TENCENT SECURITY CONFERENCE 2018
2018腾讯安全国际技术峰会

A Holistic Approach to Automotive Security

Timo van Roermund, NXP Semiconductors

About me

Timo van Roermund

Join my network on LinkedIn:

Role & responsibilities

- Director Automotive Security – NXP Semiconductors
- Head of NXP's Automotive Security Team
- In charge of NXP's automotive security strategy, technology, solutions, and processes

External contributions

- Regular speaker at international conferences; program committee member for Cyber Secure Car (2015-2017) and escar EU (since 2018)
- Active contributions to security standards and consortia

Education

- MSc. in Computer Science and Engineering – Eindhoven University of Technology

© 2018 NXP Semiconductors. All rights reserved.

NXP – Global #1 in Automotive Semiconductors

2400+
AUTO ENGINEERS

30+
AUTO SITES WORLDWIDE

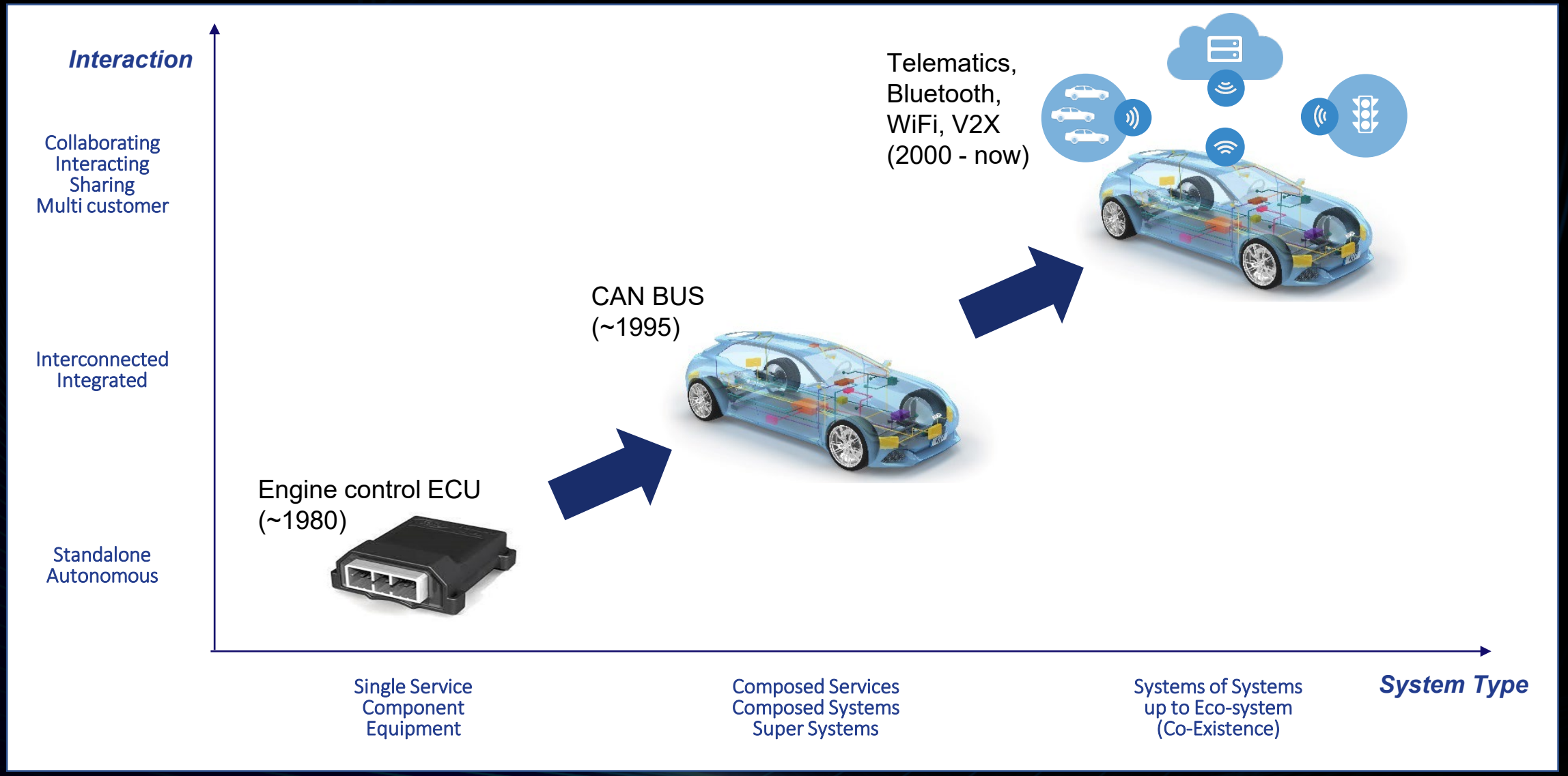
#1
AUTO SEMI SUPPLIER GLOBALLY

~40%
OF NXP'S REVENUE IS FROM AUTO

60+
YEARS OF EXPERIENCE IN AUTO

© 2018 NXP Semiconductors. All rights reserved.

History: vehicle electronics & connectivity



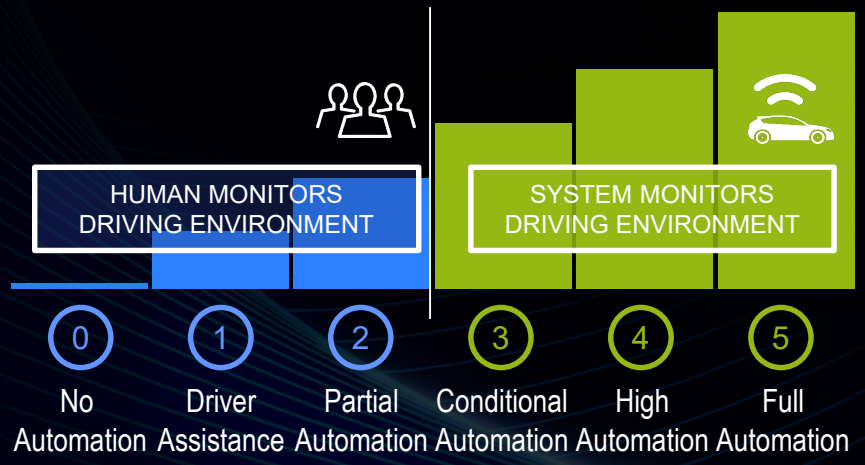
© 2018 NXP Semiconductors. All rights reserved.

Next: autonomy

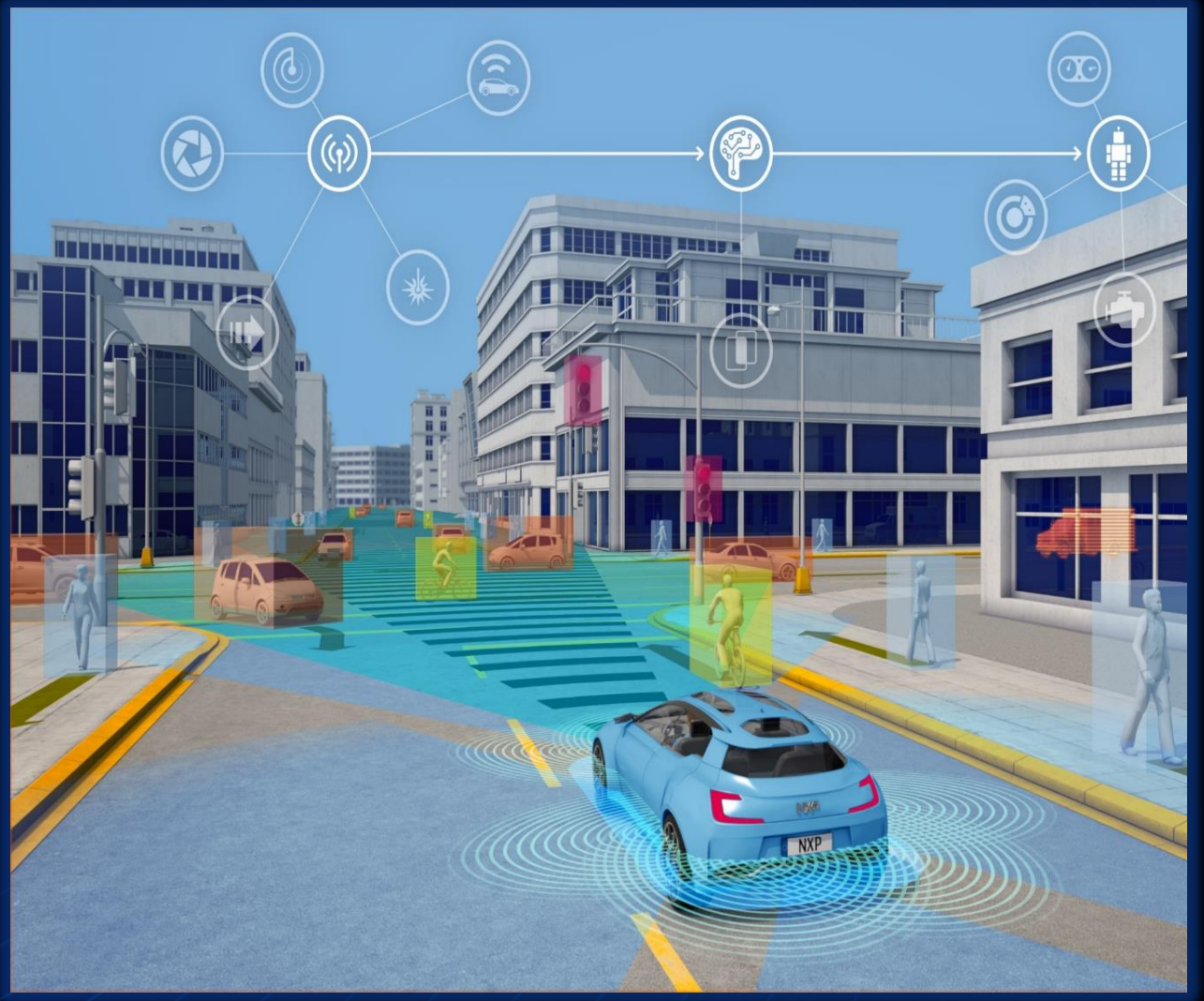
Cars are becoming self-driving robots

The potential benefits are huge:

- Drivers spend 200-300 hours in their car (annually)
- Cars are parked (unused) 95% of the time
- > 90% of road accidents caused by human mistakes



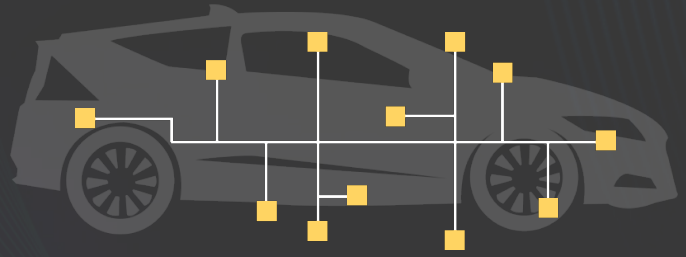
Source: SAE J3016



© 2018 NXP Semiconductors. All rights reserved.

