NXP Automotive Cybersecurity Program

John Cotner

Security Architect - Automotive

October 2019 | Session #AMF-AUT-T3878

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

Company Public – NXP, the NXP logo, and NXP secure connections for a smarter world are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2019 NXP B.V.

Agenda

Auto Security

- What & Why
- Approach
- Solutions
- Processes

Did You Know?

>50

Vehicle hacks
published since 2015

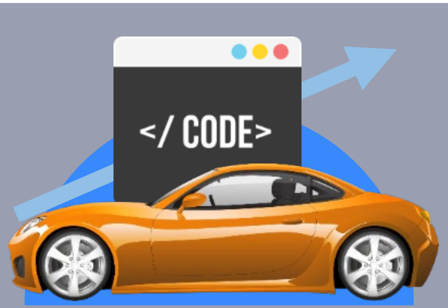
1.4 M

Vehicles recalled
in the largest
incident to date

Why hacking?

Valuable data
attracts hackers

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



Why is it possible?

High system complexity
implies high vulnerability

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

Why now?

Wireless interfaces
enable scalable attacks

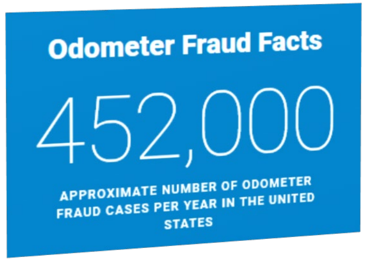
250 M connected vehicles on the road in 2020

Security is a must-have for connected & autonomous vehicles

Cybersecurity Threats in Automotive

Local Attacks → Remote Attacks

Tampering the odometer



Odometer Fraud Facts

452,000

APPROXIMATE NUMBER OF ODOMETER FRAUD CASES PER YEAR IN THE UNITED STATES

https://www.nhtsa.gov/equipment/odometer-fraud

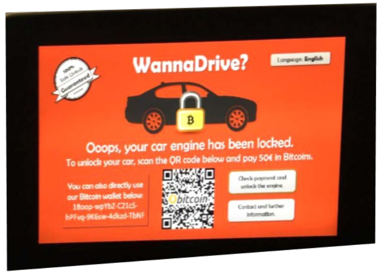
Vehicle theft by relay attack

https://www.youtube.com/watch?v=8pffcngJJq0

Engine tuning

Workshop around the corner, or in your garage

Ransom for a drive



WannaDrive?

Language: English

100% Safe Unlock Guaranteed

Ooops, your car engine has been locked.

To unlock your car, scan the QR code below and pay 50€ in Bitcoins.

You can also directly use our Bitcoin wallet below: 1Boop-wpYbZ-C21cS-hPFvq-9K6sw-4dkzd-TbNF

Check payment and unlock the engine.

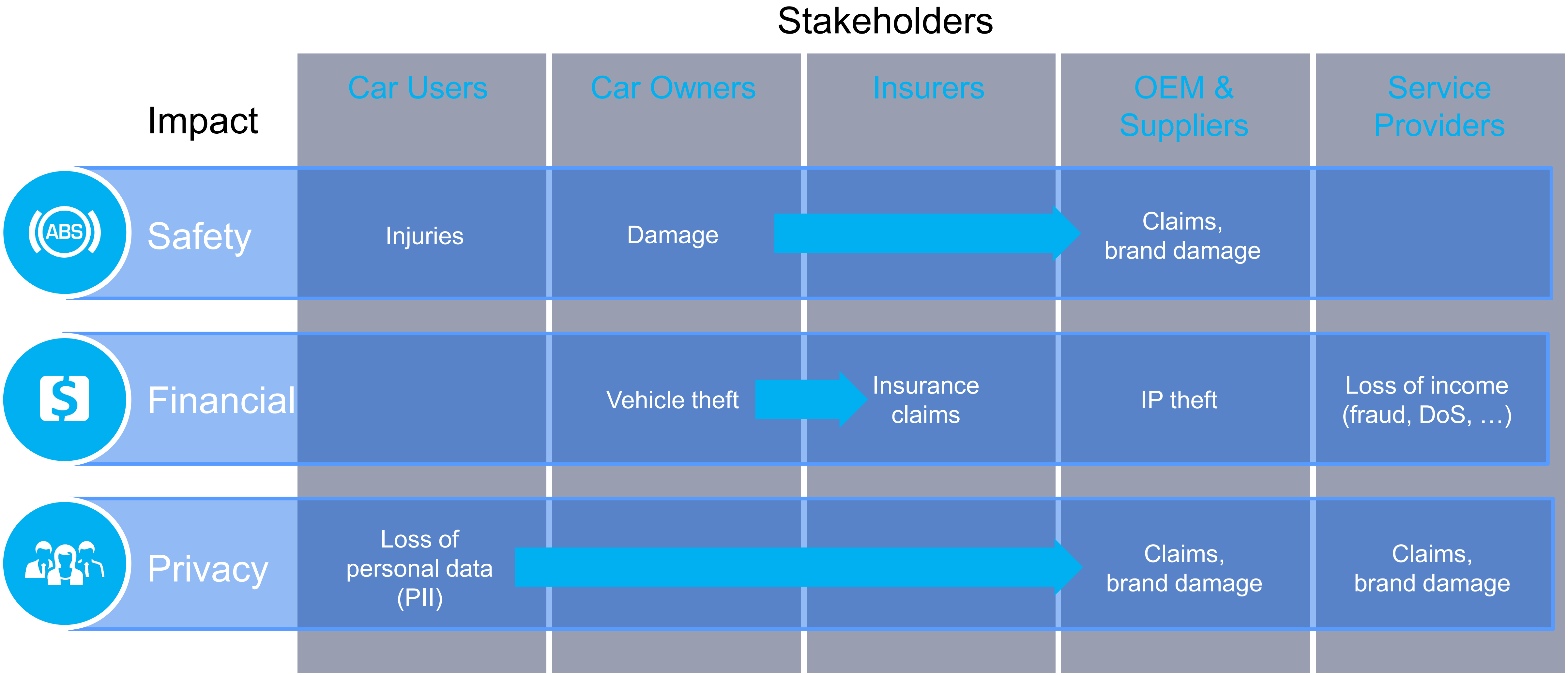
Contact and further information.

VDI Conference on IT Security for Vehicles
(Berlin / July 2017)

Remote hack of an unaltered car (July 2015)

https://www.youtube.com/watch?v=MK0SrxBC1xs

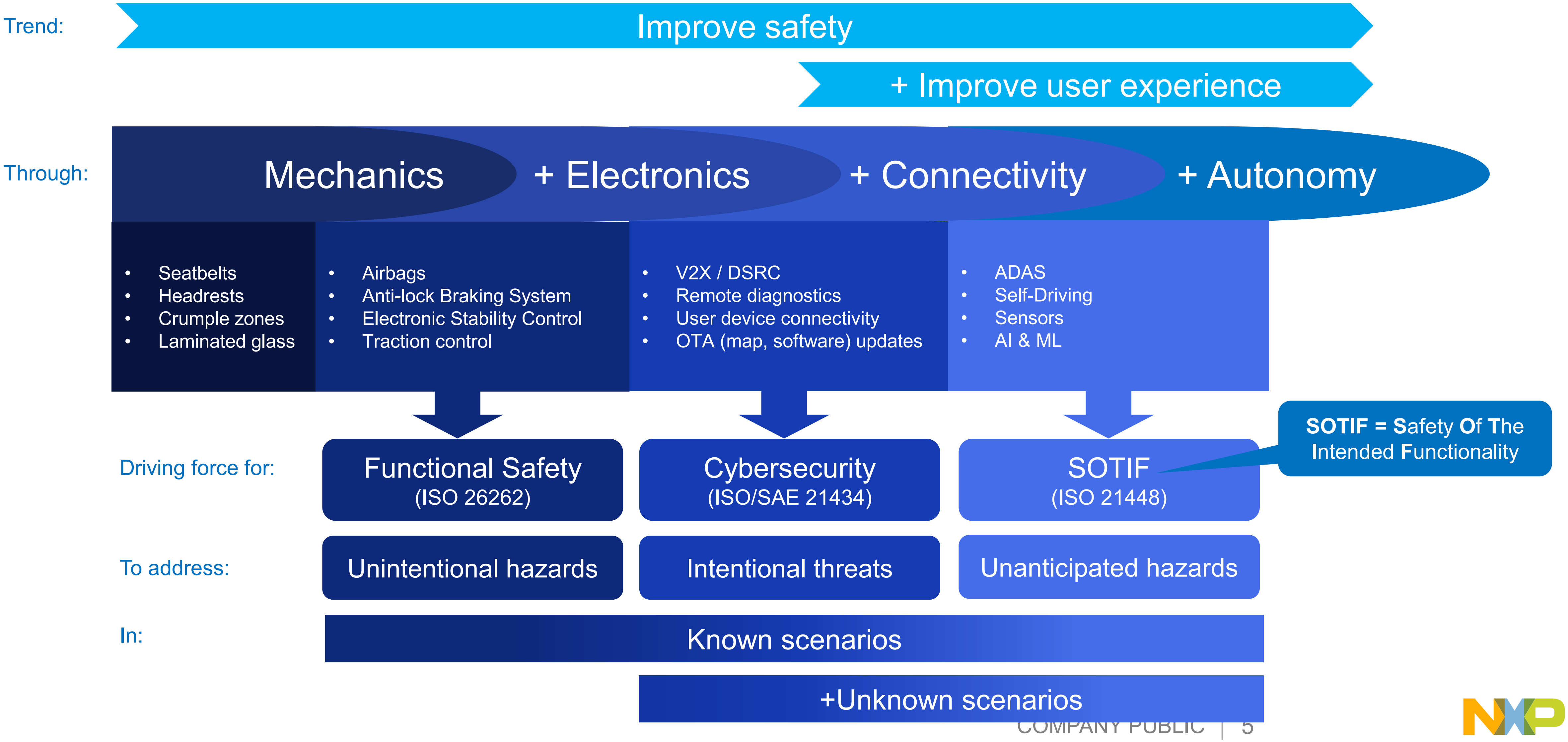
What is at Risk and who is Affected?



Stakeholders

Impact	Car Users	Car Owners	Insurers	OEM & Suppliers	Service Providers
Safety	Injuries	Damage →	→	Claims, brand damage	
Financial		Vehicle theft →	Insurance claims	IP theft	Loss of income (fraud, DoS, …)
Privacy	Loss of personal data (PII) →	→	→	Claims, brand damage	Claims, brand damage

Vehicle Safety & Cybersecurity



Trend:

Improve safety

+ Improve user experience

Through:

Mechanics

- Seatbelts
- Headrests
- Crumple zones
- Laminated glass

+ Electronics

- Airbags
- Anti-lock Braking System
- Electronic Stability Control
- Traction control

+ Connectivity

- V2X / DSRC
- Remote diagnostics
- User device connectivity
- OTA (map, software) updates

+ Autonomy

- ADAS
- Self-Driving
- Sensors
- AI & ML

Driving force for:

Functional Safety (ISO 26262)

Cybersecurity (ISO/SAE 21434)

SOTIF (ISO 21448)

SOTIF = Safety **O**f **T**he **I**ntended **F**unctionality

To address:

Unintentional hazards

Intentional threats

Unanticipated hazards

In:

