

WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

July 10, 2024

This Session will be recorded.






This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR



TRAFFIC LIGHT PROTOCOL (TLP)

VERSION 2.0 DEFINITIONS

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<div><div>TLP:RED</div><div></div></div> <div>Not for disclosure, restricted to participants only.</div>	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
<div><div>TLP:AMBER+STRICT</div><div></div></div> <div>Limited disclosure, restricted to participants' and its organization.</div>	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
<div><div>TLP:AMBER</div><div></div></div> <div>Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.</div>	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
<div><div>TLP:GREEN</div><div></div></div> <div>Limited disclosure, restricted to the community.</div>	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
<div><div>TLP:CLEAR</div><div></div></div> <div>Disclosure is not limited.</div>	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: <https://www.us-cert.gov/tlp>

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ Intelligence Highlights
11:15	DHS CISA Community Update <ul style="list-style-type: none">➤ Jeff Terra, Joint Cyber Defense Collaborative (JCDC)
11:20	Featured Speaker: <ul style="list-style-type: none">➤ Richard Hayton, Chief Strategy and Innovation Officer, Trustonic➤ Title: Time for TEEs. What they are, and why they have become a key technology for Automotive
11:55	Q&A & Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: Slides are at **TLP:CLEAR** and on our [website](#). Discussions are **TLP:GREEN** & may be shared across Auto-ISAC Community, “off the record”

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions! *“Cybersecurity is a Team Sport!”*

31
OEM Members

21
Navigator
Partners

❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

48 Supplier &
Commercial
Vehicle Members

20
Innovator
Partners

Membership represents **99%**
of cars and trucks on the road in
North America

Coordination with **26**
critical infrastructure ISACs
through the National Council of
ISACs (NCI)

2024 BOARD OF DIRECTORS

Thank you for your Leadership!



Kevin Tierney
*Chair of the
Board of the Directors*
GM



Josh Davis
*Vice Chair of the
Board of the Directors*
Toyota



Stephen Roberts
*Secretary of the
Board of the Directors*
Honda



Tim Geiger
*Treasurer of the
Board of the Directors*
Ford



Oliver Creighton
Chair of the EuSC
BMW



Andrew Hillery
Chair of the CAG
Cummins



Amine Taleb
Chair of the SAG
Harman



Maryann Combs
Polaris



Bob Kaster
Bosch



Brian Witten
Aptiv

AUTO-ISAC MEMBER ROSTER

As of July 3, 2024

Highlight = New Active Members

79 MEMBERS + 2 PENDING

Aisin	Ferrari	Magna	Rivian
Allison Transmission	Flex	MARELLI	SiFive, Inc.
Amazon	Ford	Mazda	Stellantis
American Axle & Manufacturing	General Motors	Mercedes-Benz	Stoneridge
Aptiv	Geotab	Mitsubishi Electric	Subaru
AVL List GmbH	Harman	Mitsubishi Motors	Sumitomo Electric
BMW Group	Hitachi (Astemo - Affiliate)	Mobis	thyssenkrupp
BorgWarner	Honda	Motional	Tokai Rika
Bosch (ETAS - Affiliate)	Hyundai	Navistar	Toyota (Woven - Affiliate)
Bose Automotive	Infineon	Nexteer Automotive Corp	Valeo
ChargePoint	Intel	Nissan	Veoneer
CNH Industrial	Jaguar Land Rover	NXP	Vitesco
Continental (Elektrobit - Affiliate)	JTEKT	Oshkosh Corp	Volkswagen (Cariad - Affiliate)
Cummins	Kia America, Inc.	PACCAR	Volvo Cars
Daimler Truck	Knorr Bremse	Panasonic (Ficosa - Affiliate)	Volvo Group
Dana Inc.	KTM	Phinia	Waymo
Deere & Company	Lear	Polaris	WirelessCar
Denso	LG Electronics	Qualcomm	Yamaha Motors
e:fs TechHub GmbH	Lucid Motors	Renault SAS	ZF
Faurecia	Luminar	Renesas Electronics	

Pending: IAV GmbH, Zoox

AUTO-ISAC BUSINESS UPDATES AND EVENTS

- **Community Call:** Wednesday, August 7, 2024 **Time:** 11:00 – 12:00 p.m. ET **TLP:GREEN** **Speaker:** Bob Lyle, Riscosity **Title:** “The State of Privacy Risks in the Automotive Industry”
- **2023 Annual Report** **TLP:CLEAR** available to Auto-ISAC Community on our [website](#).
- **Public Auto-ISAC Website Survey:** Please assist us in creating a better online experience for our Members, partners, and the community! Take our [Website Survey here](#)! Extended until **Friday, July 12th, 2024**.
- **Auto-ISAC** **TLP:CLEAR** **8th Annual Cybersecurity Summit** will be held October 21 – 24, 2024 in Detroit, Michigan. Agenda details and registration can be found [here](#)!
- **APIsec University** is hosting a free virtual **APISEC-CON Automotive** on **July 25th** focused on API security in the automotive and transportation industry. Learn more at <https://conf.apisecuniversity.com>.

AUTO-ISAC SUMMIT

2024 Auto-ISAC Cybersecurity Summit

REVVING UP RESILIENCE: SECURITY MEETS INNOVATION

October 22-23 | MGM, Detroit, MI

In-person & Virtual

[Information and registration](#)





AUTO-ISAC INTELLIGENCE HIGHLIGHT

RICKY BROOKS, INTELLIGENCE OFFICER

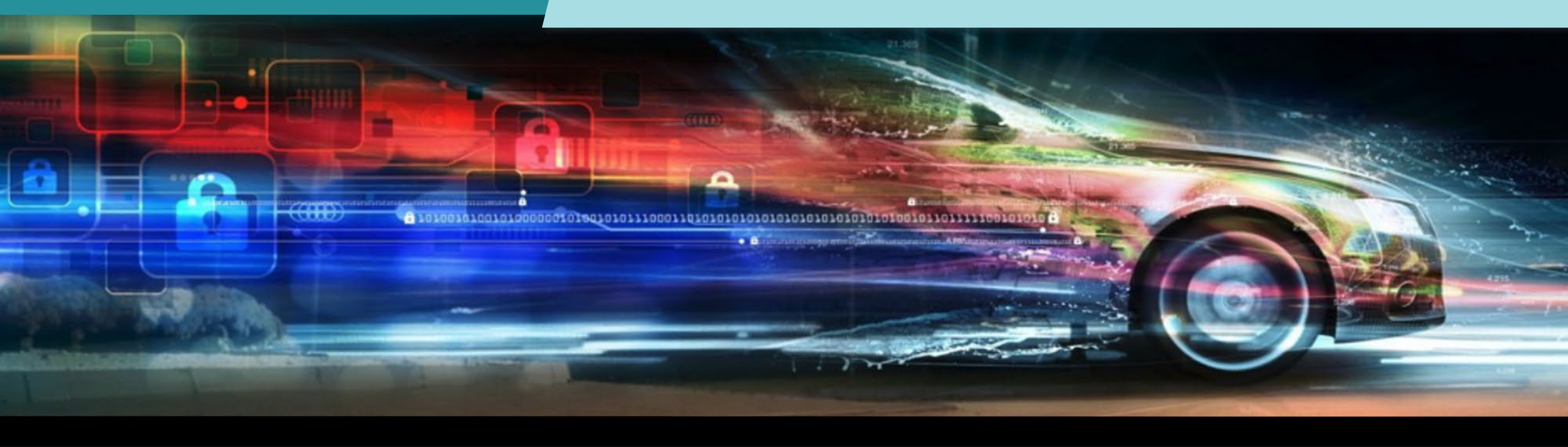
This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR



AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; **TLP:GREEN** Auto-ISAC 2024 Threat Assessment was released March 21; we welcome your feedback.
 - **Send feedback**, intelligence, or questions to analyst@automotiveisac.com
- Intelligence Notes
 - Geopolitical tensions involving Russia, China, North Korea, and Iran remain **high** with Russia-Ukraine and Israel-Hamas in crises (**Russia-Ukraine** ^{1 2}, **Israel-Hamas/Israel-Hezbollah** ^{3*}, **Iran**, **China** ^{4 5 6 7*}, **North Korea** ⁸)
 - Ransomware ^{9 10} Groups Targeting Automotive: [8Base](#), [Akira](#), [Arcus Media](#), [Black Basta](#), [BlackSuit*](#), [Cactus](#), [LockBit 3.0](#), [Play](#), [Qilin](#), [Space Bears](#) (**New**: [Brain Cipher](#), [Eldorado](#))
 - **CDK Global**: Dealerships mostly restored ([Link](#)); Blacksuit suspected ([Link](#), [Link](#)), TTPs unknown.
 - **Notable Vehicle Research**: Jamming attacks against UWB ([Link](#)); Trajectory prediction attack via LiDAR-induced deceptions ([Link](#)); Frequency-domain backdoor attacks on autonomous driving models ([Link](#)); Adversarial attack on in-vehicle intrusion detection system ([Link](#)); Attacking J1939 ([Link](#)).
 - **Notable TTPs**: APTs hiding cyberespionage behind ransomware ([Link](#)); Ransomware compromise of bioenergy ICS ([Link](#))*; Using public rootkits, trusted third-party services for command and control, Secure Shell backdoors, and custom malware for cyberespionage ([Link](#)); Impersonating companies that victims works for ([Link](#)); Exploiting Linux Kernel use-after-free ([Link](#)); Exploiting Cisco 0-day ([Link](#)); Exploiting ARM 0-day ([Link](#)); Abusing F5 load balancers ([Link](#)); Exploiting new MOVEit flaw ([Link](#)); **Notable Tools**: Team of large language model agents working together ([Link](#)); Fuxnet* ([Link](#)); TRANSLATEX ([Link](#)); Xctdoor ([Link](#)).



