Inf2: Software Engineering and Professional Practice

Lecture 16: Standards and Functional Safety

Michael Glienecke

Developed from presentations by Aurora Constantin and Michael Mats

Standards

Content

- What are standards for?
- A quality standard: ISO 9001:2015
- Avionics Standards Structure
- IEC 61508: Industrial Process Management Framework

What are standards for?

- A standard typically establishes criteria or processes that should be followed in order that a particular product or service can be sold in a sector.
- Here we focus on international standards, but most countries have internal organisations (e.g., BSI in the UK, DIN in Germany).
- There are a variety of standards organisations that operate internationally e.g., ISO, IEC, ITU (look them up).
- Some standards are “generic” and span many sectors but inside each sector there can be quite elaborate standards structures.

What do standards do

- Mandate certain qualities of processes and products to:
  - **Promote industrial and market efficiency**: by providing a "level playing field" for companies to compete on. Companies cannot compete unfairly by producing inferior products/services that do not meet the standard.
  - **Foster international trade**: if the standard is agreed internationally then it supports international trade because the standard is accepted in all countries that agree to the standard
  - **Lower barriers to market entry**: Standards can build markets around the agreed standards, and this makes it easier for entrants to gain funding to develop service/products and starts to build tools and techniques to build products/services to standard.
  - **Diffuse new technologies**: if a new technology has an agreed standards this de-risks the purchaser because there are alternate products/services and suppliers that fulfill the role of the
  - **Protect human safety/security and the environment**: by ensuring products and services are not harmful to humans or the environment. This often involves balancing cost against the level of harm.

ISO 9001:2015 – A Generic Standard

- ISO: International Organisation for Standardisation.
- 160 member National Standards Organisations
- Some Key standards:
  - ISO 9001: Quality Management Systems (QMS)
  - ISO 14001: Environmental Management Systems (EMS)
  - ISO 27001: Information Security Management Systems (ISMS)
- ISO 9001:
  - International consensus on good practice
  - Focusses on meeting customer requirements and other stakeholders
  - Places requirements on organisations
  - Covers any organization regardless of size, sector, culture, …

ISO 9001:2015 in operation

- It sets goals for WHAT must be achieved
- Does not say HOW to achieve these goals
- QMSs will vary significantly across organisations
- Is a tool for management to manage quality effectively
- QMS that comply with ISO 9001 are often preferred or mandated when other organisations procure products or commission services. In particular if the procuring organization is ISO 9001 compliant this will require compliance in suppliers (this can be a significant competitive advantage).

ISO 9001:2015

- This is the 5th edition of ISO 9001 and follows 7 principles:
  1. Customer focus
  2. Leadership
  3. Engagement with people
  4. Process approach
  5. Improvement
  6. Evidence-based decision making
  7. Relationship management

Risk-based management

- ISO 9001 supports risk-based management that balances the cost of risk against the benefits of Opportunities
- Improves customer confidence
- Supports consistency of quality
- Promotes a culture of risk awareness that helps prevent negative events

ISO 9001:2015 main sections

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

Plan Do Check Act

- Cyclic process – sections 1-3 Re background
- Plan: sections 4-6
- Do: sections 7 and 8
- Check: section 9
- Act section 10

Plan

4. Context of the organization
   - Capturing the organization
   - Capturing the needs of stakeholders
   - Scoping the range of the QMS
   - QMS and processes
5. Leadership
   - Commitment of leadership
   - Policy development
   - Roles, responsibilities, authority
6. Planning for the QMS
   - Actions to tackle risks and opportunities
   - Quality objectives and mechanisms to achieve them
   - Planning changes

Do

7. Support
   - Resources
   - Competence
   - Awareness
   - Communication
   - Documentation
8. Operation
   - Operational planning
   - Requirements on quality for products and services
   - Service/product design
   - Control of use of external products and services
   - Production of services and products
   - Release of products and services
   - Controlling non-conforming outputs, products and services

Check, Act

- Check
  9. Performance Evaluation
     - Monitoring, measurement, analysis, evaluation
     - Internal Audit
     - Management review
- Act
  10. Improvement
      - General
      - Non-conformity and corrective action
      - Continual Improvement

Certification

- There is a certification process that checks compliance
- Involves audits of the process
- And re-audit

Question

- Can you think of a product or service you use regularly?
- What are the key quality attributes for you?
- Do you think these are measurable?
- How do you think they could be improved?

