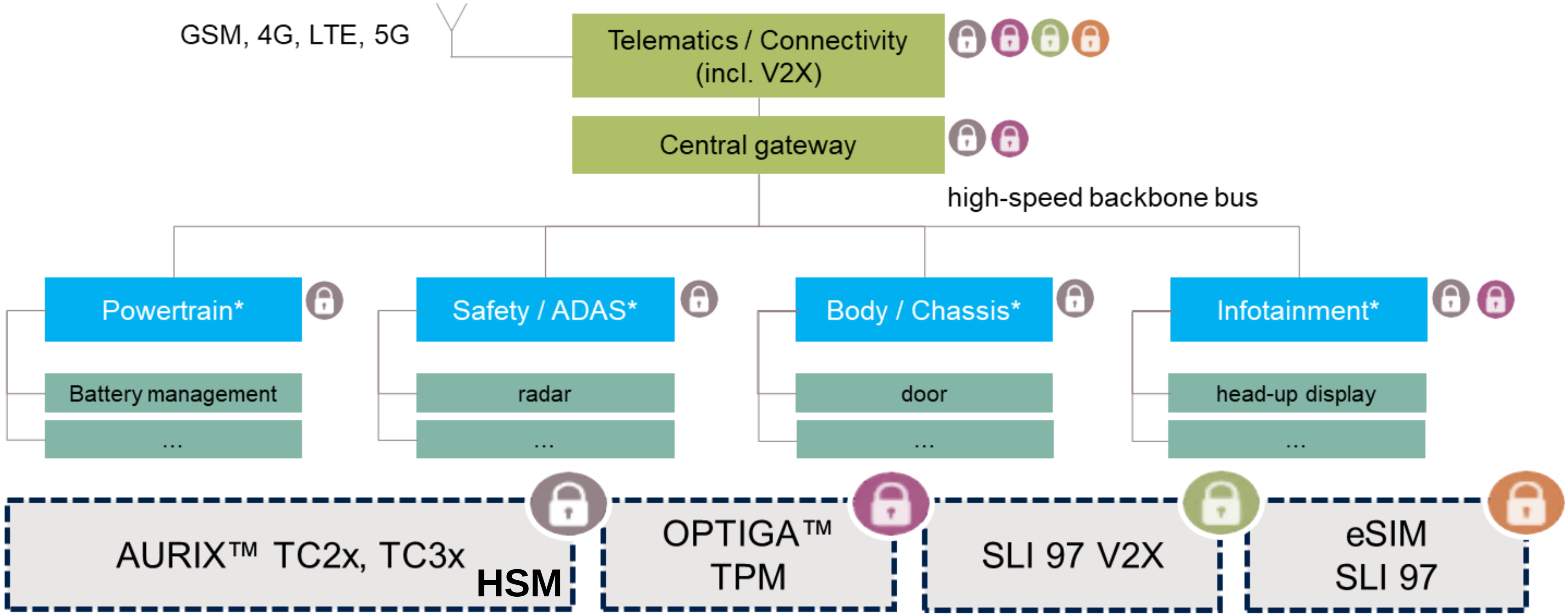
차량용 MCU의 사이버 보안 대응

Infineon Technologies Korea
17 November 2022
이경수

Contents

1. 보안 모듈이 통합 된 MCU와 외부 보안 전용 HW 칩의 비교
2. 자동차 보안 관련 활동 (MCU & System)
3. 자동차 보안 요구 사항 비교 (MCU & System)
4. MCU 보안 모듈의 변화
5. MCU의 ISO/SAE 21434 대응
6. 자동차 보안 관련 이슈 발생 시 MCU 제조사의 대응

Integrated Security & Discrete HW Security



On board security across all domains

- HW Security Module (HSM)
- Full EVITA compliant (2nd gen)
- Ethernet security features
- Unique chip individual keys
- Security SW lib (SHE+)
- ASIL-D Safety Features against fault attacks
- Automotive qualified
- Zero ppm automotive quality

