Security in ^{4}SDV

Lessons learned from integrating MotionWise Safety Middleware in customer ECUs

IFIP WG 10.4

HÉCTOR BRAVO

JUNE 28, 2025

tttech auto

part of NXP

Introduction

Héctor Bravo

Manager of
Security Engineering

M +34 662 084 837
hector.bravo@tttech-auto.com

- In **TTTech Auto**, now **NXP**, since 2018
- Held roles as **Security Engineer**, **System Engineer** and **Security Manager**
- Currently **leading Security Engineering** across the organization
- Responsible for projects & products compliance with **ISO/SAE 21434**, **ASPICE for Cybersecurity** and other norms
- Until 2018, contributed to the **smart card** and **IOT Security** industries, including **HSM** and **Secure Elements**
- Familiar with smart cards standards such as **Global Platform**, **ETSI**, **Java Card**, **GSMA**, **EMV** and more

tttech auto
part of NXP

Agenda

01 TTTech Auto's Role

02 From Distributed to Centralized Architectures

03 Cybersecurity at Scale

04 Assumptions from Hardware

05 Agile & Automotive Security

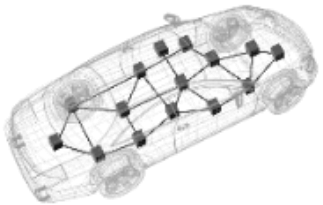
06 Conclusions

07 Q&A

TTTech Auto's Role in the Industry

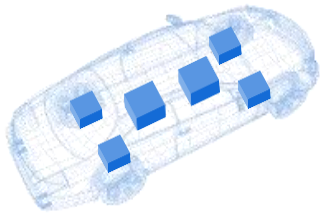
SDV Paradigm Shift and Complexity Explosion

- Shifting focus to electronic user experiences
- Connected mobility and automated driving
- SDVs require continuous updates of enjoyable and safe functionality
- Driven by exponential growth of SoCs performance



Distributed E/E architecture
(*n* ECUs : n functions)

Transformation



Centralized E/E architecture
with Zones
(2 High-Perf ECUs : *n* functions)

