



**FTF 2016**  
TECHNOLOGY FORUM

# 4 LAYERS OF SECURITY FOR CONNECTED CARS

**FTF-AUT-N1811**

TIMO VAN ROERMUND, ANDY BIRNIE  
GLOBAL AUTOMOTIVE SECURITY  
FTF-AUT-N1811  
MAY 17, 2016

PUBLIC USE



# AGENDA

- What is security?
- Why do we need security in automotive?
- NXP's approach to automotive security
- Product overview



# Today: 90% of Auto Innovation via Electronics

## NXP: THE GLOBAL MARKET LEADER IN AUTOMOTIVE SEMICONDUCTOR SOLUTIONS

### #1 INFOTAINMENT

TUNERS  
SOFTWARE-DEFINED DIGITAL RADIO  
MULTIMEDIA PROCESSORS  
SOUND SYSTEM DSPs & AMPLIFIERS  
NFC BT PAIRING  
WIRELESS POWER CHARGING  
POWER MANAGEMENT

### STANDARD PRODUCTS

LOGIC  
POWER  
DISCRETES

### #1 VEHICLE NETWORKING

CAN/LIN/ FLEXRAY  
ETHERNET  
CENTRAL GATEWAY CONTROLLER  
SECURITY  
RF

### #1 BODY

MICROCONTROLLERS  
POSITION/ ANGLE SENSORS  
SYSTEM BASIS CHIPS

### ADAS & SECURITY

### POWERTRAIN & CHASSIS

MICROCONTROLLERS  
PRESSURE/ MOTION SENSORS  
BATTERY MANAGEMENT  
DRIVERS

### #1 SECURE CAR ACCESS

IMMOBILIZER/ SECURITY  
REMOTE KEYLESS ENTRY  
PASSIVE KEYLESS ENTRY/ GO  
BI-DIRECTIONAL KEYS  
NFC  
ULTRA WIDE BAND

### #1 SAFETY

MICROCONTROLLERS AIRBAG  
ANALOG AIRBAG  
MICROCONTROLLERS BRAKING  
ANALOG BRAKING  
SENSORS BRAKING  
TIRE PRESSURE MONITORING

#1 Auto Analog/ RF

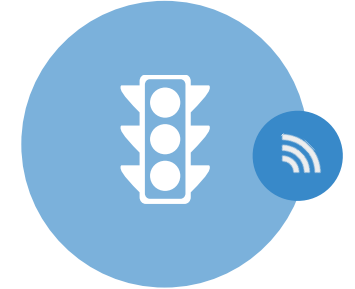
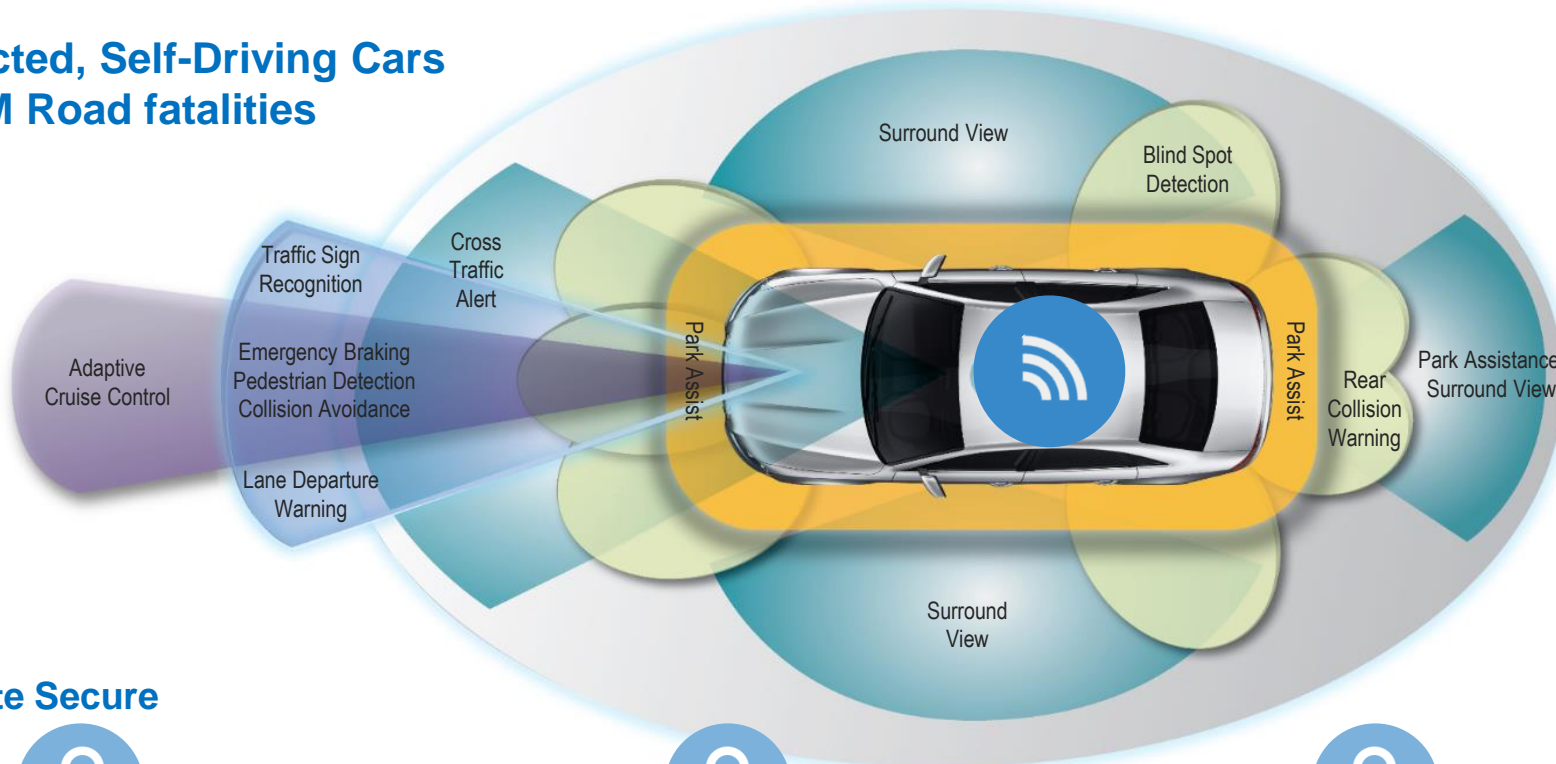
#1 Auto MCU (ex JPN)

#1 Auto Merchant MEMS Sensors



# Tomorrow: Enabling the **Secure Connected Car**

**Secure Connected, Self-Driving Cars will Save >1,3M Road fatalities globally**



**NXP Offers Complete Secure ADAS System....**



SENSE
Radar Vision Secure V2X

Secure Network



THINK
Processing Sensor Fusion Security

Secure Network



ACT
Powertrain Chassis Braking

**...including Big Data Infrastructure**



BIG DATA
Digital Networking Infrastructure Security



# THE NEED FOR SECURITY



# Increasing Connectivity = Increasing Risks

FBI: Estimated 3 Trillion USD Annual Damage from Hacking

Requiring maximum protection of . . .



Privacy

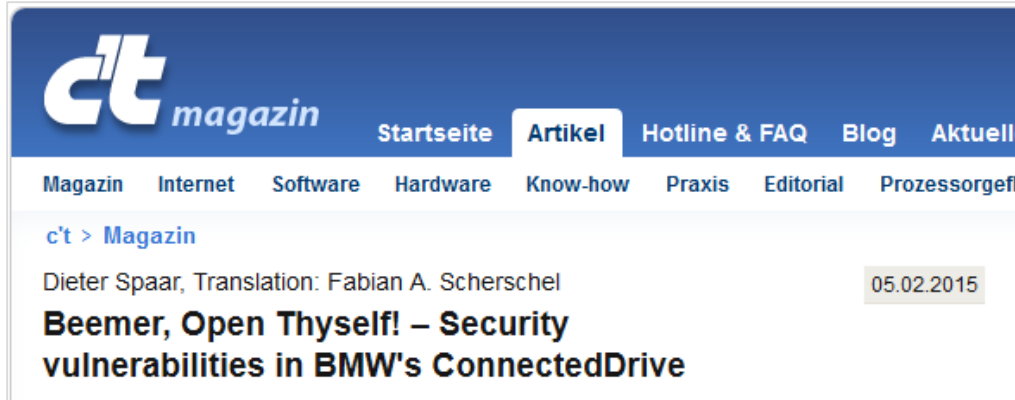


Personal Assets



Lives

# Car Hacking is 'Hot' ...



ct magazin Startseite Artikel Hotline & FAQ Blog Aktuell

Magazin Internet Software Hardware Know-how Praxis Editorial Prozessgef

c't > Magazin

Dieter Spaar, Translation: Fabian A. Scherschel 05.02.2015

## Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive



JALOPNIK Damon Lavrinc

Filed to: CAR HACKING 2/18/15 5:40pm

## How A 14-Year-Old Hacked A Car With \$15 Worth Of Radio Shack Parts



Forbes / Security 2 FREE Issues of F

JUL 14, 2015 @ 12:00 PM 26,209 VIEWS

## Tesla Model S Digital Weaknesses To Be Exposed By Hackers Next Month



Hackers Remotely Kill a Jeep on the Highway—With Me in It

BUSINESS DESIGN ENTERTAINMENT GEAR SCIENCE SECURITY

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



BBC Sign in News Sport Weather Shop Earth More

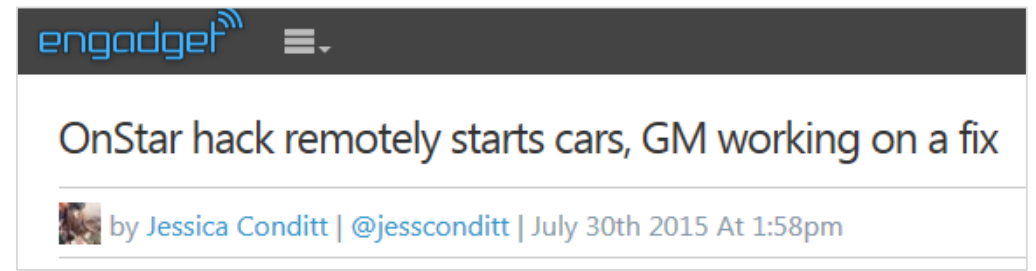
## NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

## Car hack uses digital-radio broadcasts to seize control

By Chris Vallance 22 July 2015



engadget

## OnStar hack remotely starts cars, GM working on a fix

by Jessica Conditt | @jessconditt | July 30th 2015 At 1:58pm



# ... and It's Real!

- Hackers took over the control of a Jeep that was driving on the highway from their basement
- Did it come as a surprise? Not really...



## Report - The Most Hackable Cars (Aug. '14)

*"2014 Jeep Cherokee, 2015 Cadillac Escalade and 2014 Toyota Prius were the most hackable."*

*"The most hackable cars had the most [computerized] features and were all on the same network and could all talk to each other."*

*"The least hackable ones had [fewer] features, and [the features] were segmented, so the radio couldn't talk to the brakes."*

*Charlie Miller, security engineer*

**WIRED** SUBSCRIBE

### Hackers Remotely Kill a Jeep on the Highway—With Me in It

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

The paper: <http://illmatics.com/Remote%20Car%20Hacking.pdf>



# The Connected Car...

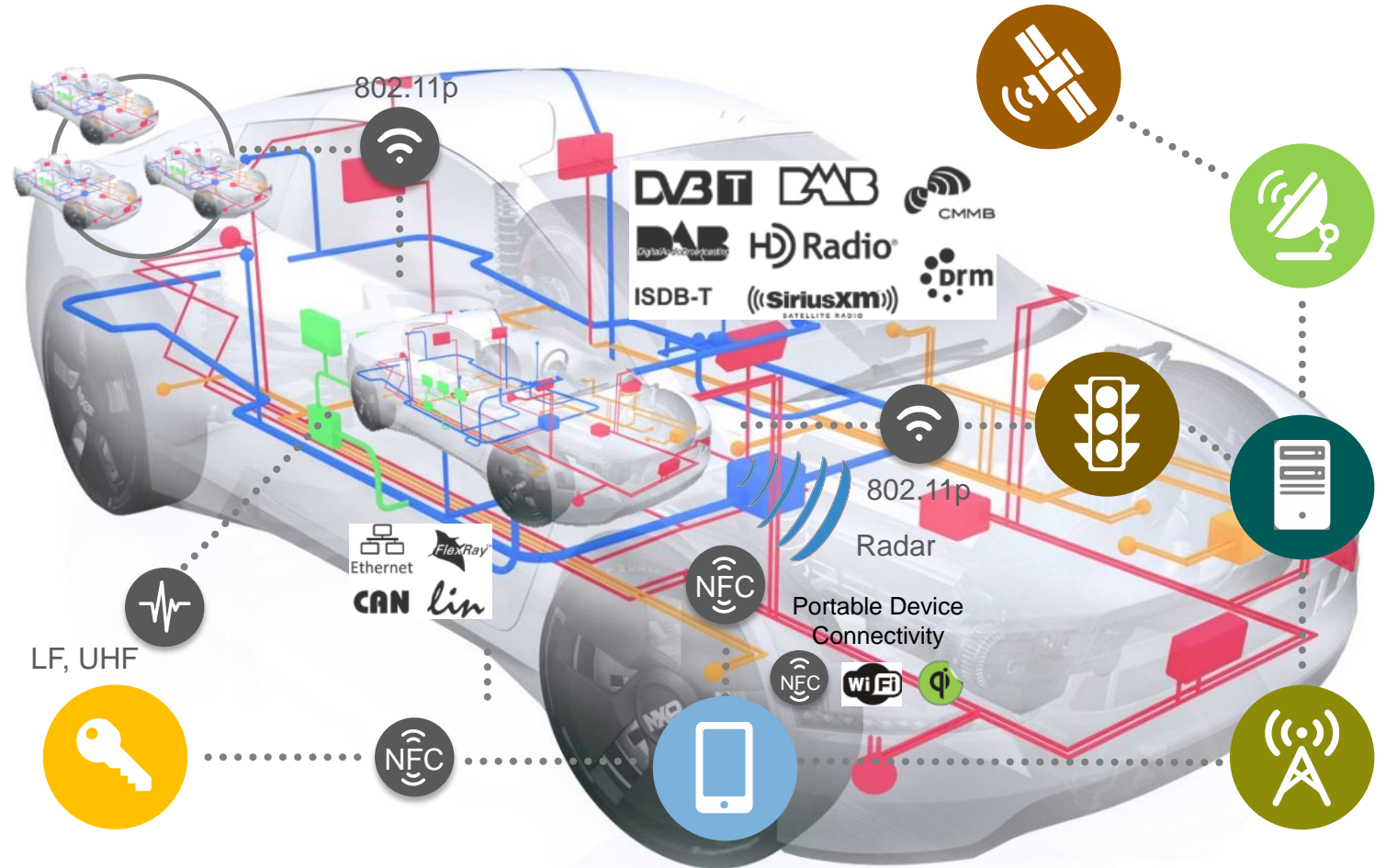
A Cloud-connected Computer Network on Wheels

