ISO 26262

Functional Safety Management in the Autonomous Car industry and the overview of the required safety lifecycle

TÜV SÜD America

PSES San Diego Chapter
Meeting Sep. 12, 2017
Functional Safety Expert: Peter Spence

Peter Spence
“Functional Safety Expert” consultant with TÜV SÜD America since July 2014

Background:

- 9 years Weapon Eng. Office Nuclear Safety, Royal Navy
- 5 years Exxon-Mobil, PLC/Logic Controls Software, Safety shutdown systems
- 2 years Samsung Electronics, PLC/Instrumentation Logic controls/Safety shutdown systems, risk assessment/analysis
- 5 years Applied Materials, Semi design 300mm Projects
- International standardization (ISO 26262, ISO 13849 & IEC 62061, IEC 61800-5-2, IEC 61508, System Test and logic design, IEC 61010).
- Bsc from University of London, England
The year 2016 marks the 150th anniversary of TÜV SÜD. Since 1866, the company has been partnering businesses and inspiring people to trust in new technologies.

Today, TÜV SÜD has grown into an international service company with global representation in over 800 locations, and with over 50 per cent of its employees working outside Germany.

In the decades to come, it will continue to make the world a safer place as a future-oriented company shaping the “next practice” in safety, quality and sustainability.
TÜV SÜD Auto Service GmbH

- National and international Homologation
- Vehicle Emission Testing
- Analytical Expertise

TÜV SÜD Rail GmbH

- Team Automotive
  - Evaluation of concepts, systems, components and processes regarding means of functional safety
  - Automotive specific safety
  - Trainings regarding functional safety
  - ISO 26262 Audits and Assessments
  - Electronic Annexes – ECE 13 and ECE 79

TÜV SÜD Rail GmbH

- Head of Functional Safety
- Evaluation of safety systems for railway, infrastructure and automation
- Evaluation of generic safety systems (μC, SW Tools)
- IEC 61508, ISO 25119, EN 50128, ISO 26262 ...
ISO 26262 Services: CTCT

- Workshops
- Development accompanying support
- Assessments
- Supplier Audits
- Penetration Tests

ISO 26262 Training:
- Basic – Advanced – Expert
- IEC 62443 Training
- Functional Safety Certification Program (FSCP)

- Product Certification
- Generic SW Tool Certification
- Process Certification

- ISO 26262 Training:
- Basic – Advanced – Expert
- IEC 62443 Training
- Functional Safety Certification Program (FSCP)

- Testing
- Consulting

- Assessments
- Supplier Audits
- Penetration Tests

- Workshops
- Development accompanying support
Agenda

- What is Functional safety?
- Principles and Concepts
- Principles and Concepts per ISO 26262
  - Requirements management and traceability
  - Tool qualification and certification
Functional Safety Standard - Overview

**International (Generic)**
- ISO/IEC 15504: SPICE/Automotive SPICE
- ISO/IEC 12207: Software lifecycle process

**Medical**
- IEC 62304: Software for medical devices

**Machines**
- ISO 13849
- IEC 62061: Safety of machines

**Gas measure techniques**
- EN 50271
- EN 50402: Functional safety of gas warning systems

**Process industry**
- IEC 61511: Safety instrumented systems for the process industry sector

**Railway**
- EN 50126
- EN 50128
- EN 50129

**Avionics**
- ARP 4761
- ARP 4754
- RTCA/DO 178C
- RTCA/DO 254

**Automotive**
- ISO 26262: Functional safety “road vehicles”

**Nuclear Power**
- IEC 60880: Nuclear power - control technology, Software aspects
- IEC 61513
What is functional Safety?

- Probability:
  - always
  - sporadic
  - seldom
  - improbable
  - impossible

- Severity:
  - nothing
  - low
  - medium
  - high
  - extreme

Risk evaluation:
- risk not acceptable
- risk acceptable
- acceptable risk
What is functional safety?

