NXP AUTOMOTIVE CYBERSECURITY LIFECYCLE

JOHN COTNER
SECURITY ARCHITECT - AUTOMOTIVE

AMF-AUT-T2792 | AUGUST 2017

SECURE CONNECTIONS FOR A SMARTER WORLD

The Need for Automotive Cybersecurity

Vehicles are getting powerful, but also complex

“Complexity is the worst enemy of security.”

Bruce Schneier
Chief Technology Officer of IBM Resilient, a fellow at Harvard's Berkman Center, and a board member of EFF.

Cannot guarantee full security coverage of the millions lines of code

- Tiered ecosystem of car manufacturing leads to security integration issues.
- Aftermarket products may share the critical buses.

Did You Know?

>20

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
NOW WIDELY RECOGNIZED BY AUTOMAKERS AND GOVERNMENTS

Solutions for Automotive Cybersecurity

COMPLETE SOLUTIONS

- **FASTER TTM**
- **FULL SCALABILITY**

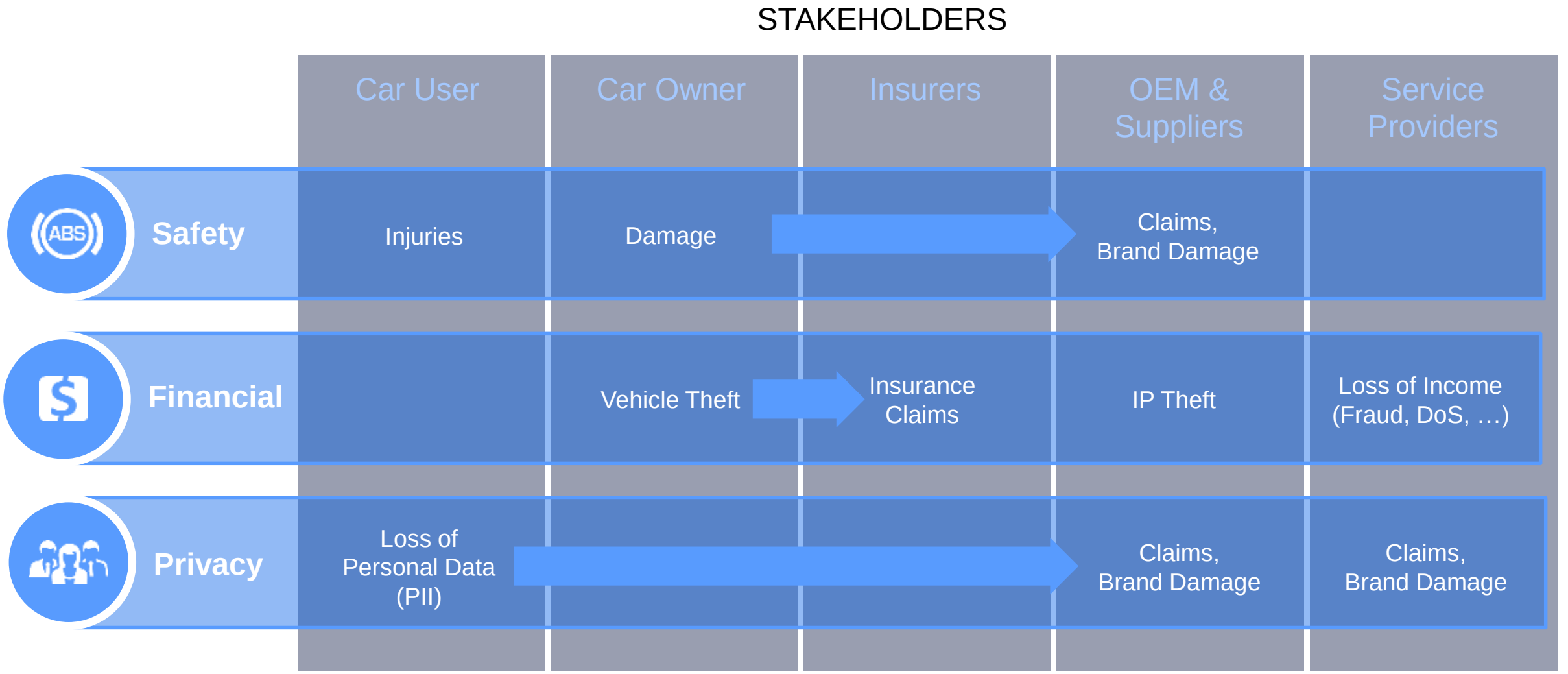
NXP Leads Domain Based Vehicle Architectures:

- Connectivity
- Driver Replacement
- Powertrain & Vehicle Dynamics
- Body & Comfort
- Driver Experience

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
- System security solutions are (usually) **custom-made**
  - Different use cases & architectures may (will) require different security solutions
  - But they often use **generic building blocks**
- **100% secure** (or safe) **does not exist** in the real world
  - The challenge is to find the right balance between risk and protection (cost)

What is at risk, and whom is affected?



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…)

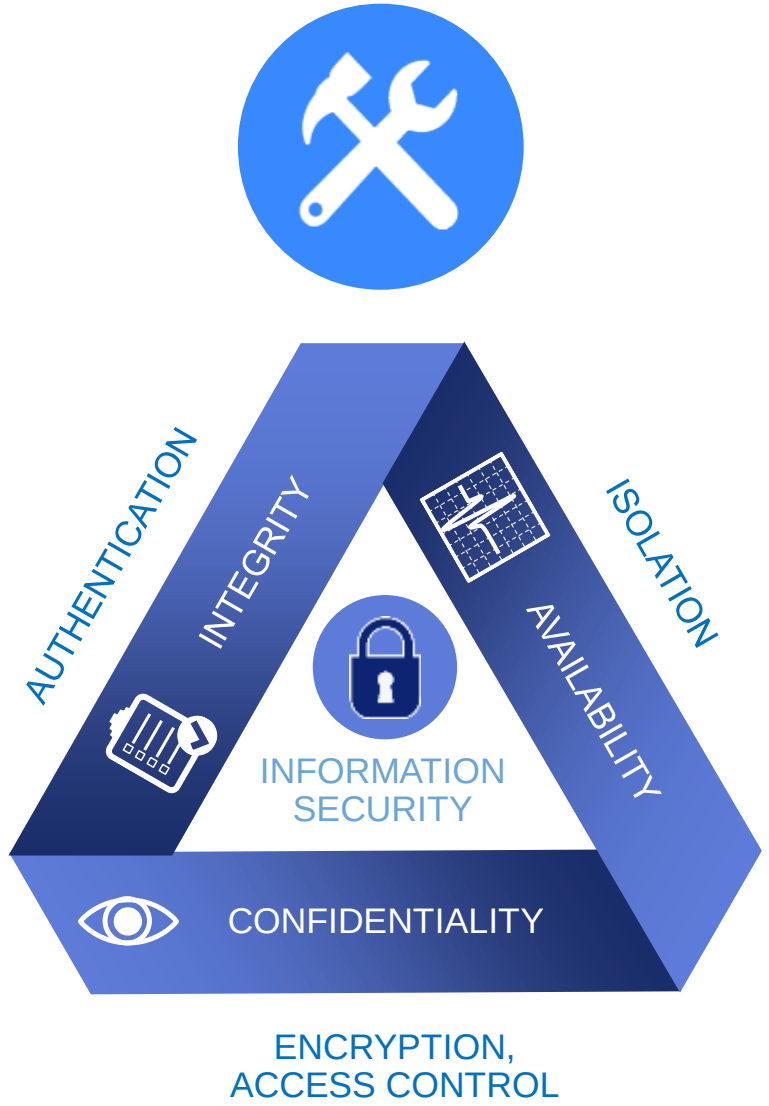
Restricting Access – e.g. using:

- 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(!)



