VEHICLE PLATFORM 변화에 따른 AUTOMOTIVE SECURITY 대응방안

Automotive Processor Marketing Director
Sangman Chung

NOVEMBER 2022

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

NXP SEMICONDUCTORS

Key Facts from Automotive Perspective

Headquarters in
The Netherlands
29,000 employees

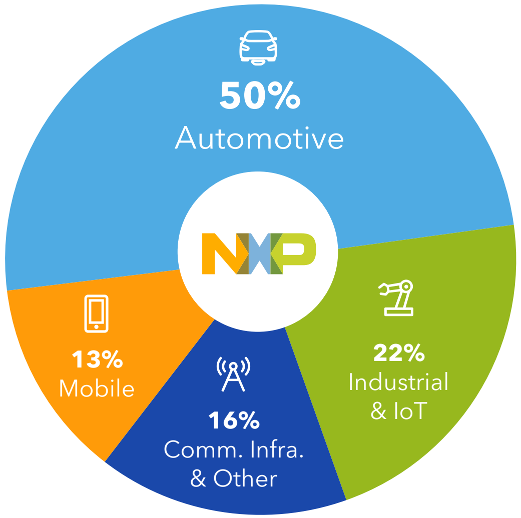
11,000 engineers;
9,000 patent families

$11.1B 2021 Revenue

Growth YoY :
+28% NXP total;
+44% Automotive
2021 growth vs. 2019:
+25% NXP; +30% Automotive

Capacity committed for expected growth to ~$15B in 2024 (+8-12% p.a.)

2021 Revenue
by end-market exposure



Automotive Technology Leadership:

Radar systems

Domain and zonal processors

Electrification systems
(BMS & eMotor Control)

General Purpose MCU

Advanced Analog

Audio infotainment

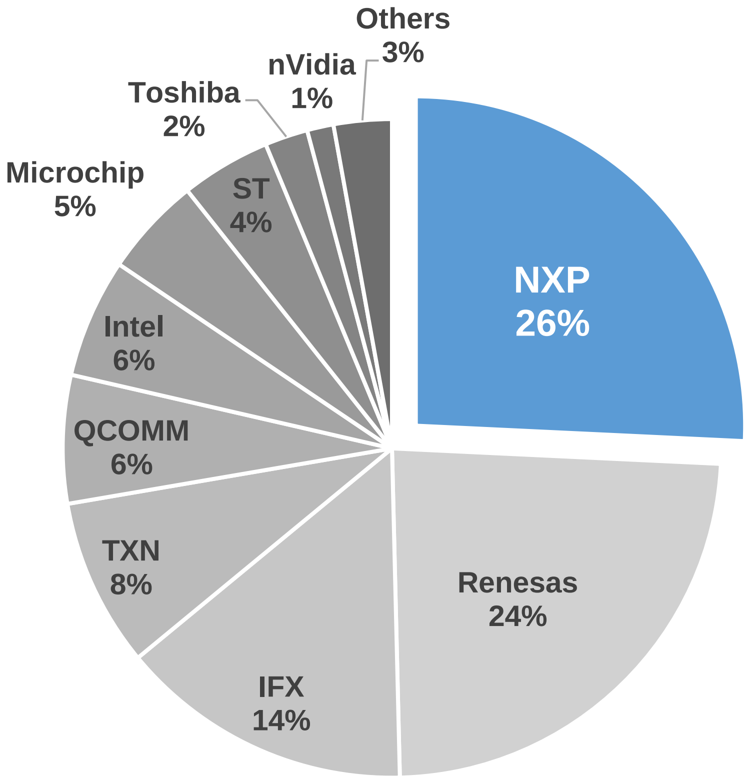
In-vehicle networking

Secure access solutions

Network-to-cloud; Secure OTA

NXP: THE LEADER IN AUTOMOTIVE PROCESSORS ENABLING THE SOFTWARE DEFINED REVOLUTION

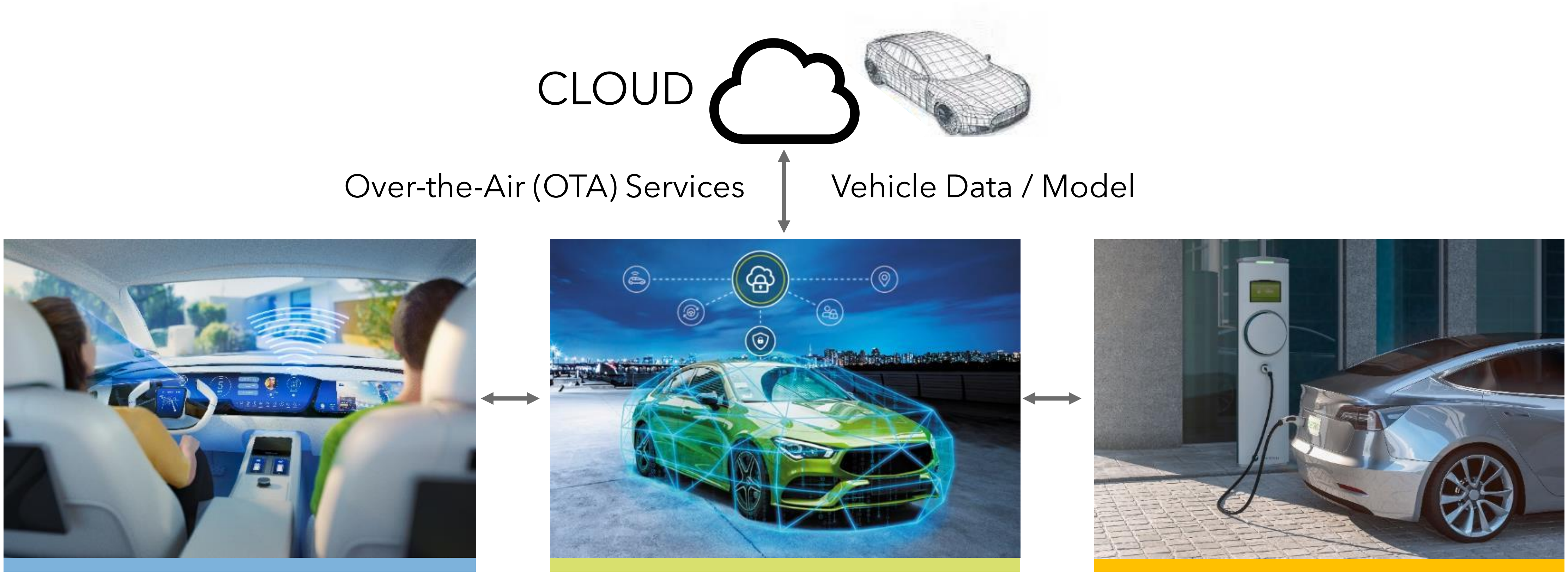
2021 AUTO PROCESSOR MARKET SHARE



Source: **Strategy Analytics** – March 2022

VEHICLE COMPUTE AND ARCHITECTURAL TRENDS

THREE FUTURE CAR MISSIONS → ONE CLEAR PATH TOWARDS SOFTWARE-DEFINED CAR



CLOUD

Over-the-Air (OTA) Services

Vehicle Data / Model

Autonomous
New sensing, thinking

Service Oriented
New EE architecture

Electric
New energy mgmt

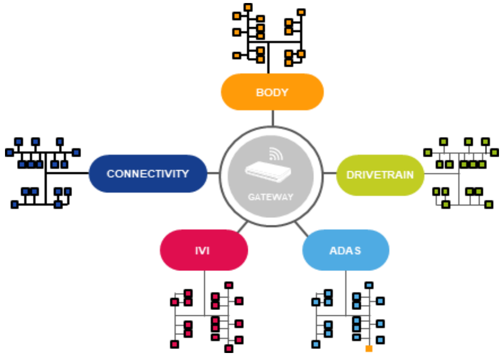
Making cars fully service-oriented requires a deep EE transformation

But this is the necessary step towards SDV

EVOLUTION TOWARDS FULL ZONAL PLATFORMS → THE FOUNDATION FOR SDV

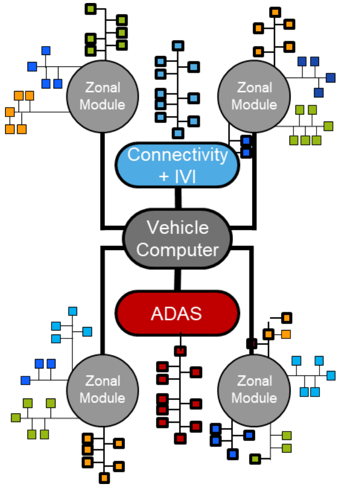
2022
Domain Platforms

Logical Domains



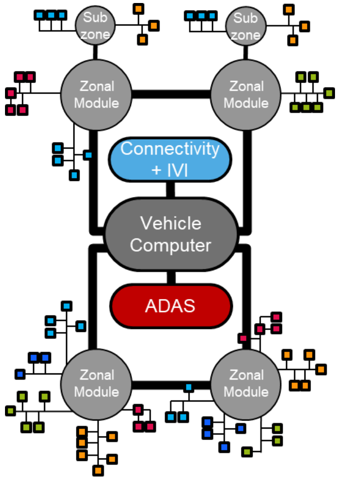
2025+
Hybrid Zonal Platforms

Body Domain Zone Clustering



2030+
Full Zonal Platforms

Multi-domain Zone Clustering



Simplify HW
Create central
service area

High ECU aggregation
All functions
are services

TWO PARALLEL ARCHITECTURAL CHANGES

1

Logical transformation:
Scalable and centralized software development

- First step toward software-defined vehicle
- More isolation for improved security
- Centralized over-the-air (OTA) update for software upgrades

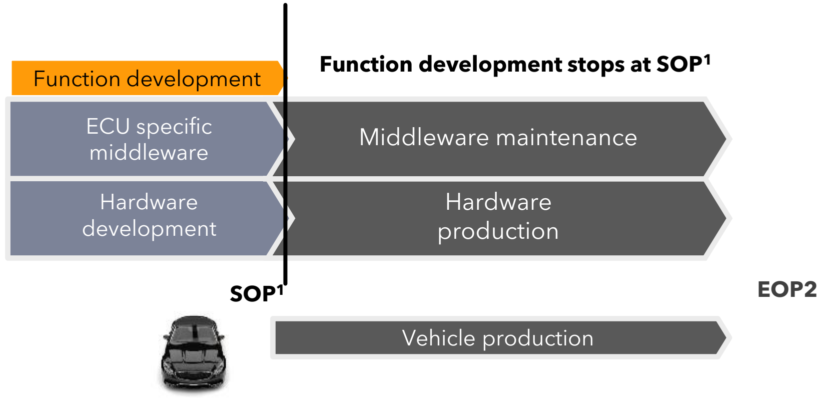
2

Physical transformation:
Zonal aggregation and ECU clustering

- Dramatically reduced material and manufacturing cost
- Eases EE upgrades and scalability
- Creates a central IP-based area for SOA

SDV REPRESENTS CONTINUED INVESTMENT WITH A LONG-TERM SILICON PLATFORM

Vehicle based on legacy EE architecture



Function development

Function development stops at SOP[1]

ECU specific middleware

Middleware maintenance

Hardware development

Hardware production

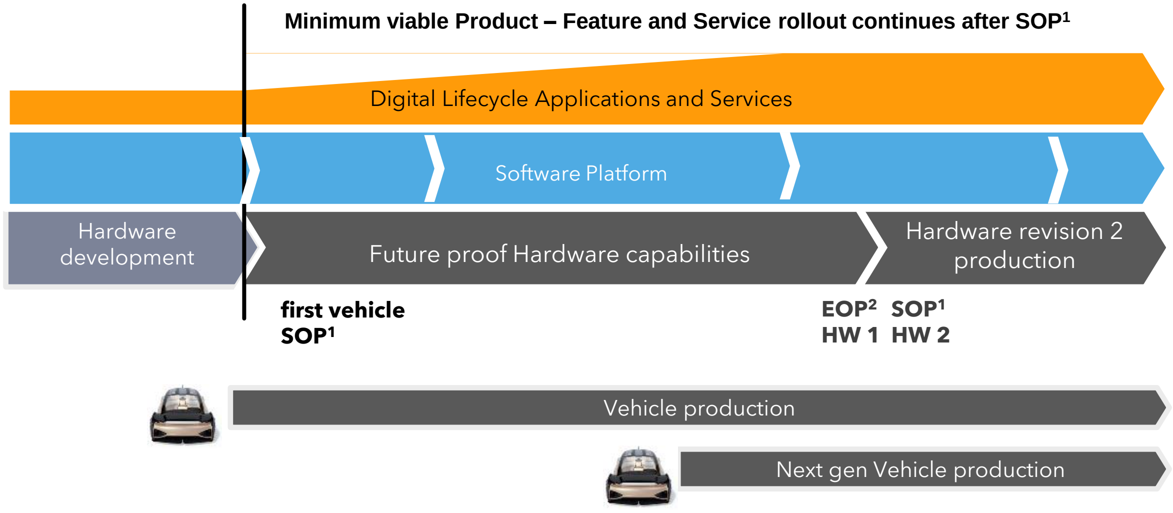
SOP[1]

