Deloitte.

Automotive Security | Standardization activities and attacking trend

Ingo Dassow, Deloitte

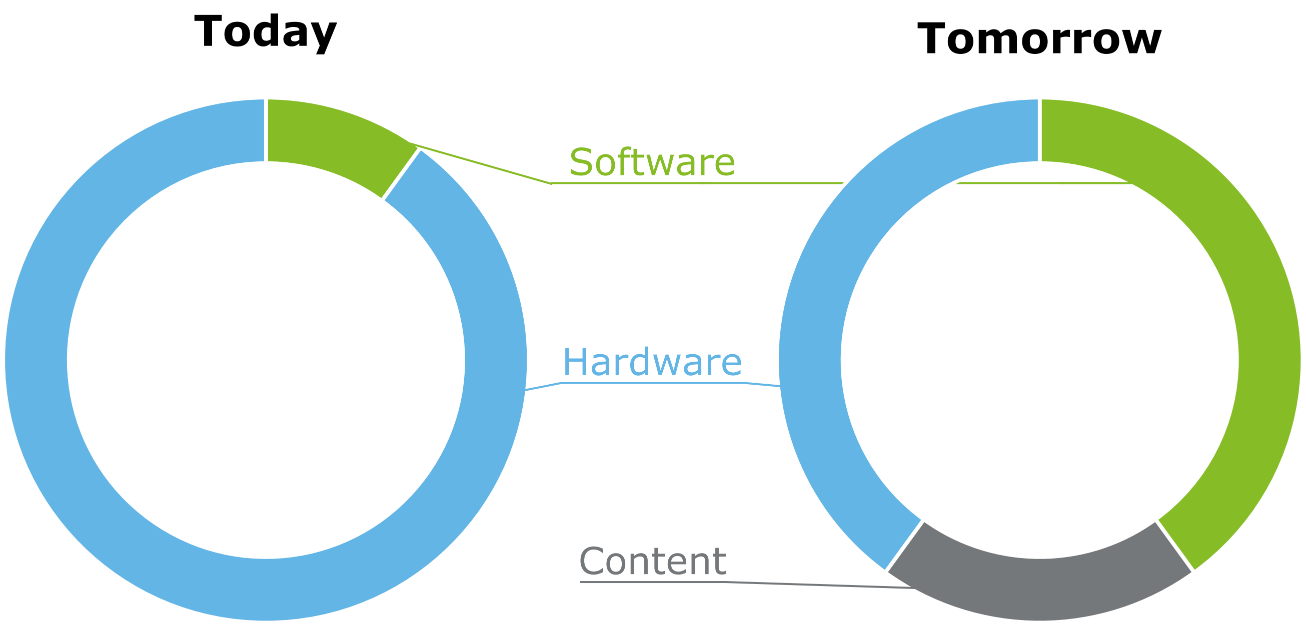
November 2017

Automotive Risk Overview

Trends and risks for connected vehicles

Value and Components of a Car

Autonomous driving and shared mobility will leverage a change of the value of the car with an increasing number of market players



Majorly provided by OEM & suppliers

- Body Shell
- Powertrain
- Lightning
- Seats
- Components & Interfaces

Provided by any company – OEM, supplier, or tech firm with expertise on OS level / in-car-apps – in order to control or enhance connected car functions

- Infotainment
- Driver interfaces
- Safety & Security functions
- Autonomous functions

Entertainment
Music and video streaming to in-car entertainment system

Social media
Direct connection to social media channels such as Facebook

Points of interest
POI displayed on in-car screens such as hotels, restaurants, free parking

Navigation
Maps displayed on in-car screens incl. route optimization

Traffic
Real-time traffic updates displayed on in-car screens

Maintenance
Automatic failure diagnostics and tracking of vehicle health

Fuel tracking
Fuel efficiency tracking and forecasting incl. up-to-date pricing

Emergency
Direct connection to emergency hotlines in case of accidents

Theft protection
Automatic notification of car owner and GPS tracking of car

Driver assistance systems
Security features like lane/distance assistant, drowsiness detection

Autonomous driving
Self-driving functions

Parking Assistant
Driverless parking including parking sensors and video systems

Access
Remotely lock and unlock vehicle via internet-connected device

Challenges of automated vehicles

…pose new tasks to address in the future

Automotive Cyber Security

Available and upcoming standards

Standards Overview

Many of the established standards cross industrial boundaries and can be used for automotive security. A globally aligned standard for vehicle security is still missing.

