

Functional Safety

IEC 61508

NPSS Presentation Oct 24, 2007

Functional Safety

- Issues to be discussed:
 - Overview of Functional Safety
 - Main Aspects of Functional Safety and how IEC 61508 relate
 - Certification Process
 - Functional Safety Management
 - Hardware Analysis
 - Software Analysis

Overview of Safety

In the Past:

- All safety related standards took a deterministic view of safety

Results:

- Different safety philosophies and requirements
- Mainly oriented to low complex components

Overview of Safety

Today:

- Design's have become more complex
- Complex components have become part of most safety designs
- Industries want safety design's to reduce Risk to person, environment and to be cost effective
- Designer's want standards to be application independent
- Way to reduce systematic failures

What is Functional Safety?

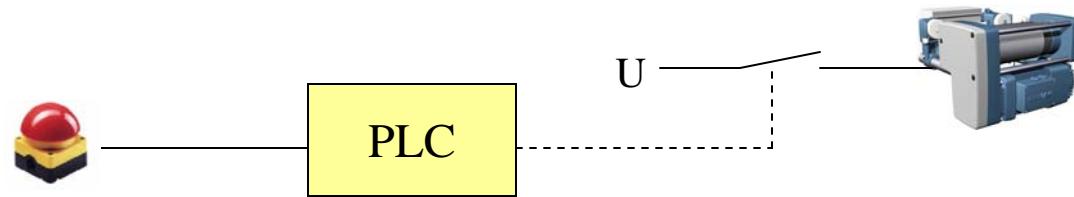
Functional Safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.
(per IEC 61508-0)

Functional Safety is the way to evaluate and determine the risk of using complex and simple circuit to perform a safety function. The safety function must always be performed under normal/undisturbed conditions and under fault conditions (Fail Safe).

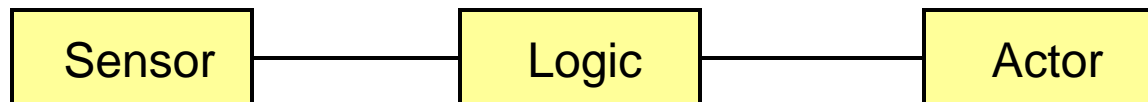
Note: Neither safety or functional safety can be determined without considering the system as a whole and the environment with which they interact.

What is a Safety Function ?

A **function** of a safety related system to reduce the risk in an application with the goal **to achieve a safe state**.



The safety function is always related to a **safety loop**, not to a component or device.



Brief History of Functional Safety

- In Germany in the 1980's it was recognized that there was a need for a method in which complex device could be evaluated as part of the safety function.
- As such DIN V VDE 0801 was introduced.
- Over time this grew and formed the basis for the IEC 61508 standard

