AURIX^{TM} Knowledge Lab 2021

Battery management in control!

AURIX^{TM} Knowledge Lab 2021

Battery management in control!

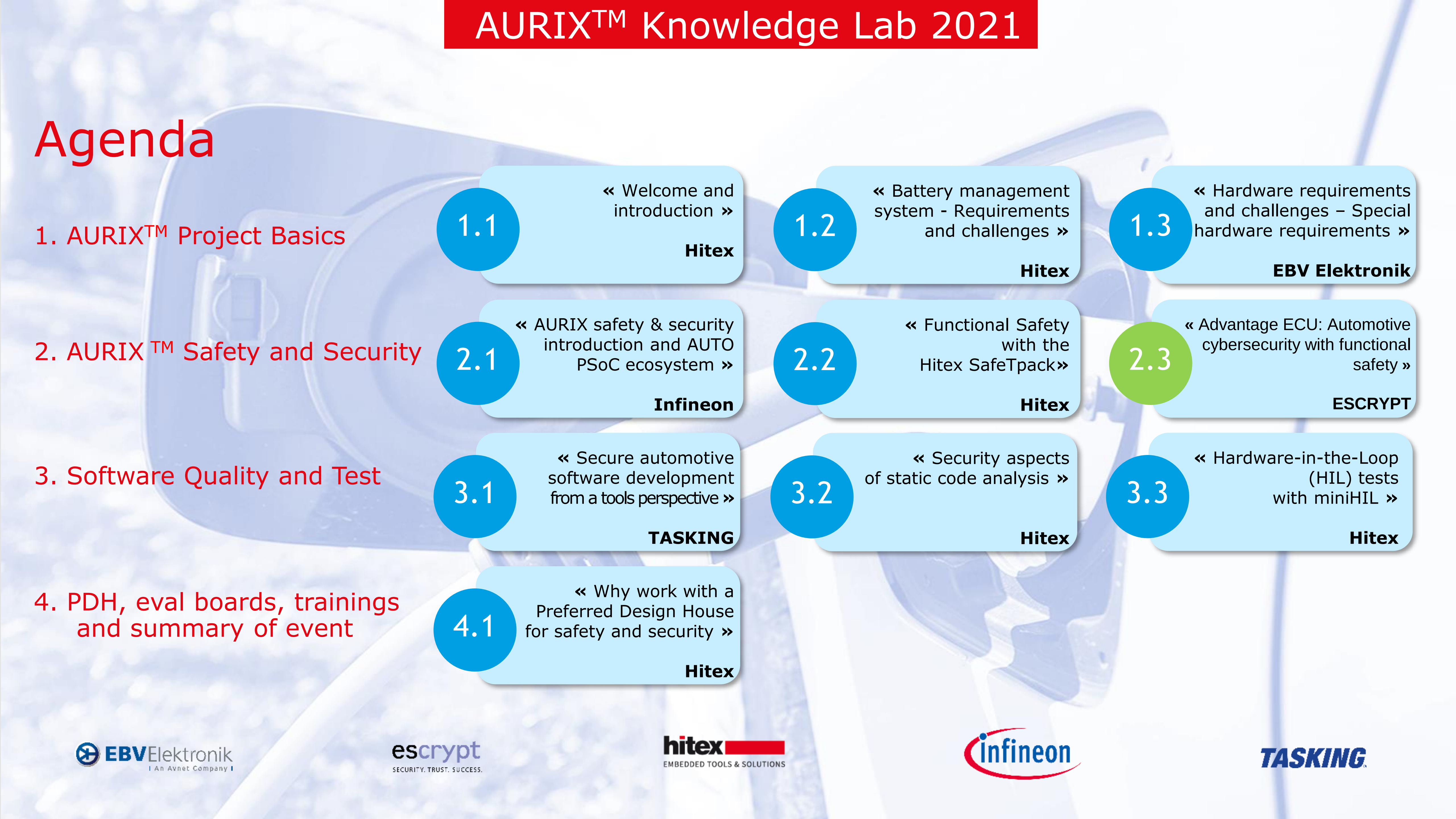
EBV Elektronik
An Avnet Company

TASKING®

escrypt
SECURITY. TRUST. SUCCESS.

