Automotive Functional Safety
Complexity, Confidence, Compliance, Certification
Farmington, 2018-03-22
Inspiring trust since 1866
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.
ISO 26262 Services: CTCT

- Product Certification
- Generic SW Tool Certification
- Process Certification
- ISO 26262 Training: Basic – Advanced – Expert
- IEC 62443 Training
- Functional Safety Certification Program (FSCP)
- Assessments
- Supplier Audits
- Penetration Tests
- Workshops
- Development accompanying support
- Certification
- Training
- Testing
- Consulting
Bio Thomas Maier

Business Development Manager at TÜV SÜD Rail since July 2016

Background:
- 6 years at UL, principal engineer for functional safety
- 8 years at Danfoss Drives, functional safety in motion control.
- 3 years at LM Ericsson A/S: software processes and tools, CMMi, UML and SDL
- 3 years at Daimler-Benz: system safety and functional safety of drive-by-wire systems and in avionics.
- 4 years at the Joint Research Centre of the European Commission: system & software safety in fusion technology.
- Dr.-Ing. from University of Stuttgart
Agenda

• What is Functional safety?
• Challenges
• Principles and Concepts per ISO 26262
  • Demonstration of functional safety
• Certification
Today: Automotive safety depends on numerous software-intensive control systems
Immediate future:
Connected car, autonomous driving

- Functional safety challenges:
  - Advanced sensing and intelligence
  - Driver responsibility
  - System of systems, socio-technical system
  - Cybersecurity as a safety risk
Functional Safety Challenges…

- **System safety**
  - Complexity
  - Hidden interconnections and interactions
  - Unpredictable behavior (non linear, chaotic, backward coupling, …?)
  - "Human factor", unpredictable use scenario

- **System and product life-cycle**
  - Hazards not only in operation, but also in production, transport, disposal?
  - Faults introduced through supply chain
  - Software easy to modify

- **Hardware random failures**
  - Of course …

- **Systematic failures**
  - Increased complexity of microelectronics and software
Functional Safety Challenges…

- **System safety**
  - Complexity
  - Hidden interconnections and interactions
  - Unpredictable behavior (non-linear, chaotic, backward coupling, …?)
  - "Human factor", unpredictable use scenario

- **System and product life-cycle**
  - Software easy to modify
  - Faults introduced through supply chain
  - Hazards not only in operation, but also in production, transport, disposal?

- **Hardware random failures**
  - Of course …

- **Systematic failures**
  - Increased complexity of microelectronics and software
Functional Safety Challenges…

1. IDENTIFY!

• System safety
  ▪ Complexity
  ▪ Hidden interconnections and interactions
  ▪ Unpredictable behavior (non-linear, chaotic, backward coupling, ...?)
  ▪ "Human factor", unpredictable use scenario

• System and product life-cycle
  ▪ Software easy to modify
  ▪ Faults introduced through supply chain
  ▪ Hazards not only in operation, but also in production, transport, disposal?

2. ACHIEVE!

• Hardware random failures
  ▪ Of course …

• Systematic failures
  ▪ Increased complexity of microelectronics and software
Functional Safety Challenges…

1. IDENTIFY!

- System safety
  - Complexity
  - Hidden interconnections and interactions
  - Unpredictable behavior (non-linear, chaotic, backward coupling, ...?)
  - "Human factor", unpredictable use scenario

2. ACHIEVE!

- System and product life-cycle
  - Software easy to modify
  - Faults introduced through supply chain
  - Hazards not only in operation, but also in production, transport, disposal?

- Hardware random failures
  - Of course ...

3. MAINTAIN!

- Systematic failures
  - Increased complexity of microelectronics and software
Functional Safety Challenges…

1. IDENTIFY!
- System safety
  - Complexity
  - Hidden interconnections and interactions
  - Unpredictable behavior (non-linear, chaotic, backward coupling, …?)
  - "Human factor", unpredictable use scenario

2. ACHIEVE!
- System and product life-cycle
  - Software easy to modify
  - Faults introduced through supply chain
  - Hazards not only in operation, but also in production, transport, disposal

3. MAINTAIN!
- Hardware random failures
  - Of course …

4. DEMONSTRATE!
- Systematic failures
  - Increased complexity of microelectronics and software
### 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>
<thead>
<tr>
<th>Severity class</th>
<th>Probability class</th>
<th>Controllability class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C1</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>
### 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)

- **Safety culture, assessment, safety case**
  - Increasing independence, …
  - increasing assessment effort, …
  - increasing tool qualification, ...
  - … the higher the ASIL.

- **Development Interface Agreements**
Functional Safety Management

**Item Development**

- 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)
## 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)

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

- **Safety mechanisms, and metrics**
  - With increasing target values for
    - Architectural metrics and diagnostic capabilities (SPFM & LFM), ...
    - Probability of failures (PMHF)
    - ... the higher the ASIL.
Fault concepts and hardware metrics:

**Architectural metrics**

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

### Single-point fault metric

\[
\text{ASIL B} \geq 90 \% \quad \text{ASIL C} \geq 97 \% \quad \text{ASIL D} \geq 99 \%
\]

### Latent fault metric

\[
\text{ASIL B} \geq 60 \% \quad \text{ASIL C} \geq 80 \% \quad \text{ASIL D} \geq 90 \%
\]
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>$&lt;10^{-8} \text{ h}^{-1}$</td>
</tr>
<tr>
<td>C</td>
<td>$&lt;10^{-7} \text{ h}^{-1}$</td>
</tr>
<tr>
<td>B</td>
<td>$&lt;10^{-7} \text{ h}^{-1}$</td>
</tr>
</tbody>
</table>

- 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.
### 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)

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

- Safety mechanisms, and metrics with increasing target values for
  - Architectural metrics and diagnostic capabilities (SPFM & LFM), …
  - Probability of failures (PMHF)
  - … the higher the ASIL.