Security Engineering by Ross Anderson

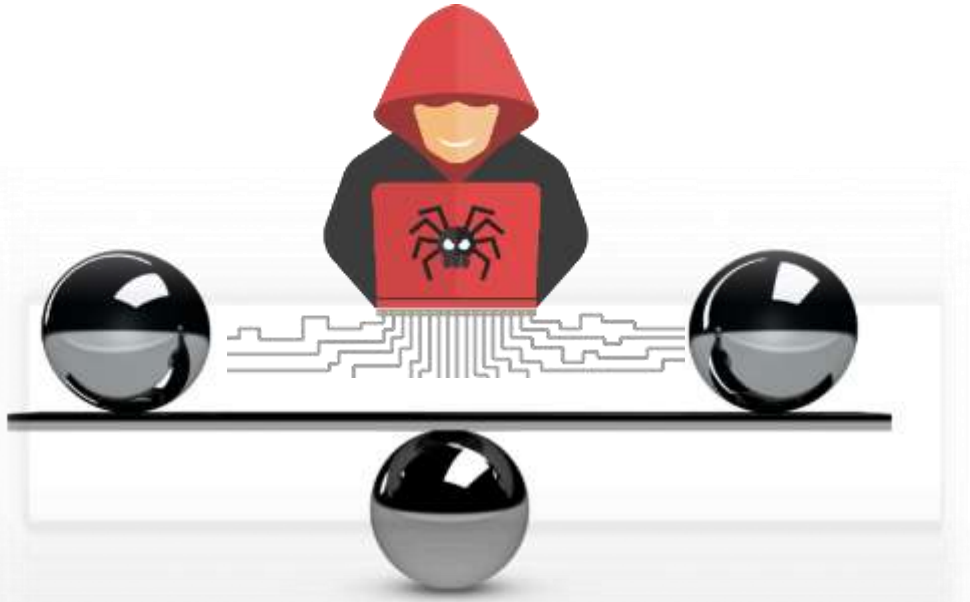
http://www.cl.cam.ac.uk/~rja14/book.html

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?

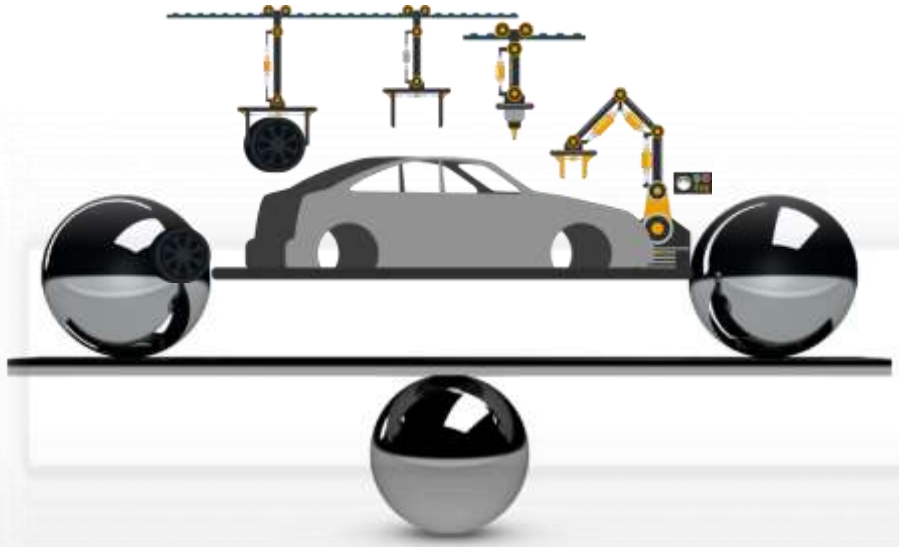
The “Good Guys” must make a Risk Analysis

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"

Proven History In Driving Security

eGovernment

Bank Cards

Smart Mobility (MIFARE) Cards

Tags & Authentication

Readers

Mobile

Automotive:

Mid 1990s
- Censorship
- Immobilizers

Early 2000s
- Enhanced Censorship
- Remote Keyless Entry

Mid 2000s
- High Assurance Boot & Fault Detection Sensors
- Passive Keyless Entry

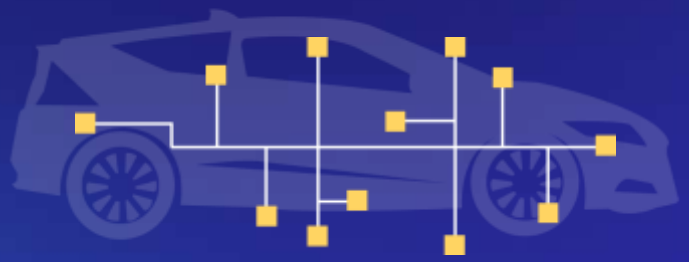
Late 2000s
- Crypto Services Engine (SHE), Active Shields
- Keyless Entry RF Transceivers

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

Security by Design.

Source: Bielefeld University, Germany.

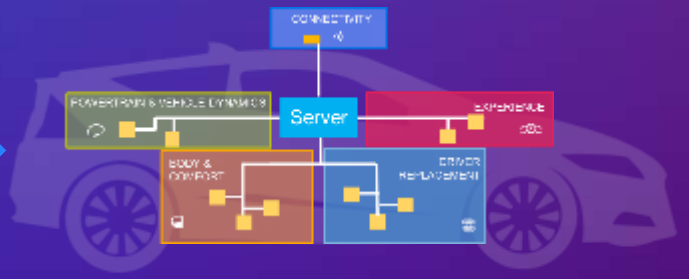
Automotive Security – Way Forward



TODAY

APPLY BEST PRACTICES:

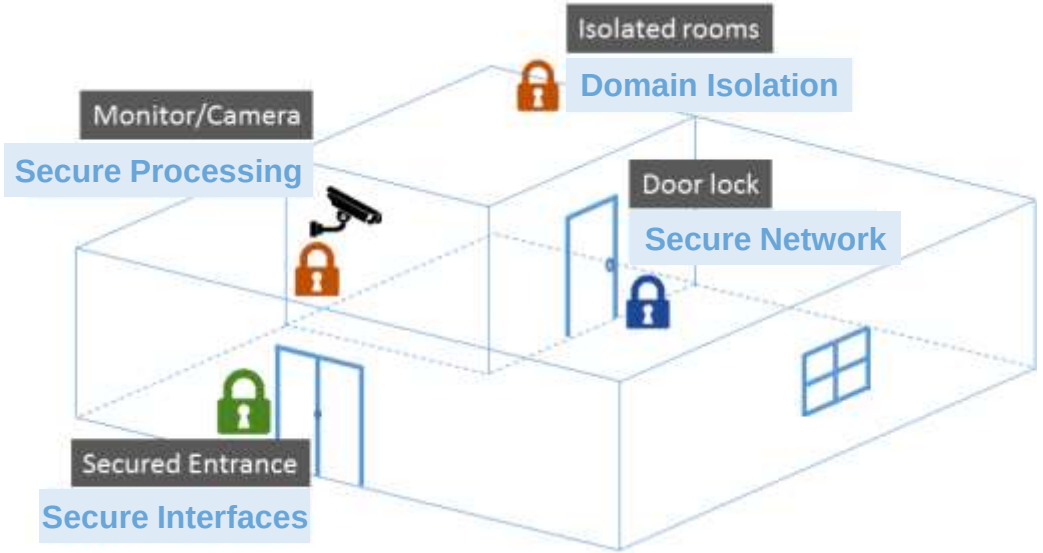
- Security-by-design & Privacy-by-Design (as opposed to being an afterthought)
- Lifecycle Management (incl. FOTA)



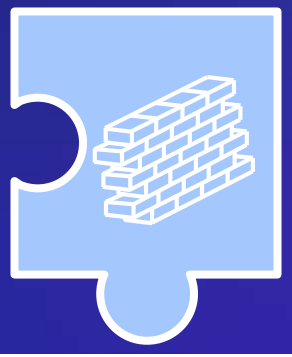
FUTURE

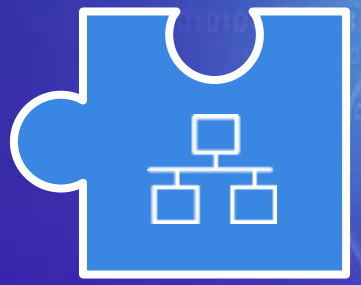
Essential element:
Defense-in-Depth approach

- 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

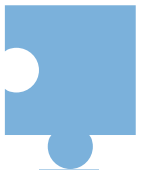
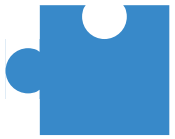
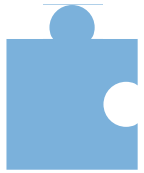
Secure
Internal Communication

