11. Avoiding Human Error

GAS DETECTOR FUNCTIONAL SAFETY

OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Purpose

Introduce the techniques used to minimise human error when implementing an SIS.

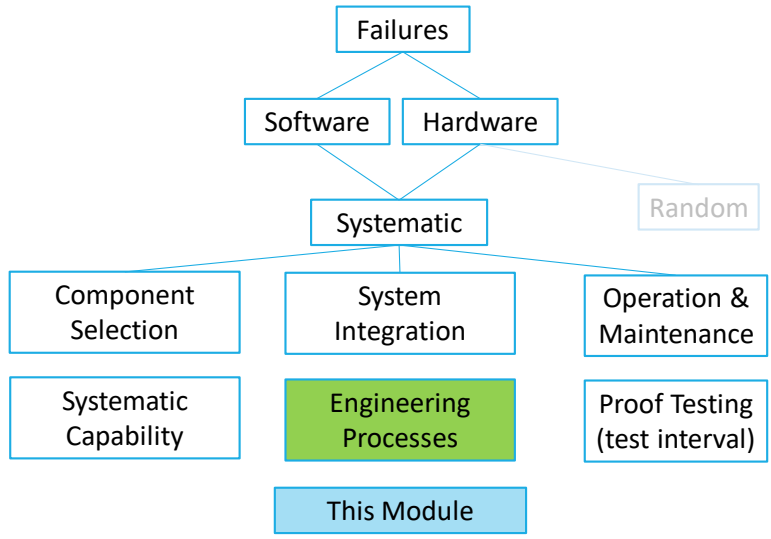
TOPICS

Functional Safety Management

Assurance techniques

- Verification
- Validation
- Functional Safety Assessment
- Audit

Minimising Human Error



Standards Compliance

- ☑ Target SIL must be specified for each SIF based on hazard and risk analysis

Processes for SIS throughout lifecycle must comply

Each SIF must meet target SIL requirements for

- ☑ Hardware Fault Tolerance (architectural constraints)
- ☑ Random failure rate (PFD_{avg})
- ☑ Systematic Capability of each component

- selected components must allow the SIF to meet HFT & PFD_{avg} requirements

Why manage Functional Safety?

> 90% of major accident events are caused by human failure
- systematic failures

Truly random hardware failures are rare
- most failures are due to some form of human error i.e. are systematic
- e.g. pressure transmitter λ_{DU}:

  random 1/2800 y
  random + systematic 1/22 y

To reduce systematic failures we must actively manage functional safety safety

MUCH MORE IMPORTANT THAN CALCULATING PFD_{avg} !!!

What is Functional Safety Management?

All the phases of the lifecycle we have discussed need to be managed
- as for any other engineering or operations activities
- a specialised quality management system

Functional Safety Management (FSM) is the discipline of managing all aspects of the Functional Safety lifecycle

Key requirements:
- define a lifecycle
  - for your activities
- for each phase specify who is responsible
- ensure they are competent
- ensure all recommendations are closed out
- arrange for specified activities of lifecycle to be carried out
  - including Functional Safety Assessment & Audit

See IEC 61511-1 Ed.2 sections 5 & 6

Functional Safety Management System

The "Quality System" that manages all the aspects of Functional Safety

May be part of another management system
- quality management system
- process safety management system
- project management system
- etc.

Pulls together all the requirements to manage Functional Safety
- in a coherent system
- based on written procedures aligned with the lifecycle

Based on a "lifecycle" for all the functional safety activities in that organisation
- corporate
- site
- project

Responsibilities

Operating company generally must identify responsibilities for IEC 61511 lifecycle phases
- from Hazard & Risk Assessment to Decommissioning
- for most major projects responsibilities will be split between process licensor, engineering contractor, systems vendor and operator

Should also ensure operating representation in early phases
- delegate totally to a consultant or contractor at your peril!
- only the operator can take responsibility for balancing risk and economics

For phases within your responsibility
- specify who (people, department or organisation) is responsible
  - to perform the work
  - to assess the work
- inform them!
- ensure they are competent
- plan when work is done and document

Competence

Competence shall be assessed & documented, addressing

- engineering knowledge, training and experience appropriate to the
  - process technology
  - SIS technology
  - field devices used
  - hazard & risk analysis
- knowledge of the legal and regulatory requirements
- relevant management and leadership skills

Appropriate to the

- potential consequence of the event
- SIL of the SIF
- novelty and complexity of the application and technology

Manage using a procedure and regular assessments

- e.g. competency matrix updated at annual performance reviews

Suppliers

Suppliers must

- deliver products or services as specified
- have a quality management system (QMS)

Procedures required to evaluate suppliers' QMS

If a supplier makes functional safety claims used by the organisation to claim compliance to IEC 61511-1, the supplier must have a FSMS

- that complies with IEC 61508-1 clause 6

Be careful about delegating <u>your</u> responsibilities to a consultant or supplier!