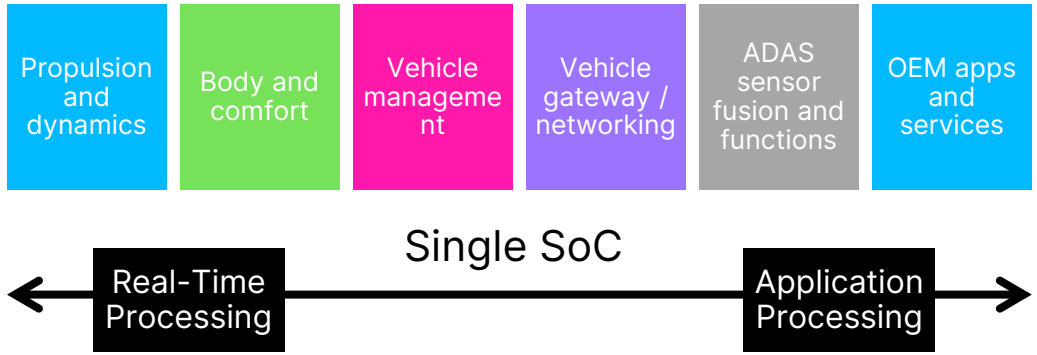
Paradigm Shift

Vehicle super-integration processors

New and powerful capabilities come with configuration complexity

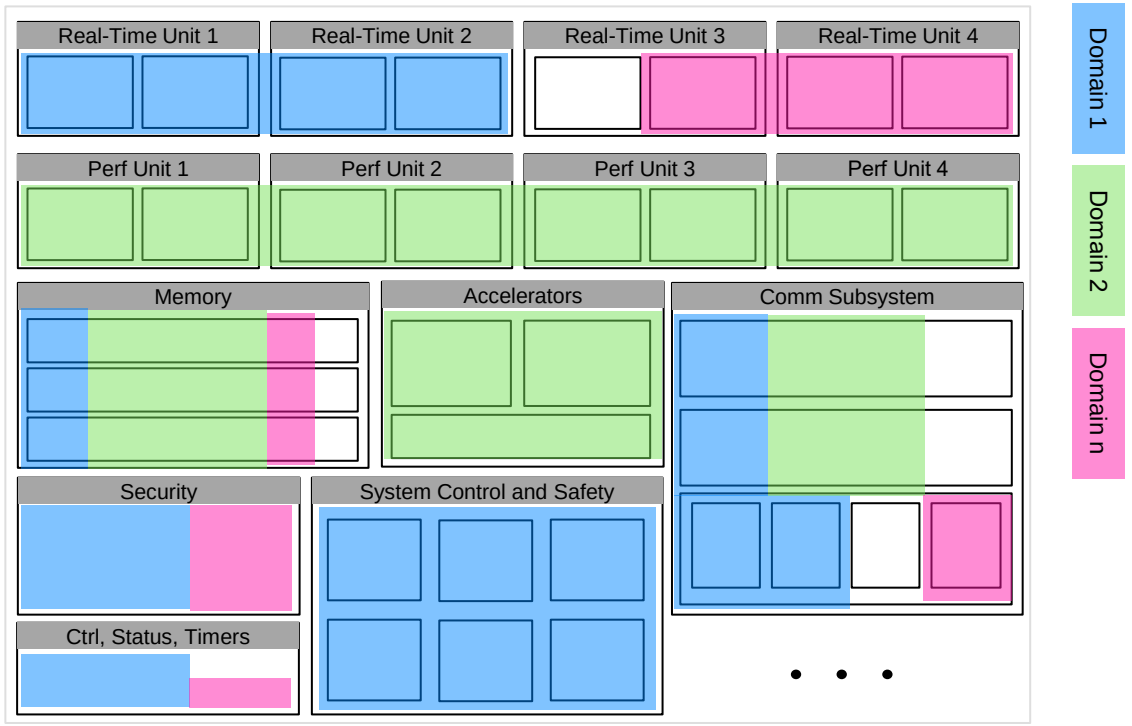
Super-integration Processors

- Migration from domains and zones to central compute with super-integration of vehicle functionse of use-cases from high-level application
- Broad rang processing to real-time demands



Configuration Complexity

- Enhanced HW partitioning functionality for multiple integrated domains



From SDV to 4SDV

SYSTEM • SAFETY • SECURITY • SOFTWARE

4SDV

System

- System engineering
- System architecture
- ...

Safety

- Addressing safety goals
- Safe real-time execution and communication
- Freedom from interference / partitioning
- Fail-operational
- ...

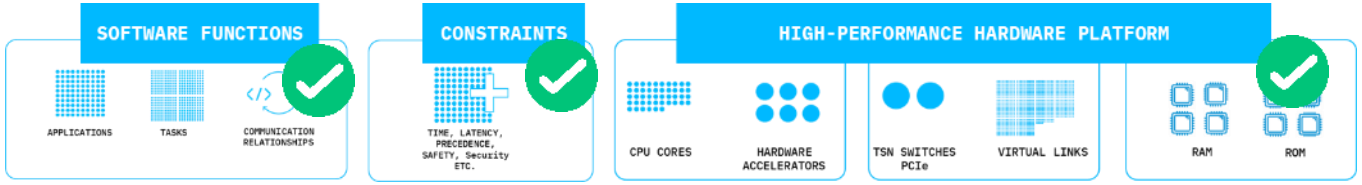
Security

- Secure Boot & Over-The-Air-Updates
- Secured on-board & edge to cloud communication
- ...

Software

- Fully automated SW integration (CI/CD)
- Cloud-to-edge re-/simulation capabilities
- ...

Formalization for the 4SDV



1 Formal Model

- **Mathematical** formalism, based on years of **R&D** and validation in **customer projects** (60 pages of formulas)
- **Complete**, **rigorous**, and **comprehensive correctness** check with SMT Solver
- Ensures **well-defined** and **unambiguous** requirement expression

2 Formal Input description

- A scriptable and human-readable format based on JSON
- Enables automated deployment and V&V automation

Building an open industry consolidated model

> We are interested to work with partners to define an open industry consolidated model

> we are ready to contribute our formal model and input Language format

1

$$\forall [v_a, v_b] \in \mathcal{E}, \forall f_i, f_l \in \mathcal{F} \ni [v_a, v_b] \in R_i \wedge [v_a, v_b] \in R_l \wedge i \neq l$$

$$\forall J_{ij}^{[v_a,v_b]} \in \mathcal{J}_i^{[v_a,v_b]}, \forall s_{ijk}^{[v_a,v_b]} \in \mathcal{S}_{ij}^{[v_a,v_b]}, \forall J_{lm}^{[v_a,v_b]} \in \mathcal{J}_l^{[v_a,v_b]}, \forall s$$

$$\forall [v_x, v_a] \in R_i, \forall [v_y, v_a] \in R_l :$$

$$\Big(\big(\exists w_o \in \mathcal{W}^{[v_a,v_b]} \ni z_{ijk}^{w_o} = 1\big) \wedge \big(\exists w_p \in \mathcal{W}^{[v_x,v_a]} \ni z_{ijk}^{w_p} = 1\big)$$

$$\big(\exists w_q \in \mathcal{W}^{[v_a,v_b]} \ni z_{lmn}^{w_q} = 1\big) \wedge \big(\exists w_r \in \mathcal{W}^{[v_y,v_a]} \ni z_{lmn}^{w_r} = 1\big)\Big) \implies$$

$$\Big(\big((x^{w_o} + y^{w_o} + \delta_n \leq x^{w_r} + [v_y, v_a].\delta_{tx}^{min} + [v_y, v_a].\delta_t) \vee$$

