P & I Design Ltd

Process Instrumentation Consultancy & Design

2 Reed Street, Gladstone Industrial Estate,
Thornaby, TS17 7AF, United Kingdom.
Tel. +44 (0)1642 617444 Fax. +44 (0)1642 616447
Web Site: www.pidesign.co.uk

PHILLIPS 66

BRAMHALL TERMINAL

GANTRIES OVERFILL PROTECTION

SAFETY INSTRUMENTED SYSTEM BRM-SIS2

MANAGEMENT MANUAL

Contents

P & I Design Ltd

Process Instrumentation Consultancy & Design

2 Reed Street, Gladstone Industrial Estate,
Thornaby, TS17 7AF, United Kingdom.
Tel. +44 (0) 1642 617444 Fax. +44 (0) 1642 616447
Web Site: www.pidesign.co.uk

CONOCOPHILLIPS

BRAMHALL TERMINAL

ROAD LOADING

SAFETY INSTRUMENT SYSTEM

FUNCTIONAL SAFETY ASSESSMENT

STAGE 4

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	20.01.12	D R Ransome	DSR	Client	FSA Stage 4	
B	30.03.17	D S Regan	DBF	Client	FSA Closed	
						Document No. **SI181001_RPT**

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION HISTORY

Rev	Description
A	Original Issue at FSA Stage 4

2 SCOPE

ConocoPhillips have installed an Independent High Level Alarm system to provide a SIL 1 rated automatic shutdown system to prevent road tanker overfills.

The overfill protection system is required to comply with the international standard BS EN 61511.

Functional Safety Assessment (FSA) is a component part of the process to demonstrate compliance with BS EN 61511 and that the system is providing the intended protection. Prior to this FSA no previous FSA's have been conducted.

This report has been prepared as a Functional Safety Assessment Stage 4 "After gaining experience in operating and maintenance". However, as no previous assessment have been completed this FSA will also review Stages 1 to 3.

3 INTRODUCTION

The fuel storage depot is owned and managed by ConocoPhillips Ltd. and classified as a top tier site under the COMAH Regulations. The Major Incident Investigation Board (MIIB) established following the explosions and fires at the Buncefield oil terminal on 11th December 2005 has made a number of recommendations that impact on storage sites across the UK where gasoline in particular is handled and stored in significant quantity. Subsequent to the MIIB recommendations, 2 industry/HSE bodies BSTG and PSLG have produced guidance associated with petroleum storage.

The Bramhall terminal is not one of the sites required to implement the recommendations of the PSLG Guidelines.

Specification and design of a system that meets BS EN 61511 involves a series of defined phases as part of an overall lifecycle of the storage tank facility with hazard and risk assessment, through safety requirements specification, design, installation, commissioning and validation, operation and maintenance, modification to ultimately decommissioning. Included in this process is a requirement for Functional Safety Assessments (FSA) to be conducted at key stages of the lifecycle – See Section 4.0).

3.1 Assumptions and Constraints

1 The safety instrumented function will operate as a demand mode system with demands placed on the system from operations no greater than once a year.

2 The information made available to the FSA is a fair and valid representation of the operations of the ConocoPhillips, Bramhall terminal for overfill protection on the tanks.

3 All documents are to be made available including “Management of Functional Safety” the “LOPA study report”, the “Safety Requirements Specification” and “SIS Design Report”, and all design documentation. On initial review it appears that some lifecycle documentation may not be available for this FSA, in which case the FSA has determined what additional documentation should be retrospectively produced.

4 This document is to be read in conjunction with document SI181002_RPT – SIS Compliance Document.

5 PX now have full responsibility for the operations of the Bramhall terminal.

3.2 Team Membership

Date of Review – Thursday 15th December 2011 at ConocoPhillips, Bramhall Terminal

The FSA review team:-

ConocoPhillips:
The FSA review team:-

Matt Dearnley	ConocoPhillips Terminals Engineer
Peter Lee	PX, Terminal Manager
Mark Reading	PX, Terminal Engineer
Les Proud	B C & T Project Manager
Dave Ransome	P&I Design Ltd. Independent FSA Facilitator
Dave Regan	P&I Design Ltd. Certified Functional Safety Expert

The competency of the personnel above can be demonstrated from the individuals job description and training files.

