

# Next Generation Automotive Security Solutions

Marius Rotaru

Automotive Software Architect & Technical Director

---

October 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



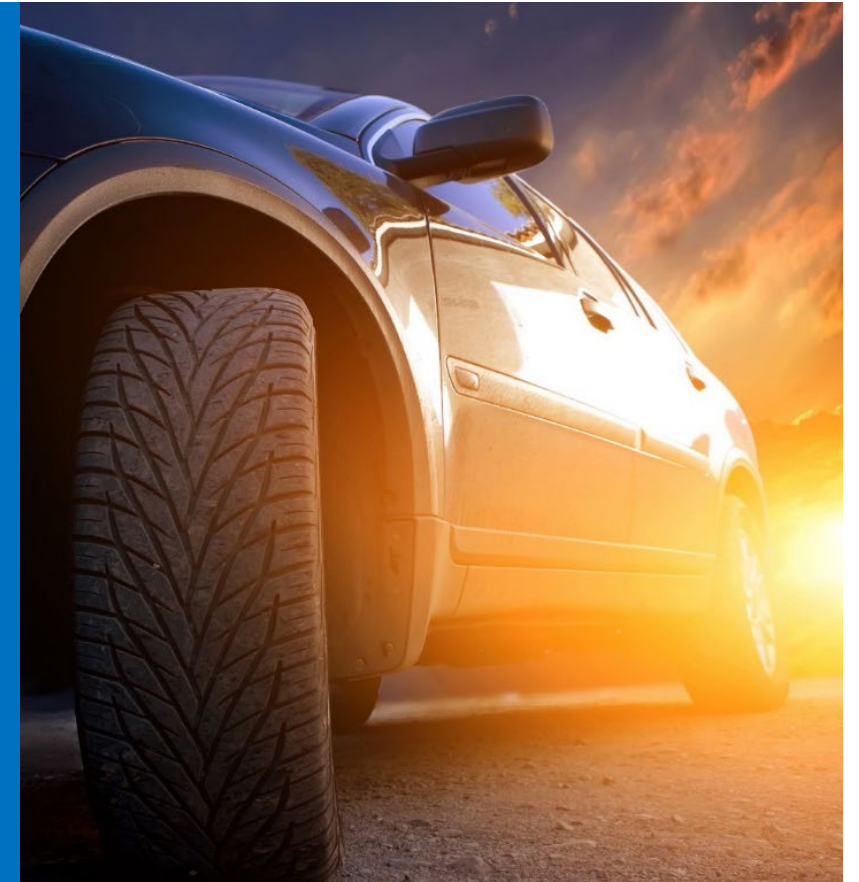
**2400+**  
AUTO  
ENGINEERS

**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

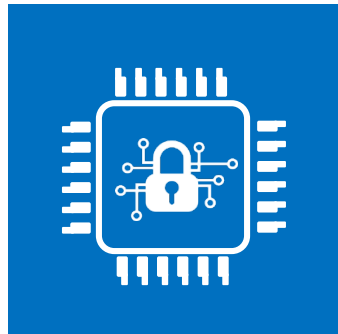
2018 Global Auto Semi Market: \$37.7B

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

# Functional Safety & Security – System-Level Concerns

IC-level Safety & Security Solutions



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

+

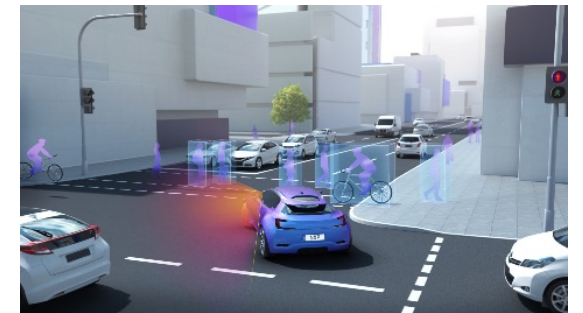
Safe & Secure Domain Architectures



- Domain isolation
- Firewalls
- Network intrusion detection

=

Safe and Secure Mobility



- Fail operational
- Resilient against cyber attacks

# NXP's Approach to Automotive Security

System & Application View



# NXP's Approach to Automotive Security

Customer Support

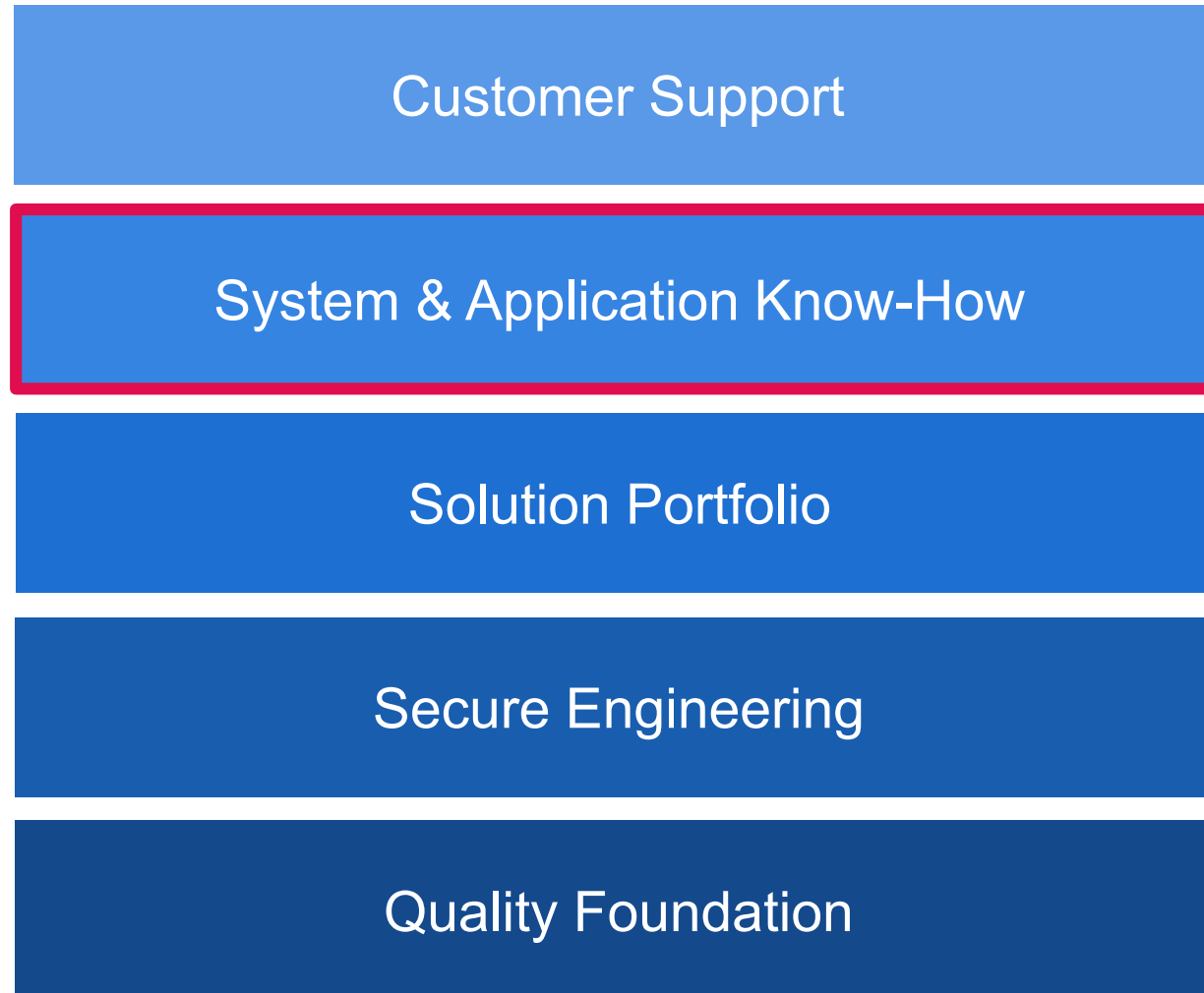
System & Application Know-How

Solution Portfolio

Secure Engineering

Quality Foundation

# NXP's Approach to Automotive Security



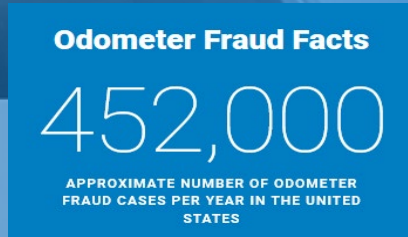


# Example of Cybersecurity Threats in Automotive

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



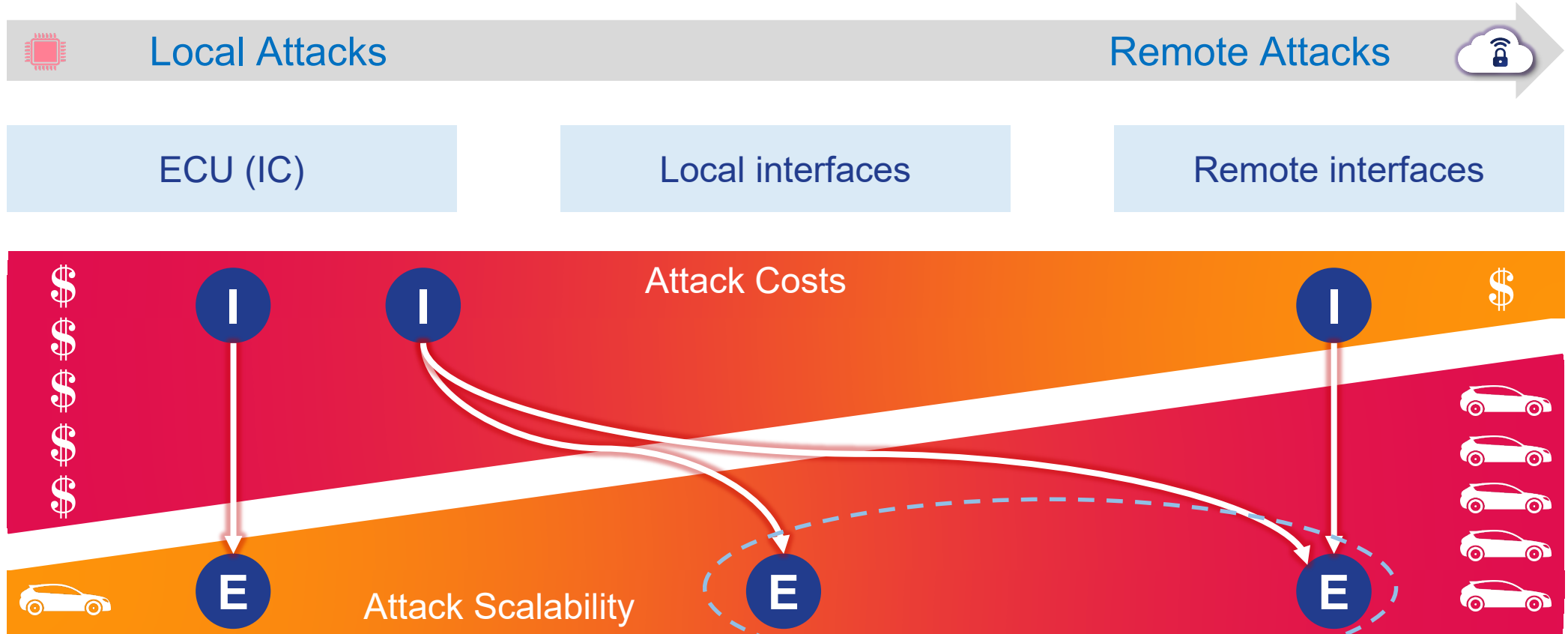
VDI Conference on IT Security for Vehicles (Berlin / July 2017)

Remote hack of an unaltered car (July 2015)



