Global Platform®

Automotive Security Roundtable

24 October 2024, Tokyo

Agenda

10:00:00	Welcome	Ana Lattibeaudiere, CEO GlobalPlatform
10:10:00	GlobalPlatform in Japan	Eikazu Niwano, Chair of Japan Task Force, GlobalPlatform and NTT
10:20:00	Introduction to Automotive in GlobalPlatform	Francesca Forestieri, Head of Automotive
	Hardware Protections Security Environments	
10:40:00	Attack Methodology	Gil Bernabeu, CTO GlobalPlatform
11:00:00	Break	
11:30:00	Protection Profiles	Gil Bernabeu, CTO GlobalPlatform
11:50:00	Keystore: SAE J3101 & GlobalPlatform	Francesca Forestieri; Head of Automotive
12:20:00	Secure Elements as Evolution & Migration from HSMs	Laurent Tabaries, STm
12:50:00	Lunch	
14:00:00	OEM Use Case	Vincent Mailhol, Woven
14:30:00	Post Quantum Cryptography Updates	Olivier Van Nieuwenhuyze, ST
15:00:00	TEEs on automotive ECUs, mixed criticalities, spectrum: today & tomorrow	Trustonic, Richard Hayton
15:30:00	SBOM in Automotive	Dennis Kengo Oka, BlackDuck
16:00:00	SESIP Certification as a means to generate artefacts for UNECE 155 & ISO 21434 compliance	Jorge Wallace Ruiz, DeKRA
16:30:00	Invitation to Japan Task Force	Eikazu Niwano, NTT

Global Platform™

おはようございます”
(ohayou gozaimasu)
for “Good morning,

ùはじめまして
(Hajime mashite) Nice
to meet you

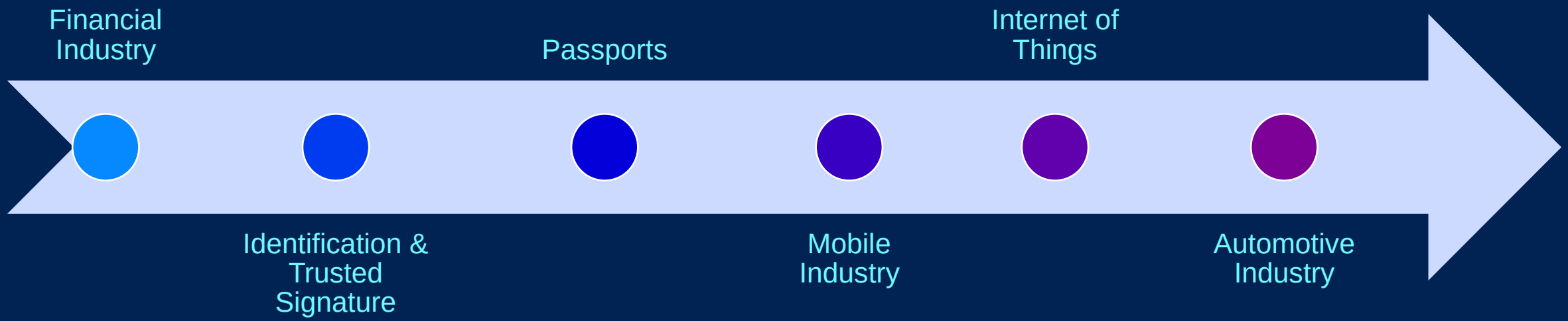
お疲れ様です
(Otsukaresama desu)
‘thank you for your
hard work in coming to
meet with us’

Ana Lattibeaudiere, CEO

GlobalPlatform

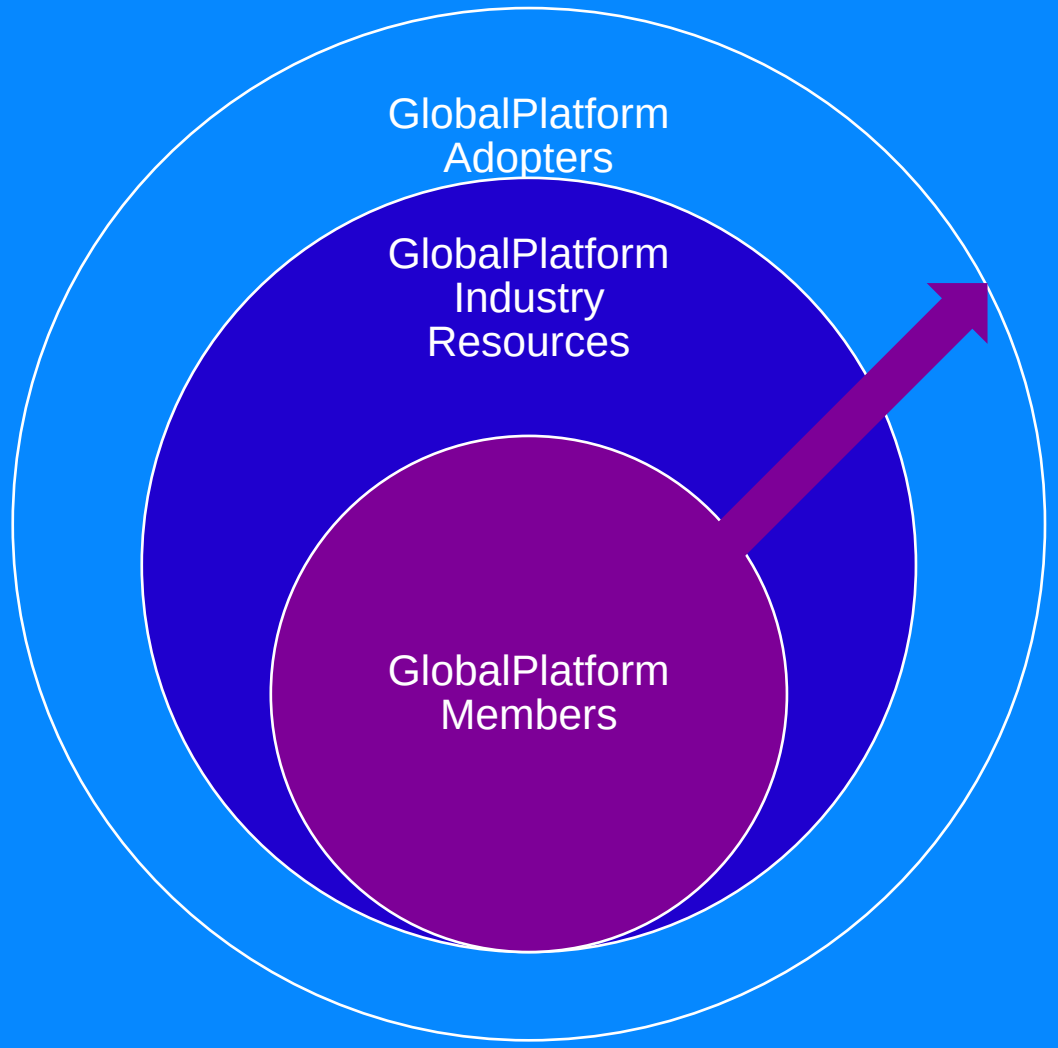
THE standard for managing applications on secure chip technology, with over 20 years of experience

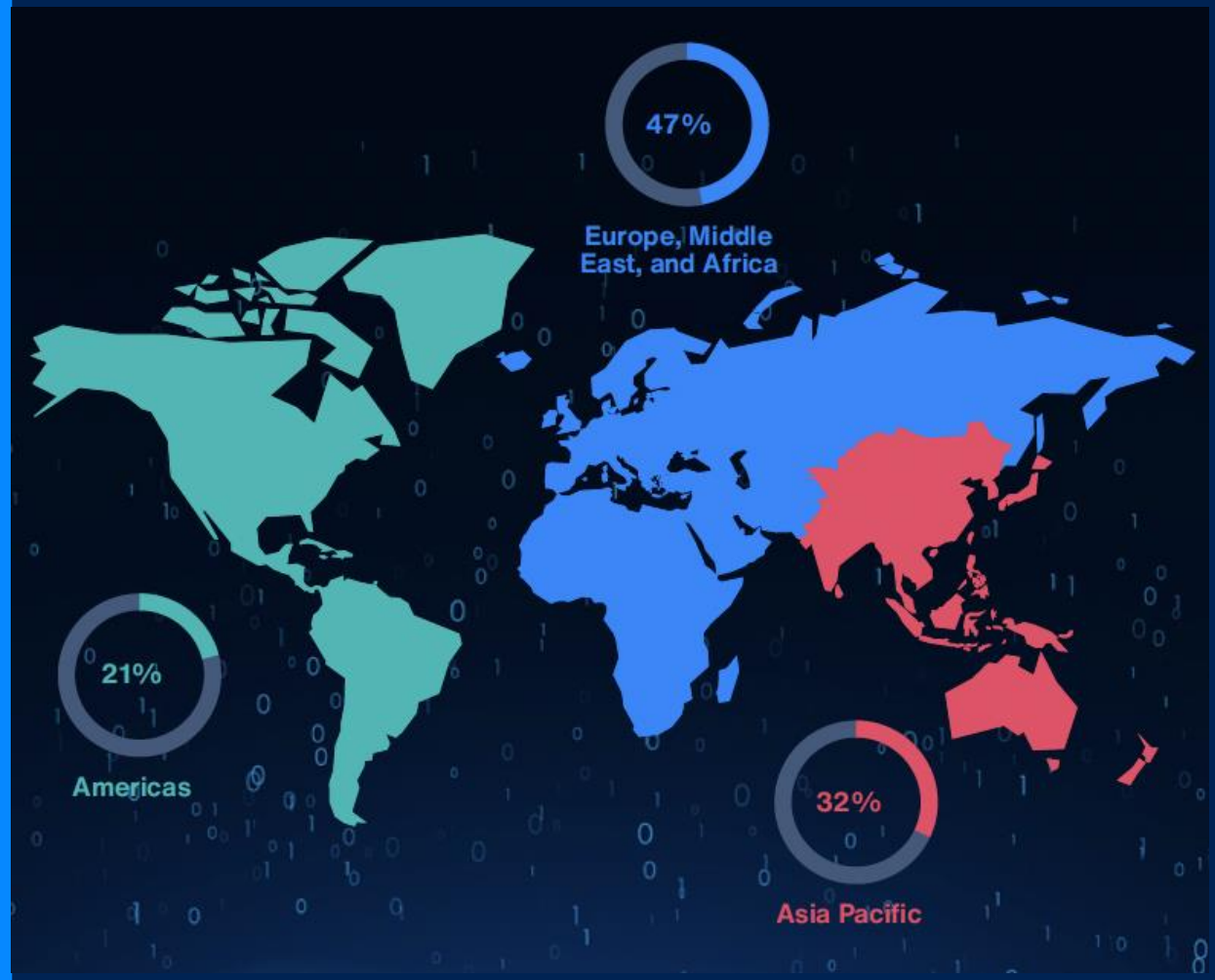
- **62 billion+ Secure Elements shipped worldwide are based on GlobalPlatform specifications**
- **Over 15 billion GlobalPlatform-compliant Trusted Execution Environment in the market today**



With 89 Members, covering Silicon Providers, Software, Automotive Industry, Governments, Laboratories around the world

GlobalPlatform's Market Adoption





GlobalPlatform Specifications: Royalty Free Use: https://globalplatform.org/specs-library/

Our Members

Full

ANALOG DEVICES — AHEAD OF WHAT'S POSSIBLE™
Apple
arm
Bundesamt für Sicherheit in der Informationstechnik
BCTC 银行卡检测中心 BANK CARD TEST CENTER
T··
ERICSSON
fime
Google
galitt — a Sopra Steria company
G+D Mobile Security
HID
HUAWEI
IDEMIA — augmented identity
infineon
mastercard
NTT
NXP
ORACLE
Qualcomm
SAMSUNG
life.augmented
T-Mobile
THALES
TRUSTONIC
verizon
VISA
winbond

Participant

Applus+
COMPRION — Test it. Prove it. Move it.
DEKRA
DNP
OPUS Lab
HONOR
財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY
orange
riscure — Challenge your security
SERMA — SAFETY & SECURITY
SGS brightsight
Quarkslab
TRUSTCB — TRUST AND VERIFY
UL Valid
woven by TOYOTA

Observer, Public Entity and Consultants

AMEX
AT&T
bdr BUNDESDRUCKEREI
CARIAD
cea leti
CB
cisco
楚天龙 CHUTIAN DRAGON 龙行天下 品赢未来
DEPARTMENT OF DEFENSE
DISCOVER
eTAS
东信和平 EASTCOMPEACE
FEITIAN — WE BUILD SECURITY
intel
JCB
kaspersky
Kigen
kona i
MASKTECH
MK smart — Smart Digital Security
PQSHIELD
Rambus
SAMSUNG
SAMSUNG SDS
上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Company Limited
SK
SPREADTRUM
synapse mobile networks
TELUS
TOSHIBA
UBIVELOX
UNISOC
xardpay
XCURE CORP.
RENESAS — BIG IDEAS FOR EVERY SPACE
BACTECH
Digital Cubes
INTERNET OF TRUST
MoneTECH
NEXTENDIS — INNOVATION CONSULTANCY
SAFEPAY
zwipe

GlobalPlatform Collaborative Partners

GlobalPlatform's Success in International Digital Security Services

Publicly available on a royalty free basis

Protection Profiles

- Common set of security needs
- "I want" this level of security

3rd Party Certification

- A mechanism to provide Vendors the ability to make claims regarding their security products
- I "Provide"

Common Criteria definitions source: https://commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf

Global Platform™

GlobalPlatform in Japan

Eikazu Niwanosan (NTT)
Japan Task Force Chair
Board of Directors

Associations in Japan among GP Partners

- Expanding Smart Card/ID to Consumer Device and Automotive Industries
- Accelerate Collaboration with Foreign based Associations

Mission of JTF (Japan Task Force)

JTF was:

- established in 2011
- Being a pilot for fiscal year 2012
- Official Task Force in 2013

10th Anniversary + 1 :
Beginning Year of New Decade

Purpose

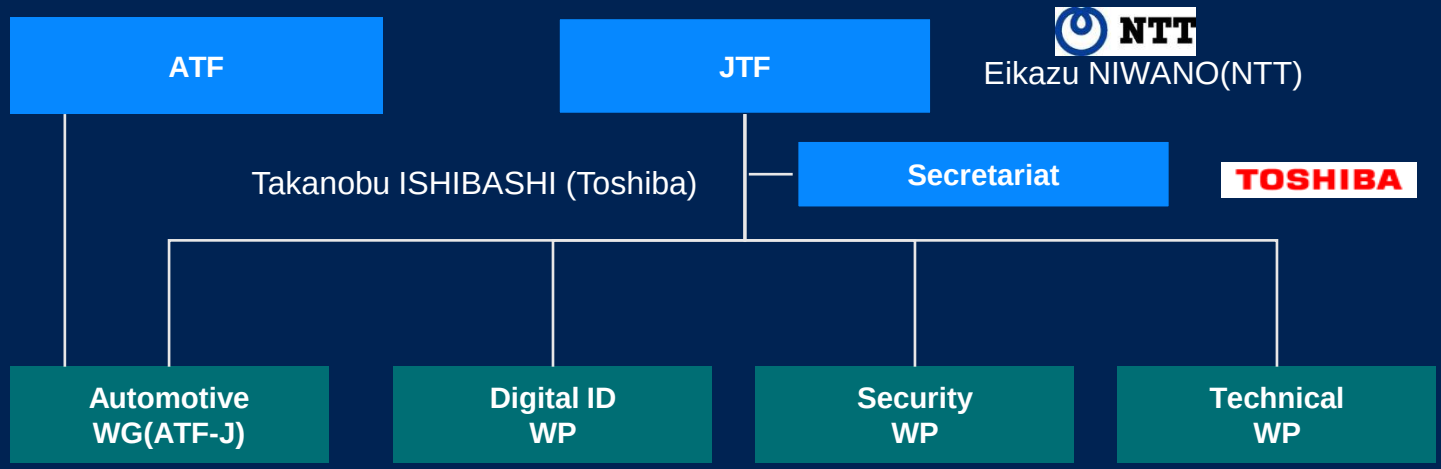
Create a forum where Japan's GP members can gather to **discuss business and functional requirements for specific market sectors within the region**

To share those requirements with GlobalPlatform through the Task Force and Advisory Council process

To obtain current information from, and directly interact with, GlobalPlatform executives

JTF Organizational Structure

- According to the structure of GP Headquarters
- Consists of Working Group and Work Program
  - Working Group: for strengthen promotion with chair
  - Work Program: for information sharing basically



Regular Members

NTT TOSHIBA FeliCa Networks DNP ORACLE TRUSTONIC THALES

- Members; **49 persons** from **18 entities** (including GP dedicated organizations and staffs)
- Entities other than regular entities (including GP dedicated organization and members)
  - **Alliance management**
  - **FIME**
  - **GlobalPlatform (Dedicated Staff)**
  - **Google**
  - **IDEMIA**
  - **JCB**
  - **NXP**
  - **PQShield Ltd.**
  - **Qualcomm Technology**
  - **Thales**
  - **Winbond**

JTF Activities

Technical Study

- GP specification analysis
- Domestic technical analysis

GP Proposal/Reflection to GP Document

Ad hoc Meeting

Secure Device Forum

SDF

Workshop

Hackathon

Orientation

Strategy Planning

- Regional requirements analysis
- RTF collaboration (with CTF)
- Exchange of opinions with GP executives

Regional Requirement

JTF Policy <-> RTF Policy

GP Board Request

Monthly Meeting

Regional Advisory Council

Information Sharing

- GP information shared
- Shared internal and external regional information

Monthly Meeting

TechTalk

GP technology/ Solution Map

GP Status Report

Domestic/Global Status Report

GP Document Summary

Disseminations and Deployments

- Use case analysis
- Creation of promotional tools
- Corporate solicitation
- Domestic bodies discussion
- Speech at external event
- Publication

Regional Requirement

JTF Policy <-> RTF Policy

GP Board Request

Monthly Meeting

Regional Advisory Council

Global Platform

Automotive in GlobalPlatform

Francesca Forestieri

Demands on Increased Cybersecurity in Automotive

International Automotive Targets

UNECE 155 – Cybersecurity Management Systems (CSMS)

- SAE/ISO 21434 Cybersecurity Management Systems
- ISO/PAS 5112:2022 Road vehicles — Guidelines for auditing cybersecurity engineering
- SAE J3101 Hardware Protected Security Environments for Ground Vehicles

UNECE 156 – Software Update Management System (SUMS)

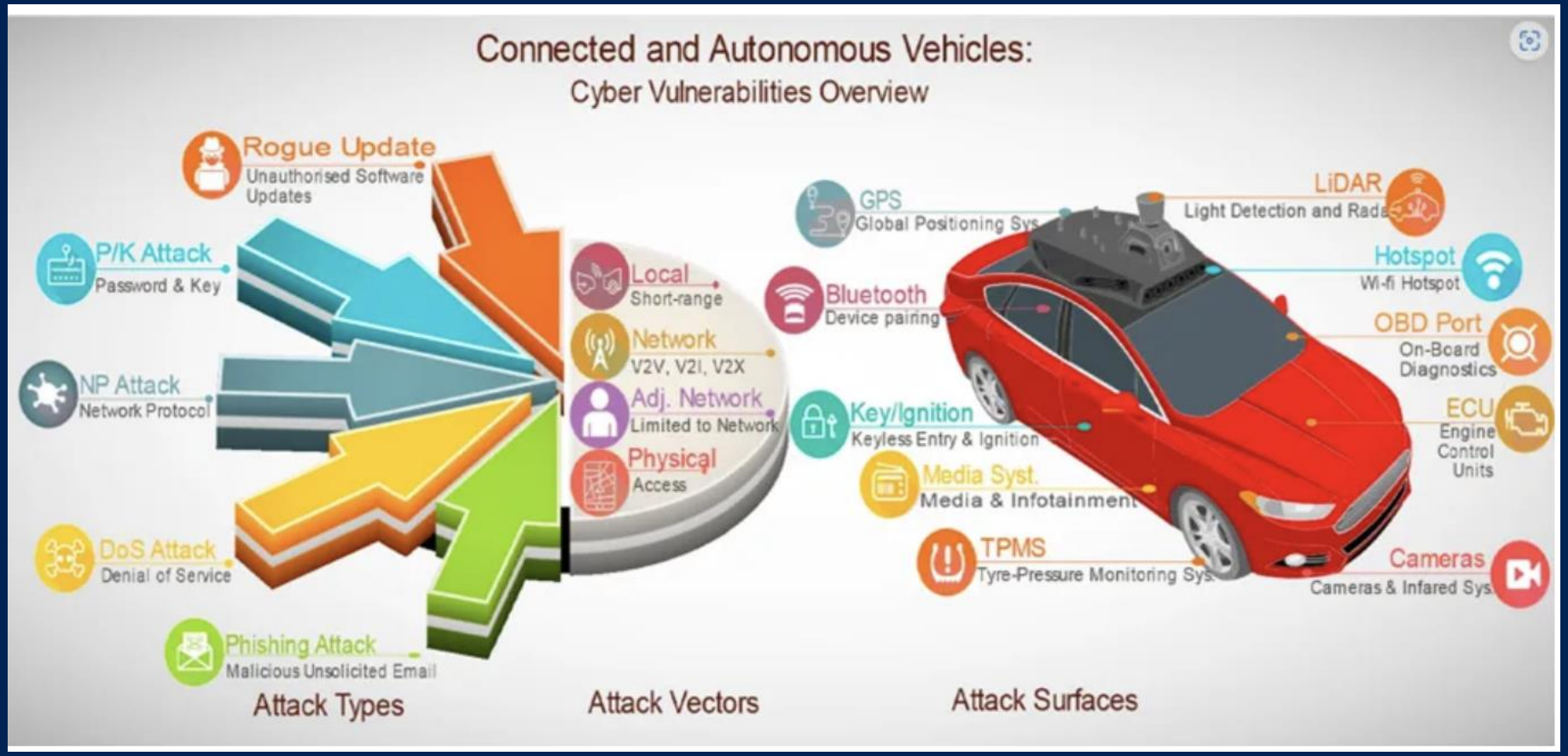
- ISO/FIDS 20489 Software Update Management System (SUMS)

Right to Repair Regulations

Relevant International Multi-Sector Regulations

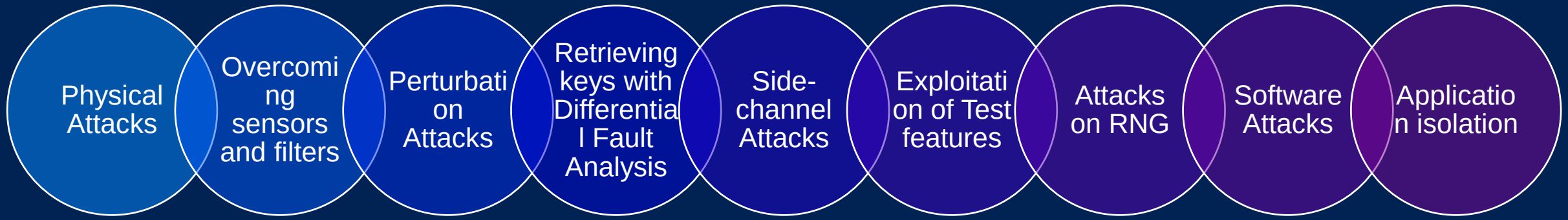
- National & EU Cybersecurity Acts
- Software bill of materials (SBOM)
- European Cyber Resilience Act (CRA)
- EU Radio Equipment Directive 2014/53/EU (RED)
- Privacy - e.g. GDPR

Move Towards Software Defined Vehicles…. Security Risks Increase

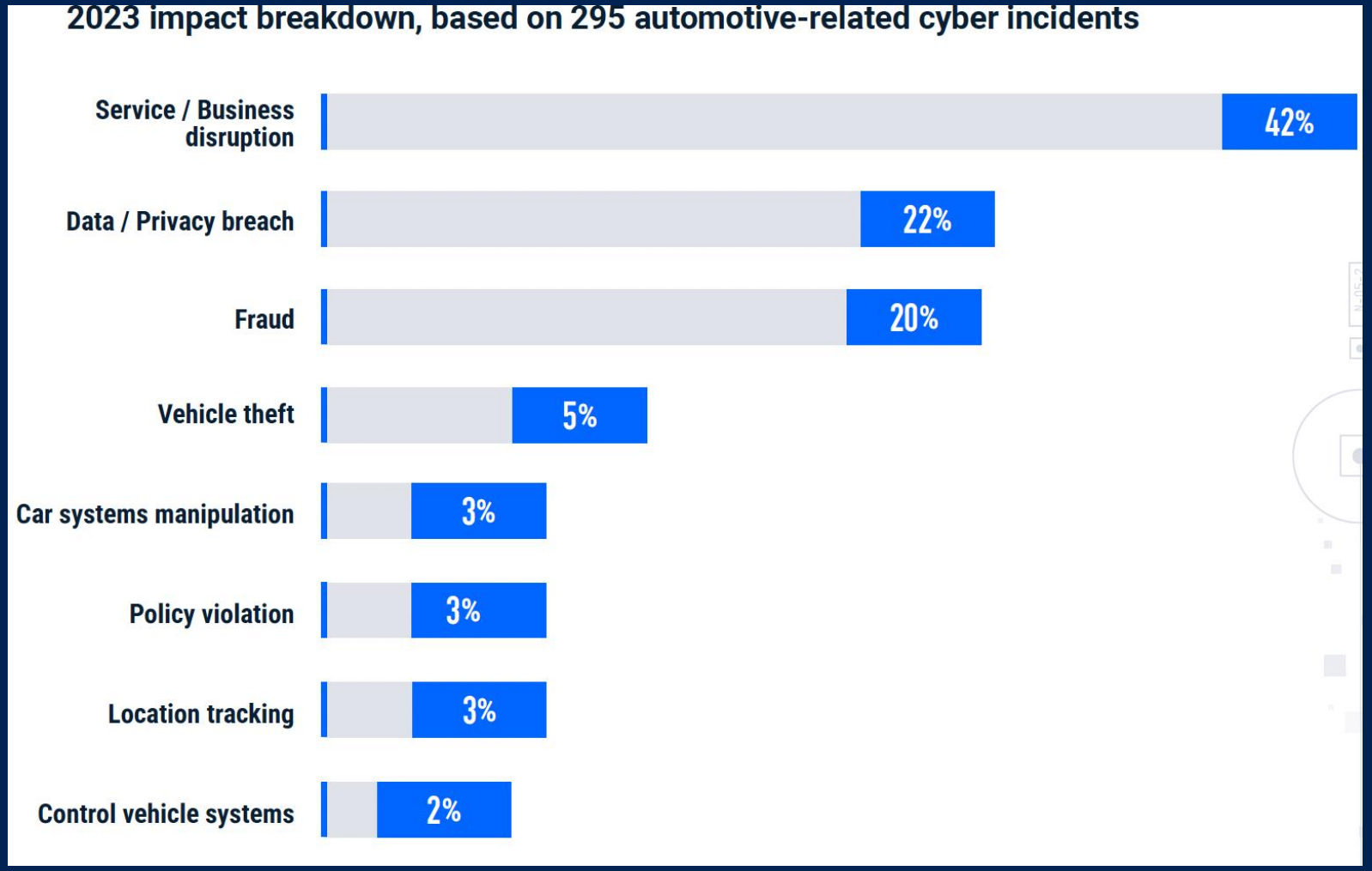


https://medium.com/@sheebz.rathi/cyber-security-in-autonomous-vehicles-c2738d186aa6

Attack Paths



What Are the Consequences of Cyber Incidents?



- Financial repercussions
- Recalls or OTAs
- Production shutdowns
- Ransomware payments
- Damage to brand reputation and customer trust
- Large regulatory fines

Source:(Upstream 2024). https://upstream.auto

Cost of Security Threats

THREAT ACTOR TYPE
White hat

FLEET SIZE
3+ million electric vehicles

Impact	Description	Baseline	Financial Impact
Vehicle Safety, Operations & Recall	Aurora Labs' cost per OTA update per vehicle by type.[13] Estimations used to calculate the OTA cost: 5 large ECUs @ 500MB; 10 small ECUs @ 0.42MB.	$0.39 for Line-of-Code Update	$1,250,000 - $2,000,000
Vehicle Safety, Operations & Recall	The cost of battery replacement for vehicles with permanent battery damage.[14]	0.01% - 0.05% of fleet impacted; $15,000 per vehicle	$5,250,000 - $26,250,000
Legal & Regulatory Compliance Issues	Class-action lawsuit litigation and settlement costs for vehicles with temporary battery damage.[15]	0.5%-1% of fleet impact; $600 per plaintiff; $500,000 in legal fees	$11,000,000 - $21,500,000
	Total Potential Financial Impact		$17,500,000 - $49,750,000

https://upstream.auto/reports/global-automotive-cybersecurity-report/

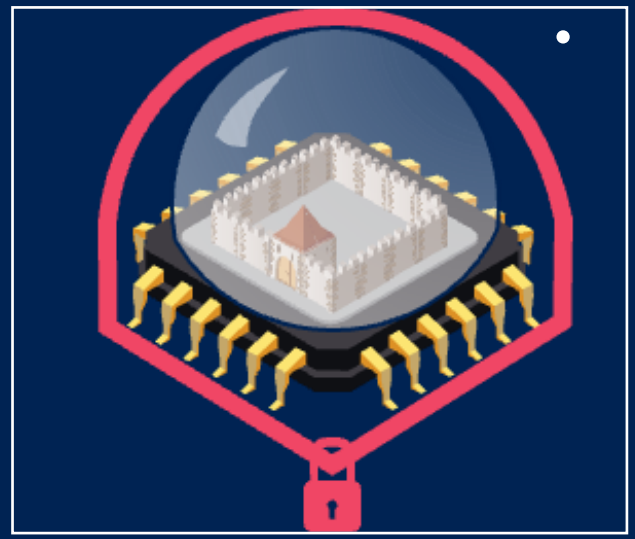
Global Platform™

GlobalPlatform Technologies

Francesca Forestieri

GlobalPlatform Foundation Technologies

Secure Element

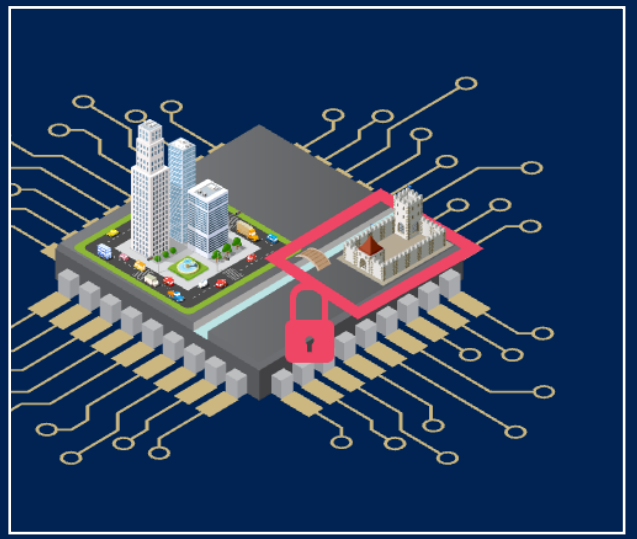


A secure enclave protected against physical and software attack

- Tamper resistant hardware
- Install, update OTA applications (not just keys)
- In OVER 192 Million Connected Cars in 2023 (Juniper Research)

https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20–%209th%20January%202023,from%20192%20million%20in%202023

Trusted Execution Environment



- A secure operating system running on a standard CPU alongside regular OS/Applications
  - Protected against attack by hardware chip features + software mechanisms
- In Over 100 Million Vehicles as of 2023 (Confidential Source)

- Runs a full operating system providing standardized APIs and functions
- 3rd party Security Certification
- Full support for App and OS update over-the-air

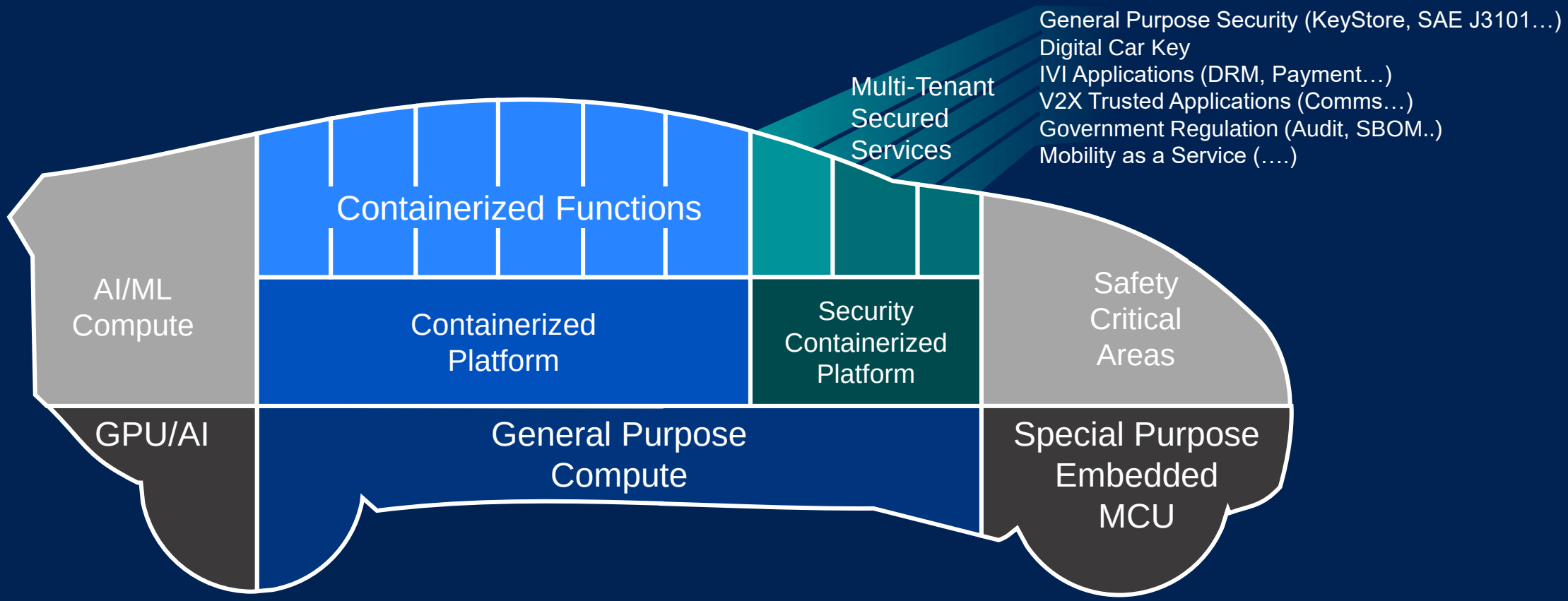
Global Platform™

Secure Components

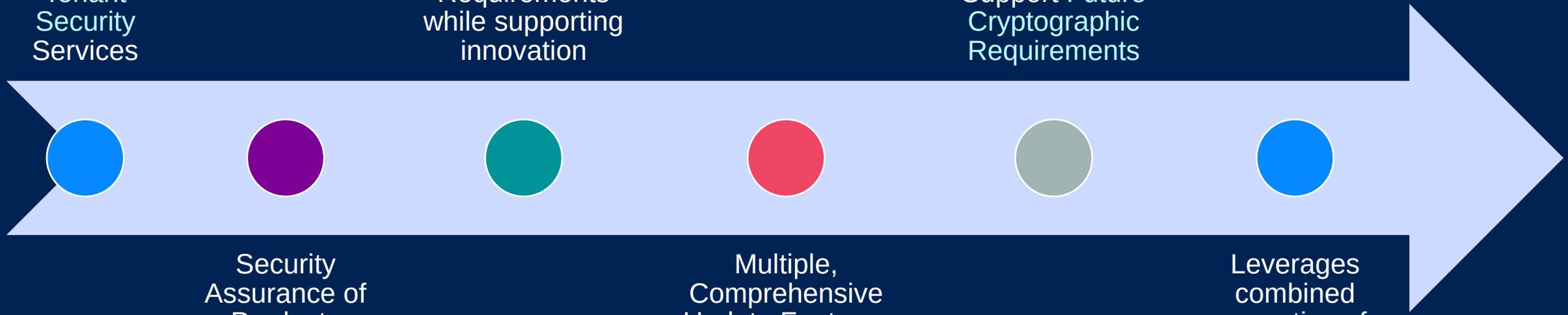
offer a standardised controlled and protected execution environment with the following characteristics:

- **Root of Trust**
  - Identification and binding that allows you to create a chain of trust based upon secure services
  - Key Injection at Production Level (part of certification of Secure Component)
- **Isolation**
  - Between the Trusted Environment vs. the Rest of the Real World and
  - Between Each Trusted Application
- **Secure Service Management**
  - From trusted applications from different actors
  - Remote update and Services to the application
- **Types of Secure Services**
  - State-of-the-art cryptography
  - Attestation (e.g. signed claim)
  - Trusted storage
  - Secure transactions and communication
  - Trusted access to peripherals

GlobalPlatform & Software Defined Vehicles:
Security is Much More than Key Stores



Securing Any SDV Service with GlobalPlatform



Why Engage in Security Standardisation (vs a solely Proprietary Solution):
Optimised Products

Lower cost of mass market produced solutions

- Better value for money as organization can focus engineering on differentiators and less on aspects that do not provide competitive advantage
- The "costs" of common features is depreciated across the community
- Leveraging common set of requirements WHILE incorporating greater sophistication on cybersecurity solutions than in the past

More Vendor Options

- Reducing vendor lock-in given portability of services
- Increased second source options

Simplified ECU development

- Reduction of Integration Costs
- Faster development of new ECU generations, given the increase in portability of common services (i.e. for non-differentiator services)

Robust Ecosystem

- Multiple Skilled Stakeholders to support service developments
- International Coverage of Multiple markets

Tailoring GP solutions for different ECU categories

Complex Multi-app ECUs

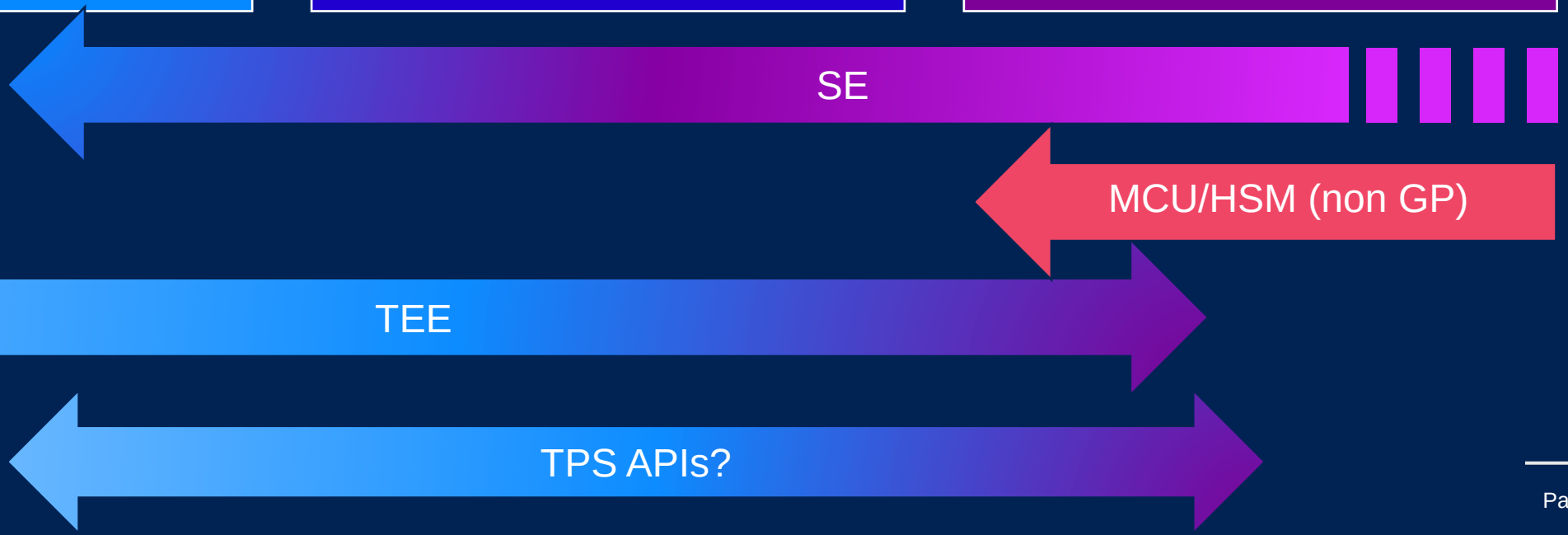
- High Performance Compute
- Real time Telematics Control Unit
- High Performance Compute IVI
- High Performance Compute ADAS

Multi-app ECUs

- Zonal Control Units

Embedded ECUs

- Actuation & Control with CAN /CAN Flexible Data-rate
- Often Safety Critical (ASIL-D)



Why HPSE Standards in Automotive are Critical For Future

Francesca Forestieri

Despite All The Risks…..

