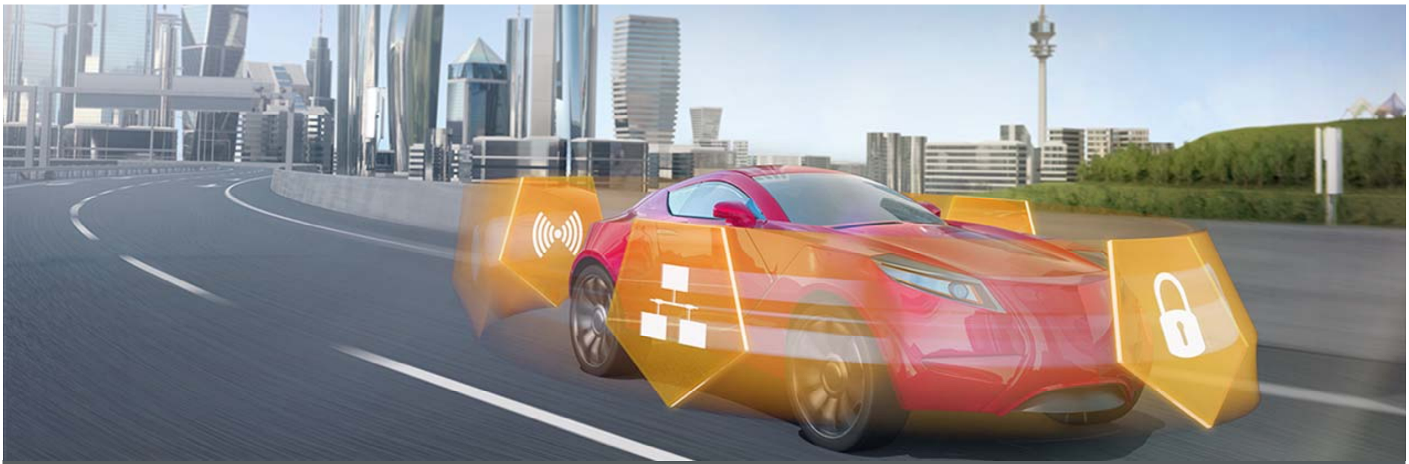
VECTOR



Automotive Cybersecurity Webinar

@VectorVCS

V1.0 | 2019-03-17

VECTOR

Agenda

1.	Welcome
2.	Challenge Cybersecurity
3.	Practical Guidance and Vector Experiences
4.	Case Study
5.	Conclusions and Outlook

VECTOR

Why Vector Consulting Services?

- **Vector Group** is global market leader in automotive software and engineering toolchain with over 2,700 employees
- **Vector Consulting Services** is supporting clients worldwide
  - Product development, IT
  - Trainings, coaching, processes, tools, interim support
  - Cybersecurity, safety, ASPICE, requirements engineering, etc.
  - Agile transformation and change

www.vector.com/consulting

www.vector.com/consulting-career


Automotive


Aerospace


IT & Finance


Digital Transformation


Medical


Transport

VECTOR

Vector Offers the most Complete Portfolio for Security/Safety

Vector Cybersecurity and Safety Solutions

Consulting
- SecurityCheck and SafetyCheck
- TARA
- Security concept
- Code analysis
- PenTesting
- Virtual Security Manager

AUTOSAR Basic Software

HW based Security

Tools
- PLM with PREEvision
- Architecture
- Test
- Diagnosis

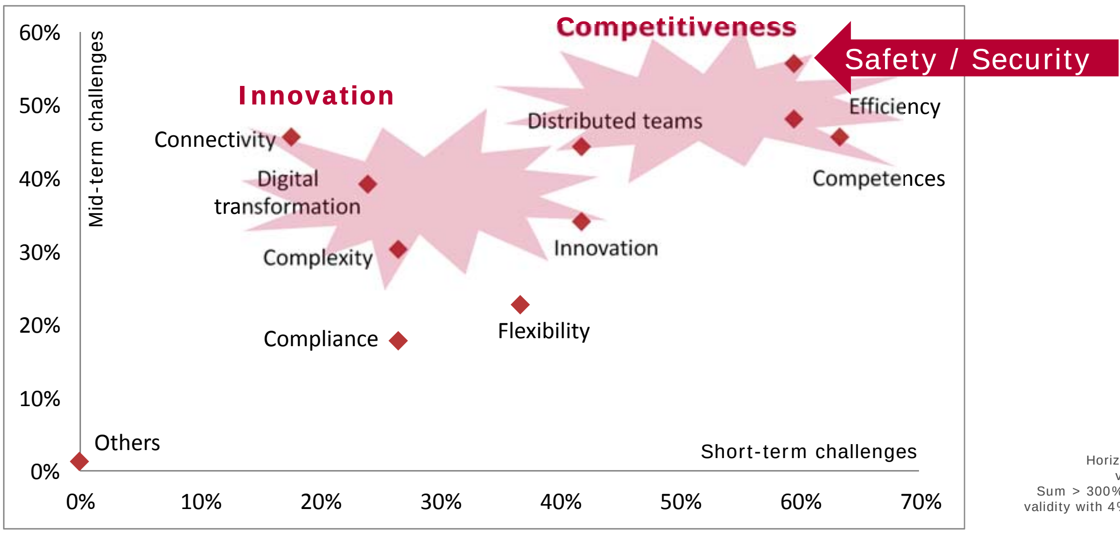
Engineering Services for Safety and Security

www.vector.com/security

Agenda

1. Welcome
2. Challenge Cybersecurity
3. Practical Guidance and Vector Experiences
4. Case Study
5. Conclusions and Outlook

Vector Client Survey 2019: The Fight of Two Forces

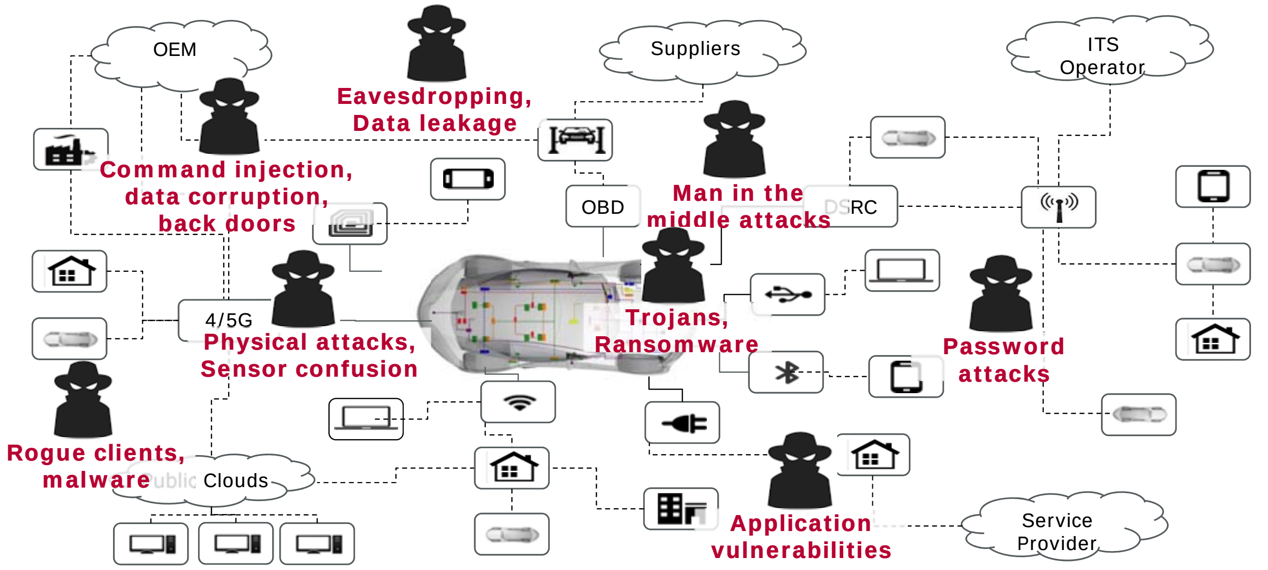


Vector Client Survey 2019.
Details: www.vector.com/trends.
Horizontal axis shows short-term challenges; vertical axis shows mid-term challenges.
Sum > 300% due to 5 answers per question. Strong validity with 4% response rate of 2000 recipients from different industries worldwide.

Vector provides tailored consulting solutions to keep OEM and suppliers competitive:
Efficiency – Quality – Competences

VECTOR

ACES (Autonomy, Connectivity, e-Mobility, Services) ▶ **Cyberattacks** ▶ **Hazards**



Automotive cybersecurity will be the major liability risk in the future.
Average security gap is detected in 70% of cases by a third party – and will be exploited.