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

# Attack Costs vs. Attack Scalability

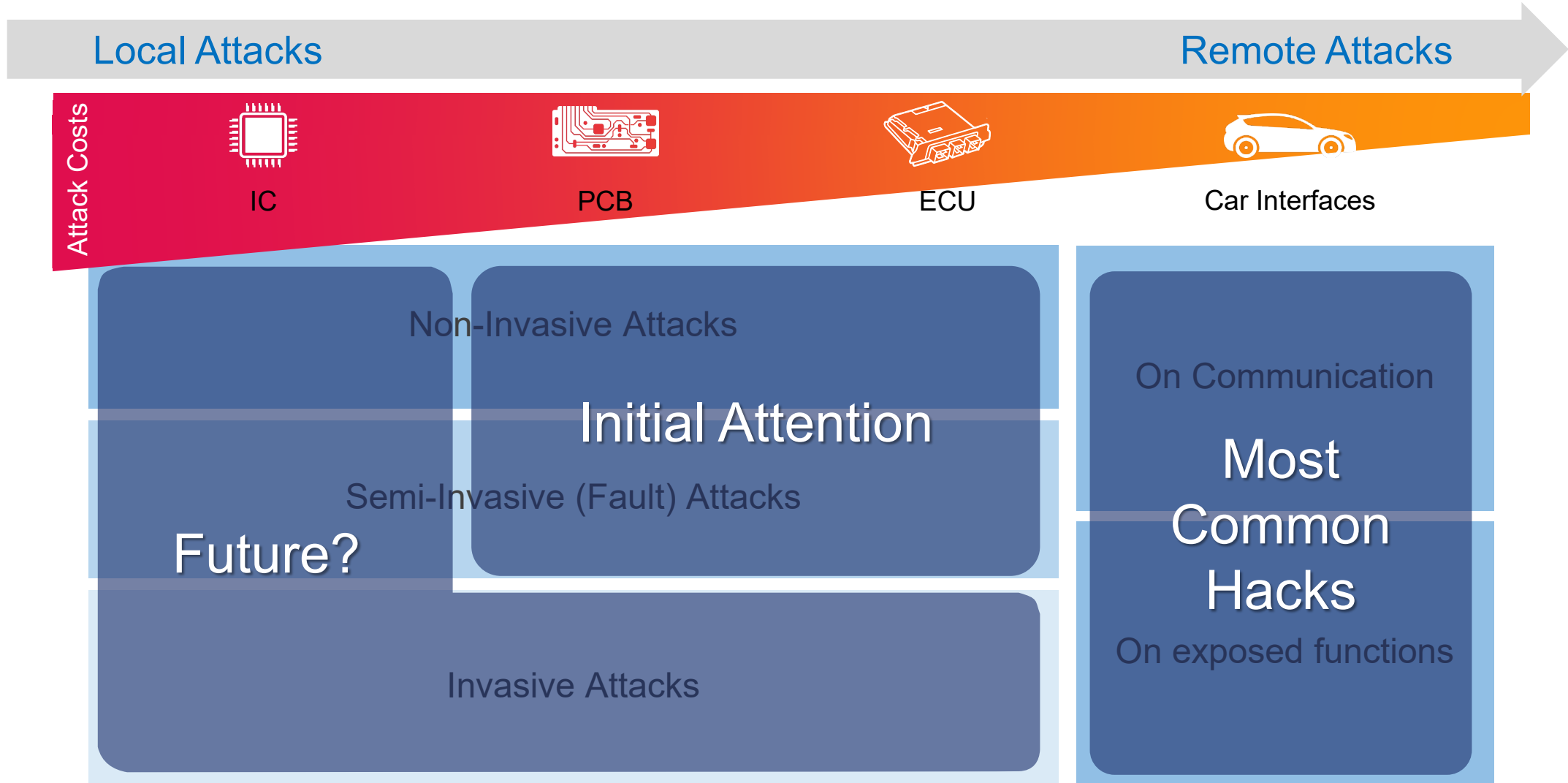


**I** Identify vulnerability

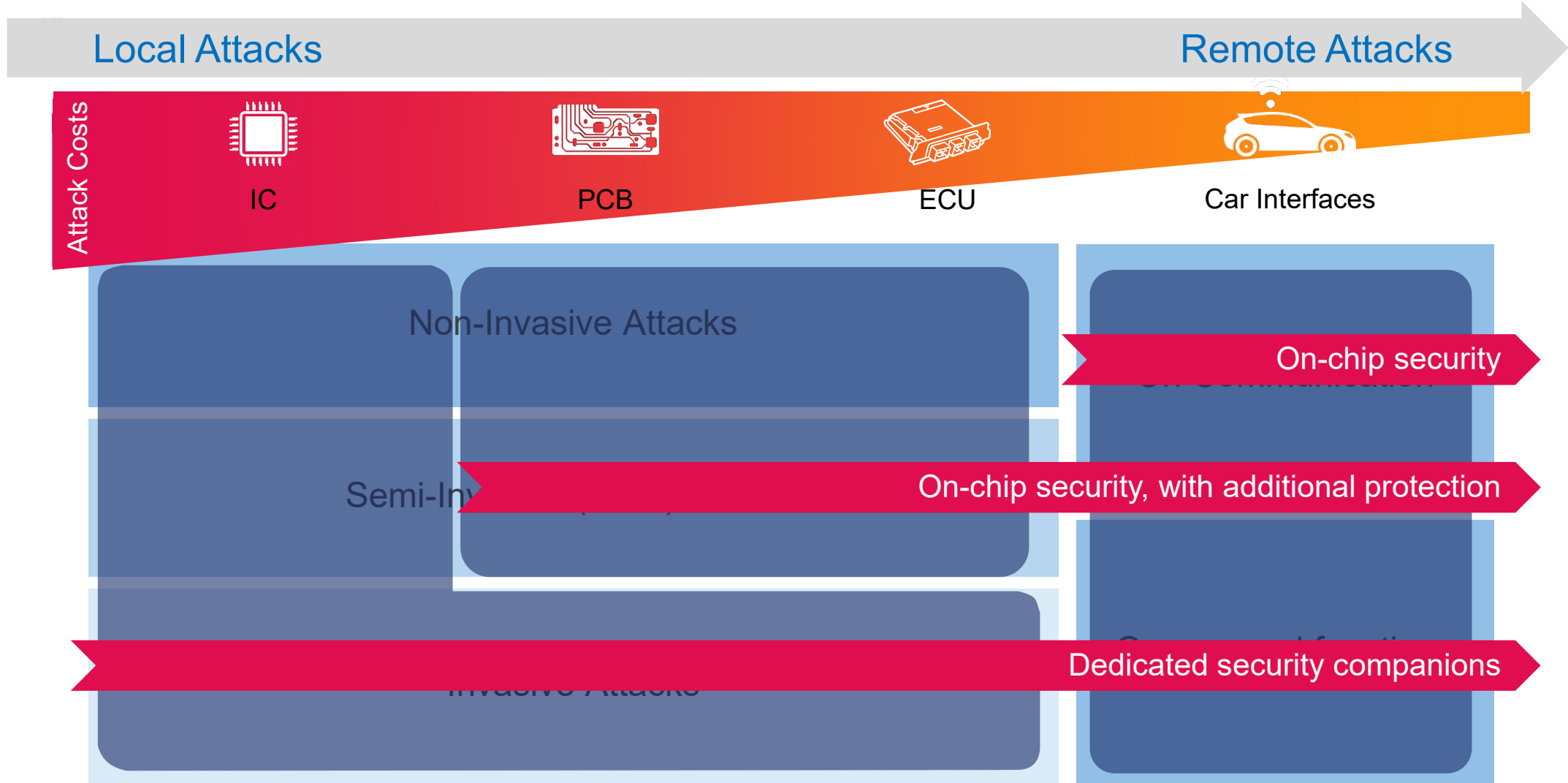