Secure
Software Execution

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

- Regardless of the actual architecture and implementation

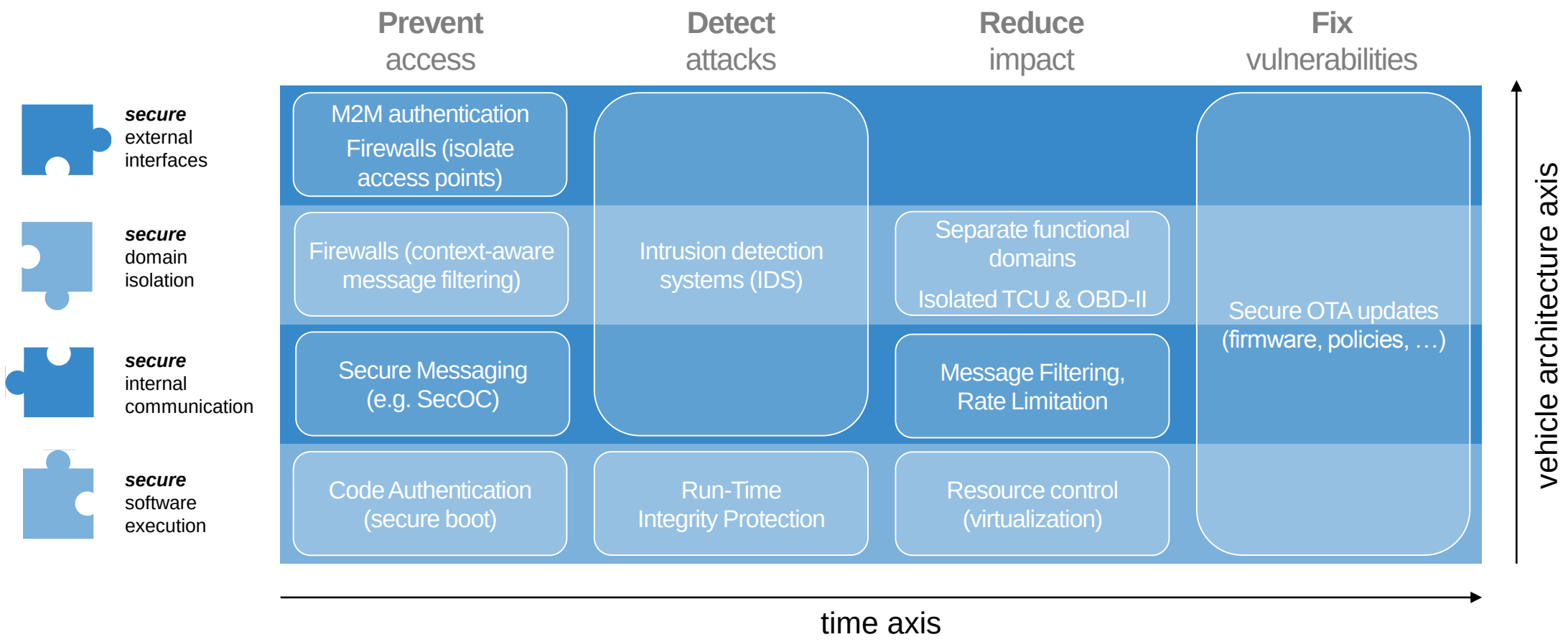
Explanation of the Core Cyber Security Principles

Principle	Concerns	Examples
 ***secure*** external interfaces	• Who is trying to access my network, and for what purpose? • How to prevent spoofing, data manipulation and/or theft?	• Only the OEM server can send firmware updates • Only real vehicles & infra can send V2X messages
 ***secure*** domain isolation	• How to separate domains (with different criticalities)? • How should they (in a controlled manner) be able to interact?	• The infotainment system can receive position & speed • But it cannot send control messages to the brakes
 ***secure*** internal communication	• Who is on my network? And who is sending messages? • How to prevent data manipulation (or theft)?	• Only genuine ECUs can be installed in the network • Messages cannot be replayed (repeated)
 ***secure*** software execution	• How do I ensure that software cannot be modified (hacked)? • How do I enable secure updating (/ fixing) of the software?	• Monitoring execution (run-time integrity checks) • Secure boot / firmware image verification
*perimeter security **	• How to prevent people from getting close to the electronics? • How to prevent unauthorized access to (/use of) a vehicle?	• Install the electronics systems behind steel & glass • (Electronic) door locks

* Perimeter security forms an important aspect of *physical security* for vehicles, but it is *not* a cyber security principle. As such, perimeter security is only listed here for completeness. In other words: one must *not* rely on perimeter security for the protection of the electronic systems against cyber attacks. For example, electronic car access systems must be protected against cyber attacks using the 4 principles listed above.

Applying The Core Security Principles

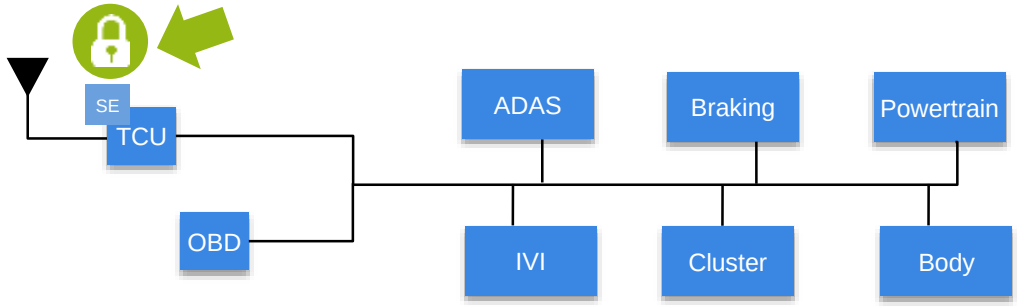
Securing the Vehicle's E&E Architecture using a Defense in Depth approach



