Vector Consulting

- **Vector Group** is a “hidden champion” and global market leader in automotive software and engineering tools with well over 3,000 employees.

- **Vector Consulting** supports clients worldwide for improving product development, IT and agile transformations.

- **Christof Ebert** is managing director at Vector Consulting Services. He serves on industry advisory boards, is a professor in Stuttgart and Paris, and author of “Systematic Requirements Engineering”.

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

@VectorVCS
Agenda

1. Welcome
2. Risk-Oriented Security
3. Systematic Security Engineering
4. Case Studies and Examples
5. Conclusions and Outlook
Outlook 2020: Risk of Vicious Circle

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

Vector provides tailored consulting solutions to keep OEM and suppliers competitive:
Competitiveness – Quality – Innovation
Combined Safety and Security Need Holistic Systems Engineering

**Functional Safety**
- Goal: Protect health
- Risk: Internal hazards, driven by failures and defects
- Governance: ISO 26262 etc.
- Methods:
  - HARA, FTA, FMEA, ...
  - Fail operational, ...
  - Redundancy, ...

**Cybersecurity**
- Goal: Protect assets
- Risk: External threats, driven by humans
- Governance: ISO 21434 etc.
- Methods:
  - TARA, Def. Coding...
  - Cryptography, ID/IP, ...
  - Key management, ...

**Privacy**
- Goal: Protect personality
- Risk: Data threats, driven by humans
- Governance: ISO 27001 etc.
- Methods:
  - TARA, ...
  - Cryptography, ...
  - Explicit consent, ...

**Liability ➔ Risk management ➔ Holistic systems engineering**
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.
Standards Demand Risk-Oriented Approach

**Functional Safety**
- IEC 61508, ISO 26262, ISO 21448
- Hazards and risk mitigation
- Safety engineering and culture
- ISO 26262 ed.2 refers to shared methods across standards, e.g. TARA
- Increasing focus on SOTIF and compliance

**Cybersecurity**

SAE 3061, ISO 21434
Overall Cybersecurity management, cybersecurity activities along its lifecycle

UNECE
OEM perspective, Vehicle cybersecurity and data protection, Software updates

TISAX (Trusted Information Security Assessment Exchange)
Exchange platform for IT-Security assessment results with focus on data and prototype protection

For (re)liable and efficient ramp-up connect security to safety governance
Focus on governance. ISO 21434 does NOT prescribe any technology or solutions

---

### Standard ISO 21434: Automotive Cybersecurity

#### 1. Scope

<table>
<thead>
<tr>
<th>5.4.1</th>
<th>5.4.2</th>
<th>5.4.3</th>
<th>5.4.4</th>
<th>5.4.5</th>
<th>5.4.6</th>
<th>5.4.7</th>
<th>5.4.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity governance</td>
<td>Cybersecurity culture</td>
<td>Cybersecurity risk management</td>
<td>Organizational cybersecurity audit</td>
<td>Information sharing</td>
<td>Management systems</td>
<td>Tool management</td>
<td>Information security management</td>
</tr>
</tbody>
</table>

#### 2. Normative references

#### 3. Terms and abbreviations

#### 4. General considerations

6. Overall cybersecurity management

6.4.1 Cybersecurity responsibilities & their assignment

6.4.2 Cybersecurity planning

6.4.3 Tailoring of the cybersecurity activities

6.4.4 Reuse

6.4.5 Component out of context

6.4.6 Off-the-shelf component

6.4.7 Cybersecurity case

6.4.8 Cybersecurity assessment

6.4.9 Release for post-development

7. Continuous cybersecurity activities

7.3 Cybersecurity monitoring

7.4 Cybersecurity event assessment

7.5 Vulnerability analysis

7.6 Vulnerability management

#### 8. Risk assessment methods

8.3 Threat identification

8.4 Threat scenario identification

8.5 Impact rating

8.6 Attack path analysis

8.7 Attack feasibility rating

8.8 Risk determination

8.9 Risk treatment decision

#### Annex A.1 (Informative)
UNECE clause, selection of most critical

7.1.1.2 The initial assessment must verify: A process whereby information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified.

7.1.1.5 The initial assessment must verify: A process whereby any interdependencies of the updated system with other systems can be identified.

7.1.2.1 The vehicle manufacturer shall record, and store at their premises for each update applied to a given vehicle type: Documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards used to demonstrate their compliance.

7.1.2.2 The vehicle manufacturer shall record, and store at their premises for each update applied to a given vehicle type: Documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identification for the type approved system’s hardware and software (including software versions) and any relevant vehicle or system parameters.

7.1.2.3 The vehicle manufacturer shall record, and store at their premises for each update applied to a given vehicle type: For every RXSWIN, there shall be an auditable register describing all the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN.

