Measurement of Safety Integrity of E/E/PES according to IEC61508

Mr. Chen Zhenkang | TUV Rheinland Singapore
18. May. 2018 | Singapore | World Metrology Day 2018
Agenda

1. TÜV Rheinland: a Certification Body for Functional Safety
2. Functional Safety & IEC61508
3. Safety Integrity Level (SIL)
4. Fault Analysis
5. Safety-related Parameters
6. Functional Safety Management (FSM)
7. Q&A
1. TÜV Rheinland: a Certification body for Functional Safety
TÜV Rheinland

- Leading provider of technical services worldwide
- Founded in 1872 and headquartered in Cologne, Germany
- 19,000 people in more than 500 locations in 69 countries
- Our goal is to be the world’s best independent provider of technical services for testing, inspection, certification, consulting and training to the industrial, transportation and healthcare sectors
TÜV Rheinland, a Certification Body for:
Functional Safety products, Systems and Applications

Part of TÜV Rheinland certificated Functional Safety Products and/or Functional Safety Management Systems:

- ABB
- Schneider Electric
- Yokogawa
- Phoenix Contact
- SIEMENS
- Rockwell Automation
- Allen-Bradley
- HIMA
- Endress + Hauser
2. Functional Safety and IEC61508
Safety

IEC 61508-4, 3.1

Safety:

**Freedom from unacceptable risk** of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment. [IEC 61508-4, 3.1; ISO/IEC Guide 51:1999, definition 3.1]
Functional Safety:

...part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.
Functional Safety explained

Functional Safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

Functional safety is the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or provide mitigation to reduce the fight consequence of the hazardous event.

[Ref.: http://www.iec.ch/functionalsafety/explained/]
Functional Safety Examples

Functional Safety relies on **active systems**.

- **Prevention**: The activation of a level switch in tank containing a flammable liquid, when a potentially dangerous level has been reached, which causes a valve to be closed to prevent further liquid entering the tank and thereby preventing the liquid in the tank from overflowing.

- **Mitigation**: The detection of smoke by sensors and the ensuring intelligent activation of a fire suppression system.

Safety achieved by measures that rely on **passive systems** is not functional safety.

- A fire resistant door or insulation to withstand high temperatures are measures that are passive in nature and can protect against the same hazards as are controlled by functional safety concepts but are not instances of functional safety.

[Ref.: http://www.iec.ch/functionalsafety/explained/]
IEC 61508: Functional safety of E/E/PE safety-related systems

(E/E/PE: electrical/electronic/programmable electronic)

• International Standard for Functional Safety
  – Edition 2.0 : 2010

• It sets out a generic approach for all safety lifecycle activities for systems comprised of E/E/PE elements that are used to perform safety functions.

  This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series.
Generic and Sector / Application Standards

IEC 61800-5-2
Electrical Driver

IEC 61513
Nuclear Sector

IEC 60880
Nuclear Software

IEC 60335-1
Household appliance software

IEC 61511
Process Sector

ISO 13849-1
Machinery

IEC 62061
Machinery

EN 62304
Medical Software

ISO 26262
Road Vehicle

EN 50156
Furnace

IEC 61508
E/E/PES Functional Safety

IEC 61511
Process Sector

EN 50156
Furnace
3. Safety Integrity Level (SIL)
Risk

Risk (R) is the combination of the Probability (P) of occurrence of harm and the Severity (S) of that harm.

\[ R = P \times S \]

IEC61508-4: 3.1.6

Note:
The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event, and the possibility to avoid or limit the harm.
## Risk Parameter and Classification

