

Functional Safety & Security: Next Generation Automotive Security Solutions

Marius Rotaru

Automotive Software Architect & Technical Director

June 2019 | Session #AMF-AUT-T3680



SECURE CONNECTIONS
FOR A SMARTER WORLD

Agenda

- Introduction
- NXP's Approach to Automotive Security
 - System & Application View
 - AMP's Security Solution
 - Secure Engineering
- Conclusion

NXP – Global #1 in Automotive Semiconductors



2400+
AUTO
ENGINEERS

30+
AUTO SITES
WORLDWIDE

#1
AUTO SEMI
SUPPLIER GLOBALLY

~50%
OF NXP'S
REVENUE IS
FROM AUTO

60+
YEARS OF
EXPERIENCE
IN AUTO



NXP Makes Safe and Secure Mobility Happen

Technology Leadership

#1 Auto Microprocessors
#1 Auto Analog / RF / DSP
#2 Auto Microcontrollers
#1 Auto Application Processors



Applications Leadership

#1 Car Infotainment
#1 Secure Car Access
#1 In-Vehicle Networking
#1 Safety
#2 Powertrain



in Auto Semiconductors

2018 Global Auto Semi Market: \$37.7B

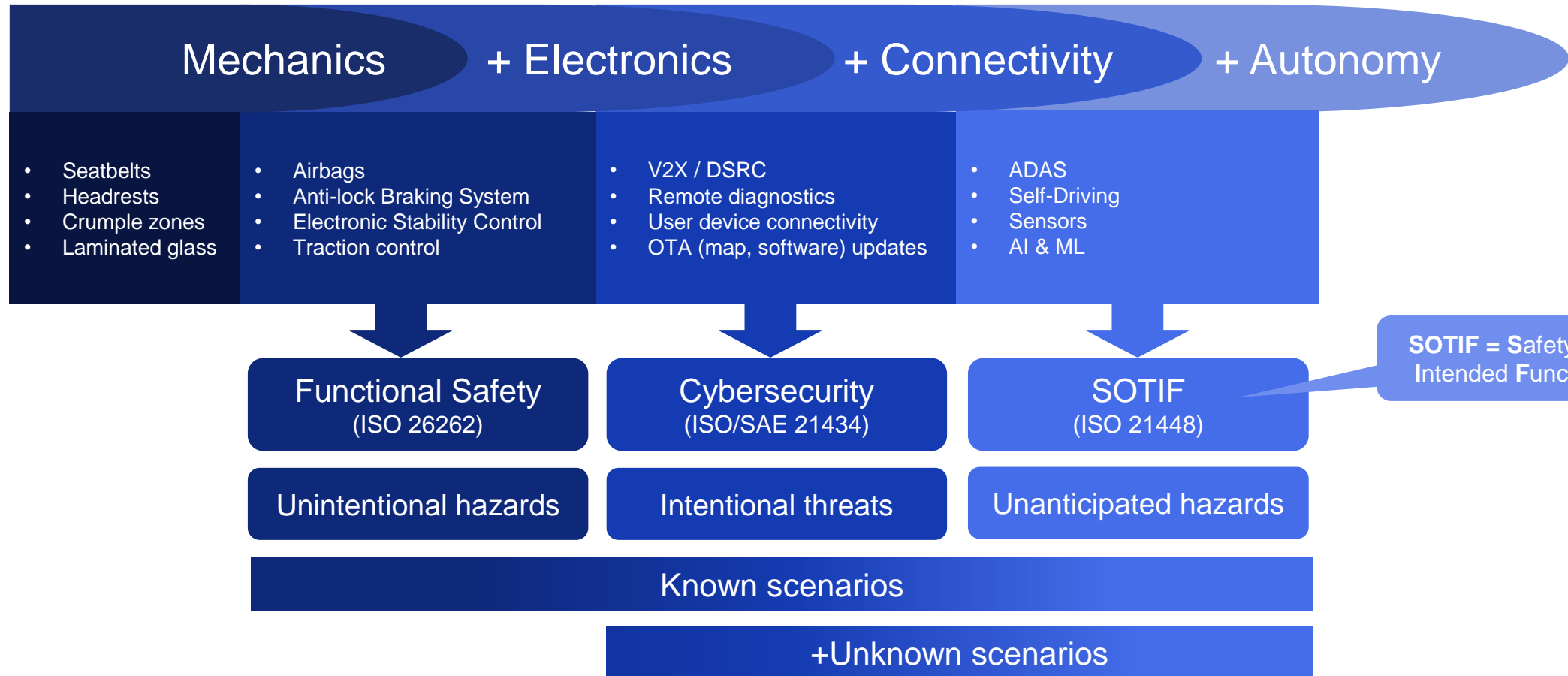
Innovation Leader ADAS
Innovation Leader Security

1. Based on 2018 Auto TAM
2. Auto RF/DSP includes Secure Car Access, Radio/Audio, V2X and Radar Transceivers
3. Source: Strategy Analytics, IHS Markit, NXP

Vehicle Safety & Cybersecurity

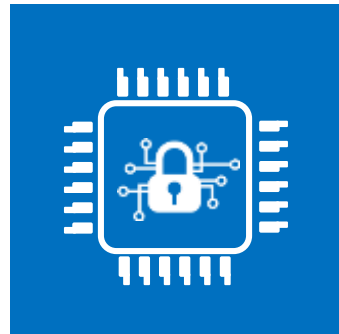
Improve safety

+ Improve user experience



Functional Safety & Security – System-Level Concerns

IC-level Safety & Security Solutions



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

+

Safe & Secure Domain Architectures



- Domain isolation
- Firewalls
- Network intrusion detection

=

Safe and Secure Mobility



- Fail operational
- Resilient against cyber attacks

NXP – Making Safe & Secure Mobility a Reality

Solution Portfolio



The most complete system solutions for fastest time to market and scalability.

Innovation Power



In-house high performance processing, security and mobile eco-system capabilities.

Safe & Secure



Zero defect methodology. Leading with security and functional safety.