4 Layers To Securing A Car

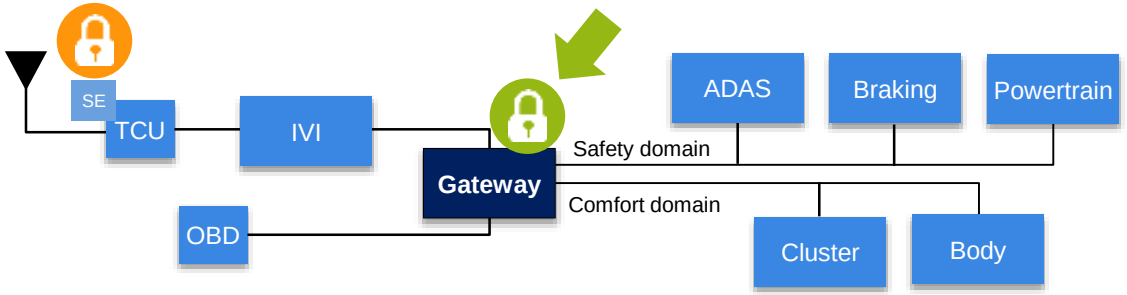
Layer 1: **Secure Interface**

Secure M2M authentication, secure key storage



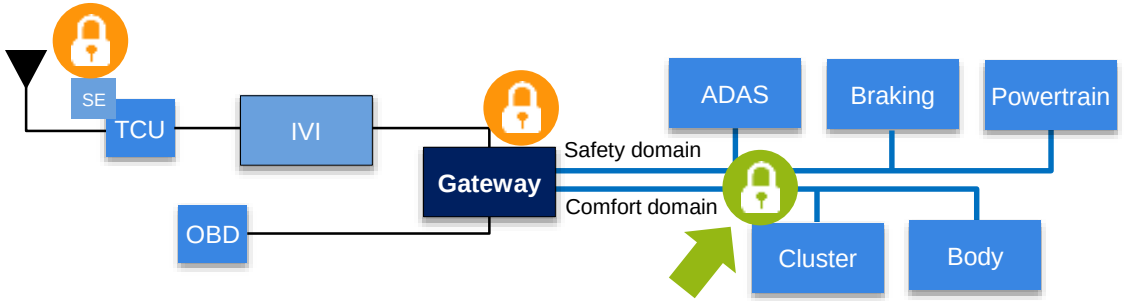
Layer 2: **Secure Gateway**

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



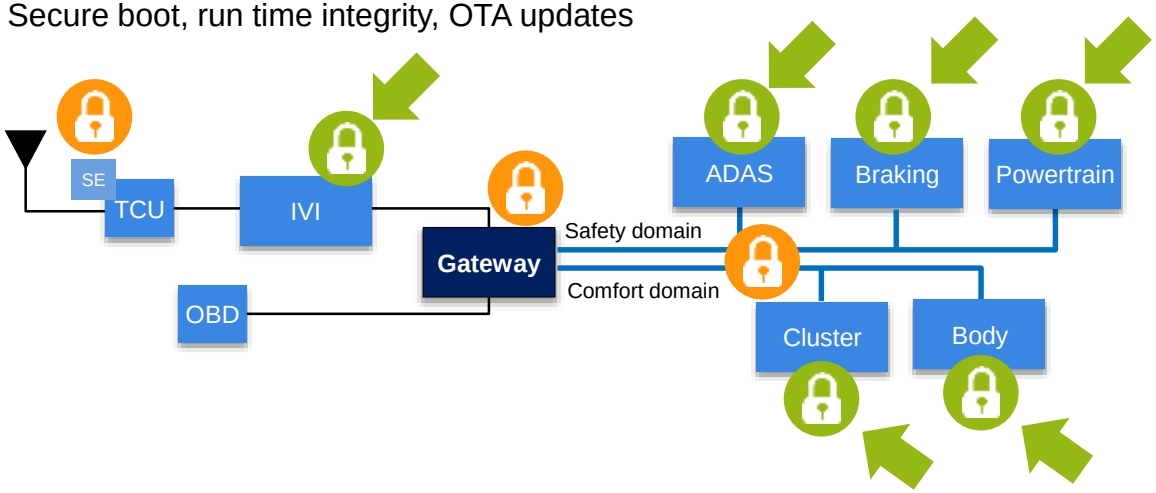
Layer 3: **Secure Network**

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



Layer 4: **Secure Processing**

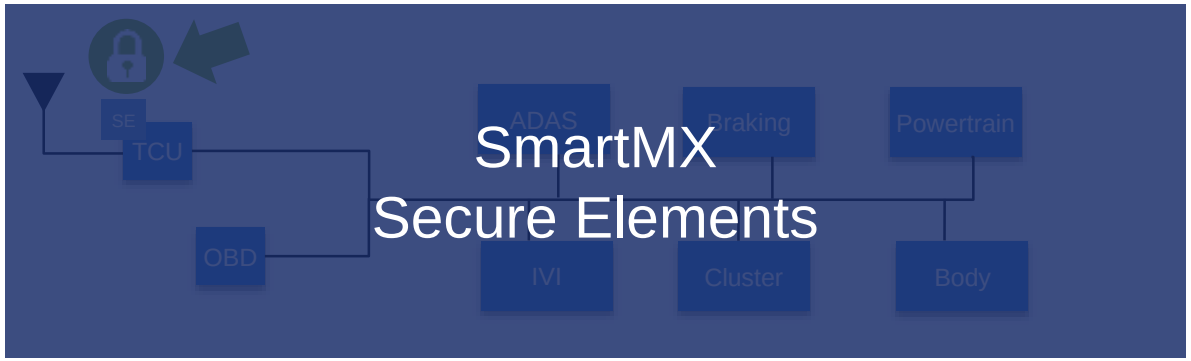
Secure boot, run time integrity, OTA updates