FEATURED SPEAKER

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR



MEET THE SPEAKER



Richard Hayton

Richard Hayton is an experienced technology leader. With over 30 years in the cybersecurity industry, he is a regular speaker and influencer on matters of cybersecurity.

Richard is a board member at GlobalPlatform and chairs the Trusted Environments and Services (TES) Group, and the Automotive Task Force. Before joining Trustonic, Richard was Chief Architect for Citrix Mobility, where he was responsible for crafting the XenMobile Enterprise Mobility Suite. During his 20 years at Citrix, Richard led projects ranging from embedded software to global enterprise systems, with a focus on user and developer experience.

Richard holds a Ph.D. in Computer Science from Cambridge University, focusing on identity federation for users, devices, and services.

The background of the slide is a dark blue gradient. It features a wireframe grid pattern overlaid on a faint image of a car, likely a Volvo, shown from a side profile. Scattered across the grid are several teal-colored padlock icons, some of which are open and some are closed. The overall theme suggests cybersecurity and digital trust.

TRUSTONIC

Trusted Execution Environments

Richard Hayton.

Chief Strategy and Innovation Office, Trustonic Ltd.

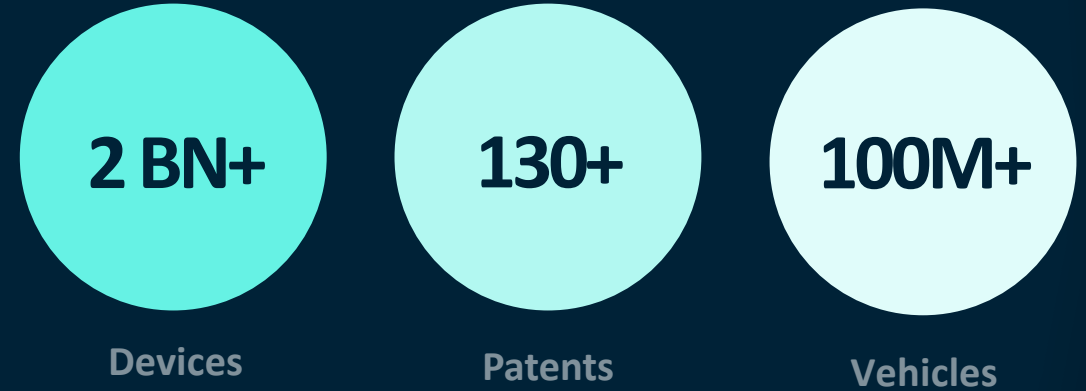
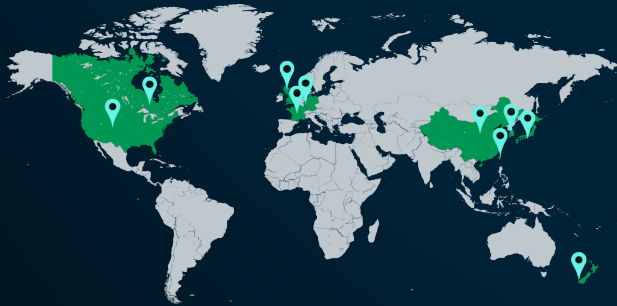
Chair Automotive Task Force, GlobalPlatform

Chair Trusted Environments and Services Committee, GlobalPlatform

Trustonic

Who Are We

- Founded by ARM, Gemalto & G&D in 2010
- Independent since 2020
- Provider of the Kinibi OS
- Deployments in 27M+ vehicles + 2Bn+ devices
- Supporting IVI, Telematics, Connectivity, Network Gateways, ADAS.
- Zero reported breaches
- Global operations and support



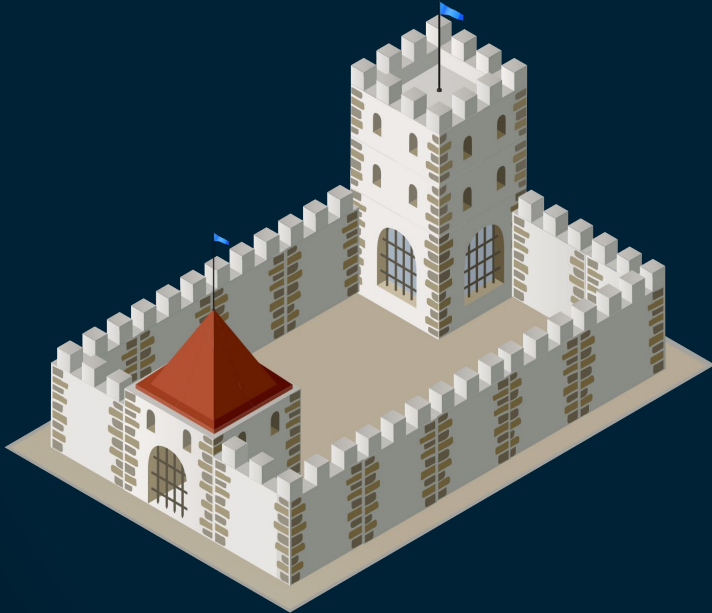
GLOBAL SILICON PARTNERS

Work with the leading SOC vendors to integrate at the BSP level

HARDWARE BACKED SECURITY: TRUSTED EXECUTION ENVIRONMENT



Trusted Execution Environments



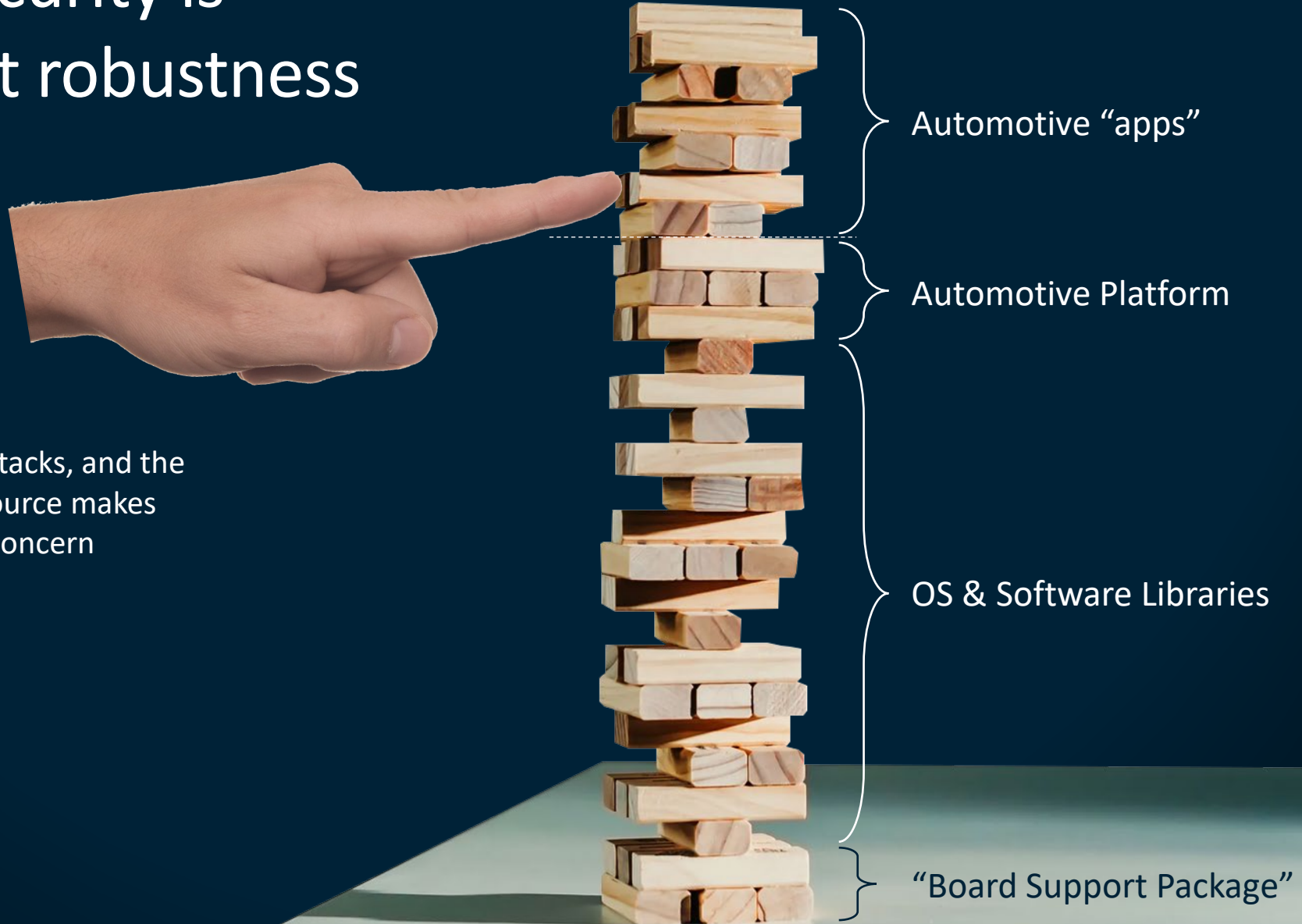
TEEs are an “environment” to run security related software in embedded devices.