- **A networked computer**

- up to 100 ECUs per car
- and many sensors
- inter-connected by wires
- more and more software

- **Increasingly connected to its environment**

- to vehicles & infrastructure
- to user devices
- to cloud services



# ... is an Attractive Target for Hackers!

**Valuable Data**

- Collection of data/info
- Storage of data
- Diagnostic functions



 **Protect Privacy**

**High Vulnerability**

- Increasing number of nodes
- More advanced features
- X-by-Wire



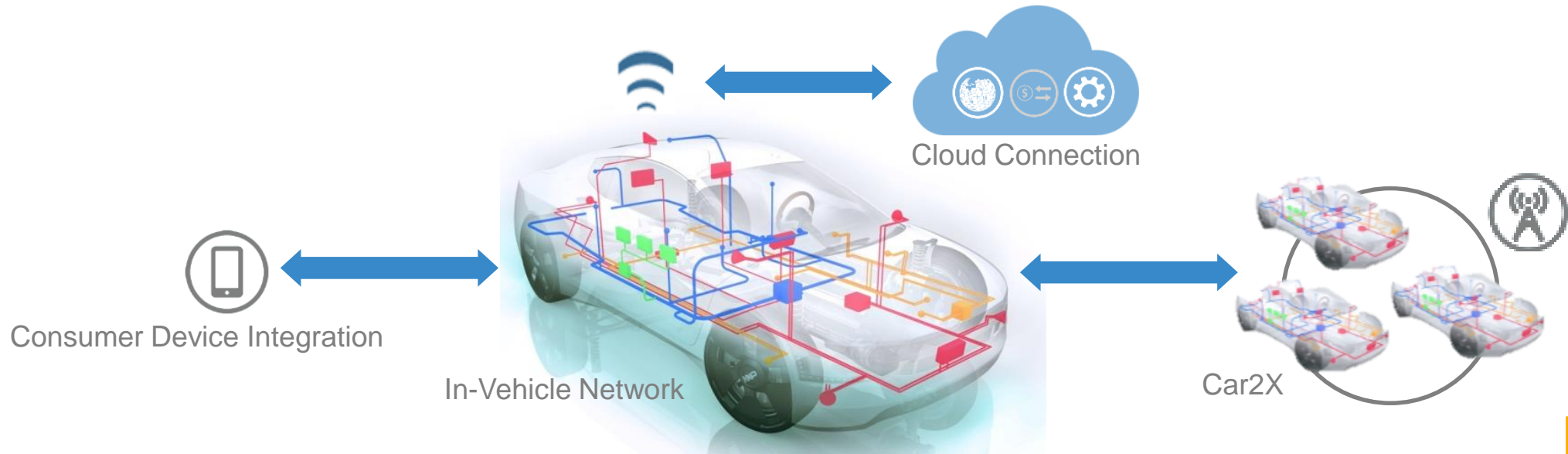
 **Increase Safety**

**Easy (Remote) Access**

- Fully Connected Car
- External & internal interfaces
- Wired & wireless interfaces



 **Prevent Unauthorized Access**



# WHAT IS SECURITY



# Security Requires a Different Mindset



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

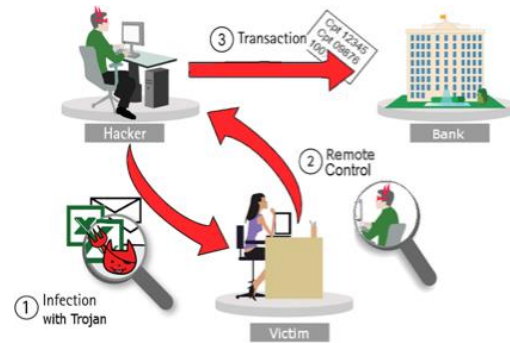
# What is Security?

- Security is a **quality aspect**...
  - Attackers should not be able to subvert the proper operation of a system
- ...in an **uncontrolled** and **evolving environment**
  - Attackers do not obey to “the rules”
  - Attack(er)s only get better over time
- Security must be an **integral part of the system design**
  - Security is as strong as the weakest link → point solutions usually don't work
  - Secure by design vs. security as an afterthought
- **100% secure does not exist** in the real world
  - It's about finding the right balance between costs (protection level) and benefits (risk reduction)

# Functional Security vs. Physical Security

## Logical Attacks

- Targeting devices that are remotely accessible
- Attack Potential: (enhanced) basic



## Physical Attacks

- Targeting devices that live in a hostile environment
- Attack Potential: moderate to high



Invasive Attacks

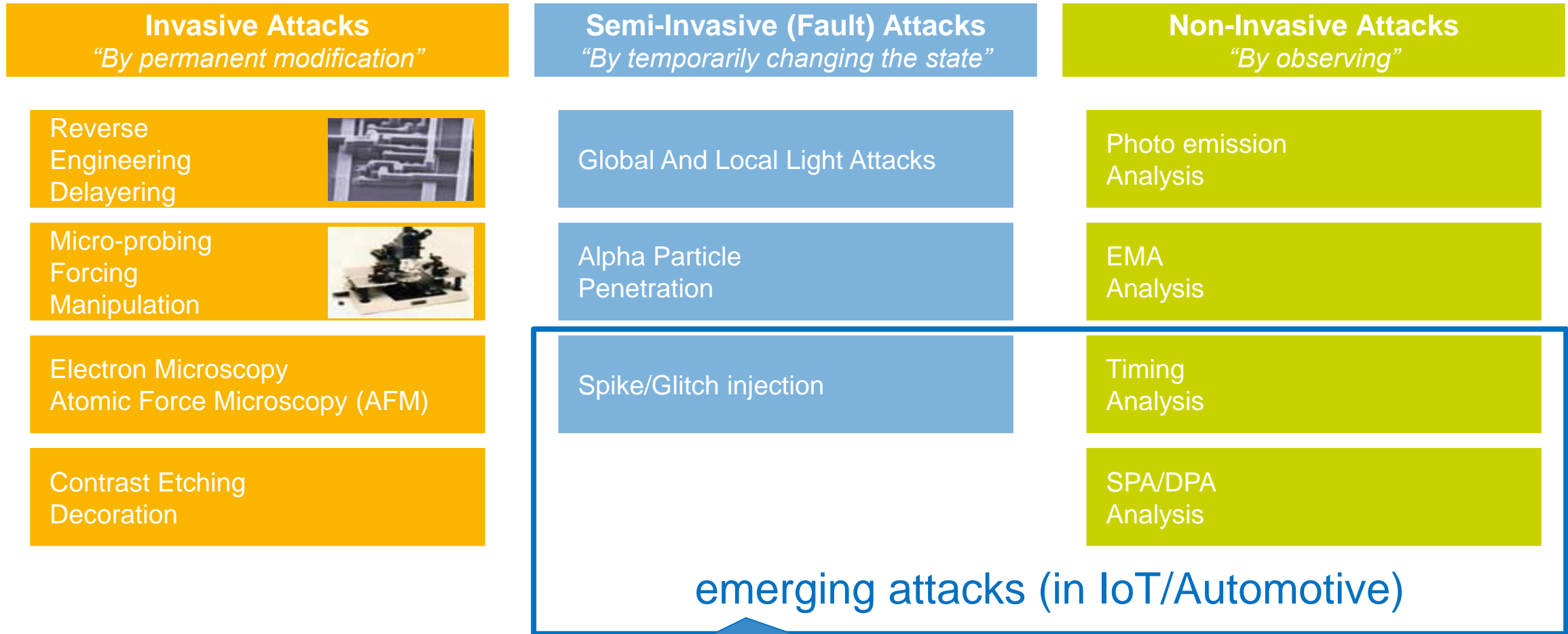


Information Leakage Attacks



# Classification of Physical IC Attacks

Countermeasures (“Tamper-resistance”) Require Very Specific IC Designs...



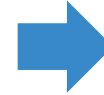
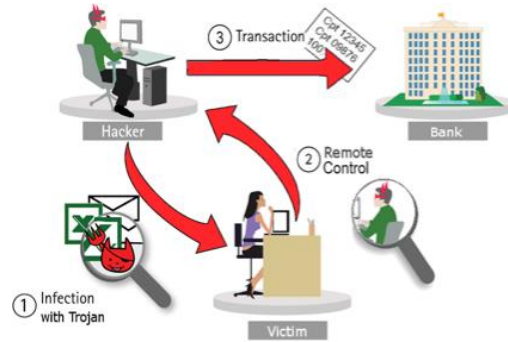
**ChipWhisperer:** \$130 kit (open source software, hardware and training).  
Objective: enable engineers/hobbyists to perform side-channel attacks.



# Functional Security vs. Physical Security

## Logical Attacks

- Targeting devices that are remotely accessible
- Attack Potential: (enhanced) basic



## Functional Security

- “Internet security” with strong crypto, secure protocols, secure boot, e2e security, authentication
- Supported by hardware (for isolation, acceleration)
- Implementation is not important: a skilled attacker in possession of a device will hack it

## Physical Attacks

- Targeting devices that live in a hostile environment
- Attack Potential: moderate to high

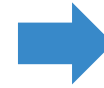


Invasive Attacks

Fault Injection



Information Leakage Attacks



## Physical Security

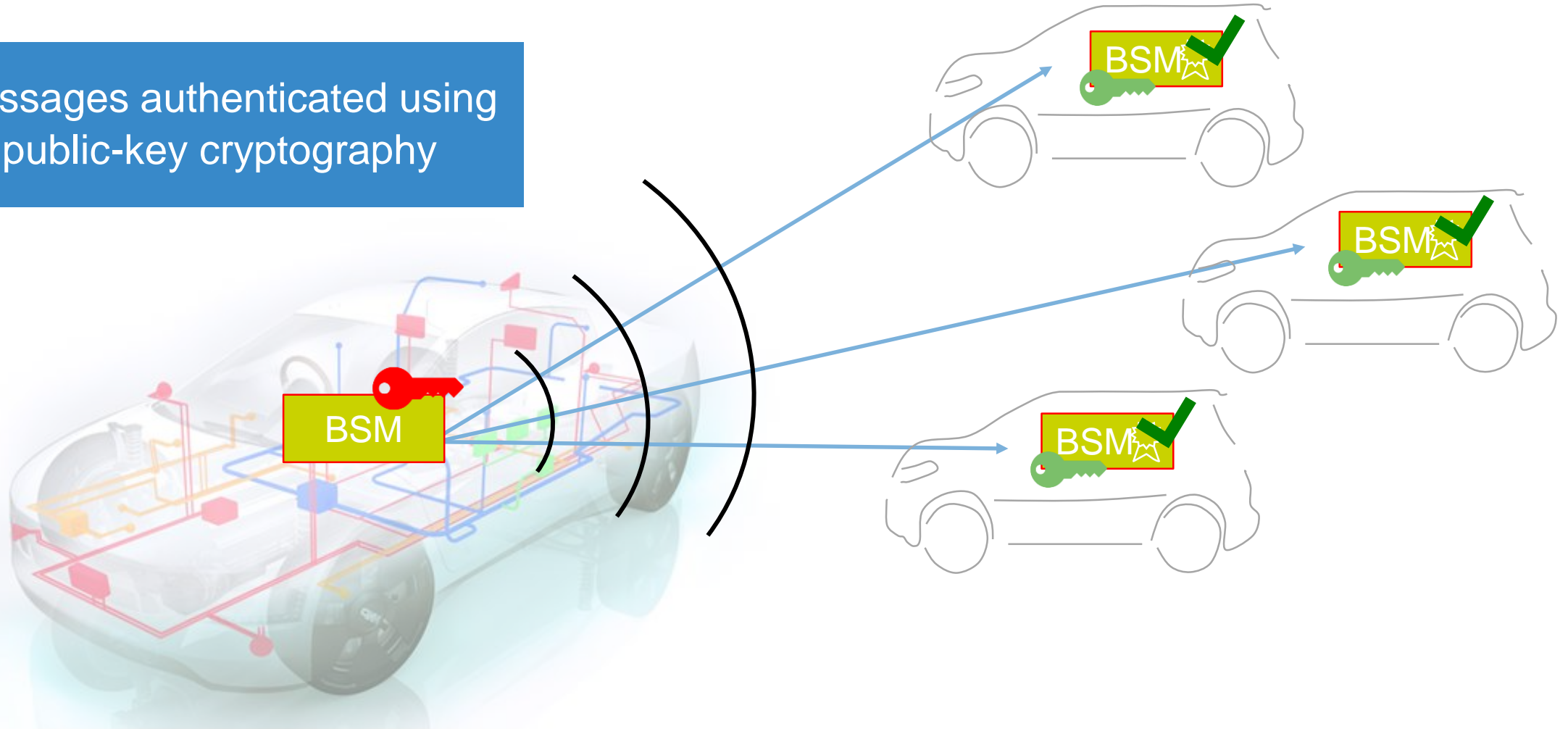
- Functional security, **plus** protection against physical attacks such as side-channel analysis, fault injection, reverse engineering, etc.
- Supported by dedicated, hardened hardware (providing a high level of tamper-resistance)
- Implementation of HW & SW matters: high resistance against a skilled attacker in possession of the device

Physical attacks are difficult... but they may lead to remote (scalable) attacks!