Authentication, secured key store, on-chip key generation & management

- Tamper resistant hardware
- TPM2.0 SW compliant
- Initial keys and certificates
- Automotive qualified Hardware + Software certified acc. to Common Criteria

Secured V2X communication

- Tamper resistant hardware
- Crypto libraries available
- Initial keys and certificates
- Automotive qualified Hardware certified acc. to Common Criteria

Enabling cellular connectivity

- Tamper resistant hardware
- eSIM SW functionality
- Initial keys and certificates
- Automotive qualified
- Hardware certified acc. to Common Criteria

Integrated Security

Discrete Hardware Security

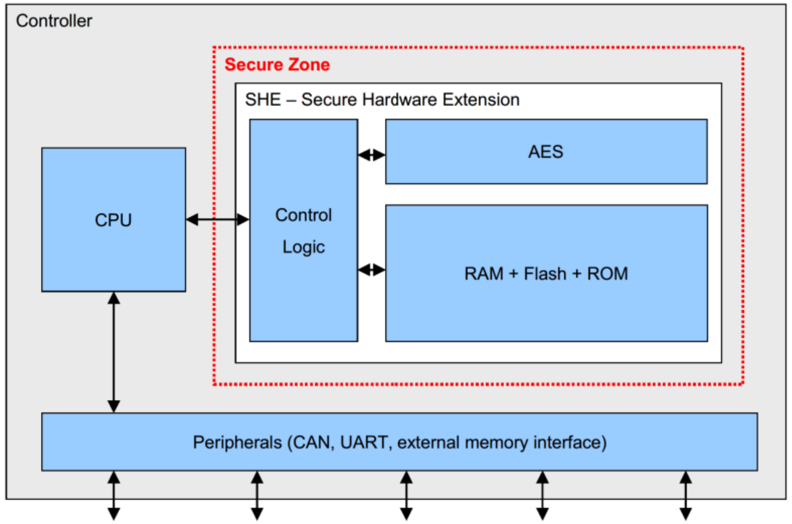
Integrated Security & Discrete Hardware Security

› Security by design
› Security certified hardware/software
  – Common Criteria (EAL4+)
  – FIPS security certification
  – TPM standard
  – ..
› Tamper resistant hardware
› On-chip key generation
› Key management
› Secure CPU & Storage
› HW Cryptographic Engines

Automotive Cyber Security Activity (defined security in MCU)

German OEMs

- ***SHE(Secure Hardware Extension)*** Functional Specification by HIS, 2009
  - The Secure Hardware Extension (SHE) is an on-chip extension to any given microcontroller.
  - It is in-tended to move the control over cryptographic keys from the software domain into the hardware do-main and therefore protect those keys from software attacks.
  - However, it is not meant to replace highly secure solutions like TPM chips or smart cards (i.e., no tamper resistance is required by the specification)

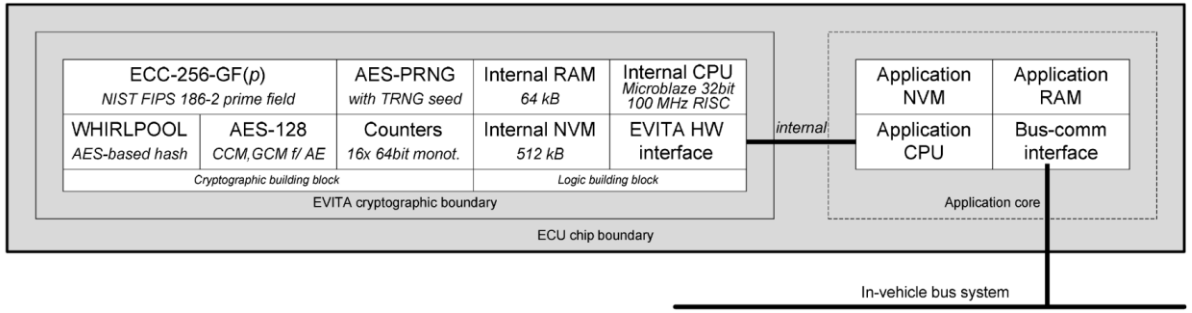


Controller
Secure Zone
SHE – Secure Hardware Extension
CPU
Control Logic
AES
RAM + Flash + ROM
Peripherals (CAN, UART, external memory interface)

