NXP AUTOMOTIVE CYBER SECURITY

JOHN COTNER

SECURITY ARCHITECT - AUTOMOTIVE

AMF-AUT-T2694 | JUNE 2017

SECURE CONNECTIONS
FOR A SMARTER WORLD

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: Those that have been hacked and will be again."

- Robert Mueller, sixth director of the FBI

"A system is *good* if it does what it's supposed to do and *secure* if it doesn't do anything else."

- Dr. Eugene "Spaf" Spafford, Purdue

THE NEED FOR AUTOMOTIVE CYBERSECURITY

DID YOU KNOW?

>10

Vehicle hacks
published since 2015

1.4M

Vehicle recalled
in the largest
incident to date

Why hacking?

Valuable Data
attracts hackers

Gigabytes of data generated per vehicle, each day

Why is it possible?

High System Complexity
implies high vulnerability

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

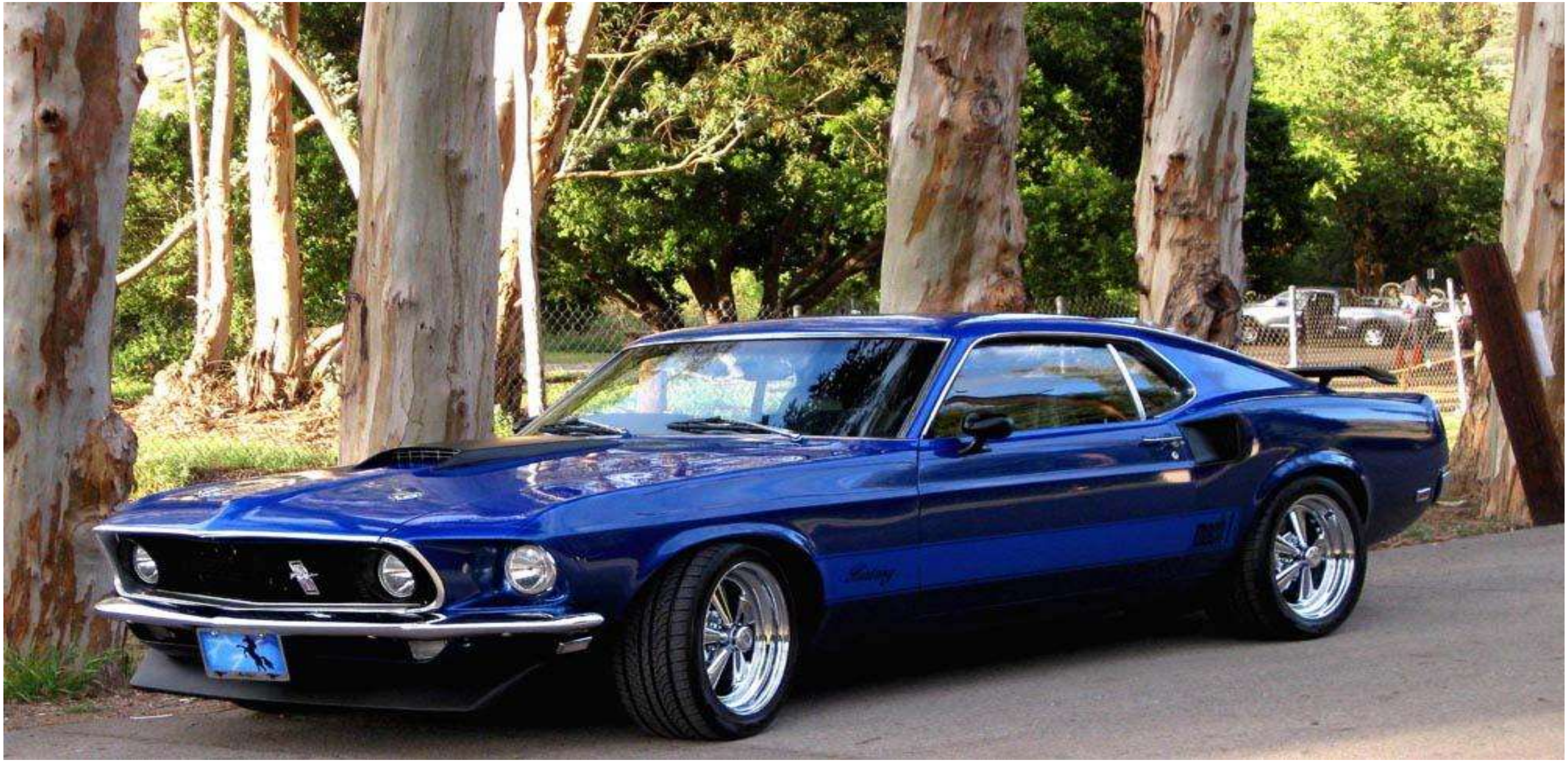
Why now?

Wireless Interfaces
enable scalable attacks

250M connected vehicles on the road in 2020

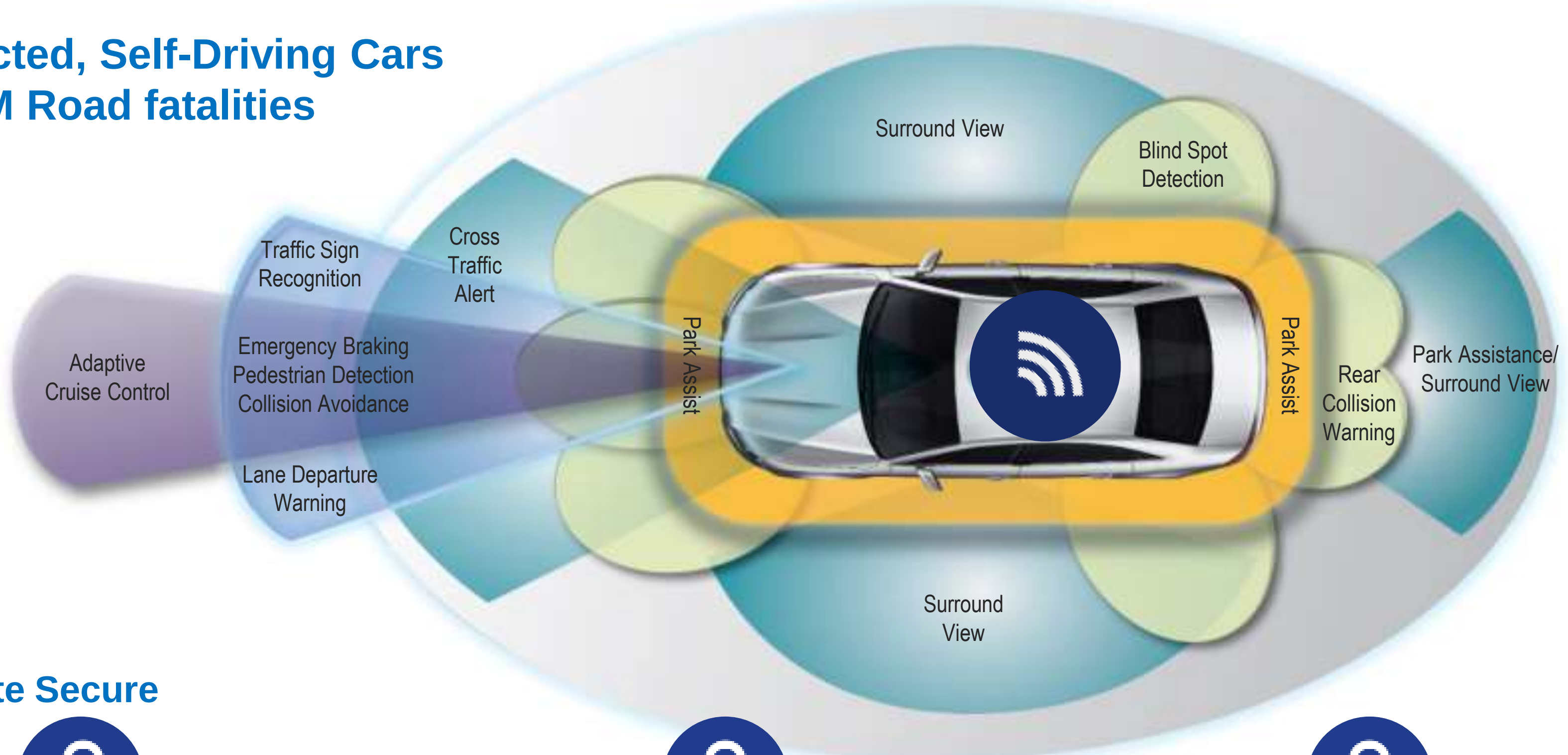
SECURITY IS A MUST-HAVE FOR CONNECTED & AUTONOMOUS VEHICLES

DEFENSE?



Enabling the **Secure** Connected Car

Secure Connected, Self-Driving Cars will Save >1.3M Road fatalities globally

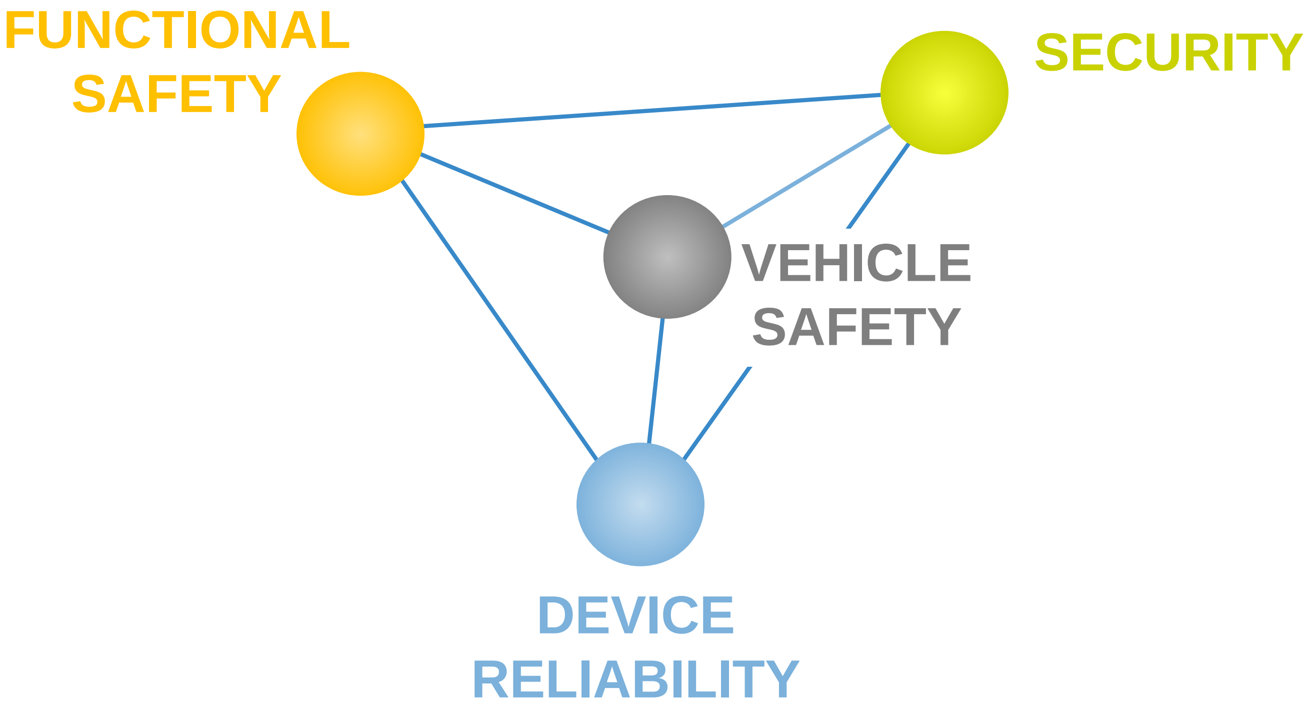


NXP Offers Complete Secure ADAS System….