Global Platform sets the standards for TEEs APIs & Protection Profiles (for certification)

Industries such as Automotive make use of TEEs to security specific applications or services

Automotive security is primarily about robustness



- The sheer size of software stacks, and the use of unsupported open source makes securing code a significant concern
- Security != Cryptography

Moving critical systems to a safe place reduces risk

- Software problems will occur
- By isolating critical systems, the scope of any impact is reduced & attack surfaces are minimized
- The TEE OS is less complex, and typically has far fewer dependencies – making it a more robust environment than a regular OS
- TEEs are designed to be certified – for example Trustonic's Kinibi TEE is EAL5+ certified

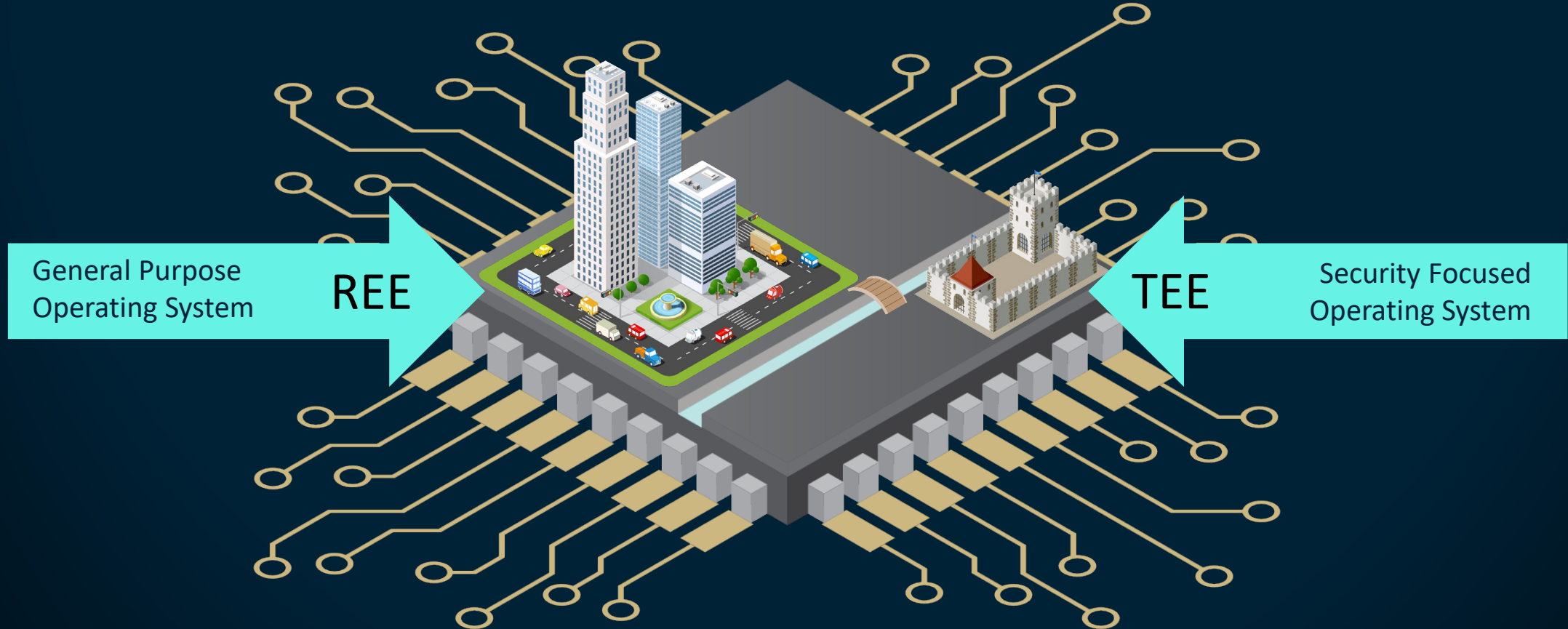
Regular OS



TEE OS

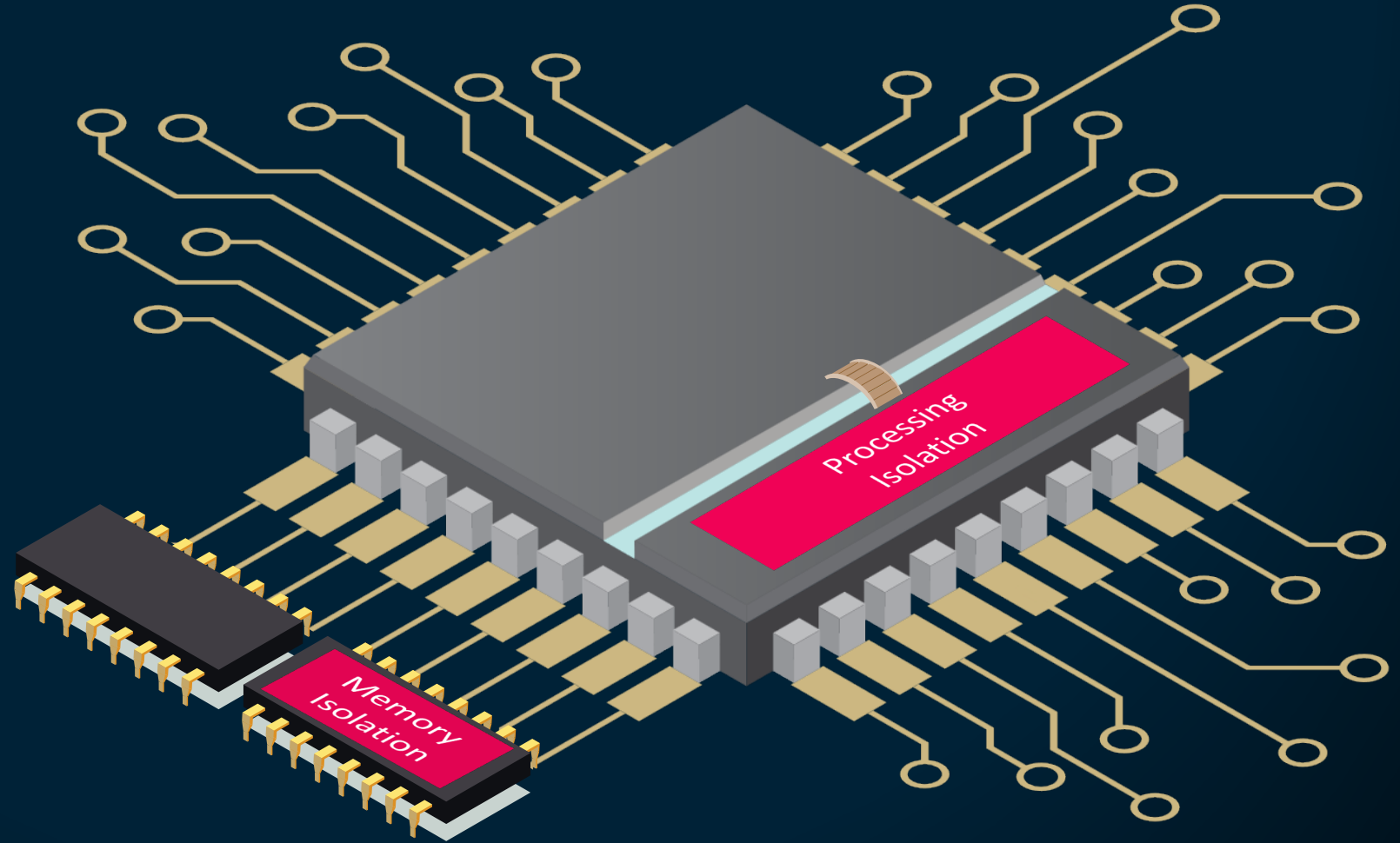


What is a Trusted Execution Environment?



