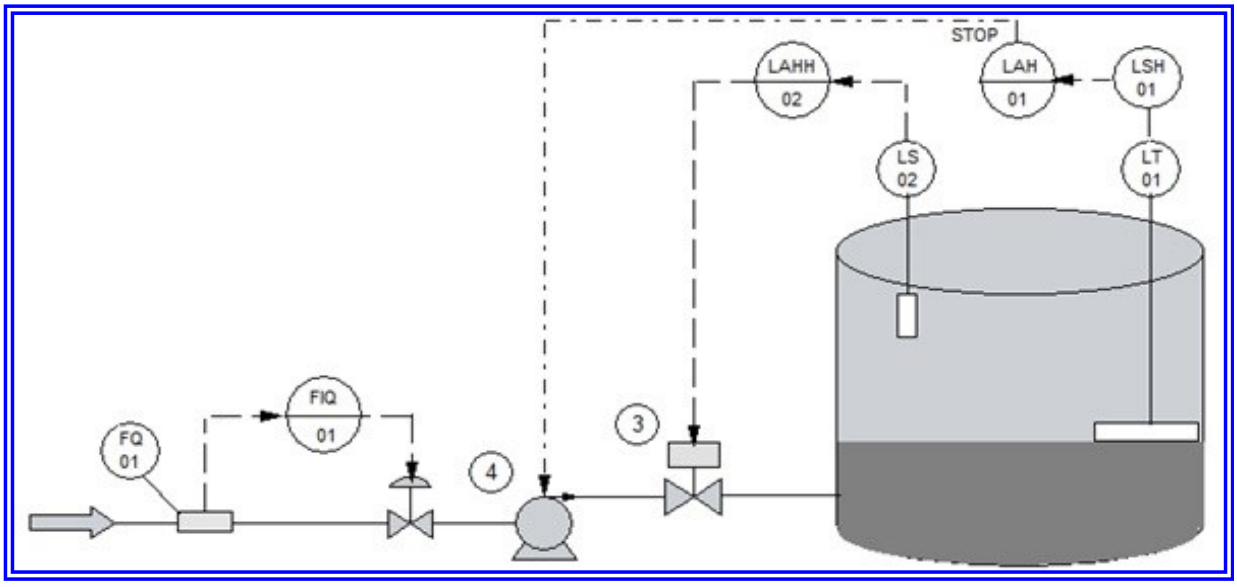
LIFECYCLE
SAFETY INSTRUMENTED SYSTEMS
FOR
THE REFINERY AND STORAGE INDUSTRY



David R Ransome
P & I Design Ltd

First Edition, August 2013
P&I Design Ltd

Released by
P & I Design Ltd
2 Reed Street, Thornaby TS17 7AF
www.pidesign.co.uk

drr@pidesign.co.uk

Printed by Billingham Press Ltd, Billingham TS23 1LF

Contents

Preface

P & I Design Ltd have been associated with providing clients with support for their process instrumented safety systems for over 30 years. Initially, called high integrity systems and then designed in accordance with the guidelines of PES. More recently, the design and lifecycle of Safety Instrumented Systems is required to be in accordance with the International Standard IEC 61508 and IEC 61511.

We have been associated with the Storage Industry for over 25 years.

Our clients being many of the member companies of either the Tank Storage Association (TSA) or United Kingdom Petroleum Industry Association (UKPIA).

Following the explosion at the Herefordshire Oil Storage Terminal on 11th December 2005. we have worked closely with industry, the trade associations and the regulator to provide assistance in ensuring process safety is paramount within the industry sector. This work includes being part of the Buncefield Standards Task Group (BSTG), Process Safety Leadership Group (PSLG) and Chemical and Downstream Oil Industry Forum, producing guidelines for risk assessment and Safety instrumented System Design.

With our multi-disciplined team, we can provide customer support throughout the IEC 61511 lifecycle phases. Including Risk Assessments utilising HAZOP, LOPA and the use of process modelling software to simulate process changes and disruptions, through design, commissioning, validation and operational support.

This document will present a summary of a practical life cycle approach to Safety Instrumented Systems (SIS) for the Storage Industry.

The Author

David Ransome is Chairman of P & I Design Ltd based in Teesside UK. A Chartered Engineer and a Fellow of the Institute of Measurement and Control with over 40 years' experience in the Chemical and Process Industry. Over recent years he has been involved with the PSLG working groups on LOPA and Safety Instrumented Systems, during that time was part of the team that wrote PSLG guidance on LOPA studies and Instrumentation in SIS. He has worked with CDOIF producing guidance on Prior Use equipment in SIS and is currently working on leak detection guidance.

