Functional Safety with ISO 26262

Webinar
Christof Ebert, Arnulf Braatz
Vector Consulting Services
Welcome to the Webinar

Vector Consulting Services

- ... supports clients worldwide in improving their product development and IT and with interim management
- ... with clients such as Accenture, Audi, BMW, Bosch, Daimler, Huawei, Hyundai, Lufthansa, Munich RE, Porsche, Siemens, Thales, ZF
- ... offers with the Vector Group a portfolio of tools, software components and services
- ... is globally present as a group with over 1300 employees and well over 250 Mio. €

- www.vector.com/consulting
- www.vector.com/safety
Agenda

Welcome to the Webinar

- **Motivation**
  - Concepts and Challenges
  - Vector Experiences
  - Conclusions and Outlook
Motivation

Challenges in 2015 – Results from Vector Client Survey

Evolution since 2014: Complexity management and connectivity play a dominant role, while in 2014 the major focus was on cost reduction.

Vector Client Survey 2015; www.vector.com/trends; Sum > 100% because 3 answers per question were allowed.
Motivation

Vector – Complete Safety Solution Portfolio

**Introduction of Safety Processes (Examples)**

- Introducing ISO 26262, starting with analysis of the current state, including technical and process measures and building up safety culture
- Training and coaching for functional safety, sustainable safety culture
- Implementing consistent tool support, such as PREEvision

**Safety Management (Examples)**

- Provisioning (interim) safety managers
- Performing safety audits and supplier safety audits

**Safety Engineering (Examples)**

- Providing software components and platforms, such as MICROSAR Safe
- Facilitating safety analyses, e.g. HARA, FMEA, FMEDA, reviews
- Developing and reviewing safety concepts
Motivation

Vector Consulting Services – Leader in Functional Safety

Vector Consulting Services supports clients world-wide in efficient and effective implementation of functional safety
Agenda

Welcome to the Webinar
Motivation

Concepts and Challenges
Vector Experiences
Conclusions and Outlook
Functional Safety: Broad Exposure

**ESP**
- Unintended, single-sided brake effect on straight lane

**Electronic Park Brake**
- Unintended activation in motion

**Collision Avoidance**
- Acceleration instead of deceleration in traffic

**Airbag**
- Delayed deployment after crash detection

Exposure of practically all E/E functions ➞ Risk of liability
Concepts and Challenges

Functional Safety – Recent Call-Backs

Problems with switch:
Brake lights either don’t light up
or light up continuously

Korean OEM

Problems with acceleration:
Car unintentionally accelerates thus causing
personal damage

Japanese OEM

Problem with automatic gear control:
Gear is unintentionally switched to neutral

American OEM

Problems with airbag control:
Airbags and seat belt pre-tensioner are not or
too late activated

German OEM

Source: autoservicepraxis.de

Increasing amount of incidents ➔ Risk of global visibility
Concepts and Challenges

Functional Safety – Wide Impact

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

Functional Safety – Many Methods

1. Fault prevention
   - Guidelines
   - Processes

2. Fault detection
   - Code analysis
   - Review, Test

3. Fault tolerance
   - Redundant design
   - Memory protection

4. Failure prevention
   - Redundant Shut-off
   - Fail-safe concepts

Many methods and techniques ➔ Risk of uninformed usage
# Functional Safety – Complex Standard

**10 Parts**

**43 Chapters**

**100 work products**

**180 engineering methods**

**500 pages**

**600 requirements**

---

**Complex standard ➔ Risk of overheads and bureaucracy**

---

Source: ISO 26262
Concepts and Challenges

Liability

Manufacturer's Liability
The manufacturer has to organize the company in a way that design, production and documentation faults are eliminated or detected by checks.

Reversal of Evidence
The manufacturer has to show that he is not responsible for a fault.

Product Liability
A product, that is put in service, must provide the level of safety which can be expected by general public.

Manufacturer's liability is excluded, if a failure can not be detected using current state of science and technology at the time the manufacturer put the product into market.
Standards are the lower limit of the state of the art of science and technology.

ISO 26262 is published and thus part of the state of the art of science and technology.

Maturity models, like CMMI and SPICE, are also part of the state of the art of science and technology.