<table>
<thead>
<tr>
<th>Risk parameter</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consequence (C)</strong></td>
<td>C&lt;sub&gt;A&lt;/sub&gt; C&lt;sub&gt;B&lt;/sub&gt; C&lt;sub&gt;C&lt;/sub&gt; C&lt;sub&gt;D&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>Minor injury</td>
</tr>
<tr>
<td></td>
<td>Serious permanent injury to one or more persons; death to one person</td>
</tr>
<tr>
<td></td>
<td>Death to several people</td>
</tr>
<tr>
<td></td>
<td>Very many people killed</td>
</tr>
<tr>
<td><strong>Frequency of, and exposure time in, the hazardous zone (F)</strong></td>
<td>F&lt;sub&gt;A&lt;/sub&gt; F&lt;sub&gt;B&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>Rare to more often exposure in the hazardous zone</td>
</tr>
<tr>
<td></td>
<td>Frequent to permanent exposure in the hazardous zone</td>
</tr>
<tr>
<td><strong>Possibility of avoiding the hazardous event (P)</strong></td>
<td>P&lt;sub&gt;A&lt;/sub&gt; P&lt;sub&gt;B&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>Possible under certain conditions</td>
</tr>
<tr>
<td></td>
<td>Almost impossible</td>
</tr>
<tr>
<td><strong>Probability of the unwanted occurrence (W)</strong></td>
<td>W&lt;sub&gt;A&lt;/sub&gt; W&lt;sub&gt;B&lt;/sub&gt; W&lt;sub&gt;C&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely</td>
</tr>
<tr>
<td></td>
<td>A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely</td>
</tr>
<tr>
<td></td>
<td>A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely</td>
</tr>
</tbody>
</table>
Risk graph acc. to IEC 61508-5
(Risk \(\rightarrow\) Intended SIL)

Starting point for risk reduction estimation

Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)

\(C\) = Consequence risk parameter
\(F\) = Frequency and exposure time risk parameter
\(P\) = Possibility of failing to avoid hazard risk parameter
\(W\) = Probability of the unwanted occurrence

\(W_3\)
\(a\)
\(1\)
\(2\)
\(3\)
\(4\)
\(b\)
---

\(W_2\)
---
a
1
2
3
4

\(W_1\)
---
---
a
1
2
3

--- = No safety requirements
\(a\) = No special safety requirements
\(b\) = A single E/E/PES is not sufficient
1, 2, 3, 4 = Safety integrity level
Safety Integrity Level (SIL)

IEC61508-4, 3.5.8

Safety Integrity Level

discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

NOTE 1 The target failure measures (see 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

NOTE 3 A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SIL n safety-related system” (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.
Measurement: Target Failure Measures

IEC 61508-1 Table 2/ Table 3

Table 2 – target failure measures for a safety function operating in **low demand mode of operation**

<table>
<thead>
<tr>
<th>SIL</th>
<th>Average probability of a dangerous failure on demand of the safety function (PFDavg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
</tr>
</tbody>
</table>

Table 3 – target failure measures for a safety function operating in **high demand mode of operation** or **continuous mode of operation**

<table>
<thead>
<tr>
<th>SIL</th>
<th>Average frequency of a dangerous failure of the safety function [h⁻¹] (PFH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-9}$ to $&lt; 10^{-8}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
</tr>
</tbody>
</table>
**Risk comparison**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Probability (per year)</th>
<th>Activity</th>
<th>Probability (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Travel</strong></td>
<td></td>
<td><strong>Voluntary</strong></td>
<td></td>
</tr>
<tr>
<td>Air</td>
<td>$2 \times 10^{-6}$</td>
<td>The pill</td>
<td>$2 \times 10^{-5}$</td>
</tr>
<tr>
<td>Train</td>
<td>$3 \times 10^{-6}$</td>
<td>Rock Climbing</td>
<td>$1.4 \times 10^{-4}$</td>
</tr>
<tr>
<td>Bus</td>
<td>$2 \times 10^{-4}$</td>
<td>Smoking</td>
<td>$5 \times 10^{-3}$</td>
</tr>
<tr>
<td>Car</td>
<td>$2 \times 10^{-4}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motorcycle</td>
<td>$2 \times 10^{-2}$</td>
<td>Meteorite</td>
<td>$6 \times 10^{-11}$</td>
</tr>
<tr>
<td><strong>Occupation</strong></td>
<td></td>
<td><strong>Involuntary</strong></td>
<td></td>
</tr>
<tr>
<td>Chemical Industry</td>
<td>$5 \times 10^{-5}$</td>
<td>Falling aircraft</td>
<td>$2 \times 10^{-8}$</td>
</tr>
<tr>
<td>Shipping</td>
<td>$9 \times 10^{-4}$</td>
<td>Natural Disasters</td>
<td>$2 \times 10^{-6}$</td>
</tr>
<tr>
<td>Coal Mining</td>
<td>$2 \times 10^{-4}$</td>
<td>Cancer</td>
<td>$2.5 \times 10^{-5}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fire</td>
<td>$2 \times 10^{-5}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Being Murdered (UK)</td>
<td>$1.3 \times 10^{-5}$</td>
</tr>
</tbody>
</table>