Functional Safety means:

• Something has to work in critical situations

Functional Safety is:

• Not visible for the user
• Only partly testable for Hardware (wiring plan)
• For software it has to root in the developing process

Functional Safety Goal:

• Risk reduction according to ASIL
Safety

• Absence of unreasonable risk

Risk

• Combination of the probability of occurrence of harm and the severity of that harm

Harm

• Physical injury or damage to the health of persons

The goal is to reduce the risk to a socially accepted risk.
Due to the mostly mechatronic implementation and due to the increasing technological complexity of software and hardware it is necessary that systematic failures and random hardware errors have to be taken into account in the context of functional safety.

**Topics to be investigated**

**Legal requirements for homologation**  
(Process for Certification)

- Legally binding  
  Application of, e.g., EU directives and ECE regulations (Europe), FMVSS (USA)

**Product Liability**

- Recommended  
  Application of IEC, ISO, EN or DIN standards (“State of the art”)
Functional Safety Risks caused by malfunctions in a vehicle

**Potential Failures**

- Unintended acceleration
- Unintended deceleration
- Unintended loss of acceleration
- Unintended loss of deceleration
- Unintended vehicle movement

**Risk reduction measures**

- Functional measures
- Monitoring functions (safety functions, e.g., pinch protection)
- Reliability of target function

**Functional Failures**

- Functional measures
- Monitoring functions (safety functions, e.g., pinch protection)
- Reliability of target function

**Non Functional Failures**

- Design measures, e.g., isolation
- Organizational measures, e.g., operation procedures
- Driver instruction

- High Voltage
- Fire
- Explosion
What is Functional Safety?

- **What does it mean for a product, or subsystem, or component?**
  - **Example**: Motor drives for electrical vehicles:
    - Developed and certified to IEC 61800-5-1 or UL 508C:
      - You can touch it
      - It doesn’t start a fire
      - No dangerous emissions or emanations
    - => a **safe product** in terms of risks for fire, shock, and injury.
What is Functional Safety?

- **Example:** Motor drive in powertrain of hybrid electrical vehicle

  - Still "safe"?
  - Unintended acceleration!
  - Safety beyond the single product: **SYSTEM SAFETY**!
  - Depends on **correctness** of product's **functions**, implemented in **electronics** and **software**:

**FUNCTIONAL SAFETY**
Today:
Software-intensive automotive control systems
Immediate future: Connected car, autonomous driving

- Functional safety challenges:
  - Advanced sensing and intelligence
  - Driver behaviour and responsibility
  - System of systems, socio-technical system
  - Cybersecurity as a safety risk
ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds.

ISO 26262 does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.
ISO 26262 addresses possible hazards caused by malfunctioning behavior of safety-related E/E systems, including interaction of these systems.

Note: It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of safety-related E/E systems.

ISO 26262 does not address the nominal performance of E/E systems, even if functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, adaptive cruise control).
Concepts and principles of Functional Safety…

**….in general**

- **Risk-based**
  - Requires system approach
  - Hazard identification and risk assessment

- **Management of functional safety**
  - Lifecycle
  - Roles and organisation
    - independence of assessors
  - Supplier management

- **Address hardware random failures**
  - Architecture and failure control
    - Redundancy and diversity
    - Diagnostics
  - Reliability and failure exclusion

- **Address software-related (“systematic”) failures**
  - Fault avoidance
    - Modular design
    - Processes, methods, tools
  - Quality assurance

**…ISO 26262 in particular**

Determine risk associated with control systems, using "Automotive Safety Integrity Level": ASIL A (lowest), B, C, or D (highest)
Hazard analysis and risk assessment process

- Determination of ASIL and Safety Goals

Table 4 — ASIL determination

<table>
<thead>
<tr>
<th>Severity class</th>
<th>Probability class</th>
<th>Controllability class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C1</td>
<td>C2</td>
</tr>
<tr>
<td>S1</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>QM</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>
Hazard analysis and risk assessment example

Simple seat positioning system; Safety Goal:

"Prevent seat movement while driving with V > 5km/h, ASIL C"

=> Functional Safety requirements:

FSR_01: "Detect vehicle movement (V), ASIL C"
FSR_02: "Interrupt seat movement if V > 5 km/h, ASIL C"
FSR_03: "Ignore seat control switches if V > 5 km/h, ASIL C"
...
### Concepts and principles of Functional Safety...