**E** Exploit vulnerability

Targets for criminal organizations  
(maximized rewards)

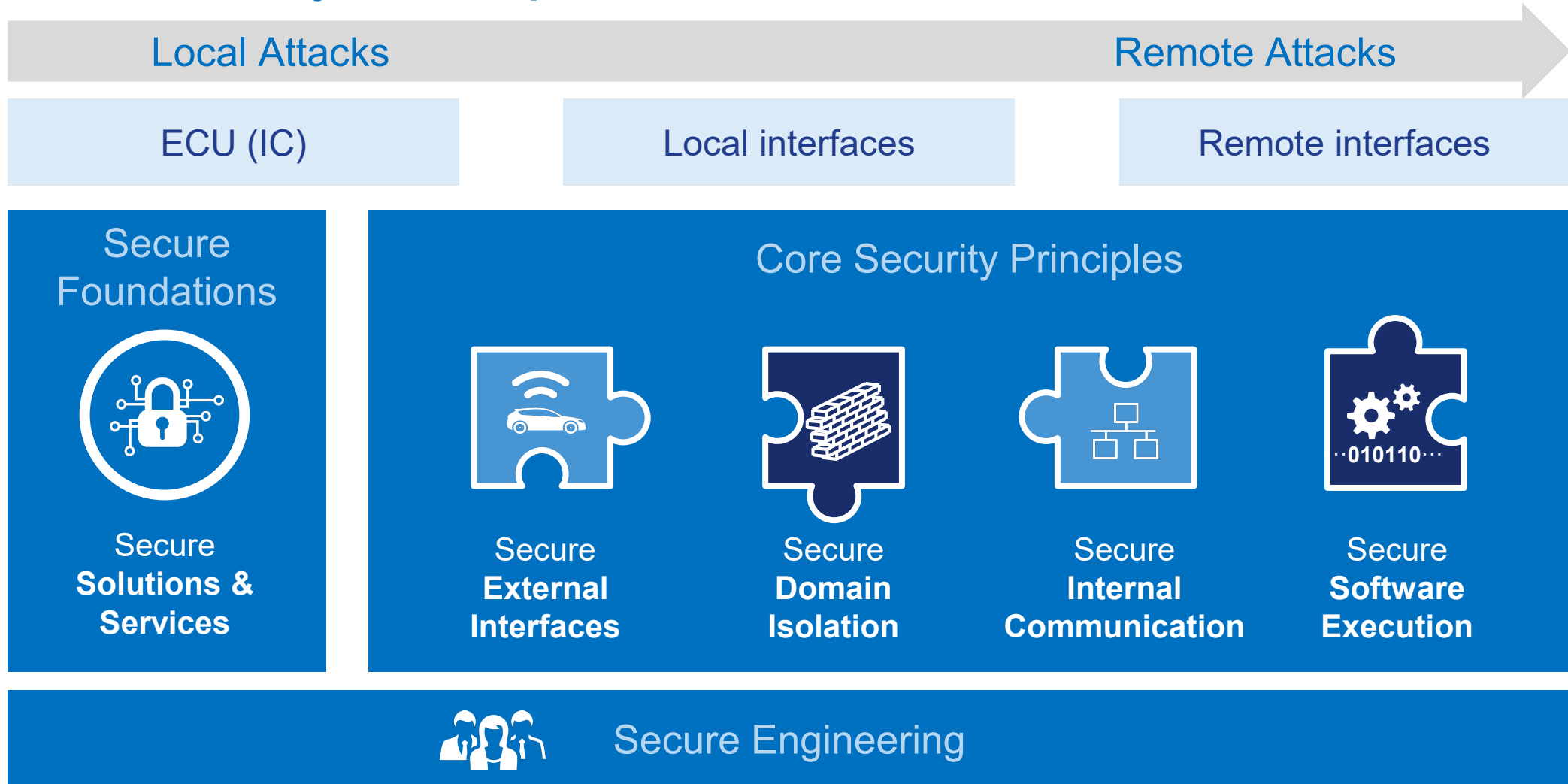
# Where to Focus?