MATT DEARNLEY, MEng in Chemical Engineering with 12 years' experience in refining and terminal operations.
PETER LEE, BSc in Chemistry, with over 13 years' experience in plant and terminal operations.
LES PROUD, CEng, Production Engineering with 20 years' experience in Terminal Engineering.
MARK READING, over 20 years' experience in refinery and terminal operations.

P&I Design Ltd.

D. Ransome	Independent Competent Person
David Regan	Certified Functional Safety Expert

The competency of the personnel above can be demonstrated from the P&I Design Quality System.

Dave Regan – SIS Designer
DAVID REGAN BEng is a Process Engineer with a degree in Chemical Engineering. He has specialised in Process Instrumentation for over 25 years and is a Certified Functional Safety Expert. He has been involved on many SIS projects including Risk Assessments and design.

Dave Ransome – Senior Consultant
DAVID RANSOME CEng FInstMC is 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 is currently working with CDOIF producing guidance on Prior Use equipment in SIS.

4 FUNCTIONAL SAFETY ASSESSMENT – DEFINITIONS AND STAGES

A Functional Safety Assessment is an investigation, based on evidence to judge the functional safety achieved by one or more protection layers (BS EN 61511, Definition 3.2.26). An FSA is a team activity where there is at least one senior competent person who is not involved in the project design team (BS EN 61511, Clause 5.2.6.1.2).

BS EN 61511-1 Clause 5.2.6.1.3 identifies five stages in the project lifecycle where an FSA is recommended:-

Stage 1: After the hazard and risk assessment has been carried out, 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: After the installation, pre-commissioning and final validation of the safety instrumented system has been completed and the operation and maintenance procedures have been developed.

Stage 4: After gaining experience in operating and maintenance.

Stage 5: After modification and prior to decommissioning of a safety instrumented system.

BS EN 61511-1 Clause 5.2.6.1.4 states that “as a minimum the assessment shall be carried out prior to the identified hazards being present (i.e. stage 3)”. This project is a modification of an existing facility and the hazards are already potentially present. This document details stage 4 Functional Safety Assessment. Document SI181002_RPT “ Safety Instrument System Compliance Document” is part of this FSA for the purposes of ensuring compliance to BS EN 61511.

4.1 Hazard and Risk Assessment (BS EN61511-1:2004 Section 8.1)

This FSA will consider if the method of Risk Assessment conducted for this project complies to the required objectives of the standard.

Extract from BS EN 61511-1:2004 – Section 8.1 Objectives

> **8.1 Objectives**
>
> The objectives of the requirements of this clause are:
>
> - to determine the hazards and hazardous events of the process and associated equipment;
> - to determine the sequence of events leading to the hazardous event;
> - to determine the process risks associated with the hazardous event;
> - to determine any requirements for risk reduction;
> - to determine the safety functions required to achieve the necessary risk reduction;
> - to determine if any of the safety functions are safety instrumented functions (see Clause 9).

As stated previously, no Stage 1 FSA has been conducted.

It was therefore decided to review the LOPA within this FSA and consider any changes or variations which have arisen since the LOPA had been conducted.

There is a LOPA spreadsheet within the design document but no report detailing the assumptions and conclusions.

Identification of risks and consequences

Risk tolerance criteria of 1×10^{-6} seems acceptable for a potential single fatality.

Nearby sites and populations

Potential escalation does not appear to have been adequately considered. It is not clear that ConocoPhillips have taken into account both on-site and off-site potential fatalities when considering societal risk and individual risk. For example, there are domestic dwellings at the boundaries of the terminal.

In the FSA this was discussed and it was considered that there was no potential for escalation for the road loading overfill case.

Initiating Events

The frequencies appear realistic.

A discussion took place on the overfill system in view of an incident at another road loading facility where the SIS did not activate on an overfill of the tanker resulting in gasoline spillage. An investigation on the road tankers used on this facility was carried out to see whether there are back-pressure systems which could shut down the vapour line before the SIS could activate. The FSA believe that the arrangement of the pipework is such that the SIS will activate prior to the relief valves on the tanker operating.

Further discussions were continued on the design and operation of the road loading facility and the installed SIS. Confirmation was given on the operation and system shutdown. See Design document section 5.1 Safety Requirement Specification and functional test procedures.

Independent Protection Layers

P.L. G - Rack Vapour line ESD shuts pump. Is this an operator action or automatic. Is the layer independent, effective and auditable?

This was confirmed that this is an automatic action from the initial Liquiphant (LE*01) to stop the pump via the PLC and removes the permissive to the loading arm. Independence is provided by these actions. Credit taken as 0.1.
In addition, this layer is also included in the new SIS logic.