…including Big Data Infrastructure

SENSE		THINK		ACT		BIG DATA
Radar Vision Secure V2X	Secure Network	Processing Sensor Fusion Security	Secure Network	Powertrain Chassis Braking		Digital Networking Infrastructure Security

GOALS FOR CONNECTED VEHICLES



SECURITY:	Zero accidents by system hacks
VEHICLE SAFETY:	Zero accidents by human error (ADAS & SOTIF)
FUNCTIONAL SAFETY:	Zero accidents by system failures (ISO 26262)
DEVICE RELIABILITY:	Zero components failures (robust product)

CONNECTED VEHICLE FEATURES THAT NEED CYBERSECURITY

EXAMPLE #1: V2X COMMUNICATIONS

Motorcycle approaching / „do not pass!“

MOTORCYCLE
APPROACHING!

Roadworks beyond line-of-sight

ROADWORKS
AHEAD!

802.11p required for Safety-critical V2X features:

Low Latency, Secure
&
Beyond-line-of-sight

Providing additional safety data earlier than any other sensor can „see“

Platooning / cooperative driving

HEAD OF TRUCK PLATOON

Emergency vehicle around corner

EMERGENCY VEHICLE
APPROACHING

EXAMPLE #1: V2X COMMUNICATIONS

Motorcycle approaching / „do not pass!“

Platooning / cooperative driving

802.11p required for Safety-

V2X communication brings great benefits…

- Improved Safety, Efficiency, Convenience & Comfort

…but also introduces new risks!

- To safety (malicious senders & messages)
- To privacy (tracking)

sensor can „see“

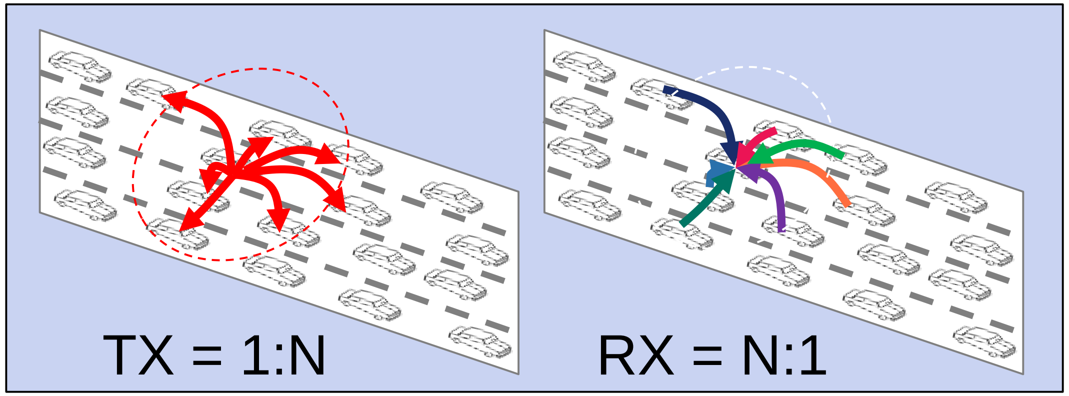
Roadworks beyond li

around corner

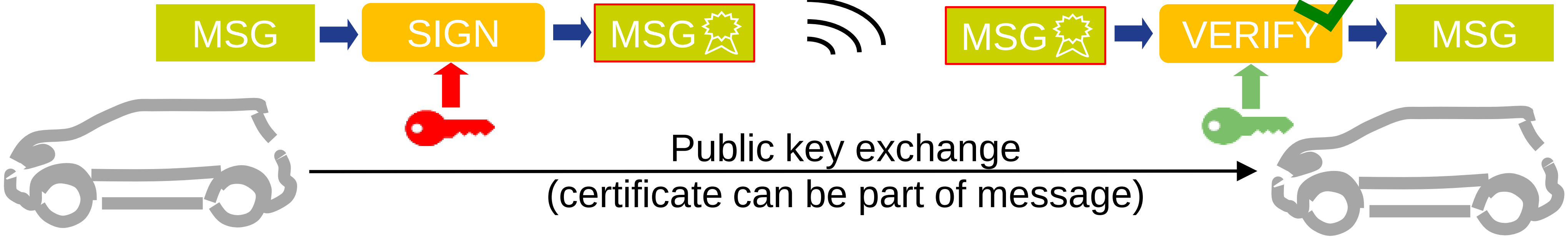
SECURING V2X COMMUNICATIONS

Performance & Security requirements

- **Digital signature: ECDSA P-256 (~ RSA 3k / AES 128)**
  - for authentication (sender identity, content integrity)
  - and non-repudiation (no plausible deniability)
- **Performance level:**
  - broadcast (*TX*) up to 20 safety messages / s
  - receive (*RX*) many more messages (100-1000 / s)
- **Security level:**
  - secret key material (pseudo-identities) involved in signature generation (*TX*)
  - only public key material involved in signature verification (*RX*)



	TX	RX
Operation	Signature generation	Signature verification
Rate	Low: ≤ 20 / s	High: 100-1000 / s
Security level	High: protection of private keys (=car identity)	Modest: only non-secret data



Public key exchange
(certificate can be part of message)

EXAMPLE #2: SOFTWARE UPDATES

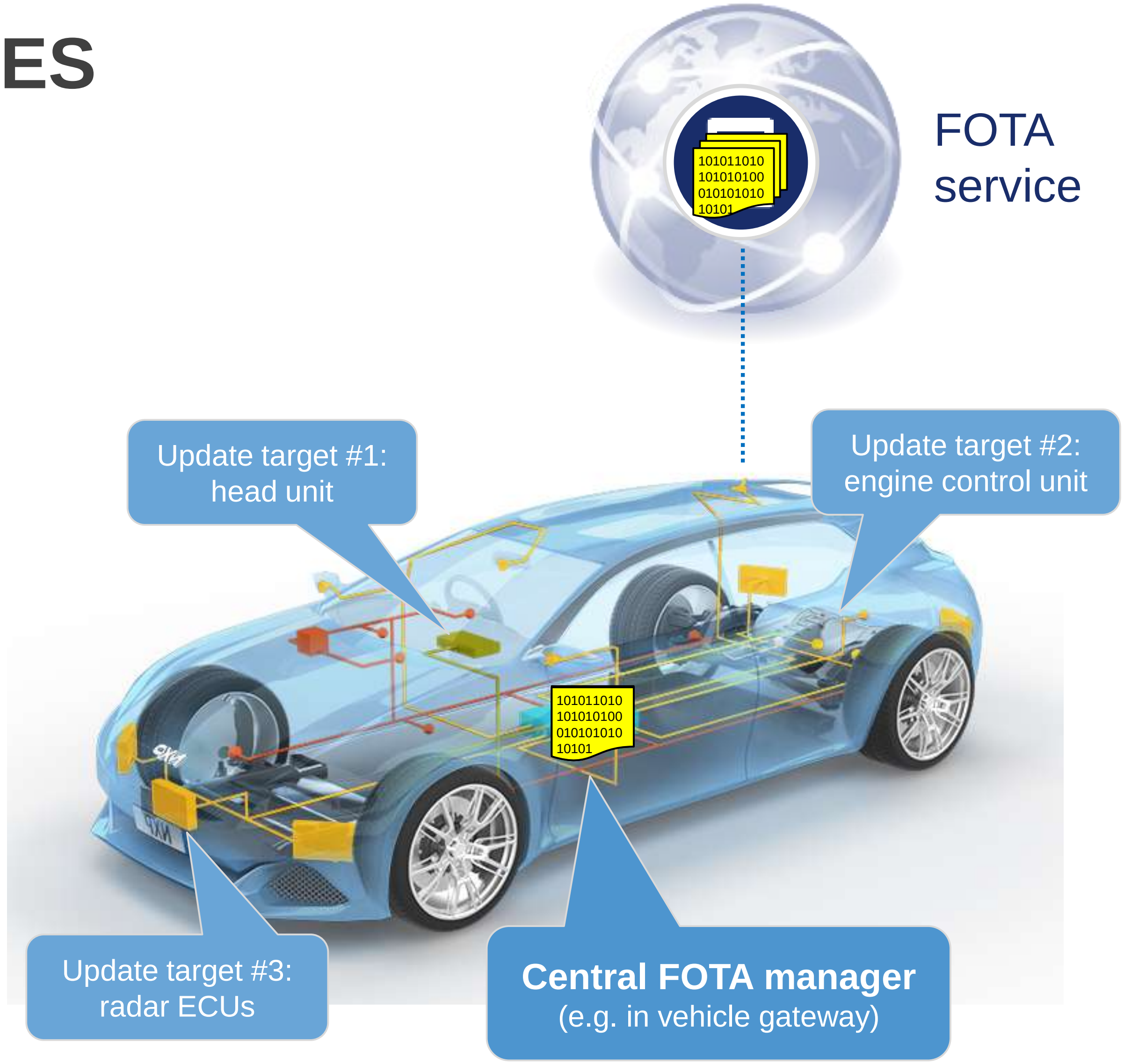
Firmware Over The Air (FOTA) Updates

- **Automobiles are complex cyber-physical devices**
  - With the increasing complexity of its software, regular software updates become a necessity

- **Firmware Over The Air (FOTA) updates bring great benefits…**
  - Cost reduction (prevent recalls)
  - Patching of security vulnerabilities

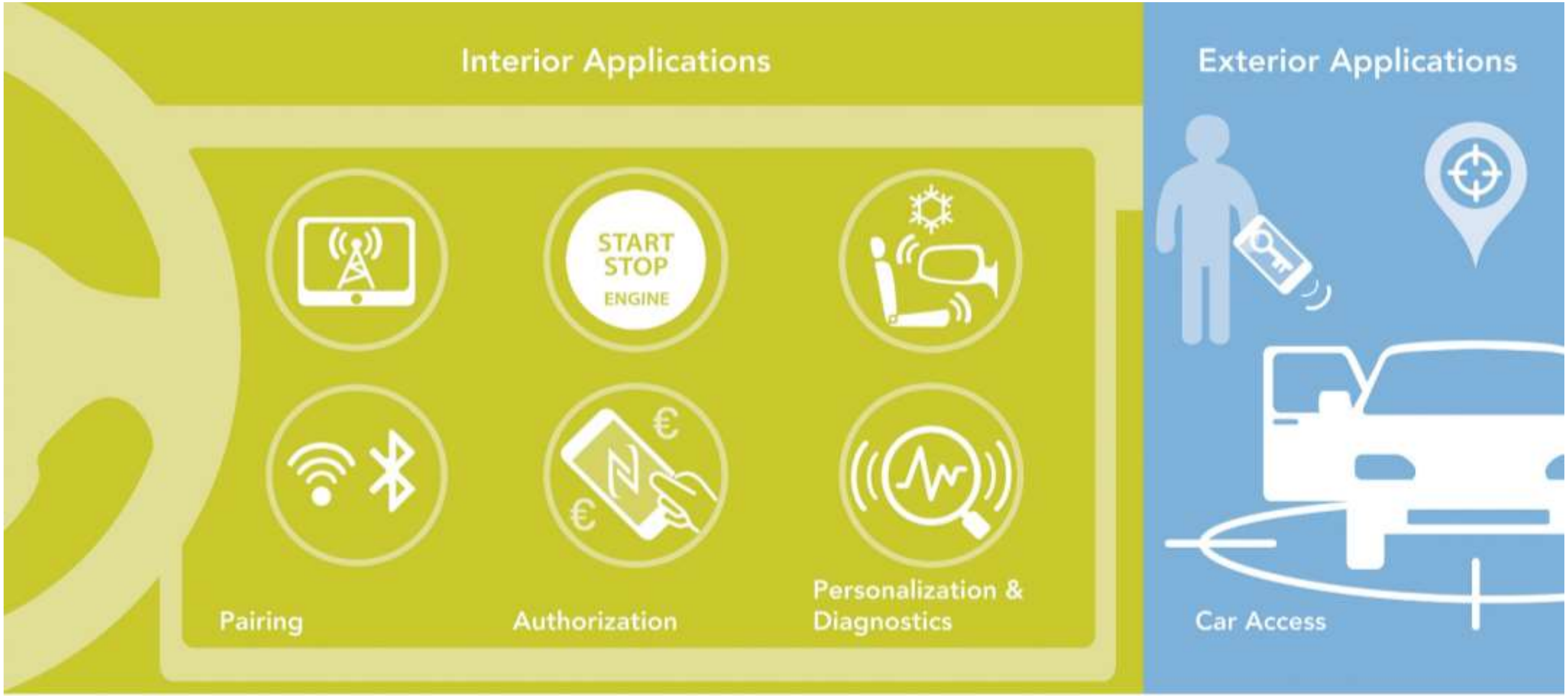
…but also introduces new risks!

