6. Safety Requirements Specification

GAS DETECTOR FUNCTIONAL SAFETY

OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Purpose

Describe the role and contents of the Safety Requirements Specification and other lifecycle documentation

TOPICS

Purpose & characteristics of SIS documentation

The Safety Requirements Specification

SIS Documentation

Two distinct purposes
- enable each of the lifecycle phases to be performed effectively
- enables verification, validation and functional safety assessment

The documentation must
- describe the installation, system or equipment and the use of it
- be accurate and up to date
- be easy to understand
- suit the purpose(s) for which it is intended through the rest of the lifecycle
- be
  - accessible
  - maintainable
  - editable

Document management

Part of "configuration management"

Formal document management is crucial
- use of out-of-date documents can have severe consequences

Controlled documents require as a minimum
- a title
- a unique reference number
- a revision number and revision history
- verification and authorisation history
- traceability to requirements

Documents to be controlled
- safety related process documents
- SIS configuration documents (logic solver program; wiring diagrams etc.)
- results of hazard & risk assessments including assumptions
- procedures related to management of the SIS
- safety manuals . . .

See IEC 61511-1 section 19 for more detailed requirements

Documentation organisation

Organise documents to suit entire lifecycle users
- not just for design and implementation!

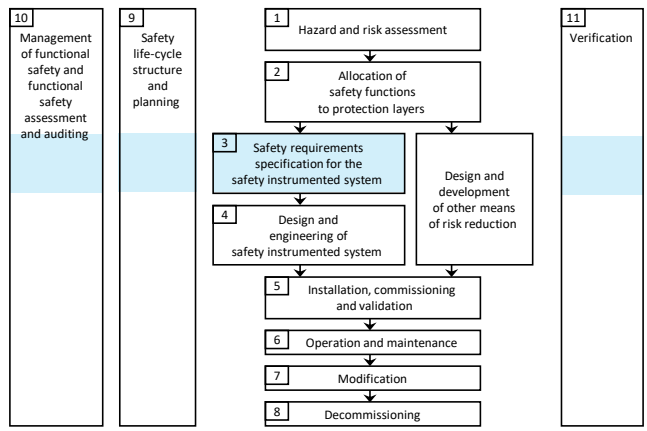
Hazard and risk assessments are often not well structured for lifecycle use
- which option was finally chosen may not be clear
- instruments not uniquely identified
- assumptions finally incorporated not clear

Consider setting up a SIF dossier
- collect all information for each SIF in a traceable form (based on SIF number)
- SIL assessment for each SIF on separate page
  - eventually separate document number
- link to dossier for each SIF from maintenance management system
  - accessible by device tag number
  - basis for proof testing

3 Safety Requirements Specification - SRS

Defines functional and integrity requirements of SIS.

Output is a set of documents ready for detail design.



Role of the Safety Requirements Specification

The set of documents underpinning all subsequent lifecycle stages

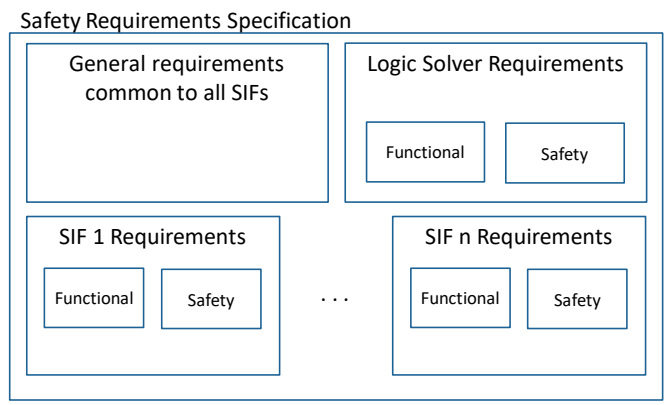
Contains for each SIF
- the functional requirements – what it does
- the safety requirements – how reliably it must perform

Contains for the SIS
- logic solver general requirements
- default requirements for each SIF e.g. process safety time

Typically a master document referencing many other documents
- Functional logic diagrams
- Hazard assessment reports
- SIL determination reports (e.g. LOPAs)

IEC 61511-1 part 10 contains detailed requirements
- a useful checklist

SRS Contents



Case Study – SRS for oxygen SIF

SIF ID:	01
Name:	Laboratory low ambient oxygen
Protects against:	Possible asphyxiation; single fatality
Likely cause(s):	Nitrogen leak and ventilation failure
SIF Function:	When oxygen concentration falls below 17% isolate nitrogen supply by closing shut-off valves
Other protection:	Evacuation alarm actuated with SIF Ventilation system
Required SIL:	SIL 2
Time between demands:	1 to 10y
Operating Mode:	Low demand
Other requirements:	. . .
References:	. . .

Summary

Described the role and contents of the Safety Requirements Specification and other lifecycle documentation

Documentation of the SIS is critical

Must be maintained up-to-date & designed for use during all subsequent lifecycle phases

The Safety Requirements Specification (SRS) is the master document that guides design and ongoing operation of the SIS

The SRS contains:

- functional and safety requirements common to all SIFs e.g. for the logic solver
- functional and safety requirements for each SIF

Questions?