Error Minimisation Techniques

Error avoidance
- standardised designs
- standardised processes & procedures
- documented procedures and checklists
- competence appropriate for the task
- . . . see later modules

Error detection and control
- Verification
- Validation
- Functional Safety Assessment
- Audit

- this module

Verification... build the product right

verification (IEC 61511 3.2.92)

"activity of demonstrating for each phase of the relevant safety life cycle

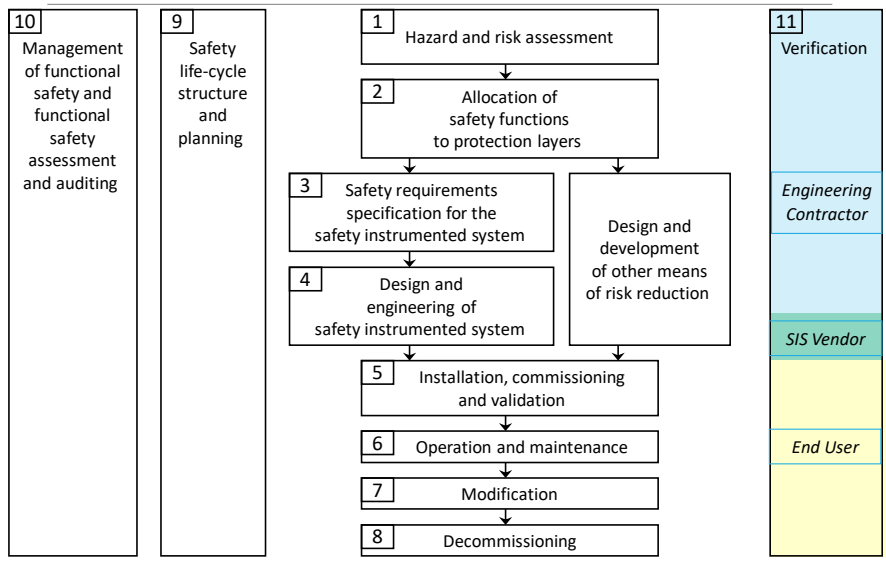
by analysis and/or tests,

that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase"

Performed progressively throughout the lifecycle

Must be planned
- see IEC 61511-1 Ed. 2 7.2.1 for a checklist of items to be included

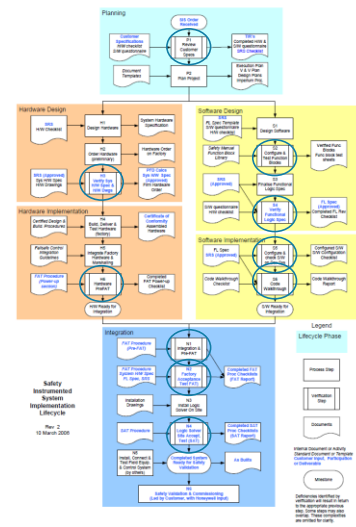
Verification in the Safety Lifecycle



Verification examples

Examples

- review of documents for completeness and correctness
- code walkthrough of software by independent person
- inspection of marshalling cubicles for correct terminations, labelling
- testing of software modules against their specifications
- continuity testing of installed SIF devices and wiring
- checking calibration of field devices
- see IEC 61511 7.2.1 for checklist



Validation

validation (IEC 61511-1 Ed. 2 3.2.88)

- confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Performed at least once just prior to operation