Infineon

hitex
EMBEDDED TOOLS & SOLUTIONS



AURIX^{TM} Knowledge Lab 2021

Agenda

1. AURIX^{TM} Project Basics

- 1.1 « Welcome and introduction » **Hitex**
- 1.2 « Battery management system - Requirements and challenges » **Hitex**
- 1.3 « Hardware requirements and challenges – Special hardware requirements » **EBV Elektronik**

2. AURIX ^{TM} Safety and Security

- 2.1 « AURIX safety & security introduction and AUTO PSoC ecosystem » **Infineon**
- 2.2 « Functional Safety with the Hitex SafeTpack» **Hitex**
- 2.3 « Advantage ECU: Automotive cybersecurity with functional safety » **ESCRYPT**

3. Software Quality and Test

- 3.1 « Secure automotive software development from a tools perspective » **TASKING**
- 3.2 « Security aspects of static code analysis » **Hitex**
- 3.3 « Hardware-in-the-Loop (HIL) tests with miniHIL » **Hitex**

4. PDH, eval boards, trainings and summary of event

- 4.1 « Why work with a Preferred Design House for safety and security » **Hitex**

EBVElektronik | An Avnet Company |

escrypt SECURITY. TRUST. SUCCESS.

hitex EMBEDDED TOOLS & SOLUTIONS

infineon

TASKING

Advantage ECU: Automotive Cybersecurity with Functional Safety

escrypt

SECURITY. TRUST. SUCCESS.

ESCRYPT: The right partner for you - Today and in the future

Solution Portfolio

Design security

Consulting, engineering, testing, and training

- Security consulting
- Security engineering
- Security testing
- Security training
- Product security organization framework (PROOF)

Enable security

Products and solutions

- Defense-in-depth vehicle protection
  - CycurHSM
  - CycurTLS
  - CycurLIB
- Secure V2X communication
  - CycurV2X-SDK
  - CycurV2X-PKI
- Intrusion detection & prevention solution (IDPS)
  - CycurIDS
  - CycurIDS-M / CycurIDS-R
  - CycurGATE
  - CycurGUARD

Manage security

Operation, monitoring and incident & response

- Managed PKI service
- Vehicle security operations center (VSOC)
- Threat intelligence and forensics
- Incident response service
- Vulnerability management

