NXP Automotive Cybersecurity Program

John Cotner

Security Architect, Automotive

October 2018 | AMF-AUT-T3192

NXP | CONNECTS

Agenda

Auto Security

- What & Why
- Ecosystem
- Approach
- Solutions
- Processes

Did You Know?

>25

Vehicle hacks
published since 2015

1.4M

Vehicle recalled
in the largest
incident to date

Why hacking?

Valuable Data
attracts hackers

Car-generated data may become a USD 750B market by 2030

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

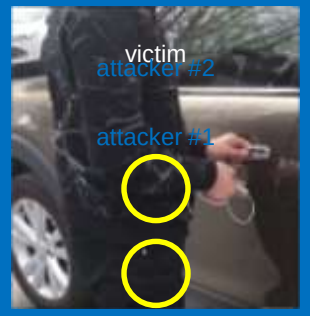
250M connected vehicles on the road in 2020

Security is a must-have for connected & autonomous vehicles

Cyber-security Threats in Cars: Local Attacks

Local Attacks
targeting one vehicle

Vehicle theft by relay attack



https://www.youtube.com/watch?v=bXfp8F4J2eI

Ransom for a drive

VDI Conference on IT Security for Vehicles, Berlin, 5.7.2017

Tampering the odometer

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

Mainly a concern for car owners / users

Cyber-security Threats in Cars: Local Attacks (ECU)

Local Attacks
targeting one vehicle

Local Attacks
targeting one ECU (chip)

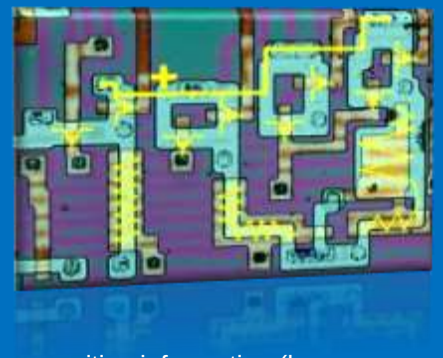
Engine tuning

Workshop around the corner, or in your garage

Reverse engineering

Analyze competitive information (HW & SW)

Chip attacks (many kinds)



Retrieve sensitive information (keys, passwords, etc.)

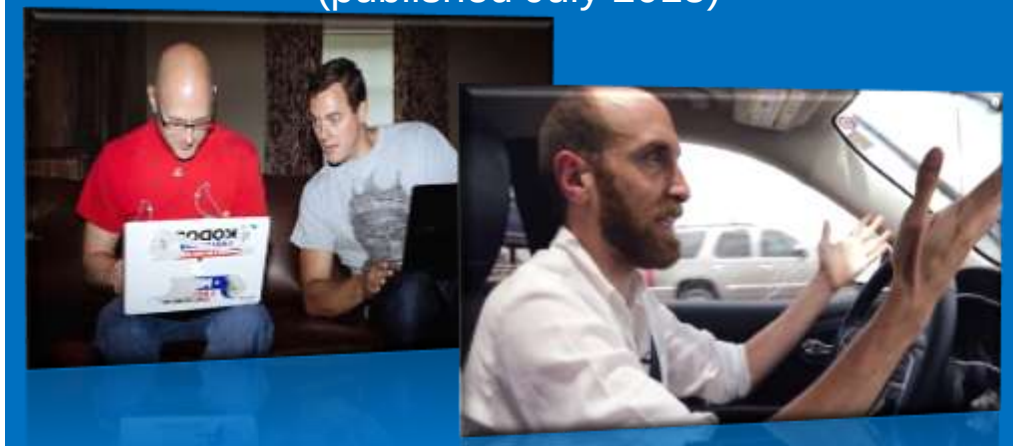
Retrieving secret keys can potentially allow for a hacker to scale remote attacks

Potentially a massive concern for car makers

Cyber-security Threats in Cars: Remote Attacks

Local Attacks targeting one vehicle	Local Attacks targeting one ECU (chip)	Remote Attacks scalable to entire fleets

Remote hack of an unaltered car
(published July 2015)



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

Yet another remote hack of an unaltered car
(published Feb 2016)

https://www.youtube.com/watch?v=egws2_WSUUE

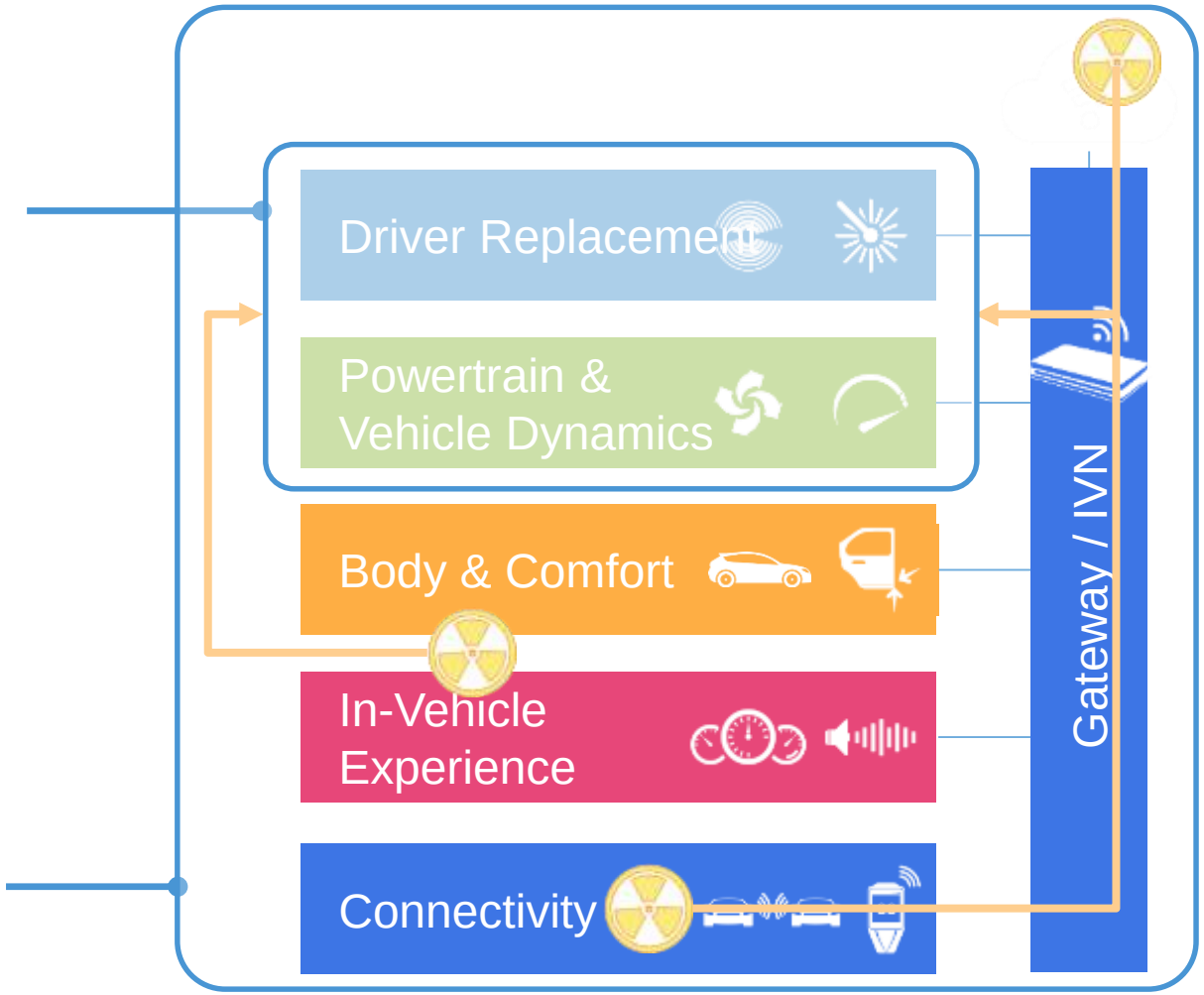
A massive concern for car makers (and users)