VECTOR

Combined Safety and Security Need Holistic Systems Engineering

Functional Safety

- Goal: Protect health
- Risk: External hazards
- Governance: ISO 26262 etc.
- Methods:
  - HARA, FTA, FMEA, ...
  - Fail operational, ...
  - Redundancy, ...

Cybersecurity

- Goal: Protect assets
- Risk: Internal threats
- Governance: ISO 21434 etc.
- Methods:
  - TARA, Def. Coding...
  - Cryptography, ID/IP, ...
  - Key management, ...

Privacy

- Goal: Protect personality
- Risk: Data threats
- Governance: ISO 27001 etc.
- Methods:
  - TARA,...
  - Cryptography,...
  - Explicit consent, ...

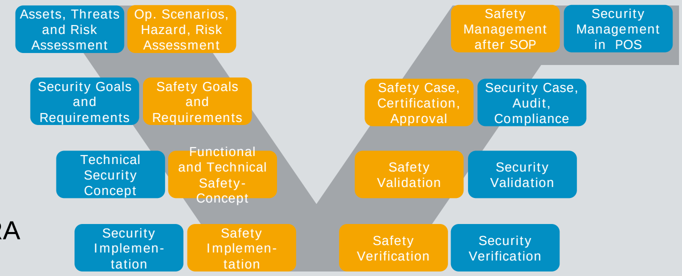
Liability ➔ Risk management ➔ Holistic systems engineering

Standards Demand Risk-Oriented Approach

Functional Safety
(IEC 61508, ISO 26262, ISO 21448)

- Hazards and risk mitigation
- Increasing focus on SOTIF and compliance
- Safety engineering and culture

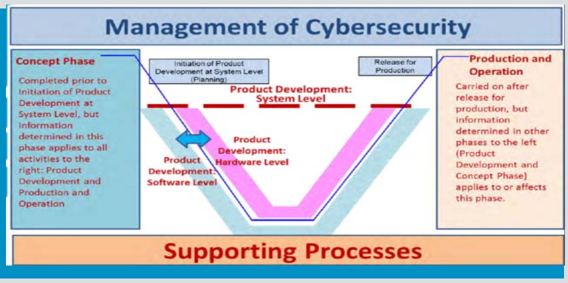
ISO 26262 ed.2 refers to shared methods, e.g. TARA



+ Security
(ISO 27001, ISO 15408, ISO 21434, SAE J3061)

- Threat and risk mitigation
- Abuse, misuse, confuse cases
- Security engineering

Security and Safety are interacting
and demand holistic systems engineering



For (re) liable and efficient ramp-up connect security to safety governance

Standard ISO 21434: Automotive Cybersecurity

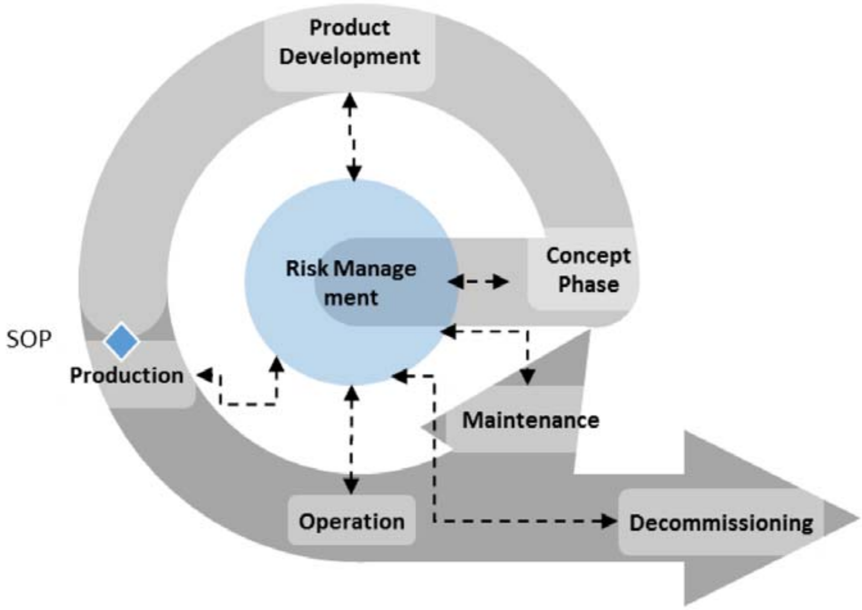
Planning

- Kickoff - 17.10.2016
- Currently: Committee Draft
- Release: 2020 (most probably)

Approach

Risk-oriented approach following the Vector method for the whole lifecycle of the product, i.e.:

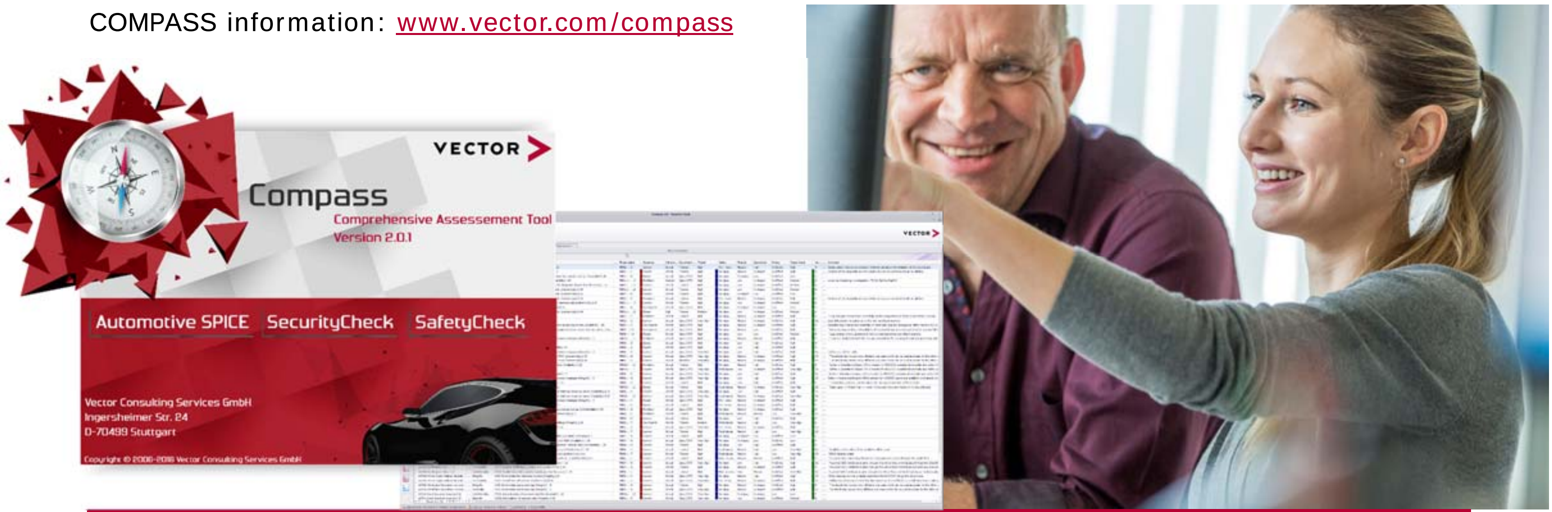
- Concept/design phase
- Product development
- Production (roll out)
- Operation
- Decommissioning (roll over)



Focus on governance. ISO 21434 does NOT prescribe any technology or solutions

Vector SecurityCheck with COMPASS

COMPASS information: www.vector.com/compass



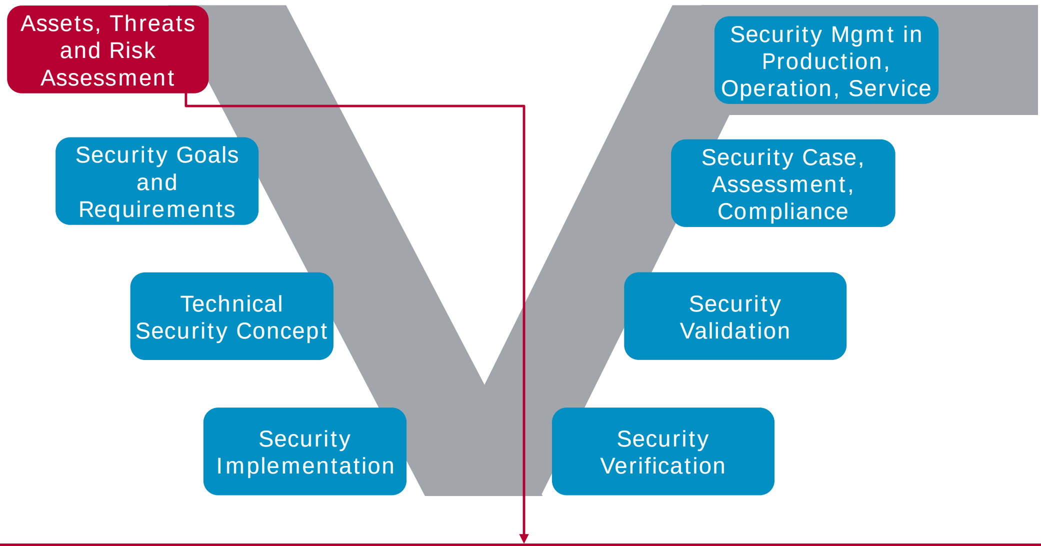
Vector SecurityCheck facilitates

- **Systematic risk assessment and mitigation**
- **Traceability and Governance** with auditable risk and measure list
- **Heuristic checklists** with continuously updated threats and mitigation