Acknowledgements

A special thanks to my colleagues at P & I Design Ltd and engineers from many companies who have provided their services on the Buncefield Standards Task Group, Process Safety Leadership Group and Chemical Downstream Oil Industries Forum, to enhance Process Safety in the Oil Industry.

Process Safety

Process safety is a blend of engineering and management skills focused on preventing catastrophic accidents and near misses, particularly structural collapse, explosions, fires and toxic releases associated with loss of containment of energy or dangerous substances such as chemicals and petroleum products. These engineering and management skills exceed those required for managing workplace safety. (Reference Energy Institute: Adapted from Center for Chemical Process Safety of the American Institute of Chemical Engineers).

Process Safety in context of IEC 61508 requires the following:

⇒ Compliance with the Safety Lifecycle

⇒ Development and implementation of Safety Management

⇒ The design of safety protection systems

⇒ Competencies of those working with Safety Related Systems

Figure 1 details the lifecycle concept as defined in IEC 61508.

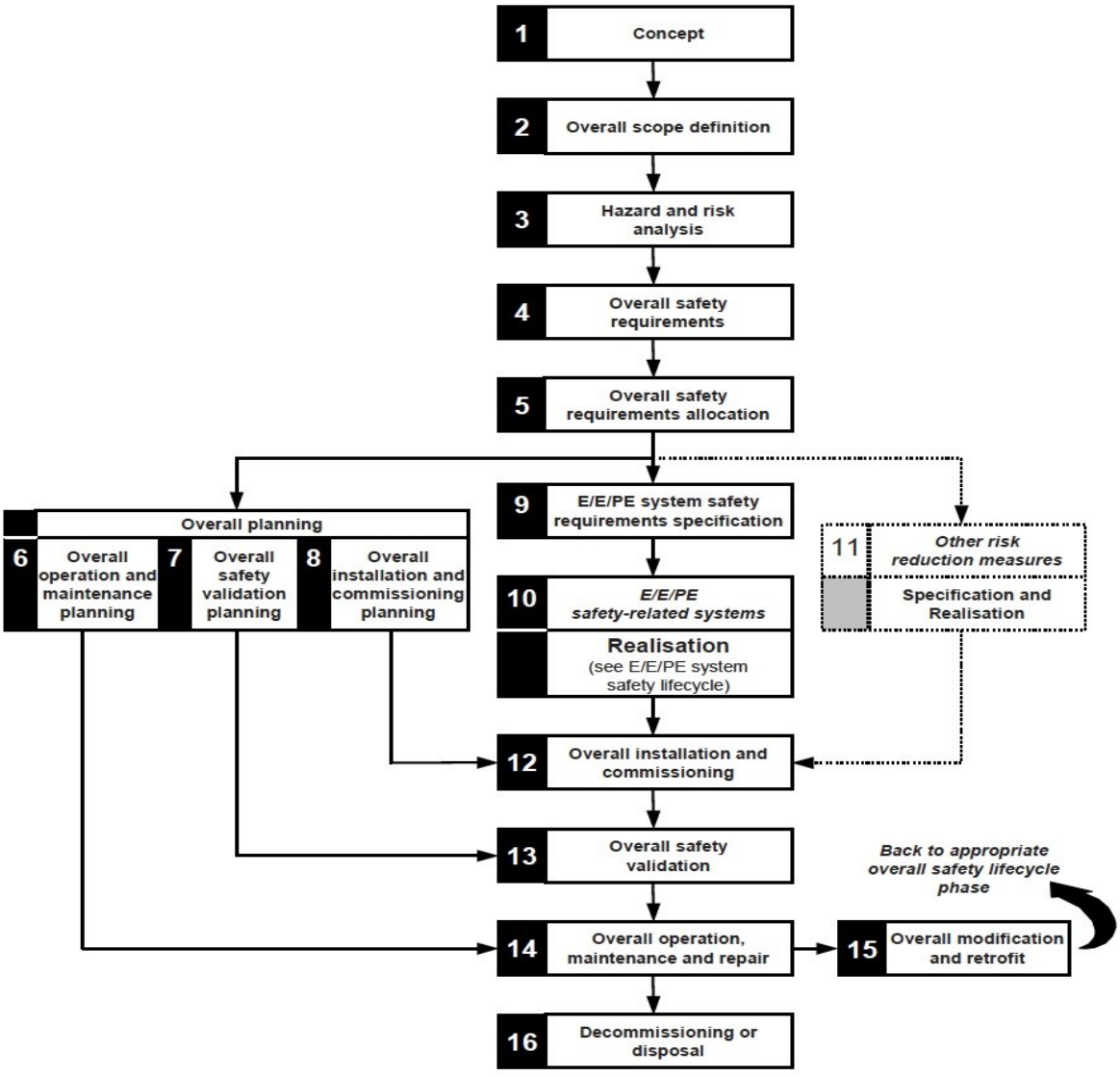


Figure 1: IEC 61508 Overall Safety Lifecycle Ref: BS EN 61508

Lifecycle

IEC 61511 defines the lifecycle for Safety Instrumented System utilised in the process industry. See Figure 2.