P.L. H and the proposed new SIL 1 protection layer appear not to be independent as the same valve is utilised by both.

P.L. H, LE*11 is the SIL 1 protection layer and shuts down the new rack gantry valves.

Conditional modifiers

Probability of ignition of 0.01 needs to be justified if it is to meet with the Competent Authority guidelines.

Probability of fatality of 0.05 need to be justified if it is to meet with the Competent Authority guidelines.

The LOPA was conducted prior to the new PSLG guidelines and HSE comments in line with ConocoPhillips Humber refinery standards.

Individual and Societal Risk

An IR assessment should be performed. No societal risk has been performed. Societal risk is purely based on total numbers (both on-site and off-site) of persons exposed to risk and is a requirement of COMAH where relevant. As a minimum, the LOPA study should show that 10 or fewer persons (in total) are exposed to risk before omitting a societal risk assessment. The FSA considered that the scenario considered was unlikely to lead to a Societal Risk.

General

It was noted that certain elements noted in previous LOPA studies assessed by the Competent Authority were not included in this LOPA as follows:
Method for IE identification
Sensitivity analysis
Environmental assessment
Details of the operation.

The LOPA was conducted prior to the new PSLG guidelines and HSE comments in line with ConocoPhillips Humber refinery standards.

The objectives as defined in BS EN 61511 Section 8.1 were considered by the FSA team:

- The hazards and hazardous events of the process and associated equipment were determined in a LOPA review.
  - The LOPA was conducted by a team of ConocoPhillips personnel each with different roles and responsibilities, the LOPA was conducted in line with ConocoPhillips standards in line with competency and roles and responsibilities.
  - The LOPA report was carried out in 2009.

- The following sequence of events leading to the following hazardous events were considered from road loading operations
  - Vapour Cloud followed by a fire.

  the following Initiating Events were identified:

  - IE1 Driver returns to Terminal with a quantity of gasoline remaining in the tanker
  - IE2 Mechanical failure of loading control valve prevents closure at termination of loading.
  - IE3 Failure of gasoline flowmeter to actuate closure of valve.
  - IE4 Driver enters incorrect volume
  - IE5 Driver inadvertently crosses loading arms

- The process risks and consequences were determined as:
  - Overfill leading to fire – Safety Issue
- The LOPA considered the requirement for Instrumented Protection and Mitigation Layers with the following being identified:

  - PL1 High Level shutdown on Road Tanker
    - As part of the required protection layers, ConocoPhillips realise that this layer, although not SIL rated, requires to be independent, auditable and effective and to maintain this, they are managing this protection layer within the safe loading pass system operated by the six major oil companies.

  - PL2 Rack Vapour line ESD stops pumps
  -
  - PL3 SIL1 Rated vapour ESD closes independent shut-off valve.

- From the original LOPA, the residual risk following the inclusion of all PL & ML's was 9.99×10^{-7} against a risk tolerance criteria (RTC) of 1.00×10^{-6} the SIS PL3 having a SIL 1 rating with an estimated PFD of 4.67×10^{-2}.

  Actual Calculated PFD of PL3 SIF as detailed in:
  Document Number 11631/15111-100, Issue 2
  Dated 20th September 2010 for the safety Instrument System is:
  SIL 1 with pfd of 1.23×10^{-2}.

ConocoPhillips confirmed that the HSE have not yet reviewed this LOPA.

4.2 Suitability of the Proposed Protection Layer

The purpose of the SIL 1 SIS protection layer is to prevent an overfill and overflow of a Road Tanker leading to a release of product capable of being ignited and possibly causing a fire.

This is achieved by use of an independent, to the normal road tanker level measurement, from a Scully System and separate independent level switch in the vapour return line, further level switch in the vapour return line. A logic solver provides monitoring of this level and on reaching a predefined value will initiate the closure of valve(s) independent of the process control. These valves are under the control of ConocoPhillips.

The level measurement is performed in the vapour line so it is unlikely then any external devices can interfere with the correct operation of the instrument and also it should be able to detect actual level not inferred level.

The valves are set to slow close at around 8 seconds to prevent surge problems in the lines and to prevent the overfill from the tanker lids occurring before the flow is shut down. This timing has been advised by ConocoPhillips, Bramhall.

The valve has been closed against process pressure to confirm the speed of closure of the valves and to ensure that the test was realistic.

