Cyber-Security for Connected, Self-Driving Robots

A Semiconductor Perspective , Nov. 2018

Johnny CHEN – Senior Manager – GC Automotive CAS
NXP Semiconductors

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP – #1 Global Automotive Semiconductor Powerhouse

2400+
AUTO ENGINEERS

30+
AUTO SITES WORLDWIDE

#1
AUTO SEMI SUPPLIER GLOBALLY

~40%
OF NXP'S REVENUE IS FROM AUTO

60+
YEARS OF EXPERIENCE IN AUTO

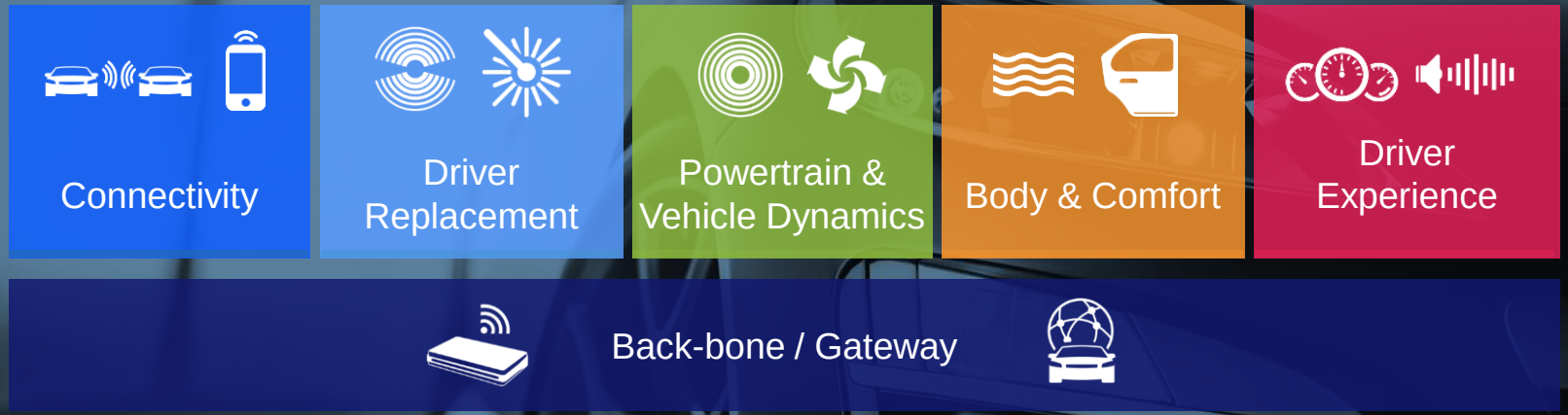
Presentation Contents

A semi-conductor perspective on the impact of cyber-security…

- On in-vehicle systems
- On our organization
- On our automotive processes
- On arising challenges for the industry

Paradigm Shift

Domain Based Vehicle Architecture



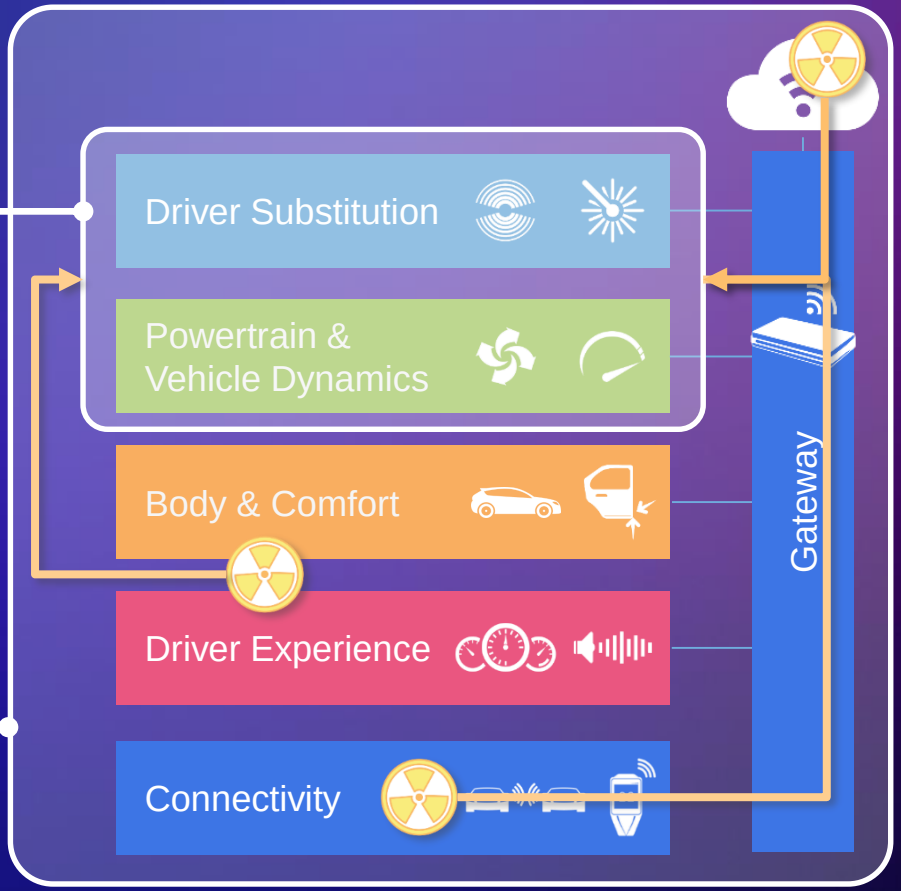
More than a brain on four wheels.
The core of safe and secure mobility.

