Cato Bratt, FSM Advisor ABB, Sikkerhetssystemkonferansen 2015, Radisson Blu Airport Hotel, Gardermoen, 5-6 Nov

Changes in IEC 61511 edition 2

Power and productivity
for a better world™

Presenter
Cato Bratt

Cato Bratt

- Worked in ABB since 1997
- I have worked for ABB for more than 15 years and is currently FSM Advisor for ABB PA OGC in Norway. As FSM Advisor in PA OGC Norway I am responsible for the FSM System.
- I am a member of the IEC 61511 committee.

Disclamer

This paper presents some of the changes in “IEC 61511 – Functional safety – safety instrumented system for the process industry sector”, edition 2.

It is based on the FDIS version of the standard, and it is the author’s interpretation of some of the changes.

Note that there may be new or different changes in the final version of the IEC 61511 edition 2.

Power and productivity for a better world™

IEC 61511
General about IEC 61511

- IEC 61511 first released in 2003
- IEC 61511 Belongs to the IEC 61508 safety umbrella standard
- IEC 61511 is intended for the process industry
    - Sector specific standard for IEC 61508
- Ca 60 people representing 17 countries have been engaged in the committee work.
- The committee usually meets twice each year.
- The committee is divided into several task teams
- Planned release of IEC61511 edition 2 is First quarter 2016
- FDIS version is now Awaiting translation within IEC

Power and productivity for a better world™

IEC 61511
General changes

- The new edition of IEC 61511 has eliminated inconsistencies, corrected several writing errors, incorporated lessons learned
- The word “should” is changed to “shall” in many clauses
- Software is exchanged with Application Program
- Bullet lists exchanged with letters

- Part one is reduced
- Part two is more than double the size
- Part three is larger

Power and productivity
for a better world™

IEC 61511
Terms, definitions and abbreviations, Clause 3

- Several definitions are rewritten to be in line with other IEC standards, and especially IEC 61508

  - 20 new definitions (from ed.1 to CDV)
  - Several definitions are rewritten
  - Some definitions are deleted

Power and productivity
for a better world™

IEC 61511
Terms, definitions and abbreviations, Clause 3

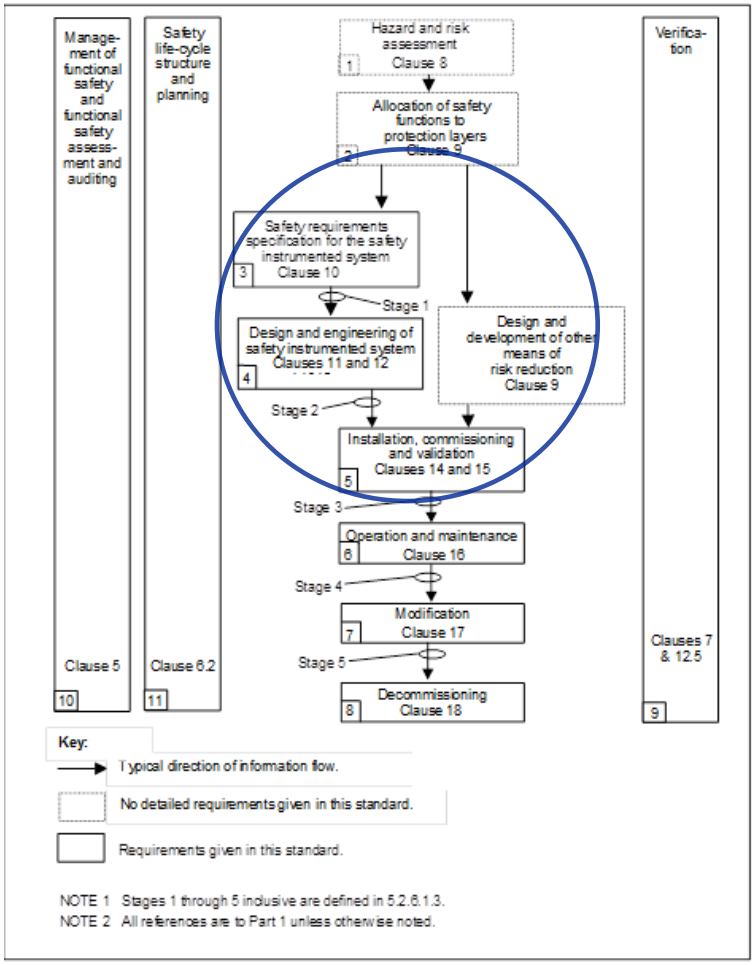
- Highlights form changes in definitions