# 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

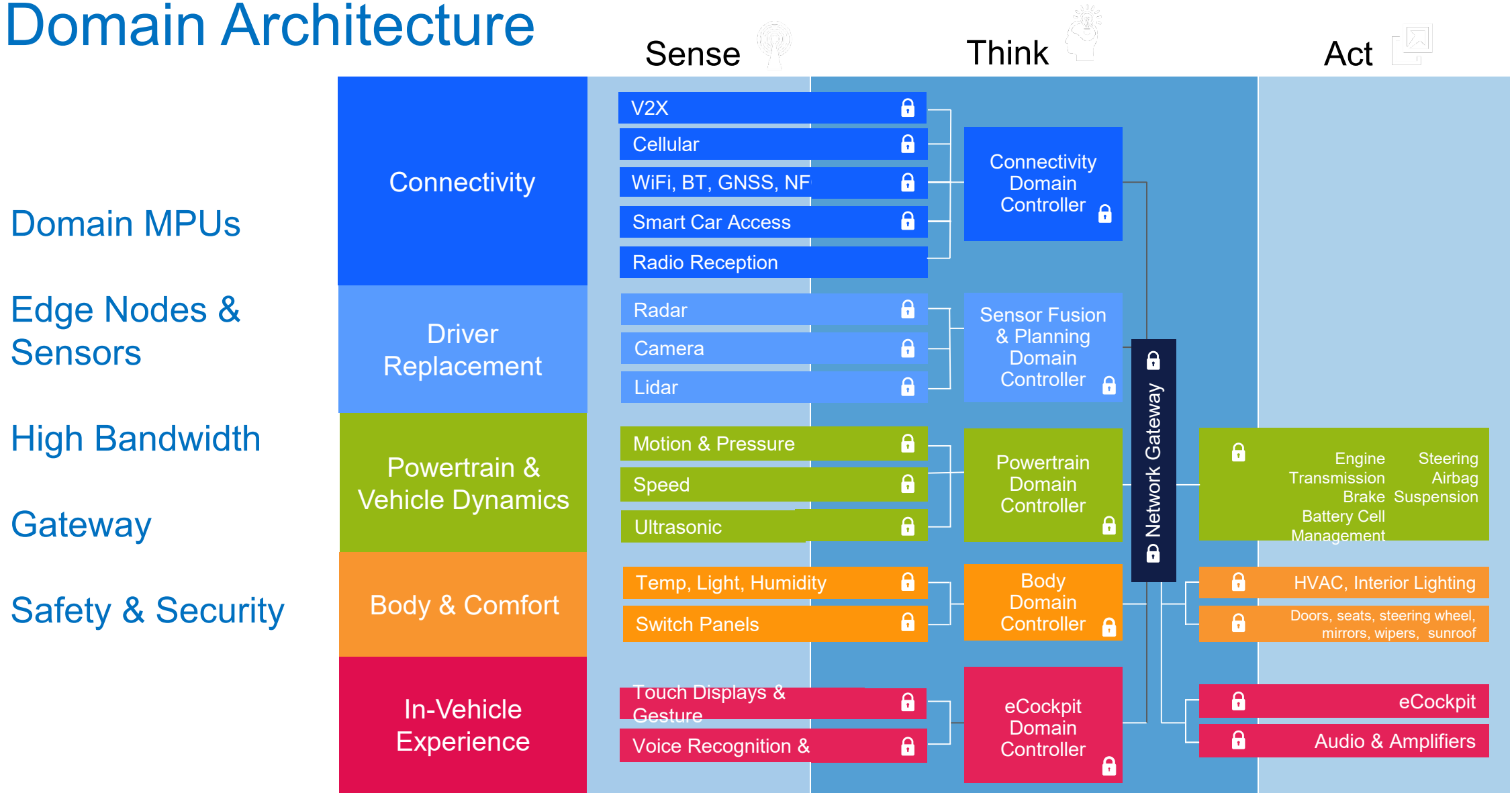


# NXP's Approach to Automotive Security






















# Domain Architecture





# NXP's Automotive Security Solutions

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









<p>In-Vehicle Experience </p>	i.MX8		<p><b>Security Controller (SECO)</b></p> <ul style="list-style-type: none"> <li> High performance</li> <li> Media content protection</li> </ul>
<p>Connectivity </p>	Layerscape		<p><b>Security Engine (SEC)</b></p>
<p>Driver Replacement </p>	S32X families		<p><b>HSE (HSM)</b></p> <ul style="list-style-type: none"> <li> High performance</li> <li> Versatile feature set</li> </ul>
<p>Gateway </p>	& MPC57xx		<p><b>CSE</b></p> <ul style="list-style-type: none"> <li> Ease-of-use</li> <li> Cost-optimized</li> </ul>
<p>Powertrain &amp; Vehicle Dynamics </p>			
<p>Body &amp; Comfort </p>			