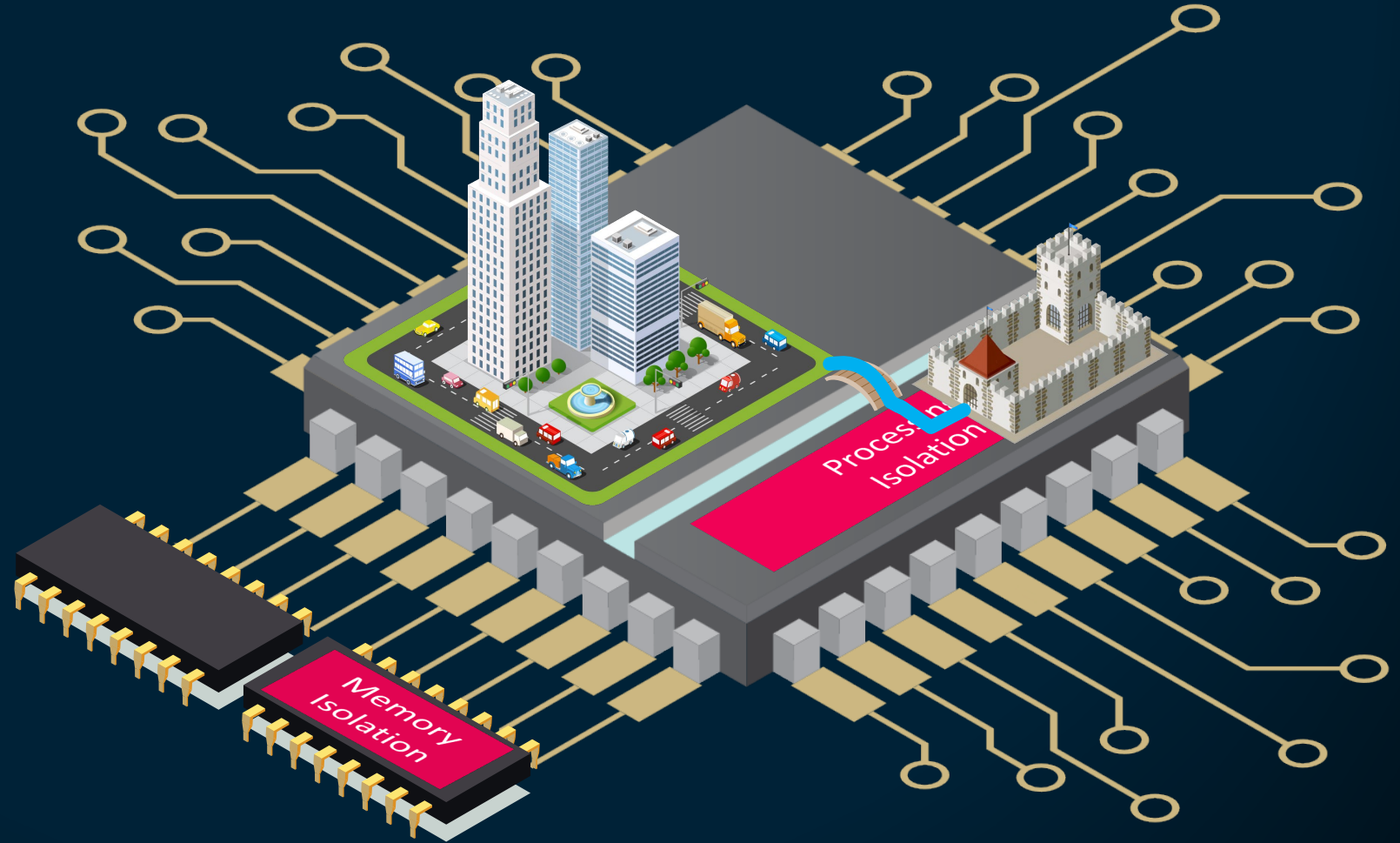
Hardware Security?

- TrustZone™ is a feature of all Arm application processors which provides hardware isolation and privileged access to security features.
- (non-Arm chips have similar solutions)



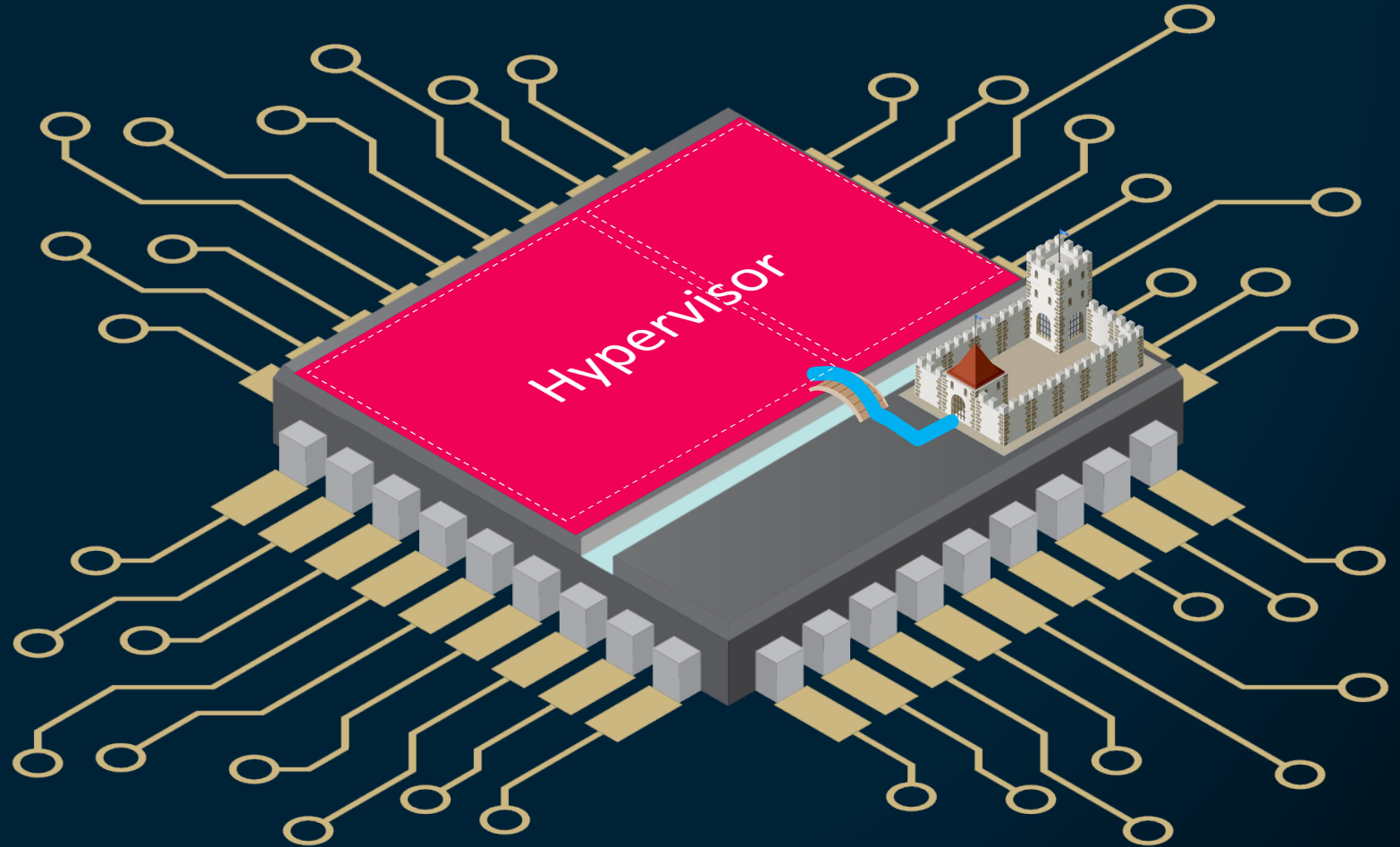
Hardware Security?