EOP2

Vehicle production

[1] SOP: Start of production, [2] EOP: End of production,

Vehicles based on SDV platform



Minimum viable Product – Feature and Service rollout continues after SOP[1]

Digital Lifecycle Applications and Services

Software Platform

Hardware development

Future proof Hardware capabilities

Hardware revision 2 production

first vehicle SOP[1]

EOP[2] HW 1

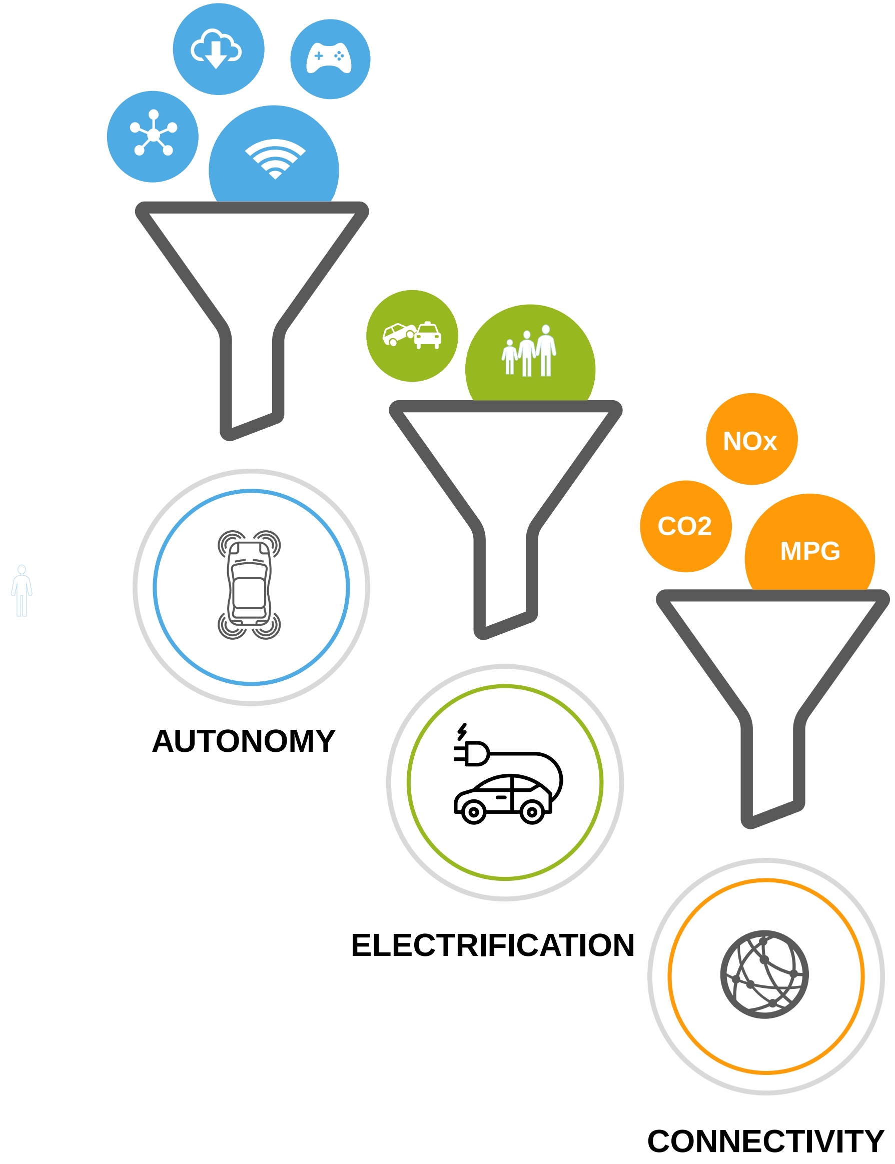
SOP[1] HW 2

Vehicle production

Next gen Vehicle production

- OEMs taking ownership of SDV platform with optimized silicon platforms
- **Software defined vehicle** architectures require **software defined networking**
- NXP can be a key strategic partner:
  - **Vehicle Compute:** NXP are a proven leader in Automotive compute market, with silicon platforms in 16nm today and with 5nm platform in development.
  - **Vehicle Networking:** NXP is the historical leader in IVN, now driving future communication standards and co-design in zonal networks with major OEMs

AUTOMOTIVE E&E TRENDS



- More Functions and Applications
- More Software
- More Computing Power
- More ECUs
- More Safety and Security

- Computing Power
- ECU Integration
- Safety
- Security
- SW Reuse

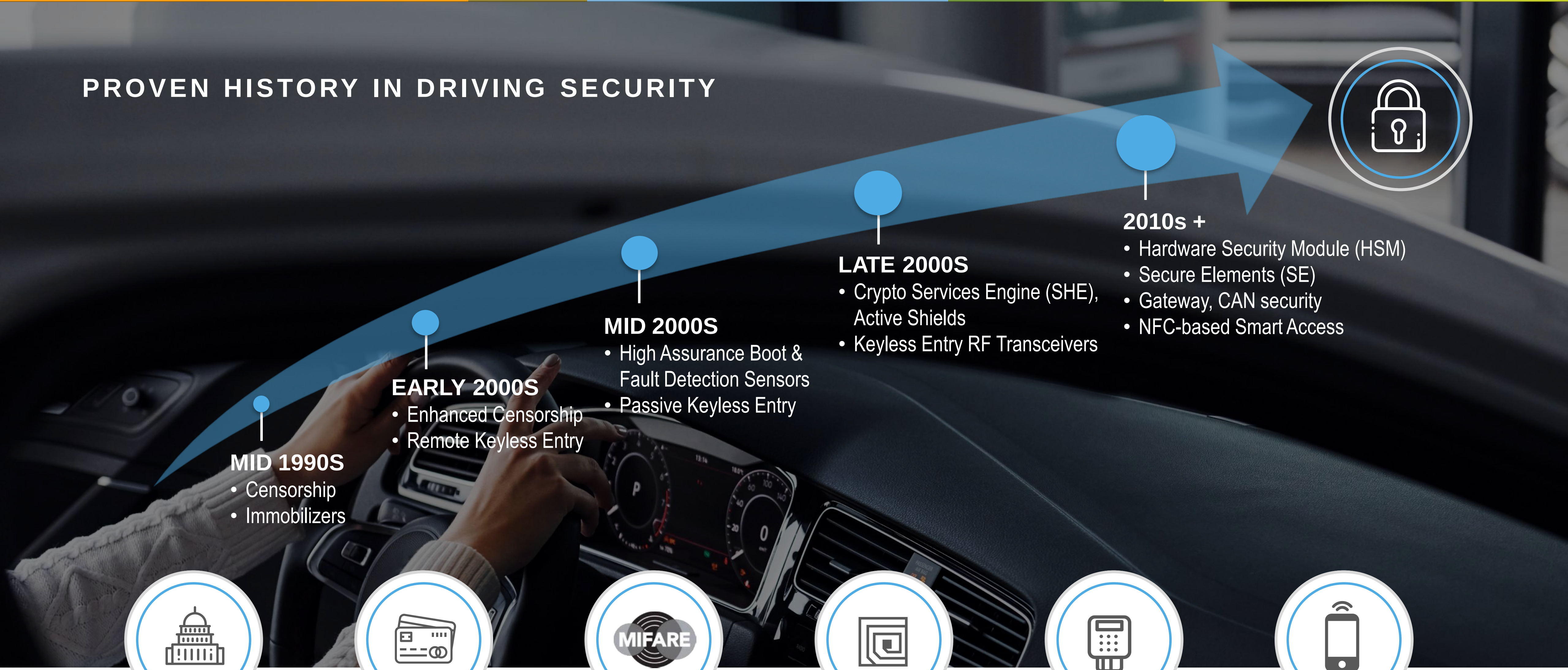
AUTOMOTIVE

Safe and Secure Mobility

MAKING SAFE & SECURE MOBILITY A REALITY

Solution Portfolio	Comprehensive System Solutions for fast time to market and scalability
Innovation Power	In-house high-performance processing, security and mobile ecosystem capabilities
Safe & Secure	Zero defects methodology Leading with functional safety and security

PROVEN HISTORY IN DRIVING SECURITY



MID 1990S
- Censorship
- Immobilizers

EARLY 2000S
- Enhanced Censorship
- Remote Keyless Entry

MID 2000S
- High Assurance Boot & Fault Detection Sensors
- Passive Keyless Entry

LATE 2000S
- Crypto Services Engine (SHE), Active Shields
- Keyless Entry RF Transceivers

2010s +
- Hardware Security Module (HSM)
- Secure Elements (SE)
- Gateway, CAN security
- NFC-based Smart Access

EGOVERNMENT

BANK CARDS

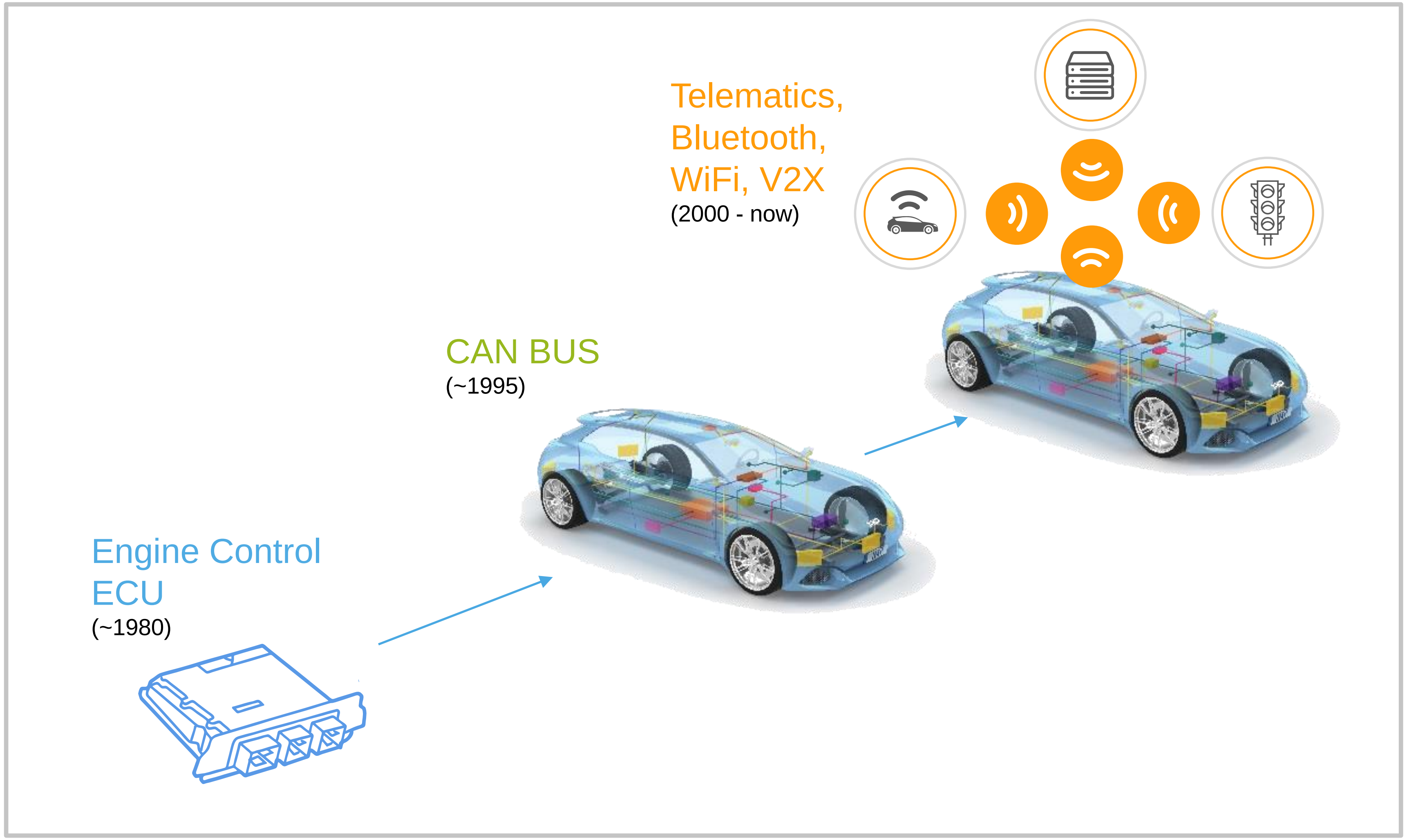
SMART MOBILITY (MIFARE) CARDS

TAGS & AUTHENTICATION

READERS

MOBILE

HISTORY: VEHICLE ELECTRONICS & CONNECTIVITY



Telematics, Bluetooth, WiFi, V2X
(2000 - now)

CAN BUS
(~1995)

Engine Control ECU
(~1980)

INTERACTION

Environment
(3rd party networks)

Local
(private networks)

None
(Standalone)

Standalone

Composed / Distributed

Systems of Systems

SYSTEM TYPE

DID YOU KNOW?