NXP's Approach to Automotive Security

System & Application View



NXP's Approach to Automotive Security

Customer Support

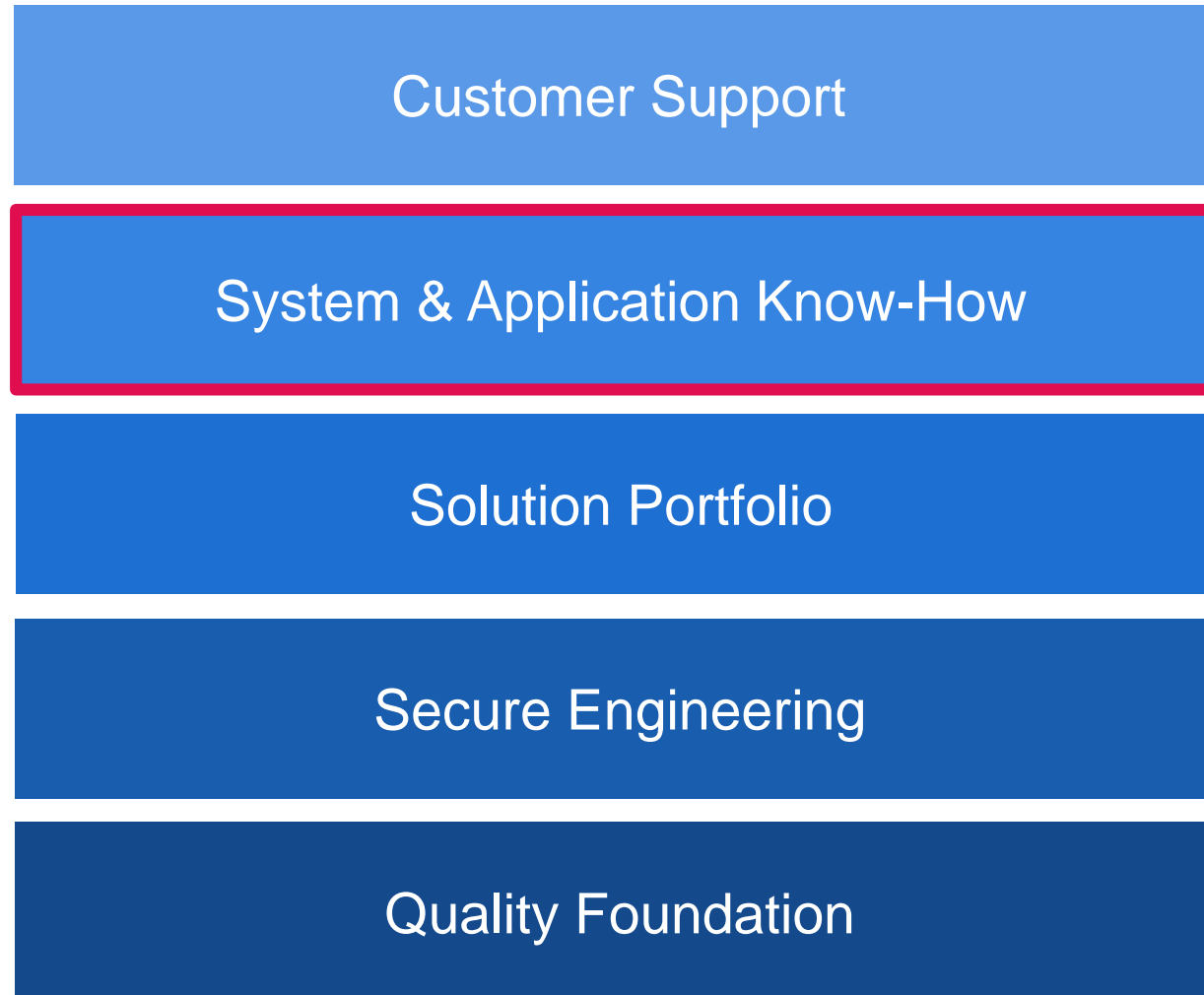
System & Application Know-How

Solution Portfolio

Secure Engineering

Quality Foundation

NXP's Approach to Automotive Security



Example of Cybersecurity Threats in Automotive

Local Attacks

Remote Attacks

Tampering the odometer



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

Engine tuning



Workshop around the corner, or in your garage

Vehicle theft by relay attack



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

Ransom for a drive



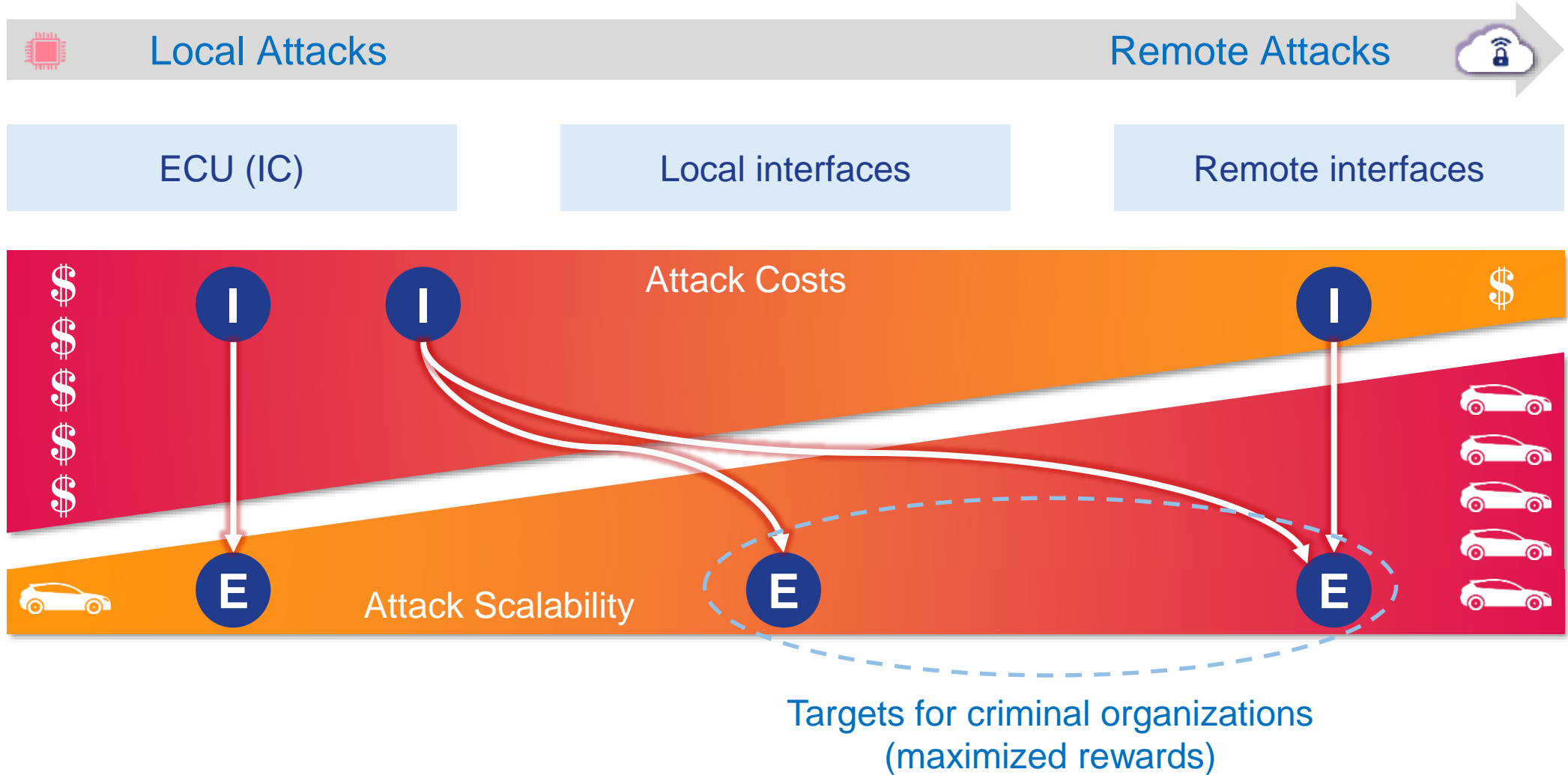
VDI Conference on IT Security for Vehicles (Berlin / July 2017)

Remote hack of an unaltered car (July 2015)