No Safety Without Security

#1 Objective: no functional hazards on mission-critical ECUs

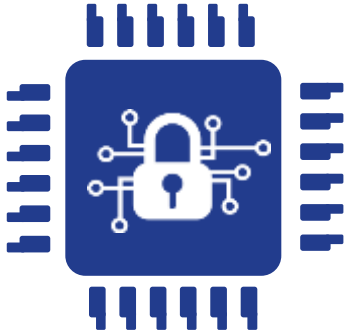
Collaterals:
System availability ensured
Information received / processed trustworthy

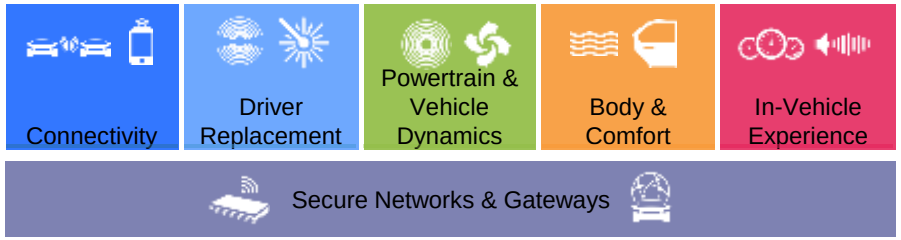
Cyber-security is a prerequisite for availability and trust in the system



Functional Safety & Security – System-level Concerns

IC-LEVEL SAFETY & SECURITY SOLUTIONS + SAFE & SECURE DOMAIN ARCHITECTURES = SAFE AND SECURE MOBILITY





- Resource Isolation
- On-Die Monitoring
- Integrity & Authenticity Checks
- …

- Domain Isolation
- Firewalls
- Network Intrusion Detection
- …

- Fail Operational
- Resilient against Cyber Attacks

Ecosystem

Automotive State of Standardization

Overall

- No global standard available as of now
- Many ‘guidance’ documents from SAE, ISAC, NHTSA, JASPAR, IPA, ENISA, UK DOT, ACEA, SAC, etc.
- Many customer specifications (some corporate-wide, some application specific)

Processes

- Joint SAE-ISO WG on Automotive Security Engineering
  - Topics: risk management (TVRA), assurance levels (CAL), product development, operations, maintenance, cybersecurity monitoring, incident response, information sharing, updates, quality management, governance, awareness, audits, …
- Auto ISAC – Developing Best Practices for cyber security. Driven by automakers and suppliers globally

Product security

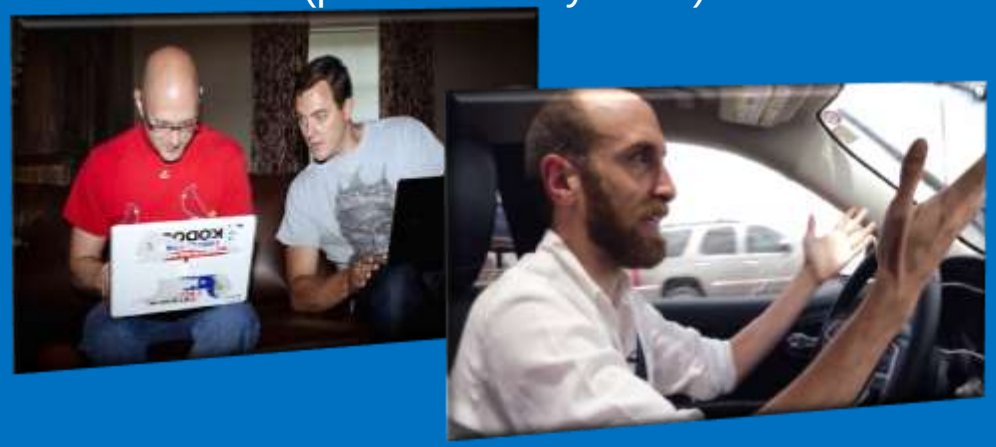
- SHE by HIS and HSM by EVITA still in some use (with modifications)
- SAE J3101 (WIP): Hardware Protected Security for Ground Vehicles
- AUTOSAR Crypto Stacks gaining a lot of momentum on MCU side
- TCG spec of TPM Auto Thin Profile has some interest (especially in Japan)

Approach

Cyber-security Threats in Cars: Remote Attacks

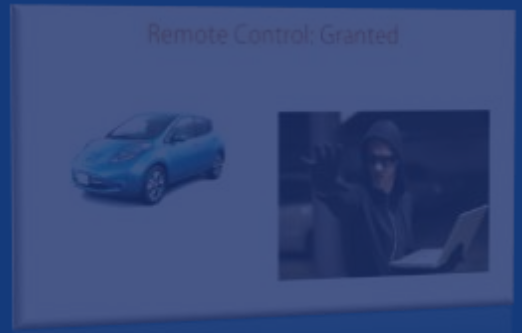
Local Attacks targeting one vehicle	Local Attacks targeting one ECU (chip)	Remote Attacks scalable to entire fleets