< SHE – Functional Specification, Simplified logical structure of SHE >

EU OEMs, Tiers, Semiconductors

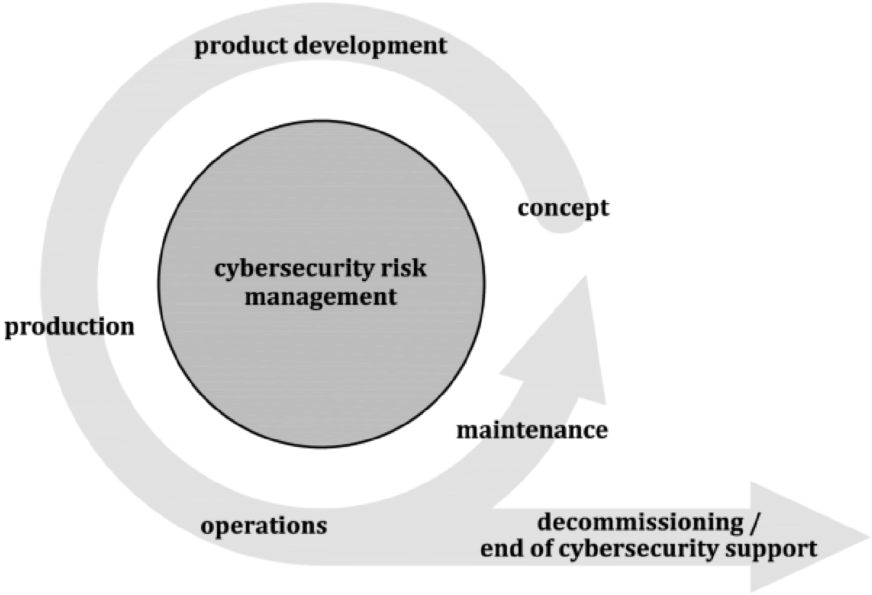
- Vehicular On-Board Security: ***EVITA*** Project, 2011
  - Providing secure platform for cryptographic functionalities that support use case
  - HSM physically separate from CPU
  - HSM in the same chip as the CPU but with a state machine and with a programmable secure core



< Vehicular On-board Security: EVITA Project, EVITA Full version >

Automotive Cyber Security Activity (defined security in E/E system)

- **ISO/SAE 21434:** Road vehicles - Cybersecurity engineering, 2021
  - Addresses the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity
  - Aims to enable the engineering of E/E systems to keep up with state-of-the-art technology and evolving attack methods
  - Requirements for cyber security risk management for road vehicles, their components and interfaces, throughout engineering, production, operation, maintenance, and decommissioning


product development
concept
cybersecurity risk management
production
maintenance
operations
decommissioning / end of cybersecurity support

