escrypt
Embedded Security by ETAS

The challenge for embedded system in Automotive industry and BOSCH’s count measure

ESCRYPT – Embedded Security

Company Profile

escrypt
Embedded Security by ETAS

ESCRYPT GmbH

Foundation:	2004
Shareholder:	100% ETAS GmbH
Headquarter:	Bochum, Germany
Turnover 2014:	5.800 k €
Employees:	100 security experts world-wide
Management:	Martin Ridder, Dr. Thomas Wollinger

Europe

Locations
Germany (Berlin, Bochum, Munich, Stuttgart, Wolfsburg), UK (York), Sweden (Lund)

Asia-Pacific

Locations
China (Shanghai), Japan (Yokohama), Korea (Seoul), Indian (Bangalore)

America

Location
USA (Ann Arbor), Canada(Waterloo)

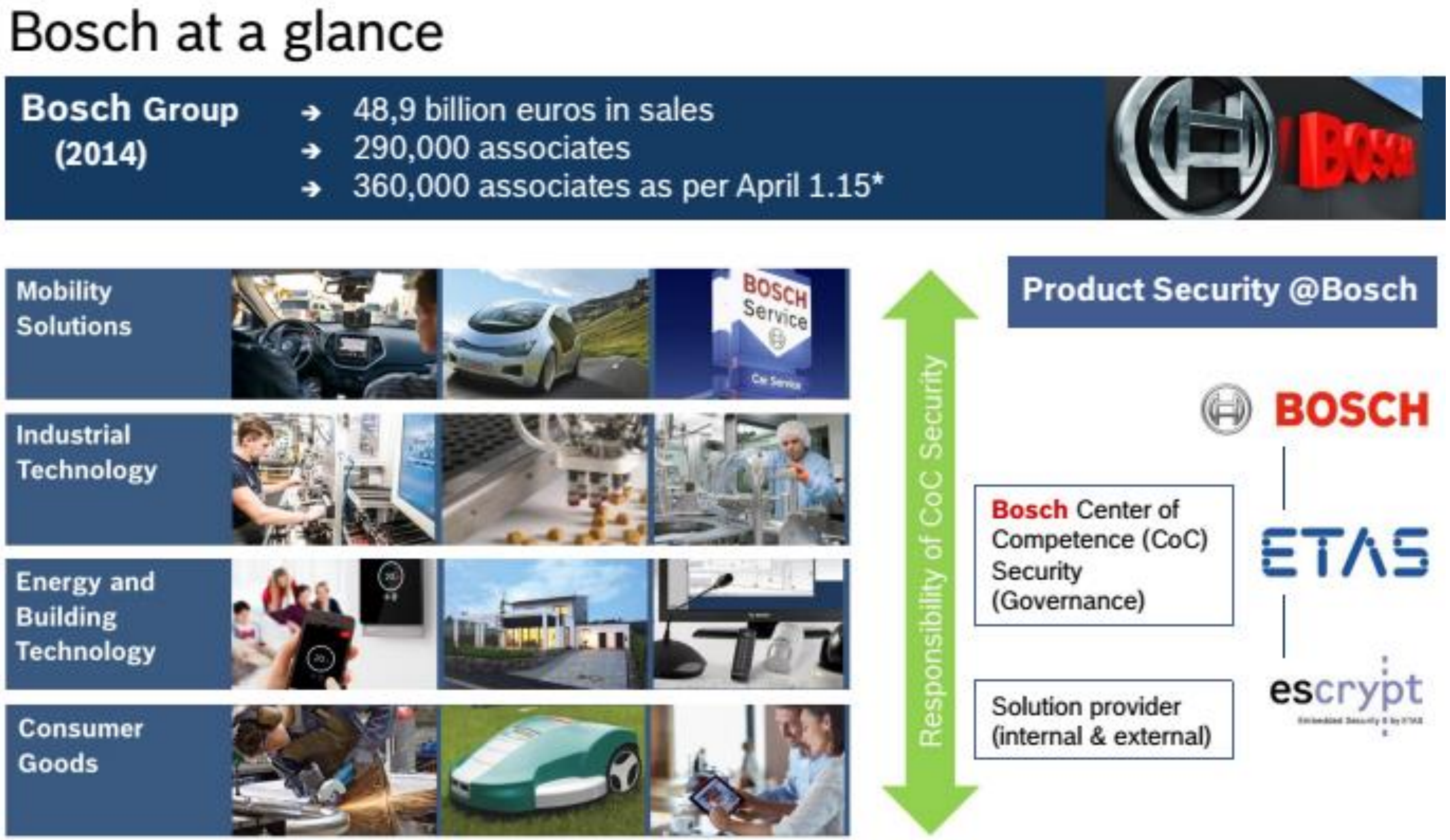
Portfolio

ESCRYPT provides a variety of products and services suited to protect devices and applications, to secure the back-end infrastructure, and to protect business models.

ESCRYPT's products are applicable to all industries with a need for embedded security.

- ✓ **Security consulting and services**
- ✓ **Security products**
- ✓ **Customized security solutions**
- ✓ **Supporting Infrastructures**

ESCRYPT – Executive Summary



Bosch at a glance

Bosch Group (2014)

- ➔ 48,9 billion euros in sales
- ➔ 290,000 associates
- ➔ 360,000 associates as per April 1.15*

Mobility Solutions

Industrial Technology

Energy and Building Technology

Consumer Goods

Responsibility of CoC Security

Product Security @Bosch

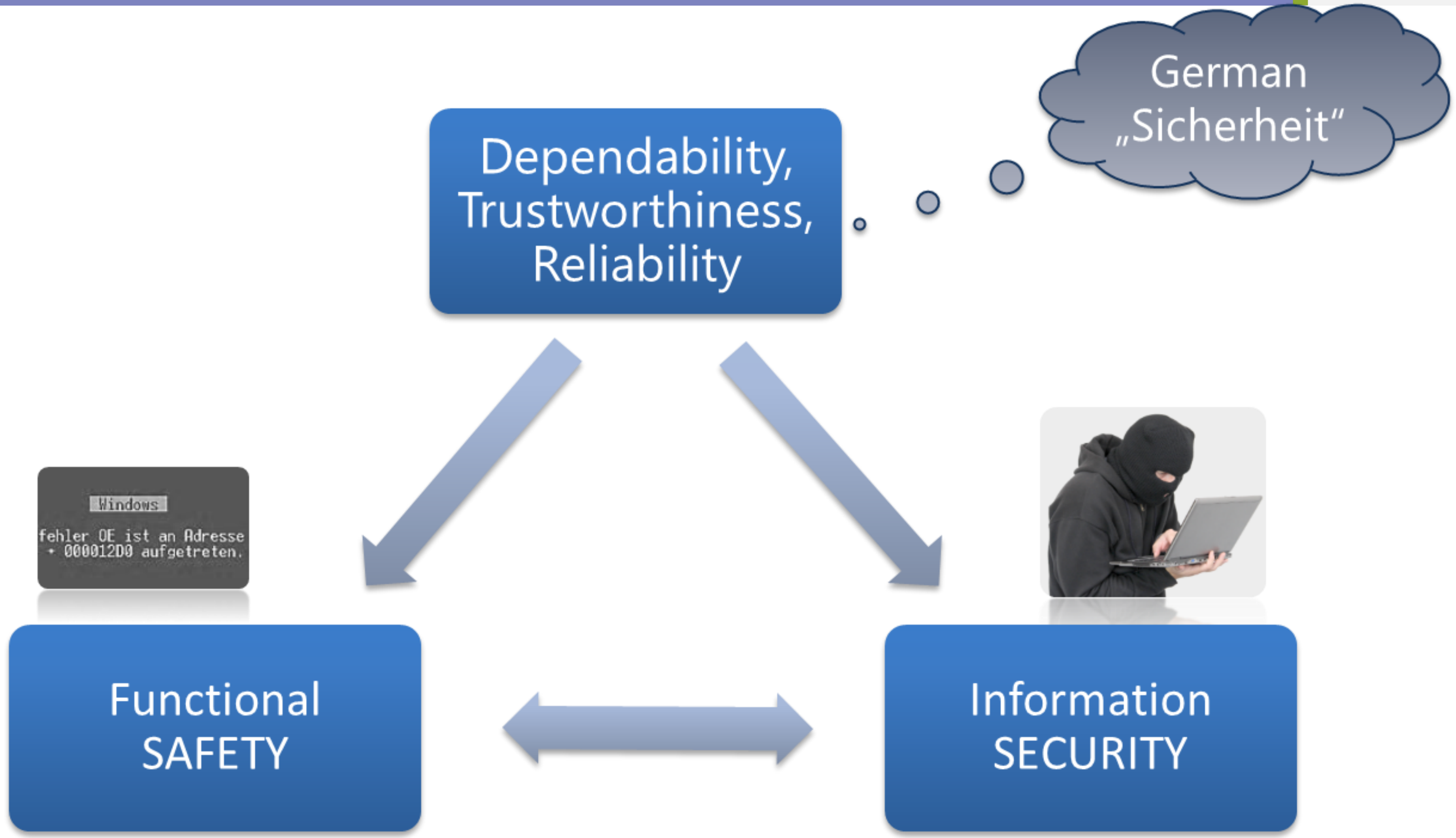
Bosch Center of Competence (CoC) Security (Governance)

Solution provider (internal & external)

BOSCH Service
Car Service
BOSCH
ETAS
escrypt

Automotive Security Solution

Security Analyses & Evaluation Scope



***Accident prevention**, i.e., protection against random failures (e.g., overvoltage) not caused by any (external) systematic forces/entities*

***Attack prevention**, i.e., protection against systematic (malicious) encroachments and manipulations (e.g., malware, hacker)*

ESCRYPT – Executive Summary

Internal: Bosch Center of Competence Security (Supported by ESCRYPT)

Mission:

The Center of Competence is responsible for the Governance function for Product Security within Bosch. It holds the core competence in security, technical data protection and cryptography. It is the guardian for Product Security.

