IEC 61508, IEC 62061, EN/ISO 13849
The impact to certification and users

Heinz Gall
TÜV Rheinland Group
TÜV Rheinland Industrie Service GmbH

Business Unit
Automation, Software and Information Technology (ASI)

gall @ de.tuv.com
www.tuvasi.com
Contents

- Information about TÜV Rheinland
- Standards development, History of functional safety standards
- Principle of standards
- Standards in Machinery Applications
- Comparison of IEC and ISO standards
- Summary regarding the standards
- Needed information for the user
- Type approval and certification
Overview: TÜV Rheinland Group

- As an international service group we document the safety and quality of new and existing products, systems and services

- **Worldwide**
  - 62 Countries
  - 360 Sites

- **Europe**
  - 19 Countries
  - 91 Sites

- **Employees worldwide**
  - approx. 12500
Overview: TÜV Rheinland Group

31 Business Fields structured in 6 Business Sectors

- Mobility
- Products
- Life Care
- Education and Consulting
- ...
- Industrial Services

The business unit Automation, Software and Information Technology (ASI) is part of the business sector Industrial Services.
Activities in the functional safety area

● Approval and Certification of E/E/PES equipment
  ● used in safety-related applications

● Certification of Functional Safety Management Systems
  ● for manufacturers, system integrators, end users
    according to the requirements of IEC 61508 / IEC 61511 / …

● Certification of Functional Safety Experts and Engineers
  ● according to the TÜV Functional Safety Programme

● Consulting regarding Functional Safety Requirements

● Certification of Safety Instrumented Systems
  ● in the process and machinery industry
History of standards

- The **first international standard** for **Functional Safety** was IEC 61508 published in 2000.

- IEC 61508 is the **basic** or umbrella **standard** for the **Functional Safety area**

- New application standards are based on IEC 61508 requirements

- The first application standard based on IEC 61508 was IEC 61511 for the process industry, Safety Instrumented Systems, in the US this is published in ISA S84…

- More and more application areas are following this way
Relation IEC 61508 and Application Standards

Application standards define for example:
- Safe state of the process: energised / de-energise
- Reaction time: milliseconds / seconds
- Demand rate: low demand / high demand
- Environmental conditions: Temperature, EMC …
Principal of the Functional Safety Standards

- Risk oriented
- Principal of Risk Reduction
- Management of Functional Safety
- Life-cycle oriented
- Definition of:
  - safety-related functions
  - Safety Integrity Level (SIL), Performance Level (PL), Safety Category (SC)
- Quantitative requirements to the Probability of Dangerous Failure
Safety Related Function

Consisting of Input, Output, Controller, Communication and power supply

Sensor → E / E / PES → Actuator

35%  15%  50%

e.g. Communication network - Failure rate of all nodes in a network < 1% of the related SIL-level regarding the communication part
Safety Related Function example

\[ \text{PFH}_{\text{tot}} = \text{PFH}_{\text{LS}} + \text{PFH}_{\text{LC}} + \text{PFH}_{\text{RemoteIO}} + \text{PFH}_{\text{BusNode}} + \text{PFH}_{\text{Controller}} + \text{PFH}_{\text{RemoteIO}} + \text{PFH}_{\text{Contactors}} + \text{PFH}_{\text{Motor}} \]
Functional Safety Definition

• Safety systems can fail because of...
  • Random failures
  • Common cause failures
  • Systematic failures

• IEC 61508 defines functional safety as follows
  • part of the overall safety relating to the EUC and the EUC control system which
depends on the correct functioning of the E/E/PE safety-related systems, other
technology safety-related systems and external risk reduction facilities

• A safety system is functionally safe if (more practical definition)
  • 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
      – Spills to the environment
      – Loss of equipment or production
Summary of requirements in general

● All systems have to fulfil the following requirements:
  ● Measures to avoid and control failures especially **systematic failures** in HW/SW, applied during design and development
  ● Architectural constraints (SFF and HFT) including diagnostic
  ● Probability of dangerous failure

● While applications shall not be unconsidered.
  e.g. reaction time, safe state, environmental conditions
European Machinery Directive (MD) as an example

- A machine according to the Machinery Directive
  - is an assembly of linked parts, from which at least one must be movable, with the appropriate actuators, control and power circuits.
  - Simple machine / Complex machinery (assembly of machines)
- The manufacturer resp. whoever puts the machine into market
  - is committed to meet the essential safety and health requirements not only of the Machinery Directive but also of all other relevant European Directives. This has to be shown by an according documentation - (Declaration of Conformity).
- A systematic analysis is necessary in order to identify all dangers and risks, which originate from the machine.
  - Under consideration of these dangers the machine has to be designed and constructed in such a manner, that all dangers are eliminated or at least are limited to a minimum.
    → Risk analysis is required!
    → This includes the control system, safety system!
Situation in machinery applications (10.2008)

Currently **3 equivalent harmonized Standards**
- in the application area of the European Machinery Directive for Functional Safety at Machinery:
  - EN 954-1:1996
  - EN ISO 13849-1:2006
  - EN 62061:2005

**EN 954-1 will become invalid in 12.2009**
- Latest from 12.2009 the **deterministic approach** of failures acc. to EN 954-1 is not sufficient any more and has to be substituted (**EN 62061**) or at least must be supplemented (**ISO 13849-1**) by the **probabilistic approach**.