# Example: Forging V2X Communication

Normal Operation: Broadcast of Basic Safety Messages

Messages authenticated using  
public-key cryptography

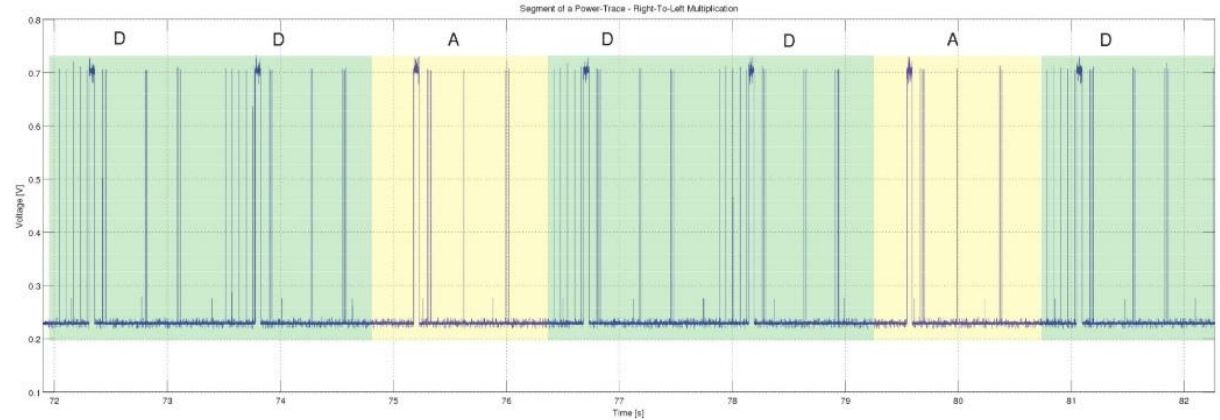




# Example: Forging V2X Communication

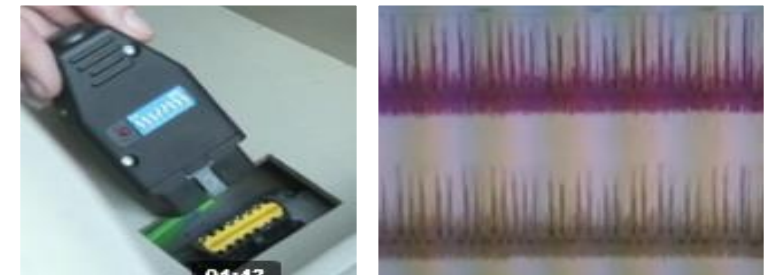
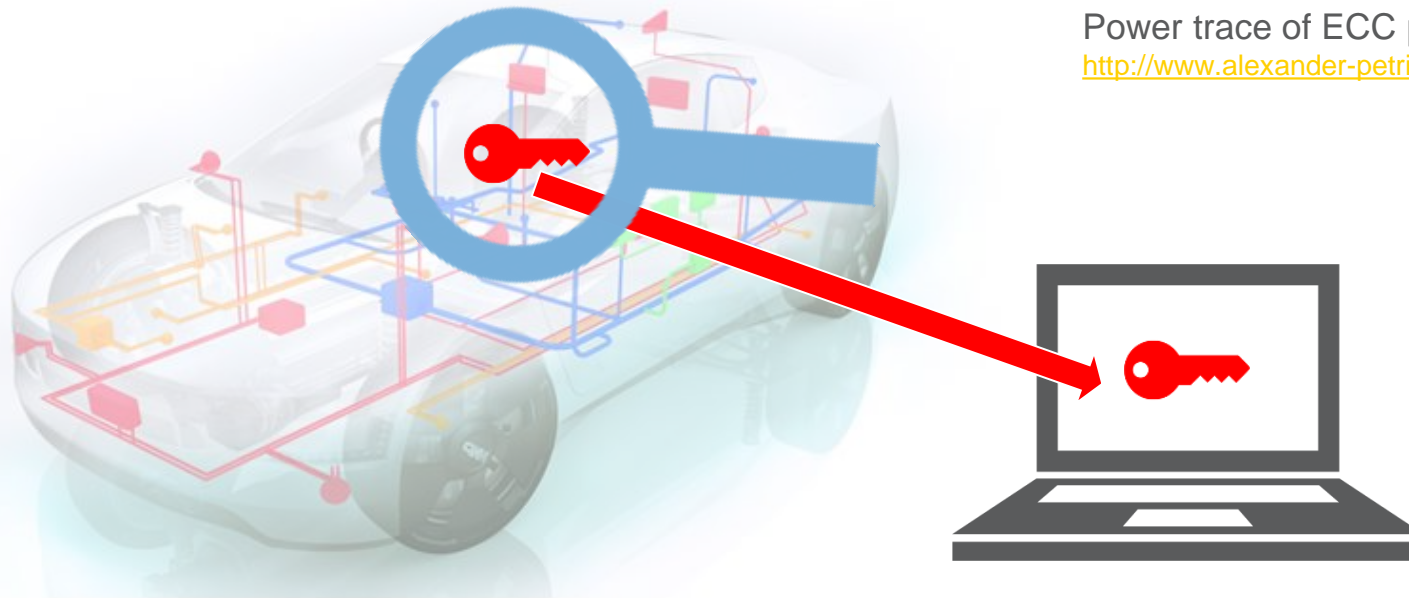
## Extracting Private Keys Using Side-Channel Analysis (SCA)

Physical attack using side channel analysis, fault injection, reverse engineering etc.



Power trace of ECC point multiplication, additions and doublings

<http://www.alexander-petric.com/2011/08/side-channel-attack-measurement-setup-2.html>



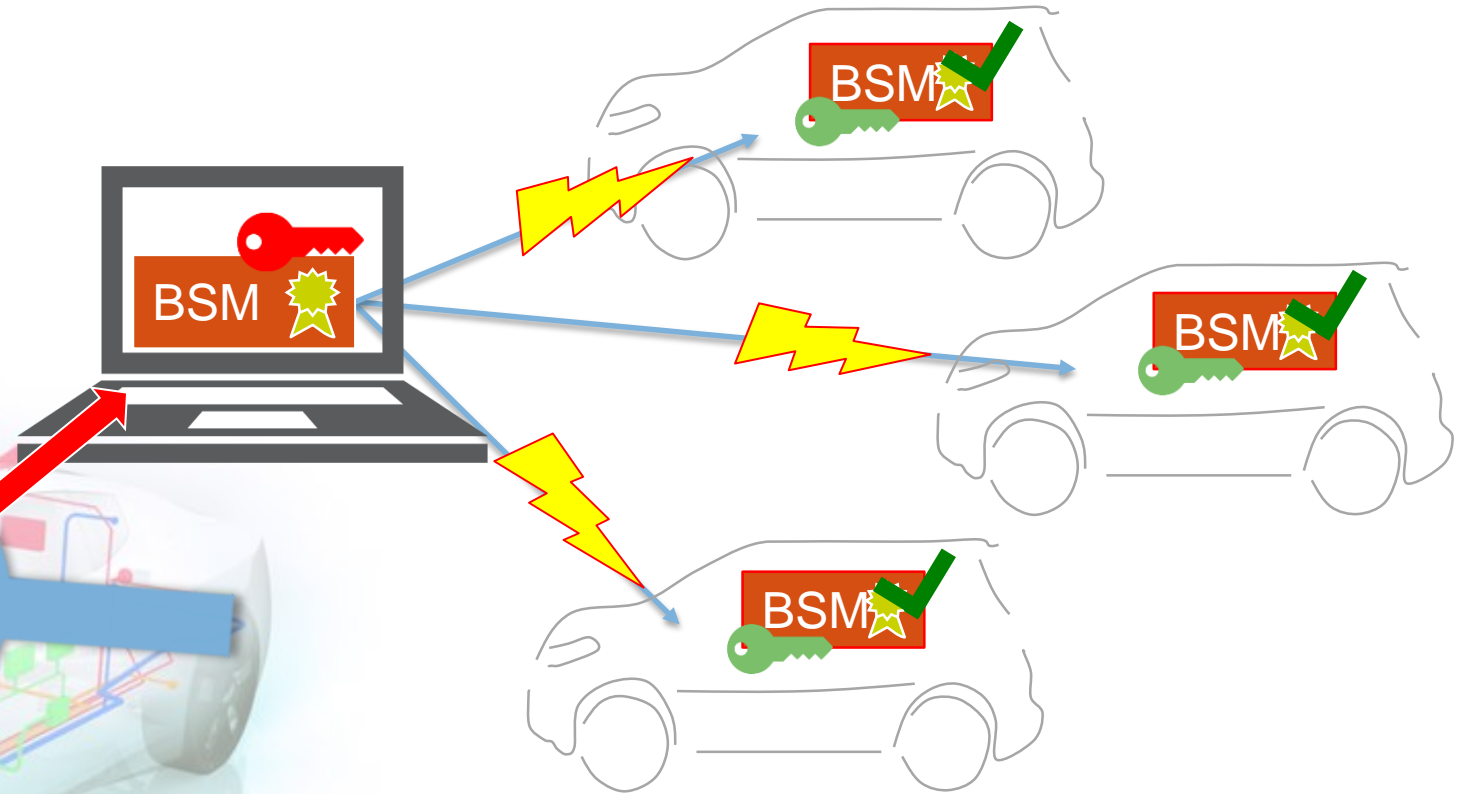
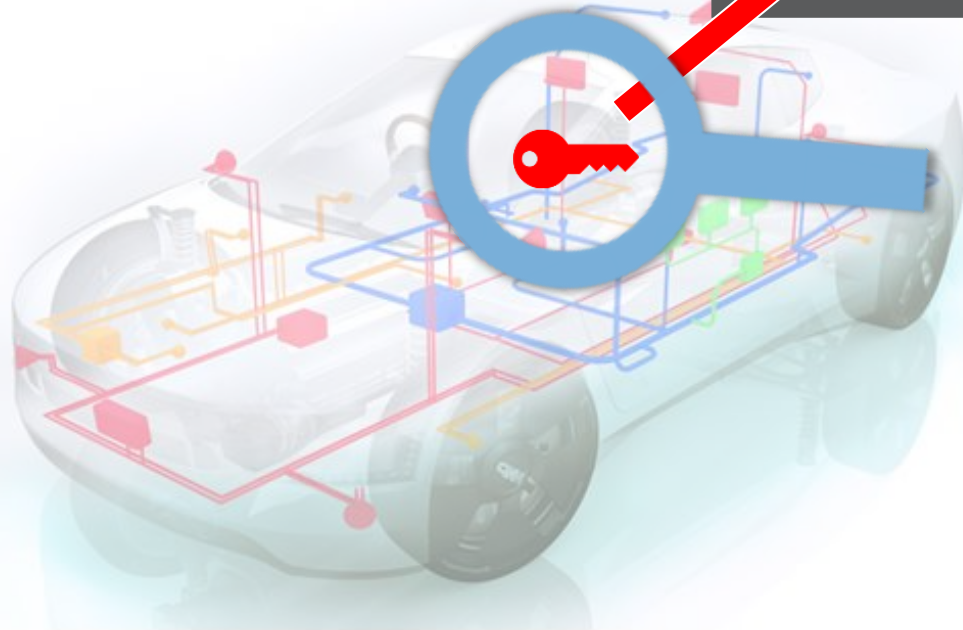
Demo of a side channel attack on smart phone  $\mu$ C by Cryptography Research