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

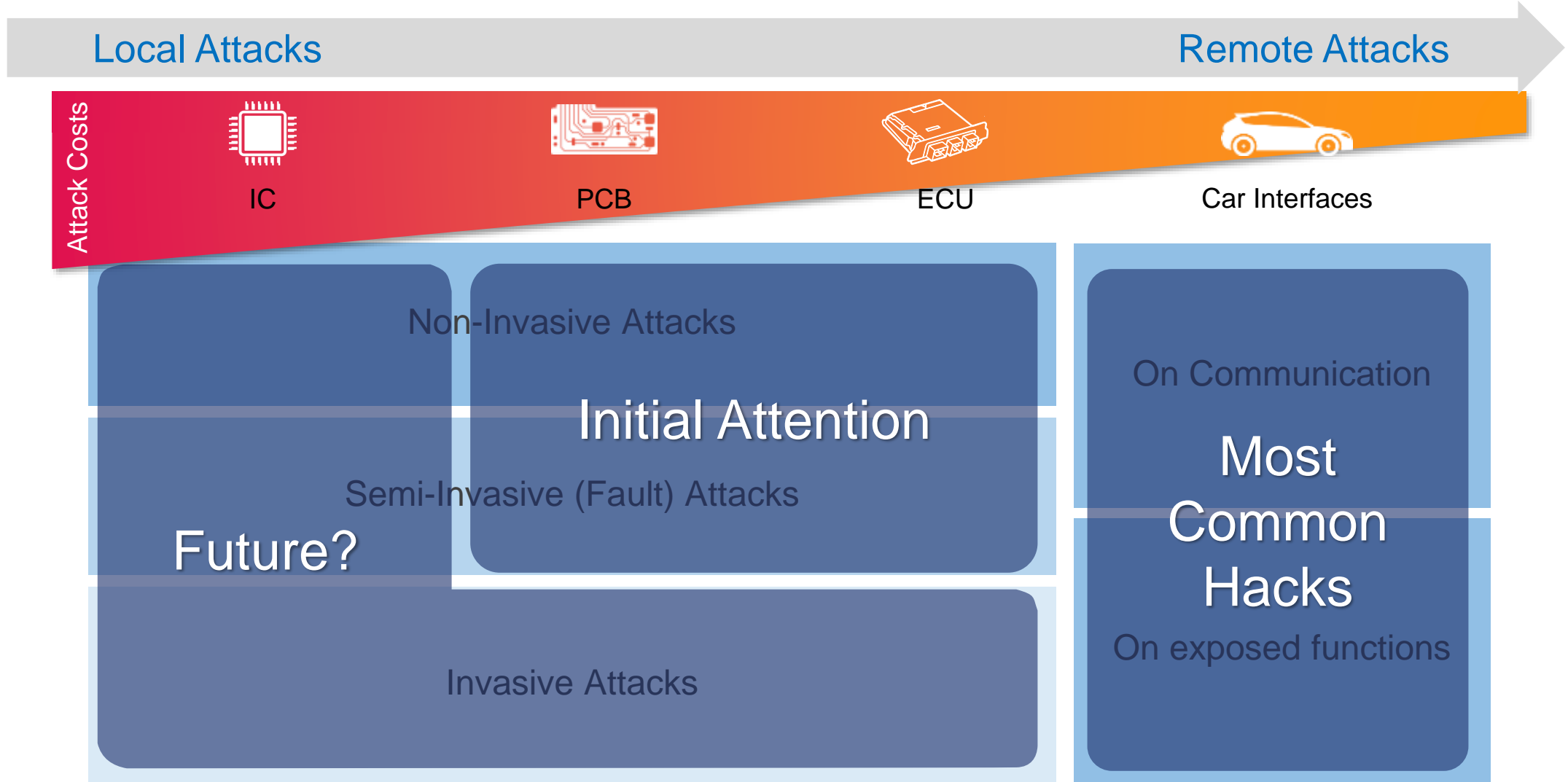
Attack Costs vs. Attack Scalability



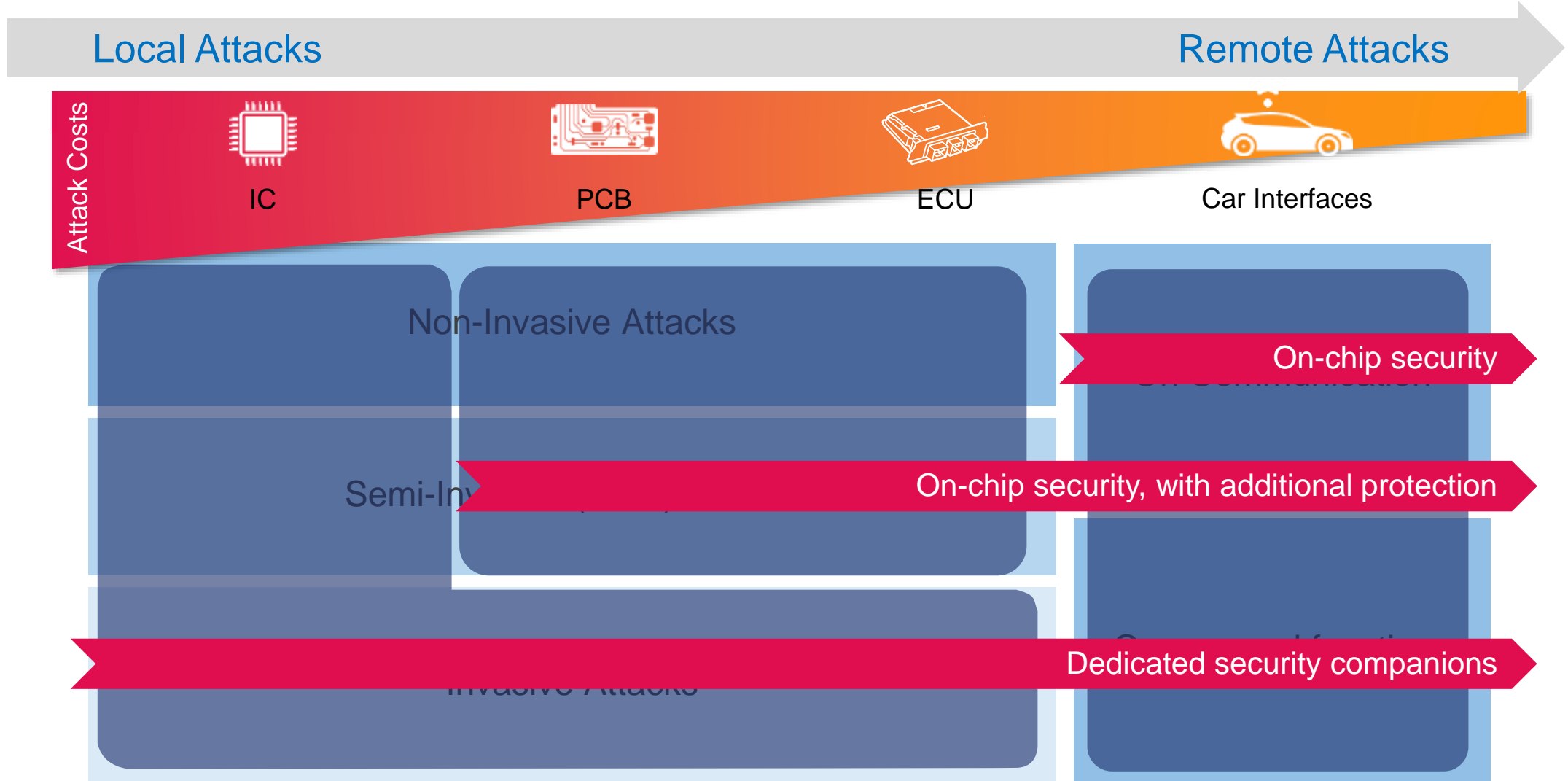
I Identify vulnerability

E Exploit vulnerability

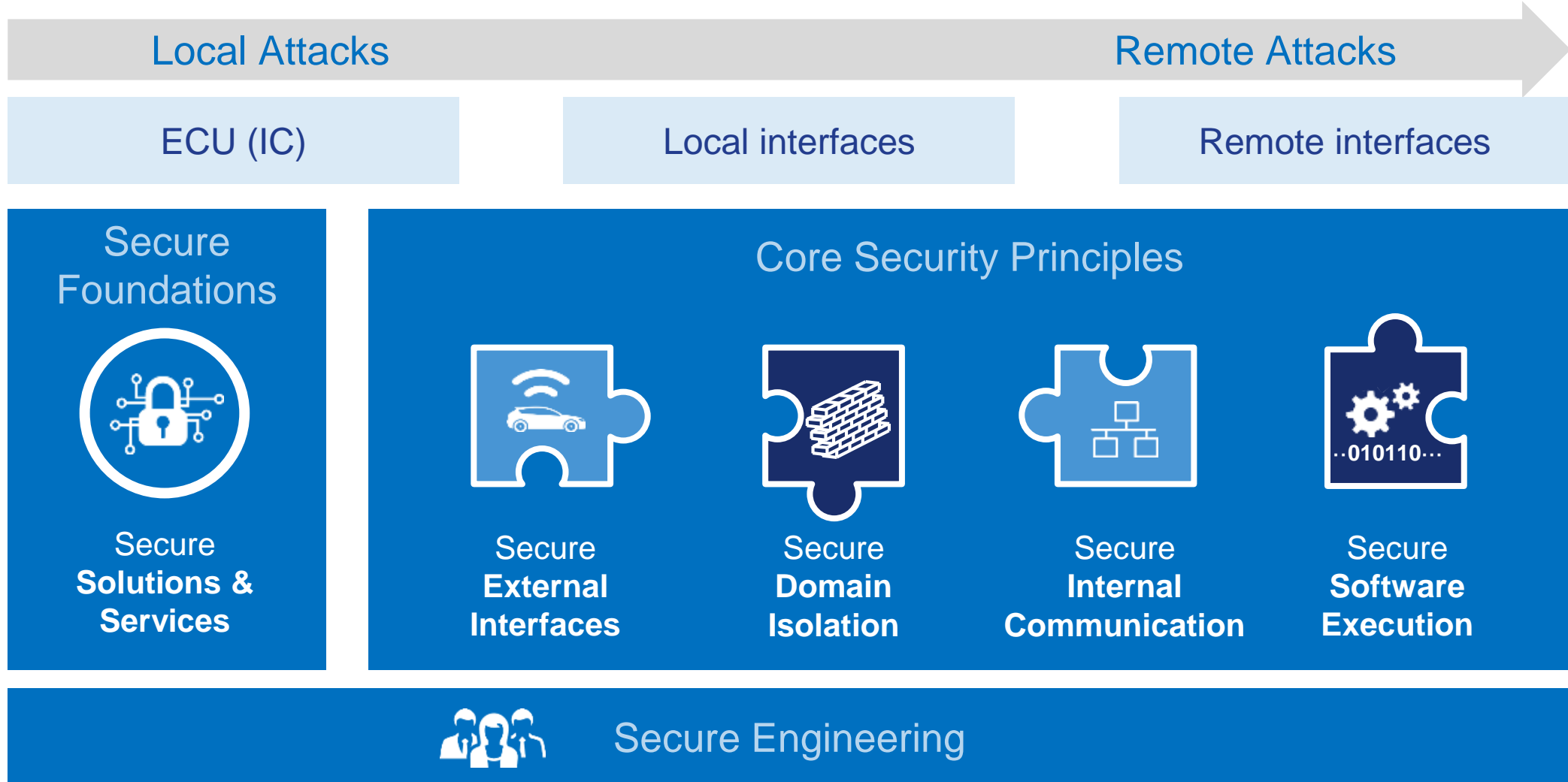
Where to Focus?