Software Defined Vehicles Need Collaboration to Be Successful

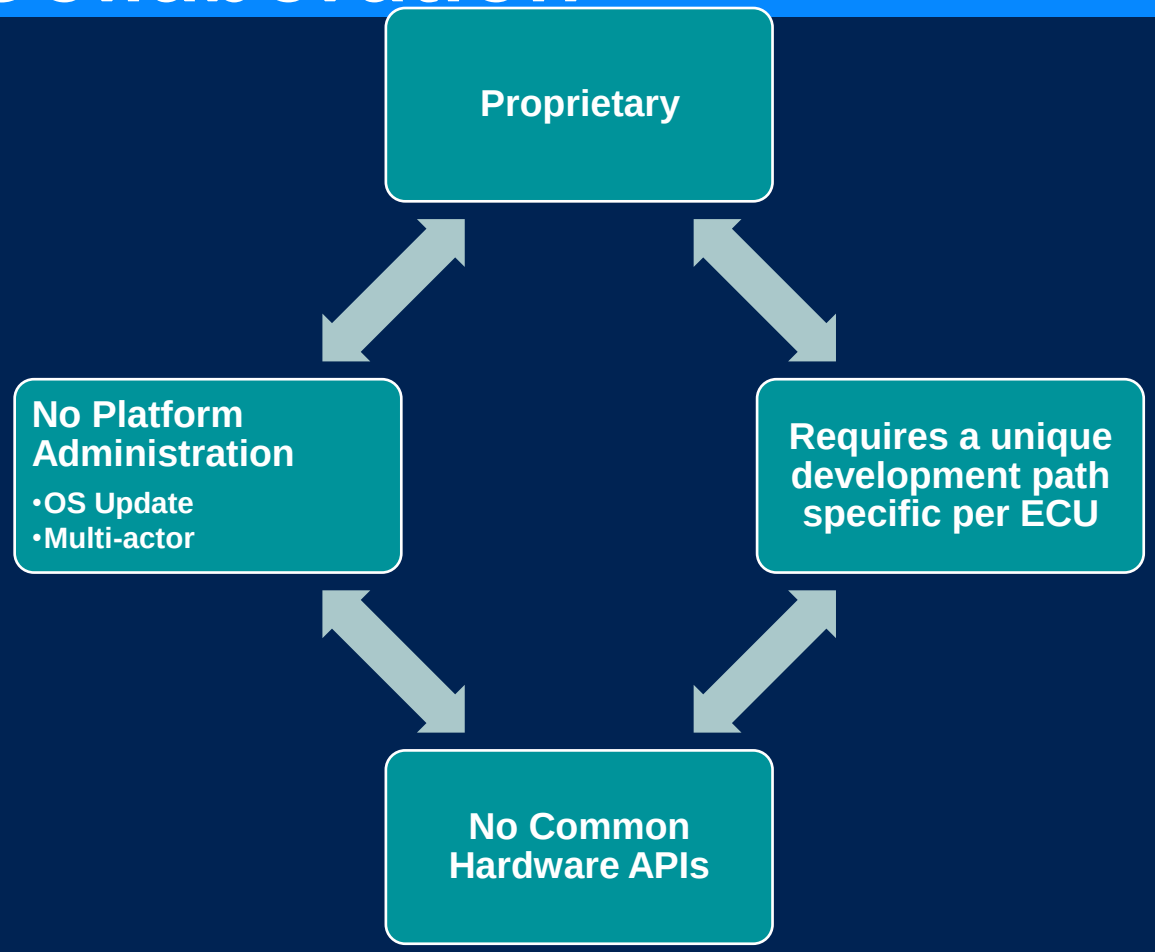
Traditional Automotive Hardware Protected Security Environments: Do Not Foster Collaboration

HSM:
- Hardware Security Modules

SHE:
- automotive Microcontroller Unit (MCU) by HSI

Evita
- Fragmented proprietary HW APIs

SHE+



Emerging Market Demands: Hardware Protected Security Environments

Moving beyond proprietary key stores…Standardised Flexibile Solutions

- Cybersecurity
- Secure Boot
- Secure Logging
- Key Negotiation
- Etc.

Define common security requirements

"Common" non-differentiator security requirements

while leaving room for differentiating security and other value – add services

Build Using standardised specifications

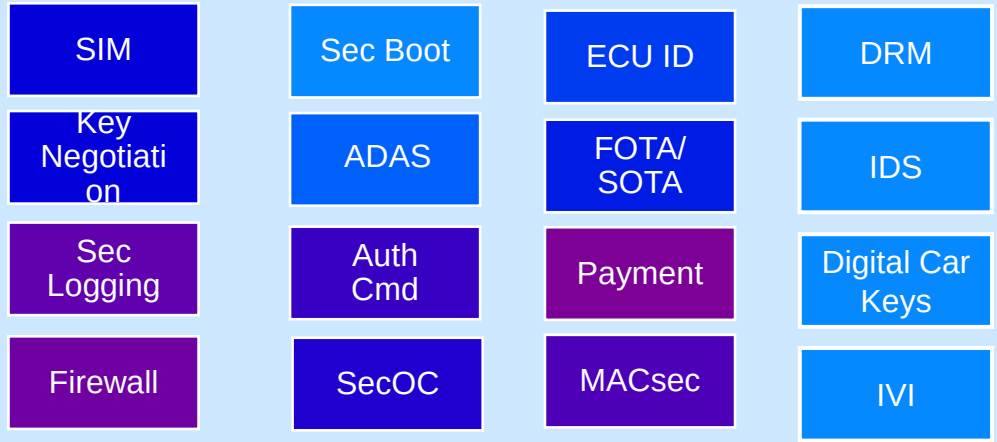
- Enables Interoperability
- Has standard HW APIs
- Facilitates Trusted Application Re-use

Resulting in

- Portability of trusted services across vendors (second sourcing options)
- Flexibility so as to develop post-production security services
- Not having to develop and maintain platform services since GlobalPlatform directly maintains the security platform and tools
- Incremental design of services possible across different ECUs (not starting from scratch)
- First opportunity to independently certify solutions

GlobalPlatform Approach

2. Trusted Applications/Applets developed/ deployed by the ecosystem, to meet the specific requirements of a particular ECU or a customer solution using standardized APIs



1. Platform: Standardized APIs & Management command, update, state-of-the-art crypto, crypto agility …

Secure Component Platform:
Functionally and Security Certified

Hardware

This approach fits well with Software Defined Vehicles with upper layer security certification

Standardisation Enables Choice: Fit for Purpose

Configurations may be defined by

- GlobalPlatform
- JasPar
- OEMs

Configuration Choose:

- What Trusted Applications are Needed,
- Performance
- Hardware
- Robustness
- Security Level

Same Approach Used by Other Industries to Leverage GP Technologies

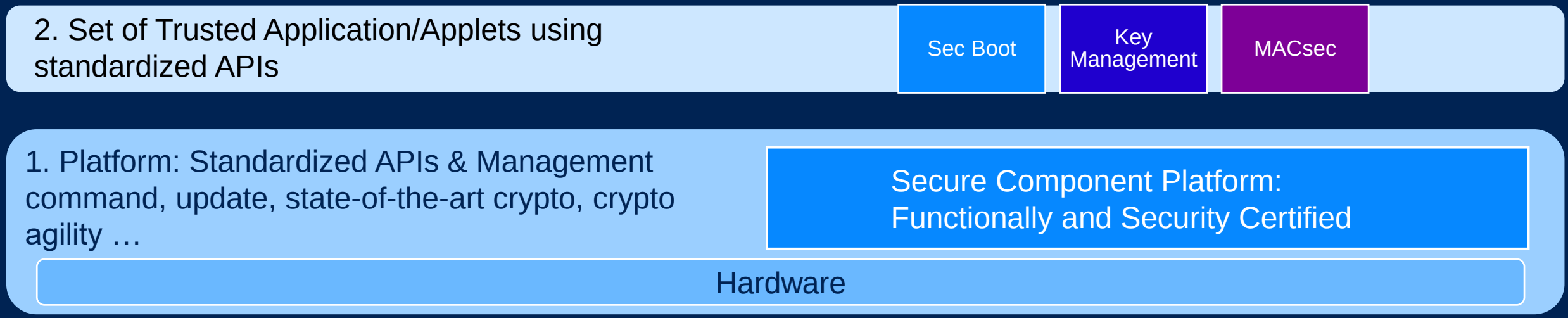
- SAM (Secure Applications in Mobile) defined by GSMA
- Financial applications defined by EMVCO
- Authentication by FIDO Alliance

GSMA

EMVCo

fido alliance

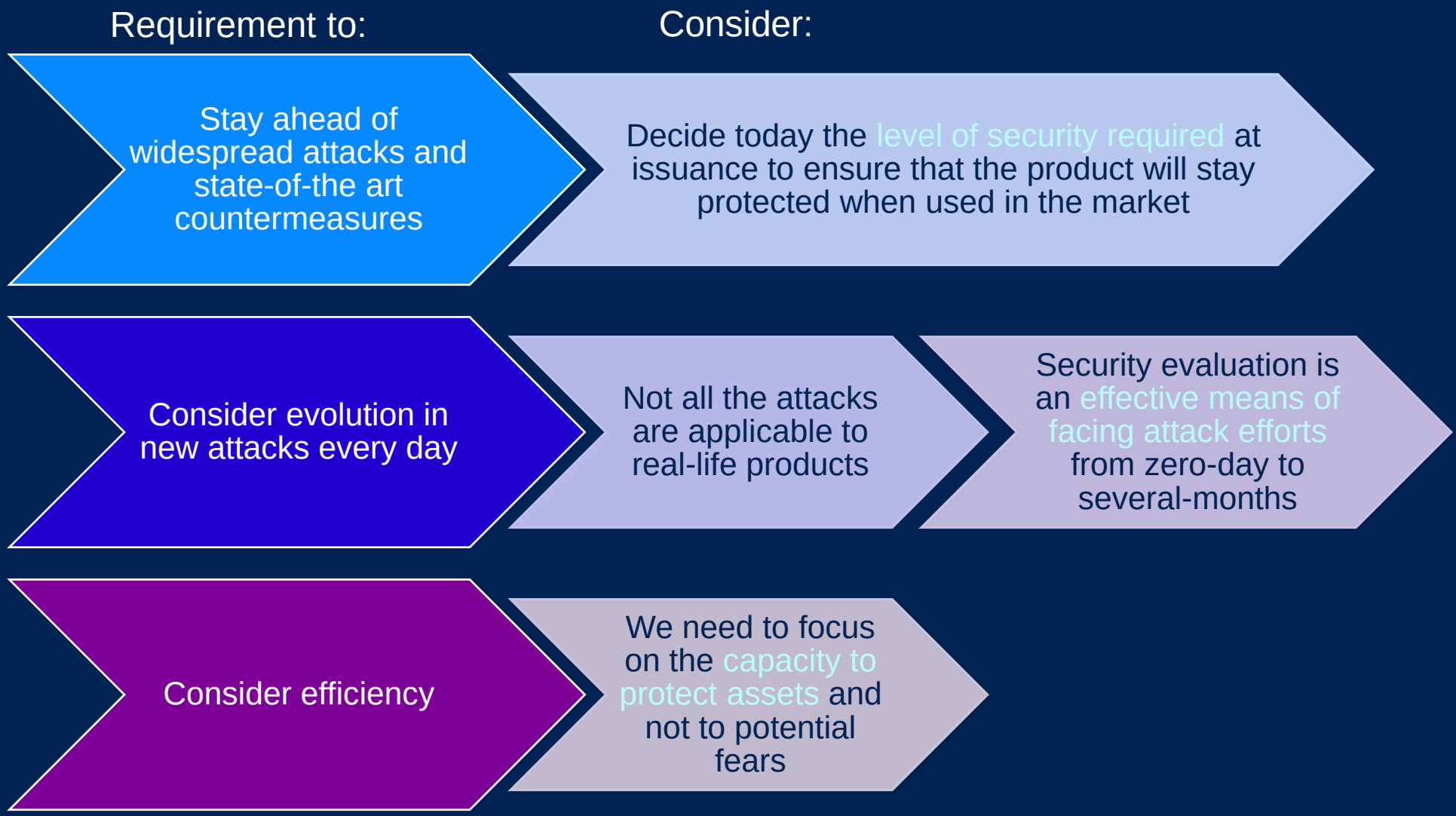
Example HSM-like with GlobalPlatform Secure Element



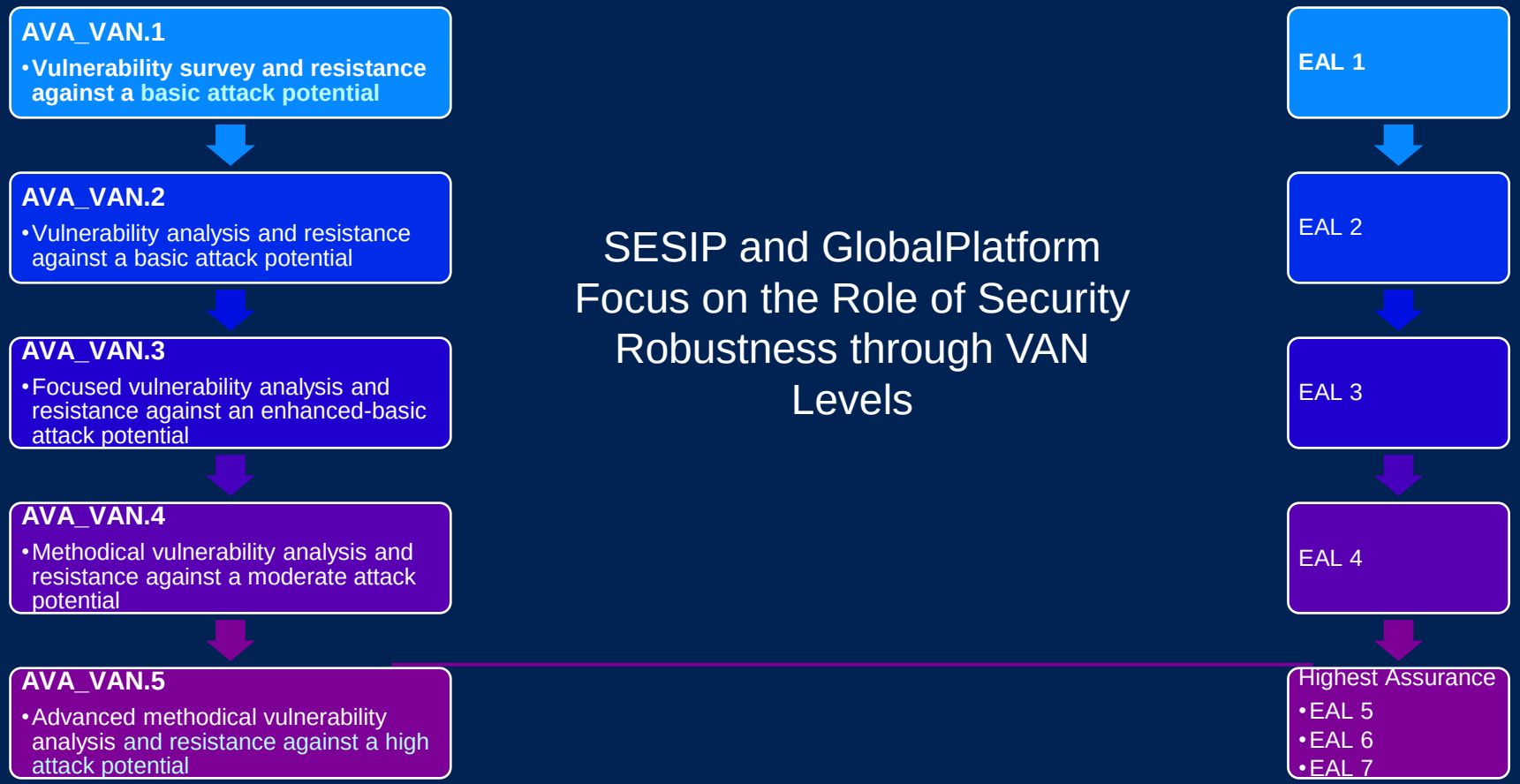
Attack Methodology

Gil Bernabeu

Understanding Potential to Protect Assets



Assessing Robustness through Vulnerability Levels: Defined by ISO 15408: 2022



VAN Levels (i.e. Robustness against Attacks) go from 1 to 5 (Maximum) while EAL Levels (i.e. CC Evaluation Assurance Levels) Range from 1 to 7 (Maximum).

GlobalPlatform's Methodology for Measuring Attack Criticality

Attack Quotation

Expertise	Time	Tools	# Product knowledge	# of dev products	#of final products

Black Hat and Fraud Operators 2023

Source:(Upstream 2024). https://upstream.auto

GlobalPlatform's Methodology for Measuring Attack Criticality

To Show that Your Product Reaches a Specific AVA_VAN Level,

Certification Labs Use Appropriate Attacks for the Relevant [Attack] Quotation

As an example,

- **GlobalPlatform TEE certification requires resistance against attacks below 21 points =**
- **AVA_VAN 3**

Every Market Selects a Relevant Level of Robustness: Some Current Automotive Market Examples

Payment ID/telco Industrial

EMVCo
Payment Card / SE

CC / FIDO L3+ / GSMA
ID / SE

CC (>= EAL4+)
Meter Gateway

IEC 62443 (SL4)
PLC

Digital Car Key
Secure Element

VAN 5

VAN 4

SE Protection Profile

PCI
PoS

CC / FIDO L3
ID / TEE
TEE

CC (EAL3)
Smart Meter

IEC 62443 (SL3)
PLC

IVI Systems
TEE

VAN 3

TEE Protection Profile

IEC 62443 (SL1 / 2)
PLC

RED directive
Child Devices

VAN 2

VAN 1

PLC : Programmable Logic Controller

Regular Revision of GlobalPlatform's Attack Methodology: Attack Expert Group Role is Crucial

but also

Verifying the assumptions behind

- Expertise
  - Some attacks are now widely known in the field
- Tools
  - Tools to create attacks are now accessible (laser, new APIS, ..)
- Product knowledge
  - Some Product design is now public /disclose

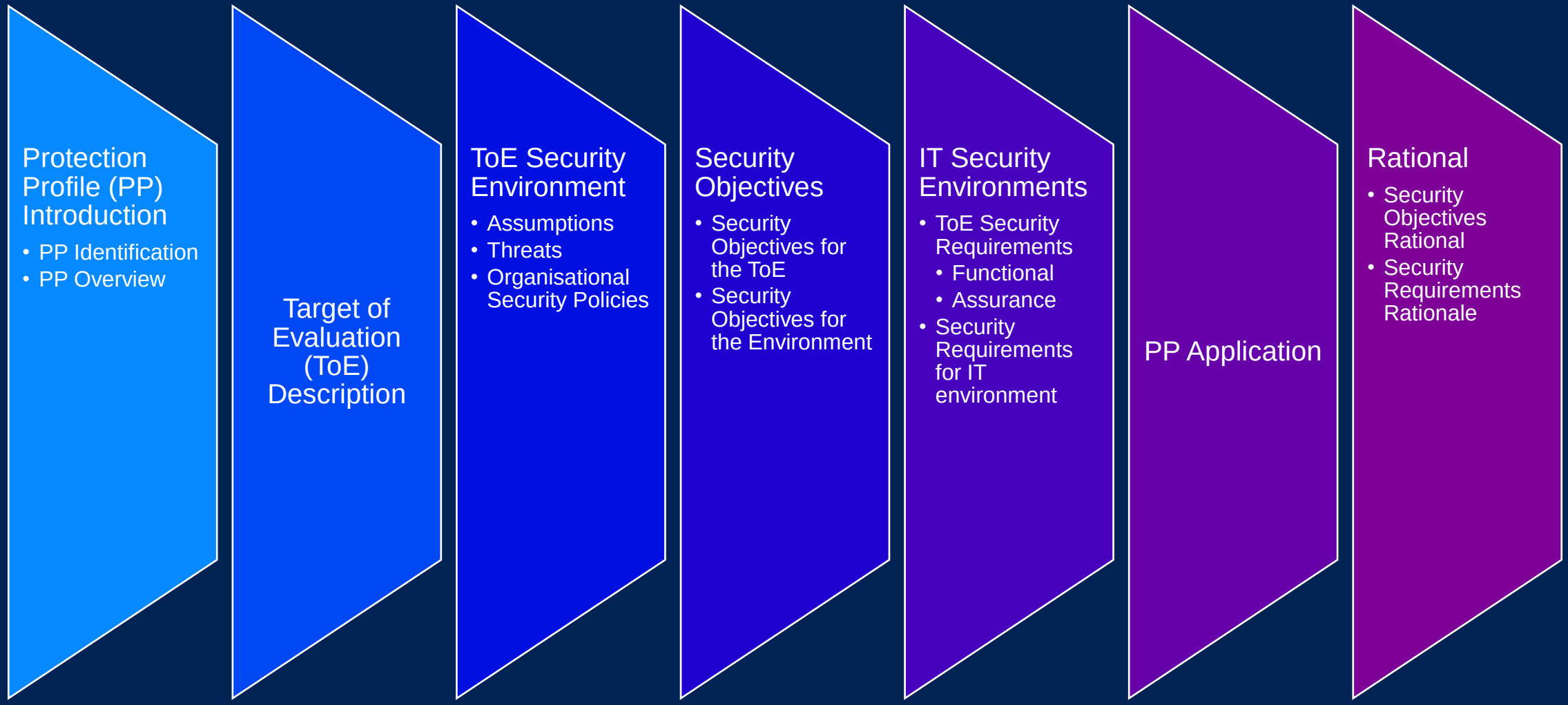
Ex. Attack Subgroup from the EU Senior Officials Group Information Systems Security (JHAS SOG-IS)

Regular update is key to maintain the value of the robustness

Protection Profiles

Gil Bernabeu

Protection Profile Contents



Defining Measurable Security Levels

Ranking Security According To The Robustness

GlobalPlatform	Common Criteria			
High	VAN 5	SE Protection Profile		Attacks methodology Pen testing
	VAN 4			
Medium	VAN 3	TEE Protection Profile MCU Protection Profile		Attacks methodology Pen testing
Low	VAN 2			Attacks methodology Pen testing
	VAN 1			

Global Platform™

GP Protection Profiles

GP Sets Security Objectives

Set of security objectives and requirements for a category of products

- Independent from any specific implementation
- Reusable
- Enables the development of functional standards
- Helps in defining the security specification of a product

GP Defines Implementation Requirements

A set of security requirements which are useful and efficient to satisfy identified objectives

Products will be tested to ensure they meet these requirements

Accredited Lab Evaluates Profile

Evaluated by an accredited Common Criteria (CC) lab

- The lab checks that the Protection Profile is consistent, i.e. requirements match the objectives, objectives are consistent with products and usage

Protection Profile is Published

GlobalPlatform Protection profile accessible from http://www.globalplatform.org/specificationsdevice.asp

The protection profile can then be used by 3rd party labs to validate a product meets the agreed security level

Common Criteria

SESIP

Why are Protection Profiles so Important?

Evaluation of a TEE product against the TEE protection profile verifies:

Existence of all of the factors required to create an isolated environment and to protect device and application assets

Factors have been implemented correctly.

TEE products that have been certified by GlobalPlatform offer

- a clearly-defined level of security
- are protected against vulnerabilities that are subject to widespread, software-based exploitation.

GlobalPlatform ranks in field attacks

- decide whether or not the TEE should be protected from a specific attack.
- Products are state of the art for the expected countermeasures on the platform

GlobalPlatform evaluation methodology has been created from the ISO standard.

Used by multiple security communities.

Examples of Japanese Issued CC Protection Profiles

Protection Profile	Version	Assurance Level	Issued	Scheme	Certified	Categories
Protection Profile for ePassport IC with SAC (PACE) and Active Authentication 2.10	2.10	EAL4+ ALC_DVS.2 AVA_VAN.5	2022-02-21	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Protection Profile for ePassport IC with SAC (BAC + PACE) and Active Authentication 2.10	2.10	EAL4+ ALC_DVS.2	2022-02-21	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit 1.2	1.2	EAL1+ ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 ALC_FLR.1 AVA_VAN.2	2022-09-30	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Public Transportation IC Card Protection Profile 1.12	1.12	EAL5+ ALC_DVS.2 AVA_VAN.5	2018-09-04	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Personal Number Cards Protection Profile	1.00	EAL4+ ALC_DVS.2 AVA_VAN.5	2014-05-15	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Protection Profile for ePassport IC with SAC (PACE) and Active Authentication 1.00	1.00	EAL4+ ALC_DVS.2 AVA_VAN.5	2016-03-22	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Protection Profile for ePassport IC with SAC (BAC + PACE) and Active Authentication 1.00	1.00	EAL4+ ALC_DVS.2	2016-03-22	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Resident Registration Card V2 Embedded Software Protection Profile, Version 1.0	1.0	EAL4+ AVA_VAN.5	2011-02-28	JP	Certification Report	ICs, Smart Cards and Smart Card-Related Devices and Systems
Protection Profile for Hardcopy Devices	1.0	None	2017-05-29	JP	Certification Report	Multi-Function Devices

Importance of Certification for Automotive: because….

01

Demonstrates quality and robustness (UNECE-155)

02

Makes it easier to write and respond to RFCs

03

Provides a basis for legal defence if there ever is a breach

04

V-Model ensures good security process.

Certification ensures a level of security is achieved in practice.

Common Criteria

SESIP

Global Platform™

Global Platform™

Standards Alignment with SAE J3101: Keystore

Francesca Forestieri

How UNECE 155 Compliance Possible with Process and Product Security

Process

ISO /SAE 21434

Product

SAE J3101 Hardware Protected Security Environments

=

Compliance

Cybersecurity Vehicle Management

- Compliance with UNECE 155
- Demonstration of Best Practices

SAE Hardware Protected Security Environments J3101: Common Security Use Case Requirements

Profile	Key Protection 6.2	Cryptographic Algorithms 6.3	Random Number 6.4	Critical Security Parameters 6.5	Algorithm Agility 6.6	Interface Control 6.7	Secure Execution Environment 6.8	Self-Test 6.9
Confidentiality	X	X			?		X	X
Integrity	X	X		X	?		X	X
Availability	X	X			?	X	X	X
Access Control	X	X	X		?	X	X	X
Non-Repudiation	X	X	X	X	?		X	X

NOTE: If algorithm agility is not supported, the profile shall be classified as “limited use” (7.6).

Methodology – GlobalPlatform Specifications Assessed

GP TECHNOLOGY	DOCUMENT REFERENCE	TITLE	VERSION	REFERENCE LINK
SE	GPC_SPE_034	Card Specification [GPCS]	2.3.1	https://globalplatform.org/specs-library/card-specification-v2-3-1/
	GPC_SPE_174	Secure Element Protection Profile [SE PP]	1.0	https://globalplatform.org/specs-library/secure-element-protection-profile/
		GlobalPlatform Card API	1.7.1	https://globalplatform.org/specs-library/globalplatform-card-api-org-globalplatform/
TEE	GPD_SPE_009	TEE System Architecture [TEE Sys Arch]	1.3	https://globalplatform.org/specs-library/tee-system-architecture/
	GPD_SPE_010	GPD TEE Internal Core API [TEE Core]	1.3.1 / 1.4	https://globalplatform.org/specs-library/tee-internal-core-api-specification/
	GPD_SPE_021	TEE Protection Profile [TEE PP]	1.3	https://globalplatform.org/specs-library/tee-protection-profile-v1-3/
	GPD_SPE_025	TEE TA Debug Specification [TEE Debug]	1.0.1	https://globalplatform.org/specs-library/tee-ta-debug-specification-v1-0-1/
	GPD_SPE_120	TEE Management Framework (TMF) including ASN.1 Profile [TMF]	1.1.2	https://globalplatform.org/specs-library/tee-management-framework-including-asn1-profile-1-1-2/
	GPD_GUI_069	TEE Initial Configuration [TEE Config]	1.1	https://globalplatform.org/specs-library/tee-initial-configuration-v1-1/
	GPD_GUI_089	TMF Initial Configuration [TMF Config]	1.0	https://globalplatform.org/specs-library/tmf-initial-configuration-v1-0/
SE and TEE	GP_TEN_053	Cryptographic Algorithm Recommendations [Crypto Rec]	2.0	https://globalplatform.org/specs-library/globalplatform-technology-cryptographic-algorithm-recommendations/
	GP_REQ_025	Root of Trust Definitions and Requirements [RoT]	1.1.1	https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/

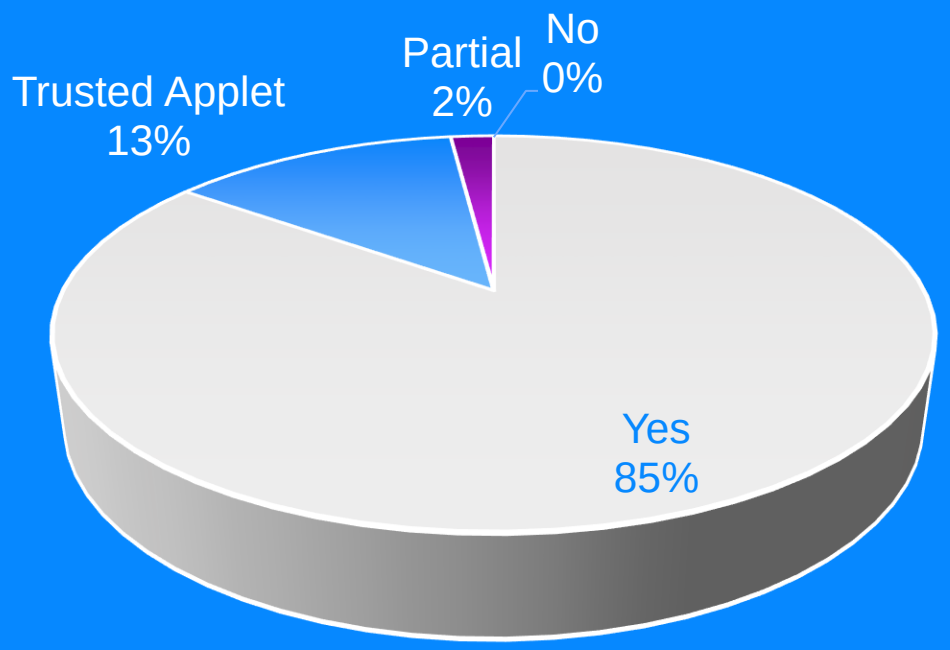
Methodology – Requirements Assessment

Reviewed each J3101 requirement in the context of both the GlobalPlatform Specifications for Secure Elements and for Trusted Execution Environments

Requirement ID	Condition	Requirement Description	SE Supported	SE Mapping	TEE Supported	TEE Mapping
		Types of Keys				
REQ_6.2.3.1_10:	[MANDATORY]	The hardware protected security environment shall support digital certificates if public keys (asymmetric cryptography) are employed. The digital certificates should be X.509 or IEEE 1609.2 compatible formats.	YES – Trusted Application	X.509 is supported. IEEE 1609.2 is supported through an Application/Configuration.	YES – Trusted Application	X.509 is supported. IEEE 1609.2 is supported through an Application/Configuration.
REQ_6.2.3.1_20:	[OPTIONAL]	The hardware protected security environment shall support either ephemeral or long-term symmetric keys, or both.	YES		YES	
		Key Storage				
REQ_6.2.3.2_10:	[MANDATORY]	A hardware protected security environment must securely store all cryptographic keys and explicitly control access to each.	YES	Mandated by [SE PP].	YES	Mandated by [TEE PP].
REQ_6.2.3.2_20:	[MANDATORY]	A keystore may be direct storage of the keys within the hardware protected security environment, or use of external storage external to the hardware protected security environment that is protected by encryption and integrity mechanisms implemented within the hardware protected security environment.	YES		YES	Mandated by [TEE PP].
REQ_6.2.3.2_30:	[OPTIONAL]	Key storage capacities should only be constrained by the physical limits of the underlying hardware. Allocation of storage between differing uses should be defined under each application specified for the hardware protected security environment, both in maximums and minimums. Denial of service due to exhaustion of available resource should be mitigated by a resource manager implemented in either hardware or firmware as a part of the hardware protected security environment.	YES	The SE PP mandates the physical limit of memory storage. In the GP API there is a mechanism for Granted Memory per memory type in the installation/registry to avoid DoS.	YES	The TEE PP mandates the physical limit of memory storage. In the TEE Core API there is a mechanism for Memory Allocation per memory type in the installation/registry to avoid DoS.