Activities:

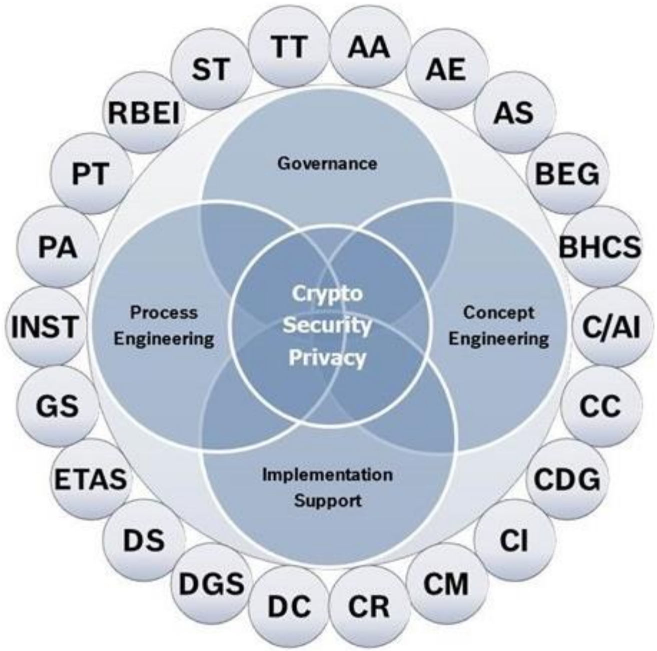
The CoC governance function for product security includes:

- Integration of security into Bosch development processes
- Security standardization support
- Security activities of cross-divisional interest
- Compilation of training material
- Maintenance of a Bosch-wide security knowledge base
- Being first contact in security-related issues

Service:

Beyond its governance function, the CoC Security provides security services to product divisions to fulfil their security requirements.

CoC Security - Participating Bosch Units



ESCRYPT – Executive Summary

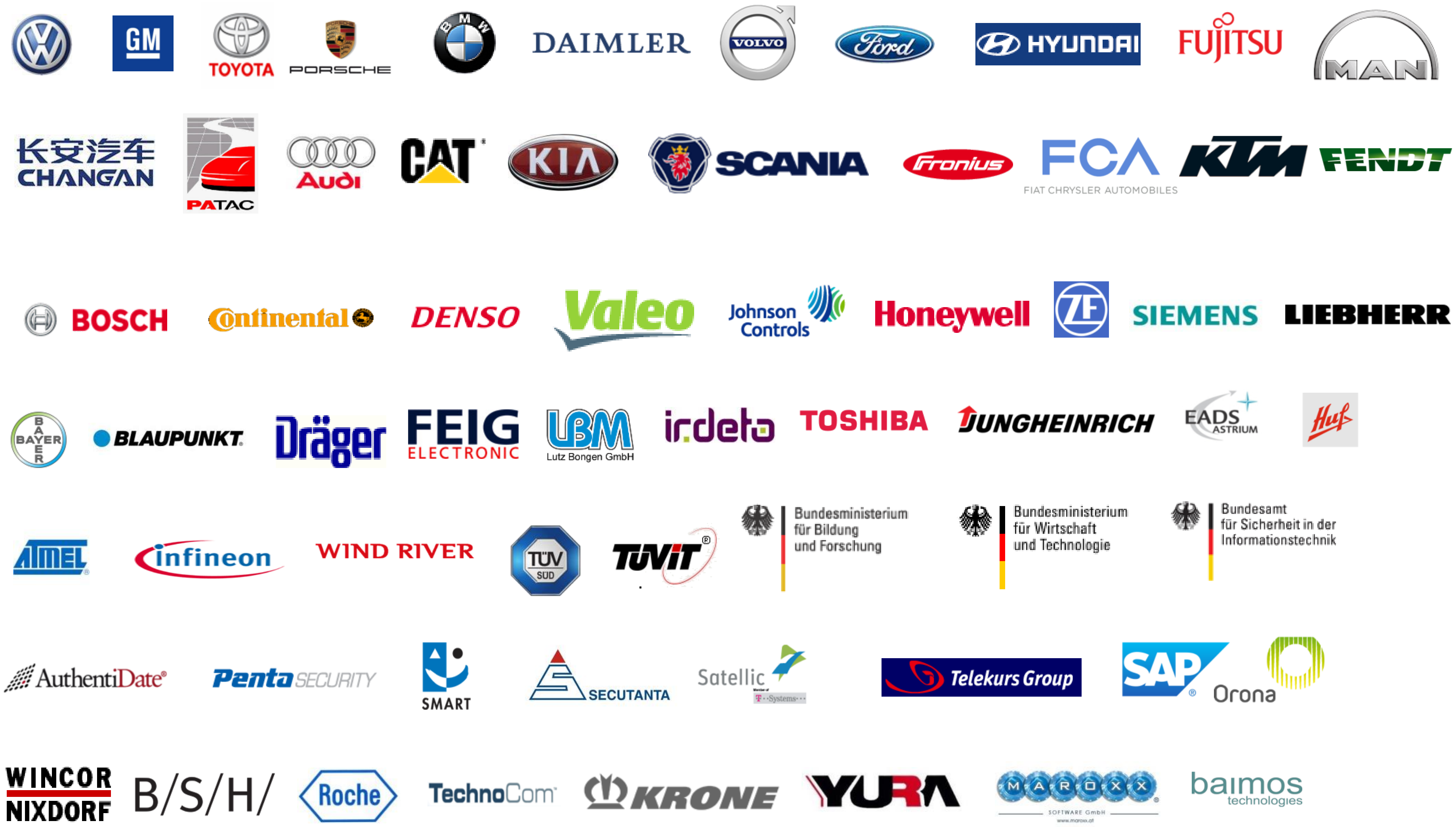
External: Independent security supplier

- The leading provider of automotive security solutions:
  - Security consulting and services
  - Security products
  - Security developments tailored for specific industries
- Consulting for development and organizational processes
- Security solutions for individual ECU and in-vehicle network
- Security protection for the connected vehicles
- Security analysis skills together with strong research

