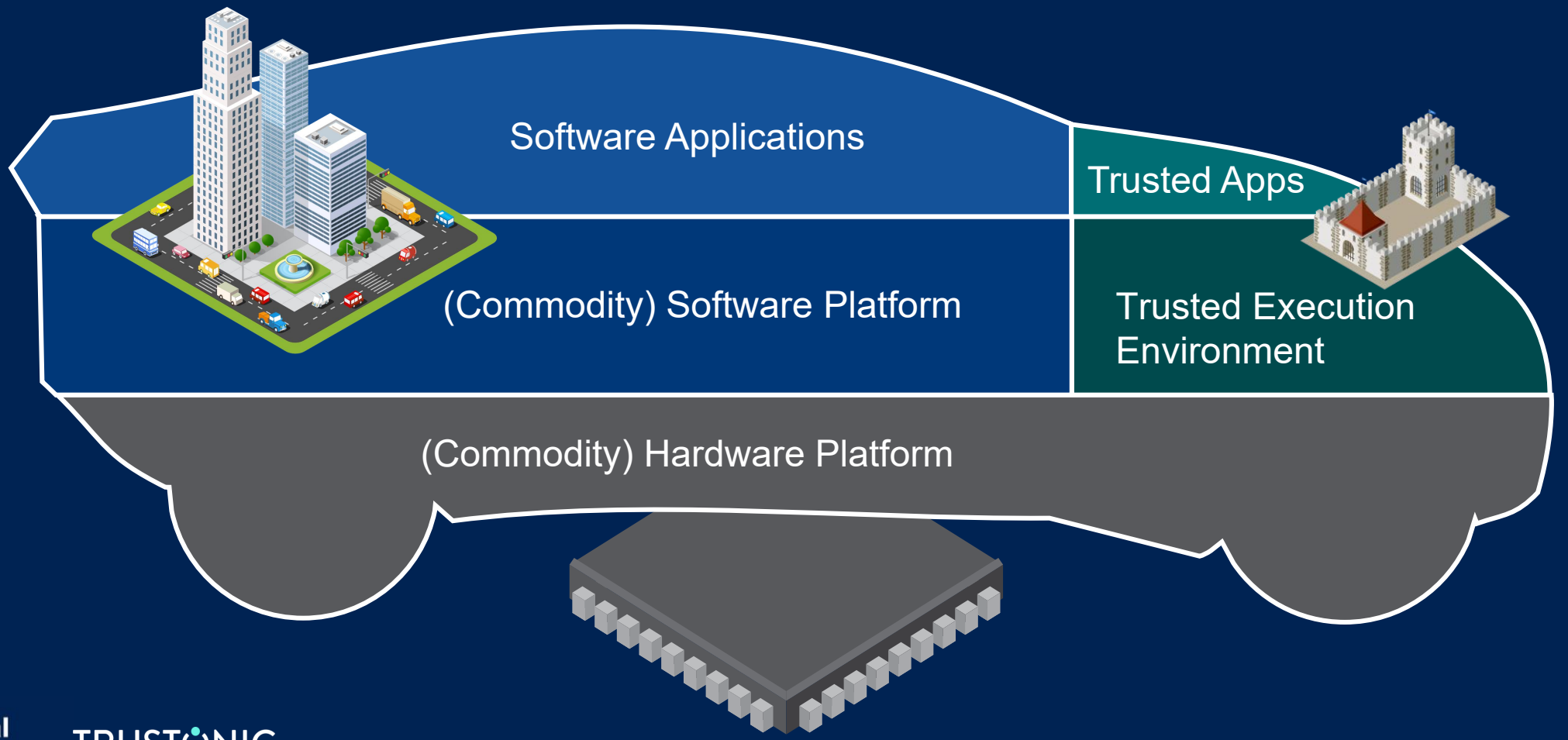
- China is defining its own algorithms.
- Europe is recommending HYBRID schemes
- There is some disagreement over PQ-safe key sizes for AES.