Hazard and Risk Assessment

There are many techniques that can be employed to risk assess a process. Often risk assessment is started by conducting a Hazard and Operability Study (HAZOP), Process Simulation Software can assist in modelling the process, providing a facility to see the response to process changes. The HAZOP will identify where protection is required, it does not however, quantify the level of protection that is required. The techniques utilised for this type of assessment range from simple Risk Graphs to full Quantified Risk Assessment (QRA). One of the most utilised technique is Layer of Protection Analysis (LOPA).

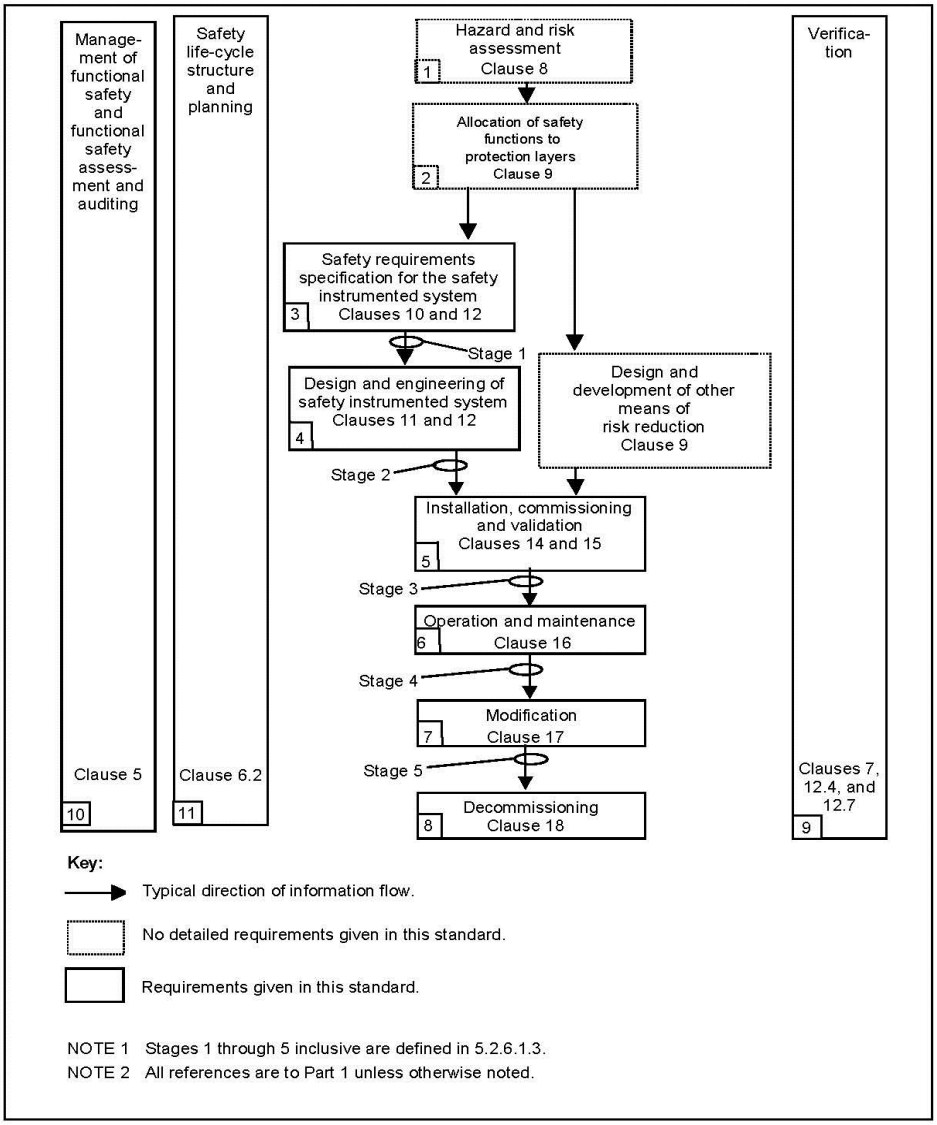


Figure 2: IEC 61511 SIS safety lifecycle phases—Ref: BS EN 61511

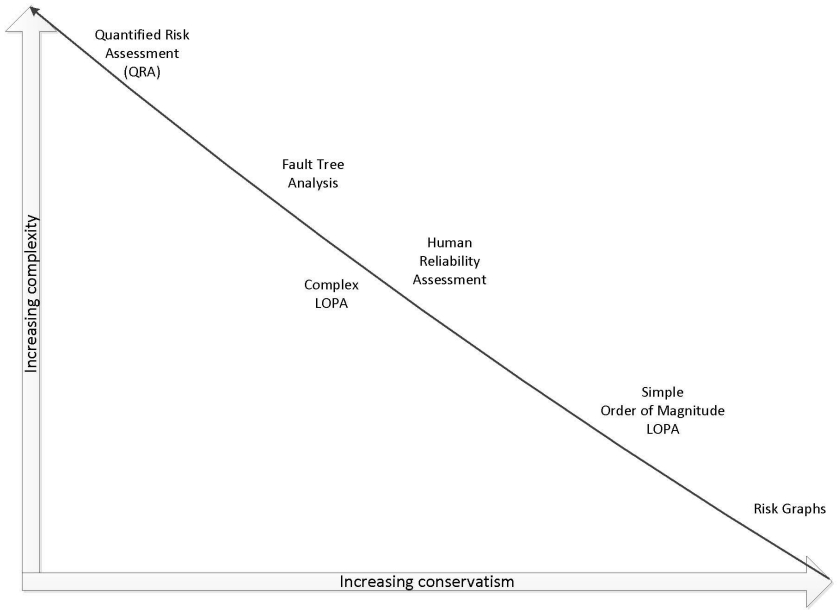


Figure 3: Risk Assessment Techniques — Complexity vs. Conservatism

As can be seen in Figure 3, different techniques for conducting risk assessments vary in complexity. It is important to ensure sufficient conservatism for the less complex techniques.

Layer of Protection Analysis (LOPA)

The LOPA technique is a scenario based risk assessment methodology.