No Safety Without Security

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

Collaterals:
System availability ensured
Information received / processed trustworthy

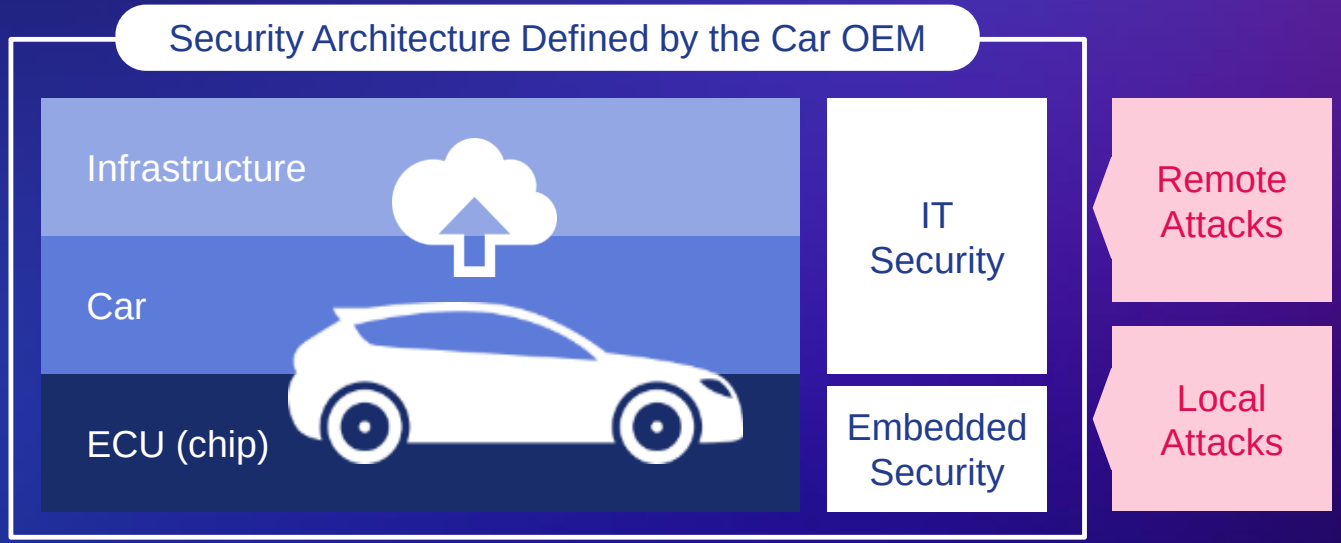
Cyber-security is the mean to establish availability and trust in the system



Industry Commitment to Security

Interaction with Functional Safety?

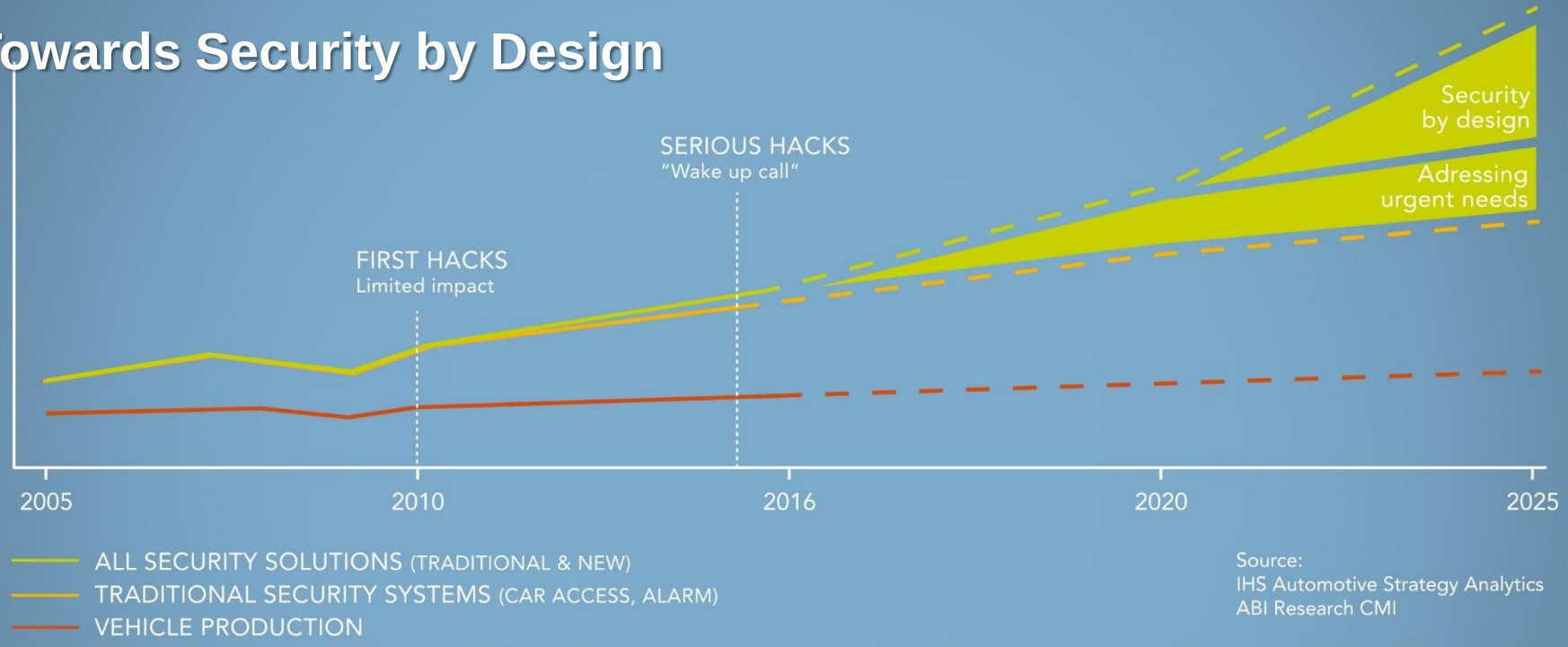
Overall Cost of Implementation?