$$(x^{w_q} + y^{w_q} + \delta_n \leq x^{w_p} + [v_x, v_a].\delta_{tx}^{min} + [v_x, v_a].\delta_t)\big) \vee$$

$$\big(w_o = w_q\big) \vee$$

$$\big((w_o \neq w_q) \wedge (w_o.q \neq w_q.q)\big)\Big)$$

$$\Big(\big(\phi_i + r_i + j \times T_i \geq \phi_l + r_l + m \times T_l\big) \wedge (p_i > p_l)\Big) \implies$$

$$\Big(\nexists s_{lmn} \in \mathcal{S}_{lm} \ni \big((x_{lmn} \geq \phi_i + j \times T_i) \wedge (x_{lmn} + y_{lmn} \leq \max_{\forall s_{ijk} \in \mathcal{S}_{ij}} \{x_{ijk}\})\big)\Big)$$

$$\Big(\big(\phi_i + r_i + j \times T_i \geq \phi_l + r_l + m \times T_l\big) \wedge (p_i \leq p_l)\Big) \implies$$

$$\Big(\Big(\big(\phi_i + r_i + j \times T_i = \phi_l + r_l + m \times T_l\big) \wedge (p_i = p_l) \wedge (\rho_j < \rho_m)\Big) \vee$$

$$\Big(\nexists s_{ijk} \in \mathcal{S}_{ij} \ni \big(x_{ijk} + y_{ijk} \leq \max_{\forall s_{lmn} \in \mathcal{S}_{lm}} \{x_{lmn}\}\big)\Big)\Big)$$

Checking input for compliance with model

System specification is in scope

First level check

2

```
{    "ecu_name": "RDB2",
     "host_name": "PerformanceHost00",
     "schedule_type": "TIME-TRIGGERED",
     "rnbl_default_stack_size": 524288,
     "cores": [ {
         "core_id": 0,
         "macrotick": {
           "value": 100,
           "unit": "us“ },
         "task_overhead": {
           "task_switch_overhead": {
             "value": 200,
             "unit": "us“ } }, ]

{ "swc_runnables": [ {
     "id": {
       "ecu": "RDB2",
       "host": "SafetyHost00",
       "swc": "CpApTest1_SH00",
       "name": "RTest1_SH00_0“ },
  "bsw_tasks": [ {
     "id": {
       "ecu": "RDB2",
       "host": "SafetyHost00",
       "name": "Task_10ms_QM_C0“ },
     "parameters": {
       "period": {
         "value": 10,
         "unit": "ms“ },
       "execution_budget": {
         "value": 250,
         "unit": "us“ },
       "consider_overheads": true },
     "requirements": {
       "earliest_activation": {
         "value": 1750,
         "unit": "us“ },
       "allowed_cores": [ 0 ]  }
  },
```

Global Computation Chains Created with MotionWise Schedule

Coordinate applications and workloads on chip and off chip

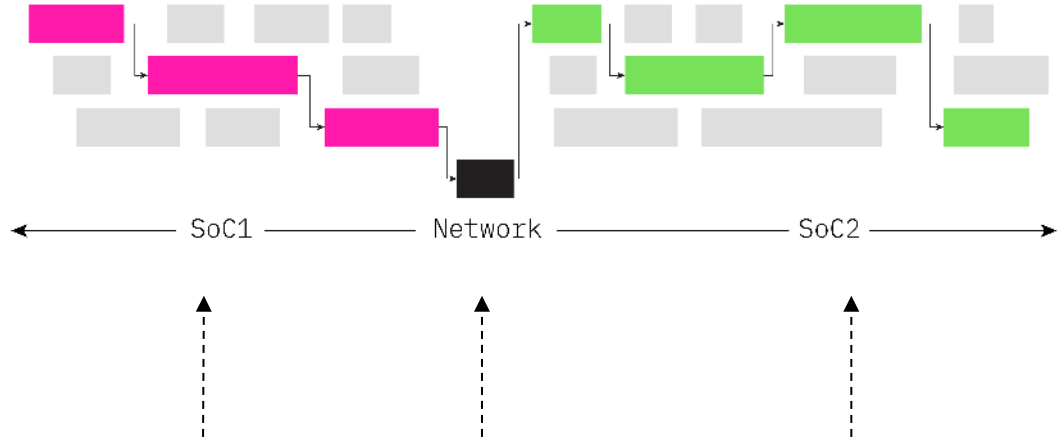
Define constraints → Find the global solution → Deploy on target

- **Precedence constraints**
- **Jitter**
- **End-to-End latency**
- **Unlimited* number of chains**

Provide timing **requirements** not scheduling configuration

MotionWise Schedule Tooling

Automatically generate corresponding configuration



- **Abstracts host and network configurations**
- **Enabled by time synchronized execution with a single common time base**