< Overall cybersecurity risk management >

Security Requirements for System and MCU

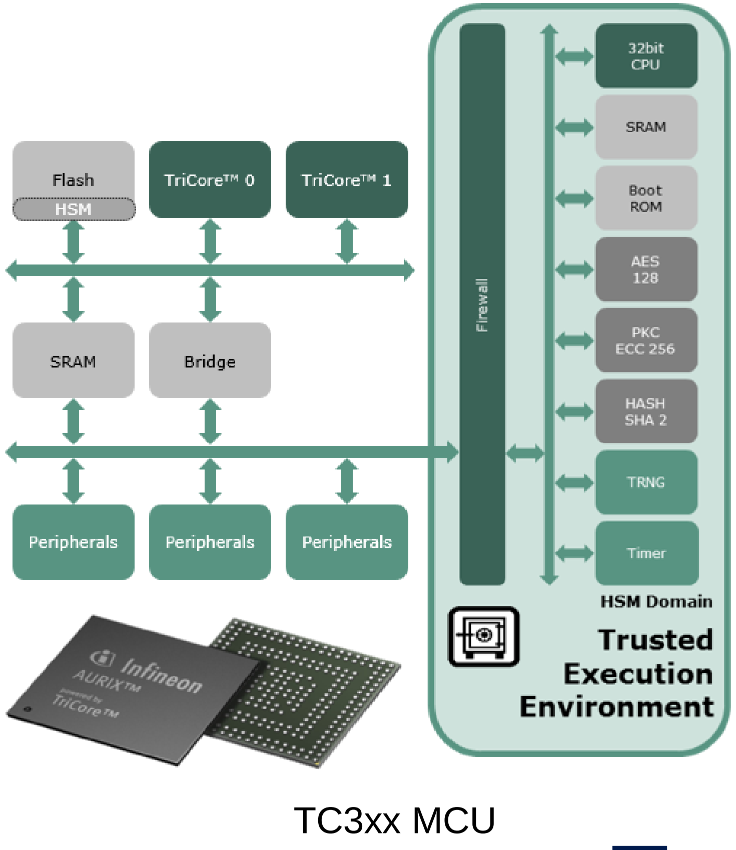
Security Requirement for System (Use cases)

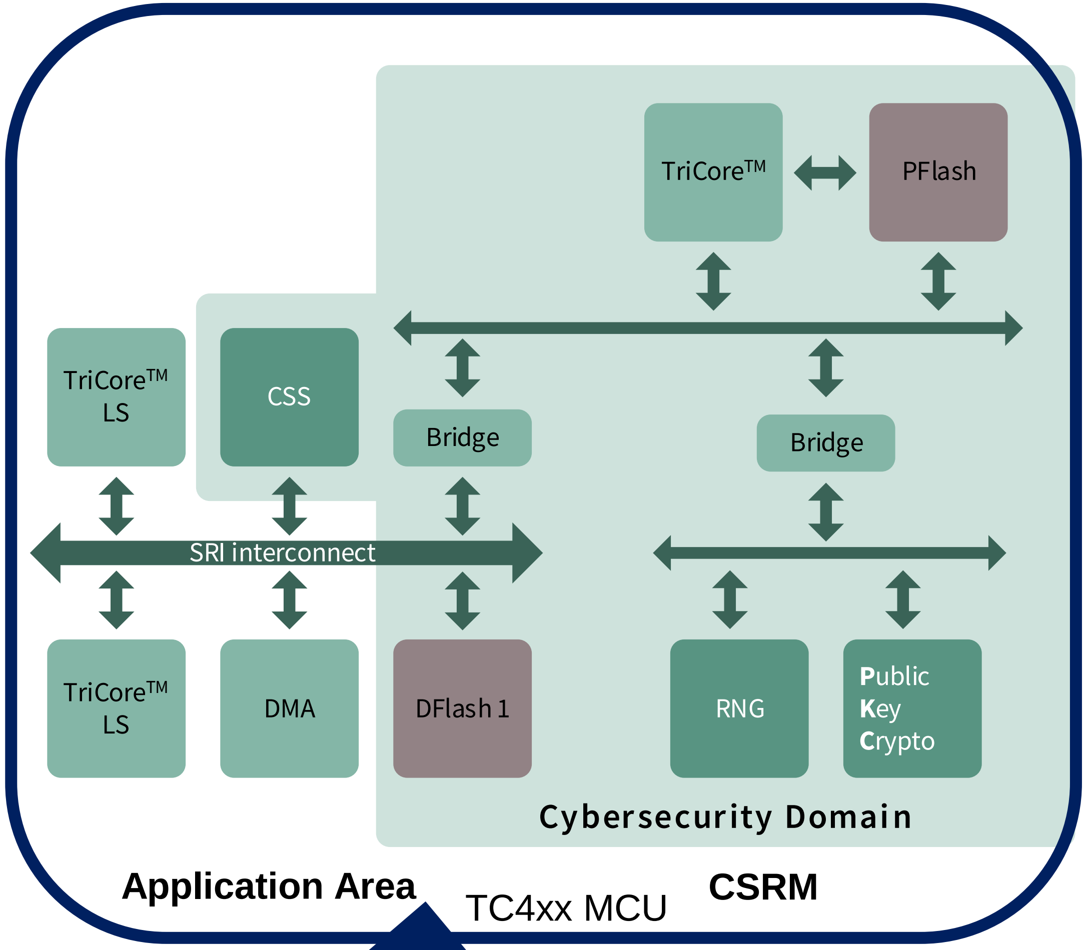
- Secure Boot
- Secure Debug
- Secure On-board communication (SecOC)
- Protected Diagnostics
- Protected software update (incl. SOTA)
- Protected key management
- Feature-activation/ -deactivation
- On-board key generation & distribution
- Component protection
- IDS (Intrusion Detection System)