>150

Vehicle cyber incidents
In 2019

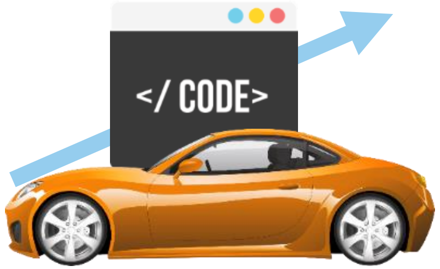
1.4 M

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

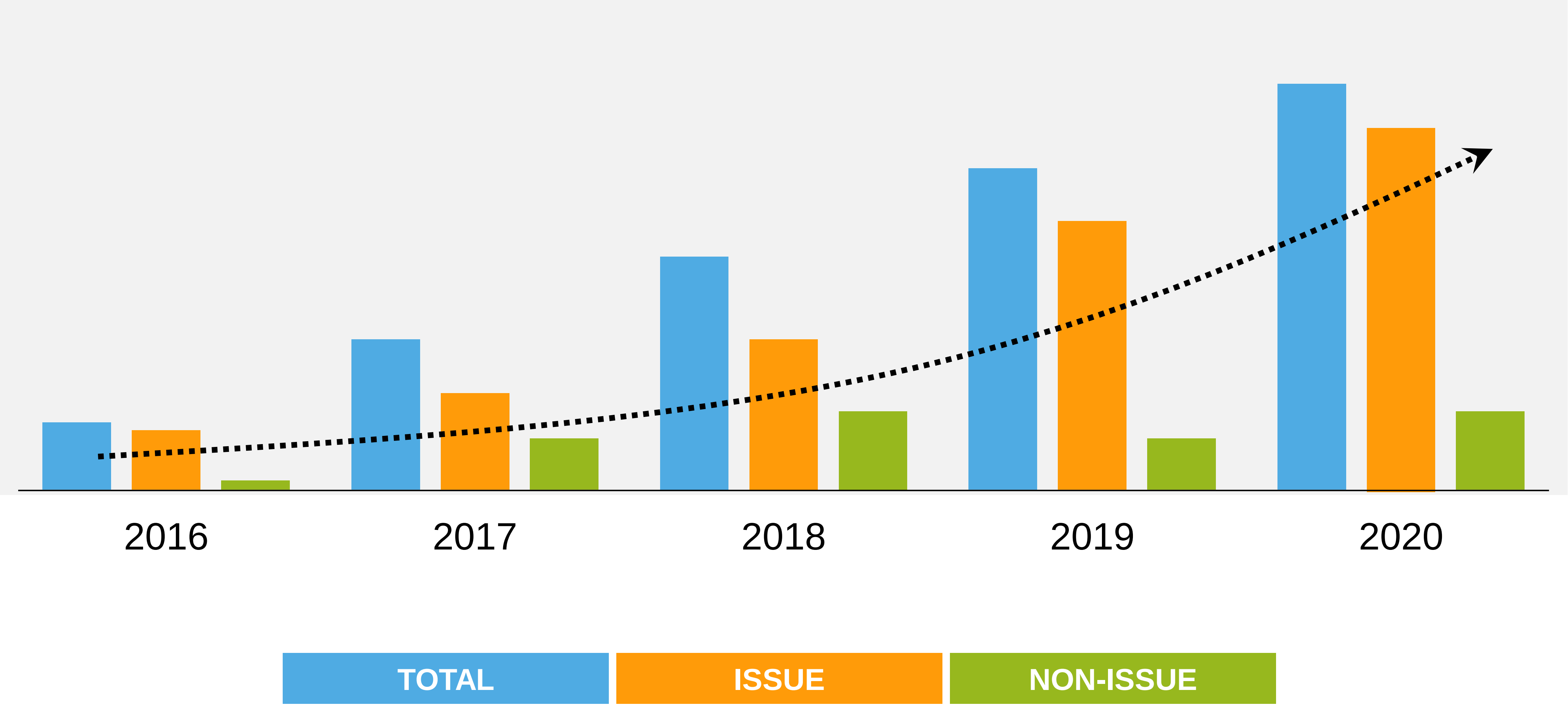
WHY NOW?

Wireless interfaces
enable scalable attacks

250 M connected
vehicles on the
road in 2020

SECURITY IS A MUST-HAVE FOR CONNECTED & AUTONOMOUS VEHICLES

IS IT REAL?

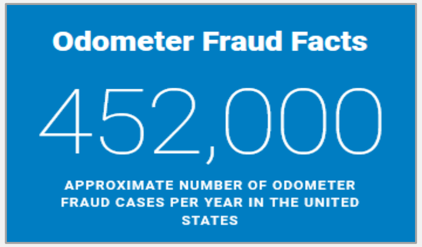


CYBERSECURITY THREATS IN AUTOMOTIVE

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

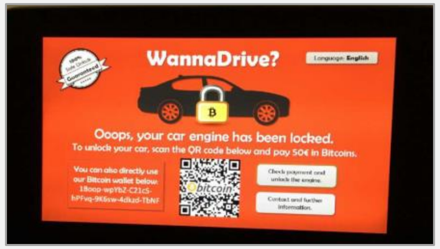
Vehicle theft by relay attack

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

Engine tuning

Workshop around the corner, or in your garage

Ransom for a drive



WannaDrive?

Language: English

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: 18oop-wpYbZ-C21cS-hPFvq-9K6sw-4dlud-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)

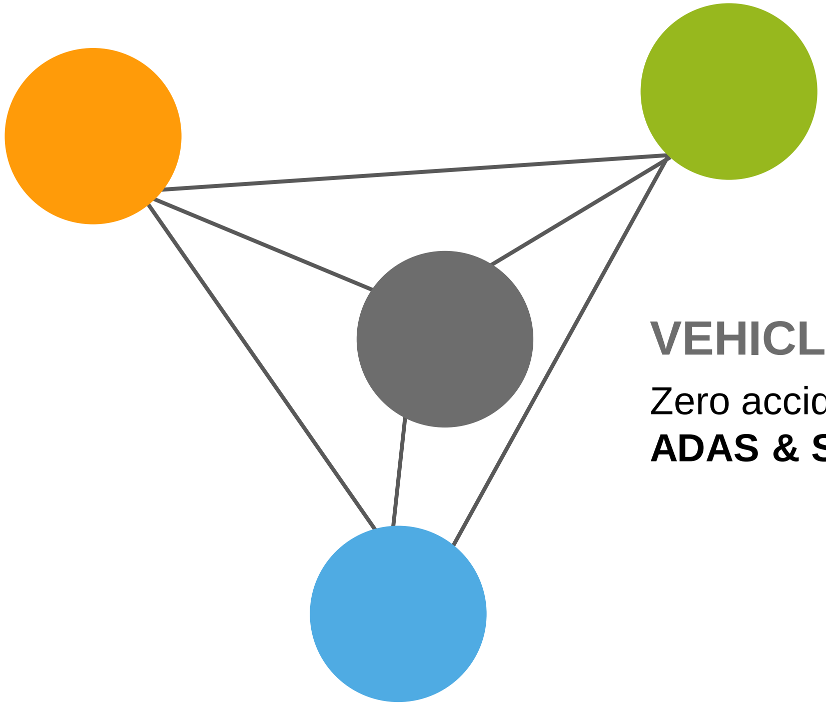
https://www.youtube.com/watch?v=MK0SrxBC1xs

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

REQUIREMENTS FOR SAFE & SECURE MOBILITY



SECURITY

Zero accidents due to system hacks
ISO/SAE 21434

FUNCTIONAL SAFETY

Zero accidents due to system failures
ISO 26262

VEHICLE SAFETY

Zero accidents due to human error
ADAS & SOTIF

DEVICE RELIABILITY

Zero accidents due to device failures
AEC-Q100

SOTIF: Safety of the intended functionality

SECURITY, FUNCTIONAL SAFETY AND SOTIF

SECURITY, FUNCTIONAL SAFETY AND **SOTIF**

IMPOSE **QUALITY DEMANDS** TO ASSURE THE **PROPER OPERATION** OF A SYSTEM

Security is concerned with **intentional threats** which are **unpredictable** and **irregular**, stemming from an **evolving** environment.

A security **assessment** focuses on the **possibility** of attacks.

Functional Safety focuses on **unintentional hazards** which have a **systematic** or **random** source, stemming from a **static** environment.

A functional safety **assessment** focuses on **bugs** and **probability** of failure.

SOTIF focuses on **unanticipated hazards**, stemming from **functional insufficiencies** of the intended functionality or **foreseeable misuse** by persons.

SOTIF **validation & release** criteria focus on **reduction** of **unknown**, **unsafe** scenarios.

NO SAFETY WITHOUT SECURITY

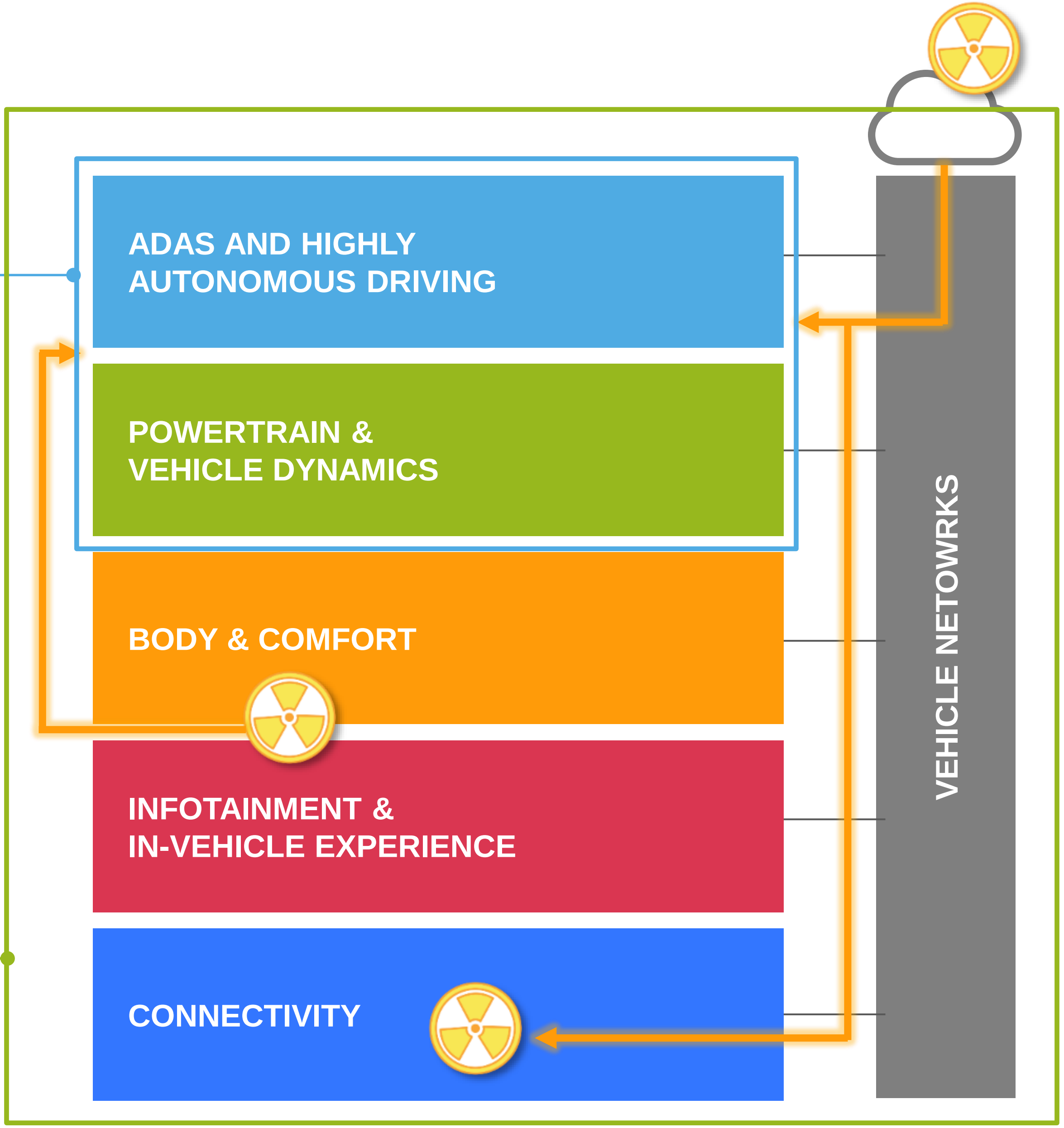
#1 Objective: no functional hazards on mission-critical ECUs