<https://www.youtube.com/watch?v=4L8rnYhnLt8>

# Example: Forging V2X Communication

Scalability: One to Many

Attacker is able to send malicious messages that are considered trustworthy

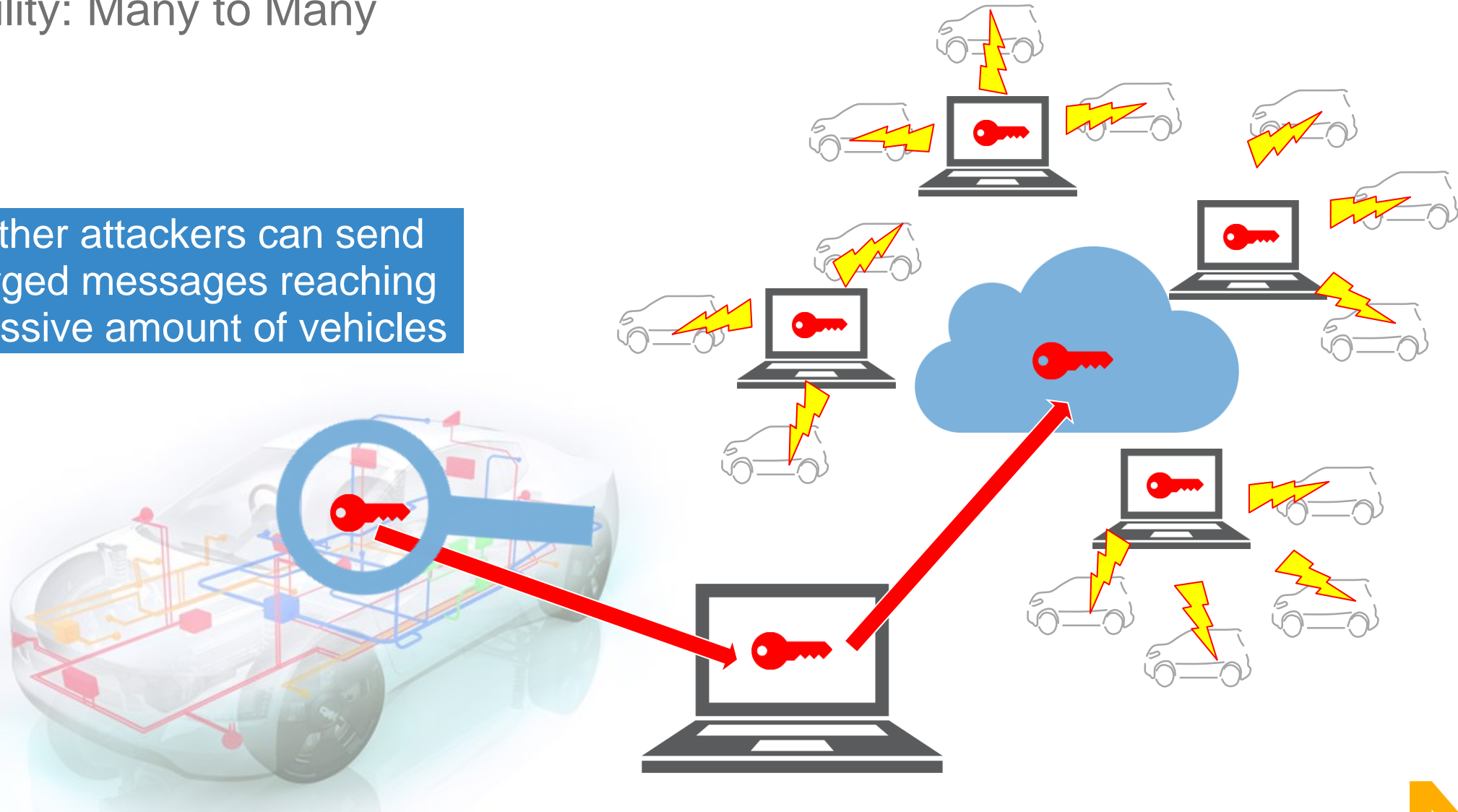


Receiving vehicles cannot recognize forged and hazardous messages

# Example: Forging V2X Communication

Scalability: Many to Many

Other attackers can send forged messages reaching massive amount of vehicles



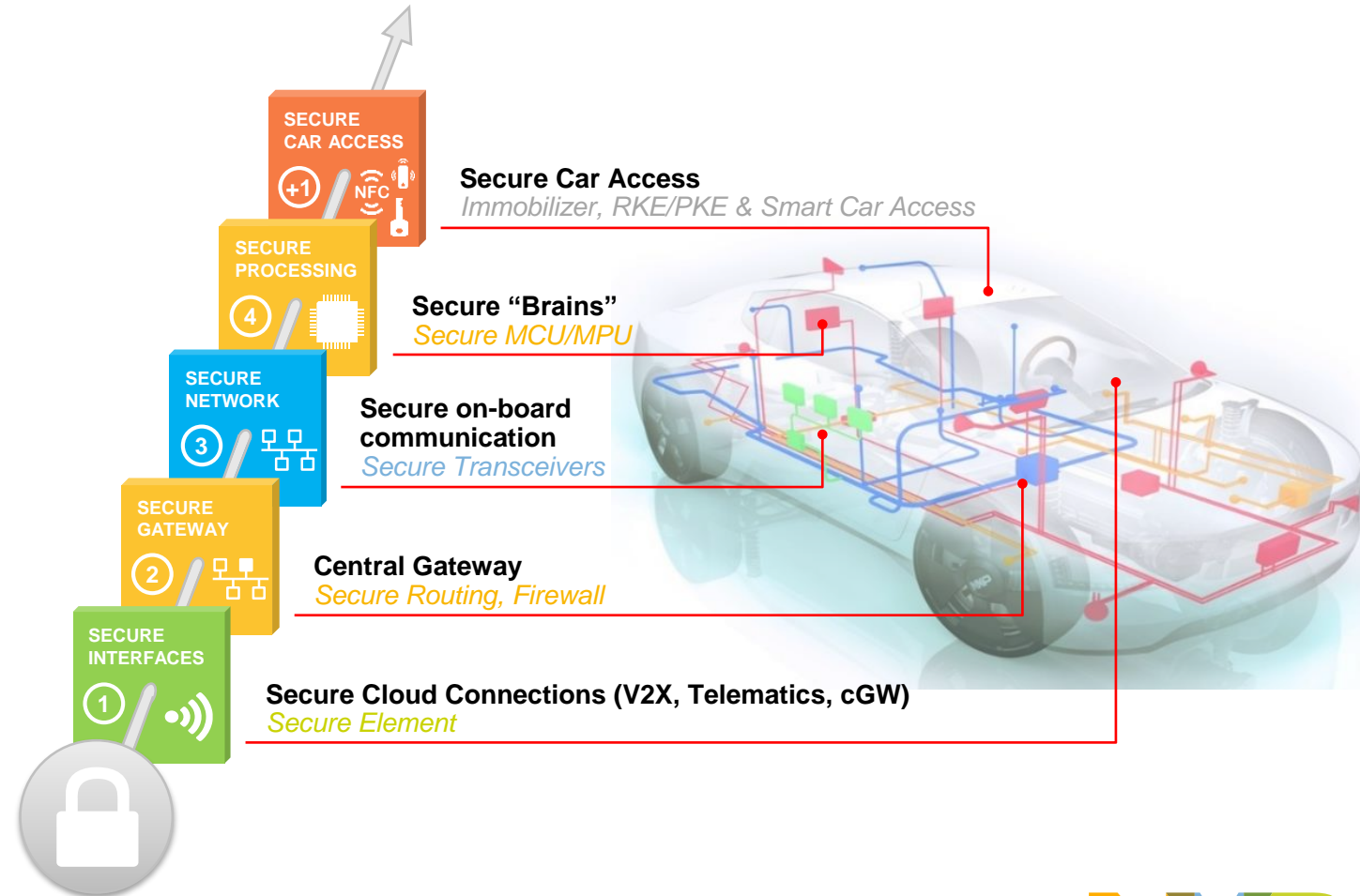
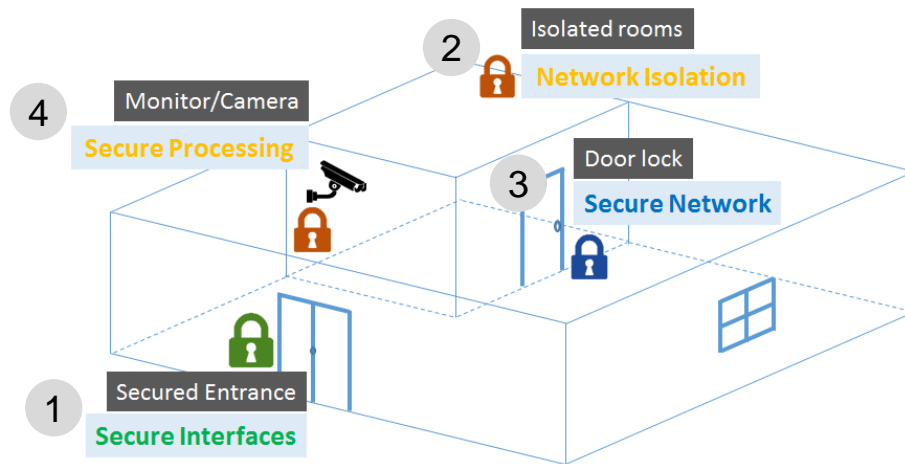
# SECURITY APPROACH



# Security Requires a Layered Approach

For Connected Cars, As Well As For e.g. Your House

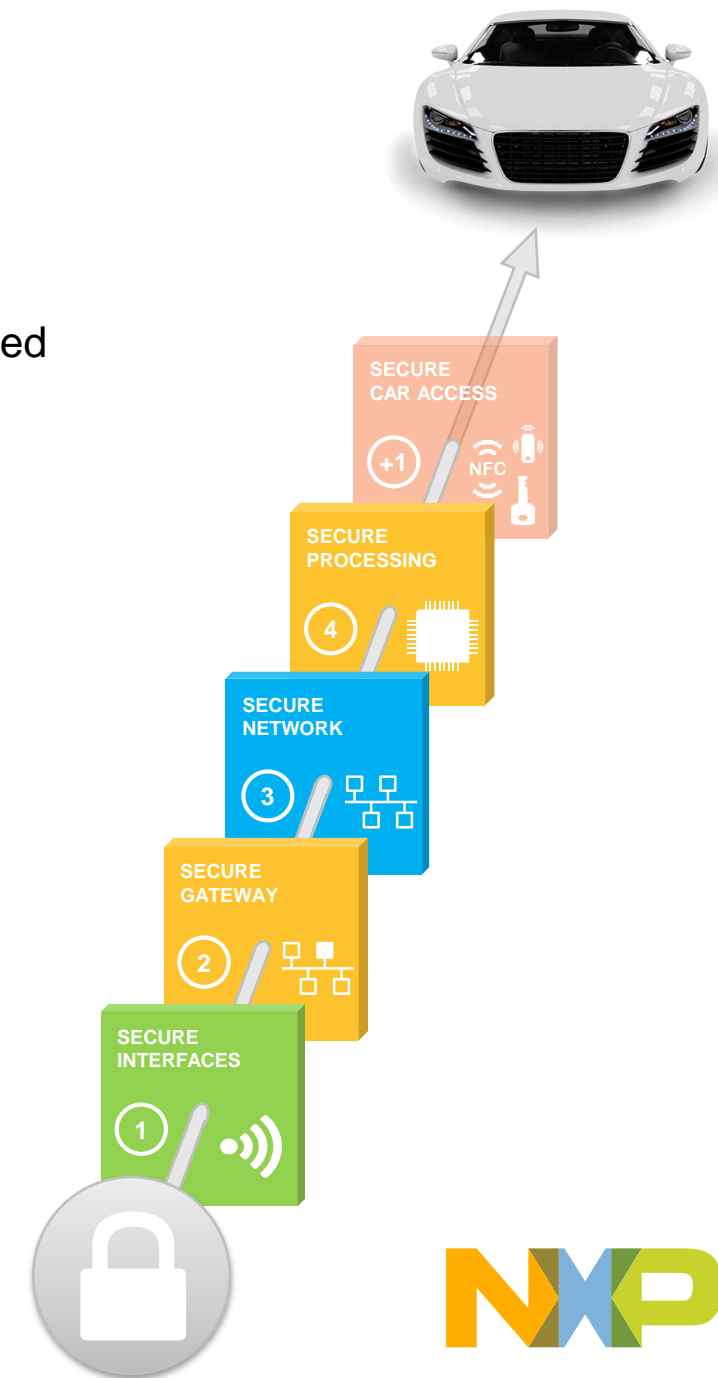
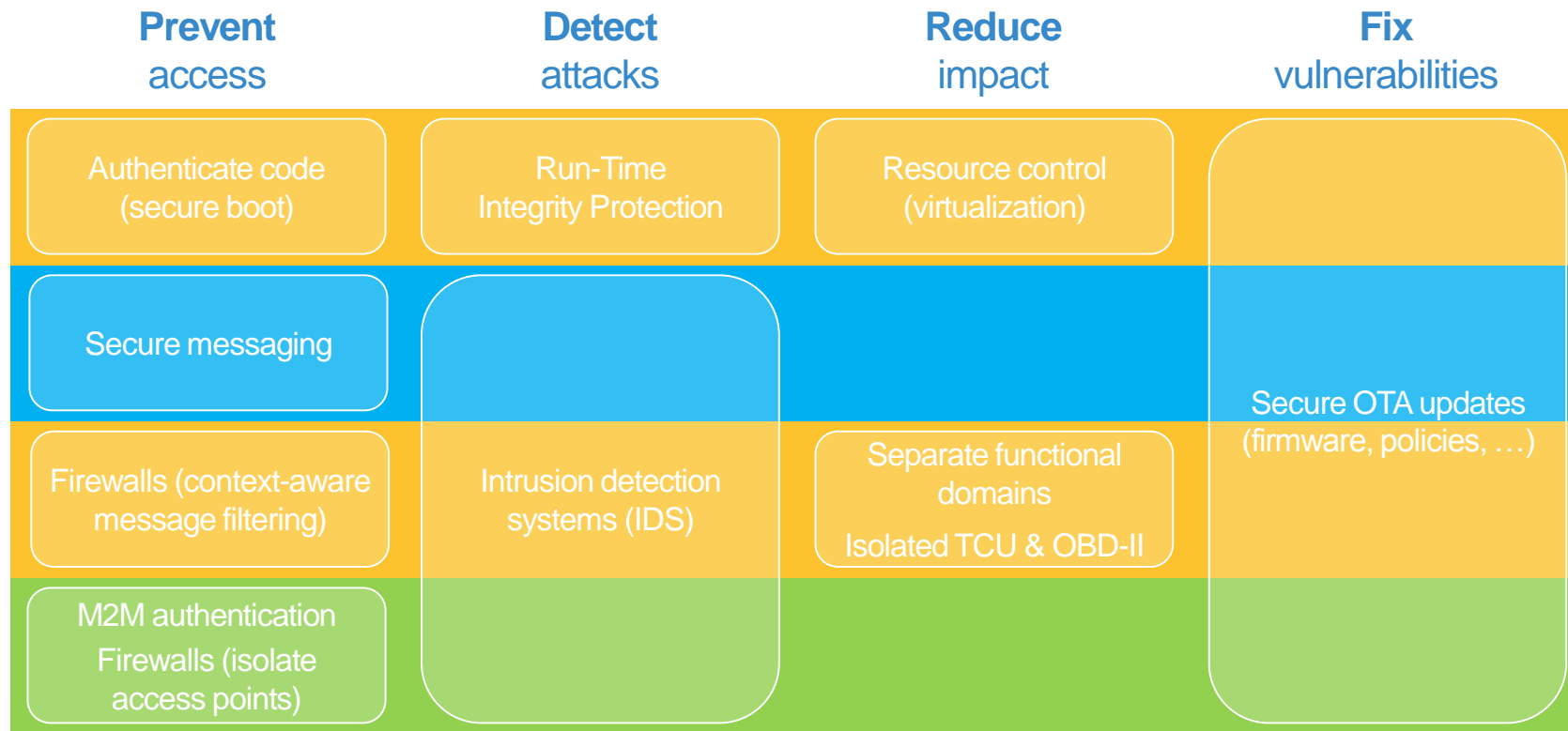
- Multiple security techniques, at different levels (a.k.a. defense-in-depth)
- To mitigate the risk of one component of the defense being compromised or circumvented



