Functional Safety (ISO26262) and SOTIF (ISO/PAS21448) Webinar

Unggul Joo, Apr 28th 2020
Welcome and Introduction

Vector Group

- **Development**
  Vector provides tools for developing, testing, calibration and diagnostics as well as software components and development services.

- **Networking**
  Vector provides components and engineering services for the networking of electronic systems.

- **Optimization**
  Vector provides a comprehensive consulting portfolio as well as suitable tools support.
Welcome and Introduction

Vector Client Survey 2020: Risk of vicious circle

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

Long-term challenges

Short-term Challenges

Innovative products
Digital transformation
Flexibility
Complexity
Distributed development
Quality
Cost and efficiency
Competences and knowledge
Others

Vector provides tailored consulting solutions to keep OEM and suppliers competitive:

Efficiency – Quality – Competences
Agenda

Welcome and Introduction

- Challenges and Concepts
  - Vector Safety Experiences
  - Conclusions and Outlook
Many functions are safety related

Electrical Power Steering
Unintended steering and loss of steering assist

Electronic Park Brake
Unintended activation in motion

Collision Avoidance
Acceleration instead of deceleration in traffic

Airbag
Unintended deployment during normal operation

Mal-functions caused by failures of E/E systems
Challenges and Concepts

Demarcation to “other” safety

**Product Safety**
- Mechanical construction
- Robustness over life-time
- Endurance

**Operational Safety**
- Avoidance of chemicals drain-out
- EMC
- Fire protection
- etc.

**Functional Safety**
- All hazards caused by safety-relevant functions in E/E-Systems.
Functional safety – Risk based approach

Risk = Severity of harmful event × Probability of occurrence

The purpose of functional safety activities is to reduce the residual risk to an acceptable level.
The **Fault Tolerant Time Interval** (FTTI) is ...

- the transient time interval, during which an **unsafe behavior is tolerable**.
- specific for every safety goal.
Challenges and Concepts

Functional Safety – Wide Impact

Wide impact on entire life-cycle ➔ Risk of gaps and inconsistencies
Challenges and Concepts

Functional Safety – Many Methods

Many methods and techniques ➔ Risk of uninformed usage
Challenges and Concepts

Parts of ISO 26262:2018 – 2\textsuperscript{nd} Edition – Main Changes

ISO/PAS 21448 Road vehicles -- Safety of the intended functionality (SOTIF)

1. Vocabulary

2. Management of functional safety

3. Concept phase

4. Product development at the \textit{system level}

5. Product development at the \textit{hardware level}

6. Product development at the \textit{software level}

7. Production and operation

8. Supporting processes

9. ASIL-oriented and safety-oriented analyses

10. Guideline on ISO 26262

11. Application of ISO 26262 to semiconductor

12. Adaption of ISO 26262 for motorcycles
Challenges and Concepts


- Part 2 (Safety Management):
  - Chapter 5.4.2 (Safety culture): The organization shall institute and maintain effective communication channels between functional safety, cybersecurity, and other disciplines ...
  - Chapter 6.4.9 (Confirmation Measures): Additional confirmation review of impact analysis, Functional Safety Concept and Technical Safety Concept

- Part 3 (Concept Phase):
  - Chapter 6.5.4 (Hazard Analysis and Risk Assessment): Variances shall be considered when conducting a hazard analysis and risk assessment for a T&B vehicle (type of base vehicle, vehicle configuration and vehicle operation).

- Part 4 (Product Development at the System Level):
  - Chapter 6.4.4.6 (Technical Safety Concept): Properties of a system architectural design to avoid systematic faults now without ASIL-dependent recommendations.

- Part 5 (Product Development at the Hardware Level):
  - Chapter 7.4.4.3 (Hardware Design): Verification of the validity of assumptions when integrating a SEooC into the hardware.

- Part 6 (Product Development at the Software Level):
  - Chapter 7.4.12 (Software Architectural Design): Safety mechanisms for error detection and error handling shall be applied depending on the results of the safety-oriented analyses at the software architectural level ...
Safety of the intended functionality (SOTIF) – The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons.

Note: Intentional alteration of the system operation (Feature abuse) is not in scope.
Challenges and Concepts

Overview Automotive Safety: Functional Safety & SOTIF

**SOTIF: Triggering events** are analyzed if acceptable or function needs to be modified.

**Triggering event:**
- Camera sensor blinded by sunset

**Misuse:**
- Applying highway traffic sign recognition in urban traffic

**Functional Safety:** Methods required by ISO 26262 focus on those **faults** need to be **identified and mitigated**, which potentially violate a safety goal.
Challenges and Concepts

What is and when to apply a HARA?