7.1.2.5 The vehicle manufacturer shall record, and store at their premises for each update applied to a given vehicle type: Documentation for all software updates for that vehicle type describing:
   (a) The purpose of the update;
   (b) What systems or functions of the vehicle the update may affect;
   (c) Which of these are type approved (if any);
   (d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system;
   (e) Whether the software update affects any system type approval parameter;
   (f) Whether an approval for the update was sought from an approval body;
   (g) How the update may be executed and under what conditions;
   (h) Confirmation that the software update will be conducted safely and securely.
   (i) Confirmation that the software update has undergone and successfully passed verification and validation procedures.

OEM Best practice

Software changes of a module or system made between releases are documented and tracked illustrating the main development branch with the evolution of system releases.

Integration testing of the updated system and validation of the safe and secure functioning of the vehicle.

Critical, specifically for legacy

Over the air update process and its security are managed by the OTA backend to ensure the compliance of safety and cybersecurity.

Updates affecting type approval are tested and approved for new or extended approval from authorities.

High

Every version of the software is documented to include newly added features and security mechanism/patches.

Critical, specifically for legacy

Update Release document from the OEM indicating the purpose, changes, approval, and verification of the proposed update to the vehicle.

High

Source:
ECE/TRANS/WP.29/GRVA/2020/4

UNECE will cost for volume legacy car >100 M EUR
Risk-Oriented Security

Synchronized Safety and Security

Process view

Project start

Development

Cybersecurity

Safety activities

SOP

Product view

Product maturity review gate 1

... ...

Product maturity review gate 2

ECU Schematics: RELEASED
ECU Architecture: DRAFT
ECU Layout: RELEASED
ECU FTA: DRAFT
ECU DFMEA: not started
Random hardware failure metric: RELEASED

... ...

Product maturity review gate n

... ...

+ Safety

ECU

Safe ECU
Risk-Oriented Security

Holistic Systems Engineering for Safety and Security

Process view

Product view

Legend

- Entity of Safety
- Entity of Security
- Entity of Architecture
- Entity of Requirement

13/35 © 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2020-03-25
Establish Efficient Single Master Process

Overlap needs *orchestrated master process* to remain efficient and consistent.
**Practical Legal Aspects for Cybersecurity**

### OEM
- Establish a security manager
- 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
- Security of a subsystem cannot be sustainably secured "out of context".
- Establish solid OEM-supplier Development-Interface Agreement (DIA) at project start. OEM: overall TARA, security concept, interfaces, key management, incident management. Supplier: derived 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. Therefore observe the applicable standards on both sides and assign traceable organizational responsibilities.
Agenda

1. Welcome
2. Risk-Oriented Security
3. Systematic Security Engineering
4. Case Studies and Examples
5. Conclusions and Outlook
Systematic risk-oriented security engineering across the life-cycle

1) Threat and risk analysis drive risk oriented hardening
2) Verification and validation with grey-box approach
### Systematic Security Engineering

**Determine Necessary Security Level with TARA Results**

<table>
<thead>
<tr>
<th>Asset ID</th>
<th>Asset / Vehicle Function</th>
<th>CIAAAG</th>
<th>Attack vector</th>
<th>Potential effect of attack</th>
<th>Threat ID</th>
<th>Threat</th>
<th>Expertise</th>
<th>Equipment</th>
<th>Effort</th>
<th>Impact Level (High=4; Low=1)</th>
<th>SGID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASt 01</td>
<td>Safety-Mechanisms</td>
<td>Avail</td>
<td>Available: Attacker floods CAN-Bus and thereby tries to disable vehicle primary functions.</td>
<td>ThA-1 Attack on engine control during an overtaking maneuver if system can impact safety-critical functions.</td>
<td>Tht-1</td>
<td>Layman</td>
<td>0 Critical</td>
<td>0 Standard</td>
<td>0 0 4</td>
<td>No injury No impact No effect No impact</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### Security Level (SL) vs. Impact Level (IL)

<table>
<thead>
<tr>
<th>Threat Level (TL)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>QM</td>
<td>QM</td>
<td>QM</td>
<td>QM</td>
<td>Low</td>
</tr>
<tr>
<td>1</td>
<td>QM</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>QM</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>QM</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Critical</td>
</tr>
</tbody>
</table>

---

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2020-03-25
Vector SecurityCheck with COMPASS for TARA and Continuous Documentation

Vector recommendation:
- Use a professional tool for systematic risk assessment
- Ensure governance with auditable risk and measure list
- Use heuristic checklists with continuously updated threats and mitigation

COMPASS information: www.vector.com/compass
From TARA to Requirements and Traceability

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

**Architecture**

**Test**
- Grey-Box Penetration Test, Robustness Tests, Fuzzing
- Functional Tests, Security Testing
- Unit Test, Static Code Analysis
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
HSM design objectives

- Harden ECUs against SW and selected HW attacks
- Provide HW acceleration for crypto functions
- Support ECU to ECU communication protection

HSM profiles, e.g. EVITA

- HSM full:
  - Support strong authentication (e.g. via RSA, ECC)
  - Support complex block ciphers
  - High performance
- HSM medium:
  - Secure ECU 2 ECU communication
- HSM small:
  - Secure critical sensors / actuators
  - Simple block ciphers
  - Low cost modules
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
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.
SW Updates
- Consider increasing regulation such as UNECE
- PSIRT Collaboration (Product Security Incident Response Team)

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
Secure and Transparent Software Upgrade Process Following UNECE Regulation

**Note:** This is a simplified view on the reference process and tools which Vector implements with its OEM clients. Numbering schemes in practice are very complicated with lots of inhouse proprietary tools.