Structural aspects of standards

- Example of DO 178C

DO-178C

- This is the avionics software standard.
- It is largely testing-based
- It is used by to control the development of software embedded in avionics systems.
- It sits inside a complex web of standards and regulation that is intended to ensure the safety of complex avionics software.
- This is not intended to provide detailed information about the standard but it illustrates the web of standards in a technical area.
- See: https://forums.ni.com/t5/Past-NIWeek-Sessions/What-the-New-DO-178C-Means-for-Your-Next-Test-Application/ta-p/3507847?profile.language=en pages 1-13

Inside a Standard

- IEC 61508

IEC 61508

- This is the main standard to assure the functional safety of processing equipment with Programmable Electronic Systems as subcomponents.
- It is used internationally as the standard used in the development of things like Programmable Logic Controllers that are used to control plant and equipment in an industrial context.
- The goal is to assure “Functional Safety” that derives from the integration of all the components of the system.
- The goal here is to illustrate the structure of the standard and the associated lifecycle.
- See: Introduction to Functional Safety www.ewh.ieee.org/r4/chicago/pstc/content/Functional-Safety-Overview-UL.ppt pages 1-11.

Summary

- Standards can be:
  - both generic and specific to a sector or a domain.
  - useful because they ensure minimum quality of products and services and can help build markets.
- Many sectors have software embedded into their product or service delivery.
- DO-178C is an avionics standard is a good example of how a software standard sits inside a broad framework.
- IEC 61508 is a functional safety standard that is intended to ensure functional safety – it has a specific lifecycle that takes account of all the components necessary to assure functional safety.

Functional Safety Overview

Table of Contents

Standards

- UL 991 (2004), "Tests for Safety-Related Controls Employing Solid-State Devices"
- ANSI/UL 1998 (1998), "Software in Programmable Components" (used in conjunction with UL 991 for products that include software)
- ANSI/UL 61496-1 (2010), "Electro-Sensitive Protective Equipment, Part 1: General Requirements and Tests"
- ANSI/ASME A17.1/CSA B44 (2007), "Safety Code for Elevators and Escalators"
- EN 50271 (2010), "Electrical Apparatus for the Detection and Measurement of Combustible Gases, Toxic Gases or Oxygen - Requirements and Tests for Apparatus Using Software and/or Digital Technologies"
- IEC 60335-1 (2010), "Household and Similar Electrical Appliances - Safety - Part 1: General Requirements"
- IEC 60730-1 (2010), "Automatic Electrical Controls for Household and Similar Use - Part 1: General Requirements"
- EN/IEC 61508-1 through -7 (2010), "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

Standards

- EN/IEC 61511 (2003), "Functional Safety - Safety Instrumented Systems for the Process Industry Sector
- EN/IEC 61800-5-2 (2007), "Adjustable Speed Electrical Power Drive Systems - Part 5-2: Safety Requirements - Functional"
- EN/IEC 62061 (2005), "Safety of Machinery - Functional Safety of Safety-Related Electrical, Electronic, and Programmable Electronic Control Systems"
- EN ISO/ISO 13849-1 (2006), "Safety of Machinery - Safety-Related Parts of Control Systems - Part 1: General Principles for Design"
- ANSI/RIA/ISO 10218-1 (2007), "Robots for Industrial Environments - Safety Requirements - Part 1: Robot"
- ISO/Draft International Standard 26262 (2009), "Road Vehicles - Functional Safety

Why evaluate your product/system for functional safety?

- A functional safety assessment determines whether your products meet standards and performance requirements created to protect against potential risks, including injuries and even death

- Compliance is driven by customer requirements, legislation, regulations, and insurance demands

What is Functional Safety?

The exact definition according to IEC 61508:

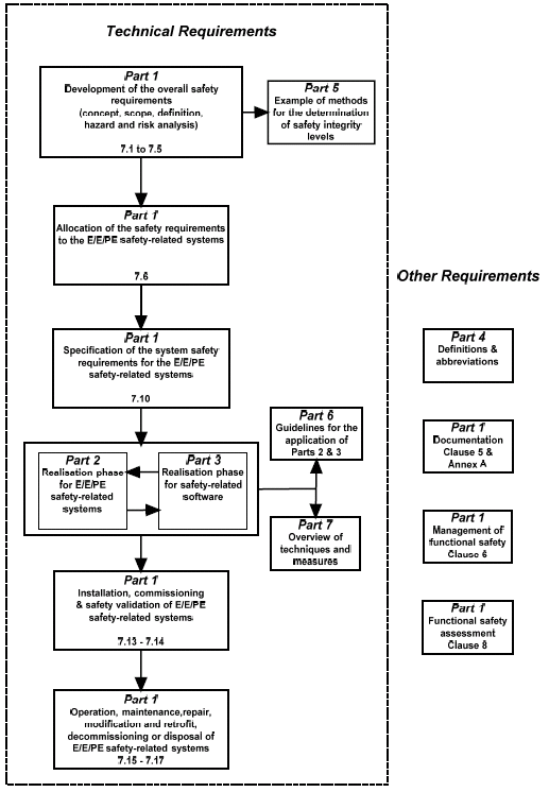
“part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures”