Different Solutions For Different Security Needs



Core Security Principles and Measures



Core Security Principles Applied to In-Depth Defenses

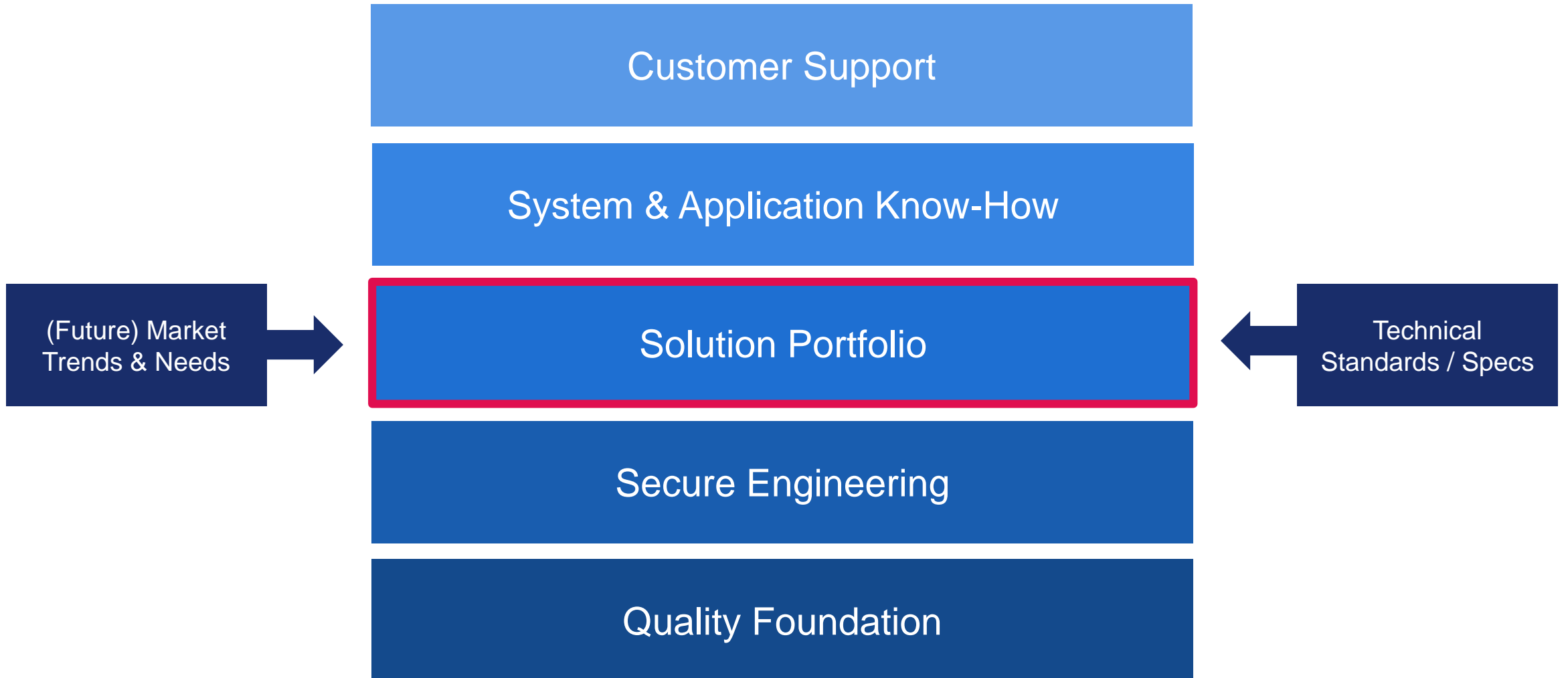
| | | Prevent access | Detect attacks | Reduce impact | Fix vulnerabilities |
|--|--|---|--|-------------------------------------|---------------------|
| Technology | Secure Interfaces  | M2M Authentication & Firewalling | | | |
| | Secure Gateway  | Firewalling (context-aware message filtering) | Intrusion 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) | |
| People & Processes  | Secure Engineering | SDLC incl. Security Reviews & Testing, ... | Threat Monitoring, Intelligence Sharing, ... | Incident Management / Response | |
| | | Security-Aware Organization, Policies, Governance | | | |