**Security companions**

 **Secure Element (SE)**

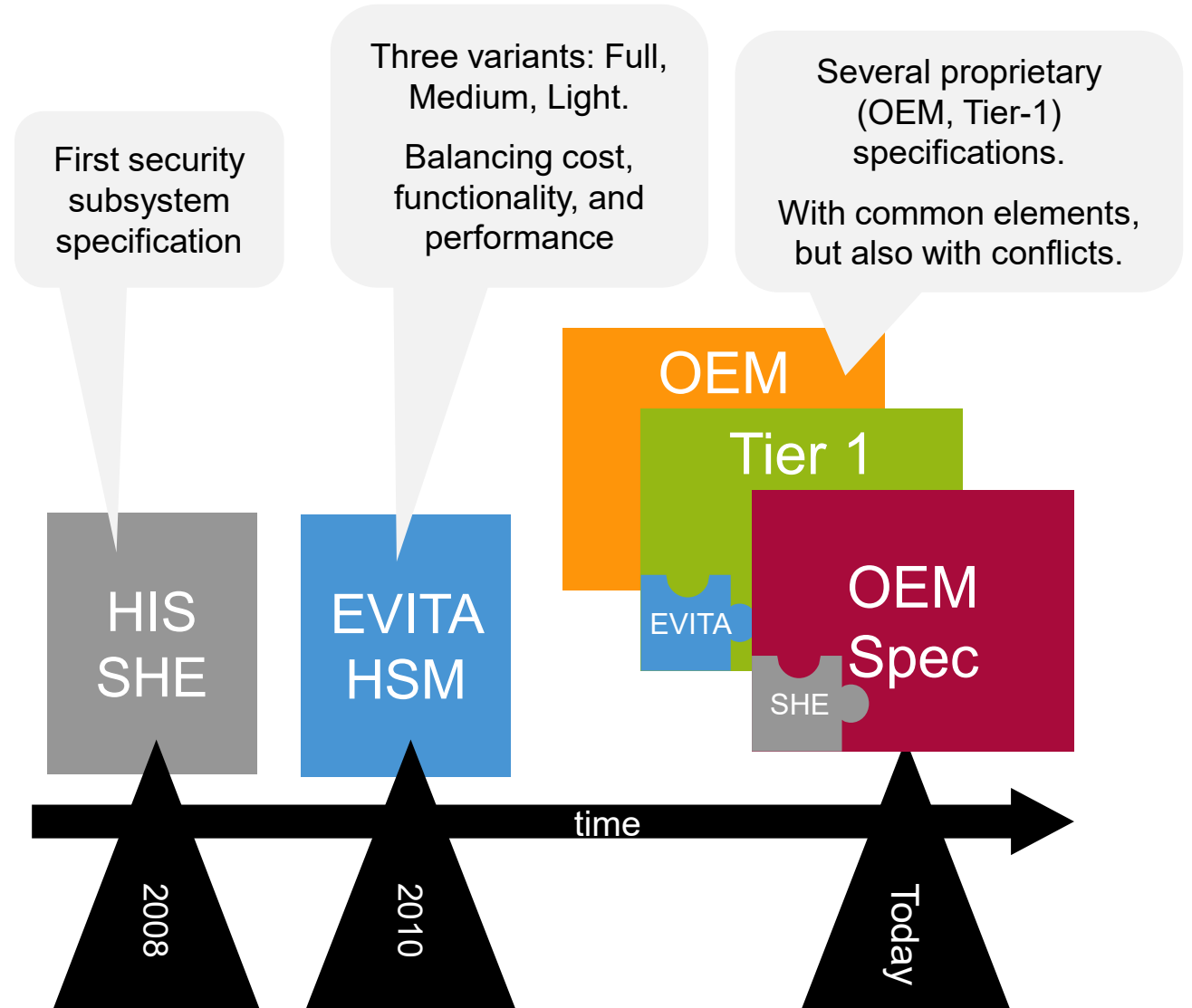
 Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

**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

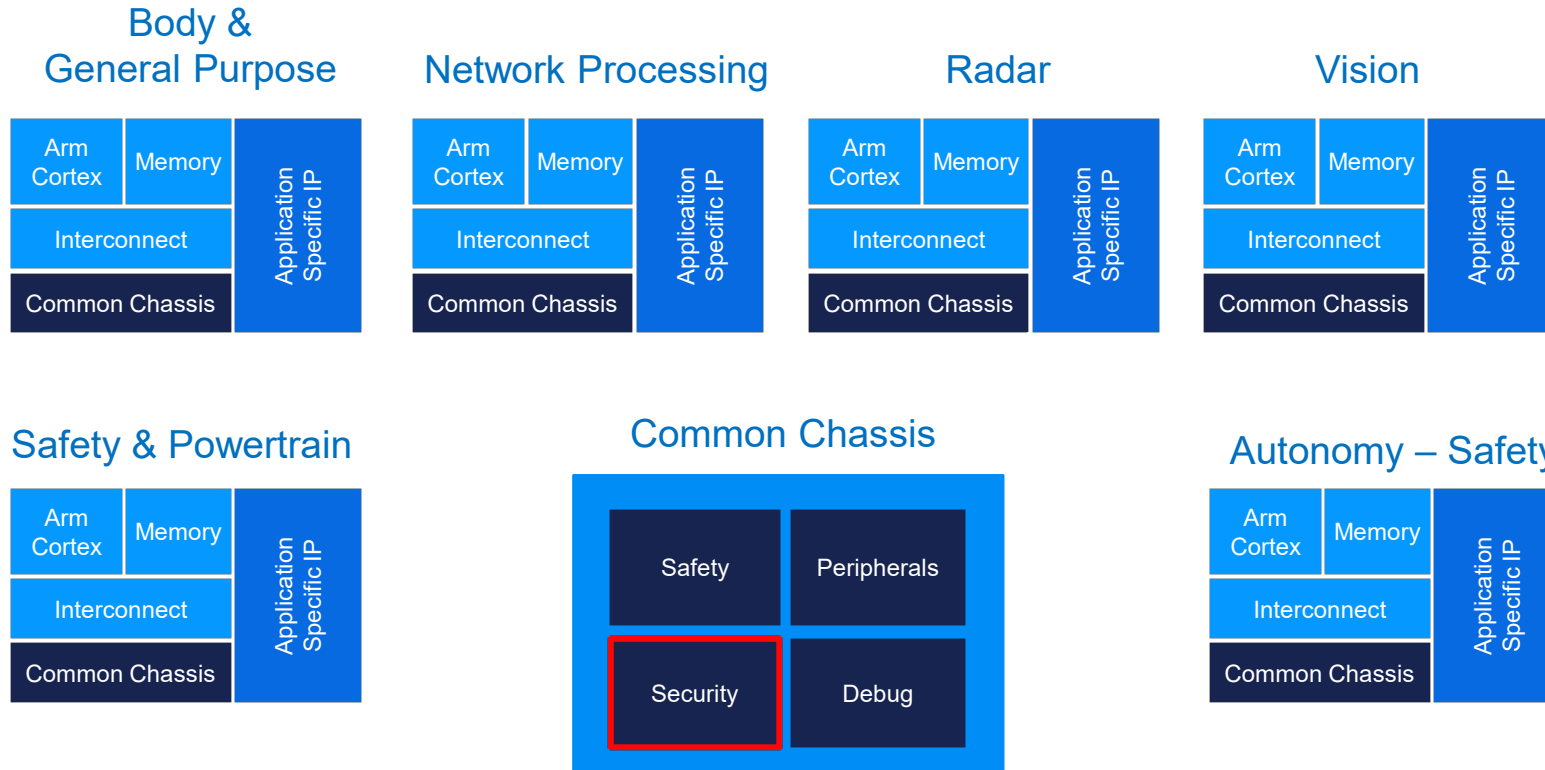
- The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem
- EVITA's HSM specification extended this concept into a programmable subsystem, in three flavors (Full, Medium, and Light), addressing a broader range of use cases
- Nowadays, OEMs are 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"> <li>Configurable, fixed function</li> </ul>	<ul style="list-style-type: none"> <li>Programmable (except EVITA Light)</li> </ul>	<ul style="list-style-type: none"> <li>Acceleration close to the interfaces (CAN and ETH MAC/PHYs)</li> <li>Support for Flash-less technologies</li> </ul>
Functionality	<ul style="list-style-type: none"> <li>Secure boot</li> <li>Memory update protocol</li> <li>AES-128 (ECB, CBC)</li> <li>CMAC, AES-MP</li> <li>TRNG, PRNG</li> <li>Key derivation (fixed algorithm)</li> <li>10+4 keys, key-usage flags</li> </ul>	<p>Same as SHE, plus:</p> <ul style="list-style-type: none"> <li>AES-PRNG</li> <li>monotonic counters (16x, 64bit)</li> </ul> <p>Plus, for EVITA Medium and Full:</p> <ul style="list-style-type: none"> <li>WHIRLPOOL, HMAC-SHA1, ECDH and ECDSA (P256)</li> </ul>	<ul style="list-style-type: none"> <li>Further crypto algorithms (e.g. RSA, SHA1-3, Curve25519, ...)</li> <li>Rollback protection</li> <li>Key negotiation protocols</li> <li>Communication protocol offloading (e.g. TLS, IPsec, MACsec, ...)</li> <li>Context separation / multi-application scenarios</li> </ul>
Other			<ul style="list-style-type: none"> <li>Increased attack resistance (e.g. SCA, Fault Injection, ...)</li> </ul>
Covered by:	<p><b>NXP</b> CSE family (since 2010)</p> <p><b>NXP</b> HSM family (since 2015)</p> <p><b>NXP</b> HSE family (since 2019)</p>		