# Defense in Depth

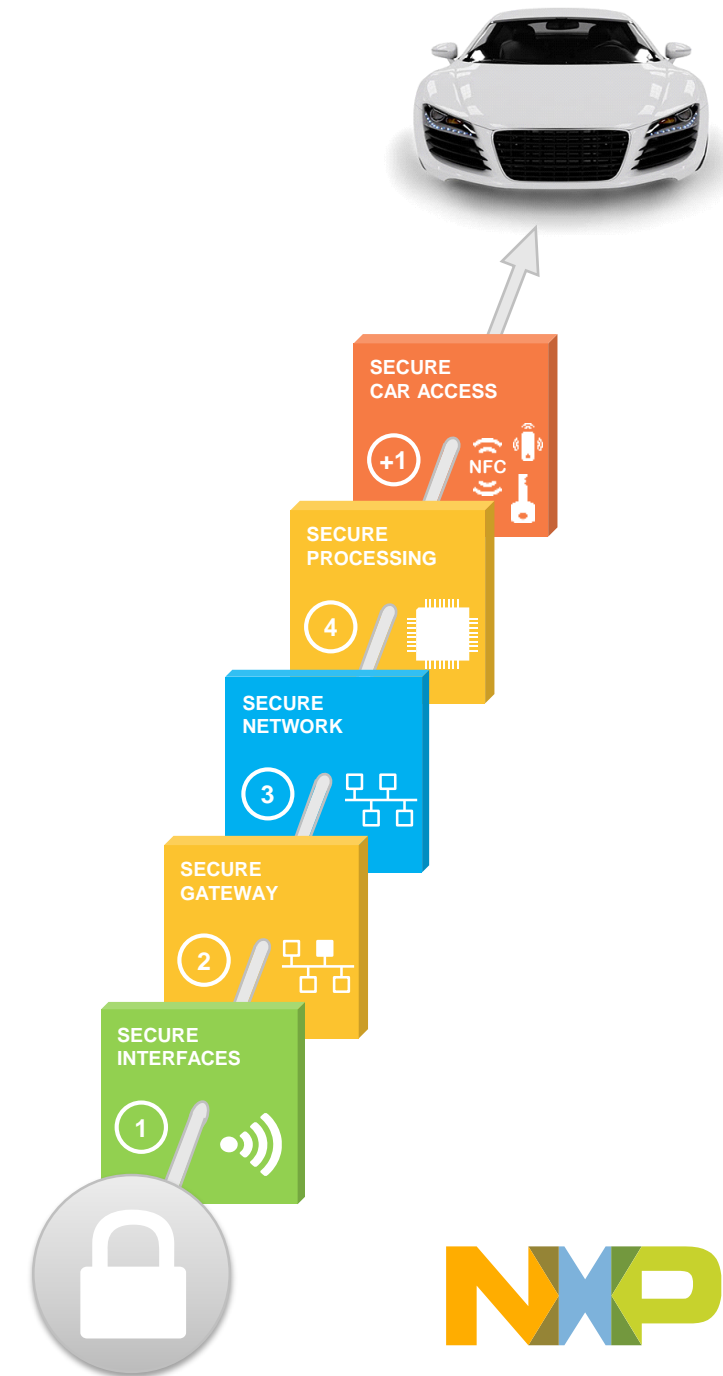
## Securing the Vehicle's Electronics Architecture

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



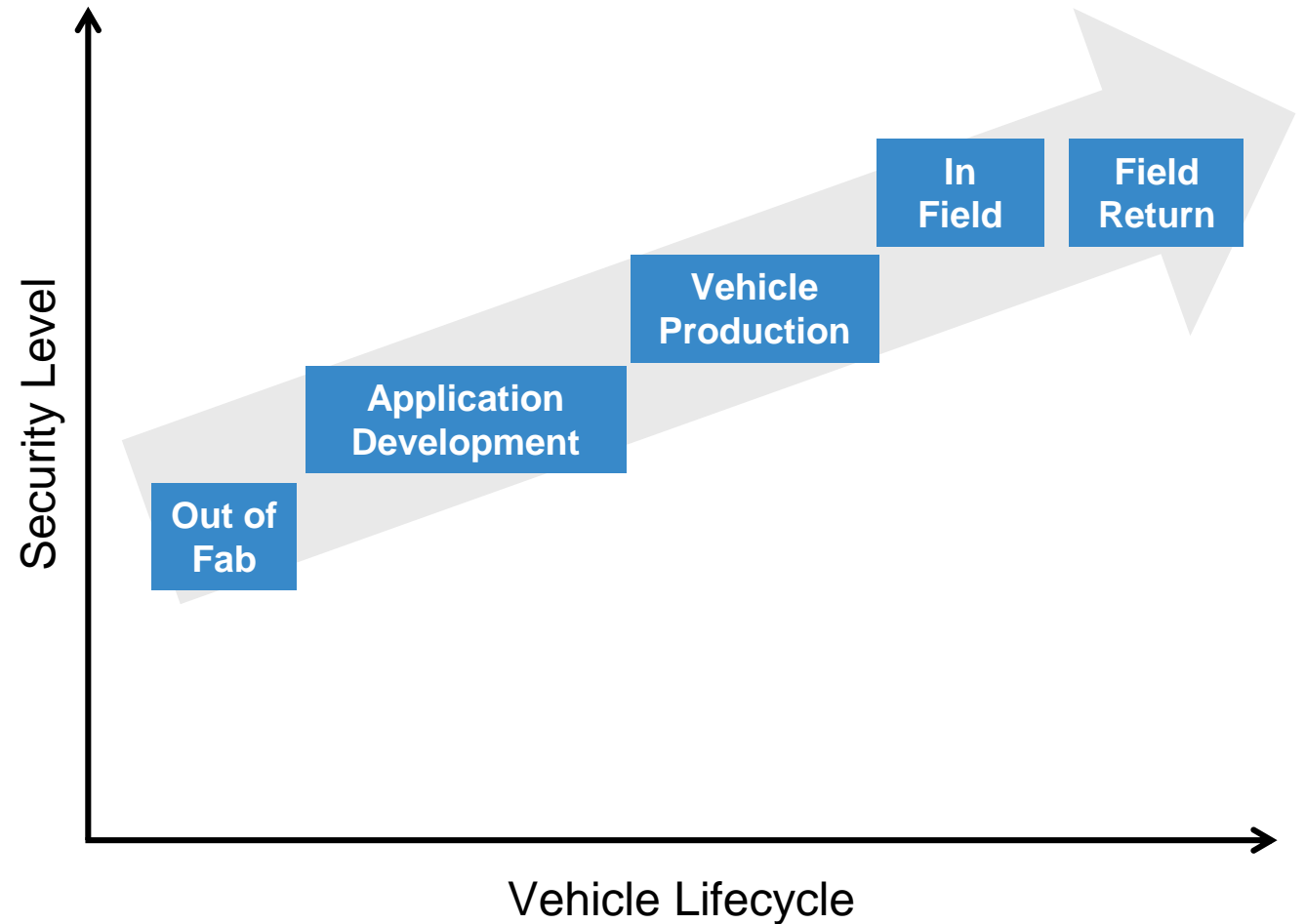
# Hardware Security is a Must

- **Crypto accelerators**,  
to guarantee strict performance requirements
  - E.g. message authentication (V2X, CAN), 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 Throughout the Entire Lifecycle

- Increased security level at each stage of the development lifecycle
- Non-reversible, non-revocable
- Enable application development, debugging and failure analysis
- Without compromising security in the production vehicle