- The TEE Operating System takes advantage of this isolation to provide secure services
- The TEE is responsible for securely booting other operating systems...
- ... and then providing security focused services for them



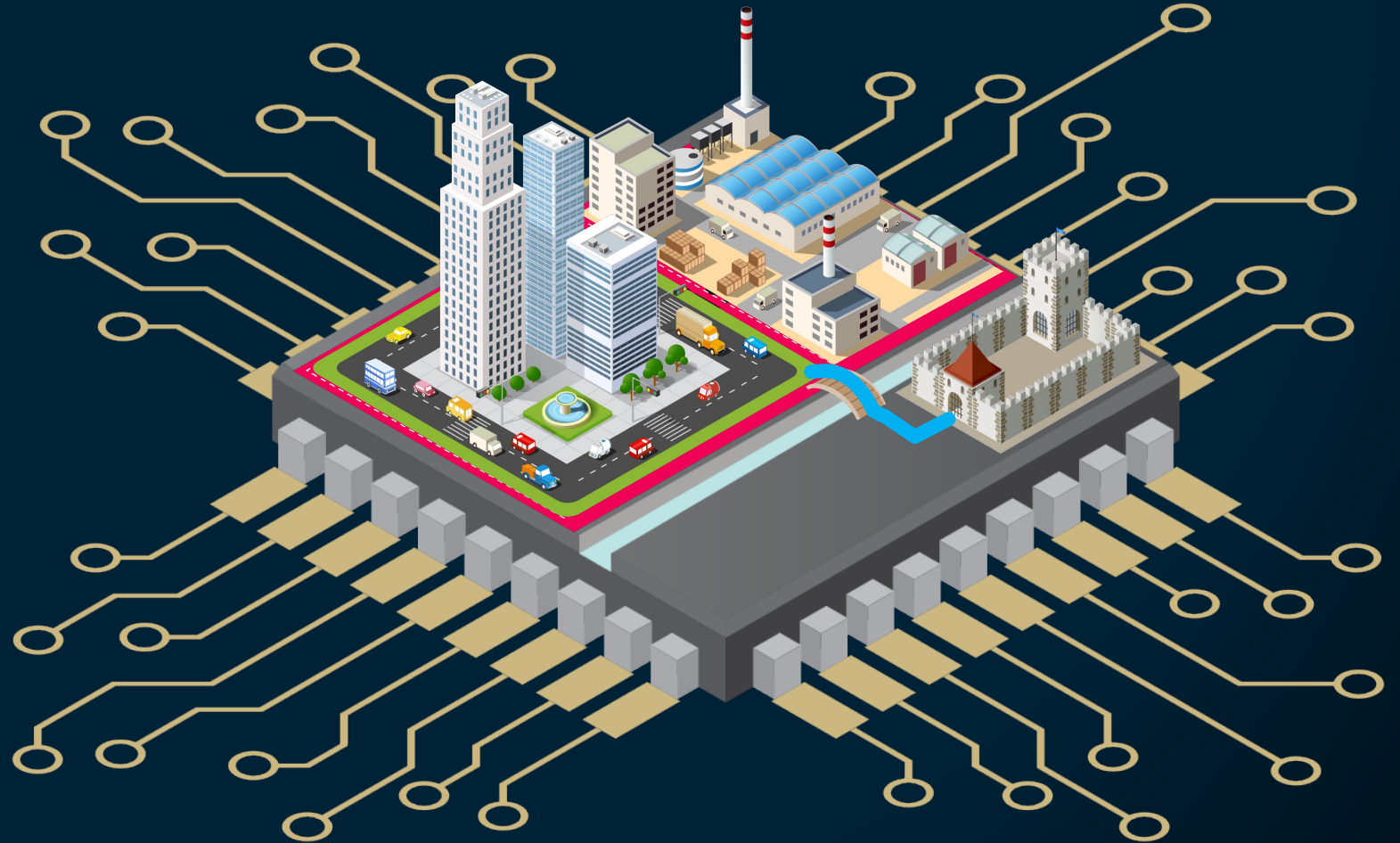
TEEs and Hypervisors

- Hypervisors enable multiple operating systems to run along side each other
- On Arm CPUs, hypervisor support is an additional mechanism alongside TrustZone



TEEs and Hypervisors

- Hypervisors enable multiple operating systems to run along side each other
- On Arm CPUs, hypervisor support is an additional mechanism alongside TrustZone

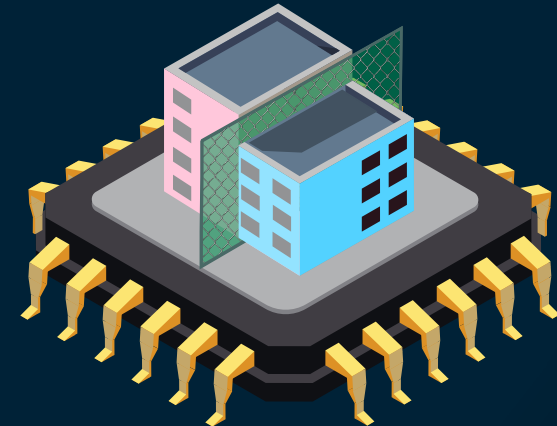


TEEs on Microcontrollers

- Microcontrollers are very common in automotive, but are far less powerful than the general-purpose CPUs that TEEs were designed for
- Microcontrollers typically run embedded software and do without complications such as virtual memory or dynamic loading.
- TEEs for Microcontrollers do exist - but are less common (and often less standard).
- Trustonic provides Kinibi-M as an embedded TEE