4.3 The recommendations arising from the hazard and risk assessment that apply to the safety instrumented system have been implemented or resolved.

In the Safety Instrument System document there is a section entitled Safety Requirement Specification (SRS). However, some items required within a SRS for a Safety Instrumented System to BS EN 61511 were not included in this document.

In order to describe the requirements for the Safety Instrumented System, BS EN 61511 details that there should be a Safety Requirement Specification (SRS) produced following the Hazard and Risk reduction phase and allocation of Safety Function to protection layers. The purpose of this document is to convey the requirements of the SIS. The SRS should include for the following:

- a description of all the safety instrumented functions necessary to achieve the required functional safety;

Document Number 11631/15111-100, Issue 2, dated 20th September 2010 details the SIF.

It was not apparent from the documentation reviewed how independent the Layers of Protection are.

In the FSA this was confirmed as being in the design basis document DB06/09 Bramall Terminal Gantry Shut-off valves.

There is no partial stroke testing, the valves are normally left open and are tested monthly in accordance with operating and test procedures. Procedure and data recording is documented in routine weekly checks book.

Operation of the SIS valves was clarified at the FSA meeting and is detailed in Section 4.1 of this document.

- requirements to identify and take account of common cause failures;

There is no reference to common cause failure. Common cause failure could be freezing of the vents in the solenoid due to moisture in the air system. Instrument Air system dew point is minus 40 deg and no problems have been observed. There could be common cause between the 2 protection layers due to them both being identical and due to the fact that there could be overfill without liquid level reaching the vapour pot. See above.

At the FSA meeting the above comments were addressed and it was confirmed that the SIS level sensor is effectively a 1oo1 configuration and the valves are effectively a maximum of 1oo1 configuration, based on actual operations and a failure of a single Accuload/DCV, and provides isolation from the terminal. Common cause failure has therefore not been considered.

- a definition of the safe state of the process for each identified safety instrumented function;

There is no reference to the process safe state.

In the FSA, it was confirmed that the system is fail safe.

- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system);

In the FSA, it was confirmed that there are no identified individual safe states which can create a separate hazard.

- the assumed sources of demand and demand rate on the safety instrumented function;

The safety instrumented function will operate as a demand mode system with demands placed on the system from operations no greater than once 10 years. The LOPA describes the assumed sources of demand.

- requirement for proof-test intervals;

Testing and maintenance requirements are referenced in the Document Number 11631/15111-100, Issue 2, dated 20th September 2010, but not in the Specification section.

- response time requirements for the SIS to bring the process to a safe state;

Determined during the FSA as 8 seconds based on surge calculation RP7948-01.

- the safety integrity level and mode of operation (demand/continuous) for each safety instrumented function;

Requirement from LOPA SIL1, System designed as SIL 2 and low demand confirmed for all SIFs, in the FSA. (1.23×10^{-3})

- a description of SIS process measurements and their trip points;

There are no process setpoints. The system will trip on a liquid level in the vent line.

Liquid Level/quantity in vapour line at activation point to be confirmed. June 2014 - Confirmed as 30 litres. ACTION COMPLETE

- a description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves;

The output action is to shut the valves, tight shut-off valves are not a requirement. Valves specified as fire-safe and antistatic. Described in design basis document Section 2.

- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives;

Document Number 11631/15111-100, Issue 2, dated 20th September 2010 provides functionality of the inputs and outputs of the logic solver. This document is part of the detailed design documentation.

- requirements for manual shutdown;

There is an ESD button which shuts down the SIS. A site fire alarm will also shut down the SIS.

- requirements relating to energize or de-energize to trip;

Document Number 11631/15111-100, Issue 2, dated 20th September 2010 provides this requirement. This document is part of the detailed design documentation.

- requirements for resetting the SIS after a shutdown;

Document Number 11631/15111-100, Issue 2, dated 20th September 2010 details there is a reset button on the panel.

- maximum allowable spurious trip rate;

At the FSA, the acceptable spurious trip rate for the SIS was confirmed as less than once every 10 years.

- failure modes and desired response of the SIS (for example, alarms, automatic shut-down);

The failure modes and desired response are detailed in the Document Number 11631/15111-100, Issue 2, dated 20th September 2010 and the design basis document.

- any specific requirements related to the procedures for starting up and restarting the SIS;

Alarms in the control room alert the operators that the system has operated. There is a reset procedure for restarting the SIS. Procedure BRM029.