Comparison: SIL3 PFH = $10^{-7}$ per hour = $8.7 \times 10^{-4}$ per year means: one fault within 1100 years!
4. Fault Analysis
Systematic and random faults

IEC 61508-4 3.6.5-6

Systematic Faults
• Software Bugs
• ...

Random Faults
• Ageing or worsening of components
• Soft Errors
• ...

![Image of fault messages]
**Type of Faults**

**Fault:** abnormal condition, that may cause **loss** or at least a **reduction** of a functional unit (system or sub-system) to perform a **required function**

Which failures have to be considered?

Failure / fault

- **Systematic failure**
  - Failure with definite cause, can only be eliminated by alteration of design, production process, operating mode, operation instructions or other influencing factors

- **Random failure**
  - Failure, occurring at a random time and whose cause can not be defined distinctively

**Fault avoidance/Fault control**

**Fault control**
Phases in which systematic faults should be avoided

The following phases have to be considered acc. to IEC 61508-2 Annex B, IEC 61508-3 Annex A, B for the avoidance and control of systematic faults:

**HW development process:**
- Specification of requirements
- design and development
- integration
- operation and maintenance
- Validation

**AP (application Program) development process:**
- Specification of AP- Safety requirements
- AP-design and development
- AP-integration
- AP-Verification
- AP-Validation
- Modification
Measures to avoid systematic faults (QM) in the HW

Table B.1 of IEC 61508-2

<table>
<thead>
<tr>
<th>Technique/measure</th>
<th>See IEC 61508-7</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project management</td>
<td>B.1.1</td>
<td>M low</td>
<td>M low</td>
<td>M medium</td>
<td>M high</td>
</tr>
<tr>
<td>Documentation</td>
<td>B.1.2</td>
<td>M low</td>
<td>M low</td>
<td>M medium</td>
<td>M high</td>
</tr>
<tr>
<td>Separation of E/E/PE system safety functions from non-safety functions</td>
<td>B.1.3</td>
<td>HR low</td>
<td>HR low</td>
<td>HR medium</td>
<td>HR high</td>
</tr>
<tr>
<td>Structured specification</td>
<td>B.2.1</td>
<td>HR low</td>
<td>HR low</td>
<td>HR medium</td>
<td>HR high</td>
</tr>
<tr>
<td>Inspection of the specification</td>
<td>B.2.6</td>
<td>– low</td>
<td>HR low</td>
<td>HR medium</td>
<td>HR high</td>
</tr>
<tr>
<td>Semi-formal methods</td>
<td>B.2.3, see also Table B.7 of IEC 61508-3</td>
<td>R low</td>
<td>R low</td>
<td>HR medium</td>
<td>HR high</td>
</tr>
<tr>
<td>Checklists</td>
<td>B.2.5</td>
<td>R low</td>
<td>R low</td>
<td>R medium</td>
<td>R high</td>
</tr>
<tr>
<td>Computer aided specification tools</td>
<td>B.2.4</td>
<td>– low</td>
<td>R low</td>
<td>R medium</td>
<td>R high</td>
</tr>
<tr>
<td>Formal methods</td>
<td>B.2.2</td>
<td>– low</td>
<td>– low</td>
<td>R medium</td>
<td>R high</td>
</tr>
</tbody>
</table>

M: mandatory; R: recommended; -: no recommendation.
**Fault:** abnormal condition, that may cause loss or at least a reduction of a functional unit (system or sub-system) to perform a required function

**Which failures have to be considered?**

- **Systematic failure:** Failure with definite cause, can only be eliminated by alteration of design, production process, operating mode, operation instructions or other influencing factors.
- **Random failure:** Failure, occurring at a random time and whose cause cannot be defined distinctively.