Complex product & supply chain

New E/E architecture & technologies

Emerging regulations

Mitigation duration & complexity

Long vehicle lifespan

Impact on safety

Scalability to millions of end points

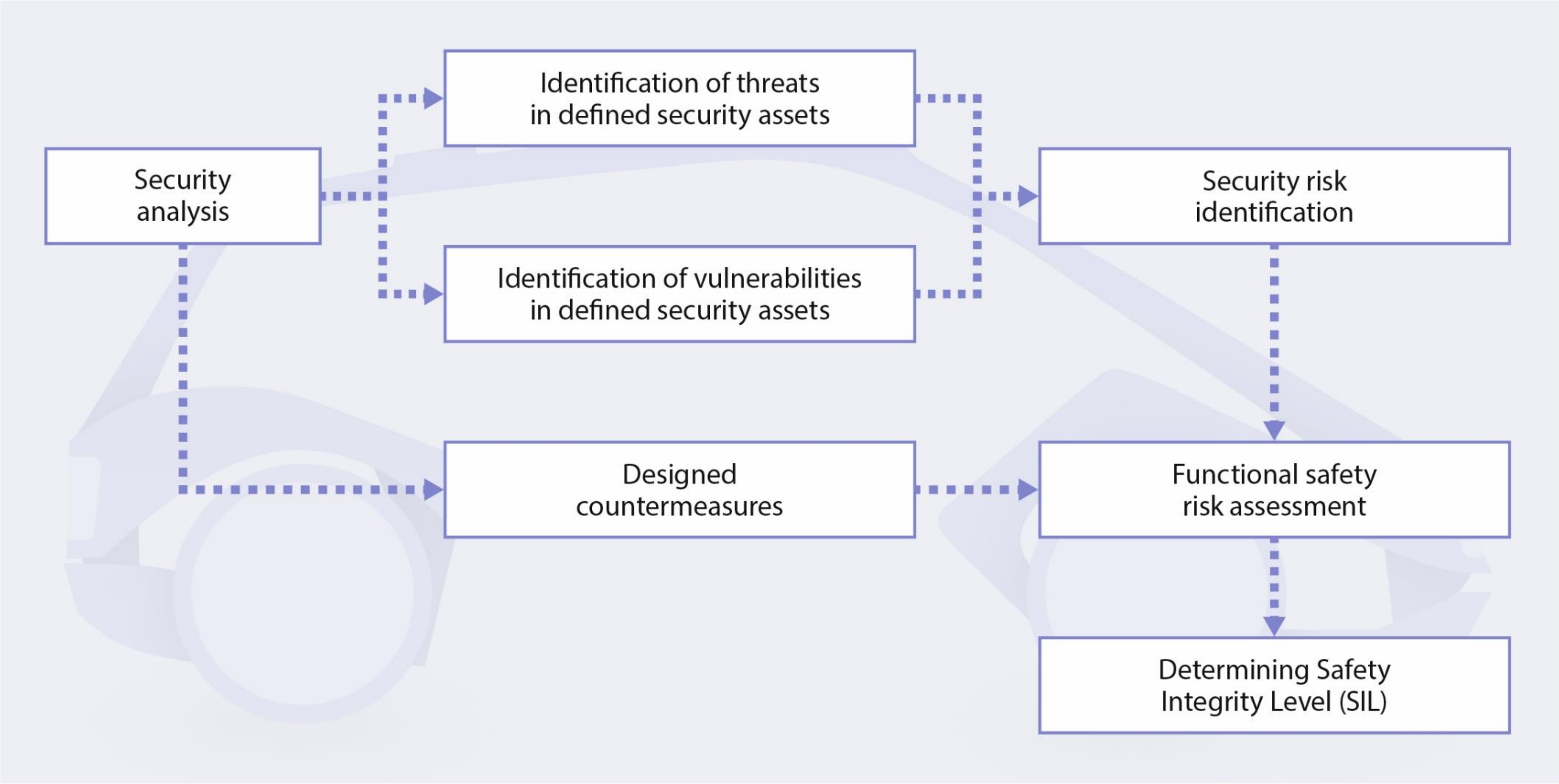
Integrating Functional Safety with Cyber Security Analysis

Introduction

- Safety and security goals are the input to derive functional safety and security requirements
- In the safety area, methods to derive technical requirements and analyze the system architecture include Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA)
- In the security area, some methods to identify threats and vulnerabilities include:
  - Deriving risk models according to NIST Special Publication 800-30
  - Security Vulnerability Analysis (SVA)
  - Threat Assessment and Remediation Analysis (TARA)
- Thorough security analysis required to identify threats and vulnerabilities in the system
- Requirements for safety functions are determined taking into account results of hazards identification
  - Safety integrity requirements result from analysis of potential hazardous events

Integrating Functional Safety with Cyber Security Analysis

Method


Security analysis
Identification of threats in defined security assets
Identification of vulnerabilities in defined security assets
Security risk identification
Designed countermeasures
Functional safety risk assessment
Determining Safety Integrity Level (SIL)

Trends and Challenges

Holistic security solution: defense-in-depth approach

Vehicles must be secured (and modern vehicles more than ever before)