The following provides a guide on how a LOPA study is conducted.

1. Establish the Scenario to be assessed.
2. What are the consequences?
3. What are the initiating events?
4. Determine the Risk Tolerance Criteria (RTC).
5. Calculate the initiating event frequencies, including any enabling events.
6. Quantify all risk reducing measures, protection layers and conditional modifiers
7. Perform LOPA calculations and compare results to the RTC .

The figure below shows the principle of the Layer of Protection technique. It is essential that each layer is independent from each other to ensure that protection is achieved.

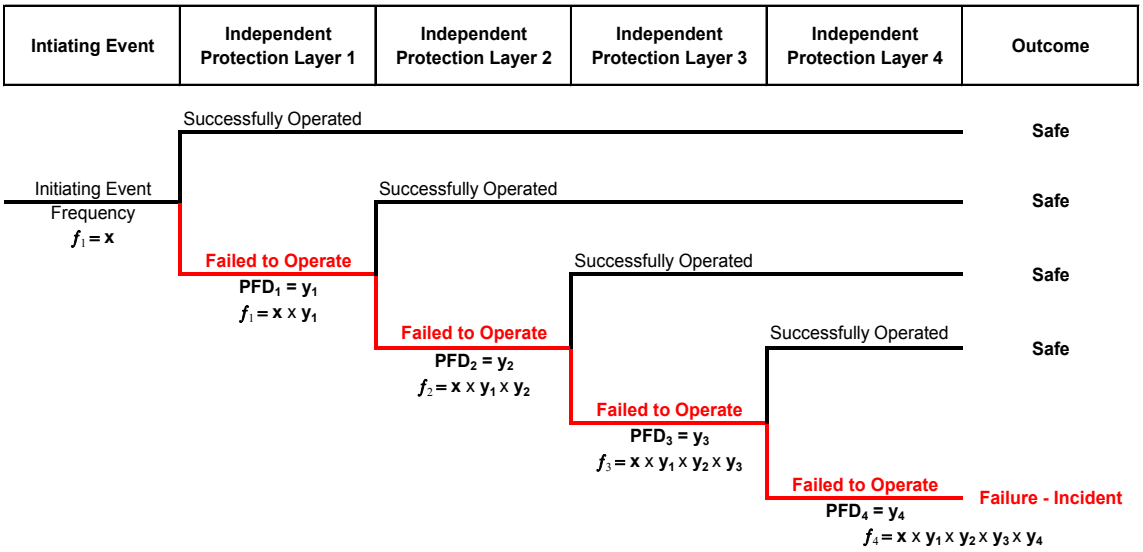


Figure 4: Layer of Protection Model

SIL Determination and allocation of Safety Instrumented Functions

By utilising the LOPA technique, if a Safety Instrumented Function (SIF) is required for a protection layer, then a Safety Integrity Level (SIL) with a required risk reduction factor or probability of failing on demand (PFD) will have been established. The chart below indicates the relationship between SIL, RRF and PFD.