**Fault avoidance/Fault control**

**Fault control**
Why do faults have to be controlled?

STOP

Bit fault

1110 0101b

1110 0101b

"0"

! ON !
4. Safety-Related Parameter
Functional Safety

A safety system is functionally safe if

- Random,
- systematic and
- common cause

failures do not lead to malfunctioning of the safety system and do not result in

- injury or death of humans
- pollution of the environment
- loss of equipment or production

The safety function of a device / control system has to be guaranteed both under normal conditions and in the existence of faults.
What has to be fulfilled normatively?

Normatively the following safety-related parameters have to be fulfilled depending on the intended SIL:

**Criteria 1:** The Architectural Constraints for the element

- **Route 1**\(_{H}\): Safe Failure Fraction (Refer: 7.4.4.2 of IEC 61508-2: 2010)
- **Route 2**\(_{H}\): Assessment of reliability data (Refer: 7.4.4.3 of IEC 61508-2: 2010)

**Criteria 2:** Target Failure Measures for a safety Function

- **PFD\(_{avg}\):** for low demand operation mode (refer: table 2 of IEC 61508-1: 2010)
  
  Average probability of a dangerous failure on demand of the safety function

- **PFH:** for high demand mode and continuous Mode (refer: table 3 of IEC 61508-1: 2010)
  
  Probability of a dangerous failure of the safety function per hour

---

How do you start and what is the basis of all this?
Failure consideration acc. To IEC 61508

Basis for the calculation of safety-related parameter

Total of all failures $\lambda$
Failure consideration acc. To IEC 61508

Basis for the calculation of safety-related parameter

Total of all **safe** failures $\lambda_s$

Total of all **unsafe** failures $\lambda_D$
Failure consideration acc. To IEC 61508

Basis for the calculation of safety-related parameter

Total of all safe failures $\lambda_s$

Total of all unsafe, not detected failures, $\lambda_{Du}$

Total of all unsafe, detected failures $\lambda_{DD}$
Safe failure fraction SFF

(with diagnostic)

$$SFF = \frac{\lambda s + \lambda DD}{\lambda}$$

Total of all safe and detected failures

Total of all failures

(With diagonalic)
Hardware Fault Tolerance (HFT)

Basis for the calculation of safety-related parameter

General: A HFT = N means that N + 1 faults can lead to a loss of the safety function.
Criteria 1:
Architectural Constraint: Route 1H based on SFF

IEC 61508-2: Table 2/Table 3

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60 %</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>60 % - &lt; 90 %</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>90 % - &lt; 99 %</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 60 %</td>
<td>not allowed</td>
<td>SIL1</td>
</tr>
<tr>
<td>60 % - &lt; 90 %</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>90 % - &lt; 99 %</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
</tbody>
</table>
\( \lambda_{Du} \) really bothers you: it will make that the safety system cannot perform the action. It’s the only one that goes into the \( \text{PFD}_{AV} \) calculation.
Average Probability of Failure on Demand (PFDAV)

Random faults occurs satirically distributed meaning at the beginning until the end of a considered time frame.

Therefore only the average value will be considered.
For a single channel system the $PFD_{AV}$ can be determined as:

$$PFD_{AV} = \frac{1}{2} \lambda_{DU} \cdot T_1$$

$T_1$ is the considered time interval (Proof Test Interval)
... for the detection of failures ($\Lambda DU$)..., so that, if necessary, the system can be restored to an “as new” condition or as close as practical to this condition.
Proof Test Interval (PTI)

... “as new” condition...

1)… in practice *100% is not achievable* for other than *low-complexity* safety-related systems. But this should be the target.

2) As a *minimum*, *all the safety function* which are executed *are checked* according to the safety requirements specification.

**Meaning:**

- Only for *simple* (not electronically) system the condition, “as new” can be *achieved* by a test of the *safety function* during the PTI.