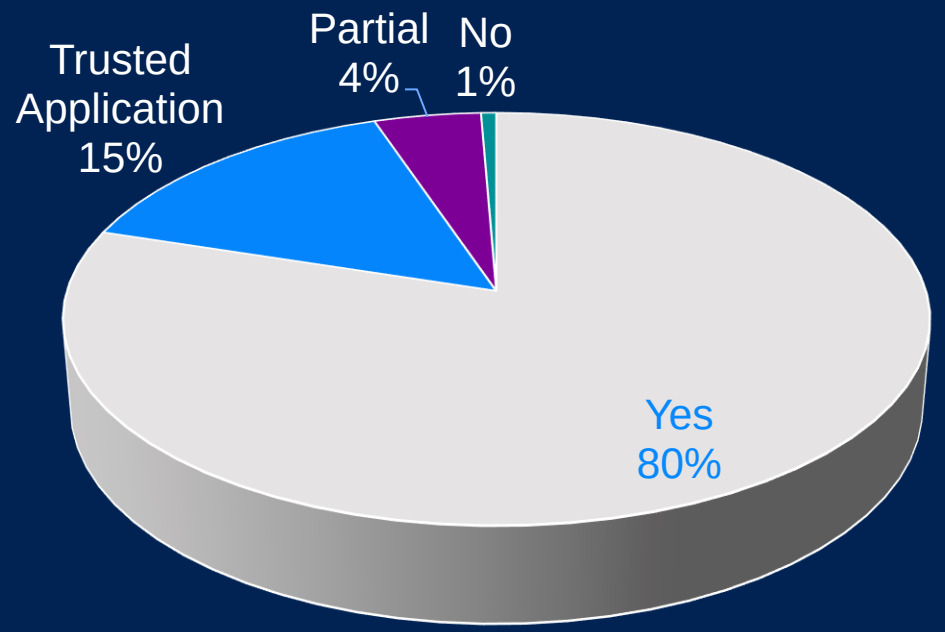
Analysis Results: GlobalPlatform Specifications

Secure Elements Fully Meet 98% J3101 Requirements



Evaluated using Common Criteria (CC) existing Protection Profile

Trusted Execution Environments Fully Meet 95% J3101 Requirements



SAE INTERNATIONAL

SURFACE VEHICLE INFORMATION REPORT

J3101-5™	FEB2024

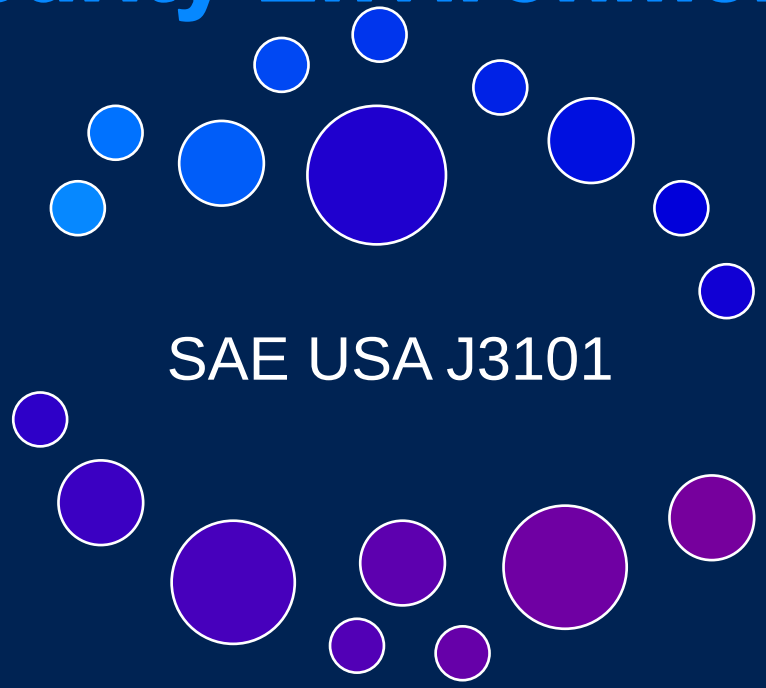
Issued XXXX-XX
Reaffirmed XXXX-XX
Stabilized XXXX-XX
Revised XXXX-XX

Superseding JXXXX MTHYEAR

Hardware Protected Security Environment –

GlobalPlatform Technologies Information Report

Why Cooperation with SAE on Hardware Protected Security Environments Is Optimal



GlobalPlatform

Defines Common Glossary of Required Hardware Protected Secure Environment Characteristics

- February 2024 1st GP Mapping to J3101 Standards Developed
- May 2024 Created J3101-5 for Mapping of how GlobalPlatform Satisfy J3101 Recommended Best Practices
- October 2024 Internal Ballot in Security Task Force Expected to Be Finalised
- November presentation to

Detailed specifications and Implementation guidelines

- Cover these HPSE requirements and more
- Globally relevant
- Secure Elements Fully Meet 98% J3101 Requirements
- Trusted Execution Environments Fully Meet 95% J3101 Requirements

Certification of components by SE or TEE providers to:

- Ensure interoperability/ portability and
- Proven security robustness (protection against attack) obtained
- Possibility of composite certification (SESIP)

Hardware Protected Security Environments in Other Regions: Open Questions

Is SAE's work on J3101 a departure point for discussing Japanese requirements?

Is there interest in standardising a Japanese version?

Would it be useful to cooperate with GlobalPlatform to explore how GlobalPlatform technologies meet eventual Japanese specific requirements?

Would it be useful to provide some educational opportunities on GlobalPlatform technologies?

Comparing Different Trust Anchors:

Generalizations

GlobalPlatform Offers Flexibility and Assurance

	Trusted Computing Group			GlobalPlatform		Automotive HSM/ Secure Enclave (Proprietary)
	DICE	MARS	TPM	Secure Element	Trusted Execution Environment	
Size	Very small (~20kB+)	Very small (~8kB)	Small implementation (~150kB+)	Mid-size implementation (~350kB up to 4MB)	Large implementation (>1MB)	Small (~150kB+) to Mid-size implementation (generally ~250kB)
APIs	Client API not standardized	Simple client API	Rich client API	Rich internal application APIs	Rich client and internal application APIs	Proprietary APIs
System Binding	Closely bound to system	Loosely bound to system	Loosely bound to system	Loosely bound to the system	Closely bound to system	Loosely bound to system
Tenant Capability	Single tenant	Single tenant	Limited multi-tenant capability	Rich multi-tenant capability	Rich multi-tenant capability	Single tenant (generally)
Certification	Probably not certified	Probably not certified	Usually high assurance (EAL4+)	Always high assurance (EAL4+)	Often medium assurance (EAL2+)	Probably not certified
Breadth of Security Services, including:	Partially standardized	Limited set of services	Designed to do a fixed set of services very well (e.g., measured boot)	Any type of secure services can be added with Trusted Applets, also using Java Card OS	Any type of secure services can be added with Trusted Applications	HSM implementations embrace many different versions depending upon supplier.
-OTA Updates	N/A	N/A	Proprietary Update	OTA Updatable in a Standardised Manner	OTA Updatable in a Standardised Manner	Proprietary Updates
-Security Use Case	Layered Boot, Application integrity, Remote attestation	Signature & Key Creation, Derived Keys	Keystore, Signature Creation and Validation, Certificate Management	Designed to support flexibility in high security use cases with more limited performance requirements	Designed to support flexibility in supporting security use cases for multiple service types with higher performance requirements (e.g. 20-50 X faster). Dramatic performance advantages due to use of Core CPUs.	Keystore, Signature Creation and Validation, Certificate Management
Mandatory requirements	References to DICE for IETF PKI		References to: TPMs for EV charging, Remote Attestation in ISO/ IETF	eSIM, Car Connectivity Consortium, Qi wireless charging, V2X for outgoing signature generation, Strongbox	V2X for signature verification	
Examples of Implementation Hardware	Usually MCU class	Usually MCU class runs at native clock rates	Usually dedicated 32 bit MCU running at 10-24 MHZ	Ex. CPU Class 32 bit MCU running at 50MHZ-100MHZ	Ex. CPU Class Cortex A8 64 bit at 2GHZ or more	Could be any variation – tends toward MCU class

Global Platform™

life.augmented

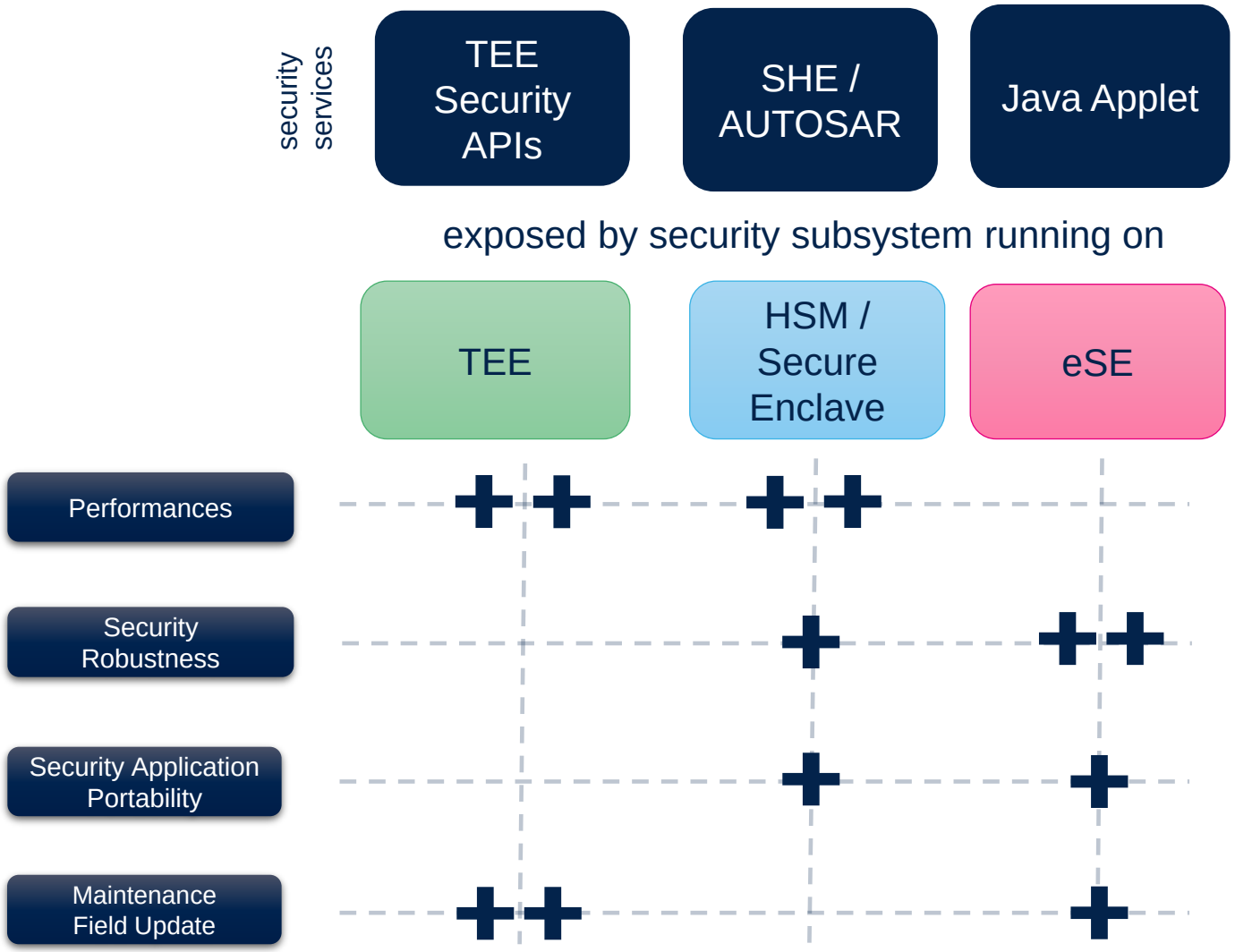
GlobalPlatform ATF Toolbox
Security Convergence

Laurent TABARIES

STMicroelectronics – GlobalPlatform meeting

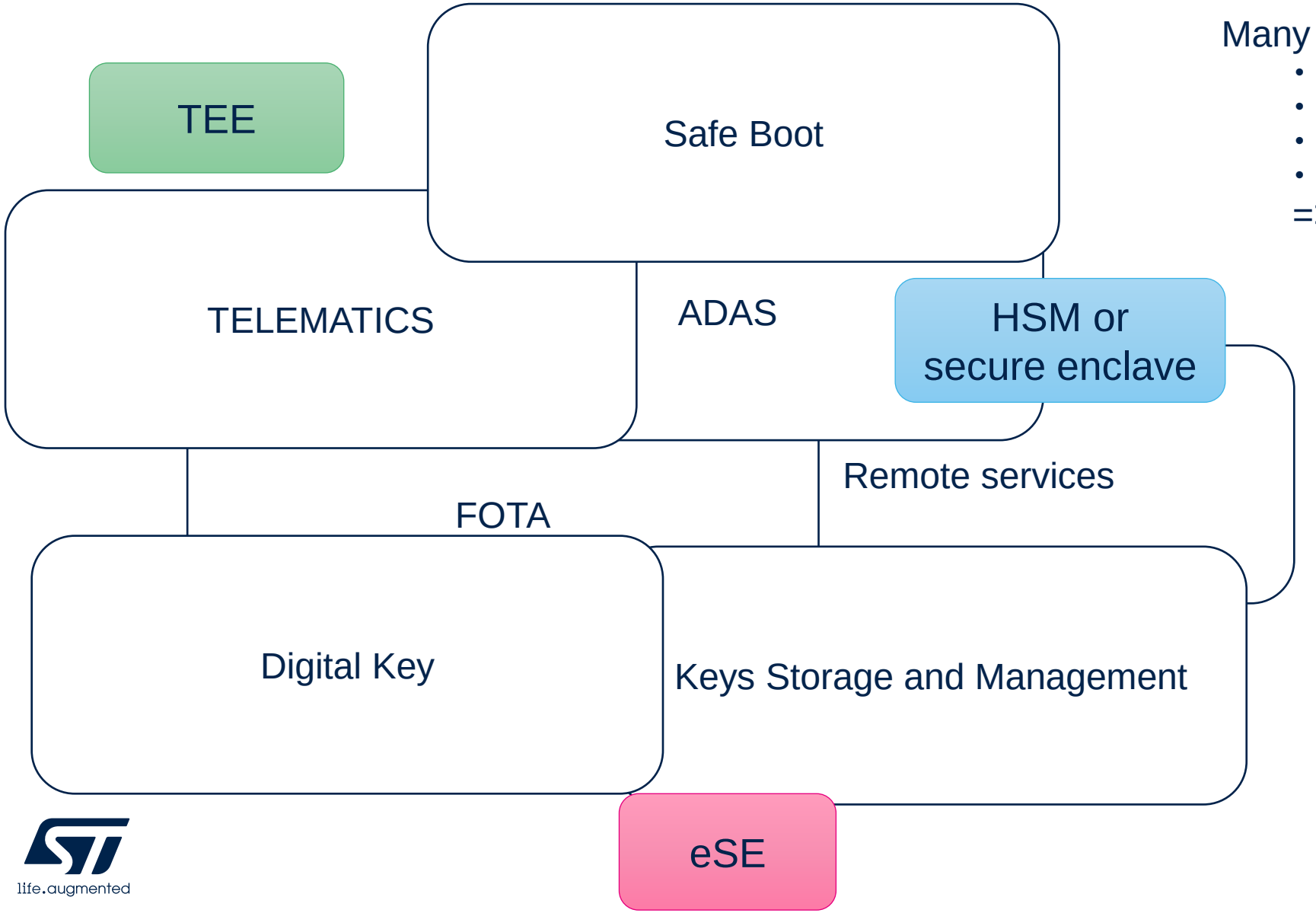
24th October 2024, Tokyo

Automotive security subsystem panorama



NB: This analysis is given as an high level overview and could be redefined according to a vote organized during any ATF meeting

Automotive security different use cases



Many use cases with different

- Definitions
- Expectations
- Constraints
- Environments

=> Non unique solution

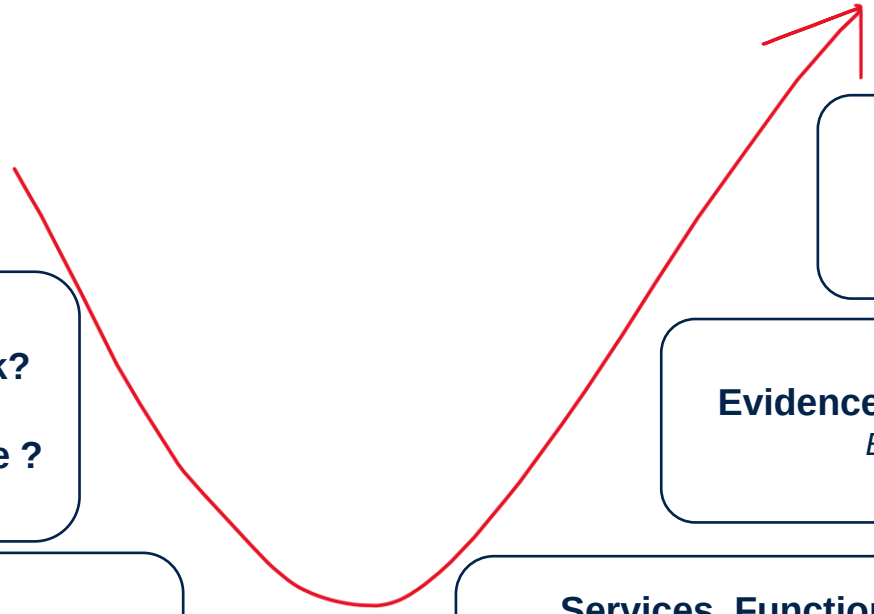
life.augmented

Use Cases “security needs” driven by

Standard (or Protection Profile) requirement
Ex: Qi, Digital Key CCC, V2X, GBA

Self assesment Analysis (use case dependant)
Security robustness : Remote or Board level Attack?
What is the asset to protect ?
Field update (patch or data perso) level of insurance ?
Ex: UWB Anchor or Lidar located in the bumper

System level integration with correlations ?
Ex : ADAS with mutiple sensors inter-connected with supervision or Battery Passeport with regular cloud connection



Easy deployment and usage
Ex: SCP or SPI GP T=1

Evidence of security level reached
Ex: SESIP level 3 or 4

Services, Functions and API availability combined with customization capabilty
Ex: Few custom functions for maintenance purpose or for proprietary legacy crypto scheme

What is the starting point, or what are the legacy constraints ?
Ex: solution EVITA with Autosar to implement new crypto function
What are the missing points and what is the rational of the change ?
Ex: Generate localy (in the Telematic Control unit)
2 applicative keys derived from a master keys received from the OEM server
Ex: Crypto or MAC flexibility might not be compatible with frozen functions available in EVITA

life.augmented

Field typical request

HSM or secure enclave

+

eSE or TEE

Ex: EVITA_full (CSM Autosar APIs) available with conservative approach
***but** new crypto algo could miss*
*or **new request** to automatize some functions*
*or **reinforce** security robustness*

Ex1: to extend EVITA FULL with new specific crypto algo

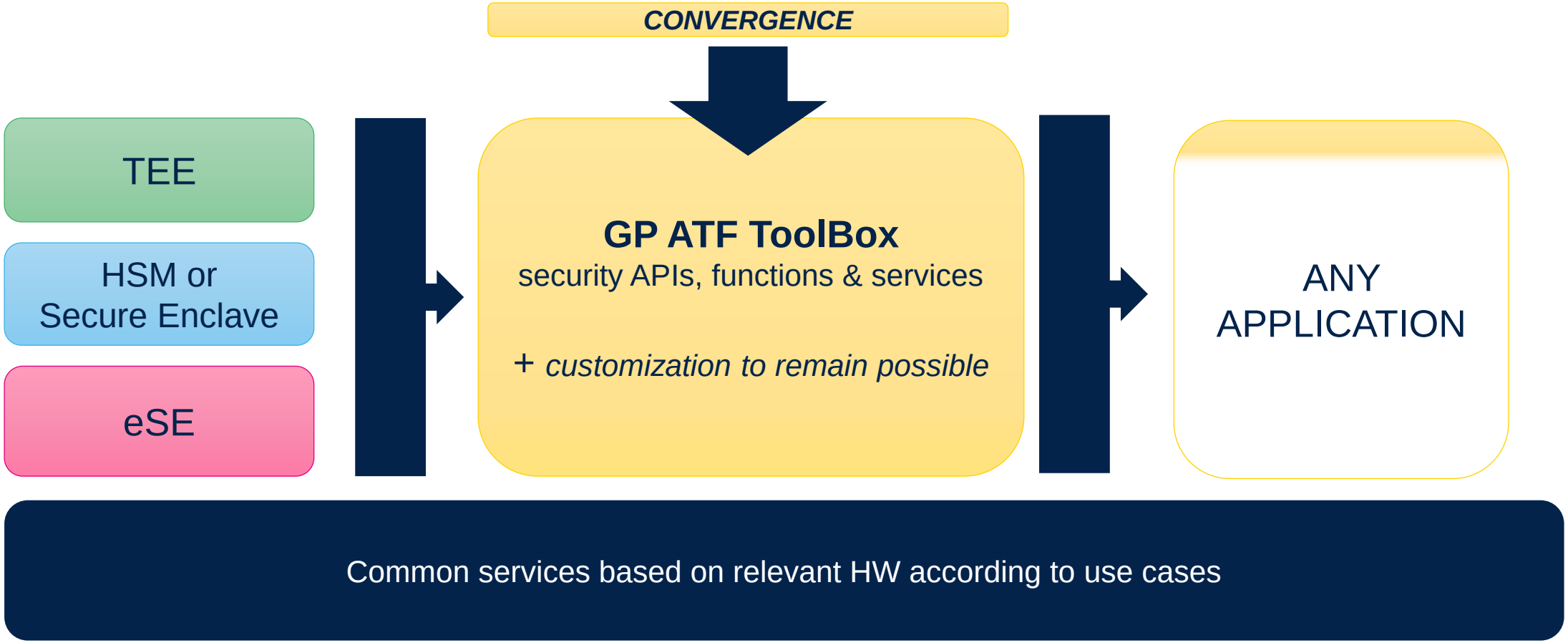
Ex2: Key Derivation Function automatized (HKDF)

Ex3: Create a robust RoT to validate paltform integrity at Boot

Mainstream OEMs/Tiers1 request is to add services/functions/APIs on top of existing solution HSM based to improve flexibility and/or security robustness

But many OEMs/Tiers1 do not know how to start ?

GP ATF Toolbox to help security convergence



GP could help to define a set of APIs, functions and services
as a **Automotive ToolBox superset**

GP ATF Toolbox in 3 steps

To identify and list mainstream APIs, functions and services :
- RoT
- Key Derivation and Key Management
- Data Personalization (with Security Domain)
- Mainstream Crypto, MAC, Hash functions
- Remote services (to leverage on top of SCP and SPI/I²C GP T=1)
- Etc ….

To formalize a GP specification (thanks to GP ATF)
and setup draft JVC Applet (on top of default JVC 3.0.5)
with incremental approach based on regular field feedbacks
to improve to solution set

To implement such GP ATF ToolBox Applet POC
- provide performance improvment metrics
- provide easy guide to ease porting and adoption
=> mainly focused on HSM, used as a proxy, to extend solution « GP ATF ToolBox » based

life.augmented

woven by TOYOTA

Global Platform Use Cases

October 24th, 2024

Vincent Mailhol

Senior Product Security Engineer

vincent.mailhol@woven.toyota

Meeting Agenda

About me

- Joined Woven by Toyota in October 2020
- Maintainer of the CAN subsystem of the Linux kernel (a.k.a Socket CAN)

index : kernel/git/torvalds/linux.git

master switch

Linux kernel source tree — Linus Torvalds

about summary refs log tree commit diff stats

author vincent mailhc search

Age	Commit message (Expand)	Author	Files	Lines
2024-02-12	can: change can network drivers maintainer	Vincent Mailhol	1	-1/+1
2023-10-04	can: etas_es58x: add missing a blank line after declaration	Vincent Mailhol	1	-0/+1
2023-10-04	can: etas_es58x: rework the version check logic to silence -Wformat-truncation	Vincent Mailhol	2	-21/+42
2023-06-22	can: length: refactor frame lengths definition to add size in bits	Vincent Mailhol	2	-101/+216
2023-06-22	can: length: fix bitstuffing count	Vincent Mailhol	1	-6/+8
2023-06-22	can: length: fix description of the RRS field	Vincent Mailhol	1	-2/+3
2022-12-19	Documentation: devlink: add missing toc entry for etas_es58x devlink doc	Vincent Mailhol	1	-0/+1

01

Software define vehicle

A story of reusability

Reusable Platform	**TNGA: Toyota New Global Architecture**
History	Physical platform that is used to build Toyota vehicles ● Accounts for 80%+ of all vehicles ● Defined variants ● Scales and is reusable

Reusable Platform	**ePF: Toyota Electronic Platform**
Software	Software platform that is used to build Toyota vehicles ● Defined variants ● Scales and is reusable ● Is certified; no bespoke software

Reusable Platform

Common hardware components

ARM based chipset

Ideally Cortex-M or Cortex-A

Standardized APIs

Standardized security controls

Supplier agnostic builds

Known technology

Known supported features

Reusable software

Testable functionality and features

Provide reusable components for engineers

Provide capability for platform to scale and be independent (loosely coupled) with the hardware

Provide a known secure and safe foundation for developing functionality

Capability to separate out the configuration of the software from the operation of said software

Automotive Specific Items

01

Functional Safety

Our software **must not** have any failure that impacts the safety of the road user, or any person that could be impacted by the road user.

02

Long Lifespan and Quality

It is possible to fix an issue via OTA in modern automobiles, but the cost is high and some items require a service visit. Toyota aims to support its vehicles in the field for **15-20** years.

03

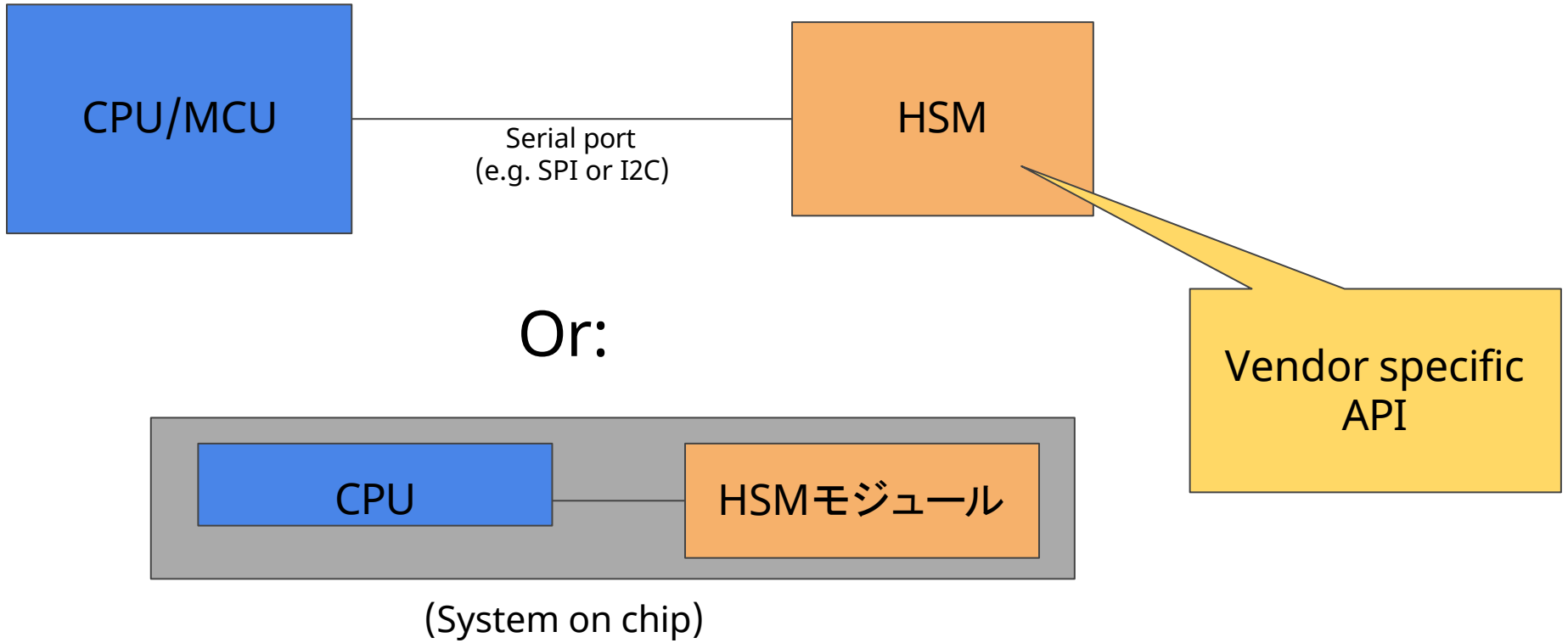
Performance

There are some scenarios, required for safety, security, or legislation that require specific actions to happen within a **defined amount** of time.

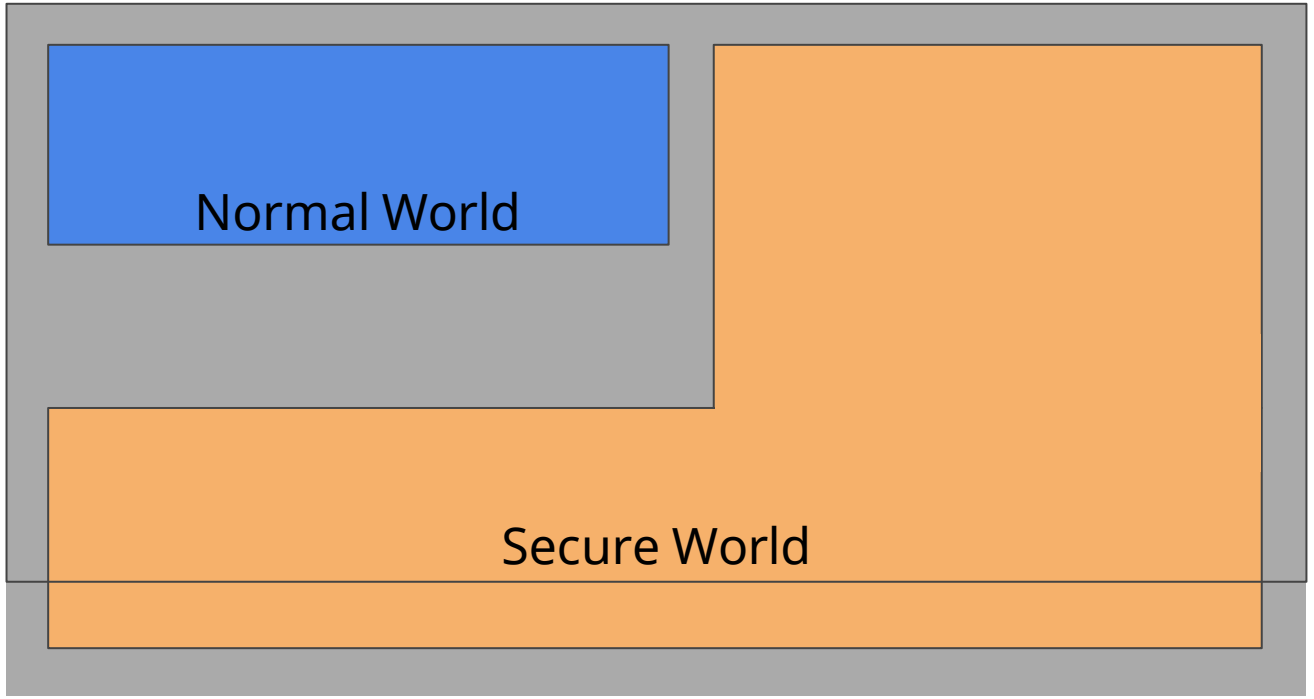
02

GlobalPlatform Standard API

Classic automotive hardware security

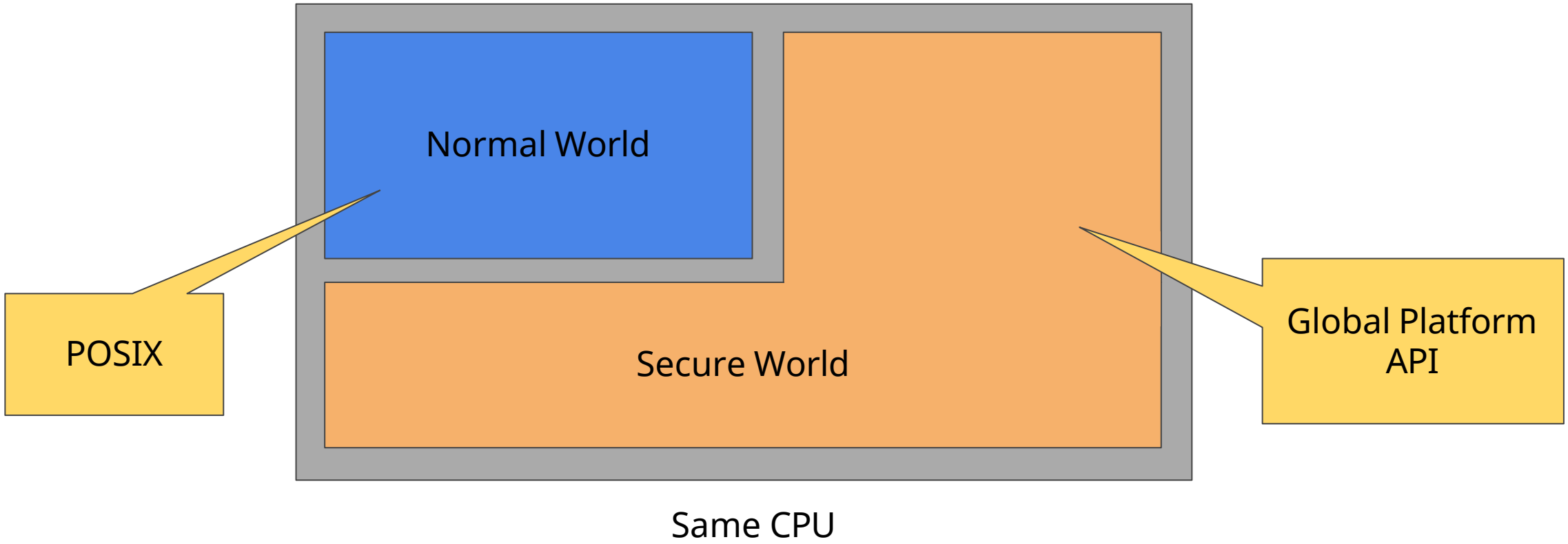


Trusted Execution Environment



Same CPU

Trusted Execution Environment + Use of standard API



Benefits of TEE with GP API

01

Cost

- Available by default on Armv8-A architectures.
- No additional module are needed.
- Code reusable

02

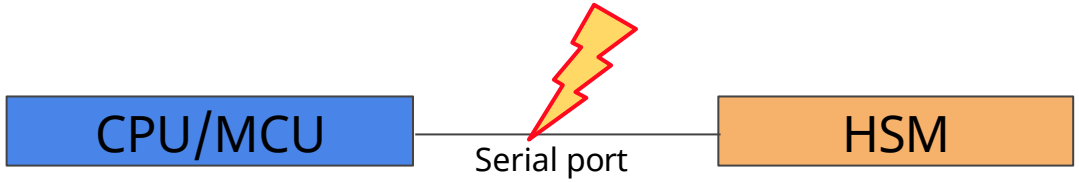
Speed

- Secure and non secure operation runs on the same CPU: less overhead communication cost.
- CPU is usually faster than HSM.

03

Security

- No serial port: more robust against hardware attacks.



03

How could reusability go wrong?