- PQC algorithms generally have large keys sizes and/or larger signatures
- Some algorithms are not suitable for hardware implementations – but this does not affect most TEEs
- PQC performance is on a par with traditional algorithms.
- Symmetric algorithms (e.g. AES) remain safe.
  - NIST asserts 128 bit remains sufficient
  - Some European entities recommend 256 bit

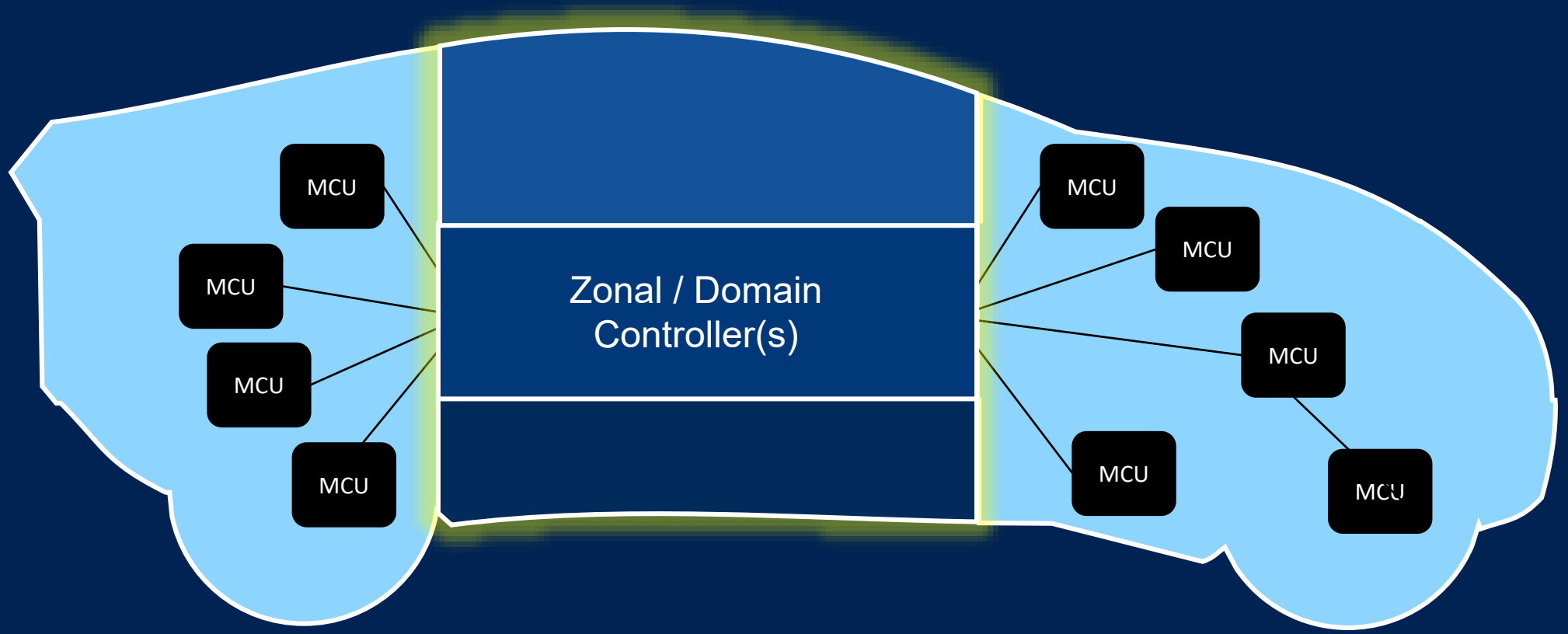
Software Defined Vehicles



TEE within Software Defined Vehicle



Reality is more complex – Lots of MCUs



Q. Can we put TEEs on MCUs?

Is the MCU problem different from the CPU problem?

Typically, similar needs but far less flexibility required
(e.g. single purpose)

Is the GlobalPlatform TEE suitable for MCUs?

Designed to be generic – but are arguably too broad /
unnecessarily complex for MCU use cases

What products exist today / will exist in future?

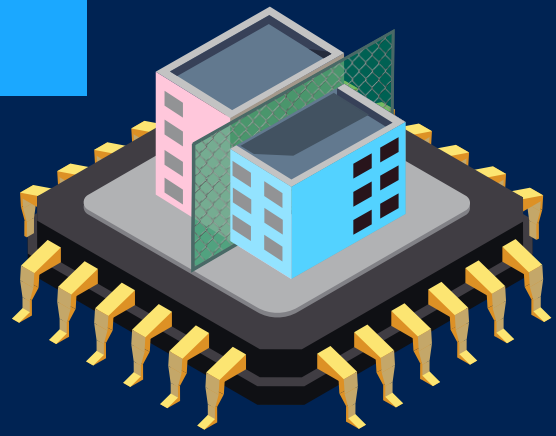
No commercial GP based MCU-TEEs
But many products using ARM PSA

A Micro-TEE?