EUC = Equipment under Control
E/E/PE or E/E/PES = Electrical/Electronic/Programmable Electronic Safety-related Systems

IEC 61508: A standard in seven parts

(Parts 1 – 4 are normative)

- 1: general requirements that are applicable to all parts.
  - System safety requirements
  - Documentation and safety assessment
- 2 and 3: additional and specific requirements for E/E/PE safety-re
  - System design requirements
  - Software design requirements
- 4: definitions and abbreviations
- 5: guidelines and examples for part 1 in determining safety integr
- 6: guidelines on the application of parts 2 and 3;
  - Calculations, modeling, analysis
- 7: techniques and measures to be used
  - To control and avoid faults



FS according to IEC 61508:

EUC + EUC Control System

Why is there something called Functional Safety?

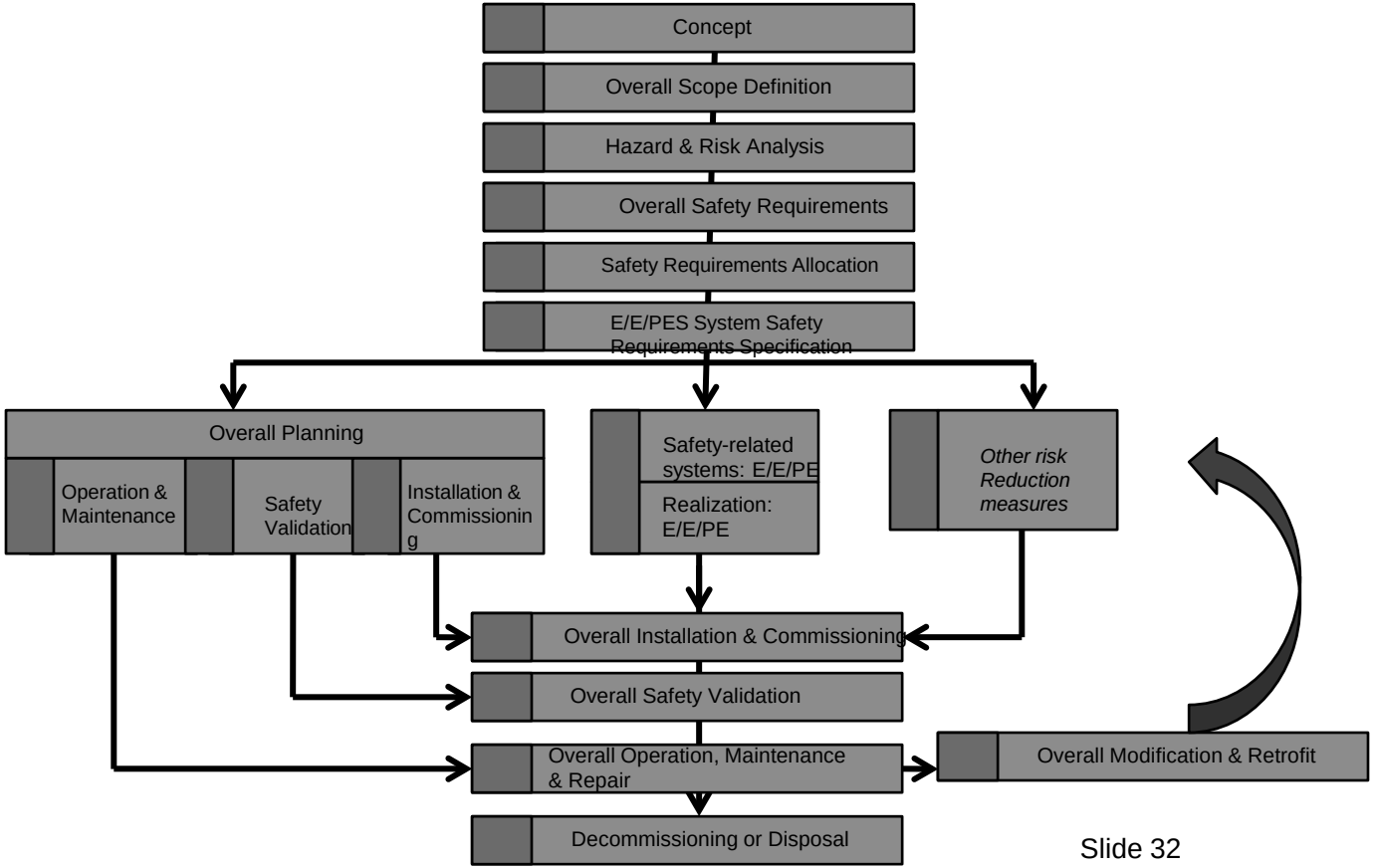
- Functional safety as a property has always existed
- The definitions of Functional safety show that it is not related to a specific technology
    - **Functional Safety, as a term and as an engineering discipline, has emerged with the advancement of complex programmable electronics**