Agenda

1. Welcome
2. Challenge Cybersecurity
3. Practical Guidance and Vector Experiences
4. Case Study
5. Conclusions and Outlook

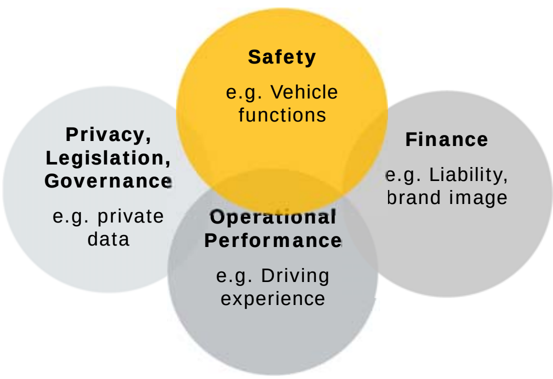
Security Engineering Starts with Systematic TARA



Threat & Risk Analysis:
1) Identify **assets** of value and **threats** caused by potential attackers.
2) Rate **impact** and **likelihood** of attacks against assets to define their **security level**.

Concept of Combined Threat/Hazard Analysis and Risk Assessment

Specific automotive asset categories



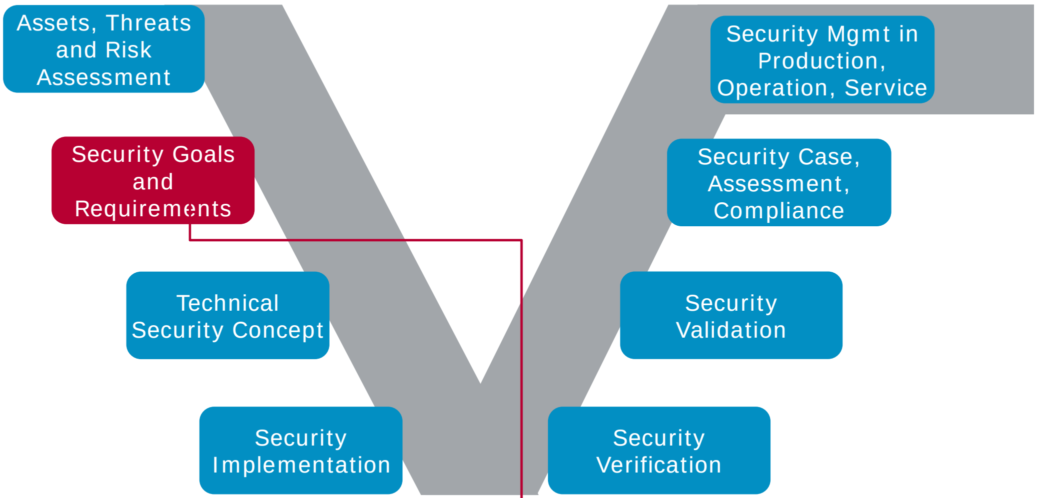
Example: Identified threats

- **Safety**
  - Injuries because of malfunctioning Passive Entry
- **Financial**
  - Extra cost due to call-back and law-suits
- **Operational Performance**
  - Car cannot be started, doors cannot be opened
- **Privacy / Legislation**
  - Theft of personal data

Consider specific automotive assets derived from
CIAAG (Confidentiality, Integrity, Authenticity, Availability, Governance) scheme

VECTOR

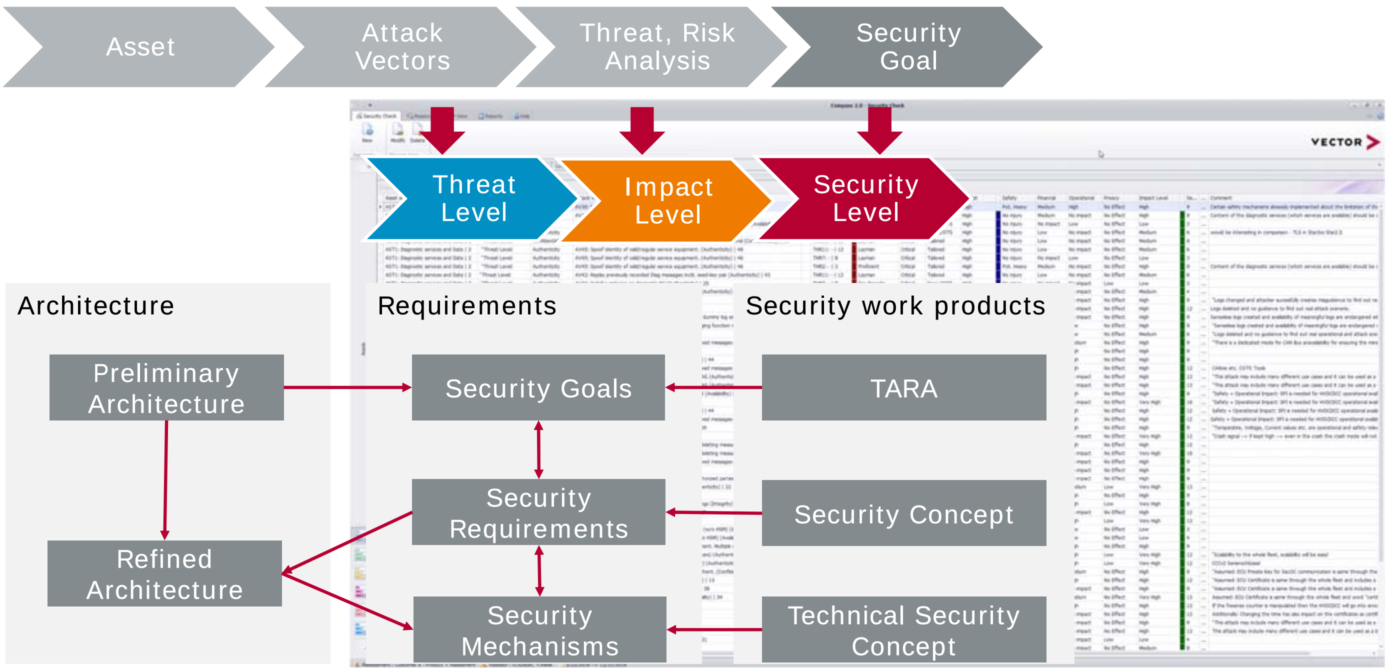
Security Engineering



SecurityCheck & Requirements:
1) **Derivation of Security Goals from threats**
2) Refinement of Security Goals to Functional Security Requirements (FSR)

VECTOR

Apply a Systematic Threat and Risk Assessment



VECTOR

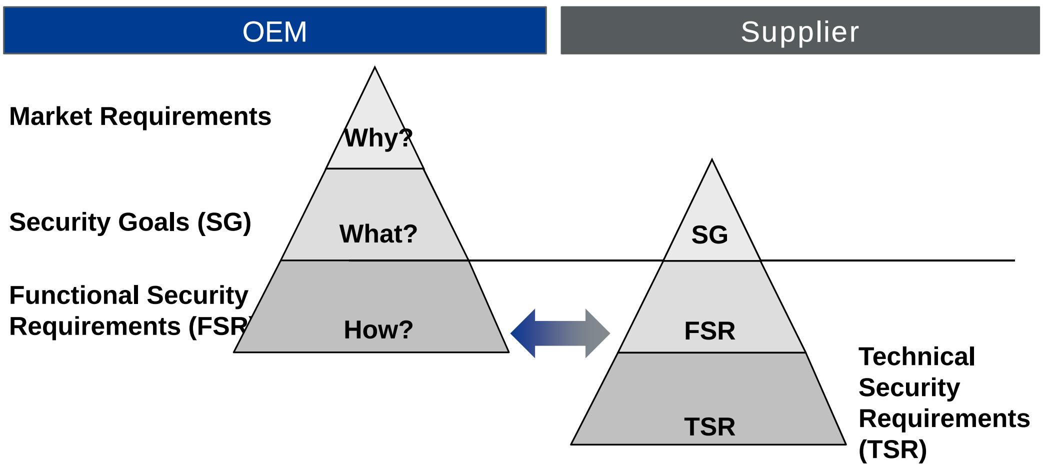
Determine Necessary Security Level with TARA Results