App

General Purpose
Partition

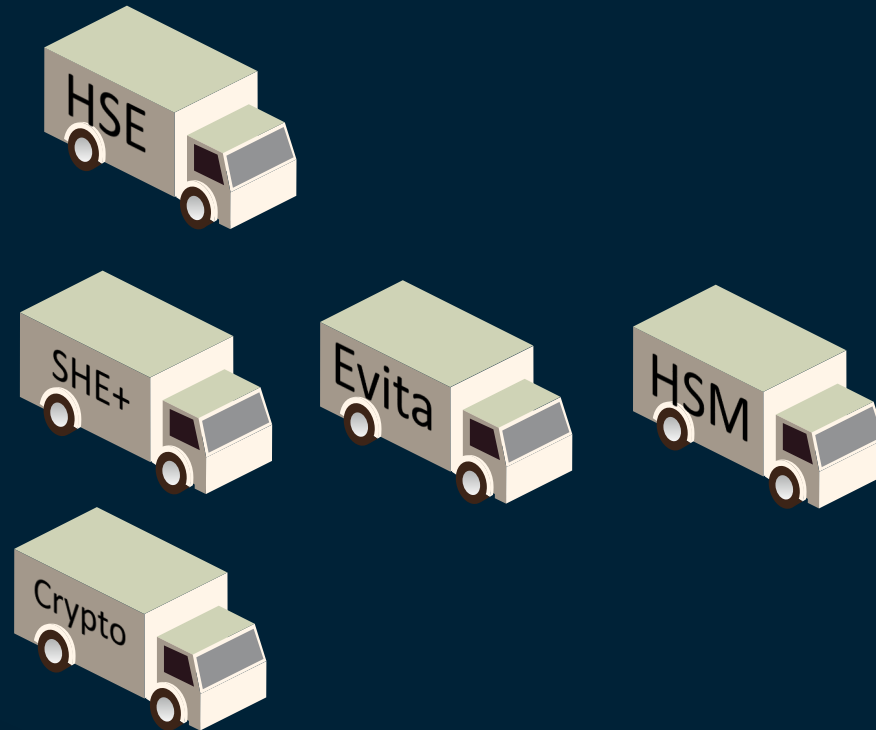


M-TEE

Security Focused
Partition

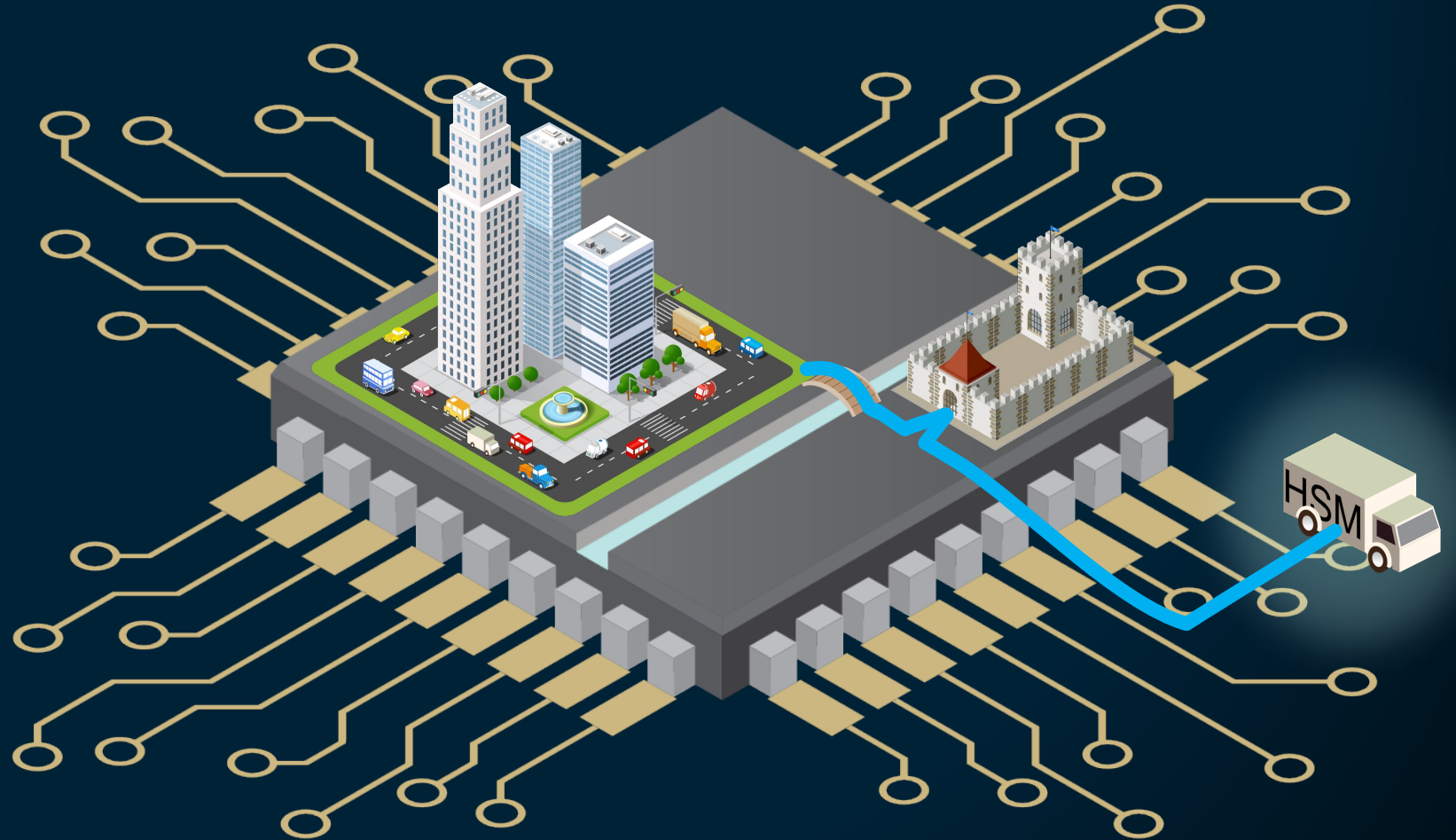
TEEs and other hardware elements

- Hardware security elements are common on automotive chipsets
- Some provide fixed function, such as 'enhanced' secure boot
- Some provide general purpose key storage
- Some provide crypto acceleration
-



TEEs + Hardware Keystore

- Hardware keystores are common in Automotive
- They often have high crypto performance – but this is limited by the relatively slow connection to the CPU
- A common pattern is to use a HSM for private key storage, and a TEE for broader functions such as key management/access control



Example System on Module with HSE + TEE Support

An example (i.MX 8/9)

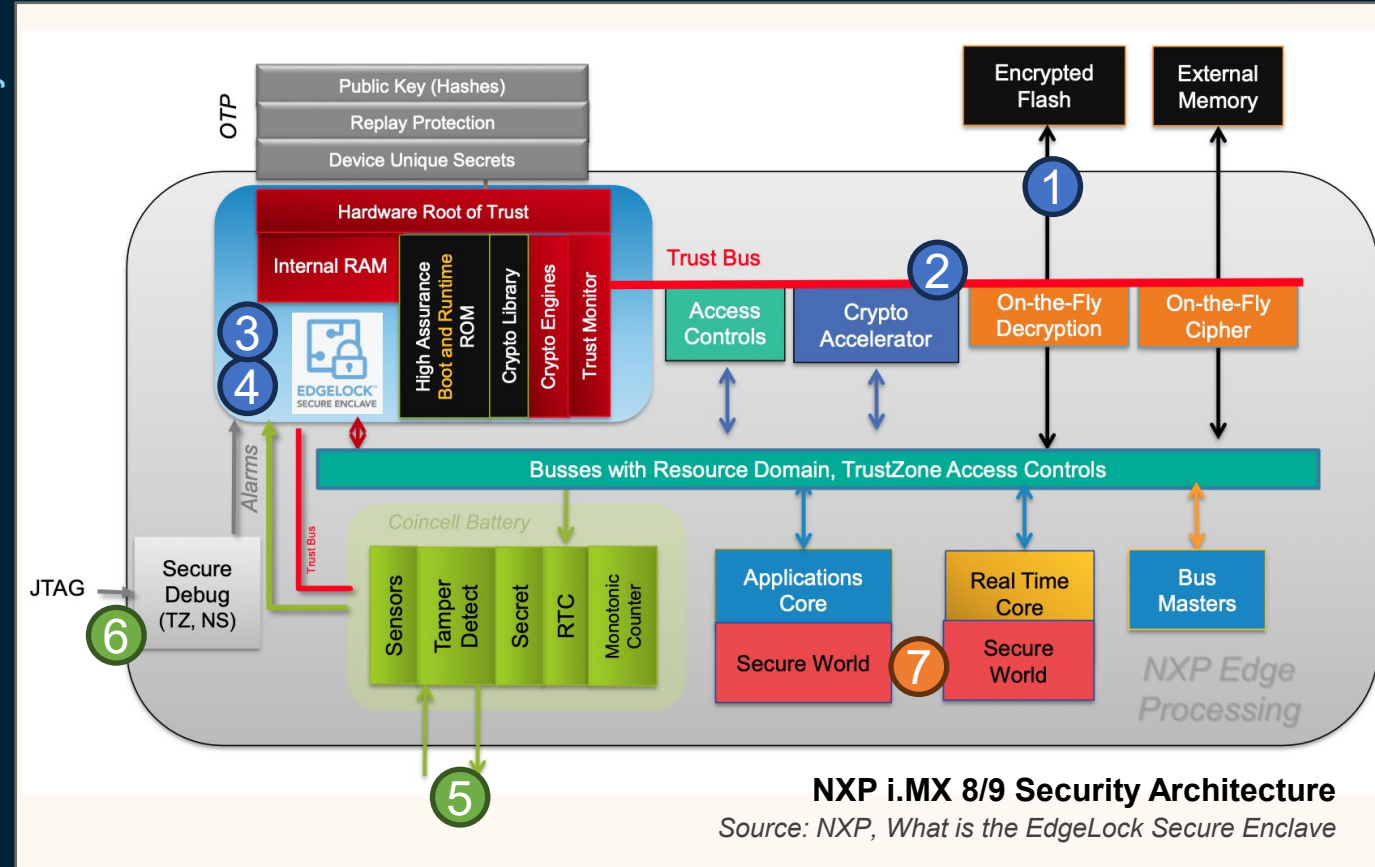
- 1 Secure Boot / Encrypted Boot
- 2 Cryptographic Accelerator
- 3 Key Storage
- 4 Unique Device Identification
- 5 Security Monitoring (Tamper)
- 6 Processor & IO Locking (Debug)
- 7 TrustZone (TEE support)