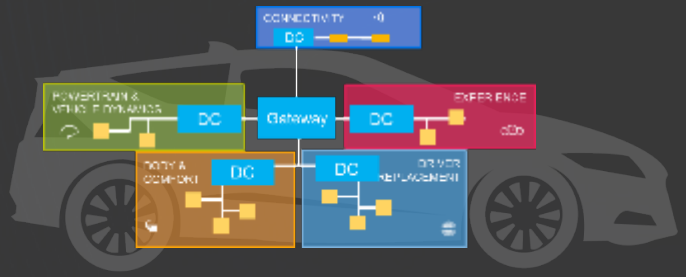
Trends in network architectures

Vehicle networks evolve, to accommodate the ever increasing amount of electronics:



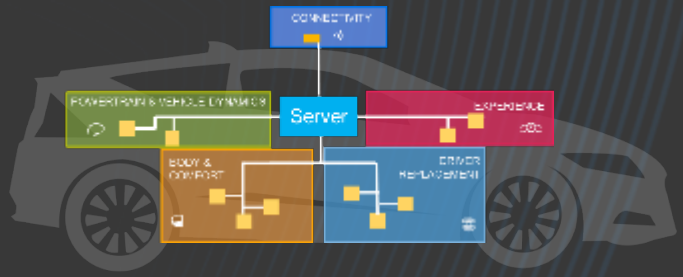
Past: Flat networks

- Direct connection between all ECUs
- Cost-effective for low # of ECUs



Next: Domain-based

- Upgradeability and Scalability
- Separation of Concerns



Future: Centralized?

- Fewer ECUs
- Flexible use of compute power

© 2018 NXP Semiconductors. All rights reserved.

Domain-Based Architectures

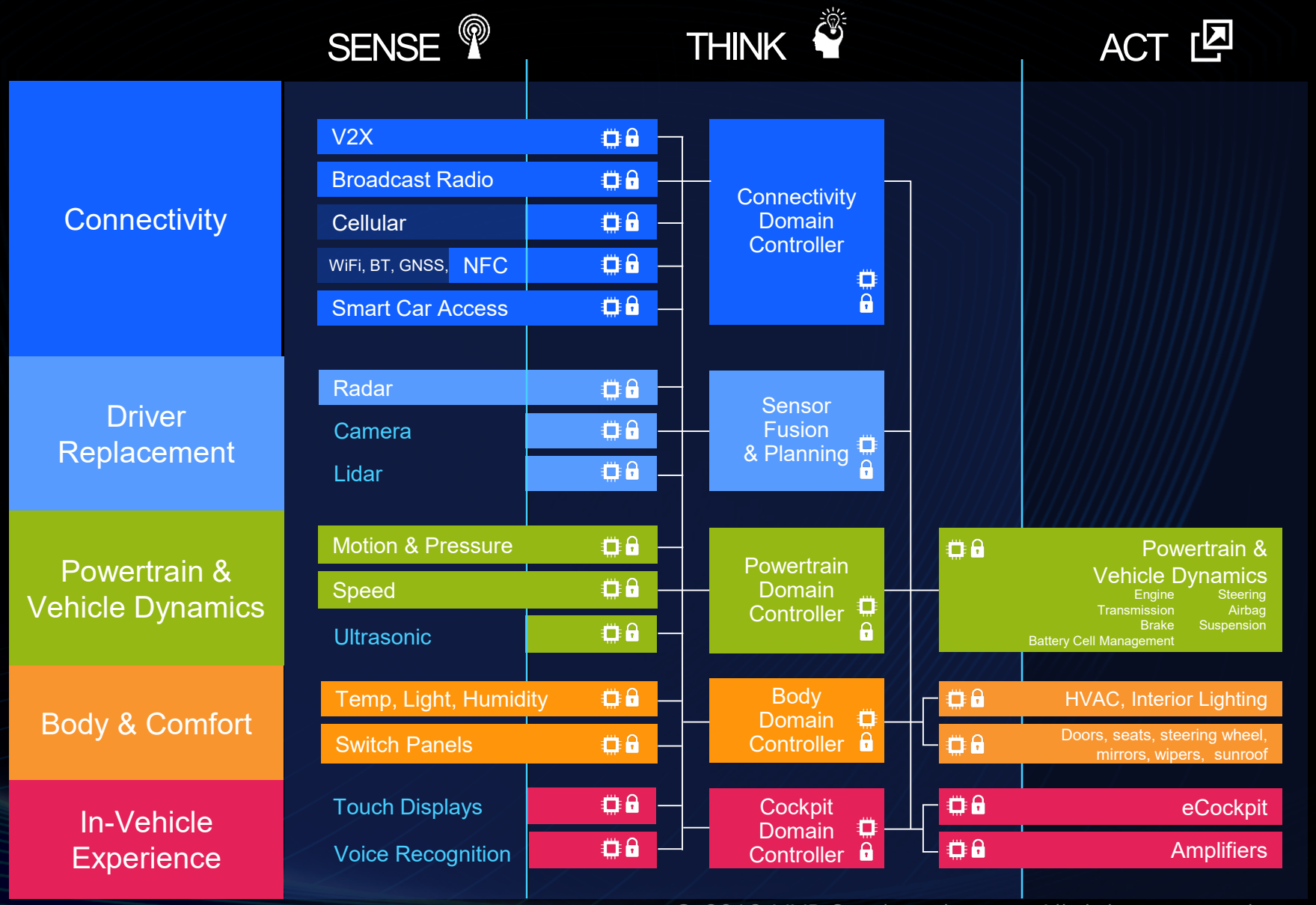
Self-Driving Vehicles

are

Cyber-Physical Systems

and

Safety is Paramount!



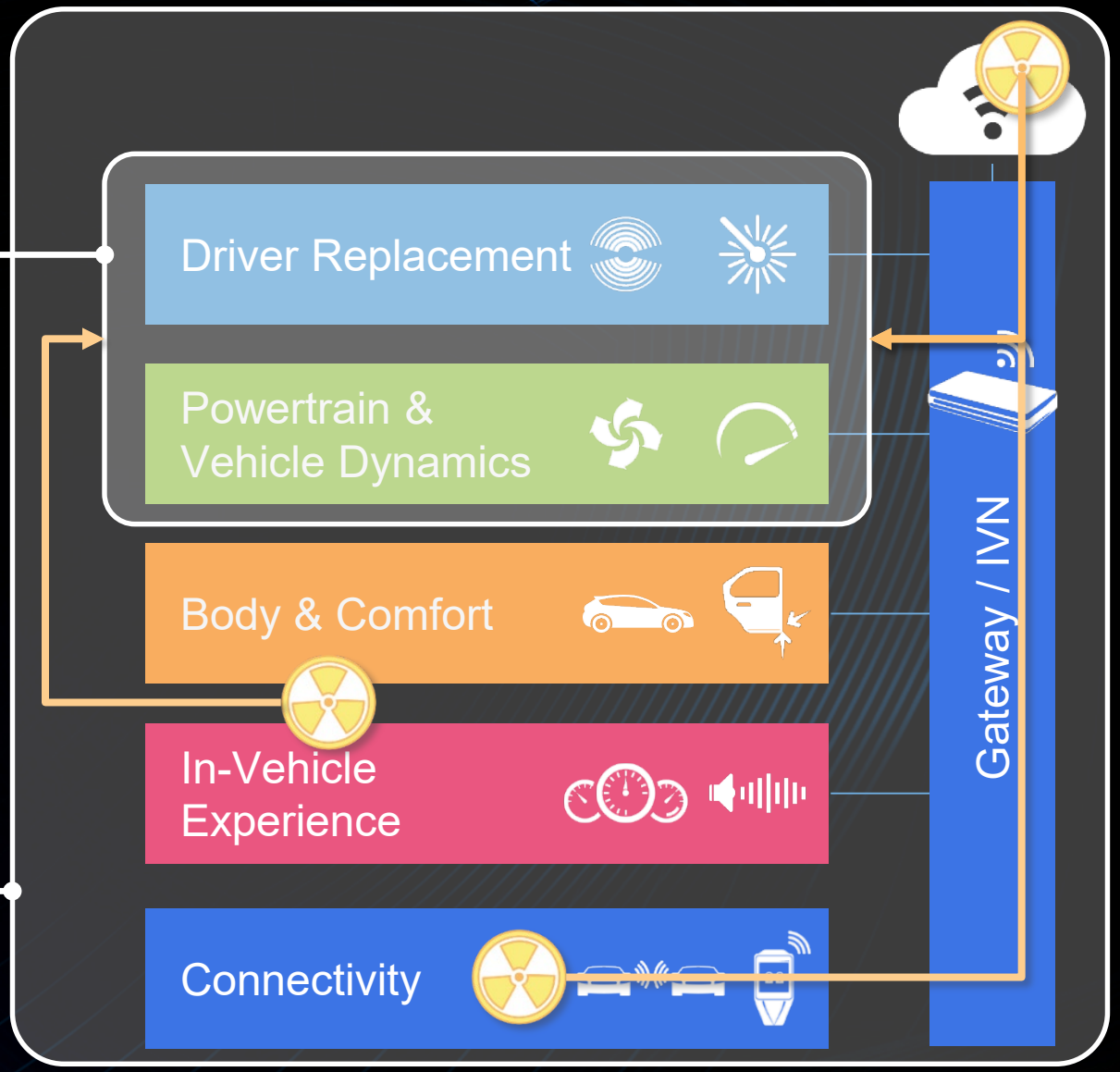
© 2018 NXP Semiconductors. All rights reserved.