Remote hack of an unaltered car
(published July 2015)



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

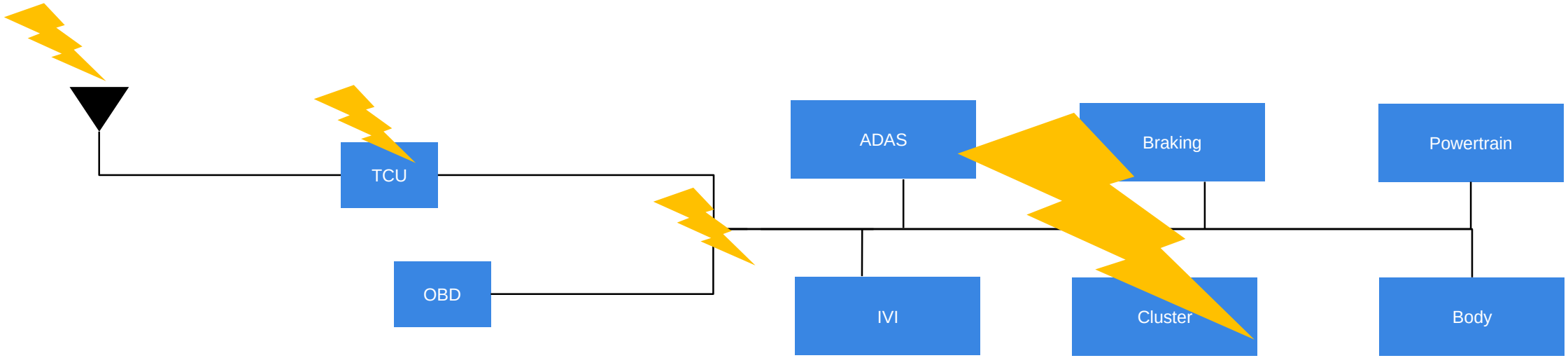
Yet another remote hack of an unaltered car
(published Feb 2016)



https://www.youtube.com/watch?v=egws2_WSUUE

A massive concern for car makers (and users)

Blueprint For Typical (Remote) Attacks

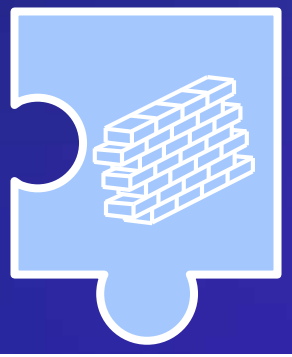


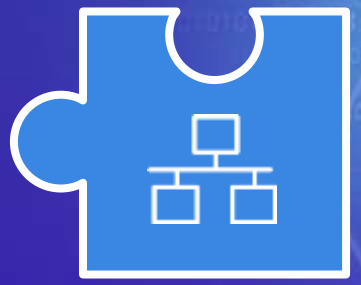
1. Connect to modem *(cellular / internet)*
2. Find & exploit vulnerabilities in the connected ECU *(e.g. Telematics module)*
3. Thereby gain access to the CAN network
4. And steal data or take over control *(e.g. slam the brakes)*

Security is often ignored, or applied as an after-thought!

No (or weak) security countermeasures, no (domain) isolation, etc.

Core Security Principles – For Defense in Depth



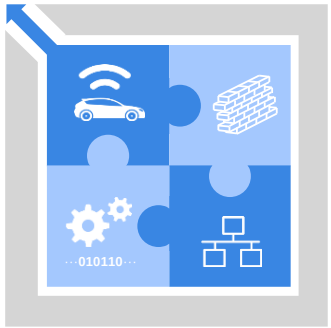


Secure **External Interfaces**

Secure **Domain Isolation**

Secure **Internal Communication**

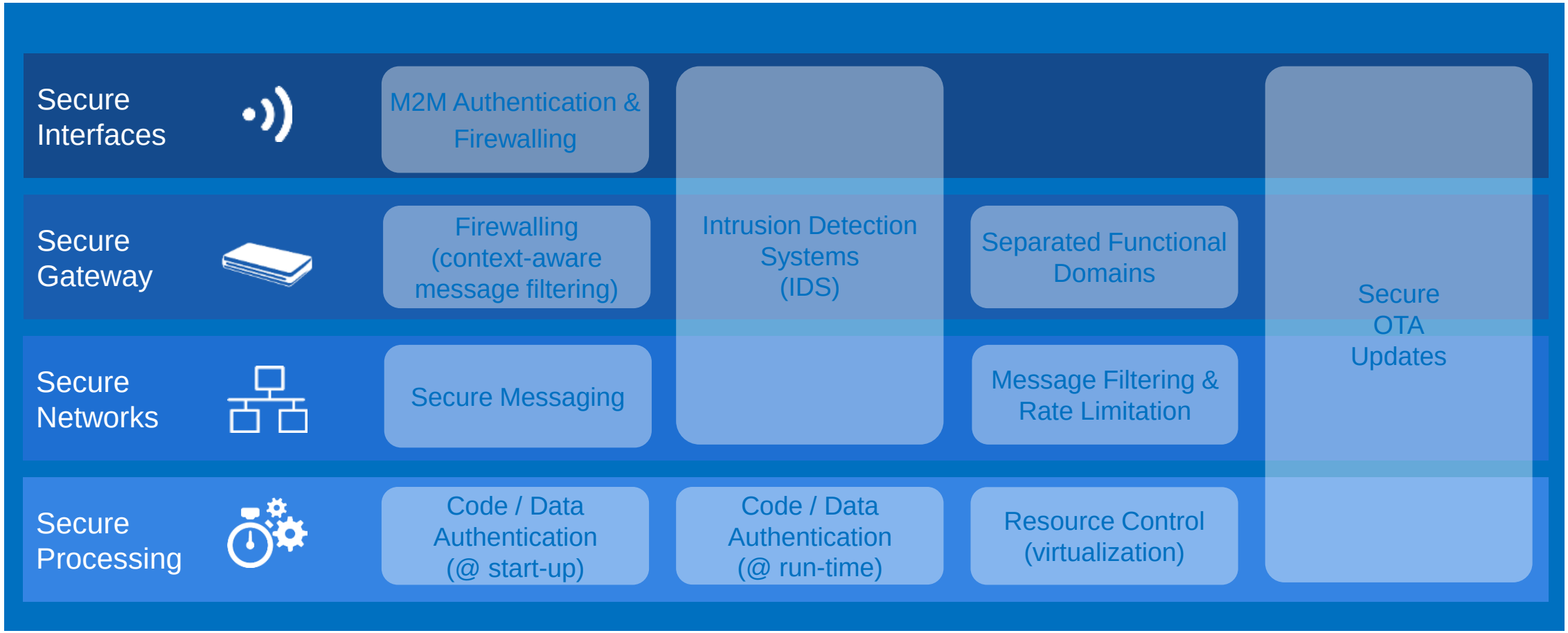
Secure **Software Execution**



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

- Regardless of the actual architecture and implementation

Applying the Core Security Principles in Vehicle Architectures



Risk Analysis

Security is not an all-or-nothing thing

- There is no such thing as ‘perfect security’