Functional safety as per IEC 61508

IEC 61508 mandates an ”overall” safety approach could also be referred to as a:

- **System safety approach or**
- **Holistic approach (accounts also for the whole life cycle of a system)**

Overall Safety Lifecycle and E/E/PES life cycle



Functional Safety Certification Process

Kick-Off Meeting

- Most effective during the product design phase
- Collaborate to ensure that the features required by the specified standard are included in the initial design
- Understand the consequence of choices being made
- Guidance from certification body on how to design product
- Discuss prototyping

Functional Safety Certification Process

Pre-Audit and IA

- Increase the probability of success of the certification audit
- Management system audit
- Engineers perform on-site GAP analysis
- Customer received concept evaluation report with detailed action items

Functional Safety Certification Process

Certification Audit

- Certification body audits the system's compliance with the designated standard and functional safety rating
- Evaluation of documentation
- Product is certified

Functional Safety Certification Process

Follow-up Surveillance

- A surveillance to verify that the protective functions of the product match the report are performed

- Certification body conducts an audit of the functional safety management system once every three years

Examples of Function Safety Products

EUC – E/E/PE System – Subsystems

- Hazard & Risk Analysis shall be conducted for the EUC and the EUC control system
- Hazardous events are identified, and the associated risk (the "*EUC risk*") determined
- If the *risk* is not acceptable, it must be reduced to a *tolerable risk* level by at least one of, or a combination of, the following:
  - External risk reduction facilities
  - Safety-related control systems, which can be:
    - Based on electrical/electronic/programmable electronic *(E/E/PE)* technology
    - Other technology

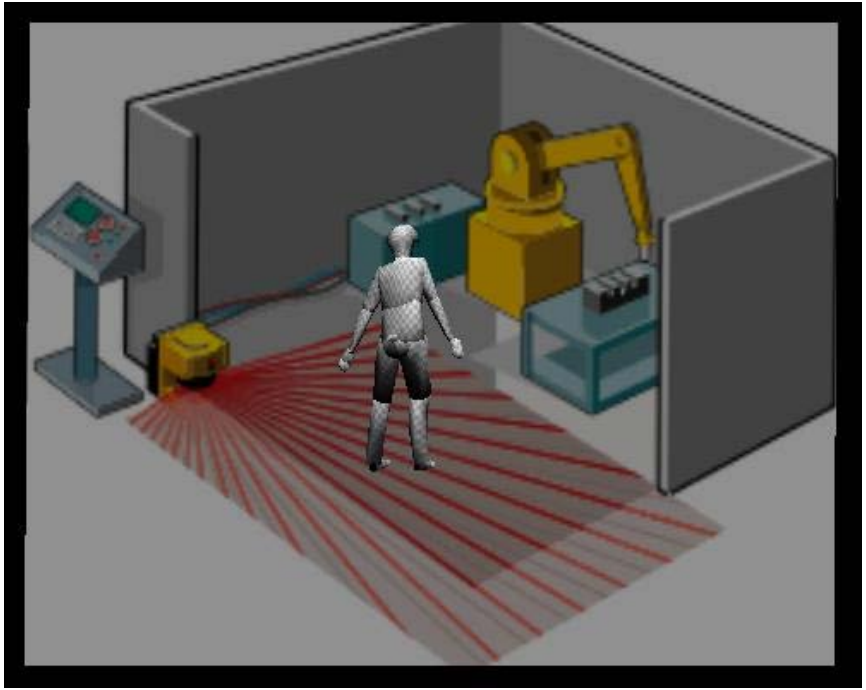
Necessary risk reduction and Safety Integrity Level (SIL)