International Organization for Standardization / International Electrotechnical Commission (ISO/IEC)

- ISO/IEC 9797-1: Security techniques – Message Authentication Codes
- ISO/IEC 11889: Trusted Platform Module
- ISO 12207: Systems and software engineering – Software lifecycle processes
- ISO 15408: Evaluation criteria for IT security
- ISO 26262: Functional Safety for road vehicles
- ISO 27001: Information Security Management System
- ISO 27002: Code of Practice – Security
- ISO 27010: Information security management for inter-sector and inter-organizational communications
- ISO 27018: Code of Practice – Handling PII / SPI (Privacy)
- ISO 27034: Application Security
- ISO 27035: Information security incident management
- ISO 29101: Privacy architecture framework
- ISO 29119: Software testing standard
- IEC 62443: Industrial Network and System Security

National Institute of Standards and Technology (NIST)

- NIST SP800-30: Guide for Conducting Risk Assessments
- NIST SP800-50: Building an Information Technology Security Awareness and Training Program
- NIST SP800-61: Computer Security Incident Handling Guide
- NIST SP800-64: Security Considerations in the System Development Lifecycle
- NIST SP800-121: Guide to Bluetooth Security
- NIST SP800-127: Guide to Securing WiMAX Wireless Communications
- NIST SP800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations
- NIST SP800-150: Guide to Cyber Threat Information Sharing

Society of Automotive Engineers (SAE)

- SAE J2945: Dedicated Short Range Communication (DSRC) Minimum Performance Requirements
- SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- SAE J3101: Requirements for Hardware-Protected Security for Ground Vehicle Applications

Addressing Automotive Security throughout the whole vehicle lifecycle

Standards are needed to support the implementation of a risk based approach in each phase of the lifecycle.

1. Collaboration with third parties
- ISO/ IEC 27010:2012
- NIST SP 800-150

2. & 3. Risk Management and Threat Detection
- ISO/ IEC 30111
- NIST 800-30, NIST 800-137

4. Establish Security-by-design
- ISO 17799
- SAE J3061
- NIST SP 800-127, NIST SP 800-121, NIST 800-64

5. Incident response
- ISO/ IEC 27035:2011
- NIST SP 800-61

6. & 7. Organizational implementation
- ISO/ IEC 27001
- NIST SP 800-50

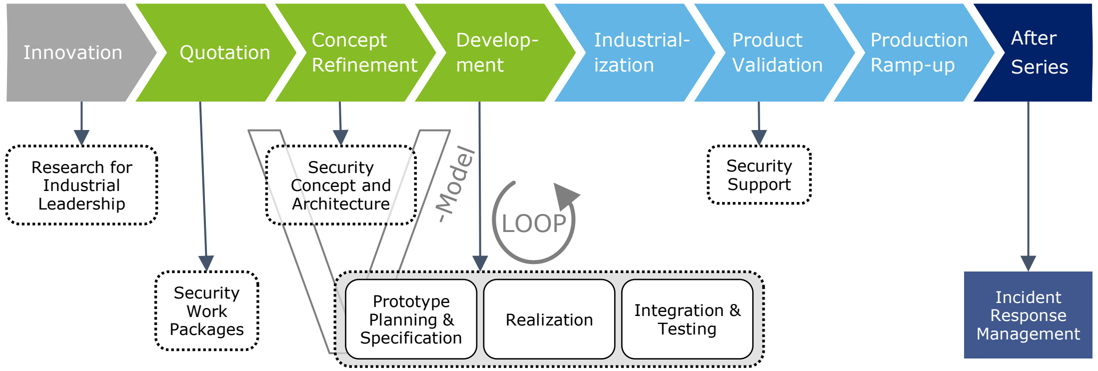
ISO/IEC WD 21434

The upcoming standard from ISO and SAE for cybersecurity engineering

Goals

- Give uniform definition of notions relevant to automotive security
- Specify minimum requirements on security engineering process and activities
- Define criteria for assessment (wherever possible)
- Describe the state of the art of security engineering in automotive E/E development
- Provide a common and internationally agreed understanding of automotive cybersecurity engineering
- Can serve as reference for legislative institutions; ensure legal certainty