For any safety function the probabilistic proof has to be supplied that the residual probability of a dangerous failure of the safety function is lower than allowed according to the results of the risk evaluation.
Why 2 standards for apparently the same?

- **Competition between 2 technical committees**
  - (IEC/TC44, ISO/TC199) during the development led to 2 Standards, which consciously differ from each other (different naming, methods etc.)

- Result are **2 Standards, which are - by definition - equivalent and compatible**

- Citation of ISO 13849-1 clause 1 (Scope):
  - "The requirements provided in this part of ISO 13849 for programmable electronic systems are compatible with the methodology for the design and development of safety related electrical, electronic and programmable electronic control systems for machinery given in IEC 62061."
Why 2 standards for apparently the same?

- **EN/IEC 62061**
  - is the consequent implementation of the generic functional safety Standard IEC 61508 for the application area safety of machinery

- **EN ISO 13849-1**
  - is the adherence to the approved deterministic approach of failures known from EN 954-1, unavoidably supplemented by qualitative (QM) and quantitative (MTTFd, DCav, CCF) aspects coming from IEC 61508

- The different approaches existing in the predecessor Standards (deterministic approach of EN 954-1 and probabilistic approach of IEC 61508) have not been removed.
  - A first step to converge or to merge has been performed.
Key Requirements acc. to ISO 13849-1

**Quantifiable Requirements:**
- Quality of the HW (MTTFd)
- Quality of the measures to detect failures (DCav)
- Sufficient measures against common cause failures (CCF)

**Qualitative (non-quantifiable) Requirements:**
- Sufficient safety integrity at failures acc. to the safety categories (deterministic approach of failures)
- Application of measures to avoid systematic failures (QM)
- Verification and validation
Measures to avoid failures:

- Installation and application of a QM-System (FSM), which provides procedures, in order that failures are avoided as much as possible during the various product life-cycle phases.
- This includes the documentation: Plans for all verification and validation activities, test and review records, etc...

Systematic Safety Integrity

Measures to detect and to control failures:

- Design/Realization of the safety related functions in order that failures/faults do not result in a loss of the safety.
- Residual probability of a dangerous failure less than allowed:
  \[ \text{PFH} \leq \text{PFHSILXmax} \]

Hardware Safety Integrity

Key requirements acc. to IEC 62061
Measures to avoid Systematic Failures

- **ISO 13849-1**:  
  - Considers particularly the life-cycle of the SW  
  - Application of a simplified V-model  
  - Requirements graduated according to the target PL  
  - However better understandable, easier to apply, more related to practice, not as complex as in IEC 61508

- **Target**:  
  - Readable, understandable, testable and maintainable SW

- No requirement to apply a full FSM system

- For products with complex programmable electronic in PL e this way is not allowed!
Measures to avoid Systematic Failures

● **EN 62061:**
  ● The essential elements are taken from IEC 61508-3
  ● Degree of measures (Annex C) is between those in IEC 61508-3 and ISO 13849-1.
  ● Additionally the application of a Management System for Functional Safety (FSM) is required:
    ● Functional Safety Plan (Safety Plan) with definition of the responsibilities
    ● Plan of all verification and validation activities (V&V Plan)
Calculation of Safety Related Reliability

- Quantitative proof of the safety related reliability according to both Standards very different!
- **EN 62061:**
  - Requires the calculation of the dangerous failure rate PFH besides the HFT and SFF for the proof of the HW Safety Integrity
  - Calculations are performed after comprehensible mathematical equations on the basis of the results of the FMEDA; intermediate step determination of the common cause factor $\beta$
  - Special know-how, knowledge of the IEC 61508 necessary
  - Results are depending on assumptions made
  - Mis-use of the calculated PFH- values, comparison with the values of the competitors
Proof of the Quantitative Requirements

- **ISO 13849-1:**
  - Attempt to manage it without special knowledge of the IEC 61508
  - Separate consideration of the category, quality of the HW (MTTFd), quality of the measures to detect failures (DCav) and common cause failures (CCF).
  - Results are merged and determine the PL.
Proof of the Quantitative Requirements

- **ISO 13849**
  - Application only allowed, if the safety structure corresponds to the designated architectures in the Standard,
  - which in practice is sometime not the case:
    - Then you could not use the procedures acc. to ISO 13849-1 in a simple way
  - Procedures very conservative, often the results of these simplified procedures are not sufficient
Comparison ISO 13949 – IEC 62061