Known scenarios

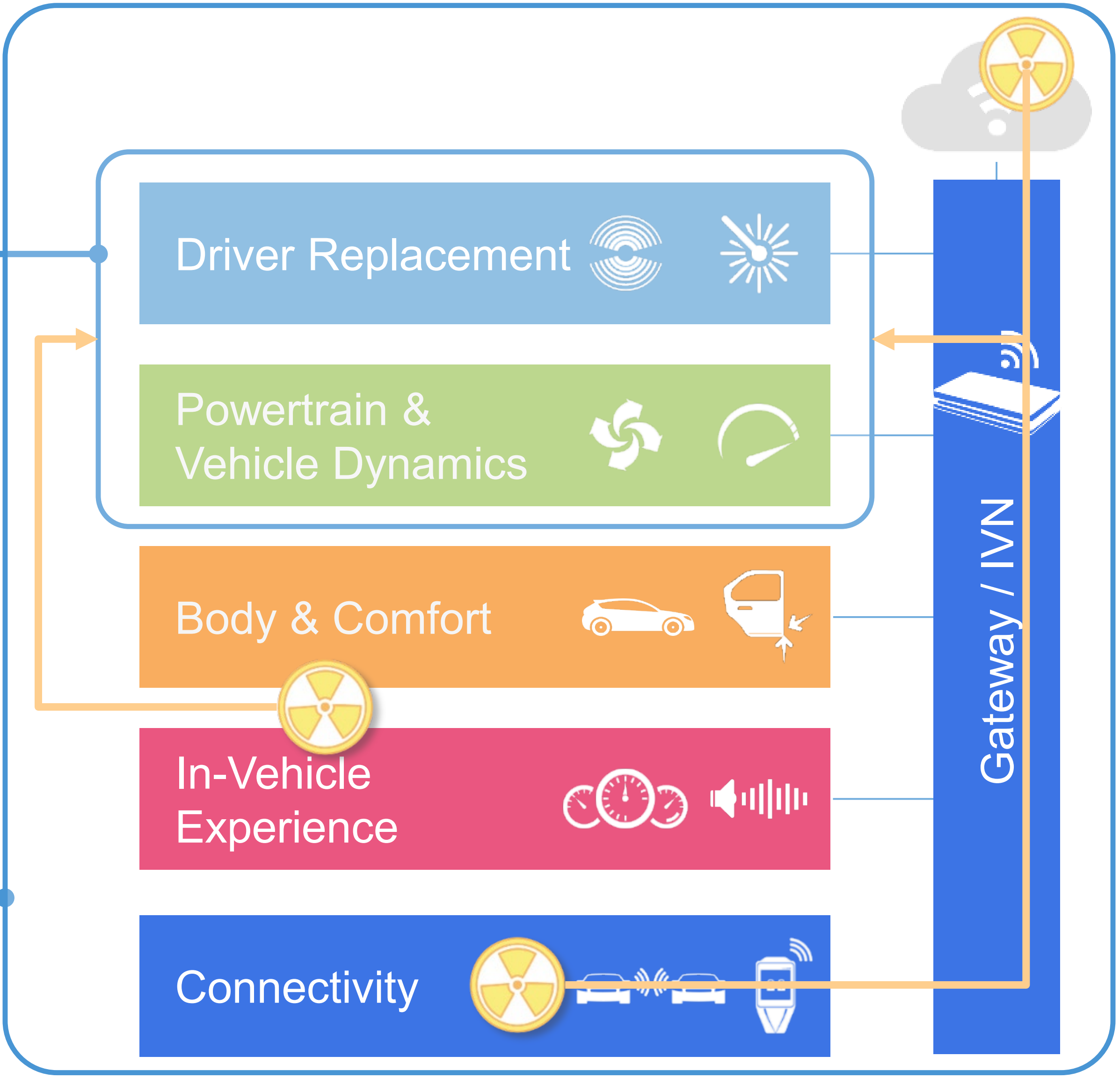
+Unknown scenarios

No Safety Without Security

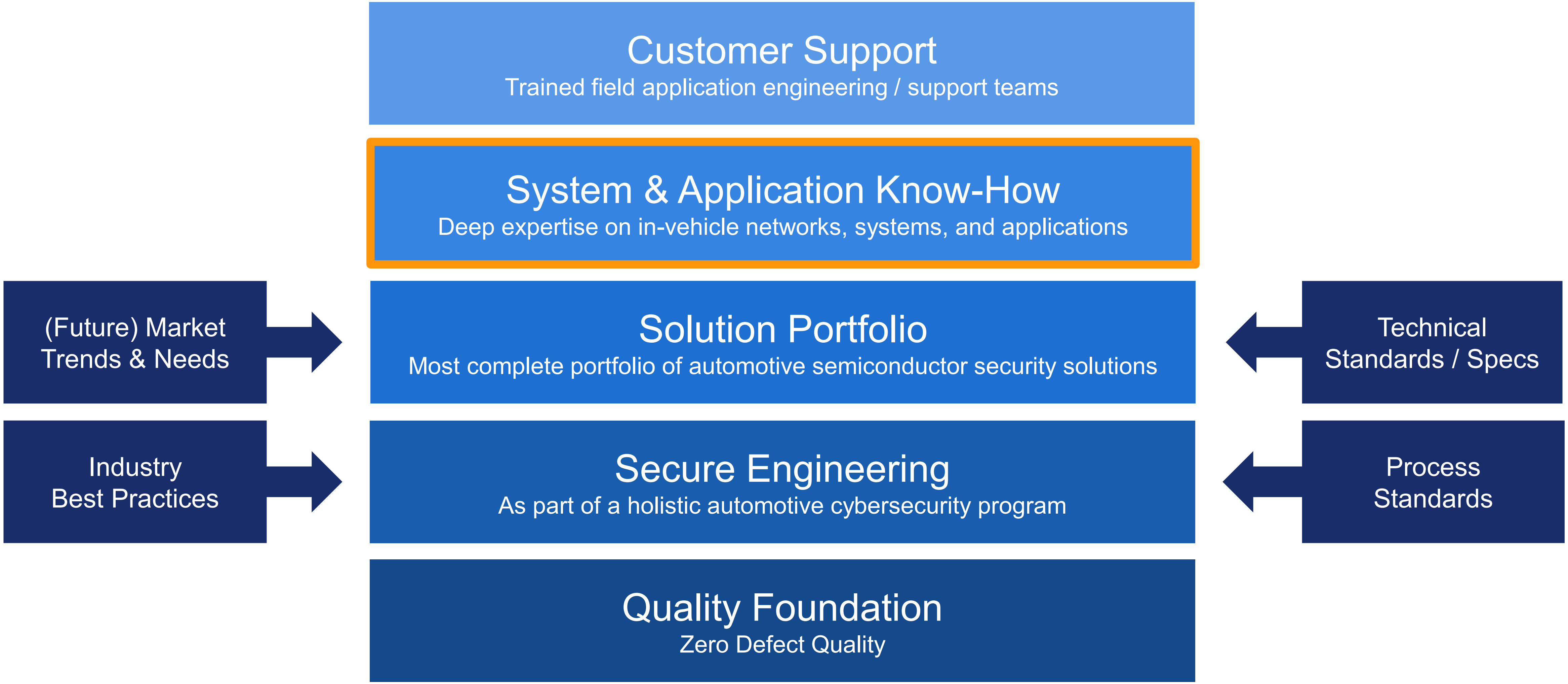
#1 Objective: no functional hazards on mission-critical ECUs

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

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



NXP's Approach to Automotive Security



Customer Support
Trained field application engineering / support teams

System & Application Know-How
Deep expertise on in-vehicle networks, systems, and applications

Solution Portfolio
Most complete portfolio of automotive semiconductor security solutions

Secure Engineering
As part of a holistic automotive cybersecurity program

Quality Foundation
Zero Defect Quality

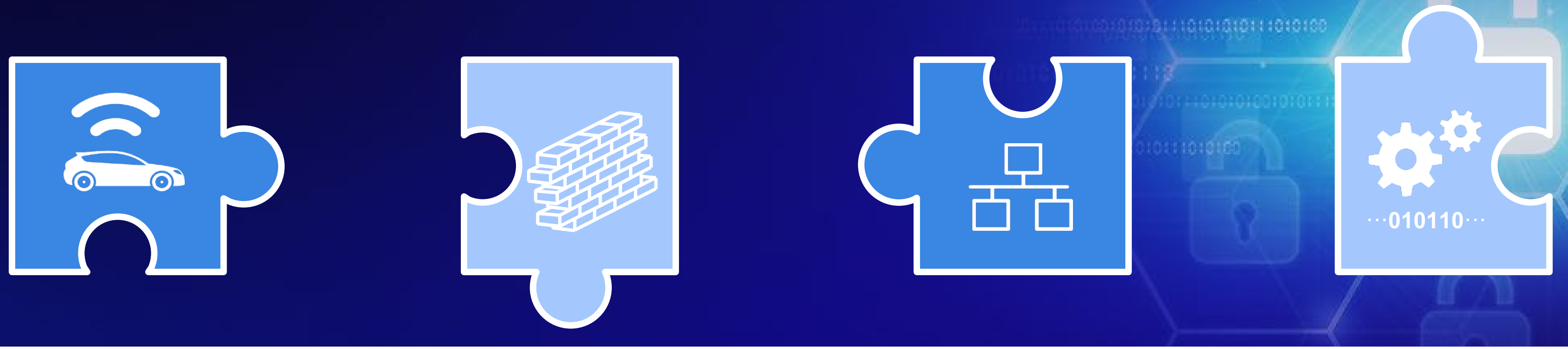
(Future) Market Trends & Needs

Industry Best Practices

Technical Standards / Specs

Process Standards

Core Security Principles for Defense in Depth

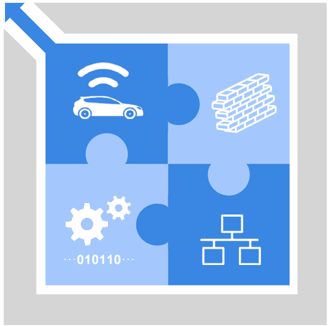


Secure **External Interfaces**

Secure **Domain Isolation**

Secure **Internal Communication**

Secure **Software Execution**



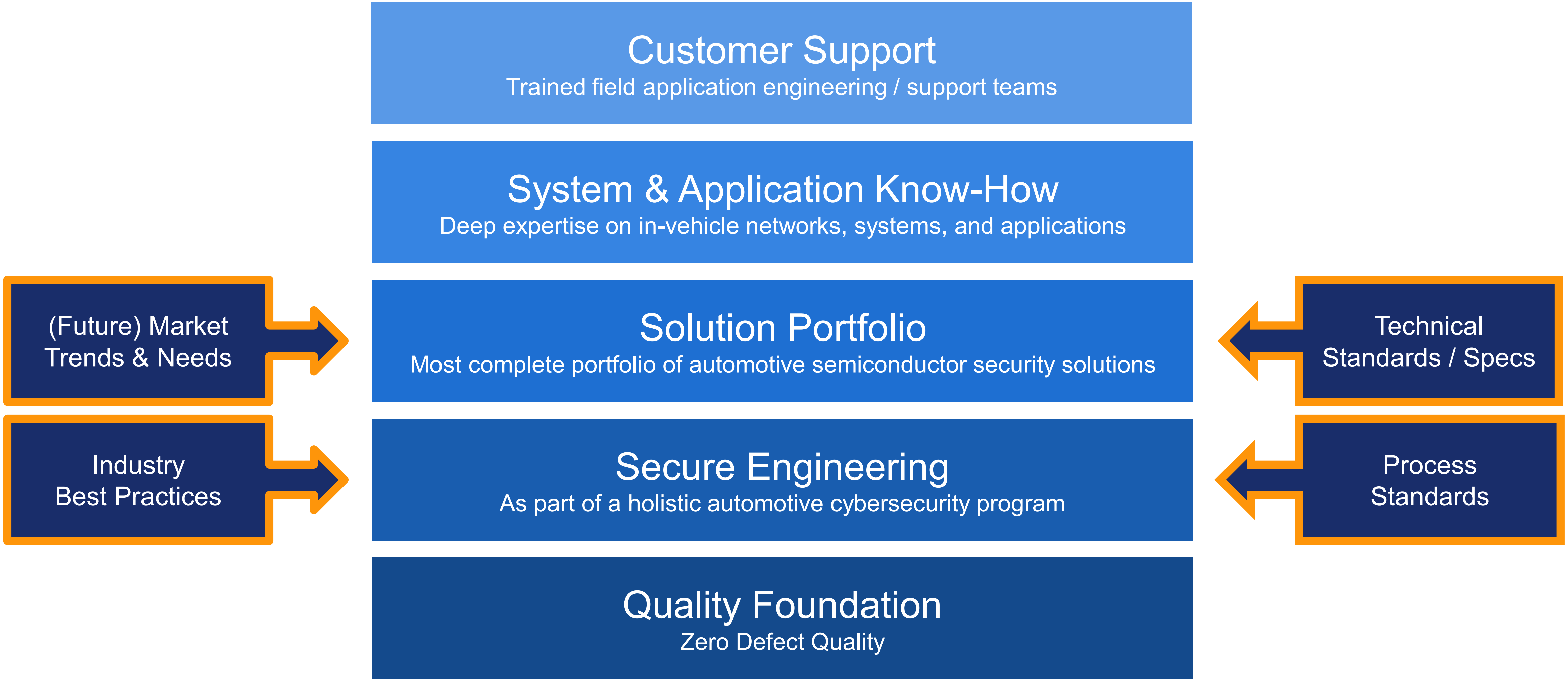
Multiple layers of protection – in ***any*** E&E network!

