THE UNIVERSITY of EDINBURGH
informatics

Lecture 21: Standards and Functional Safety

Cristina Adriana Alexandru

School of Informatics

University of Edinburgh

This lecture

- Standards
  - What are standards for?
  - What do standards do (advantages)?
  - A quality standard: ISO 9001:2015
  - An avionics software standard: DO- 178C
  - A standard for embedded software controlling hardware: IEC 61508
- Functional safety
  - What is functional safety?
  - Functional safety in standards
    - As per IEC 61508

Standards

another question

Edi

Go to wooclap.com and use the code **FOFRFH**

How do standards apply to software engineering?

Standards are crucial in software engineering, guiding all aspects of the process for all products 0% 0

Standards are not relevant to software engineering, but apply to adjacent processes in the workplace 0% 0

Click on the projected screen to start the question

Standards are not relevant to software engineering at all 0% 0

Standards are sometimes crucical in software engineering, guiding some or all aspects of the process 0% 0

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**
  - **Lower barriers to market entry**
  - **Diffuse new technologies**
  - **Protect human safety/security and the environment**

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
  - Covers any organisation 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
- Compliance means your company/product may be often preferred or mandated. 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: principles

- 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

ISO 9001:2015: 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 organisation
    - Capturing the organisation
    - 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 (ISO 9001:2015 and in general)

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

DO-178C- a software standard

- Avionics software standard
- Testing-based
- Part of a complex web of standards and regulation that is intended to ensure the safety of complex avionics software.
- 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

DO-178C

DAL	Failure Condition	Effect on Aircraft & Passengers
Level A	**Catastrophic**	Loss of aircraft, multiple fatalities
Level B	**Hazardous/Severe Major**	Large reduction in safety margin, serious or fatal injuries
Level C	**Major**	Significant safety reduction, possible injuries
Level D	**Minor**	Slight safety impact, minor discomfort
Level E	**No effect**	No impact on safety or operation

Testing requirements in DO-178C

Aspect	Level A	Level B	Level C	Level D	Level E
Testing Rigor	MC/DC Coverage	Decision Coverage	Statement Coverage	Functional Testing	None
Independence in Testing	Required	Required	Not Required	Not Required	Not Required
Requirements Traceability	Strict	Strict	Moderate	Low	None
Documentation & Reviews	Extensive	High	Moderate	Basic	Minimal
Tool Qualification Required?	Yes	Yes	Sometimes	Rarely	No

DO-178C: Activity

If we have the following piece of code:

```
if (A && B) {
    executeSafetyCheck();
}
```

marked in DAL as Level A, which of the following testing scenarios apply?

another question

Edi

Go to wooclap.com and use the code **FOFRFH**

What type of testing scenario applies?

TC1: A==false, B==true; TC2: A==true, B==false; TC3: A==true, B==true — 0% — 0

Click on the projected screen to start the question

TC1, TC3 — 0% — 0

TC2, TC3 — 0% — 0

TC1, TC2 — 0% — 0

IEC 61508- a standard for functional safety

- The main standard to assure the functional safety of processing equipment with Programmable Electronic Systems as subcomponents.
- 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.
- See: Introduction to Functional Safety www.ewh.ieee.org/r4/chicago/pstc/content/Functional-Safety-Overview-UL.ppt pages 1-11.

Testing requirements in IEC 61508

- Safety Integral Levels (SIL): how reliable a system must be in preventing dangerous failures

Testing technique	SIL1	SIL2	SIL3	SIL4
Functional testing	✓✓	✓✓✓	✓✓✓✓	✓✓✓✓
Black-box testing	✓✓	✓✓✓	✓✓✓✓	✓✓✓✓
White-box testing	✓✓	✓✓✓	✓✓✓✓	✓✓✓✓
Structural code coverage	✓	✓✓	✓✓✓	✓✓✓✓
Boundary value	✓✓	✓✓✓	✓✓✓✓	✓✓✓✓
Performance testing		✓✓	✓✓✓	✓✓✓✓
Formal methods			✓✓✓	✓✓✓✓

Functional Safety Overview

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

Why is there something called functional safety?

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

Why evaluate your product/system for functional safety?

- To make sure that while developing and then using it nobody is harmed.
- Determines whether your products meet standards and performance requirements
- Compliance is driven by customer requirements, legislation, regulations, and insurance demands

Standards for functional safety

- 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"

Standards for functional safety

- EN/IEC 61508-1 through -7 (2010), "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
- 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

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)**

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-related systems

- System design requirements
- Software design requirements

4: definitions and abbreviations

5: guidelines and examples for part 1 in determining safety integrity levels

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

Functional safety as per IEC 61508: EUC + EUC Control System

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 Internal Audits

- Increase the probability of success of the certification audit
- Management system audit
- Engineers perform on-site GAP analysis
- Customer receives 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 is 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

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

Software Drives functional safety 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
  - etc.

Achieving hardware safety integrity

- IEC 61508-2 requires application of the following principles to achieve the intended hardware safety integrity:
  - Redundancy
    - Diversity of redundant channels to eliminate common cause failures
  - Failure detection
    - per IEC 61508, detection implies a reaction to a safe (operating) state
      - For fail-safe applications, this can mean activation of the fail-safe state
  - Reliability of components
    - Probability of dangerous failure (on demand - PFD, per hour - PFH) in accordance with target failure measure of the required SIL (safety integrity level)

Additional Information

- www.ul.com/functionalsafety
- www.exida.com
- www.siemens.com
- http://www.automationworld.com/newsletters_fsn.html