Platform Security

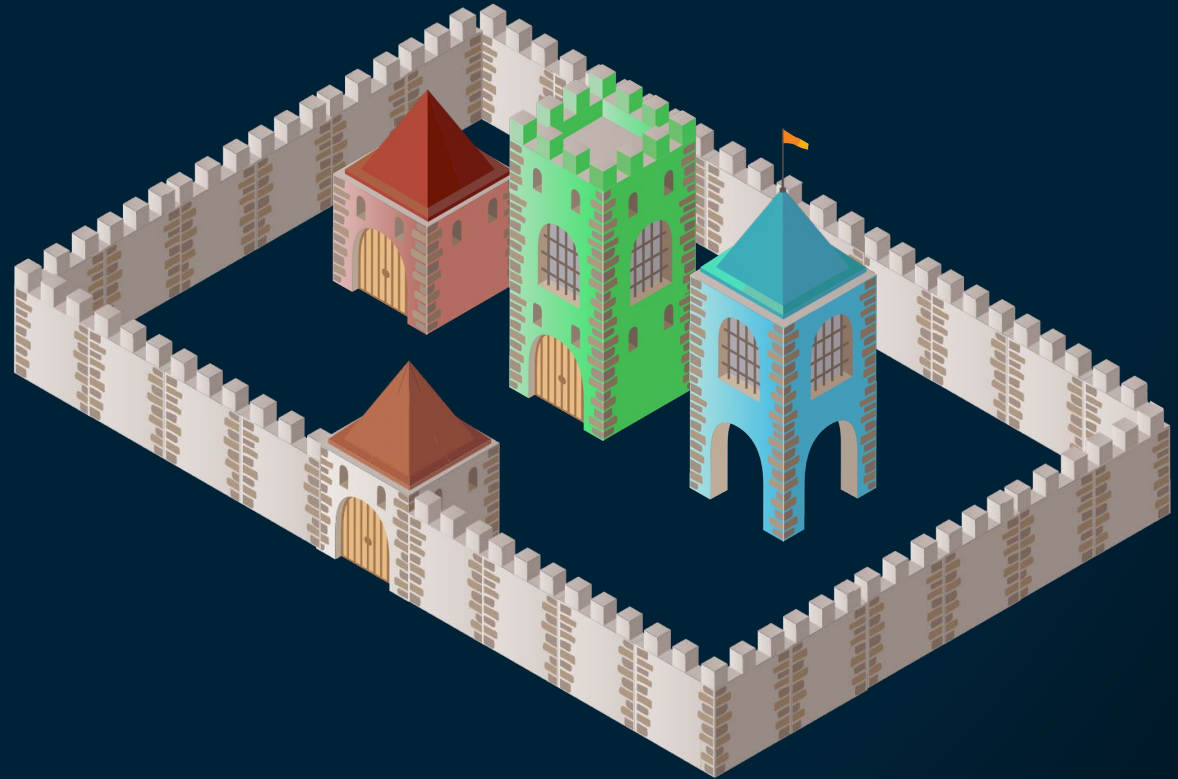
Lockdown

Application Security



Inside a TEE

- TEEs can run many trusted applications (TAs)
- Each is isolated from each other and has its own private storage
- Trusted apps can also communicate in a controlled way
- The TEE isolates the trusted application from the details of the chipset it runs on
- This makes TEE-based solutions modular and reusable



Automotive Standards

OEMs care about type approval, and there are major changes in what is required.

- UNECE 155 makes the OEM responsible for cybersecurity
- ISO/SAE 21434 gives more detail on the “what”
- SAE J3101 (Hardware Security for Ground Vehicles) is another level of detail but is still abstract

GlobalPlatform and SAE have been working together to add the “how”

- The next (?) version of J3101 will show how Trusted Execution Environments can be used to meet the requirements of J3101
- This should make it easier for products to be validated
J3101 → ISO 21434 → UNECE 155 → Regional Type Approval

Automotive Keystore – SAE J3101

SAE are working on update to J3101 to include GP mapping

SAE WIP to be balloted Internally in September

Will enable vendors to build J3101 compliant solutions using GP tech

[Someone] could define a successor to SHE++/ HSM / EVITA using TEE

[Someone] could define SESIP security profiles for SE/TEE J3101 Keystore



Key Use Cases for Automotive



IVI / Digital Cockpits

- Cryptographic Key protection
- Android Compliance
- Level 1 DRM Support
- Protecting user profiles and data



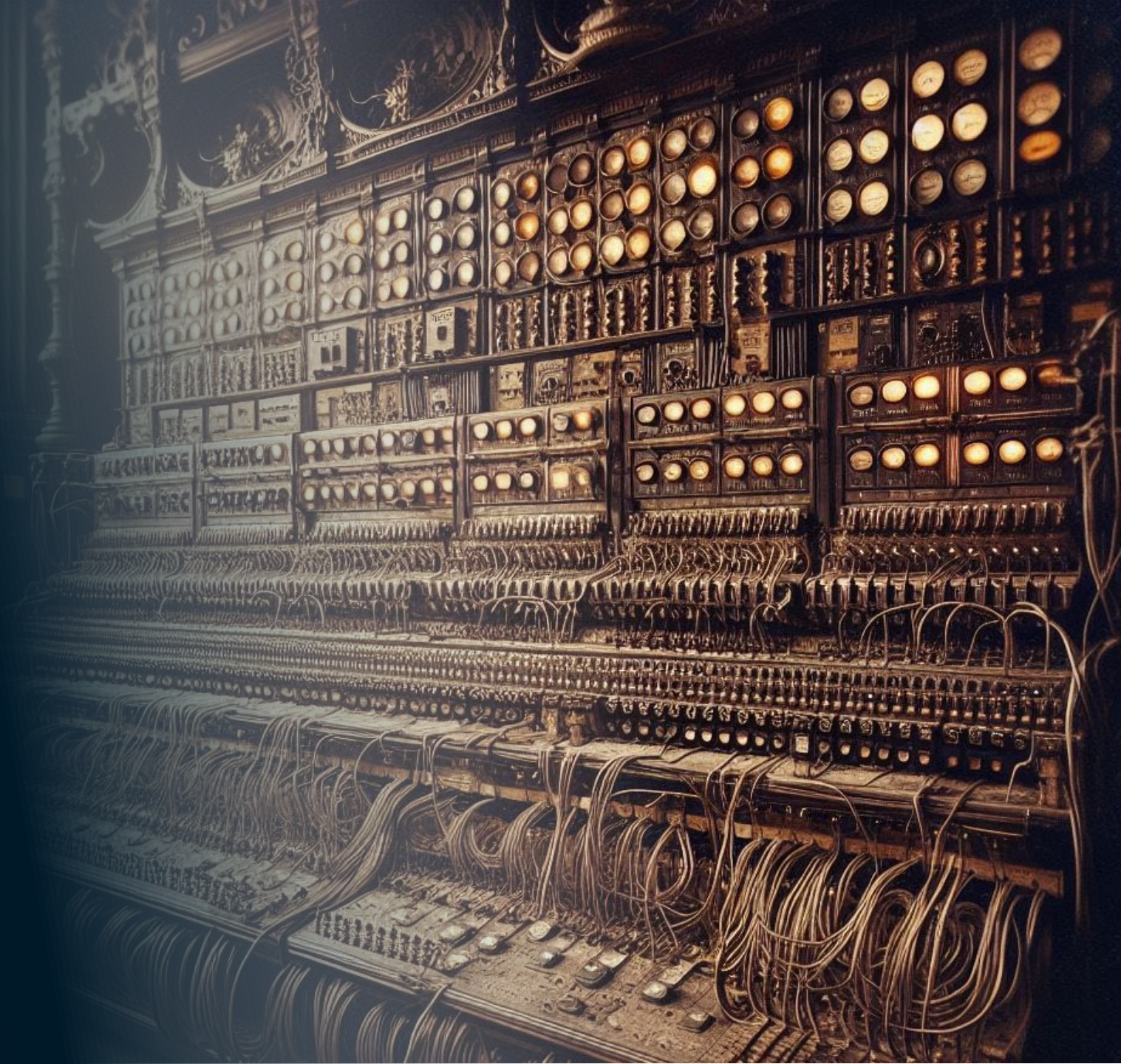
Connectivity

- Cryptographic Key protection
- Secure communications
- Attestation
- Securing OTA