Asset ID	Asset / Vehicle Function	CIAAG	Attack vector	Potential effect of attack	Threat ID	Threat	Expertise	Expertise numerical	Window of Opportunity	WoO numerical	Equipment / Effort	Effort numerical	Threat numerical	Threat level (high=4; low=1)	Safety	Financial	Operational	Privacy	Impact Level	SGID
Ast 01	Safety-Mechanisms	Avail	Availability: Attacker floods CAN-Bus and thereby tries to disable vehicle primary functions.	Attacker disables engine control during an overtaking maneuver if system can impact safety-critical functions.	Tht-1	Not further considered on advice of client because the HU is rated QM with respect to ISO 26262.	Layman	0	Critical	0	Standard	0	0	4	No injury	No impact	No impact	No effect	No impact	n/a

Security Level (SL)		Impact Level (IL)				
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

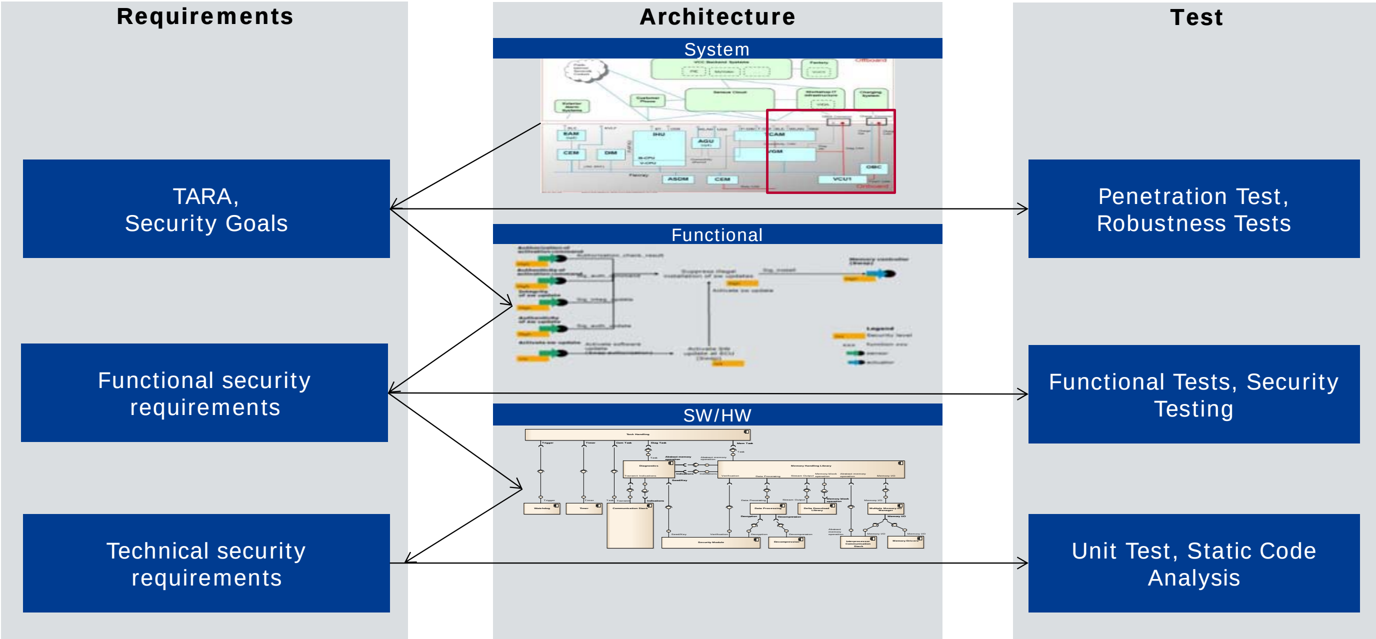
VECTOR

Security Requirements Engineering



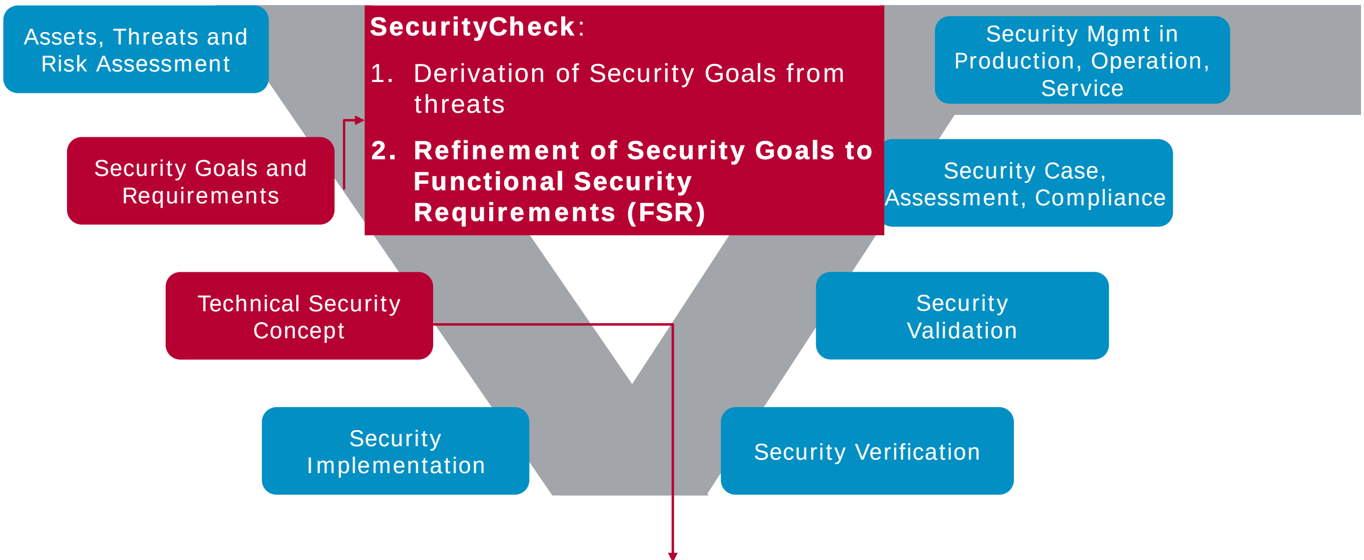
"Security out of context" does not work. Establish OEM-supplier interface, similar to DIA.
OEM: system security concept, key management
Tier 1: security concept, assumptions to OEM

Security Requirements and Traceability



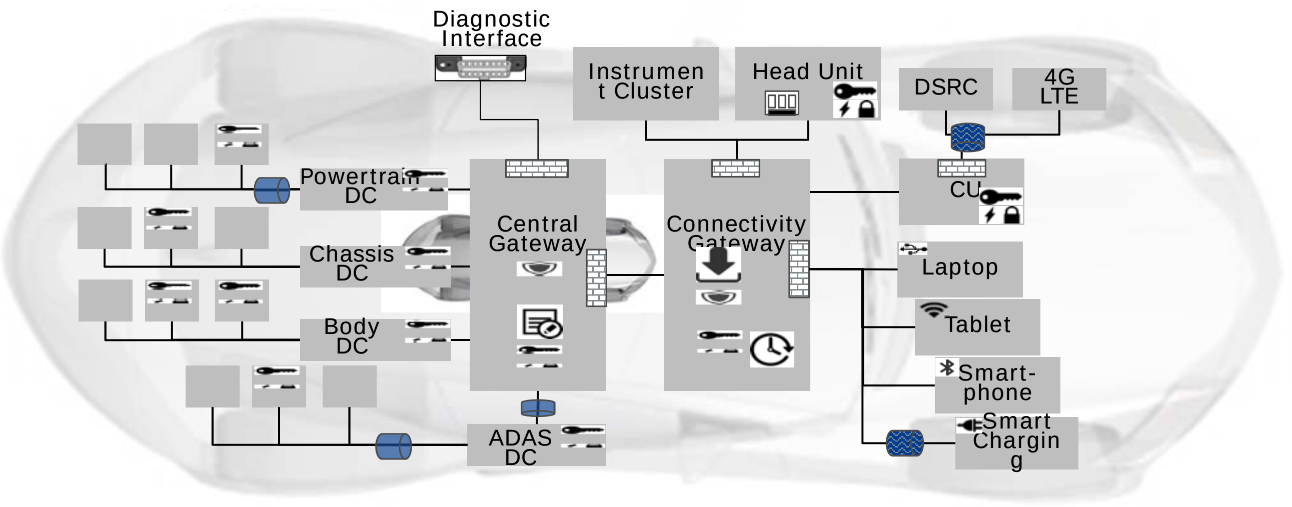
Practical Guidance and Vector Experiences

