Vector SecurityCheck – Risk-Oriented Security

Dr. Christof Ebert, Vector Consulting Services
Welcome

Vector Consulting Services

- Experts for product development, product strategy and IT in critical systems
- Interim support, such as virtual security and safety officers and interim management
- Global presence
- Trainings on Agile, Requirements, Security, Safety, CMMI/SPICE etc.
- Part of Vector Group with over 1800 employees

www.vector.com/consulting
Welcome

Vector Client Survey: Security and Safety are Major Challenges

![Graph showing short-term and mid-term challenges]

- **Mid-term challenges**
  - Security and Safety
  - Innovative Products
  - Connectivity
  - Digital Transformation
  - Distributed Development
  - Governance and Compliance
  - Complexity Management
  - Efficiency and Cost
  - Others

- **Short-term challenges**


**Safety and security** paired with **efficient engineering** are major challenges.

| 1. | Welcome |
| 2. | Risk-Oriented Development |
| 3. | Practical Guidance and Vector Experiences |
| 4. | Conclusions |
Standards Demand Risk-Oriented Approach

Functional Safety (IEC 61508, ISO 26262)
- Hazard and risk analysis
- Functions and risk mitigation
- Safety engineering

ISO 26262 ed.2 will not comprehensively address security, but include shared methods, such as TARA

+ Security (ISO 27001, ISO 15408, ISO 21434, SAE J3061)
- Threat and risk analysis
- 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
State of the Art: Functional Safety

Relevance of ISO 26262 is basically understood

1. Driving Situations                OEM
2. Hazards                          OEM
3. Risks and Safety Integrity Level OEM
4. Safety Goals → Safety Requirements OEM
5. Technical Safety Concept         OEM/Tier1
6. Safety requirements on ECU level OEM/Tier1
7. Software Safety Requirements     Tier1/Vector

Functional safety can be efficiently achieved on the basis of mature development processes
**State of the Art: Cyber Security**

**Security demands are growing fast**
- Connectivity and open channels allow security attacks
- Exploits will persist beyond “zero-day” because so far no OTA governance
- Safety-critical systems connected to potentially unsecure bus systems

**Practical experiences are available**
- Extend hazard analysis with threat analysis and automotive attack models
- Reuse existing safety artefacts to ensure robust safety case
- Define tailored security protection for safety-critical systems
- Encrypt entire bus communication, e.g. AUTOSAR
- Protect ECUs with secure boot and HW-defined security
- Completely separate infotainment and HU

Do not copy paste standards because it increases overheads and complexity
Functional Safety and Cyber Security Demand Risk-Oriented Development

Risk = Severity of harmful event × Probability of occurrence

Risk-oriented engineering means to **intelligently mitigate the residual risks**

---

- **Asset**
  - has value for
  - Stakeholders (e.g., driver, OEM)

- **Attack**
  - requires
  - Threat Agent (e.g., hacker)

- **Threat**
  - causes
  - Attack Potential
  - is reduced by
  - Security Goal

- **Security Goal**
  - is achieved by
  - Security Engineering
1. Welcome

2. Risk-Oriented Development

3. Practical Guidance and Vector Experiences

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

**Tool Support: Vector SecurityCheck (1/3)**

#### Apply tools

- **Consistent risk assessment** and management
- Enable traceability to development
- Governance by continuously updated documentation
Consider relevant assets/attacks and relate to HARA for safety coverage.
Use heuristic checklists for informed analysis – specifically for the unknown
Practical Guidance and Vector Experiences

Case Study Powertrain: Threats and Hazards

<table>
<thead>
<tr>
<th>Function</th>
<th>Hazard</th>
<th>S/E/C</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjust speed</td>
<td>Speed is unintentionally increased during normal operation in cruise control while driving in a city</td>
<td>S3/E3/C1</td>
<td>C</td>
</tr>
<tr>
<td>Change Gears</td>
<td>During driving on high speed (Highway) the gear is changing to a higher gear thus reducing acceleration when it is needed during overtaking</td>
<td>S3/E4/C3</td>
<td>C</td>
</tr>
</tbody>
</table>

Relate identified security threats to safety hazard analysis
Elements of functional architecture

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SG05 High</td>
<td>It shall be prevented that unauthentic software is installed on vehicle ECUs.</td>
<td></td>
</tr>
<tr>
<td>FSR 1</td>
<td>The authenticity and integrity of the user_command signal during reading and transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 2</td>
<td>The authenticity and integrity of the authenticity signal during reading and transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 3</td>
<td>It shall be assured that the signal allow_update generated from the input signals is calculated correctly.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 4</td>
<td>The authenticity and integrity of the allow_update signal during transmission shall be assured.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 5</td>
<td>It shall be assured that the signal change_sw generated from the input signals is calculated correctly.</td>
<td>x</td>
</tr>
<tr>
<td>FSR 6</td>
<td>If an error with regards to authenticity and integrity during reading, transmission or calculation of signals or the actuator status occurs, the system will not install the sw update.</td>
<td>x</td>
</tr>
</tbody>
</table>

Transform technical security concept to security requirements. Handle security requirements exactly like functional requirements.
Case Study Powertrain: Separate Concerns

Incrementally harden your E/E and IT functions, architectures and components.
Consider Risk-oriented Development throughout the life-cycle

Begin with the end in mind:
After Sales Support needs early development decisions:
Resilience, fail operational strategies, alert center, repair/OTA, governance
Game Changer: OTA Facilitates Security Across the Life-cycle

There is no security without continuous **Over the Air (OTA)** update strategy.
Agenda

1. Welcome

2. Risk-Oriented Development

3. Practical Guidance and Vector Experiences

4. Conclusions
Conclusions

CASE (Connectivity, Autonomy, Sharing, Efficiency) ➤ Cyber Attacks

Security will be the major liability risk in the future. Average security breach is 8 months old, and in 70% of cases detected by third party.
## Conclusion: Combine Synergistic Safety & Security Techniques Across Life-Cycle

### Conclusions

<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 guidance</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Role of Virtual Security Manager</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>Secure boot, 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>IDS/IPS, Firewall with adjusted policies</td>
<td>Medium-High</td>
<td>Medium</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-High</td>
<td>High</td>
</tr>
<tr>
<td>Test strategy, e.g. Fuzz Testing, Penetration Testing etc.</td>
<td>High</td>
<td>Medium</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>
Thank you for your attention.
For more information please contact us.


Vector Consulting Services

www.vector.com/consulting
consulting-info@vector.com
Phone: +49 711 80670-0