NXP's Approach to Automotive Security

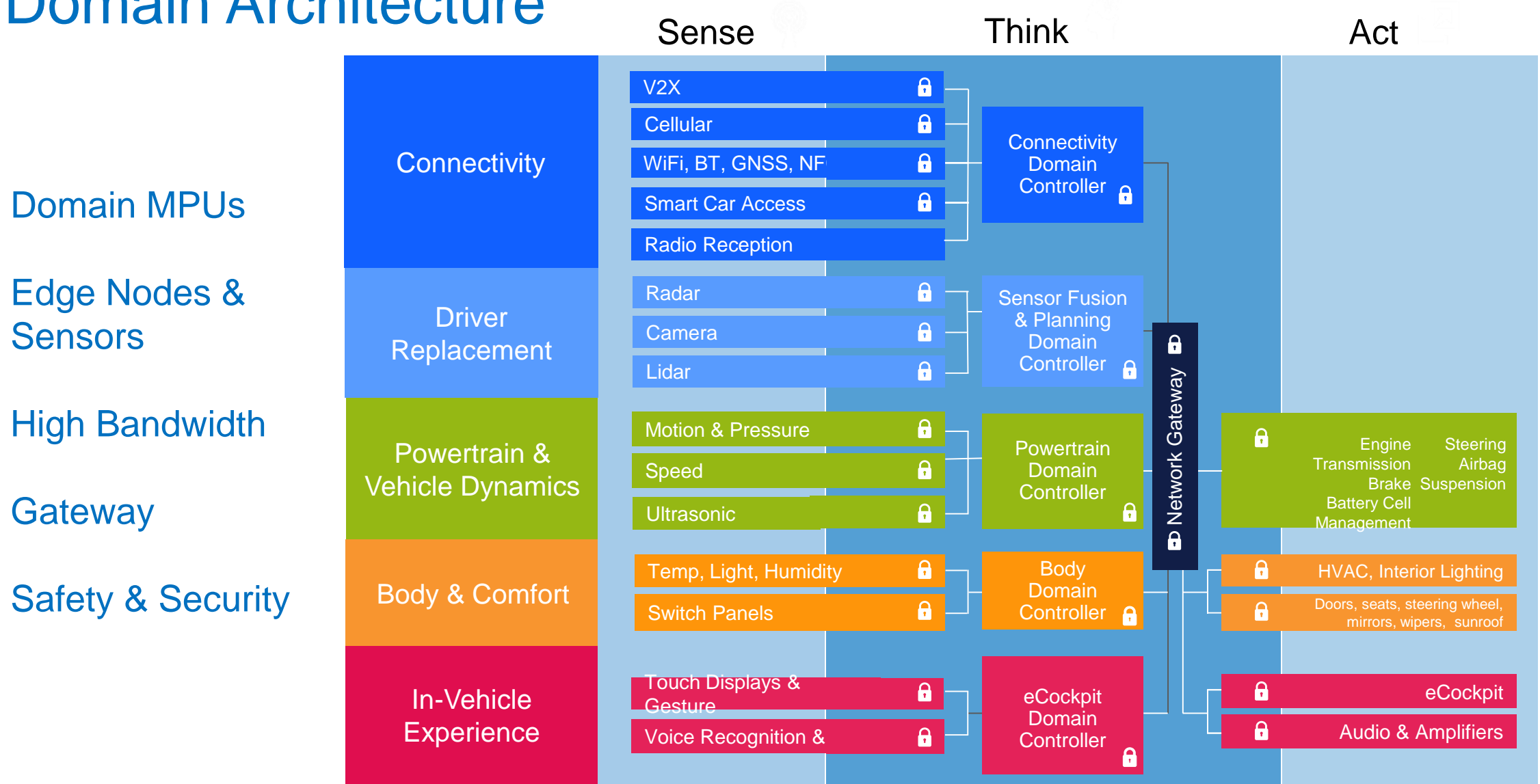
Solution Portfolio



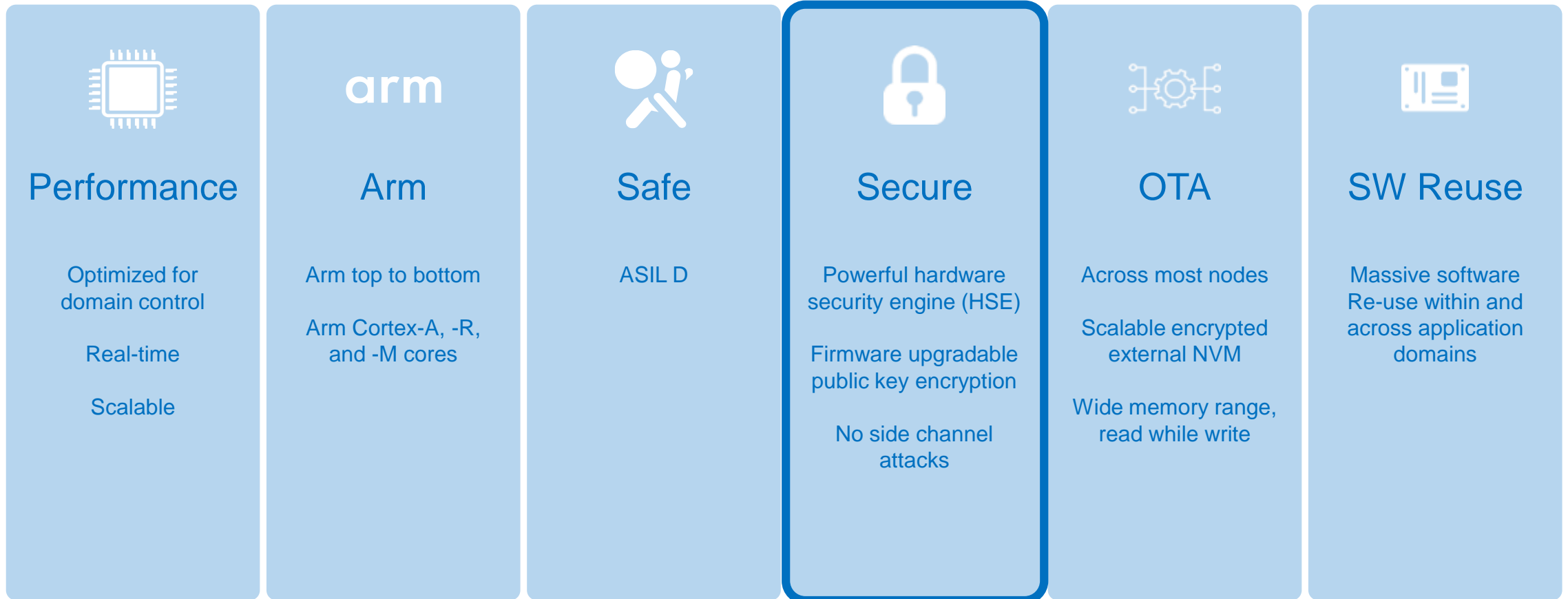
NXP's Approach to Automotive Security



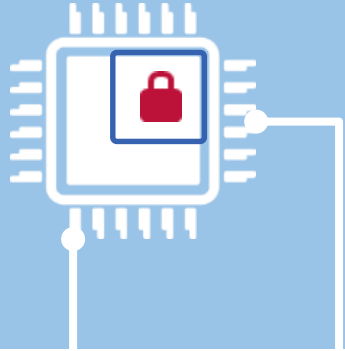
Domain Architecture



Auto Processors Tomorrow: Domain Architecture Requirements



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

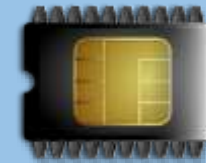


ACT



Security Companions

Security extension *for specific use*

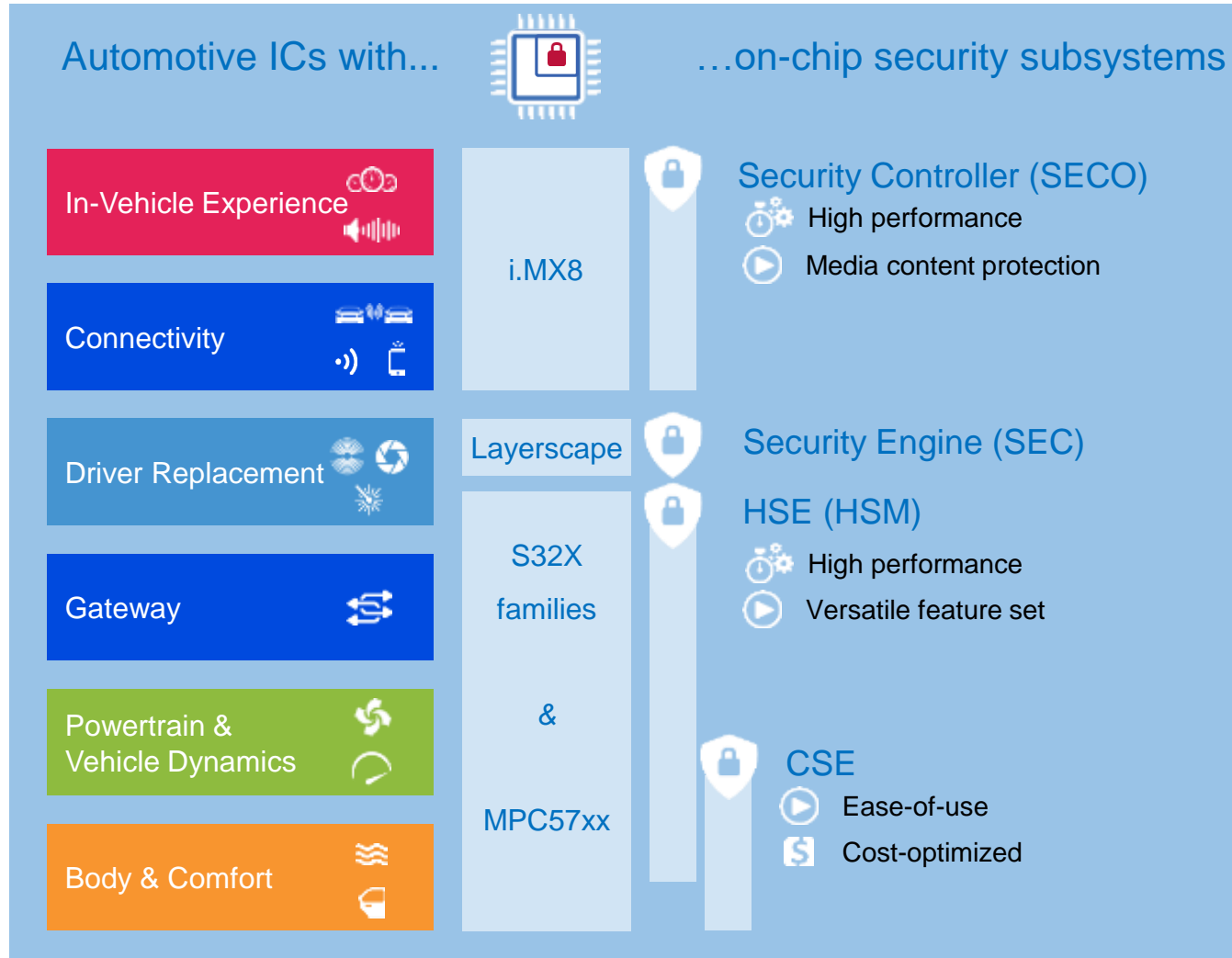


Function-specific Secure ICs

Fit-for-purpose security support



NXP's Automotive Security Solutions







Security companions

 **Secure Element (SE)**

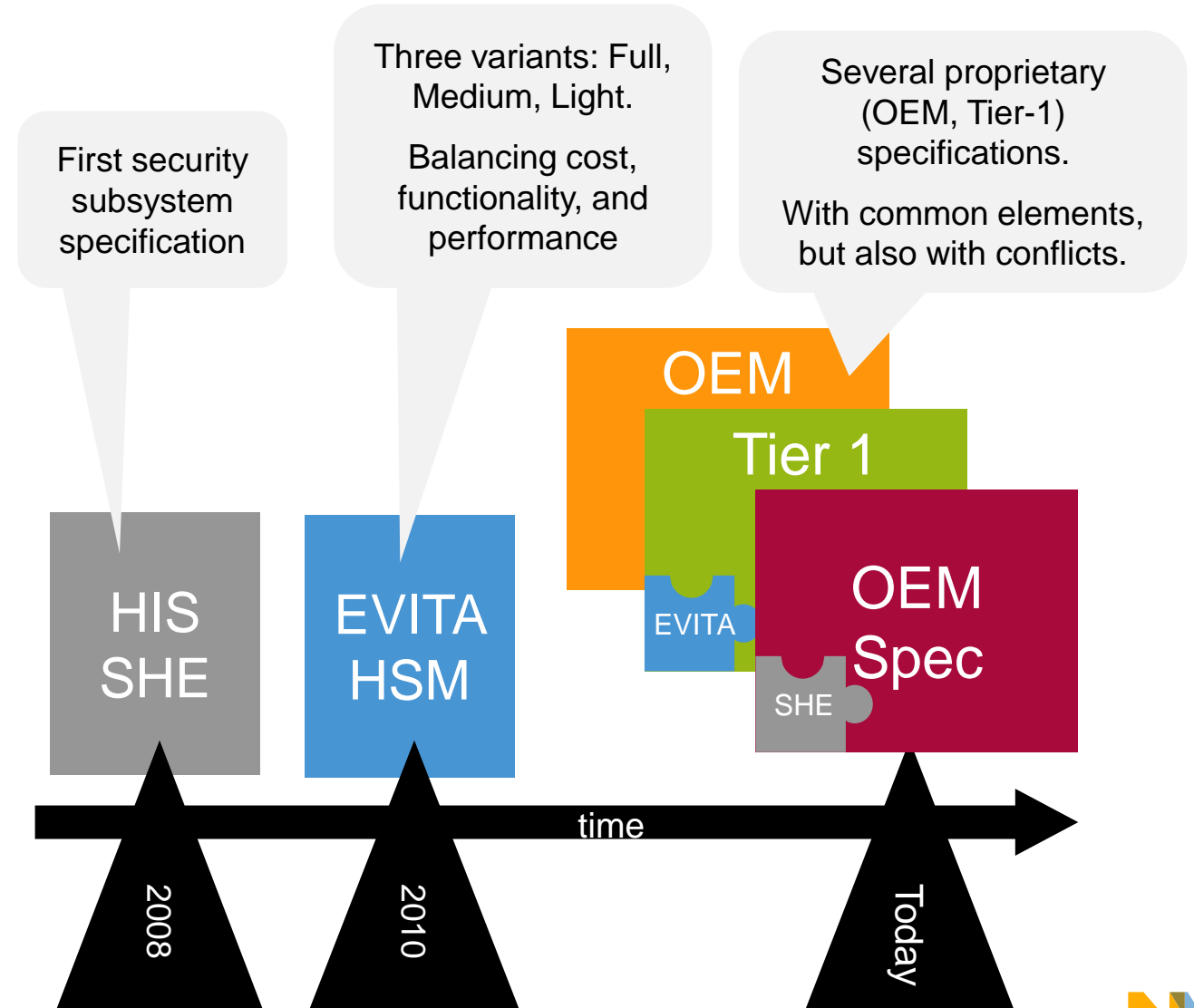
 Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