Only possible, if:

System availability ensured

Information received / processed trustworthy

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


ADAS AND HIGHLY AUTONOMOUS DRIVING
POWERTRAIN & VEHICLE DYNAMICS
BODY & COMFORT
INFOTAINMENT & IN-VEHICLE EXPERIENCE
CONNECTIVITY
VEHICLE NETOWRKS

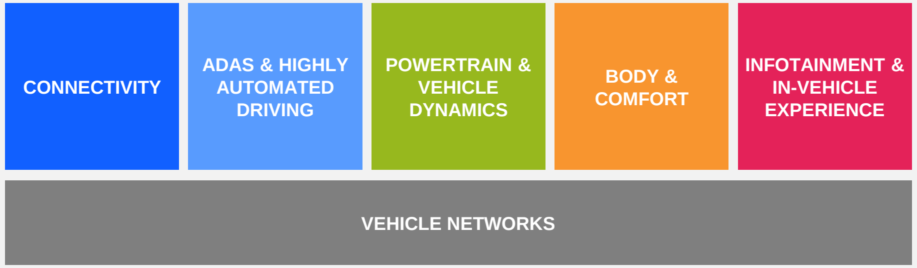
FUNCTIONAL SAFETY & SECURITY – SYSTEM-LEVEL CONCERNS

IC-LEVEL SAFETY & SECURITY SOLUTIONS

- Resource isolation
- On-die monitoring
- Integrity & authenticity checks

+

SAFE & SECURE DOMAIN ARCHITECTURES


CONNECTIVITY
ADAS & HIGHLY AUTOMATED DRIVING
POWERTRAIN & VEHICLE DYNAMICS
BODY & COMFORT
INFOTAINMENT & IN-VEHICLE EXPERIENCE
VEHICLE NETWORKS

- Domain isolation
- Firewalls
- Network intrusion detection

=

SAFE AND SECURE MOBILITY

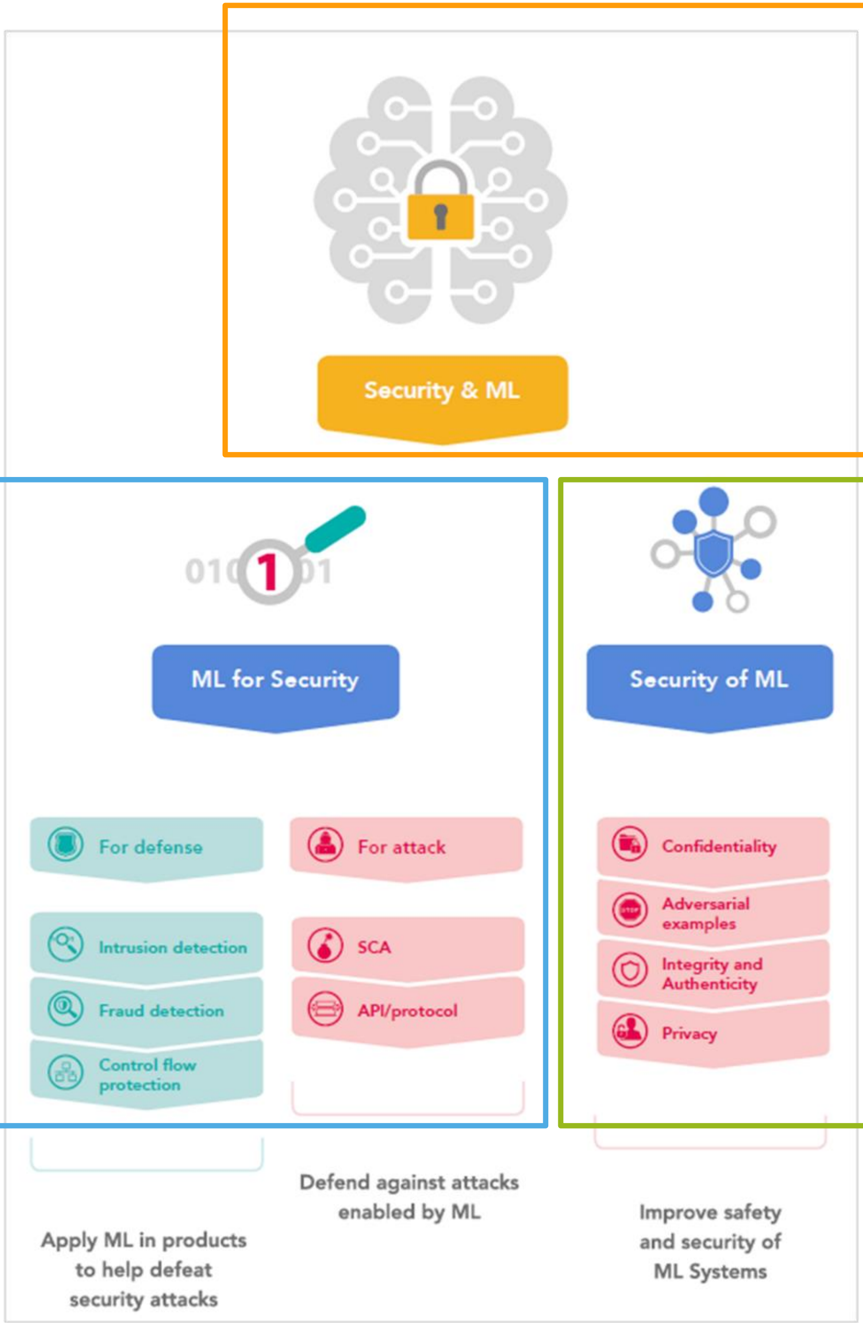
- Fail operational
- Resilient against cyber attacks

SECURITY & MACHINE LEARNING

A largely unexplored field…

…but highly relevant for modern vehicles…

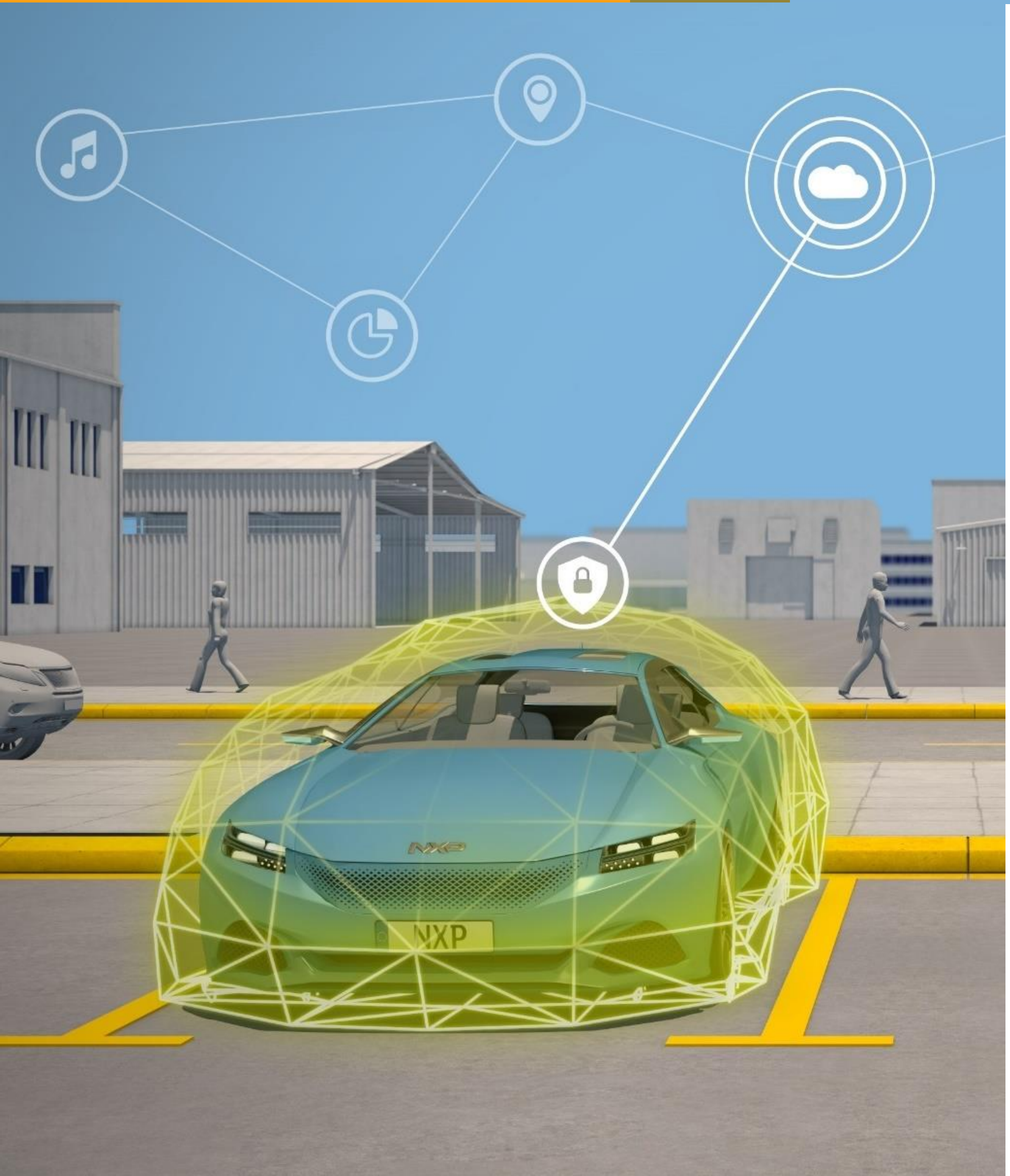
(ML can be used to improve vehicle security, but also to defeat it!)



From the NXP whitepaper ‘Artificial Intelligence of Things’.

…and even more so for autonomous vehicles!

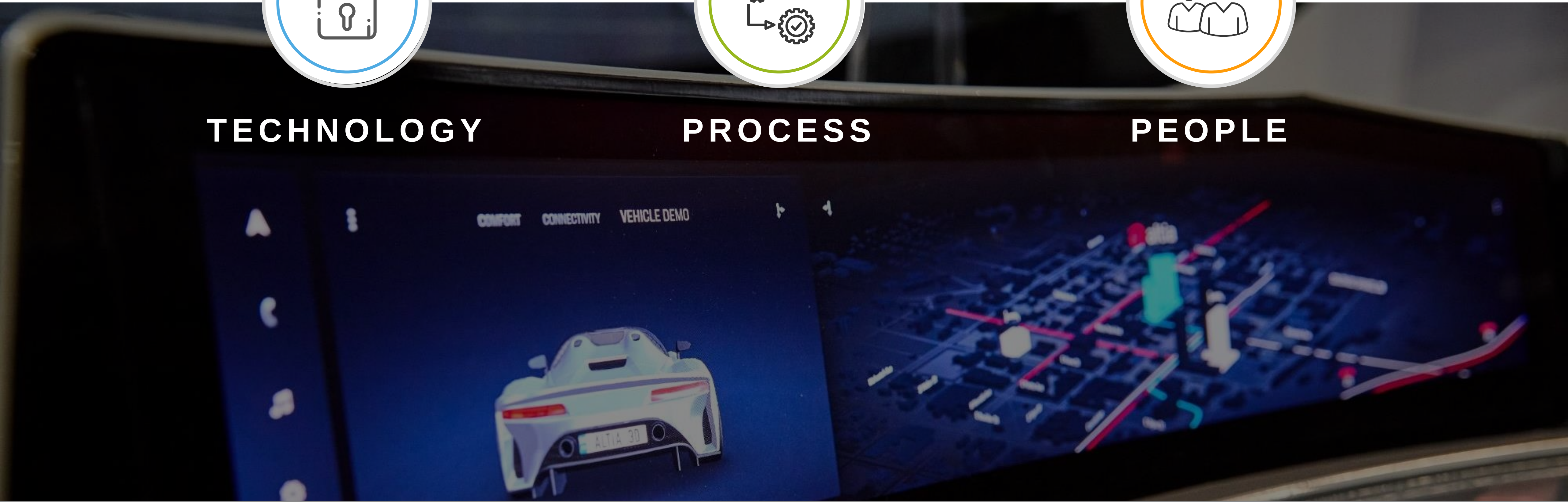
(Autonomous Vehicle automation increasingly depends on AI/ML)



