Automotive Cybersecurity Webinar

Dr. Christof Ebert, Youssef Rekik

New:
- ISO 21434 Practice
- UNECE CSMS + SUMS
Welcome

Vector Consulting Services

**Vector Group** is a global market leader in automotive software, services and engineering tools with over 3,300 employees

**Vector Consulting Services**
is supporting clients worldwide

- **Transformation**
  > Agile Transformation, SPICE
  > Cost reduction

- **Trust**
  > Safety and Cybersecurity
  > Test Methods, PenTest, Supplier Audits

- **Technology**
  > Architecture support, e.g. AUTOSAR
  > Life-cycle methods, e.g. PREEvision

- **Training**
  > Training, Coaching, Certification
  > Corporate Competence Programs

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

@VectorVCS
Industry Trends 2020: The New Normal Fuels a Vicious Circle

Quality matters: Growing threats, increasing cost pressure, high liability risks.

Challenge Cybersecurity

Vicious circle:
- cost pressure
- lack of competences
- less innovation and quality

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.
Challenge Cybersecurity

Exposure: Attacks are Increasing Fast

- The majority of attacks is carried out remotely. 76% remotely, 16% physical.
- Half of attacks done by “black hat hackers”, other half by “white hat hackers”
- Top 5 attack points make almost two thirds of attacks: Key fob, server, smartphone app, OBD, head unit
- Tesla is most often hacked, followed by traditional OEMs. Hackers prefer premium cars.
- Autonomous cars are expected to be hacked even more often due to driver having less impact to correct

Sources: Ponemon Institute study with 593 security and policy professionals; SBD Automobile Cyber Guide, 2020; Results of 2020 Open Source Security & Risk Analysis Report, Synopsis; Harman 2020; Continental 2020

We will have more cyber attacks and must NOW prepare how to mitigate FUTURE damage
Challenge Cybersecurity

Liability: Legal Exposure is Growing Across Industries

- 30% of companies have no established product cybersecurity program and dedicated R&D security team
- 63% of companies test less than half of hardware, software, and other technologies for vulnerabilities
- 82% of all code is more than 4 years out of date
- 49% of code base have high vulnerabilities in static analysis

Sources: Ponemon Institute study with 593 security and policy professionals; SBD Automobile Cyber Guide, 2020; Results of 2020 Open Source Security & Risk Analysis Report, Synopsis; Harman 2020; Continental 2020

Cybersecurity is today as relevant as functional safety – and a precondition for safety.
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.
### Terminology and Cybersecurity Standards

#### Standards Demand Risk-Oriented Approach

**Automotive Functional Safety:**

ISO 26262:2018

**Automotive Cybersecurity:**
- ISO/SAE 21434 (Draft Standard)
- SAE J3061-2016 (Guideline)

**General Cybersecurity:**
- ISO 15408 (Common Criteria)
- ISO 27001 (IT Security)
- MISRA / CERT rules
- Threat modeling, e.g. HEAVENS, EVITA etc.

**System cybersecurity requirements**

**Safety Goals**

**Hazard & Risk Assessment**

**Technical Safety-Concept**

**System Integration Test Safety**

**Verification on Unit Level**

**Production, operation, service & decommissioning**

**Approval of the release for post-development**

**Cybersecurity Validation, Pen Tests**

**Item Definition & Asset Identification**

**Item Definition**

**Functional Safety-Concept**

**System Integration Test Security**

**Verification on Unit Level**

**Cybersecurity Activity**

**Safety Case**

**Validate Safety Goals**

**Item Integration Test Safety**

**Item Integration Test Security**

**Production, operations, maintenance & decommissioning**

**Safety Activity**
Terminology and Cybersecurity Standards

Overview ISO/SAE 21434 Draft (DIS) – Focus TARA & Security Management

Security Management on organizational level

Classic Security Management

TARA (Risk Assessment)

**Cybersecurity Information:**
Information derived from data collected by the monitoring process for which relevance to an item or component has not been determined.

**Cybersecurity Event:**
Cybersecurity information, that has been confirmed as potentially relevant to an item or component.

ISO SAE 21434 (Draft DIS)

Can be applied even outside a project (Cybersecurity Information/Event)

Significant addition to safety approach
Emergent System Property: Availability, Safety and Security

International engineering standards are available to cover **E/E emergent system properties**.