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

Automotive Security Specifications

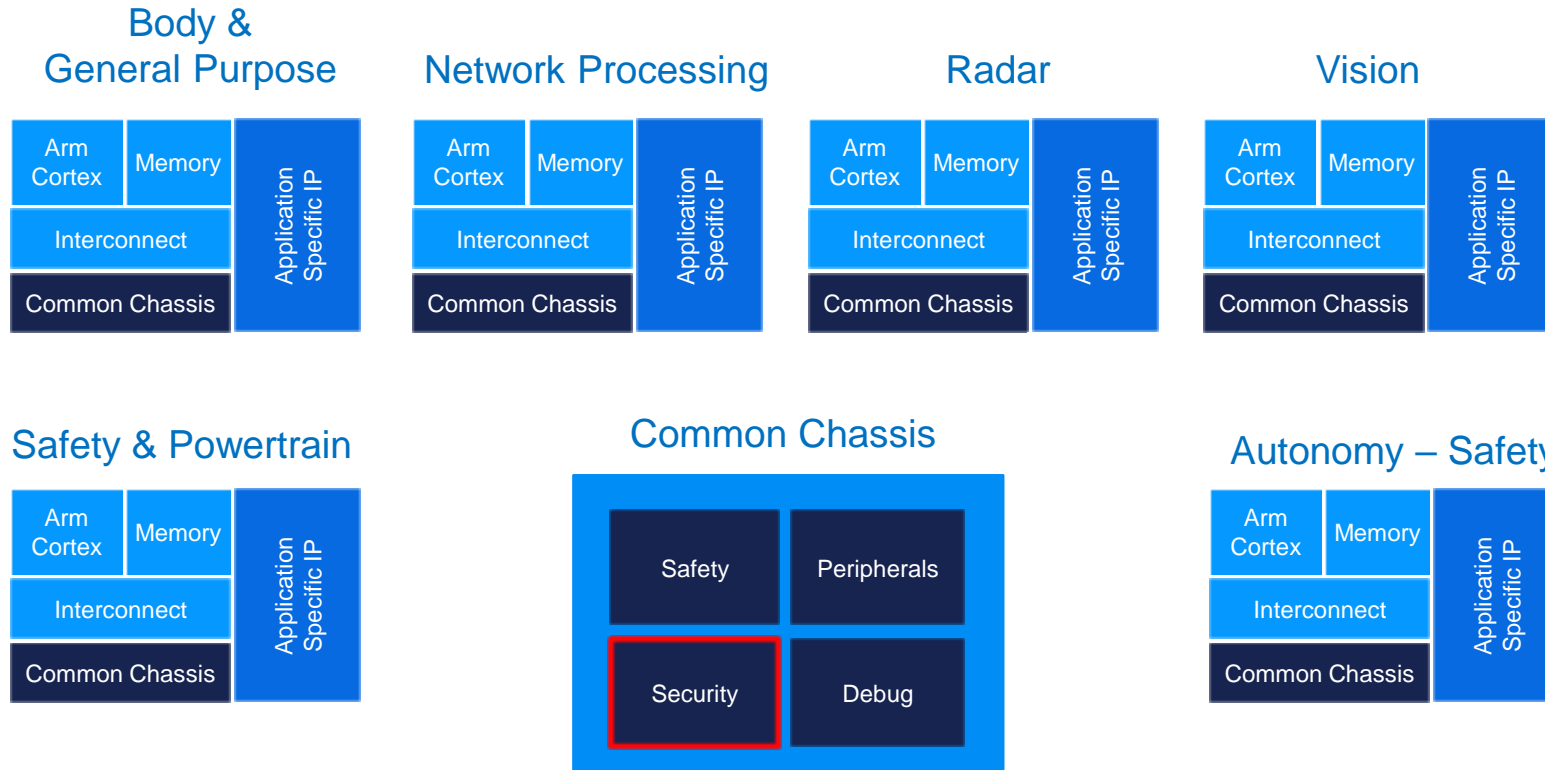
- The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem
- EVITA's HSM specification extended this concept into a programmable subsystem, in three flavors (Full, Medium, and Light), addressing a broader range of use cases
- Nowadays, OEMs are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



Security Requirements – Today's Landscape

| | SHE | EVITA (Light / Medium / Full) | More recent needs |
|---------------|---|---|---|
| Architecture | <ul style="list-style-type: none"> Configurable, fixed function | <ul style="list-style-type: none"> Programmable (except EVITA Light) | <ul style="list-style-type: none"> Acceleration close to the interfaces (CAN and ETH MAC/PHYs) Support for Flash-less technologies |
| Functionality | <ul style="list-style-type: none"> Secure boot Memory update protocol AES-128 (ECB, CBC) CMAC, AES-MP TRNG, PRNG Key derivation (fixed algorithm) 10+4 keys, key-usage flags | <p>Same as SHE, plus:</p> <ul style="list-style-type: none"> AES-PRNG monotonic counters (16x, 64bit) <p>Plus, for EVITA Medium and Full:</p> <ul style="list-style-type: none"> WHIRLPOOL, HMAC-SHA1, ECDH and ECDSA (P256) | <ul style="list-style-type: none"> Further crypto algorithms (e.g. RSA, SHA1-3, Curve25519, ...) Rollback protection Key negotiation protocols Communication protocol offloading (e.g. TLS, IPsec, MACsec, ...) Context separation / multi-application scenarios |
| Other | | | <ul style="list-style-type: none"> Increased attack resistance (e.g. SCA, Fault Injection, ...) |
| Covered by: |  CSE family (since 2010) | | |
| |  HSM family (since 2015) | | |
| |  HSE family (since 2019) | | |

Auto Processors Tomorrow – NXP’s Unique S32 Platform



Reduces SW R&D¹
by 35%

Unified HW with identical SW environment

10x the Performance²

Multiple real time OS
ADAS AI accelerators

Safe and Secure

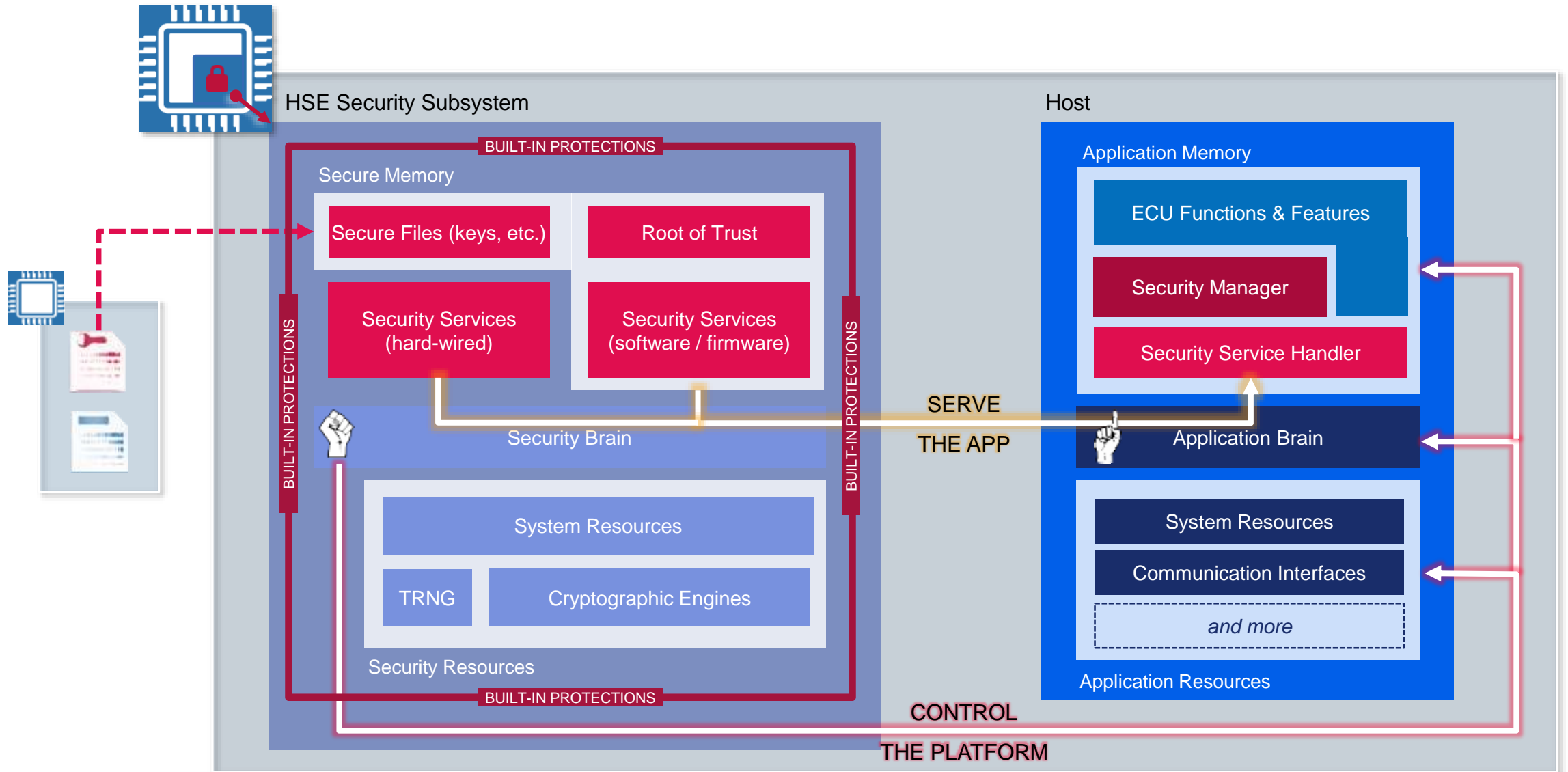
4 independent ASIL D paths
HW security engine
Ready for OTA