Safety Integrity Level	Probability of failure on demand	Availability %	Non Availability Continuous Demand	Risk Reduction Factor
SIL 1	0.1 to 0.01	90 to 99%	876 to 87.6 hours/year	10 – 100
SIL 2	0.01 to 0.001	99 to 99.9%	87.6 to 8.76 hours/year	100 - 1000
SIL 3	0.001 to 0.0001	99.9 to 99.99%	8.76 to 0.876 hours/year	1000 - 10000
SIL 4	0.0001 to 0.00001	99.99 to 99.999%	52 to 5.2 minutes/year	>10000

Figure 5: SIL, PFD and RRF relationship

Safety Requirement Specification (SRS)

The SRS is a pivotal document within the IEC 61511 Lifecycle. It's purpose is:

1. To define the Safety Instrumented Functions and Safety Integrity Levels together with Hardware Fault Tolerances (HFT) and system structure.

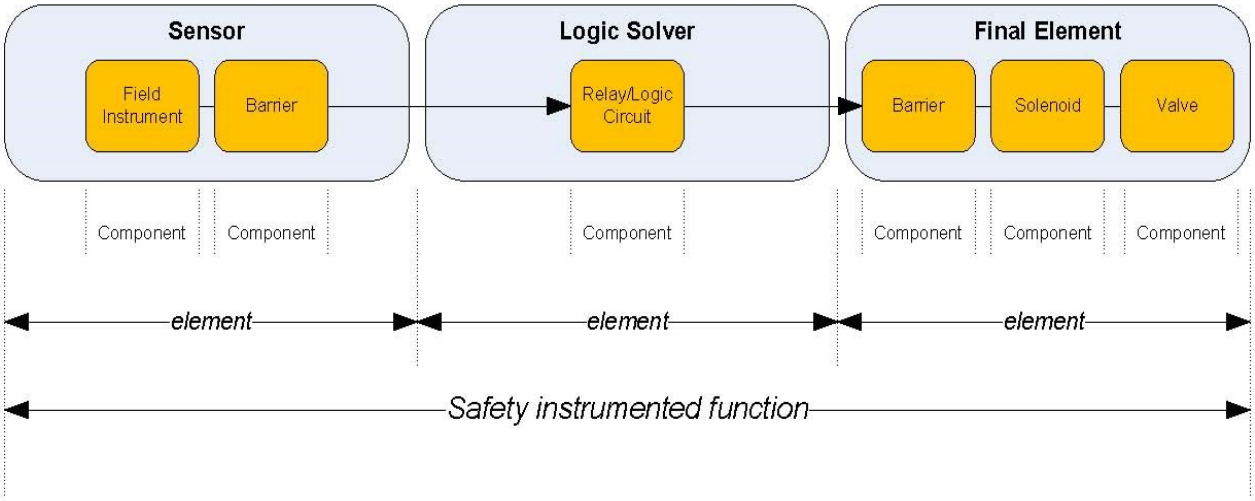


Figure 6: Elements and Components of a Safety Instrumented Function Ref: CDOIF

	Minimum required HFT unless clause 11.4.6 applies		
SIL	0	1	2
1	X		
2 (low demand mode)	X		
2 (high demand mode)		X	
3		X	
4			X

Figure 7: Hardware Fault Tolerance with regard to SIL Ref: BS EN 61511 2012 Draft

2. Provide information on:
    - i) The safe state of the process
    - ii) Time of response of the SIF
    - iii) The likely demand on the system — Low Demand or Continuous
    - iv) Settings and ranges of instrumentation and levels of concern
    - v) The process and environmental limitations
    - vi) Interface with other control systems
    - vii) Manual shutdown facilities and overrides
    - viii) Acceptable spurious trip rate
    - ix) Proof testing requirements

3. Provide the Designer with the Users requirements of the system.

Design & Engineering of the Safety Instrumented System

Often referred as the realisation phase, the detailed design and engineering of the SIS requires many documents to be produced. The diagram below gives an example of the documentation workflow that would be produced throughout the IEC 61511 lifecycle.