Secured physical access
- Lock and unlock doors
- Start driving

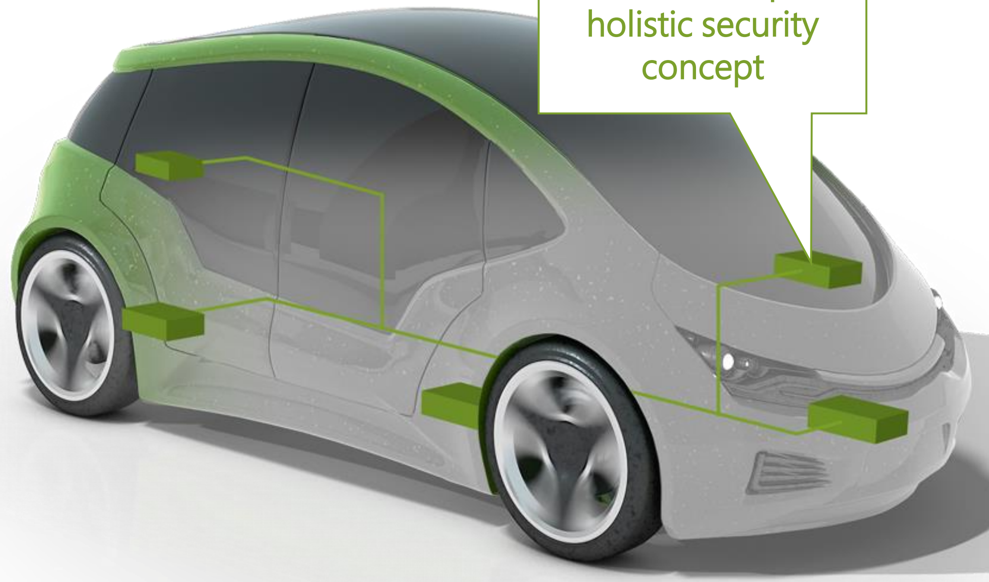
Secured external interfaces
- Diagnosis interface
- Vehicle to power grid
- Vehicle to vehicle
- Vehicle to cloud (SW update, entertainment, private data)
- Vehicle to road signals

Secured internal interfaces
- Isolation of domains
- Sensor to control unit
- Control unit to actor
- Control Unit to dashboard
- Gateway to control unit (SW update, ..)

Trends and Challenges

Holistic security solution: defense-in-depth approach

ECU‘s must be secured



Secure Access

- Ensure that no unauthorized person can download / upload / debug software or data

Secure Operation

- Ensure that no malicious software is executed (Run Time Maniplulation Detection)

Secure Startup (boot)

- Ensure that no malicious software is started

Hardware security modules are the nucleus to build complex holistic security concept