Harmonized Security Requirements?

Harmonized Security Evaluations?

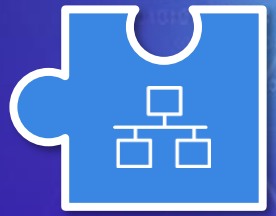
Towards Security by Design



The Core Security Principles

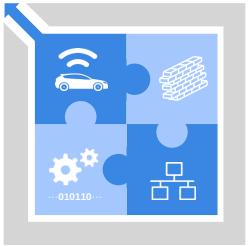
Secure
External Interfaces

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

Core Security Principles Applied to In-Depth Defenses

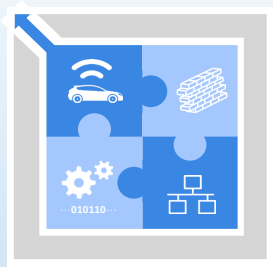
	Prevent access	**Detect** attacks	**Reduce** impact	**Fix** vulnerabilities
Secure Interfaces	M2M Authentication & Firewalling	Intrusion Detection Systems (IDS)		Secure Updates
Secure Gateway	Firewalling (context-aware message filtering)		Separated Functional Domains	
Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	

Security Requires a Holistic Approach (& Ongoing Effort)

Vehicle Lifecycle

Design	Build	Use	Scrap

Apply the core security principles



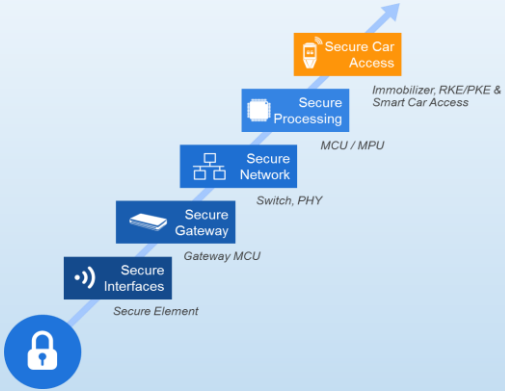
Secure **External Interfaces**

Secure **Domain Isolation**

Secure **Internal Communication**

Secure **Software Execution**

Using NXP's solution portfolio



Maintain products in the field

- Monitor
- Respond to incidents
- Contain vulnerabilities
- Fix vulnerabilities

Software Management (e.g. FOTA updates)

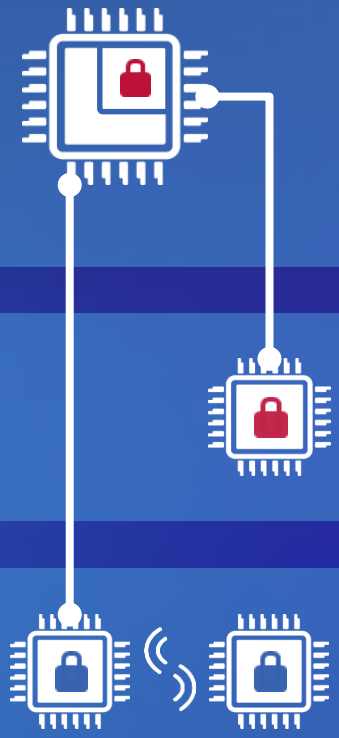
Configuration Management (e.g. feature unlocking)

Key Management (e.g. trust provisioning)

…

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

NXP’s Automotive Security Solutions Groups



Automotive ICs with On-chip Security Subsystem

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

Security Companions

Security extension *for specific use*

Function-specific Secure ICs

Fit-for-purpose security support

NXP's Automotive Security Solutions

Automotive ICs with... ...On-chip Security Subsystems

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

i.MX8

- Security Controller (SECO)
  - High performance
  - Media content protection

Layerscape

- Security Engine (SEC)

S32x & MPC57xx

- HSE (HSM)
  - High performance
  - Versatile feature set
- CSE
  - Ease-of-use
  - Cost-optimized