It´s about balancing costs and benefits

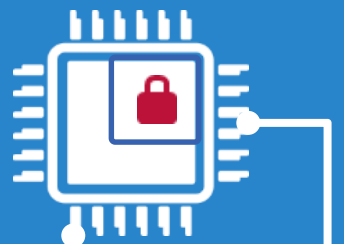
- For hacker, as well as for manufacturer

And security is not just about prevention

- Prevent to the extent possible & feasible
- Detect, & Respond (Mitigate, Fix) elsewhere

Solutions

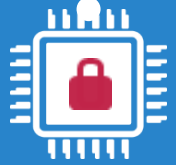
NXP’s Automotive Security Solution Groups



Automotive ICs with On-chip Security Subsystem

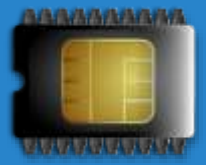
Integrated solution for best fit with application real-time constraints & for strict security policy enforcement

SENSE THINK ACT



Security Companions

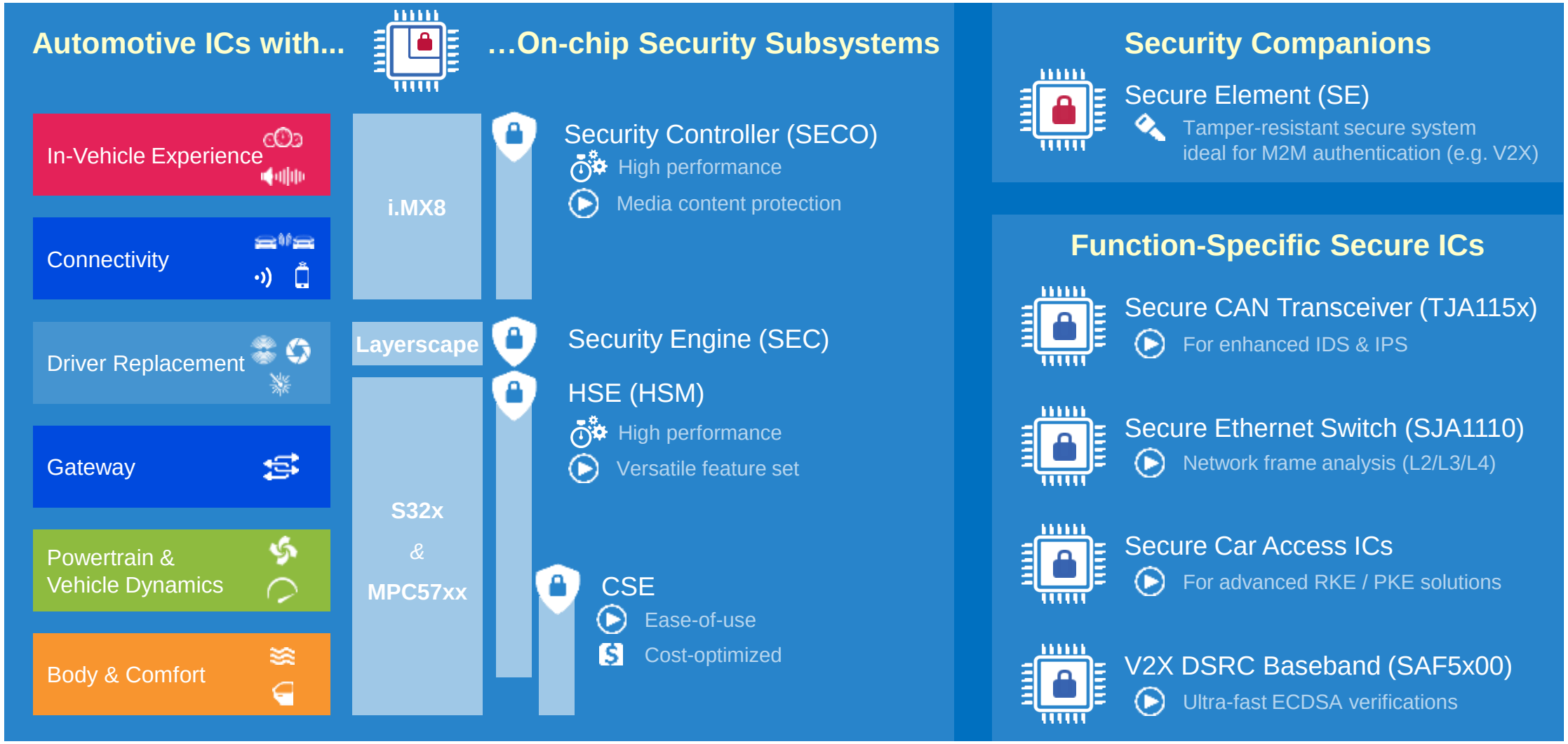
Certified security extension *for specific use*