ESCRYPT – Embedded Security

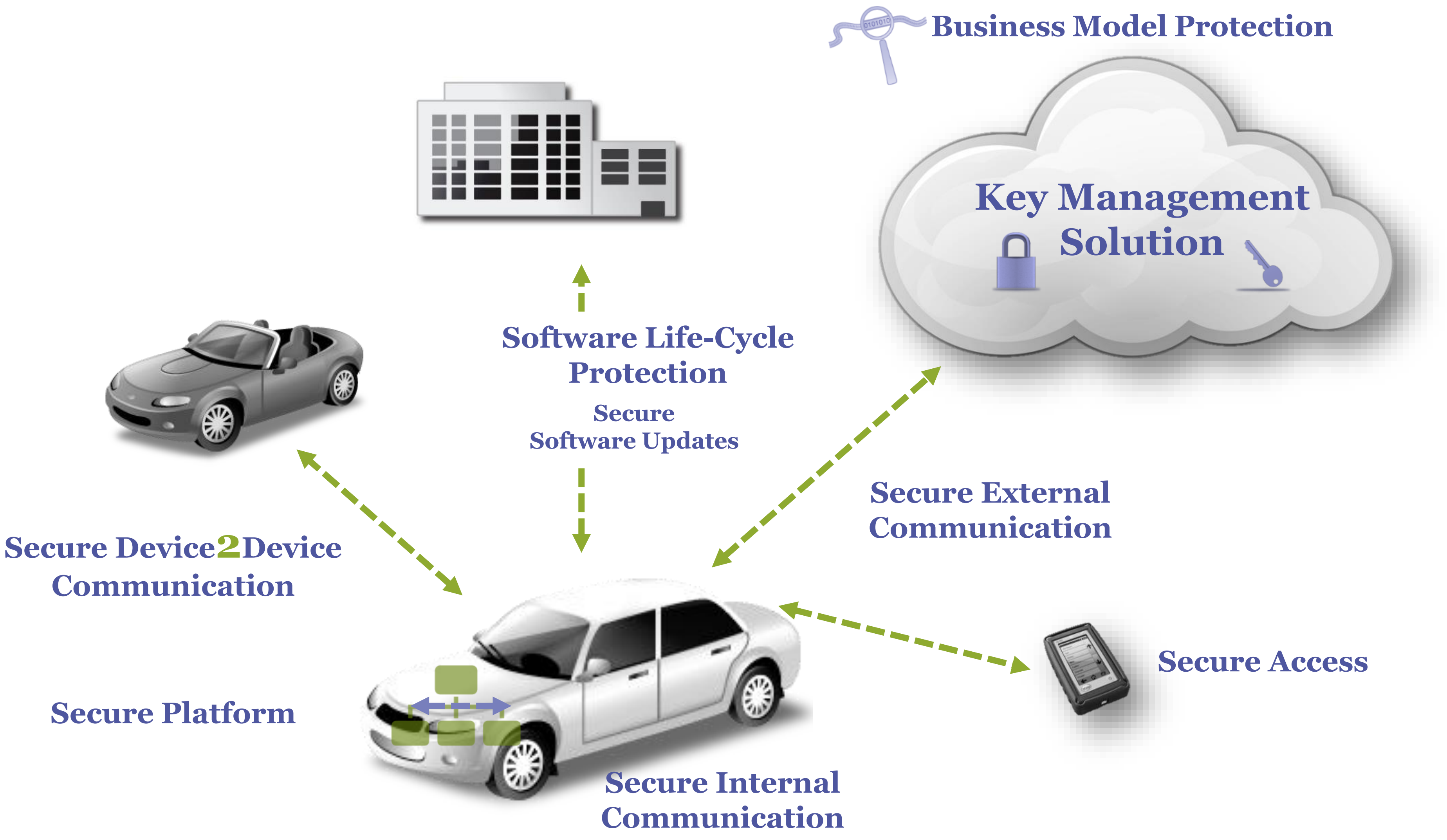
Reference Customers

escrypt
Embedded Security by ETAS



Automotive Security Solution

Security Analyses & Evaluation Scope



Business Model Protection

Key Management Solution

Software Life-Cycle Protection

Secure Software Updates

Secure External Communication

Secure Device2Device Communication

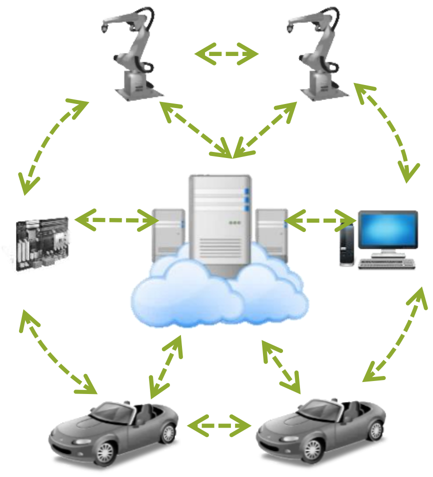
Secure Access

Secure Platform

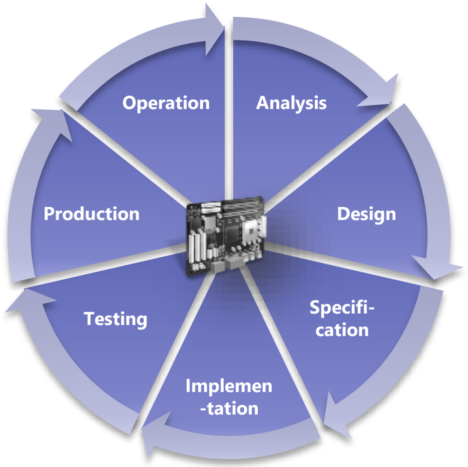
Secure Internal Communication

ESCRYPT – Embedded Security

The Solution: ESCRYPT’s Holistic Approach

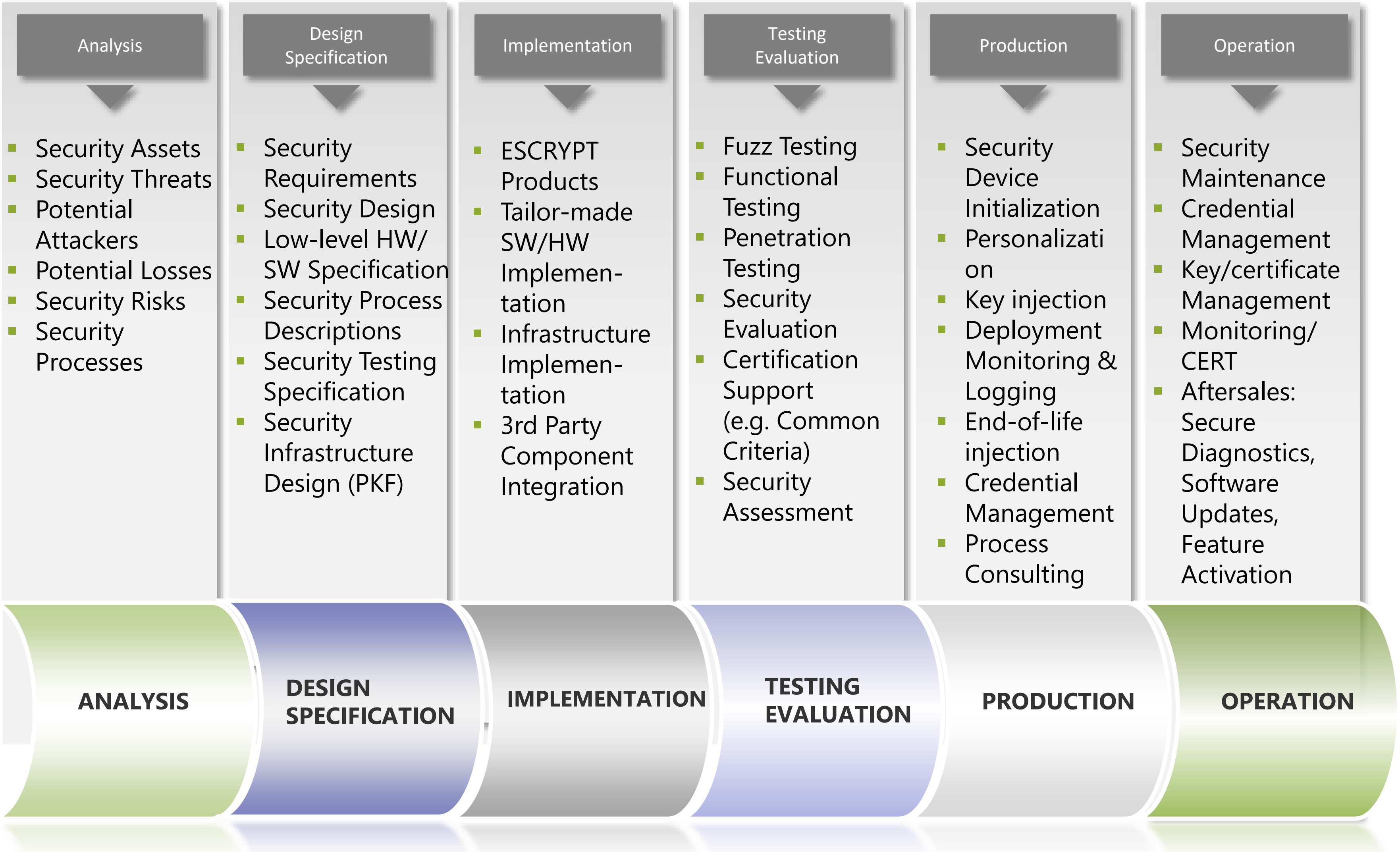


Security for the **complete system** and for the **entire life cycle.**



ESCRYPT – Embedded Security

Security for the Entire Life Cycle



Analysis

- Security Assets
- Security Threats
- Potential Attackers
- Potential Losses
- Security Risks
- Security Processes

Design Specification

- Security Requirements
- Security Design
- Low-level HW/ SW Specification
- Security Process Descriptions
- Security Testing Specification
- Security Infrastructure Design (PKF)

Implementation

- ESCRYPT Products
- Tailor-made SW/HW Implementation
- Infrastructure Implementation
- 3rd Party Component Integration

Testing Evaluation

- Fuzz Testing
- Functional Testing
- Penetration Testing
- Security Evaluation
- Certification Support (e.g. Common Criteria)
- Security Assessment

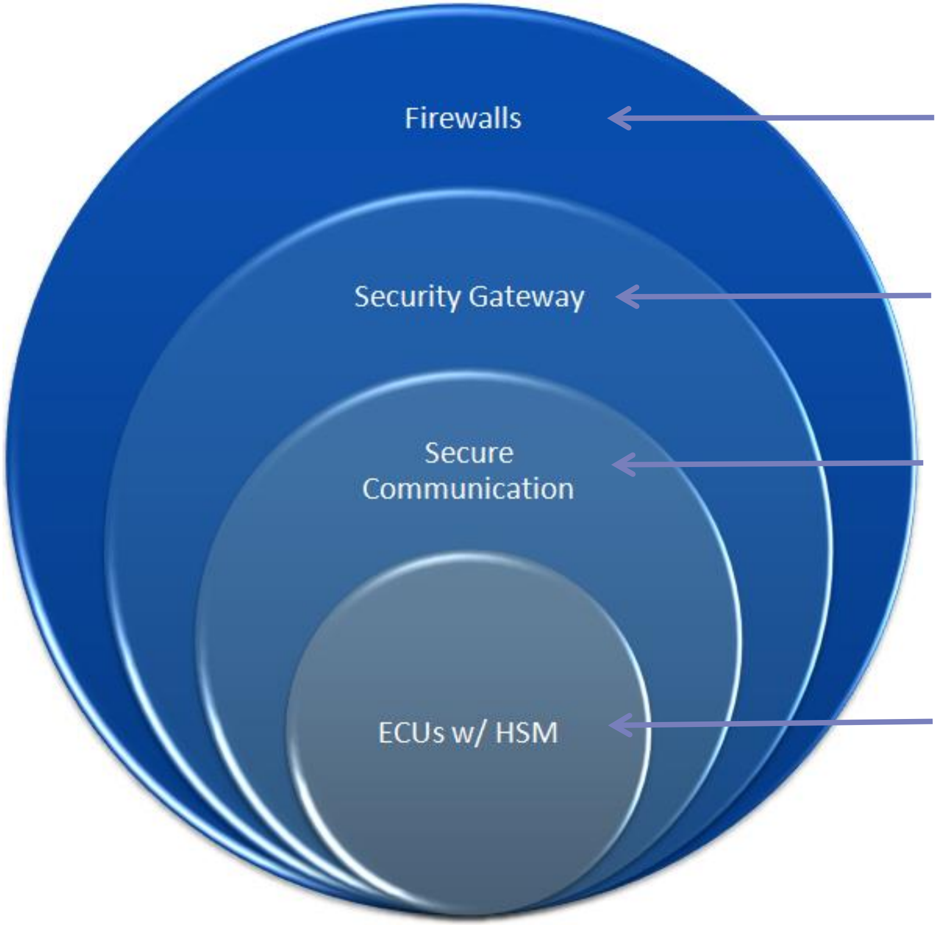
Production

- Security Device Initialization
- Personalization
- Key injection
- Deployment Monitoring & Logging
- End-of-life injection
- Credential Management
- Process Consulting

Operation

- Security Maintenance
- Credential Management
- Key/certificate Management
- Monitoring/ CERT
- Aftersales: Secure Diagnostics, Software Updates, Feature Activation