- Safety measures (Methods, Activities)
  - Increasing formality and documentation, …
  - Increasing self-test requirements, …
  - increasing verification depth …
  - … the higher the ASIL.
Reference phase model for the software development
Reference phase model for the software development

- Traceability requirements

Traceability:

- "vertical"
- "horizontal"
Fault avoidance during software development

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

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

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchical structure of software components</td>
<td>++</td>
</tr>
<tr>
<td>Restricted size of software components(^a)</td>
<td>++</td>
</tr>
<tr>
<td>Restricted size of interfaces(^a)</td>
<td>+</td>
</tr>
<tr>
<td>High cohesion within each software component(^b)</td>
<td>+</td>
</tr>
<tr>
<td>Restricted coupling between software components(^a, b, c)</td>
<td>+</td>
</tr>
<tr>
<td>Appropriate scheduling properties</td>
<td>++</td>
</tr>
</tbody>
</table>

Table 3 — Principles for software architectural design
### ISO 26262 and “FS demonstration”

<table>
<thead>
<tr>
<th>Safety validation</th>
<th>Verification review</th>
<th>Test and verification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FS assessment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FS Audit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Confirmation review</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Confirmation measures</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Compliance

- **Correctness**
- **Completeness (technical / product)**
- **Completeness (process related)**
- **Compliance**

**CONFIDENCE**
“Certification” in a ISO 26262 context

- **Not a ISO 26262 requirement**
  - Nor in any other FuSa standard (e.g., IEC 61508, ISO 13849)
  - May be required by regulations, laws, industry associations, customers, ...
    - ISO 26262 as of today not formally required by national regulations or laws.
    - Main driver for ISO 26262 **application** is product liability (ISO 26262 represents state of the art)
    - Main drivers for ISO 26262 **certification** are customers, market situation.
    - Accredited certification provides additional legal protection
  - Benefits, value?
    - The certificate/approval/listing mark/... in itself?
    - Ideally: CONFIDENCE

- **What is available with ISO 26262 certificate:**
  - **Products** (often as SEooC)
  - **Tools** and/or associated workflows
  - **Organisations, Processes**
  - **Individuals** ("Functional Safety Engineer/Professional/Expert...")

- **Main question: how much confidence do such certificates inspire?**
  - This may trigger the following sub-questions:
    - Independent, accredited certification organisation?
    - What is the technical competency of the certification organisation?
    - Addresses compliance, or also correctness and completeness?
    - If correctness and completeness are addressed, what investigation depth and rigour were applied? How much effort spent?
    - One-off certification, or combined with surveillance or follow-up?
Competency requirements for TÜV SÜD FuSa evaluation staff

• Achievement and evaluation of functional safety requires expertise in various disciplines (in addition to appropriate domain competency):
  • quality and development process management and audit
  • hazards-based safety engineering
  • requirements engineering
  • embedded control systems engineering
  • hardware engineering
  • microprocessor technology, semiconductor technology
  • formalized and model-based software engineering
  • programming languages (C, C++, assembler)
  • hardware reliability and failure models (electric, electronic, microelectronics, electromechanical, mechanical, pneumatic, hydraulic)
  • immunity against electromagnetic phenomena and other environmental impacts
  • probabilistic modeling
  • safety analysis using formalized methods and techniques (FMEA, FTA, Markov, RBD,…)
  • verification and validation
  • construction of safety cases
FuSa Evaluation Tasks Performed by TÜV SÜD

Project accompanying, three types, and their objectives:

• Review
  • complete evaluation of key work products
    − Key WP’s: those listed for confirmation and verification review
    − Sampling, focus on critical points of WP, for detailed implementation-related WP’s, reliance on process/methods/tools
  • Completeness, correctness, compliance

• Test
  • Function, fault insertion, environmental
    − performed and/or witnessed
    − sampling, selection of ”interesting” and representative test cases
  • Completeness, correctness

• Audit in accordance with FSM documentation
  • on-site, meeting people
  • Compliance, competency, safety culture
## ISO 26262 and Certification

<table>
<thead>
<tr>
<th>Correctness</th>
<th>Completeness (technical / product)</th>
<th>Completeness (process related)</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety validation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification review</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test and verification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirmation review</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirmation measures</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**INCREASED CONFIDENCE**

Independent, accredited, competent project accompanying review, test, audit.
THANK YOU !!!

Your Comments and Questions are Welcome!

Dr.-Ing. Thomas Maier
TÜV SÜD Rail GmbH
TÜV SÜD America
10040 Mesa Rim Road
San Diego, CA 92121
T: +1 858-220-0783
E: tmaier@tuvam.com
W: http://www.tuv-sud-america.com