NXP’S APPROACH TO AUTOMOTIVE SECURITY

CYBERSECURITY REQUIRES A HOLISTIC APPROACH

CORNERSTONES:

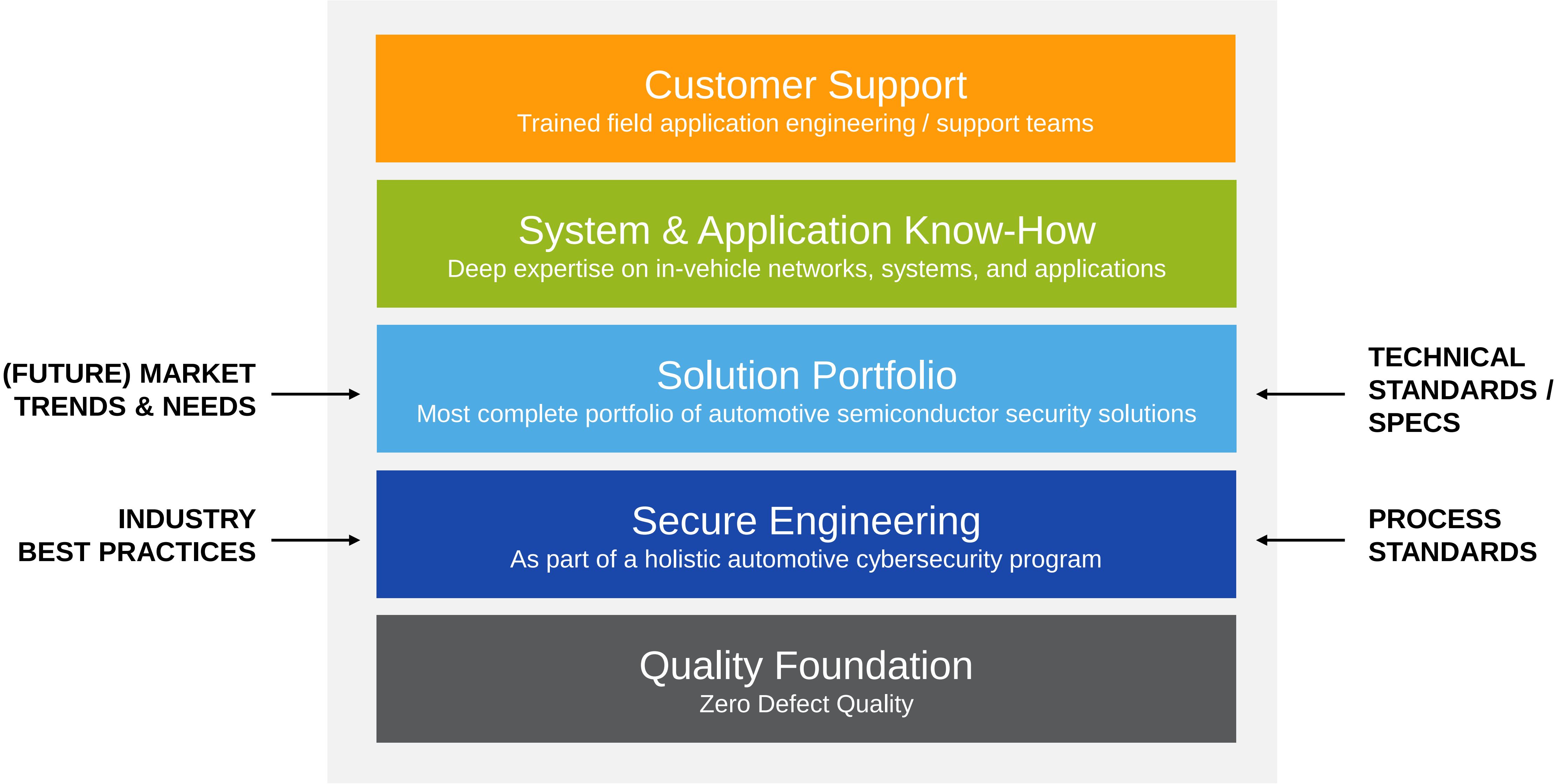


TECHNOLOGY

PROCESS

PEOPLE

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

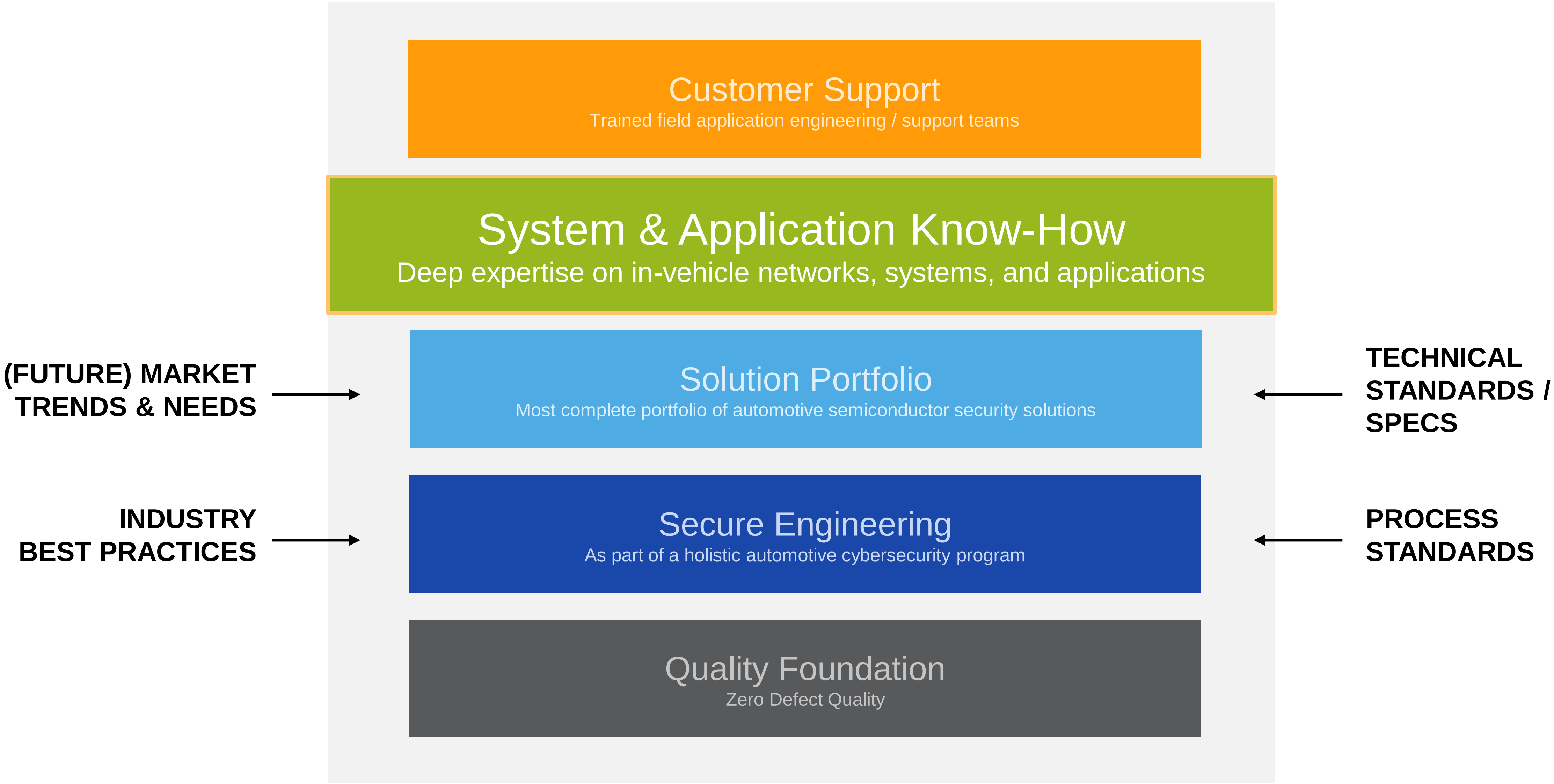
(FUTURE) MARKET TRENDS & NEEDS

INDUSTRY BEST PRACTICES

TECHNICAL STANDARDS / SPECS

PROCESS STANDARDS

NXP'S 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

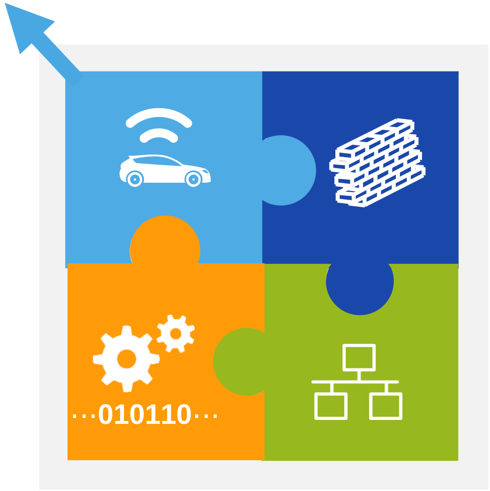
CORE SECURITY PRINCIPLES FOR DEFENSE IN DEPTH

SECURE
**EXTERNAL
INTERFACES**

SECURE
**DOMAIN
ISOLATION**

SECURE
**INTERNAL
COMMUNICATION**

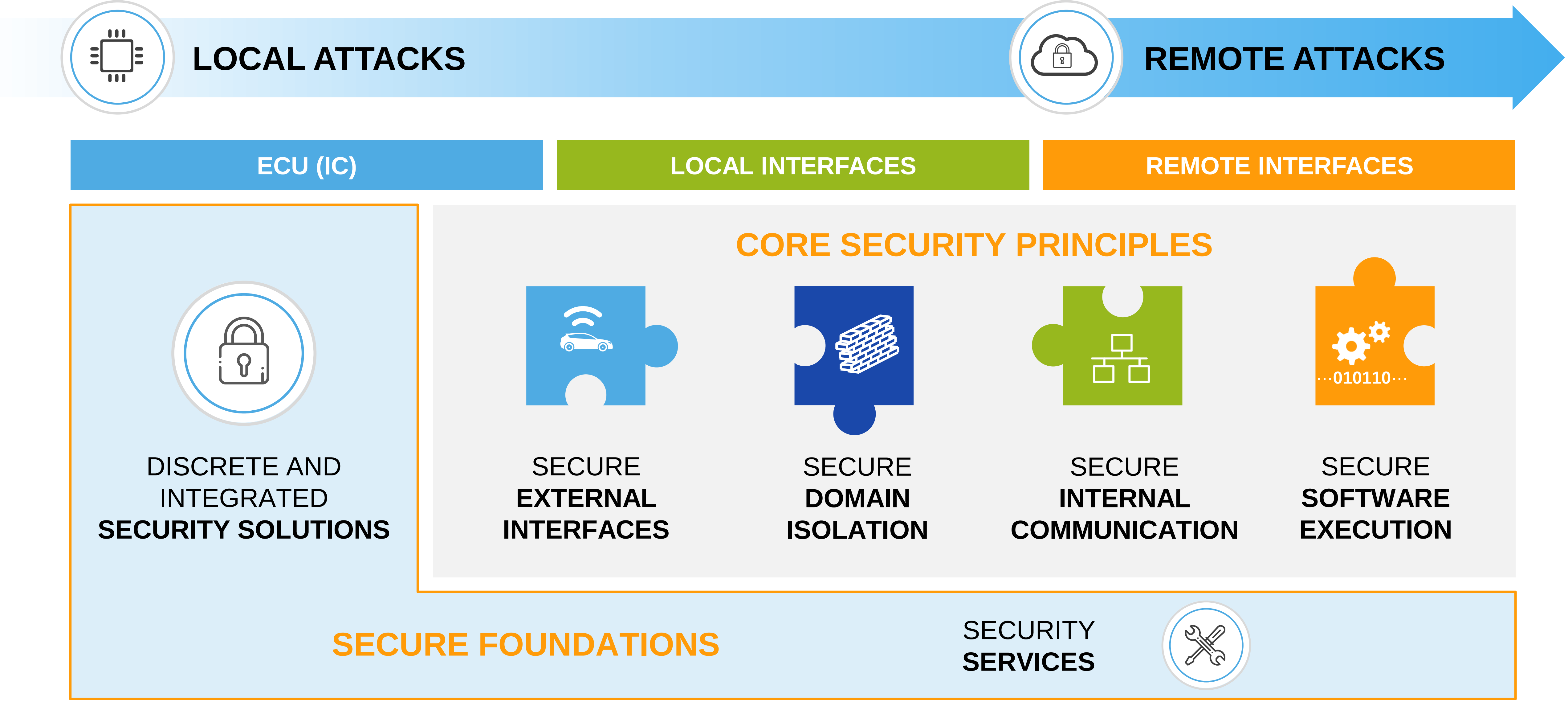
SECURE
**SOFTWARE
EXECUTION**



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

SECURITY MEASURES



LOCAL ATTACKS

REMOTE ATTACKS

ECU (IC)