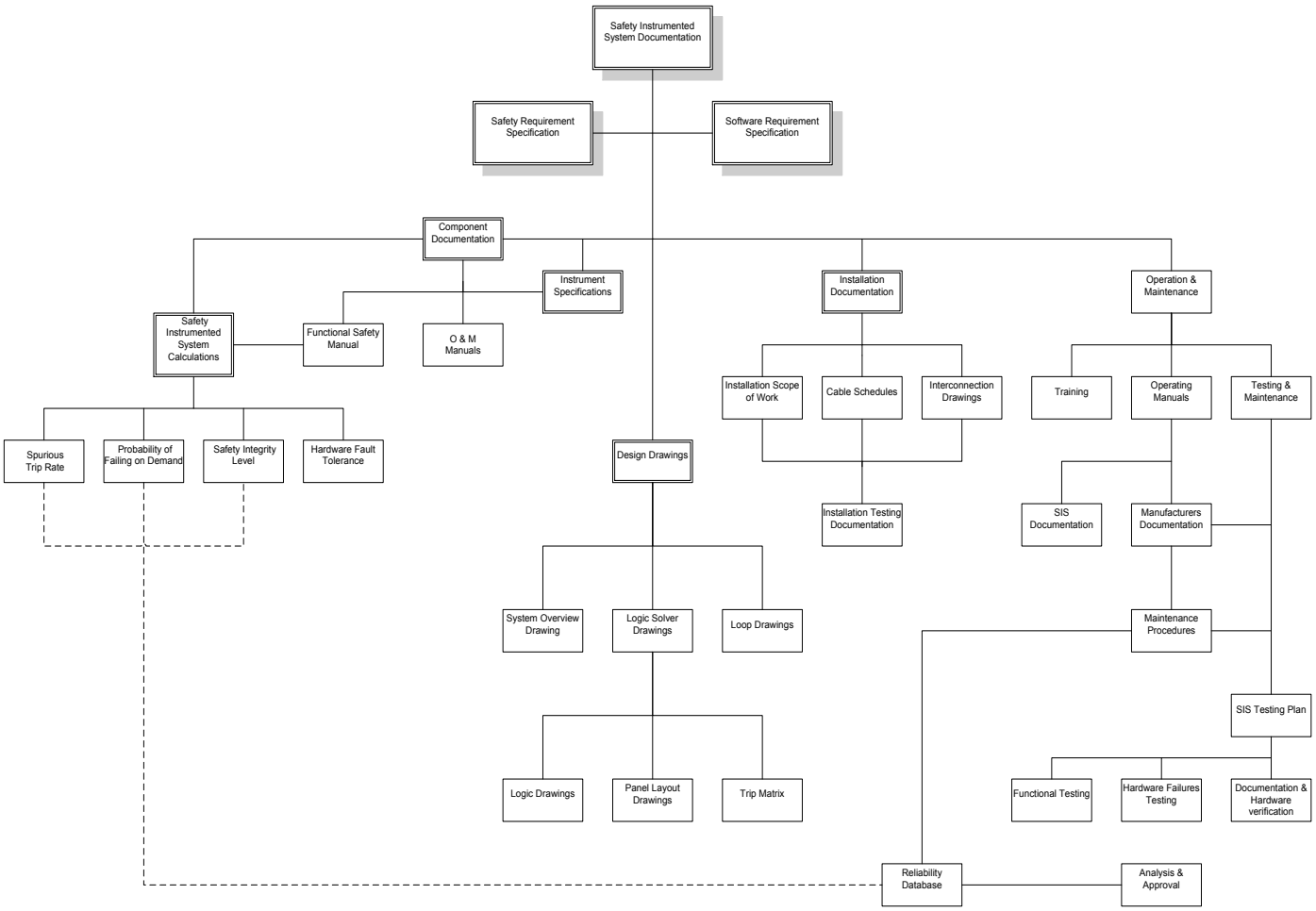


Figure 8: Typical Safety Instrumented System Documentation Workflow

It is customary for all of the validation and proof testing documentation to be produced during the design phase, together with compilation of manufacturer's documentation and operating procedures.

Installation, Commissioning and Validation.

From the Design Lifecycle phase, all the documentation required for installation, commissioning and validation will have been produced. The diagram above details the typical documentation required to ensure that the installation is completed in accordance with the design requirements.

In order to ensure the installation is completed satisfactorily, it is essential that the installer is aware of his responsibility and when the installation is complete, provides completed installation compliance documentation.