IEC 61508

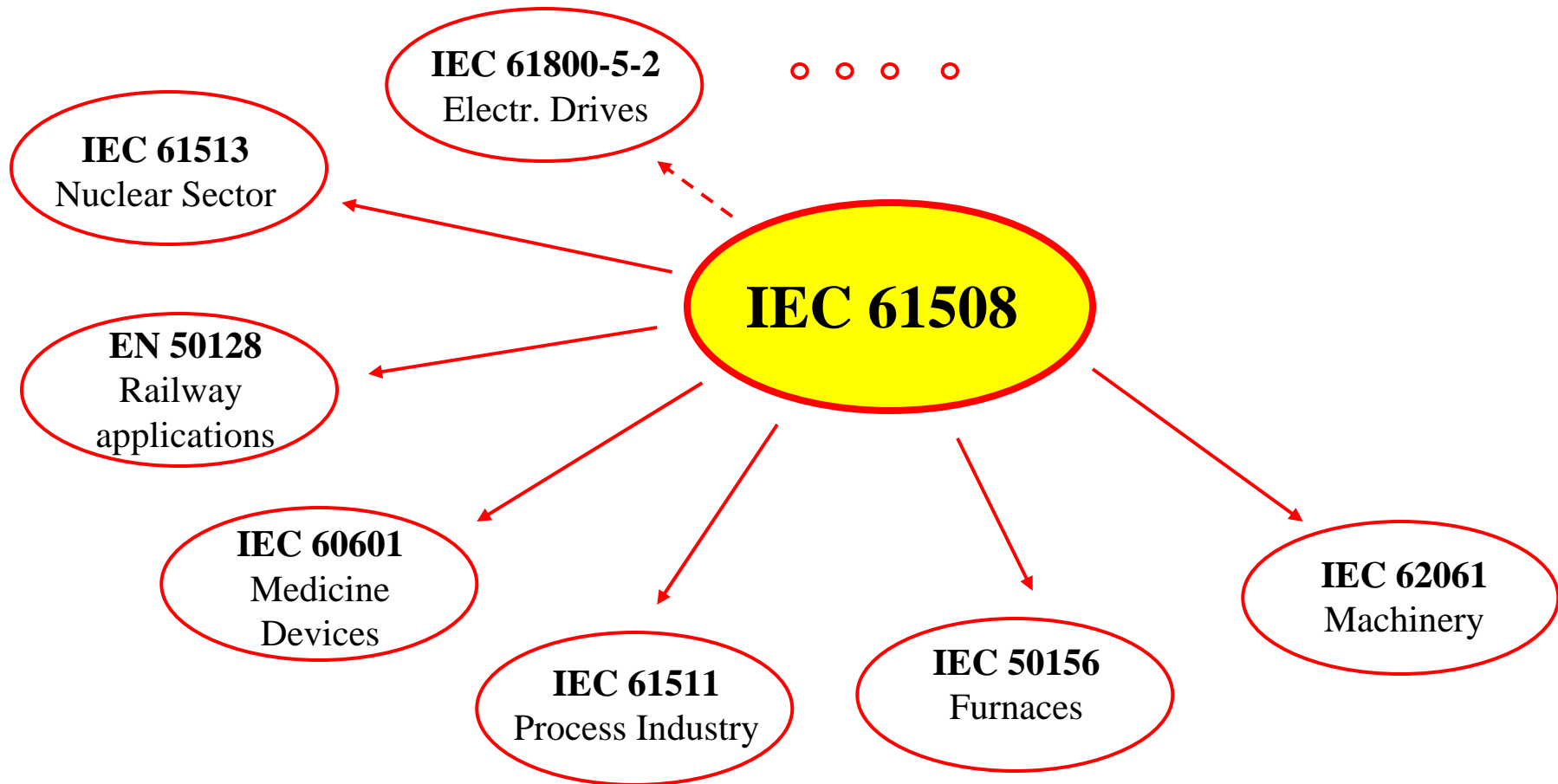
Features of IEC 61508

- Application independent but risk based-(SIL) dependent requirements
- Technology dependent / Application independent
 - Applicable for equipment/devices and complete installations, plants
- Includes the complete life-cycle of a product (Concept, Design, Implementation and De-commissioning)
- SIL is identified by:
 - Application of suitable and adequate measures for fault avoidance during the relevant life-cycle phases (QM), installation and application of a Functional Safety Management System
 - Complete documentation of design and the applied QM measures during all life-cycle phases (reproducibility)
 - Measures for fault detection and control (diagnostics)
 - Residual probability for a dangerous failure has to be less than the acceptable limit value (safety-related reliability).

Advantages of IEC 61508

- International basic safety standard, which describes the state-of-the-art of safety engineering in all aspects.
- The application of this standard is of great advantage, especially concerning the development of complex systems, reduces planning and development risks.
- The application of the life-cycle model reduces delays during development and product launch and reduces the danger, to be confronted with unpleasant surprises during the development phase.
- Product- and application independent, however risk-dependent requirements; so a comparable safety level for the protection of comparable risks is achieved
- The probability for the occurrence of faults is considered; so the measures for fault detection and control can be adjusted accordingly.
- Requires the consideration of complete safety functions.
- Is a basic standard for the development of safety-related products, which are applied within the application area of the sector standard IEC 61511, EN 50156, IEC 62061, etc.

Basic Standard and Sector-Application Standard



Weakness of IEC 61508

- Large effort for documentation, which in case of development of low complex products is disadvantageous and causes considerable time delay.
- Comprehensive standard and not easy to read and to understand for a layman.

Legal Position of EN 61508

- Not a harmonized standard in the sense of an European Directive
- Can not be used exclusively for the proof of CE-conformity
- Application and compliance with the standard is voluntary, but recommendable, especially for programmable and complex electronic systems, like Safety PLCs e.g.. Only in this case it can be guaranteed, that the required safety objectives are achieved.
- Application of the standard are recommendable for reasons of product liability, because it describes the state-of-the-art of safety (good engineering practice).