No safety without security

#1 Objective: no functional hazards on mission-critical ECUs

Only possible, if:
System availability ensured
Information received / processed trustworthy

Cyber-security is a prerequisite for availability and trust in the system



© 2018 NXP Semiconductors. All rights reserved.

Did you know?

>50

Vehicle hacks
published since 2015

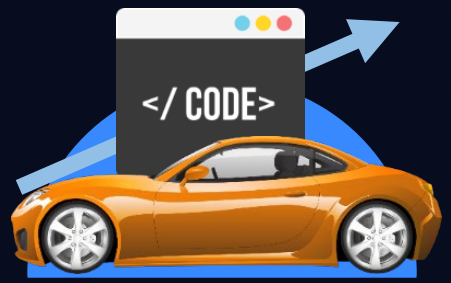
1.4M

Vehicle recalled
in the largest incident to date

Why hacking?

Valuable Data
attracts hackers

Car-generated data may become a USD 750B market by 2030



Why is it possible?

High System Complexity
implies high vulnerability

Up to 150 ECUs per car, up to 200M lines of software code

Why now?

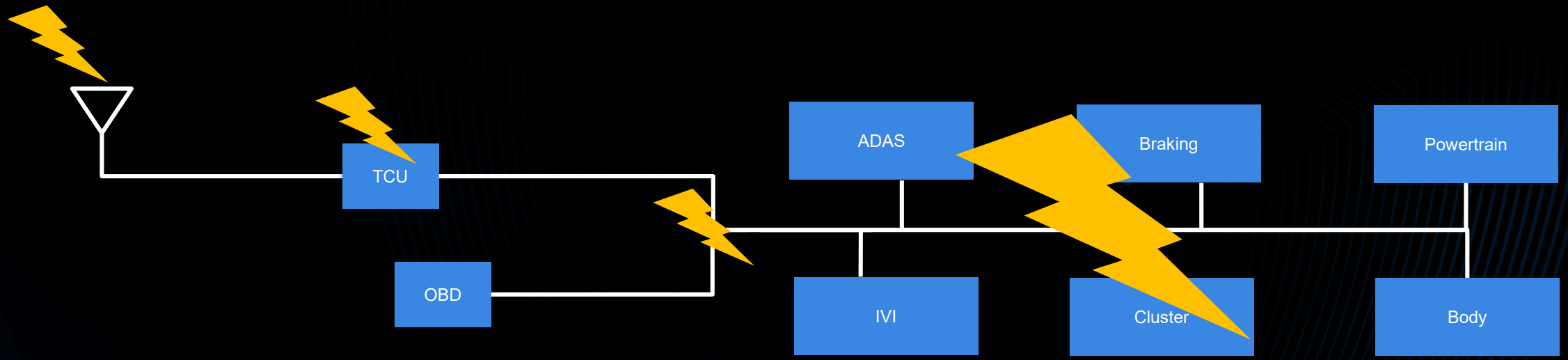
Wireless Interfaces
enable scalable attacks

250M connected vehicles on the road in 2020

SECURITY IS A MUST-HAVE FOR CONNECTED & AUTONOMOUS VEHICLES

© 2018 NXP Semiconductors. All rights reserved.

Blueprint for typical (remote) attacks



1. Connect to modem *(cellular / internet)*
2. Exploit vulnerabilities in the connected ECU *(e.g. TBox, IVI, …)*
3. Thereby gain access to the CAN network
4. And steal data or take over control *(e.g. slam the brakes)*

Security ignored, or applied as an after-thought!

No (or weak) security countermeasures, no (domain) isolation, etc.

© 2018 NXP Semiconductors. All rights reserved.

Way forward

- Typical pattern (recap):
  - Identify a vulnerability …
    - Through reverse engineering, usually with local access

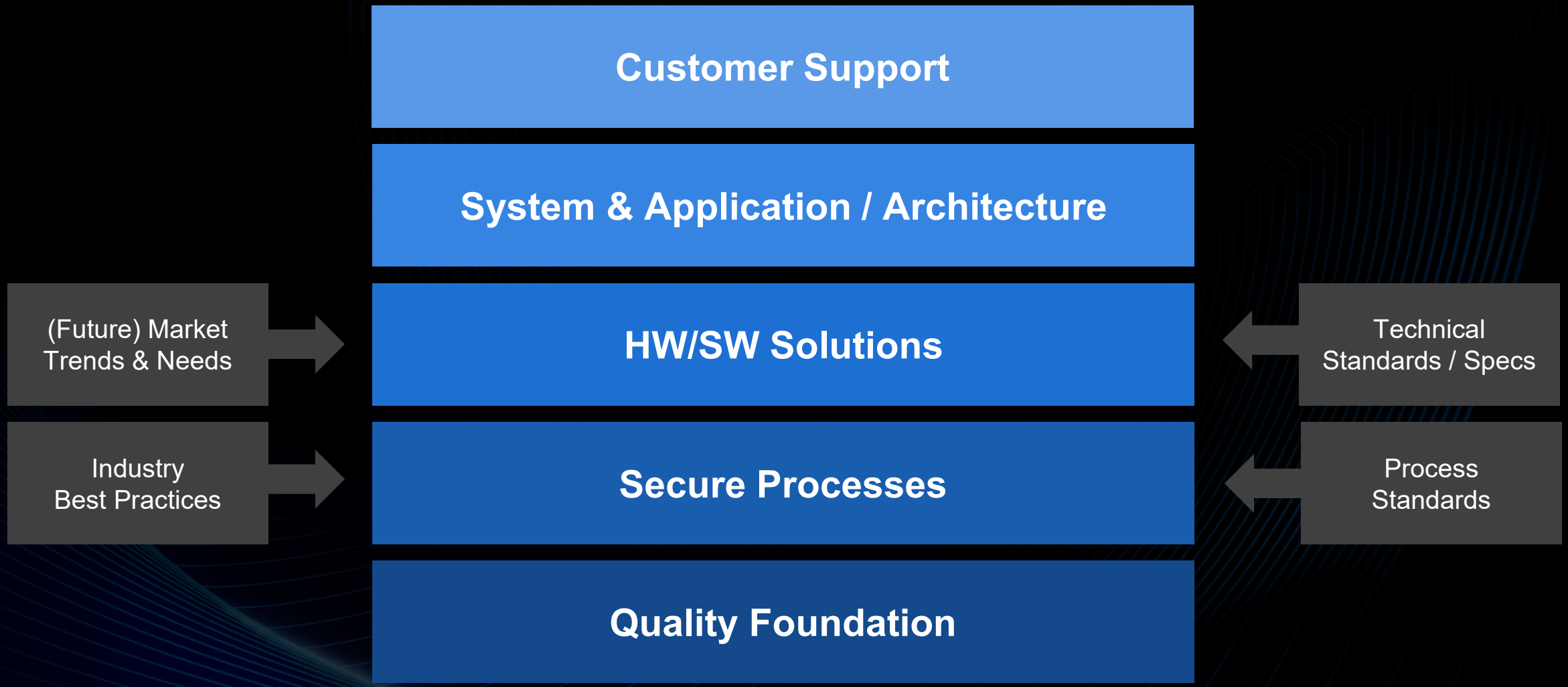
    … and then exploit it
    - If possible, remotely
  - Once on the network, pivot to other ECUs (extend the attack chain)
  - If possible, scale to multiple vehicles / entire fleets

- Apply a combination of:
  - Technical countermeasures ...
    - Secure boot, M2M authentication, secure communication, firewalls, …

    … in a robust implementation
    - Secure software *and* hardware
  - Improvements to the network architecture
    - Make it (more) resilient, by design
  - Reducing / preventing common weaknesses
    - Secure coding standards to reduce the # of vulnerabilities, no shared secrets/keys, …