LOCAL INTERFACES

REMOTE INTERFACES

DISCRETE AND INTEGRATED **SECURITY SOLUTIONS**

CORE SECURITY PRINCIPLES

SECURE **EXTERNAL INTERFACES**

SECURE **DOMAIN ISOLATION**

SECURE **INTERNAL COMMUNICATION**

SECURE **SOFTWARE EXECUTION**

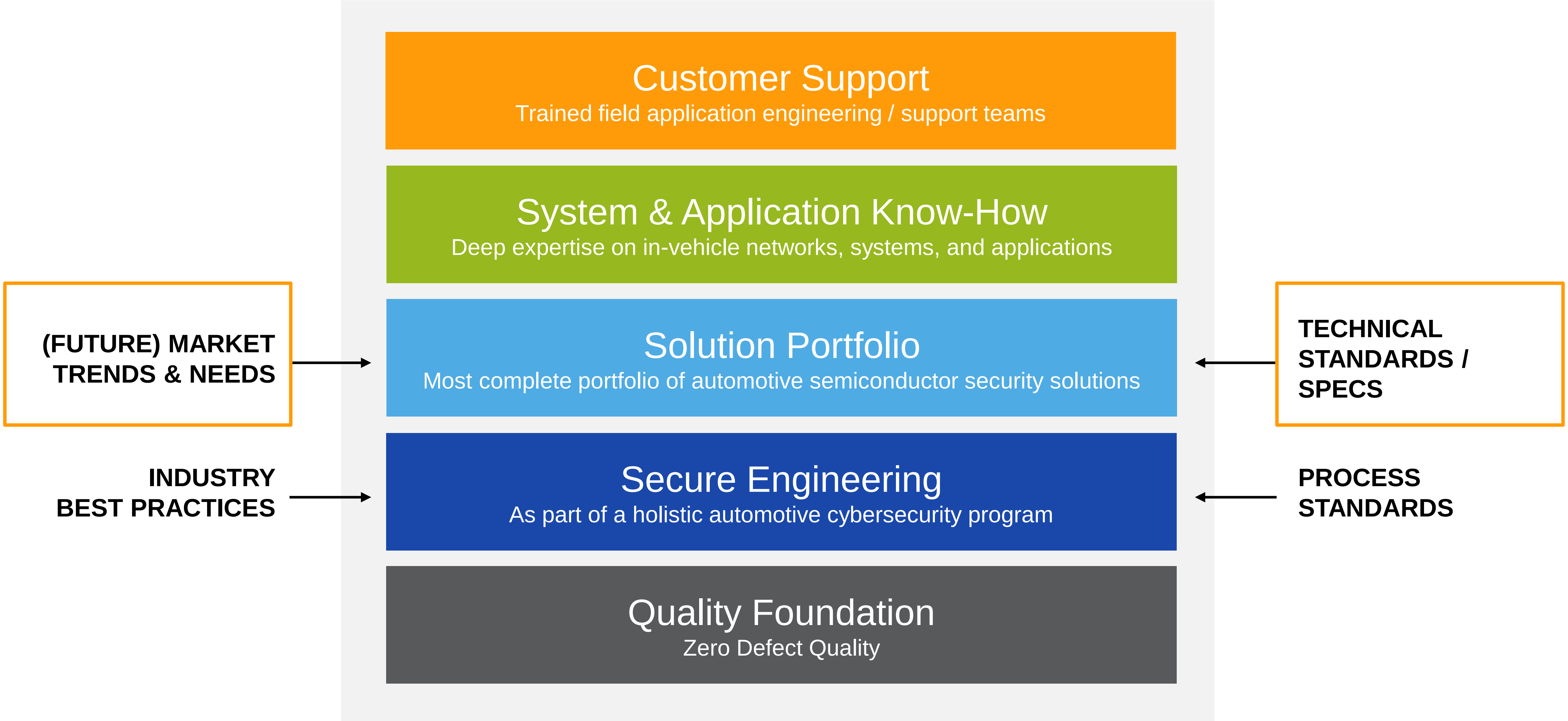
SECURE FOUNDATIONS

SECURITY **SERVICES**

HOLISTIC APPROACH – SOLUTIONS AND ORGANIZATION

<table>
<tr><th></th><th><b>PREVENT</b>
ACCESS</th><th><b>DETECT</b>
ATTACKS</th><th><b>REDUCE</b>
IMPACT</th><th><b>FIX</b>
VULNERABILITIES</th></tr>
<tr><td><b>SECURE INTERFACES</b></td><td>M2M Authentication & Firewalling</td><td>Secure Ranging (e.g. FiRa)</td><td></td><td rowspan="4">Secure Updates</td></tr>
<tr><td><b>SECURE DOMAIN ISOLATION</b></td><td>Firewalling (context-aware message filtering)</td><td rowspan="2">Network Intrusion Detection Systems (NIDS)</td><td>Separated Functional Domains</td></tr>
<tr><td><b>SECURE NETWORKS</b></td><td>Secure Messaging</td><td>Message Filtering & Rate Limitation</td></tr>
<tr><td><b>SECURE PROCESSING</b></td><td>Code / Data Authentication (@ start-up)</td><td>Code / Data Authentication (@ run-time)</td><td>Resource Control (virtualization)</td></tr>
<tr><td rowspan="2"><b>SECURE ENGINEERING</b></td><td>SDLC incl. Security Reviews & Testing, …</td><td>Threat Monitoring, Intelligence Sharing, …</td><td colspan="2">Incident Management / Response</td></tr>
<tr><td colspan="4">Security-Aware Organization, Policies, Governance</td></tr>
</table>

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

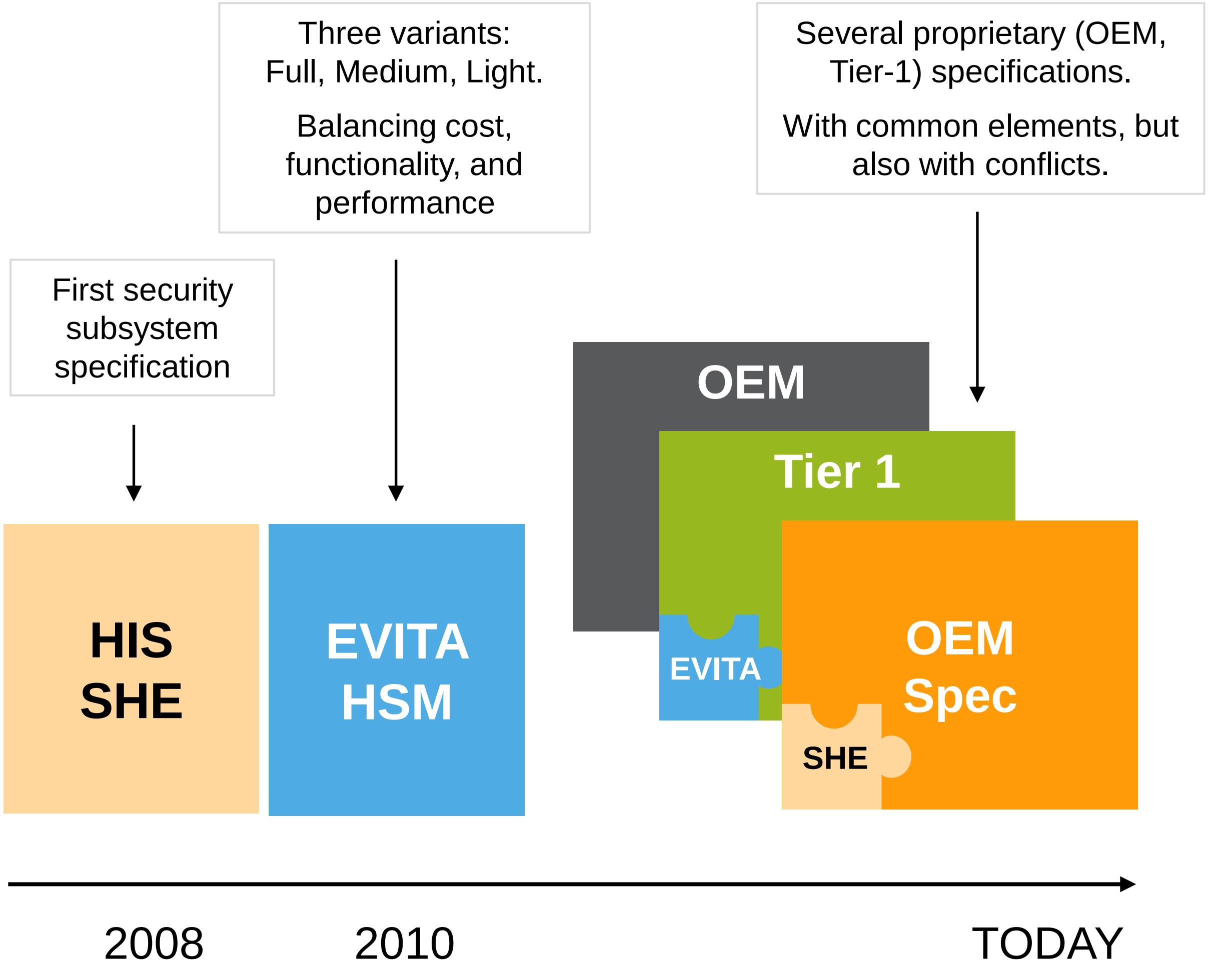
PROCESS STANDARDS

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.
HIS SHE
EVITA HSM
OEM
Tier 1
EVITA
OEM Spec
SHE
2008
2010
TODAY

SECURITY REQUIREMENTS – TODAY’S LANDSCAPE

	2008 SHE *	2010 EVITA (Light / Medium / Full)	Now / Future More recent needs
ARCHITECTURE	• Configurable, fixed function	• Programmable (except EVITA Light)	• Acceleration close to the interfaces (CAN and ETH MAC/PHYs) • Support for Flash-less technologies
FUNCTIONALITY	• Secure boot • Memory update protocol • AES-128 (ECB, CBC) • CMAC, AES-MP • TRNG, PRNG • Key derivation (fixed algorithm) • 10+4 keys, key-usage flags	Same as SHE, plus: • AES-PRNG • monotonic counters (16x, 64bit) Plus, for EVITA Medium and Full: • WHIRLPOOL, HMAC-SHA1, ECDH and ECDSA (P256)	• Further crypto algorithms (e.g. RSA, SHA3, Curve25519, …) • Rollback protection • Key negotiation protocols • Communication protocol offloading (e.g. TLS, IPsec, MACsec, …) • Context separation / multi-application scenarios
OTHER			• Resistance against glitch attacks • ISO/SAE 21434 readiness/compliance

Covered by:

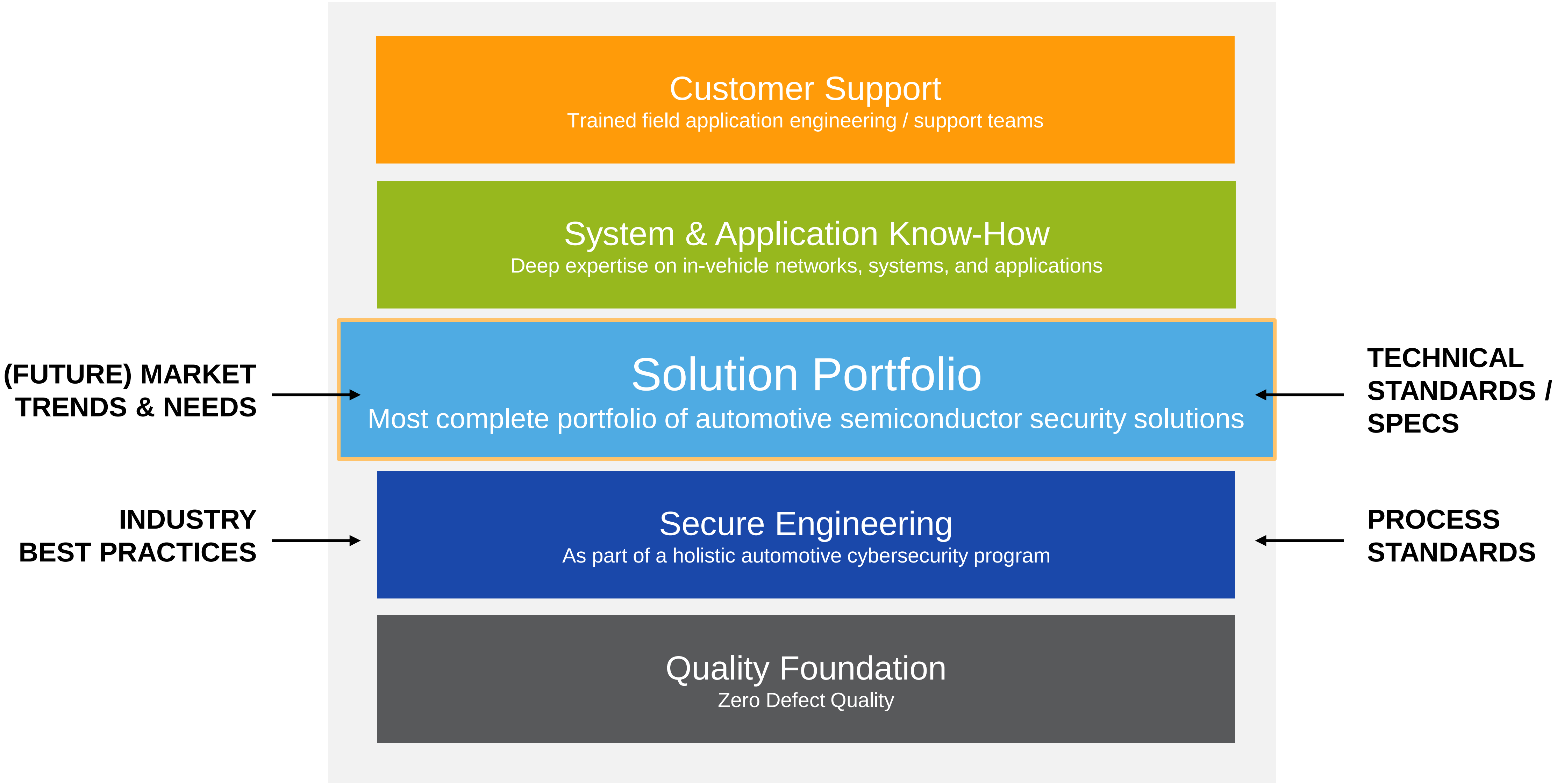
NXP CSE family (since 2010)

