Functional Safety and Cyber-Security – Experiences and Trends

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 1900 employees

www.vector.com/consulting
Vector Client Survey: Security and Safety are Major Challenges

Vector recommendation: **Efficiently implement safety and security**

Join 2018 survey now and win a training or book

www.vector.com/trends-survey
1. Welcome
2. Safety needs Security
3. Risk-Oriented Development
4. Practical Guidance and Vector Experiences
5. Conclusions
Safety needs Security

ACES (Autonomy, Connectivity, Efficiency, Services) ▶ Cyber-Attacks

Security will be the major liability risk in the future. Average security breach is detected in of 70% cases by third party – after 8 months.
<table>
<thead>
<tr>
<th>Agenda</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Welcome</td>
</tr>
<tr>
<td>2.</td>
<td>Safety needs Security</td>
</tr>
<tr>
<td>3.</td>
<td>Risk-Oriented Development</td>
</tr>
<tr>
<td>4.</td>
<td>Practical Guidance and Vector Experiences</td>
</tr>
<tr>
<td>5.</td>
<td>Conclusions</td>
</tr>
</tbody>
</table>
Risk-Oriented Development

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 27001 etc.
- Methods:
  - TARA, ...
  - Cryptography, ID/IP, ...
  - Key management, ...

**Privacy**
- Goal: Protect personality
- Risk: Data threats
- Governance: Privacy laws
- Methods:
  - TARA, ...
  - Cryptography, ...
  - Explicit consent, ...

**Liability ➔ Risk management ➔ Holistic systems engineering**
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  
2. Hazards  
3. Risks and Safety Integrity Level  
4. Safety Goals → Safety Requirements  
5. Technical Safety Concept  
6. Safety requirements on ECU level  
7. Software Safety Requirements

Functional safety can be efficiently achieved on the basis of mature development processes
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
Risk-Oriented Development

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**
<table>
<thead>
<tr>
<th>Agenda</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Welcome</td>
<td></td>
</tr>
<tr>
<td>2. Safety needs Security</td>
<td></td>
</tr>
<tr>
<td>3. Risk-Oriented Development</td>
<td></td>
</tr>
<tr>
<td>4. Practical Guidance and Vector Experiences</td>
<td></td>
</tr>
<tr>
<td>5. Conclusions</td>
<td></td>
</tr>
</tbody>
</table>
Consider specific automotive assets derived from CIAAG (Confidentiality, Integrity, Authenticity, Availability, Governance) scheme
Customer Benefits

- Efficient implementation of cybersecurity and functional safety
- Full Life-Cycle support from requirements to concept, design, test and after-sales
- Traceability and governance
- Support for heterogeneous environments
- Package offering with consulting, e.g. Vector SafetyCheck or Vector SecurityCheck
Case Study Powertrain: Threats and Hazards

### Adjust Speed
- **Hazard**: Speed is unintentionally increased during normal operation in cruise control while driving in a city.
- **S/E/C**: S3/E3/C1
- **ASIL**: C

### Change Gears
- **Hazard**: During driving on high speed (Highway) the gear is changing to a higher gear thus reducing acceleration when it is needed during overtaking.
- **S/E/C**: S3/E4/C3
- **ASIL**: C

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

<table>
<thead>
<tr>
<th>Security Goal</th>
<th>Functional Security Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Requirement</td>
</tr>
<tr>
<td>SG05 High</td>
<td>It shall be prevented that unauthentic software is installed on vehicle ECUs.</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>
</tr>
<tr>
<td>FSR 2</td>
<td>The authenticity and integrity of the authenticity signal during reading and transmission shall be assured.</td>
</tr>
<tr>
<td>FSR 3</td>
<td>The authenticity and integrity of the sw_update during reading and transmission shall be assured.</td>
</tr>
<tr>
<td>FSR 4</td>
<td>It shall be assured that the signal allow_update generated from the input signals is calculated correctly.</td>
</tr>
<tr>
<td>FSR 5</td>
<td>The authenticity and integrity of the allow_update signal during transmission shall be assured.</td>
</tr>
<tr>
<td>FSR 6</td>
<td>It shall be assured that the signal change_sw generated from the input signals is calculated correctly.</td>
</tr>
<tr>
<td>FSR 7</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>
</tr>
</tbody>
</table>

