

IICA gas Detector Functional Safety Course

12. Operation & Maintenance



12. Operation & Maintenance

GAS DETECTOR FUNCTIONAL SAFETY
OVERVIEW COURSE



Mod 12 Rev 0 16 April 2018

IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018

1

Purpose

Describes the responsibilities of those operating and maintaining an SIS.

TOPICS

Management's responsibilities

Training

Manage bypasses

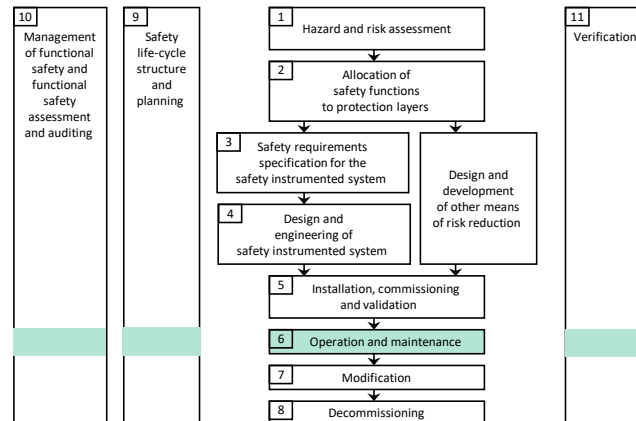
Proof test as per SRS

Control modifications to the SIS

Monitor SIS performance compared to assumptions in SRS

Operations and Maintenance

Operate and maintain the SIS to preserve functional safety as per SRS



Mod 12 Rev 0 16 April 2018

IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018

3

Operations' responsibilities

Train operators & maintainers

- what the SIS does
- how to use/maintain the SIS

Manage "bypasses" ("overrides") responsibly

- only for designated purposes for limited time

Proof test each SIF

- at frequency based on SIL verification
- promptly fix any faults found (!)

Control modifications to the SIS

- to maintain functional safety at all times

Monitor design assumptions for each SIF

- demand rate
- reliability data
- then update test intervals (or more) if required

Mod 12 Rev 0 16 April 2018

IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018

4

Training & procedures

What does each SIF do?

What hazardous event does each SIF protect against?

- [what should I do if it doesn't work?](#)

How should the operator respond to SIS fault alarms?

- [required responses to diagnostic alarms should be documented](#)

Use of bypasses & reset switches

- [when is it OK to bypass a SIF and what procedure needs to be followed?](#)

How and when are the SIF components proof tested?

- [what compensating measures are needed during test](#)

Written detailed procedures required for proof testing for each SIF

- [must describe every step including returning to service](#)

Bypasses

False alarms encourage complacency

Faulty detectors should be bypassed following an appropriate procedure

There may also need to be bypasses for operational reasons

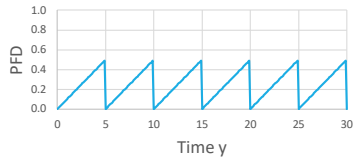
All need to be carefully controlled and compliance with procedures audited

IICA gas Detector Functional Safety Course

12. Operation & Maintenance

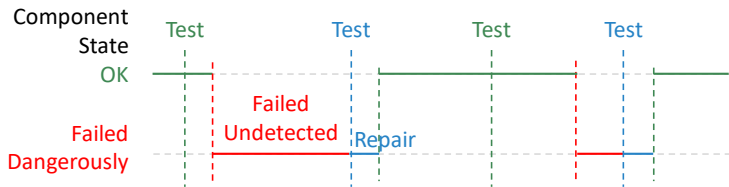
Why Proof Test?

Probability SIF has failed increases with time



$$PFD_{avg} = \lambda_{DU} TI / 2$$

Proof Test of a demand mode SIF uncovers failures undetected by diagnostics



After a Proof Test SIF is often assumed to be “as new”

- but must consider actual proof test coverage factor

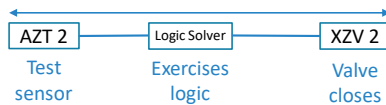
Mod 12 Rev 0 16 April 2018

IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018

7

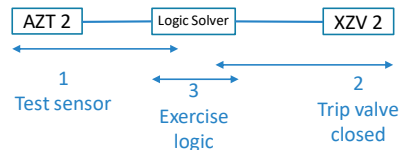
Proof testing strategies

Ideally perform end to end function test



- should usually be practical in a laboratory environment
- subsystem test intervals may be different, though

Partial testing is allowed



Ensure overlap so all elements are tested

Mod 12 Rev 0 16 April 2018

IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018

8

IICA gas Detector Functional Safety Course

12. Operation & Maintenance

SIS performance data collection

Must periodically review reliability assumptions in SIS design

- Initiating event frequency (or “demand rate”)
- SIF component reliability
- LOPA protection layer reliability (if relevant)

Collect demand and failure data continuously

Periodically compare against assumptions

- e.g. every 5 years

Update data

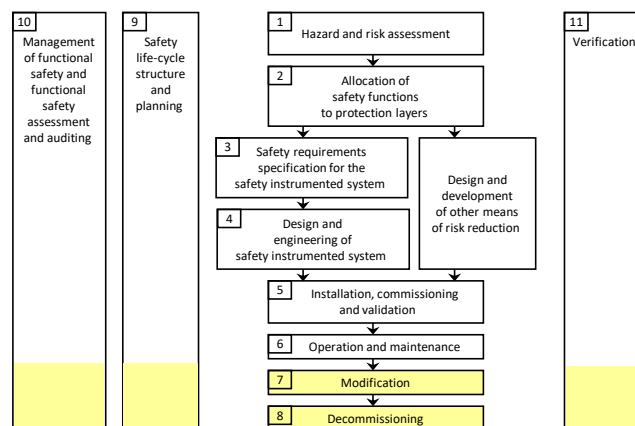
If required

- change test intervals
- modify SIS components

Modification & Decommissioning

Ensure functional safety is retained during and after modifications

Ensure decommissioned SIS or SIFs does not reduce functional safety



Aim of control of modifications

Also called Management of Change (MOC)

Must preserve functional safety after modification

- how does the proposed modification impact functional safety?
- what measures are needed to ensure the required functional safety is achieved?

Must preserve functional safety during modification

- modification must be planned
- Functional Safety Assessment must be performed prior to undertaking the modification (IEC 61511 Ed.2 new requirement - see 17.2.3, 17.2.6, 5.2.6.1.9)

Applies to:

- SIS hardware
- SIS software
- BPCS that may impact demand rates on SIS or SIS diagnostics
- process changes that may impact SIS including demands

Similar requirements for controlling decommissioning

Modification tips

Integrate with facility MOC procedure

- SIS can be impacted by a wide range of other modifications
- include checklist that can activate detailed SIS MOC process
- Check whether SIL determination impacted e.g. protection layers

Key requirements

- specify scope precisely
- analyse impact on functional safety
 - determine which lifecycle step to start from
- plan modification
- authorise modification
- Functional Safety Assessment
- implement
- validate
- update documentation

Summary

Described the responsibilities of those operating and maintaining an SIS.

Operations management's responsibilities are to:

- Train operators and maintainers
- Manage bypasses appropriately
- Proof test as per SRS
- Monitor SIS performance compared to assumptions in SRS
- Control modifications to the SIS

Questions?