Their application is therefore expected.
## A Structured Approach

### 1. Vocabulary

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-5</td>
<td>Overall safety management</td>
</tr>
<tr>
<td>2-7</td>
<td>Safety management after the item’s release for production</td>
</tr>
</tbody>
</table>

### 2. Management of functional safety

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5</td>
<td>Initiative development at the system level</td>
</tr>
<tr>
<td>3-6</td>
<td>Specification of the technical safety requirements</td>
</tr>
<tr>
<td>3-7</td>
<td>System design</td>
</tr>
<tr>
<td>3-8</td>
<td>Item integration and testing</td>
</tr>
</tbody>
</table>

### 3. Concept phase

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-5</td>
<td>Initiative development at the system level</td>
</tr>
<tr>
<td>4-6</td>
<td>Specification of the technical safety requirements</td>
</tr>
<tr>
<td>4-7</td>
<td>System design</td>
</tr>
<tr>
<td>4-8</td>
<td>Item integration and testing</td>
</tr>
</tbody>
</table>

### 4. Product development at the system level

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-5</td>
<td>Development of the function level</td>
</tr>
<tr>
<td>5-6</td>
<td>Specification of hardware safety requirements</td>
</tr>
<tr>
<td>5-7</td>
<td>Hardware design</td>
</tr>
<tr>
<td>5-8</td>
<td>Evaluation of the hardware architectural metrics</td>
</tr>
<tr>
<td>5-9</td>
<td>Evaluation of the safety goal violations due to random hardware failures</td>
</tr>
<tr>
<td>5-10</td>
<td>Hardware integration and testing</td>
</tr>
</tbody>
</table>

### 5. Product development at the hardware level

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-5</td>
<td>Development of the software level</td>
</tr>
<tr>
<td>6-6</td>
<td>Specification of software safety requirements</td>
</tr>
<tr>
<td>6-7</td>
<td>Software architectural design</td>
</tr>
<tr>
<td>6-8</td>
<td>Software unit design and implementation</td>
</tr>
<tr>
<td>6-9</td>
<td>Software unit testing</td>
</tr>
<tr>
<td>6-10</td>
<td>Software integration and testing</td>
</tr>
<tr>
<td>6-11</td>
<td>Verification of software safety requirements</td>
</tr>
</tbody>
</table>

### 6. Product development at the software level

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-5</td>
<td>Production</td>
</tr>
<tr>
<td>7-6</td>
<td>Operation, service (maintenance and repair), and decommissioning</td>
</tr>
</tbody>
</table>

### 7. Production and operation

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-5</td>
<td>Interfaces within distributed developments</td>
</tr>
<tr>
<td>8-6</td>
<td>Specification and management of interfaces</td>
</tr>
<tr>
<td>8-7</td>
<td>Configuration management</td>
</tr>
<tr>
<td>8-8</td>
<td>Change management</td>
</tr>
<tr>
<td>8-9</td>
<td>Verification</td>
</tr>
<tr>
<td>8-10</td>
<td>Documentation</td>
</tr>
<tr>
<td>9-5</td>
<td>Requirements decomposition with respect to ASIL tailoring</td>
</tr>
<tr>
<td>9-6</td>
<td>Criteria for coexistence of elements</td>
</tr>
<tr>
<td>9-7</td>
<td>Analysis of dependent failures</td>
</tr>
<tr>
<td>9-8</td>
<td>Safety analyses</td>
</tr>
</tbody>
</table>

### 9. ASIL-oriented and safety-oriented analyses

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
Basic Concept of ISO 26262: Risk Classification by „ASIL“

Risk = Severity \times Probability

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

Exposure  Controllability  Integrity

ASIL

Automotive Safety Integrity Level

(= required integrity of a function)

Residual Risk  Tolerated Risk  Risk by add. Function

QM  A  B  C  D

Integrity

vgl. IEC 61508:2010

S: Severity
E: Exposure
C: Controllability
I: necessary Integrity
QM: Quality Management
Development – Determination of ASIL

Risk = Severity × Probability

R = S × P_E × P_C × P_I

S: Severity
E: Exposure
C: Controllability
I: necessary Integrity
QM: Quality Management

Source: ISO 26262-3:2011
### Concepts and Challenges

#### Development – Classification Example Brake-by-wire-System

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>Vehicle State</th>
<th>Road Condition</th>
<th>Environment Condition</th>
<th>E</th>
<th>C</th>
<th>S</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Braking Effect</td>
<td>&gt; 100 km/h</td>
<td>Wet</td>
<td>Highway</td>
<td>E3</td>
<td>C3</td>
<td>S3</td>
<td>C</td>
</tr>
<tr>
<td>Unexpected Braking Effect</td>
<td>&gt; 50 km/h</td>
<td>Dry</td>
<td>Main Road</td>
<td>E4</td>
<td>C2</td>
<td>S3</td>
<td>C</td>
</tr>
<tr>
<td>Asymmetric Braking Effect</td>
<td>Parking &lt; 10 km/h</td>
<td>Dry</td>
<td>Side Road</td>
<td>E4</td>
<td>C2</td>
<td>S1</td>
<td>A</td>
</tr>
</tbody>
</table>

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

**Controllability (Average Driver):**
- C2: Hazardous situation is usually controllable
- C3: Hazardous situation is usually not controllable

**Severity:**
- S1: Light to moderate injuries
- S3: Critical injuries
Approaches to Risk Reduction

Concepts and Challenges

Random faults

- Redundancy
- Diagnosis, Monitoring
- Cut off
- Reliability
- Self-Tests
- ...