### Security Goal and derived functional security req.

- **SG05 High**: It shall be prevented that unauthentic software is installed on vehicle ECUs.
- **FSR 1**: The authenticity and integrity of the user_command signal during reading and transmission shall be assured.
- **FSR 2**: The authenticity and integrity of the authenticity signal during reading and transmission shall be assured.
- **FSR 3**: The authenticity and integrity of the sw_update during reading and transmission shall be assured.
- **FSR 4**: It shall be assured that the signal allow_update generated from the input signals is calculated correctly.
- **FSR 5**: The authenticity and integrity of the allow_update signal during transmission shall be assured.
- **FSR 6**: It shall be assured that the signal change_sw generated from the input signals is calculated correctly.
- **FSR 7**: 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.

### Security Goal to functional security architecture

**Transform technical security concept to security requirements. Handle security requirements exactly like functional requirements.**
Incrementally harden your E/E and IT functions, architectures and components.
Practical Guidance and Vector Experiences

Security by Design: Implementation, Verification and Validation

- **Design**
  - Use programming rules such as MISRA-C
  - Avoid injectable code
  - Enforce high cryptographic strength
  - Assign least privileges to any function
  - Static and dynamic code analysis

- **Test**
  - Encryption cracker, vulnerability scanner
  - Network traffic analyzer, stress tester, interface scanner
  - Layered fuzzing testing

- **Life Hacking**
  - Penetration testing
  - Governance and social engineering attacks

Test for the unknown. Run automatic regression tests with each delivery.
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

Practical Guidance and Vector Experiences

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

OEM Side

- Data or program with variable length X
- Hash function $y = h(x)$
- Create signature $\text{sign}(y, \text{key})$ of fixed length with RSA or HMAC

Update Process

- **Bootloader**
  - Bootloader Application Layer
  - **Security (Crypto) (Optional)**
  - Data Decompression (Optional)
  - Multiple Memory Manager

- **Flash-Tool**
  - Data or program to flash
  - Signature
  - vFlash

- **Communication Stack**
- CAN, LIN, FlexRay, MOST, Ethernet

**Bootsloader Updater**

- Flash-Treiber
  - HIS Device Driver 1
  - HIS Device Driver 2
  - HIS Device Driver n
1. Welcome
2. Safety needs Security
3. Risk-Oriented Development
4. Practical Guidance and Vector Experiences
5. Conclusions
Conclusions

Risk-Oriented Development Must Cover the Entire Life-Cycle

- Systematic safety and security engineering
- Scaleable incident monitoring and response
- Multiple modes of operation (normal, attack, emergency, fail operational, fail safe, etc.)
Conclusions

Integrated Development for Safety and Security

Similar to Safety, Security needs to be an integrated part of the development process.

Build security upon existing safety governance.
## Conclusions

**Conclusion: Combine Synergistic Safety & Security Techniques Across Life-Cycle**

<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>Virtual Safety / 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>
Vector Offers Comprehensive Portfolio for Cybersecurity and Functional Safety

Vector Cybersecurity and Safety Solutions

Security and Safety Consulting
Trainings
SecurityCheck, SafetyCheck, Virtual Safety Manager, Virtual Security Manager

AUTOSAR Basic Software:
MICROSAR Safe

HW based Security

Tools for Design, Test and Lifecycle support:
PREEvision
DaVinci
CANoe
CANdela and Indigo

Engineering Services for Safety and Security
Further Information: Vector White Papers on Automotive E/E Trends

- **Mobility**: From driving to multi-modal mobility services and sharing culture
- **Business Models**: From incumbent tiered supply-chain to flexible new players from IT industry
- **E/E architecture**: From distributed electronic controllers to standardized three-tier architecture
- **IT architecture**: From proprietary building blocks to open IT systems with off-the-shelf components and adaptive SOA.
- **Development lifecycle**: From the classic V model with rather heavy release cycles to agile DevOps-like approach.
- **Governance**: From encapsulated safety-critical functions to interwoven quality assurance for liability, safety, cyber-security, privacy.
- **Culture**: From R&D vs. IT separation to convergence.
- **Competences**: From automotive embedded electronics to IT as a core competence of all engineers.

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