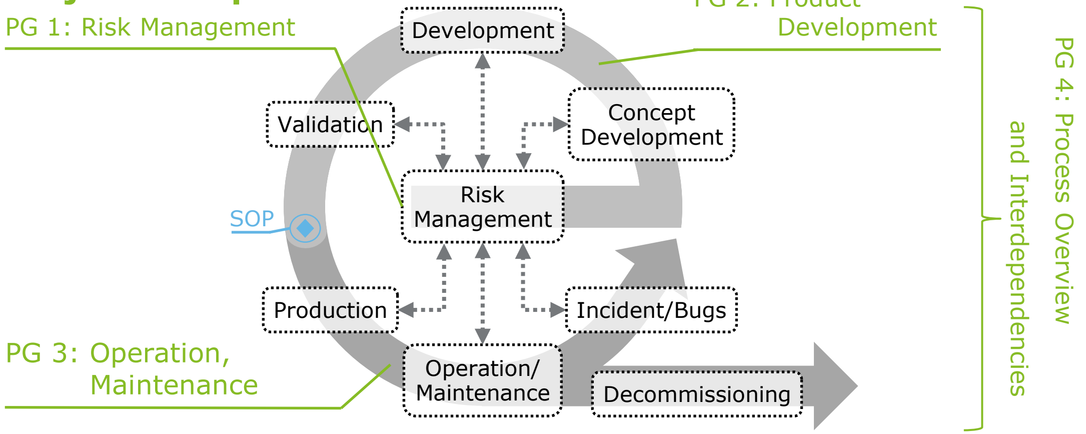
Security in the Product Life Cycle



Scope

- Requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g. concept, design, development), production, operation, maintenance, and decommissioning
- Framework for a cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders
- Is applicable to road vehicles that include electrical and electronic (E/E) systems, their interfaces and their communications
- Not prescribe specific technology or solutions related to cybersecurity.

Project Groups



ISO/SAE 21434

Overall schedule from start on the 1st October 2016 until the publication on the 1st October 2019

Start JWG
October 1st ,2016

JWG
drafting the document

January **2017**

January **2018**

ISO WD-ballot for technical comments
2018-02-15

JWG
drafting the document

SAE Level 1 Technical committee ballot for technical comments

ISO CD-ballot for technical comments
2018-09-15

JWG
drafting the document

SAE Level 1 Technical committee ballot for technical comments

January **2019**

ISO DIS-ballot for technical comments
2019-03-15

JWG
preparation of the document for publication

SAE Level 1 Technical committee ballot for technical comments

Joint publication of ISO/SAE-Standard
October 1st, 2019

WD: Working Draft; CD: Committee Draft; DIS: Draft International Standard

First Achievements

Security Level (CAL)
- Inspired by EAL (CC)
- Risk Profiles

Production and Operation
- Security in Manufacturing
- Development of Software Updates

Distributed Development
- Data-Exchange between customer and supplier in different engineering phases
- Clarifying Responsibilities

Incident Management
- Field Monitoring
- Incident Mitigation

Integration of Safety and Security
- Identification of touch points
- Harmonization between both processes
- Considered in Risk Management

Privacy
- Considered in the Risk Management to be protected by Cybersecurity
- No legal prescriptions (not a regulation)

Automotive Risk Methodology

General Risk Evaluation Approach

Deloitte Automotive Cyber Security (ACS) services

to address the industry challenges based on our insights from different OEMs

ACS Management System
Risk based Approach for managing Automotive Cyber Security throughout the whole vehicle lifecycle.

ACS Security Architecture
Gap-Analysis to find strategy and roadmap for holistic security implementation.

Protective Measures

Detective Measures

Secured communication InVehicle IDPS

ACS Managed Services
Supporting services that should be built OEM and Tier1 independent

Advanced Threat Intelligence

Fleet SIEM

Incident Response

ACS Pentesting
Security checks by penetration testing on different applications, systems and components to support the security improvement process, using most current hacking techniques.

ACS Development Lifecycle
Integration of security activities throughout the development lifecycle enables timely and risk-based identification, as well as remediation of security vulnerabilities.

Leading questions in automotive risk methodology

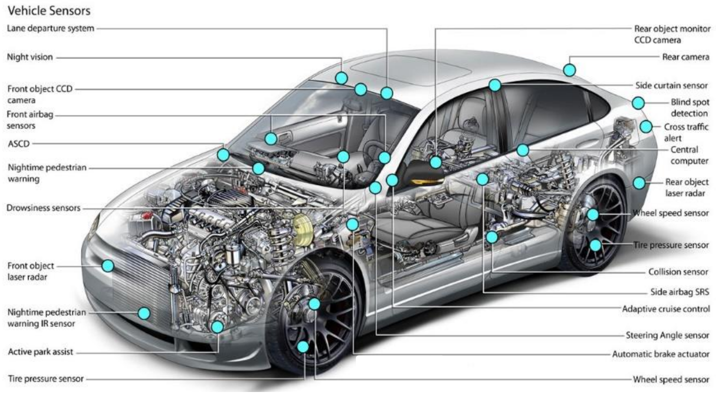
As a basis for the vehicle risk evaluation approach, fundamental definitions and assumptions of risk management can be applied

Cyber Attack[1]

"An **attack, via cyberspace**, targeting an enterprise's use of cyberspace for the **purpose of disrupting, disabling, destroying, or maliciously controlling** a **computing environment / infrastructure**; or destroying the integrity of the data or stealing controlled information."