- To mitigate the risk of one component of the defense being compromised or circumvented
- Regardless of the actual vehicle network architecture and implementation

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)	

NXP’s Approach to Automotive Security



Customer Support
Trained field application engineering / support teams

System & Application Know-How
Deep expertise on in-vehicle networks, systems, and applications

(Future) Market Trends & Needs

Solution Portfolio
Most complete portfolio of automotive semiconductor security solutions

Technical Standards / Specs

Industry Best Practices

Secure Engineering
As part of a holistic automotive cybersecurity program

Process Standards

Quality Foundation
Zero Defect Quality

Standards and Best Practices

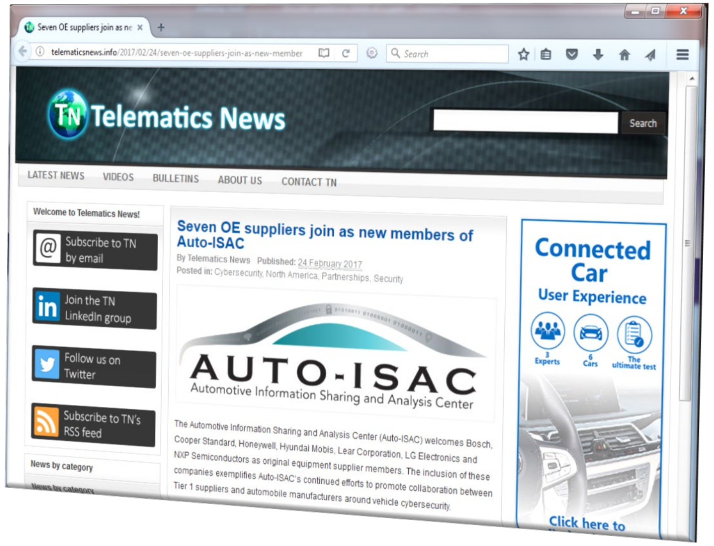
NXP is an active member of Auto-ISAC

- A key forum and network for automotive cybersecurity
- Enables leveraging industry know-how & best practices
- And sharing intelligence on threats & vulnerabilities

We also participate in standards development; e.g.:

- ISO/SAE 21434
- SAE TEVEES18 (J3061, J3101, …)
- AUTOSAR WP-X-SEC
- IEEE 1609 WAVE, ETSI TC ITS
- Car Connectivity Consortium (CCC) – Digital Key Specification

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



Seven OE suppliers join as ne
telematicsnews.info/2017/02/24/seven-oe-suppliers-join-as-new-member
Search
Telematics News
Search
LATEST NEWS
VIDEOS
BULLETINS
ABOUT US
CONTACT TN
Welcome to Telematics News!
Subscribe to TN by email
Join the TN LinkedIn group
Follow us on Twitter
Subscribe to TN's RSS feed
News by category
AUTO-ISAC
Automotive Information Sharing and Analysis Center
Connected Car
User Experience
3 Experts
6 Cars
The ultimate test
Click here to

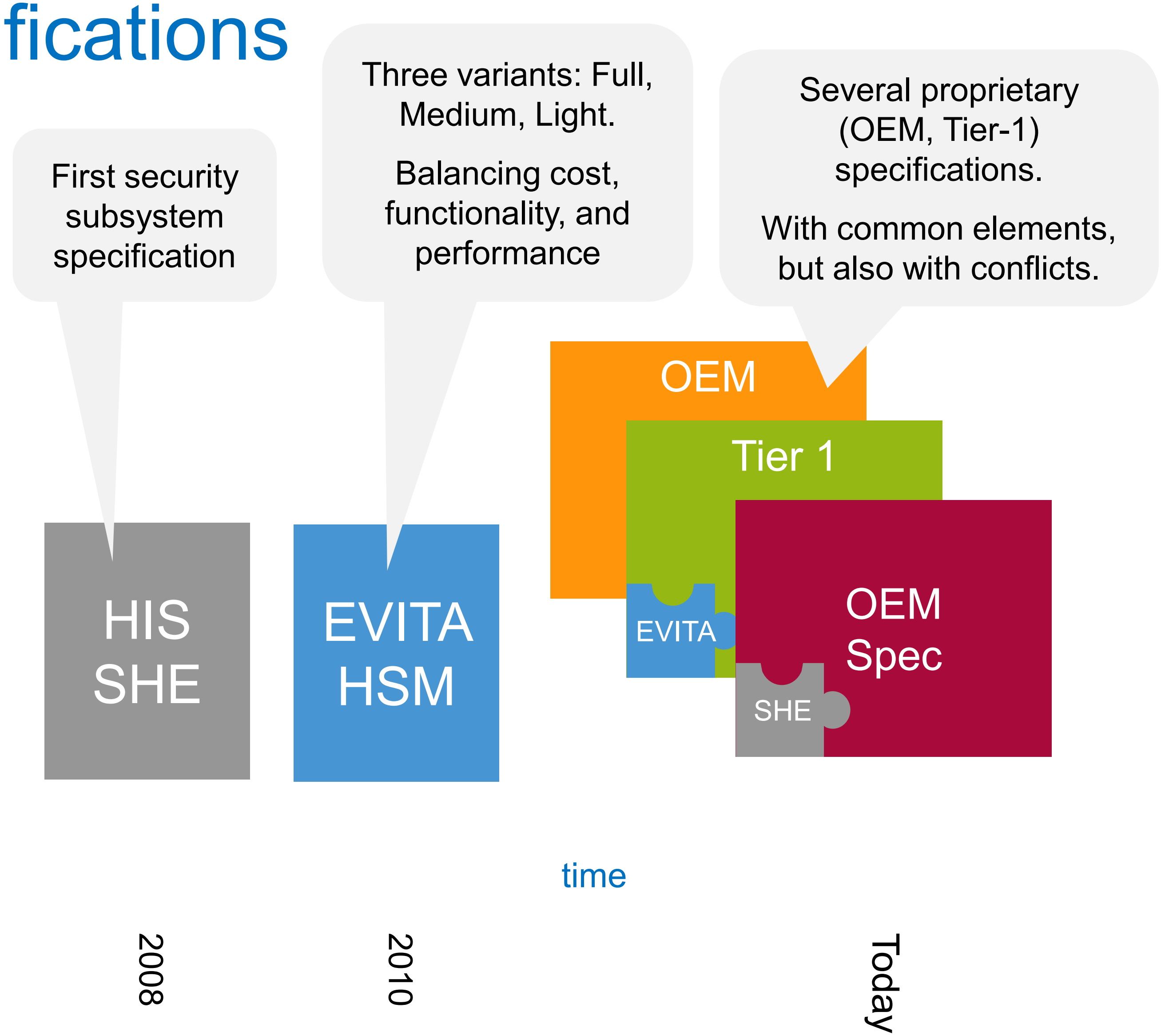
Seven OE suppliers join as new members of Auto-ISAC

By Telematics News Published: 24 February 2017
Posted in: Cybersecurity, North America, Partnerships, Security

The Automotive Information Sharing and Analysis Center (Auto-ISAC) welcomes Bosch, Cooper Standard, Honeywell, Hyundai Mobis, Lear Corporation, LG Electronics and NXP Semiconductors as original equipment supplier members. The inclusion of these companies exemplifies Auto-ISAC's continued efforts to promote collaboration between Tier 1 suppliers and automobile manufacturers around vehicle cybersecurity.

Automotive Security Specifications

- The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem
- EVITA’s HSM specification extended this concept into a programmable subsystem, in three flavors (Full, Medium, and Light), addressing a broader range of use cases
- Nowadays, OEMs are creating their own technical specifications, including select aspects of SHE, EVITA, and FIPS 140-2


First security subsystem specification

Three variants: Full, Medium, Light.

Balancing cost, functionality, and performance

Several proprietary (OEM, Tier-1) specifications.

With common elements, but also with conflicts.

ISO/SAE 21434 – Automotive Cybersecurity Engineering

What is ISO / SAE 21434?

- Provides a framework for automotive security engineering
- Security-equivalent of ISO 26262 (Functional Safety)

Status: in development

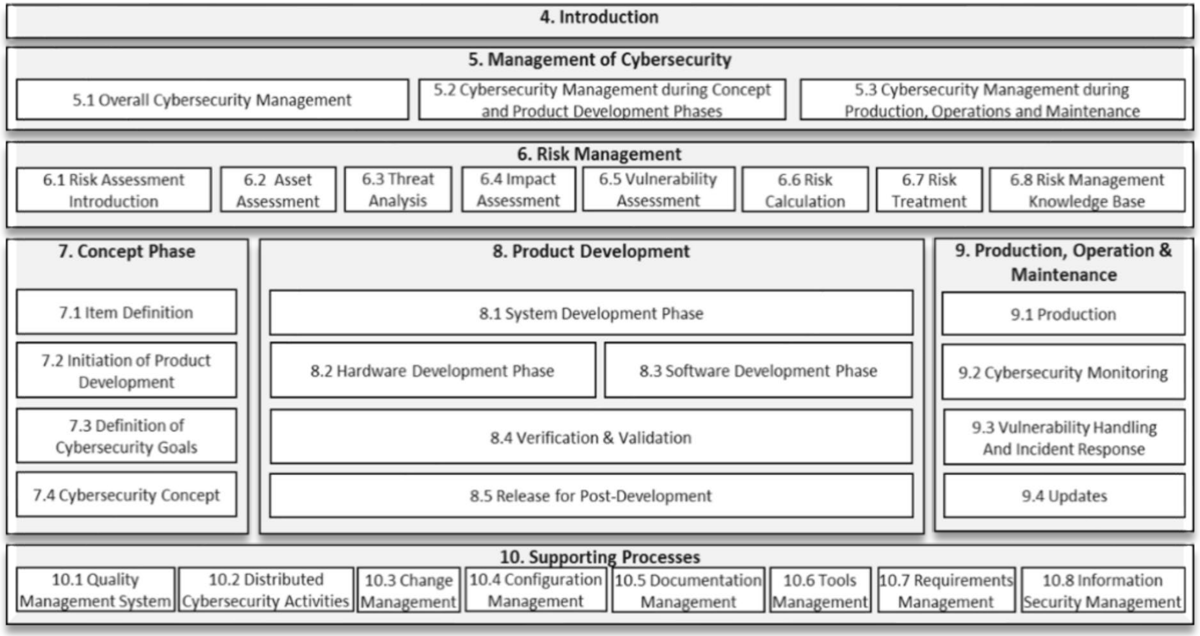
- Publication expected end of 2020

Compliance will likely become mandatory

- ISO/SAE 21434 is considered as a basis for compliance with the security requirements in the upcoming UNECE international whole vehicle type approval (IWVTA) scheme
- Automotive customers (OEMs, Tier-1s) are already asking suppliers if they intend to be compliant

NXP is targeting full compliance

- Several of the key elements are already in place



4. Introduction

5. Management of Cybersecurity
5.1 Overall Cybersecurity Management
5.2 Cybersecurity Management during Concept and Product Development Phases
5.3 Cybersecurity Management during Production, Operations and Maintenance

6. Risk Management
6.1 Risk Assessment Introduction
6.2 Asset Assessment
6.3 Threat Analysis
6.4 Impact Assessment
6.5 Vulnerability Assessment
6.6 Risk Calculation
6.7 Risk Treatment
6.8 Risk Management Knowledge Base

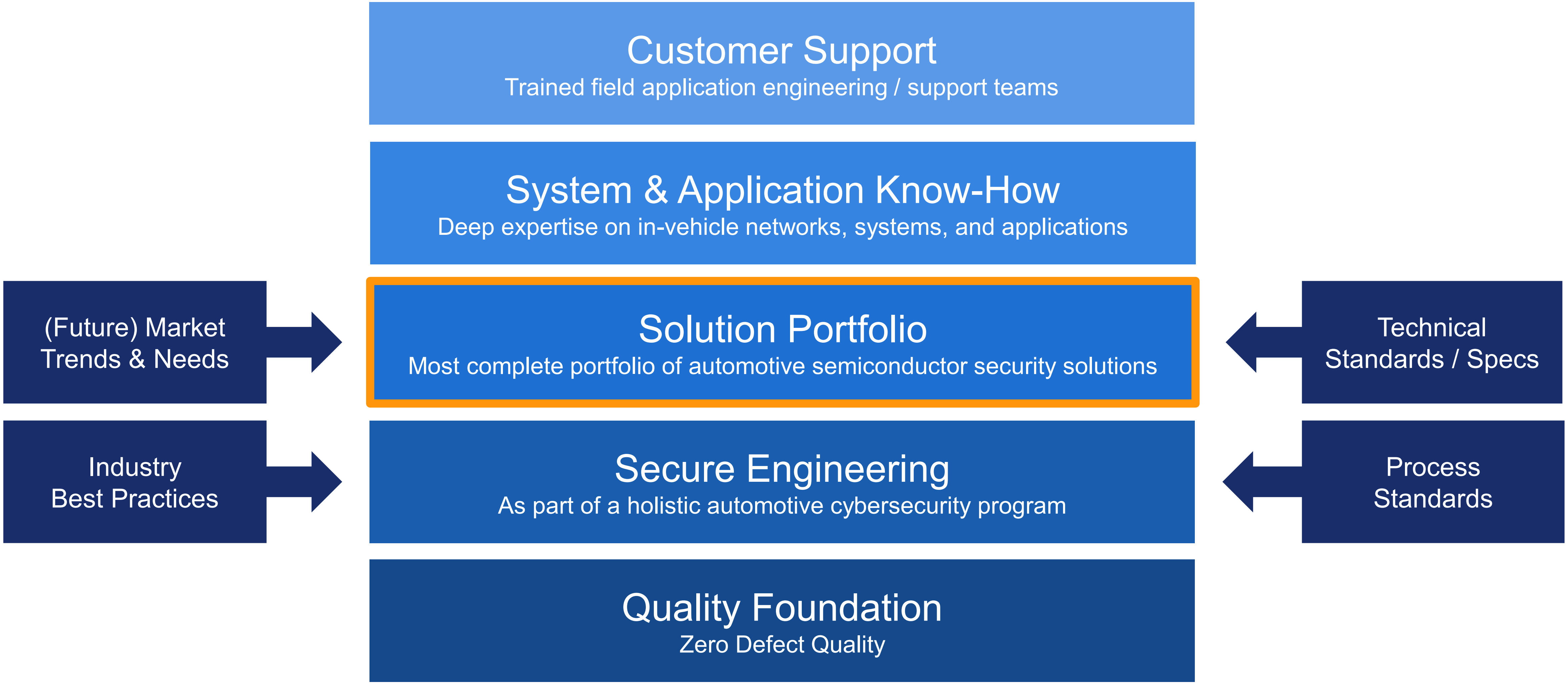
7. Concept Phase
7.1 Item Definition
7.2 Initiation of Product Development
7.3 Definition of Cybersecurity Goals
7.4 Cybersecurity Concept