**Unsecure Scenarios**
- Security-related but QM
  - ISO SAE 21434, SAE J3061-2016

**Unreliable Scenarios**
- QM
  - ASPICE, IATF 16949, ISO 9001

**Unsafe Scenarios**
- SOTIF
  - ISO/PAS 21448

**Functional Safety**
- ISO 26262

**Cybersecurity attacks on Safety**
- ISO SAE 21434, SAE J3061-2016
**Terminology and Cybersecurity Standards**

**Legal Situation: Product Liability Demands Using Standards**

**Functional Safety**
- Generic E/E systems development: IEC 61508
- Automotive functional safety: ISO 26262
- Coexistence of quality standards: ISO 26262 refers to shared methods across standards, e.g. TARA
- SOTIF: ISO 21448

**Cybersecurity**
- Product development: ISO 21434, SAE J3061 (Cybersecurity process and lifecycle activities)
- Enterprise IT Security: ISO 27001 (Security mgmt), TISAX (Trusted Information Security Assessment Exchange)

**Homologation**
- Vehicle cybersecurity and data protection: UNECE R155 CSMS (Cybersecurity Management System)
- Software update management: UNECE R156 SUMS (Software Update Management System)

**Process Maturity**: ISO 330xx
Application of methodological Frameworks Automotive SPICE or CMMI

**Product Development Process**: ISO 9001, ISO/TS 16949

**Product Liability:**
A product, that is put in service, must provide the level of safety which can be expected by general public.
A secure product is based on the successful institutionalization of cybersecurity over all areas of product development.

The basis is a **security-oriented awareness** in the **organization** means an established **cybersecurity culture**.
The **cybersecurity case** is a collection of all security relevant work products.

- Input for a **cybersecurity assessment** and **release** for post-development.
- The cybersecurity case provides a **structured argument** for the achieved **degree of cybersecurity**

ISO SAE 21434 (Draft DIS), chapter 6.1
Overall & Project Dependent Cybersecurity Management

Practice: Cybersecurity Team and Project Team

Legend
- Cybersecurity Manager
- Chief Technical Lead
- Software Lead Team 1
- Software Lead Team 2
- Hardware Lead
- Production Lead
- Team Member
- Kanban Board

Industrialization
SW Team 1
SW Team 2
HW Team
Testing Team

Cybersecurity Engineering
Supply Chain: Need for Robust Interface Agreements

**OEM**
- Establish a system-wide safety and security responsibility
- Connect safety and security requirements in their system impact
- Align IT and E/E organizations because both contribute, e.g. key management
- Communicate security strategy and assumptions to your suppliers.
- Ask suppliers to sign a statement "The contractor will observe all relevant standards, laws and legal provisions..."

**Supplier**
- Demand context information. Security of a subsystem cannot be sustainably secured "out of context".
- Establish OEM-supplier Cybersecurity Interface Agreement (CIA) at project start. OEM: overall risk assessment, safety/security concept, interfaces, etc. Supplier: derived safety/security concept, assumptions to OEM, life-cycle deliverables.
- Perform periodic workshops on assumptions that you make to harden your subsystem.

Product liability holds for all products along the supply chain: OEM and supplier.
Risk-Oriented Security and Security Analysis

**TARA: Focus Risk Assessment Methods**

1. **Asset identification**
   - Asset Candidates, Cybersecurity properties

2. **Threat Scenario identification**
   - Assets, Damage Scenario
   - e.g. STRIDE

3. **Impact Rating**
   - (Assessed against Safety, Financial, Operational & Privacy)
   - Damage Scenario

4. **Attack Path Analysis**
   - Threat Scenario per Damage Scenario and known vulnerabilities
   - Attack paths per Threat Scenario

5. **Risk Treatment Decision**
   - Risk Values (1..)
   - • Avoiding risk
   - • Reducing risk
   - • Sharing risk
   - • Accepting risk

6. **Risk Determination**
   - Impact of Damage Scenario
   - Attack Feasibility (Ease of Exploitation)

**Cybersecurity Properties**

- Risk assessment applies to entire life-cycle. It is NOT tied to any specific phase.
### Determine Necessary Security Level with TARA Results

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AST 7</td>
<td>CAN Communication</td>
<td>Integrity</td>
<td>Compromise bus communication and inject not allowed messages (Integrity)</td>
<td>False positive alarm signals are sent to CAN-Bus. Safety functions activated although not needed</td>
<td>8</td>
<td>ECU Safety functions cannot be used due to heavy operational impact.</td>
<td>Layman</td>
<td>Spec COTS 3</td>
<td>Low</td>
<td>Pot</td>
<td>High</td>
<td>Calm</td>
<td>Moderate</td>
<td>High</td>
<td>SG16</td>
<td>The ECU shall ensure message authentication and message integrity through CAN-Bus</td>
<td></td>
</tr>
</tbody>
</table>

#### CAL (Risk value)

<table>
<thead>
<tr>
<th>Impact Rating (Annex H)</th>
<th>Negligible</th>
<th>Moderate</th>
<th>Major</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very low</td>
<td>--- (1)</td>
<td>--- (1)</td>
<td>--- (1)</td>
<td>--- (1)</td>
</tr>
<tr>
<td>Low</td>
<td>CAL1 (1)</td>
<td>CAL1 (2)</td>
<td>CAL2 (2)</td>
<td>CAL3 (3)</td>
</tr>
<tr>
<td>Medium</td>
<td>CAL1 (1)</td>
<td>CAL2 (2)</td>
<td>CAL3 (3)</td>
<td>CAL4 (4)</td>
</tr>
<tr>
<td>High</td>
<td>CAL2 (1)</td>
<td>CAL3 (3)</td>
<td>CAL4 (4)</td>
<td>CAL4 (5)</td>
</tr>
</tbody>
</table>