- all interfaces between the SIS and any other system (including the BPCS and operators);

Document Number 11631/15111-100, Issue 2, dated 20th September 2010 details this. This document is part of the detailed design documentation.

- a description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode;

Documented in the Design Basis and in Document Number 11631/15111-100, Issue 2, dated 20th September 2010

- the application software safety requirements as listed in 12.2.2;

No user Software is necessary. Not Applicable

- requirements for overrides/inhibits/bypasses including how they will be cleared;

There is no override of the sensor or valve as per PSLG recommendations.

- the specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors;

Operation of the road loading facility will not be possible in the event of a failure of the SIS

- the mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;

The terminal have considered MTTR. The loss of a single gantry would not bring the terminal operations to a halt.

- identification of the dangerous combinations of output states of the SIS that need to be avoided;

The system is designed to fail safe and no dangerous combinations of output states have been identified.

- the extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;

The system is designed for and installed in the UK and been operational for 2 years and all environmental conditions have been tested.

- identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation;

The terminal operation for a single gantry will not be allowed whilst the SIS is not functioning. Operation Procedure for loss of Safety System BRM-POL-010 (This may be revised to a PX document) is to be issued. June 2014, ACTION COMPLETE, new procedure BRM-OP-014 issued.

- definition of the requirements for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire.

The valves are specified as firesafe.

Chemical and Downstream Oil Industry Forum (CDOIF)

CDOIF guidance assessing the suitability of road tanker loading system architectures. Automatic Overfill systems for Terminal Loading Racks.

Section 1.1
Assessing the Suitability of Road Tanker Loading System Architectures

The adequacy of the measures used to control risks during filling operations should be assessed. This can be achieved by asking a number of questions regarding the architecture of a loading system.

1. *Is the flow control valve, and any associated pilot valves, correctly specified for the function it is expected to perform?*

2. *In the event of a failure of the flow control valve, is there a secondary automated valve to stop fuel flow?)*

3. *Is a secondary automated valve triggered correctly in the event of a failure of the primary flow control system?*

4. *Is a secondary automated valve positioned so that it will prevent or mitigate against overfilling of a road tanker, taking into account realistic scenarios?*

5. *Are wetted valves tested at a suitable frequency, according to specific criterion?*

6. *Are wetted valves maintained according to appropriate instructions?*

7. *Are indications of failures recorded and assessed, and actions to address these taken?*

Any dependencies between risk control measures should be identified, and eliminated if possible. It is good practice to be able to detect the failure of a measure as soon as possible after it occurs, possibly by automated means, so that adequate risk control is maintained.

The FSA confirmed the following as per the CDOIF document

1. Yes
2. Yes
3. Yes
4. Yes
5. Yes - Time to close to be documented
6. Yes – Maintenance and failure reporting procedures to be confirmed
7. Yes

4.4 Project Design Change Procedures are in place and have been properly implemented.

This FSA was conducted at Stage 4 and not stage 2. Design changes appear to have been conducted directly between ConocoPhillips and BC&T as part of the Design Basis Memorandum.

Terminal management and operations are being handed over at the time of this FSA.
PX to confirm how they will provide management of change now the system is operational and they have taken over the operation and management of the terminal. ConocoPhillips will approve any changes of MOC and technical changes.

A modification and management of change procedure has been developed to ensure SIS systems are not modified or changed without due regard to process safety. Terminal Process Safety Check Sheet.

4.5 The recommendations arising from the previous functional safety assessment have been resolved.

No previous functional Safety Assessments have been carried out.

4.6 The Safety Instrument System is designed, constructed and installed in accordance with the safety requirement specification, any differences having been identified and resolved.

Design

The system appears to be designed in accordance with the Safety Requirement Specification and the Design Basis Memorandum. DRR to confirm and document. Action completed. October 2015, reviewed by DSR/DBF.

Installation and Testing of the Installed System

The wiring and installation has been verified by B C & T. The system has now been operational since 2009 and no problems have been uncounted.

No FSA stage 3 was performed and for this FSA stage 4, no inspection of the installation was carried out.

The system will be independently inspected and tested by P&I Design. Action completed. October 2012

The following documentation is to be reviewed independently by D. R. Ransome outside this FSA meeting: Action completed. June 2016, reviewed by DSR/DBF.