Questions

- **What kind of attack schemes are relevant in the context of vehicles?**
- **What are the critical infrastructure components and functions in vehicles?**
- **What is the intention of attackers / the purpose of an attack in the context of vehicles?**

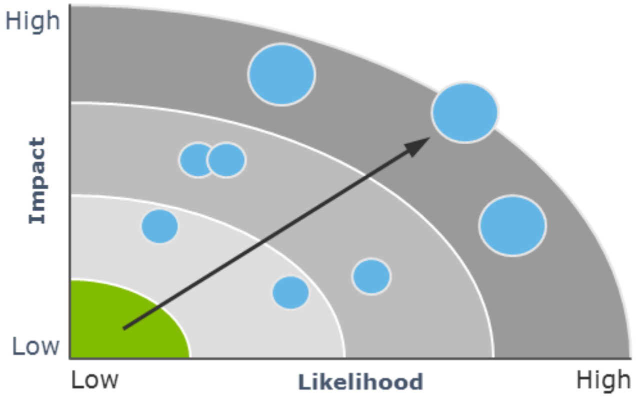


Risk[2]

"The level of **impact** on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a **threat** and the **ease of exploitation** of that threat occurring."

Questions

- **What is the impact of a successful attack in terms of the critical infrastructure components and functions in vehicles?**
- **What are relevant threats in the vehicle environment?**
- **What is the ease of exploitation of attacks in the context of vehicles, considering existing vulnerabilities?**