Security and E/E - Layered Architecture



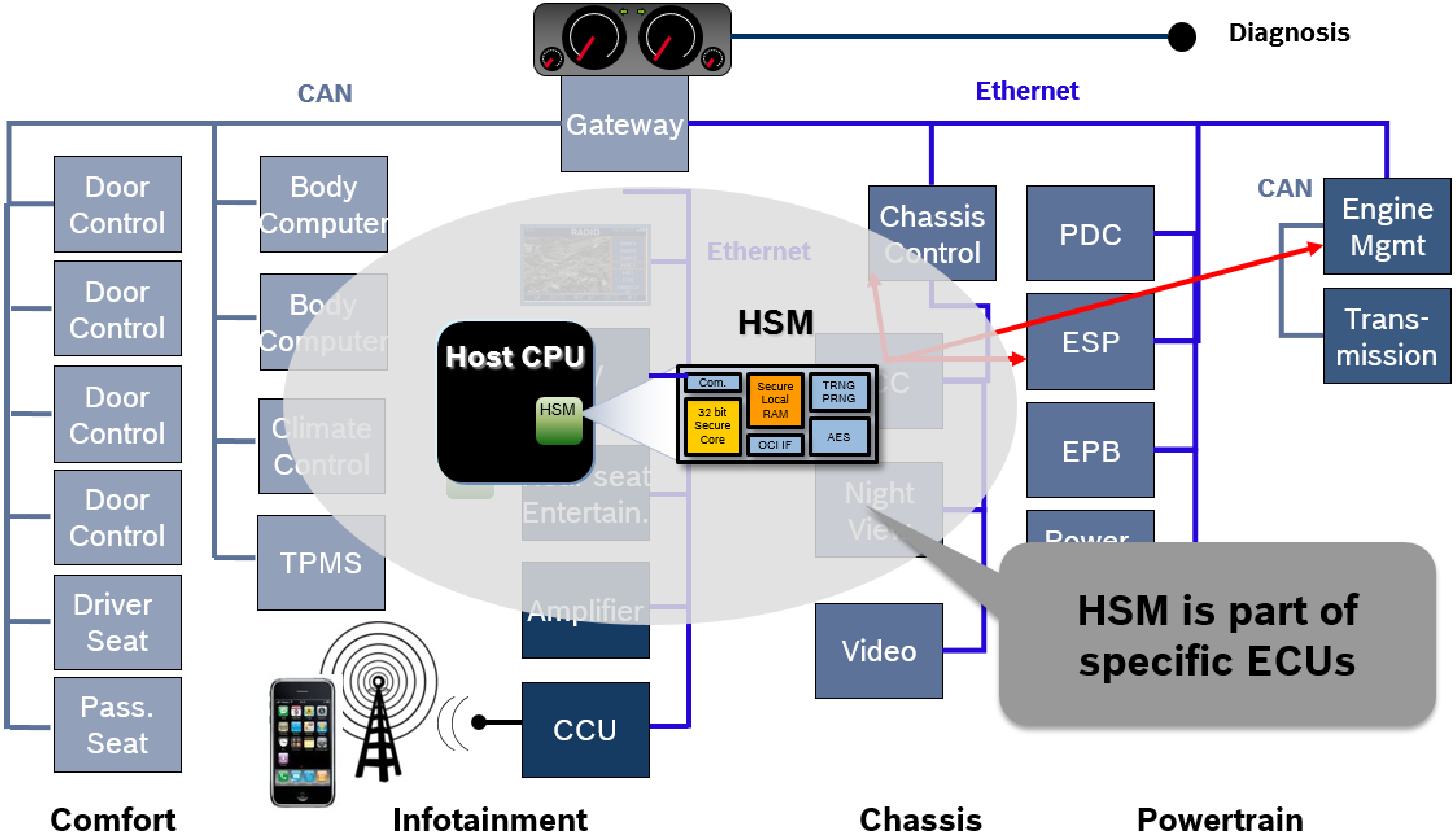
Firewalls to protect
external interfaces

Gateways to control the communication
between different domains inside
of the vehicle

Protection of vehicle internal communication
by authentication and integrity protection
of messages

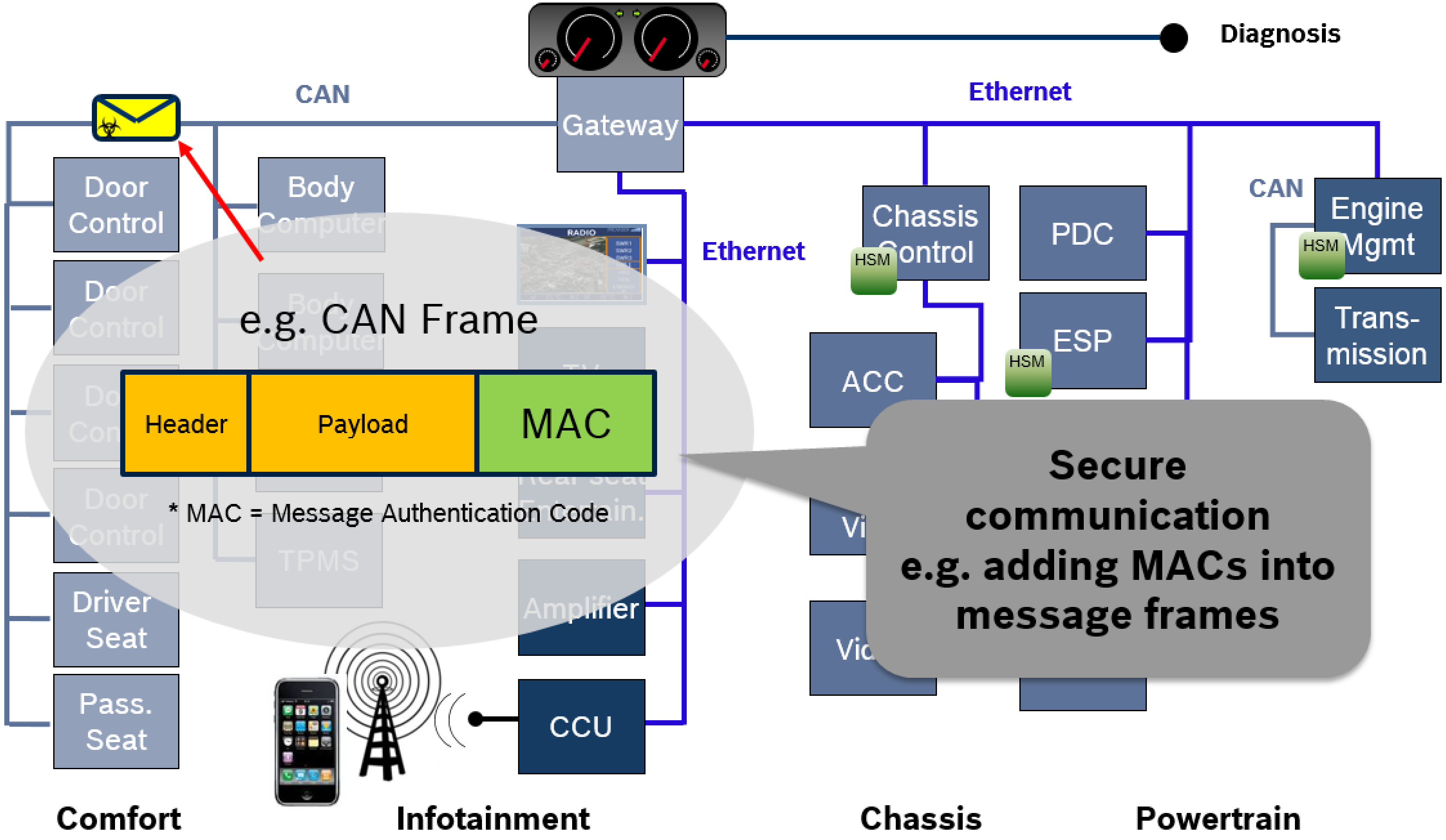
Hardware Security Module (HSM) to
secure single ECUs and provide means
to execute security mechanisms