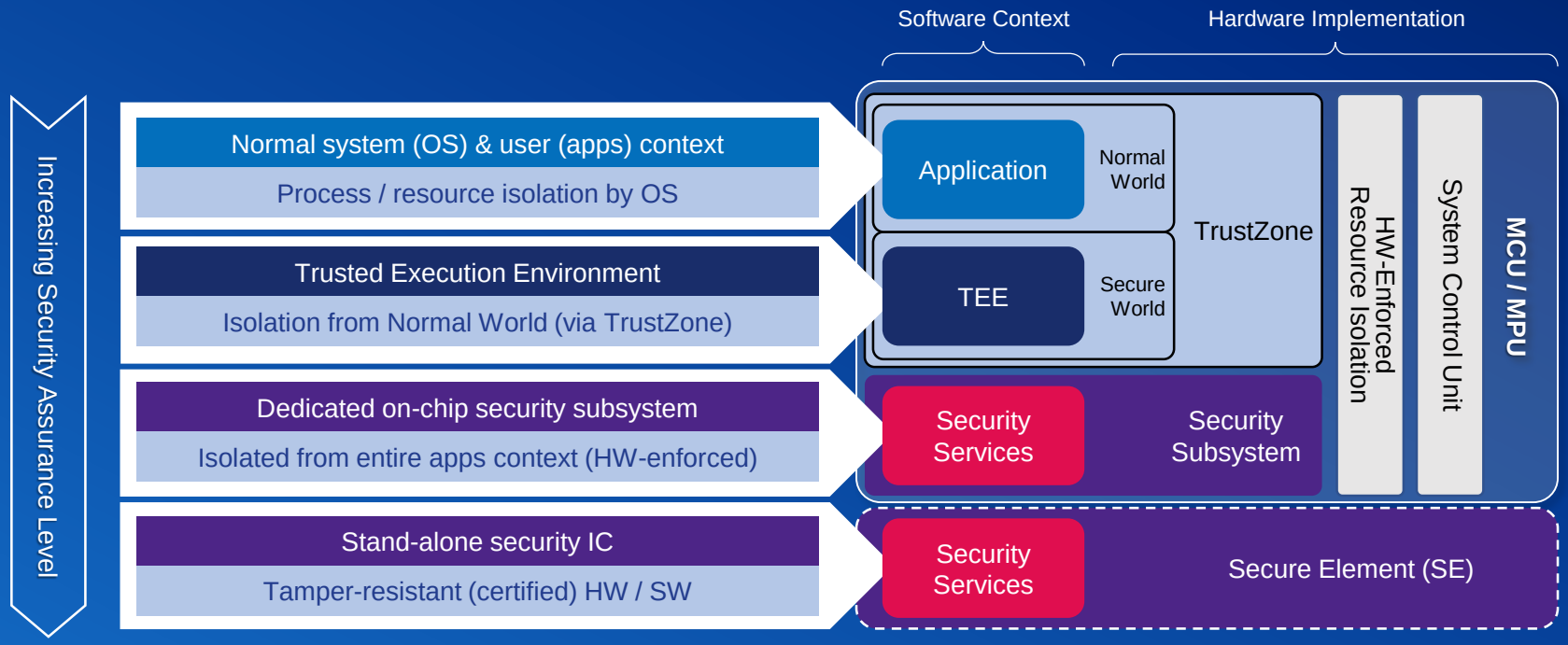
Security Companions

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

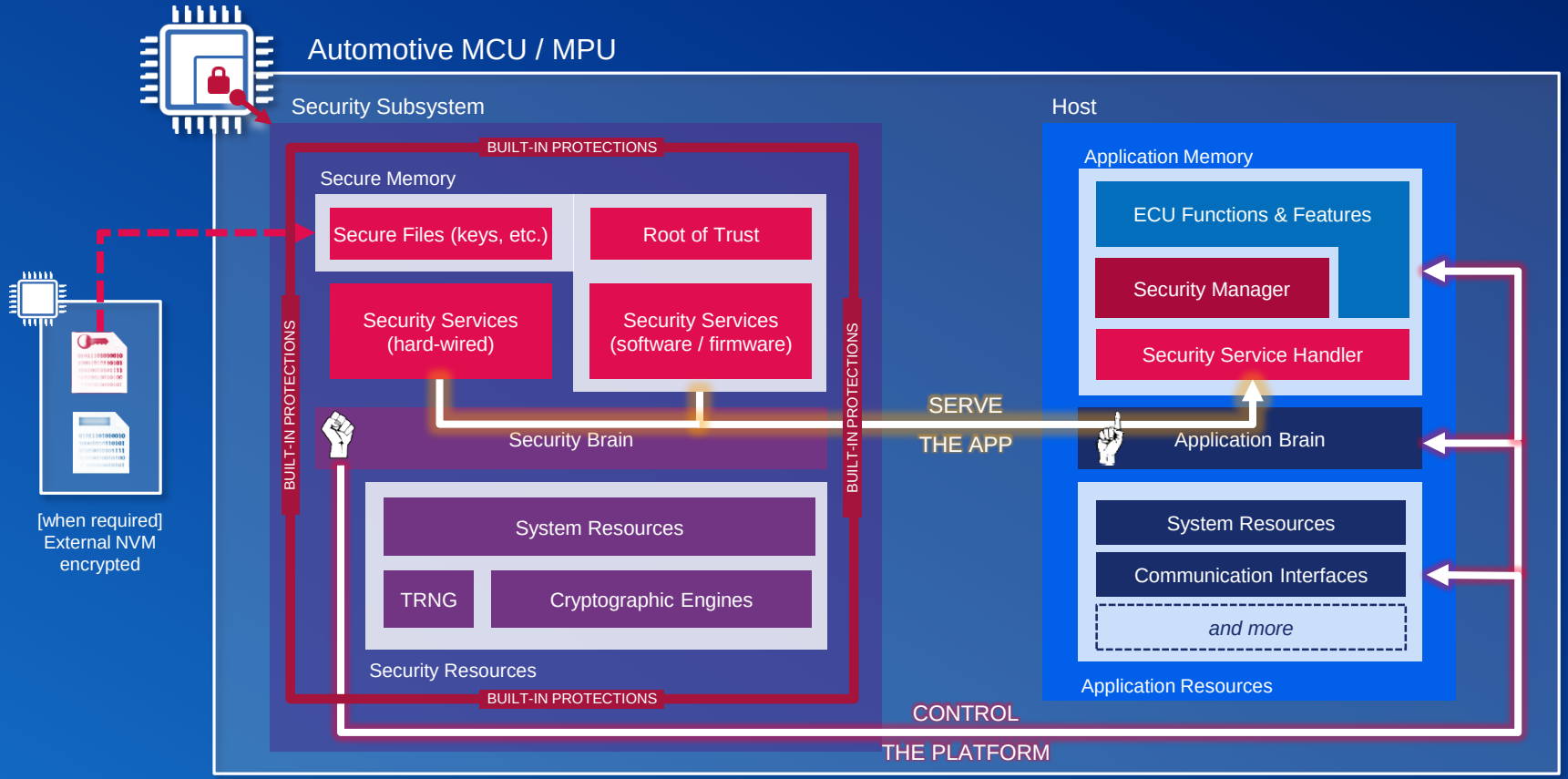
Function-Specific Secure ICs

- Secure CAN Transceiver (TJA115x)
  - For enhanced IDS & IPS
- Secure Ethernet Switch (SJA1110)
  - Network frame analysis (L2/L3/L4)
- Secure Car Access ICs
  - For advanced RKE / PKE solutions
- V2X DSRC Baseband (SAF5x00)
  - Ultra-fast ECDSA verifications