Study case on Ariane 5

Failure in the Inertial Reference System (SRI)

Overflow on 16 bit integer

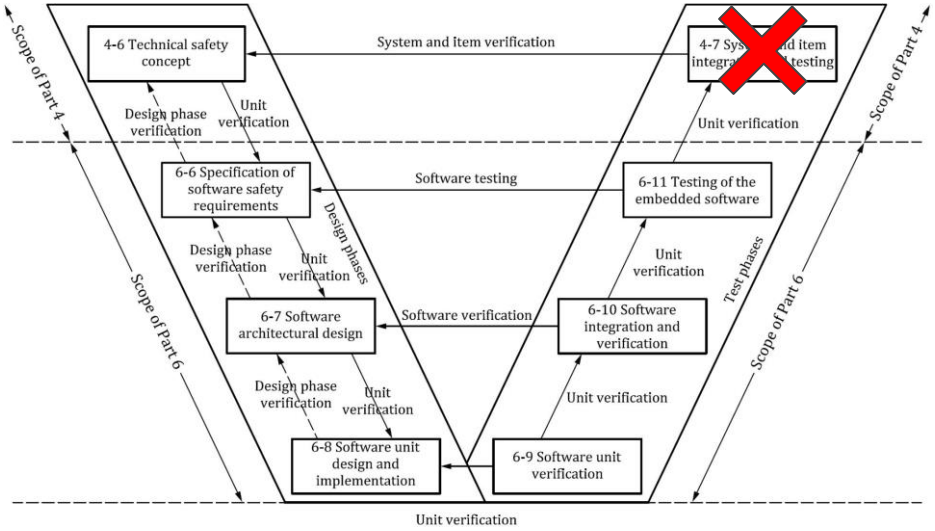
Consequences: $370M loss

Ariane 5 launch (June 1996)

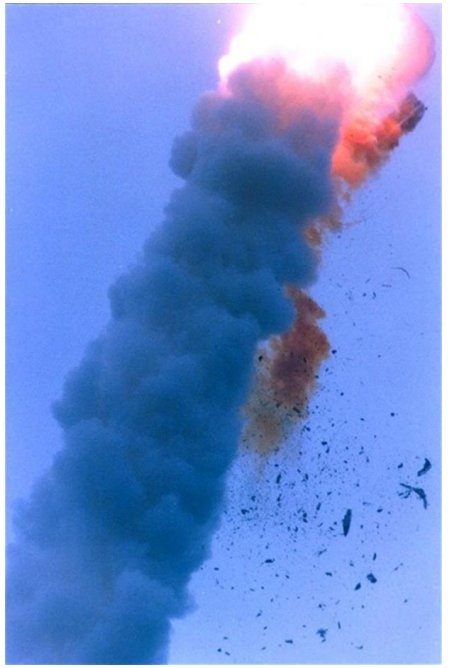
SRI developed for Ariane 4

Ariane 4

No integration tests



SRI reused in Ariane 5



Ariane 5

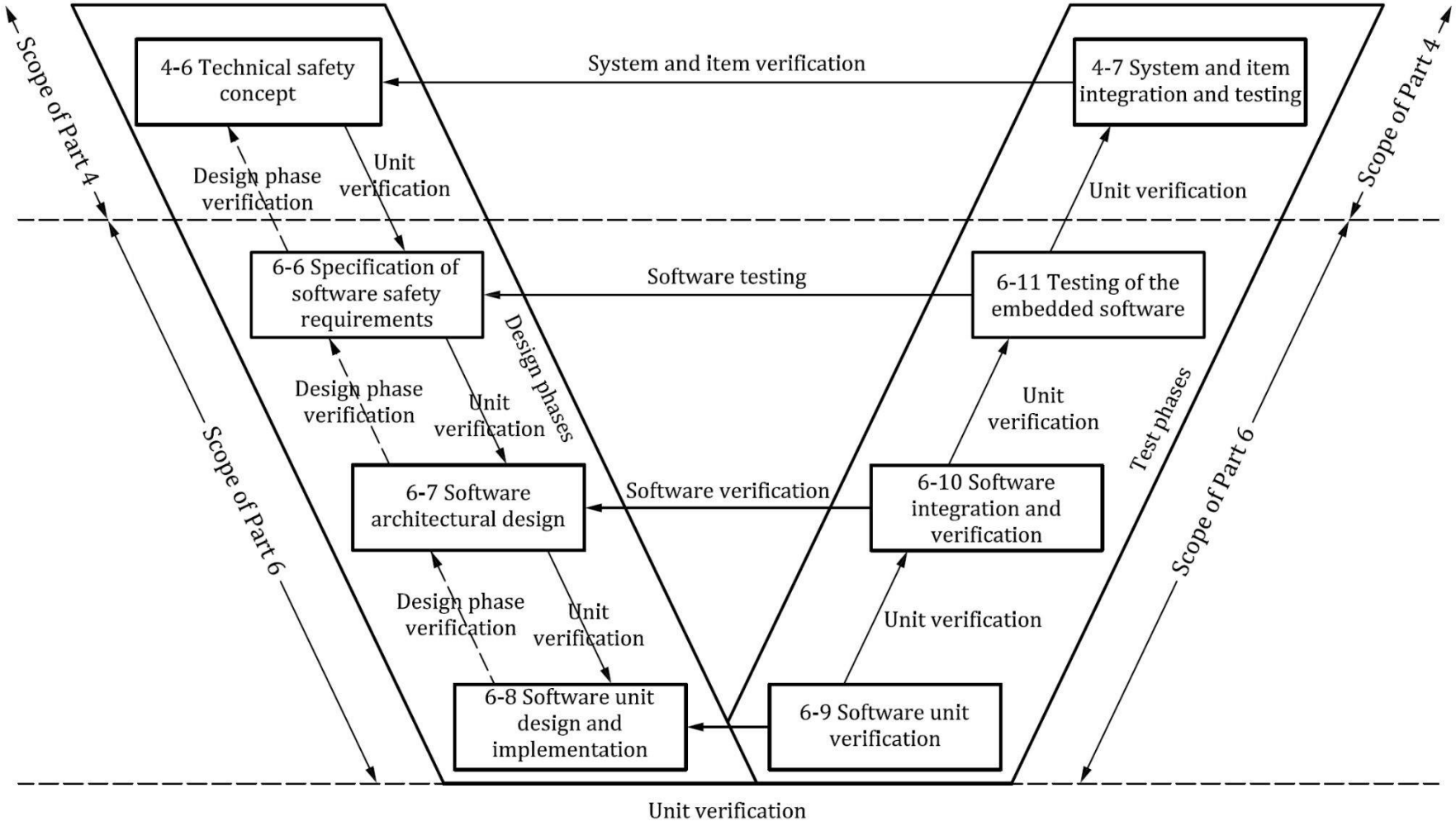
04

How to prevent failure

Processes and testing

Processes

- ISO 26262
- ISO 21434
- MISRA
- …

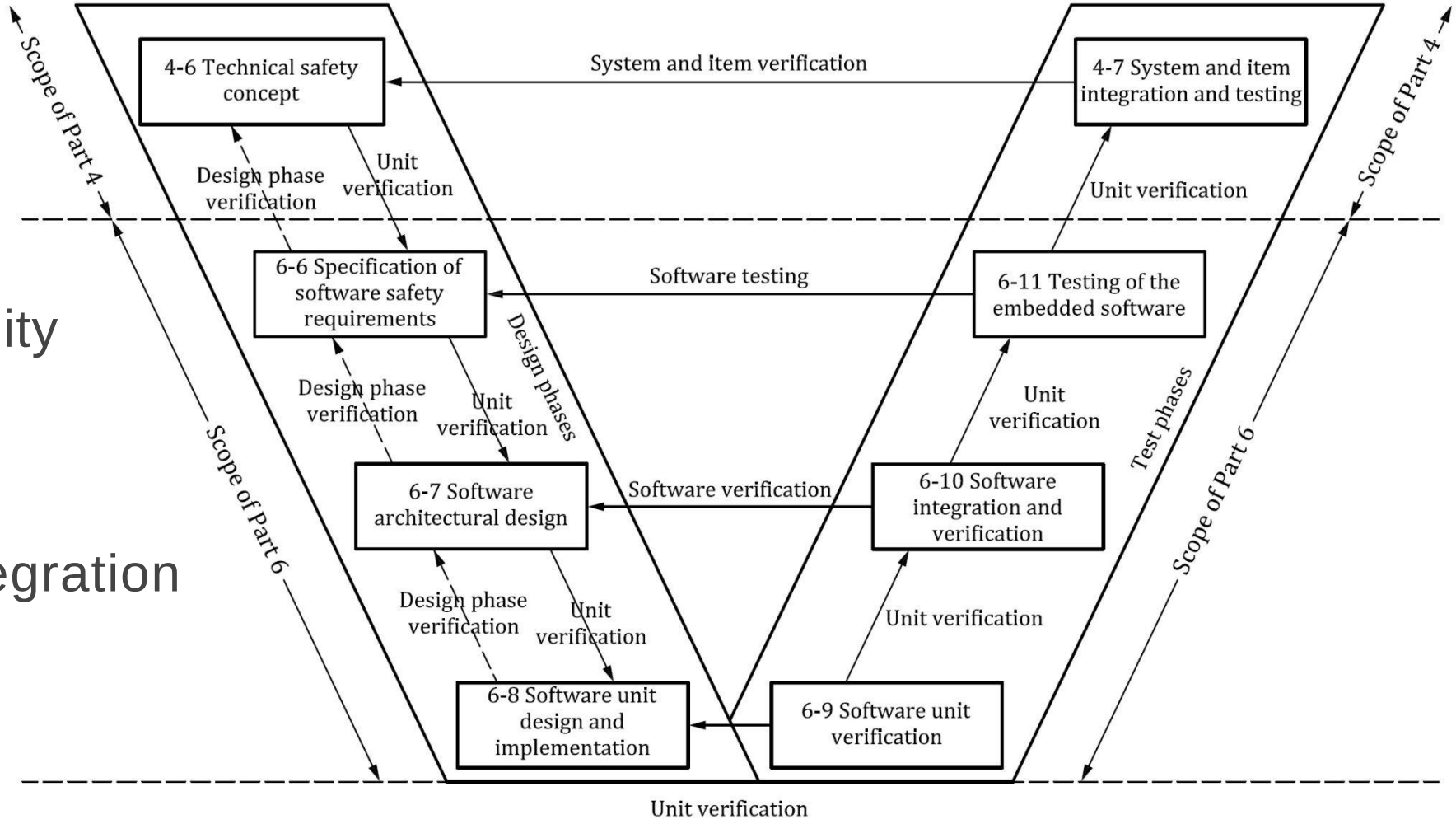


Automation:

- Reduce cost
- Increase reliability

Example:

- Continuous integration
- SIL
- HIL



05-1

Global Platform Properties

Global platform allow to query security properties

Example with time:

Table 7-1: Values of the `gpd.tee.systemTime.protectionLevel` Property

Value	Meaning
100	System time based on REE-controlled timers. Can be tampered by the REE. The implementation SHALL still guarantee that the system time is monotonic, i.e. successive calls to `TEE_GetSystemTime` SHALL return increasing values of the system time.
1000	System time based on a TEE-controlled secure timer. The REE cannot interfere with the system time. It may still interfere with the scheduling of TEE tasks, but is not able to hide delays from a TA calling `TEE_GetSystemTime`.

Global platform allow to query security properties

Code:

```
uint32_t system_time_procection_level = 0;

TEE_GetPropertyAsU32(TEE_PROSPSET_TEE_IMPLEMENTATION,
                     "gpd.tee.systemTime.protectionLevel",
                     &system_time_procection_level);
switch (system_time_procection_level) {
case 100:
        ERROR("Warning: REE-controlled timer");
        break;
case 1000:
        /* TEE-Controller timer: OK */
        break;
default:
        ERROR("Unknown system time protection level?!");
        break;
}
```

Global platform allow to query security properties

Other properties:

- `gpd.tee.cryptography.*`: check which cryptography algorithms are supported. Allow for crypto agility
- `gpd.tee.trustedStorage.*`: check the protection level of the secure storage

Global platform allow to query security properties

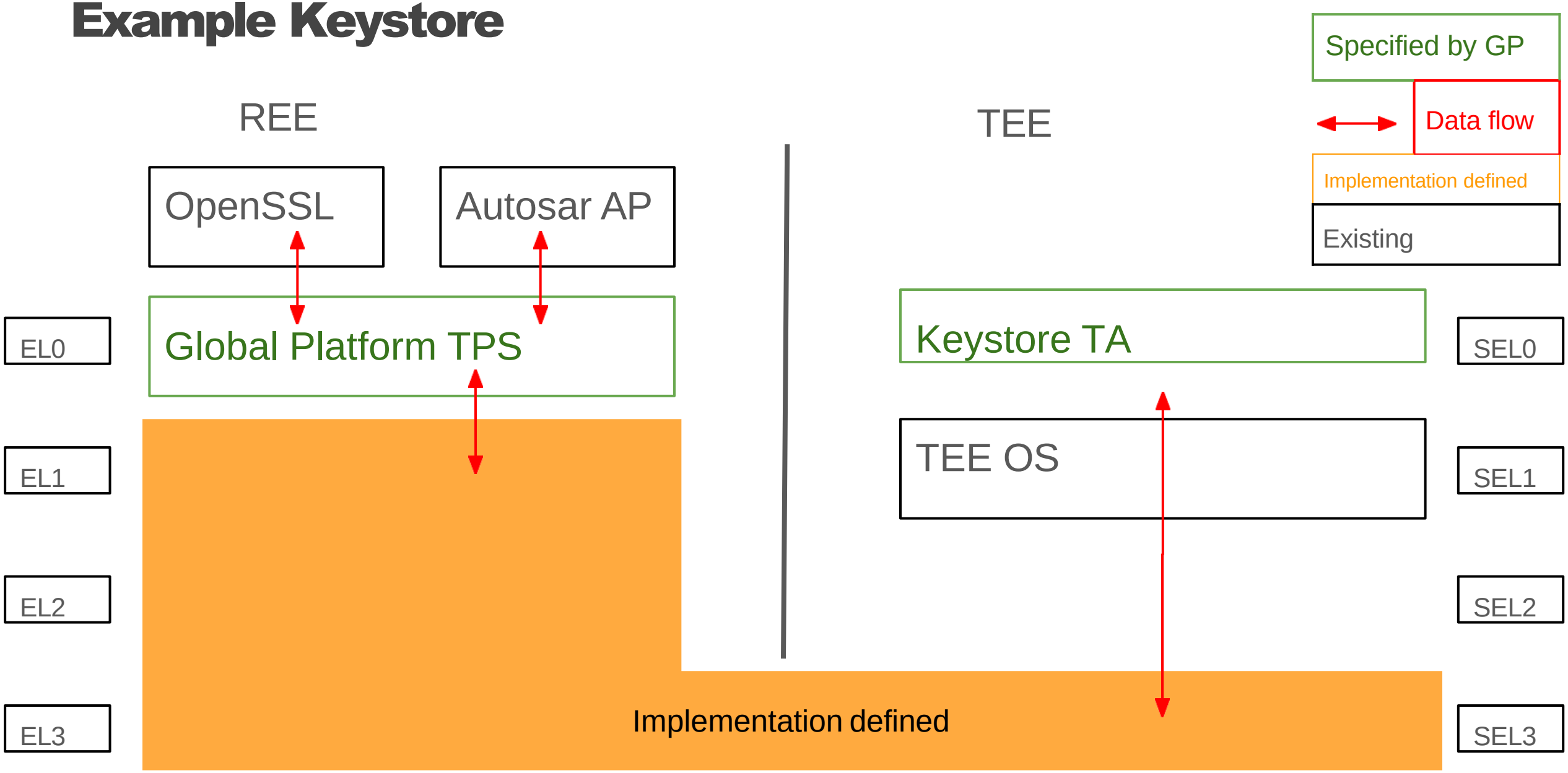
Idea: introduce new properties for the random generator:

- `gdp.tee.rng.prng`: pseudo random generator
- `gdp.tee.rng.trng`: true random generator (unspecified)
- `gpd.tee.rng.nist`: compliance to NIST SP 800-90*
- `gpd.tee.rng.bsi`: compliance to AIS 20 and AIS 31
- …

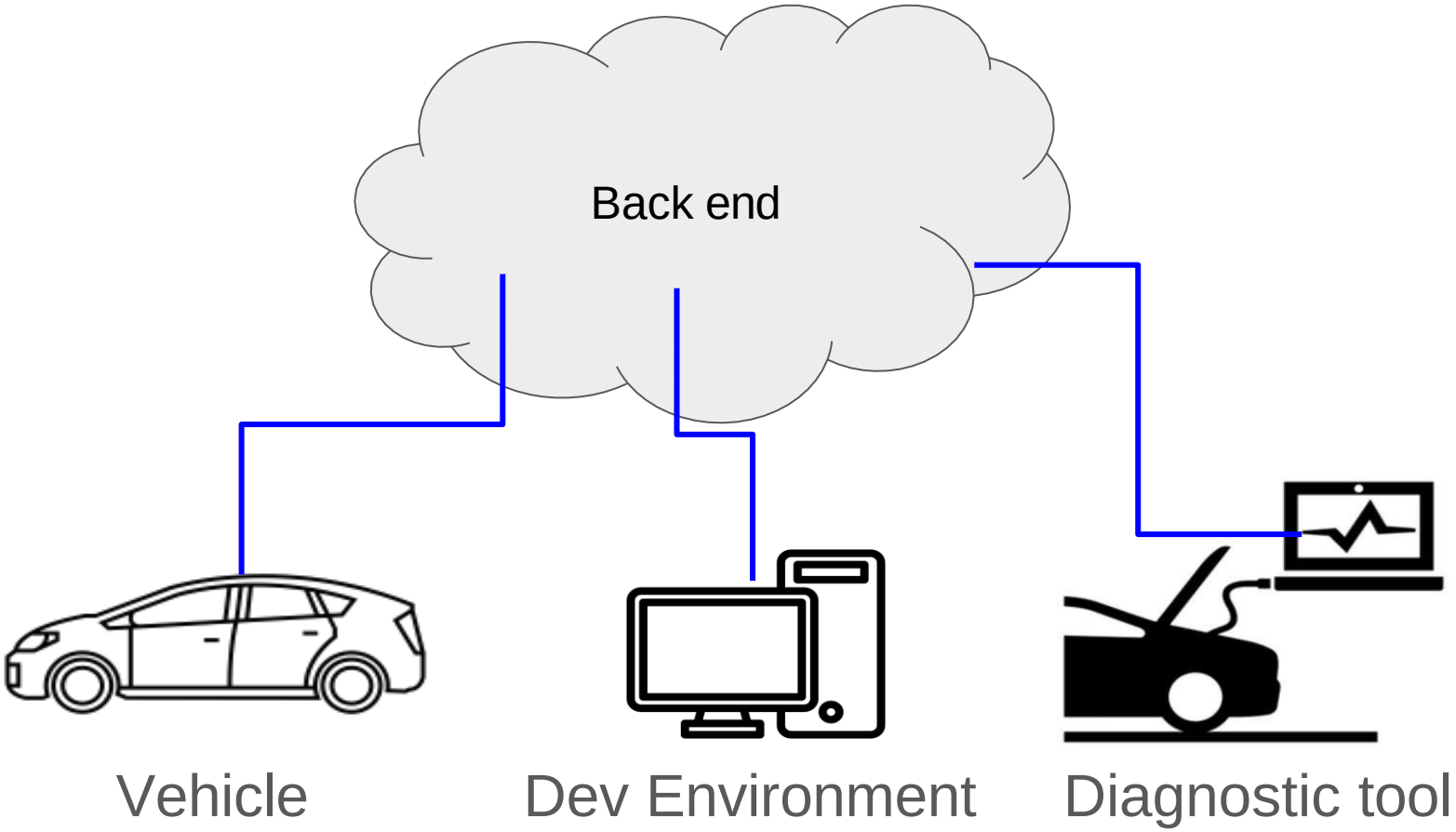
05-2

Trusted Platform Services (TPS)

Example Keystore



Example Keystore



Trusted Platform Service benefits

01

Standardised services

Open standard: less internal effort
Competition between vendor

02

Maximise portability

The same use application could run regardless if the device has a TEE, a secure element or nothing (example during development).

03

Service discovery

Flexibility: can query which services are available.

Thank you

Global Platform™

Oct 24/25th, 2024

Post Quantum Cryptography Update

Olivier Van Nieuwenhuyze

GlobalPlatform Policies

Please be aware that this meeting is being held in accordance with **GlobalPlatform's Bylaws and GlobalPlatform policies issued thereunder,** including but not limited to:

- Antitrust Policy
- IPR Policy
- Member Confidentiality Requirements
- Meeting Protocol and Guidelines

Above policies are set forth in the **GlobalPlatform Process and Procedures Manual** or **IPR Policy v5.0**, available on the Member website: Resources → Documents

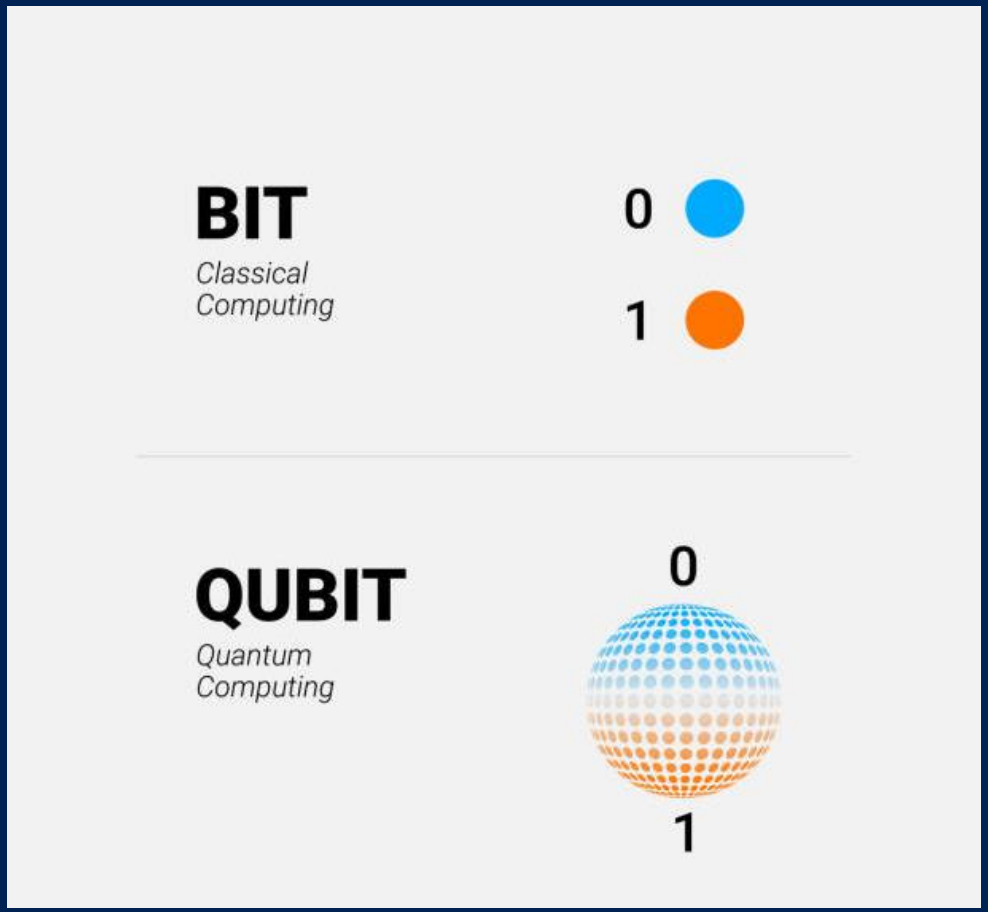
Patent Call

"Please be aware that this meeting is being held under the GlobalPlatform Intellectual Property Rights Policy. If you do not have a copy of this policy, please contact (or inform) the chairperson during this meeting. You may also view and download a copy of the policy at the Membership section of the GlobalPlatform Website.

At this time, each person in attendance is required to inform the chairperson if they are personally aware of any claims under any patent applications or issued patents which would be likely to be infringed by an implementation of any specification or other work product which is the subject of this meeting. You need not be the inventor of such patent or patent application in order to inform GlobalPlatform of its existence, nor will you be held responsible for expressing a good faith belief which proves to be inaccurate."

The Quantum Computer

QUBIT

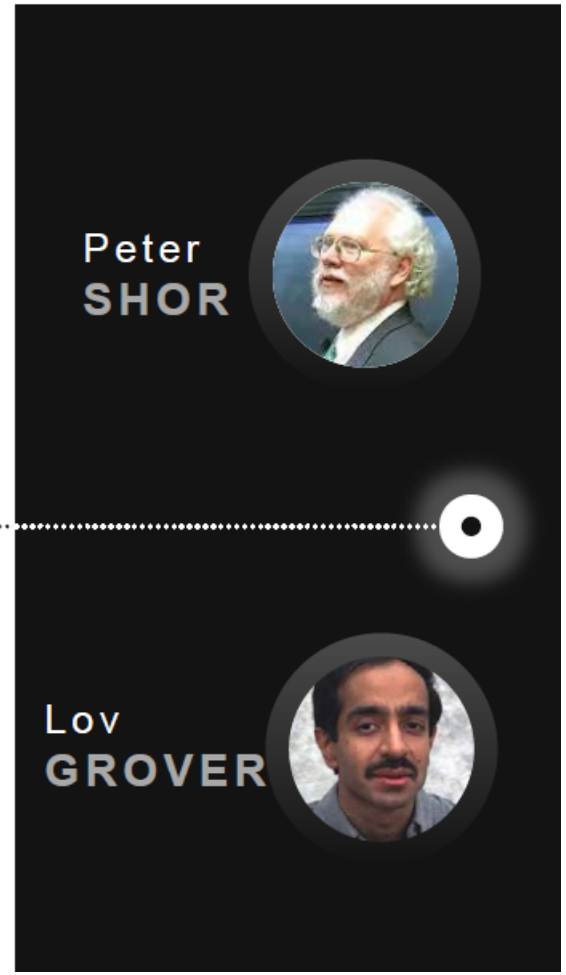


Global Platform™

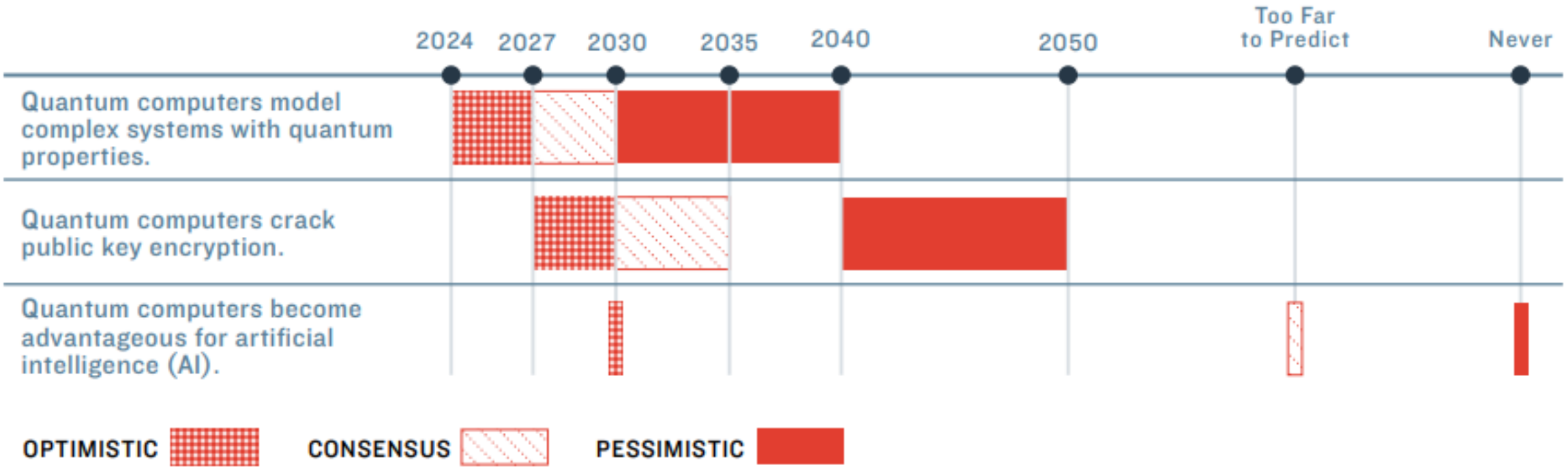
How Quantum Computer Impacts Cryptography?

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	No longer secure
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
AES	Symmetric key	Encryption	e.g. longer keys needed
SHA-2, SHA-3	----------	Hash functions	e.g. larger output needed

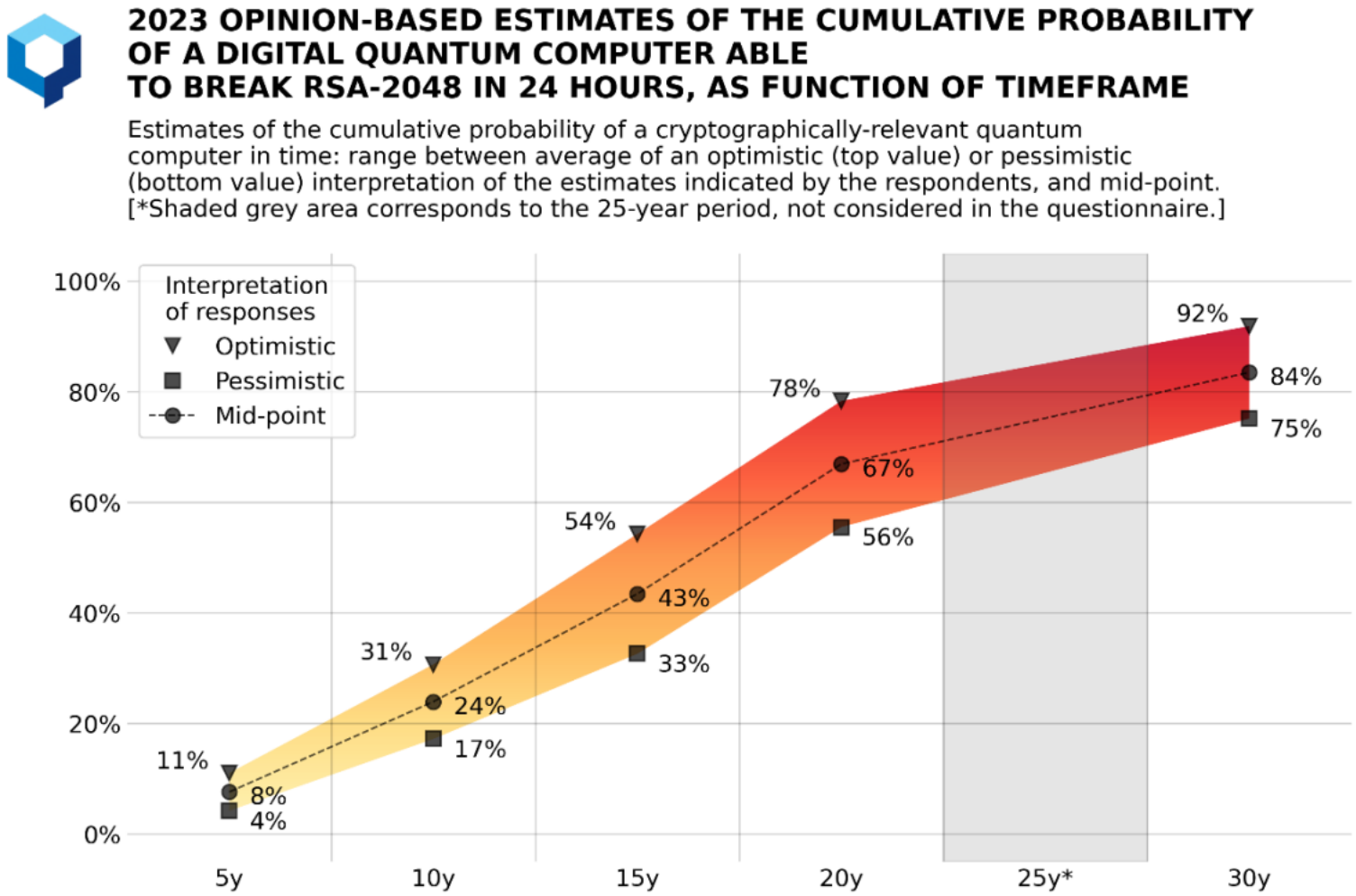


PQC predictions (2022)



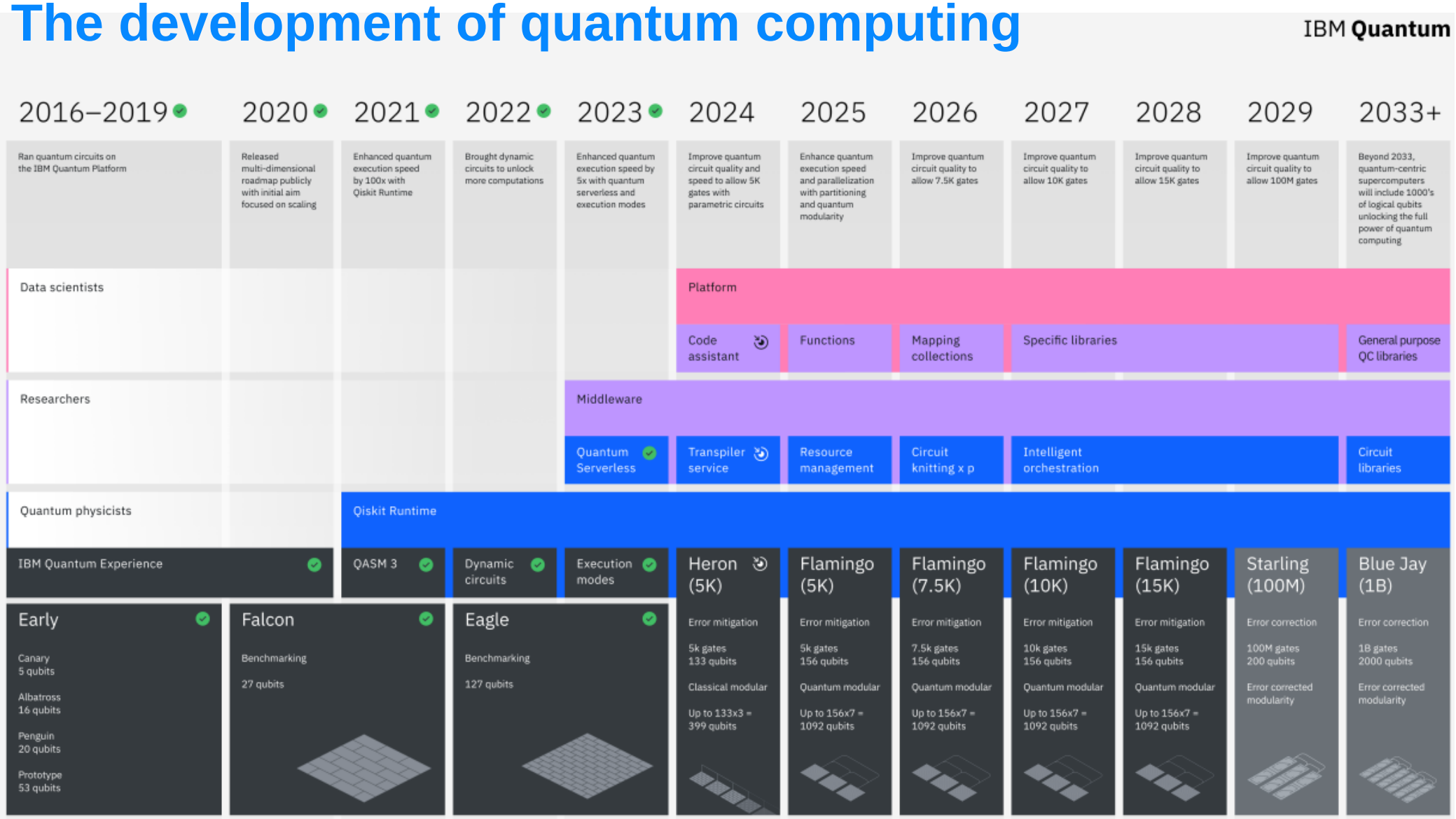
*Source: https://www.cisoforum.com/wp-content/uploads/2022/01/chinese-threats-quantum-era.pdf

PQC Predictions (2023)



Source : https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

The development of quantum computing



*Source: https://www.ibm.com/quantum/technology

The challenges facing current cryptography

The limitations of current cryptographic systems

- Vulnerability to quantum attacks
- Long-Term security concerns

The threat posed by quantum computers

- Quantum supremacy
- Risk of data breaches

The impact on security infrastructure

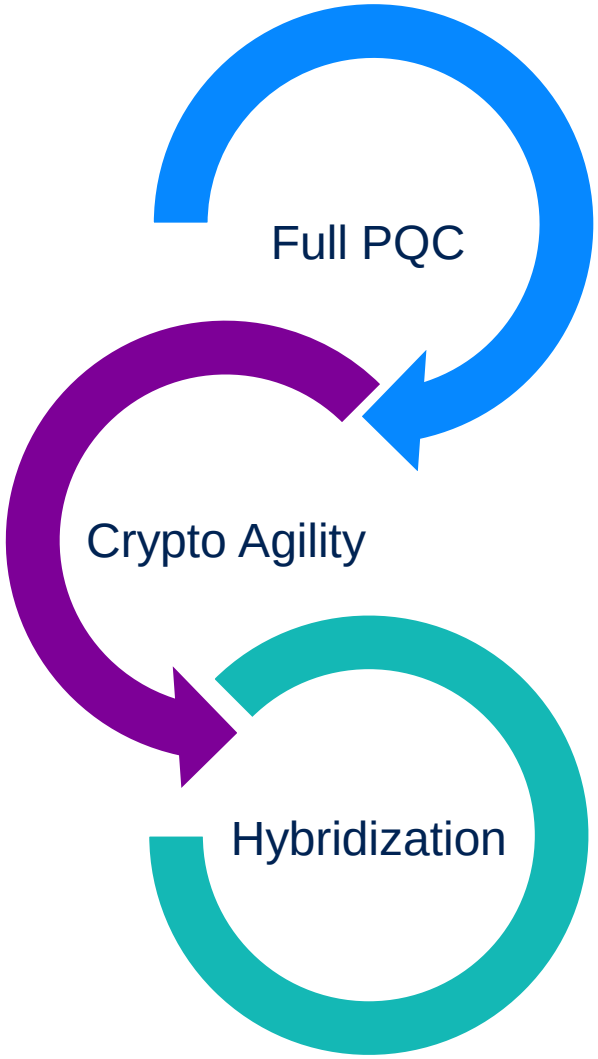
- Re-evaluation of security protocols
- Urgency of the transition

PQC: is it really a problem?

Yes.

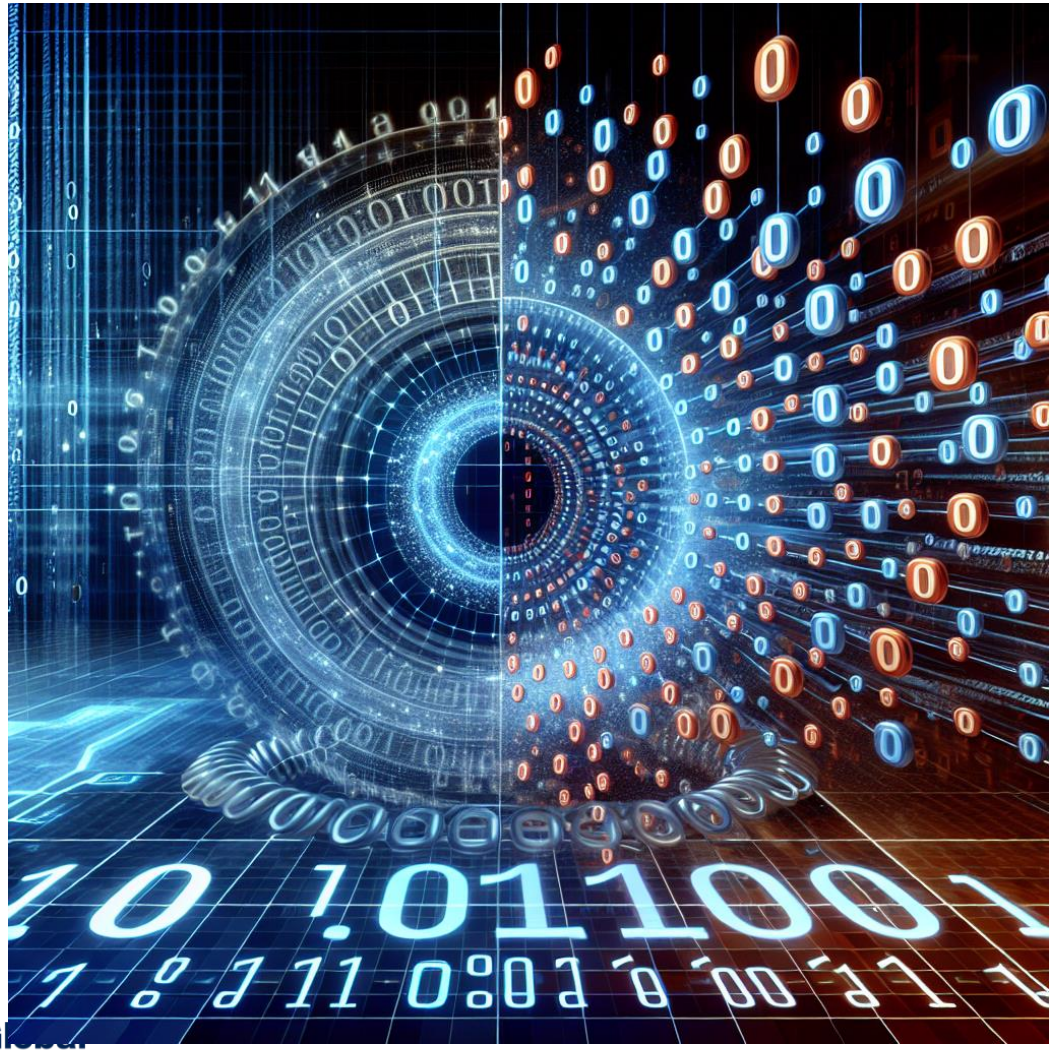
- Finding the right solution can require significant effort.
- Migrating / deploying the solution is difficult and time-intensive.
- It is also urgent. There is a real risk today of “store now, decrypt later” attacks.