- A bad (e.g. manipulated) FOTA can have serious consequences on safety & privacy


FOTA service
101011010
101010100
010101010
10101
Update target #1: head unit
Update target #2: engine control unit
Update target #3: radar ECUs
Central FOTA manager
(e.g. in vehicle gateway)

Typical FOTA approach, using a central update manager that orchestrates the update process

EXAMPLE #3 - Automotive NFC: security needed for most use cases



- Multimedia Streaming
- Wi-Fi Pairing
- BT Pairing

- Driver Authorization (Engine Start)
- Payment Services

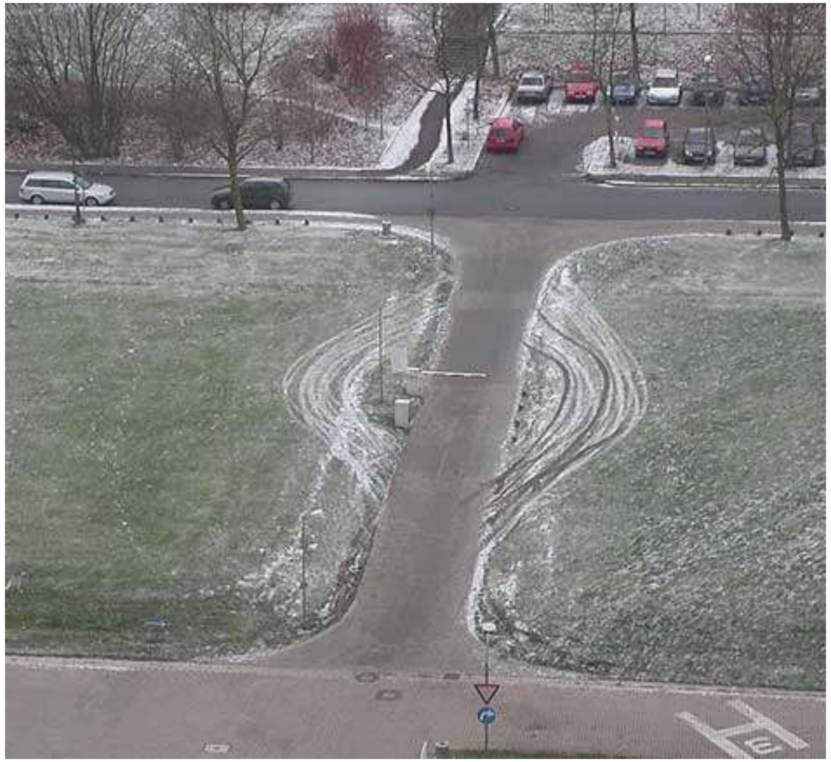
- Air Condition, Seat, Mirror Settings
- Transmit Vehicle Diagnostics Data

- Smartphone Car Access
- Car Sharing
- Fleet Management

WHAT IS SECURITY

Security Requires a Different Mindset

Hacker:
Let’s make it fail



Security engineer:
Think about how things can be made to fail...
…and prevent such failures!

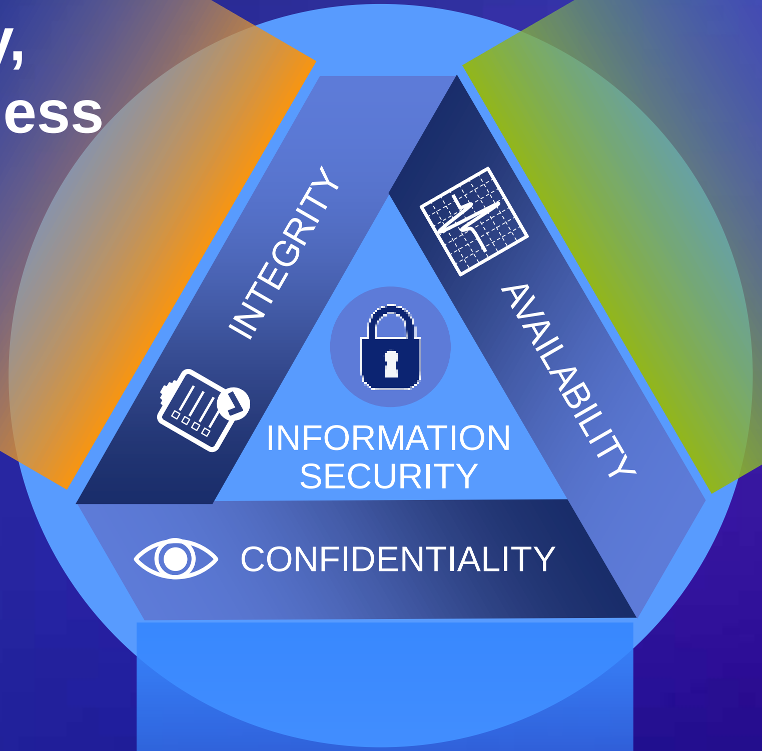
WHAT IS AT RISK, AND WHOM IS AFFECTED?

	STAKEHOLDERS				
IMPACT	Car User	Car Owner	Insurers	OEM & Suppliers	Service Providers
Safety	Damage, Injuries	→	→	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

SECURITY ATTRIBUTES

Integrity is about **accuracy, consistency** and **completeness**
(of data, the system state, etc.)

- Damage, Injuries due to Malfunctioning of Systems
- Theft of Goods (e.g. Vehicle)
- Unpaid use of services



Availability is about **assurance of operation**
(operational safety, service performance)

- Damage, Injuries due to Unavailability of Systems
- Loss of Income due to Unavailability of Services

Confidentiality is about **keeping secrets secret**
(hide information from unauthorized entities)

- IP Theft
- Loss of Personal Data (PII)

SECURITY TOOLBOX

MIX OF TECHNOLOGIES AND BEST PRACTICES

Cryptography – an important basis, but not a substitution for security

- Crypto algorithms like AES, RSA, SHA2 are ‘basic building blocks’
- (Please don’t invent your own crypto algorithm…)

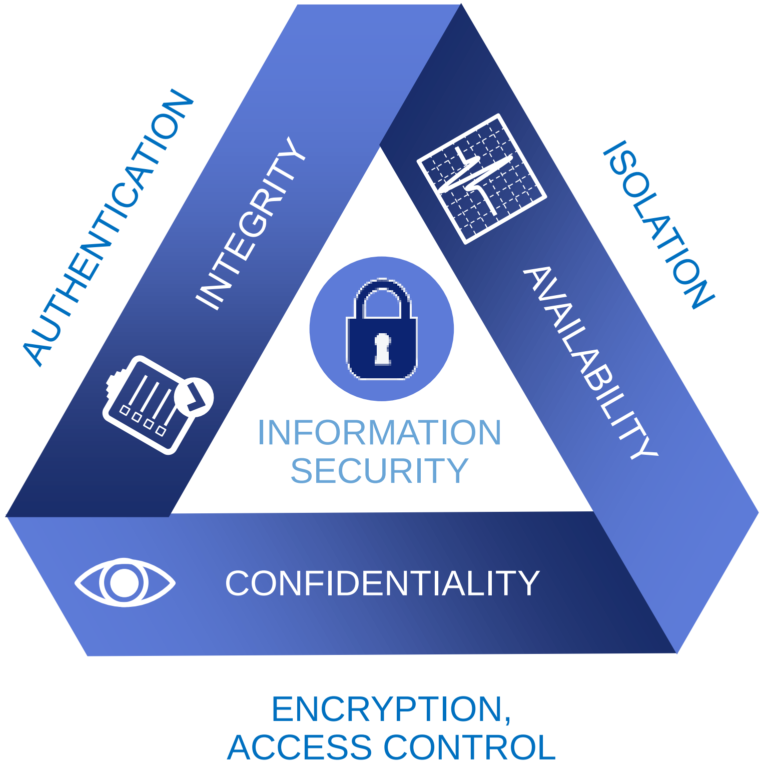
Restricting Access – e.g. using:

- Physical Isolation (e.g. separate networks and “air gaps”)
- Logical Isolation (e.g. firewalls between networks)
- Access Control (e.g. identification, authentication & authorization)

Other tools:

- Monitoring (e.g. intrusion detection systems)
- Software updates (e.g. SOTA / FOTA)
- Design, code and protocol reviews
- Defensive, secure and clean programming
- Security assessment (Pen Test, …)
- Formal proof systems, …

Most security vulnerabilities are caused by design & implementation weaknesses(!)



THE "BAD GUYS" MAKE A COST-BENEFIT ANALYSIS

Every attacker makes an (implicit or explicit) Cost-Benefit Analysis:

Cost

money & time spent
know-how needed
risk of being caught
…

Benefits

(stolen) goods
(stolen) data
publicity
…

When the balance is right (benefits > cost), **an attacker may (will) strike!**

It may be hard to quantify cost and benefits

Examples: What is the value of stolen data? Or publicity, e.g. for researchers?