- For complex (electronically/programmable) *systems* the condition “as new” cannot only *be achieved* by a *test of the safety function* during the PTI.
Therefore:

• In case of complex systems a PTI > 10 years should be aimed at, as the necessary high diagnosis detects many failures.

• Otherwise the complex systems should be checked by the manufacturer during the proof test or should be replaced by a new system.

• The product life cycle shall not exceed the proof-test interval

Target: product life cycle < proof-test interval (PTI)
Average probability of failure on demand (PFD\textsubscript{AV})

For a two channel system the PFD\textsubscript{AV} can be determined as:

\[
PFD_{AV} \approx \lambda_{CH1} \cdot \lambda_{CH2} \cdot \frac{T_1^2}{3} + \frac{\beta}{2} \cdot (\lambda_{CH1} + \lambda_{CH2}) \cdot \frac{T_1}{2}
\]

Consideration of common cause failures in case of multi channel system shown by $\beta$. 

TÜVRheinland®
Criteria 2:
Target Failure Measures

IEC 61508-1 Table 2/ Table 3

Table 2 –target failure measures for a safety function operating in low demand mode of operation

<table>
<thead>
<tr>
<th>SIL</th>
<th>Average probability of a dangerous failure on demand of the safety function (PFDavg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ 10^{-5} to &lt; 10^{-4}</td>
</tr>
<tr>
<td>3</td>
<td>≥ 10^{-4} to &lt; 10^{-3}</td>
</tr>
<tr>
<td>2</td>
<td>≥ 10^{-3} to &lt; 10^{-2}</td>
</tr>
<tr>
<td>1</td>
<td>≥ 10^{-2} to &lt; 10^{-1}</td>
</tr>
</tbody>
</table>

Table 3 –target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

<table>
<thead>
<tr>
<th>SIL</th>
<th>Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ 10^{-9} to &lt; 10^{-8}</td>
</tr>
<tr>
<td>3</td>
<td>≥ 10^{-8} to &lt; 10^{-7}</td>
</tr>
<tr>
<td>2</td>
<td>≥ 10^{-7} to &lt; 10^{-6}</td>
</tr>
<tr>
<td>1</td>
<td>≥ 10^{-6} to &lt; 10^{-5}</td>
</tr>
</tbody>
</table>
6. Functional Safety Management (FSM)
Why is FSM necessary?

Aim: Avoidance of specification-, design-, development-, manufacturing- and commissioning errors

Source: "Out Of Control", Composition of incidents that occurred to control systems, carried out by UK HSE (September 2004)
A Safety system is only as safe as the process that developed it:

- Integrates to existing management systems and business processes e.g. quality management, safety management, project execution, engineering management, systems engineering, procurement, supplier management, maintenance management.

- Covers the appropriate phase of the lifecycle e.g. PH&RA, Design and Engineering, operation

- Covers the competency and responsibilities of the organization performing the work
Who makes what?

IEC 61508-1, 6.2

- **Organisations / Departments**
  shown in an organisation chart

- **Persons**
  shown in a table

<table>
<thead>
<tr>
<th>name</th>
<th>Role in project</th>
<th>comp. departm.</th>
<th>qualification competence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pete Smith</td>
<td>project-leader</td>
<td>ASI / develop.</td>
<td>experiences in similar complex projects</td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...?
### Who is responsible for what?

IEC 61508-1, 6.2

<table>
<thead>
<tr>
<th>Phase</th>
<th>Life cycle Milestone</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Safety requirement specification (SRS)</td>
<td>Mr. Miller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Normative lifecycle phases are not mandatory
- Other project specific or company specific lifecycles are permitted
- Additional phases or sub-phases may be necessary to describe a product life cycle.
When do we do what?

IEC 61508-1, 6.2

<table>
<thead>
<tr>
<th>Phase</th>
<th>Life cycle Milestone</th>
<th>Responsible</th>
<th>Input documents</th>
<th>Output documents</th>
<th>Verification</th>
<th>Assessment FS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Safety requirement specification (SRS)</td>
<td>Mr. Miller</td>
<td>Marketing requirements Meeting minutes of marketing department</td>
<td>SRS</td>
<td>Mr. Smith</td>
<td>TÜV Rheinland</td>
</tr>
<tr>
<td>.....</td>
<td>SRS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- At the end of a phase, the **results** have to be summarized in an **“output” document**.
- The **verification of an “input” to “output” document** has to be performed by an assigned person.
How to “verify”?