What is the solution?



Global Platform™

What are the challenges of PQC migration?



Compatibility issues

- Legacy systems
- Interoperability

Performance concerns

- Computational overhead
- Resource constraints

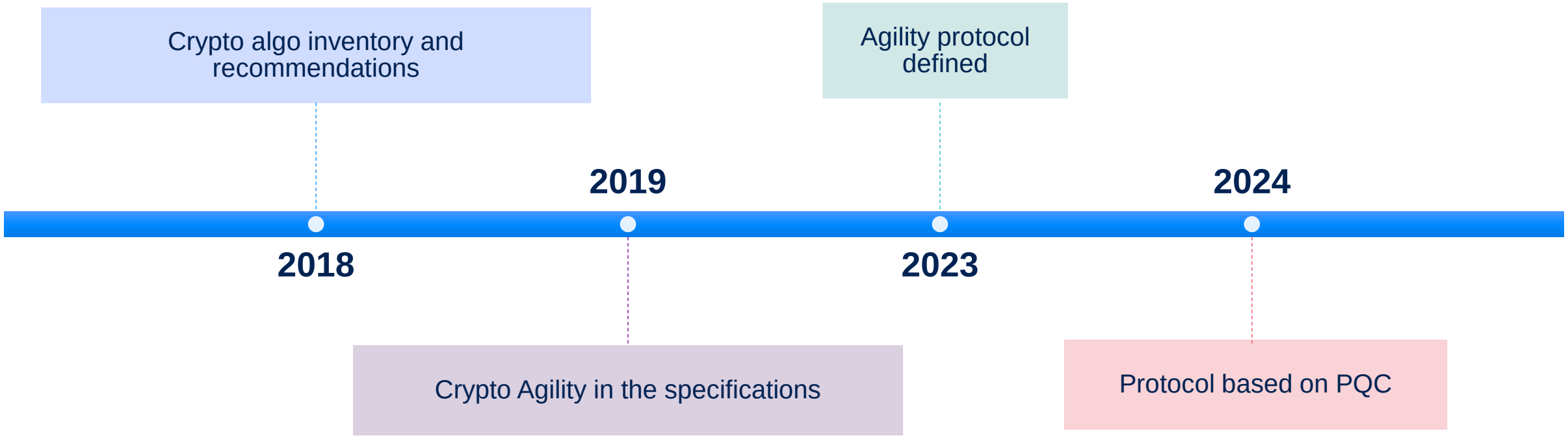
Implementation complexities

- Algorithm selection
- Security assurance

Transition strategy

- Phased approach
- Training and awareness

Timeline


Crypto algo inventory and recommendations
Agility protocol defined
2019
2024
2018
2023
Crypto Agility in the specifications
Protocol based on PQC

NIST Solution

Full PQC

Standard

- **ML-KEM - FIPS 203**: Published August 2024.
- **ML-DSA - FIPS 204:** Published August 2024.
- **SHL-DSA FIPS 205:** coming soon.

Additional round with remaining algorithms

New Round for Additional Round for Digital Signature

Global Platform™

PQC development challenges

- Availability of standardized PQC algorithm (e.g. : ML-KEM, ML-DSA …)
- Replacing existing protocols such as Diffie Hellman to other mechanism (modify the exchange dynamic)
- Cryptography security strength vs the HW feasibility

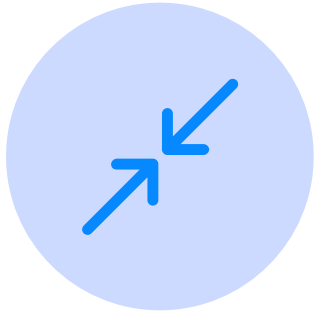
Security strength / Crypto algos	Symm. Algos	Factoring (RSA)	DLP (DSA, DH)	ECC (ECDSA, ECDH)	Hash	ML-KEM	ML-DSA
≤ 80 bits	3DES 2 keys	1024	1024	160	SHA-1		
112 bits	3DES 3 keys	2048	2048	224	SHA-224		
128 bits	AES-128	3072	3072	256	SHA-256	ML-KEM-512	ML-DSA-44
192 bits	AES-192	7680	7680	384	SHA-384	ML-KEM-768	ML-DSA-65
256 bits	AES-256	15360	15360	512	SHA-512	ML-KEM-1024	ML-DSA-87

PQC migration into the existing infrastructure

CONSTRAINT OF THE DEPLOYMENT

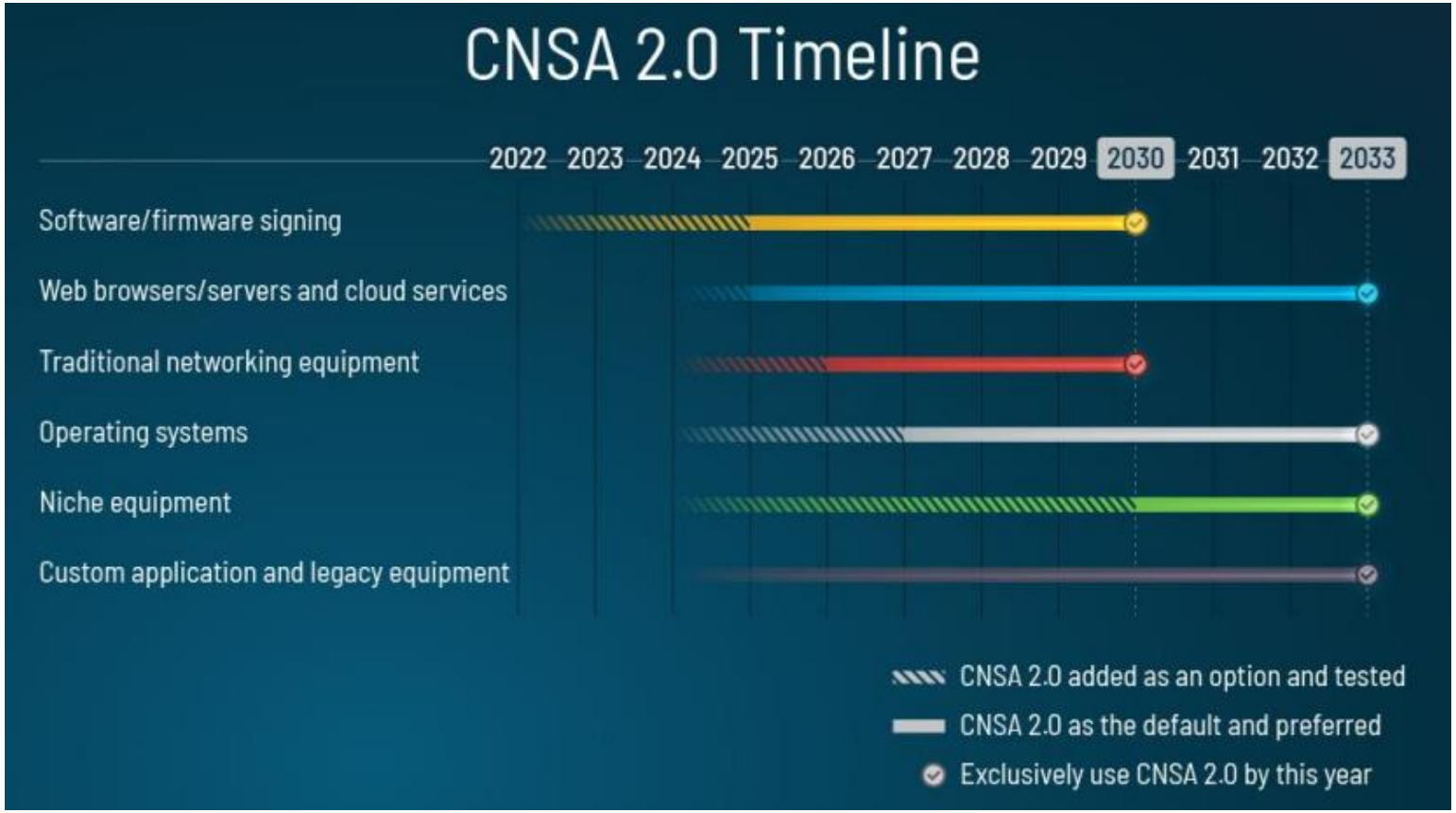
CRYPTOGRAPHY AGILITY

REGULATION



USAGE OF THE HYBRIDIZATION

Regulations Increase the complexity



EU required different security levels (than US) but some countries mandate the hybridization

Conclusions

CHALLENGE TO MIGRATE AND DEPLOY SYSTEM ON THE CURRENT INFRASTRUCTURE

CHALLENGE TO BE COMPLIANT WITH THE REGULATION

TECHNOLOGY DEPLOYMENT AND FEASABILITY

Global Platform™

The standard for secure digital services and devices

→globalplatform.org

TRUSTONIC

Global Platform™

TEEs on automotive ECUs, mixed criticalities, spectrum: today & tomorrow

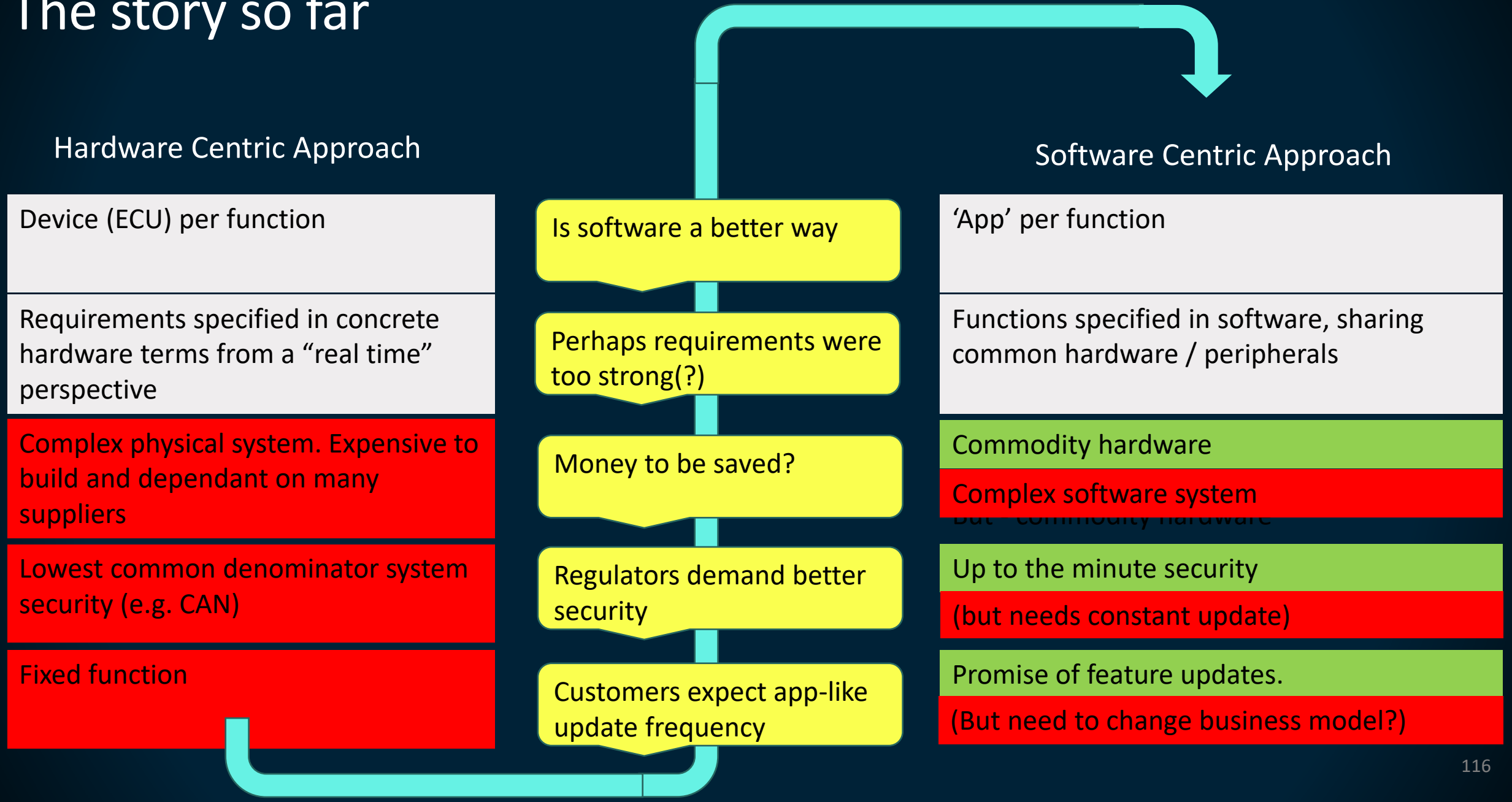
Richard Hayton

Chief Strategy and Innovation Office, Trustonic Ltd.

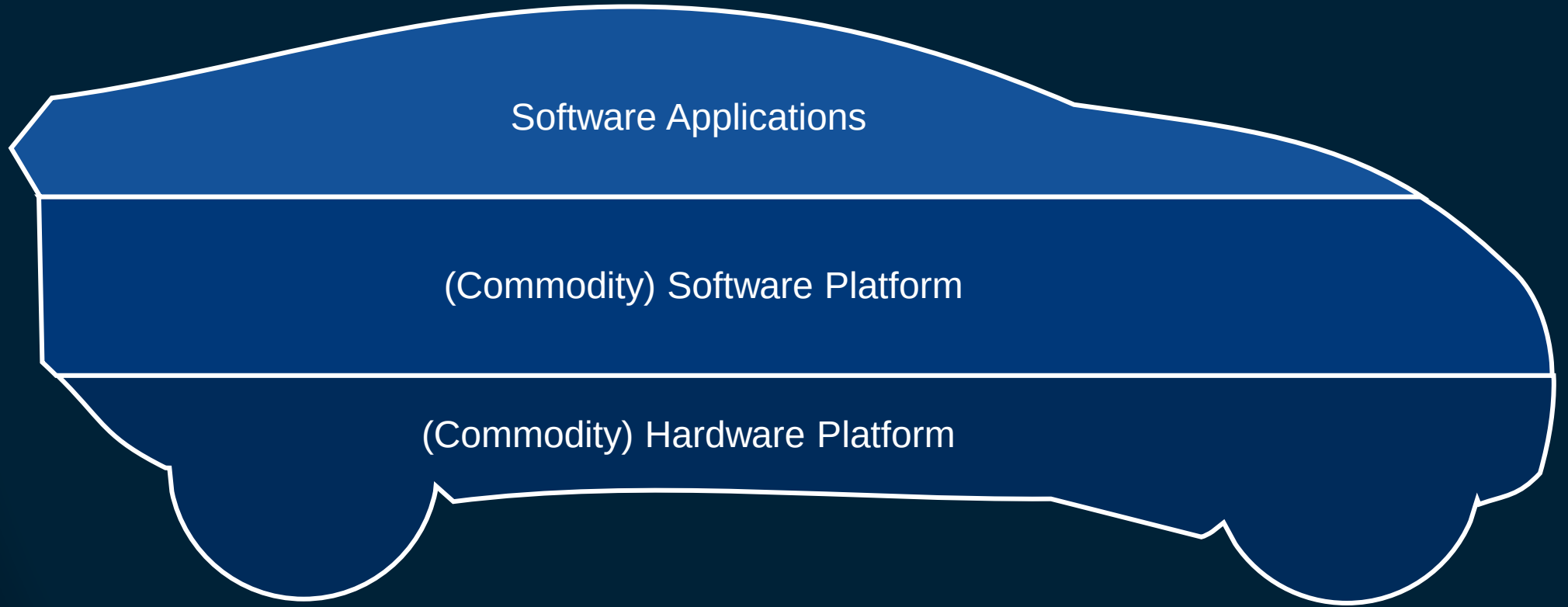
Chair Automotive Task Force, GlobalPlatform

Chair Trusted Environments and Services Committee, GlobalPlatform

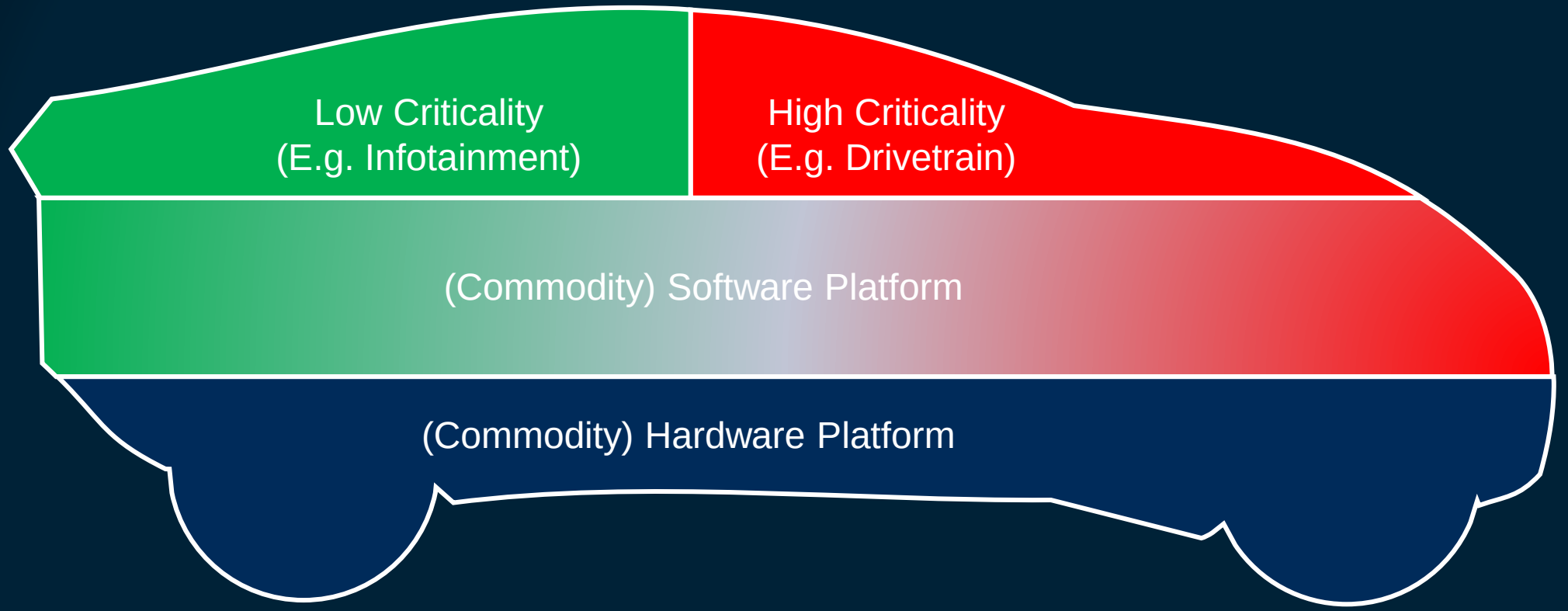
The story so far



Software Defined Vehicles



Robustness Needs for Mixed Criticality



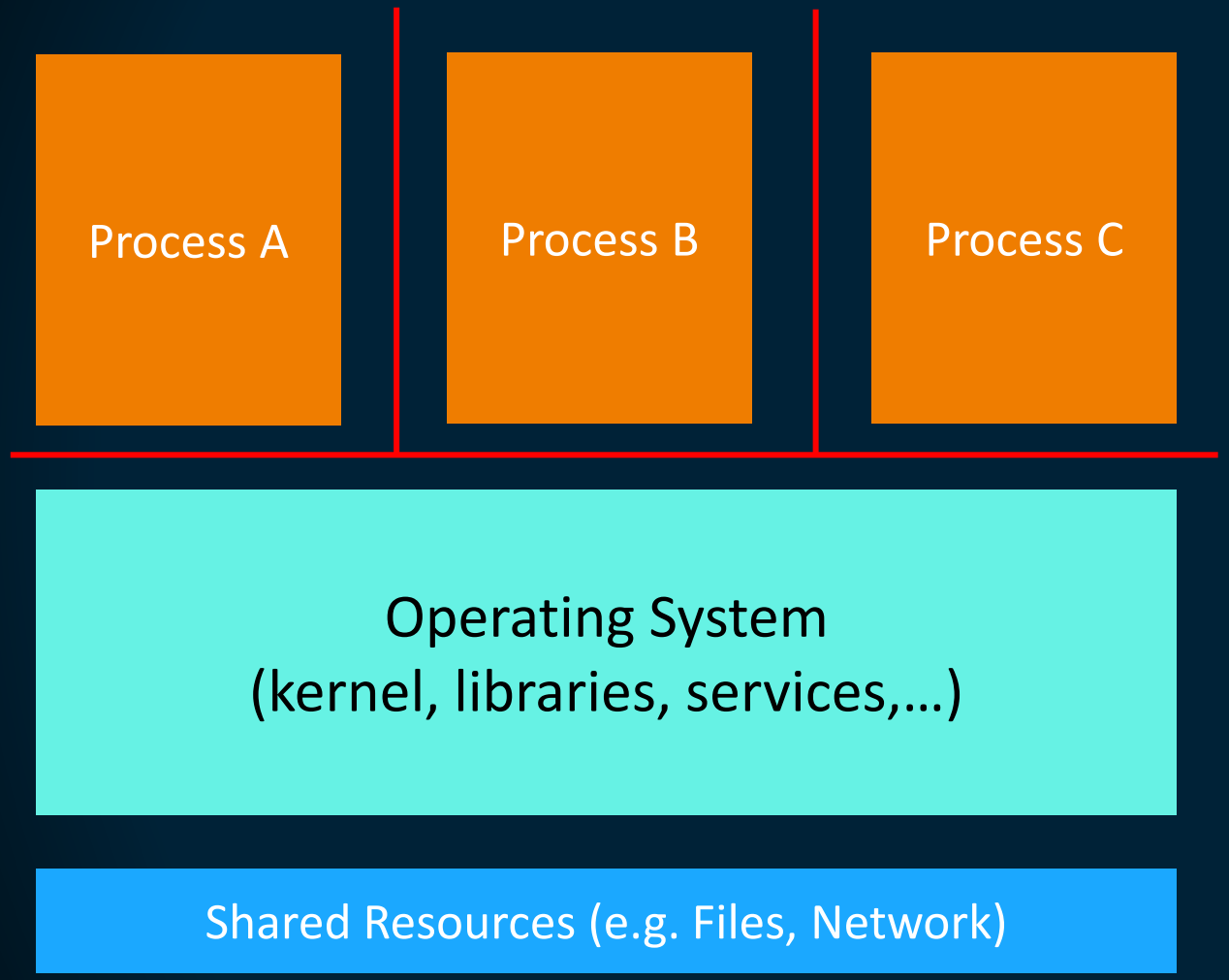
- - **Security** (attack on low criticality does not impact high criticality)
- - **Failure** (failure of low criticality does not impact high criticality)
- - **Performance** (degradation of low criticality does not impact high criticality)
- - **Update** Resilience (update to low criticality does not impact high criticality)

Sharing & Isolation Technologies

- Modern CPUs are incredibly powerful (but not cheap)
- Processors, Containers and Hypervisors allow compute resources to be shared whilst
  providing isolation
- This is great for flexibility
- How does it stack up for robustness?

GETTY IMAGES HTTPS://WWW.WIRED.COM/STORY/A-ROBOT-TEACHES-ITSELF-TO-PLAY-JENGA/

Regular Operating System Sharing (Processes)



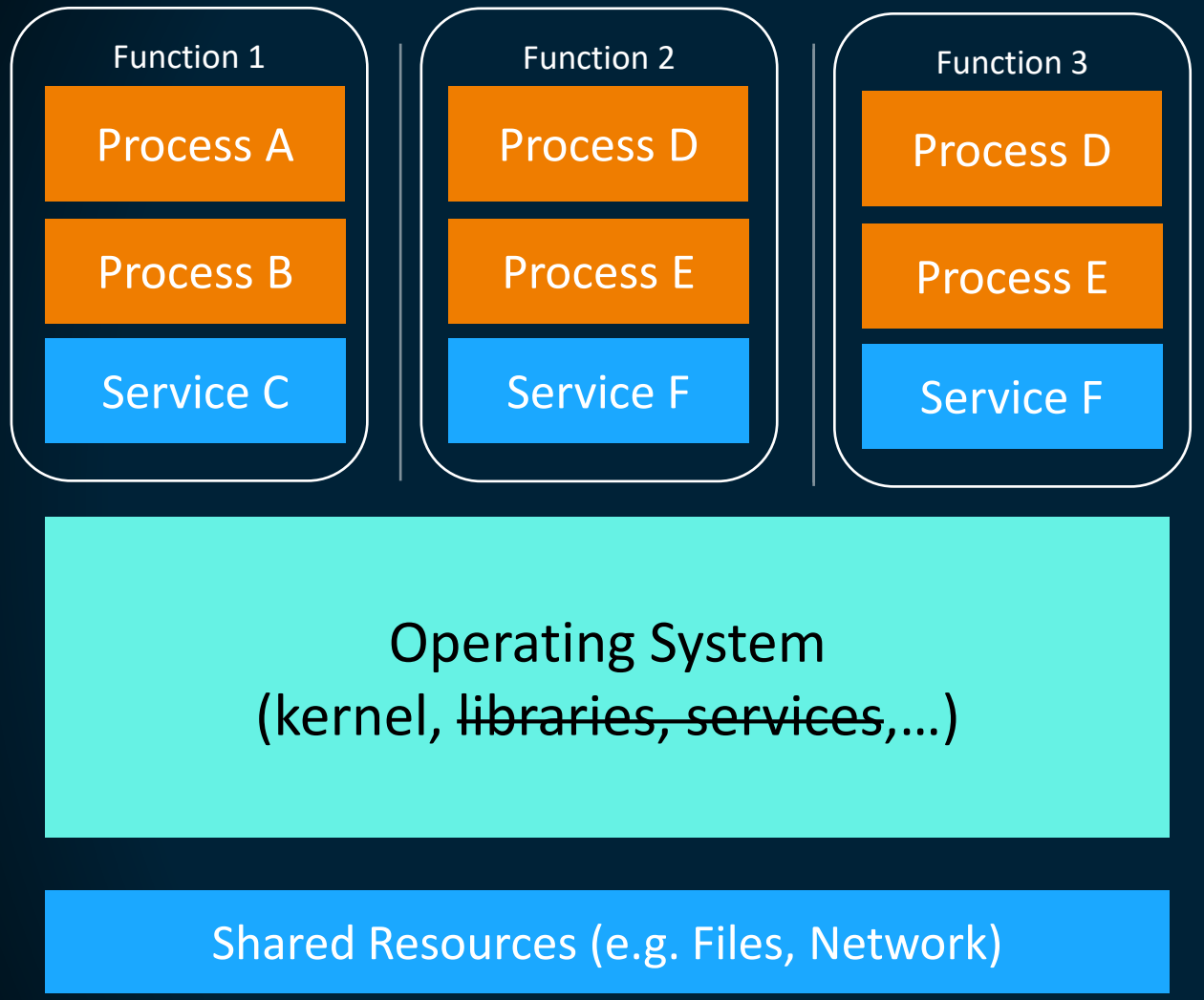
The operating system is shared

- It is responsible for isolating each process and for sharing of other resource
  - Processor (CPU) allocation
  - Physical memory allocation
  - File/Network/Peripheral access

Whilst the OS provides strong process isolation, it is far from perfect especially when shared services are considered

Most operating systems have limited isolation in terms of **Performance** and **Update.**

Containers



Containers are a brilliant solution to manage much of the software complexity in Linux

They allow a multi-process solution to be bundled and run against a known set of libraries

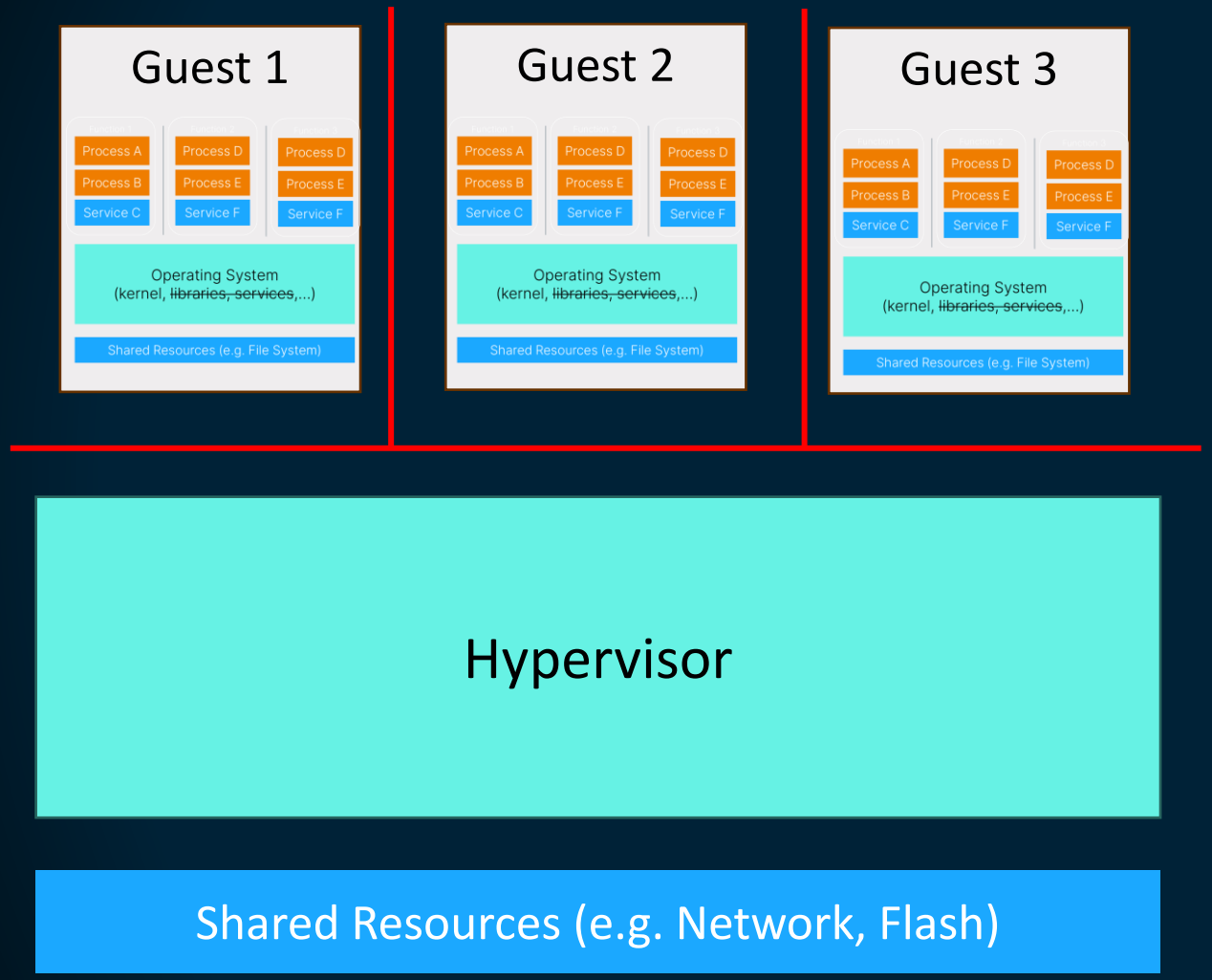
They also make it easier to update and manage software, improving isolation for **Update** and **Failure**

However, containers don't change the **security** or **performance** equations.

An attack on a process can still affect all other processes on the same host.

Containers are for management not security

Hypervisors



Hypervisors provide another layer of isolation and sharing

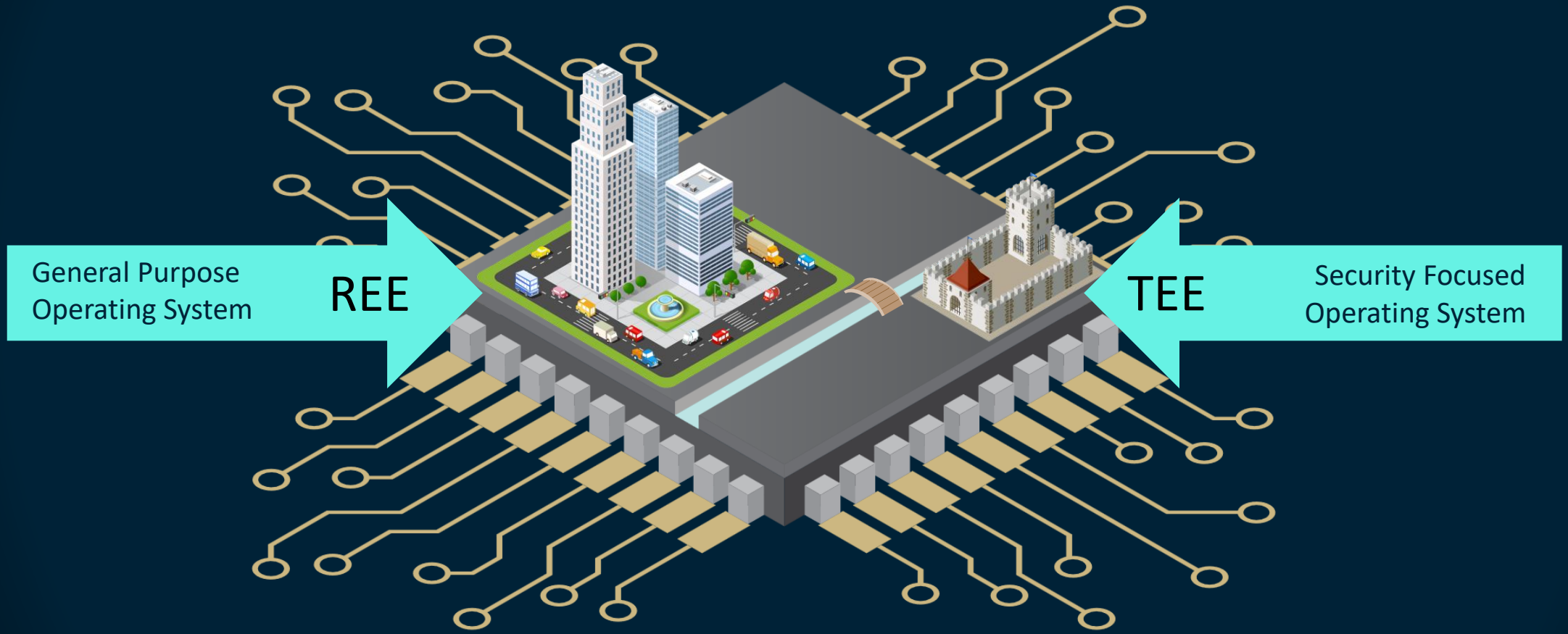
They isolate multiple operating systems (Guests) from each other, and allow each "virtualized" hardware, so that each acts as if it was on its own box.

Hypervisors must share (or allocate) cores, memory and peripherals to guests.

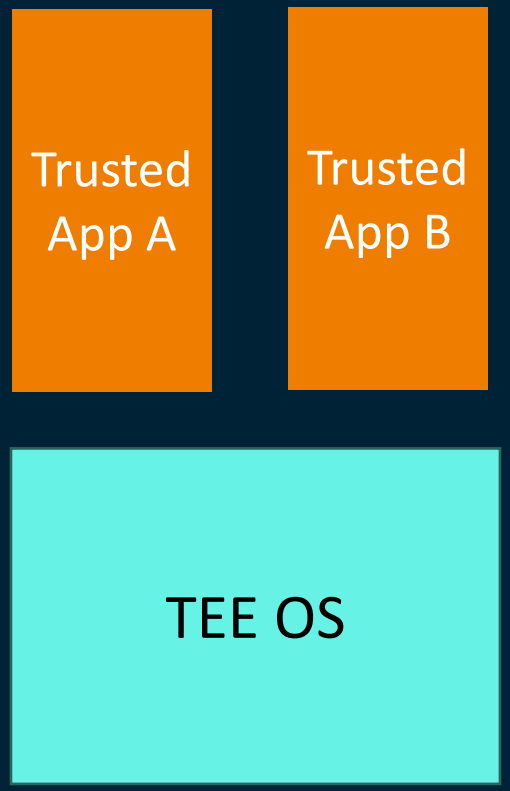
Memory is usually statically allocated, but *separation* Hypervisors also statically allocate cores. This means better isolation at the cost of overall performance.

