[Company Name]

[Description]

Safety Requirement Specification

Document Number: Click here to enter text.

Revision: Click here to enter text.

Date: Click here to enter a date.

P & I Design Ltd
2 Reed Street
Thornaby
TS17 7AF
01642 617444
www.pidesign.co.uk

Version 1.1 February 2017

Contents

1 Revision Control

Revision	Enter Revision.
Date of Revision	Click here to enter a date.
Description	Click here to enter text.
Created By	Enter Digital Signature.
Checked By	Enter Digital Signature.
Approved By	Enter Digital Signature.

Revision	Enter Revision.
Date of Revision	Click here to enter a date.
Description	Click here to enter text.
Created By	Enter Digital Signature.
Checked By	Enter Digital Signature.
Approved By	Enter Digital Signature.

Revision	Enter Revision.
Date of Revision	Click here to enter a date.
Description	Click here to enter text.
Created By	Enter Digital Signature.
Checked By	Enter Digital Signature.
Approved By	Enter Digital Signature.

Revision	Enter Revision.
Date of Revision	Click here to enter a date.
Description	Click here to enter text.
Created By	Enter Digital Signature.
Checked By	Enter Digital Signature.
Approved By	Enter Digital Signature.

Revision	Enter Revision.
Date of Revision	Click here to enter a date.
Description	Click here to enter text.
Created By	Enter Digital Signature.
Checked By	Enter Digital Signature.
Approved By	Enter Digital Signature.

2 Safety Instrumented System

2.1 Introduction

This document has been prepared for the Safety Instrumented System (SIS) as detailed within this document. A Safety Requirement Specification is part of the life cycle documentation of the SIS in accordance with BS EN 61508 & BS EN 61511 and is intended to be a working document throughout the life of the Safety System.

SIS Unique Identifier	Enter SIS Number.	
Title	Click here to enter title	
Location	Click here to enter location.	
Safety Integrity Level Required (If different for individual SIF's see details in Section 2.2 and on cause and effect matrix)	Choose a SIL	Choose a SC

2.2 Functional Description

SIS Description	Click here to enter SIS Description
SIF Description	xxssssfsfgdgdasgdsg

2.3 Reference Documentation

In addition to this document the SRS comprises of the following documentation.

Cause & Effect Matrix	Enter document reference for cause & effect matrix.
Schematic Overview Drawing	Enter document reference for overview drawing
Other	Enter document reference
Other	Enter document reference

3 Risk Analysis & Allocation of Safety Functions

The SIS detailed in this SRS is required as a result of a Hazard & Risk Assessment which deemed the requirement for an additional protection layer with the following Safety Instrumented Functions (SIF), each with a specified Safety Integrity Level (SIL).

3.1 Risk Assessment

Date of Risk Assessment	Click here to enter a date.
Document Number	Enter Document Number.
Revision utilised for this SRS	Enter Revision.
Type of Assessment	Choose an item.
Summary of Outcome of Risk Assessment	Click here to enter text.

3.2 Security Risk Assessment

IEC 61511 places a requirement that the SIS security should be risk assessed.

Date of Risk Assessment	Click here to enter a date.
Document Number	Enter Document Number.
Revision utilised for this SRS	Enter Revision.
Type of Assessment	Choose an item.
Summary of Outcome of Risk Assessment	Click here to enter text.

3.3 Allocation of Safety Functions

This SRS utilises a cause & effect matrix to provide information on each of the required SIF's. Detailed below is information on the cause & effect terminology. The cause & effect matrix details all of the SIS inputs and outputs together with the action to be taken on activation.