- Added clarity to the definitions of **common cause failures** and **common mode failures** (3.2.7.1 and 3.2.7.2)
- The relation between **Low Demand**, **High Demand** and **Continuous Control** from IEC 61508 is now defined as: (3.2.41)
  - Demand mode SIF = Low Demand and High Demand
  - Continuous mode SIF = Continuous Control
- **Systematic Capability** (SC) is now included in the new edition of IEC 61511
- Definition of **process safety time** added (3.2.54.1)

IEC 61511
Management of functional safety, Clause 5

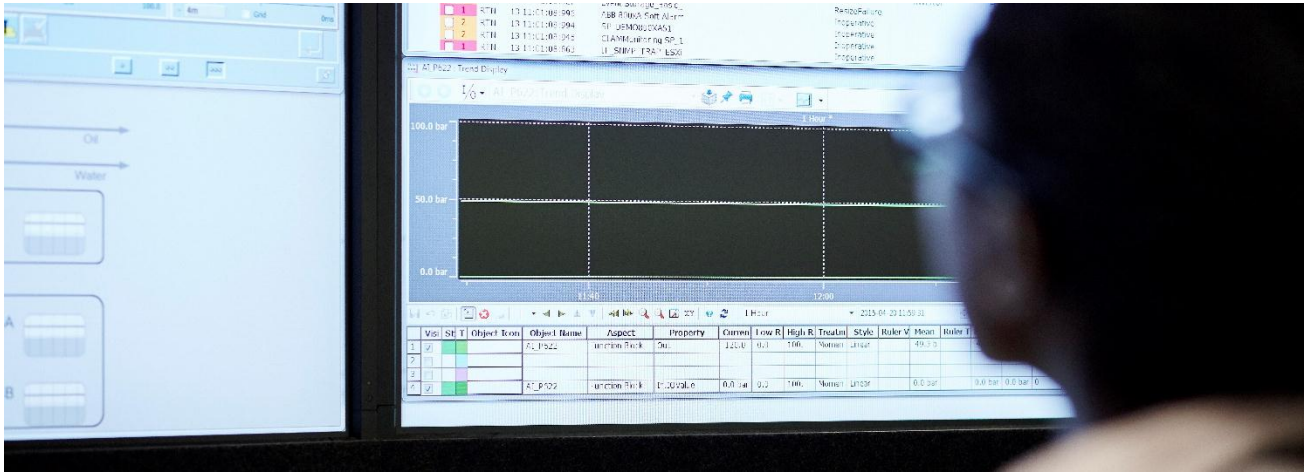
- Competency requirements are strengthened
  - Old: the list of knowledge areas is listed in a note with wording should
  - New: list of knowledge areas that **shall** be addressed
  - New: A procedure to control competency is required
  - New: Periodic competency assessment is required

IEC 61511
Management of functional safety, Clause 5



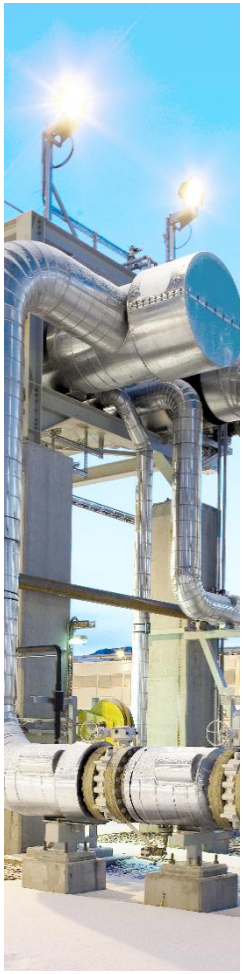
- Old: at least one FSA, latest at stage 3
- In addition two new requirements
- New: FSA carried out on a modification shall consider the impact analysis (5.2.6.1.9)
- New: FSA shall be carried out periodically during operational and maintenance (5.2.6.1.10 related to 17.2.3)
- Safety planning (5.2.4)
- Old: named safety plan
- New: named SIS Safety Life-Cycle Plan