- IEC 61508 is a standard for *E/E/PE safety related systems (E/E/PES),* or subsystems. Therefore, the following is addressed by this standard:
  - The part of *necessary risk reduction* allocated to an *E/E/PES* is expressed as a failure probability limit (*target failure measure*), which in turn is used to select the so called *Safety Integrity Level (SIL)*
  - This means SIL is an attribute of an E/E/PES (or subsystem), i.e. of a system/device/product that provides risk reduction

E/E/PE safety-related system and risk reduction

- EUC risk
  - risk arising from the EUC or its interaction with the EUC control system
- Tolerable risk
  - risk which is accepted in a given context based on the current values of society
- Necessary risk reduction
  - risk reduction to be achieved by the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities in order to ensure that the tolerable risk is not exceeded
- Residual risk
  - risk remaining after protective measures have been taken
  - must be equal or lower than tolerable risk

EUC Risk



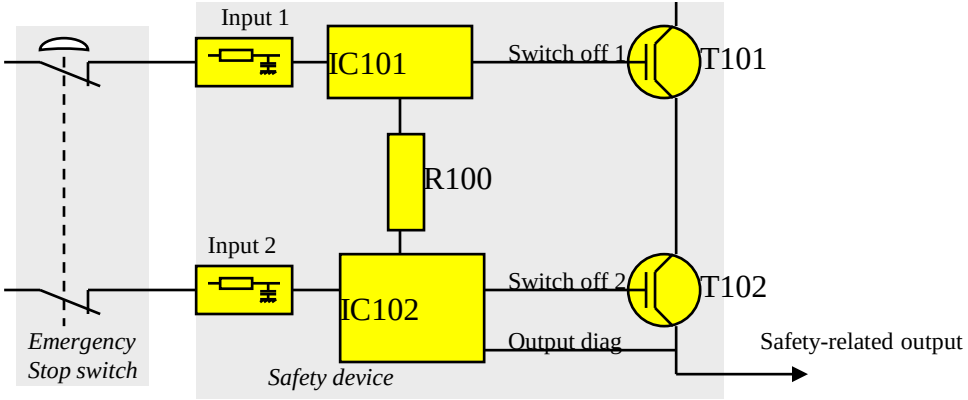
Software Drives FS Requirements - IEC 61508-3

- Electromechanical systems are rapidly being replaced by (software) programmable electronic systems due to:
  - **Lower cost parts**
  - **Greater redesign flexibility**
  - **Ease of module reuse**
  - **Less PCB space required**
  - **Improved Efficiency**
  - **Greater functionality**

Software is Being Used Increasingly

- Software controls motor-driven equipment safety parameters such as:
    - PRESSURE generated by a compressor
    - Motor SPEED of an inline gasoline pump
    - POSITIONING of Fuel/Air valves in a combustion control
    - FORCE applied by a robotic arm
    - Air FLOW RATE within a combustion chamber
    - …the possibilities are limitless…

FMEDA Table (Design level)



Component reference	Component function	Failure modes	Effects	failure distribution	Criticality	DC	λ [FIT]	λD	λS	λDD	λDU	Detection reqmts	Exclusion reqmts
R100	**energetic separation between channels, cross communication for diagnostics**				**0,9**		**1**	**0,9**	**0,1**	**0,813**	**0.087**		
		short circuit	no separation between channels	0,2	1	0,6		0,2	0	0,12	0,08	sample test, off line	MELF resistor
		open circuit	no cross communication	0,7	1	0,99		0,7	0	0,693	0,007	cross comparison between channels	
		0,5< value <2	no effect	0,1	0	0		0	0,1	0	0		select value high enough to ensure separation

Simplified approaches proposed by other standards

- Also ISO 13849-1 and IEC 62061 suggest simplified methods for determining the probability of random HW failure
- ISO 13849-1 approach is based on ”designated architectures” for the different Categories
- IEC 62061 approach is based on ”basic subsystem architectures”
- These simplified approaches claim to err towards the safe direction, and make a number of assumptions
- If the assumptions cannot be made, or if just more precise (and less conservative) values are desired, then more detailed reliability modeling may be applied

Additional Information

Websites:

www.ul.com/functionalsafety

www.exida.com

www.siemens.com

http://www.automationworld.com/newsletters_fsn.html

Questions?