8. Product Development
8.1 System Development Phase
8.2 Hardware Development Phase
8.3 Software Development Phase
8.4 Verification & Validation
8.5 Release for Post-Development

9. Production, Operation & Maintenance
9.1 Production
9.2 Cybersecurity Monitoring
9.3 Vulnerability Handling And Incident Response
9.4 Updates

10. Supporting Processes
10.1 Quality Management System
10.2 Distributed Cybersecurity Activities
10.3 Change Management
10.4 Configuration Management
10.5 Documentation Management
10.6 Tools Management
10.7 Requirements Management
10.8 Information Security Management

NXP's Approach to Automotive Security



Customer Support
Trained field application engineering / support teams

System & Application Know-How
Deep expertise on in-vehicle networks, systems, and applications

Solution Portfolio
Most complete portfolio of automotive semiconductor security solutions

Secure Engineering
As part of a holistic automotive cybersecurity program

Quality Foundation
Zero Defect Quality

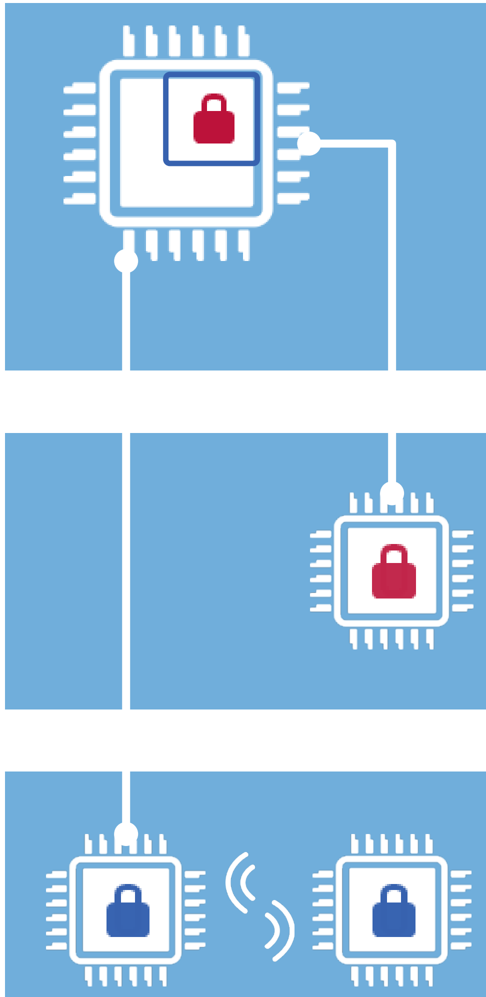
(Future) Market Trends & Needs

Industry Best Practices

Technical Standards / Specs

Process Standards

NXP’s 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

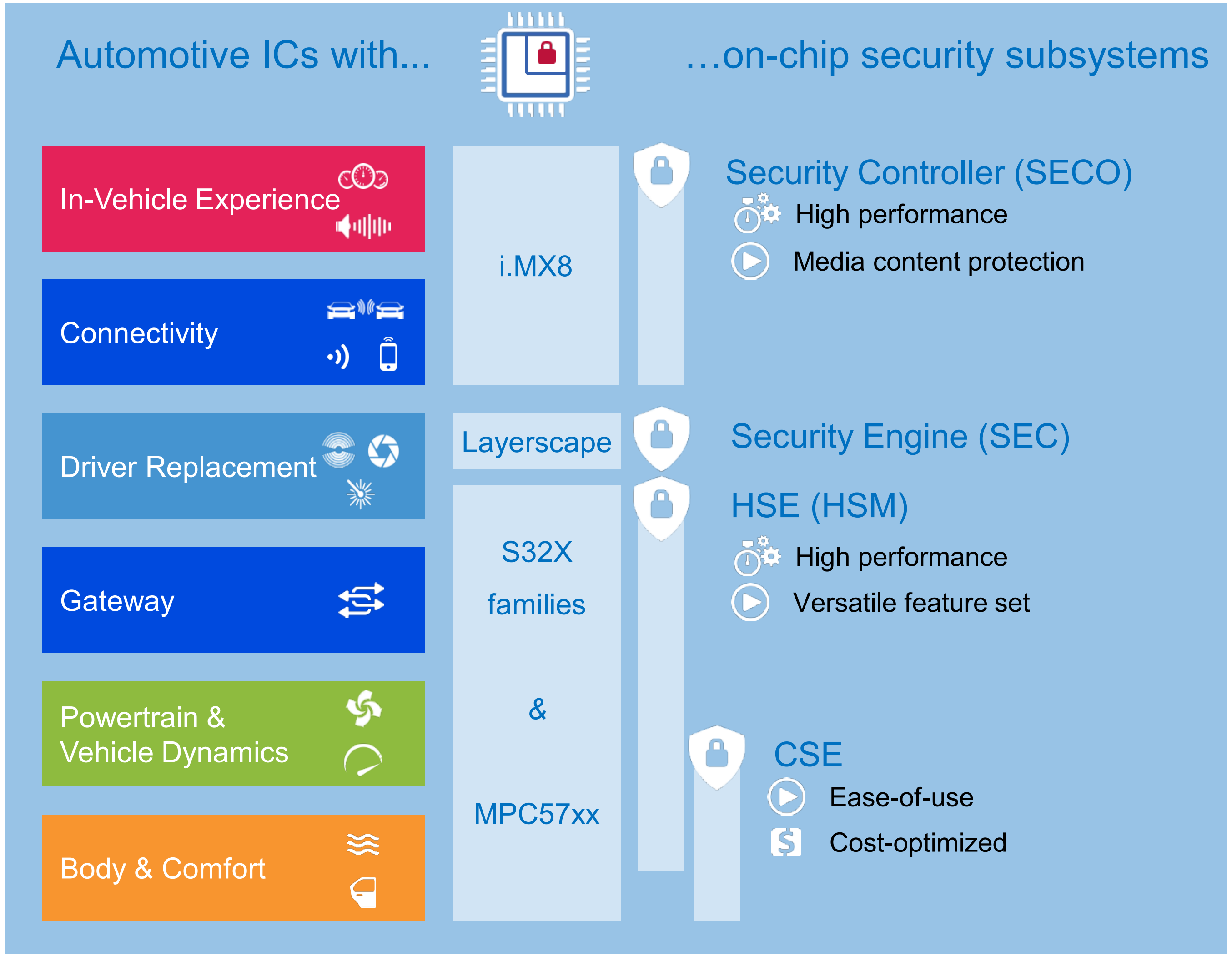
Security Companions

Security extension *for specific use*

Function-specific Secure ICs

Fit-for-purpose security support

NXP’s Automotive Security Solutions



Automotive ICs with... …on-chip security subsystems

In-Vehicle Experience

Connectivity

Driver Replacement

Gateway

Powertrain & Vehicle Dynamics

Body & Comfort

i.MX8

Layerscape

S32X families & MPC57xx

Security Controller (SECO)
- High performance
- Media content protection

Security Engine (SEC)

HSE (HSM)
- High performance
- Versatile feature set

CSE
- Ease-of-use
- Cost-optimized

Security companions

Secure Element (SE)

Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

Function-specific secure ICs

Secure CAN Transceiver (TJA115x)

For enhanced IDS & IPS

Secure Ethernet Switch (SJA1110)

Network frame analysis (L2/L3/L4)

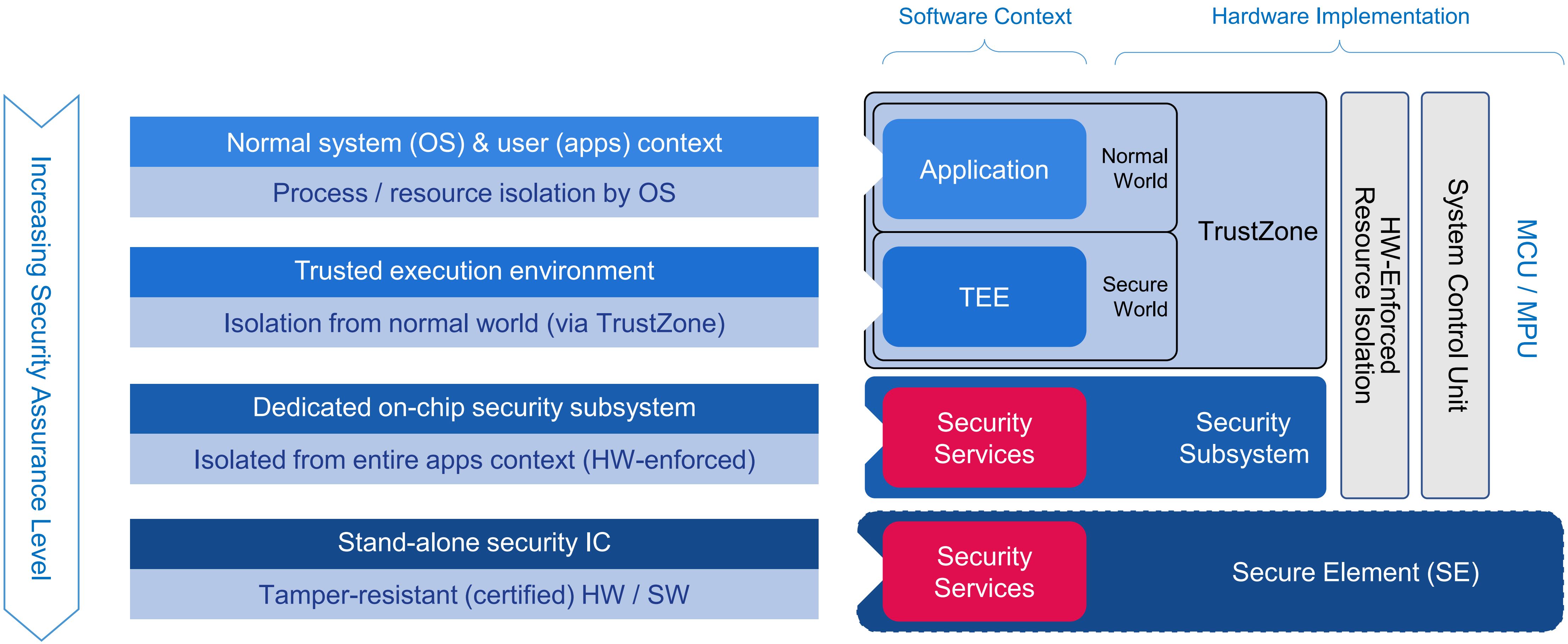
Secure Car Access ICs

For advanced RKE / PKE solutions

V2X DSRC Baseband (SAF5x00)