Security Engineering



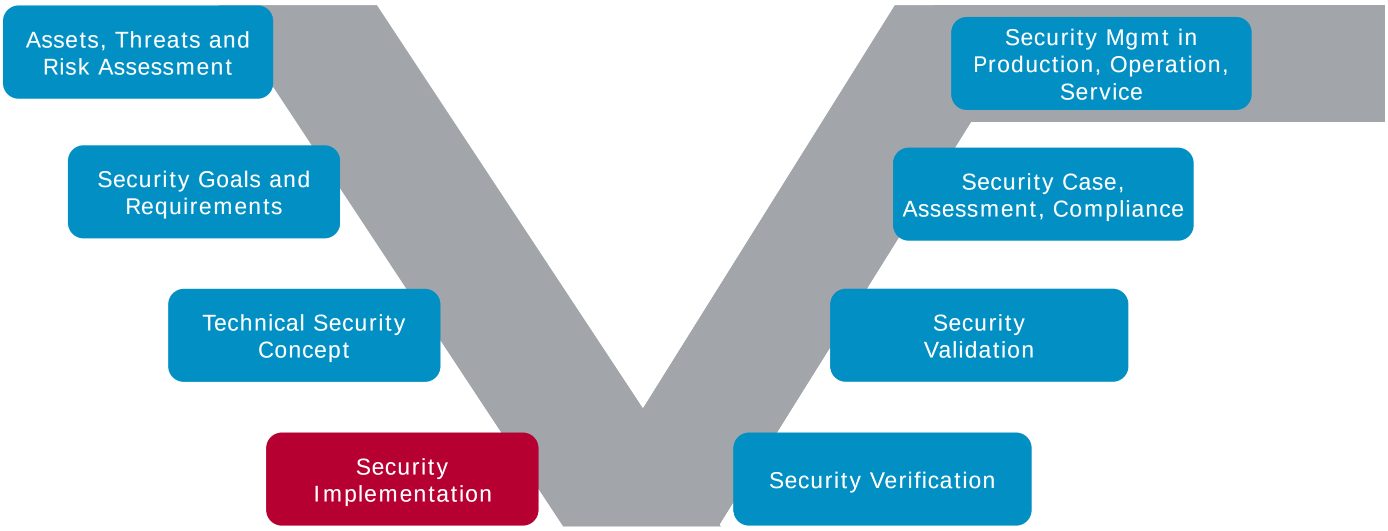
Technical Security Concept:
1) Refinement of system architecture to technical component level (SW/HW components)
2) **Technical Security Requirements (TSeR)** are refined out of the Security Concept

Security Mechanisms allocated in Reference Architecture



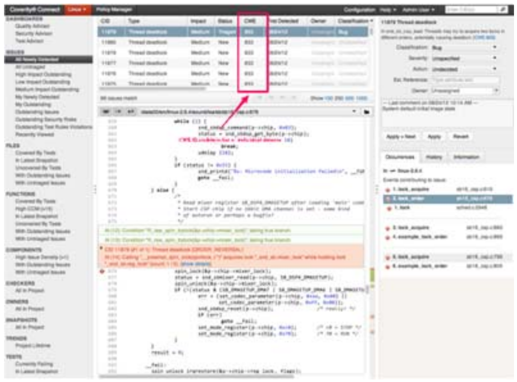
Firewall
Key Infrastructure
Crypto Primitives
Monitoring / Logging
Hypervisor
ID / IP
Secure On Board Comm.
Secure Off Board Comm.
Download Manager
Secure Flash/Boot
Secure Synchronized Time Manager

Security Engineering



VECTOR

Security by Design: Secure Coding



- **Goal**
  - **Avoid design and code errors which can lead to security exploits**
- Approach
  - **Use a hardened OS with secure partitioning**
    Avoid embedded Linux due to its complexity and rapid change and thus many security gaps, (e.g. NULL function pointer dereferences, which allow hackers to inject executable code).
  - **Deploy secure boot strategy**
    Starting with first-stage ROM loader with a pre-burned cryptographic key, the next levels are verified before executing to ensure authenticity of each component of the boot
  - **Apply rigorous static code analysis**
    Tools like Coverity, Klocwork or Bauhaus allow security checks, such as NULL pointer dereferences, memory access beyond allocated area, reads of uninitialized objects, buffer and array underflows, resource leaks etc.
  - **Use modified condition / decision coverage (MC / DC)**
    Detect backdoors

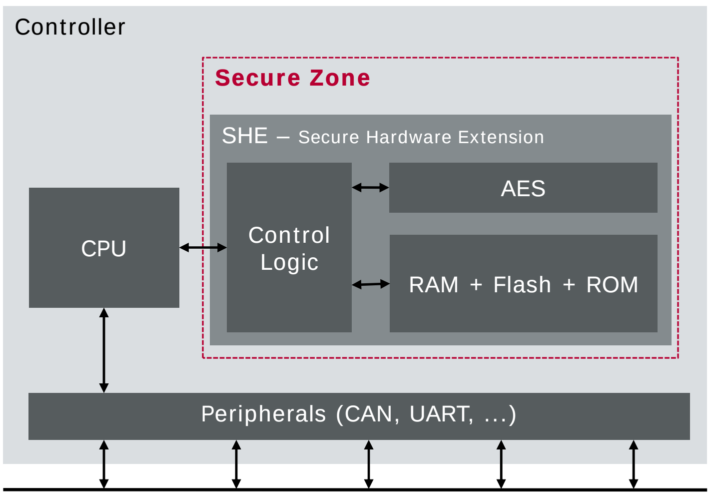
VECTOR

Security by Design: Hardware-Based Security

Goal:
Separate security privileged functions from the applications of the ECU by hardware

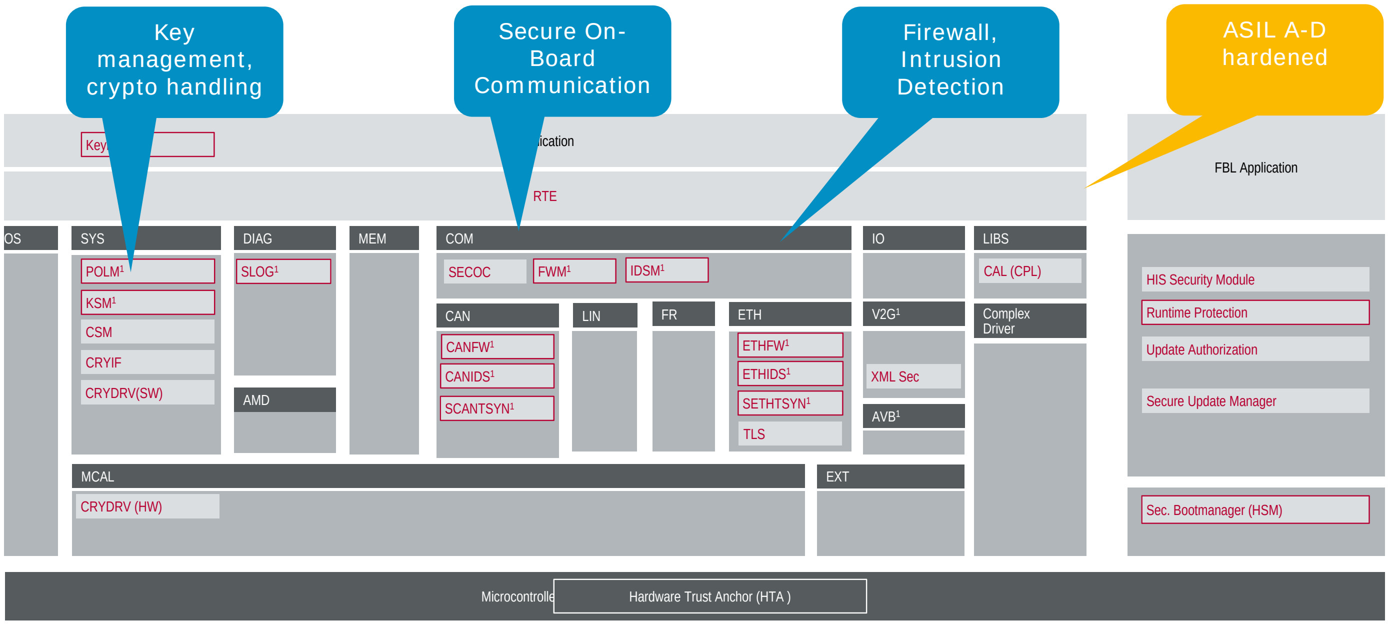
Approach:
Secure Hardware Extension

- On-chip extension to microcontroller
- Secure Boot directly triggered by hardware upon start
- Pre-shared cryptographic key
- Memory for secure storage of (cryptographic) data
- Hardware extension for cryptographic primitives