Secure Software Update

- Ensure that no malicious software is programmed into the ECU

Secure Communication

- Ensure authenticity and integrity of data received

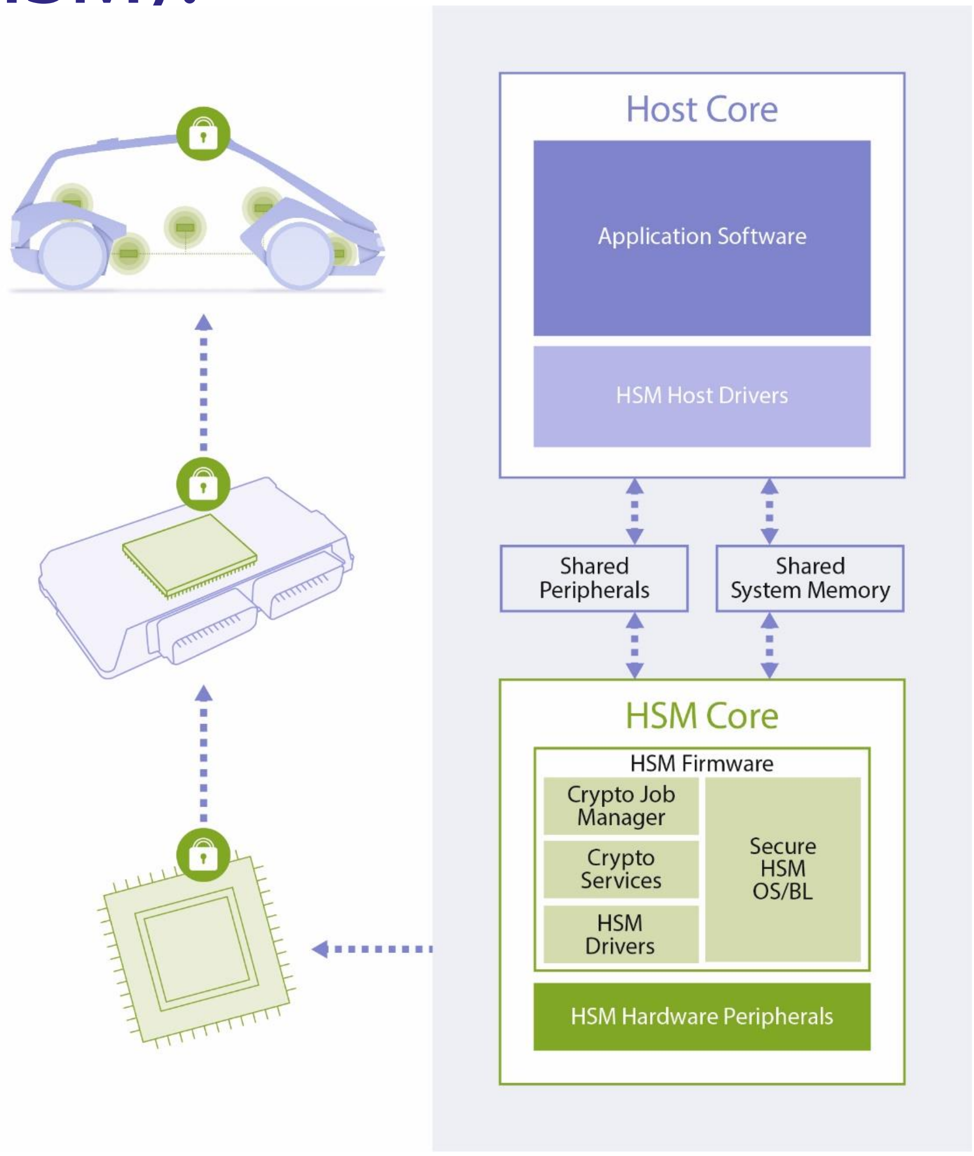
Secure Production

- Ensure that secure data (key, certificates) cannot be accessed by a malicious person

What is a Hardware Security Module (HSM)?

The Nucleus of Automotive Security

- Dedicated HW component based on EVITA architecture on target (Microcontroller/SoC) for the purpose of embedded security
- Isolated from host, has own processor, HW cryptographic functions and dedicated memory
- Ensures confidentiality, integrity and authenticity of in-vehicle software and data
- HSM firmware adds additional security functions to the hardware
  - Security functions bundled into complex security protocols to support dedicated OEM use cases
  - Pre-emptive real-time operating system ensures optimized, priority-driven resource utilization (Also in multi-core context)
- HSM functions are made available to the host application via an API interface
- HSM core and software form the trust anchor for the vehicle systems.



Host Core

Application Software

HSM Host Drivers

Shared Peripherals

Shared System Memory

HSM Core

HSM Firmware

Crypto Job Manager

Crypto Services

HSM Drivers

Secure HSM OS/BL

HSM Hardware Peripherals

Use Case 1:

Freedom of interference

Use case:

- HSM used within integrated vehicle ECU environment
- Co-existence of HSM with software solutions performing safety-relevant functions with assigned safety goals up to ASIL D

Safety goal:

- Achieve freedom from interference according to ISO 26262

Approach #1:

- Domain separation using HW functions on the chip (e.g. Memory Protection Units, dedicated protection mechanisms)

Why is this approach ineffective?