Ultra-fast ECDSA verifications

Secure Execution: In-Depth Approach with NXP Solutions



Increasing Security Assurance Level

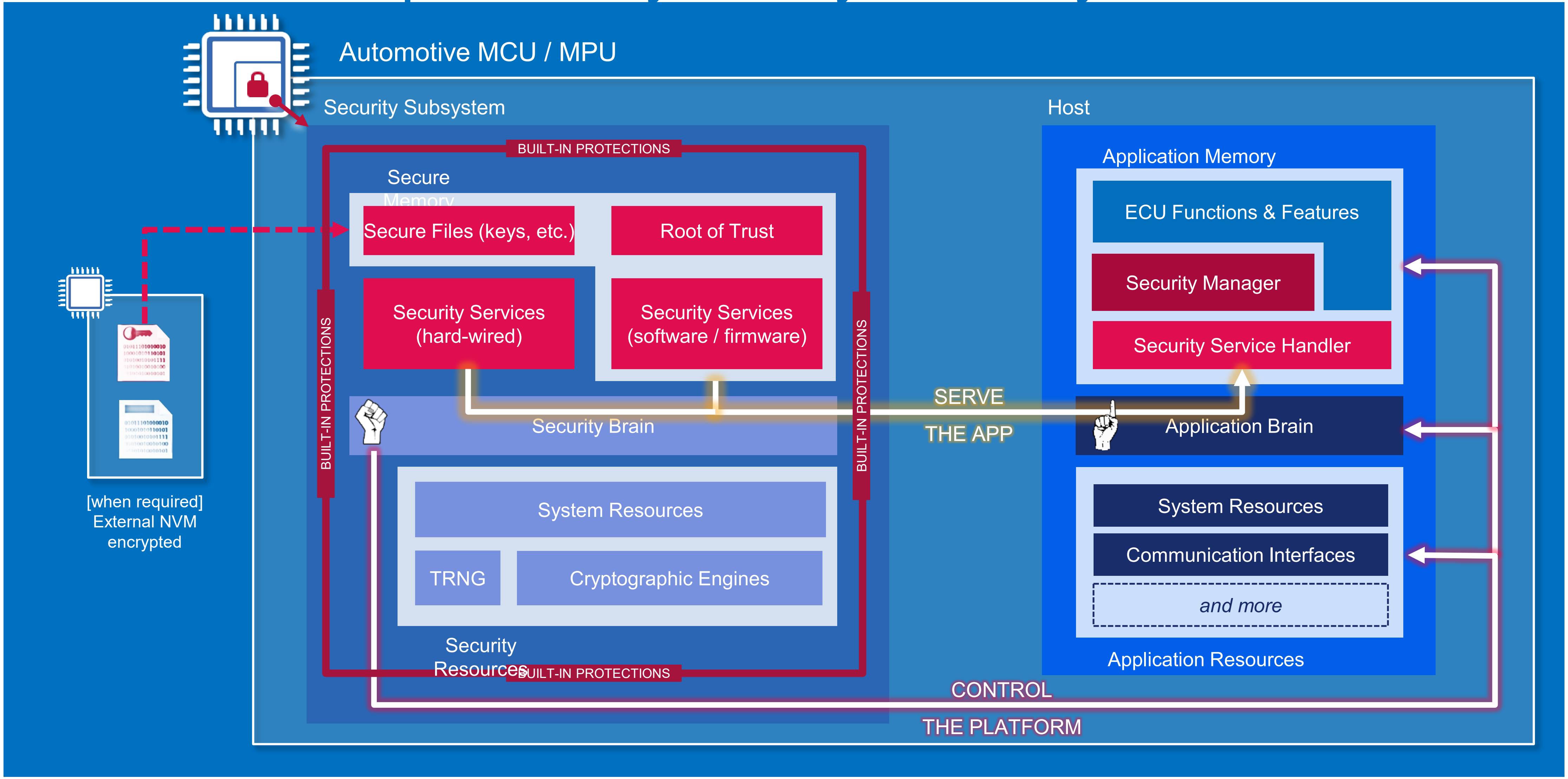
Normal system (OS) & user (apps) context
Process / resource isolation by OS

Trusted execution environment
Isolation from normal world (via TrustZone)

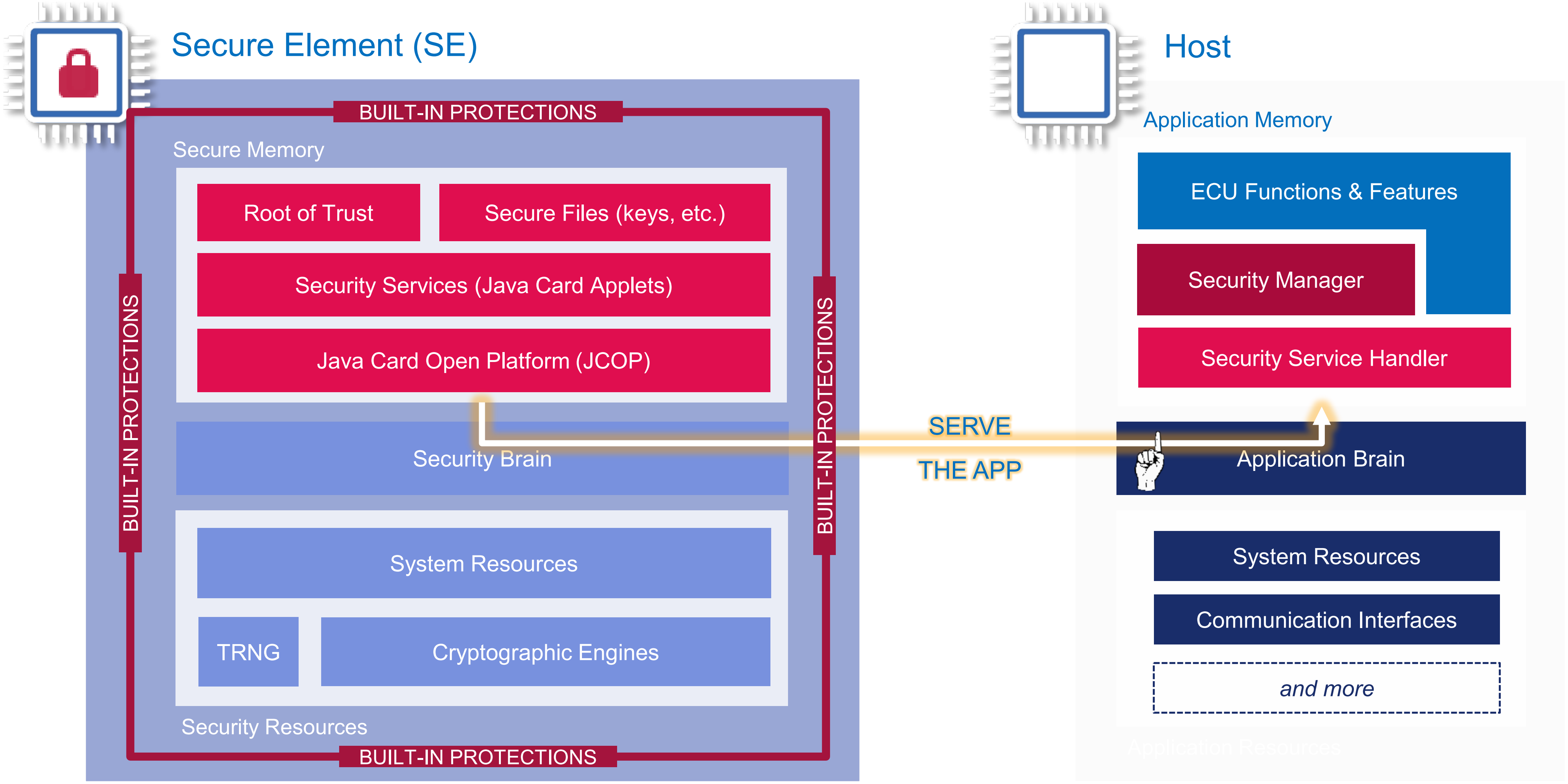
Dedicated on-chip security subsystem
Isolated from entire apps context (HW-enforced)

Stand-alone security IC
Tamper-resistant (certified) HW / SW

NXP’s On-Chip Security Subsystem: System Overview



NXP’s Secure Element: System Overview



Secure Element (SE)

BUILT-IN PROTECTIONS

Secure Memory

Root of Trust

Secure Files (keys, etc.)

Security Services (Java Card Applets)

Java Card Open Platform (JCOP)