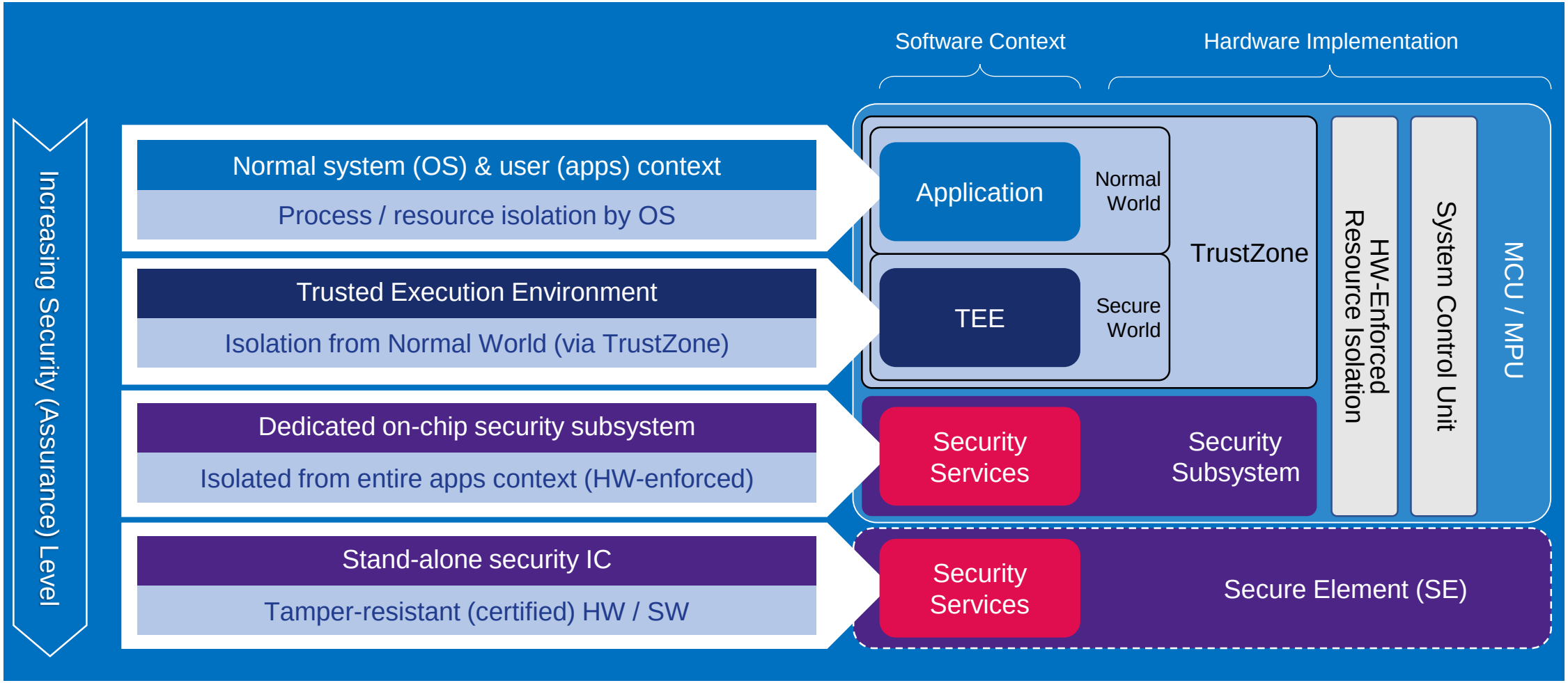
Function-specific Secure ICs

Fit-for-purpose security support

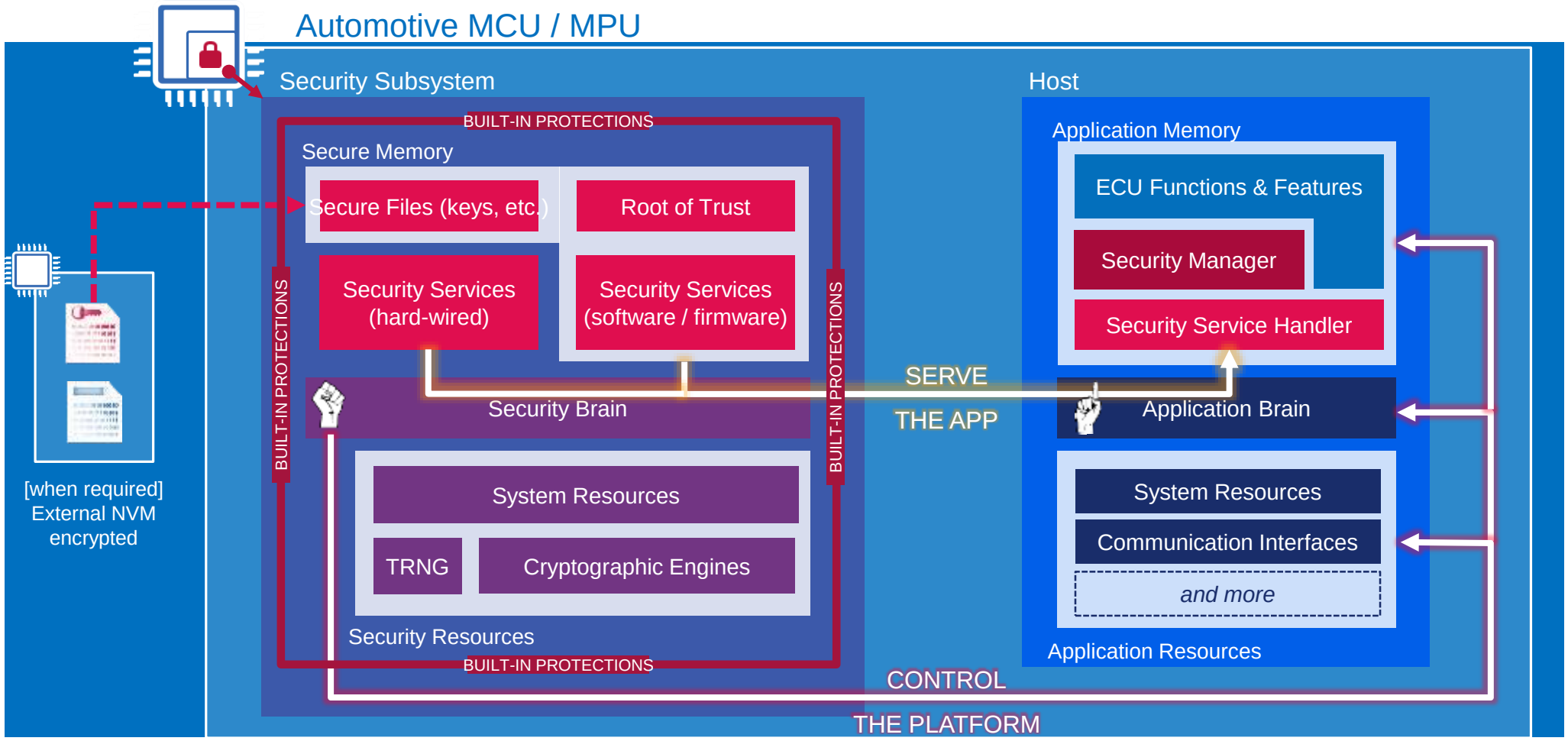