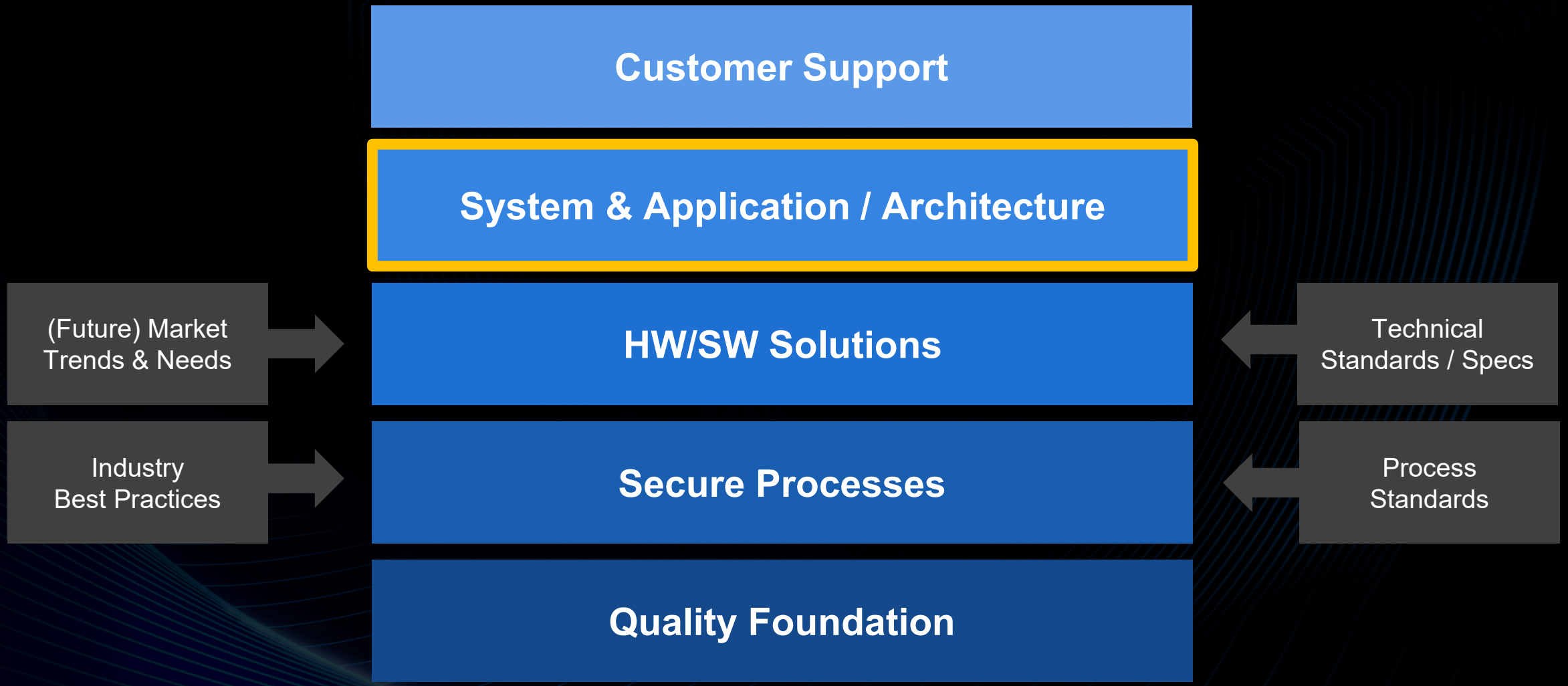
© 2018 NXP Semiconductors. All rights reserved.

Holistic approach to automotive security



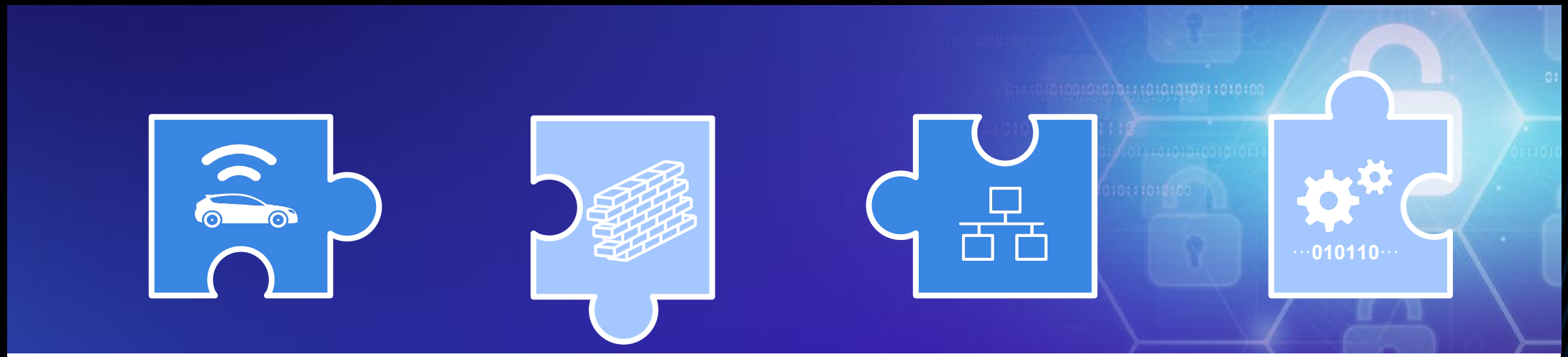
© 2018 NXP Semiconductors. All rights reserved.

Holistic approach to automotive security



© 2018 NXP Semiconductors. All rights reserved.

Core Security Principles – Defense in Depth

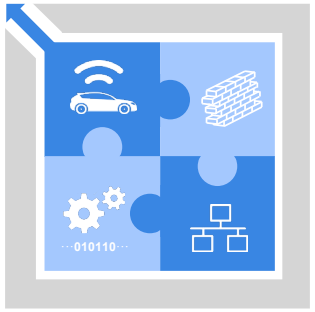


Secure **External Interfaces**

Secure **Domain Isolation**

Secure **Internal Communication**

Secure **Software Execution**



They need to be in place in ***any*** E&E network

- Regardless of the actual architecture and implementation

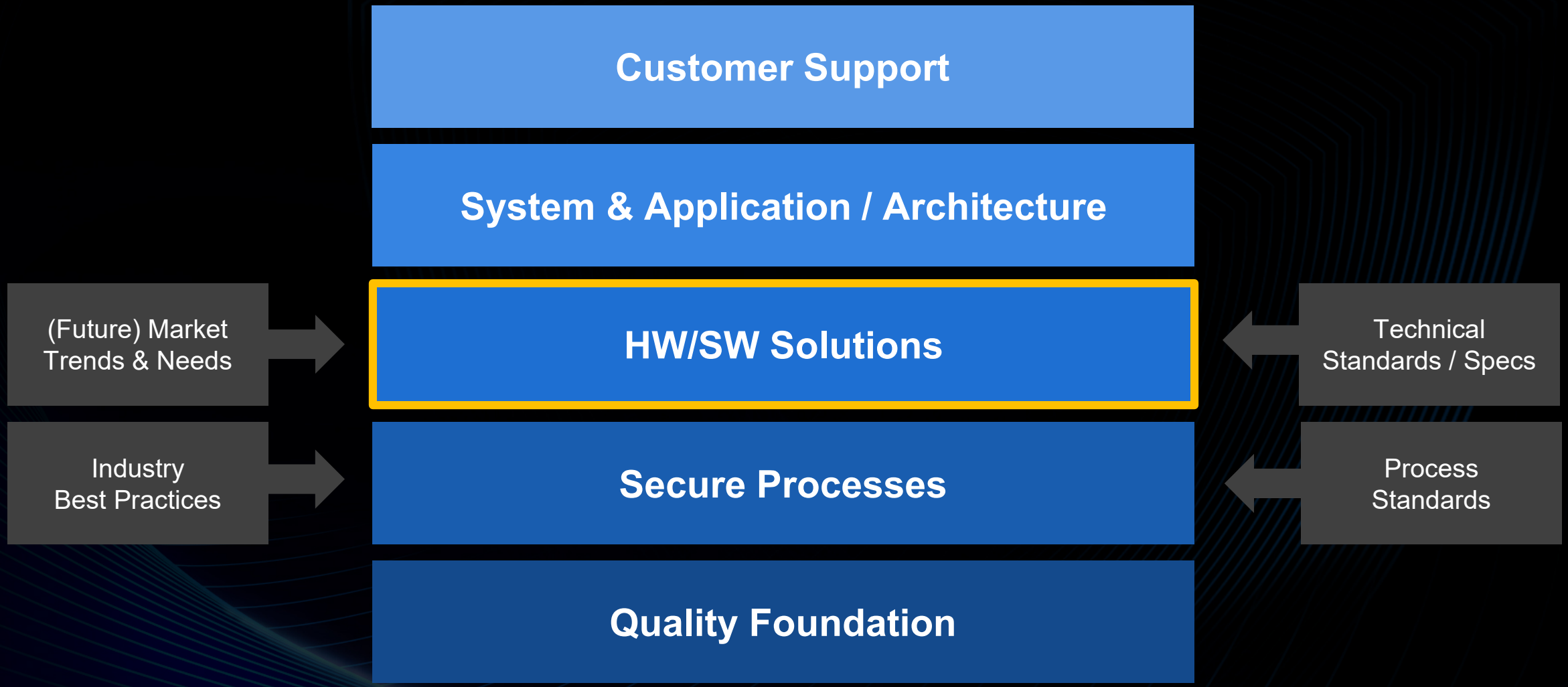
© 2018 NXP Semiconductors. All rights reserved.

Applying The Core Security Principles

	Prevent access	**Detect** attacks	**Reduce** impact	**Fix** vulnerabilities
Secure Interfaces	M2M Authentication & Firewalling			
Secure Gateway	Firewalling (context-aware message filtering)	Intrusion Detection Systems (IDS)	Separated Functional Domains	Secure Updates
Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	