E/E Architecture: HSM



HSM is part of specific ECUs

E/E Architecture: Secure Communication



e.g. CAN Frame

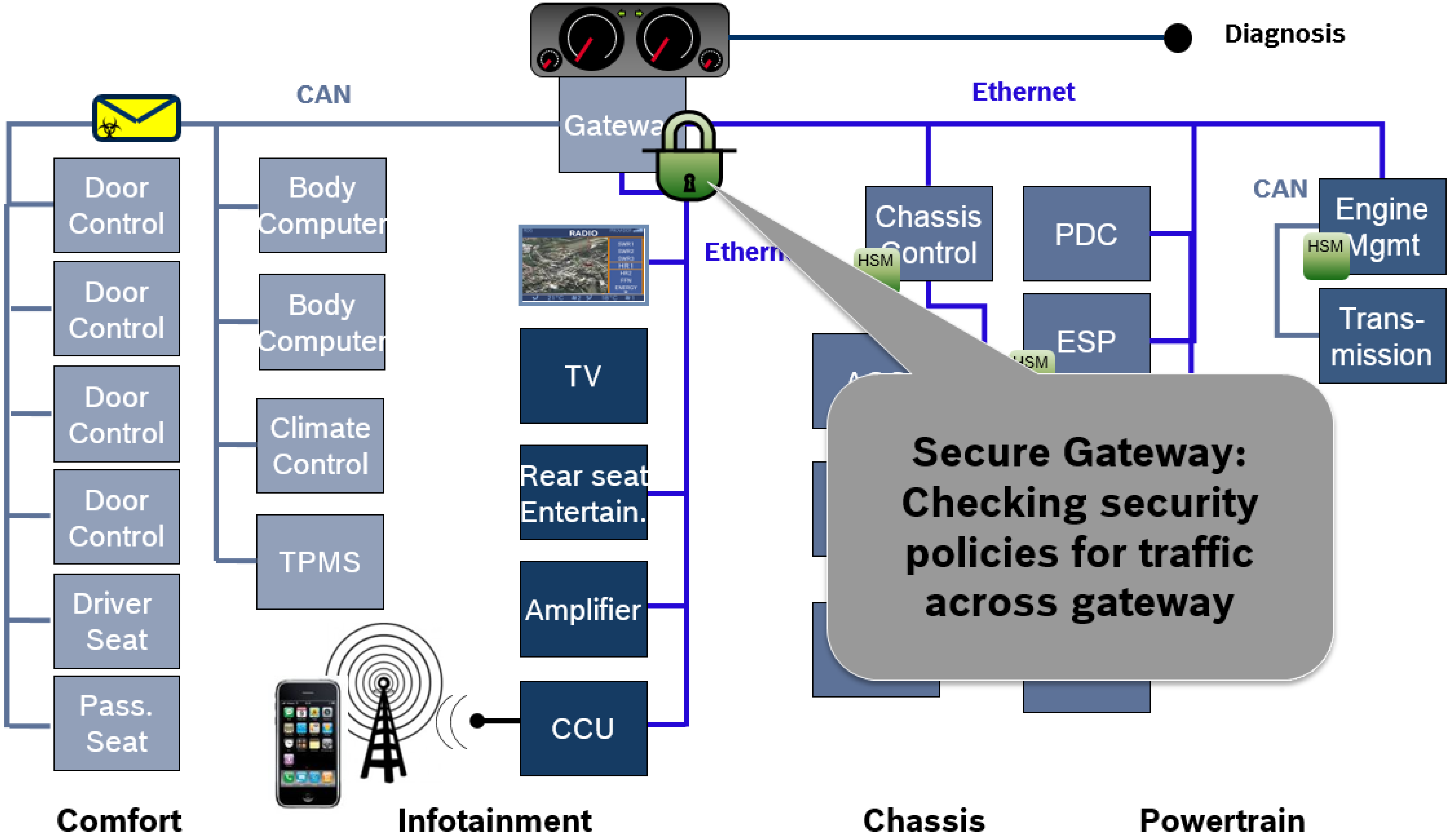
* MAC = Message Authentication Code

Secure communication e.g. adding MACs into message frames

ESCRYPT – Embedded Security

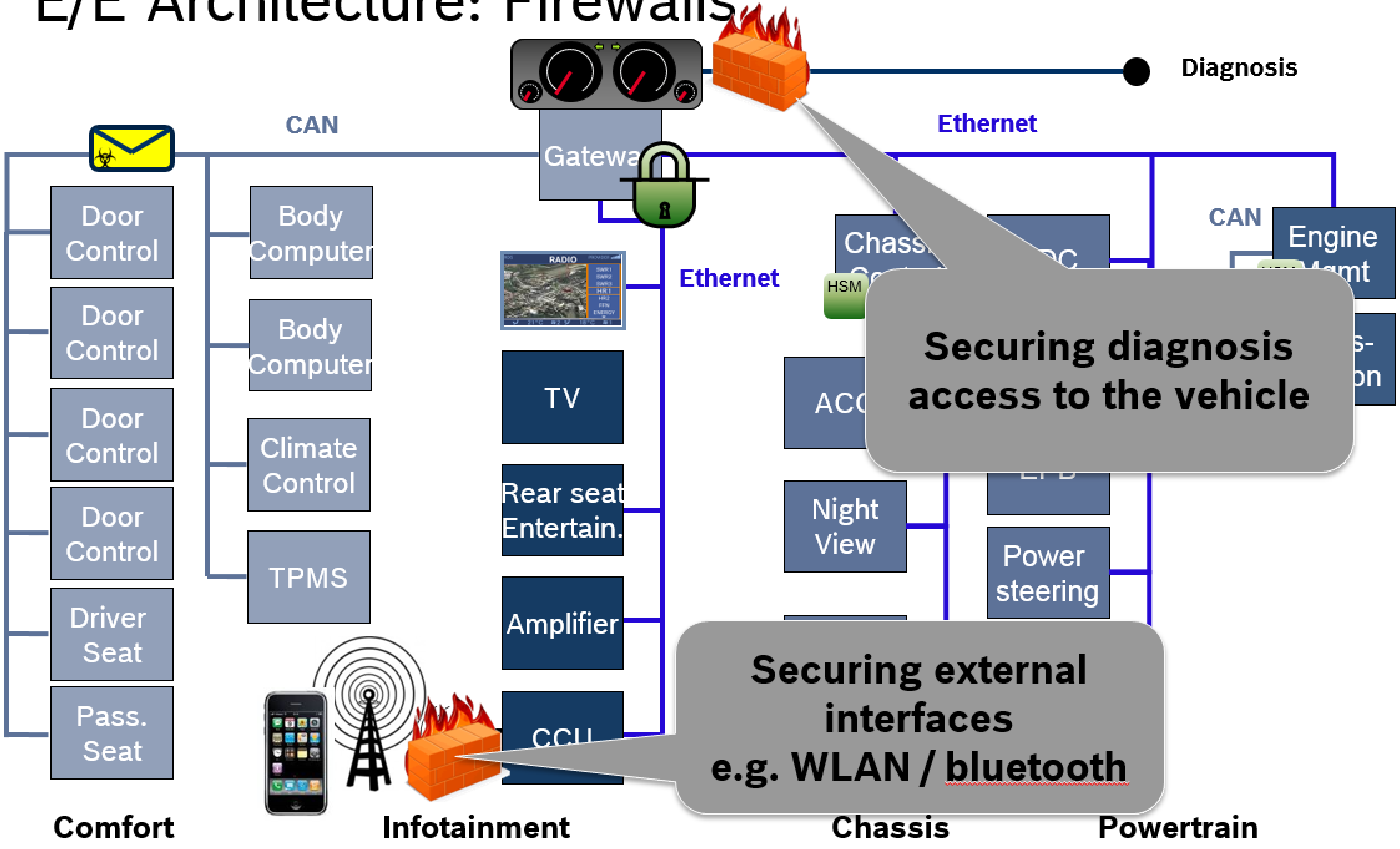
The Solution: ESCRYPT's Approach

E/E Architecture: Gateways



Secure Gateway: Checking security policies for traffic across gateway

E/E Architecture: Firewalls

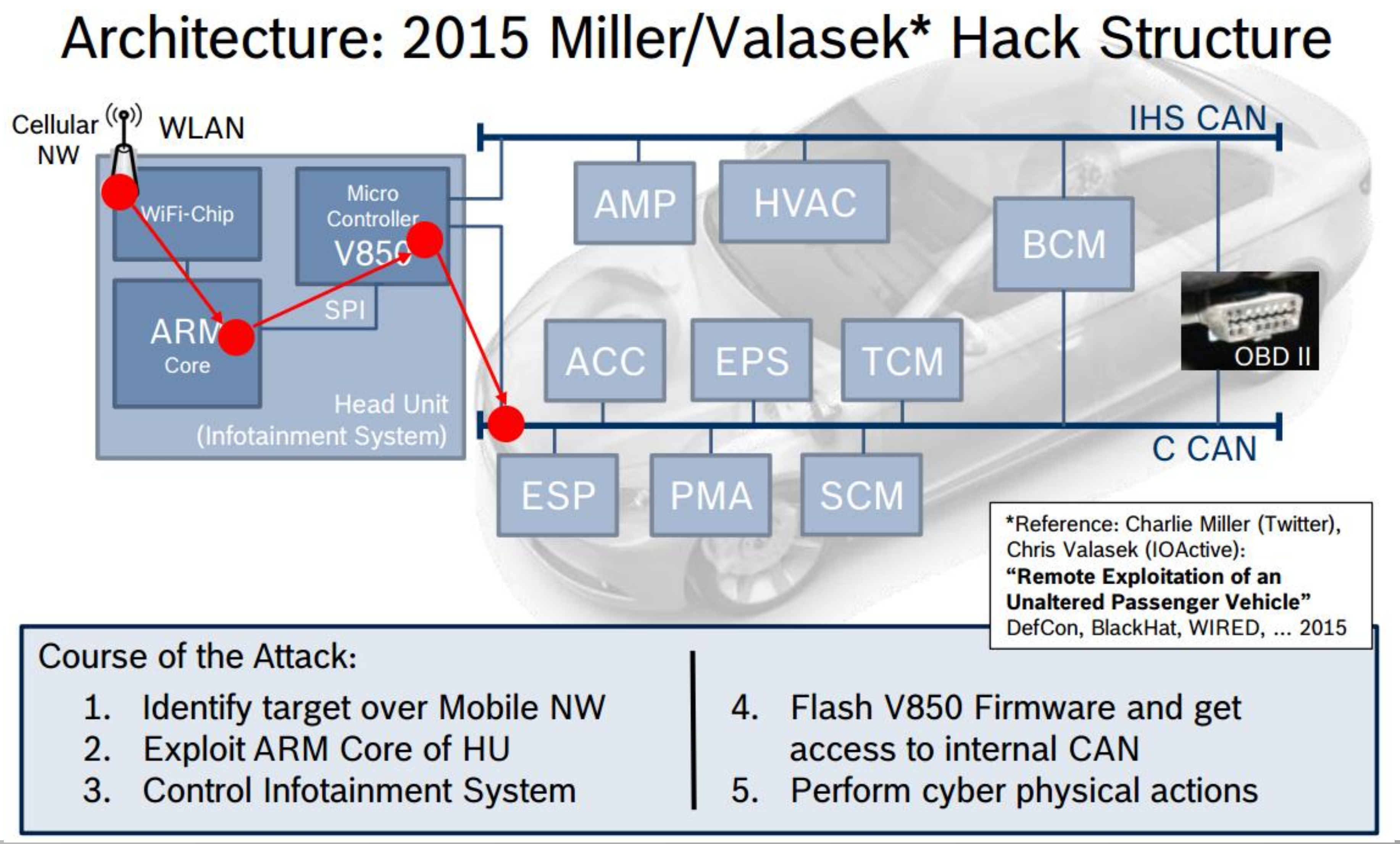


Securing diagnosis access to the vehicle

Securing external interfaces e.g. WLAN / bluetooth

Full Vehicle

Attack example



Architecture: 2015 Miller/Valasek* Hack Structure

*Reference: Charlie Miller (Twitter), Chris Valasek (IOActive):
“Remote Exploitation of an Unaltered Passenger Vehicle”
DefCon, BlackHat, WIRED, ... 2015

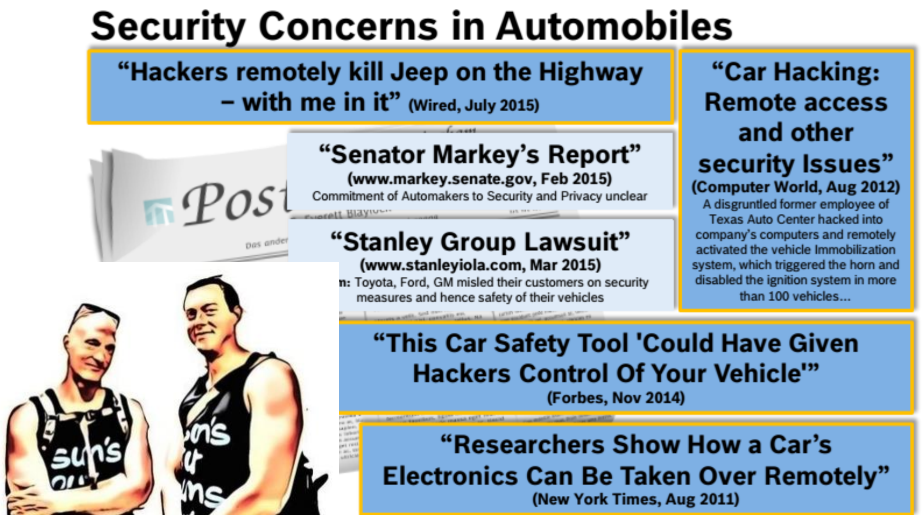
Course of the Attack:

1. Identify target over Mobile NW
2. Exploit ARM Core of HU
3. Control Infotainment System
4. Flash V850 Firmware and get access to internal CAN
5. Perform cyber physical actions

ESCRYPT – System Provider

Main security challenges to China OEMs

- Various inter-connection vehicle application with remote connection and remote control.
- Limited security protection for key assets.
- State of art security events and count measures, such as Chrysler Jeep remote attack, SAE J3061…



Security Concerns in Automobiles

"Hackers remotely kill Jeep on the Highway – with me in it" (Wired, July 2015)

"Senator Markey's Report"
(www.markey.senate.gov, Feb 2015)
Commitment of Automakers to Security and Privacy unclear

"Stanley Group Lawsuit"
(www.stanleyiola.com, Mar 2015)
n: Toyota, Ford, GM misled their customers on security measures and hence safety of their vehicles

"Car Hacking: Remote access and other security Issues"
(Computer World, Aug 2012)
A disgruntled former employee of Texas Auto Center hacked into company's computers and remotely activated the vehicle Immobilization system, which triggered the horn and disabled the ignition system in more than 100 vehicles…

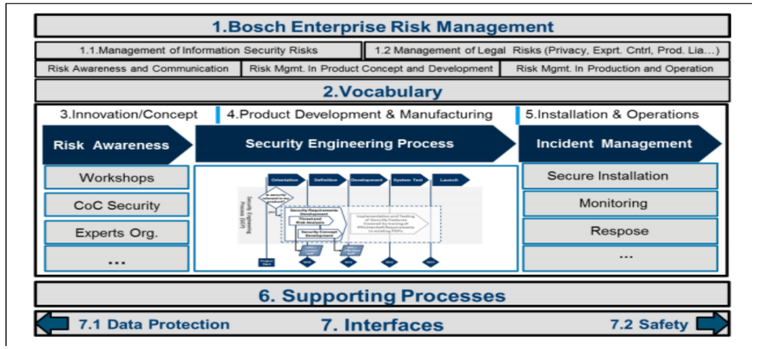
"This Car Safety Tool 'Could Have Given Hackers Control Of Your Vehicle'"
(Forbes, Nov 2014)

"Researchers Show How a Car's Electronics Can Be Taken Over Remotely"
(New York Times, Aug 2011)

SAE INTERNATIONAL

SURFACE VEHICLE RECOMMENDED PRACTICE	J3061™	JAN2016
	Issued	2016-01

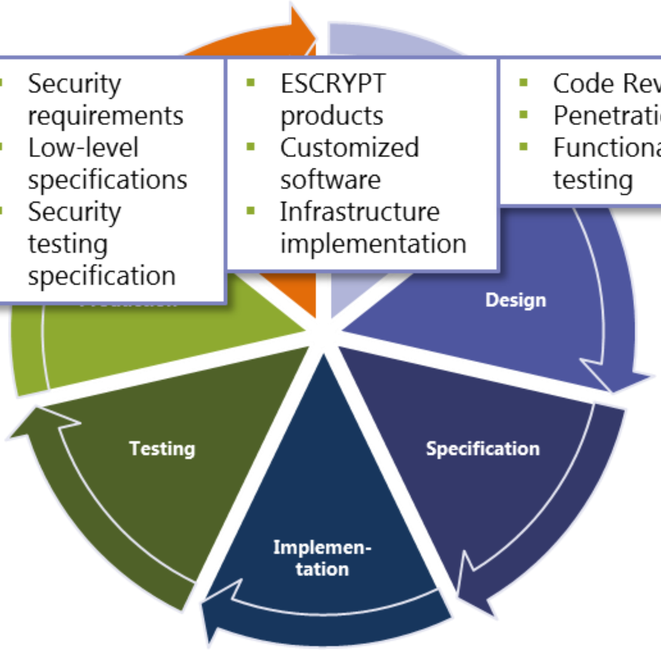
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems



1.Bosch Enterprise Risk Management
1.1.Management of Information Security Risks
1.2 Management of Legal Risks (Privacy, Exprt. Cntrl, Prod. Lia…)
Risk Awareness and Communication
Risk Mgmt. In Product Concept and Development
Risk Mgmt. In Production and Operation
2.Vocabulary
3.Innovation/Concept
4.Product Development & Manufacturing
5.Installation & Operations
Risk Awareness
Security Engineering Process
Incident Management
Workshops
CoC Security
Experts Org.
…
Secure Installation
Monitoring
Respose
…
6. Supporting Processes
7.1 Data Protection
7. Interfaces
7.2 Safety

ESCRYPT – System Provider

Assistance for the entire life-cycle…



▪ Security risk analysis ▪ Cost-benefit analysis	▪ Secure product design ▪ Security concepts ▪ Secure infrastructure design	▪ Security requirements ▪ Low-level specifications ▪ Security testing specification	▪ ESCRYPT products ▪ Customized software ▪ Infrastructure implementation	▪ Code Review ▪ Penetration test ▪ Functional testing	▪ Personalization ▪ Secure access & configuration ▪ Key injection & back-end registration	▪ Monitoring and CERT ▪ Security maintenance ▪ Aftersales: software updates, secure diagnostics, feature activation
Analysis	**Design**	**Specification**	**Implementation**	**Testing**	**Production**	**Operation**

ESCRYPT – System Provider

Main security requirements from China customers:

1. Security knowledge importing
2. Security analysis and solution definition
3. Security process compliance
4. Security component development and introduction
5. Security testing
6. Backend security solution

ESCRYPT – System Provider

ESCRYPT solutions:

1. Security knowledge importing

Organizational trainings:

1. Fundamentals of Security Engineering and SDL
2. Security trends and attack
3. Establishing security for components and systems based on cryptography
4. Requirements for developing secure embedded systems
5. Secure system design and secure architecture

Professional trainings:

1. Introduction to cryptography and IT-security
2. Automotive HSM (Hardware Security Module)
3. SHE (Secure Hardware Extensions)
4. Key management system
5. Flash over the air

ESCRYPT – System Provider

Security training list

Day 1	**Automotive Security Basics**
AM	Fundamentals of Security Engineering and SDL / Holistic security Design of Systems
PM	Introduction to cryptography
	• Symmetric key cryptography
	• Hash functions
	• Public key cryptography
	• Certificates and PKI
	• Security Certification
	• Introduction to security in the IT industry
Day 2	**Secure System Design and Secure Architecture**
AM	Secure Design Lifecycle 1
	• System Modeling
	• Security Objectives and Threat Analysis
	• Risk Assessment
	• Security Requirements
	• Security Concept
PM	Secure Design Lifecycle 2
	• Security testing
	• Test Tools for Security functionality
	• Security Evaluation
	• Supplier Audit

Day 3	**Trends & Automotive Security, Software**
AM	Trends & Attacks
	• Automotive security: threats and trends
	• State-of-the-Art in Automotive Hacking
PM	Automotive Security, Software
	• Secure Diagnostic Interface
	• Secure in-vehicle communication
Day 4	**Automotive Security, Hardware**
AM	Introduction to Automotive HSMs and the Bosch HSM
PM	• Secure Hardware Extension, SHE and SHE+
	• Application SW integration, CycurHSM & AUTOSAR CSM
Day 5	**Firewall, Software updates & Connectivity**
AM	• Application SW integration, CycurHSM & AUTOSAR CSM cont.
PM	• Software Updates over-the-air
	• Key management
	• Connectivity
	• Car-to-car communications

ESCRYPT – System Provider

ESCRYPT solutions:

2. Security analysis and solution definition

   – Provided E/E architecture consulting

   – Analyzed the network planned by the OEM

   – Security threat and risk analysis

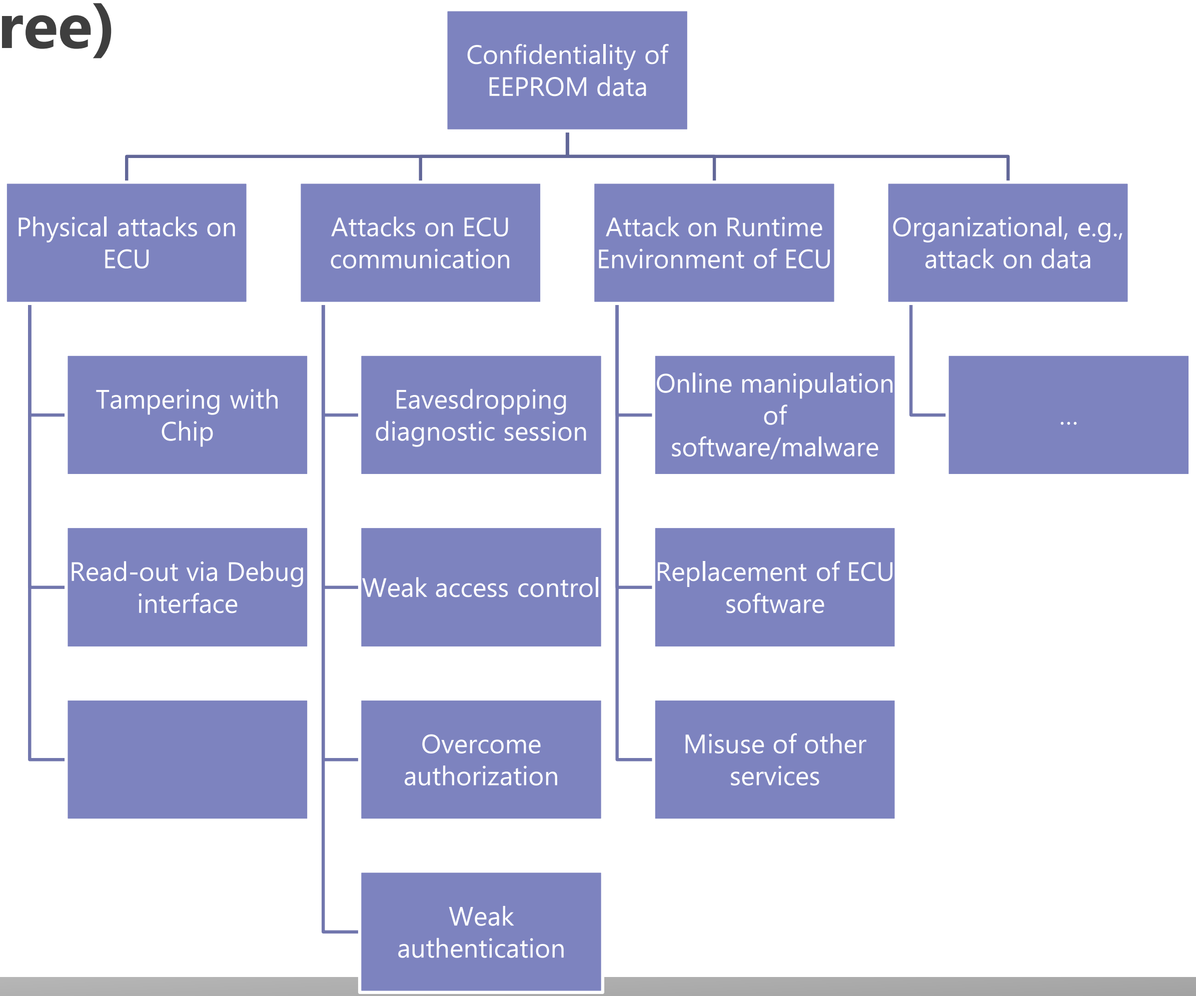
   – Security concept development

   – Proposed improvements

   – Proposed firewall rules

ESCRYPT – System Provider

Security thread and risk analysis (Security asset and Attack tree)



Confidentiality of EEPROM data

Physical attacks on ECU
- Tampering with Chip
- Read-out via Debug interface

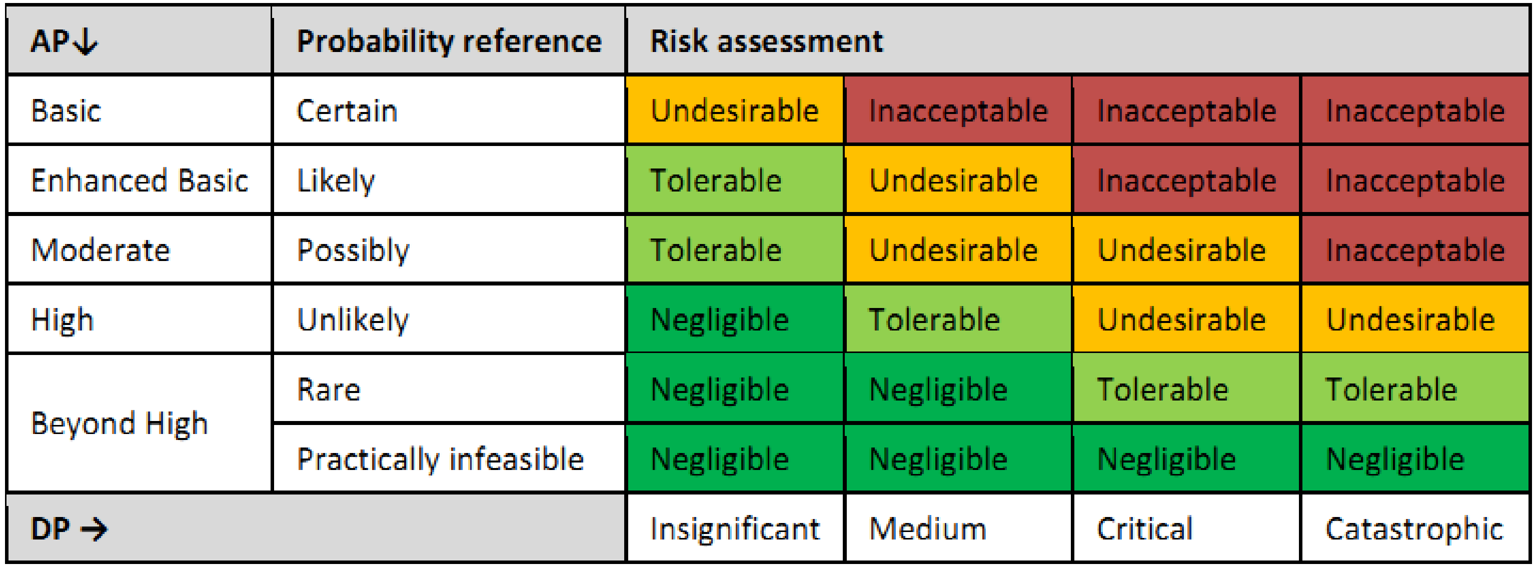
Attacks on ECU communication
- Eavesdropping diagnostic session
- Weak access control
- Overcome authorization
- Weak authentication

Attack on Runtime Environment of ECU
- Online manipulation of software/malware
- Replacement of ECU software
- Misuse of other services

Organizational, e.g., attack on data
- …

ESCRYPT – System Provider

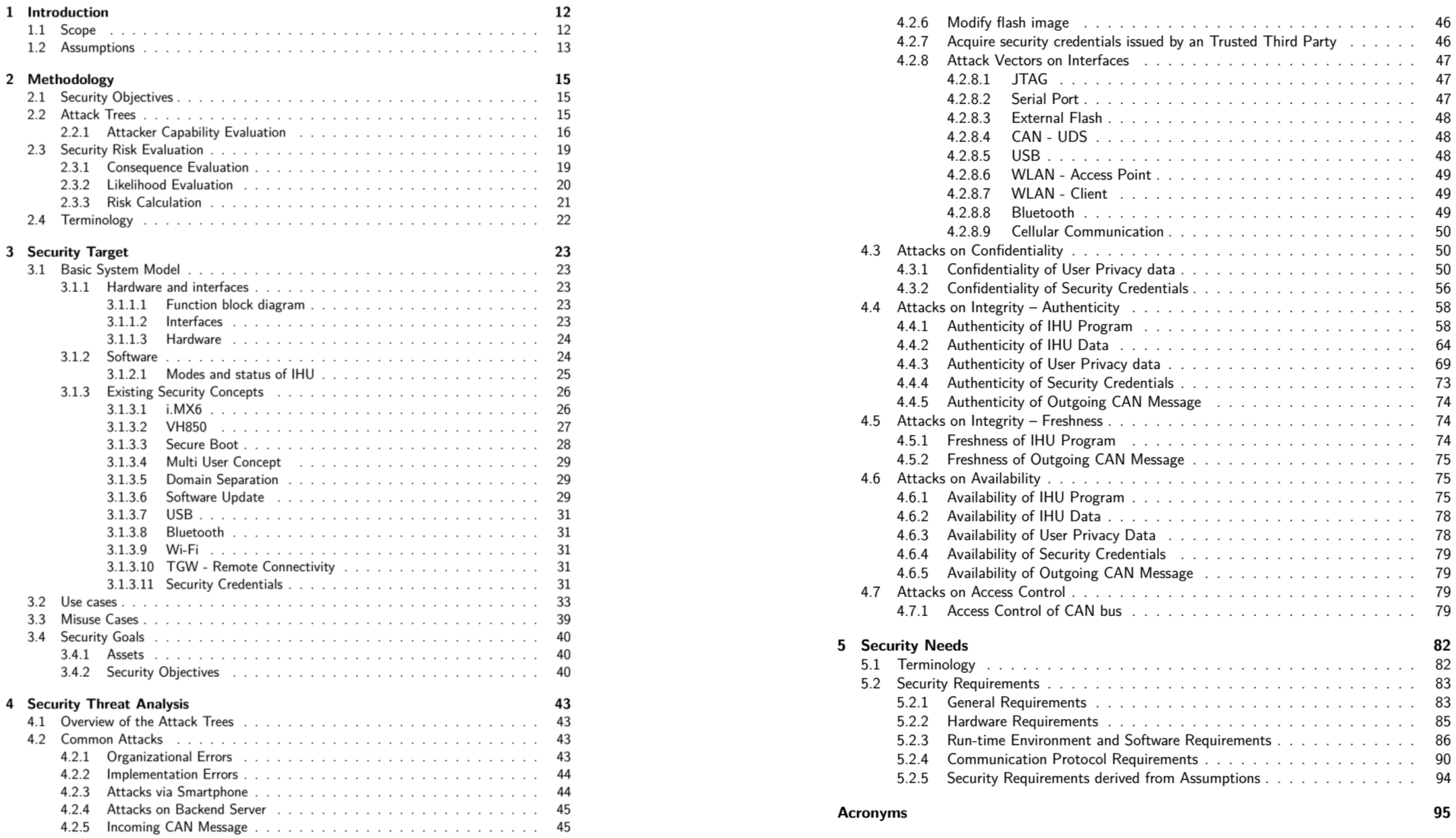
Security thread and risk analysis (Risk assessment)



AP↓	**Probability reference**	**Risk assessment**			
Basic	Certain	Undesirable	Inacceptable	Inacceptable	Inacceptable
Enhanced Basic	Likely	Tolerable	Undesirable	Inacceptable	Inacceptable
Moderate	Possibly	Tolerable	Undesirable	Undesirable	Inacceptable
High	Unlikely	Negligible	Tolerable	Undesirable	Undesirable
Beyond High	Rare	Negligible	Negligible	Tolerable	Tolerable
	Practically infeasible	Negligible	Negligible	Negligible	Negligible
DP →		Insignificant	Medium	Critical	Catastrophic