NXP's Automotive Security Solutions



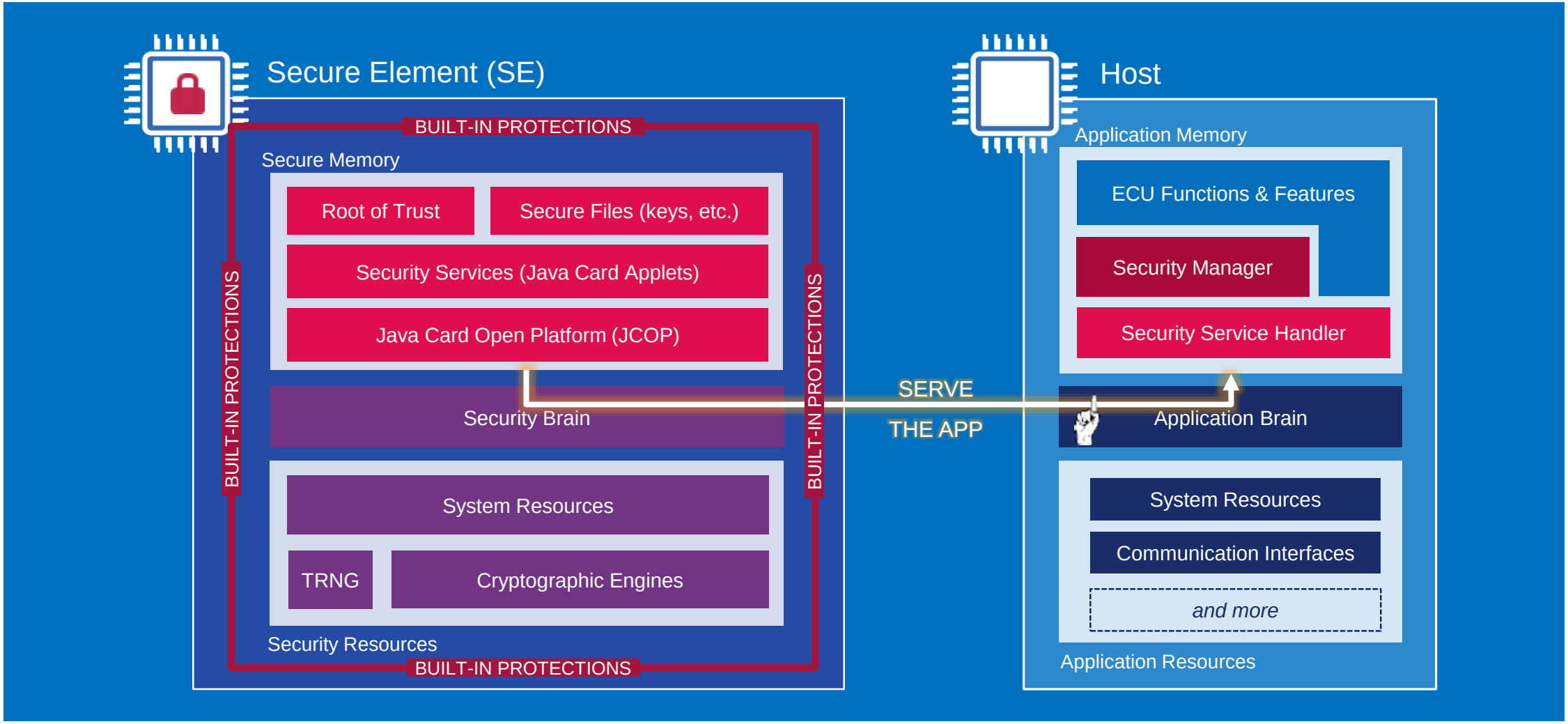
Secure Execution: In-depth Approach With NXP Solutions