VECTOR

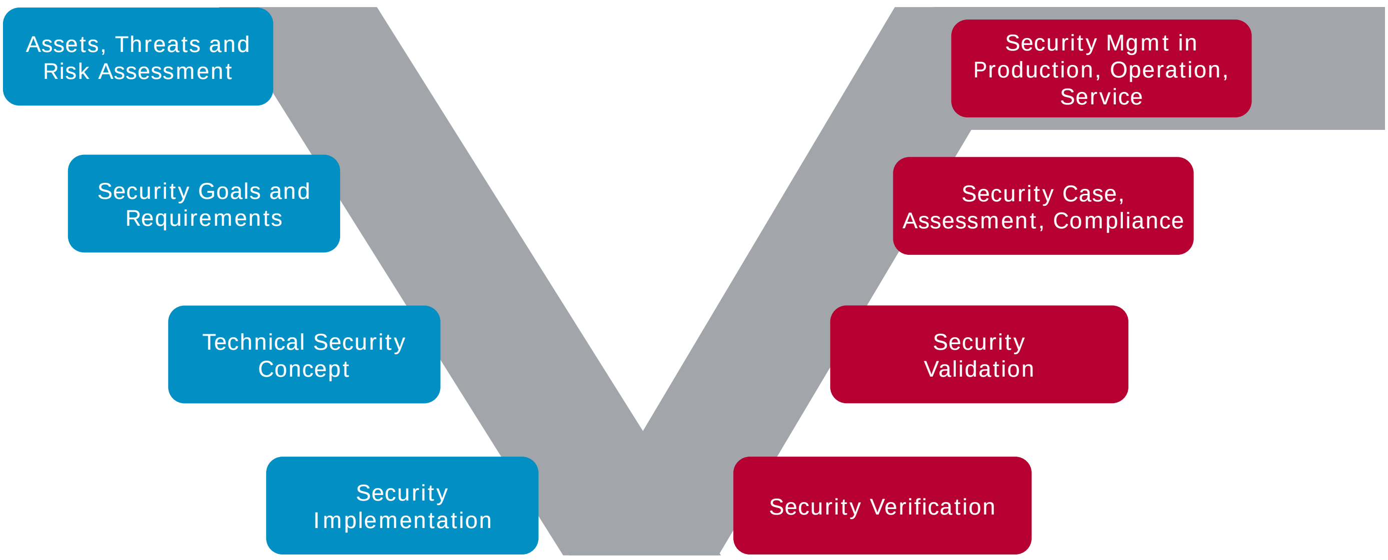
Safety and Security by Design: MICROSAR 4.3ff and FBL



[1] Extensions for AUTOSAR

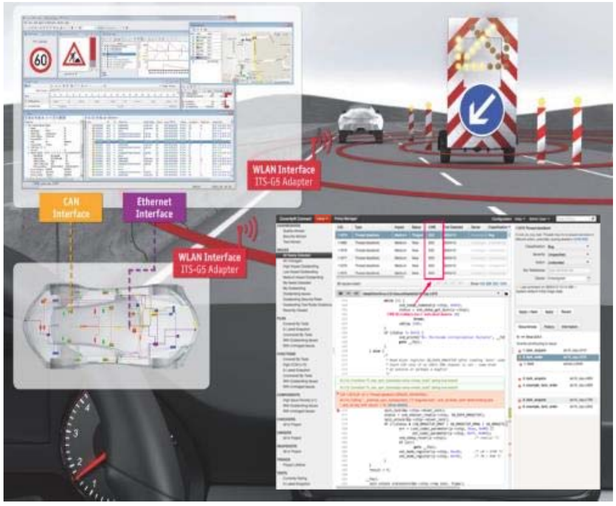
VECTOR

Security Engineering



Safety and Security by Design: Implementation, Verification and Validation

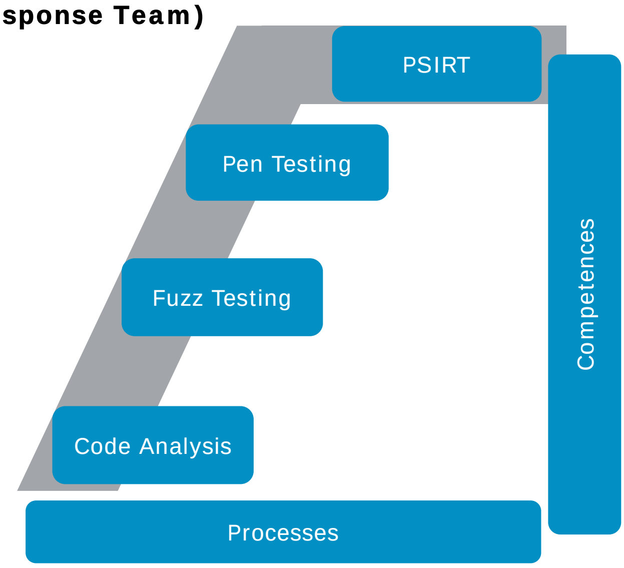
- **Design**
  - Defensive coding, e.g. memory allocation, avoid injectable code, least privileges
  - Selected programming rules such as MISRA-C, CERT
  - High cryptographic strength in line with performance needs
  - Key management and HW-based security
  - Awareness and governance towards social engineering
- **V&V Methods and Tools**
  - Static / dynamic code analyzer
  - Unit test with focused coverage, e.g. MCDC
  - Interface scanner, layered fuzzing tester, encryption cracker, vulnerability scanner
  - Penetration testing, starting with TARA concept



Classic coverage test is not sufficient anymore. Test for the known – and for the unknown.
Ensure automatic regression tests are running with each delivery.

Test Methodology

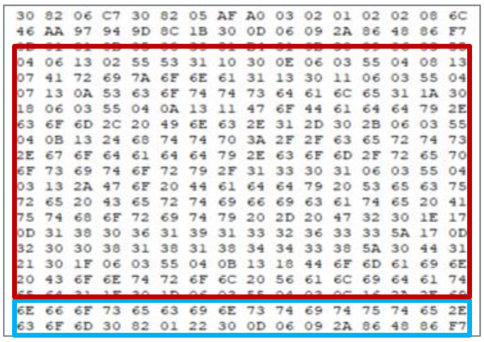
- **PSIRT Collaboration (Product Security Incident Response Team)**
  - Handover, task assignments and distribution
- **Pen Testing**
  - Vector Grey-Box PenTest based on TARA
  - DoS, Replay, Mutant/Generated Messages
  - Development of misuse, abuse and confuse cases
- **Fuzz Testing**
  - Fuzzing the Application SW, Grey box analysis
  - Brute-force CAN Fuzzer
- **Code Analysis**
  - CQA, Coverage (e.g., VectorCAST)
  - Design, architecture, (opt) defect analysis
- **Processes**
  - Testing, development, customer care
- **Competences**
  - Inhouse capabilities, person/teams etc.