Evaluate integrity required:

- The hazard analysis and risk assessment is performed based on the definition of the safety item.
- It is a systematic analysis of the desired behavior of the item.
- It aims to the identification of potential hazard and resulting measures.
- The results of the HARA are the safety goals with the ASILs.
Risk assessment and classification

Challenges and Concepts

Severity (S)  Exposure (E)  Controllability (C)

Malfunction may affect controllability

Persons involved in considered situation

ASIL
### Severity, Exposure and Controllability

#### Severity classifications of the hazardous event

<table>
<thead>
<tr>
<th>S0</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No</strong> injuries</td>
<td><strong>Light and moderate</strong> injuries</td>
<td><strong>Severe and life-threatening</strong> injuries (survival <em>probable</em>)</td>
<td><strong>Life-threatening</strong> injuries (survival <em>uncertain</em>), <strong>fatal</strong> injuries</td>
</tr>
</tbody>
</table>

#### Exposure classifications of the hazardous event

<table>
<thead>
<tr>
<th>E1</th>
<th>E2</th>
<th>E3</th>
<th>E4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very low</strong> probability</td>
<td><strong>Low</strong> probability</td>
<td><strong>Medium</strong> probability</td>
<td><strong>High</strong> probability</td>
</tr>
</tbody>
</table>

#### Controllability classifications of the hazardous event

<table>
<thead>
<tr>
<th>C0</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controllable <em>in general</em></td>
<td><strong>Simply controllable</strong></td>
<td><strong>Normally controllable</strong></td>
<td>Difficult to control or <strong>uncontrollable</strong></td>
</tr>
</tbody>
</table>
### Challenges and Concepts

**ASIL determination – Evaluation of ranking**

<table>
<thead>
<tr>
<th>Severity class</th>
<th>Exposure class</th>
<th>Controllability class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S1</td>
<td>C1</td>
</tr>
<tr>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E2</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E3</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E4</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td>S2</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>A</td>
</tr>
<tr>
<td>S3</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>B</td>
</tr>
</tbody>
</table>

**Source:** ISO 26262-3:2018

- **S:** Severity
- **E:** Exposure
- **C:** Controllability
- **I:** necessary Integrity
- **QM:** Quality Management
## Development – HARA for deriving Safety Goals and ASIL

### Challenges and Concepts

<table>
<thead>
<tr>
<th>Malfunction of Adaptive Front Steering</th>
<th>Operational Situation</th>
<th>E</th>
<th>C</th>
<th>S</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steering inversion</td>
<td>&gt; 50 km/h &lt; 100 km/h</td>
<td>E4</td>
<td>C3</td>
<td>S3</td>
<td>D</td>
</tr>
<tr>
<td>Oversteering</td>
<td>&gt; 50 km/h &lt; 100 km/h</td>
<td>E4</td>
<td>C3</td>
<td>S3</td>
<td>D</td>
</tr>
<tr>
<td>Oversteering</td>
<td>Parking &lt; 10 km/h</td>
<td>E4</td>
<td>C1</td>
<td>S1</td>
<td>QM</td>
</tr>
</tbody>
</table>

**Exposure:**
- E3: 1-10% of average operating time
- E4: >10% of average operating time

**Controllability (Average Driver):**
- C1: Hazardous situation is simply controllable
- C3: Hazardous situation is usually not controllable

**Severity:**
- S1: Light to moderate injuries
- S3: Critical injuries
Basic Concept of ISO 26262: Risk Classification by „ASIL“

Risk = Severity \times Probability

R = S \times P_E \times P_C \times P_I

ASIL

Automotive Safety Integrity Level

(= required integrity of a function)

Residual Risk  Tolerated Risk  Risk by add. Function

E/E functions  Safety functions

Source: IEC 61508:2010
Challenges and Concepts

Efficient Traceability and Consistency

**Safety Goals**
- SG1: HZ1, HZ3, ASIL B (Safety Goal 1)
- SG2: HZ2, ASIL D (Safety Goal 2)
- ...

**Functional Safety Requirements**
- FSR 1: SG1, ASIL B, Funct. Safety Req. 1
- FSR 2: SG1, ASIL B, Funct. Safety Req. 2
- ...

**Technical Safety Requirements**
- TSR 1.1: FSR 1, ASIL B, HW/SW, Tech. Safety Req. 1.1
- TSR 1.2: FSR 1, ASIL B, HW/SW, Tech. Safety Req. 1.2
- ...