SIF Number	Unique safety instrumented function number, if the function is not SIL rated this may be blank or a description of the type of function will be displayed
Tag Number	SIS component unique number
SIL	The required Safety Integrity Level for the Safety Instrumented Function
MooN	Subsystem architecture – M number of components out of N number of components required to perform the SIF
Type	This SRS provides a simplified system model of the structure of the SIF, the system model type is referenced on the cause & effect matrix
Calibration	Calibrated range of the sensor in engineering units, not applicable for contact point switches
Set	Process setting of trip point, ↓ Trip on falling ↑ Trip on Rising in engineering units / %. Or activation state of trip input e.g. activated, closed, opened.
Origin	Set point derived from reference e.g. Level of Concern, process calculations, physical limits.
Sensor Elements	Description of device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches) Elements may also be subdivided by plant or geographical area. Sensor Element Subsections - MANUAL SHUTDOWN - Manual action on SIS to achieve a safe state E.G Emergency Shutdown / isolation system. AUTOMATIC SHUTDOWN – Automated action of SIS working by itself with no direct human control
Final Elements	Description of equipment which implements the physical action necessary to achieve a safe state. e.g. valves, switch gear, motors. Elements may also be subdivided by plant or geographical area
SIS Status	The SIS operator interface, note this is not part of the SIS and is for information to the operator
NP	This indicates that the action taken utilises a non-programmable technique
PE	This indicates that the action taken utilises a programmable electronic technique
Notes	Provides additional information on the function

4 SIL Design & Verification Considerations

The following information is to be the basis of design for the SIS. SIL verification is a combination of evaluating component random hardware failure rates - Probability of Failing on Demand (PFD) together with systematic failures and Systematic Capability (SC) together with hardware fault tolerance of the subsystems.

4.1 Random Hardware Failure Rate

Individual component failure rate can be expressed in several ways:

4.1.1 IEC 61508 SIL Certificated Devices

When a component manufacturer has provided the device for external assessment to an accredited test facility, a certificate will be provided. The certificate will normally express the suitability for the component as SIL capable, with a SIL number being provided, it will also state what Hardware Fault Tolerance (HFT) is required to incorporate the device or devices into a SIS to achieve the SIL. The certificate may provide failure rate data quoted as PFD or λ (total failure rate per hour) with detailed failure modes: safe detected, safe undetected, dangerous detected and dangerous undetected. Failure rate is normally expressed as FITS (1 FIT = 1 x 10^{-9} hours).

Certification of components is often based upon Failure Mode and Effects Diagnostic Analysis (FMEDA), this analysis does not take into effect external factors that may contribute to random hardware failures and a shift in the PFD.

Recently certified components may also have on the certificate, the systematic capability. SC which is expressed by a number and this number equates to the same scale as that of SIL.

4.1.2 Mean Time Between Failures (MTBF)

MTBF is expressed in years, $MTBF_{(d)}$ represents mean time between dangerous failures. It is also the reciprocal of failure rate. These figures are often supplied by manufacturers of components based upon components that have not been externally certified. The concern of supplier only MTBF data is that it may be grossly overstated. This is due to the fact that many components are never returned to the manufacturers and are simply disposed of by the end user.

4.1.3 In Service Failure Data

If end user data is available and the sample size used to provide the data is sufficiently large, then this data is more likely to reflect in service random hardware failure rates. However, figures should not be used which claim better than on the equivalent component certification.

4.2 SIS Subsystem Requirements

The following tables provide information on the operating requirement and constraints of the SIS components;

4.2.1 Sensor(s)

Sensor Duty	Click here to enter duty.		
Process	Choose a process	Choose a process	
Process Temperature	Choose a temperature	Choose a temperature	
Sensor Location	Choose a location.		
Electrical Area Classification	Choose a Zone.	Choose a Gas Group.	Choose T class
Environmental and other Conditions **Tick Box of all that may apply**	☐ High Humidity ☐ Flooding ☐ Lightning ☐ Vibration ☐ Electromagnetic ☒ Radio Interference ☐ Electrostatic Discharge Other Considerations: Click here to enter text.		
Preferred Technology	Choose a technology.	Note: If PE devices are employed then programmability must be restricted to sensor settings and calibration	
Preferred Subgroup Architecture	Choose an architecture	Note: If not 1oo1 then preference to be given to components of different technologies and or manufacturers	
SIL Capability	Choose a SIL	Choose a SC	
SIL Compliance	Choose a method.	Note: If Prior Use then utilise the CDOIF - Demonstrating prior use of elements of a safety instrumented function in support of BS EN 61511, available on HSE website	