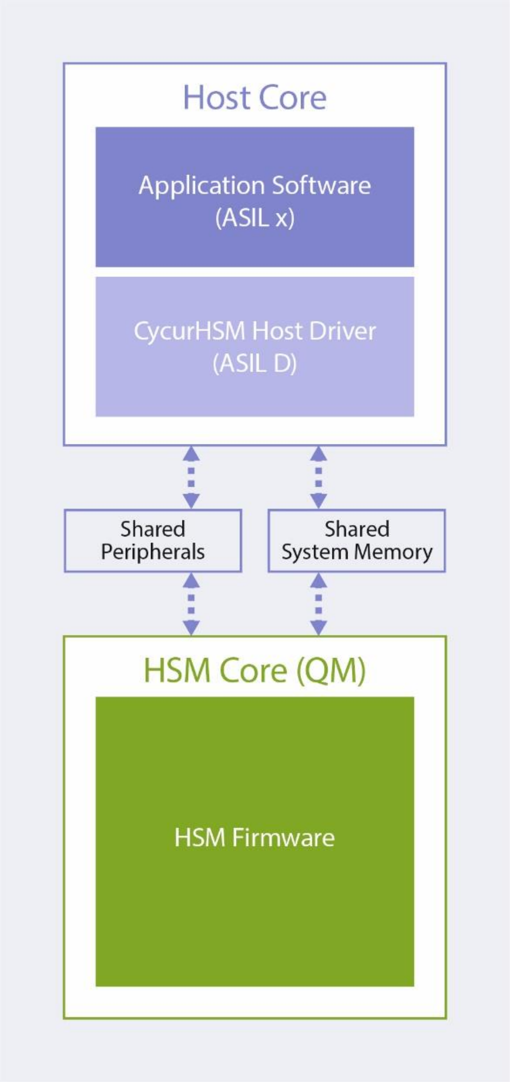
- Context switching required between two separated, protected domains
- Performance degradation
- Potential interference with other runtime requirements
- Not ideal option for low-cost devices

Use Case 1:

Freedom of interference

✓ Solution:

- Qualified HSM firmware includes host driver developed according to ASIL requirements
  - Allows easy integration into vehicle ECU
  - Reliably prevent interference between the HSM and the host core with its safety-relevant functions
  - No partitioning or memory protection required
- HSM designed as Safety Element out of Context per ISO26262



Use Case 2:

Safe CMAC

Use case: Faults in cybersecurity mechanisms have a safety-critical impact

- On-board communication messages and signals exchanged between ECUs are safety-relevant.
- Message corrupted but nevertheless forwarded, leading to hazardous situations

Approach #1:

- On-board communication messages and signals exchanged between ECUs are safety-relevant.
- AUTOSAR specifies End-to-End (E2E) protection for exchanging safety-relevant data
- The E2E concept detects and handles faults on both the hardware and software side in the communication network during runtime
- Concept adequate for safety-compliant communication up to ASIL D

Alternative:

- Safe CMAC, which secures safety-critical messages using a Cipher-based Message Authentication Code (CMAC)

Use Case 2:

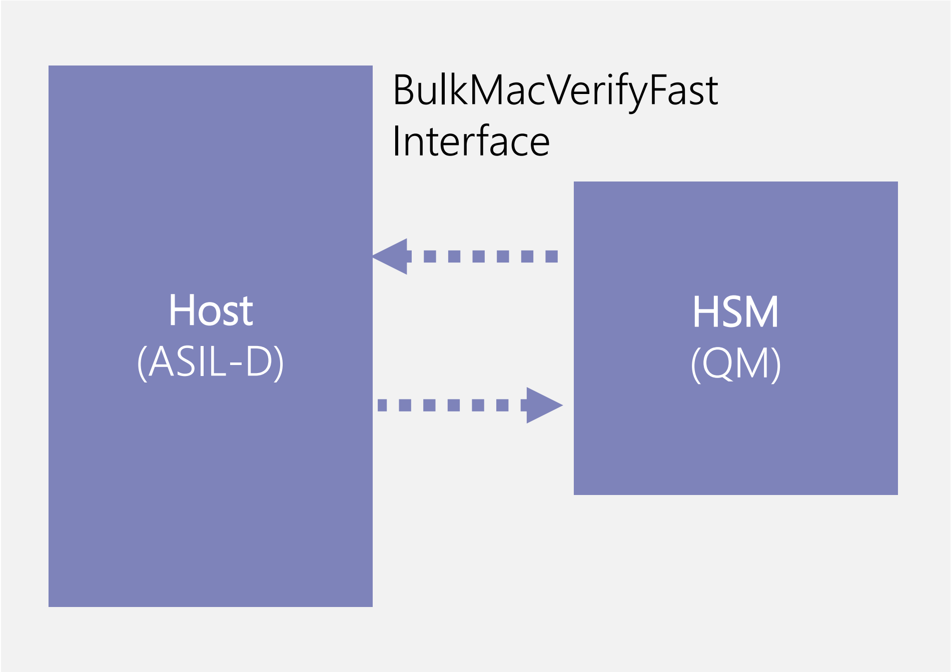
Safe CMAC

Challenge:

- Customers need an ASIL-D qualified CMAC Verification
- Method to complement AUTOSAR E2E while avoiding the overhead caused
- Requirement to avoid forwarding non-authentic messages
- HOST is ASIL D while HSM is QM Element
- HSM trustworthy for Security, HOST for Safety

Safety Goals:

- No false MAC shall be verified valid
- Freedom from interference

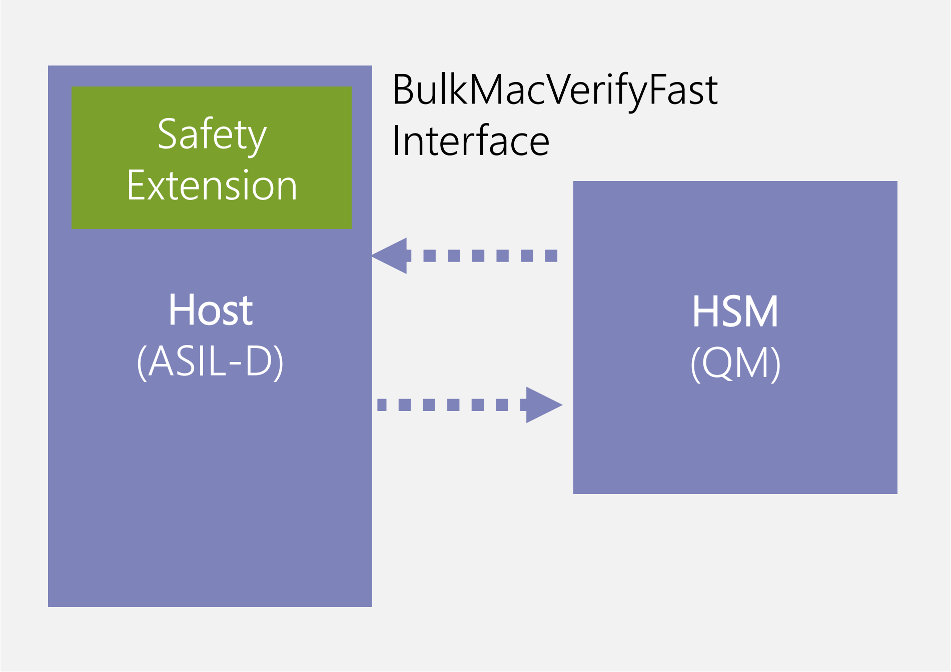


Use Case 2

Safe CMAC

✓ Solution:

- Every message in the in-vehicle network usually includes a CMAC that is routed to the HSM to validate the authenticity of the message
- Extend the existing Interface with a new safety API
- Verification takes place on HOST and HSM side
- HSM not aware of the CMAC of a message
- HSM generates the CMAC of the message for verification purpose



Thank you

ESCRYPT GmbH
Headquarters

Wittener Straße 45
44789 Bochum
Germany

Phone: +49 234 43870-200

info@escrypt.com
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.