Security Requirement for MCU

- Secure CPU core
- Secure Storage (Secured PFLASH/DFLASH)
- Secure Debug
- HW Cryptographic Engines (Hash, AES, ECC, RSA)
- TRNG
- SOTA (HW A&B Swap)
- Supporting security standards (e.g., ISO 21434)

Security Module and Trusted execution environment in MCU





Cyber Security Satellite (CSS)

- Parallelization of HW accelerators is service provider to application area
- Multiple HW accelerators to increase throughput, avoiding performance bottlenecks

Cyber Security Real-time Module (CSRM)

- CSRM as trusted secure HW environment
- Private PFlash within CSRM which supports individual security SW updates independent of application core

There is a compromise between high performances and security

Infineon automotive product development process follows ISO/SAE 21434 recommended practice already today

- **Security** is a mandatory **precondition** for **safety**
- Safety and security are complementary; Infineon is **market leader** in **automotive safety**
- Infineon is **global market leader for security products** for **more than 20 years**
- Infineon was the **first supplier** to join **Auto-ISAC** and among the first to join the **ISO/SAE 21434**

Process Compliance for Cyber Security Management System (CSMS)

- **Cyber Security Management** (overall and project dependent)
- **Continuous Cyber Security Activities** (e.g. monitoring, risk asse ssment, vulnerability analysis)
- **Risk Assessment Methods** (e.g. threat identification)
- **Concept Phase** (e.g. cybersecurity goals)
- **Product Development Phase** (e.g. integration and verification)
- **Post Development Phase** (e.g. cybersecurity incident response)

+

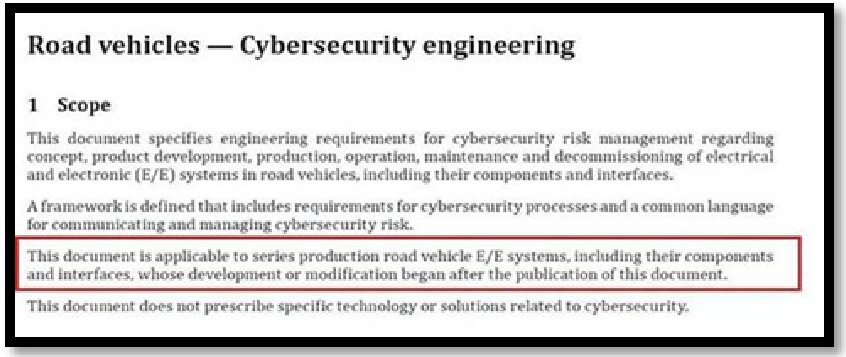
Product Compliance

All relevant future Infineon automotive product developments from 01/2022

- In **cooperation** with leading Tier1‘s and OEM‘s
  - Shared threat and attack feasibility evaluation
  - Shared damage scenario analysis
- Fully developed according **ISO/SAE 21434**
  - Incl. all **CSMS** work packages
  - Incl. software components
- Product Lifecycle Management
- Selected use-cases based on market feedback

Infineon’s **comprehensive product development process** will be certified according to **ISO/SAE 21434** by an **external audit**
Infineon’s **latest automotive product generations** will be **externally certified according to ISO/SAE 21434**