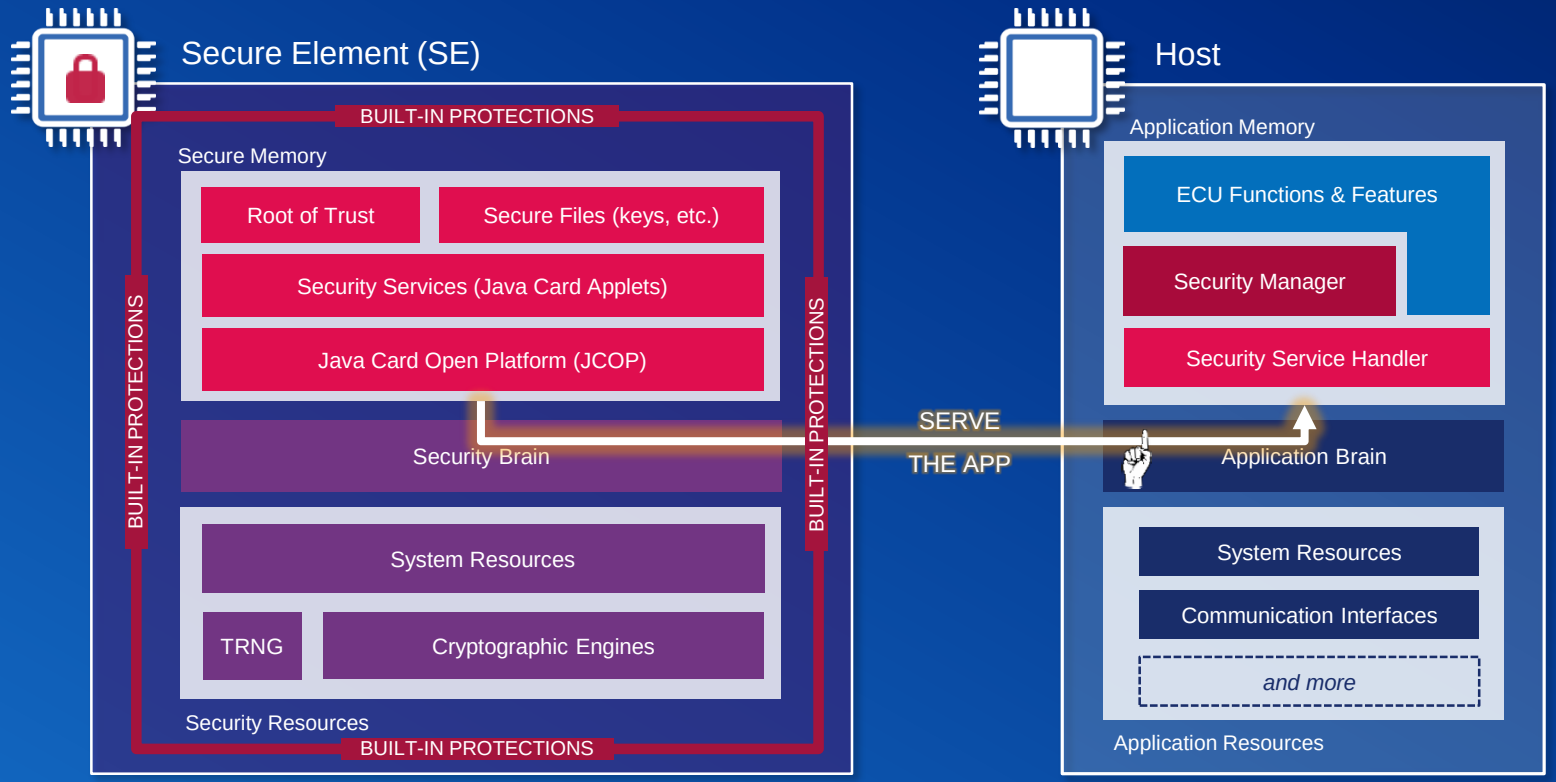
Secure Execution: In-depth Approach with NXP Solutions



