1. Welcome

2. Challenge Cybersecurity

3. Practical Guidance and Vector Experiences

4. Case Study

5. Conclusions and Outlook
Welcome

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](http://www.vector.com/consulting)
[www.vector.com/consulting-career](http://www.vector.com/consulting-career)

---

Welcome

**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

- Tools
  - PLM with PREEvision
  - Architecture
  - Test
  - Diagnosis

- HW based Security

**Engineering Services for Safety and Security**

[www.vector.com/security](http://www.vector.com/security)
Challenge Cybersecurity

Vector Client Survey 2019: The Fight of Two Forces

Innovation
- Connectivity
- Digital transformation
- Complexity
- Compliance
- Innovation
- Distributed teams
- Efficiency
- Competences
- Safety / Security
- Flexibility

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

Challenge Cybersecurity

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

Challenge Cybersecurity

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
Challenge Cybersecurity

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
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.

Consider specific automotive assets derived from CIAAG (Confidentiality, Integrity, Authenticity, Availability, Governance) scheme.
**Practical Guidance and Vector Experiences**

**Security Engineering**

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

**Apply a Systematic Threat and Risk Assessment**


- Architecture: Preliminary Architecture → Refined Architecture
Practical Guidance and Vector Experiences

Determine Necessary Security Level with TARA Results

<table>
<thead>
<tr>
<th>Asset ID</th>
<th>CIAAG Attack vector</th>
<th>Potential effect of attack</th>
<th>Threat ID</th>
<th>Threat Expertise</th>
<th>Expertise window of opportunity</th>
<th>Equipment effort</th>
<th>Effort Expertise</th>
<th>Expertise numerical</th>
<th>Impact Level of attacker</th>
<th>Safety mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset 01</td>
<td>Malicious CAN bus flooding</td>
<td>Attacker floods CAN-Bus and thereby tries to disable vehicle primary functions.</td>
<td>Threat 1</td>
<td>Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Malicious CAN bus flooding</td>
<td>Attacker disables engine control during an overtaking maneuver if system can impact safety-critical functions.</td>
<td>Threat 2</td>
<td>Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Malicious CAN bus flooding</td>
<td>Attacker floods CAN-Bus and thereby tries to disable vehicle primary functions.</td>
<td>Threat 3</td>
<td>Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Malicious CAN bus flooding</td>
<td>Attacker disables engine control during an overtaking maneuver if system can impact safety-critical functions.</td>
<td>Threat 4</td>
<td>Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

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

Supplier: detailed functional and technical security requirements
Security Requirements and Traceability

**Requirements**
- TARA, Security Goals
- Functional security requirements
- Technical security requirements

**Architecture**
- System
- Functional
- SW/HW

**Test**
- Penetration Test, Robustness Tests
- Functional Tests, Security Testing
- Unit Test, Static Code Analysis

Practical Guidance and Vector Experiences

Security Engineering

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

**Technical Security Concept:**
1) Refinement of system architecture to technical component level (SW/HW components)

**Technical Security Requirements (TSeR):**
- Security Case, Assessment, Compliance
- Security Validation
- Security Implementation
- Security Mgmt in Production, Operation, Service
Practical Guidance and Vector Experiences

Security Mechanisms allocated in Reference Architecture

Security Engineering

- Assets, Threats and Risk Assessment
- Security Goals and Requirements
- Technical Security Concept
- Security Implementation
- Security Validation
- Security Verification
- Security Mgmt in Production, Operation, Service
- Security Case, Assessment, Compliance
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

---

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
Practical Guidance and Vector Experiences

Safety and Security by Design: MICROSAR 4.3ff and FBL

Key management, crypto handling

Secure On-Board Communication

Firewall, Intrusion Detection

ASIL A-D hardened

FBL Application

HIS Security Module

Runtime Protection

Update Authorization

Secure Update Manager

Sec. Bootmanager (HSM)

1 Extensions for AUTOSAR

Practical Guidance and Vector Experiences

Security Engineering

Assets, Threats and Risk Assessment

Security Goals and Requirements

Technical Security Concept

Security Implementation

Security Validation

Security Case, Assessment, Compliance

Security Mgmt in Production, Operation, Service

Security Verification
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.

---

**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.
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.

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

Case Study
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

**System Architecture**

---

© 2019. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2019-03-17
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 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
ADAS – Step 3: Security Goals

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

Security goals are high level 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
Case Study
ADAS – Step 4: Security Mechanisms (1/3)

Plausibility Checks, e.g. Vehicle Speed, Engine_Status

- Braking while driving with speed > 10 km/h
- Deliberate Manipulation
- Systematic / Random HW Fault

- Overtake Brake ECU
- Manipulation of Radar Object on CAN Bus

AND

- Write message to CAN
- Create correct message on CAN

AND

- Overtake ECU on same CAN Bus
- Create authenticated CAN message

AND

- Know-How CAN message
- Connection to ECU

AND

- Secure Diagnostics
- Flash Firmware on ECU
- Know-How Firmware
- Access to Flash

Secure Communication

Secure Download
Case Study
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

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

Conclusions and Outlook

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

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

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

---

Conclusions and Outlook

**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.