ESCRYPT – System Provider

Security thread and risk analysis



ESCRYPT – System Provider

Security mechanism list for reference

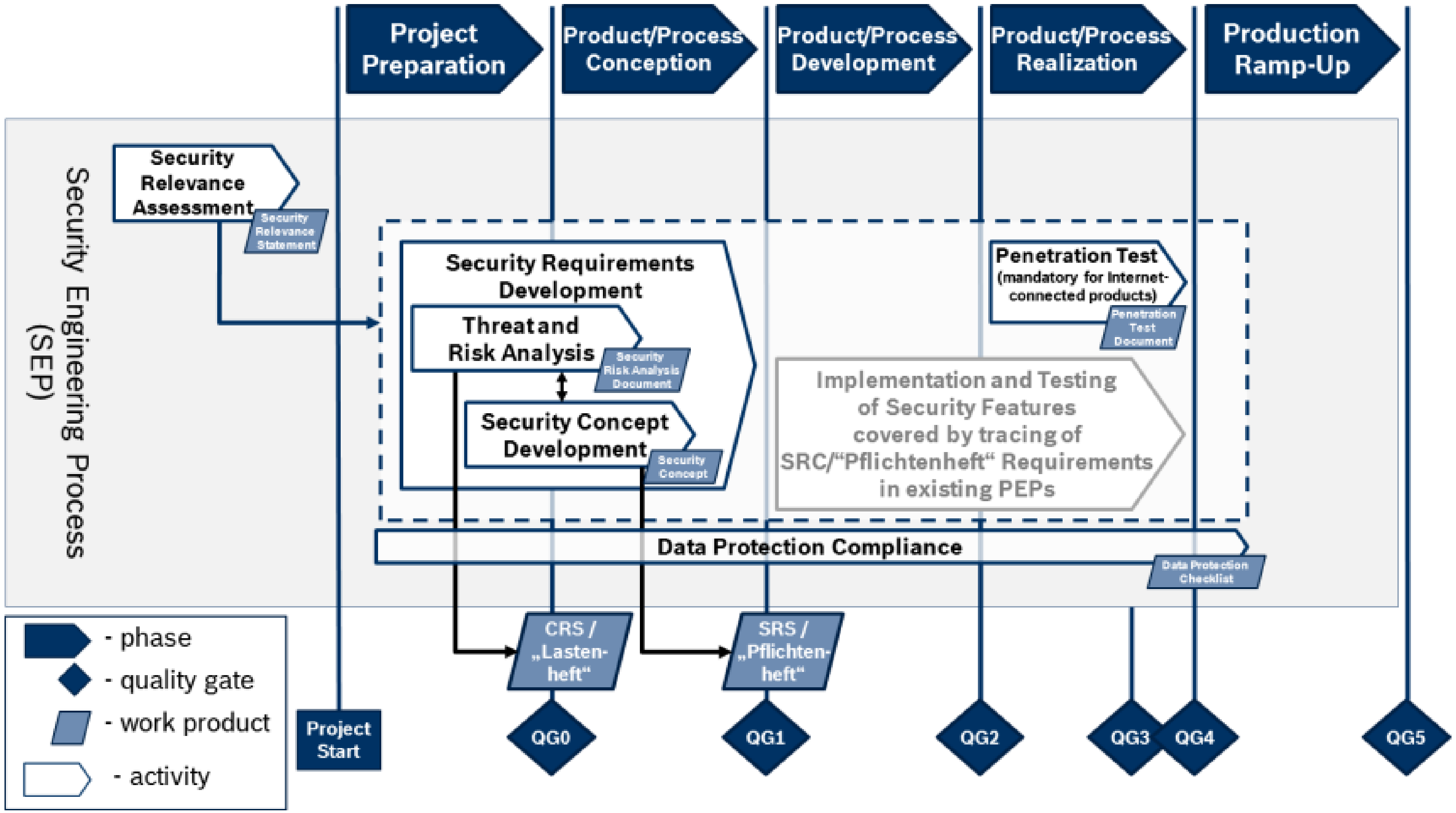
1. Secure boot loader
2. Digital signature for key data
3. MAC protection for CAN message
4. HSM protection (or trust zone solution)
5. Key Management solution
6. Cryptography
7. Access control
8. Memory protection
9. Debugger interface and backdoor…

ESCRYPT – System Provider

4. Security process compliance
    - Security Engineering Process detailed deployment consulting
    - Security process tailoring
    - Security activity support
    - Security gateway review
    - Security audit support

ESCRYPT – System Provider

Security thread and risk analysis (Overview)


Project Preparation
Product/Process Conception
Product/Process Development
Product/Process Realization
Production Ramp-Up
Security Engineering Process (SEP)
Security Relevance Assessment
Security Relevance Statement
Security Requirements Development
Threat and Risk Analysis
Security Risk Analysis Document
Security Concept Development
Security Concept
Penetration Test (mandatory for Internet-connected products)
Penetration Test Document
Implementation and Testing of Security Features covered by tracing of SRC/“Pflichtenheft“ Requirements in existing PEPs
Data Protection Compliance
Data Protection Checklist
CRS / „Lastenheft“
SRS / „Pflichtenheft“
Project Start
QG0
QG1
QG2
QG3
QG4
QG5
- phase
- quality gate
- work product
- activity

ESCRYPT – System Provider

ESCRYPT solutions:

5. Security component development and introduction

CycurLIB

Cryptographic library for embedded Systems

CycurTLS

Transport Layer Security (TLS) for embedded platforms

CycurACT

Secure feature activation for embedded devices

CycurFLASH

Secure flashing solution for embedded devices

CycurV2X

The
IEEE 1609.2
ETSI TS 103 097
security stack

CycurKEYS

Cryptographic key management server for secure management of embedded applications

CycurHSM

Automotive-qualified software stack for Hardware Security Modules

ESCRYPT – System Provider

ESCRYPT solutions:

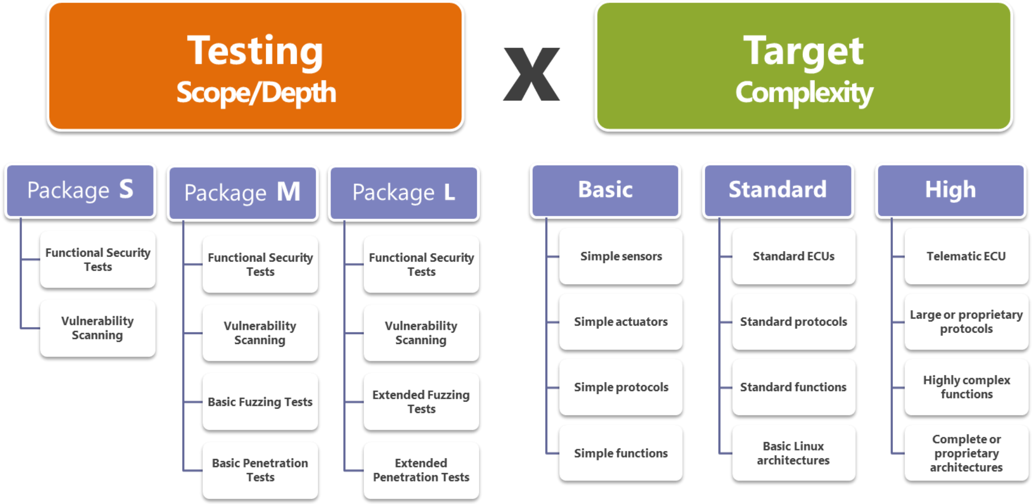
6. Security penetration testing

In order to improve quality, trust, and dependability of such a embedded system, usually additional test methods that are designed **from an attacker's point of view** are needed since:

- Practical implementation can deviate from specification
- Fatal implementation errors can lead to security weaknesses
- Physical implementation can introduce additional security risks

Security penetration test can be:

- Component level
- Domain level
- Vehicle level



Testing Scope/Depth X **Target** Complexity

Package **S**
- Functional Security Tests
- Vulnerability Scanning

Package **M**
- Functional Security Tests
- Vulnerability Scanning
- Basic Fuzzing Tests
- Basic Penetration Tests

Package **L**
- Functional Security Tests
- Vulnerability Scanning
- Extended Fuzzing Tests
- Extended Penetration Tests

Basic
- Simple sensors
- Simple actuators
- Simple protocols
- Simple functions

Standard
- Standard ECUs
- Standard protocols
- Standard functions
- Basic Linux architectures

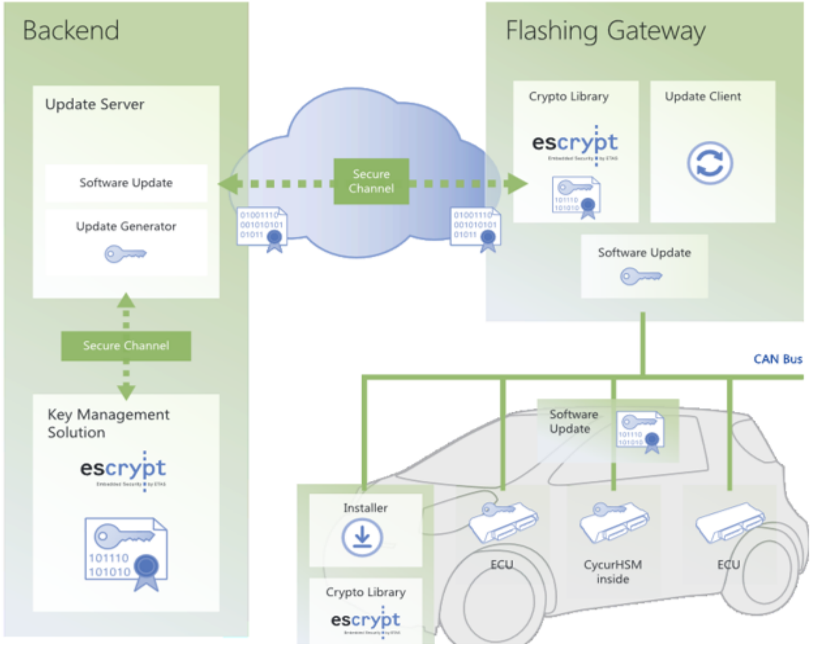
High
- Telematic ECU
- Large or proprietary protocols
- Highly complex functions
- Complete or proprietary architectures

ESCRYPT – System Provider

ESCRYPT solutions:

7. Backend security solution

- Key management solution(KMS) for OEMs and Tire1s
- Flash over the air (FOTA)



Partners

BOSCH
Invented for life

Red Bend
Software

arynga

Innovators and leaders in the development of software lifecycle management technologies.

Thank you for your kind attention!

escrypt