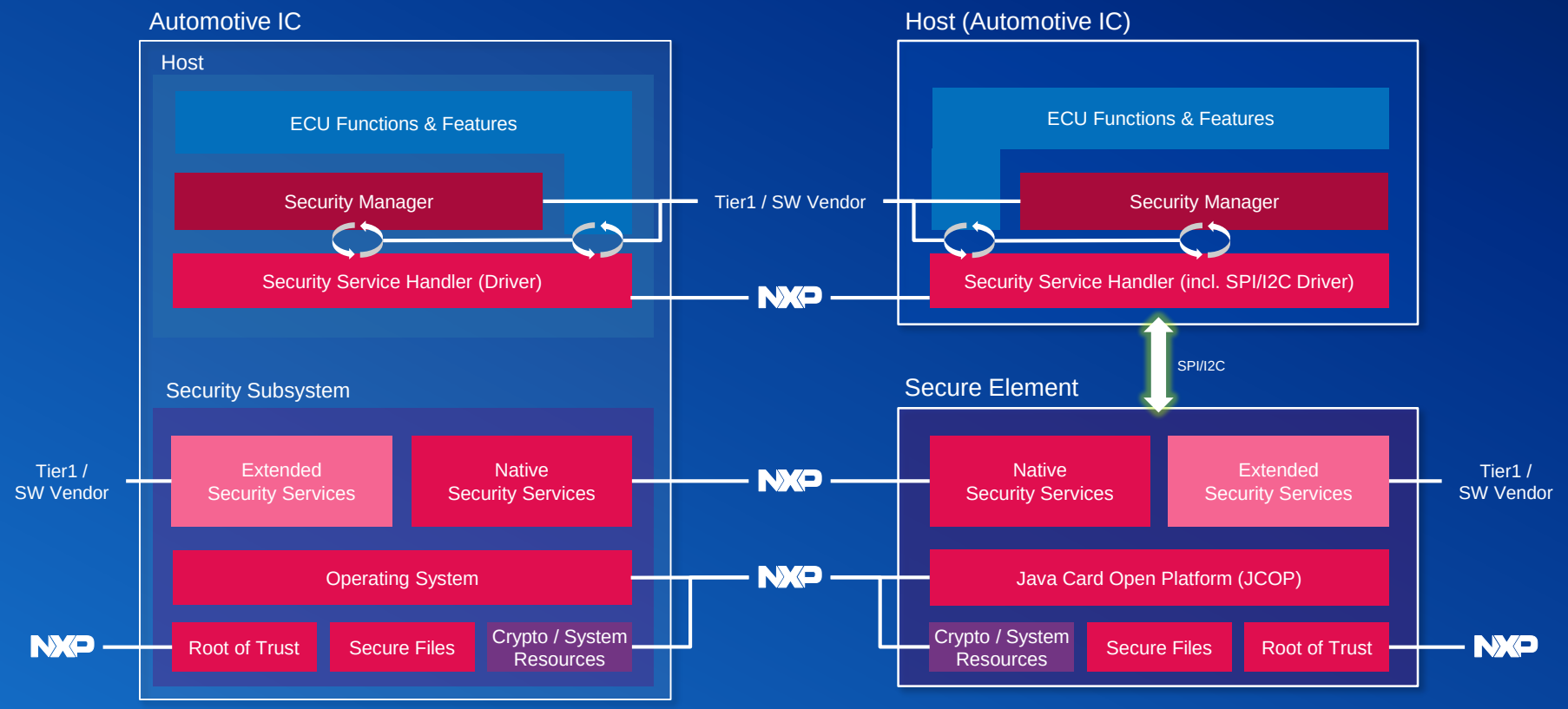
NXP's On-chip Security Subsystem: General System Overview