Vector Grey-Box PenTesting

Asset select	...	CIAAG	Attack Vector select	...	Threat select	Expertise	Window...	Equipment ...	Threat
AST16: Bootloader Software | 17	...	Integrity	AV1: Compromise bootloader SW (Integrity) | 2		THR6: - | 7	Layman	Critical	Tailored	High
AST17: Flash and RAM | 18	...	Confidentiality	AV31: Physical access to the board and Access to the HW details (Confidentiality) | 32		THR3: - | 4	Layman	Critical	Standard	Very High

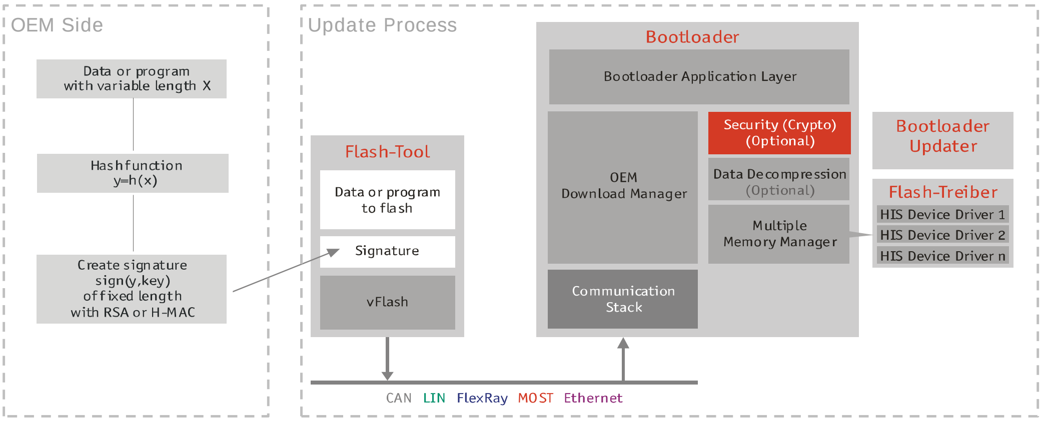
By taking our TARA as input, We put our focus into the Flash asset and with physical access to the board we initiate an attack to read the contents of the flash during runtime



After analyzing the data dump we got from the flash we can read the root certificate and the ECU key in clear text

Rather than brute force PenTest, we use in our test labs grey-box PenTesting based on TARA, misuse cases and broad Vector networking competences

Deploy Security for Service and Operations: OTA



Ensure that each deployment satisfies security requirements

- Governance: Safety/security documentation is updated and validated
- Data encryption: Protection of intellectual property by encryption
- Authorization: Protection against unauthorized ECU access
- Validation: Safeguarding of data integrity in the flash memory
- Authentication: Verification of authenticity through signature methods

Agenda

1. Welcome
2. Challenge Cybersecurity
3. Practical Guidance and Vector Experiences
4. Case Study
5. Conclusions and Outlook

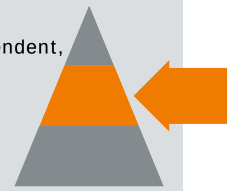
Advanced Driver Assistance System – Overview

ADAS Basic Functions (simplified use cases)

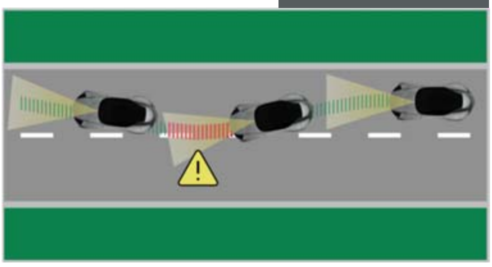
- Warn driver when vehicle is getting too close to preceding vehicle
- Warn driver if vehicle is leaving the driving lane
- Perform action such as counter-steering or braking to mitigate risk of accident

Level of Analysis

- ADAS function is defined
- Function level (implementation-independent, function-focused)
- Probably, other risk assessment stages before or after this step

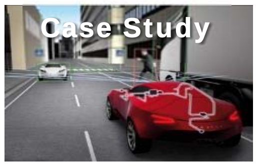


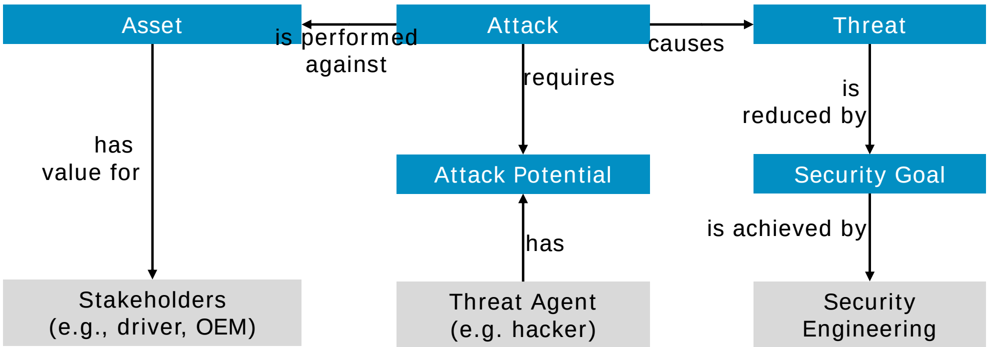
Scenario



System Architecture

ADAS – Step 1: Assets





Step 1: Agree assets to be protected

- A1: Network messages received or send by ADAS
- A2: ADAS Software, including safety mechanisms
- A3: Security keys
- A4: Driving history and recorded data

ADAS – Step 2: Threat and Risk Analysis (TARA)

Assessment

- Assess attack potential (Vector SecurityCheck, STRIDE, etc.)
  consider expertise required, window of opportunity, equipment required
- Use external (!) expert judgment
- Identify attacks without taking into account potential security mechanisms

Attacks

- A1-AT1: Messages for braking are blocked.
- A1-AT2: Messages are replayed.
- A2-AT1: Safety mechanism, no lane keeping during manual take-over, compromised and not working.

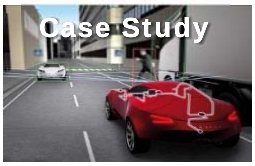
Threats

- A1-AT1-T1: Vehicle does not brake although the driver presses the braking pedal.
  (Possible injuries in case failure of braking leads to an accident.)
- A1-AT2-T1: Display of warning messages with high frequency and without reason.
  (Replay of warning messages at critical situations can lead to erroneous behavior and massive driver distraction.)
- A2-AT1-T1: Lane is kept during manual take-over.
  (Heavy injuries because of failed take-over.)

A ... Asset
AT ... Asset Attack
T ... Threat

Case Study

ADAS – Step 3: Security Goals



Asset / Function	Attack	Threat	Threat Level	Impact Level	Risk
Messages received (e.g. steering angle, lane information) or send by the ADAS-System (warning message, counter steering request)	Confidentiality: Attacker **overhears messages** including risky overtaking maneuvers.	Information about driver's behavior is forwarded to insurance agency that **increases insurance fees** for the driver.	Medium	Very High	High
Messages received (e.g. steering angle, lane information) or send by the ADAS-System (warning message, counter steering request)	Authenticity: **Messages are replayed**.	**Display of warning messages with high frequency and without reason.**	Medium	Medium	Medium
Software of the ADAS-System (including safety mechanisms)	Availability: **Safety mechanism**, *no lane keeping during manual take-over*, compromised and not working.	Vehicle stays on opposite lane during manual take-over although driver wants to return to his lane.	Medium	Very High	High