# Auto Processors Tomorrow – NXP’s Unique S32 Platform



Reduces SW R&D<sup>1</sup>  
by 35%

Unified HW with identical SW environment

10x the Performance<sup>2</sup>

Multiple real time OS  
ADAS AI accelerators

Safe and Secure

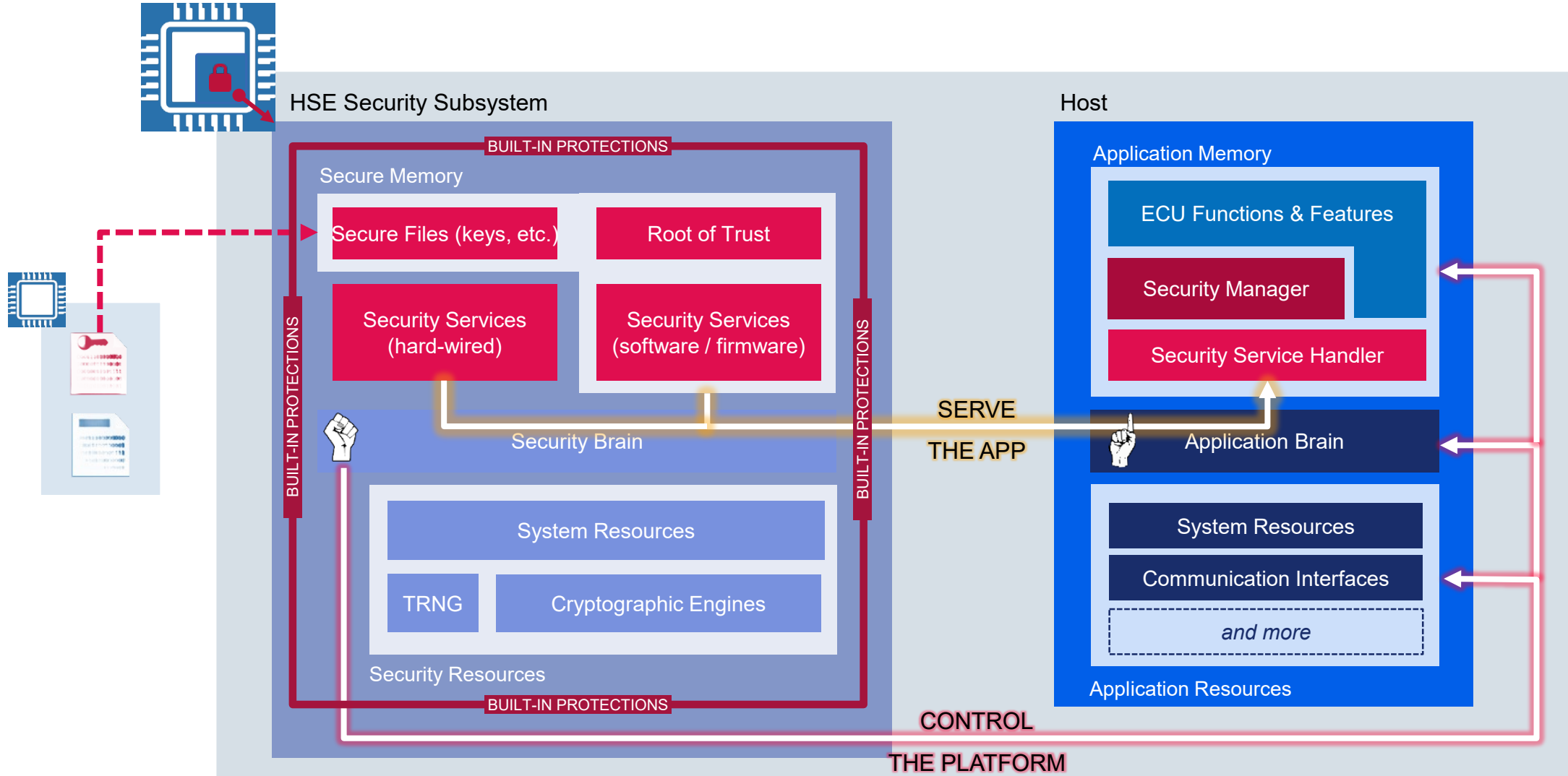
4 independent ASIL D paths  
HW security engine  
Ready for OTA