#### Attack Feasibility Rating

- **Very low**: --- (1)
- **Low**: CAL1 (1), CAL1 (2), CAL2 (2), CAL3 (3)
- **Medium**: CAL1 (1), CAL2 (2), CAL3 (3), CAL4 (4)
- **High**: CAL2 (1), CAL3 (3), CAL4 (4), CAL4 (5)
From TARA to Requirements, Design, Test, and Traceability

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

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

- **Test**
  - Grey-Box Penetration Test, Robustness Tests, Fuzzing
  - Functional Tests, Security Testing
  - Unit Test, Static Code Analysis
Systematic Security Engineering

Security Reference Architecture with Separated Topologies

**Vector recommendation:**
- Divide subnets towards manageable units
- Separate connectivity (e.g. cluster, TCU, Head Unit, etc.) from safety-critical components
- Connect safety and security operationally for efficiency – and effectiveness
AUTOSAR allows secure communication stack
Apply safety and security by design, i.e. design principles, traceability SG to FSR/TSR
Use hardened base software, preferably with secure boot
Security Implementation, Verification and Validation

**Design**
- Defensive coding, e.g. memory allocation, avoid injectable code, least privileges
- Programming rules such as MISRA-C, SEI 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
- Risk-based penetration testing

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

Security by Lifecycle: Verification, Validation and Life-Cycle Management

- **PSIRT Collaboration (Product Security Incident Response Team)**
  - Handover, task assignments and distribution

- **OTA Updates: Ensure that each deployment satisfies security requirements**
  - Data encryption: Protection of intellectual property by encryption
  - Authorization: Protection against unauthorized ECU access
  - Validation: Safeguarding of data integrity e.g. in the flash memory
  - Authentication: Verification of authenticity through signature methods
  - Governance: Safety/security documentation is continuously updated

- **Pen Testing**
  - Connect with misuse, abuse and confuse cases
  - Vector Grey-Box PenTest based on TARA and risks
  - DoS, Replay, Mutant/Generated Messages

- **Fuzz Testing**
  - Brute-force CAN Fuzzer for fuzzing the Application SW

- **Code Analysis**
  - CQA, Coverage (e.g., VectorCAST)
  - Design, architecture, (opt) defect analysis
Case Study: Autonomous System

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**
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
Case Study: Autonomous System

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.)
# Case Study: Autonomous System

## ADAS – Step 3: Security Goals

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

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

- Braking while driving with speed > 10 km/h
  - OR
  - Deliberate Manipulation
    - OR
      - Overtake Brake ECU
      - Manipulation of Radar Object on CAN Bus
    - Systematic / Random HW Fault
      - Plausibility Checks, e.g. Vehicle Speed, Engine_Status
  - AND
    - Write message to CAN
    - Create correct message on CAN
Case Study: Autonomous System

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

- Write message to CAN
  - Overtake ECU on same CAN Bus
    - AND
      - Secure Diagnostics
        - Flash Firmware on ECU
          - AND
            - Enter programming Session (0x27)
            - Know-How Firmware
              - AND
                - Access to Flash
                  - Secure Download
    - AND
      - Know-How CAN message
        - Create authenticated CAN message
          - Secure Communication
            - Create correct message on CAN
              - AND
                - Write message to CAN
Case Study: Autonomous System

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
Summary and Discussion

Security Requirements Engineering 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.)
Vector Offers the most Complete Portfolio for Security/Safety

Vector Cybersecurity Solutions

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

Tools
- COMPASS SecurityCheck and TARA
- VectorCAST for code analysis and coverage
- Security Manager Extension for Vector Tools und Fuzz Testing
- PLM with PREEvision
- Diagnosis

AUTOSAR Basic Software

HSM for HW based Security

Engineering Services for Security

www.vector.com/security
Summary and Discussion

Grow Your Competences in Risk-Oriented Development

Trainings
- Open trainings: www.vector.com/consulting-training
- Worldwide in-house trainings

Webinars and Podcasts
- Webinars and recordings
  www.vector.com/webinar-security
  www.vector.com/webinar-safety

Free white papers etc.
- www.vector.com/media-consulting

COMPASS for SecurityCheck, SafetyCheck and TARA:
www.vector.com/compass

Ensure that cybersecurity training is mandatory for all software and systems engineers
Thank you for your attention.
Please contact us for consulting support.


Vector Consulting Services

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