“What you see is what you get” execution

* physical HW limitation applies

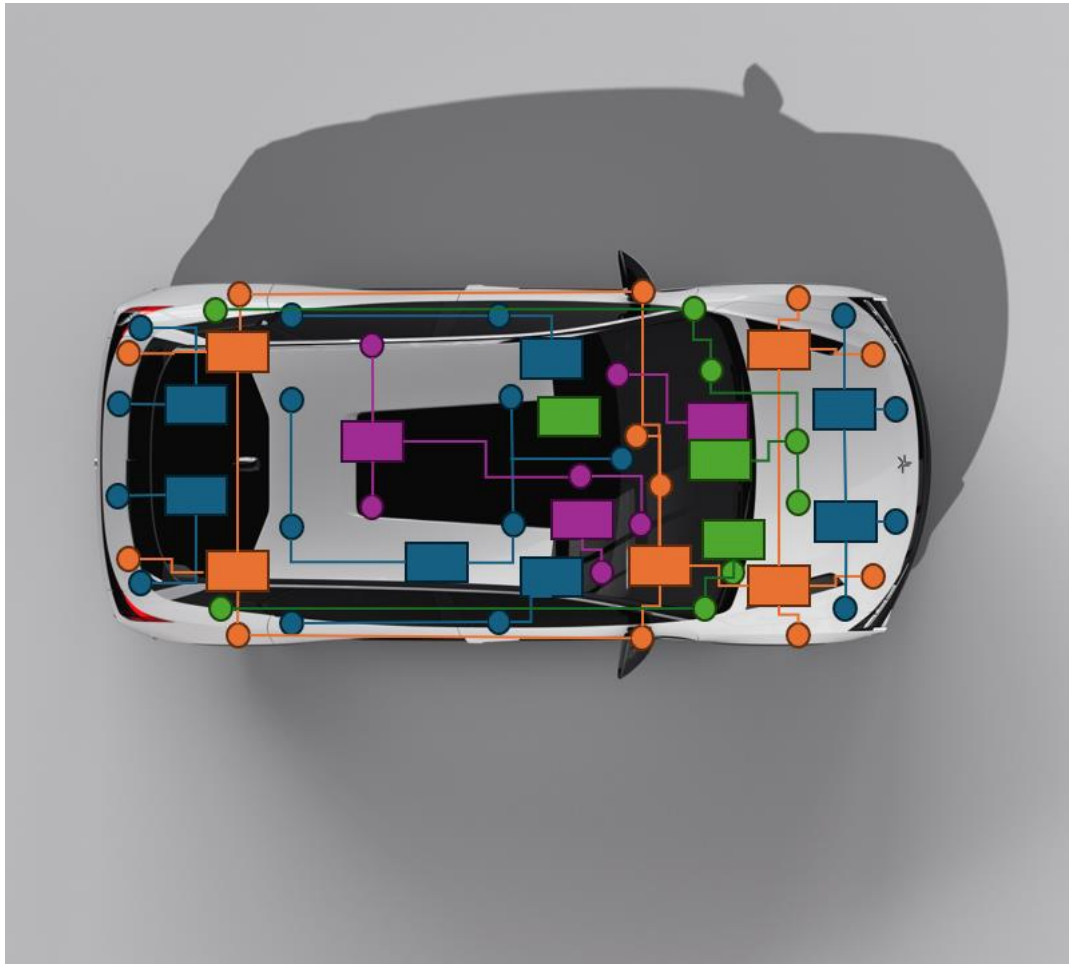
Cybersecurity Lessons Learned

From Distributed to Centralized Architecture

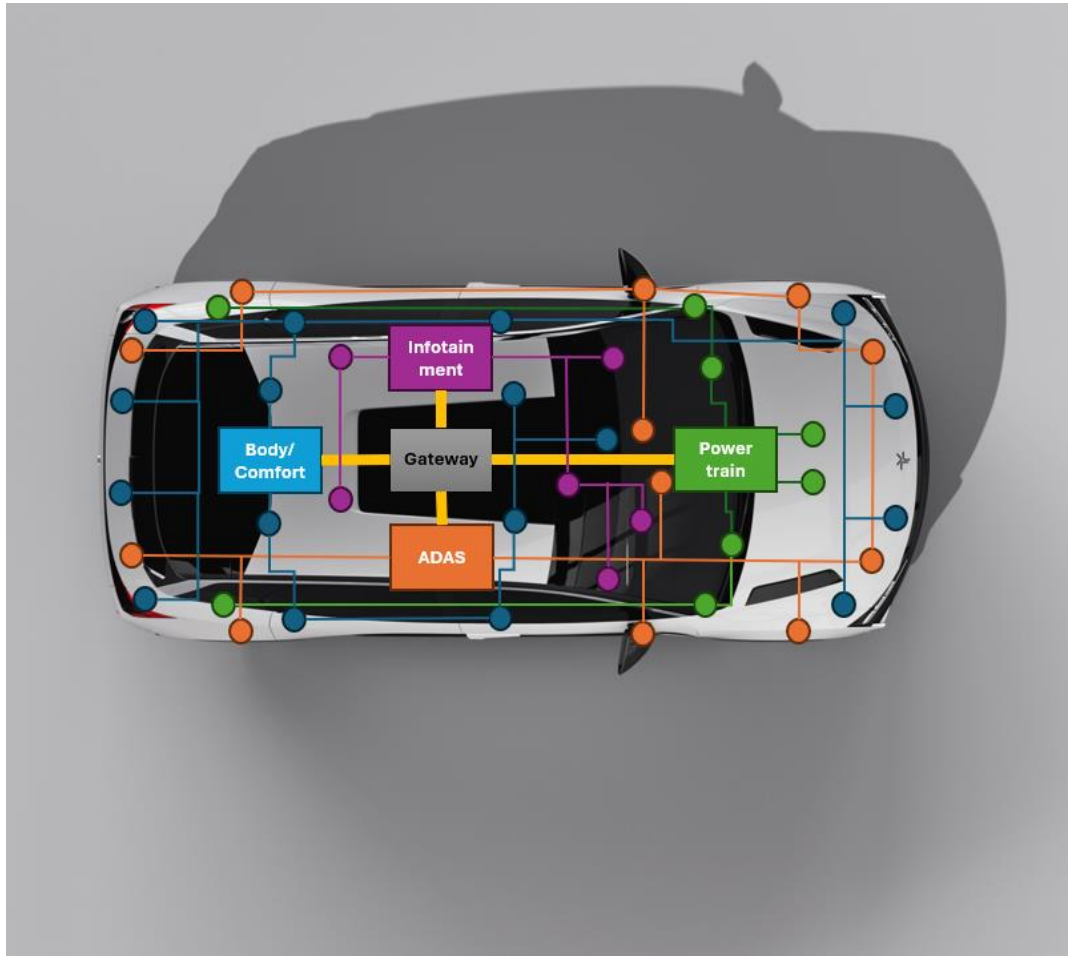
Distributed VS. Centralized Architecture

From Distributed architecture to Centralized architecture

Distributed Architecture



Centralized Architecture



How Centralization Improves Security

From Distributed Architecture to Centralized Architecture

Fewer ECUs

Minimizes the attack surface by limiting the number of potential entry points for attackers. This simplification enhances threat modeling and enables more effective centralized security controls, though it also increases the criticality of each of the ECUs

Efficient use of HSM

Allows multiple functions or domains to share cryptographic resources, reducing hardware redundancy and cost. This centralized approach also improves performance by offloading intensive cryptographic operations to a dedicated, secure environment.

Unified Security Policy