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



# S32 HSE – More than a Cryptographic Engine

## Accelerates

Cryptographic operations

## Offloads

the app with a dedicated intelligence

## Establishes Trust

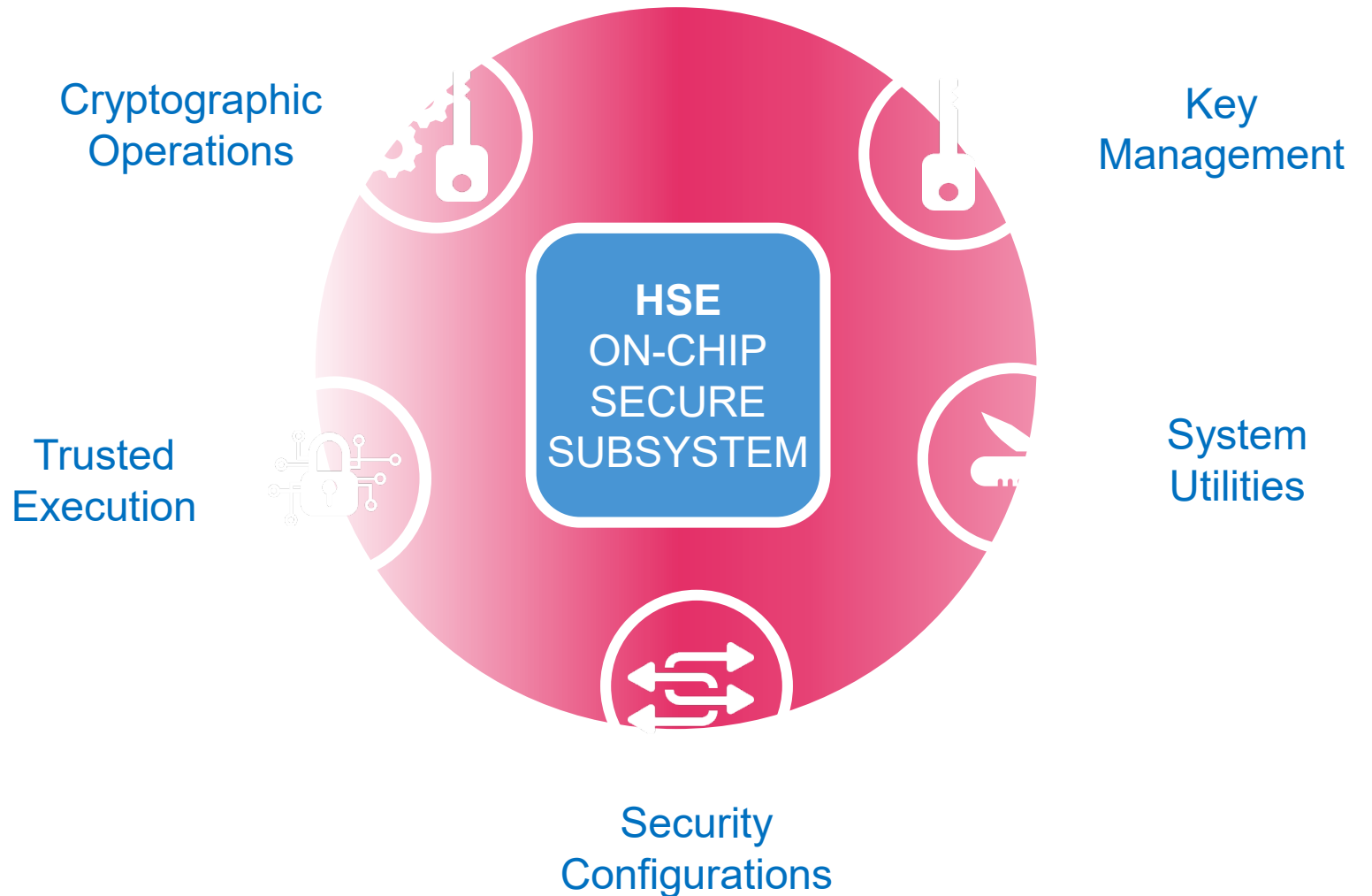
Secure Boot + Root of Trust

## Controls

The platform

## Easily Integrates

In your design



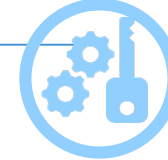
# S32 HSE: Service Examples

## 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

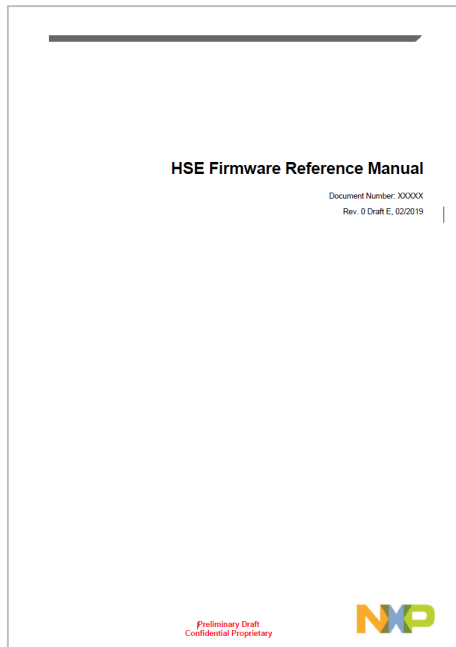


# S32 HSE: API Integration Support

Reference Manual detailing the HSE configuration & usage

HSE API description available in HTML & PDF format

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

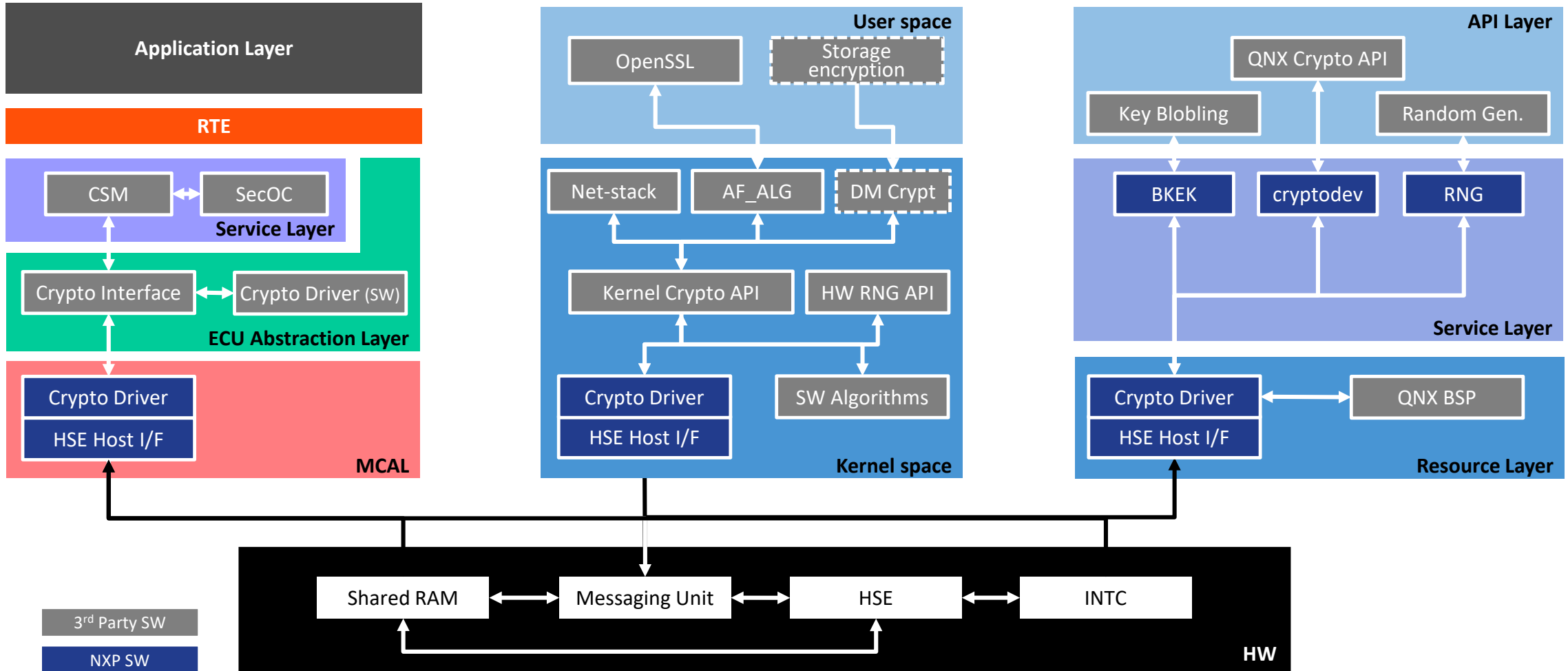


**NXP HSE Interface** Rev0.1  
NXP Semiconductors

<b>hseAccessMode_t</b>	accessMode	INPUT: Specifies the access mode: ONE-PASS, START, UPDATE, FINISH. STREAMING USAGE: MANDATORY for all steps.
uint32_t	streamId	INPUT: Specifies the stream to use for START, UPDATE, FINISH access modes. Each interface supports a limited number of streams per interface, up to HSE_STREAM_COUNT. STREAMING USAGE: MANDATORY for all steps.
<b>hseMacScheme_t</b>	macScheme	INPUT: Specifies the MAC scheme. STREAMING USAGE: MANDATORY for all steps.
<b>hseAuthDir_t</b>	authDir	INPUT: Specifies the direction: generate/verify. STREAMING USAGE: MANDATORY for all steps.
<b>hseKeyHandle_t</b>	keyHandle	INPUT: The key to be used for the operation. + For HMAC, key-sizes greater than hash algorithm block-size are not supported (Limitation). STREAMING USAGE: MANDATORY for START step.
uint32_t	inputLength	INPUT: Length of the input message. Can be zero. STREAMING USAGE: + START: Must be a multiple of block length (for HMAC-hash or AES). Cannot be zero for HMAC. + UPDATE: Must be a multiple of block length (for HMAC-hash or AES). Cannot be zero. Skip instead of passing zero. + FINISH: Can be any value (for CMAC & XCBC-MAC, zero length is invalid).