Systematic faults

- „Make unavoidable fault safe“
- „Avoid fault“

Technical measures against random hardware faults:

- Redundancy
- Diagnosis, Monitoring
- Cut off
- Reliability
- Self-Tests
- ...

Methodic measures in the development process:

- Design Methods
- Analysis Techniques
- Defensive Programming
- Test Methods
- Safety Case
- Traceability of Requirements
- Proof of Safety
- ...

“Make unavoidable fault safe”

“Avoid fault”
Welcome to the Webinar
Motivation
Concepts and Challenges

Vector Experiences

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

Consistently plan and systematically maintain safety artefacts
Vector Experiences – Development Interface Agreement (DIA)

**List of relevant artifacts**

**Minimum scope:** ~60 artifacts

**Project specific tailoring, application and tracking**

Use the DIA for comprehensive definition of the customer/supplier interfaces. Extend the usage to not safety related artifacts.
Support by Vector Consulting Services and PREEvision tool:

- Predefined operation scenarios and operating modes
- Automatic ASIL calculation
- Traceability of safety goals to requirements and design artifacts
Support by Vector Consulting Services and PREEvision tool:

- Single source for item definition, based on features, requirements, operating scenarios, dependencies
- Model-based design of functional and technical safety concept, including ASIL decomposition and requirement based tests
Vector Experiences

Vector Experiences – Security Directly Impacts Safety

Functional Safety (ISO 26262)

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

Security demands implicitly addressed

+ Security

- Security threats
- Misuse cases and mitigation
- Security engineering

For better efficiency and clear focus security engineering should be embedded to safety framework from hazards to after-sales updates
Example: Driver Assistance

New functions ...
- Complex functionality
- High data volume
- Link to the outer world (Car2X; vehicle as IP node)

... result in new Challenges
- New safety concepts (architectures with more redundancy)
- Support of high-performance micro-controllers
- Support of high-performance software development
- Safety functions have to be secured against over-the-air-attacks
  > avoid misuse of services and functions
  > avoid unintended reprogramming of functions

Vector experience: Review your safety concepts in line with security challenges. Derive safety requirements from misuse cases.
Agenda

Welcome to the Webinar
Motivation
Concepts and Challenges
Vector Experiences

• Conclusions and Outlook
Success Factor – Implement Functional Safety

Conclusions and Outlook

Products

**Technical measures** against hardware and software failures to
- avoid failures and
- make unavoidable failures safe.

Examples: **Redundancy, Reuse** with AUTOSAR

Processes

**All development activities** are concerned as well as **production** and **field observation**.

Examples: **Hazard analysis** during concept definition, **consistent modeling** in PREEvision

People

New **roles and skills** as well as **cultural changes** for engineering and management staff.

Examples: **Safety engineering** skills, **safety manager** role, **safety culture**

Functional safety must focus on processes and people – not only on the product and its features
Conclusions and Outlook

Success Factor – Change Towards Safety Culture

<table>
<thead>
<tr>
<th>Classic Development Culture</th>
<th>Safety Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient budget and time for relevant safety measures</td>
<td>Necessary measures are planned according to safety analysis – and reliably implemented</td>
</tr>
<tr>
<td>Shadow organization of safety experts and staff teams</td>
<td>Safety expertise is embedded into the regular line and project organization</td>
</tr>
<tr>
<td>Risk analysis is done superficially for documentation purposes and not maintained</td>
<td>Risk analysis and FMEA are developed at the beginning of system development and are continuously updated</td>
</tr>
<tr>
<td>System architecture is not considered in safety goals and requirements</td>
<td>System architecture explicitly covers the safety goals and requirements</td>
</tr>
<tr>
<td>Changes are accepted at any time for practically all system parts</td>
<td>Changes are analyzed with respect to their effects on functional safety using a strict change management</td>
</tr>
<tr>
<td>Safety audits are conducted only sporadically</td>
<td>Safety audits are established as a normal and standardized behavior</td>
</tr>
</tbody>
</table>

Implementing functional safety implies a profound culture change
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 capable MCU’s are available

- **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

ISO26262 Will Further Evolve

Committee Draft (CD) release  Release ISO26262 ed. 2

2015 2016 2017 2018

Evolution – Some Topics

1. Extension of scope, e.g. for buses and trucks
2. Improved Safety Analysis Methods for software
3. More detailed requirements for semiconductors, security etc.
4. Support for safety case for ADAS
5. HARA supported by traffic accident statistics
6. Assessment and Audit process improvement

Vector is contributing to the evolution of ISO 26262
Questions?
For more information about Vector and our safety portfolio please visit

www.vector.com/safety

Prof. Dr. Christof Ebert, Dr. Arnulf Braatz
Vector Consulting Services GmbH
Your Partner in Achieving Engineering Excellence

Phone +49 711 80670-0       www.vector.com/consulting
Fax +49 711 80670-444        consulting-info@vector.com