Hypervisors are the accepted "best option" for providing strong isolation

Trusted Execution Environments



Comparing a TEE OS to a Regular OS



A TEE OS is conceptually very similar to a regular OS in terms of isolation

However, as TEEs are built for security the security isolation is **very good**

GlobalPlatform standardizes APIs and Security isolation – but says nothing about isolation related to **Performance, Failure or System Update.**

This is a new area of discussion within GlobalPlatform

A TEE OS is a service OS

Trusted Apps are used to provide trusted sub-function for REE applications rather than full ECU functions

Trusted Apps compete for resources

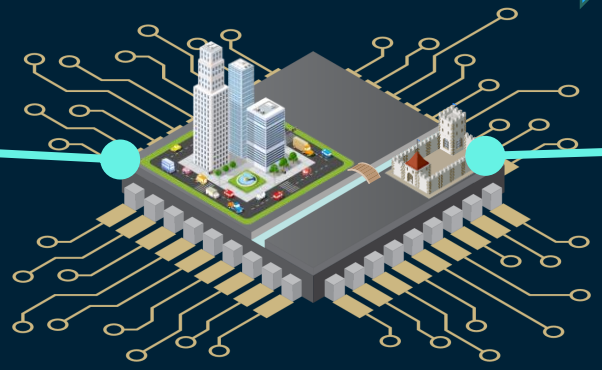
Regular App

- Cryptography / Key Storage
- Protected media (DRM)
- Data Management
- Secure Biometrics…

Trusted App

Trusted App

REE OS

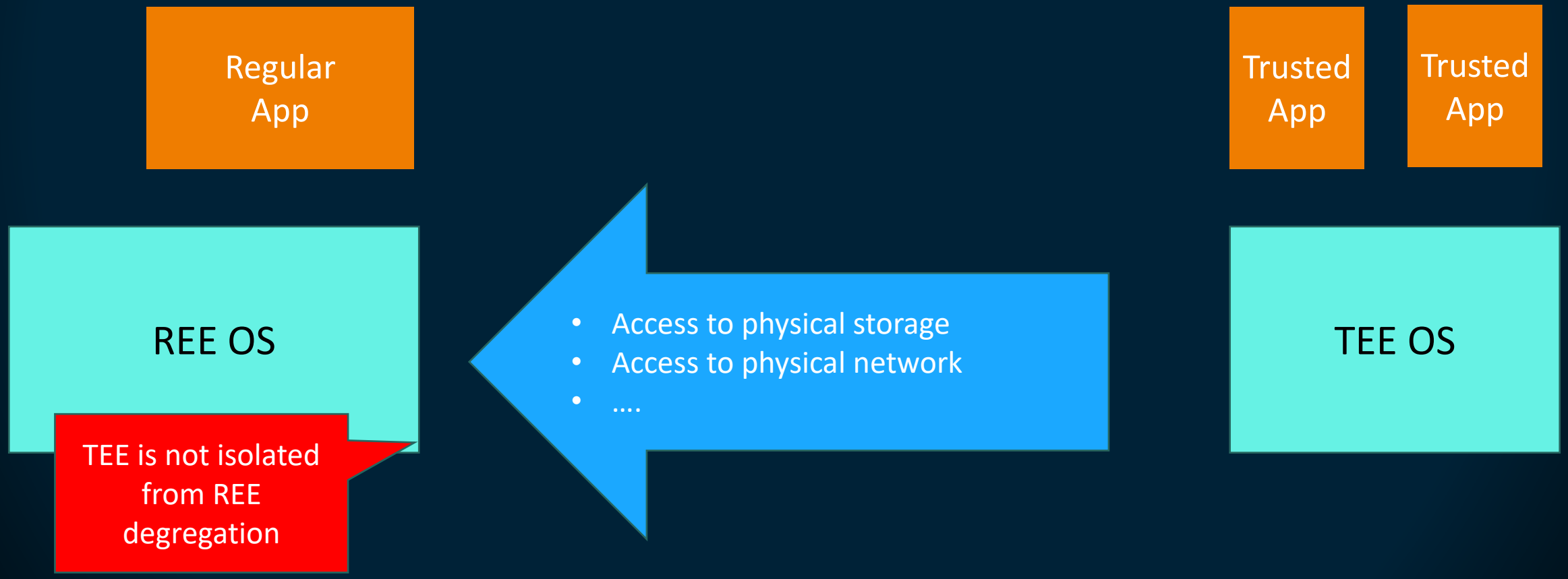


TEE OS

TEE may not provide resource isolation across TAs

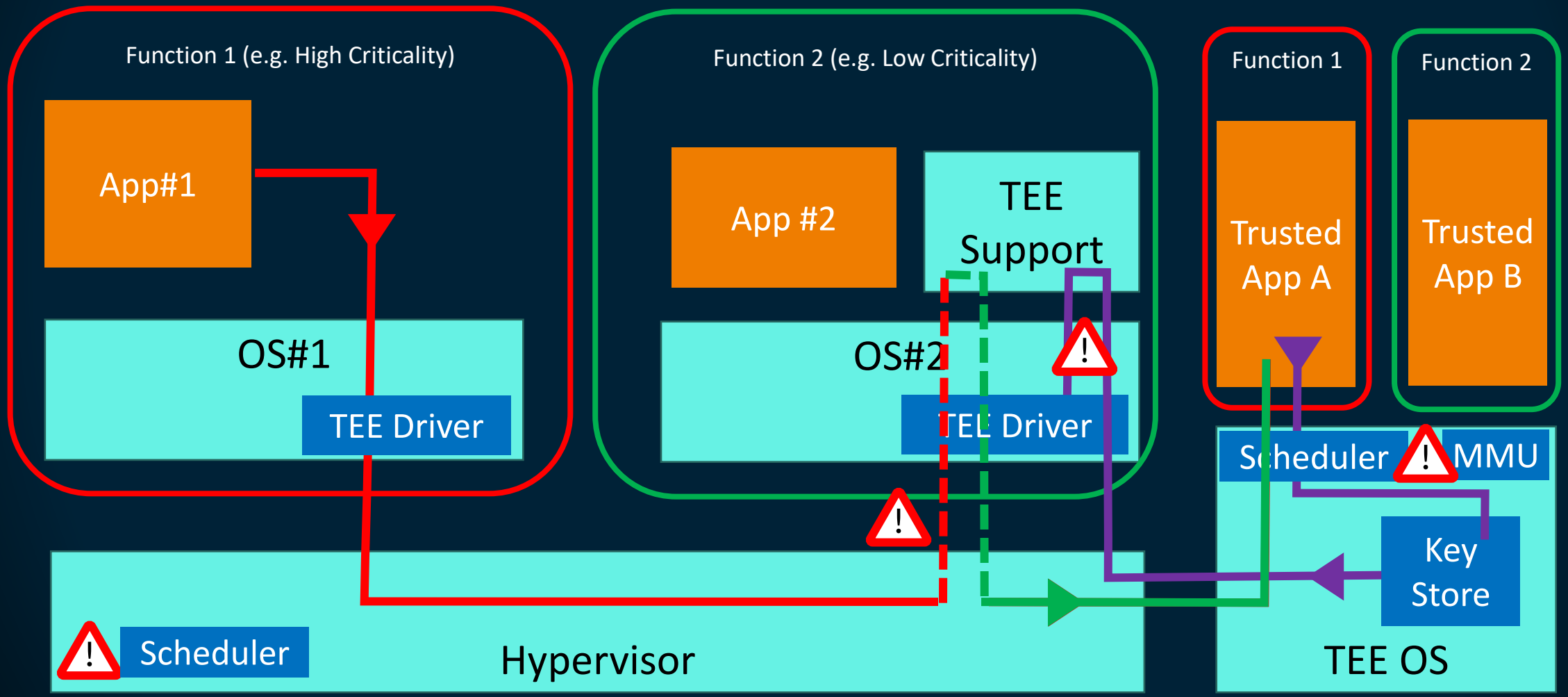
TEE OS usually relies on [a] REE OS

Features like storage or networking are usually delegate back to the REE



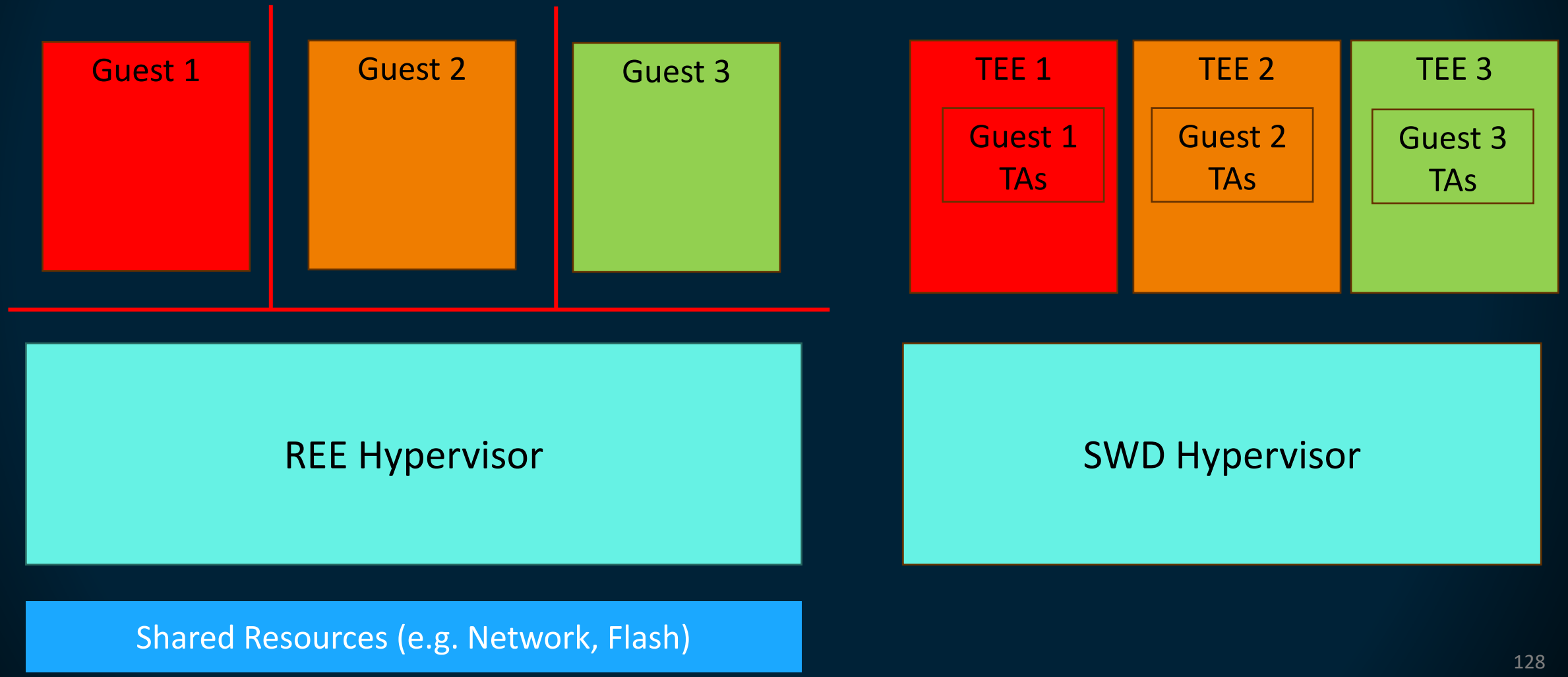
Hidden isolation challenges

- Priority Inversion; shared services; unexpected reliance on low criticality systems



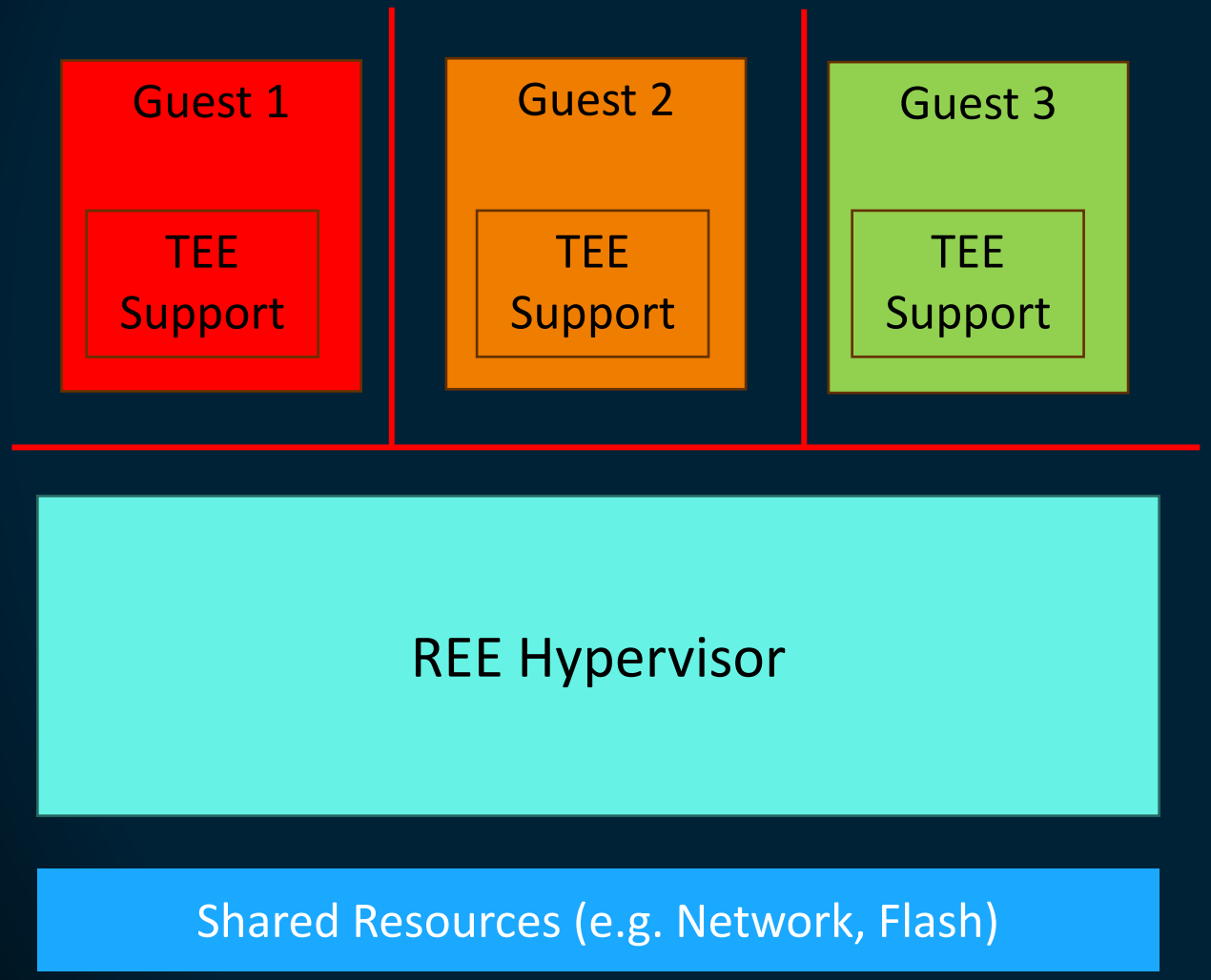
Meeting TEE Challenges (1)

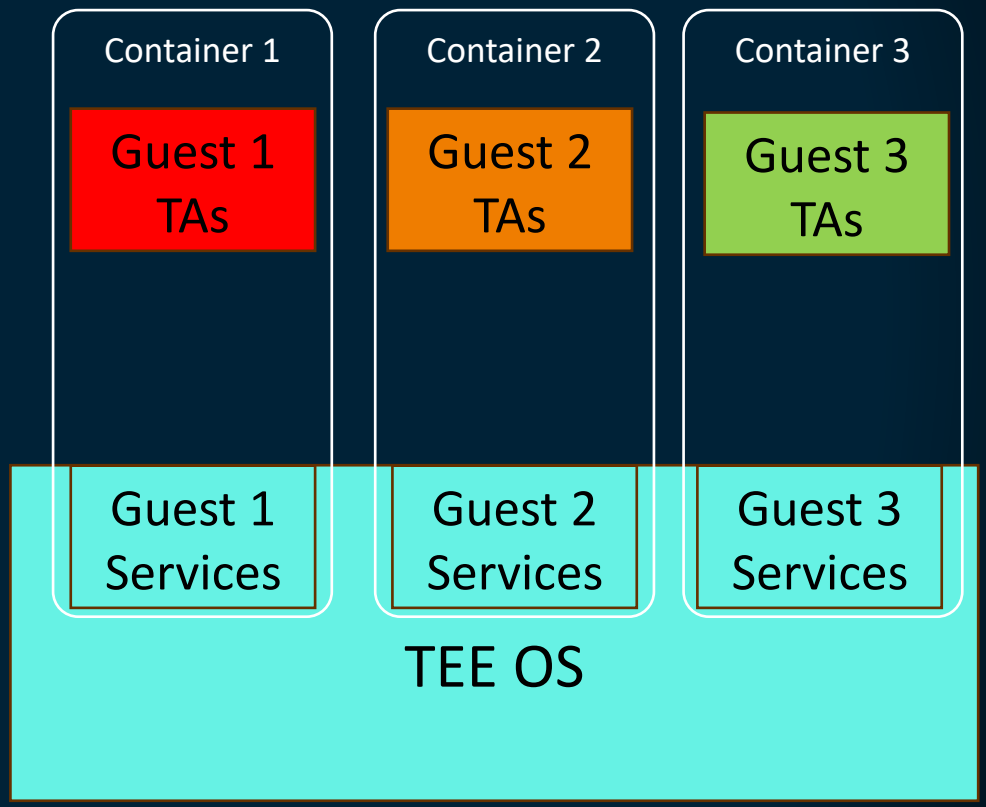
- We can [in theory] introduce a hypervisor to secure world – but this is very heavyweight!



Meeting TEE Challenges (2)

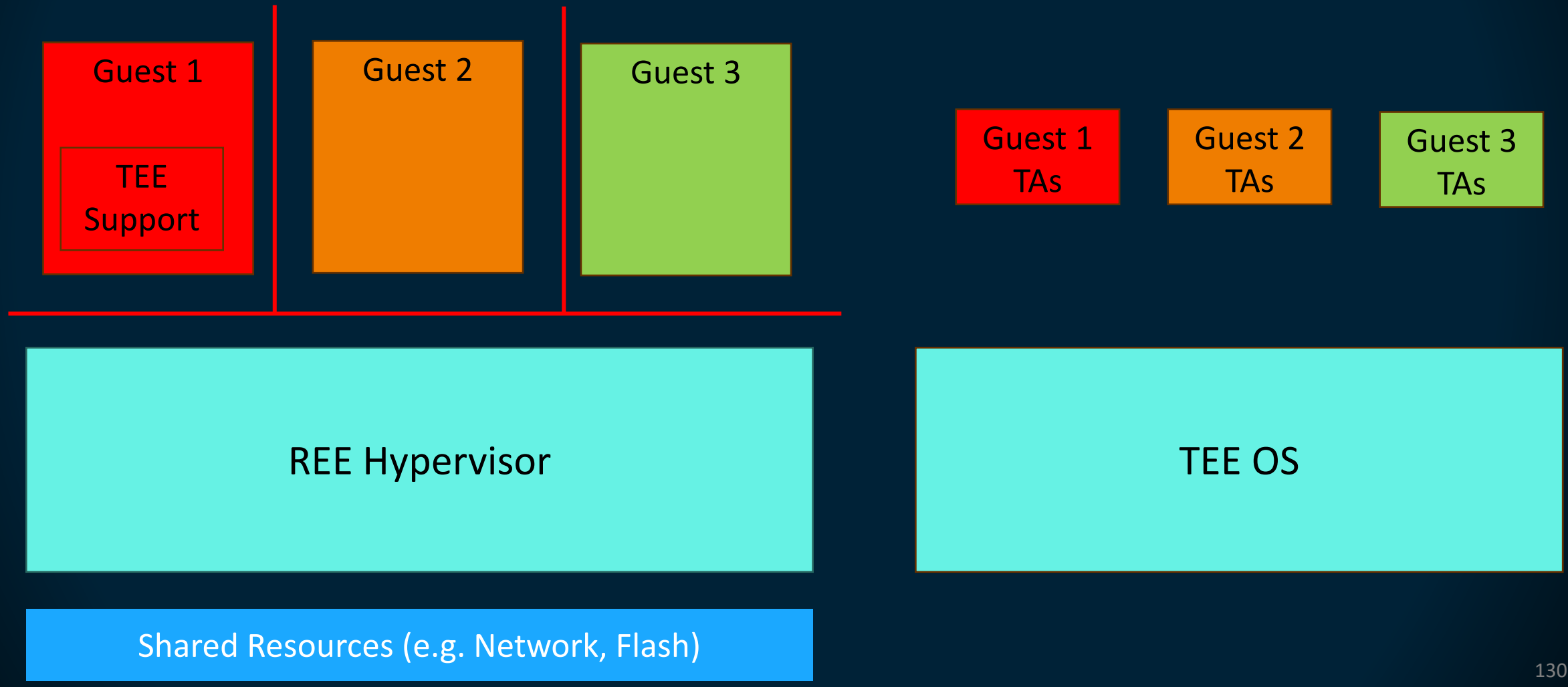
- Could ‘containerizing’ the TEE and spreading support across guests solve isolation problems?





Meeting TEE Challenges (3)

- A common pragmatic option is to ensure the TEE support services are in a High Criticality guest



Summary

- Software Defined Vehicles need a combination of technologies
  - Containers
  - Hypervisors
  - TEEs

- The first-generation solutions statically allocated resources for different criticalities
  - Cores/Memory (Separation Hypervisors)
  - TEEs/Security Processors (Allocated to a single guest)

- There is a desire for more sharing to reduces costs / improve efficiency

- Different commercial solutions “may exist”
  - Not currently covered by standards
  - But GlobalPlatform is starting discussions

BLACKDUCK®

SBOM in Automotive – Know What's in Your Car

Dennis Kengo Oka
Senior Principal Automotive Security Strategist and Executive Advisor

GlobalPlatform Automotive Security Roundtable
2024/10/24, Tokyo, Japan

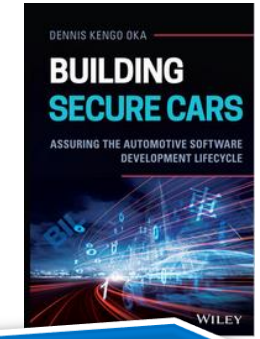
Speaker Information: Dennis Kengo Oka

BLACKDUCK®

Senior Principal Automotive Security Strategist &
Executive Advisor

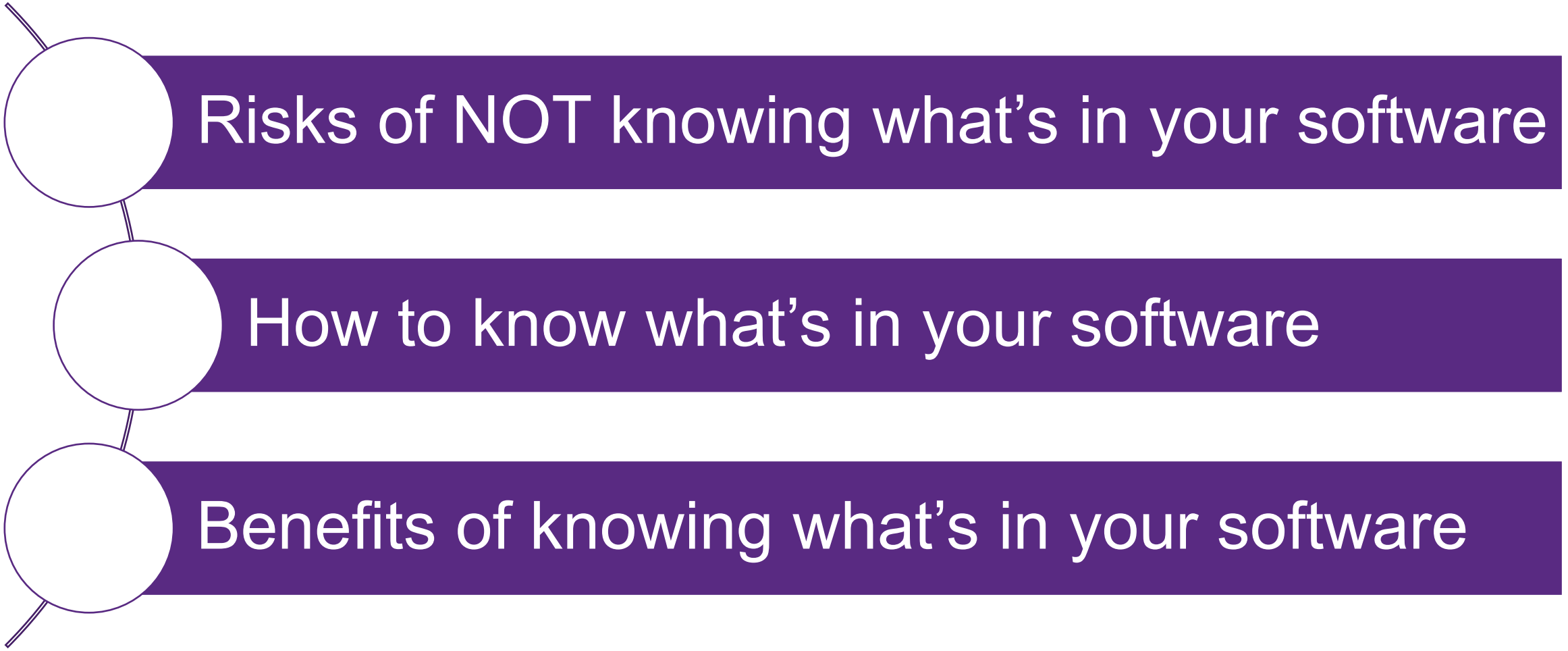
Solutions for secure automotive software development

dennis.kengo.oka@blackduck.com

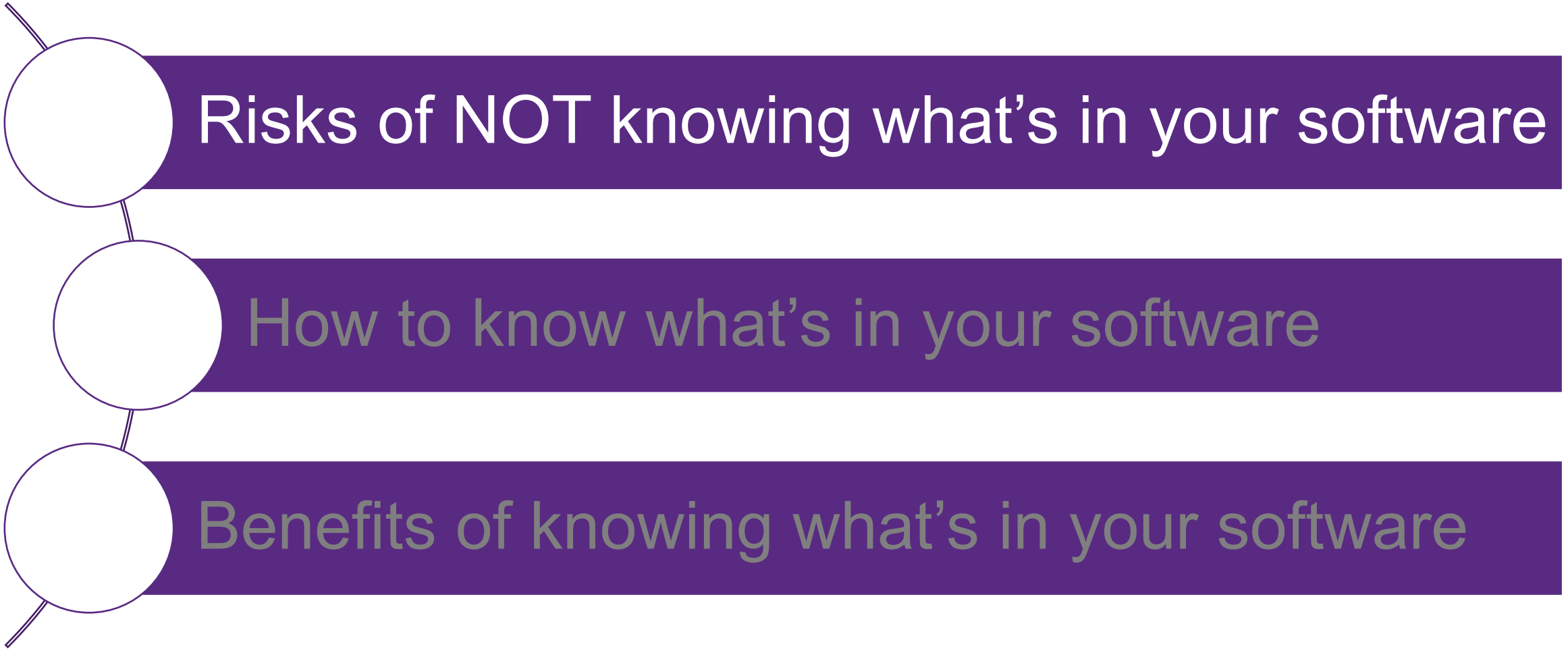


Author of the books: "*Building Secure Cars: Assuring the Automotive Software Development Lifecycle*" and "*Building Secure Automotive IoT Applications: Developing Robust IoT Solutions for Next-Gen Automotive Software*"

Agenda

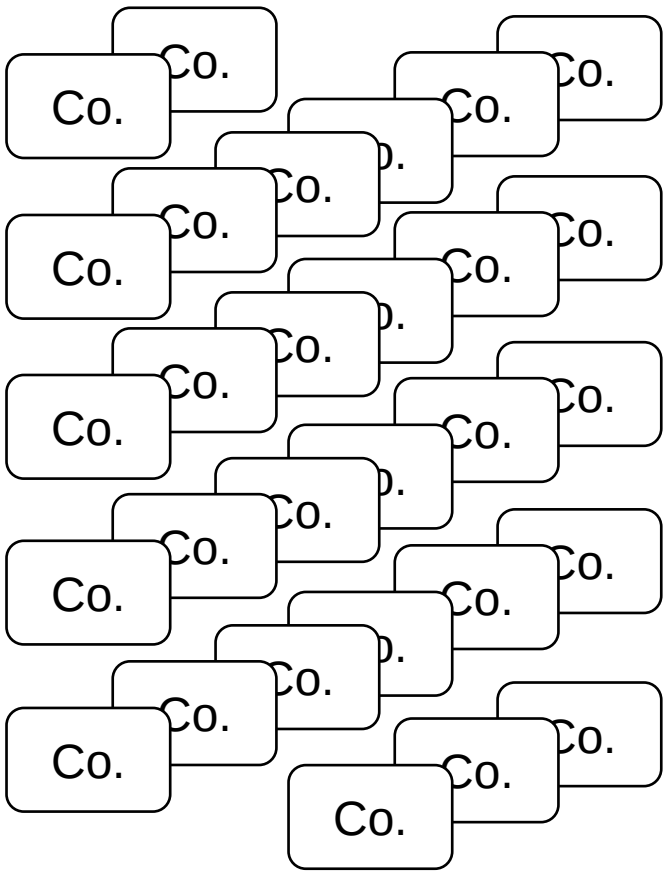


Agenda



Automotive Supply Chain

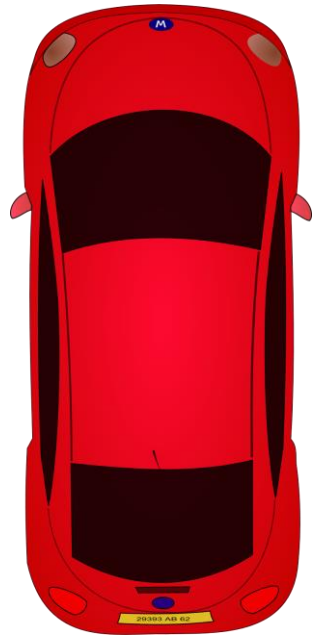
~200+ Software Suppliers



~70-100 ECUs

ECU	ECU	ECU
ECU	ECU	ECU
ECU	ECU	ECU
ECU	ECU	ECU
ECU	ECU	ECU
ECU	ECU	ECU
ECU	ECU	ECU
ECU	ECU	ECU

Vehicle

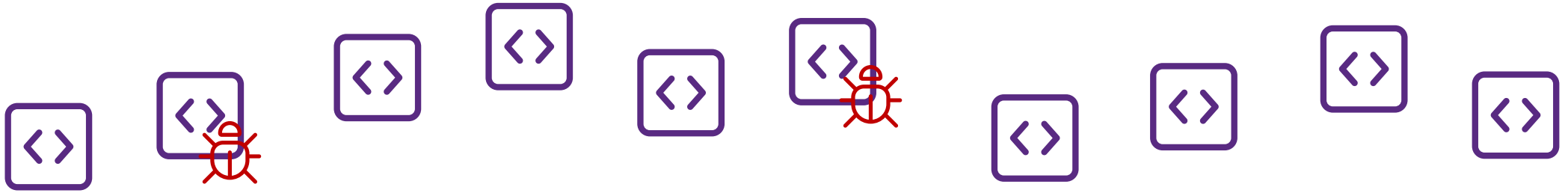


BlueBorne: Bluetooth Vulnerabilities Expose Billions of Devices to Hacking

- Estimated more than 5 billion affected devices
- Bluetooth implementations in Android, iOS, Linux and Windows

Is Your Car Vulnerable?

- Which vulnerabilities affect which versions of software?
- Which software versions are included in my products?
- I.e., which products are vulnerable?
- (is the vulnerability exploitable, how easy/hard is it to exploit etc.)