After inspection of the installation, Site Acceptance Tests (SAT) are conducted. This will include commissioning of the system and full validation to ensure that functional safety has been achieved and that the SIS operates as required.

Verification

Throughout all lifecycle phase, verification of all activities is a requirement of the standard.

An efficient system of management for analysis and approval is required to ensure all activities of the SIS are recorded and available. Databases or Data Repositories are useful for large systems. P & I Design Ltd utilize and are agents for the ProSys DR IEC 61511 Compliant Software for this purpose.

Late Lifecycle Phases

Operation and Maintenance

It is essential that all operators and maintenance technicians appreciate their roles and responsibilities when working with Safety Instrumented Systems.

Operators must know how the system operates and what actions to take in the event of any activation. It is quite possible that a SIS which operates in a low demand mode may not activate because of an actual demand on it throughout an operators working life.

Maintenance Technicians must ensure that when working on SIS that they ensure the system is fully operable after any maintenance work. It is good practice to perform as found and as left tests after any maintenance activity.

Proof testing of the SIS is essential to ensure that it is performing as intended. The original SIL and PFD calculations are based on mathematical modeling, so actual reliability data must be built up in service.

In order to provide efficient analysis and approval of the system, effective records must be kept, these should include:

Genuine activations, Spurious trips, Equipment failures, Any maintenance activity, All proof testing

Proof testing, where possible should be end to end and if possible, whilst not taking the process into a dangerous state, should involve activation by the process.

In many circumstances the above is not practical, where this is the case then testing procedures and testing plans should be developed to ensure the complete system is tested to ensure that any partial testing does not degrade the required PFD and SIL of the system.

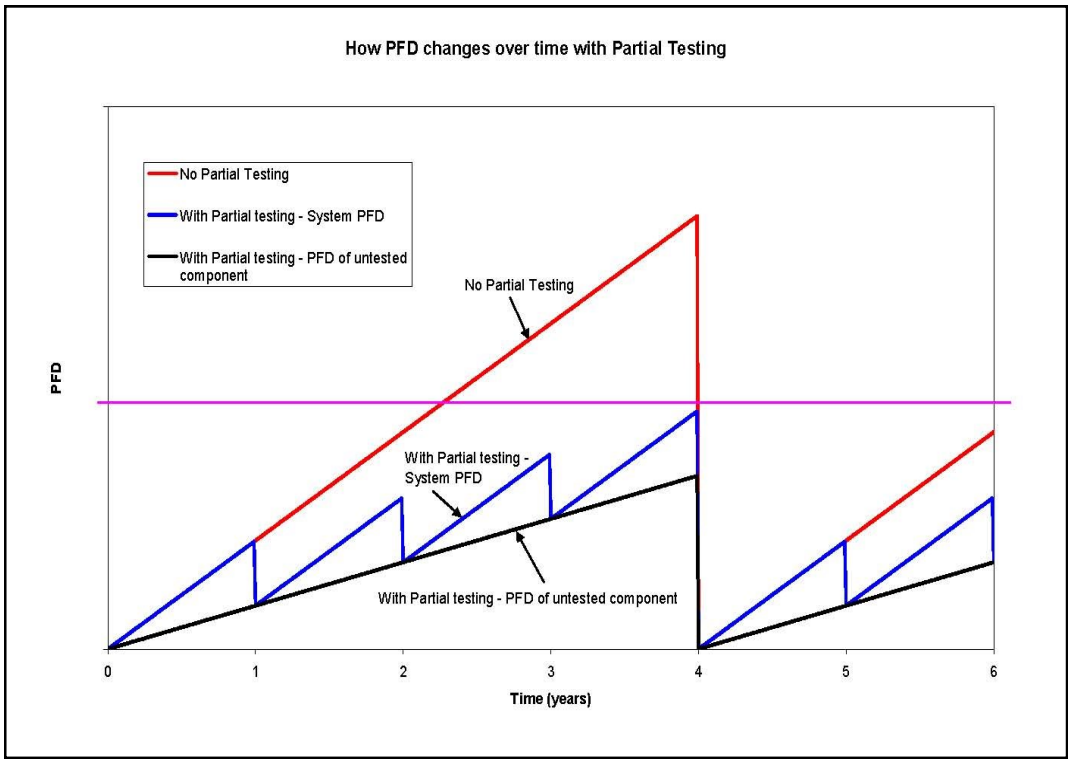


Figure 9: PFD changes due to Partial Testing Ref: HSE

Modification

No modifications to the Safety Instrumented System should be performed without following a documented procedure for modification, to ensure functional safety.