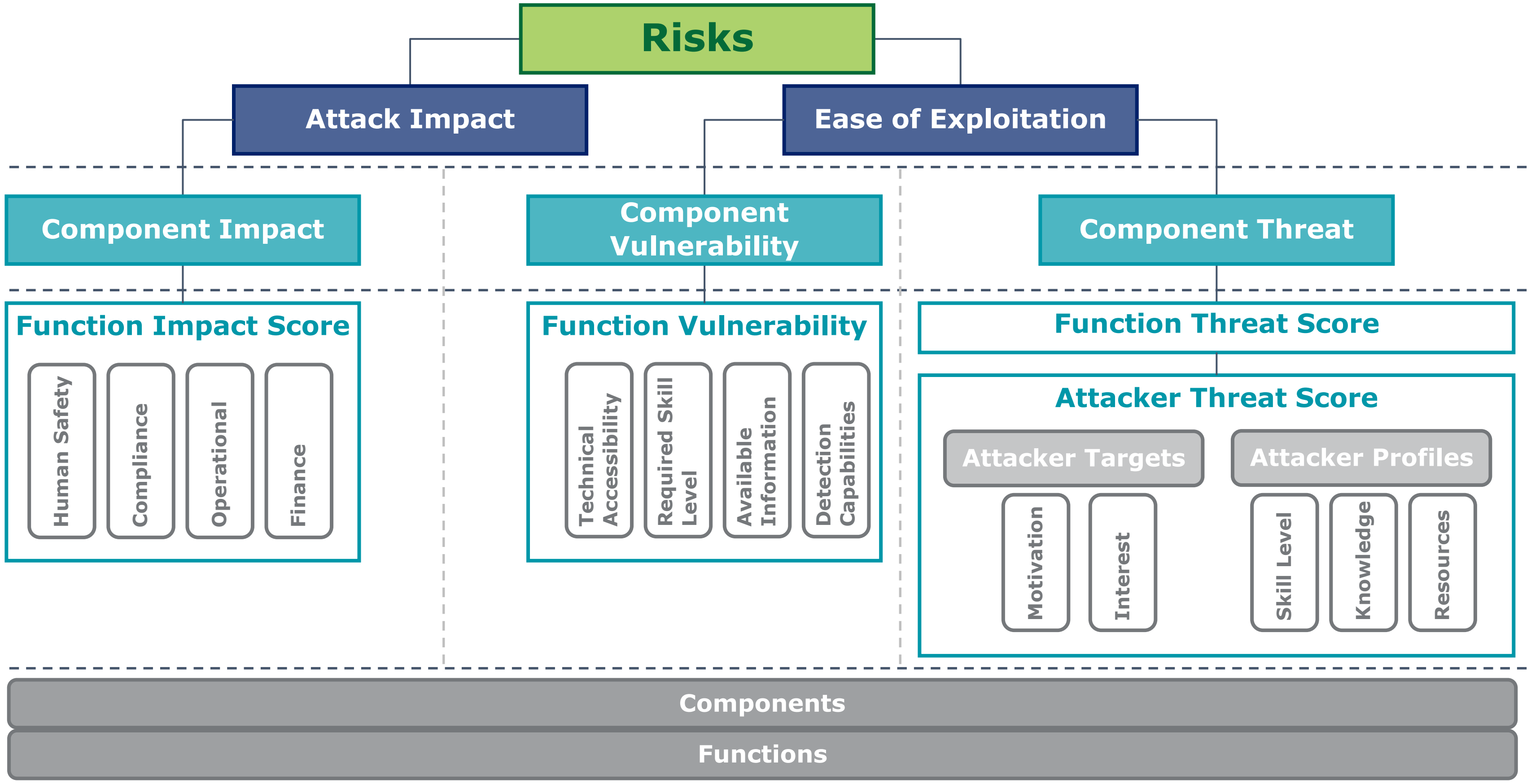


[1] Source: CNSSI-4009 / National Institute of Standards and Technology's (NIST) Glossary of Key Information Security Terms 2013 2nd Revision
[2] Source: SP 800-60 / National Institute of Standards and Technology's (NIST) Glossary of Key Information Security Terms 2013 2nd Revision

Overview on Automotive Risk Methodology

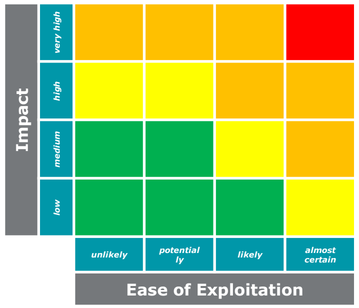
The risk evaluation approach is based on the ease of exploitation and attack impact, both drilled down to meaningful criteria in the automotive environment

The Deloitte approach for an efficient automotive risk assessment is based on the popular and established CVSS and TARA methodology. The combination of a generic and expandable approach (CVSS) with a established approach (TARA) within the automotive industry and our long-standing practical experience ensure an efficient and target-oriented risk methodology.



Risk Evaluation

Key Assumptions



- The overall risk matrix is a product of attack impact and ease of exploitation

- The ease of exploitations a product of component vulnerabilities and threats
- Risk scores for components are a result of the risk scores for the functions related to them

- Function threat is resulting from the highest attacker threat score
- Several attackers might be interested in a function
- Different attackers might have deviating motivation to get control over a function

- Vehicles consist of several components
- Components provide several functions
- Functions contains data interfaces that present possible attack vectors and needs special attention

Example testing steps for a component vulnerability (1/3)

Circuit level assessment

01 Identifying electronic parts used by the component (e.g. MCU/CPU, flash/EEPROM, memory, interface drivers, etc.)

02 Identifying on-board target interfaces (e.g. JTAG, UART, I2C, etc.)

03 Extracting firmware (e.g. by debugging, flash reading, firmware update, etc.)

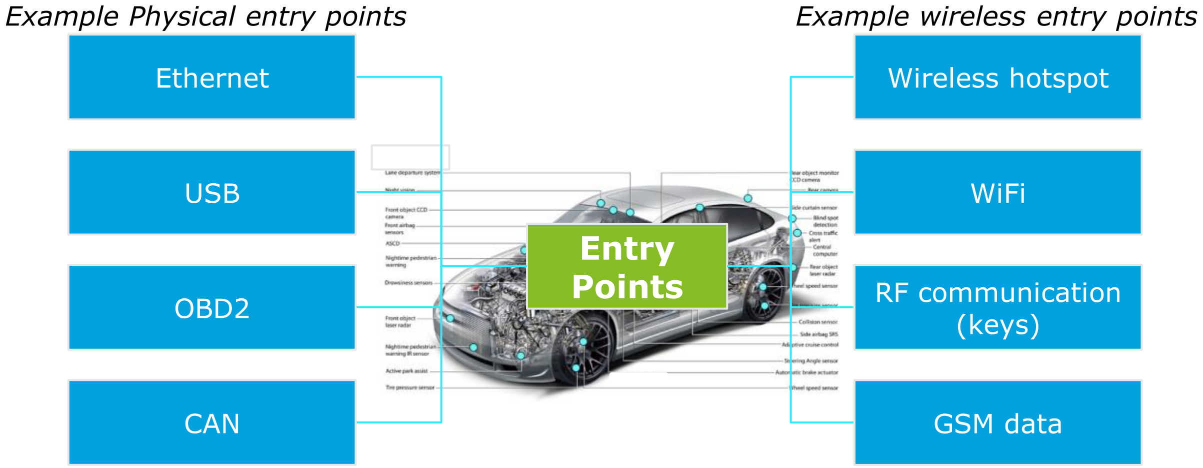
04 Investigating the component design from security perspective