Need to know which software are included in our products

OSS Risks

Security

- Vulnerabilities in OSS that can be exploited

License

- Lawsuits due to non-compliance with license terms and conditions

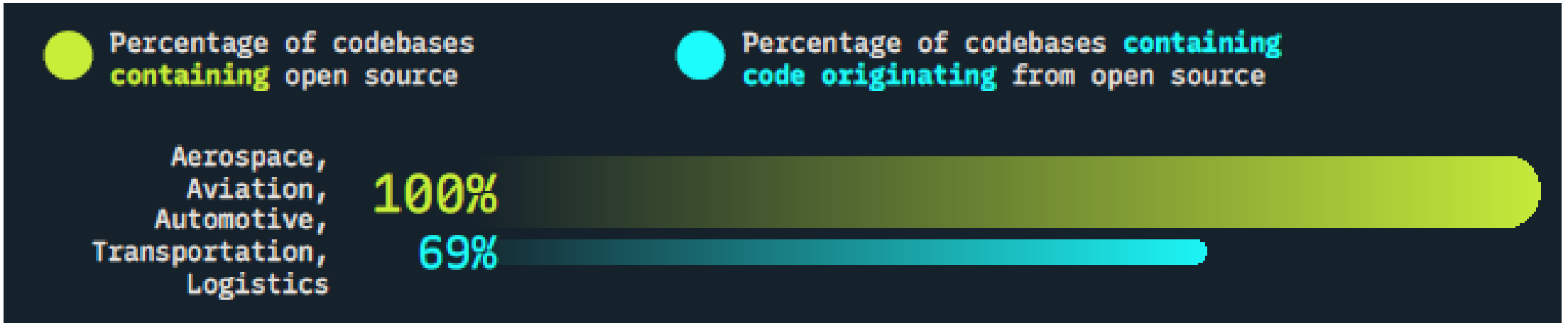
Maintenance

- No timely bug fixes or addition of new functionality due to inactive OSS communities

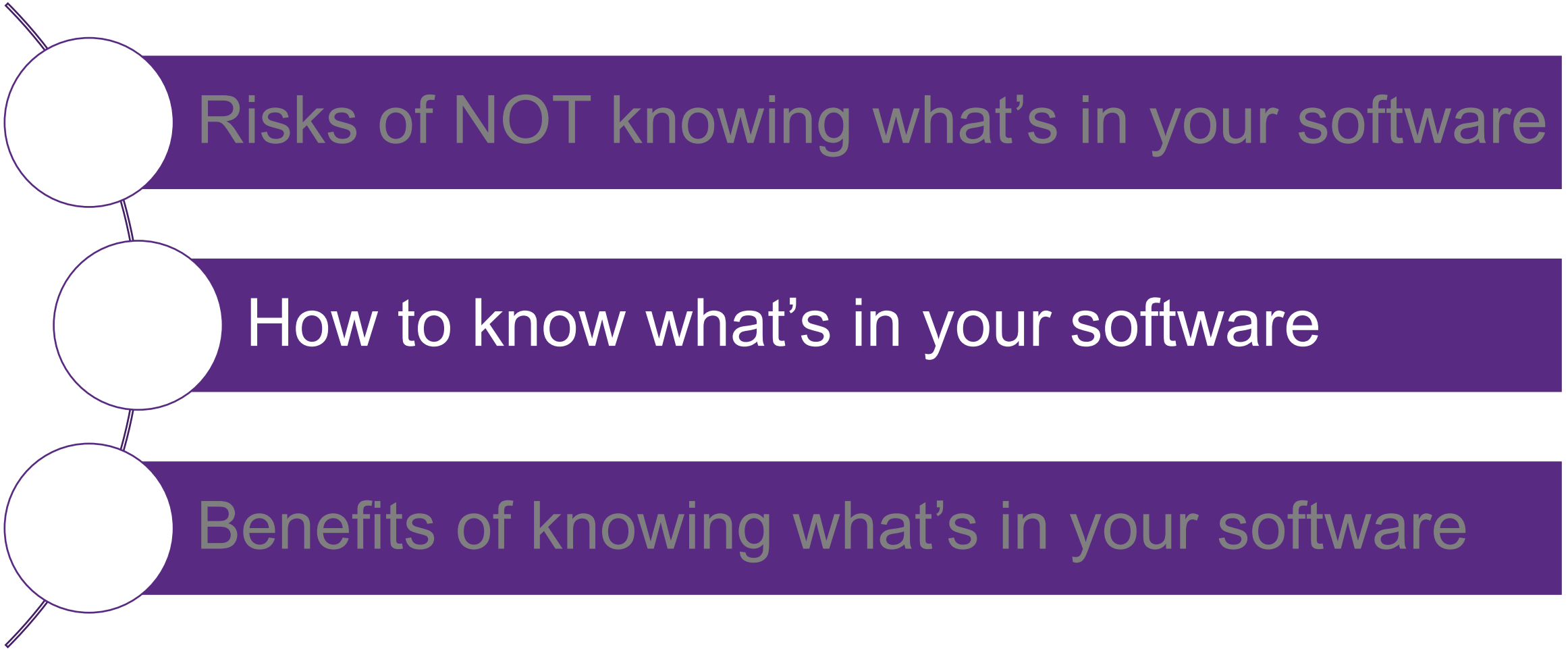
Open Source Security and Risk Analysis Report 2024 (OSSRA)

https://www.blackduck.com/blog/open-source-trends-ossra-report.html

OSSRA 2024 - Automotive

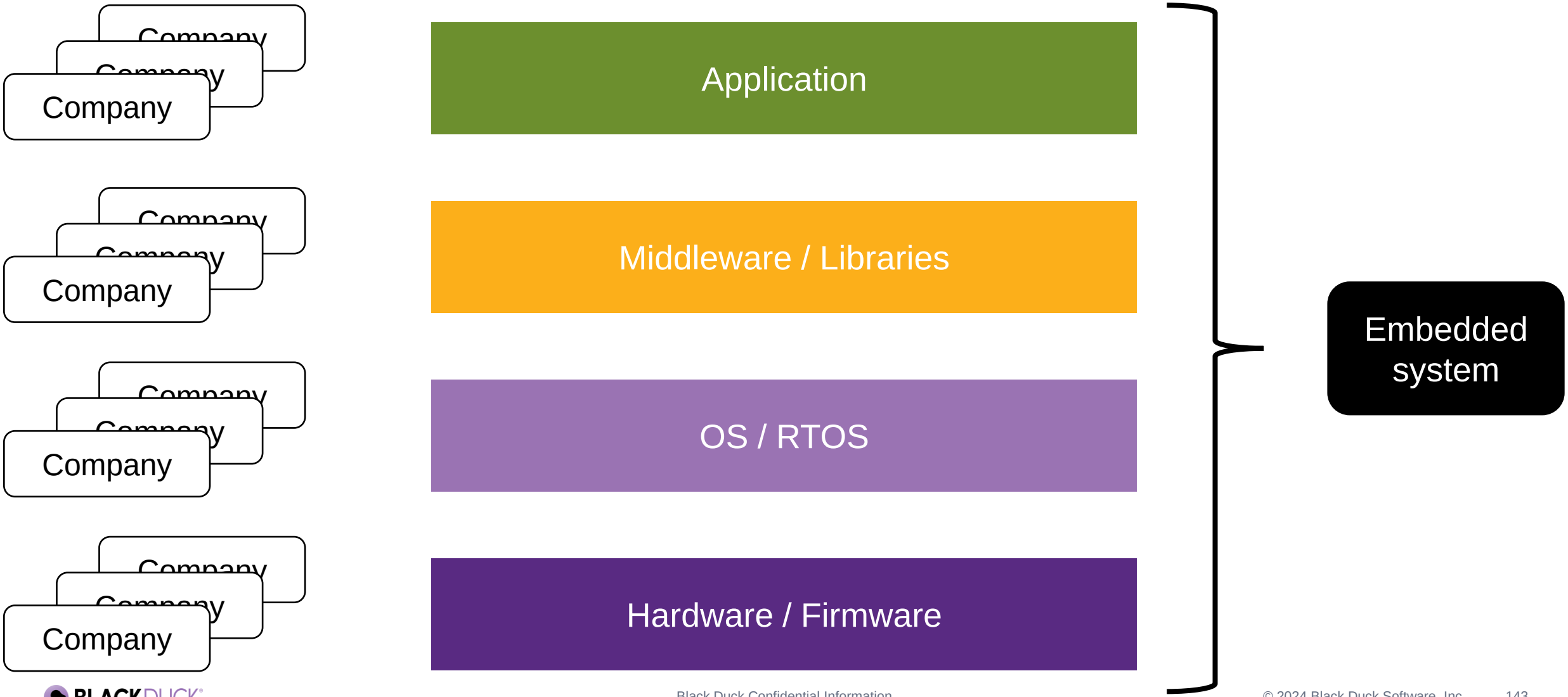


Agenda



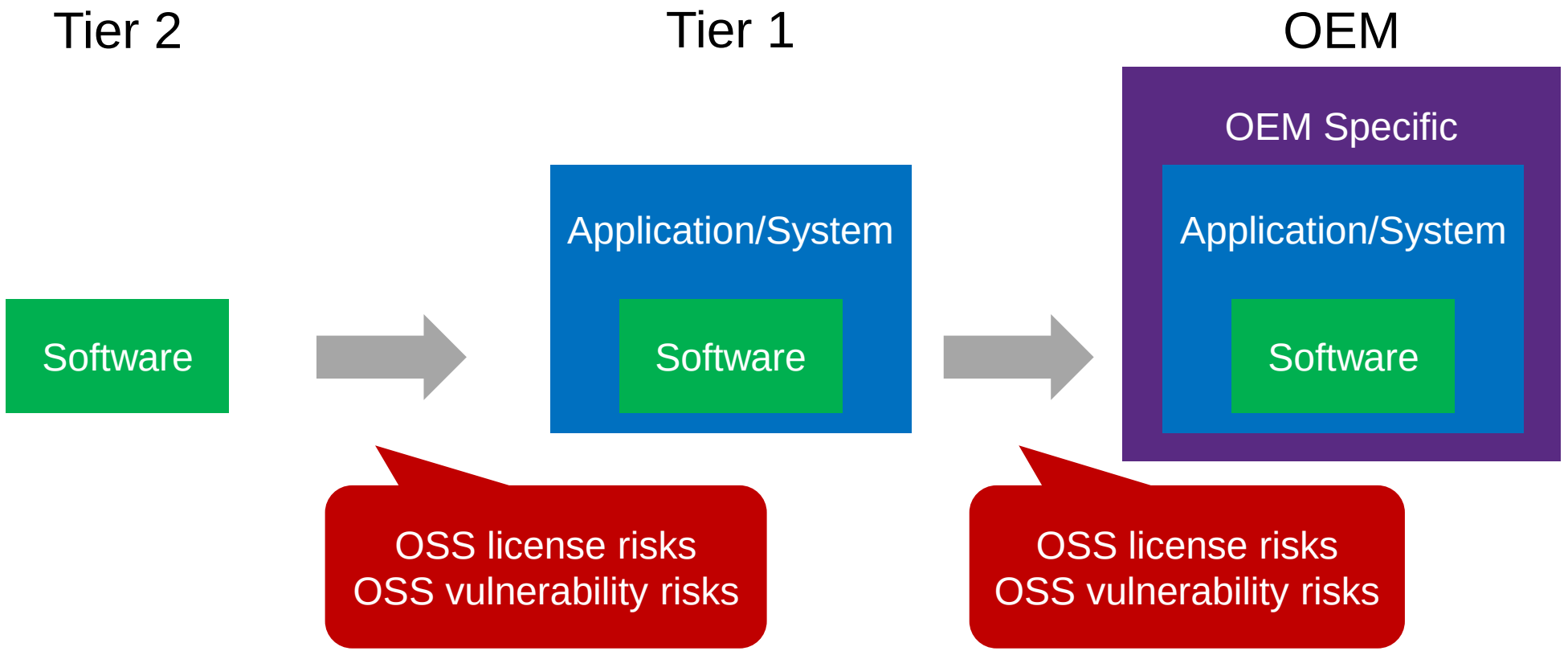
OS: Operating System
RTOS: Real Time Operating System

Complex Supply Chain for Embedded Systems



OSS: Open-Source Software
OEM: Original Equipment Manufacturer

Software Supply Chain OSS Risks



Binary supplied - Two options for the receiving side:

- Trust what the supplier tells you what's in the binary
- Perform binary analysis with a software composition analysis tool

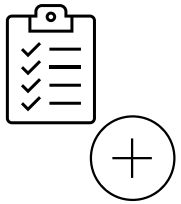
Recommendations:

- Trust but verify
- Scan both source code and binaries, if possible

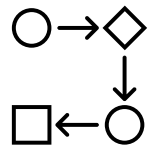
Overview of OSS Processes

- **OSS whitelist**
  - List of acceptable OSS components
  - Requires periodic reviews

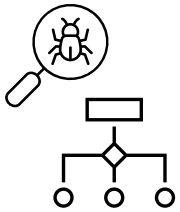
- **OSS policies**
  - Acceptable licenses
  - Number of vulnerabilities/criticality
  - How long OSS project has existed
  - Number of active developers



- **Process for adding OSS to the whitelist**
  - Evaluation criteria
  - Approver

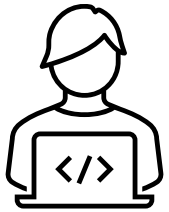


- **OSS utilization process**
  - Store OSS component information
  - Cybersecurity monitoring of OSS components

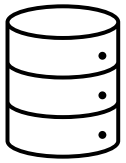


- **OSS vulnerability process**
  - Addressing OSS vulnerabilities

Development Process and Tools



Developers



Source code

Build

Static application security testing

Functional test tools

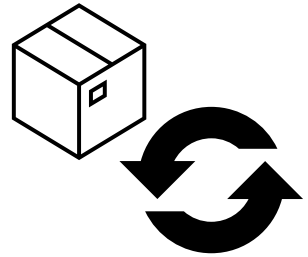
Interface test tools
Network test tools

Fuzz testing tools

Dynamic application security testing

Software composition analysis

- SBOM
- License information
- Vulnerability information



Deploy

Software Composition Analysis is the Foundation

Visibility
Know what components are entering your code

Security
Be alerted to vulnerabilities in development and production

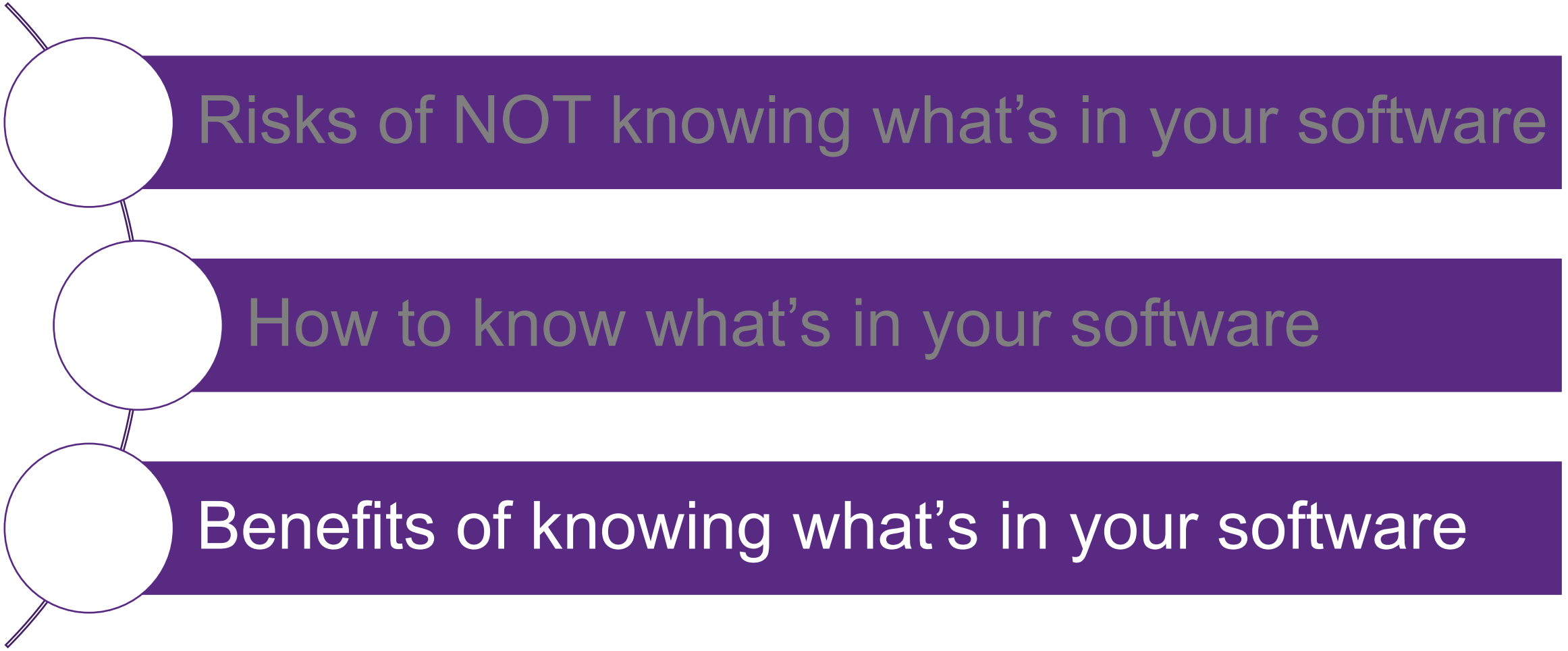
Compliance
Avoid IP and legal risks due to OSS license violations

Control
Automate policies to govern what components enter your code

Know what's in your code
Establish visibility & control of your software supply chain

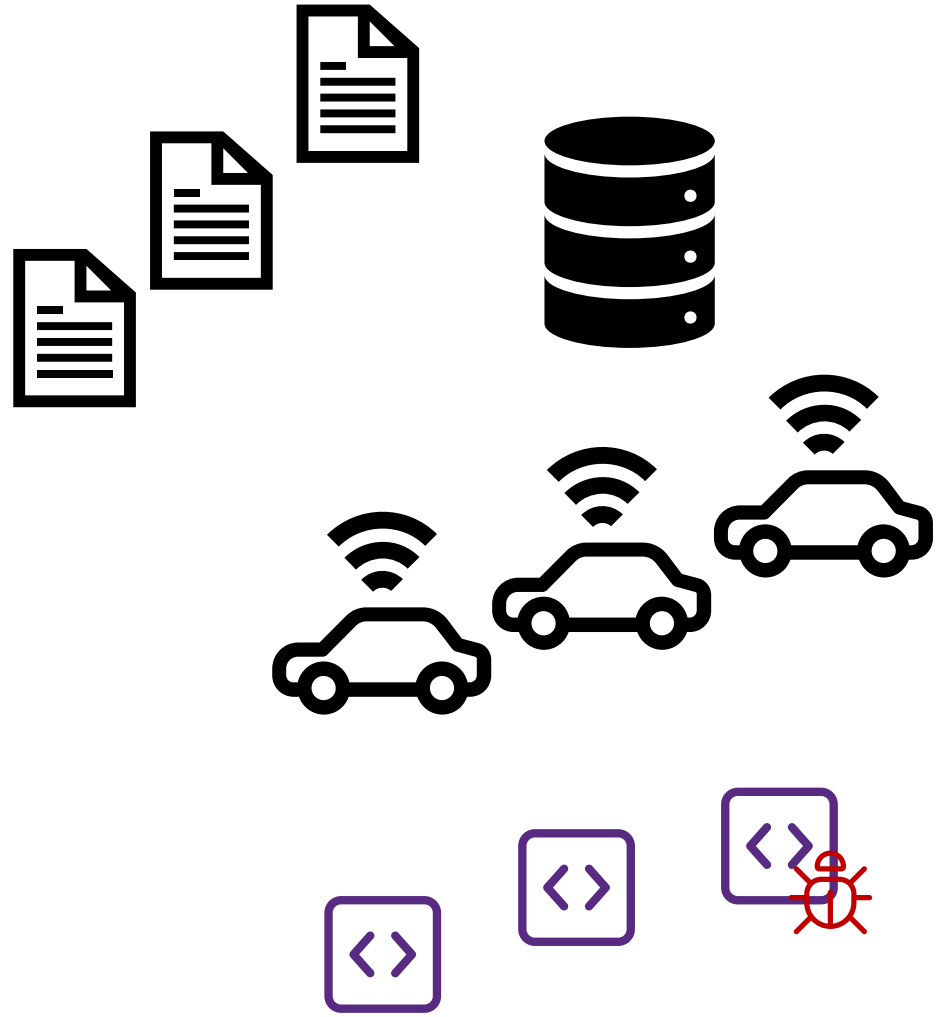
Software Composition Analysis (SCA)

Agenda

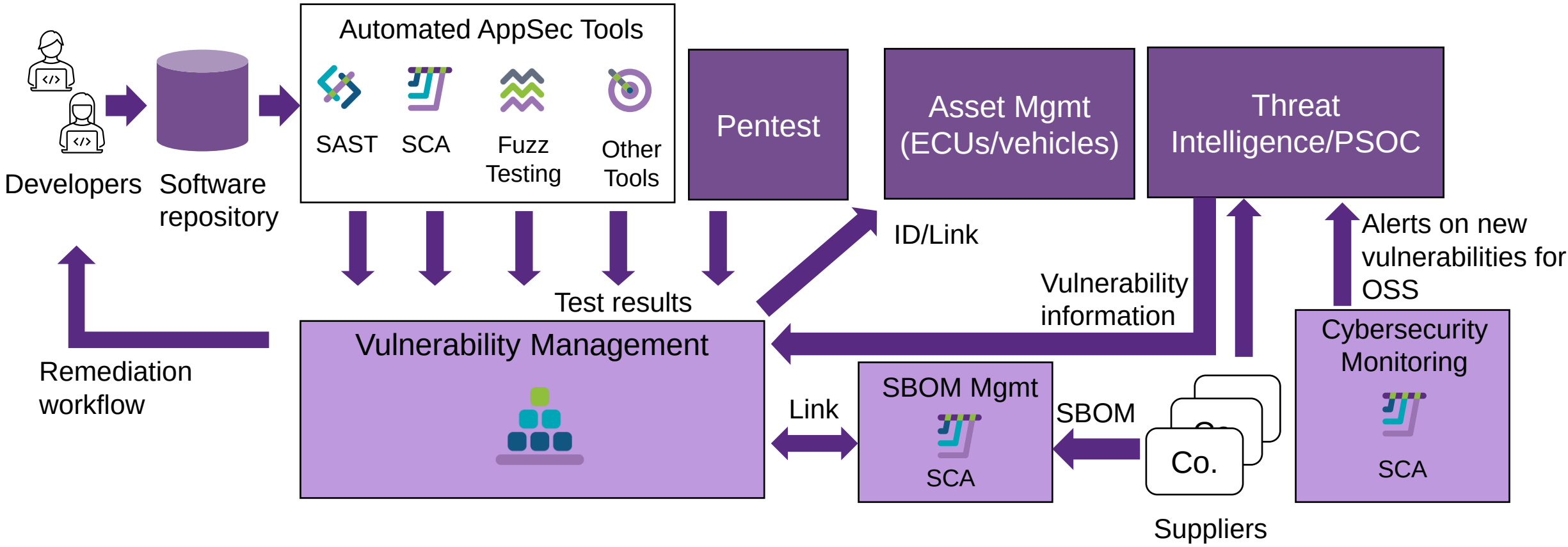


Use Cases for SBOM

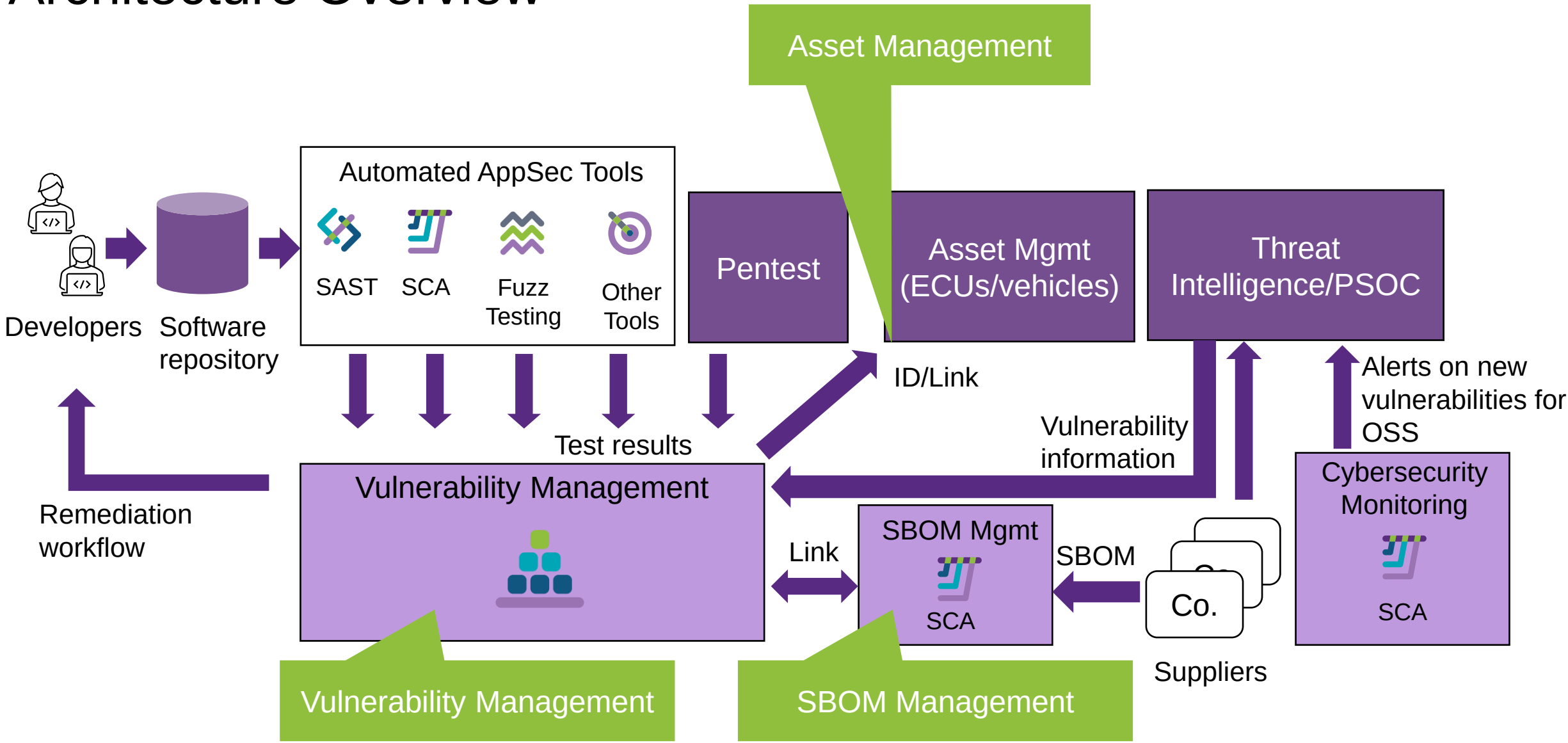
- SBOM Management
  - Create, import and aggregate SBOM
- Asset Management
  - Map SBOM to products (ECUs/vehicles)
- Vulnerability Management
  - Import supplier or OSS vulnerability information
  - Map vulnerabilities to software/SBOM
  - (manage vulnerabilities found during development)



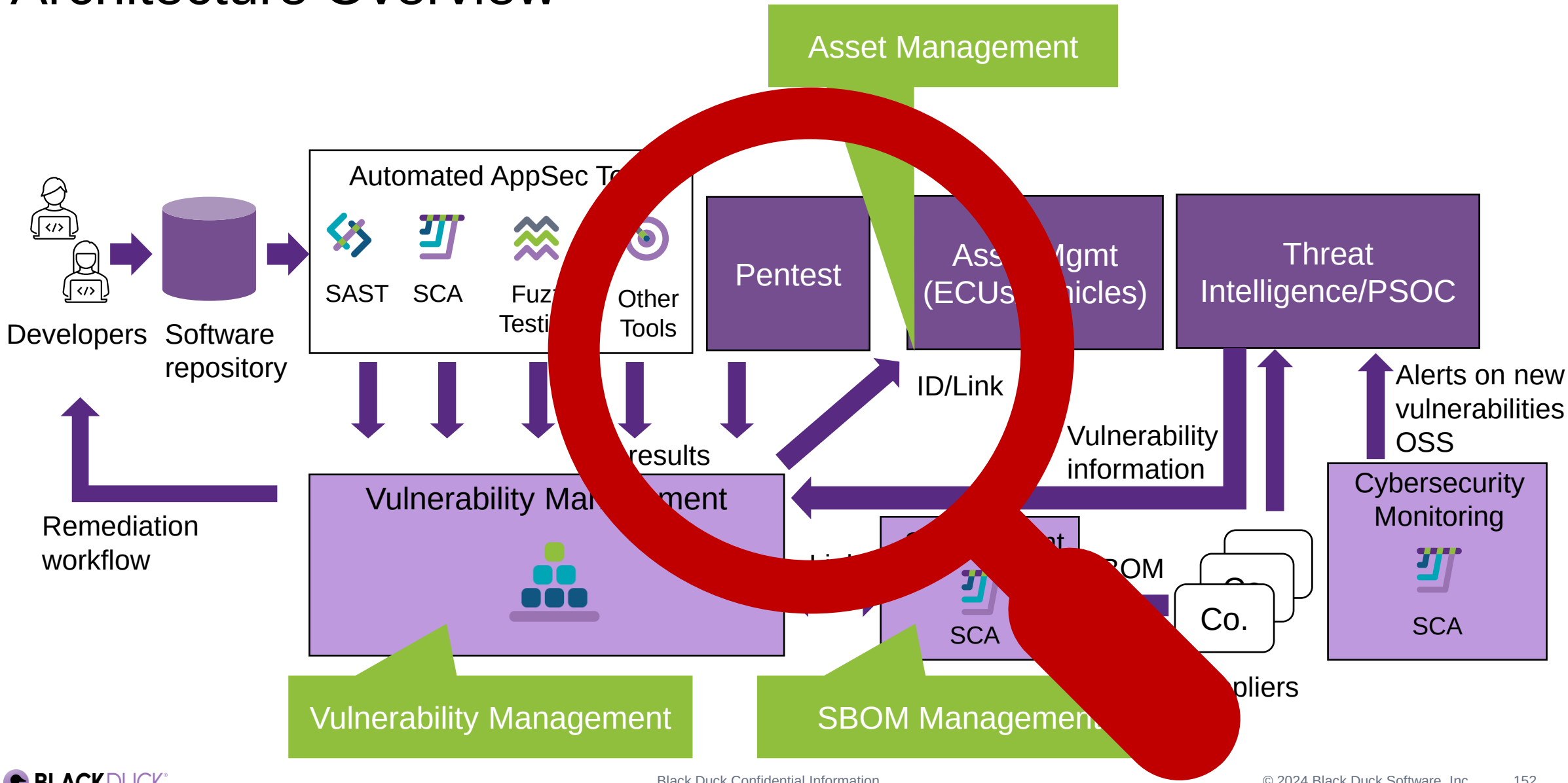
Architecture Overview



Architecture Overview



Architecture Overview



From Vehicle to Software Components

From SBOM

VIN
1FTEW2E42KKC60719
4T1BF1FK5DK689209
3GTEK13398J195521
1B4GT54L7VK237083
1FTJF35F7VJC32686
1JCUB7814EK139344
..

ECUs
Engine AA
Airbag AB
Gateway AA
Brake AA
Infotainment AB
Telematics AC
…

Hardware/Software
MCU XX
Wi-Fi module XX
Bluetooth module XY
…
Software AB v1.0
Firmware AB v1.0
…

Components
Linux kernel 4.14.48
openssl 1.0.2h
glibc 2.23
zlib 1.2.8
curl 7.58.0-r0
libpng 1.2.44
..

curl 7.58.0-r0

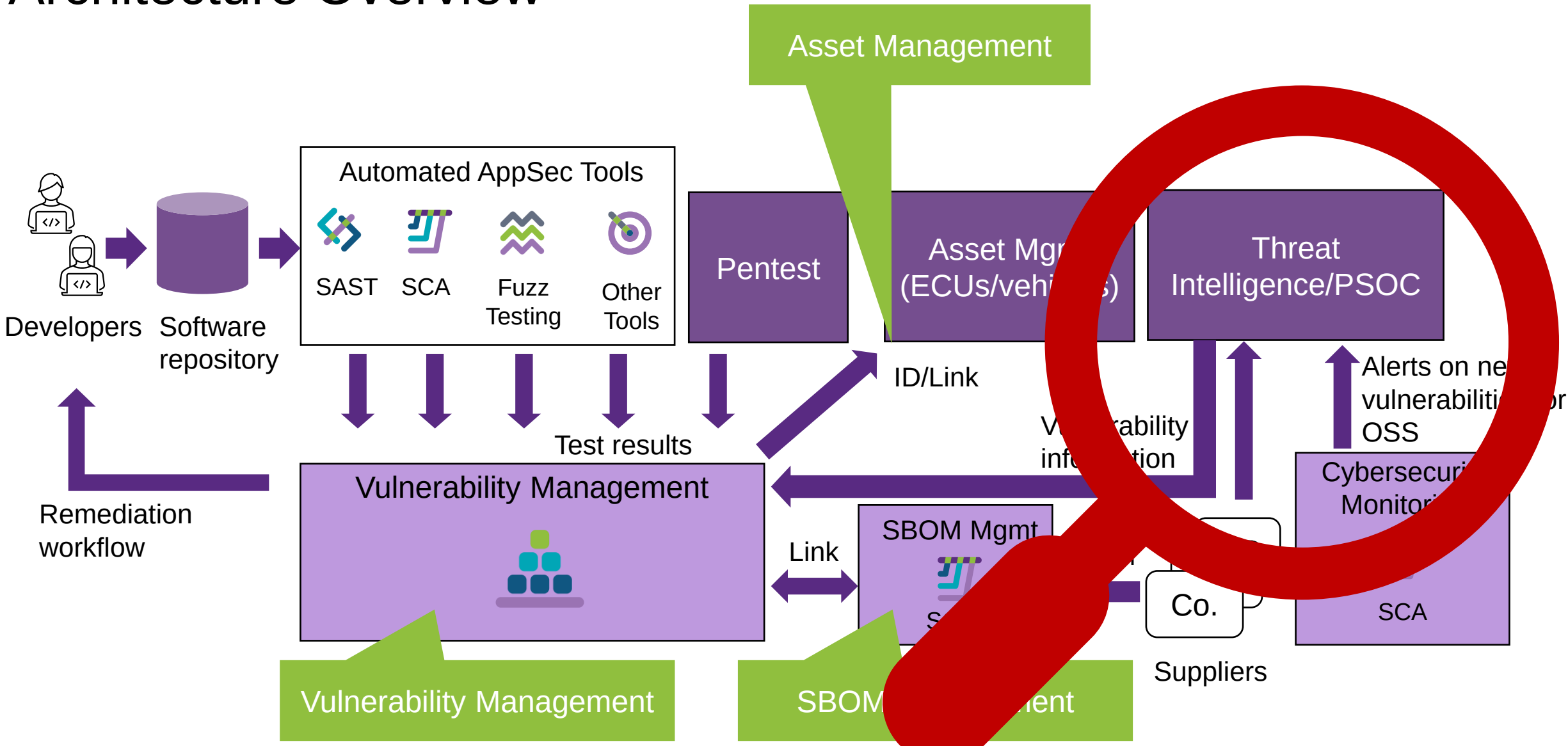
Vulnerabilities	CVSS v3
CVE-2019-3822	9.8
CVE-2018-14618	9.8
CVE-2018-16839	9.8
…	…

curl 7.58.0-r0

License
MIT - Permissive

VIN: Vehicle Identification Number CVSS: Common Vulnerability Scoring System

Architecture Overview



Evaluate the Risks for New Vulnerabilities

Evaluate criticality of vulnerability

Evaluate impact (no. of vehicles affected)

curl 7.58.0-r0

Vulnerabilities	CVSS v3
CVE-2027-XXXX	10
…	…

Software
Software AA v1.0
Software AB v1.0
Software AC v1.0
Software AD v1.0
Software AE v1.0
Software AF v1.0
…

ECUs
Infotainment AA
Infotainment AB
Infotainment AC
Infotainment AD
Telematics AE
Telematics AF
…

VIN
1FTEW2E42KKC60719
4T1BF1FK5DK689209
3GTEK13398J195521
1B4GT54L7VK237083
1FTJF35F7VJC32686
1JCUB7814EK139344
..