IEC 61511
Safety life-cycle requirements, clause 6



- Minor changes to this clause
- Safety life-cycle figure moved to clause 6
- Application program safety life-cycle moved to clause 6

IEC 61511
Verification, clause 7



- Verification has a new clause which handles testing (7.2.2). In the original version testing wasn't specifically mentioned.
- A more holistic approach
  - Both HW and application program testing is described
- New structure also visible in clause 7
  - Also application program verification and test is included in clause 7
- More descriptive requirements for testing in general.

Power and productivity for a better world™

IEC 61511
Process hazard and risk assessment, clause 8

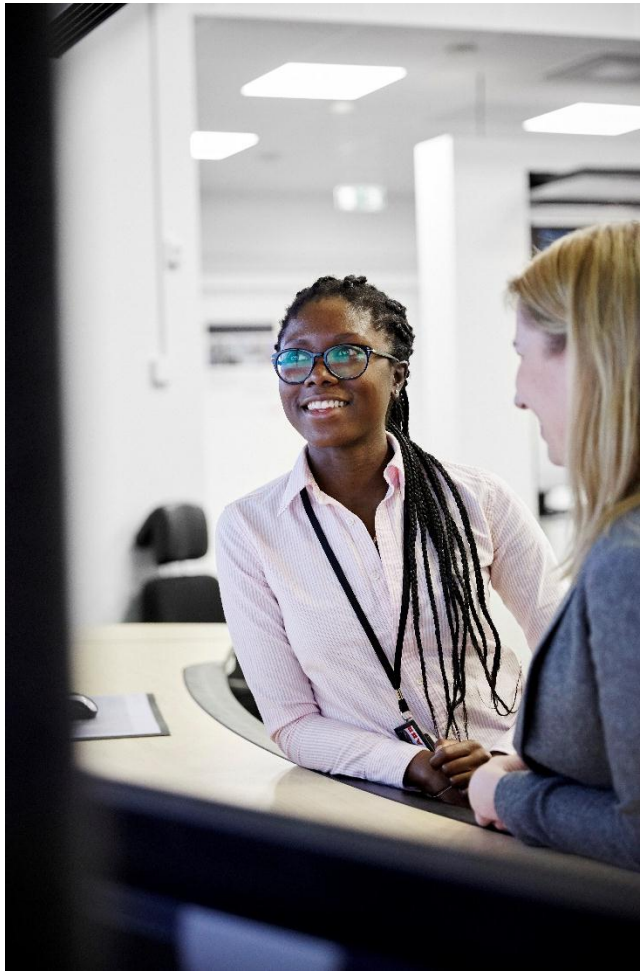
- New requirements containing security risk assessment (8.2.4).
- Need for a security risk assessment for the SIS and associated devices:
  - Description of identified treats that could exploit vulnerabilities and result in security events
  - This shall be considered for the different lifecycle phases (design, implementation, commissioning, operation and maintenance).
  - Detailed on SIS security is found in ISA TR84.00.09, ISO/IEC 27001 and IEC 62443

Power and productivity for a better world™

IEC 61511
SIS safety requirements specification (SRS), clause 10

- The well known 27 requirements to be included in the SRS have now increased to 29
- Some highlighted changes:
  - “a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification (e.g., field tag list);”
  - “requirements relating to proof test implementation;”
- New name for **software safety requirements specification** is now **application program safety requirements specification**
  - The requirements for Application program safety requirement specification is moved form clause 12.2.2 to 10.3.3-10.3.6