IEC 61508-1, 6.2

<table>
<thead>
<tr>
<th>Phase</th>
<th>Life cycle Mile stones</th>
<th>Techniques and measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Safety requirement specification (SRS)</td>
<td>See IEC 61508-2 table B.1</td>
</tr>
<tr>
<td>2</td>
<td>...</td>
<td>See IEC 61508-2 table B.1</td>
</tr>
<tr>
<td>3</td>
<td>...</td>
<td>See IEC 61508-3 Annex B, table B.7</td>
</tr>
<tr>
<td>.....</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Company own measures, guidelines are also allowed.
- The applied measure for fault avoidance does not have to be indicated explicitly. It should rather be defined what measures are taken.
Competence

IEC 61508-1, 6.2
i.e. training, technical knowledge, experience and qualifications
For improvement:
… by participations on
Trainings and Workshops for Functional Safety…

TÜV Rheinland offers a wide range of program on this subject.
What requirements do suppliers have to fulfill?

EC61508-1, 6.2

- Suppliers are for example manufacturers of printed circuit boards or electronic manufacturing services or in general the production

- List of suppliers, their component and/or devices

- Does the supplier have a quality management system acc. to ISO 9001?

- Is an equivalent quality standard applied?

**General:**
An adequate quality management system **has to exist.**
Who assesses the functional safety?

IEC 61508-1, 8

• Normative level of independence (Table 5 IEC 61508-1):

<table>
<thead>
<tr>
<th>Minimum level of independence</th>
<th>Safety integrity level/Systematic capability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Independent person</td>
<td>X</td>
</tr>
<tr>
<td>Independent department</td>
<td>X2</td>
</tr>
<tr>
<td>Independent organization</td>
<td>X2</td>
</tr>
</tbody>
</table>

NOTE: See 8.2.15, 8.2.16 and 8.2.18 for details on interpreting this table.

• For SIL2 & SIL3 an independent organization generally is involved.

• Advantage in competition
  
  X: minimum level of independence
  
  X2 is more appropriate than X1 due to: lack of experience, higher degree of complexity, greater degree of novelty of design/technology.
  
  Y: the level of independence is considered as insufficient.
What do we do in case of modifications?

IEC 61508-1, 6.2

Procedures shall be developed for:
- **initiating modifications** to the E/E/PE safety-related systems (see IEC 61508.1, 7.16.2.2);
- **obtaining approval and authority** for modifications.
How do we keep the documents together?

IEC61508-1, 6.2 Configuration management

• What kind of configuration controls are available?

• Definition of all parts of a system for example by release lists with date, checksums, size of data, amount of pages and document checksum

• How can it be avoided that unauthorized components are implemented?
What has to done after a (dangerous) incident?

IEC61508-1, 6.2

**Dangerous incidents** or incidents with a possibility to produce hazards…

have to be **analyzed**…

to minimize the probability of a repeat occurrence.
Management of Functional Safety

Safety-Plan
• Who is doing what?
• What kind of development phases (milestones) exist?
• Who is responsible for which development phase?
• What are the input and output information about each phase?
• How are the output information verified to the input information?
• How are modification handled?
• How is the consistency of documents assured?
• What type of quality management do suppliers have?

Verification and Validation (V&V) Plan
• Which measures for fault avoidance have been applied?
• Are the V&V results documented?
• Are the V&V tools documented?
7. Q&A
About me

Mr. Chen Zhenkang
• FS Assessor for process industry, TUV Rheinland Asia Pacific
• Head of Industrial Services, TUV Rheinland Singapore

Expertise:
• Safety Instrumented Systems
• Functional Safety Management
• Safety Life-Cycle Management
• Functional Safety Assessment

Knowledge of Major Design Code:
• IEC61508
• IEC61511

Contact:
• Email: zhenkang.chen@tuv.com
• Phone: + 65 9114 9987