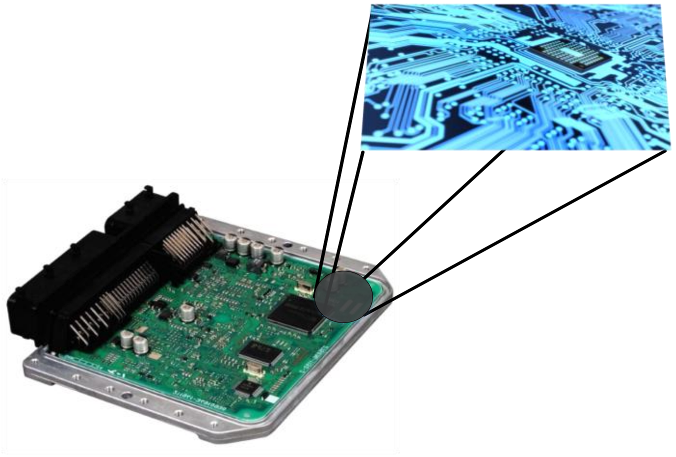
05 Security features of sub components

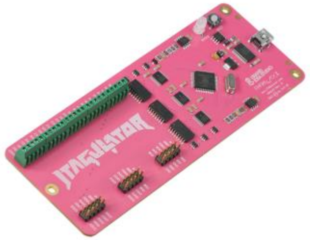
- Secure / authenticated boot
- Debug interfaces
- Location and method of data/code storage

06 Security of signal routing

07 Security of MCU/CPU interfaces







Source: https://www.parallax.com/product/32115

Example testing steps for a component vulnerability (2/3)

Firmware level assessment

Investigating and reverse engineering the firmware, time limited analysis

01 Booting

- authentication / encryption
- programming errors in boot flow

02 Software update

- delivery and protection of update image
- checking authenticity / encryption
- programing errors in checking / flashing flow