APIs?
GlobalPlatform TEE APIs
Arm Platform Security Architecture?

M-REE

General Purpose Partition



M-TEE

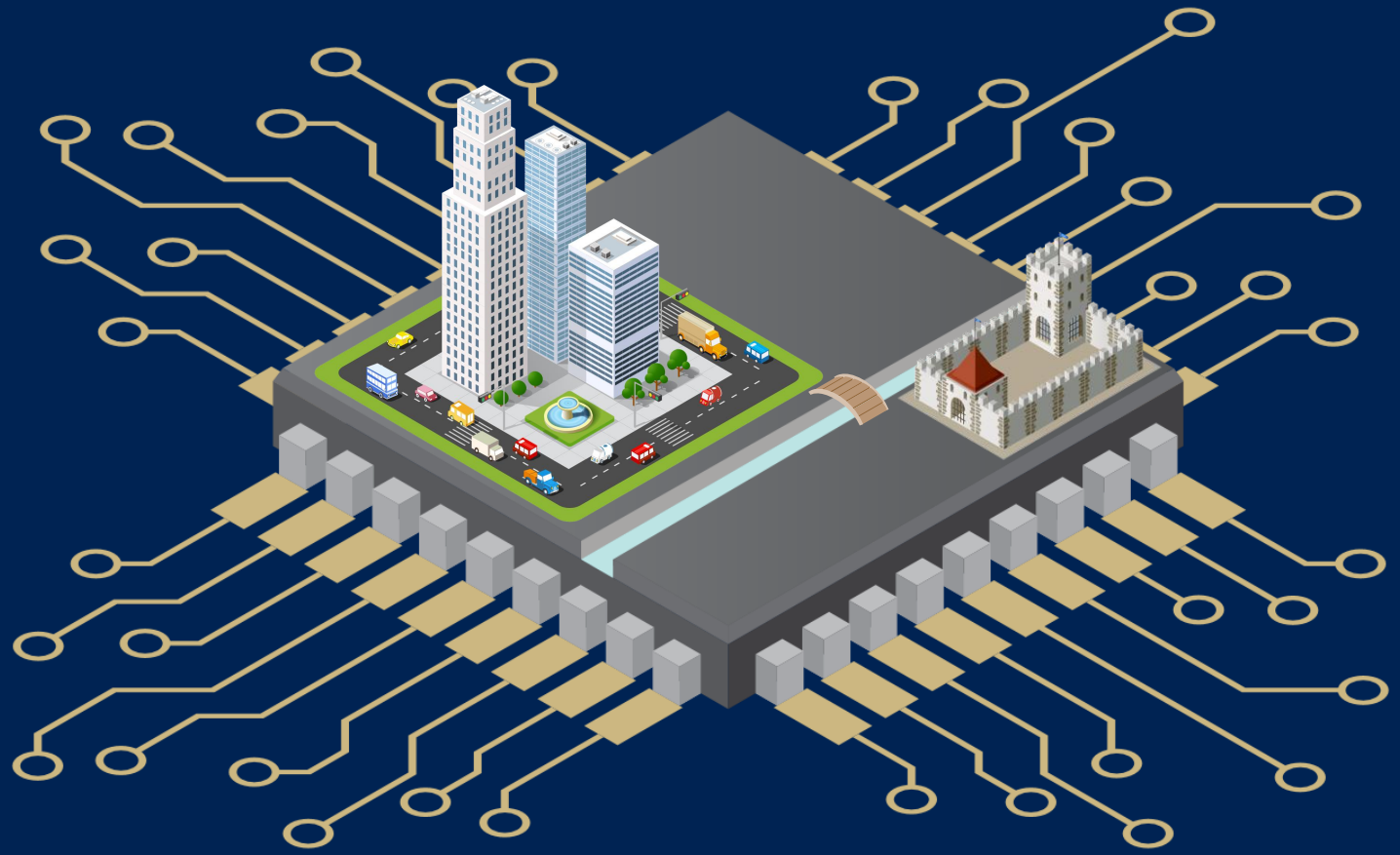
Security Focused Partition

Certification / Compliance
Common Criteria, SESIP or other?