Allows consistent application of security rules (such as authentication, access control, and logging) across all vehicle functions from a central point. This reduces the risk of configuration errors, simplifies compliance, and improves overall system integrity by eliminating fragmented or conflicting security implementations

Streamlined TARA

TARA becomes more manageable due to fewer components and clearer system boundaries. This allows for faster identification of threats, more accurate mapping to assets, and reduced duplication of effort across the development lifecycle.

Simplified Key & Identity Management

Enables secure provisioning, storage, and rotation of cryptographic keys and digital identities from a single control point. Reduces complexity, minimizes the risk of misconfiguration across multiple ECUs, and streamlines compliance with security standards

Monitoring & Incident Response

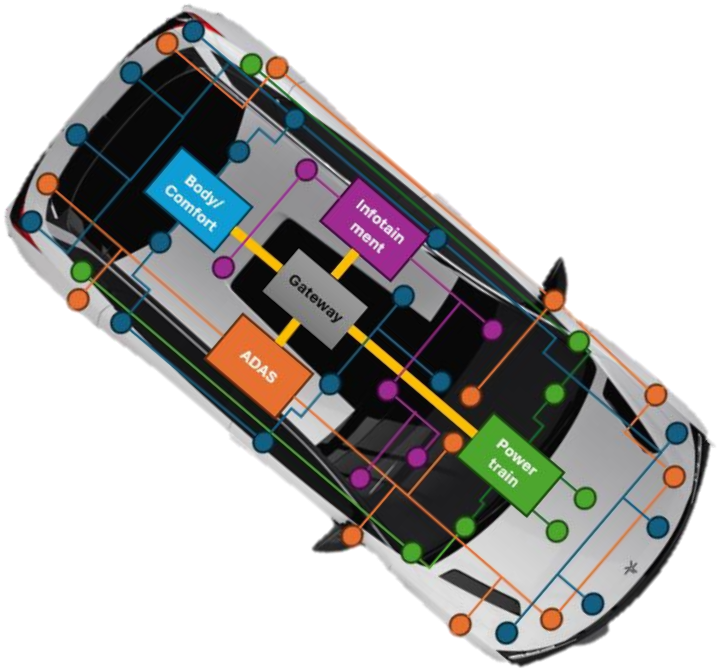
Provides a unified view of system activity, making it easier to detect anomalies and potential threats in real time. This centralized visibility enables faster, more coordinated responses to security incidents, improving overall system resilience and reducing downtime.