NXP HSM family (since 2015)

NXP HSE family (since 2019)

* Adopted by AUTOSAR as “Specification of Secure Hardware Extensions”

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

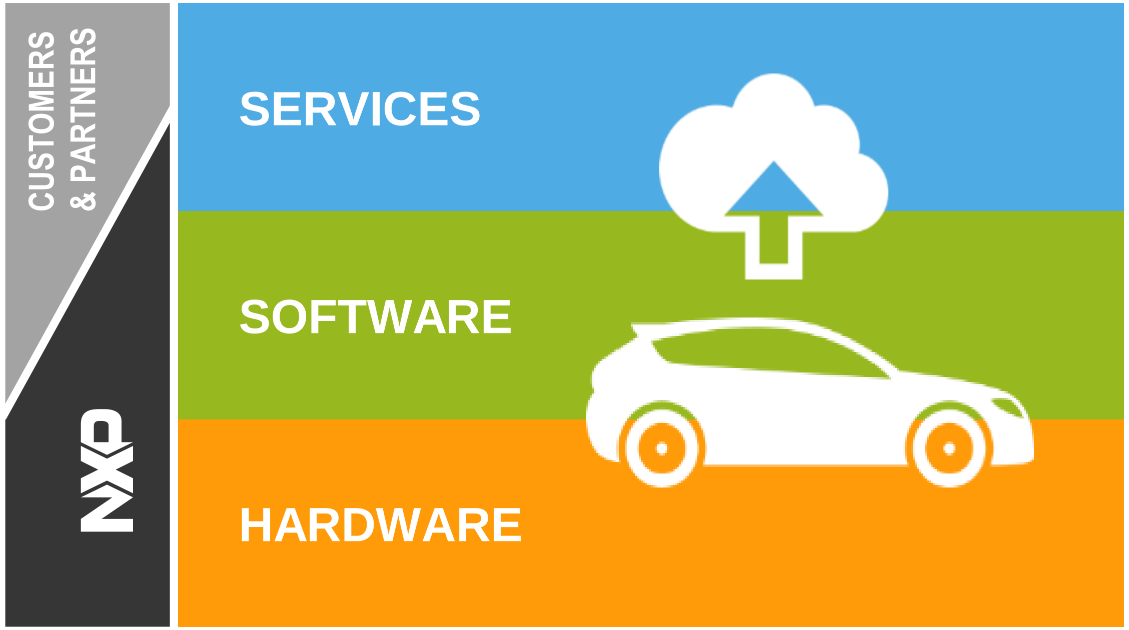
(FUTURE) MARKET TRENDS & NEEDS →

INDUSTRY BEST PRACTICES →

← TECHNICAL STANDARDS / SPECS

← PROCESS STANDARDS

Vehicle security requires a tight integration of hardware, software and services



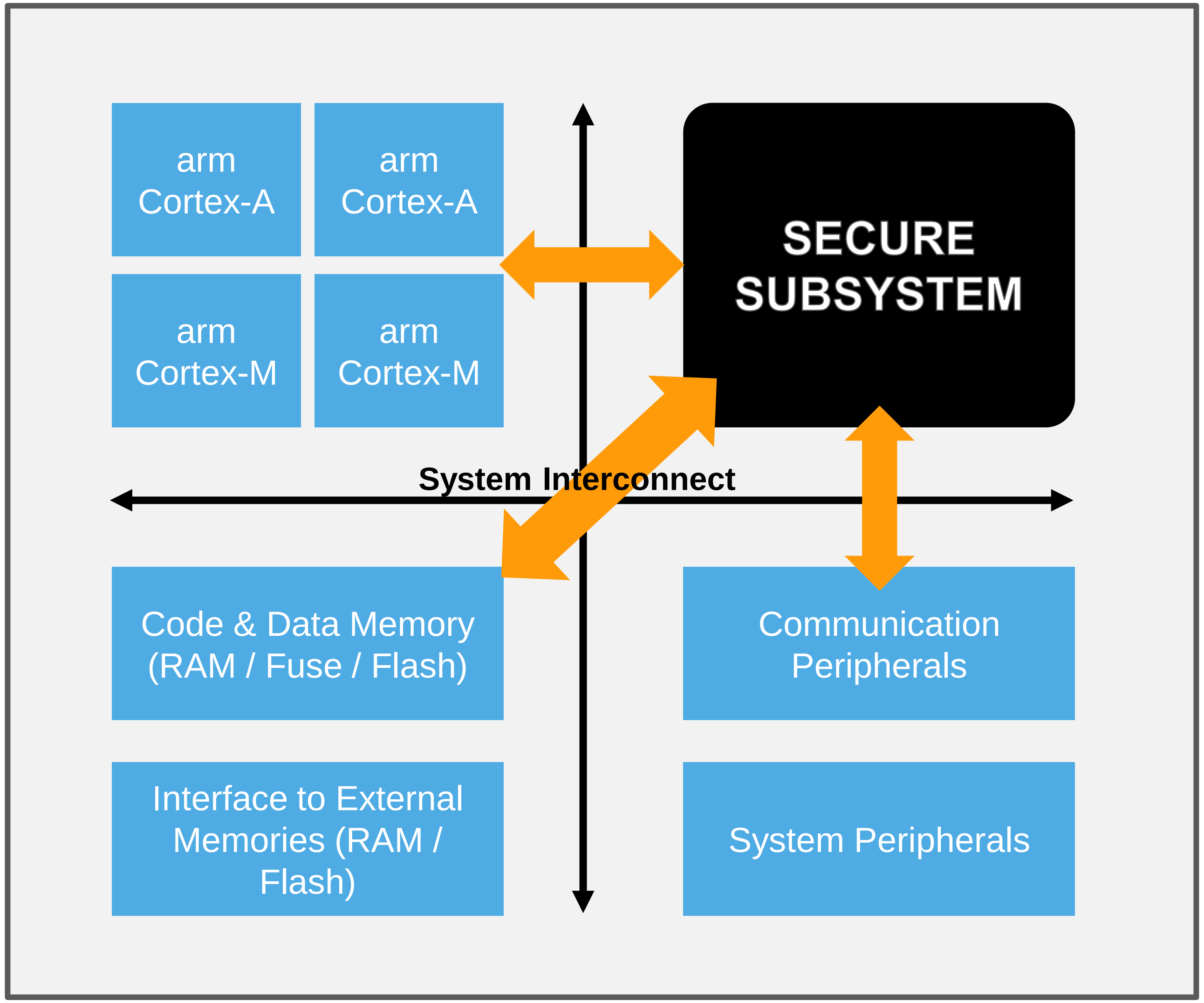
Complementary strengths:

- Threat monitoring & response – e.g. cloud analytics
- Device & identity management – e.g. trust provisioning

- Flexibility / updateability – e.g. FOTA/SOTA for fixing bugs and vulnerabilities

- Performance – e.g. crypto accelerators
- Immutability – e.g. hardware enforced isolation (HSM)
- Tamper resistance – e.g. sensors, glue logic, shields

ON-CHIP SECURE SUBSYSTEM



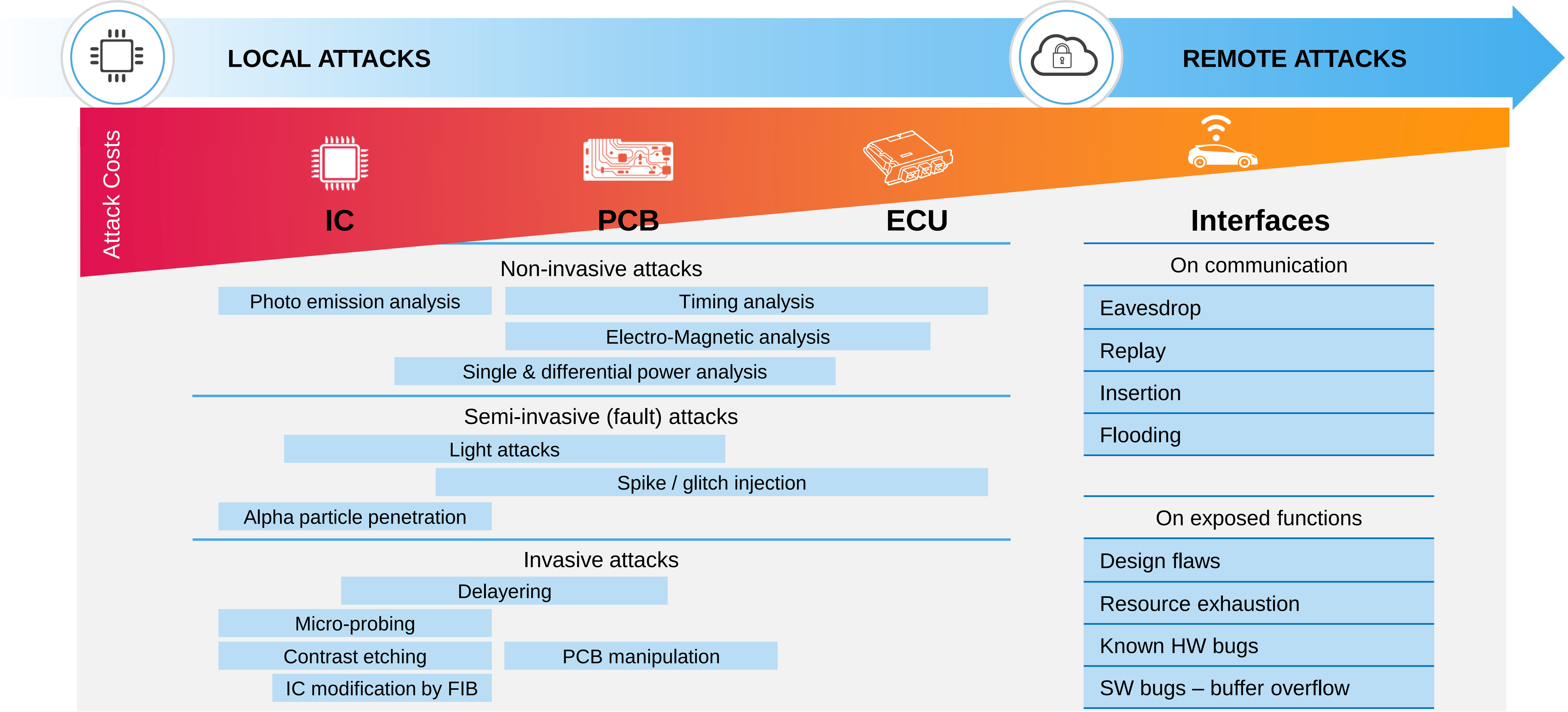
Provides the system with generic (crypto) services

Enforces system confidentiality and trust

For select secure subsystems

Controls the system (reset)