Range of Application

Safety-related applications, endangering people and environment

- Industrial machinery
- Automated production lines (robots, etc.)
- Chemical industry (measuring, control and monitoring equipment)
- Oil-rigs, oil platforms
- Nuclear power plants
- Furnaces (flat heating -- power station)
- Elevators, conveyors
- Stage machinery at theatres and opera houses
- Radio control for hoists, locomotives
- Special purpose vehicles (garbage truck, crane truck, machines for constructural engineering, etc.)
- and more

Examples of Test Objects

- Safeguards and safety components at machinery (electro-sensitive protective equipment, e.g.)
- Programmable or configurable controllers with safety functions
- Drive systems with safety functions
- Bus systems, devices with safety related bus communication
- Electronic controls in nuclear power plants
- Furnaces, controls and safeguards for fuel / air
- Safety related modules and components (relays with forcibly guided contacts, position switches, valves, ASICs, e.g.)
- Software products (compiler, programming- and configuration tools, operating systems, ...)
- and more

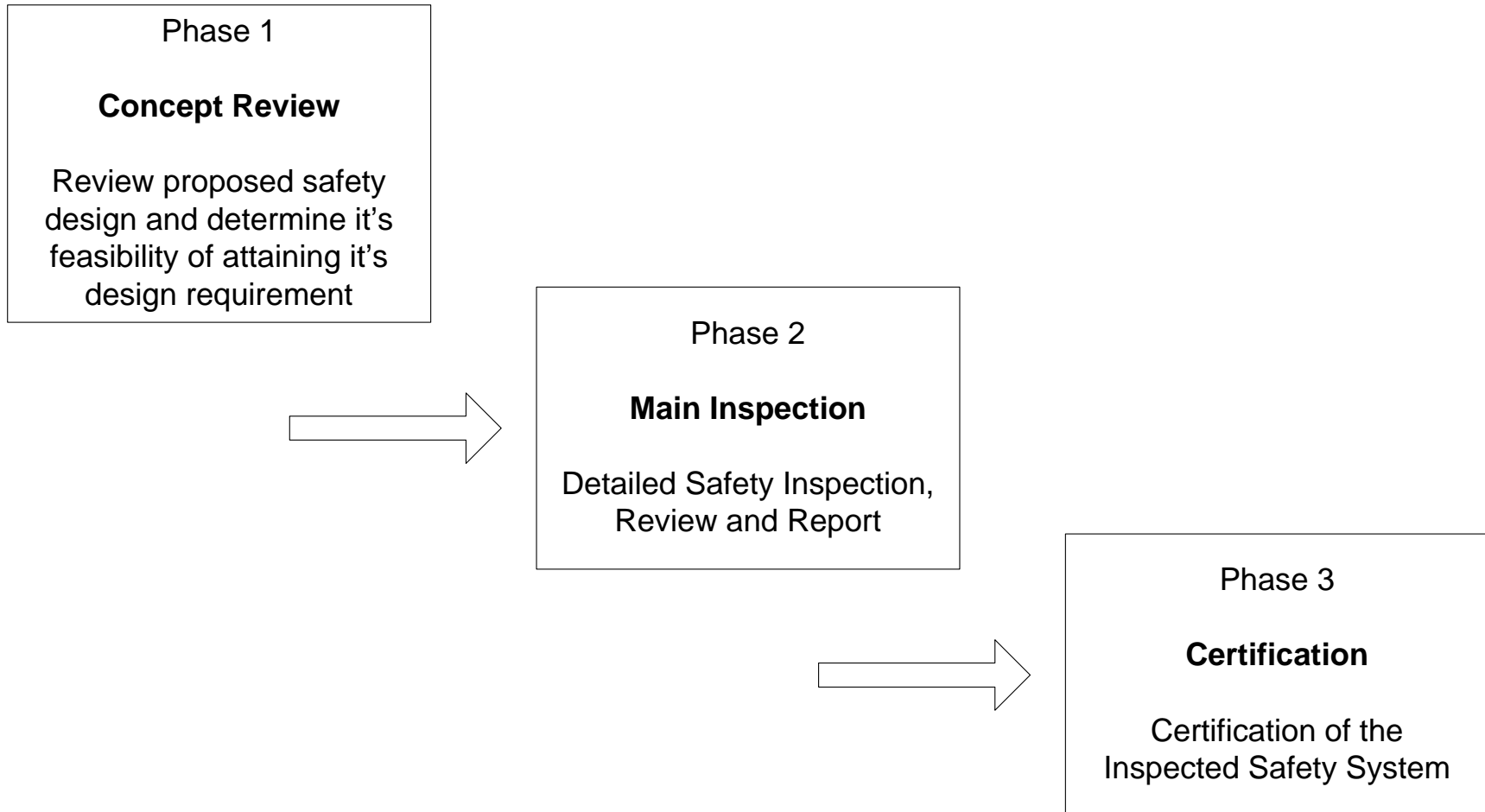
Certification Process

24-Oct-07

TÜV Rheinland Service GmbH



Certification Process



Concept Review

Object / Test Phase	Method	Results / Objective
<ul style="list-style-type: none">• Required Task / Application	<ul style="list-style-type: none">• Assessment / Analysis	<ul style="list-style-type: none">• Classification of a requirement class (RC) and respective safety integrity level (SIL)
<ul style="list-style-type: none">• Required Specifications / Safety Concept	<ul style="list-style-type: none">• Inspection / FMEA	<ul style="list-style-type: none">• Authorized and valid requirements, specifications and safety concept
<ul style="list-style-type: none">• Task Plan for the Main Inspection	<ul style="list-style-type: none">• Inspection / Analysis	<ul style="list-style-type: none">• Valid test plan for hardware, software and system integration
<ul style="list-style-type: none">• Results	<ul style="list-style-type: none">• Writing Report	<ul style="list-style-type: none">• Authorize report documenting the performance of the system to meet the requirements and identify critical areas of the design that need to be addressed in the design before the main review

Main Inspection (FSM)

Object / Test Phase	Method	Results / Objective
<ul style="list-style-type: none">• Project Management Documentation	<ul style="list-style-type: none">• Inspect Documentation	<ul style="list-style-type: none">• Review Project management Documentations