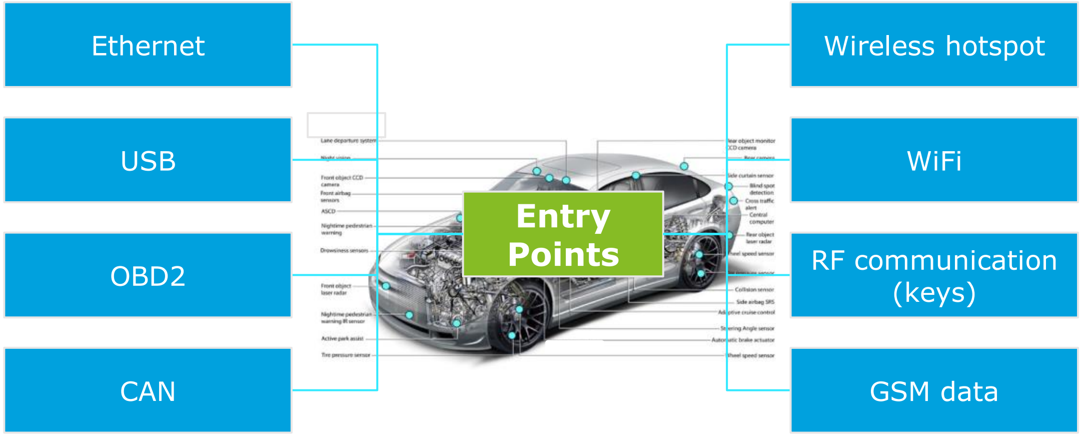
03 Main software / firmware

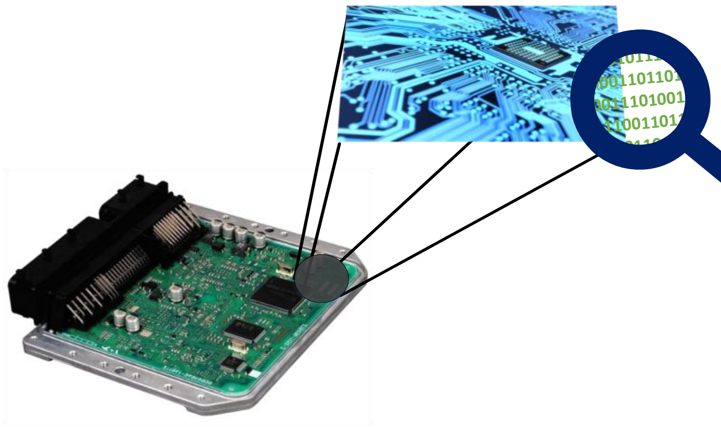
- communication handling
- authentication / encryption
- use of known vulnerable software components
- data storing / handling / user files and input

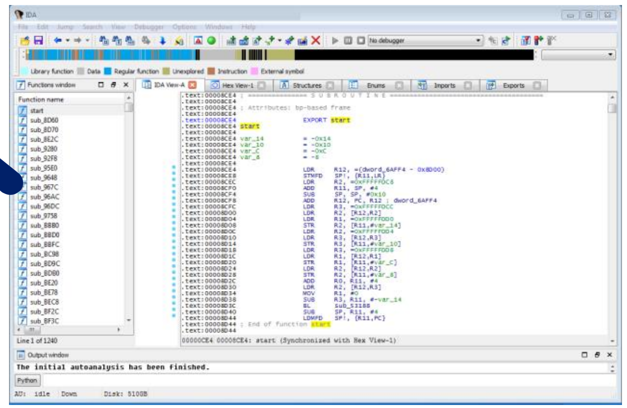
04 Preparing and executing Proof-of-Concept attacks against the revealed weaknesses

Example Physical entry points

Example wireless entry points







IDA Pro for reverse engineering

Example testing steps for a component vulnerability (2/3)

Interface level assessment

01 Identifying the communication channels of a component (e.g. CAN, OABR)

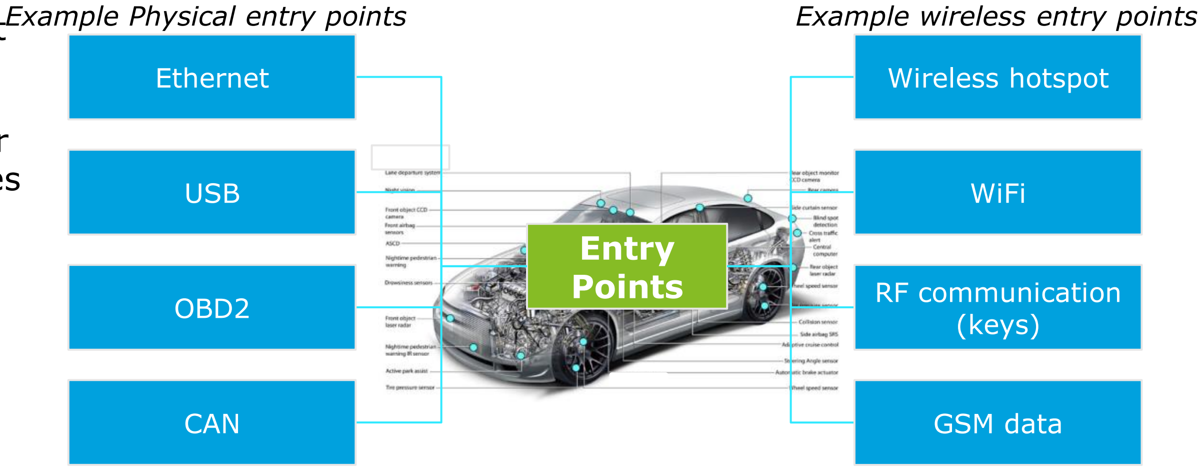
02 Capturing and analyzing of communication started by or targeting the component during various operation modes