ATTACK CLASSES & TYPES



LOCAL ATTACKS

REMOTE ATTACKS

Attack Costs

IC

PCB

ECU

Interfaces

Non-invasive attacks

Photo emission analysis

Timing analysis

Electro-Magnetic analysis

Single & differential power analysis

Semi-invasive (fault) attacks

Light attacks

Spike / glitch injection

Alpha particle penetration

Invasive attacks

Delayering

Micro-probing

Contrast etching

PCB manipulation

IC modification by FIB

On communication

Eavesdrop

Replay

Insertion

Flooding

On exposed functions

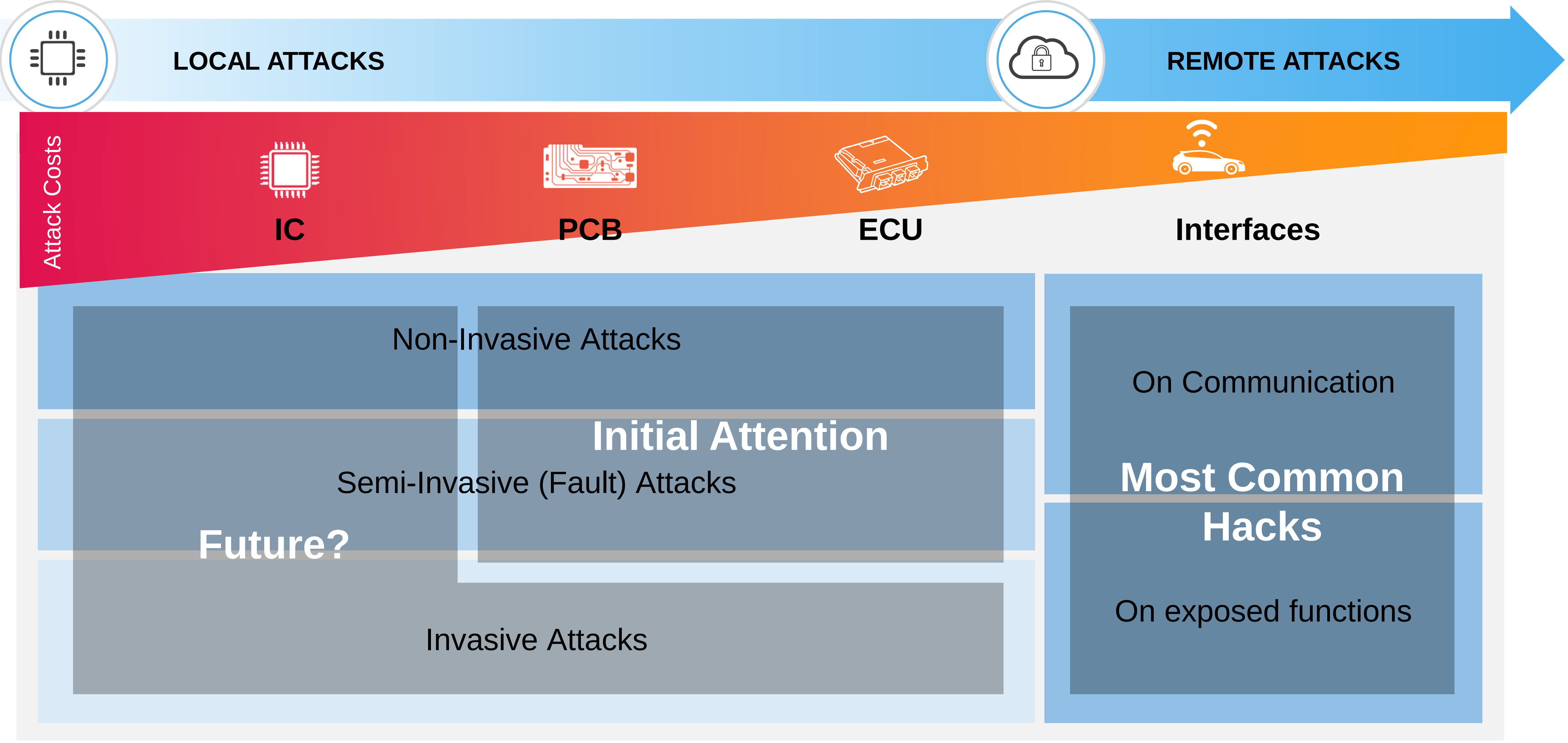
Design flaws

Resource exhaustion

Known HW bugs

SW bugs – buffer overflow

ATTACK CLASSES & TYPES



LOCAL ATTACKS

REMOTE ATTACKS

Attack Costs

IC

PCB

ECU

Interfaces

Non-Invasive Attacks

Initial Attention

Semi-Invasive (Fault) Attacks

Future?

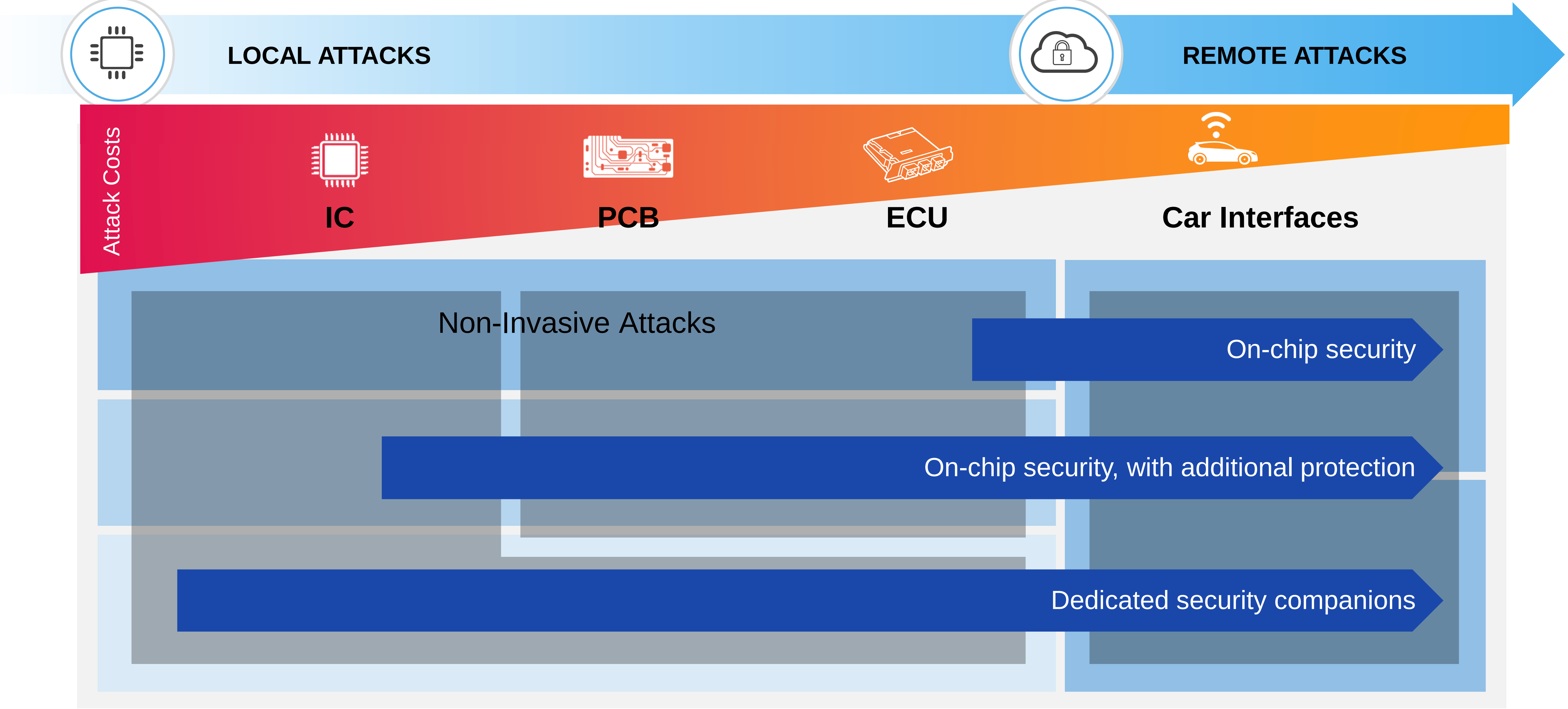
Invasive Attacks

On Communication

Most Common Hacks

On exposed functions

ATTACK CLASSES & TYPES



LOCAL ATTACKS

REMOTE ATTACKS

Attack Costs

IC

PCB

ECU

Car Interfaces

Non-Invasive Attacks

On-chip security

On-chip security, with additional protection

Dedicated security companions

COLLABORATION, INFORMATION SHARING

With industry partners, researchers, CERTs, …

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Charter of Trust

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

NXP is a founding member of the Charter of Trust (Feb. 2018)

CONCLUSION

- Vehicles become increasingly complex – electronics, software, services
- Security is essential –
  people must be able to trust their cars
- NXP leads the industry, with:
  - The most complete portfolio of automotive semiconductor security solutions
  - Complemented by a comprehensive, holistic, automotive cybersecurity program

www.nxp.com/automotivesecurity

blog.nxp.com/category/automotive

YOUR KEY TAKEAWAYS!

CYBERSECURITY NEEDS A HOLISTIC APPROACH

Solutions + Processes & Policies + Organization

NXP’S SECURITY PROGRAM: MATURED OVER TIME

Certified as compliant with ISO 21434

LEADING PORTFOLIO OF AUTOMOTIVE SECURITY SOLUTIONS

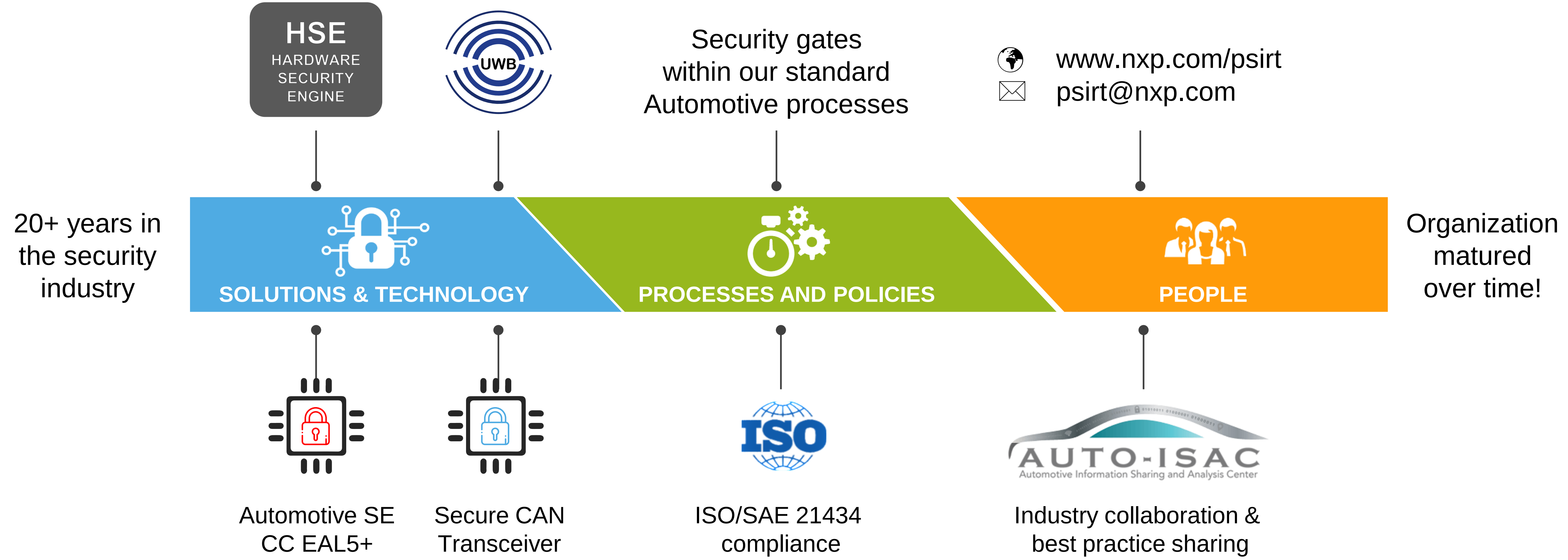
Exceeding market requirements

Going further

blog.nxp.com/category/automotive

www.nxp.com/automotivesecurity

YOUR KEY TAKEAWAYS!



20+ years in the security industry

SOLUTIONS & TECHNOLOGY

PROCESSES AND POLICIES

PEOPLE

Organization matured over time!

Security gates within our standard Automotive processes

www.nxp.com/psirt
psirt@nxp.com

Automotive SE CC EAL5+

Secure CAN Transceiver

ISO/SAE 21434 compliance

Industry collaboration & best practice sharing

Going further www.nxp.com/automotivesecurity blog.nxp.com/category/automotive

SECURE CONNECTIONS
FOR A SMARTER WORLD