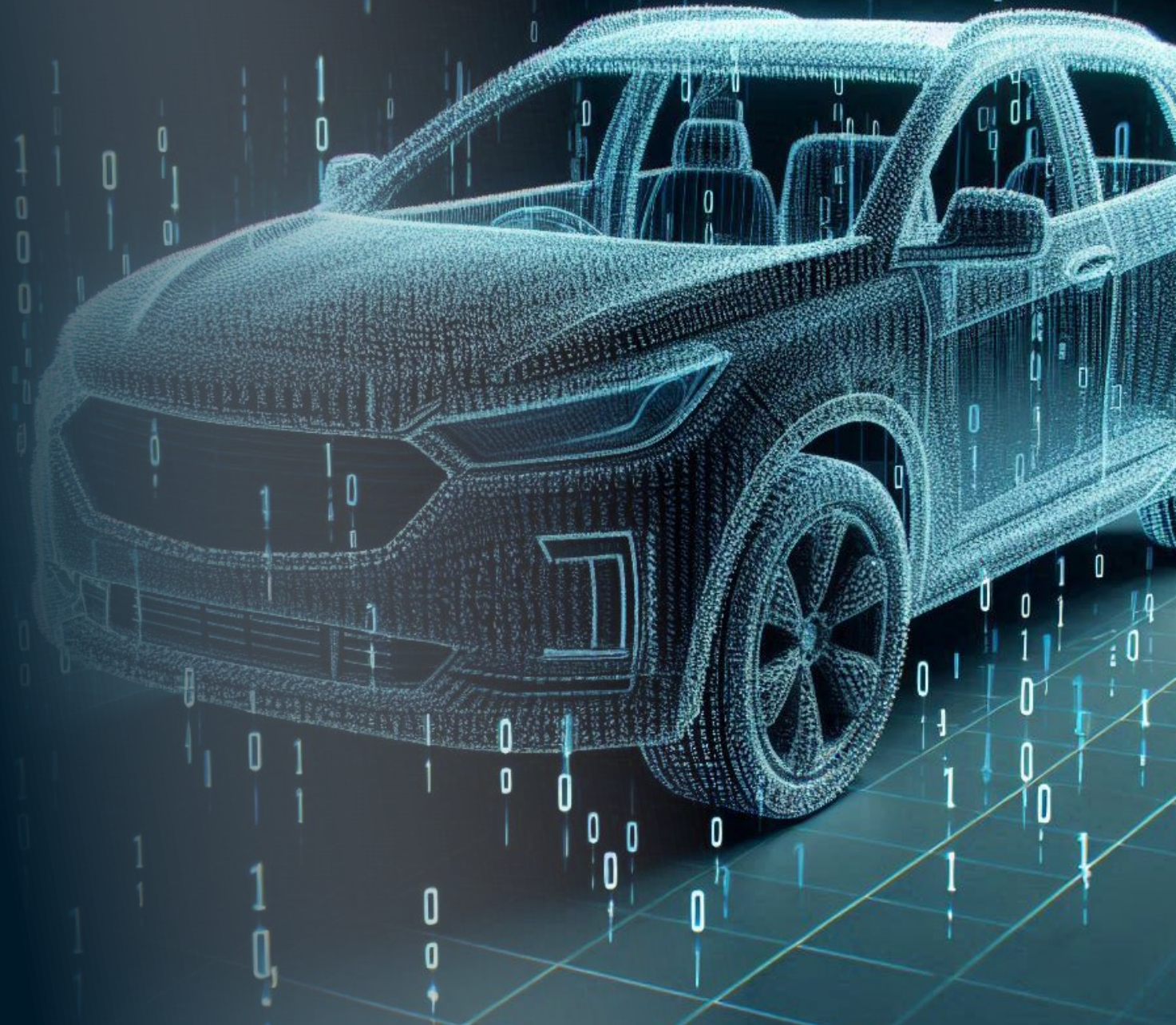


Network Gateways

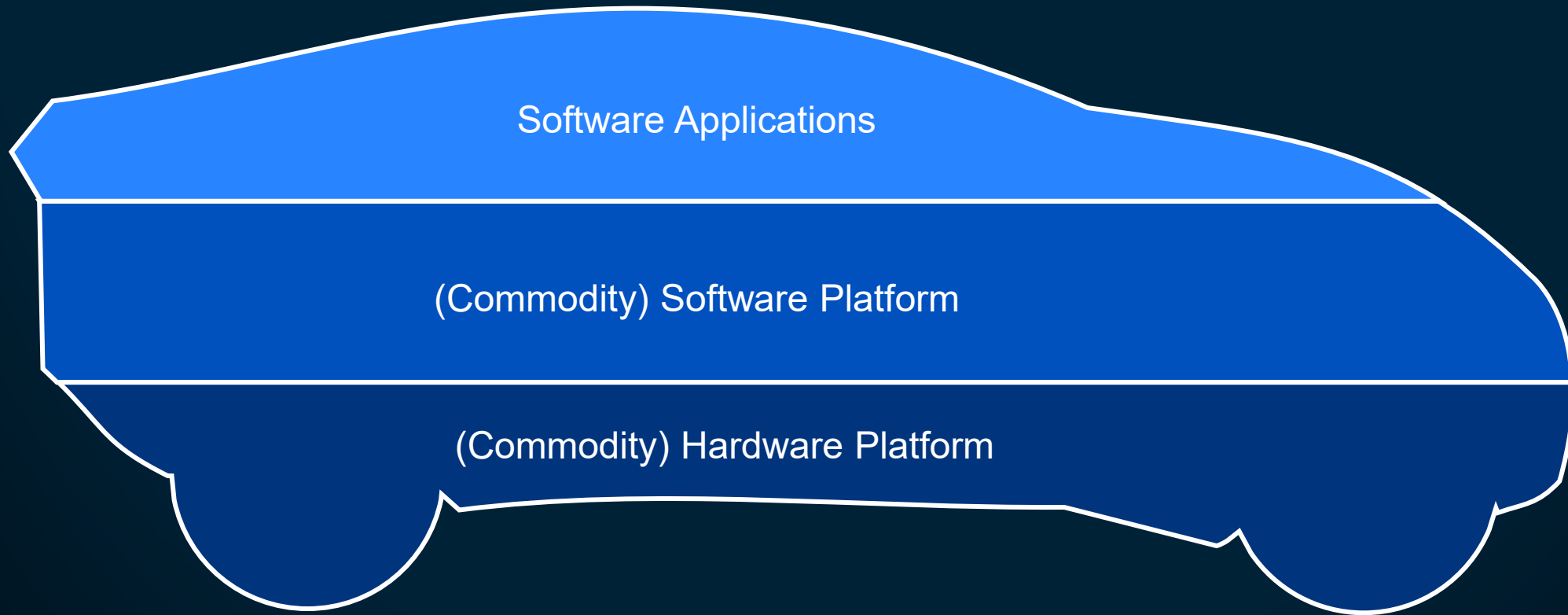
- Zero Trust In Vehicle
- Configuration Management
- Logging & Audit
- IDPS



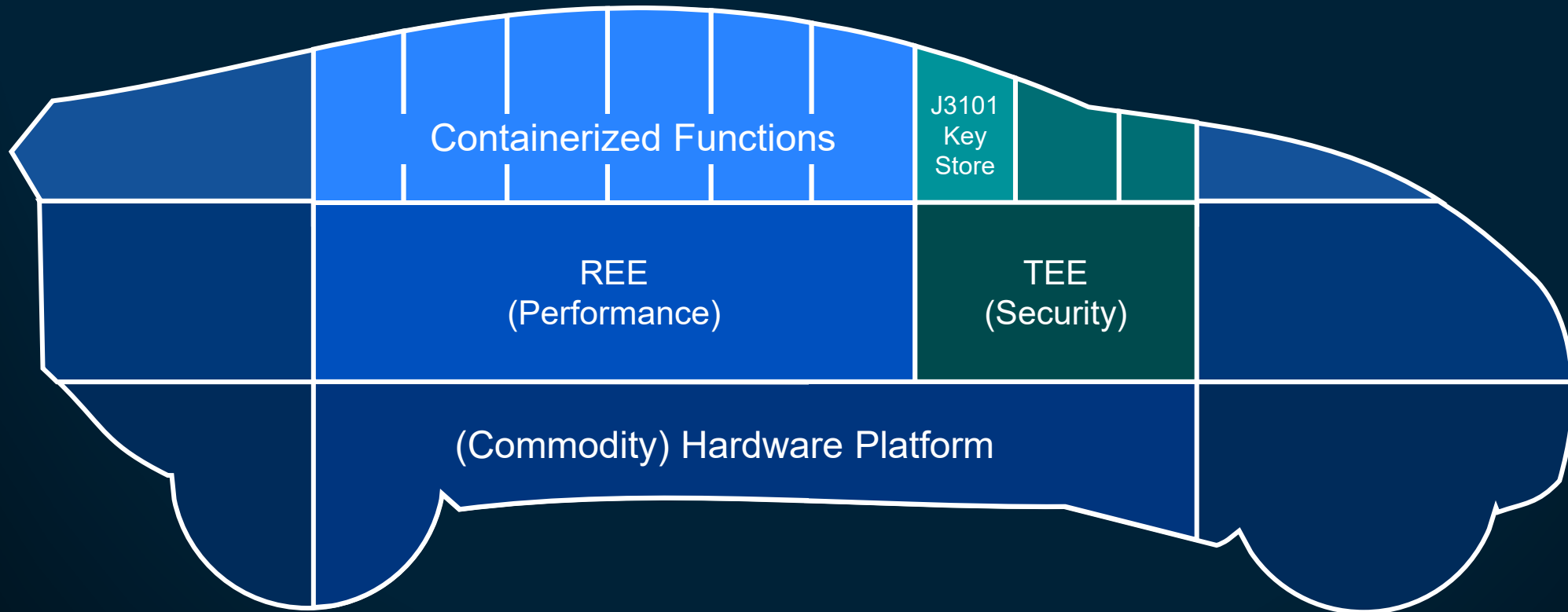
Software Defined Vehicles



SDV Concept



TEEs and the Software Defined Vehicle



Initial focus on domain/zonal controllers

Summary

- Global legislation and data opportunities means a renewed focus on software security
- TEEs provide a robust & Flexible platform for secure code execution
- Complementary to HSEs and HSMs
- In the future TEEs will be present in increasing numbers of components, enabling new use cases and vehicle wide trust.



TRUSTÖNIC

Thank You - Questions

TRUSTONIC

For more information, please contact
richard.hayton@trustonic.com

OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE
TOPICS FOR DISCUSSION?*

THANK YOU



OUR CONTACT INFO

Faye Francy
Executive Director



20 F Street Northwest
Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com



AUTOMOTIVEISAC.COM