The World’s First Fully Scalable Safe Auto Compute Platform

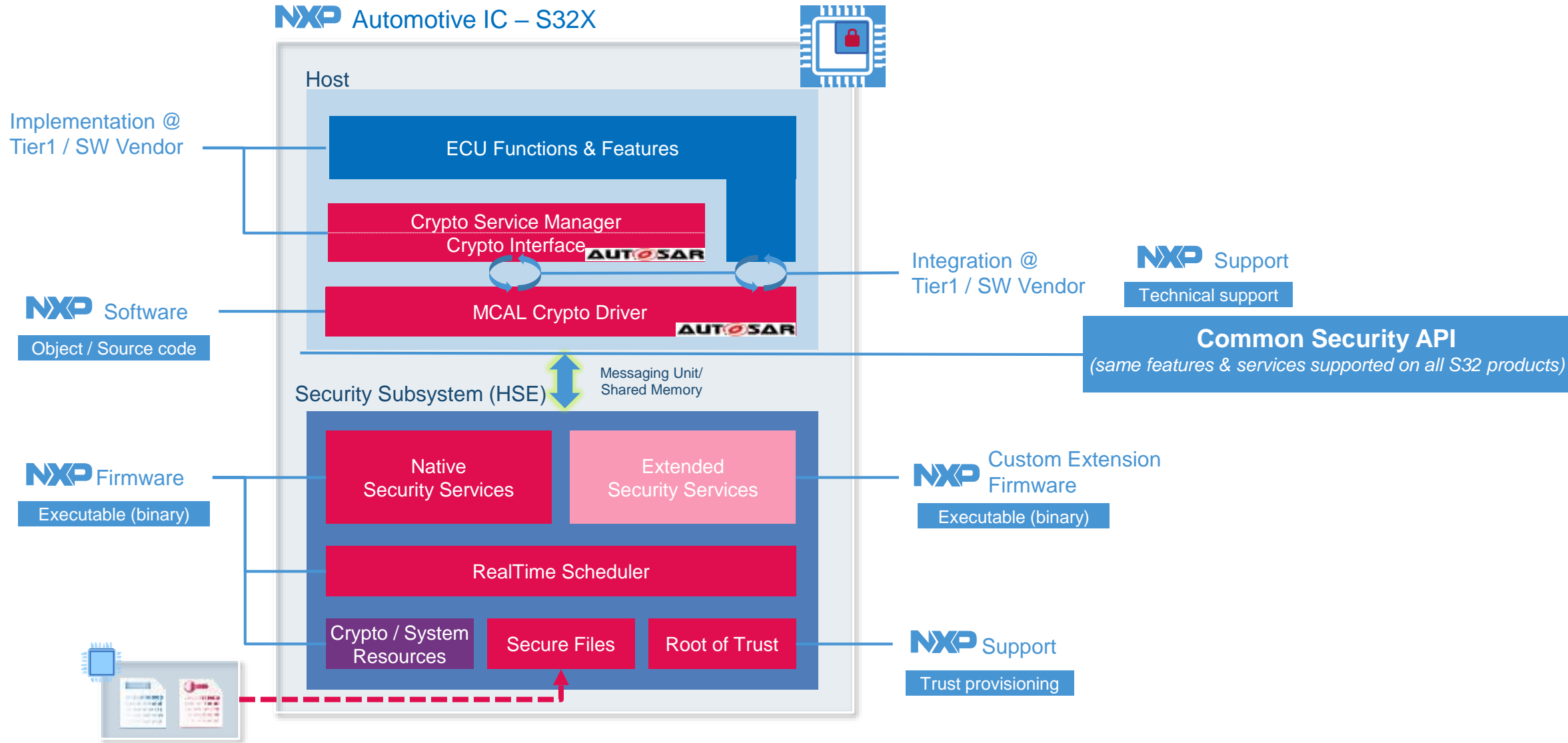
Unprecedented Design Win Pipeline → 1.5x of Previous Generations

1. Based on analysis of existing NXP Software code in existing customers’ applications
2. Based on publicly available competitor roadmap performance statements versus today’s best safe auto platform

S32 Hardware Security Engine (HSE) – System Overview



NXP's Security Software Components in Play



S32 HSE – More than a Cryptographic Engine

Accelerates

Cryptographic operations

Offloads

the app with a dedicated intelligence

Establishes Trust

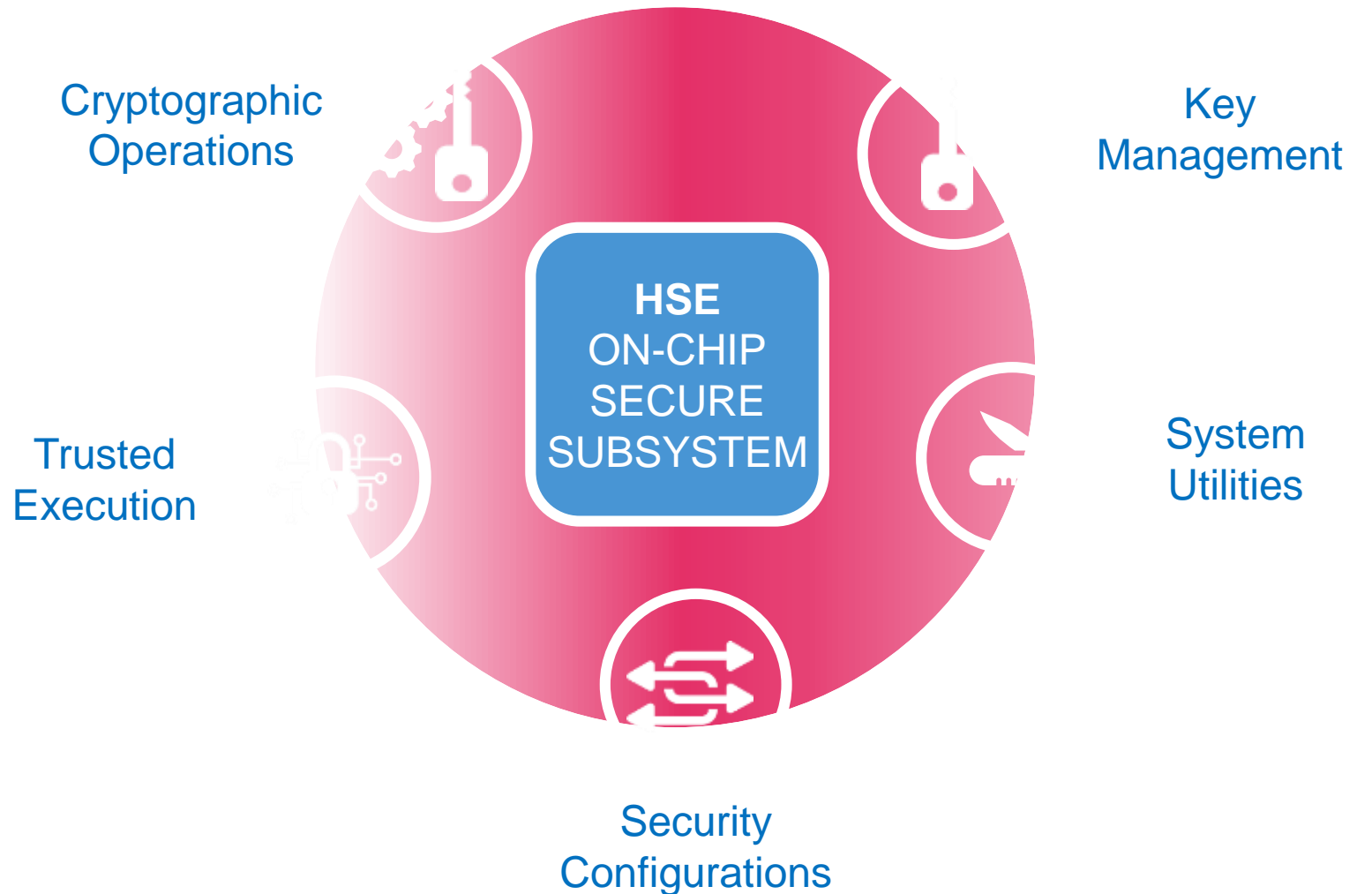
Secure Boot + Root of Trust

Controls

The platform

Easily Integrates

In your design



S32 HSE: Native Security 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

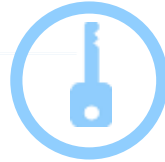
- System initialization & configuration
- Functional tests
- Security policy manager
- Service updates & extension