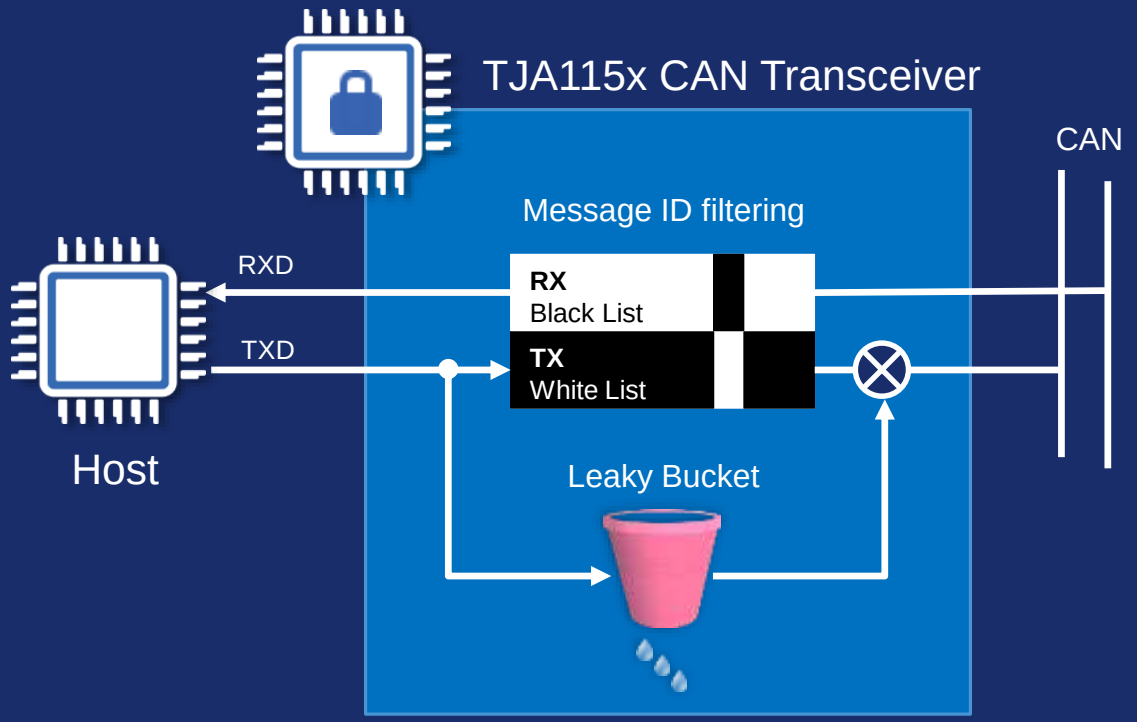


NXP's On-chip Security Subsystem: General System Overview



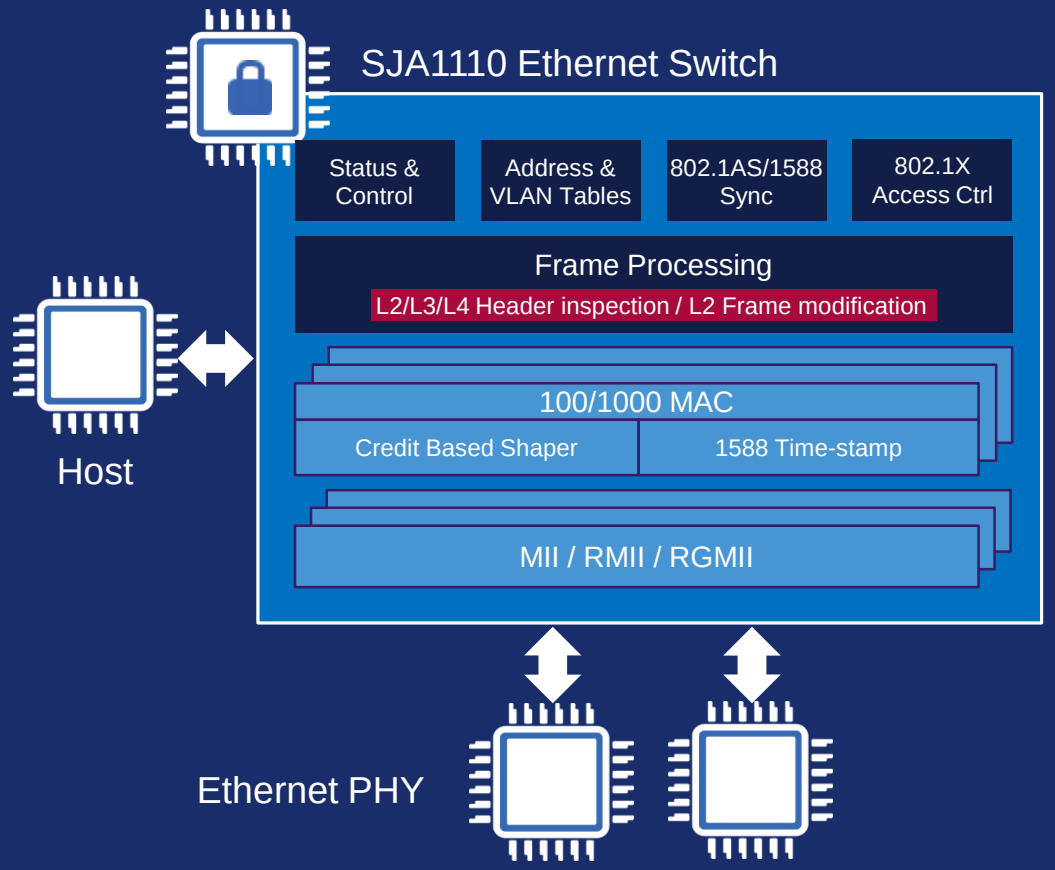
NXP's Secure Element: System Overview





NXP's Secure CAN Transceiver

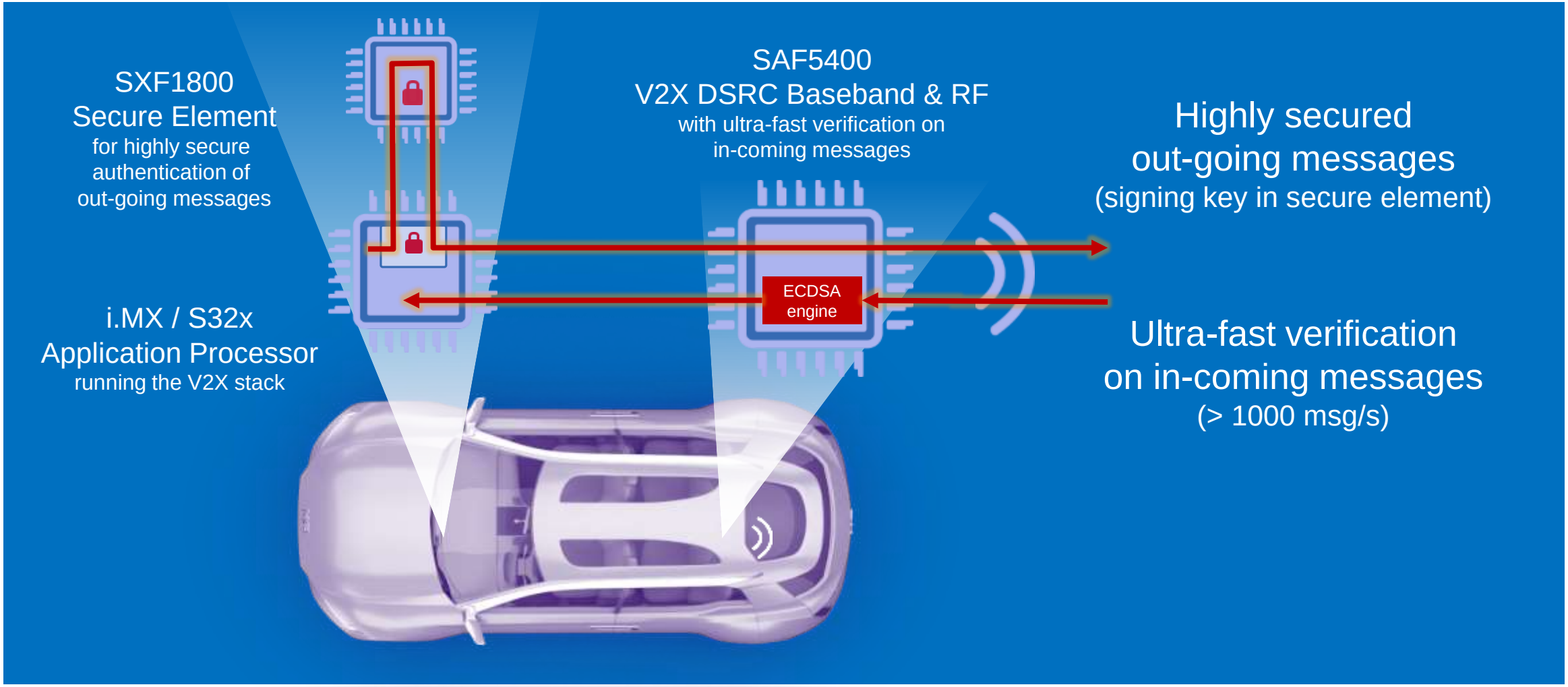
- Intrusion detection & prevention (IDS / IPS)
  - On-the-fly CAN ID filtering (TX) and bus-guarding (RX) based on user configurable white & black lists
  - Configuration based on ID & masking
- Flooding prevention (DoS)
  - Threshold on message transmission: leaky bucket strategy weighted on frame size
- "1:1" replacement to any CAN transceiver
  - Configurable via specific CAN frames
  - In-field reconfiguration possible
  - Automotive qualified (AEC-Q100)
  - Operating T° -40°C to 125°C



NXP's Secure Ethernet Switch

- **Authentication**
  - Port-based authentication (IEEE 802.1X)
  - Port-reachability HW enforcement & limitation
  - Address-learning with disable option
  - One-time MAC-address learning
- **DoS**
  - Data-rate limitation: port-based / priority-based / stream-based / broadcast
- **Traffic Isolation**
  - Up to 4096 VLAN / priority dynamic update at run-time; double tagging

NXP’s V2X Reference Security Architecture



Processes

Our Automotive Value Proposition

Solution Portfolio

The most complete System Solutions for fastest TTM and Scalability.