- **Advantage ISO 13849-1 (a.o.):**
  - Includes also non-electrical components
  - Considers the maximum operating time of components with wear out:
    \[ T_{10d} = 0.1 \times MTTF_d = B_{10d}/nop \]
  - Result of the assessment of a safety function: Designation of the PL, no value for the dangerous failure rate (PFH)

- **Advantage EN 62061 (a.o.):**
  - Applicable for all architectures, electrical technologies and all safety levels (universally applicable for all electronic controls)
  - Calculation with \( \lambda \)-values, in comparison calculation with MTTF-values at ISO 13849-1
  - SIL-classification represents the connection with other safety related applications, as process industry, furnaces, automotive and others
Summary
ISO 13849 and IEC 62061

● Coexistence of both standards actually necessary,
  ● as one Standard does not cover all

● Liaison Group (IEC/TC44 & ISO/TC199)
  ● compiles a common Technical Report, which will be added as an Annex to both Standards

● By the introduction resp.
  ● the co-consideration of the probabilistic approach of failures concerning functional safety at machines a shift in direction has been initiated, which will take still many years, until the new approach is widely applied.
Summary
ISO 13849 and IEC 62061

● Experiences from many seminars and trainings on the subject
  “New Standards in machinery applications: ISO 13849-1 and EN 62061“:
  ● Machine builders and users are overburdened with the new Standards, even if they have experience with EN 954-1.
  ● Manufacturers of safety components are already very well prepared to the new Standards.

● Request of manufactures:
  ● Type approval acc. to both Standards ISO 13849-1 and EN 62061.
  ● Both PL and SIL have to be approved and confirmed.

● Manufacturers of safety products still today desire,
  ● that the “old“ approved and known Standard EN 954-1 is mentioned on the certificate (in addition to ISO 13849-1).
What information is necessary for the user

- Validated developed HW/SW acc. to IEC / ISO / EN

- Quantitative Values
  - HFT, SFF, DC, MTTF, \((\lambda_{DU}, \lambda_{DD}, \ldots)\)
  - Probability figures, PFD / PFH / PL /…….
  - including Guidance for Calculation
  - Proof Test Interval, Installation and Maintenance guide

- Use of the system: (conditions for the application)
  - Normally energised, de-energised
  - Low demand, high demand mode of operation

This information is available in the test report or safety manual.

This is shown with the Certificate.

This information is available on the Certificate and in the safety manual.
What kind of certificates are available?

- Controllers, PLC’s
  - Sufficient number of Systems
  - Information is published on the Internet

- Field Devices / Safety components

- Functional Safety Management
  - Manufacturer and System Integrator, no User till now

- Functional Safety Experts and Engineers

http: //tuvasi.com
List of approved PLC’s
or
http: //tuv-fs.com
Definition of certification

Definition:

- Certification is a **process** by which **sufficiently independent qualified entities** can attest that the **claimed functions** of a system or process are performed at a **verifiable level of dependability**

In practice:

- TUV certifies what you state your product/system can do and
- TUV certifies functional safety based on standards

- Functional safety standards **and** application standards
Certification of products

- TÜV certification consists of:
  - Functional safety aspects (required)
  - Basic safety aspects (required)
    - EMC & electrical safety
    - Environmental safety (Temperature, vibration, humidity, etc.)
  - Application specific aspects (optional)
    - Process industry
    - Burner management
    - Machinery
    - Etc.
Process of Type Approval / Assessment and Certification

Phase 1
Concept Review
Validated & Authorised Requirement Specification

Phase 2
Main Inspection
Extensive Safety Technical Inspection & Report

Phase 3
Certification
Certification of the Inspected Devices
Why Certification?

- Benefits of certification
  - Independent verification of your safety implementation
  - Review can be used for third parties
    - Insurance companies
    - Local governments

- Drawbacks for certification
  - Longer return of investment

- Costs of an accident
  - 5 to 8 times the initial investment of the plant
Contact information

TÜV Rheinland
Precisely Right.

TÜV Industrie Service GmbH
Automation, Software and Information Technology (ASI)

USA
TUV Rheinland North America, Inc.
Heinz Gall, Matthias Haynli
12 Commerce Road
Newtown, CT 06470

☎ 001 203-426-0888
Fax 001 203-426-4009
eMail hgall@us.tuv.com
http://www.us.tuv.com

Germany
TÜV Industrie Service GmbH
Heinz Gall, Stephan Häb
Am Grauen Stein
51105 Cologne

☎ 0049 221 806 1790
Fax 0049 221 806 1539
eMail tuevat-asi@de.tuv.com
http://tuvasi.com

Japan
TÜV 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
eMail ji@jpn.tuv.com
http://www.jpn.tuv.com
Come visit us at booth #15 B
Add value with the safety chain
Thank you for your attention