ISO 26262 + FMEA
Concepts + Polarion Template

Timothy.stroebele@polarion.com
Manager PSO
Agenda

• ISO 26262 Concepts
• Polarion goes ISO 26262
• Polarion FMEA
• Q&A Session
• Next Steps
Application that can cause harm (a risk):
• Airbag exploding when infant is sitting in front seat

Need to assess the risk:
• Infant getting injured – „not good at all“

Find a mitigation strategy, e.g. a safety function:
• Detecting infant in front seat and disabling airbag
  a) Sensor delivers signal to
  b) Software/Hardware controlling an
  c) Actuator (disalber)

Functional Safety is then:
• An infant in front seat is not exposed to an unacceptable (unreasonable) risk
- Functional Safety for Road Vehicles
- ISO 26262 is an adaptation of IEC 61508 for the automotive industry
• Provides an Automotive Safety Lifecycle, which covers all phases from initial definition and planning till disassembling of the product

• Supports tailoring the necessary activities during these lifecycles phases

• Provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Level, ASILs) based on „Item“

• Uses ASILs for specifying the item‘s necessary safety requirements for achieving an acceptable residual risk

• Provides requirements for validation and confirmation measures
• The ASIL is a key component

• The ASIL is determined at the beginning of the development process

• The intended functions of the system are analyzed with respect to possible hazards

• ASIL asks: „If a failure arises, what will happen to the driver and associated road users?“
ISO 26262 – Functional Safety for Road Vehicles

ISO 26262 – Main Parts

1. Management of functional safety
2. Concept Phase
3. Product development at the system level
4. Production & Operation
5. Product development at the hardware level
6. Product development at the software level
7. Supporting Processes and safety-oriented analysis
ISO 26262 – Functional Safety for Road Vehicles

Hazard Analysis and Risk Assessment

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-5</td>
<td>Item Definition</td>
</tr>
<tr>
<td>3-6</td>
<td>Initiation of the safety lifecycle</td>
</tr>
<tr>
<td>3-7</td>
<td>Hazard analysis and risk assessment</td>
</tr>
<tr>
<td>3-8</td>
<td>Functional safety concept</td>
</tr>
</tbody>
</table>

- Hazard Identification
- Hazard Classification
- Hazard Determination
- Safety Goal Determination
What is the Automotive Safety Integrity Level (ASIL)?

- Automotive specific risk-based approach for determining risk classes

ISO 26262 – Functional Safety for Road Vehicles

- Automotive Safety Integrity Level (ASIL)

Probability of Exposure + Controllability + Severity of Failure = ASIL

QM A B C D
ISO 26262 – Functional Safety for Road Vehicles

Hazard Classification

- Scored E0 – E4 (Incredible – High probability)
- How often explodes an airbag while an infant is sitting in front seat?

- Scored C0 – C3 (Controllable in general – Difficult to control or manage)
- Is the infant or the driver able to control the explosion of the airbag?

- Scored S0 – S3 (No injuries – Life-threatening injuries)
- How severe will the infant injured?
ISO 26262 – Functional Safety for Road Vehicles

Hazard Determination

Probability of Exposure + Controllability + Severity of Failure = ASIL

Airbag Example:
E2 (low probability) + C3 (difficult to control) + S3 (life-threatening) = ASIL B
Polarion goes ISO 26262
Problem: Project “Silos” Exist

- Requirements Management
- Development And Release Management
- Quality Assurance

Functional Safety
Challenge: Eliminate Silos
Integrate ALM Artifacts

- Hazards
- Requirements (safety, system, software, hardware)
- Design Specifications
- Tasks
- Test Cases
- Change Requests

Information is Shared NOT Segregated
Polarion ISO 26262 Project Template

With Polarion, Functional Safety is Traceable and Auditable!

Polarion Answers:

• Who made changes to Hazard Analysis?

• When were changes made?

• What is/was done to mitigate hazards?

• Complies inheritance of ASIL to ISO 26262?

• Coverage: Do we have defined at least one functional safety requirement for a safety goal?
ISO 26262 – Concept Phase:

- **Work Item Types:**
  - Hazard
  - Safety Goal
  - Functional Safety Requirement
  - Custom Fields, Link Roles, Workflow

- **Work Produkts:**
  - Dokument Item Definition
  - Dokument Hazard Analysis and Risk Assessment
  - Dokument Functional Safety Concept

- **Reports:**
  - Traceability & Coverage
  - Check Compliance

- **ISO 26262 – Part 3 “How-To” Knowledgebase**
Demo Scenario
Next Steps

• Download ISO 26262 Template from http://extensions.polarion.com

• Try it LIVE

• Watch a demo