Supporting Safety Critical Applications

A modern “City-like” operating system enables lots or different applications to run at once, but is generally not suitable for safety critical or real time functions

Supporting safety critical functionality in Software Defined Vehicles remains an active area of discussion



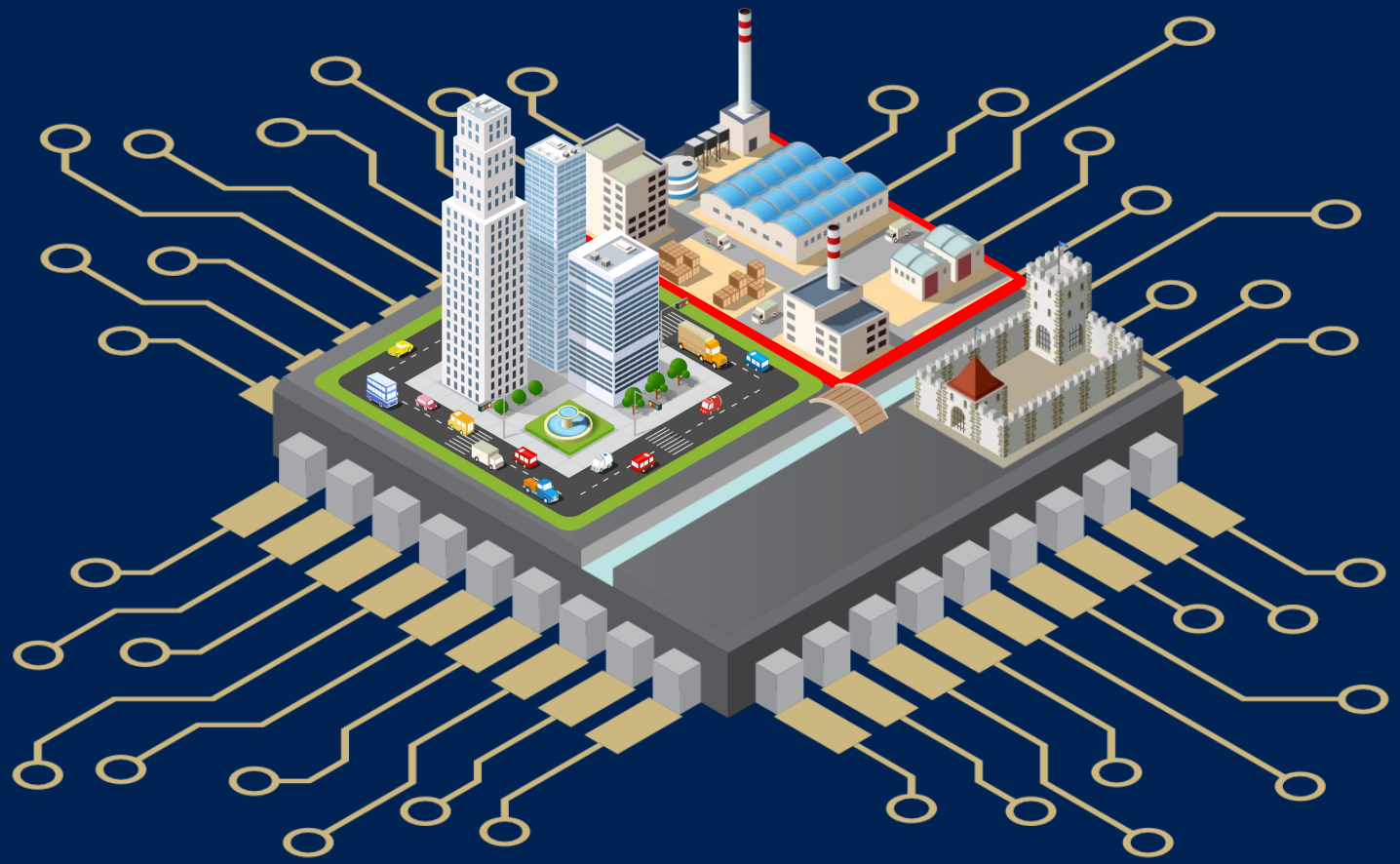
Supporting Safety Critical Applications

A modern “City-like” operating system enables lots or different applications to run at once, but is generally not suitable for safety critical or real time functions