#### in general
- **Risk-based**
  - Requires system approach
  - Hazard identification and risk assessment

#### ISO 26262 in particular
- Determine risk associated with control systems, using "Automotive Safety Integrity Level": ASIL A (lowest), B, C, or D (highest)

#### Management of functional safety
- Lifecycle
- Roles and organisation
  - independence of assessors
- Supplier management

#### Address hardware random failures
- Architecture and failure control
  - Redundancy and diversity
  - Diagnostics
- Reliability and failure exclusion

#### Address software-related ("systematic") failures
- Fault avoidance
  - Modular design
  - Processes, methods, tools
  - Quality assurance

Safety culture, assessment, safety case
- Increasing independence, ...
- Increasing assessment effort, ...
- Increasing tool qualification, ...
- ... the higher the ASIL.
- Development Interface Agreements
Functional Safety Management

Safety Development Capability

Management of Functional Safety
- Overall Safety Management
- FSM before SoP
- FSM after SoP

Supporting Processes
- Distributed Development
- Safety Requirements
- Configuration Management
- Change Management
- Verification
- Documentation
- Software Tools
- Qualification of Software
- Qualification of Hardware
- Proven in Use Argument

Safety Culture

Quality Management System (ISO 9001 / TS 16949)
Normative requirement on quality management during the safety lifecycle:
- ISO/TS 16949, ISO 9001, or equivalent.

ISO 26262 is within the ISO/TS 16949 process frame; it extends and instantiates the requirements.
- Instantiation: ISO/TS clause 7.3 "Design and Development" is addressed by ISO 26262's core processes on System, HW and SW level.
- Extension: ISO 26262 implements the system approach (vehicle "items") and relies on final OEM responsibility, ...
  ... Whereas ISO/TS is focused on component / sub-system supplier responsibility.

Increased alignment with ISO 26262 of IATF 16949:2016:

- Requirements for safety-related parts and processes /* FMEAs, training of staff involved, transfer of safety requirements throughout supply chain */
- Enhanced product traceability requirements to support latest regulatory changes /* ISO 26262 implies responsibility to monitor and maintain functional safety after release for production*/
- Requirements for products with embedded software /* Embedded software is crucial for functional safety, ISO 26262-6 and supporting processes of ISO 26262-8*/
- Clarification of sub-tier supplier management and development requirements /* ISO 26262 has specific supplier-related requirements, e.g.: supplier selection and functional safety assessment, development interface agreement (DIA)*/
- Addition of corporate responsibility requirements /* Functional Safety management is not only project-specific, but impacts corporate level. ISO 26262 requires to install a Safety Culture in the organization.*/
Safety Case and Functional Safety Assessment

**Claims**

- Correctness ! & Completeness !
  - Safety Goals
  - Technical Safety Concept SW & HW Architecture Descr.
  - SW Requirements Specification
    - SW State machine diagram
  - SW Detailed Architecture Specification
    - SW Detailed Design
  - SW Source Code
  - HW Requirements Specification
  - HW Design documentation
    - Safety Plan, Validation Plan
  - Modification Procedure

**Evidence**

- to a sufficient level of Confidence!
  - Confirmation Reviews
  - Conformance & Audit reports
- Integration Test Spec. & Report
- System Test Spec. & Report
- Block-level FTA
- HW Test Spec. & Report
- Component FMEDA
- SW Test Spec. & Report
- SPF Metric, LF Metric Calculation, PMHF
- SW Module test spec. & report
  - SW Criticality Analysis Report
  - SW Static Analysis Report

**Arguments**

- Instruction for use
- SW Requirements Specification
- Component SW State machine diagram
- SW Detailed Architecture
- SW Detailed Design
- HW Requirements Specification
- HW Design documentation

**Compliance !**

- Traceability between all information elements – the „backbone“ of the safety case
Traceability and Construction of Safety Case

Implementing, Refining

- Hazards and risks
- Functional failure modes
- Component failure modes
- Coding rules and restrictions
- System Safety Requirements
- SW safety Requirements
- HW Block
- HW Component
- SW Module
- method, function
- Source code section
- SW qualifi. Test case and result
- Module test case and result
- SW static analysis result
- Validation test case and result
- Integration test case and result