4.2.2 Logic Solver

Duty	Click here to enter duty.		
Description	Click here to enter text.		
Logic Solver Location	Choose a location.		
Electrical Area Classification	Choose a Zone.	Choose a Gas Group.	Choose T class
Environmental and other Conditions **Tick Box of all that may apply**	☐ High Humidity ☐ Flooding ☐ Lightning ☐ Vibration ☐ Electromagnetic ☐ Radio Interference ☐ Electrostatic Discharge Other Considerations: Click here to enter text.		
Preferred Technology	Choose a technology.	Note: If PE devices are employed then a Software Specification is to be produced in accordance with Clause 12 BS EN 615611	
Preferred Subgroup Architecture	Choose an architecture	Note: If not 1oo1 or 1oo2D then preference to be given to components of different technologies and or manufacturers.	
SIL Capability	Choose a SIL.	Choose a SC.	
SIL Compliance	Choose a method	Note: If Prior Use then Clause 11.5.5 BS EN 61511 applies	

4.2.3 Final Element(s)

Final Element Duty	Click here to enter duty.		
Process	Choose a process	Choose a process	
Final Element Type	Choose a type. Click here to enter text.		
Process Temperature	Choose a temperature	Choose a temperature	
Final Element Location	Choose a location.		
Electrical Area Classification	Choose a Zone.	Choose a Gas Group.	Choose T class
Environmental and other Conditions **Tick Box of all that may apply**	☐ High Humidity ☐ Flooding ☐ Lightning ☐ Vibration ☐ Electromagnetic ☐ Radio Interference ☐ Electrostatic Discharge ☐ Pressure Surge Other Considerations e.g. Tight shut off, slow closing etc. Click here to enter text.		
Preferred Technology	Choose a preferred technology.	Note: If PE devices are employed then programmability must be restricted to settings and calibration	
Preferred Subgroup Architecture	Choose an architecture.	Note: If not 1oo1 then preference to be given to components of different technologies and or manufacturers	
SIL Capability	Choose a SIL	Choose a SC	
SIL Compliance	Choose a method	Note: If Prior Use then utilise the CDOIF - Demonstrating prior use of elements of a safety instrumented function in support of BS EN 61511 available on HSE website	

4.3 SIS General Requirements

4.3.1 General

SIS Mode of Operation	Choose Demand Mode.
Sources of Demand on SIS	Click here to enter text.
Method of tripping	Choose an item.
Process Safe State	Click here to enter text.
Description of any process safe states that occurring together can create a separate hazard	Click here to enter text.
Description of any dangerous combinations of output states	Click here to enter text.
Are there any requirement for the SIS survive a major accident event. i.e. Tight shut off, firesafe etc.	Click here to enter text.
Methods of maintaining a safe state in the event of a fault	Click here to enter text.
Additional requirements for start up, shut down or maintenance	Click here to enter text.
Are by-passes or overrides required	Choose an item.
Description of the method of manually bringing the system to a safe state, both for normal operation and in an emergency	Click here to enter text.
What actions are to be taken to avoid common cause failure	Click here to enter text.
Requirements for resetting after activation	Click here to enter text.
What precautions will be employed to alleviate anticipated systematic failures	Click here to enter text.
What is the maximum allowable spurious trip rate	Click here to enter text.
What is the mean time to repair and are there any requirements for spare parts	Click here to enter text.
What interfaces exist between the SIS and BPCS	Click here to enter text.
Are there any permissive inputs into or out of the SIS which could impact on the operation of this or other protection systems	Click here to enter text.

4.3.2 Process Safety Time

It is essential for safe operation that sufficient time exists for the protection layers to complete their functions before the process reaches a dangerous state. For any safety function, the process safety time must be longer than the SIS response time.