Infineon AURIX TC3xx Hardware and Software Support for ISO/SAE 21434



Road vehicles — Cybersecurity engineering

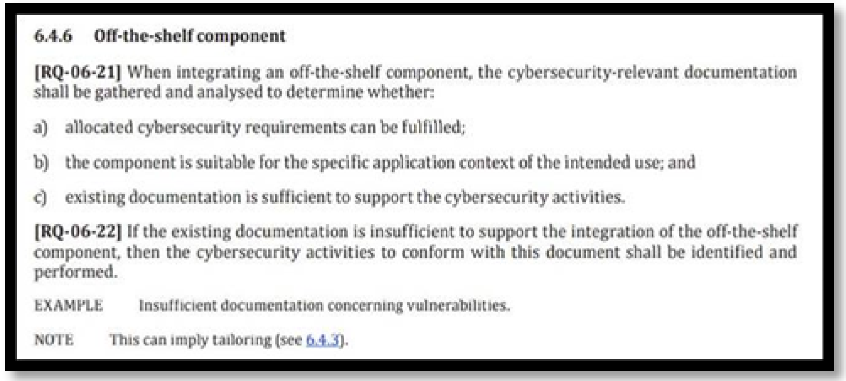
1 Scope

This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.

This document does not prescribe specific technology or solutions related to cybersecurity.



6.4.6 Off-the-shelf component

[RQ-06-21] When integrating an off-the-shelf component, the cybersecurity-relevant documentation shall be gathered and analysed to determine whether:

a) allocated cybersecurity requirements can be fulfilled;

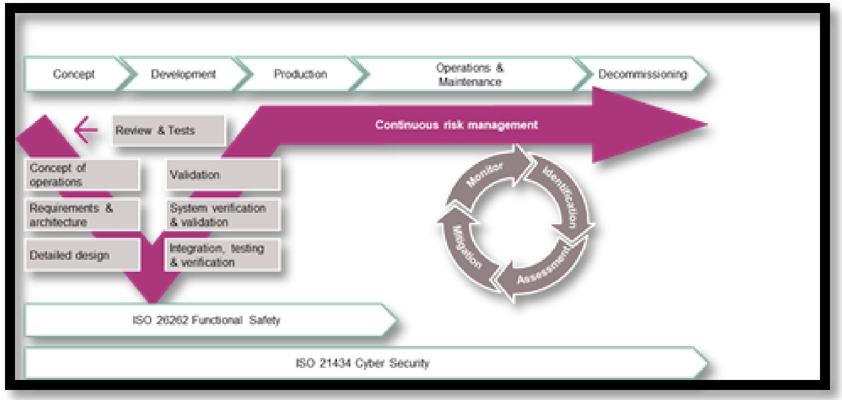
b) the component is suitable for the specific application context of the intended use; and

c) existing documentation is sufficient to support the cybersecurity activities.

[RQ-06-22] If the existing documentation is insufficient to support the integration of the off-the-shelf component, then the cybersecurity activities to conform with this document shall be identified and performed.

EXAMPLE Insufficient documentation concerning vulnerabilities.

NOTE This can imply tailoring (see 6.4.3).



- ISO21434 applicable to series production system whose development began after publication in 08/2021
- AURIX TC3xx HW and SW were developed before ISO21434

- For off-the-shelf components like TC3x HW & SW the integrator has to check if the cybersecurity requirement (for the ECU/system) can be fullfilled