**Item Definition**

**Preliminary Architecture / System Architectural Design**

**System Architectural Design**

**Efficient Traceability and Consistency**

Hazard Analysis & Risk Assessment

Functional Safety Concept

Allocation of FSRs to architectural elements

Technical Safety Concept

Allocation of TSRs to architectural elements

Refinement of Architectural Design

System Architectural Design (external input)
FMEA and FTA – Safety Analysis on System and HW level

Challenges and Concepts

Most common methods for safety-oriented analyses

- **FMEA**
  - = Failure Mode Effect Analysis
  - **Inductive** analysis method
  - Used to identify **root causes** of failures and **effects** of failures in the system.
  - Can only be applied to an existing design or implementation.

- **FTA**
  - = Fault Tree Analysis
  - **Deductive** analysis method
  - Used to identify **root causes** of failures and their **correlation** in the system.
  - Development of design alternatives
  - Discovery of unexpected scenarios
Challenges and Concepts

Approaches to Risk Reduction

Objectives:
- Avoid failures
- Make unavoidable failures safe

ISO26262 (ASIL)

Random Failure

Technical measures against random HW failures:
- Redundancy
- Safety mechanisms ("Diagnostics")
- Self-tests
- ...

Systematic Failure

Technical measures against systematic system, HW and SW failures:
- Redundancy
- Diagnostics
- Self-tests
- Modular HW/SW architecture
- Architecture patterns
- Defensive programming
- ...

Product Measures

Process Measures

Methodological measures to ensure the application of a safety-conform development process:
- Top-down design flow
- Requirements based engineering
- Design methods
- Analysis techniques
- Test methods
- Traceability
- Reproducibility
- Detailed process requirements
- ...

Failure
Agenda

Welcome and Introduction

Challenges and Concepts

- **Vector Safety Experiences**

Conclusions and Outlook
Vector Experiences – Support Throughout the Life-Cycle

Consistently plan and systematically maintain safety artefacts
SW Safety Analysis assumes occurrence of SW faults based on complexity of SW.
Example FSC – SysML Block Diagram as Vector Best Practice

Functional safety is about **requirements & solution** development (*Two-Pillar approach*)
**Vector Experiences – Development Interface Agreement (DIA)**

- **List of relevant artefacts**
- **Minimum scope:** ~ 60 artefacts
- **Project specific tailoring, application and tracking**

---

**Use the DIA for comprehensive definition of the customer/supplier interfaces. Extend the usage to not safety related artefacts**
Vector Experiences – Security Directly Impacts Safety

**Functional Safety**

(ISO/PAS21448, ISO 26262)

- Hazard analysis and risk assessment
- Functions and risk mitigation
- Safety engineering

**Security not sufficiently addressed**

**+ Security**

(J3061, ISO/SAE 21434)

- Threat, Attack and risk analysis
- Attack paths and vulnerabilities
- Security engineering

- Security & Safety are interacting and demand holistic systems engineering
- For fast start security engineering should be connected to safety framework
Agenda

Welcome and Introduction

Challenges and Concepts

Vector Safety Experiences

Conclusions and Outlook
Conclusions and Outlook

ISO26262 Experience

- **Increasing functional safety capabilities**
  - Majority of OEM’s include ISO26262 compliance in their contracts
  - Independent audits and assessments are performed
  - Methods for qualitative and quantitative analysis are available
  - ASIL D HW and SW components are available as Seooc

- **But...**
  - Many suppliers do not have **full ISO26262 compliance** because they develop based on legacy systems
  - Suppliers and OEMs need to further improve field observation and abilities to efficiently maintain a safety case
  - **New suppliers**, e.g. for electric powertrain or ADAS, struggle with ramping up a safety process
  - Security risks increasingly hamper functional safety
  - Functional safety processes in many cases **create overheads** – which could be done at much lower cost

Functional safety can be efficiently achieved on the basis of mature development processes together with a competent partner.
Conclusions and Outlook

Vector: Comprehensive Portfolio for Security and Safety

Vector Cyber Security and Safety Solutions

- Security and Safety Consulting
- AUTOSAR Basic Software
- HW based Security
- Tools (PLM, Architecture, Test, Diagnosis etc.)

Engineering Services for Safety and Security

Trainings and media

- Training “Functional Safety with ISO 26262” and “Cybersecurity” in Seoul, continuously
  https://vector-academy.com/vk_class_functional_safety_ko.html
  https://vector-academy.com/vk_class_cybersecurity_ko.html

- In-house trainings tailored to your needs available worldwide
- Virtual trainings
- Free white papers...
  www.vector.com/media-safety

- Vector Forum – Automotive systems, Software etc.

Vector Consulting

- Consultants with broad industrial exposure and experiences
- Professional consulting, innovative approaches and excellent quality
- Objective-driven solutions tailored to your specific needs
- Sustainable and measurable results achieved through a close working partnership