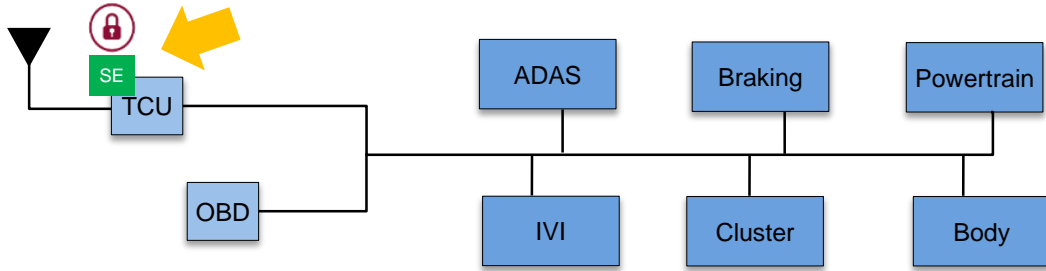




# 4 Layers to Securing a Car

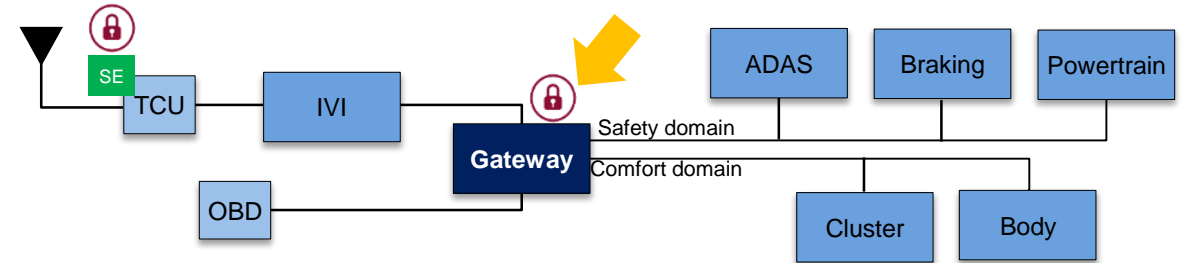
## Layer 1: Secure Interface

Secure M2M authentication, secure key storage



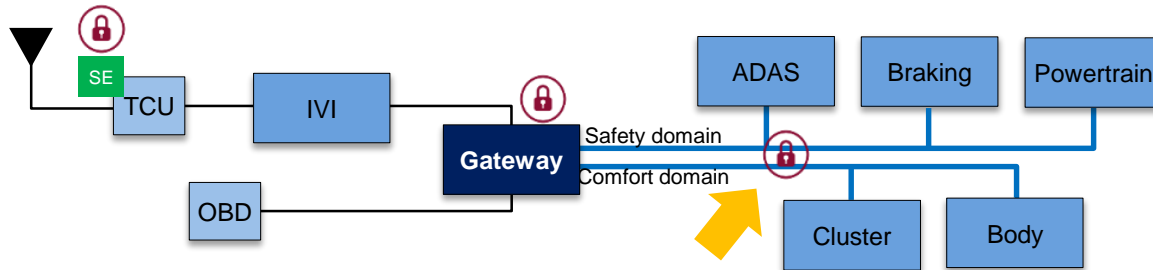
## Layer 2: Secure Gateway

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



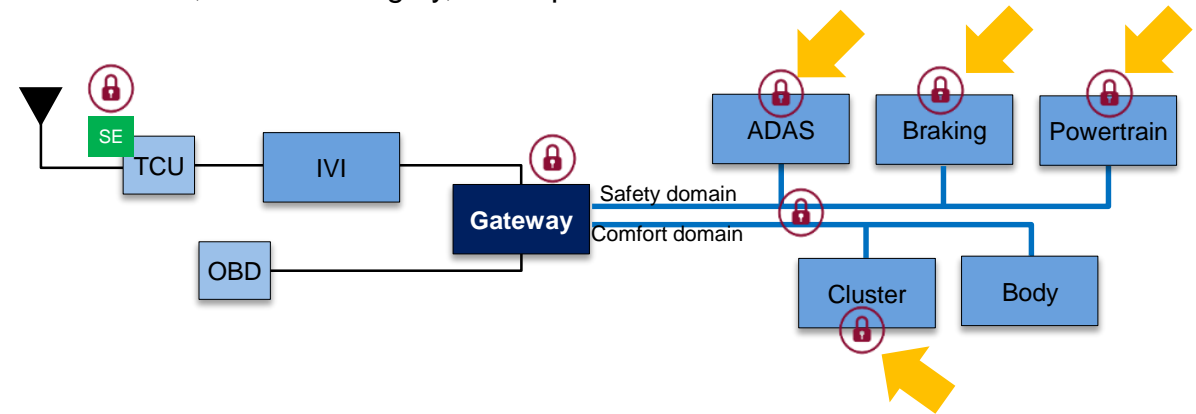
## Layer 3: Secure Network

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

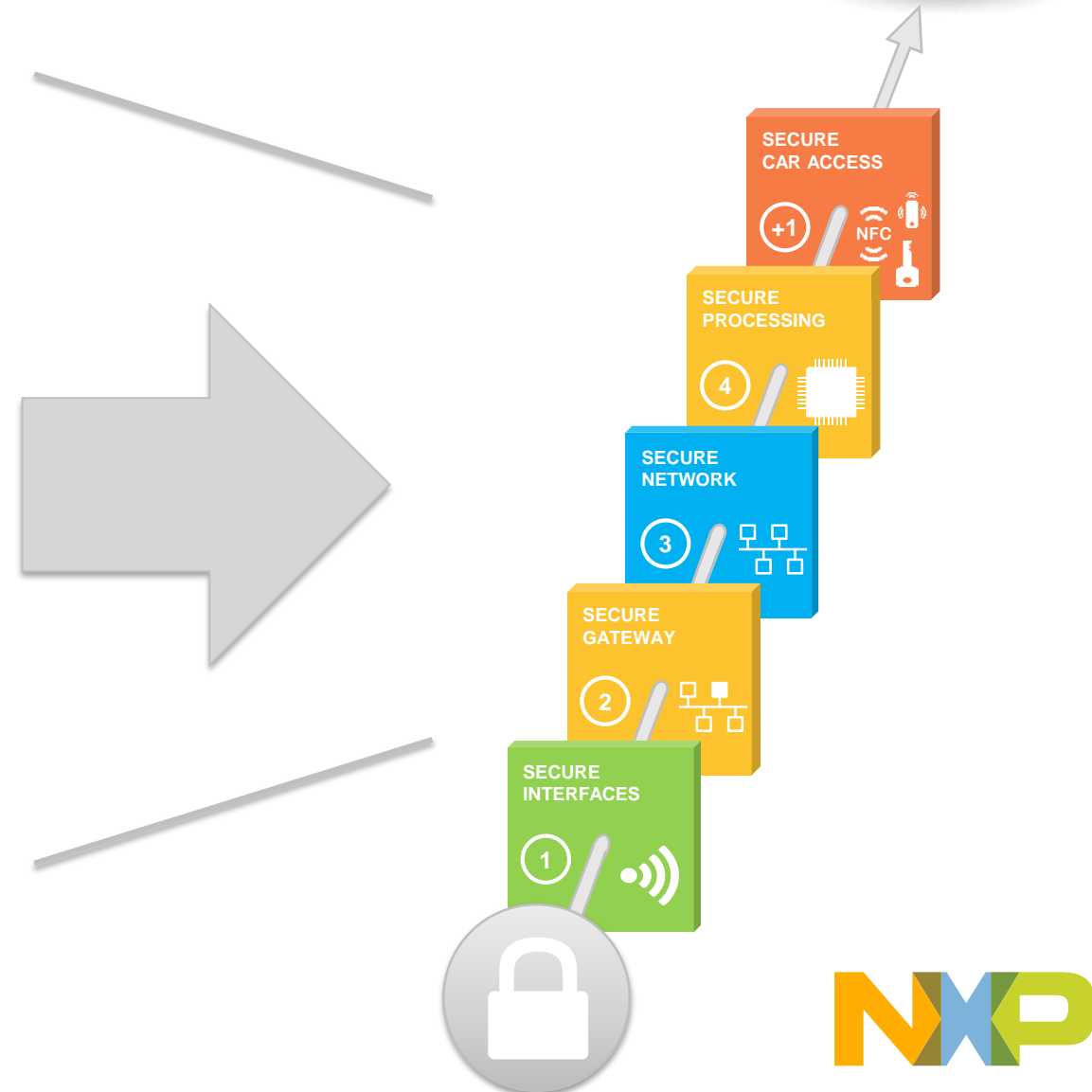
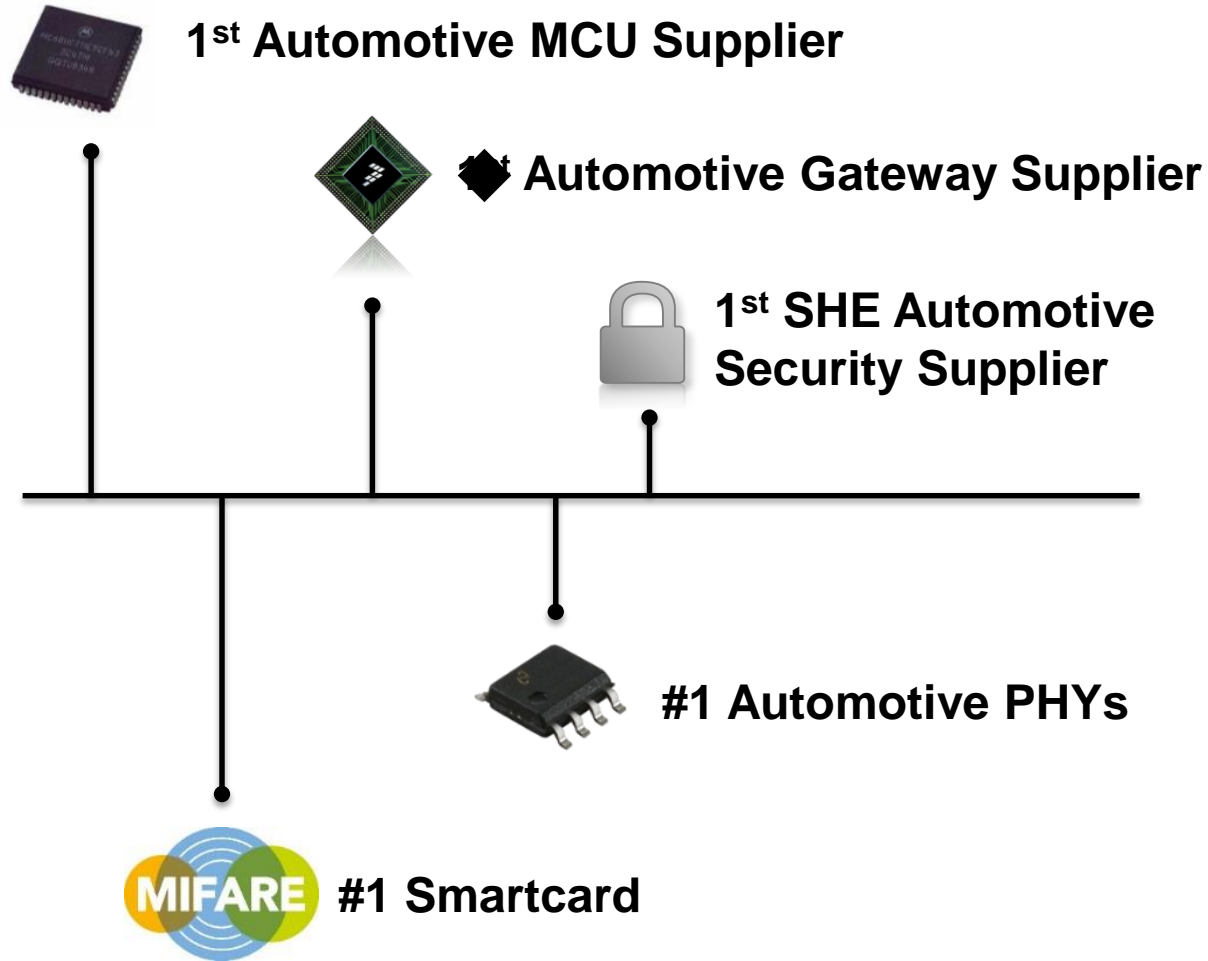


## Layer 4: Secure Processing

Secure boot, run time integrity, OTA updates



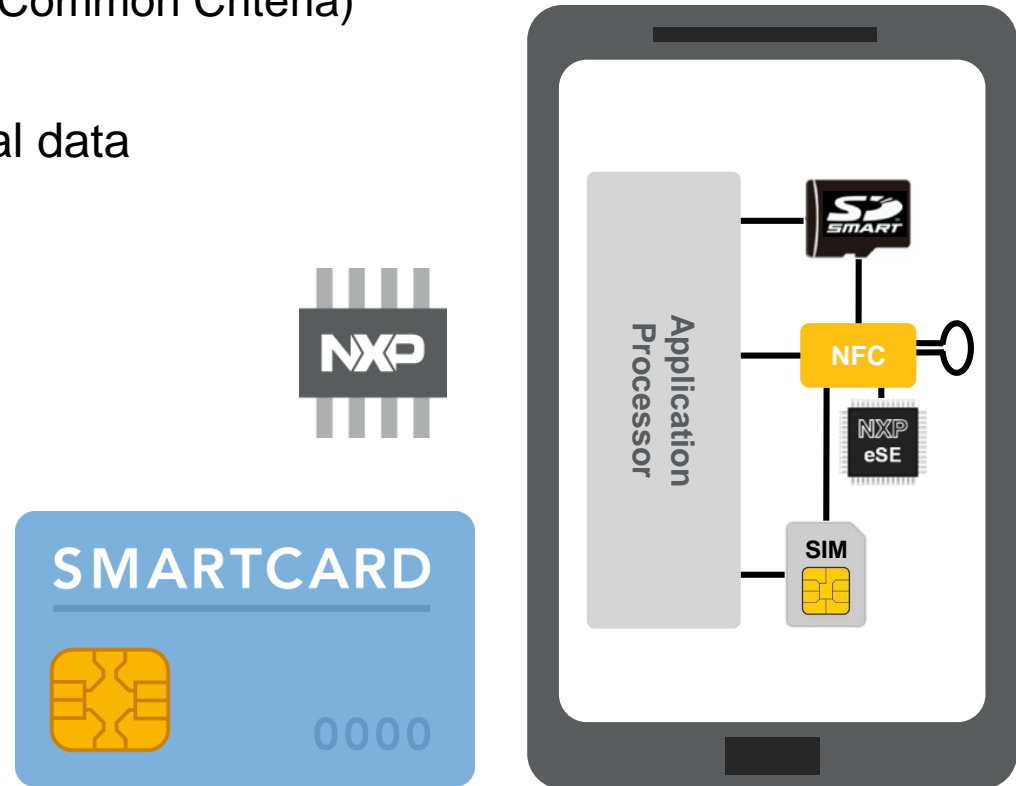
# Building on a Strong Legacy



# 4+1 LAYERS

# Layer 1 – Secure Element: What is It?

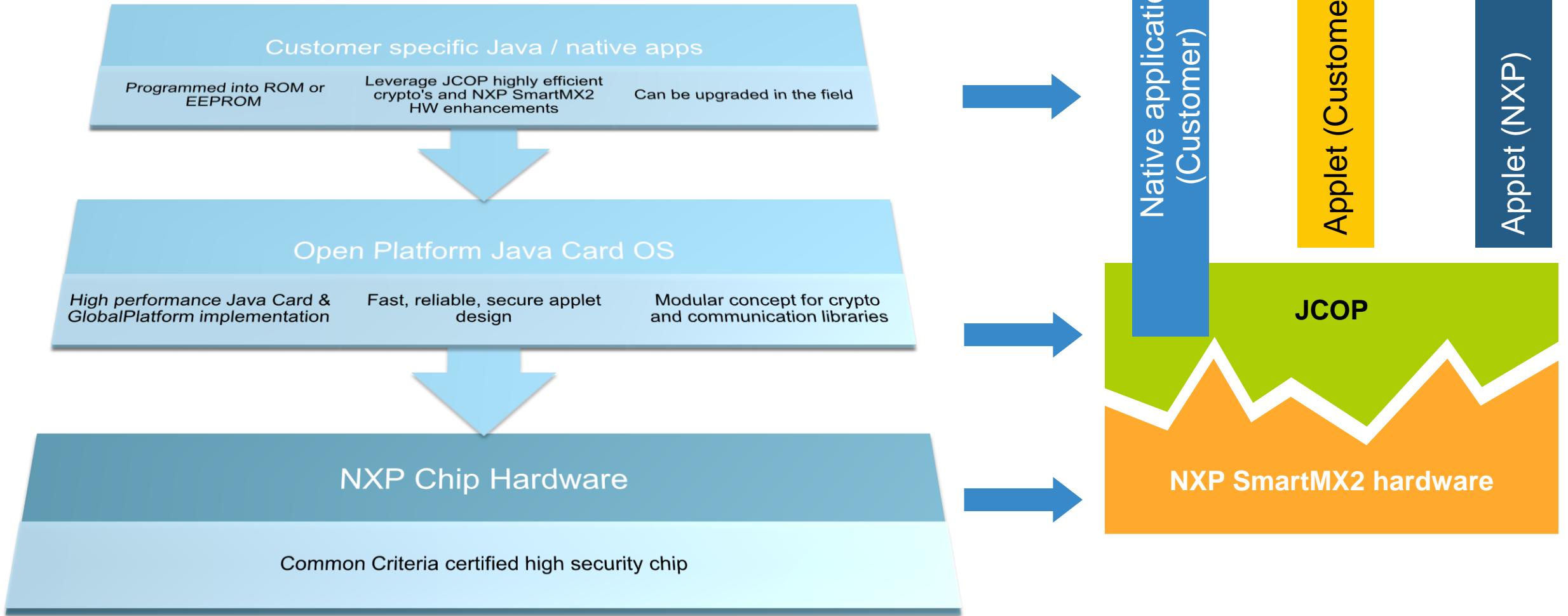
- A tamper-resistant platform, that protects against physical attacks
  - Proven security, via 3<sup>rd</sup> party evaluation and certification (Common Criteria)
- Securely hosts security applications and their confidential data
  - Banking cards, electronic passports, V2X, Telematics, ...
- Provides 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





# Secure JAVA CARD OS (JCOP)

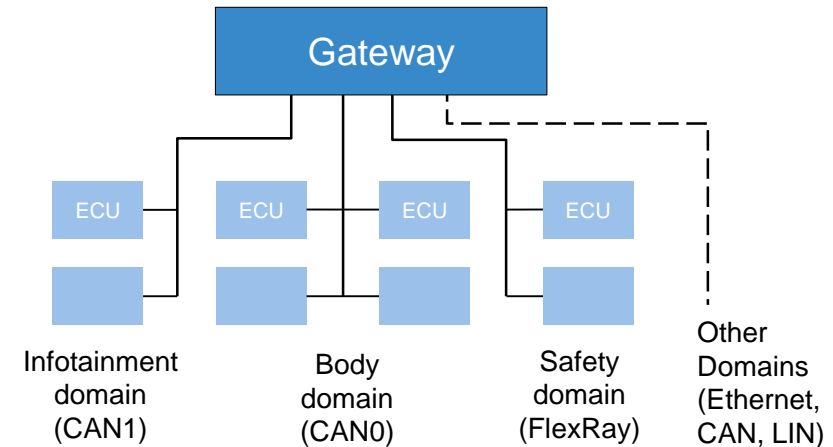
Rich Platform, Enabling Fast Software Development



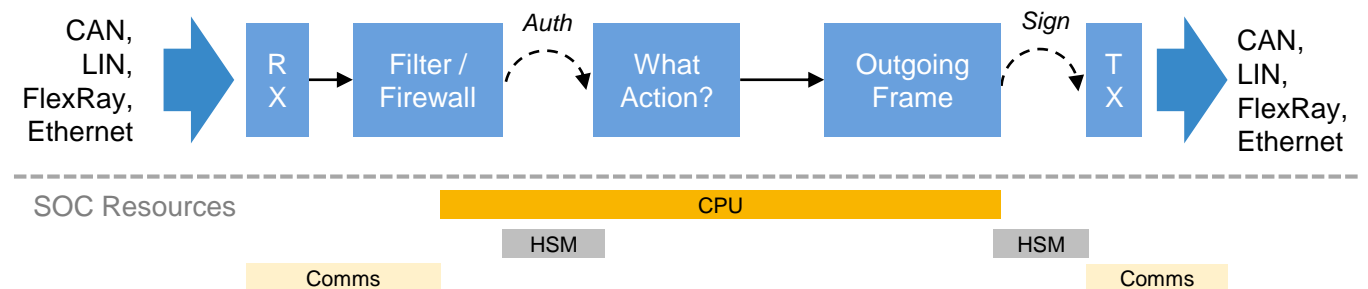
# Layer 2 – Gateway: What is It?