IEC 61511
SIS design and engineering, clause 11



- **Safety Manual** (3.2.73 and 11.2.13)
  - New definition and requirement
  - End user must consider if safety manual for the facility is necessary
  - Covering
    - Operations
    - Maintenance
    - Fault detection
    - Constrains
  - Manufacturer IEC 61508 compliant safety manuals is input to end user facility safety manual

Power and productivity for a better world™

IEC 61511
SIS design and engineering, clause 11

- Reliability data clause 11.9
- Three new clauses in short requires
  - Reliability data shall be; credible, traceable, documented, justified
  - shall be based on field feedback from similar devices used in a similar operating environment.
  - Reliability data uncertainties shall be assessed

Power and productivity for a better world™

IEC 61511
SIS design and engineering, clause 11

SIL	Minimum required HFT
1 (Any mode)	0
2 (low demand mode)	0
2 (high demand/continuous mode)	1
3 (Any mode)	1
4 (Any mode)	2

- Align the IEC 61511 with route 2H of IEC 61508-2:2010.
- The Safe Failure Fraction (SFF) is removed,
- New Hardware Fault Tolerance (HFT) table without the SFF (11.4.5).

IEC 61511
Classical example with push button

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

- Push Button SFF=50%, SIL2 requirement in CAP
- Based type A table from Route 1_H (61508-2)
- HFT=1 required to achieve SIL2

Power and productivity for a better world™

IEC 61511
Classical example with push button

- With the new table in 11.4.5
- Only HFT=0 is required for SIL2
- Push buttons with only one contact set gives several benefits to the design and the end user
  - One contact set is mechanically more reliable
  - One contact set make it is strait forward to do a proof test
  - One contact set makes it is less complex
- In some cases added redundancy does not necessary give added safety, and this is reflected in this new requirement

IEC 61511
SIS Application Program Development, clause 12

- There have been major changes in the structure of clause 12,
- Application program safety life cycle is moved to clause 6.
- Application program safety requirements specification is moved to clause 10.3.3-10.3.6, and some description text is moved to part two as guidance.
- Stricter rules on how to document independents between non safety functions and safety functions (12.2.4)
  - “12.2.4 Where the application program of the SIS is to **implement both safety and non-safety functions, then all of the application program shall be treated as part of the SIS** and shall comply with this standard and in addition, **it shall be shown through assessment and test that the non-safety functions cannot interfere with the safety functions**.”

Power and productivity for a better world™

IEC 61511
SIS Application Program Development, Clause 12

- Changes to clause 12 continued
- ”12.2.7 The application program shall be designed in such a way that **all parts of the application program are executed on every application program scan** unless there is a specific alternate requirement that is supported in the safety manual. Process safety time requirements shall be considered when establishing application program scanning requirements.“
- “12.4.2 The following information shall be contained in the **application program** or related documentation:
- f) **identification of each SIF** and its SIL; ”

IEC 61511
SIS operation and maintenance, clause 16

- New clause: ”**Compensating measures** that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied…..” (16.2.3)
- New clause: “The status of all bypasses shall be recorded in a bypass log. All bypasses need authorization and indication.” (16.2.7)

Power and productivity for a better world™

IEC 61511
Part 2 changes

- A lot of new examples are provided so that part 2 will become more relevant to the change from software to application programming, and on how to comply with this standard from the application program point of view.

- In general edition 2 part 2 has a lot more guidance text and help to the user. I.e. application program examples are included in part 2.

Power and productivity
for a better world™

IEC 61511
Conclusion

- More consistent, practicable and clear in the requirements
- Has improved the structure and definitions more in line with the parent standard IEC 61508.
- Includes many end user requirements and experience
- Highlights user experience (e.g. prior use)
- Increases the need for written procedures to improve functional safety management
- Drives the need for end users to collect reliability data
- Includes focus and attention on Security
- With the improved examples and guidelines in part 2 it should make the standard easier to read and understand

Power and productivity
for a better world™