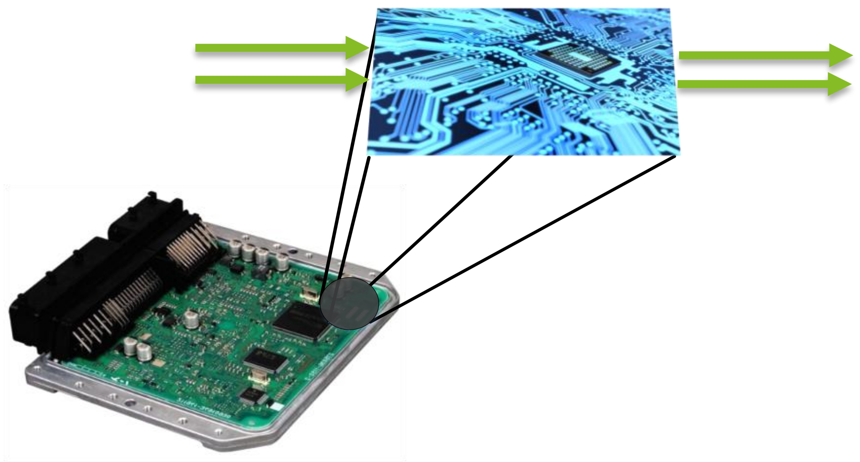
- standard operation (vehicle off, ACC on, engine running, in motion)
- flashing
- coding
- diagnostic

03 Correlating data with specification information (received from OEM or downloaded from internet)

Finding weaknesses

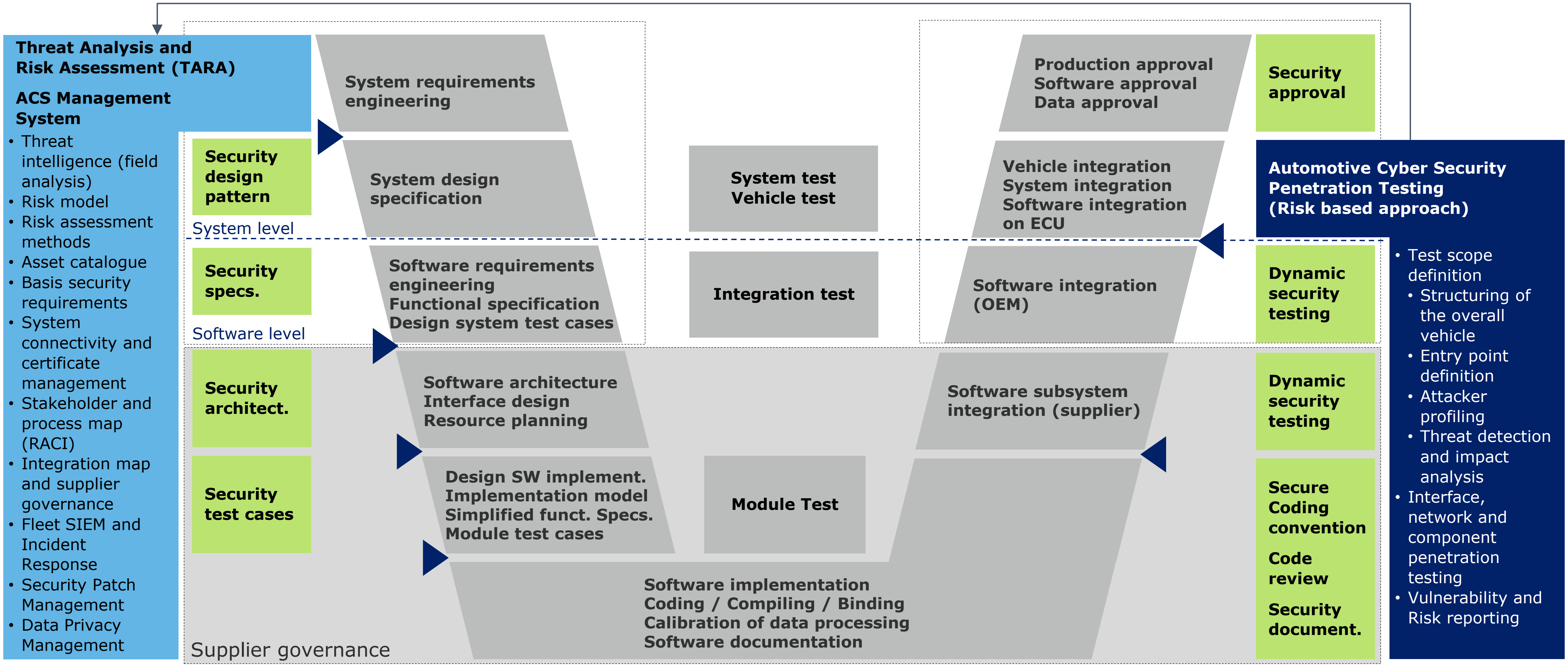
- message manipulation via MitM
- secure access and authentication spoofing / bypassing,
- triggering functions via replaying





Automotive Cyber Security integration in the V-Model

Security modules are aligned with the development methodology to harmonize all activities and quality gates



ACS development activities | System and software development activities | Harmonized software & ACS quality gates