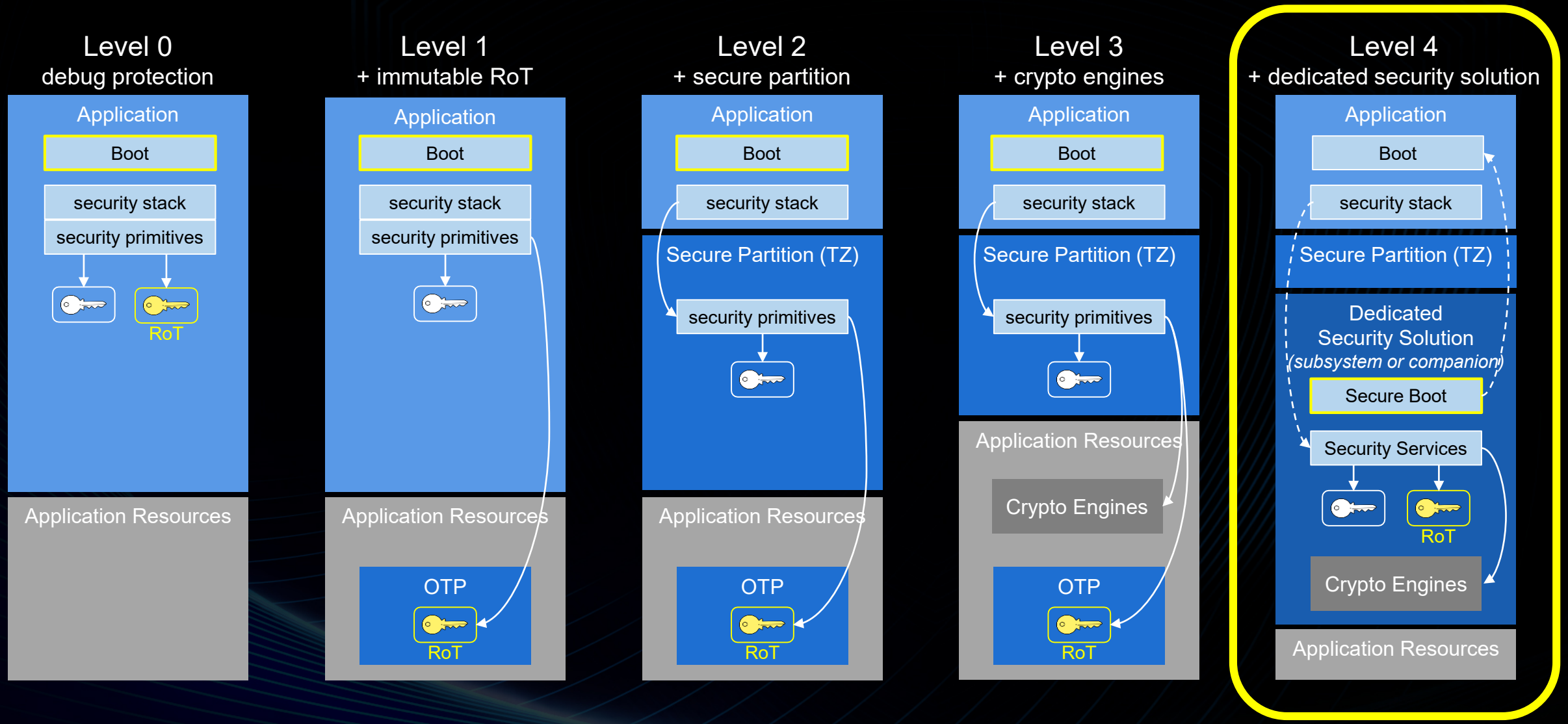
© 2018 NXP Semiconductors. All rights reserved.

Holistic approach to automotive security



© 2018 NXP Semiconductors. All rights reserved.

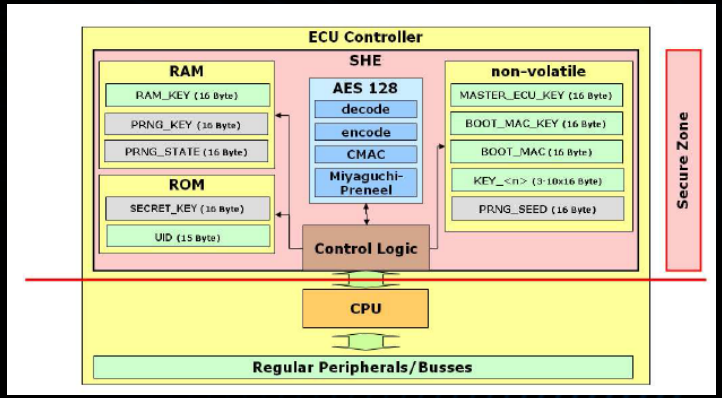
How can hardware help to enhance the security of software?



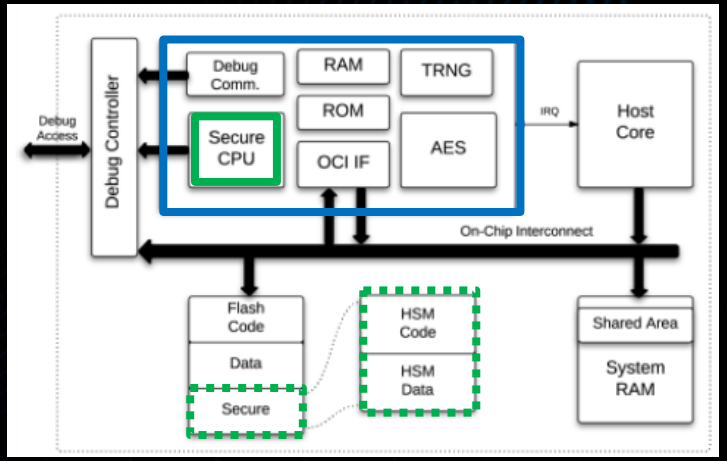
© 2018 NXP Semiconductors. All rights reserved.

Specifications – HIS SHE / EVITA HSM

- Both specify an on-chip security module, featuring:
  - A state machine (SHE), or a programmable core (HSM)
  - An AES accelerator, RNG and dedicated memory (key slots)
- A basic building block for protecting SW and data
  - Use cases: secure boot, secure FOTA update, secure storage, secure (IVN) communication, …
- Primary goal: protect against software-based attacks
  - SHE and HSM both move the control over crypto keys from the software domain, into the hardware domain
  - To protect those crypto keys from leaking / being cloned



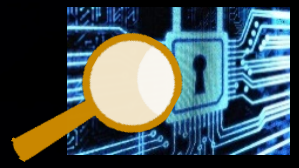
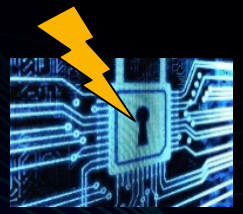
Secure Hardware Extension (SHE, ~2008)
(HIS consortium: VW, Audi, Porsche, Daimler, BMW)

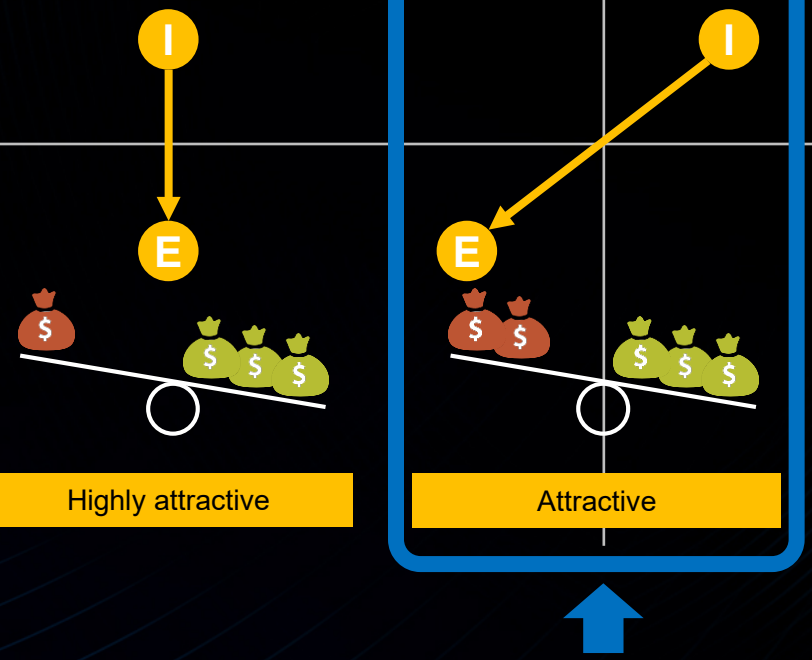


Hardware Security Module (HSM, ~2012)
(EVITA project)

© 2018 NXP Semiconductors. All rights reserved.

Should we only care about remote / logical / software-based attacks?

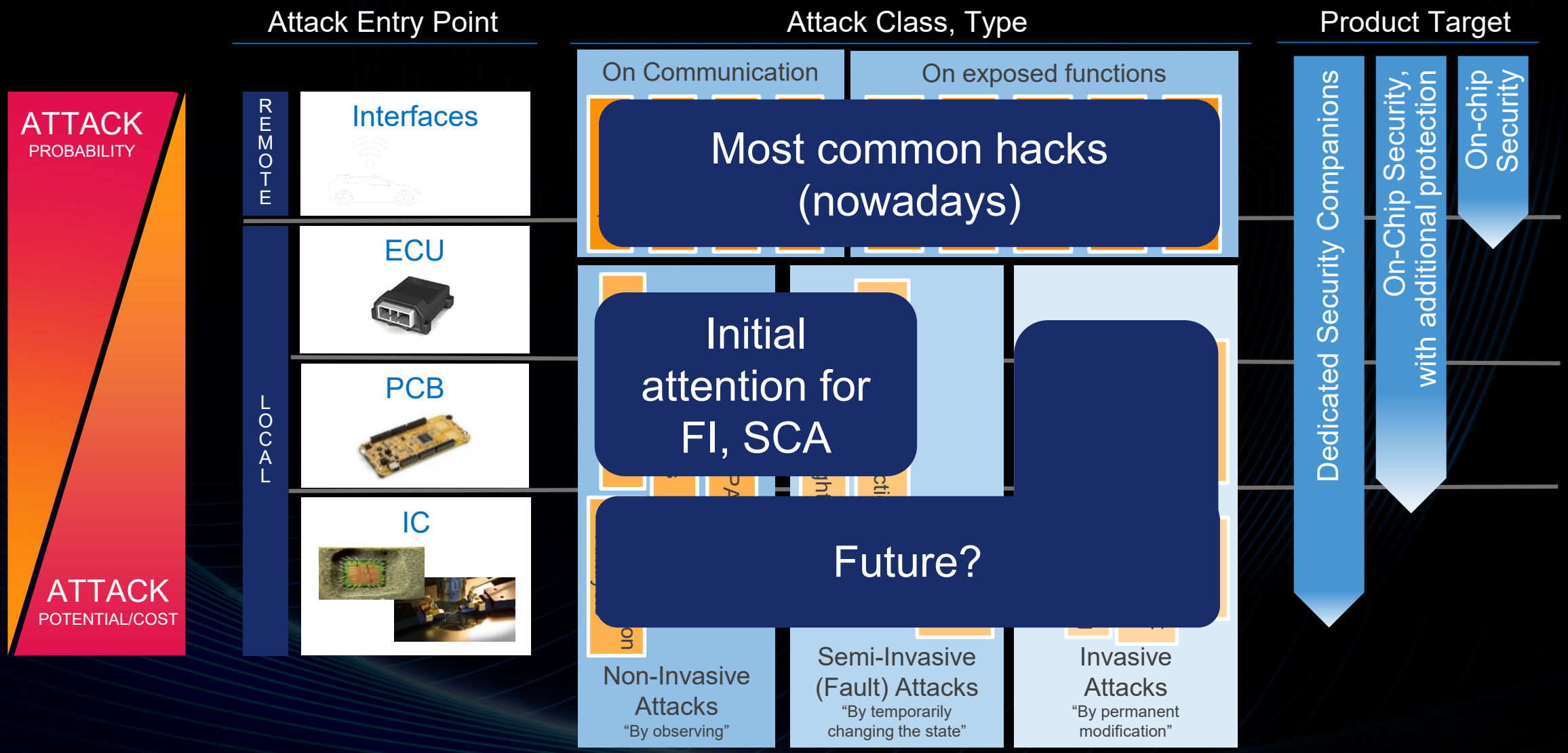
Attack phases	remote (logical access)		local (physical access)
1. Identification *Vulnerability analysis* 	*Cost:* *Low*	**Remote attack**	**Hybrid attack**	**Physical attack**	*Cost:* *Medium – High*
2. Exploitation *Exploit vulnerabilities* 	*Cost:* *Low* *Scalability:* *High* *(many devices)*	Highly attractive	Attractive	Attractive, *if the* assets per device are highly valuable	*Cost:* *High* *Scalability:* *Low* *(single device)*



Hybrid attacks are not the easiest… but may lead to large-scale attacks!