### OEM

1. **Legal requirements**
   OEM maintains information and traceability from legal requirements (e.g. UNECE clauses) to functions to mapping into generic ECU and SW. Reviews and impact analysis by means of traceability, reviews, checklists and architecture experts.

2. **ECU part information**
   OEM maintains a 150% database with PLM and PDM for all ECUs and Software.

3. **Vehicle configurations**
   OEM maintains a database with specific configuration of each vehicle.

4. **Vehicle update impact analysis**
   OEM analyzes impact of actual vehicle configuration and identifies necessary updates.

5. **Vehicle update production**
   OEM selects specific updates, verifies vs type approval parameters, produces SW update package.

6. **Vehicle SW update delivery**
   OEM securely delivers the update to the vehicle by means of Transport Layer Security (TLS), either directly with OTA, or indirectly by flashing at service station.

7. **Vehicle synch with OEM**
   After successful SW update information is sent to OEM with BOM, PDM.

### Vehicle

1. **Vehicle identification**
   Vehicle comes to service station (or OTA at any physical place) and is identified for SW updates.

2. **Vehicle SW update**
   Vehicle receives updates, verifies integrity and uploads. It updates its internal vehicle PDM/BOM and OEM PDM/BOM DB.

3. **Vehicle onboard PDM/BOM system for specific vehicle**
Case Studies and Examples

Reference Project: Vector SecurityCheck

**Situation**
- Vector is supporting many OEMs with security analysis of their suppliers
- Vector supports OEMs and tier-1 with code quality analysis (CQA), SecurityCheck and hardening

**Goals**
- Systematically analyze security in a given product
- Fast track approach with quick win results
- Actionable results covering process, competence and technical dimensions

**Client Quote: Hyundai**
- Very professional consulting with high commitment and dedication for the project.
Situation
Vector is supporting a leading global tier 1 supplier in cybersecurity and agile development process.

Goals
- Evaluate product with TARA and propose security concept.
- Set up competences and security policies for sustainability.
- Perform cost trade-off analysis to prioritize security mechanisms.
- Implement security engineering with agile development and frequent upgrades over the air (OTA).

Client Quote Claas
Vector Consulting Services is a good partner for Claas to implement cybersecurity.
Claas had great benefits from the Vector team for TARA and Security Engineering.
Case Studies and Examples

Reference Project: PenTesting

**Situation**
- Vector is supporting many OEM, tier1 and tier2 suppliers with PenTesting

**Goals**
- Set up qualification strategy with Vector test tools and mapping to Fuzzing, PenTesting and regression test
- Provide grey-box PenTesting concept

**Client Quote Panasonic**
- Vector Consulting Services supported Panasonic with cybersecurity, demonstrating an outstanding level of expertise.
- The goal of a comprehensive TARA integrated into a security concept was achieved.
- The support was intense and very successful!
Agenda

1. Welcome
2. Risk-Oriented Security
3. Systematic Security Engineering
4. Case Studies and Examples
5. Conclusions and Outlook
Conclusions and Outlook

Security as well as Safety 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.)
Conclusions and Outlook

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 and Fuzz Testing
• PLM with PREEvision
• Diagnosis

AUTOSAR Basic Software

vHSM for HW based Security

Engineering Services for Security

www.vector.com/security
Conclusions and Outlook

Grow Your Competences in Risk-Oriented Development

**COMPASS** information: [www.vector.com/compass](http://www.vector.com/compass)

**Trainings**
- Open trainings: [www.vector.com/consulting-training](http://www.vector.com/consulting-training)
- Worldwide in-house trainings tailored to your needs
- Automotive Cybersecurity: [www.vector.com/training-security](http://www.vector.com/training-security)
- Functional Safety: [www.vector.com/training-safety](http://www.vector.com/training-safety)

**Webinars and Podcasts**
- Further webinars and recordings
  - [www.vector.com/webinar-security](http://www.vector.com/webinar-security)
  - [www.vector.com/webinar-safety](http://www.vector.com/webinar-safety)

**Free white papers etc.**
- [www.vector.com/media-consulting](http://www.vector.com/media-consulting)
Thank you for your attention.
For more information please contact us.


Vector Consulting Services

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