4 Layers To Securing A Car

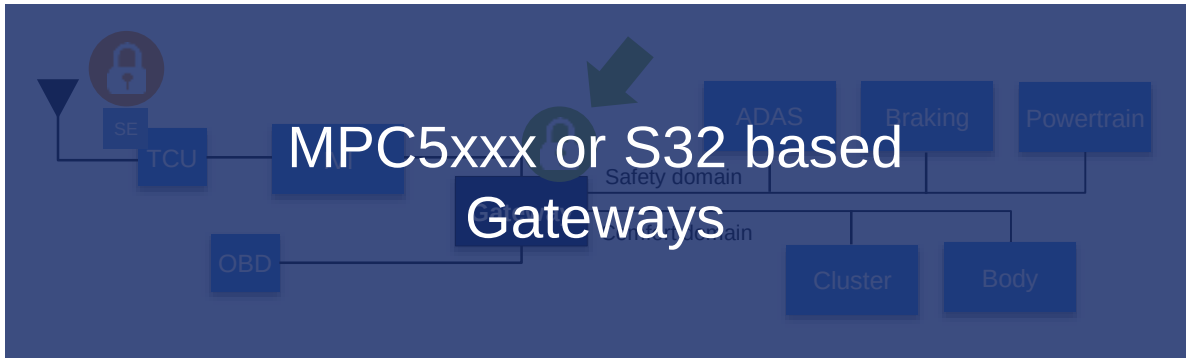
Layer 1: **Secure Interface**

Secure M2M authentication, secure key storage



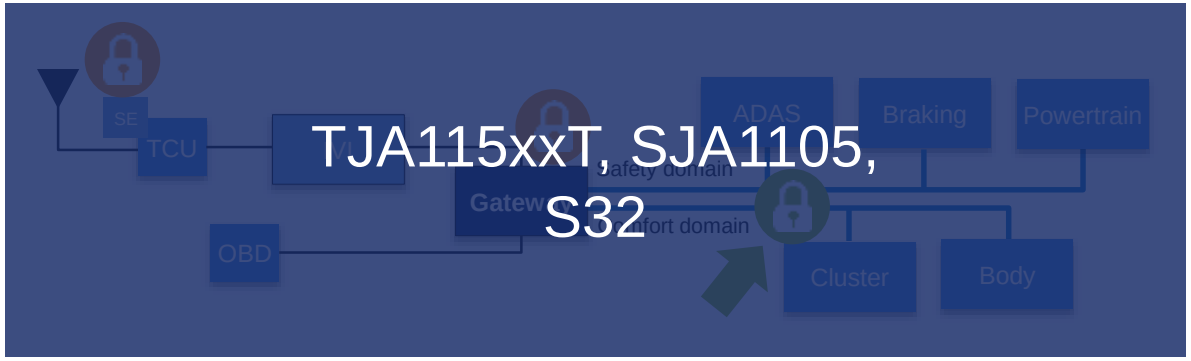
Layer 2: **Secure Gateway**

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



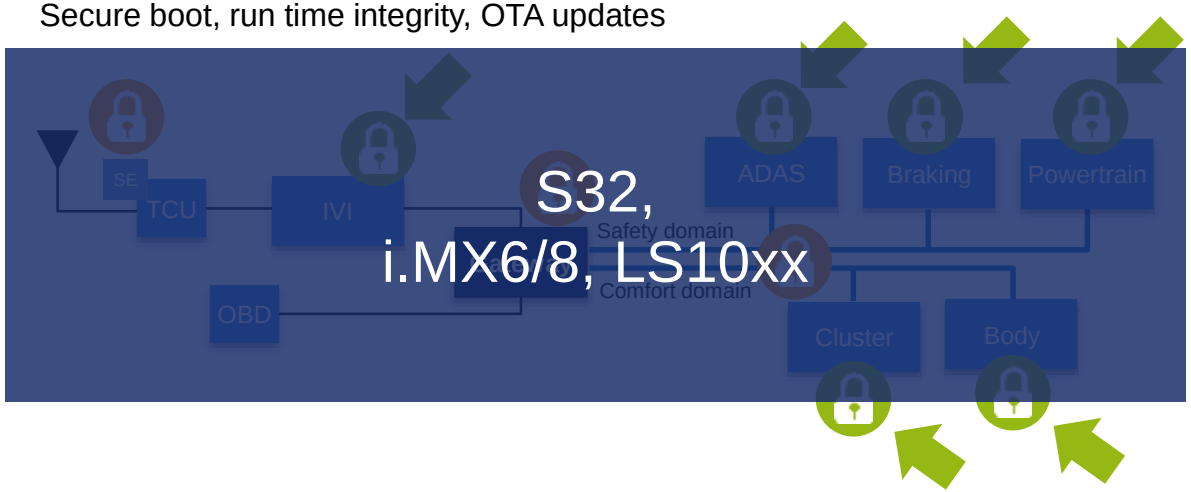
Layer 3: **Secure Network**

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



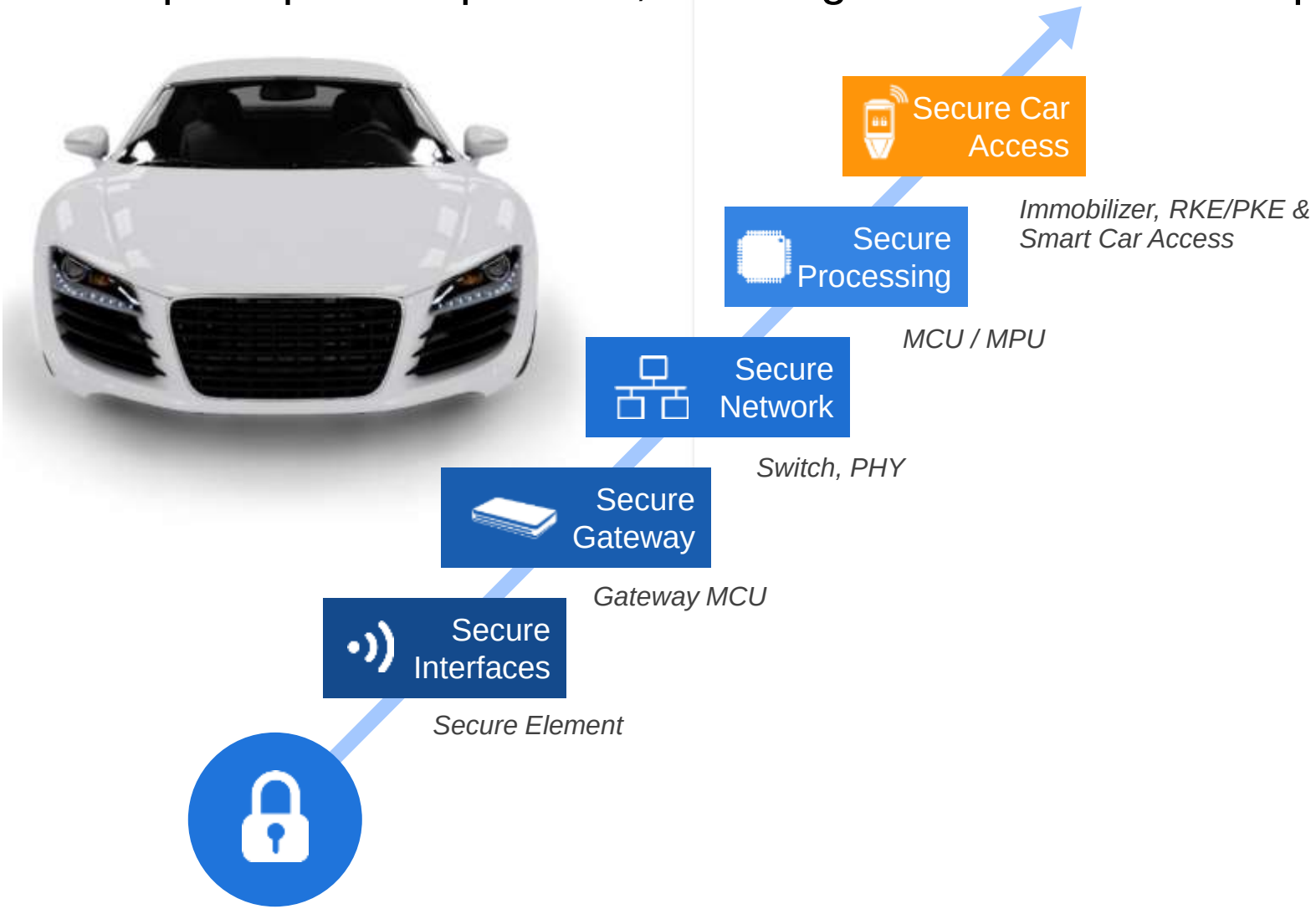
Layer 4: **Secure Processing**

Secure boot, run time integrity, OTA updates



NXP’s 4+1 Automotive Security Framework

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



NXP **#1** in Auto HW Security

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

Plus **‘Best In Class’** Car Access Systems

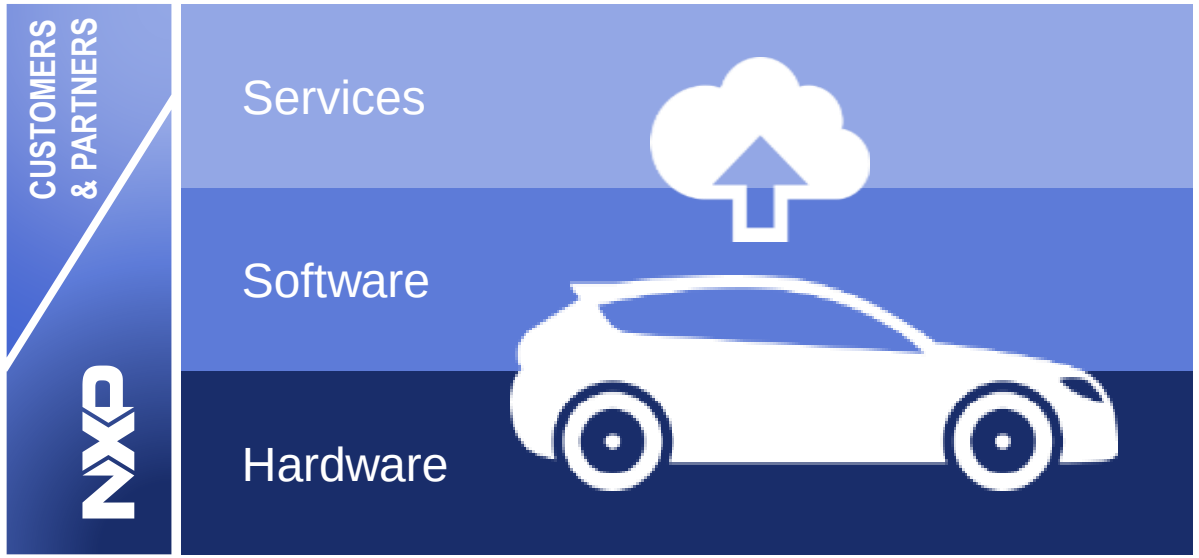
Recognized Thought & Innovation Leader

> 900 security patent families, **~ 200** specific to Automotive

Partner of Choice for OEMS, T1s & Industry Alliances

Hardware, Software and Services

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



Complementary strengths:

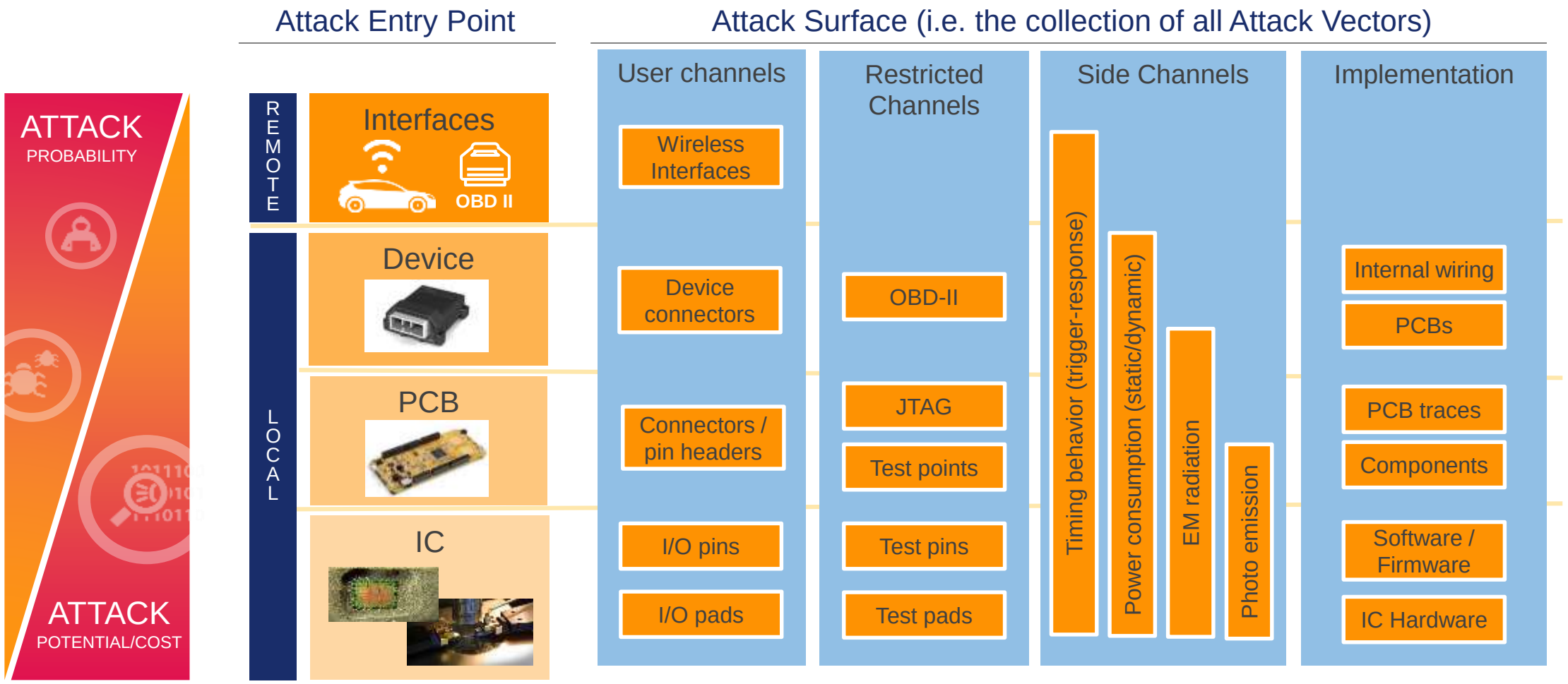
- Threat Monitoring & Response – e.g. Cloud Analytics
- Device & Identity Management – e.g. Trust Provisioning

- Flexibility / Updateability – e.g. FOTA/SOTA For Fixing Bugs, Vulnerabilities

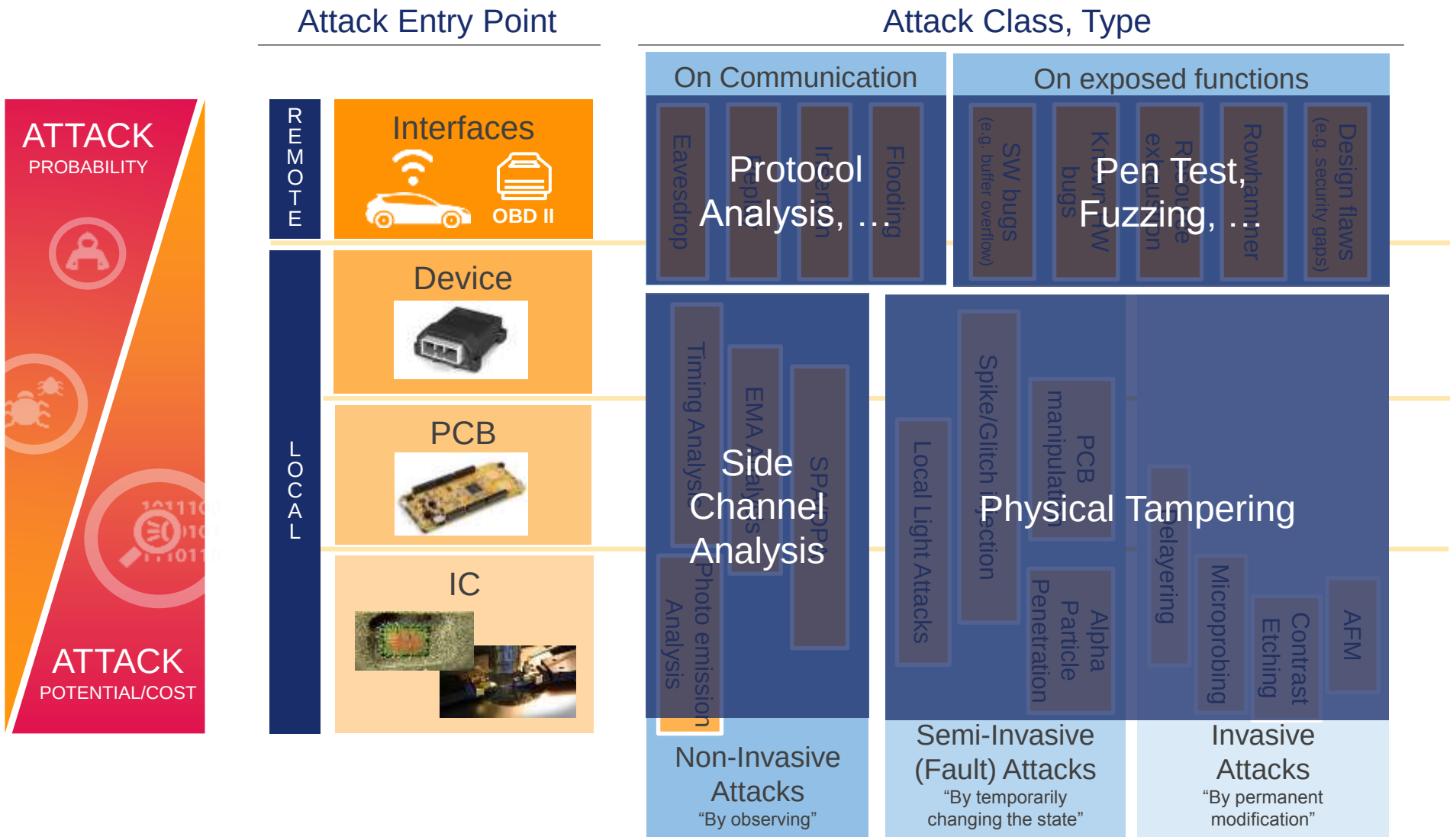
- Performance – e.g. Crypto Accelerators
- Immutability – e.q. Hardware Enforced Isolation (HSM)
- Tamper Resistance – e.g. Sensors, Glue Logic, Shields

Wide industry agreement that all 3 are needed (at least since Mirai Botnet)

Vehicle Attack Surface



NXP Attack Terminology



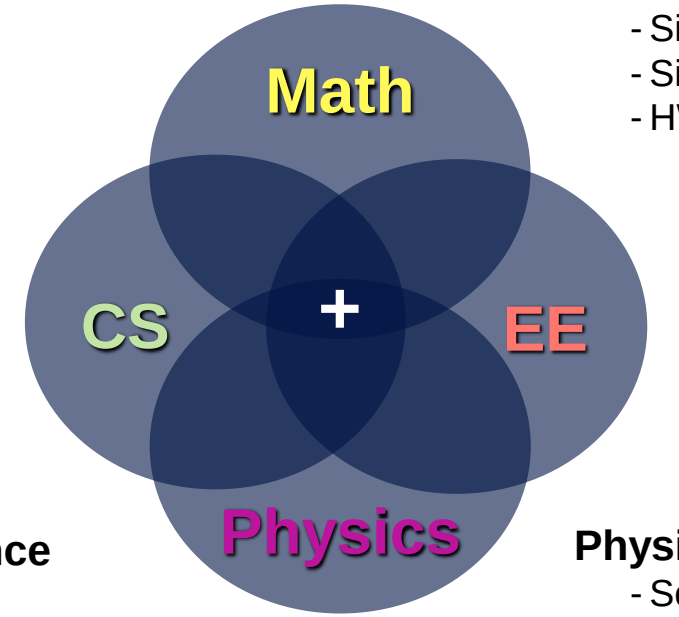
Vulnerability Analysis - TEam

Vulnerability Analysis

- **Side-Channel Analysis & Tools**
- **Fault Injection & Simulation**
- **Software VA**