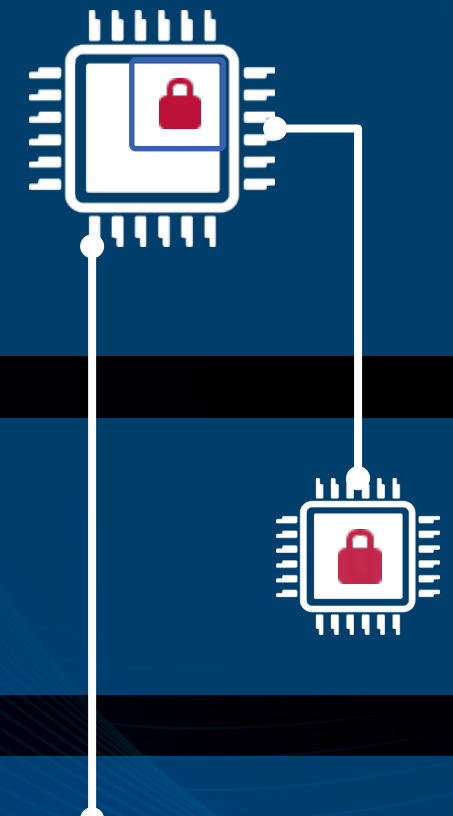
© 2018 NXP Semiconductors. All rights reserved.

Different Solutions For Different Security Needs



© 2018 NXP Semiconductors. All rights reserved.

Automotive Security Solutions Groups



Automotive ICs with On-chip Security Subsystem

Integrated solution for best fit with application real-time constraints & for strict security policy enforcement

SENSE THINK ACT

Security Companions

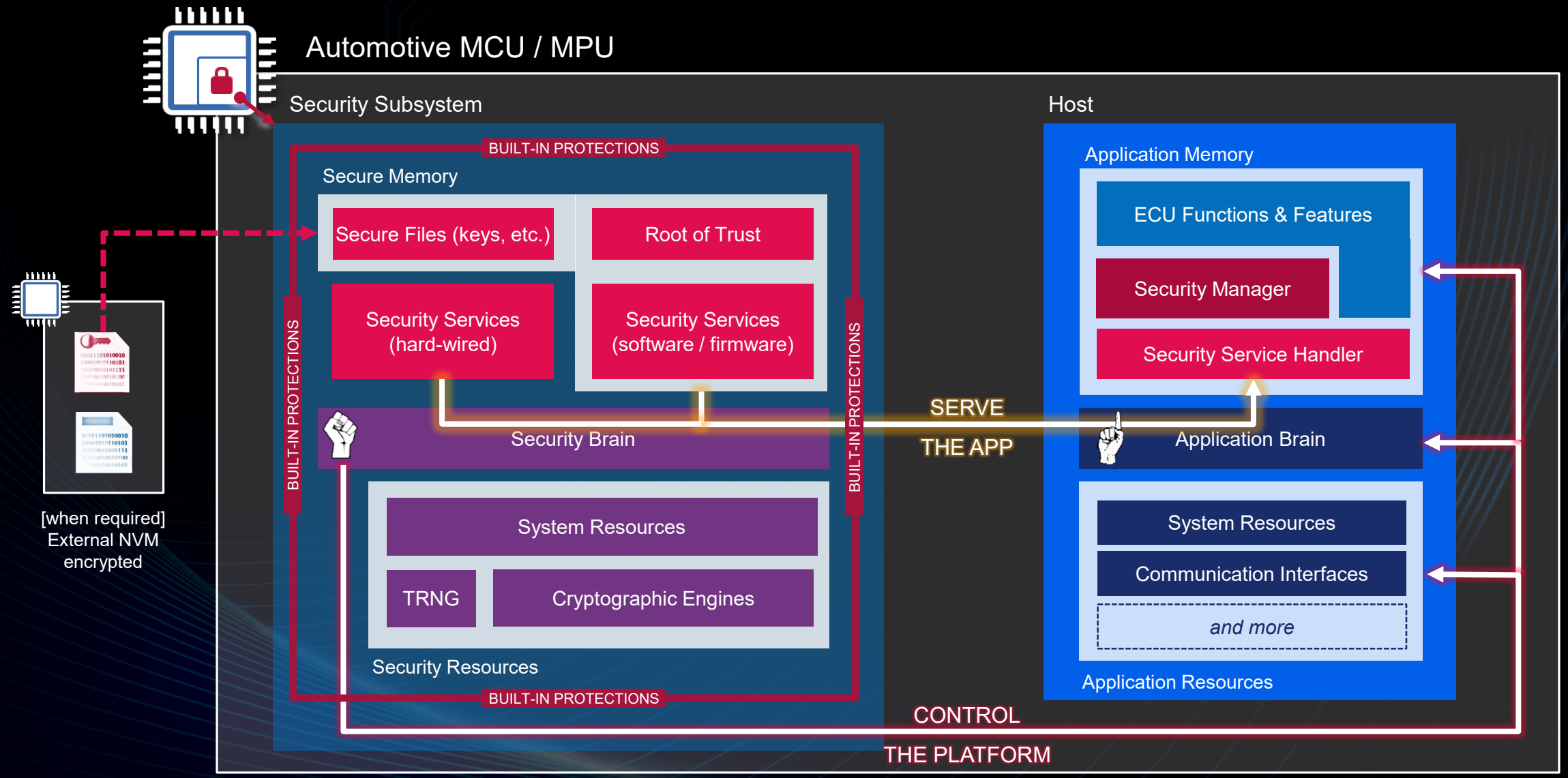
Security extension *for specific use*.
Highest levels of protection.

Function-specific Secure ICs

Fit-for-purpose security support

© 2018 NXP Semiconductors. All rights reserved.

ICs with On-Chip Security Subsystems – Overview



© 2018 NXP Semiconductors. All rights reserved.

Offering a Rich Set of Services…

Cryptographic functions
- Encryption / decryption
- MAC generation / verification
- Hashing
- Signature generation / verification

Key management
- Key import & export
- Key generation
- Key derivation
- Key exchange

Random number generation
- Pseudo-random numbers based on true random seed

Memory checks
- Memory verification at start-up (secure boot)
- Memory verification at run-time