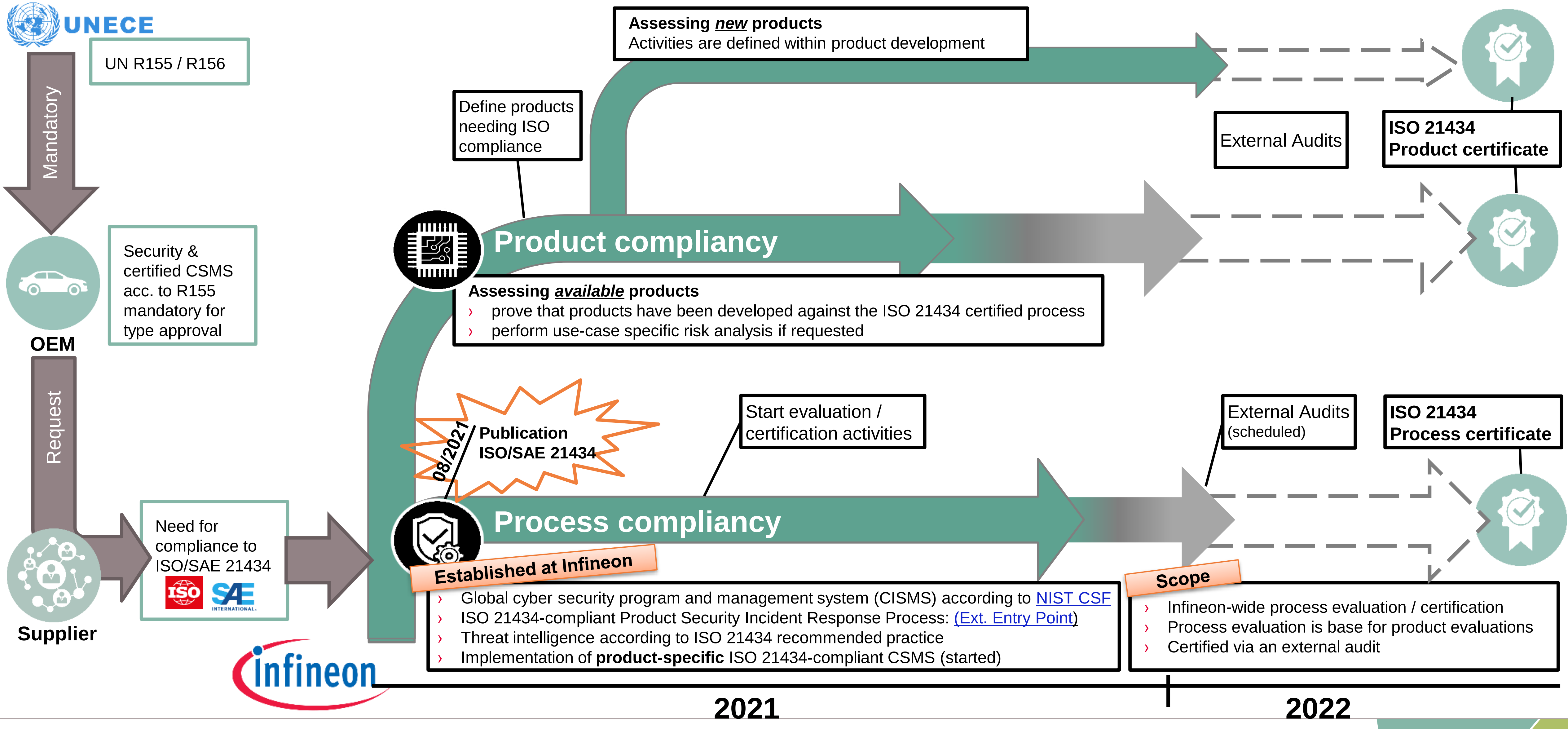
- TC4x will be developed in accordance to ISO21434 guidelines

Cyber Security Management System (CSMS) for ISO 21434 Process Compliance

ISO 21434 based Work Packages for CSMS	TC3x, T2G	TC4x
Cybersecurity Management 5. Organizational Cybersecurity Management 6. Project Dependent Cybersecurity Management	✓	✓
Continuous Cybersecurity Activities 8.3. Cybersecurity Monitoring 8.4. Cybersecurity Event Evaluation 8.5. Vulnerability Analysis	✓	✓
Risk Assessment Methods 15.3 - 15.9 Asset, Threat Scenario identification, impact rating, attack path analysis, attack feasibility rating, risk determination, and risk treatment decision	NA	✓
Concept phase 9.4. Cybersecurity Goals 9.5. Cybersecurity Concept	NA	✓
Product development Phase 10.4.1. Design 10.4.2. Integration and Verification	NA	✓
Post-development Phase 12. Production 13.3. Cybersecurity Incident Response 13.4. Updates	Cyber incident response only ✓	✓