- **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

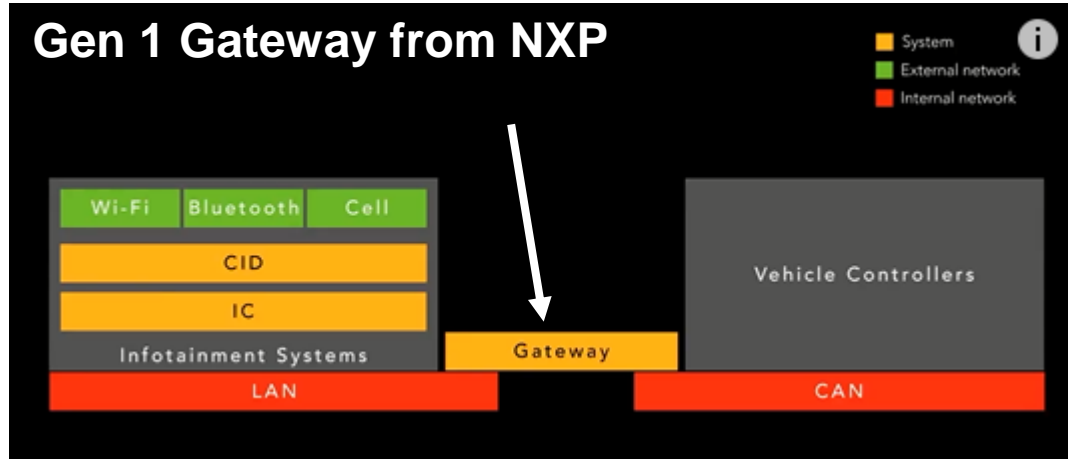
## Vehicle Architecture (Simplified)



## Gateway Function



# The Tesla 'Model S' Hack



***“We believe that the Tesla Model S is an archetype for what all cars will look like in the future – others will follow”***

**Marc Rogers**



***What every car company should do:***

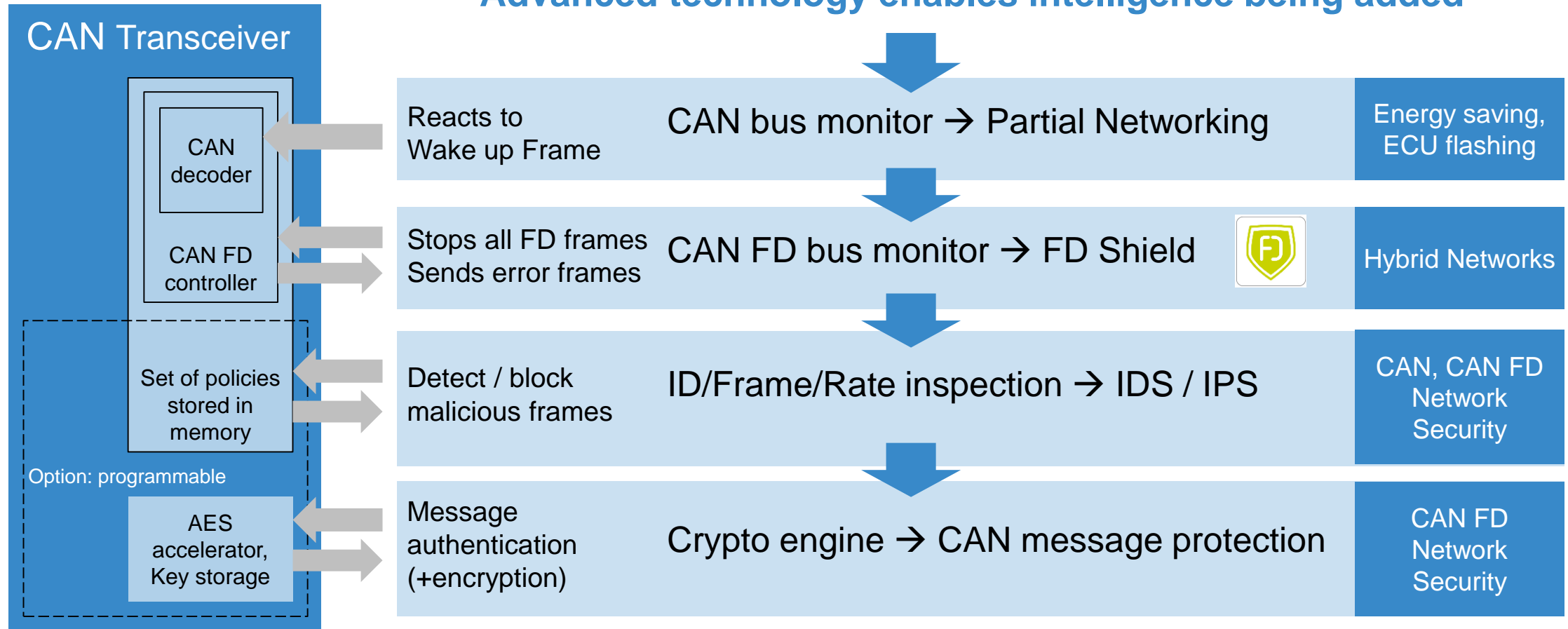
1. OTA Update process
  - Without customers having to subscribe to separate data service
2. Isolation of vehicle and infotainment systems
  - Have a “[gateway](#)”
  - Spend a lot of effort securing the “[gateway](#)”
3. Harden each component individually
  - Assume infotainment is compromised

*M. Rogers*



# Layer 3 – Secure Network: What is It?

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





# Product Solutions

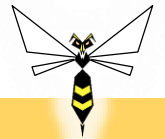
## Stinger:

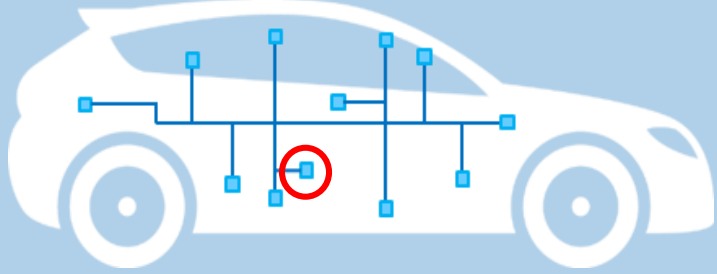
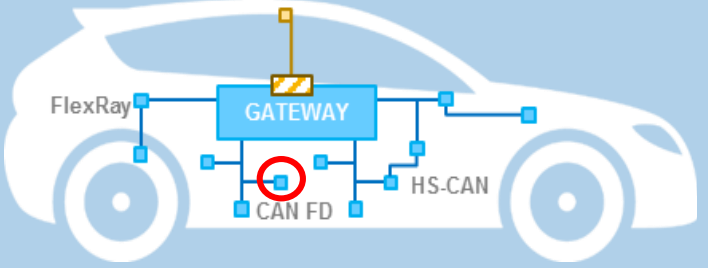
Programmable CAN message monitor



## GoldBEE:

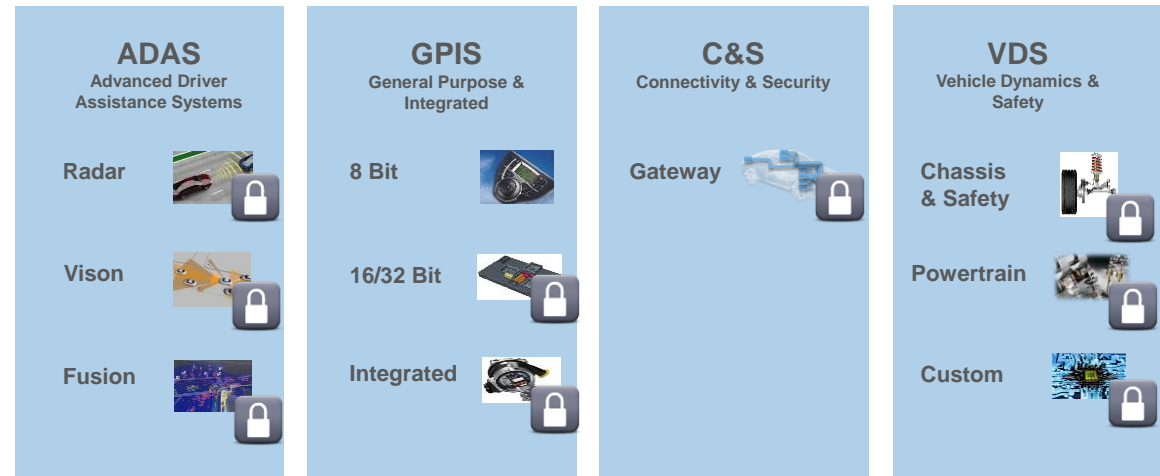
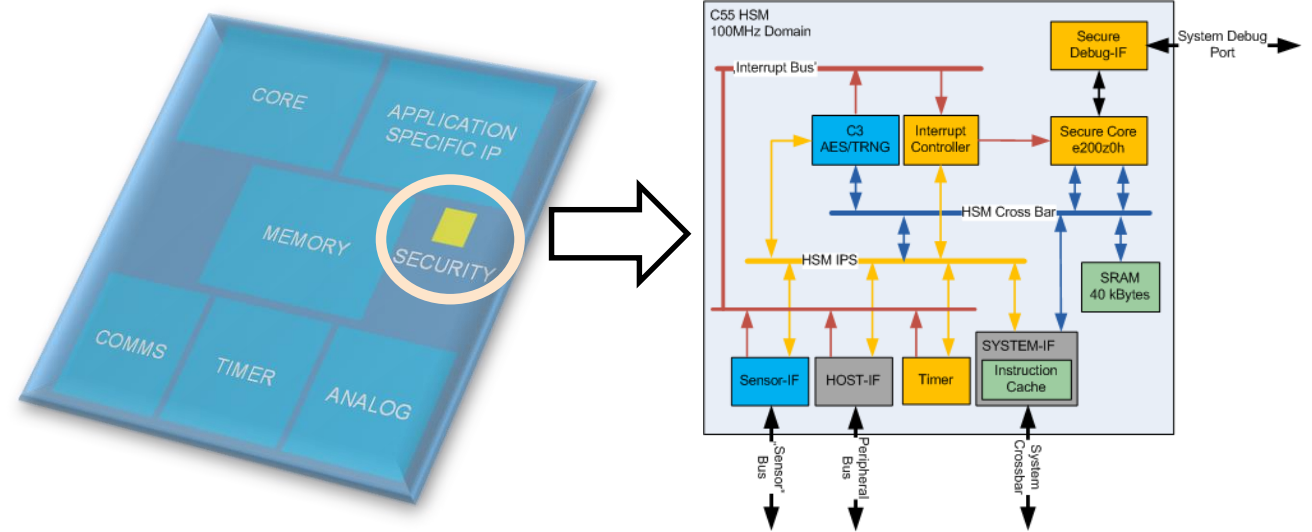
Fully integrated secure CAN node



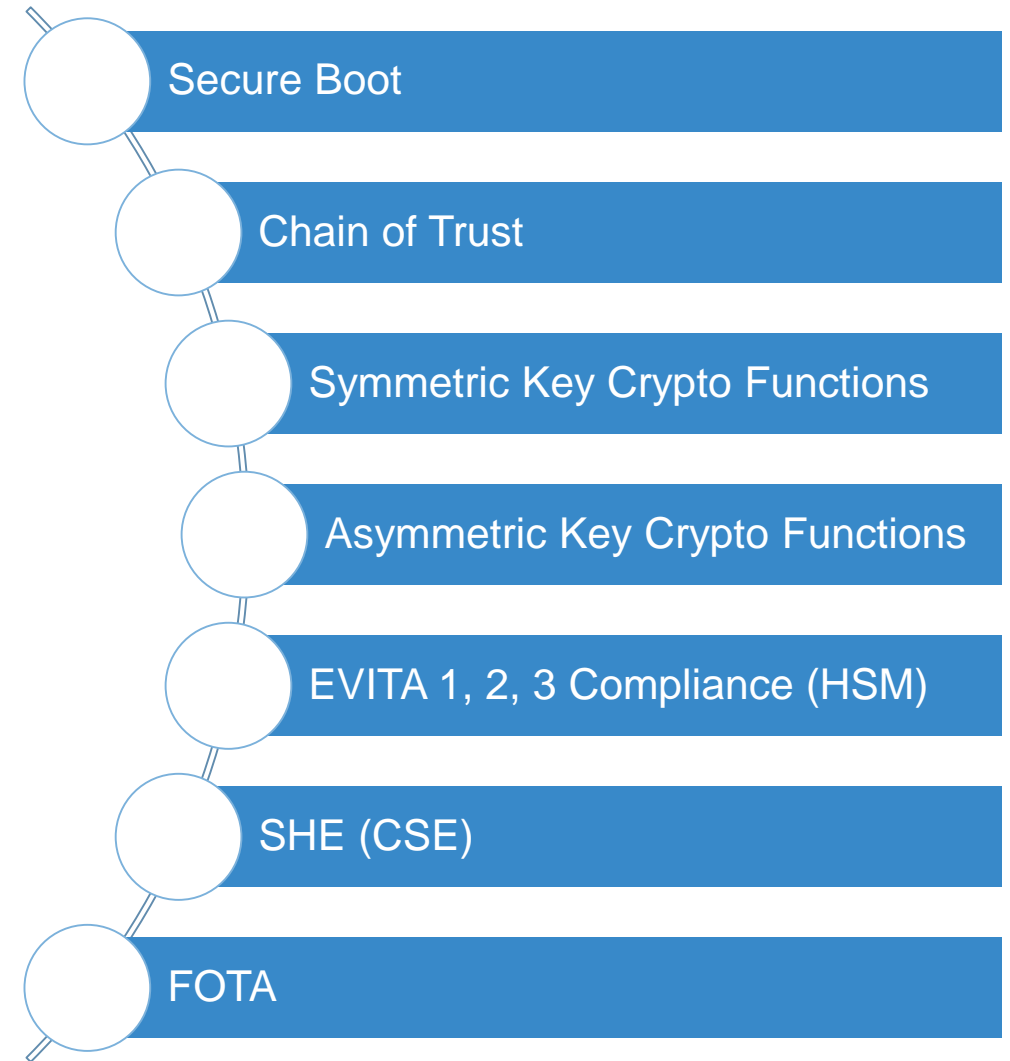
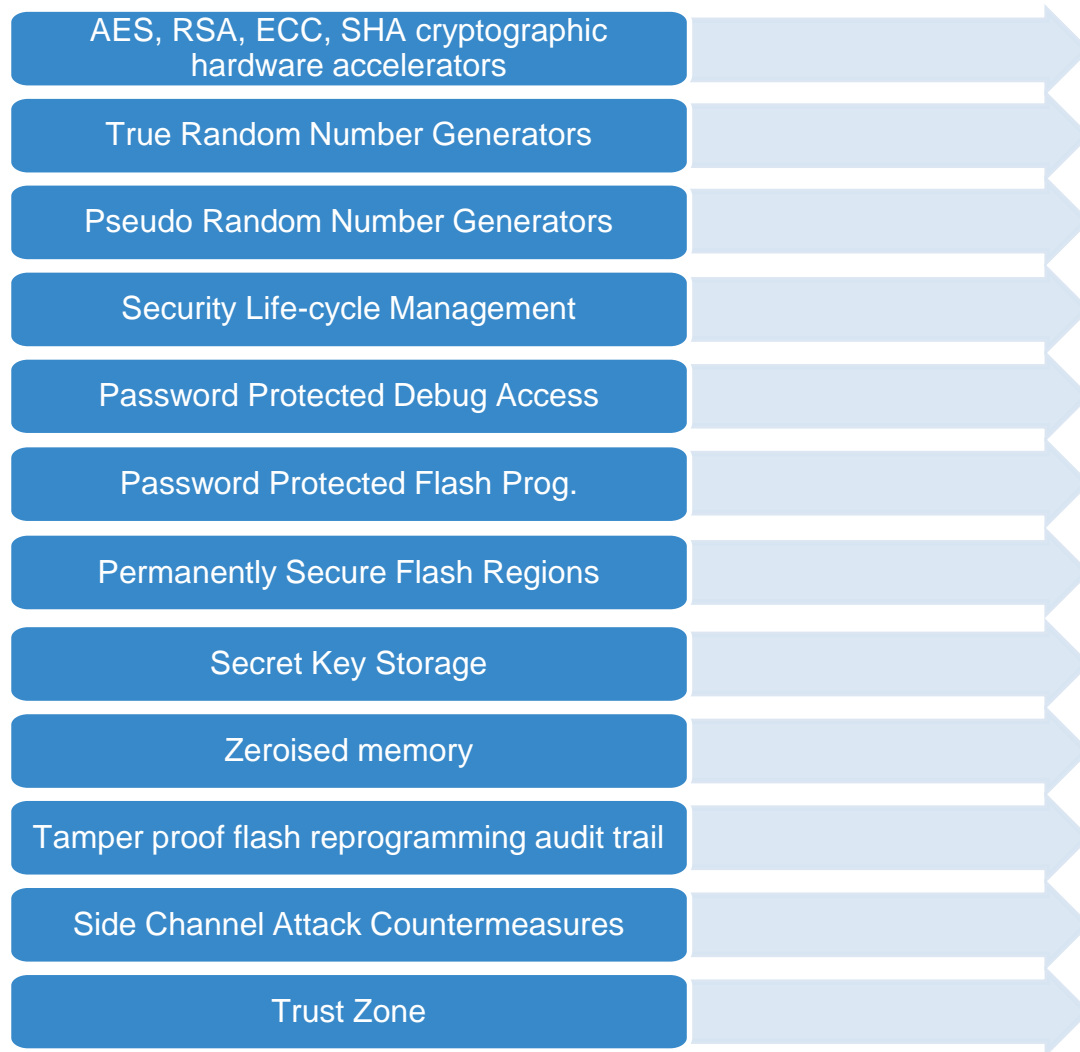
<p>Security Function</p>	<p>Stop unauthorized messages, prevent flood attacks (IDS/IPS)</p>	<p>Encrypt/authenticate IVN communication (firmware and regular messages)</p>
<p>Where to use</p>	 <p>Any node, in any existing CAN Network</p>	 <p>Peripheral nodes, in CAN/CAN FD Networks</p>
<p>Value Proposition</p>	<p>Basic plug-in CAN security, short TTM, transparent to MCU HW/SW</p>	<p>Affordable <b>upgrade of legacy modules</b> (security level comparable with EVITA-medium)</p>