- may be done progressively
- must be planned and documented

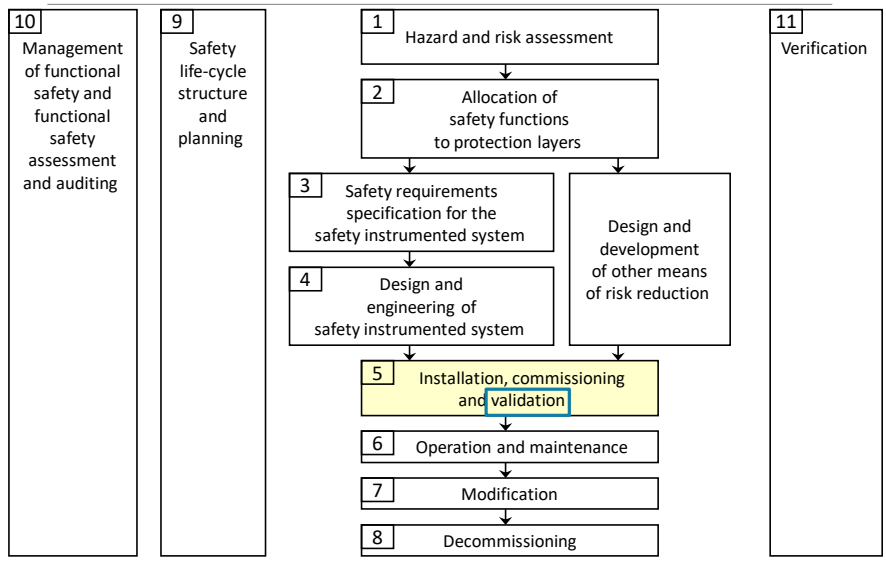
Confirms that the installed and commissioned SIS and its associated SIF(s) achieve the requirements as stated in the SRS

- through testing and inspection

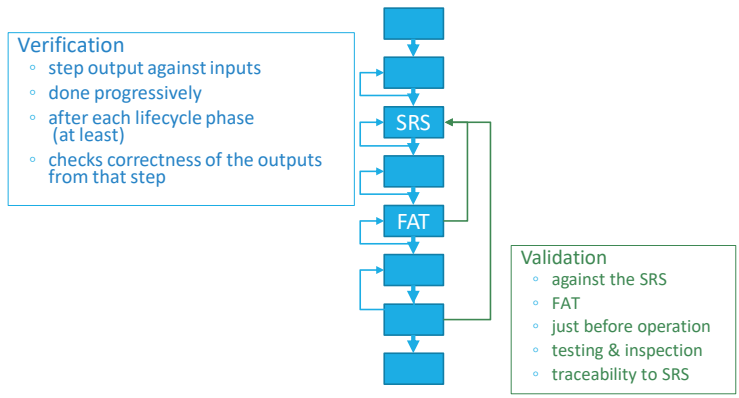
Software validation is often done comprehensively as part of Factory Acceptance Test

- only the normal functionality is tested during final system validation

Validation in the Safety Lifecycle



Verification vs Validation



Audit

functional safety audit (IEC 61511-1 Ed. 2 3.2.27)

- systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

May be part of the Functional Safety Assessment for a project or

May be part of assessing a Functional Safety Management System

- independent of a specific project

Similar to a typical quality system audit, but focussing on functional safety

Functional Safety Assessment

functional safety assessment (FSA) (IEC 61511-1 Ed. 2 3.2.26)

- investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers

Overall assessment of whether the functional safety is achieved

By a team, at least one of whom is not involved in the lifecycle phases being assessed

At least one required prior to the identified hazards being present

- often done in stages e.g.
  - after the SRS
  - after design of the SIS
  - after installation and validation
- can also be done during operation and after major modifications or decommissioning
- see IEC 61511 Ed. 2 5.2.6.1 for checklist requirements

Requires experience as is based on judgement

May incorporate audit and validation

V & V Planning

All assurance activities must be planned

Typical required contents of the plans:

- scope of the assurance activity
  - what will be checked
- timing
- who will be involved and their required independence
- techniques to be used
- documentation
- how non-conformances will be handled

IEC 61511-1 Ed. 2 has detailed requirements for each activity

- useful checklist format
- 7.2.1 Verification
- 15.2.1 Validation

Summary

verification: "build the product right"
- confirms that each step is correct
- performed at each step

validation: " build the right product"
- confirms that the installed SIS meets the Safety Requirements Specification
- just prior to start-up (as a minimum)
- software often validated in Factory Acceptance Test

audit
- confirms that the procedures are appropriate and are being followed

functional safety assessment
- judgement as to whether the required safety is being met

All must be planned & documented

Appropriate independence required

Standards Compliance

- Target SIL must be specified for each SIF based on hazard and risk analysis
- Processes for SIS throughout lifecycle must comply
- Each SIF must meet target SIL requirements for
  - Hardware Fault Tolerance (architectural constraints)
  - Random failure rate (PFD_{avg})
  - Systematic Capability of each component
    - selected components must allow the SIF to meet HFT & PFD_{avg} requirements

Summary

Introduced the techniques used to minimise human error when implementing an SIS.

All phases of the lifecycle must be actively managed and planned
- using a Functional Safety Management System
- a Quality System for Functional Safety

Verification checks that each step is done correctly

Validation checks that the SIS meets the requirements of the SRS

Functional Safety Assessment judges whether the desired safety is being achieved

Audits check whether the right procedures exist and are being followed

Questions?