Math
- Crypto
- Coding
- Statistics
- Stochastics

Electrical Engineering
- Signal Acquisition
- Signal Processing
- HW Design

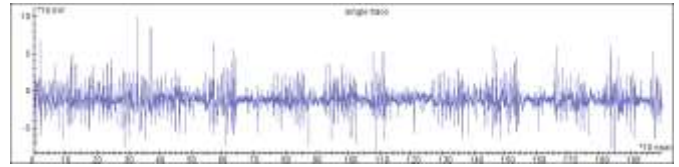


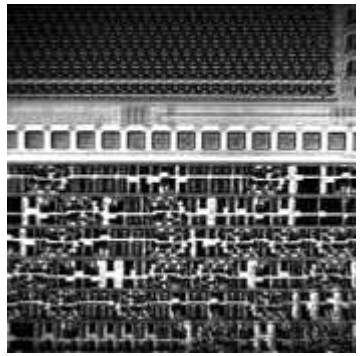
Computer Science
- Algorithms
- Whitebox Implementations
- SW Hacking

Physics
- Semiconductor Physics
- Material Sciences
- Optics & Photonics

Vulnerability Analysis - Competences

- **Side Channel Analysis & Tools**
  - Power Analysis
  - Electromagnetic Emanation Analysis
  - Photonic Emission Analysis
- **Fault Injection & Simulation**
  - Laser Fault Injection
  - Electromagnetic & BBI Fault Injection
  - Internal & External Glitch Injection
- **Software**
  - Code Lifting & Reverse Engineering
  - Malicious JavaCard Testing
- **Invasive Methods**
  - Focus Ion Beam & Electron Microscopy
  - Nano-Probing & Forcing Signals
  - Delayering & Reverse Engineering





```
ROM:1FFF0200
ROM:1FFF0204
ROM:1FFF0208
ROM:1FFF020C
ROM:1FFF0210
ROM:1FFF0214
ROM:1FFF0216
```

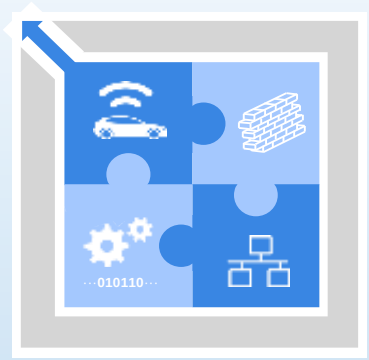
```
LDR.W   R2, =0x400FC184 ; R2->CRP control register
LDR.W   R3, =0x2FC      ; R3->CRP control value in flash
LDR.W   R5, =0x43218765
LDR.W   R6, =0x12345678
LDR.W   R4, [R3]        ; R4=CRP control value from flash
CMP     R4, R5
IT NE
```

Security REQUIRES A HOLISTIC APPROACH (& Ongoing Effort)

Vehicle Lifecycle

Design | **Build** | **Use** | **Scrap**

Apply the Core Security Principles:



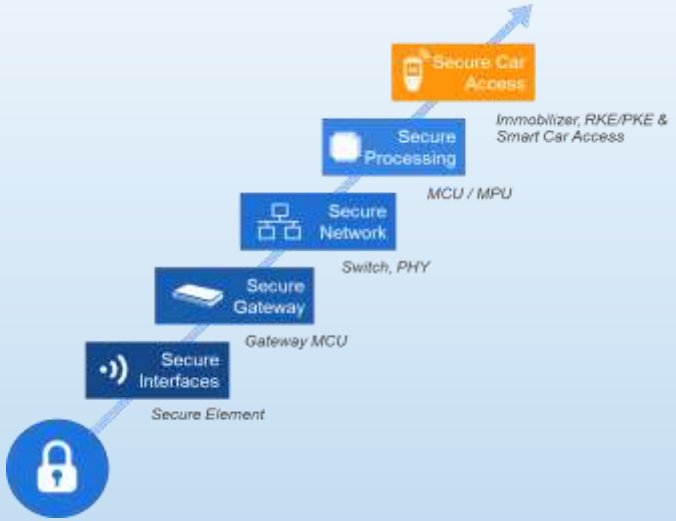
Secure **External Interfaces**

Secure **Domain Isolation**

Secure **Internal Communication**

Secure **Software Execution**

Using NXP's leading product portfolio:



Maintain products in the field:

- Monitoring
- Incident response
- Containing vulnerabilities
- Fix vulnerabilities

Software Management (e.g. FOTA updates)

Configuration Management (e.g. feature unlocking)

Crypto Key Management (e.g. Trust Provisioning)

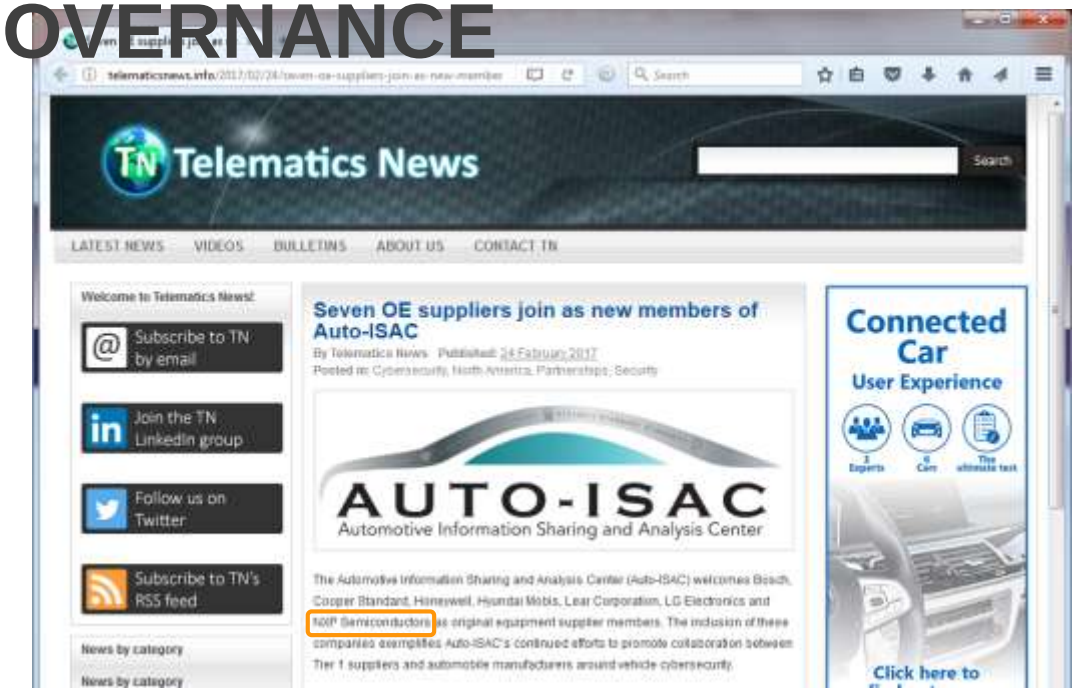
…

Security Policies, Processes, Governance / Risk management and Continuous Improvement

Security POLICIES, Processes and GOVERNANCE

- **Security must be an integral part of the lifecycle**
  - In product design, implementation and maintenance
  - But also in associated processes

- **We take our responsibility**; e.g.:
  - Secure Development and Manufacturing Processes
  - Threat Intelligence Feed (e.g. Auto ISAC)
  - External Audits for Product / Site Security
  - Product Security Incident Response Team
  - Security Awareness Trainings for Employees