# 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



# Security Features on NXP Secure MCUs



# 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



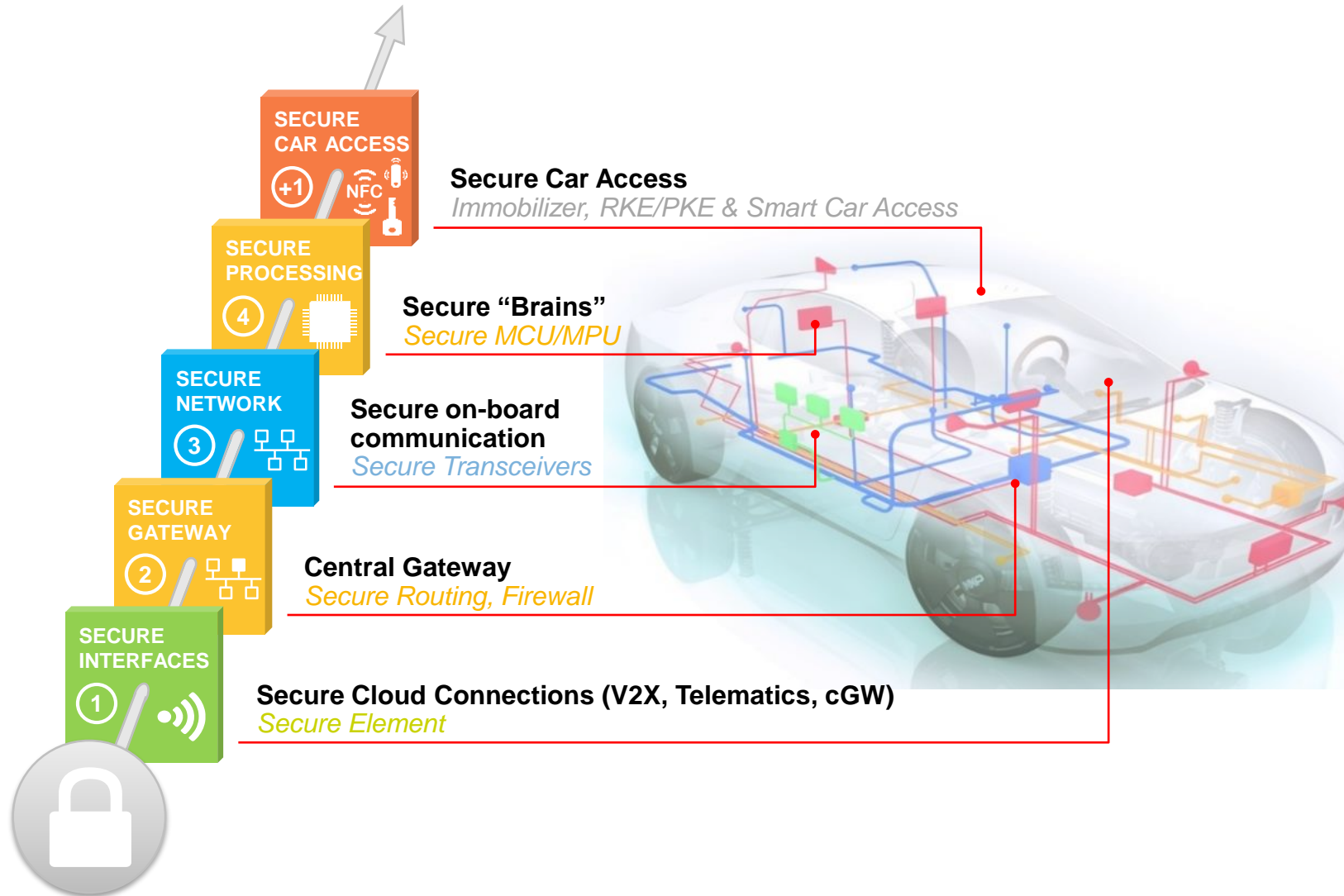
- Car Access via NFC enabled phones/wearables
- NFC key advantage: secure transport of keys
- Alternative: Car access via phone using BLE and key fob as 'Gateway'



# CONCLUSIONS



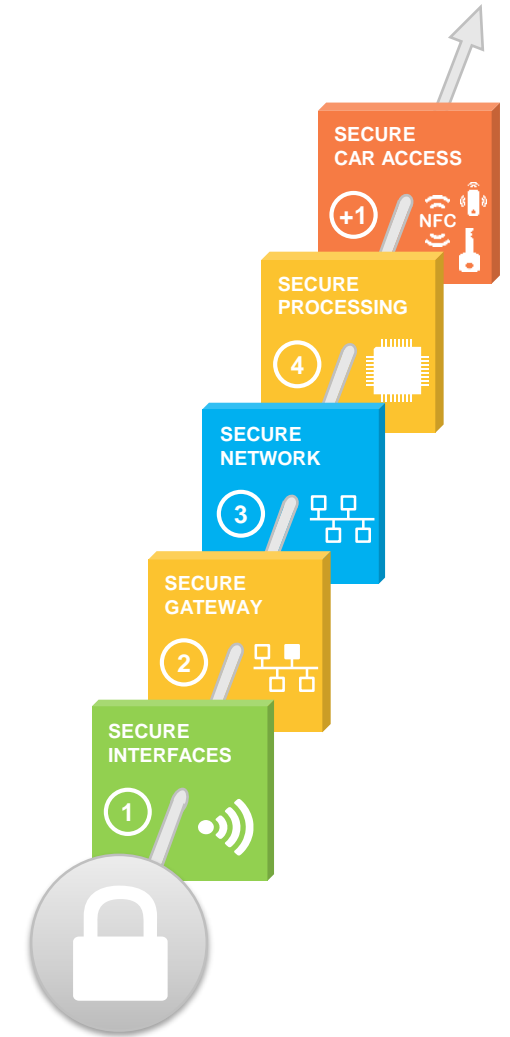
# NXP Automotive Security (4+1 Solution)



- NXP #1 in Auto HW Security
- 4-Layer Cyber Security Solution
- 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

# Related Sessions

Category	Topic	Session	Type	Timeslot
Generic	4 Layers of Automotive Security for Connected Cars	FTF-AUT-N1811	Lecture	Mon 2:00 PM
	Automotive Cyber Security: A Tough Issue Needing Robust Solutions	FTF-AUT-N1763	Panel discussion	Wed 4:45 PM
	Security vs Functional Safety - Complementary or Contradictory?	FTF-AUT-N1814	Lecture	Wed 4:45 PM
Layer 1	Creating Secure Networks for V2X Communications	FTF-AUT-N1764	Lecture	Tue 2:30 PM
Layer 2	Trends in Vehicle Architectures: Central Gateway	FTF-AUT-N1813	Lecture	Tue 11:00 AM
	Automotive Gateway Security Made Easy	FTF-AUT-N1792	Hands-on workshop	Wed 2:30 PM
Layer 3	CAN Security	FTF-AUT-N1815	Lecture	Tue 5:45 PM
	Secure CAN Networks	FTF-AUT-N1783	Hands-on workshop	Wed 4:45 PM
Layer 4	Recent Advances in Secure MCU Security Offerings	FTF-AUT-N1812	Lecture	Mon 3:15 PM
	Maximizing Security using the Secure MCU Features	FTF-AUT-N1810	Lunch & Learn	Tue 1:15 PM
	Techniques for Crypto Key Mgmt Using i.MX Application Processors	FTF-DES-N1894	Lecture	Tue 3:30 PM
Layer +1	Future RF Technologies - UltraWideBand for Car Access	FTF-INS-N1777	Lecture and demo	Mon 4:15 PM
	Secure Car Access and Remote Management	FTF-AUT-N1776	Lecture and demo	Tue 12:00 PM
	NFC for Connected Cars	FTF-AUT-N1781	Lecture	Tue 4:45 PM



**Securely!**

# NXP connects the car

# THANK YOU!

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

**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)

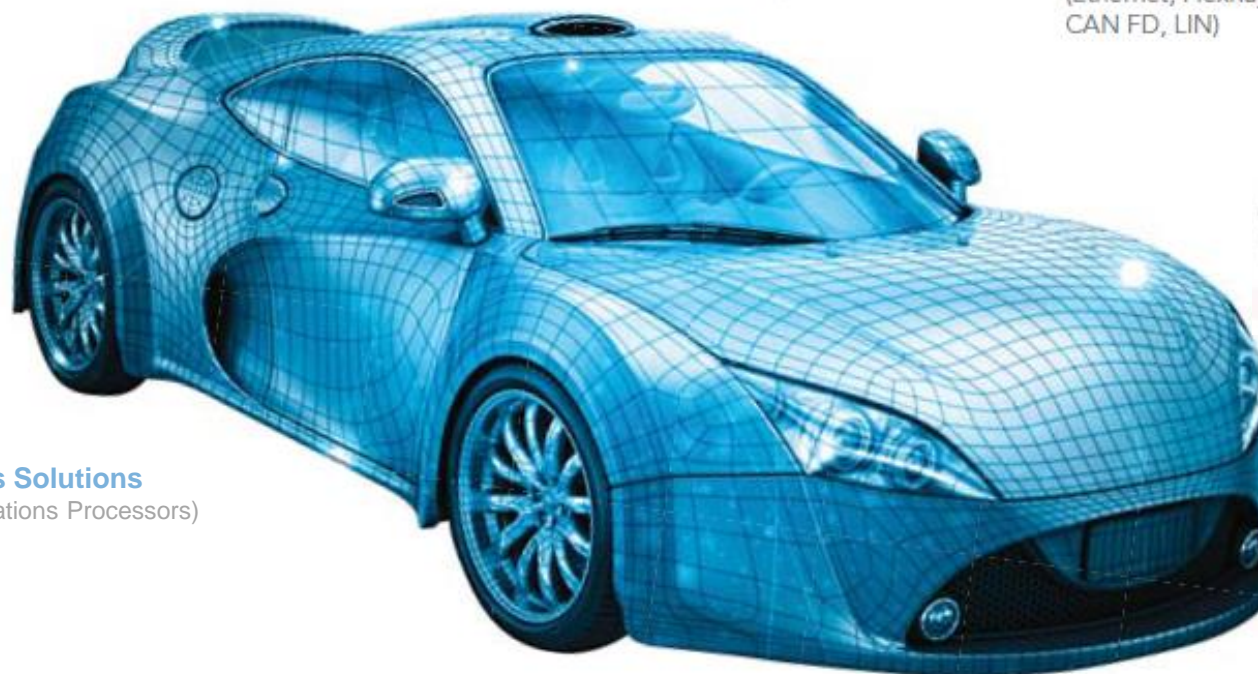
**Car-to-x Communication**  
(802.11p via Software-defined Radio, Authentication)

**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)





SECURE CONNECTIONS  
FOR A SMARTER WORLD

## ATTRIBUTION STATEMENT

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, CoolFlux, EMBRACE, GREENCHIP, HITAG, I2C BUS, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE Classic, MIFARE DESFire, MIFARE Plus, MIFARE Flex, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TrenchMOS, UCODE, Freescale, the Freescale logo, AltiVec, C 5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C Ware, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, Ready Play, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, SMARTMOS, Tower, TurboLink, and UMEMS are trademarks of NXP B.V. All other product or service names are the property of their respective owners. ARM, AMBA, ARM Powered, Artisan, Cortex, Jazelle, Keil, SecurCore, Thumb, TrustZone, and  $\mu$ Vision are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. ARM7, ARM9, ARM11, big.LITTLE, CoreLink, CoreSight, DesignStart, Mali, mbed, NEON, POP, Sensinode, Socrates, ULINK and Versatile are trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org. © 2015–2016 NXP B.V.