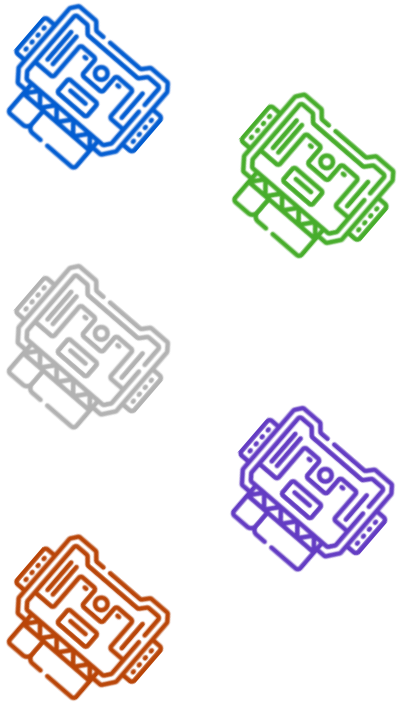
Cybersecurity at Scale

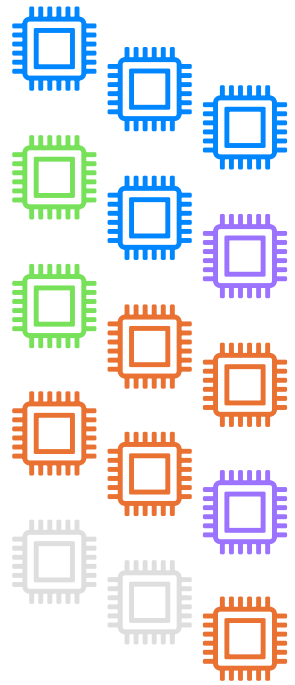
Supply chain

Cybersecurity at Scale (OEM, Tier 1, Tier 2...)

OEM (Vehicle Manufacturer) → TIER 1 (ECU Supplier) → TIER 2 (SoC and SW Suppliers)

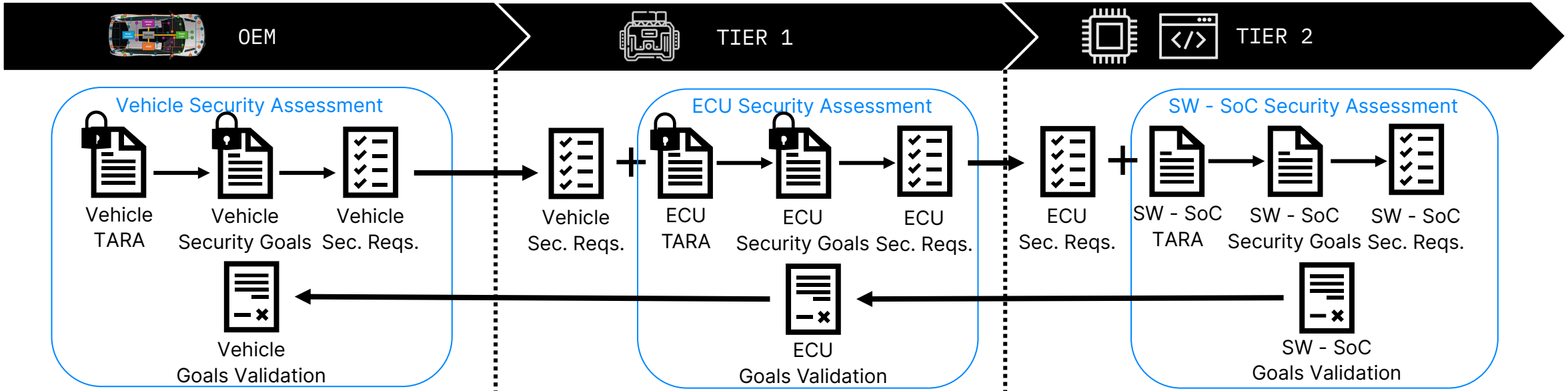






Cybersecurity Supply Chain

Cybersecurity at Scale (OEM, Tier 1, Tier 2...)



- Vehicle is the item
- TARA at vehicle level
- Sec. Reqs. transferred to suppliers
- Validation of the Vehicle Security Goals

- ECU is the item
- TARA at ECU level
- Vehicle's TARA not available
- Limited vehicular context
- Analysis based on assumptions
- Validation of the ECU Security Goals

- SoC + SW is the item
- TARA at SoC level
- Vehicle and ECU's TARA not available
- Very limited vehicular context
- Limited ECU context
- Analysis is based on assumptions
- Validation of the SoC Security Goals

Consequences of an incomplete security supply chain

Cybersecurity at Scale (OEM, Tier 1, Tier 2…)

Duplicate Efforts

- OEMs conduct vehicle-level TARA but only share filtered output or high-level requirements with suppliers.
- Tier X lacks the full vehicular context, which could lead to redundant or unaligned analysis, consuming time and resources in all the supplier chain.