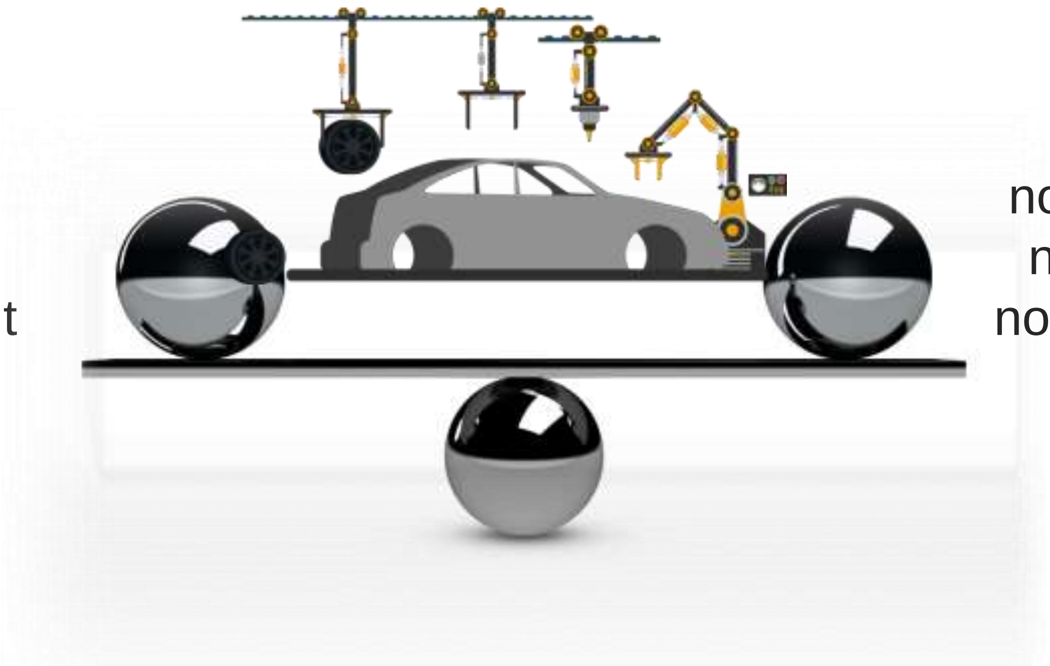
THE “GOOD GUYS” MUST MAKE A RISK ANALYSIS

A manufacturer must balance costs and benefits

Based on a Threat, Vulnerability & Risk Assessment (TVRA)

Cost

countermeasures
stricter processes
security assessment
…



Benefits

no / less loss of goods
no / less loss of data
no / less brand damage
…

Security is an upfront payment, much like an insurance premium

Countermeasures will imply direct (recurring) costs
But they also aim at reducing the risk and thereby, to prevent future cost

SECURITY & FUNCTIONAL SAFETY (ISO 26262)

They are similar…

Both are **quality aspects**, needed to ensure the **proper operation** of a system

…but they are not the same

Functional Safety is concerned with unintentional hazards,
which are predictable & regular

- Resulting from natural phenomena (e.g. extreme temperatures or humidity), or from human negligence or ignorance (e.g. improper design or use)
- The environment doesn’t change (and neither do the laws of physics…)

Security is concerned with intentional hazards,
which are rather unpredictable & irregular

- Resulting from attacks planned and carried out by humans
- Hackers get smarter / better over time; and they don’t follow “the rules”

NXP Automotive Security Strategy

#1 SEMICONDUCTOR SUPPLIER IN THE IDENTIFICATION INDUSTRY

#1

eGovernment

#1

Bank Cards

#1

Smart Mobility (MIFARE) Cards

#1

Tags & Authentication

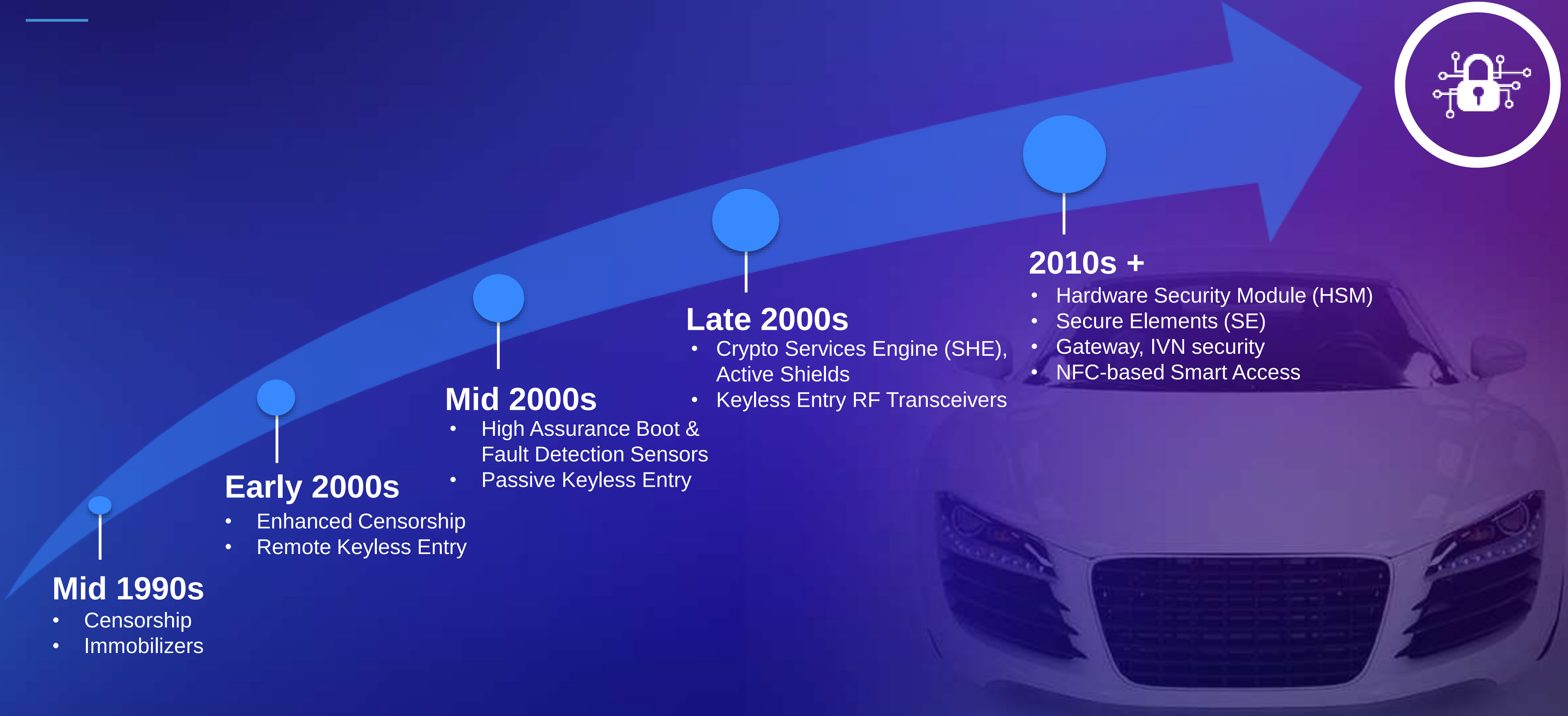
#1

Readers

#1

Mobile

PROVEN HISTORY IN DRIVING AUTOMOTIVE SECURITY



Mid 1990s

- Censorship
- Immobilizers

Early 2000s

- Enhanced Censorship
- Remote Keyless Entry

Mid 2000s

- High Assurance Boot & Fault Detection Sensors
- Passive Keyless Entry

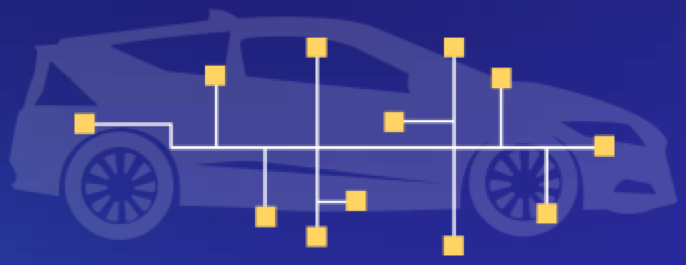
Late 2000s

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

2010s +

- Hardware Security Module (HSM)
- Secure Elements (SE)
- Gateway, IVN security
- NFC-based Smart Access

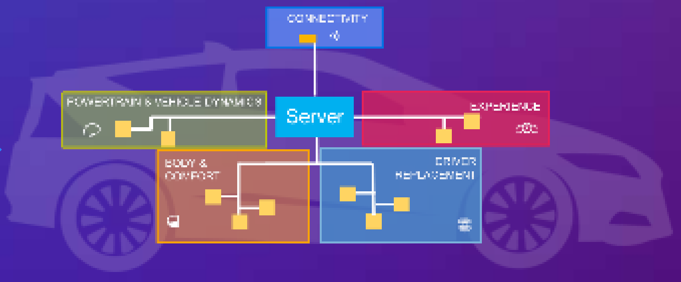
AUTOMOTIVE SECURITY – WAY FORWARD



TODAY

APPLY BEST PRACTICES:

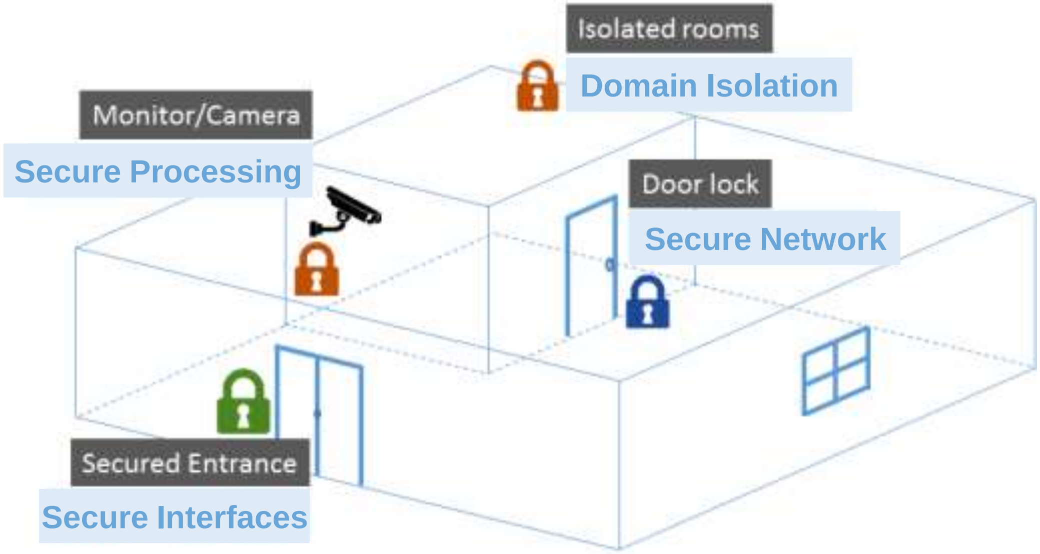
- Security-by-design & Privacy-by-Design (as opposed to being an afterthought)
- Lifecycle Management (incl. FOTA)



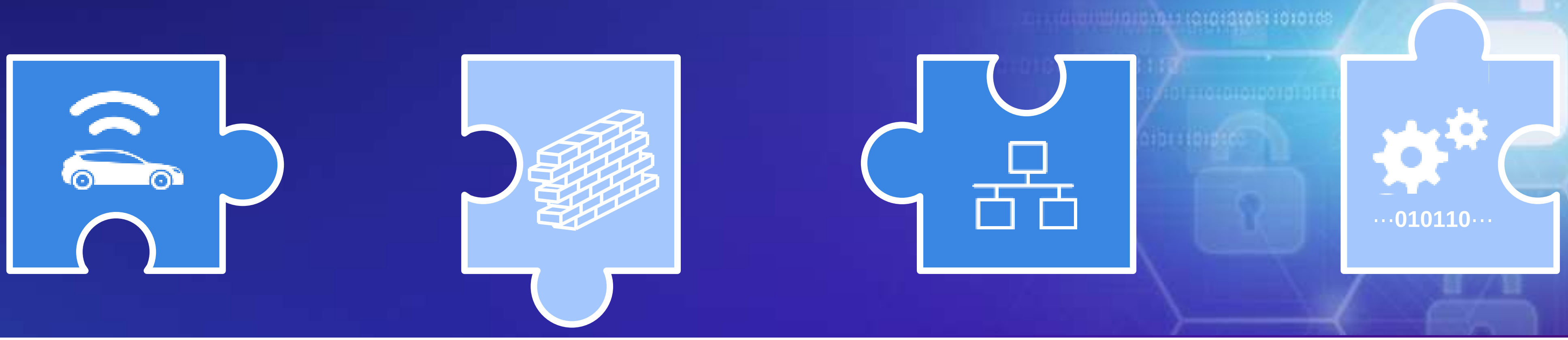
FUTURE

Essential element:
Defense-in-Depth approach

- Multiple layers of protection, at different levels in the system
- To mitigate the risk of one component of the defense being compromised or circumvented