Case Study

ADAS – Step 3: Security Requirements

Security goals are high level security requirements

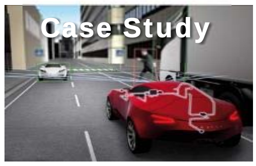
Security Goals

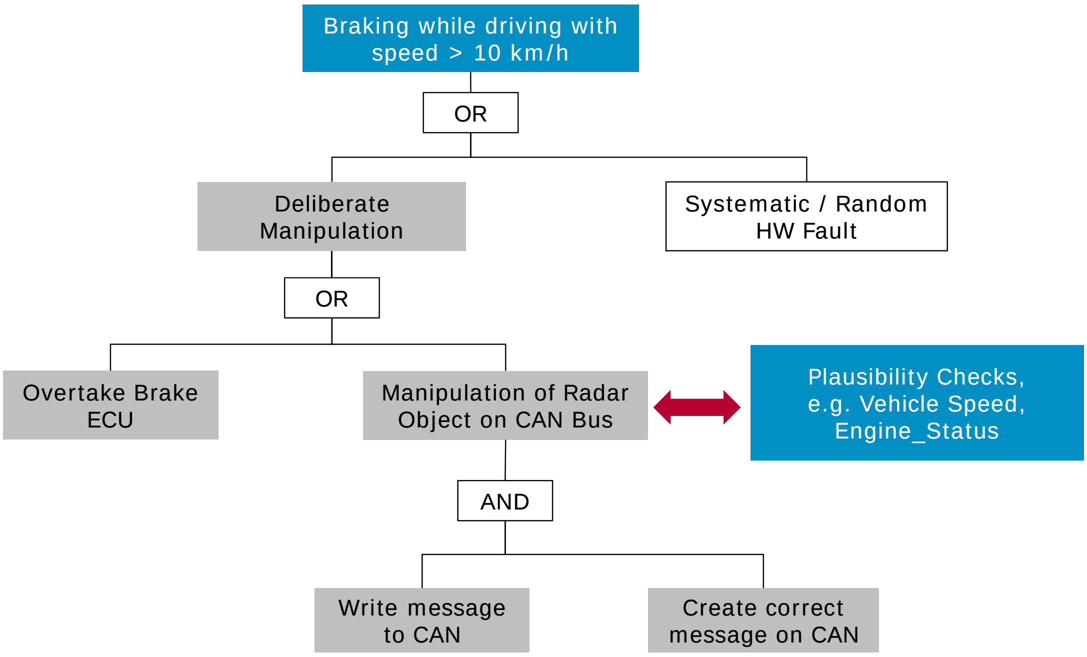
Functional Security Requirements

Technical Security Requirements

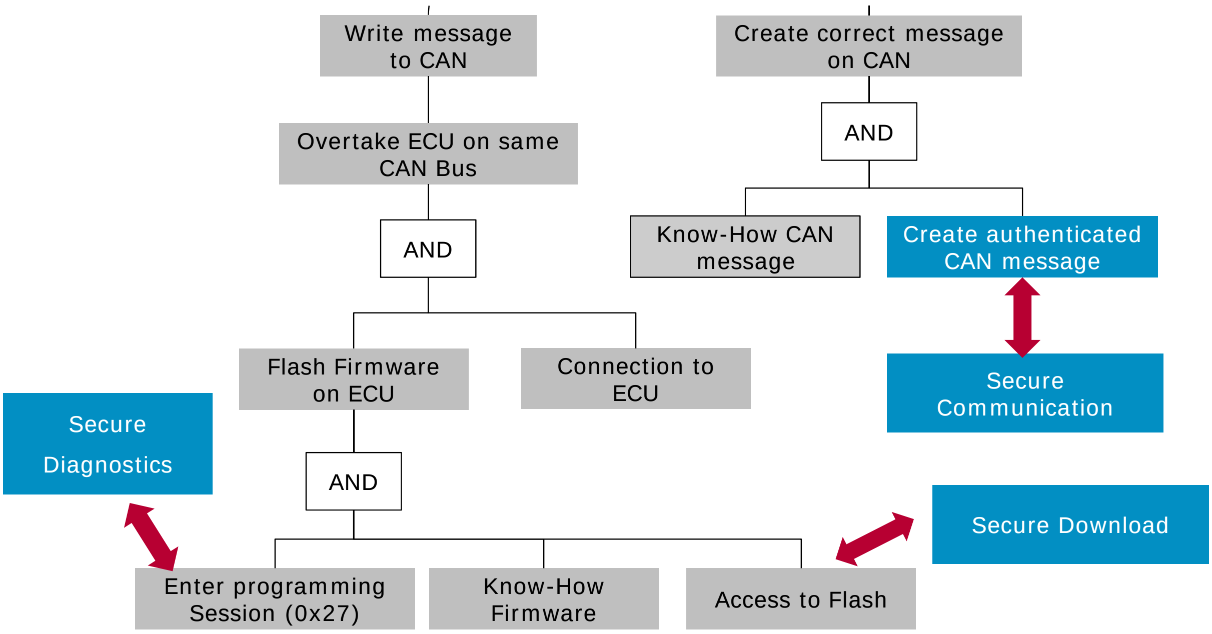
- A1-AT1-T1-SG1: The system shall prevent manipulation of the messages send by the driver assistance system
- The integrity of communication between driver assistance and sensors shall be ensured
- The MAC shall be calculated by a SHE-compliant hardware trust anchor using the algorithm RSA2048
- The MAC shall be truncated after x byte

ADAS – Step 4: Security Mechanisms (1/3)

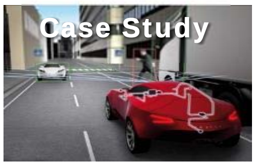




ADAS – Step 4: Security Mechanisms (2/3)



ADAS – Step 4: Security Mechanisms (3/3)



Secure Diagnostics

- No Keys on Diagnostic Tool
- Secure Access with organizational access management and guidelines

Secure Internal Communication

- Efficient encryption and message authentication (e.g., H-MAC)
- Rationality Checks (e.g., Vehicle speed < 10 km/h)

Secure Download

- PKI with RSA-2048
- Closing Programming Interface

Secure Implementation

(e.g. Standard Architecture, Design Rules, Coding Guidelines, Process Rules, etc)

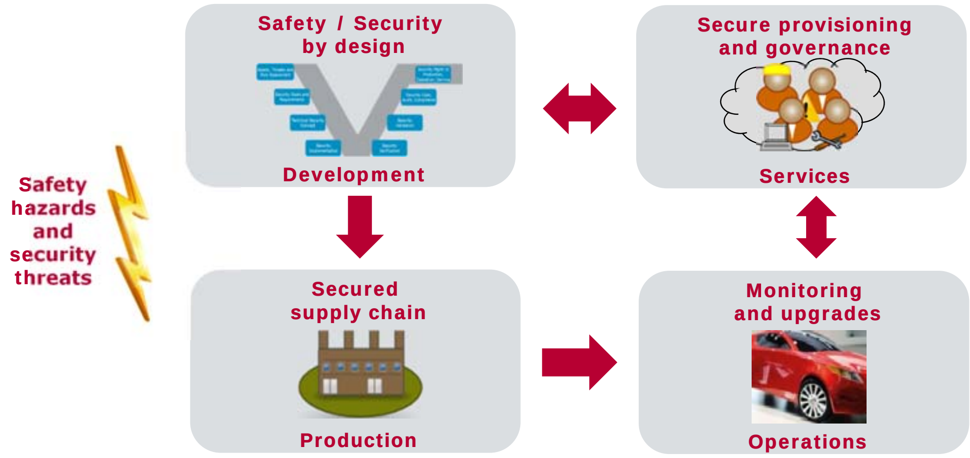
Reduce likelihood of attack

Resulting Risk		Consequence				
		very low	low	medium	high	very high
Likelihood	very high	medium	high	high	very high	very high
	high	low	medium	high	high	very high
	medium	low	low	medium	high	high
	low	very low	low	low	medium	high
	very low	very low	very low	low	low	medium

Agenda

1. Welcome
2. Challenge Cybersecurity
3. Practical Guidance and Vector Experiences
4. Case Study
5. Conclusions and Outlook

Safety and Security Must Cover the Entire Life-Cycle



Needs for safety and security along the life-cycle:

- Systems and service engineering methods for embedded and IT
- Scalable techniques for design, upgrades, regressions, services
- Multiple modes of operation (normal, attack, emergency, etc.)

Value - Supporting you in choosing the right technique

Security Techniques	Cost	Benefit
Quick Wins		
Vector SafetyCheck and Vector SecurityCheck for risk assessment and implementation guidance	Low	Medium
Virtual Security Manager for fast ramp-up and consistency	Medium	High
Safety and Security Training and compliance audits	Low	High
Technology		
IDS/IPS, Firewall with adjusted policies	Medium	Medium
Secure boot, encrypted communication, storage	High	High
Secure run-time (e.g. CFI, DFI, MACs)	High	High
Process and Governance		
Development for safety and security	Medium	High
Defensive and robust design, static analysis	Medium	High
Test strategy, e.g. Fuzz Testing, Penetration Testing etc.	Medium	High
Secure Key Management	High	Medium
Security task force and response team (internal or virtual)	Medium	High

Grow Your Competences in Risk-Oriented Development

COMPASS information: www.vector.com/compass

Trainings

- Open trainings: www.vector.com/consulting-training
- Worldwide in-house trainings tailored to your needs
- Automotive Cybersecurity: www.vector.com/training-security
- Functional Safety: www.vector.com/training-safety

Webinars and Podcasts

- Further webinars and recordings
  www.vector.com/webinar-security
  www.vector.com/webinar-safety

Free white papers etc.

- www.vector.com/media-consulting

Vector Cybersecurity Symposium 2019

- **Date**
  - 3. April 2019
- **Event location**
  - Stuttgart, Germany
  - Free registration: https://consulting.vector.com/vc_events_detail_en,,1695056,detail.html
- **Topics**
  - Experiences in security projects with cybersecurity at OEMs and TIER1s
  - Interaction between functional safety and cybersecurity
  - COMPASS practical demo
  - Trends and guidance: PenTesting, test, cryptography and security standards
  - Networking, exhibition and discussion with Vector product specialists

Thank you for your attention.
For more information please contact us.

Passion. Partner. Value.

Vector Consulting Services

@VectorVCS

www.vector.com/consulting
consulting-info@vector.com
Phone: +49-711-80670-1520