Supporting safety critical functionality in Software Defined Vehicles remains an active area of discussion

One common approach is to add a second or third operating system which are more focused on safety critical applications

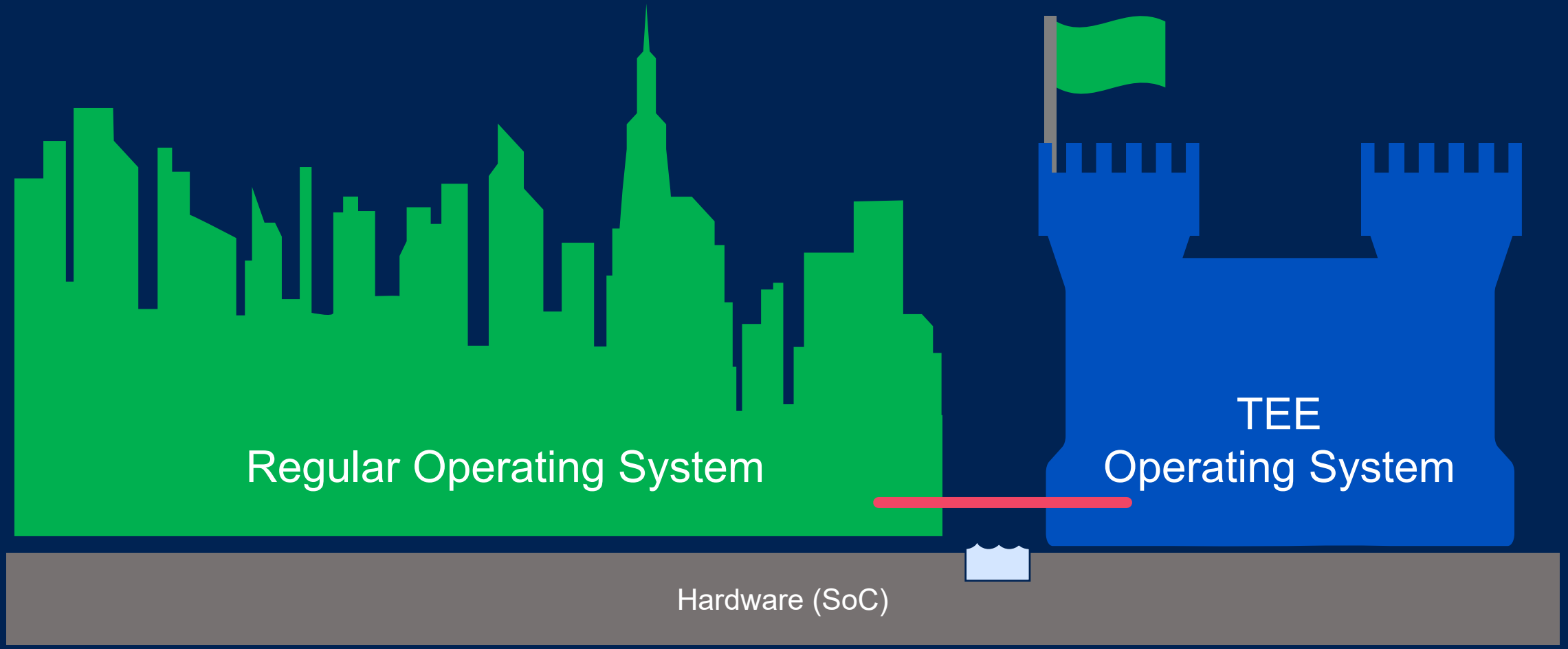
An open discussion is how (or if) the TEE should support mixed-criticality clients



Architecture

TEE supports multiple isolated services (called Trusted Applications)