CORE SECURITY PRINCIPLES

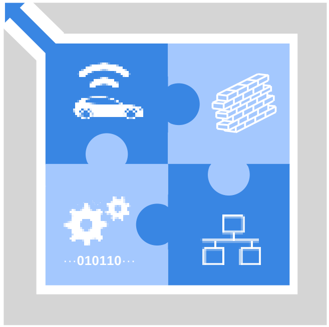


Secure **External Interfaces**

Secure **Domain Isolation**

Secure **Internal Communication**

Secure **Software Execution**



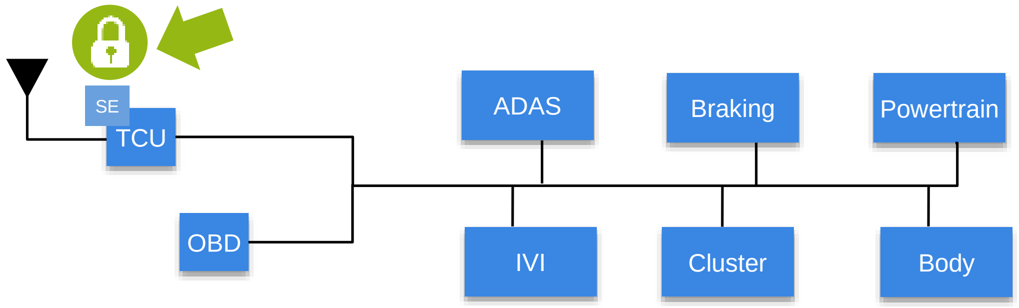
They need to be in place in ***any*** E&E network

- Regardless of the actual architecture and implementation

4 LAYERS TO SECURING A CAR

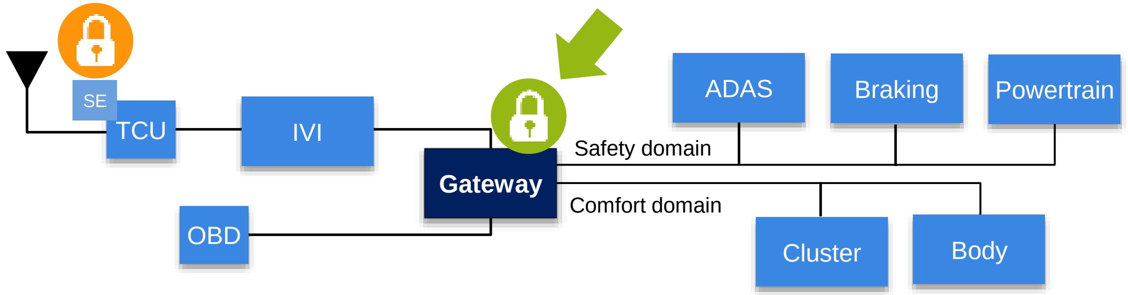
Layer 1: **Secure Interface**

Secure M2M authentication, secure key storage



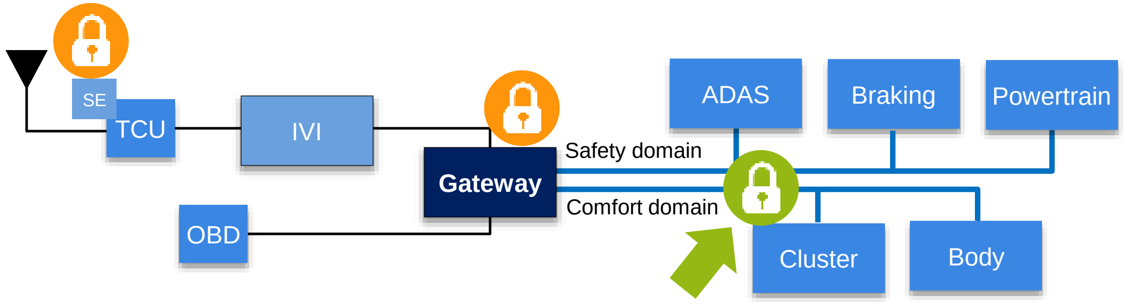
Layer 2: **Secure Gateway**

Domain isolation, firewall/filter, centralized intrusion detection (IDS)



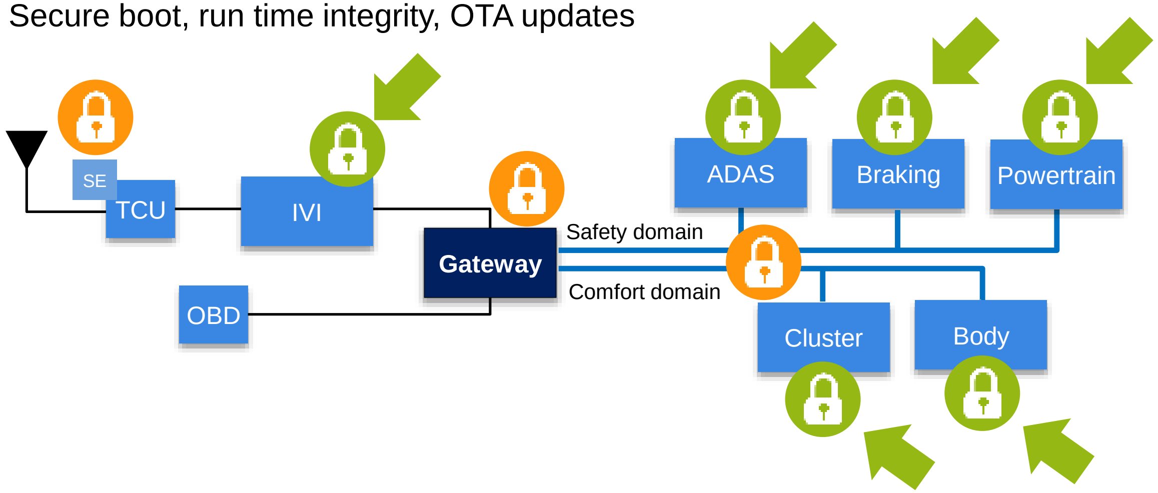
Layer 3: **Secure Network**

Message authentication, CAN ID killer, distributed intrusion detection (IDS)



Layer 4: **Secure Processing**

Secure boot, run time integrity, OTA updates

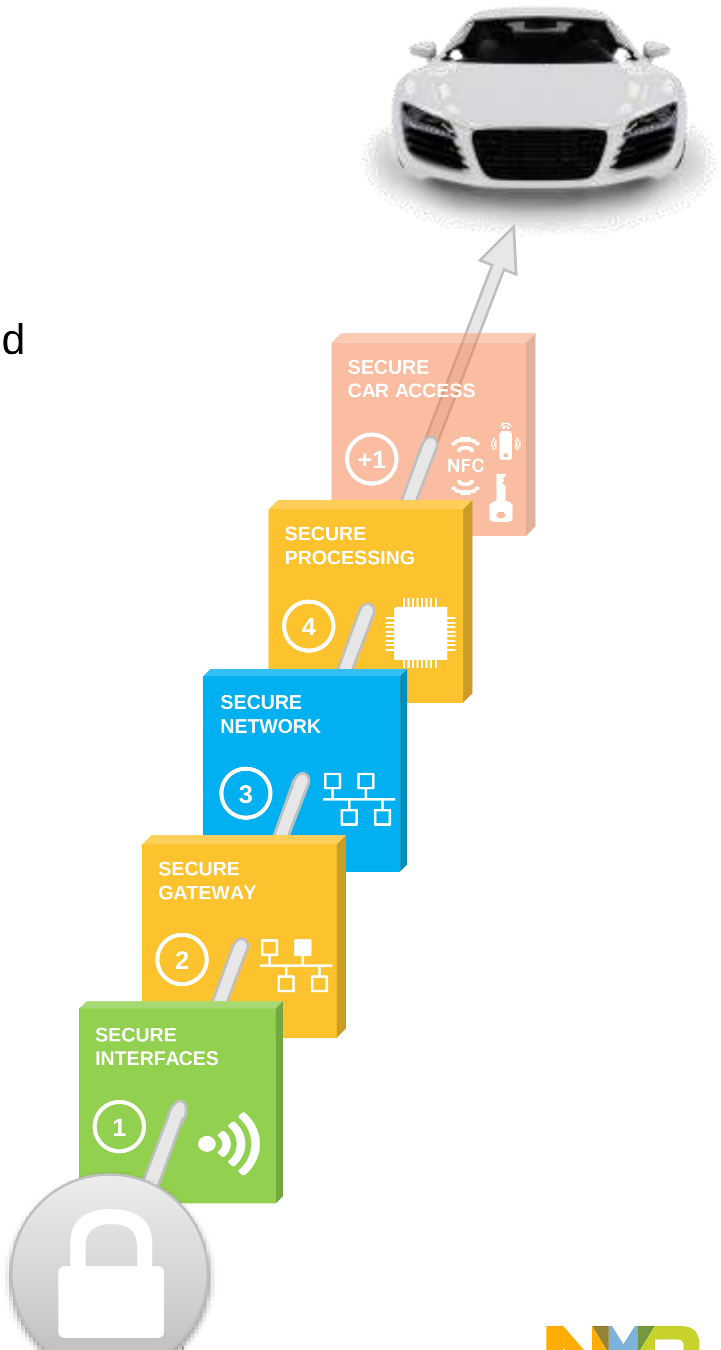


Defense in Depth

Securing the Vehicle’s Electronics Architecture

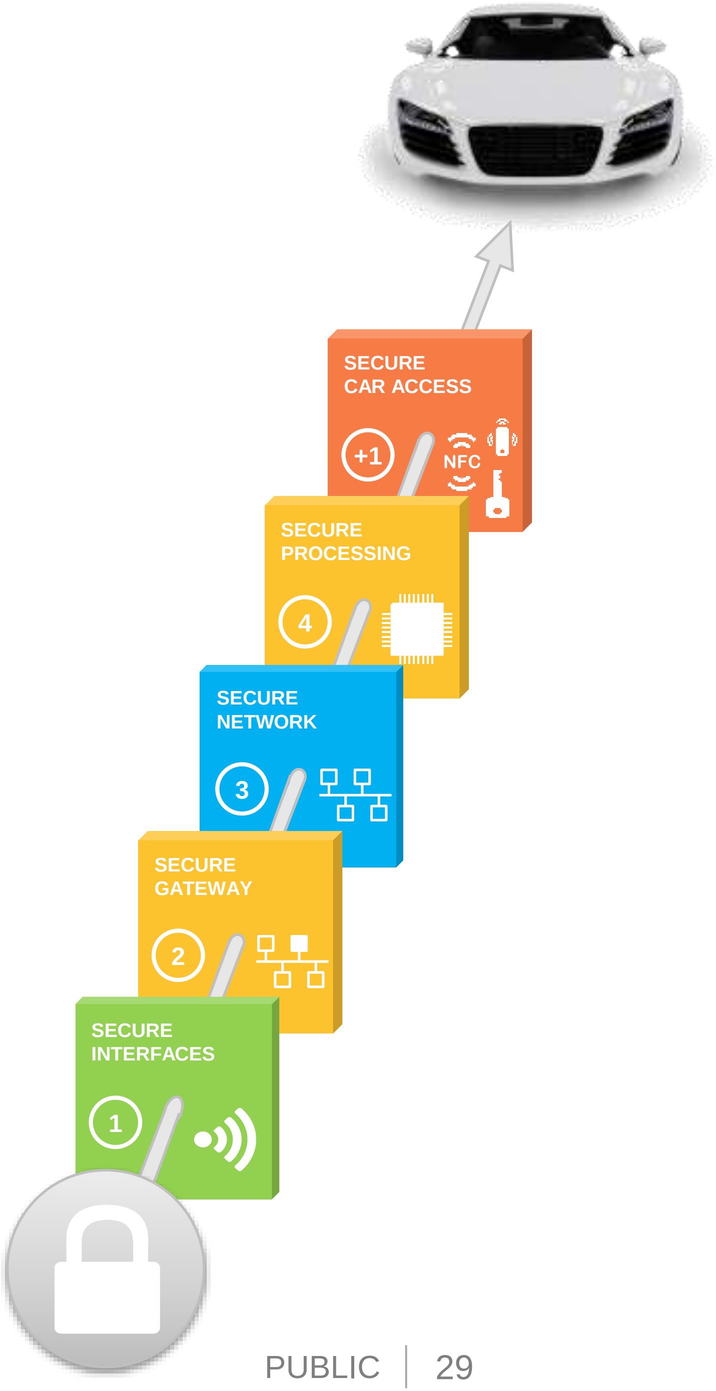
- Multiple security techniques, at different levels in the architecture
- To mitigate the risk of one component of the defense being compromised or circumvented