Secure network protocols

- SSL / TLS offload
- IPsec offload

S32 HSE: Service Examples

Key Management



Key file management

Key import

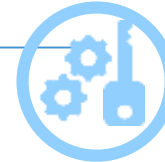
Key export

Key generation

Key derivation

Key exchange

Cryptographic Operations



AES
Encryption & decryption

CMAC/ HMAC
Generation & verification

RSA/ ECC signature
Generation & verification

RSA OAEP
Encryption & decryption

ECIES
Encryption & decryption

Random number
generation

Secure Boot Secure Use



Strict secure boot

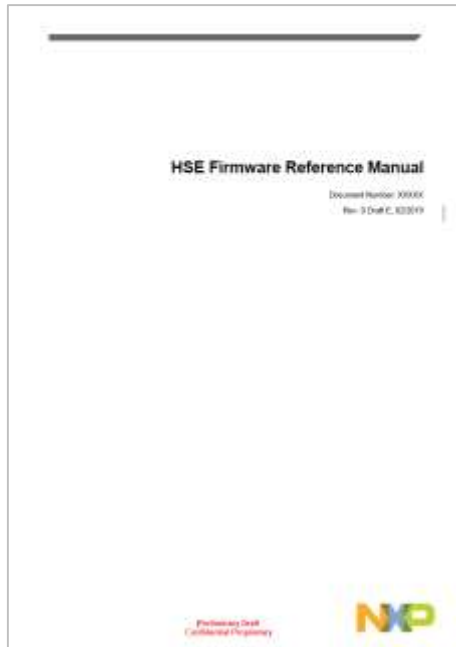
Parallel secure boot

On-demand verification

Configurable sanctions

S32 HSE: API Integration Support

Reference Manual detailing the HSE configuration & usage



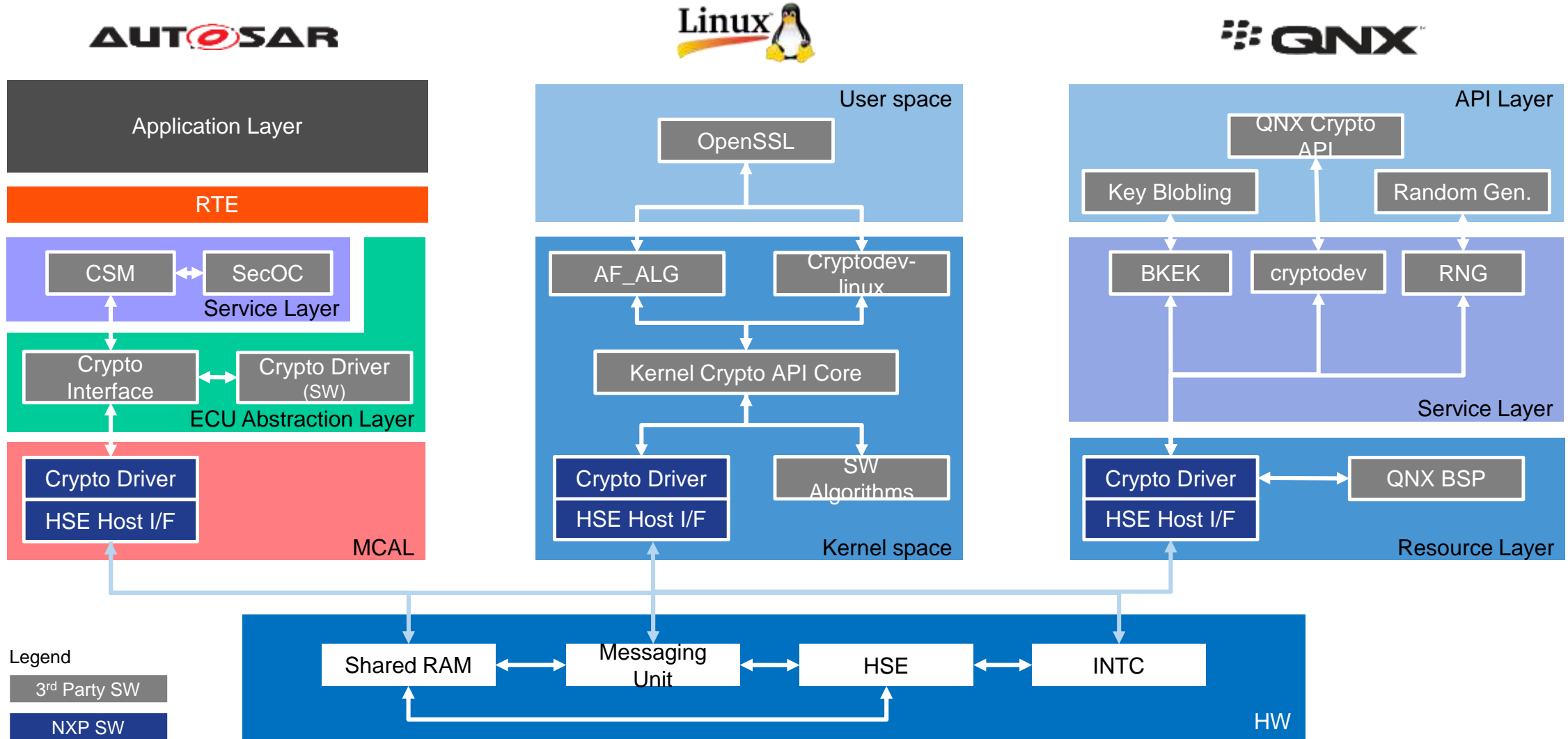
HSE API description available in HTML & PDF format

| Function Name | Return Type | Description |
|---------------|-------------|---|
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |
| accuconnect | void | API: Specifies the access mode: (0=NONE, 1=START, 2=UPDATE, 3=STOP) |

NXP HSE firmware (binary) & reference driver (source code)



Integrating NXP's HSE in Standard Security Stack



S32 HSE: Go-to-Market Strategy

NXP is committed to be a “one-stop shop” for its HSE solution

HSE solution = HW (HSE subsystem) + FW (HSE services)

Key Benefits

Best Performances
Best Security Assurance Level
Faster Time-to-Market
Low ASP

Extras

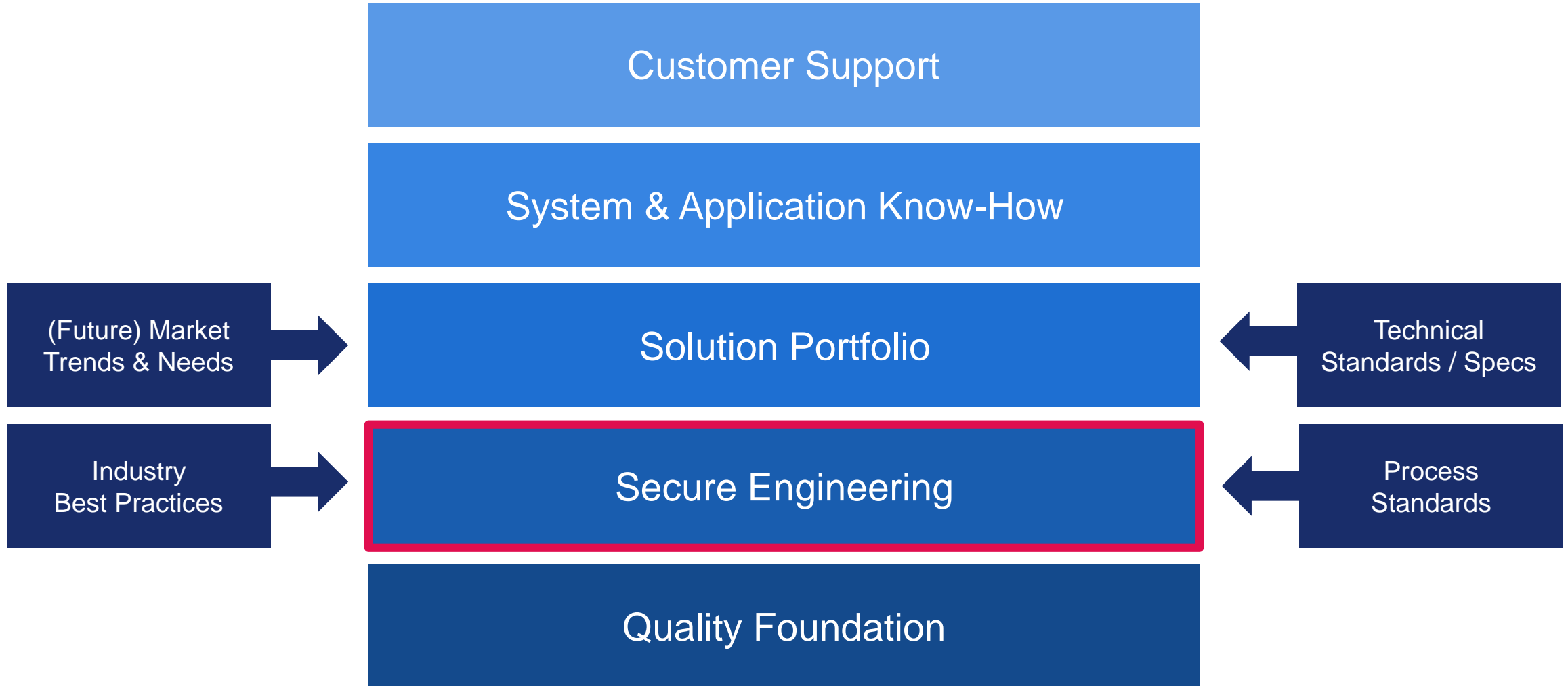
Seamless Integration
(Standard SW Stacks)
Custom Extensions When Necessary
In-Field Updatable

NXP's Approach to Automotive Security

Secure Engineering



NXP's Approach to Automotive Security



NXP's Automotive Cybersecurity Program

- Holistic approach to product security...
 - Broad portfolio of security solutions
 - Secure product engineering process
 - Internal / external security evaluation (VA)
 - Product security incident response team (PSIRT)
 - Security-aware organization (incl. training)
 - Threat intelligence feed
- ... and IT cyber security
 - CSO/ SOC
 - Information security policies
 - Computer security incident response team (CSIRT)
 - Site security (ISO 27001 cert.)

In collaboration with third parties

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



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



Conclusions

- 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
 - The **World's First Fully Scalable Safe Auto Compute Platform** with a **Hardware Security Engine (HSE)** optimized for different applications
 - Comprehensive, holistic, automotive cybersecurity program



SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com/automotivesecurity



**SECURE CONNECTIONS
FOR A SMARTER WORLD**