<b>HOST_ADDR</b>	pinput	INPUT: The input message. NOTE: The input message for GMAC is the AAD (as specified by AEAD-GCM). STREAMING USAGE: MANDATORY for UPDATE and FINISH.
<b>HOST_ADDR</b>	pTagLength	INPUT/OUTPUT: Holds the address to a memory location (an uint32_t variable) in which the tag length in bytes is stored. + GENERATE: + On calling service (input), this parameter shall contain the size of the buffer provided by pTag. + For GMAC, valid tag lengths are 4, 8, 12, 13, 14, 15 and 16. Tag-lengths greater than 16 will be truncated to 16. + For HMAC, valid tag lengths are [1, hash-length]. Tag-lengths greater than hash-length will be truncated to hash-length. + For CMAC & XCBC-MAC, valid tag lengths are [4, cipher-block-length]. Tag-lengths greater than cipher-block-length will be truncated to cipher-block-length. + When the request has finished (output), the actual length of the returned value shall be stored. + VERIFY: + On calling service (input), this parameter shall contain the tag-length to be verified. + For GMAC, valid tag lengths are 4, 8, 12, 13, 14, 15 and 16. + For HMAC, valid tag lengths are [1, hash-length]. + For CMAC & XCBC-MAC, valid tag lengths are [4, cipher-block-length]. STREAMING USAGE: MANDATORY for FINISH.
<b>HOST_ADDR</b>	pTag	OUTPUT/INPUT: The output tag for "generate"; the input tag for "verify". STREAMING USAGE: MANDATORY for FINISH.



# 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

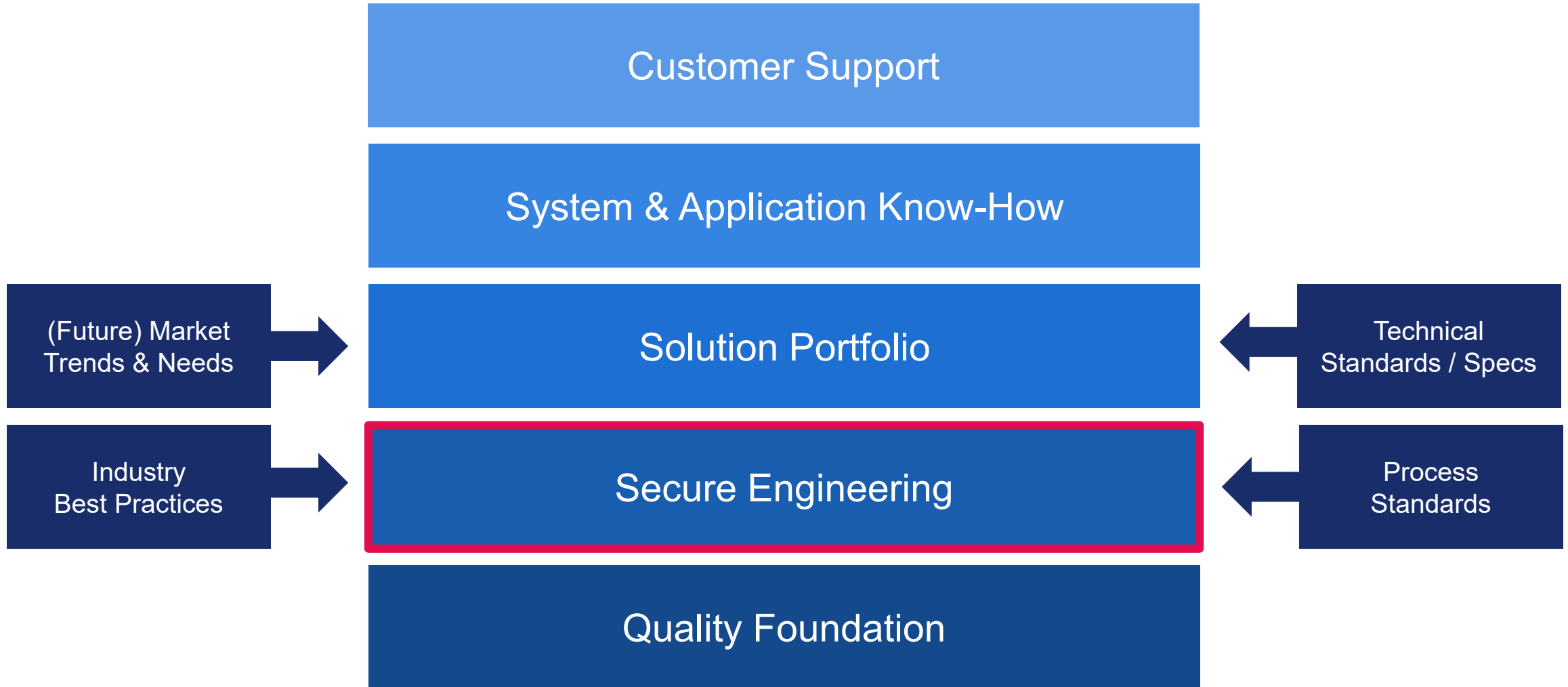
Seamless Integration  
(Standard SW Stacks)  
Custom Extensions When Necessary  
In-Field Updatable

# 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

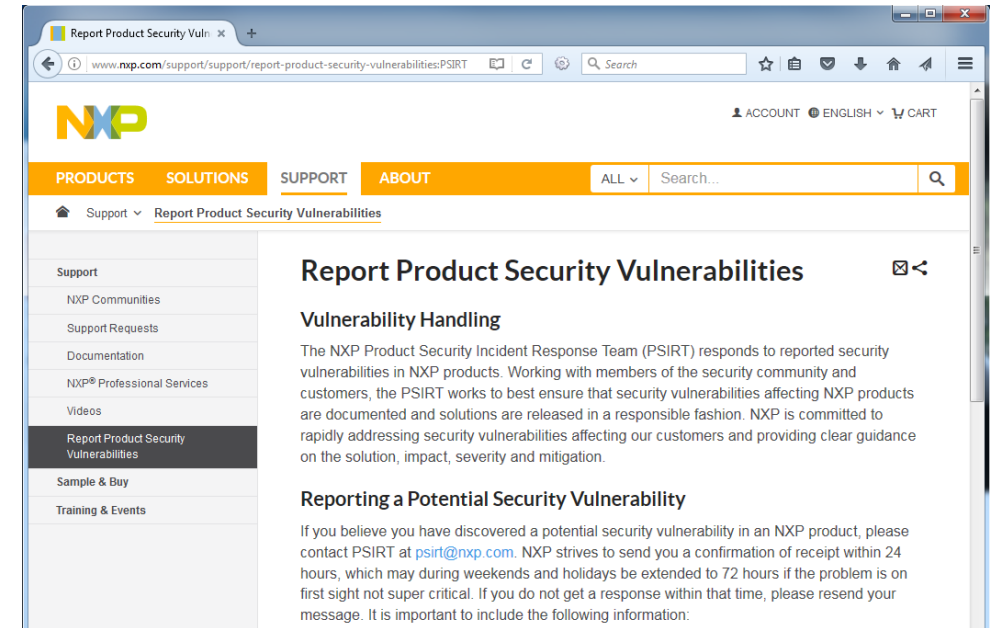
Global across products / markets / regions  
Established in 2008 after the MIFARE Classic hack

## 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](http://www.nxp.com/automotivesecurity)





**SECURE CONNECTIONS  
FOR A SMARTER WORLD**