Prevent access	**Detect** attacks	**Reduce** impact	**Fix** vulnerabilities
Authenticate code (secure boot)	Run-Time Integrity Protection	Resource control (virtualization)	Secure OTA updates (firmware, policies, …)
Secure messaging	Intrusion detection systems (IDS)		
Firewalls (context-aware message filtering)		Separate functional domains Isolated TCU & OBD-II	
M2M authentication Firewalls (isolate access points)			



Hardware Security is a Must

- **Crypto accelerators**,
  to guarantee strict performance requirements
  - E.g. message authentication (V2X, CAN/Ethernet), secure boot
- **Hardware-enforced isolation**,
  to protect against software attacks
  - E.g. system vs. user mode, TrustZone, SHE/HSM
- **Tamper-resistant hardware**,
  to protect against advanced, physical attacks
  - E.g. Secure Elements



SECURITY PROCESSES AND SERVICES

Security must be an integral part of the lifecycle

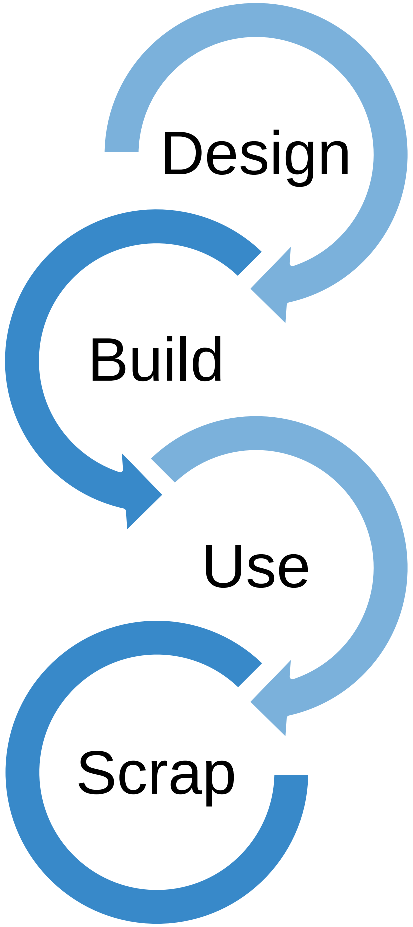
- In product design, implementation and maintenance
- But also in associated processes

NXP takes its responsibility; e.g.:

- Secure Development and Manufacturing Processes
- Threat Intelligence Feed (e.g. Auto ISAC[1])
- External Audits for Product / Site Security
- Product Security Incident Response Team[2]

We offer security services; e.g.:

- Trust Provisioning
- Consultancy to customers



- Requirement specification
- Architecture design
- Detailed design

- Implementation
- Validation & Verification

- Maintenance (FOTA)
- Upgrades (Feature unlock)

- Failure analysis
- Decommissioning

[1] NXP joined Auto ISAC in August 2016
[2] http://www.nxp.com/about/about-nxp/corporate-responsibility/product-security-incident-response-team:PSIRT

4+1 LAYERS

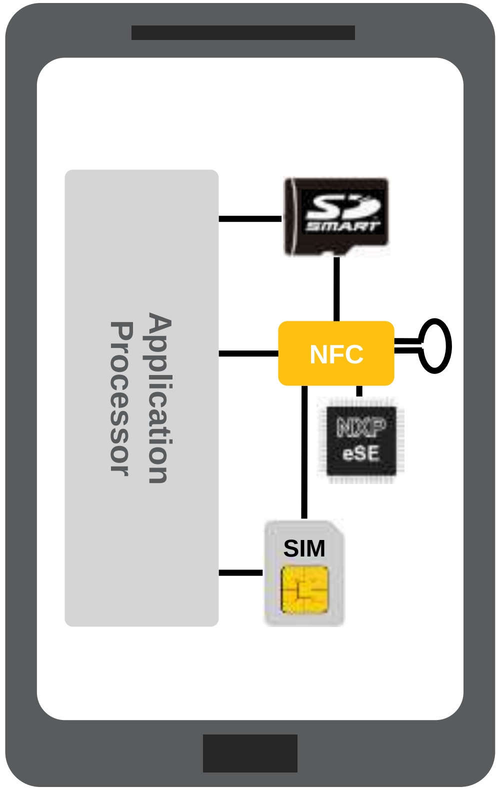
Layer 1 – Secure Element: What is It?

- A tamper-resistant platform, that protects against physical attacks
  - Proven security, via 3rd party evaluation and certification (Common Criteria)

- Securely hosts security applications and their confidential data
  - Banking cards, electronic passports, V2X, Telematics, …

- Provides secure crypto processing
  - AES, RSA, ECC, TRNG, …

- And secure key- and certificate handling
  - Generate and store secret keys
  - Store and validate Certificates
  - Manage security profiles

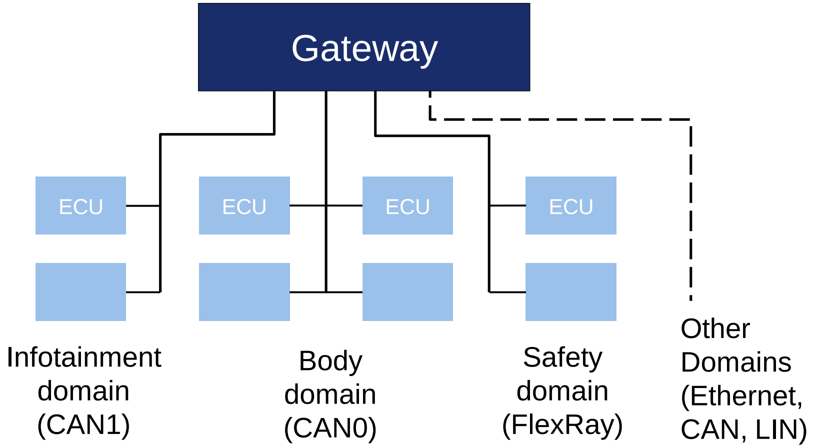


Layer 2 – Gateway: What is It?

- **Gateway is THE central node in the vehicle architecture**
  - Connects all the vehicle domains across all the interfaces (Ethernet, CAN FD, LIN)
  - Provides network isolation and security between functional domains and networks
  - Includes hardware accelerated crypto capability (HSM/CSE)
  - Transmits message to ECU on destination domain (adding secure signature to message)

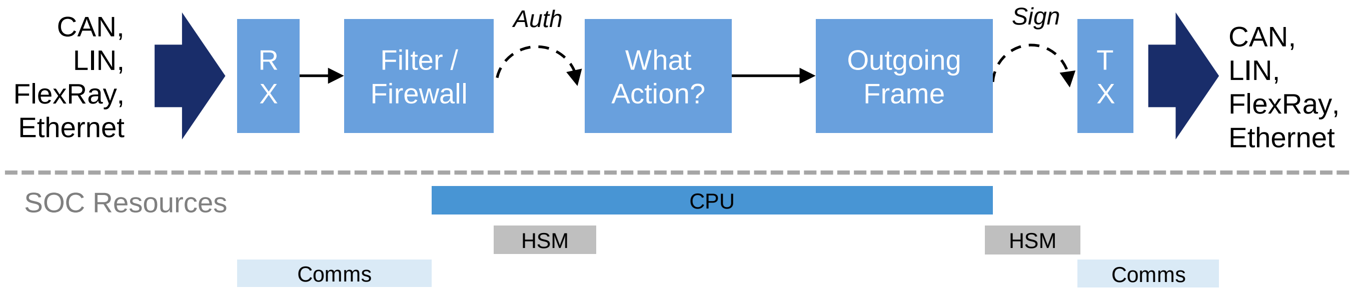
- **~20% adoption in vehicle architecture today, moving to ~50% by 2020**
  - NXP will be #1 in this market by 2018

Vehicle Architecture (Simplified)



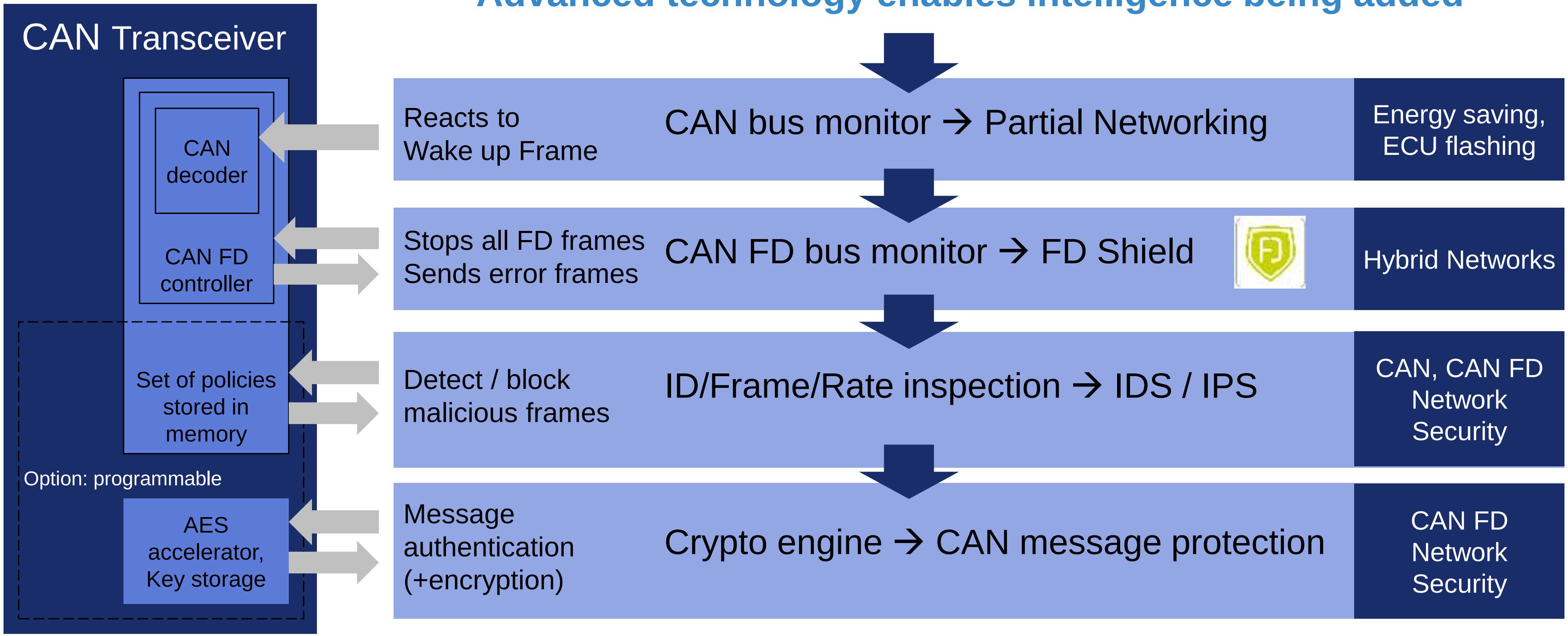
Gateway
ECU
ECU
ECU
ECU
Infotainment domain (CAN1)
Body domain (CAN0)
Safety domain (FlexRay)
Other Domains (Ethernet, CAN, LIN)

Gateway Function



Layer 3 – Secure Network: What is It?