Monotonic counters
- Incrementing and reading volatile & non-volatile counters

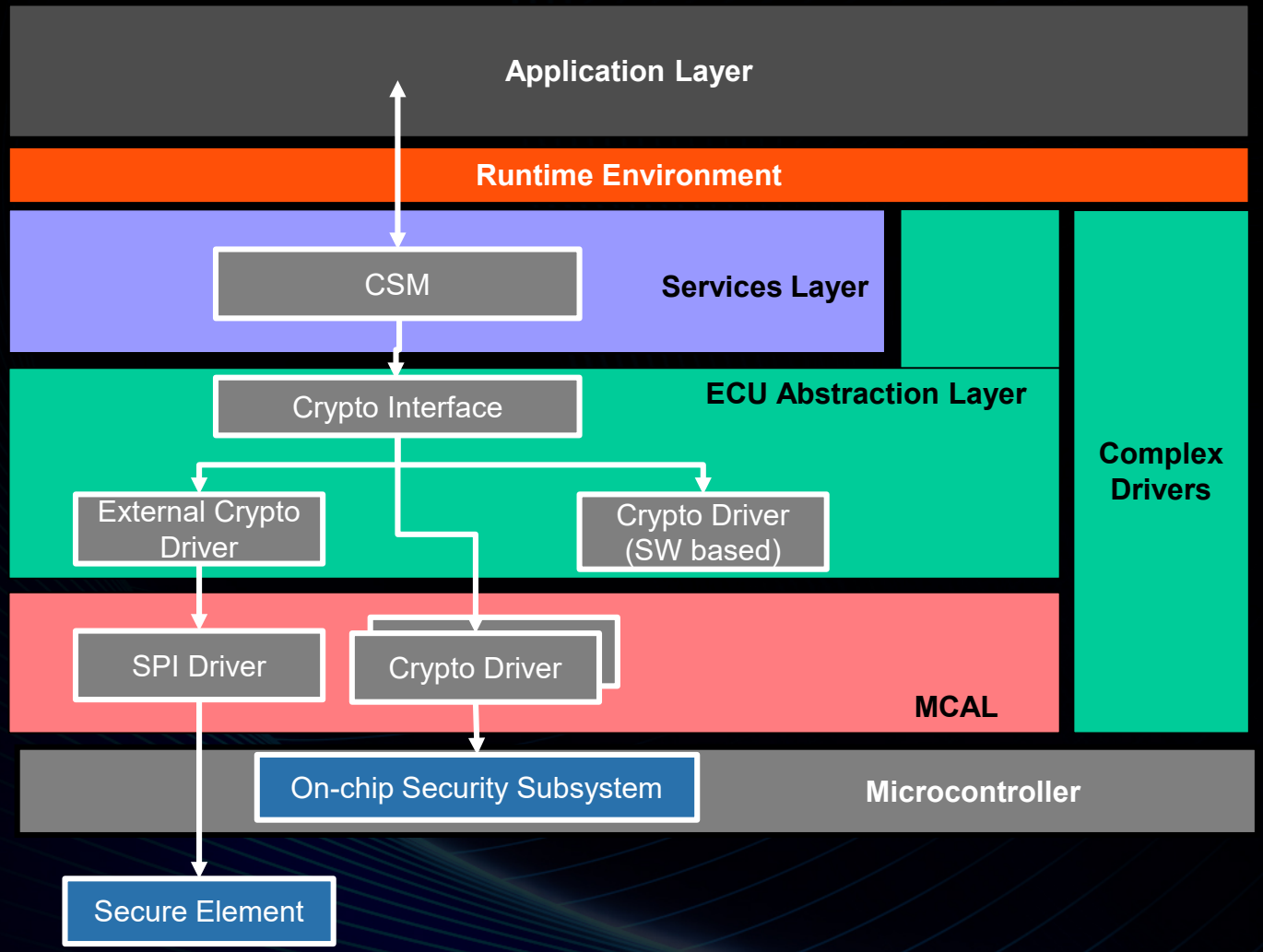
Secure time base
- Secure tick to host

Administration
- System initialization & configuration
- Functional tests
- Security policy manager
- Service updates & extension

Secure network protocols
- SSL / TLS offload
- IPsec offload

© 2018 NXP Semiconductors. All rights reserved.

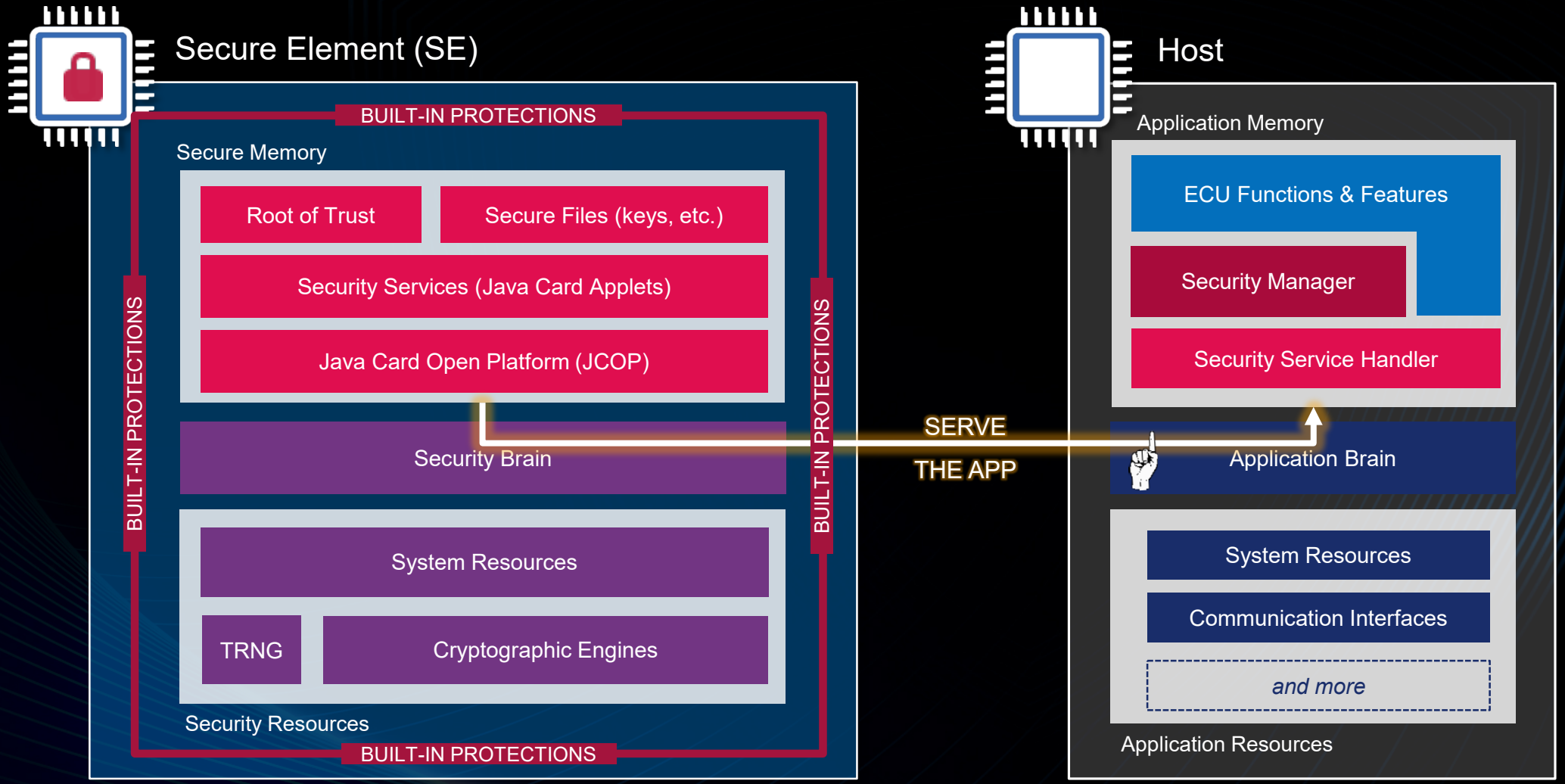
...to Higher-Layer Software Stacks



← Example: AUTOSAR 4.3 (Crypto Stack)

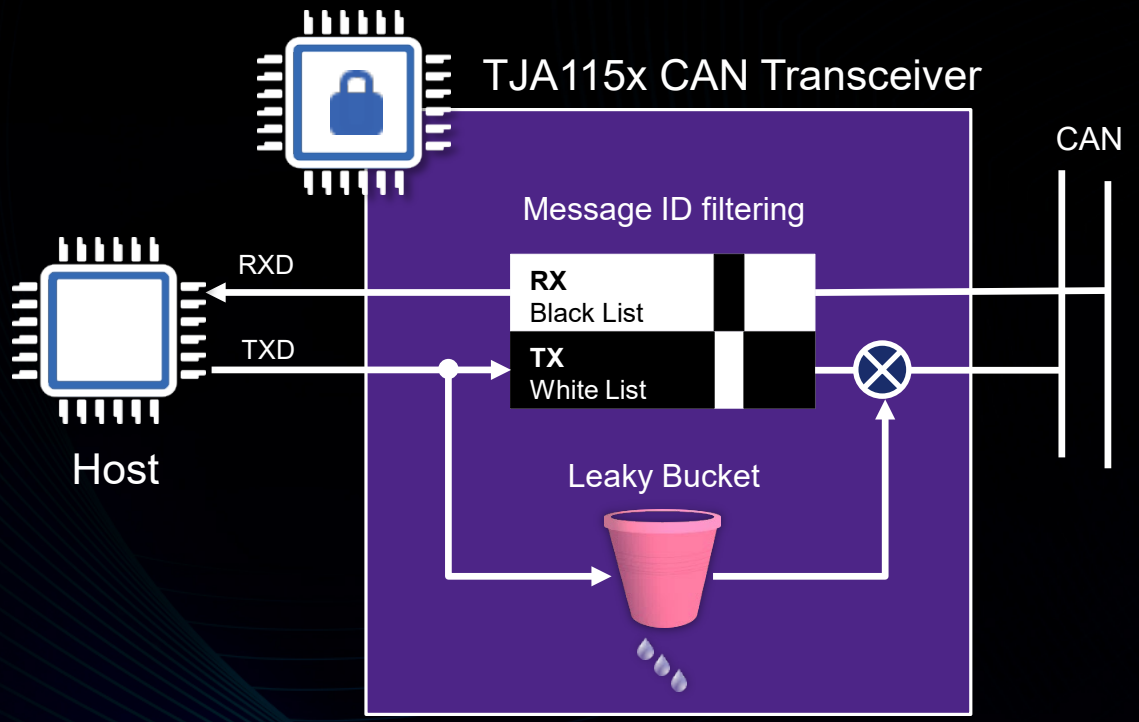
© 2018 NXP Semiconductors. All rights reserved.

Security Companions – Overview



© 2018 NXP Semiconductors. All rights reserved.