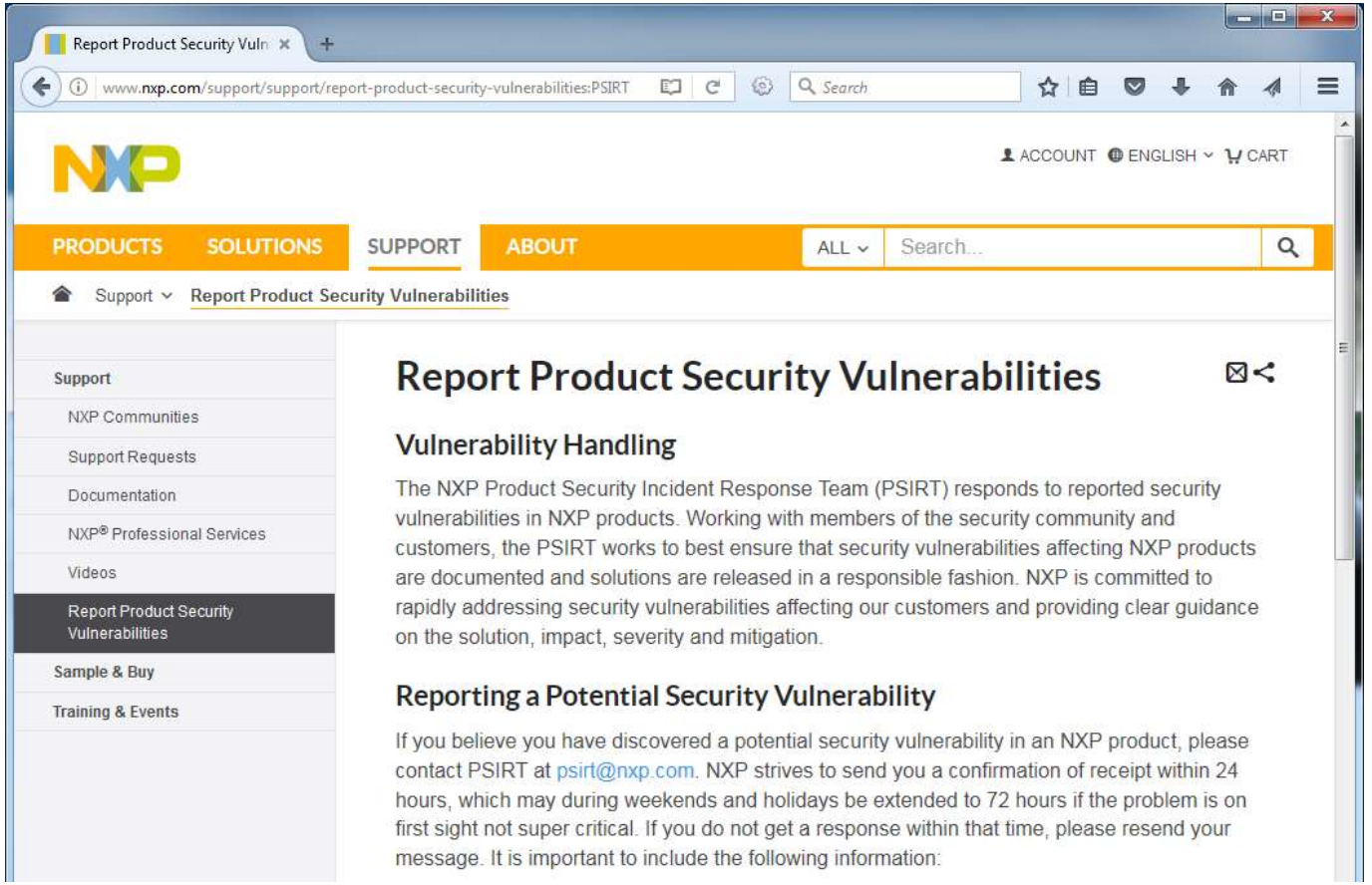
NXP was amongst the first suppliers to join the Auto-ISAC (Aug. '16)

Goals of the Auto-ISAC:
- Intel Sharing
- Analysis
- Best Practices
- Partnerships
- Community Development

Best Practice Guides (WIP)
- Incident Response
- Collaboration & Engagement
- Governance
- Risk Assessment and Management
- Security by Design
- Threat Detection and Protection
- Training & Awareness

PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT)

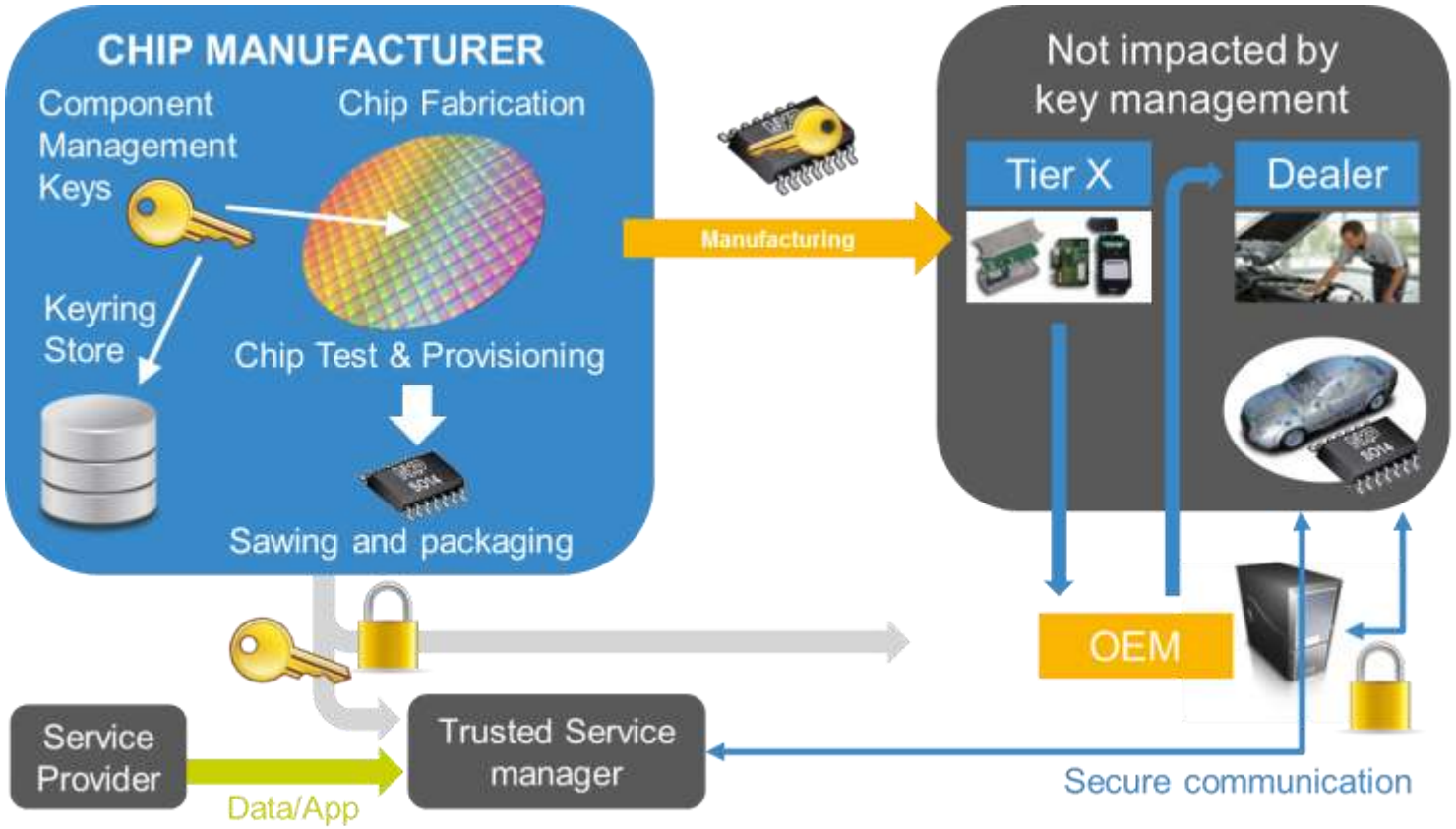
- We’re committed to responsible disclosure
- The team responds to reported security vulnerabilities
  - Receive & acknowledge report
  - Evaluate vulnerability
  - Identify solutions
  - Communicate
- We are working with the security community and with our customers
- We continuously evaluate & benchmark our process
  - E.g. against Auto-ISAC’s best practice guide for incidence response



Contact: www.nxp.com/psirt, psirt@nxp.com

SECURITY SERVICES – Trust Provisioning

- In-house capabilities for Trust Provisioning
  - Crypto key insertion, IC personalization, etc.
  - Utilizing secure (physical and IT) environments, processes etc.
- In volume production for banking & eID (passport) markets
- Initial demand in the Automotive market



CONCLUSION

- Automotive Innovation is changing towards developing self-driving robots
- Security is essential – people must be able to trust their cars
- NXP leads the industry, with the 4+1 security framework
- Plus the most scalable security solutions, protecting:
  - Software – secure processing solutions
  - Communication – secure networking solutions
  - Access – secure wireless interface solutions

www.nxp.com/automotivesecurity

SECURE CONNECTIONS
FOR A SMARTER WORLD