Analysis
Design
V&V
Concepts and principles of Functional Safety…

<table>
<thead>
<tr>
<th>In general</th>
<th>ISO 26262 in particular</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk-based</strong></td>
<td>Determine risk associated with control systems, using &quot;Automotive Safety Integrity Level&quot;: ASIL A (lowest), B, C, or D (highest)</td>
</tr>
<tr>
<td>- Requires system approach</td>
<td></td>
</tr>
<tr>
<td>- Hazard identification and risk assessment</td>
<td></td>
</tr>
<tr>
<td><strong>Management of functional safety</strong></td>
<td>Safety culture, assessment, safety case</td>
</tr>
<tr>
<td>- Lifecycle</td>
<td>- Increasing independence, …</td>
</tr>
<tr>
<td>- Roles and organisation</td>
<td>- increasing assessment effort, …</td>
</tr>
<tr>
<td>- independence of assessors</td>
<td>- increasing tool qualification, …</td>
</tr>
<tr>
<td>- Supplier management</td>
<td>- the higher the ASIL.</td>
</tr>
<tr>
<td><strong>Address hardware random failures</strong></td>
<td><strong>Safety mechanisms, and metrics</strong></td>
</tr>
<tr>
<td>- Architecture and failure control</td>
<td>with increasing target values for</td>
</tr>
<tr>
<td>- Redundancy and diversity</td>
<td>- Architectural metrics and diagnostic capabilities (SPFM &amp; LFM), …</td>
</tr>
<tr>
<td>- Diagnostics</td>
<td>- Probability of failures (PMHF)</td>
</tr>
<tr>
<td>- Reliability and failure exclusion</td>
<td>- the higher the ASIL.</td>
</tr>
<tr>
<td><strong>Address software-related (&quot;systematic&quot;) failures</strong></td>
<td></td>
</tr>
<tr>
<td>- Fault avoidance</td>
<td></td>
</tr>
<tr>
<td>- Modular design</td>
<td></td>
</tr>
<tr>
<td>- Processes, methods, tools</td>
<td></td>
</tr>
<tr>
<td>- Quality assurance</td>
<td></td>
</tr>
</tbody>
</table>
Fault concepts and hardware metrics:

Architectural metrics

ISO 26262-5; Figure C.1 — Fault classification of safety-related hardware elements of an item

=> FMEDA as a key activity and work product
Fault concepts and hardware metrics:

Architectural metrics

ISO 26262-5; Figure C.1 — Fault classification of safety-related hardware elements of an item

<table>
<thead>
<tr>
<th>Safety Mechanisms</th>
<th>Fault Tolerance, Redundancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe faults</td>
<td>Single-point fault metric</td>
</tr>
</tbody>
</table>

**Single-point fault metric**

<table>
<thead>
<tr>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥90 %</td>
<td>≥97 %</td>
<td>≥99 %</td>
</tr>
</tbody>
</table>

**Latent fault metric**

<table>
<thead>
<tr>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥60 %</td>
<td>≥80 %</td>
<td>≥90 %</td>
</tr>
</tbody>
</table>

Driver notices something alarming
Fault concepts and hardware metrics:  
Reliability metrics

- Either: “Probabilistic Metric for random Hardware Failures” (PMHF)  
  - to evaluate the violation of the considered safety goal using, for example, quantified FTA or Markov and to compare the result of this quantification with a target value.

<table>
<thead>
<tr>
<th>ASIL</th>
<th>Random hardware failure target values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>&lt;10^{-8} h^{-1}</td>
</tr>
<tr>
<td>C</td>
<td>&lt;10^{-7} h^{-1}</td>
</tr>
<tr>
<td>B</td>
<td>&lt;10^{-7} h^{-1}</td>
</tr>
</tbody>
</table>

- FTA = Fault Tree Analysis is a quantitative methodology used for verification.
- Markov modelling method is used in determining the safety availability and reliability of complex equipment (i.e. logic solvers).