Example of a Function-Specific Secure IC – NXP's Secure CAN Transceiver

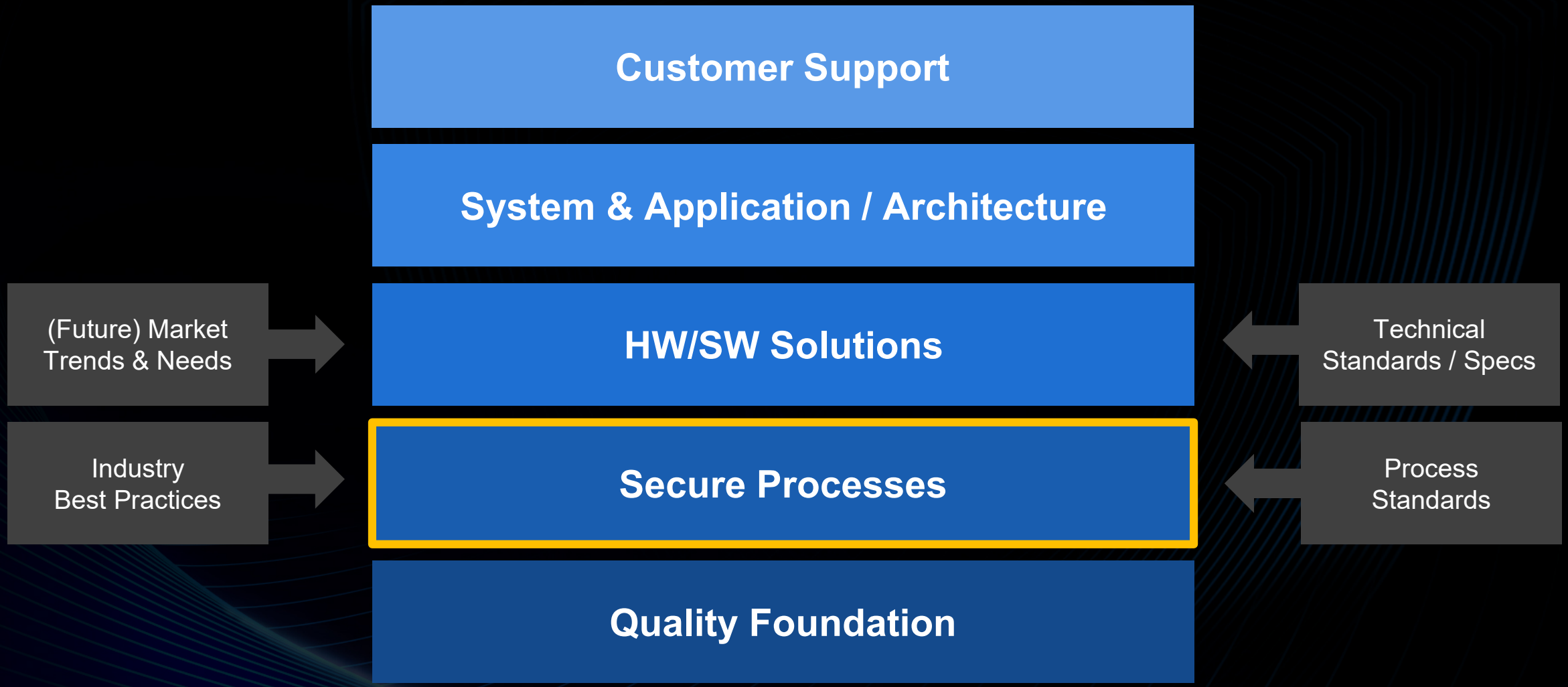


Do we always need crypto? NO!

- Intrusion detection & prevention (IDS / IPS)
  - On-the-fly CAN ID filtering and bus-guarding
  - Based on user configurable white and black lists
- Flooding prevention (DoS)
  - Threshold on message transmission: *leaky bucket* strategy
- "1:1" replacement to any CAN transceiver
  - In-field reconfiguration possible

© 2018 NXP Semiconductors. All rights reserved.

Holistic approach to automotive security



© 2018 NXP Semiconductors. All rights reserved.

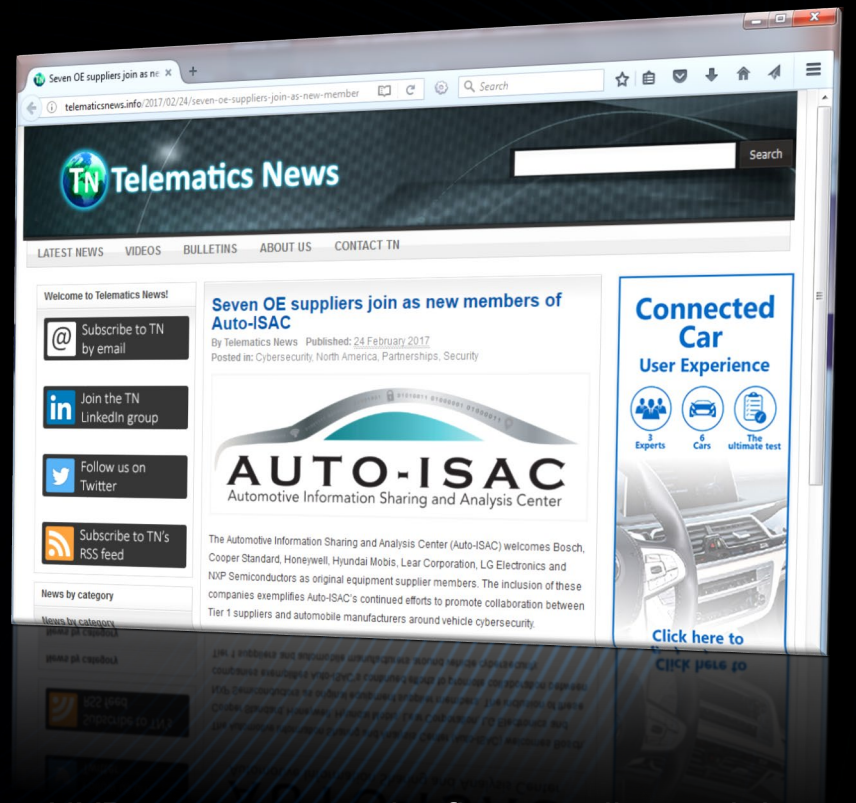
NXP's Automotive Cybersecurity Program

Holistic Approach to Security:

- Secure Solutions
- Secure Product Engineering Process
- Internal / External Security Evaluation (VA)
- Product Security Incident Response Team
- Security-Aware Organization (incl. Trainings)
- Threat Intelligence Feed

Leveraging Our IT Cyber Security Framework:

- CSO / SOC / CSIRT, Information Security Policies, Incident Management & Response Processes, Site Security (ISO 27001 cert.), …



NXP was amongst the first suppliers to join the Auto-ISAC (Aug. 2016)

© 2018 NXP Semiconductors. All rights reserved.

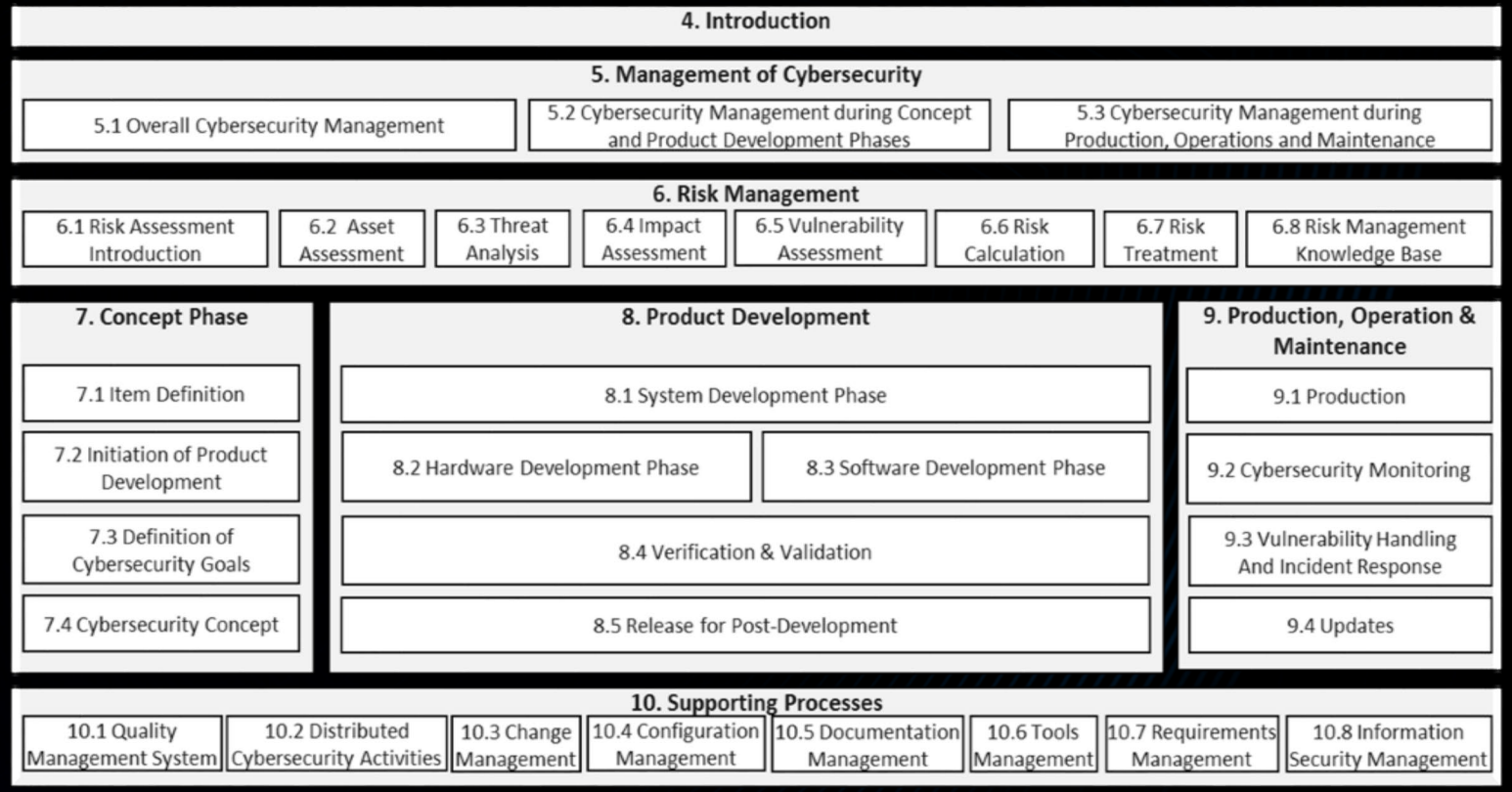
ISO/SAE 21434 – Automotive Cybersecurity Engineering

What is it?

- Provides a framework for security engineering
  - Focus: processes & WoW, governance, assessments, assurance levels, evidence, …
- Similar to what ISO 26262 is, for Functional Safety

Status: in development

- Publication in 2020 (target)



© 2018 NXP Semiconductors. All rights reserved.

Conclusion

- Automotive Innovation is changing towards developing self-driving robots
- Security is essential – people must be able to trust their cars
- Automotive security must be addressed holistically, involving:
  - Vehicle network architecture improvements
  - Secure software *and* hardware
  - Security culture, processes, WoW, …

www.nxp.com/automotivesecurity

© 2018 NXP Semiconductors. All rights reserved.

THANKS