Starting from an ultra-low Emission, 5Mbps-fast CAN transceiver
Advanced technology enables intelligence being added



CAN Transceiver

CAN decoder

CAN FD controller

Set of policies stored in memory

Option: programmable

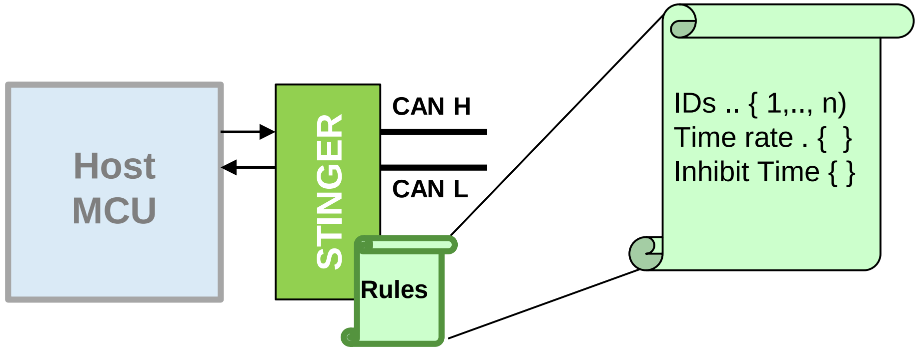
AES accelerator, Key storage

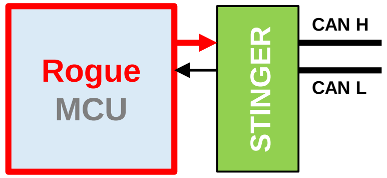
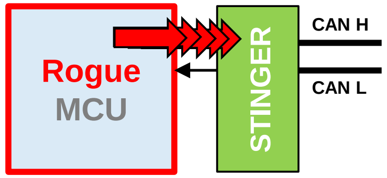
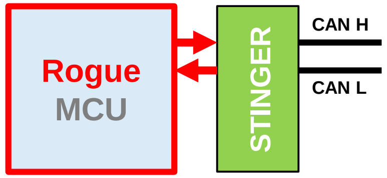
Reacts to Wake up Frame	CAN bus monitor → Partial Networking	Energy saving, ECU flashing
Stops all FD frames Sends error frames	CAN FD bus monitor → FD Shield	Hybrid Networks
Detect / block malicious frames	ID/Frame/Rate inspection → IDS / IPS	CAN, CAN FD Network Security
Message authentication (+encryption)	Crypto engine → CAN message protection	CAN FD Network Security

Layer 3 Secure Network Solution – STINGER

CAN Transceiver with non-crypto Security Function:
Contains the impact of a rogue MCU - Performs passive access Prevention (APS) with the help of a network specific set of policies stored in the CAN transceiver.

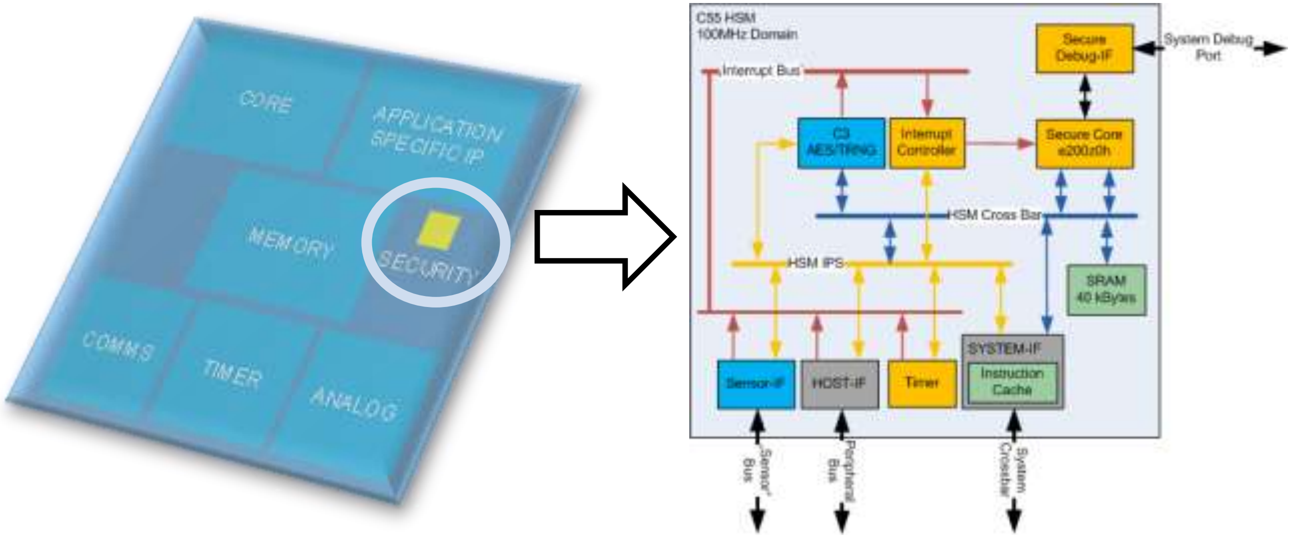
- **Supported:** Outbound filtering, Flooding prevention, Bus arbitration hijack prevention
- **Not-Supported:** Pattern recognition, Deep packet inspection



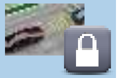
APS	**Message ID Blocking**		**Stopping un-authorized IDs** Example - Preventing the transmission of frames ,by the rogue MCU host, used for triggering the illegal diagnostic or flashing session.
	Flooding Prevention		**Denial of Service protection: Flooding Prevention** Maximum allowed transmission rate for a given node based on the rate filters
	Bus Hijack Prevention		**Denial of Service protection: Bus Arbitration Hijacking Prevention** Maximum allowed arbitration time for a given node

Layer 4 – Secure Processing: What is It?

- Secure MCU - Defined by hardware accelerated Crypto capability
- IP can be applied to any MCU/Processor
- Use cases:
  - CAN Message authentication
  - Secure boot – FW auth.
  - Key storage
  - Encryption
  - OTA software updates in the field



ADAS
Advanced Driver Assistance Systems

Radar 

Vison

Fusion

GPIS
General Purpose & Integrated

8 Bit

16/32 Bit

Integrated

C&S
Connectivity & Security

Gateway

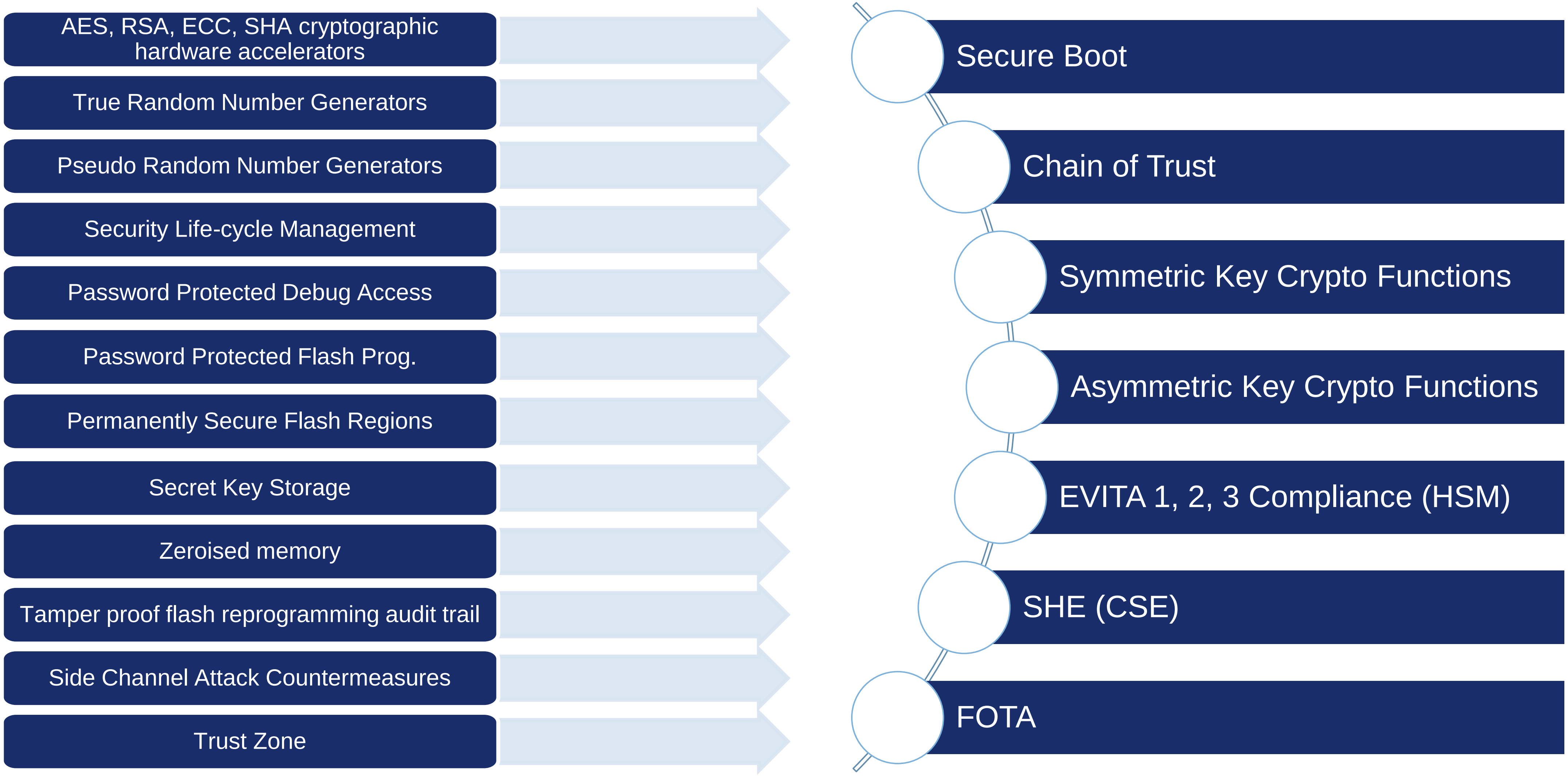
VDS
Vehicle Dynamics & Safety

Chassis & Safety

Powertrain

Custom

Security Features on NXP Secure MCUs



- AES, RSA, ECC, SHA cryptographic hardware accelerators
- True Random Number Generators
- Pseudo Random Number Generators
- Security Life-cycle Management
- Password Protected Debug Access
- Password Protected Flash Prog.
- Permanently Secure Flash Regions
- Secret Key Storage
- Zeroised memory
- Tamper proof flash reprogramming audit trail
- Side Channel Attack Countermeasures
- Trust Zone

- Secure Boot
- Chain of Trust
- Symmetric Key Crypto Functions
- Asymmetric Key Crypto Functions
- EVITA 1, 2, 3 Compliance (HSM)
- SHE (CSE)
- FOTA

Layer +1 – Secure Car Access: What is It?