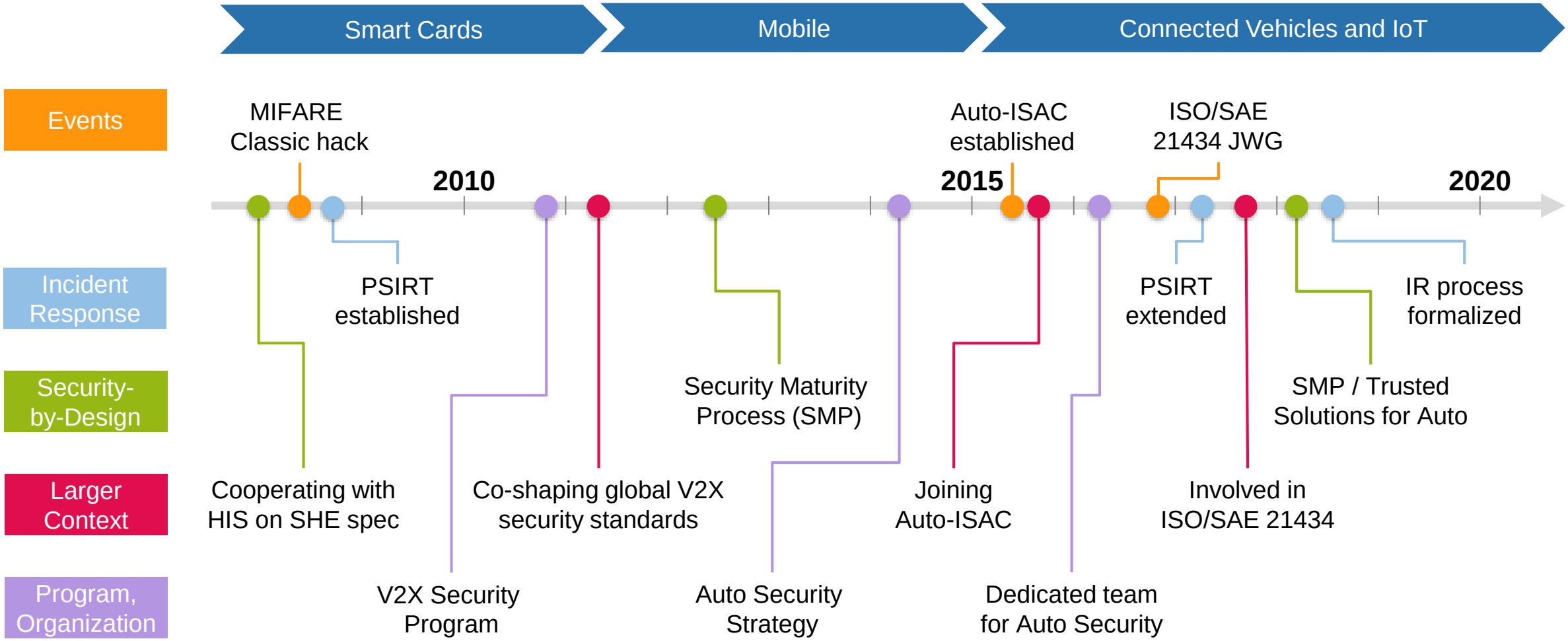
Innovation Power

In-house High Performance Processing, Security and Mobile Eco-System Capabilities.

Safe and Secure

Zero Defect Quality. Leading with Security and Functional Safety.

Security Culture and Organization – Matured Over Time



NXP's Automotive Cybersecurity Program

Holistic Approach to Security:

- Broad Portfolio of Security Solutions
- Secure Product Engineering Process
- Internal / External Security Evaluation (VA)
- Product Security Incident Response Team
- Security-Aware Organization (incl. Trainings)
- Threat Intelligence Feed

Leveraging our Cyber Security Framework:

- CSO / SOC / CSIRT, Information Security Policies, Incident Management and Response Processes, Site Security (ISO 27001 cert.), …

NXP was amongst the first suppliers to join the Auto-ISAC (Aug. 2016)

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

1 Receive report → 2 Evaluate vulnerability → 3 Define solution → 4 Communicate → 5 Evaluate process → 6 Closure

Product Development – Security Maturity Process

Threat Intelligence, BPWG, …

Lessons Learned (e.g. from IR)

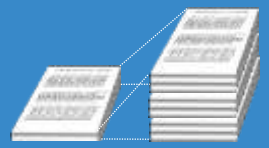
PROJECT LIFECYCLE

CONCEPT | DEFINITION | PLANNING | EXECUTION | CLOSURE

Security Milestones

Training and Awareness

Standards (ISO 21434, SAE J3061, …)



Monitoring security implementations at each gate

Independent and un-biased reviews – “4 eyes” principle

Process implementation can be adjusted per project

+ Trusted Solutions:
Framework and support to guide engineering teams

Training and Awareness – What Do We Do?

Trainings and Knowledge Transfer

- Regular basic security trainings
- Expert trainings on dedicated topics – internally and through external partners

Awareness

- Regular bulletins and campaigns to increase awareness
- Internal and external information sharing, through:
  - Regular internal meetings and online portal
  - Workshops with partners
  - Bi-directional sharing with Auto-ISAC, CERTs, …

Process Framework (ISO/SAE 21434)

Industry
(Auto-ISAC, Nat Council of ISACs, Customer Req, …)

SDOs
(ISO, NIST, SAE …)

GOs
(DoT/NHTSA, DHS, ENISA, FBI, NCCIC …)

NGOs
(CERTs, FIRST, …)

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com