A modification plan should be developed to make any corrections, enhancements or adaptions to the SIS, ensuring that the required SIL and PFD is maintained. Any modification of the SIS will require re-entering the safety lifecycle at an appropriate step to the consequences of the modification.

Decommissioning

When the SIS is to be decommissioned a decommissioning plan must be developed.

It is essential to review its functionality and relationship with other protection layers to ensure that removal will not put an additional demand on other systems.

Development and implementation of Safety Management.

As shown on Figure 2, Management of Functional Safety and Functional Safety Assessments continues throughout the total SIS lifecycle.

In order for the SIS to function correctly, management procedures must ensure that all aspects of the lifecycle are correctly managed and that everybody involved is aware of their roles and responsibilities and are competent to perform their required tasks.

A controlling document is useful to monitor and maintain the management of the system. This document should detail each lifecycle phase with the relevant tasks and persons responsible and involved in that particular task.

The document should also detail the stages where Functional Safety Assessments, which are a fundamental requirement of the lifecycle, are to be conducted.

The standard advises five stages for Functional Safety Assessments:

Stage 1: After Risk Assessment when the required protection layers have been identified and the Safety Requirement Specification has been developed

Stage 2: After the Safety Instrumented System has been designed

Stage 3: Following installation, commissioning and validation of the SIS

Stage 4: After gaining experience in operating and maintenance of the SIS

Stage 5: After modification and prior to decommissioning of the SIS

The number, size and scope of the assessment is decided upon specific circumstances considering the following;

Size and duration of the project

Degree of complexity

Safety Integrity Level

Consequence in the event of failure

Degree of standardisation and previous experience with similar designs

Safety regulatory requirements

Competencies of those working with Safety Related Systems.

For a person to be competent, they need qualifications, experience, and qualities appropriate to their duties.

These include:

- Training to ensure the necessary knowledge is acquired for the tasks required to be performed
- Adequate knowledge of the hazards and failures of the equipment for which they are responsible
- A knowledge and understanding of the working practices used in the organization
- The ability to communicate effectively with their peers, with any staff working under their supervision, and with their supervisors
- An appreciation of their own limitations and constraints, whether knowledge, experience, facilities or resources and a willingness to point these out

Training

Training is an essential component of competency. It is important that training programmes are developed suitable to an individuals role and responsibility. Training records should be produced and retained. Often a task skill matrix is produced to ensure that the correct training and skills are available.

P & I Design Ltd

Established in 1978, providing Consultancy, Engineering Design and Support Services to the Process Industry.

Our multi-disciplined teams expertise allows us to provide support to our Clients from Project conception through to detailed design, commissioning and operational support.

Process & Environmental Engineering

E&I & Process Control

Safety Studies & Systems

SERVICES

P & I Design have been providing Design Services to the Process Industries for over 30 years.

Our Engineering staff includes Engineers and Technicians with expertise in:-

- Process & Environmental Engineering
- Electrical & Instrumentation Systems
- Process Control
- Safety Studies & Safety System Design
- IT Services
- Installation Supervision
- Commissioning
- 24/7 Support

IT Services

Commissioning & Support

Contact Us

SAFETY STUDIES & SYSTEMS

P & I Design have since its inception been involved in providing Safety Studies for the Process Industry. These include HAZID (Hazard identification) & HAZOP (Hazard & Operability) Studies.
Since the introduction of IEC 61508 and subsequent BSEN 61508 & BSEN 61511 we have been providing LOPA studies and SIL determination.
The use of LOPA as a risk assessment tool has developed significantly since the explosion at the Hereford Oil Storage Depot at Buncefield in December 2005.

ENGINEERING SUPPORT

Our extensive range of services include:-

- Total engineering of process plant from initial conception through to final commissioning.
- Complete Consultancy on projects, providing design, specification, procurement, inspection, installation supervision and acceptance.
- Provision of qualified chemical, instrumentation and software engineering personnel.
- Process Simulation and Modelling.
- Engineering software products, CHEMCAD & ProSys DR software.
- Custom designed I.T. Systems , network & Support.

P & I Design Ltd are UK agents for:

Chemstations™
CHEMCAD™ process simulation software

ProSys DR
PROTECTIVE SYSTEMS DATA REPOSITORY
IEC 61511 Compliant Database

P & I Design Ltd
2 Reed Street, Gladstone Industrial Estate
Thornaby, Stockton-on-Tees, TS17 7AF, United Kingdom
PHONE: 01642 617444
FAX: 01642 616447
email: drr@pidesign.co.uk
web: www.pidesign.co.uk