Security Brain

System Resources

TRNG

Cryptographic Engines

Security Resources

Host

Application Memory

ECU Functions & Features

Security Manager

Security Service Handler

Application Brain

System Resources

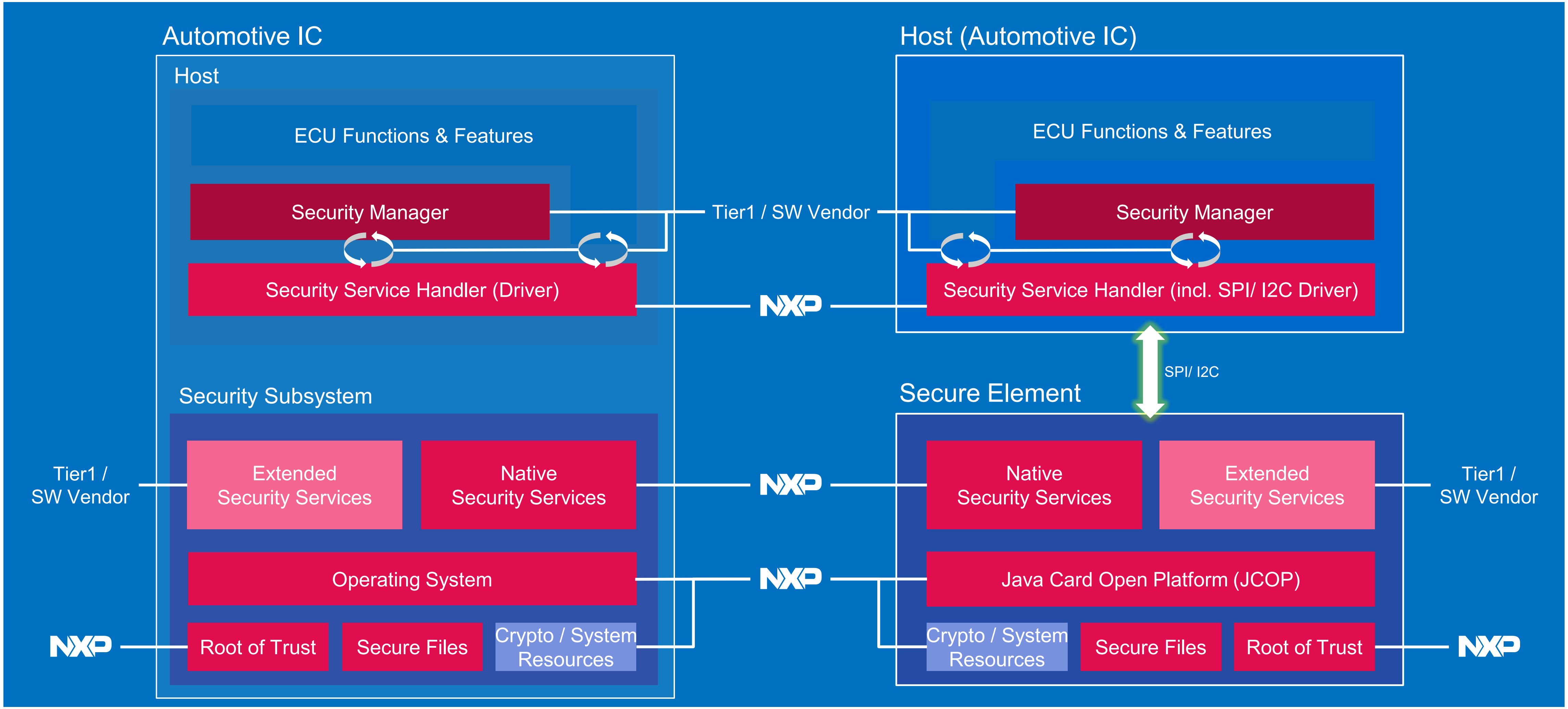
Communication Interfaces

and more

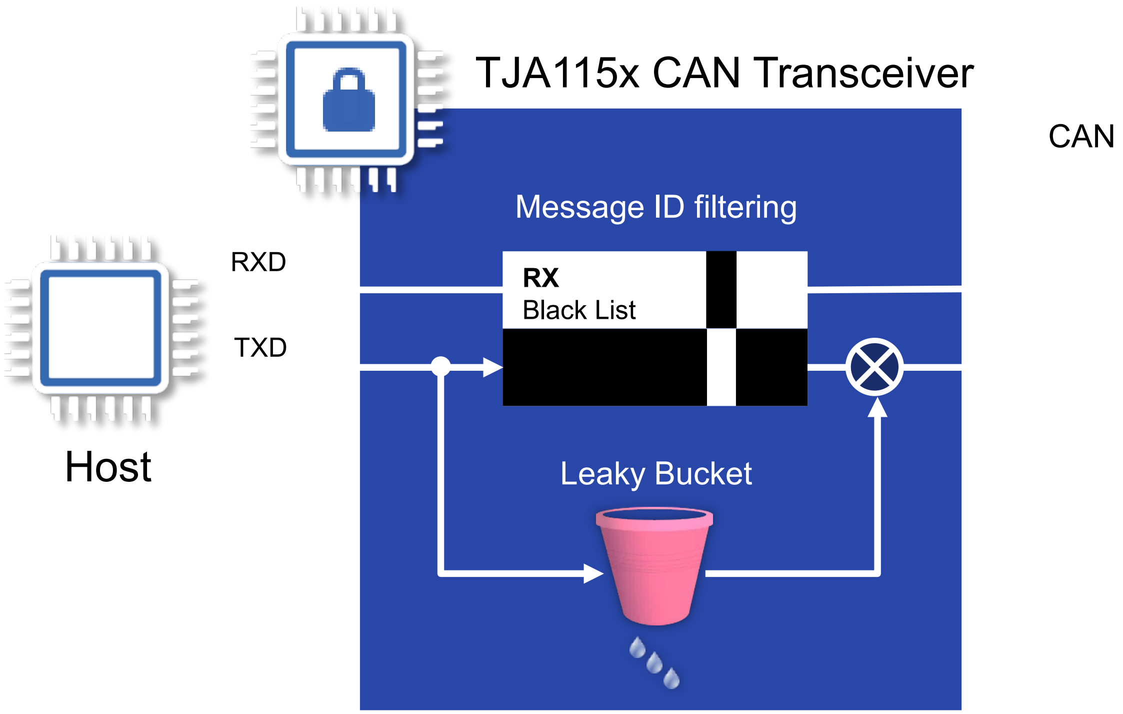
Application Resources

SERVE THE APP

Software Components in Play

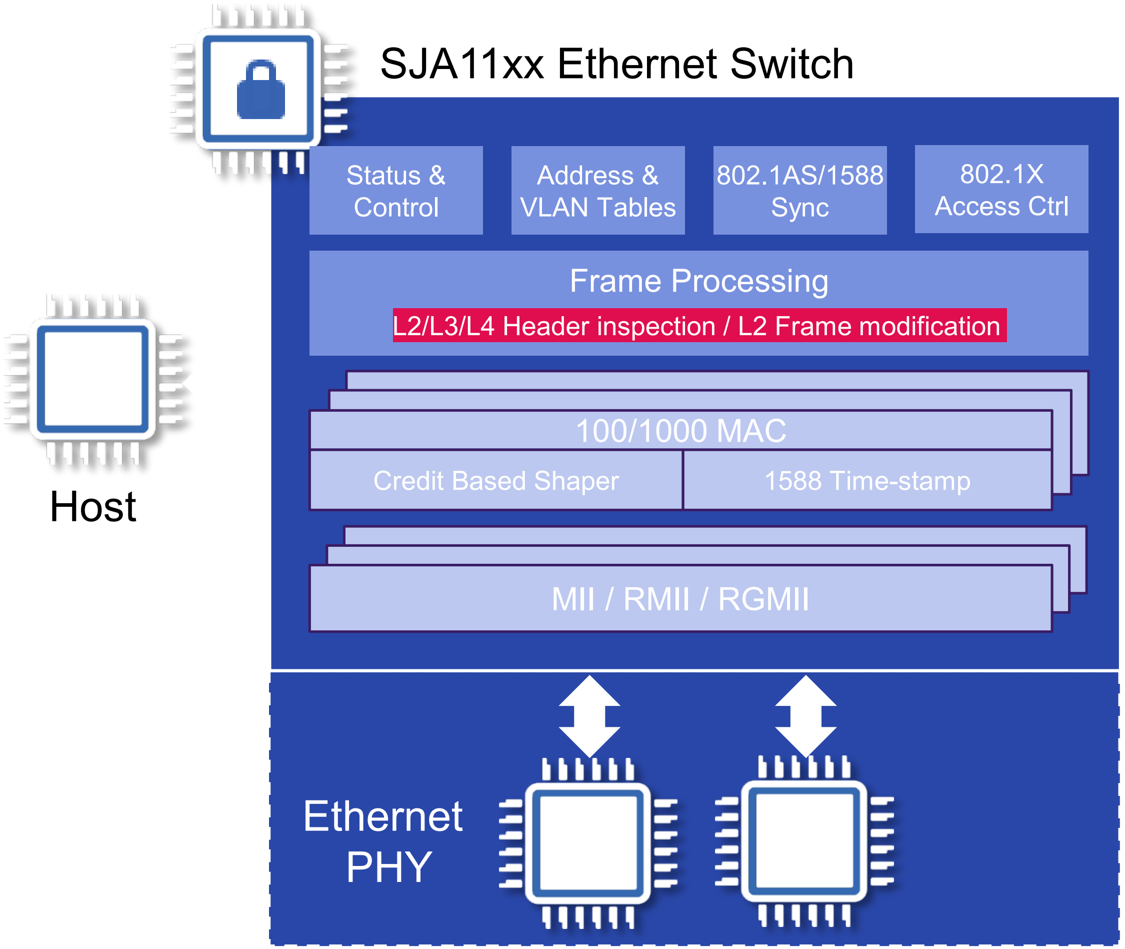


NXP’s Secure CAN Transceiver



- Intrusion detection & prevention (IDS / IPS)
  - On-the-fly CAN ID filtering (TX) and bus-guarding (RX) based on user configurable white & black lists
  - Configuration based on ID & masking
- Flooding prevention (DoS)
  - Threshold on message transmission: leaky bucket strategy weighted on frame size
  - “1:1” replacement to any CAN transceiver
- Configurable via the CAN bus
  - In-field reconfiguration possible
  - Automotive qualified (AEC-Q100)
  - Operating T° -40°C to 125°C

NXP's Secure Ethernet Switch



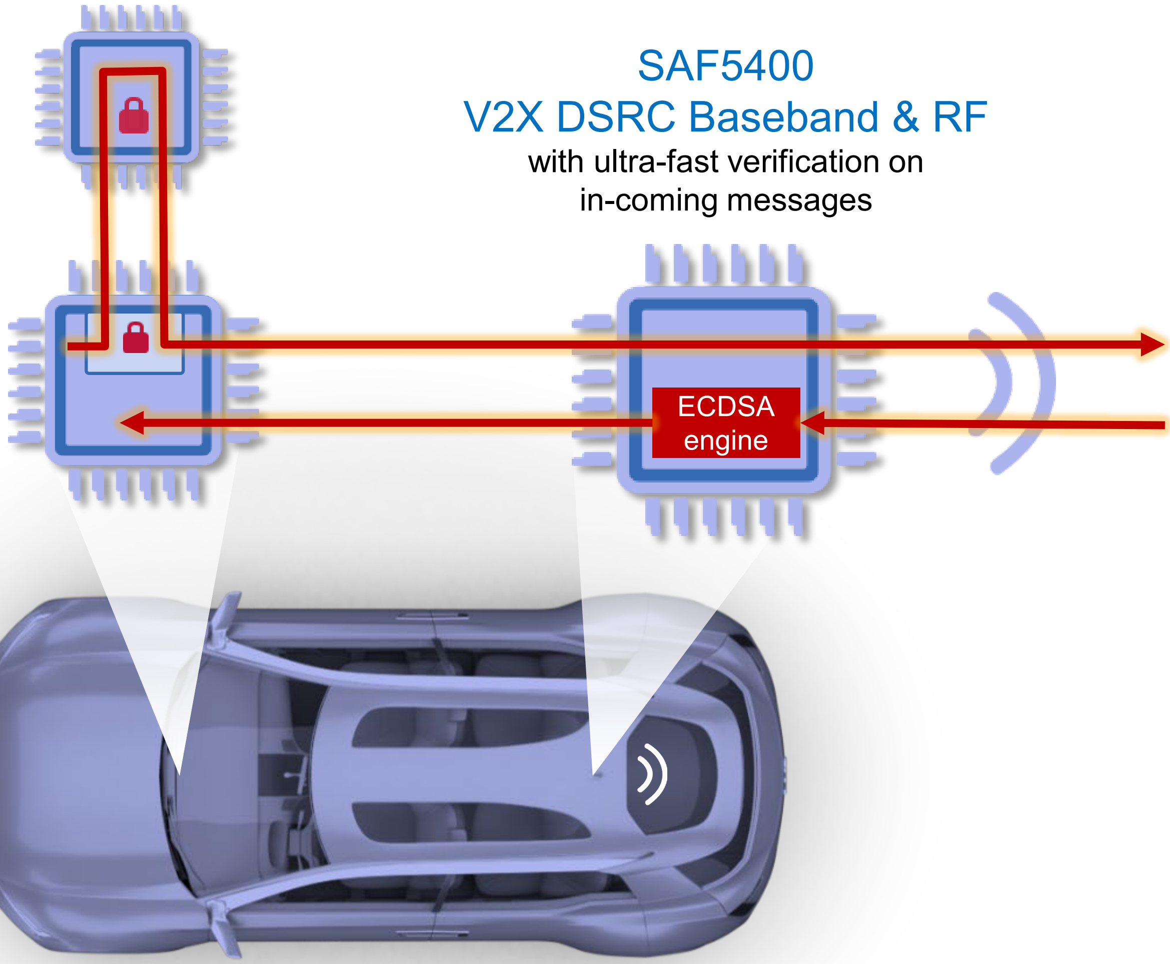
- Authentication
  - Port-based authentication (IEEE 802.1X)
  - Port-reachability HW enforcement & limitation
  - Address-learning with disable option
  - One-time MAC-address learning
- Flooding prevention (DoS)
  - Data-rate limitation: port-based / priority-based / stream-based / broadcast
- Traffic isolation
  - Up to 4096 VLAN / priority dynamic update at run-time; double tagging
- TT & TSN Features (SJA1105TEL only)
  - 802.1Qbv time-aware traffic, (pre-std) IEEE 802.1Qci

NXP's V2X Reference Security Architecture

SXF1800
Secure Element
for highly secure authentication
of out-going messages

i.MX / S32x
Applications Processors
running the V2X stack

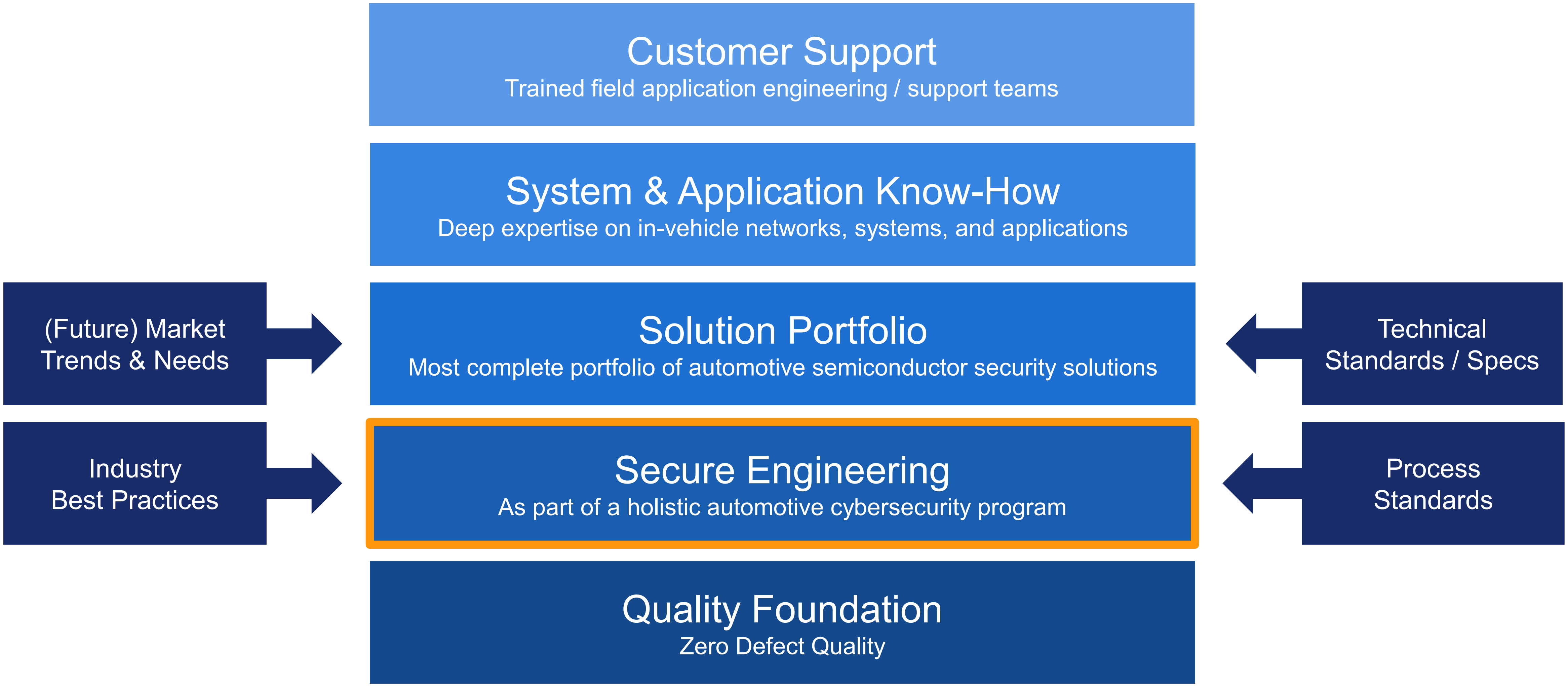
SAF5400
V2X DSRC Baseband & RF
with ultra-fast verification on
in-coming messages