<ul style="list-style-type: none">• Required Specifications / Safety Concept	<ul style="list-style-type: none">• Inspect Documentation	<ul style="list-style-type: none">• Confirmation of Documentations
<ul style="list-style-type: none">• Manufacturing Documentation Task	<ul style="list-style-type: none">• Inspect Documentation	<ul style="list-style-type: none">• Inspect Manufacturing Procedure and Certifications
<ul style="list-style-type: none">• User Documentation	<ul style="list-style-type: none">• Inspect Documentation	<ul style="list-style-type: none">• Review Documentations and verify it meets the Requirements

Main Inspection (Hardware)

Object / Test Phase	Method	Results / Objective
<ul style="list-style-type: none">• All Components	<ul style="list-style-type: none">• Inspection of Documentation• Visual Inspection of Components and Modules• Inspection of Electrical safety, shielding and earthing• Practical Function Tests	<ul style="list-style-type: none">• Confirmation of Requirements Specified in the Concept Review• Confirmation of Consistency to Documentation• Confirmation of Efficiency• Confirmation of Consistency with Documentations

Main Inspection (Hardware)

Object / Test Phase	Method	Results / Objective
<ul style="list-style-type: none"><li data-bbox="197 618 533 699">• Safety relevant Components<li data-bbox="197 870 533 911">• Power Supply	<ul style="list-style-type: none"><li data-bbox="793 618 1262 756">• Analysis of the Functions, FMEA, dimensioning and load conditions<li data-bbox="793 854 1262 979">• Inspection of decoupling, protection high-, low-voltage power interruption	<ul style="list-style-type: none"><li data-bbox="1381 618 1885 846">• Confirmation of consistency to the requirements and documentation, definition of test cases<li data-bbox="1381 911 1885 951">• Confirmation of measures

Main Inspection (Software)

Object / Test Phase	Method	Results / Objective
<ul style="list-style-type: none">• Software Specification	<ul style="list-style-type: none">• Inspection of Functional Safety Development Rules and Quality Management	<ul style="list-style-type: none">• Confirmation of Requirements and Definition of Test Cases
<ul style="list-style-type: none">• Software Modules	<ul style="list-style-type: none">• Inspection to development guide lines, static analysis and inspection of test results	<ul style="list-style-type: none">• Confirmation that the design requirements are met