Misaligned Security Controls

- Lack of visibility into the vehicle-level assumptions, the suppliers may lead to:
  - Overengineering
  - Miss critical threats
- OEMs can assume certain mitigations are handled downstream, suppliers that are unaware of it, can omit controls

Impact on System Integration

- Misaligned security goals can lead to:
  - Performance issues
  - Functional mismatches
  - Late-stage redesign

Why do OEMs not share Security Analysis?

Cybersecurity at Scale (OEM, Tier 1, Tier 2...)

Confidentiality and Intellectual Property Concerns

- TARA contains sensitive information about vehicle architecture, attack surface, vulnerabilities...
- Fear of data leak or misusage, specially if the suppliers work with multiple OEMs.

Control Over Security Architecture

- Retain control over the security posture
- Enforce top-down approach. Ensuring suppliers implement only what is requested

Trust and Maturity Gaps on suppliers

- Suppliers may lack cybersecurity maturity to handle properly customer sensitive information
- Safer to transfer only derived requirements or security controls.

Assumptions from Hardware

Hardware Security Assumptions

Security Controls

01 Trusted HW Root of Trust

- Secure Boot
- Tamper Detection
- HW Fault Tolerance

02 Secure Crypto

- Integrated HSM
- State of the art crypto accelerators
- Secure use of keys

03 Secure key storage

- HSM memory partition
- Readable only by HSM
- Isolated, protected and non-accessible.

04 Memory Protection

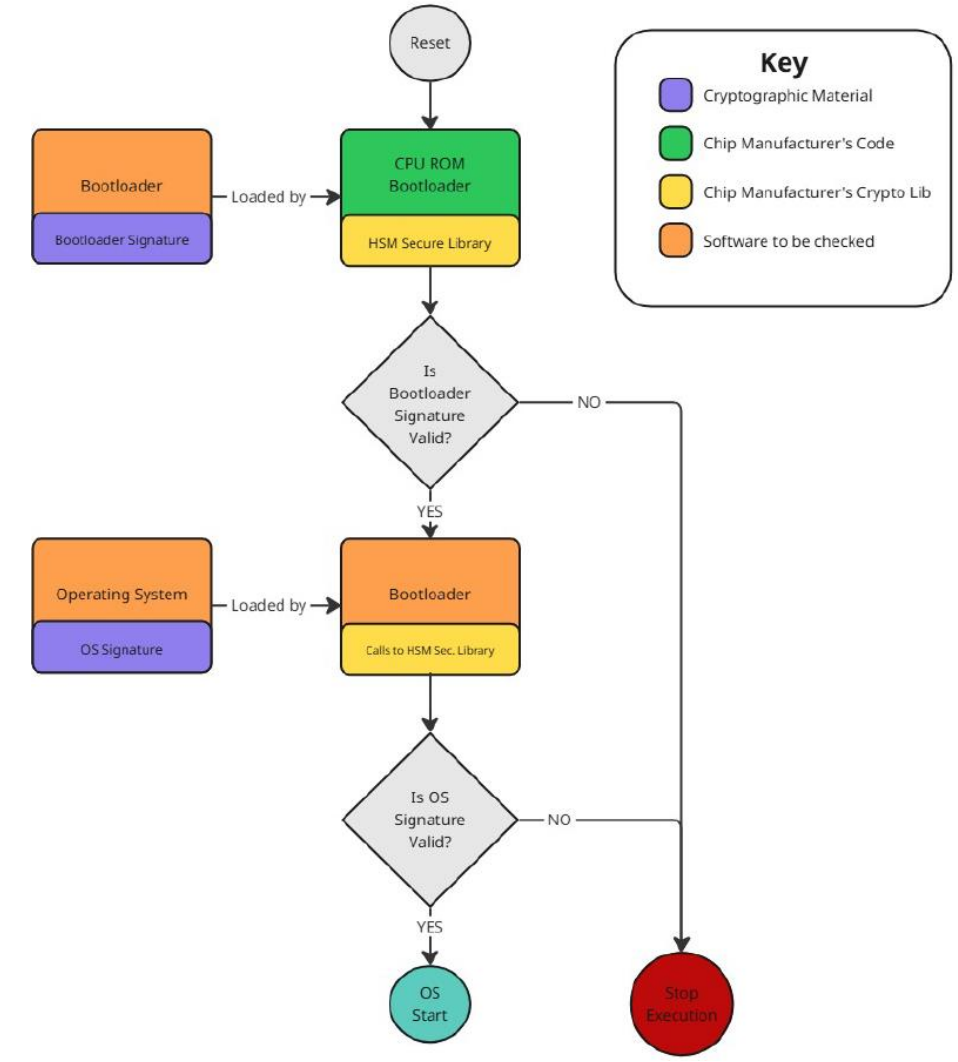
- MPU/MMU capable
- Isolation between memory regions prevents unauthorized access
- Prevents unauthorized code execution