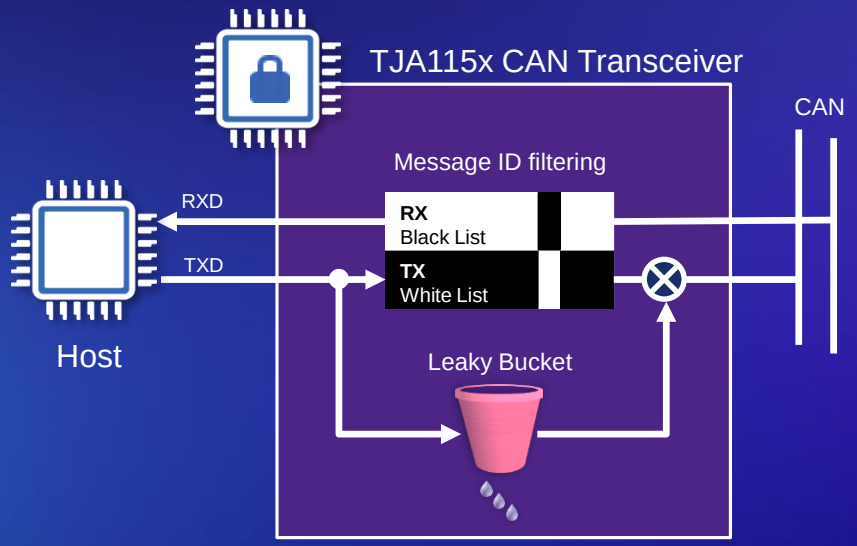
NXP’s Secure Element: System Overview



Software Components in Play

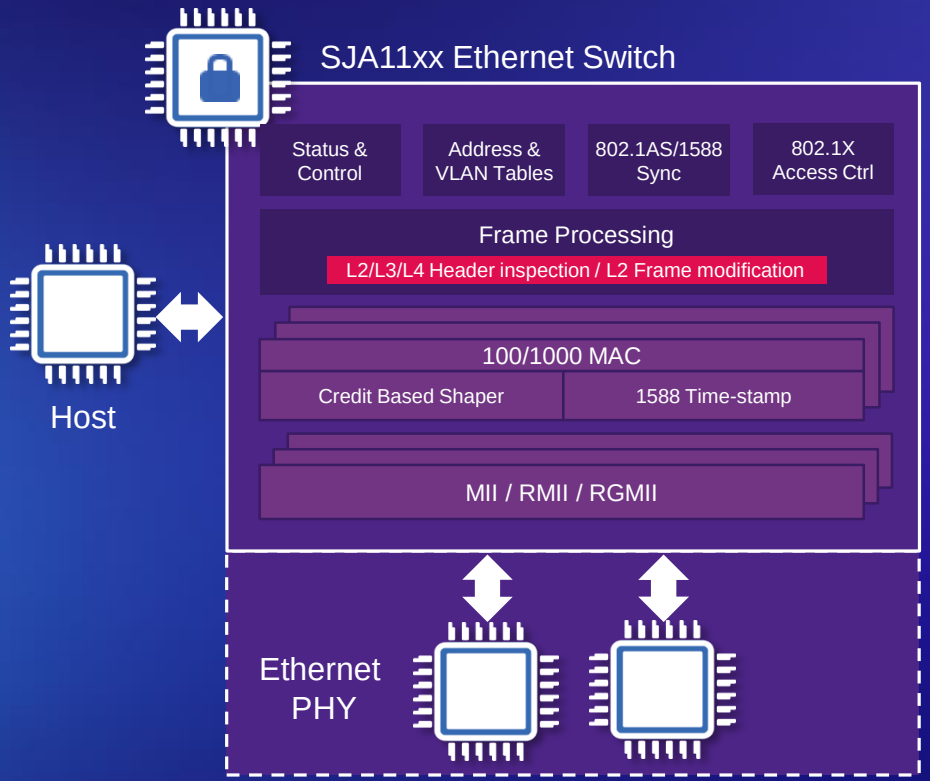


NXP’s Secure CAN Transceiver



- 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

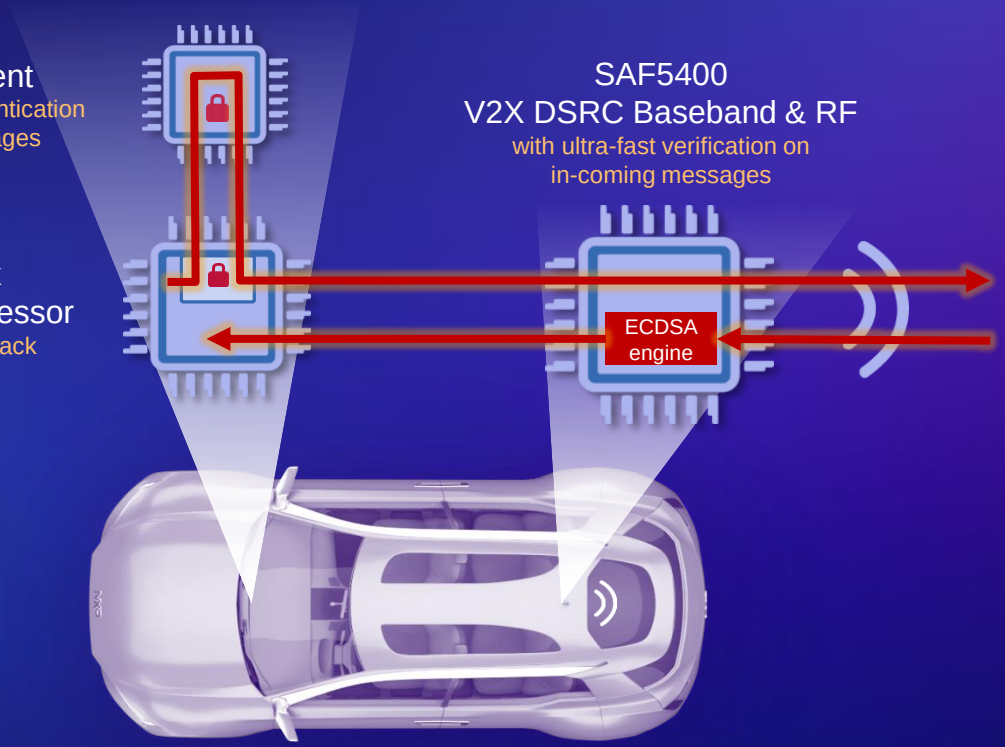


- Authentication
  - Port-based authentication (IEEE 802.1X)
  - Port-reachability HW enforcement & limitation
  - Address-learning with disable option
  - One-time MAC-address learning
- DoS
  - Data-rate limitation: port-based / priority-based / stream-based / broadcast
- Traffic isolation
  - Up to 4096 VLAN / priority dynamic update at run-time; double tagging
- TT & TSN Features (SJA1105TEL only)
  - 802.1Qbv time-aware traffic, (pre-standard) IEEE 802.1Qci

NXP's V2X Reference Security Architecture

SXF1800
Secure Element
for highly secure authentication
of out-going messages

i.MX / S32x
Application Processor
running the V2X stack



SAF5400
V2X DSRC Baseband & RF
with ultra-fast verification on
in-coming messages

Highly secured
out-going messages
(signing key in secure element)

Ultra-fast verification
on in-coming messages
(> 1000 msg/s)

NXP’s Secure Car Access Solutions

Immobilizer

Authentication for Engine Start

PCF793x — Transponder: TP

1. LF Challenge
2. LF Response

Px799x — Base station: BS

Remote Keyless Entry

On-demand Authentication

NCF2961 — RF Tx; µC; TP*

RF signal (rolling code) (on Button press)

*Immobilizer function included

NCK2912 — RF Rx

PxF799x — BS*

Passive Keyless Entry

Hand-free, with Distance Bounding

NCF29A1 — LF Rx; TP*

NCF29Dx — RF Tx*

1. LF Wake-Up/Challenge
2. RF Response

*Immo/RKE function included

NJJ29C0 — LF Tx; BS*

NCK2912

NCF29Dx — RF Rx*

Smart Car Management

2-way RF & Distance Bonding

NCF2984 — RF Tx/Rx; µC

RF Data Exchange

NCK2983 — RF Tx/Rx; µC

Smart Access (mobile devices)

access via NFC/BLE-enabled devices

PN44x — BLE; NFC; eSE

Secure Data Exchange

(e.g. CCC Digital Key)

KW3x — BLE

NCF3320/40 — NFC

NCJ38Ax — eSE

NXP' Automotive Cyber-security Program

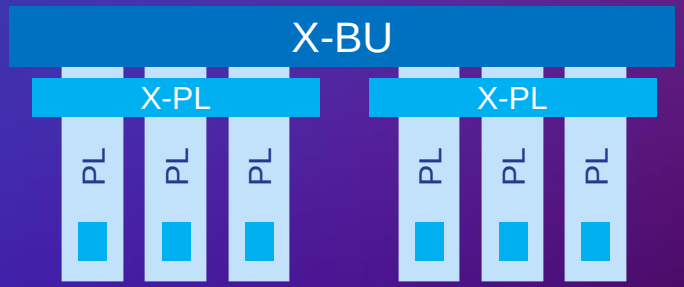
NXP was amongst the first suppliers to join the Auto-ISAC (Aug. 2016)