CVSS: Common Vulnerability Scoring System

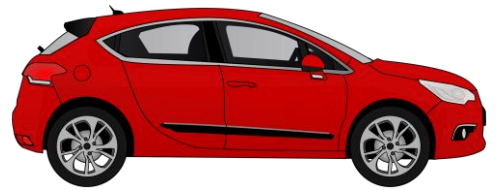
Software
Software AA v1.0
Software AB v1.0
Software AC v1.0
Software AD v1.0
Software AE v1.0
Software AF v1.0
…

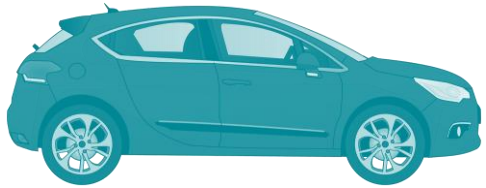
Software Repository

Vulnerable Software

OTA Platform:

- Secure communication
- Digital signatures
- …





Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.0
4T1BF1FK5DK689209	Software AB v1.0
3GTEK13398J195521	Software AC v1.0
1B4GT54L7VK237083	Software AD v1.0
1FTJF35F7VJC32686	Software AE v1.0
1JCUB7814EK139344	Software AF v1.0
..	…

OTA: Over the Air

Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

Software Repository

OTA Platform:

- Secure communication
- Digital signatures
- …

Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.0
4T1BF1FK5DK689209	Software AB v1.0
3GTEK13398J195521	Software AC v1.0
1B4GT54L7VK237083	Software AD v1.0
1FTJF35F7VJC32686	Software AE v1.0
1JCUB7814EK139344	Software AF v1.0
..	…

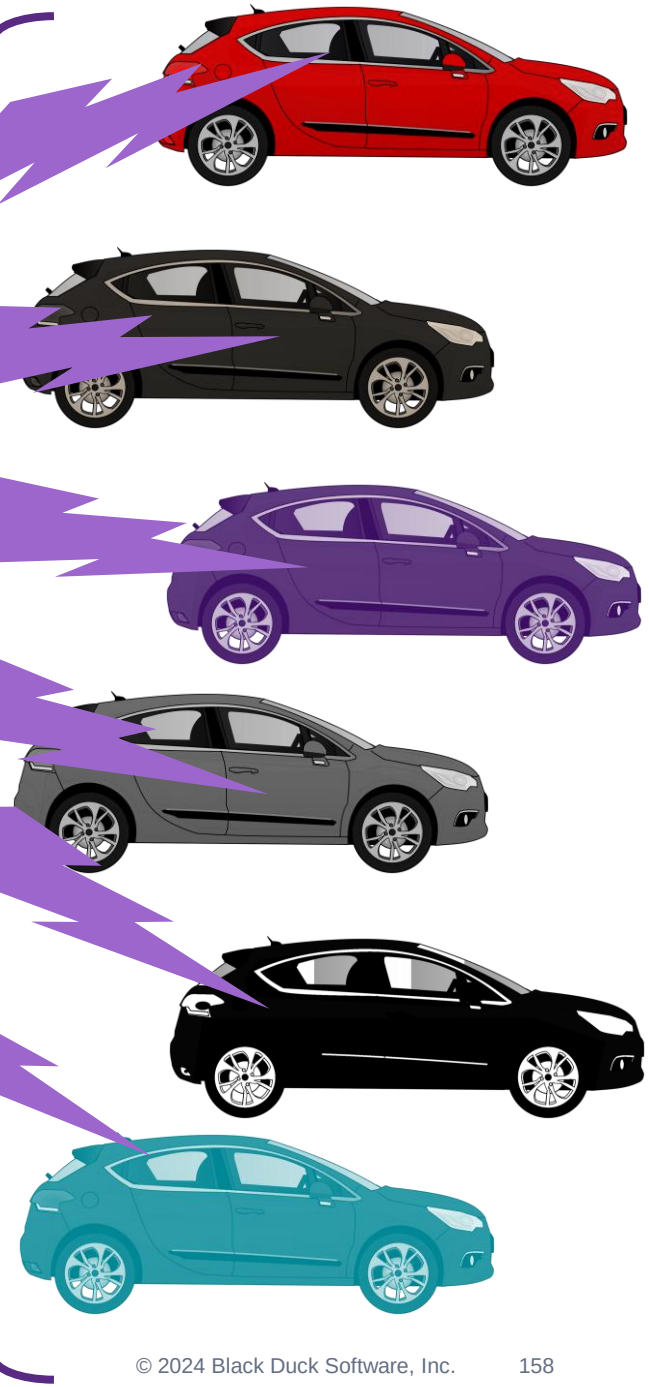
Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

Software Repository

AppSec testing to minimize new vulnerabilities before new software is pushed out

OTA Platform:

- Secure communication
- Digital signatures
- …



Asset Mgmt System

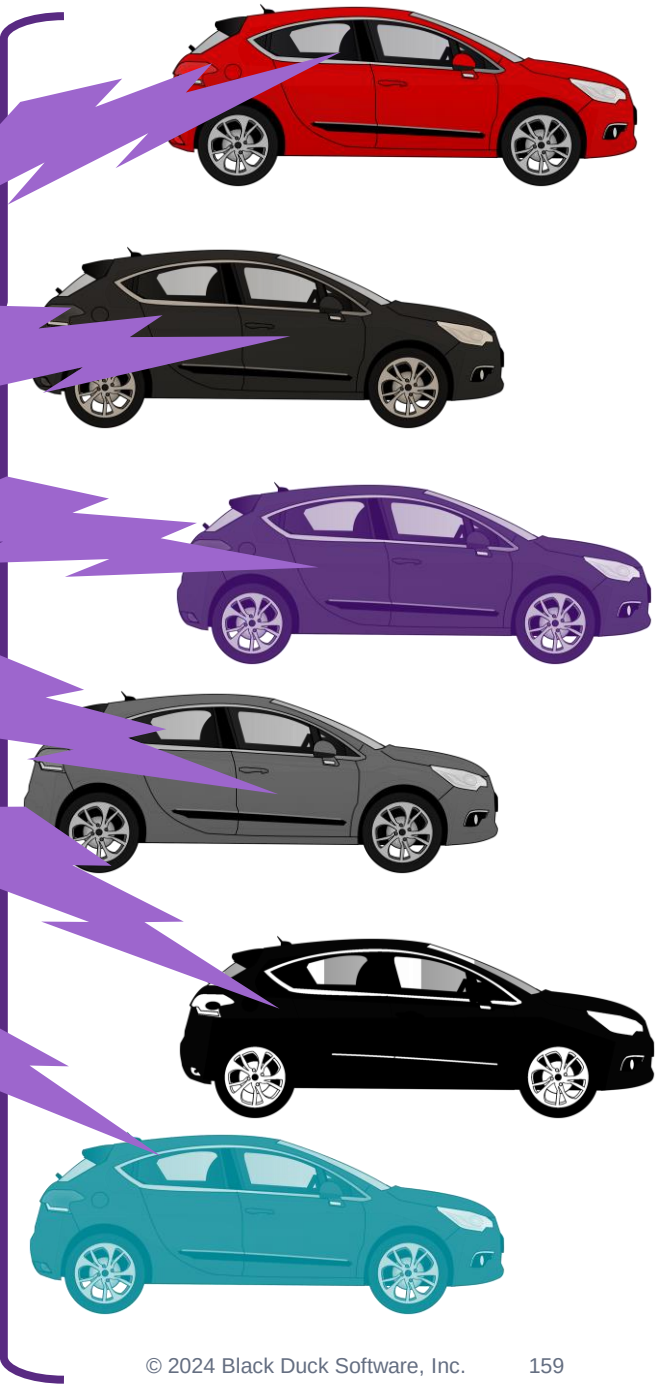
VIN	Software
1FTEW2E42KKC60719	Software AA v1.0
4T1BF1FK5DK689209	Software AB v1.0
3GTEK13398J195521	Software AC v1.0
1B4GT54L7VK237083	Software AD v1.0
1FTJF35F7VJC32686	Software AE v1.0
1JCUB7814EK139344	Software AF v1.0
..	…

Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

Software Repository

OTA Platform:

- Secure communication
- Digital signatures
- …



Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.1
4T1BF1FK5DK689209	Software AB v1.1
3GTEK13398J195521	Software AC v1.1
1B4GT54L7VK237083	Software AD v1.1
1FTJF35F7VJC32686	Software AE v1.1
1JCUB7814EK139344	Software AF v1.1
..	…

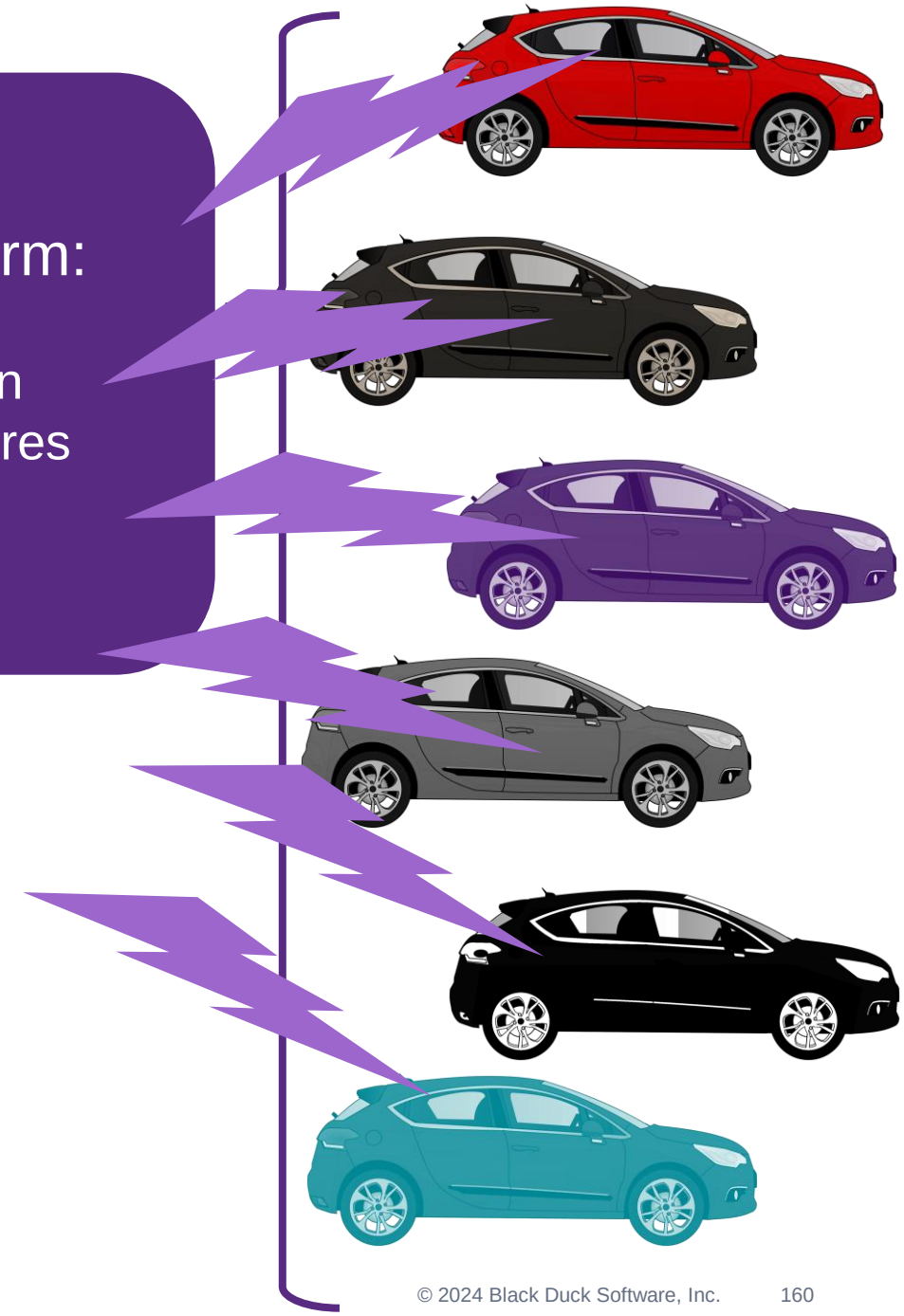
Map new SBOM to Asset Mgmt system

Software
Software AA v1.1
Software AB v1.1
Software AC v1.1
Software AD v1.1
Software AE v1.1
Software AF v1.1
…

Software Repository

OTA Platform:

- Secure communication
- Digital signatures
- …



Asset Mgmt System

VIN	Software
1FTEW2E42KKC60719	Software AA v1.1
4T1BF1FK5DK689209	Software AB v1.1
3GTEK13398J195521	Software AC v1.1
1B4GT54L7VK237083	Software AD v1.1
1FTJF35F7VJC32686	Software AE v1.1
1JCUB7814EK139344	Software AF v1.1
..	…

Call to Action

Reduce risks by knowing what's in your software

- License risks
- Vulnerabilities
- SBOM management, Asset Management, Vulnerability Management

Consider how to collaborate on SBOM

- Auto-ISAC
- NTIA
- OpenChain
- GlobalPlatform
- …

BLACKDUCK®

Thank You

Global Platform™

2024-10-24

SESIP Technical Automotive Sub WG

SESIP Certification as a means to generate artefacts for UNECE 155 & ISO 21434 compliance

Agenda

Cybersecurity Challenges – ISO 21434

Cybersecurity Testing Methods

Component Certification Framework

Discussions

Global Platform™

Cybersecurity Challenges

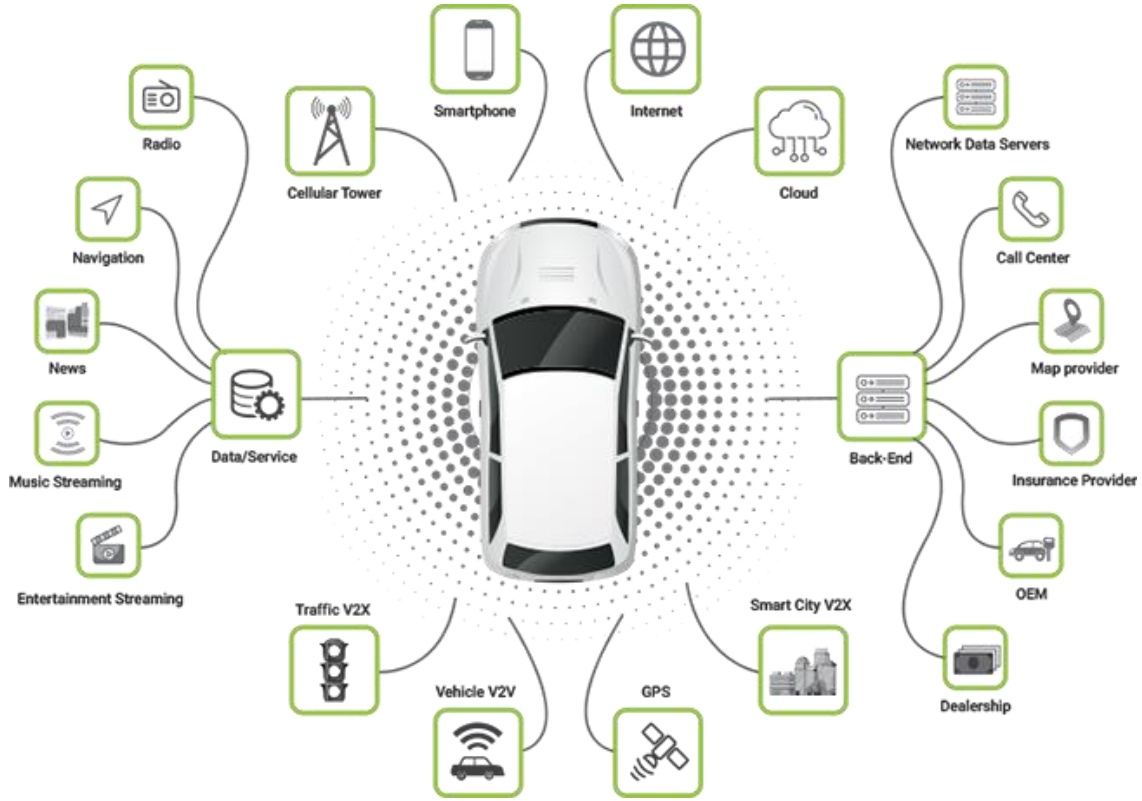
ISO 21434

Introduction

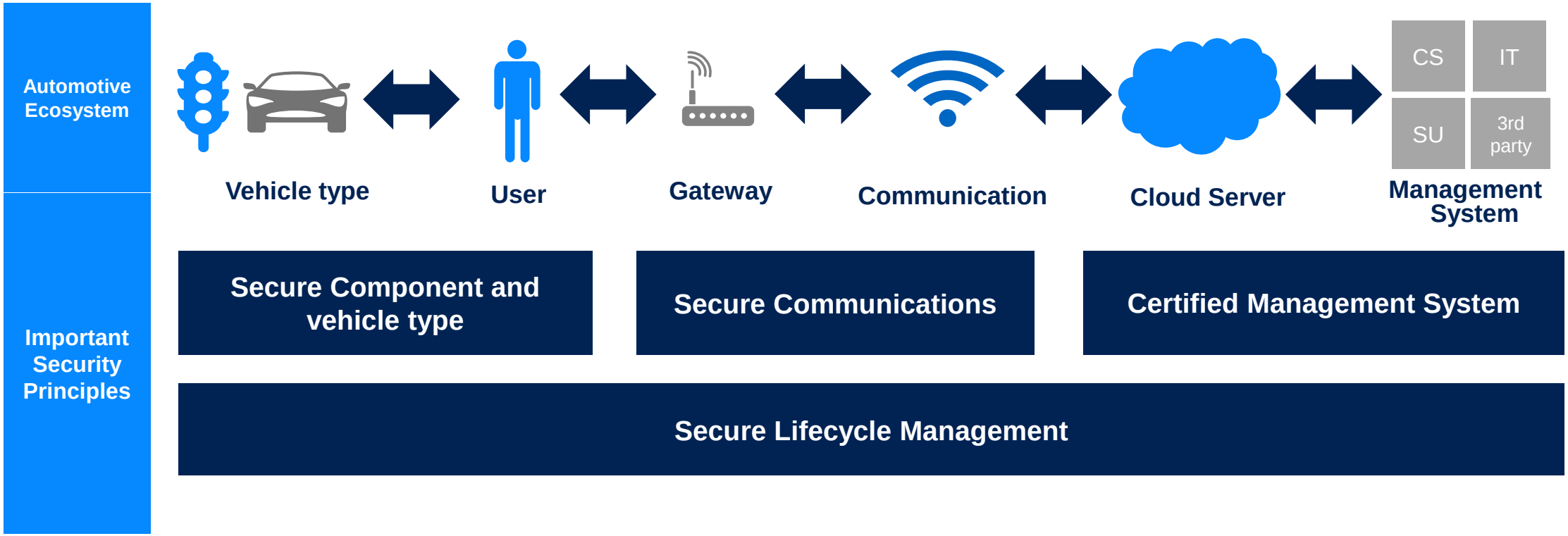
Data Centers on Wheels

A modern car can generate data volumes in the MB/GB range per day

The information generated in this way is mainly transmitted internally, but also externally via communication interfaces

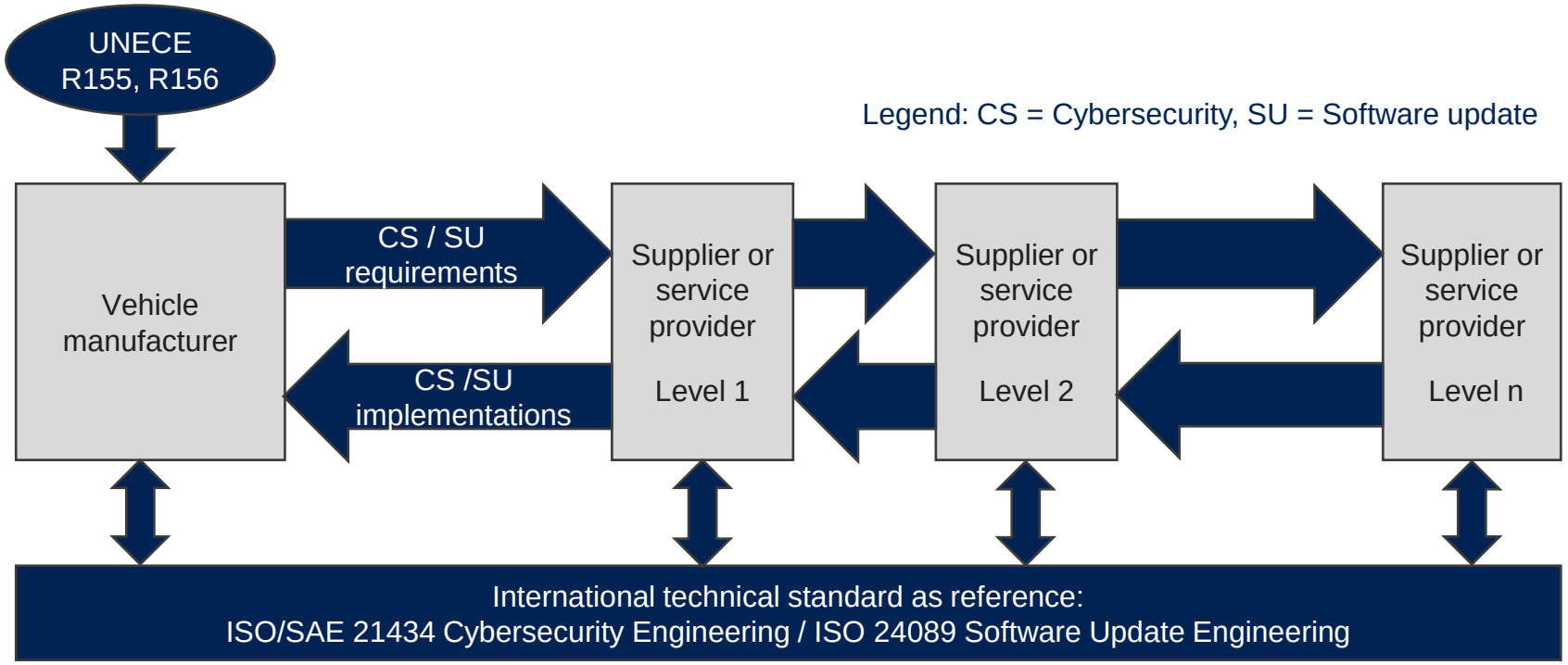


New Vehicle Ecosystem



Supply Chain Management

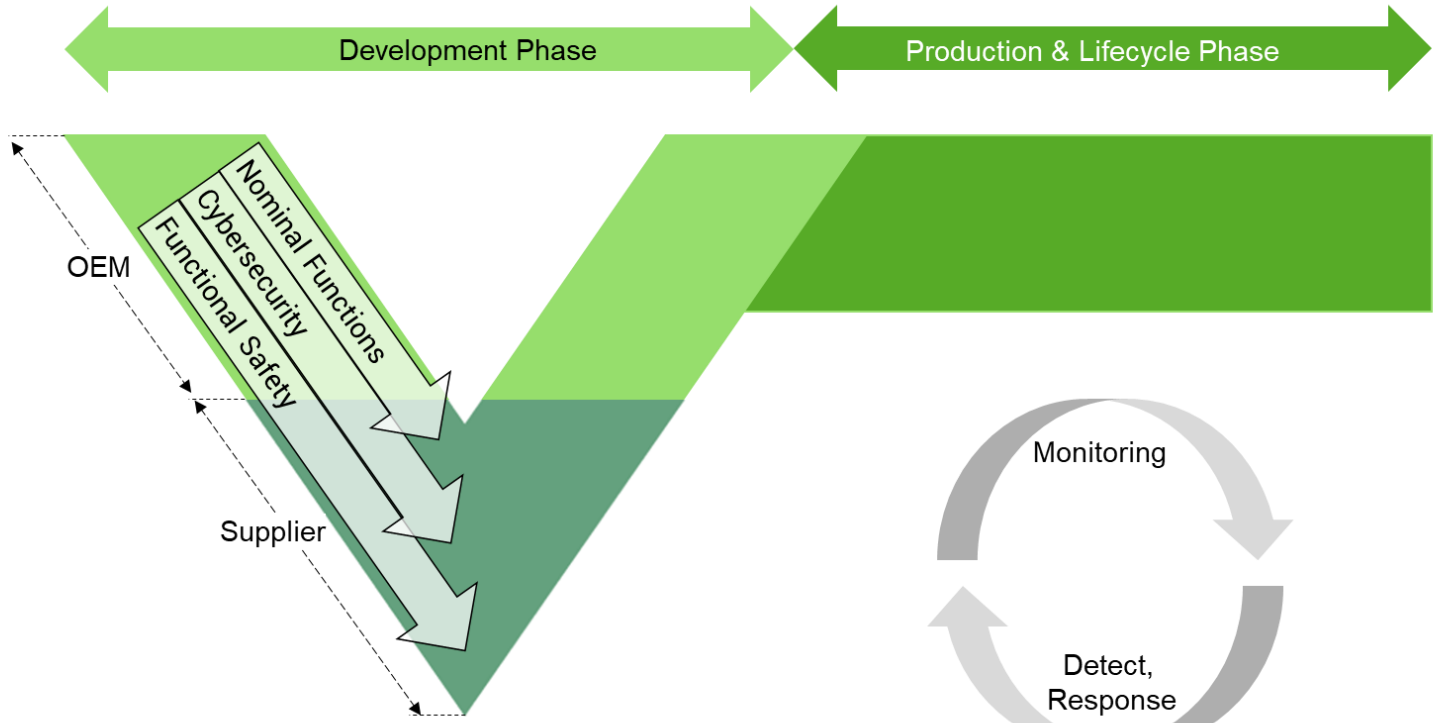
- OEMs may require their suppliers to meet all the UNECE regulatory requirements by demonstrating compliance with national/international standard frameworks, which can then be used to demonstrate compliance with the WP.29

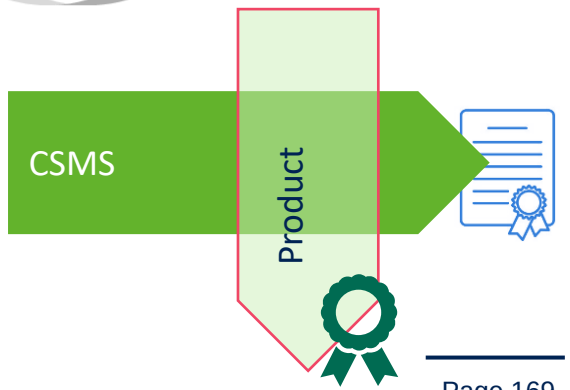


V-Cycle and Product Dimension (CSMS)

Risk management applied across the entire lifecycle

- Principle of risk minimization
- Mature organization (Process, Governance, Roles)
- Cybersecure Products
- Continuous market and product monitoring, incident detection and response



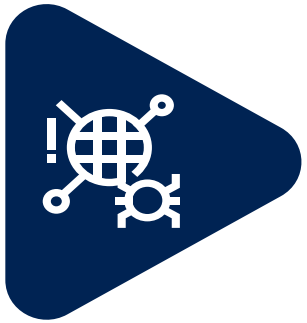


Global Platform™

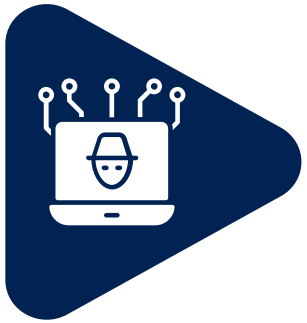
Cybersecurity Testing Methods

ISO 21434

Cybersecurity Relevant Testing Methods



Vulnerability scanning



Fuzz Testing

Penetration Testing

General evaluation of the level of security – performed continuously	Can be performed relatively early in the validation phase	Component and system level testing

▪ Identification of known vulnerabilities in different components
  ▪ Software components
  ▪ Hardware components
▪ Vulnerability scanning
  ▪ BOM based
  ▪ Network scanning tools
  ▪ Software Composition Analysis
	▪ Fuzz testing is an “automated” software testing technique
	▪ Massive amounts of “random” data, called fuzz, to crash or break the system
	▪ Find “software” bugs in code
	▪ Exploits systems vulnerabilities, so it can be fixed in due time
		▪ Penetration testing is a form of ethical hacking to find vulnerabilities
		▪ Pen-testing can also be referred to as a simulated cyber attack.
		▪ Find vulnerabilities

Framework conditions? ISO 8477

ISO 21434
Testing Method Challenges

Challenges in CS Evaluations

- Reports rejected by OEMs

- Unstructured Reporting Format
  - Incomplete Basic Information
  - Incomplete Testing information
  - Lack of Testing Procedures Documentation
- Inconsistent Vulnerability Context
- Absence of Integration with Existing Standards
- Lack of assumptions
- Rationale for selection of test cases
- Tools
- …

Global Platform™

Cybersecurity Testing

ISO 21434 – Component Certification Framework

Introduction

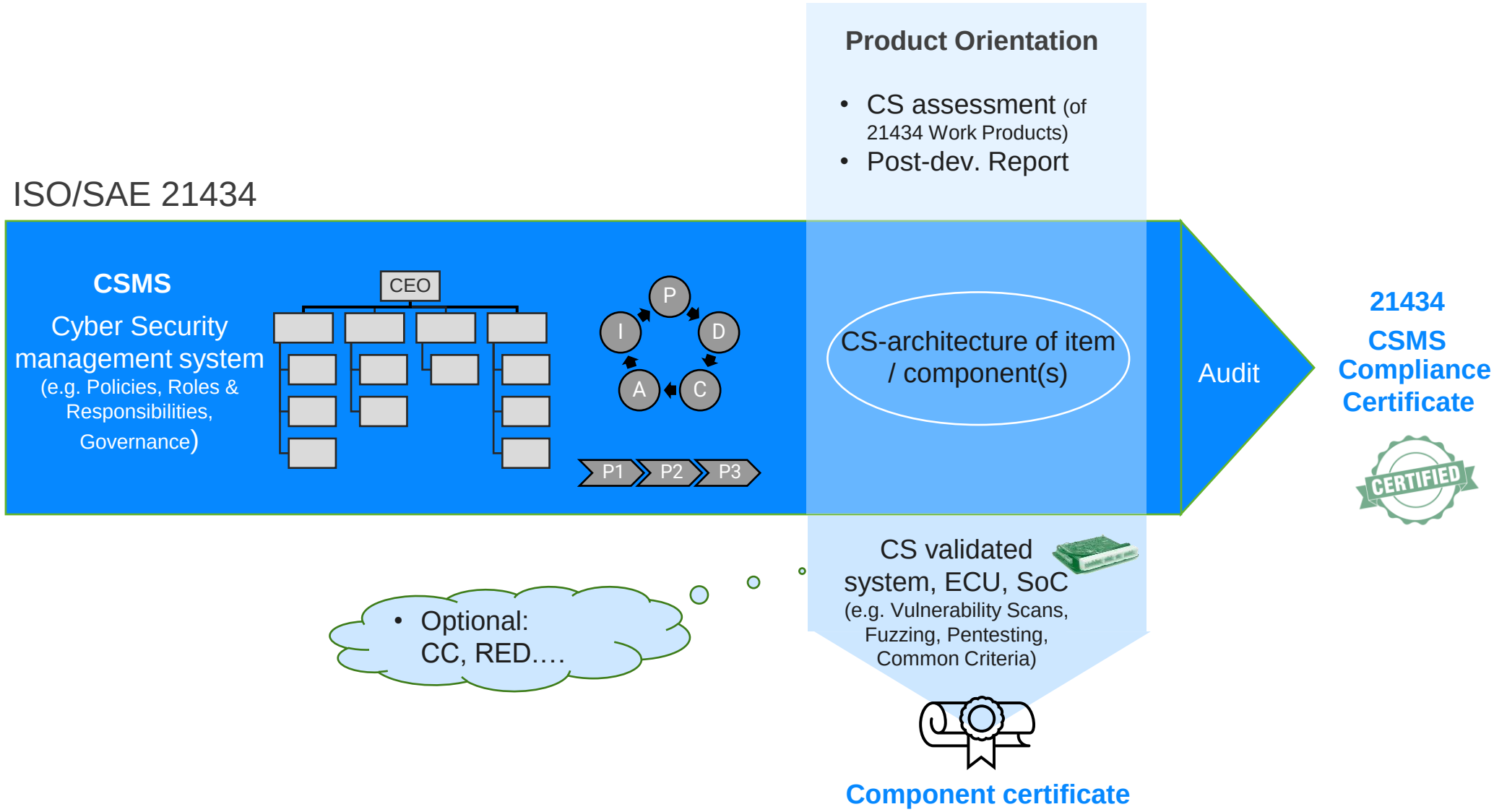
Cybersecurity (ISO 21434)

Cybersecurity: condition in which assets are sufficiently protected against threat scenarios to items of road vehicles, their functions and their electrical or electronic components.

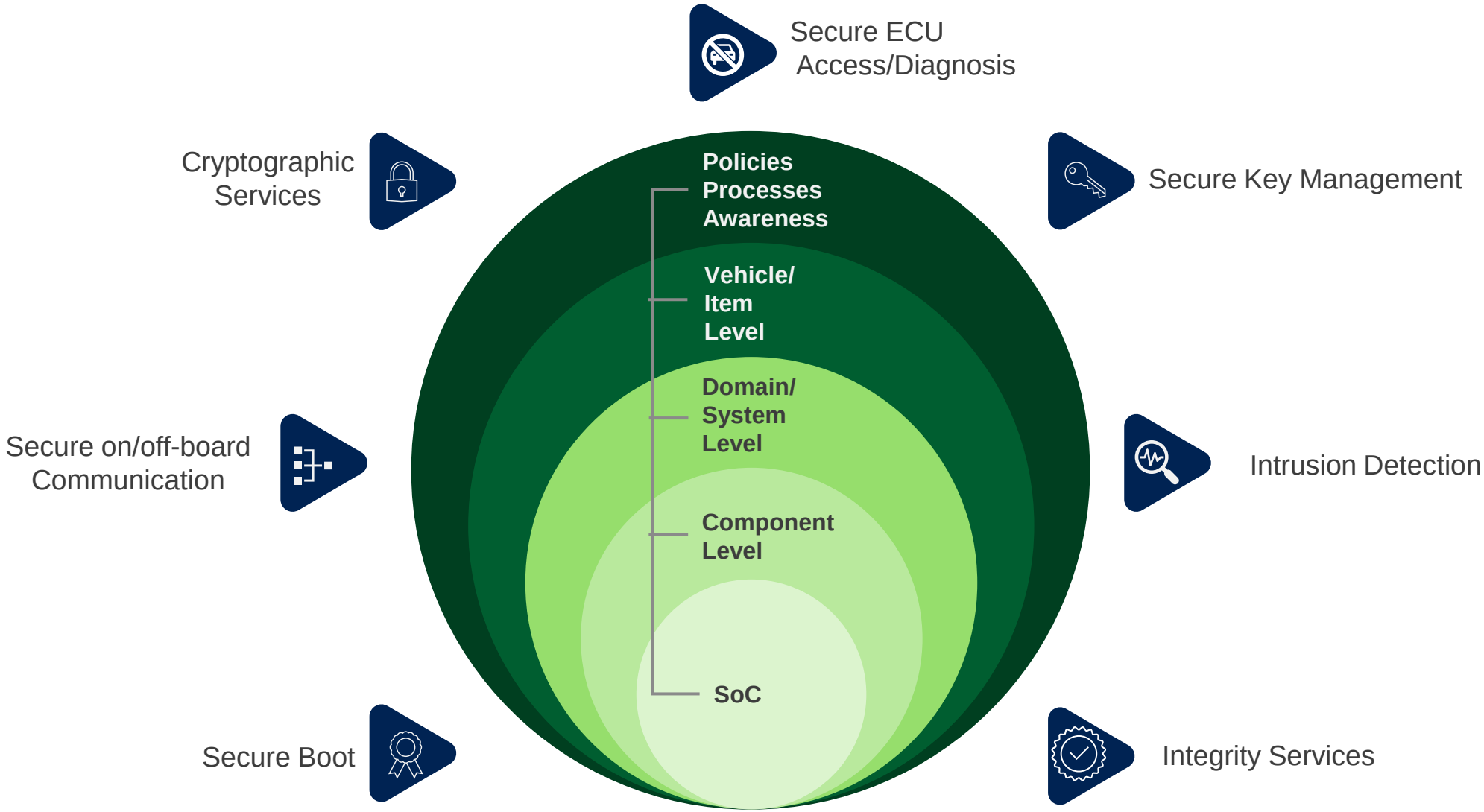
Relevant definitions

- Assets
- Items
- Components
- Sufficiently protected
- Threat scenarios

Certification Framework



Cybersecurity Layered Approach



Potential Approach

Security Evaluation

Certification scheme for components

- Covering ISO 21434 Testing Methods
  - Functional testing (*)
  - Vulnerability scanning
  - Fuzz testing
  - Penetration testing
- Risk based approach
  - Aligned with CALs (*)
- Layered approach
  - Component
  - Item
  - Vehicle
- CSMS Activities Review (?)
  - Working Packages Review
  - Processes and procedures

Global Platform™

Questions?

Open discussion

Global Platform™

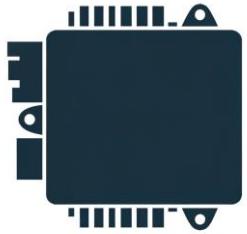
The standard for secure digital services and devices

→globalplatform.org

ECU Types

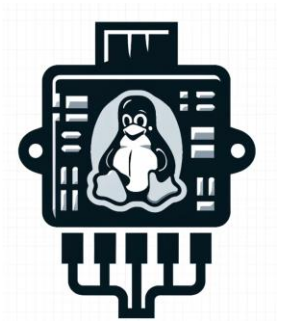
Limited Surface

- **ECU with SoC** (RTOS)
- **Wired Interfaces** (CAN, LIN, Ethernet)
- **Example:** Rear Lamp system integrating one NXP S32118K SoC using AUTOSAR OS with 2 x CAN and a LIN interface



Regular Surface

- **ECU with one VμC** (RTOS) **and another SoC** (e.g. Linux)
- **Wired Interfaces** and internal communications through **UART, SPI**, …
- **Example:** Instrument Cluster Panel with an RH850 vehicle microcontroller running AUTOSAR OS and another ARM Cortex M3 running Linux OS. Available interfaces 2 CAN, 1 LIN and 1 DoIP.



Extended Surface

- **ECU with one VμC** (RTOS) **and another SoC** (e.g. Android)
- **Wired and Wireless interfaces** (Wi-Fi, 4G/5G, Bluetooth)
- **Example:** Infotainment system using NXP RH850 Vehicle micro controller running AUTOSAR OS and ARM Cortex M3 running Android 12 including wired interfaces (2xCAN, 1 LIN, 1 DoIP) and wireless interfaces Wi-Fi (hotspot), 4G LTE and Bluetooth LE.

Global Platform™

GlobalPlatform in Japan

Eikazu Niwanosan (NTT)
Japan Task Force Chair
Board of Directors

Priority FY2024(2023.10-2024.9) and Main Results

Starting concrete collaboration with consumer device industry	• Mapping between CCDS*1 schema • SESIP Presentation at CCDS IoT Security Symposium
Gaining a foothold for collaboration with automotive industry	• Discussed the issue of MoU with automotive related associations
Regularize GP-TF collaboration	• Planned WS (CSVF*2, Technical WS on SE/TEE/SESIP) and ATF*3/CTF*4 meeting • Investigation on the status of ID Wallet in Japan
Clarify JTF activities feedback to GP	• Held Secure Device Forum (scoping overseas participation) and conducted survey analysis

*1. CCDS: Connected Consumer Device Security Council
*2. CSVF: Cyber Security Vehicle Forum
*3. ATF: GP Automotive Task Force
*4. CTF: GP China Task Force

Secure Device Forum 2024 on 18th Feb, 2024

Trends in Consumer Device Security

Various types of speakers – 11 speakers from 8 associations/public entity/private company

- GP - opening - overall trends
- GP(2 speakers) - Latest status of GlobalPlatform
- MIC[2]- cybersecurity
- METI[*3] – cybersecurity
- CCDS – IoT Labelling Program
- ECSEC Lab – IoT Platform Evaluation/SESIP
- Trustonic – Use case of TEE
- ISO SC17 – Personal ID and Authentication on Mobile Device with Secure Device
- NICSS(2) - closing - prospect

Invited and Registered “associations”/ “public entities” – 23
Attendee - 161

*1 Asia Ic Card Forum
*2 Ministry of Interior and Communication
*3 Ministry of Economy, Trade and Industry
*4 National Institute of Informatics

*5 Association of Radio Industries and Businesses
*6 Connected Consumer Device Security council
*7 Japan Network Security Association

*8 New Media Development Association
*9 The Telecommunication Technology Committee
*10 Japan Business Machine and Information System Industries Association

Long-Term Roadmap

Feedback of “regional requirements” with other regions to GP global

Imply requirements and use case/case study by region/market

- Requirements, use cases, practices, deployment status, solution map
- In Asia with CTF, in Europe and American region with European, American members

Enhancing collaboration with Japanese standardization organizations

- Consumer Device/Automotive/ID/Smart City/Critical infrastructure/ Medical: Most Important
- OT/Agriculture: Important

Technical contribution from Japan region to GP global

PQC/Advanced Crypto, TEE/PETs, digital ID and SESIP/Additional requirements

Please Join GP-JTF, Thank You!

GlobalPlatform Automotive Events Open to Non-Members

Cybersecurity Vehicle Forum

Cybersecurity Vehicle Forums

- CSVF EU
  - 4th December, Berlin co-located with Cybersecurity in SDVs
- CSVF China
  - March 2025 TBC
- CSVF USA TBC

Automotive Roundtables

- Japan Roundtable 24th of October in Tokyo

To register: https://globalplatform.org/events/

Join Us!

Follow GlobalPlatform Specifications

Become a GlobalPlatform Member: Optimise your roadmap

Contribute on Development of Automotive Specifications within GP

- Working on Identified Topics
- Identifying New Topics

automotive@globalplatform.org

会議当日はよろしくお願いいたします。
Kaigi toujitsu wa yoroshiku onegai itashimasu.
(I look forward to our next meeting.)

Global Platform™

The standard for secure digital services and devices

→globalplatform.org