Chain of Trust & Secure Boot

Security Controls

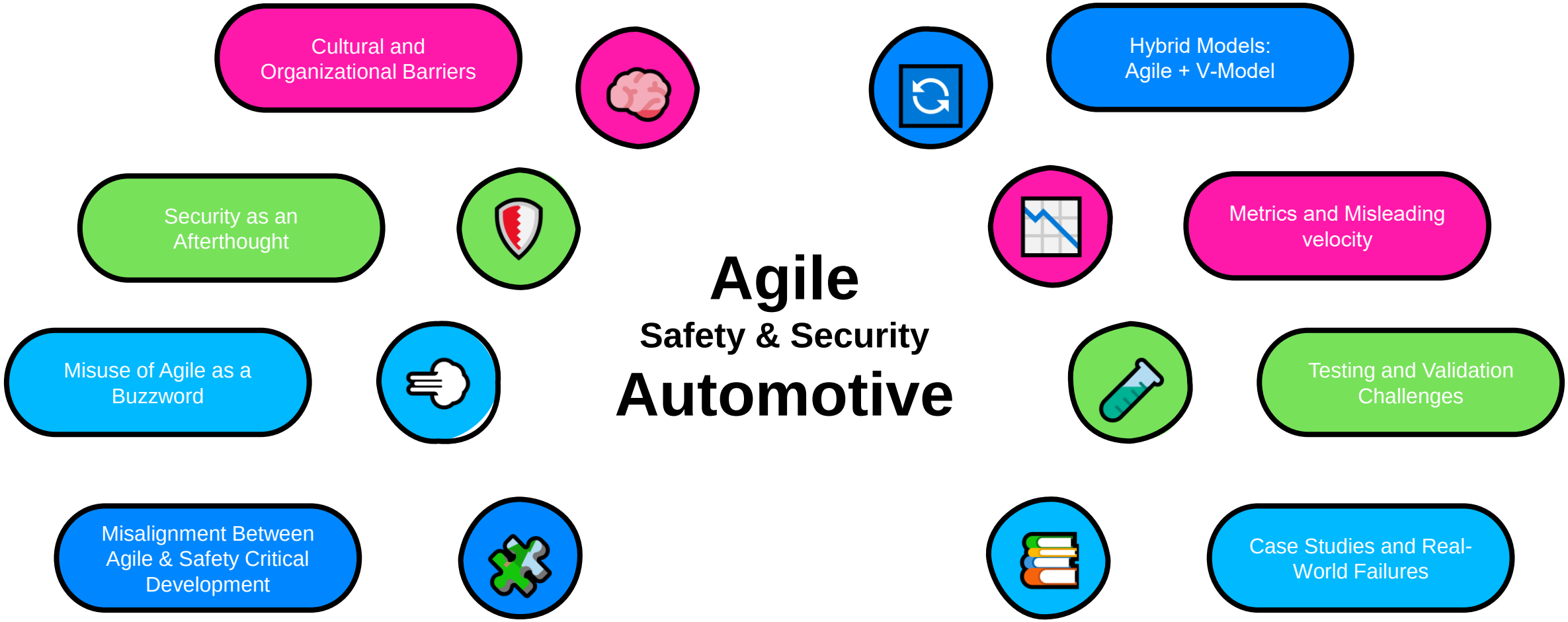
- The SW installed in every component of the HW is the intended.
- Is the foundation of the Security of the System.
- If SW tampering is detected, the system functionality is degraded.
- Increase the Boot-Up time of the System
- OEMs start-up time are very demanding
- Some customers decided to load the Bootloader and OS without signatures verification and verify them in parallel.

- When OS or BL is updated, new signatures have to be computed by the *SW Update* component, which shall replace the existing ones.
- The *SW Update* component process must be compliant with the Chain of Trust concept.



Agile & Automotive Security

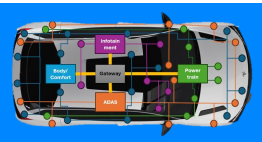
Agile & Automotive Industry
Identified Challenges



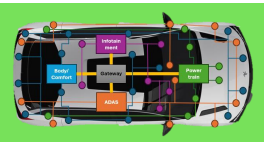
Conclusion & Takeaways

Conclusion & Takeaways

Security Engineering

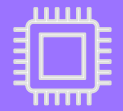


Centralized Architecture makes the attack surface smaller, simplifying the TARA vehicular analysis



Centralized Architecture makes consistent, homogenous deployment of security controls and policies

Cybersecurity Supplier Chain has room for improvement. A scaled cybersecurity framework is needed in the industry



Hardware security is the foundation—without it, everything else is fragile.

Industry is pushing for speed, but safety and security requires exhaustive analysis, testing and validation.

SW Development is fast, but safety and security validation it is not (yet).

Thank you!

Q&A

Héctor Bravo
Security Engineering Manager

tttech auto
part of NXP