Highly secured
out-going messages
(signing key in secure element)

Ultra-fast verification
on in-coming messages
(> 1000 msg/s)

NXP’s Approach to Automotive Security



Customer Support
Trained field application engineering / support teams

System & Application Know-How
Deep expertise on in-vehicle networks, systems, and applications

Solution Portfolio
Most complete portfolio of automotive semiconductor security solutions

Secure Engineering
As part of a holistic automotive cybersecurity program

Quality Foundation
Zero Defect Quality

(Future) Market Trends & Needs

Industry Best Practices

Technical Standards / Specs

Process Standards

NXP’s Automotive Cybersecurity Program

Holistic approach to product security…

- Broad portfolio of security solutions
- Secure product engineering process (SDLC)
- Internal / external security evaluation (VA)
- Product security incident response team (PSIRT)
- Security-aware organization (incl. training)
- Threat intelligence feed

… and IT cyber security

- Security Operations Center (SOC)
- Information security policies
- Computer security incident management and response (CSIRT)
- Site security (ISO 27001 cert.)

In collaboration with third parties

- Researchers, industry partners, Auto-ISAC, CERTs, …

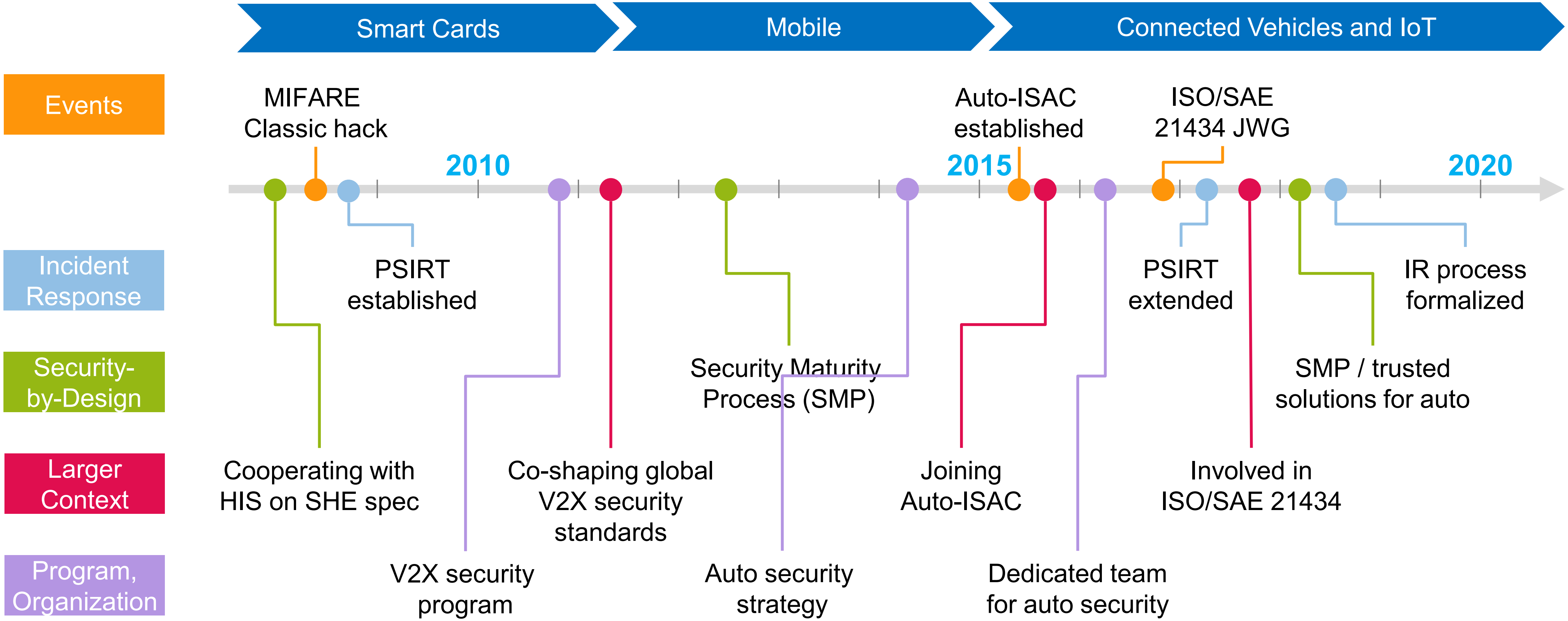
TECHNOLOGY

PROCESS

PEOPLE

Security Culture and Organization – Matured Over Time

Some of the Key Milestones



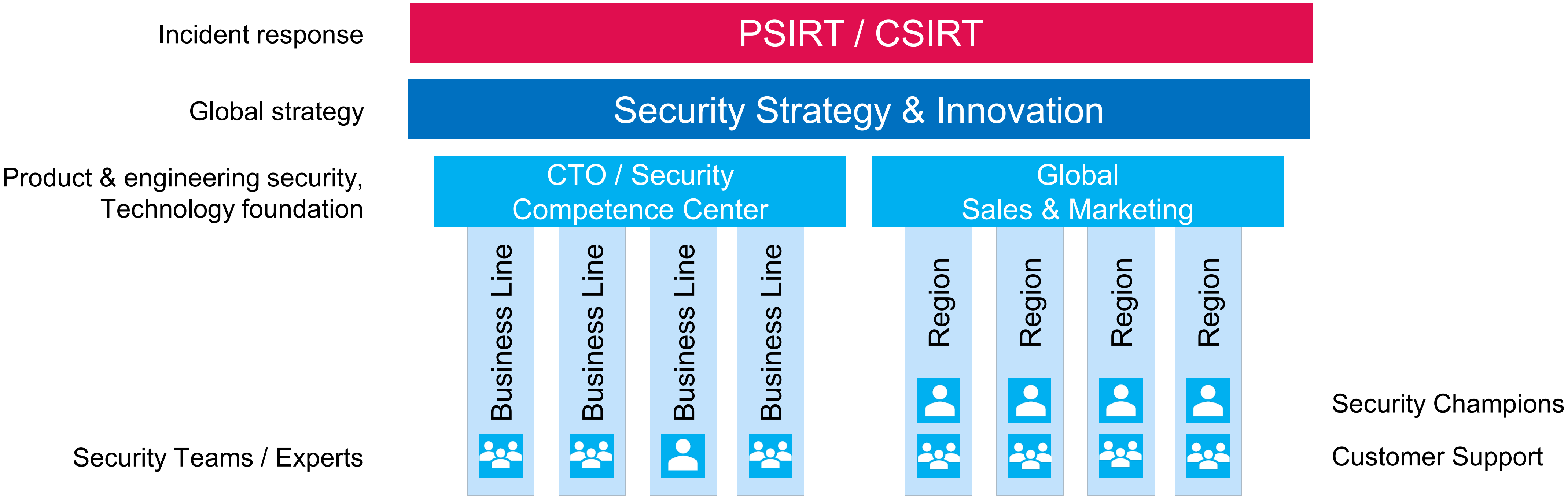
NXP’s Holistic Approach – Solutions and Organization

		Prevent access	**Detect** attacks	**Reduce** impact	**Fix** vulnerabilities
Technology	Secure Interfaces	M2M Authentication & Firewalling	Intrusion Detection Systems (IDS)		Secure Updates
	Secure Domain Isolation	Firewalling (context-aware message filtering)		Separated Functional Domains	
	Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
	Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	
People & Processes	Secure Engineering	SDLC incl. Security Reviews & Testing, …	Threat Monitoring, Intelligence Sharing, …	Incident Management / Response	
		Security-Aware Organization, Policies, Governance			

NXP’s Security Organization

Our approach

- Dedicated expert teams – security as core competence
- Collaboration across organizations / teams / backgrounds / competences / markets
- Have expertise close to our customers



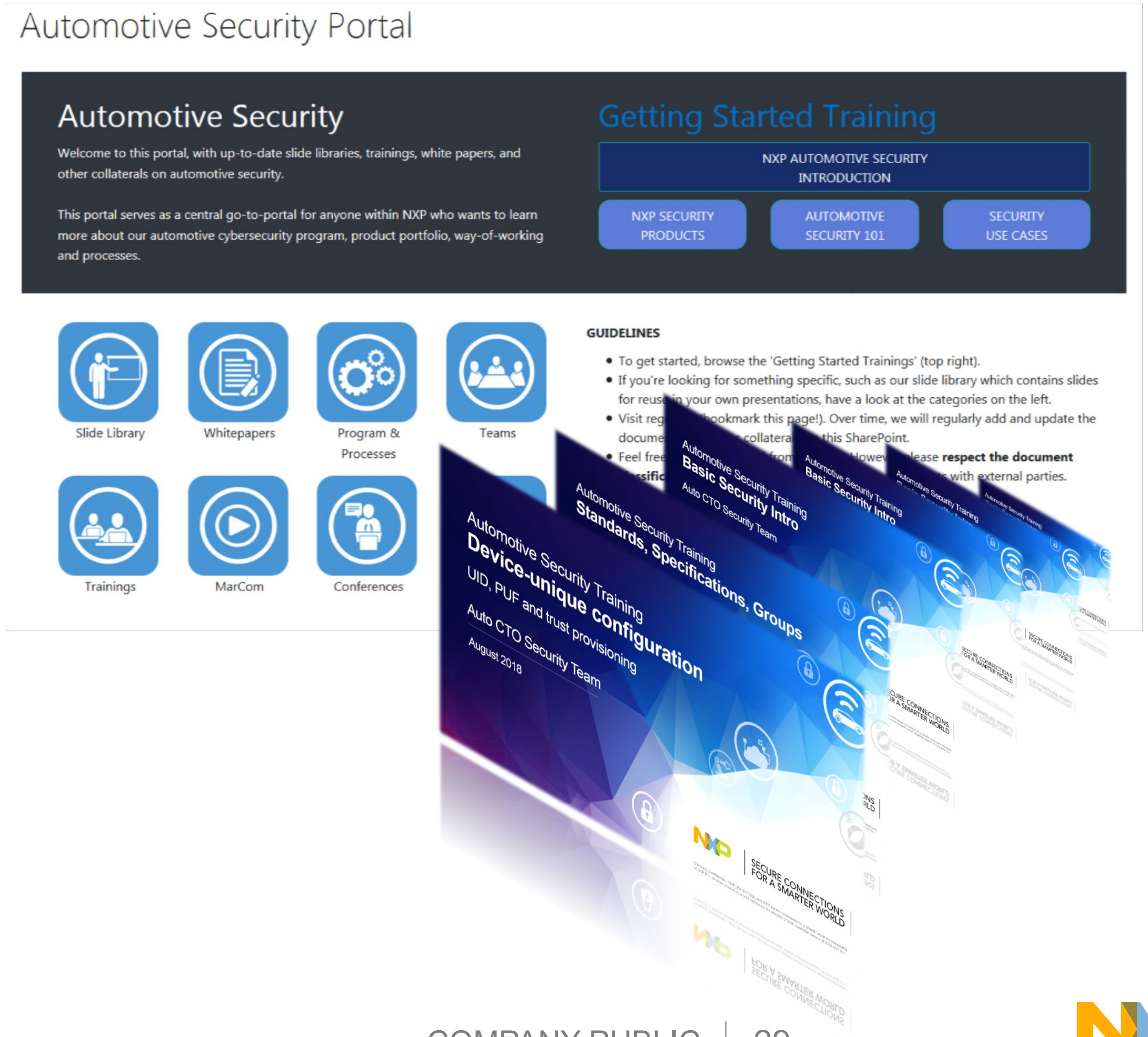
Training and Awareness – What Do We Do?