Main Inspection (Software)

Object / Test Phase	Method	Results / Objective
<ul style="list-style-type: none">• Software Module for Safety Functions	<ul style="list-style-type: none">• Additionally to Other Software modules: White Box Testing	<ul style="list-style-type: none">• Confirmation that the Safety Requirements are Met
<ul style="list-style-type: none">• Integration of Software and System	<ul style="list-style-type: none">• Dynamic Analysis and Functional Testing	<ul style="list-style-type: none">• Confirmation that the Safety Requirements are Realized

Main Inspection (Software)

Object / Test Phase	Method	Results / Objective
Application Programming		
<ul style="list-style-type: none">• Programming Applications	<ul style="list-style-type: none">• Inspection / Functional Test	<ul style="list-style-type: none">• Confirmation that the Safety Requirements are Met
<ul style="list-style-type: none">• Languages	<ul style="list-style-type: none">• Functional Test	<ul style="list-style-type: none">• Confirmation that the Safety Requirements are Met
Development Tools		
<ul style="list-style-type: none">• Compiler, assembler, Libraries , Tools, Etc	<ul style="list-style-type: none">• Assessment of Operation Proof and Validation	<ul style="list-style-type: none">• Confirmation and Validation Report

Main Inspection (Integration Testing)

Object / Test Phase	Method	Results / Objective
PE System under Test		
<ul style="list-style-type: none">• System and Safety Function	<ul style="list-style-type: none">• Black-Box-Testing, Performance of Safety Requirements	<ul style="list-style-type: none">• Confirmation of the Specific Functions and Efficiency
<ul style="list-style-type: none">• Environmental Conditions	<ul style="list-style-type: none">• Environmental Tests	<ul style="list-style-type: none">• Confirmations of the requirements
<ul style="list-style-type: none">• Results of the Type Approval	<ul style="list-style-type: none">• Reports of the Results	<ul style="list-style-type: none">• Final Report:<ul style="list-style-type: none">– Identifying the units SIL Level and Safety Parameters– Identifying an conditions of operation required to meet safety

Certification

Certification

Review of the carried out Inspection
 Review of the Test Results
 Issue of the Certificate



Benefits of a Functional Safety Type Approval

Proof of Sufficient Measures against Failures in the Hard- and Software
 Use of the Type Approval System in Different Applications.
 Fundamental Safety Functions of the System are Covered.

24-Oct-07

TÜV Rheinland Service GmbH



TUV Services

- **Consulting** Requirements concerning Functional Safety
- **Tests / Analysis**
 - Type approvals with optional certification
 - Software tests (application software, compiler)
 - Environmental tests (temperature, climatic, mech. stability, EMC, etc.)
 - Calculation of safety related reliability quantities
 - Failure mode and effect analysis (FMEA)
- **Certifications**
 - Certification and Marking
 - Functional Safety Management
- **Trainings/Workshops**
 - In-house Trainings
 - TÜV Functional Safety Program
 - Various Workshops

Automation, Software and Information Technology (ASI)

USA

TUV Rheinland of North America, Inc.
Matthias Haynl
Paul Silva
1300 Mass Ave, Ste #103
Boxboro, MA 01719 - USA



001 – 978 -266-9500
Fax 001 – 978 -266-9992
Mail mhaynl@us.tuv.com
psilva@us.tuv.com

www.us.tuv.com

Germany

TÜV Rheinland
Industrie Service GmbH
Heinz Gall
Am Grauen Stein
D-51105 Cologne



0049 – 221 – 806 1790
Fax 0049 – 221 – 806 1539
Mail tuevat-asi@de.tuv.com

www.tuvasi.com

Japan

TUV Rheinland Japan Ltd.
Joachim Iden
Wakasugi Center Bldg
Honkan 16F
Higashi Tenma 2-9-1
Kita-ku, Osaka - JAPAN



0081 – 66355-5732
Fax 0081 – 66354-8636
Mail ji@jpn.tuv.com

www.jpn.tuv.com

For Additional Information Visit
WWW.TUVASI.COM

24-Oct-07

TÜV Rheinland Group
TÜV Rheinland Service GmbH

 **TÜVRheinland®**
Precisely Right.