If not contained in this document, what document contains the details of the following:	Click here to enter details.	
What is the Process Safety Time (PST)	Click here to enter PS.	Definition: PST is the period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the equipment under control (EUC) or EUC control system and the time by which action has to be completed in the EUC to prevent the hazardous event occurring. Ref BS EN 61508
What is the Sensor response delay time S_t	Click here to enter St	Definition: This is the time the sensor takes to identify the initiation of the trip and activate its output
What is the response time of the logic solver L_t	Click here to enter Lt	Definition: This is the time the logic solver takes to process the input from the sensor and activate an output to the final element
What is the response time of the final element, inclusive of any slow closing requirements FE_t	Click here to enter FEt	Definition: This is the time the final element takes from receiving the command from the logic solver to completing its function and bringing the process to its safe state
SIF Response Time $S_t + L_t + FE_t$	Click here to SIF Response Time.	
Fraction of SIF response time to PST	Click here to enter fraction	Typically the SIF response time should be no more than half of the PST

4.3.3 Safety Manuals, Maintenance, Operation & Proof Testing

To ensure the correct design, installation, commissioning and operation of the SIS the following are to be provided.

Component Suppliers requirement **Tick Box of all that may apply**	☐ SIL certification and or reliability data ☐ SIL Verification Report ☐ Safety Manual ☐ Recommended spares list – minimum 2 years ☐ Operation and Maintenance Manual ☐ Installation Manual and Drawings ☐ ATEX certification ☐ Programming software
Designer/System Integrator **Tick Box of all that may apply**	☐ SIL Verification Report ☐ Design documentation ☐ Installation, documentation and scope of work ☐ FAT and SAT plans and procedures ☐ Proof testing plans, timescale and procedures ☐ Completed documentation manuals, including component manufacturer's documentation
Installation and Commissioning **Tick Box of all that may apply**	☐ As built marked up documentation ☐ Cable and Installation test sheets ☒ FAT Report ☐ SAT Report ☐ Validation Testing of SIF's ☐ Handover Report
Operation and Maintenance **Tick Box of all that may apply**	☐ Management of Functional Safety Documentation ☐ Management of Change Procedures ☐ Proof Testing ☐ Analysis of SIS operation and reliability records

5 Certified PFD – In service adjustment

The following section details an assessment to consider if any adjustment is to be applied to the certified or MTBF reliability data.

It is to be completed with reference to each of the SIF subsystem components. Logic solvers and non-field equipment which is mounted in control or switch rooms may not require adjustment as it is not subjected to the same susceptibilities as sensors and final elements.

If in service failure rates have been utilised for calculating the PFD then no further adjustment should be required. However, if the PFD is certificated or derived from MTBF, then consideration in adding an in service PFD should be considered.

5.1 Process and Environmental Impact

Process Duty and process conditions **Tick Box of all that may apply**	☐ Extreme of process/temperature – excursions ☐ Cavitation – surges ☐ Solids, blockages, build up ☐ Process connections – impulse tubing, wet legs ☐ Static process measurement – resulting in sticking Other: Click here to enter text.

Environmental and location Conditions **Tick Box of all that may apply**	☐ Extreme of temperature/humidity ☐ Corrosive atmosphere ☐ Lightning Strike ☐ Susceptibility to damage from external sources - location ☐ Ingress Protection failure Other: Click here to enter text.

5.2 PFD adjustment

Adjustment for sensor subsystem	Choose a susceptibility The following Failure Rate (years^{-1}) to be added to PFD of sensor subsystem: Choose a PFD.

Adjustment for logic solver subsystem	Choose a susceptibility. The following Failure Rate (years^{-1}) to be added to PFD of logic solver subsystem: Choose a PFD.

Adjustment for final element subsystem	Choose a susceptibility. The following Failure Rate (years^{-1}) to be added to PFD of final element subsystem: Choose a PFD.

6 Competence

Any person, department or organisation involved in the implementation of this SIS, irrespective of lifecycle phase, shall be competent to carry out the activities for which they are responsible. They shall be informed of their responsibilities by the appropriate organisation responsible for that lifecycle phase.

Procedures shall be in place, by all organisations involved in this SIS, to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

7 System Model

The following figures graphically represent the architecture for each different SIF type, see Section 3.2 and causes and effect matrix.