- Or: Individual evaluation of each residual and single-point fault, and of each dual-point failure leading to the violation of the considered safety goal.
  - This analysis method can also be considered to be a cut-set analysis.
<table>
<thead>
<tr>
<th>Concepts and principles of Functional Safety…</th>
<th>…ISO 26262 in particular</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>....in general</strong></td>
<td><strong>Determine risk associated with control systems, using &quot;Automotive Safety Integrity Level&quot;: ASIL A (lowest), B, C, or D (highest)</strong></td>
</tr>
<tr>
<td>- Risk-based</td>
<td></td>
</tr>
<tr>
<td>- Requires system approach</td>
<td></td>
</tr>
<tr>
<td>- Hazard identification and risk assessment</td>
<td></td>
</tr>
<tr>
<td>- Management of functional safety</td>
<td><strong>Safety culture, assessment, safety case</strong></td>
</tr>
<tr>
<td>- Lifecycle</td>
<td>- Increasing independence, …</td>
</tr>
<tr>
<td>- Roles and organisation</td>
<td>- increasing assessment effort, …</td>
</tr>
<tr>
<td>- independence of assessors</td>
<td>- increasing tool qualification, …</td>
</tr>
<tr>
<td>- Supplier management</td>
<td>… the higher the ASIL.</td>
</tr>
<tr>
<td>- Address hardware random failures</td>
<td><strong>Safety mechanisms, and metrics</strong></td>
</tr>
<tr>
<td>- Architecture and failure control</td>
<td>with increasing target values for</td>
</tr>
<tr>
<td>- Redundancy and diversity</td>
<td>- Architectural metrics and diagnostic capabilities (SPFM &amp; LFM), …</td>
</tr>
<tr>
<td>- Diagnostics</td>
<td>- Probability of failures (PMHF)</td>
</tr>
<tr>
<td>- Reliability and failure exclusion</td>
<td>… the higher the ASIL.</td>
</tr>
<tr>
<td>- Address software-related (&quot;systematic&quot;) failures</td>
<td><strong>Safety measures (Methods, Activities)</strong></td>
</tr>
<tr>
<td>- Fault avoidance</td>
<td>- Increasing formality and documentation, …</td>
</tr>
<tr>
<td>- Modular design</td>
<td>- Increasing self-test requirements, …</td>
</tr>
<tr>
<td>- Processes, methods, tools</td>
<td>- increasing verification depth …</td>
</tr>
<tr>
<td>- Quality assurance</td>
<td>… the higher the ASIL.</td>
</tr>
</tbody>
</table>
Reference phase model for the software development
Fault avoidance during software development

Table 1 — Topics to be covered by modelling and coding guidelines

<table>
<thead>
<tr>
<th>Topics</th>
<th>ASIL A</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Enforcement of low complexity(^a)</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1b Use of language subsets(^b)</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1c Enforcement of strong typing(^c)</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1d Use of defensive implementation techniques(^d)</td>
<td>o</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1e Use of established design principles</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>1f Use of unambiguous graphical representation</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1g Use of style guides</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1h Use of naming conventions</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

Table 3 — Principles for software architectural design

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL A</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Hierarchical structure of software components (^a)</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1b Restricted size of software components(^a)</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1c Restricted size of interfaces(^a)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>1d High cohesion within each software component(^b)</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1e Restricted coupling between software components(^a, b, c)</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1f Appropriate scheduling properties</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>
Reference phase model for the software development

- Traceability requirements

Traceability:
- "vertical"
- "horizontal"
Software tool classification and qualification procedure

Determine possibility that an error is introduced or not detected by tool
Determine confidence in measures for prevention and detection of malfunctions
Determine maximally required ASIL
Qualify SW tool, or methods & processes ("workflow" for the SW tool)

Methods and processes for use in acc. with ASIL
Increased confidence from use!
Tool development process evaluation!
Tool validation!
Tool in accordance with FS standard!
"Fit for Purpose" Certificate for Software Tools

Customer Information

Safe Tool Development Process

Validation

Increased Confidence from use

Trustworthiness

Quality Management

Safety Manual

Increased Confidence from use

Safe Tool Development Process

Validation

Increased Confidence from use

Quality Management
Your Comments and Questions are Welcome!

Peter Spence
TÜV SÜD
Automotive Department
Tel: 213-784-5234
mailto:pspence@tuvam.com
http://www.tuev-sued.de
http://www.tuev-sued.de/rail/training