Early TEE architecture

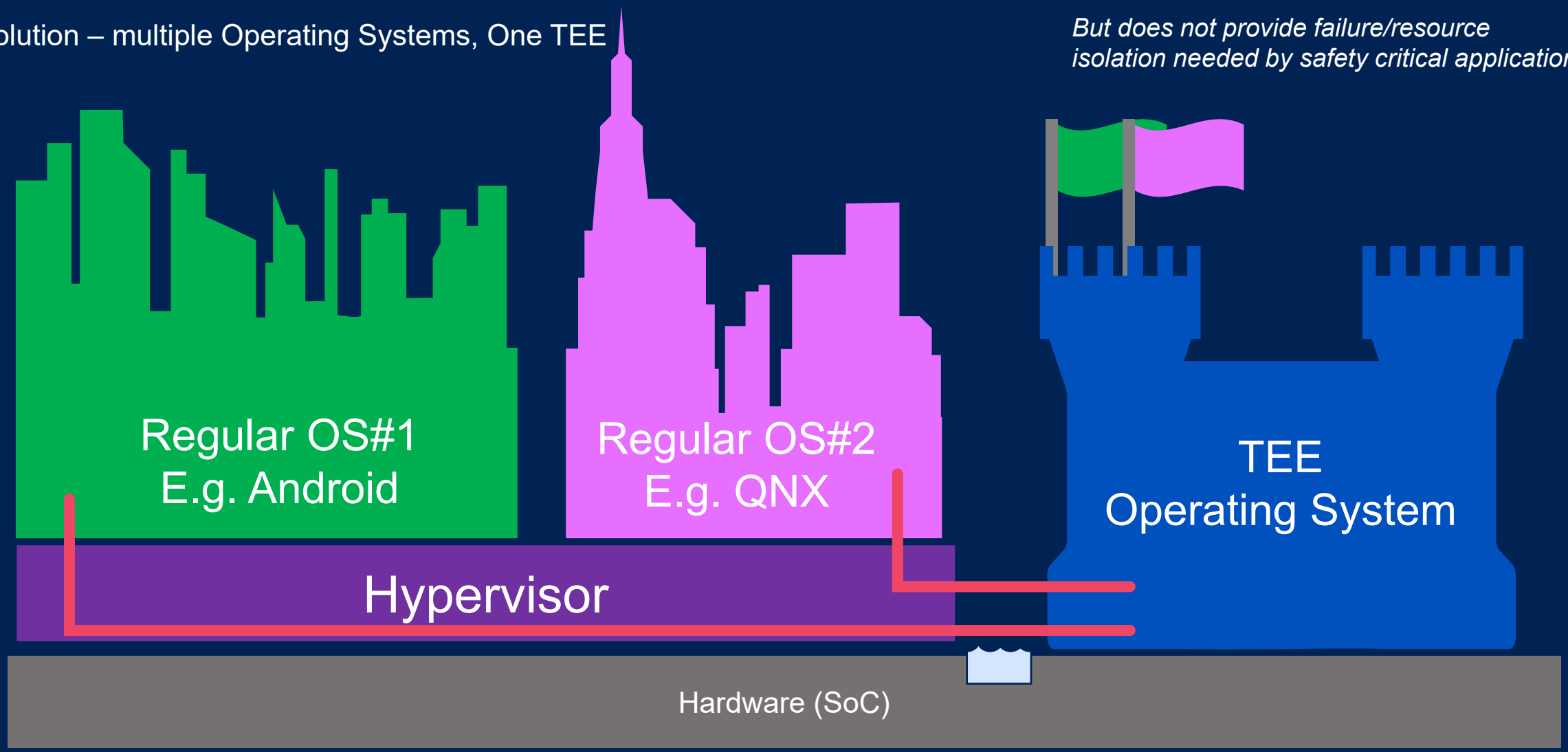


Architecture

Evolution – multiple Operating Systems, One TEE

Existing Trusted Application Isolation
Ensures security boundaries

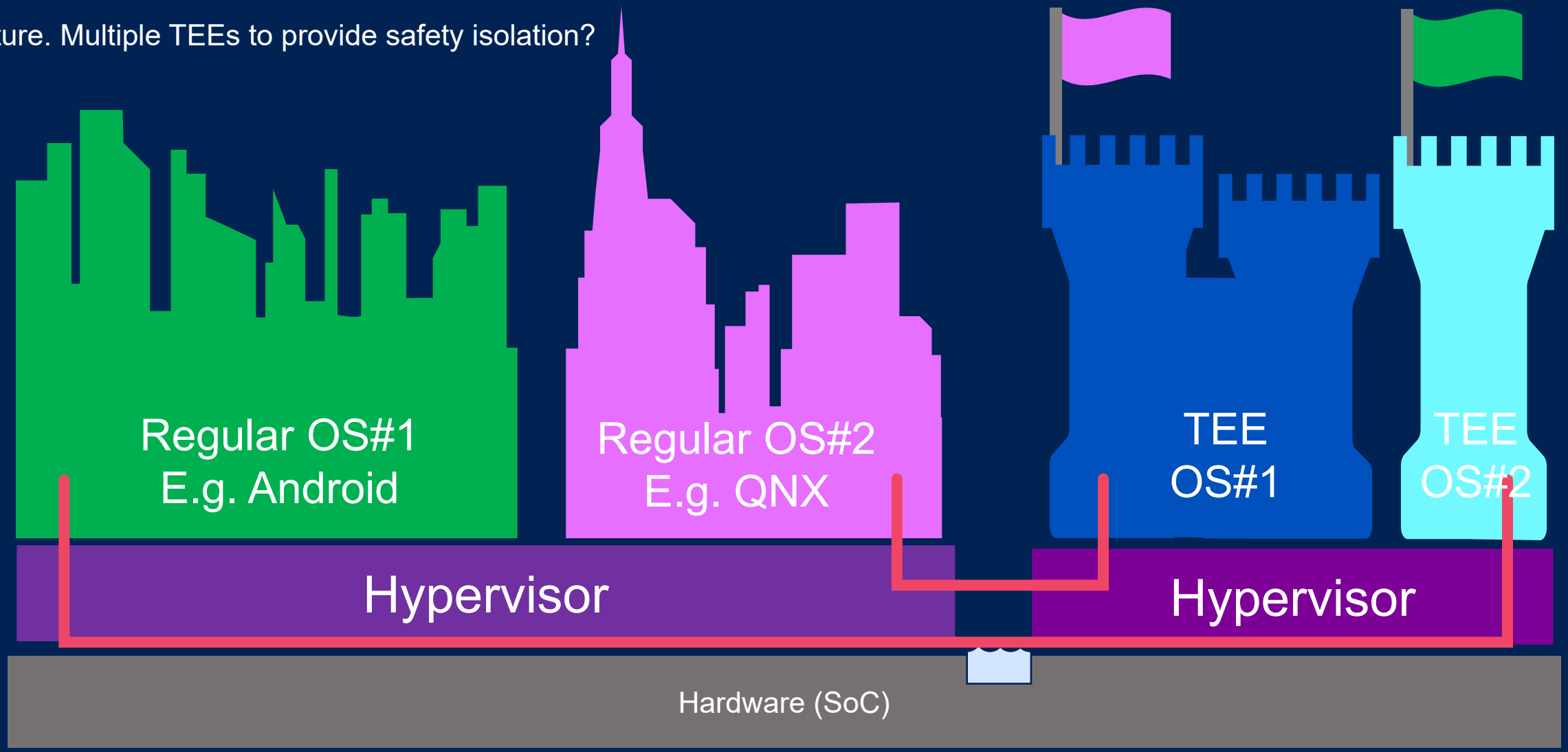
But does not provide failure/resource isolation needed by safety critical applications.



Architecture

Hypervisors in the secure world provide one approach to enabling safety isolation

Future. Multiple TEEs to provide safety isolation?



Summary

Trusted Execution Environments are a mature technology used in billions of devices.

They are used extensively in IVI and other domain controllers, and use is growing significantly

GlobalPlatform offers TEE Certification, and many companies use Common Criteria labs, with TEE Operating Systems certified up to EAL5+ (TRUSTONIC)

There is also some interest in certifying broader solutions that leverage TEEs, likely using GlobalPlatform SESIP certification.

For automotive there are several key areas

- Replacing or augmenting HSMs for performance, crypto agility or other flexibility.
- More and larger secure applications – such as for data capture and processing.
- Support for Microcontrollers (Micro-TEE)
- Support for safety critical domains (Mixed-Criticality)
- Attestation and Lifetime services

Some commercial TEEs address these needs today – and standardization work is ongoing in the TES committee at GlobalPlatform.