This is due to the fact that ISO21434 was not yet standardized during product development cycle

Infineon's commitment to the ISO/SAE 21434 gives confidence to OEMs and Tier1s to adopt Infineon solutions



Security & certified CSMS acc. to R155 mandatory for type approval

Need for compliance to ISO/SAE 21434

Define products needing ISO compliance

Assessing *new* products
Activities are defined within product development

External Audits

ISO 21434 Product certificate

Assessing *available* products

- prove that products have been developed against the ISO 21434 certified process
- perform use-case specific risk analysis if requested

Publication ISO/SAE 21434

Start evaluation / certification activities

External Audits (scheduled)

ISO 21434 Process certificate

Established at Infineon

- Global cyber security program and management system (CISMS) according to NIST CSF
- ISO 21434-compliant Product Security Incident Response Process: (Ext. Entry Point)
- Threat intelligence according to ISO 21434 recommended practice
- Implementation of **product-specific** ISO 21434-compliant CSMS (started)

Scope

- Infineon-wide process evaluation / certification
- Process evaluation is base for product evaluations
- Certified via an external audit

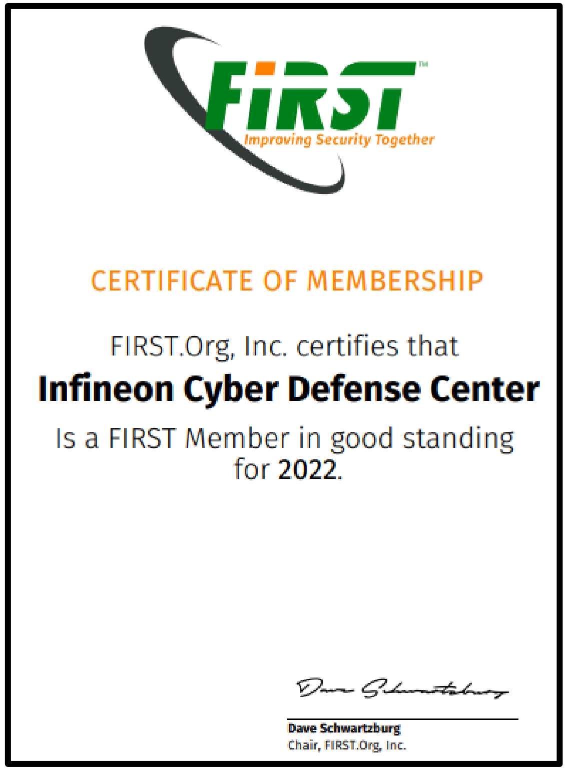
Infineon Cyber Security Program

- **Infineon Cyber Defense Center and PSIRT teams**
  - act as single point of contact for immediate response to security threats and issues affecting products, solutions, services, systems or infrastructure for Infineon Technologies and all subsidiaries globally

- **The Infineon Cyber Defense Center (CDC)**
  - is a ***dedicated team within Infineon’s Cyber Security organization, tasked to secure the Infineon infrastructure***

- **The Infineon PSIRT (Product Security Incident Response Team)**
  - is ***a team of seasoned security experts from the Infineon divisions that manages security issues related to Infineon products.*** The team acts as the central contact point for security researchers, industry groups, business partners, and other third parties to report potential product related security vulnerabilities.

- **PSIRM (Product Security Incident Response Management Process)**
  - Security vulnerability analysis, Risk assessment, Mitigation planning (validation & verification), Making security incident report



FIRST™

Improving Security Together

CERTIFICATE OF MEMBERSHIP

FIRST.Org, Inc. certifies that

Infineon Cyber Defense Center

Is a FIRST Member in good standing for 2022.

Dave Schwartzburg
Chair, FIRST.Org, Inc.

FIRST (The global Forum of Incident Response and Security Teams)
- Premier organization and recognized global leader in incident response
- Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive

Your Automotive Security Contacts

Infineon Technologies Korea
이경수
Harvey.Lee@infineon.com
010-3518-2734