- Security-Aware Organization
- Threat Intelligence Feed (e.g. Auto-ISAC)
- Product Security Incident Response Team
- Secure Product Engineering Process
- External Audits for Product & Site Security
- Trust Provisioning
- …

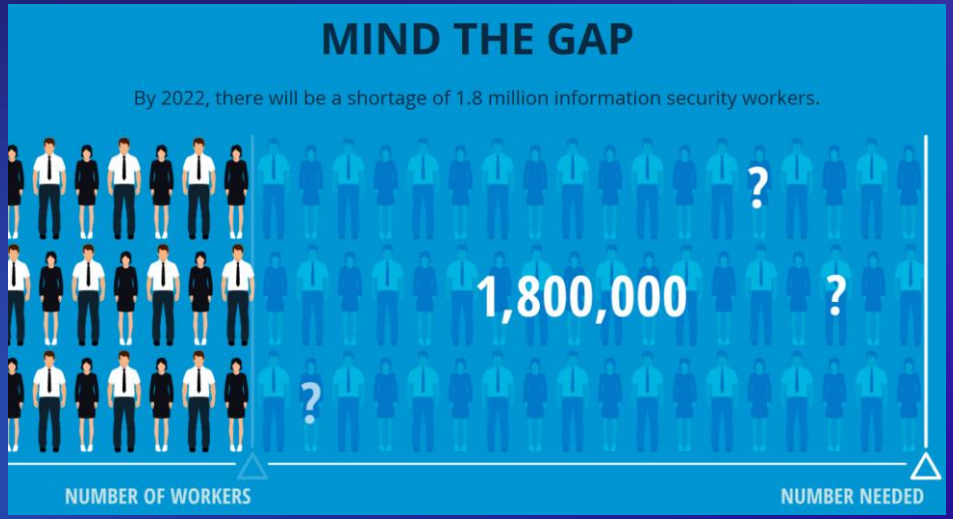
How are we Organized?

- Automotive
  - Central automotive security team
    - Centralized expertise with a dedicated focus
  - Virtual team of security experts
    - Regular interactions
    - With representatives from various product lines
    - And with the central team
    - Various backgrounds: Marketing / FAE / Sales / Strategy / MarCom
- Corporate
  - Cross BU alignment
  - Leveraging experts and expertise from different markets
    - Banking, e-identity, digital infrastructure, …

Security Accross NXP's Organization



Challenge: Finding the Right Experts



Source: Center for Cyber Safety and Education, February 2017
https://iamcybersafe.org/research_millennials/

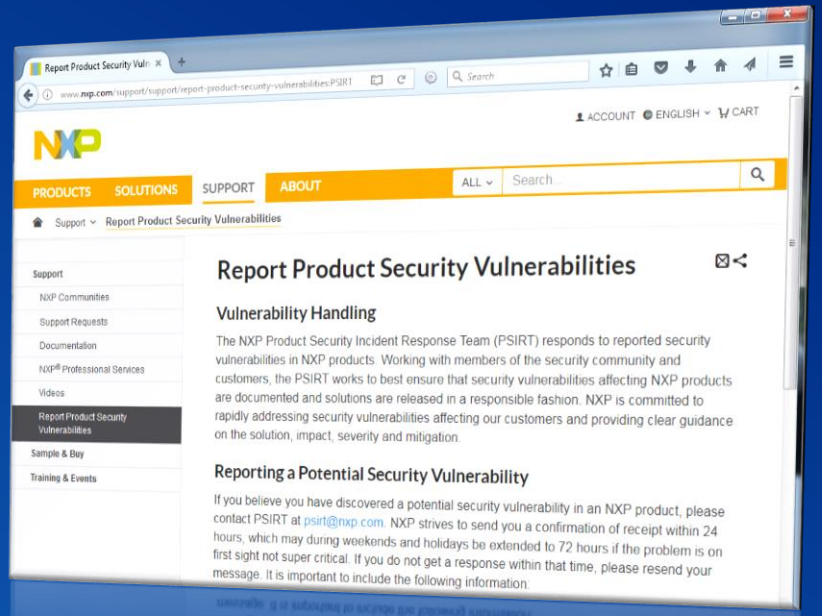
Survey over 19,000 security professionals says industry short by 1.8 million experts in 2022

Can potentially negatively impact security solutions in the Automotive industry

NXP's Product Security Incident Response Team (PSIRT)

- Global security incident response process – across products / markets / regions
- Established in 2008 after the MIFARE Classic hack
- Committed to responsible disclosure
  - Receive & acknowledge report
  - Evaluate vulnerability
  - Identify solutions
  - Communicate (direct & through CERTS & Auto-ISAC)
- Closely working with the security community and with our customers
- Continuous process evaluation & benchmarking
  - E.g. against Auto-ISAC's best practice guide

Web page: www.nxp.com/psirt
e-mail: psirt@nxp.com



Security in NXP's Automotive Product Engineering Process

One security gate for each gate in NXP' standard lifecycle

Monitoring security implementations at each gate via checklists, deliverables and dedicated reviews

Independent & un-biased analysis based on "4 eyes" principle

Process implementation can be adjusted per project
(scalability based on product scope)

Security system architecture, threat & vulnerability analysis, evaluation, certification, …

CONCLUSION

- The development of self-driving robots calls for a paradigm shift
- Security is essential –
  people must be able to trust their cars
- NXP proposes the implementation of four security principles throughout the vehicle
- NXP's cyber-security program complements the solution offering:
  - Security-aware organization
  - Security as part of our Automotive processes
  - PSIRT
  - Threat intelligence with Auto-ISAC

Visit: www.nxp.com/automotivesecurity

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com/automotivesecurity