Training and Knowledge Transfer

- Regular basic security trainings
- Expert trainings on dedicated topics – internally and through external partners

Awareness

- Regular bulletins and campaigns to increase awareness
- Internal and external information sharing, through:
  - Regular internal meetings and online portal
  - Workshops with partners
  - Bi-directional sharing with Auto-ISAC, CERTs, …



Automotive Security Portal

Automotive Security

Welcome to this portal, with up-to-date slide libraries, trainings, white papers, and other collaterals on automotive security.

This portal serves as a central go-to-portal for anyone within NXP who wants to learn more about our automotive cybersecurity program, product portfolio, way-of-working and processes.

Getting Started Training

GUIDELINES

- To get started, browse the 'Getting Started Trainings' (top right).
- If you're looking for something specific, such as our slide library which contains slides for reuse in your own presentations, have a look at the categories on the left.
- Visit reg bookmark this page!). Over time, we will regularly add and update the docume collatera this SharePoint.
- Feel free from Howev please **respect the document ssific** with external parties.

NXP AUTOMOTIVE SECURITY INTRODUCTION
NXP SECURITY PRODUCTS
AUTOMOTIVE SECURITY 101
SECURITY USE CASES
Slide Library
Whitepapers
Program & Processes
Teams
Trainings
MarCom
Conferences
Automotive Security Training
Device-unique configuration
UID, PUF and trust provisioning
Auto CTO Security Team
August 2018
Automotive Security Training
Standards, Specifications, Groups
Automotive Security Training
Basic Security Intro
Auto CTO Security Team
SECURE CONNECTIONS FOR A SMARTER WORLD

Product Development / SDLC – Security Maturity Process

Seven OE suppliers join as new members of Auto-ISAC

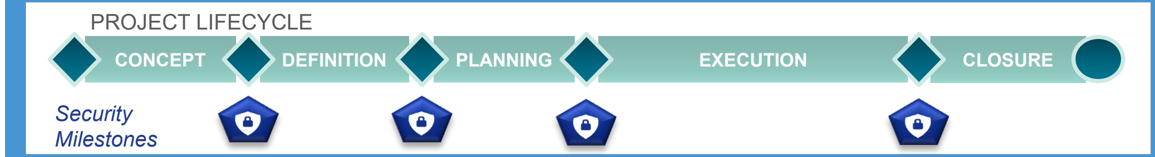
By Telematics News Published: 24 February 2017
Posted in: Cybersecurity, North America, Partnerships, Security

AUTO-ISAC
Automotive Information Sharing and Analysis Center

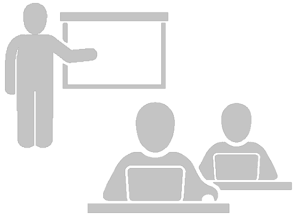
The Automotive Information Sharing and Analysis Center (Auto-ISAC) welcomes Bosch, Cooper Standard, Honeywell, Hyundai Mobis, Lear Corporation, LG Electronics and NXP Semiconductors as original equipment supplier members. The inclusion of these companies exemplifies Auto-ISAC's continued efforts to promote collaboration between Tier 1 suppliers and automobile manufacturers around vehicle cybersecurity.

Threat intelligence,
best practices, …

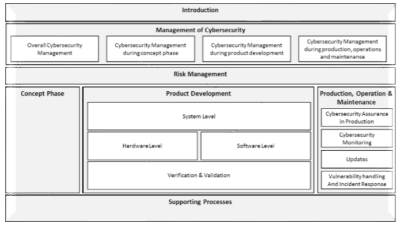
Lessons learned
(e.g. from IR)



Training
and awareness



Standards
(ISO/SAE 21434, SAE J3061, …)



Introduction

Management of Cybersecurity

Overall Cybersecurity Management

Cybersecurity Management during concept phase

Cybersecurity Management during product development

Cybersecurity Management during production, operations and maintenance

Risk Management

Concept Phase

Product Development

System Level

Hardware Level

Software Level

Verification & Validation

Production, Operation & Maintenance

Cybersecurity Assurance in Production

Cybersecurity Monitoring

Updates

Vulnerability handling And Incident Response

Supporting Processes

Monitoring security implementation at each gate

Independent and un-biased reviews – “4 eyes” principle

Process implementation can be adjusted per project

+ Trusted solutions:
Framework and support to guide engineering teams

Product Security Incident Response Team (PSIRT)

Product Security IR Process and Team

Global across products / markets / regions

Established in 2008 after the MIFARE Classic hack

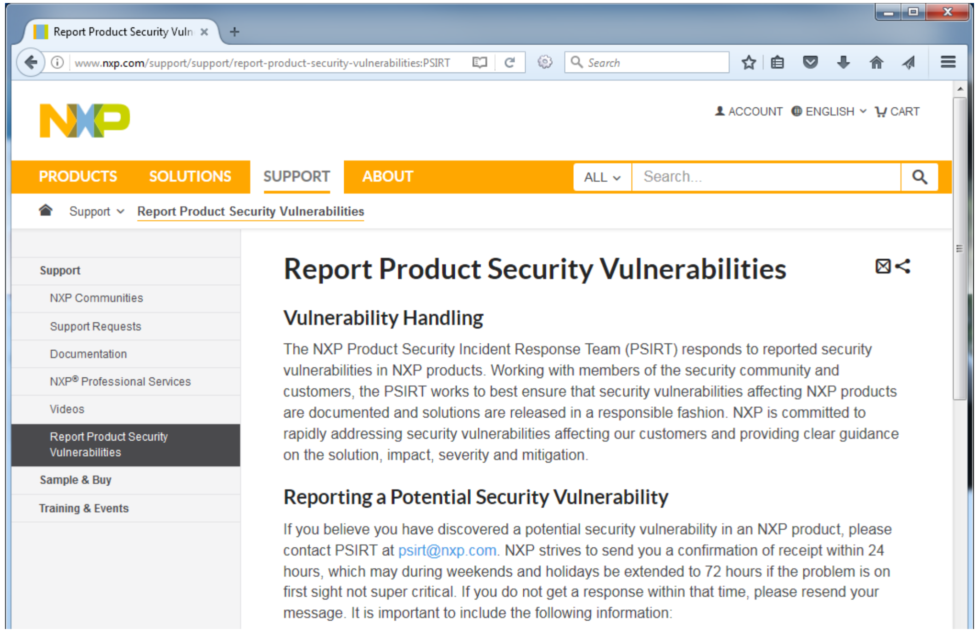
Committed to Responsible Disclosure

In alignment with the security community

With our customers, partners, Auto-ISAC, CERTs

Continuous Improvement

E.g. evaluate and benchmark against Auto-ISAC's best practice guide for incidence response



Report Product Security Vuln
www.nxp.com/support/support/report-product-security-vulnerabilities:PSIRT
Search
ACCOUNT
ENGLISH
CART
PRODUCTS
SOLUTIONS
SUPPORT
ABOUT
ALL
Search...
Support
Report Product Security Vulnerabilities
Support
NXP Communities
Support Requests
Documentation
NXP® Professional Services
Videos
Report Product Security Vulnerabilities
Sample & Buy
Training & Events

Report Product Security Vulnerabilities

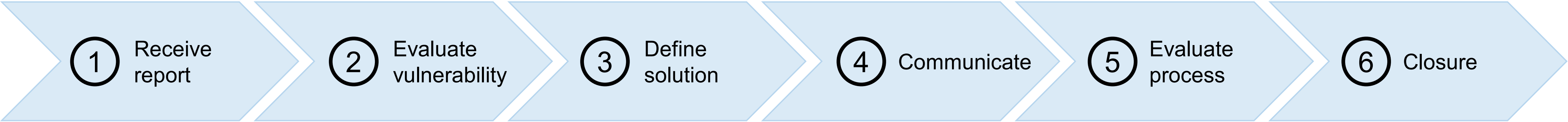
Vulnerability Handling

The NXP Product Security Incident Response Team (PSIRT) responds to reported security vulnerabilities in NXP products. Working with members of the security community and customers, the PSIRT works to best ensure that security vulnerabilities affecting NXP products are documented and solutions are released in a responsible fashion. NXP is committed to rapidly addressing security vulnerabilities affecting our customers and providing clear guidance on the solution, impact, severity and mitigation.

Reporting a Potential Security Vulnerability

If you believe you have discovered a potential security vulnerability in an NXP product, please contact PSIRT at psirt@nxp.com. NXP strives to send you a confirmation of receipt within 24 hours, which may during weekends and holidays be extended to 72 hours if the problem is on first sight not super critical. If you do not get a response within that time, please resend your message. It is important to include the following information:

Web site: www.nxp.com/psirt Contact: psirt@nxp.com


1 Receive report

2 Evaluate vulnerability

3 Define solution

4 Communicate

5 Evaluate process

6 Closure

ISO/SAE 21434 – Automotive Cybersecurity Engineering

What is ISO / SAE 21434?

- Provides a framework for automotive security engineering
- Security-equivalent of ISO 26262 (Functional Safety)

Status: in development

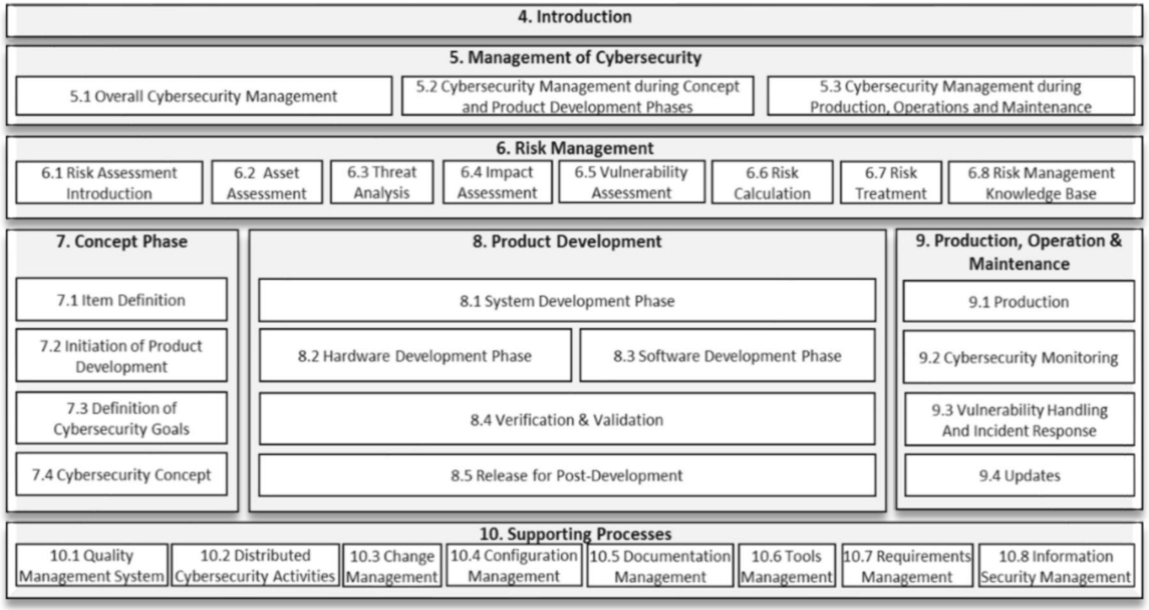
- Publication expected end of 2020

Compliance will likely become mandatory

- ISO/SAE 21434 is considered as a basis for compliance with the security requirements in the upcoming UNECE international whole vehicle type approval (IWVTA) scheme
- Automotive customers (OEMs, Tier-1s) are already asking suppliers if they intend to be compliant

NXP is targeting full compliance

- Several of the key elements are already in place



4. Introduction

5. Management of Cybersecurity
5.1 Overall Cybersecurity Management
5.2 Cybersecurity Management during Concept and Product Development Phases
5.3 Cybersecurity Management during Production, Operations and Maintenance

6. Risk Management
6.1 Risk Assessment Introduction
6.2 Asset Assessment
6.3 Threat Analysis
6.4 Impact Assessment
6.5 Vulnerability Assessment
6.6 Risk Calculation
6.7 Risk Treatment
6.8 Risk Management Knowledge Base

7. Concept Phase
7.1 Item Definition
7.2 Initiation of Product Development
7.3 Definition of Cybersecurity Goals
7.4 Cybersecurity Concept

8. Product Development
8.1 System Development Phase
8.2 Hardware Development Phase
8.3 Software Development Phase
8.4 Verification & Validation
8.5 Release for Post-Development

9. Production, Operation & Maintenance
9.1 Production
9.2 Cybersecurity Monitoring
9.3 Vulnerability Handling And Incident Response
9.4 Updates

10. Supporting Processes
10.1 Quality Management System
10.2 Distributed Cybersecurity Activities
10.3 Change Management
10.4 Configuration Management
10.5 Documentation Management
10.6 Tools Management
10.7 Requirements Management
10.8 Information Security Management

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP and the NXP logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2019 NXP B.V.