Immobilizer

- Car theft protection

Remote Keyless Entry (RKE)

Consisting of:

- Car theft protection
- Remote car door lock and unlock

Passive Keyless Entry (PKE)

Consisting of:

- Car Theft protection
- Remote car door lock and unlock
- Passive keyless entry
- Passive Start

Smart Car Management

Car-key communication for:

- Remote start
- Car finder
- Alarm Systems
- Tire pressure information
- Fuel level / Charging state
- Door lock status

Connected Keyless Entry

- Car Access via NFC enabled phones/wearables
- NFC key advantage: secure transport of keys
- Alternative: Car access via phone using BLE and key fob as ‘Gateway’

AUTOMOTIVE CYBERSECURITY ‘MOVING PARTS’

Hardware Security ‘Standards’

- **SAE J3101** – Requirements for Hardware-Protected Security for Ground Vehicle Applications
  - Status: work in progress
  - Objective: define a common set of requirements for hardware security for connected vehicles

- **HIS SHE / EVITA HSM**
  - Status: SHE was a de-facto industry standard; HSM is a de-facto list of requirements
    - HIS consortium does not exist anymore, so SHE has no formal ‘home’ anymore
    - Opportunity for new standard → SAE J3101?
  - Objective: (requirements) specification for an on-die security extension to MCUs

Software Security

- **AUTOSAR**
  - Objective: open and standardized software architecture for automotive electronic control units (excluding infotainment)
  - Status: version 4.x has been released, introducing a few security concepts
    - For crypto services (CAL and CSM) and secure on-board communication (SecOC)

- **JASPAR**
  - “Focus on standardization and common use of electronic control system software”

- **Secure Coding Standards**
  - **CERT C**
  - **MISRA C**

Application / Use Case Specific

- **ETSI TC ITS / ISO TC22**
  - Status: mature
  - Objective: specification of the ITS Station security architecture & secure 802.11p communication

- **IEEE 1609 WAVE**
  - Status: mature
  - Objective: specify systems & security architecture for 802.11p based DSRC

- **TCG TPM v2.0 Automotive Thin Profile**
  - Status: v1.0 released; but hardly/no traction in Auto industry
  - Objective: provide means for integrity reporting of software and cryptographic key creation, storage, management and use

Security Processes

- **SAE J3061** – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
  - Status: released (Jan. 2016)
  - Objective: *"To provide a <u>cybersecurity process framework</u> and guidance to help organizations identify and assess <u>cybersecurity threats</u> and <u>design cybersecurity</u> into cyber-physical vehicle systems <u>throughout the</u> entire development <u>lifecycle</u> process."*
  - Revision in progress – including Cybersecurity Assurance Testing

- **ISO/TC22 N 3556** – E&E equipment, Car informatics & on board computer systems
  - Status: work in progress
  - Objective: create security levels, similar to ASIL A-D levels
    - "Security equivalent" of ISO 26262 (functional safety)
    - "ISO equivalent" of SAE J3061

- **Japan IPA (IT Promotion Agency) 'Approaches for Vehicle Information Security'**
  - Status: released
  - Objective: provide cyber security guidelines for vehicles (e.g. apply domain separation – safety vs. comfort vs. infotainment)

- **Other**
  - Auto-ISAC, NHTSA, and U.S. DOT working on automotive cybersecurity guidelines

Other Issues Related to Automotive Cybersecurity

- **Right to Repair / Right to Tinker (who owns the vehicle?)**

- **How to work with Security Researchers / Bug Bounty and Vulnerability Disclosure Programs**

- **Consider the security goals for each operation / piece of data (Confidentiality**, **Authentication**, **Data Integrity**, and/or **Non-repudiation)**

Automotive IC Issues Concerning Cybersecurity

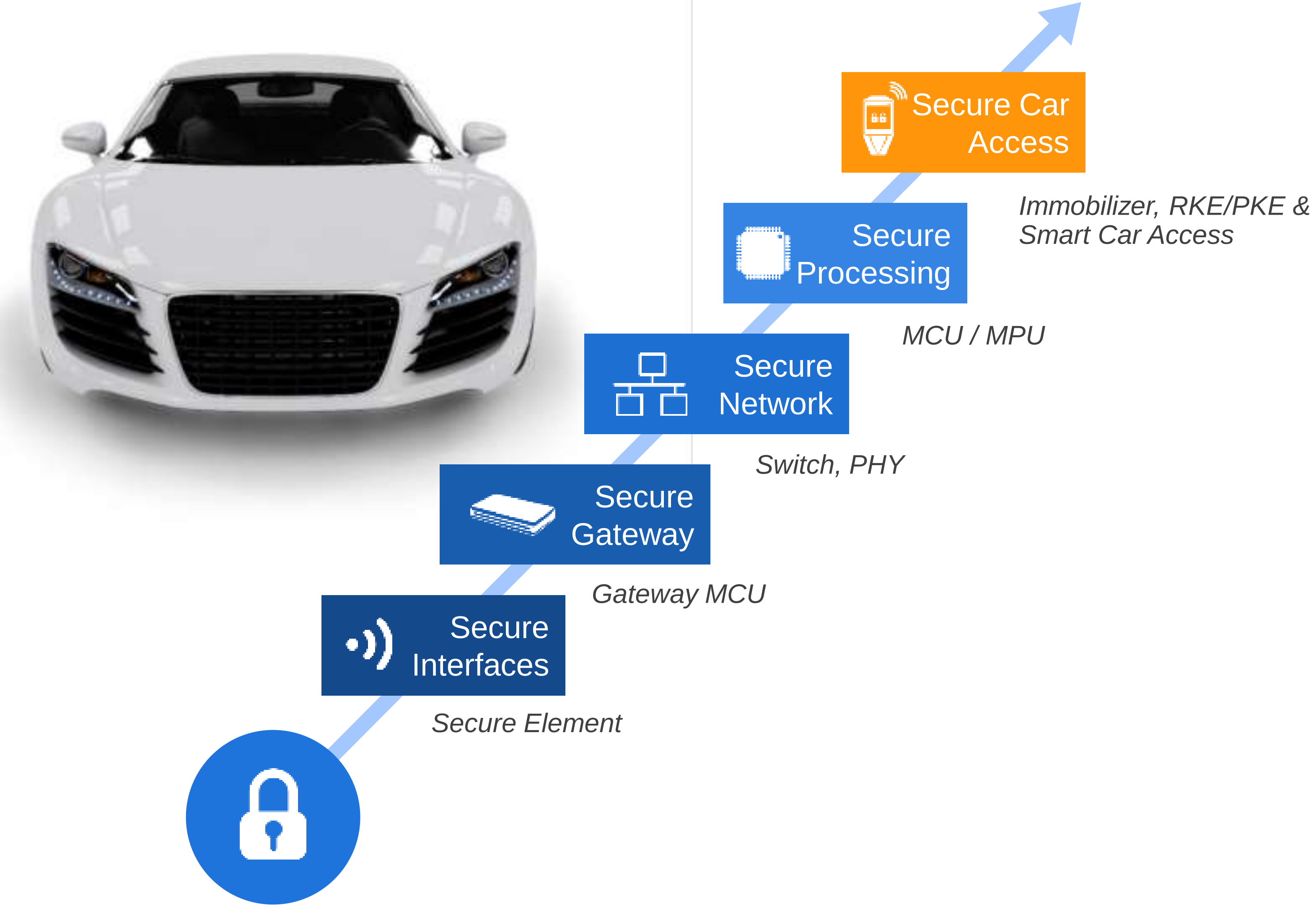
- **OEM's Requiring Tier 1 Suppliers to use available IC Security Features**

- **Consider Design Tradeoffs**
  - **Cost**
  - **Communication Latency**
  - **Boot-Up Time**
  - **Types of attacks that are in-scope for each IC**
  - **Complexity of handling cryptography keys**

CONCLUSIONS

NXP'S 4+1 AUTOMOTIVE SECURITY FRAMEWORK

Complete product portfolio, enabling our customers to implement the core security principles



Secure Car Access

Immobilizer, RKE/PKE & Smart Car Access

Secure Processing

MCU / MPU

Secure Network

Switch, PHY

Secure Gateway

Gateway MCU

Secure Interfaces

Secure Element

NXP **#1** in Auto HW Security

4-Layer Cyber Security Solution, enabling defense-in-depth

Plus **'Best In Class'** Car Access Systems

Recognized Thought & Innovation Leader

> 900 security patent families,
~ 200 specific to Automotive

Partner of Choice for OEMS, T1s & Industry Alliances

Securely!

NXP connects the car

THANK YOU!

www.nxp.com/automotivesecurity

Car-to-x Communication
(802.11p via Software-defined Radio, Authentication)

Personalization and Data Security
(NFC, Authentication)

Broadcast Reception
(Software-defined Radio, Digital Radio, AM/FM)

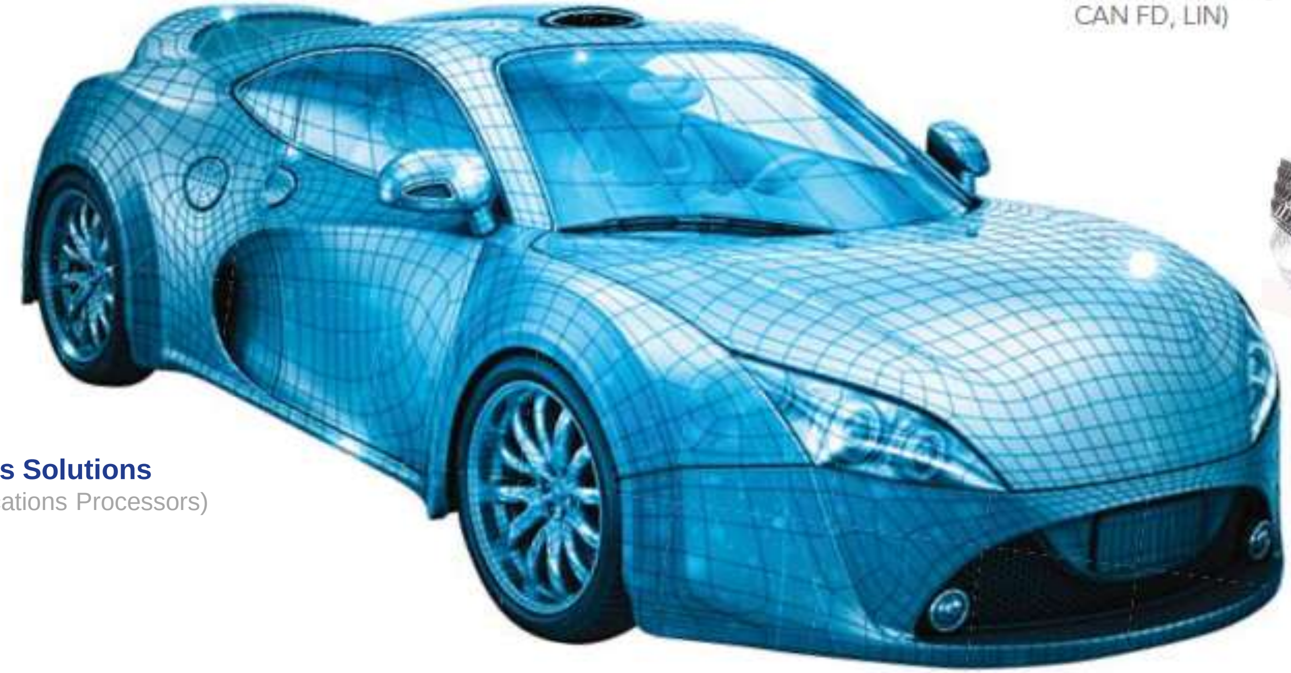
Car Access and Remote Car Management
(PKE, RKE, NFC, Authentication, Two-way RF, Passive Entry/Go)

In-Vehicle Networking
(Ethernet, FlexRay, CAN, CAN FD, LIN)

Embedded MCUs and Applications Processors
(with integrated communication interfaces, and application layer Software stacks)

Automotive Gateway Solutions
(MPC5xxx, S32G MCUs)

Telematics Solutions
(i.MX Applications Processors)



SECURE CONNECTIONS
FOR A SMARTER WORLD