Drawings:

Drawing Number	Title	Revision
11631/G0001	Master P&I Diagram Sheet 1	N
11631/G0002	Master P&I Diagram Sheet 2	L
11631/G0003	Master P&I Diagram Sheet 3	M
11631/G0004	Master P&I Diagram Sheet 4	K
11631/G0005	Master P&I Diagram Sheet 5	A
11631/E0412 Sht. 1A of 12	ESD System Wiring Diagram Gantry 3	F
11631/E0412 Sht. 1B of 12	ESD System Wiring Diagram Gantry 4	F
11631/E0412 Sht. 1C of 12	ESD System Wiring Diagram Gantry 5	F
11631/E0412 Sht. 1D of 12	ESD System Wiring Diagram Gantry 6	F
11631/E0412 Sht. 1E of 12	ESD System Wiring Diagram Storage Tank ROSVs and Pumps	F
11631/E0412 Sht. 1F of 12	ESD System Wiring Diagram Storage Tanks 11, 12, 13 ROSVs and Pumps	F
11631/E0412 Sht. 1G of 12	ESD System Wiring Diagram Ancillary Systems	F
11631/E0412 Sht. 2 of 12	ESD System Wiring Diagram	F
11631/E0412 Sht. 3 of 12	ESD System Wiring Diagram	F
11631/E0412 Sht. 4 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Tanks 1, 4, 5, 11, 12, 13	F
11631/E0412 Sht. 5 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Tanks 2, 3, 6, 7, 8	F
11631/E0412 Sht. 6 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Tanks	F
11631/E0412 Sht. 7 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Rack 4 Gantry S/Down Valves	F
11631/E0412 Sht. 8 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Rack 5 GSDVs	F
11631/E0412 Sht. 9 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Rack 5 GSDVs	F
11631/E0412 Sht. 10 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel	F
11631/E0412 Sht. 9 of 12	ESD System Wiring Diagram New ESD Extension Panel	F
11631/E0412 Sht. 12 of 12	ESD System Wiring Diagram I.S./PLC Interface Panel Rack 6 GSDVs	F

Reports:

Number	Title	No of Sheets	Revision
11631/I5111-100	Safety Instrument System Report	36	2
CoP Workbook 07.09.09	LOPA Workbook	1	?
11631/I5111-101	Safety Instrument System Analysis	14	1
11631/I5111-102	SIS Loop Testing & Commissioning	6	1
11631/I5111-103	SIS Documentation & Hardware Verification	12	1
11631/I5111-104	SIS Modification Guidelines	7	0
Various	Functional Test Procedures		
	ESV Operation and Response	1	3

11631/15111-100 Safety Instrument System

It was observed that the document deals only with SIL verification and does not consider sensor or final element suitability, this should be addressed in a supporting document. Design Basis Memorandum.

Safety Validation Software Design

No user Software is necessary. Not Applicable

Safety Check – Validation Customer Document

Function testing documentation is included, no completed testing documentation appended.

BC & T to send the completed testing documentation for inclusion in this FSA. Action completed 16/12/11, Testing implemented as a procedure in Q4

4.6.1 SIL Verification

Review of SIL Verification document including check of PFD and hardware fault tolerance calculations.

The PFD for the Safety relay (PNOZ S2) has been revised to 2.13 $x10^{-5}$ as per the attached sheet. (See Appendix 1)

The data for the valve is not included in the report.

The data for the solenoid valve is not included in the report.

4.6.1.1 SIL and PFD Verification Summary

The following tables show the reviewed calculations for the SIS.

SIL 1 is confirmed, but the PFD value has been revised from 1.23 x 10^{-3} to 1.61 x 10^{-3}.

Based on the assumed SFF as detailed below provides a calculated Spurious Trip value of 68.9 years.

SIL & PFD Verification Summary

P & I Design Ltd ***Probability of Failure on Demand (PFD) Summary***

www.pidesign.co.uk Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	Simon - Bramhall	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	SI181001_CAL	Issue:	A
SIS Number:		Date:	03.08.11

SAFETY INTEGRITY LEVEL REQUIRED

SIL 1

SAFETY INTEGRITY LEVEL ACHIEVED

Valid

CALCULATION SUMMARY

$PFD_{(SYS)}$	=	$PFD_{(S)}$		$PFD_{(L)}$		$PFD_{(FE)}$	
1.61E-03	=	1.50E-03	Valid	2.13E-05	Valid	2.00E-07	Valid
		0.00E+00	n/a	0.00E+00	n/a	4.20E-05	Valid
		0.00E+00	n/a	0.00E+00	n/a	4.58E-05	Valid
Valid		1.50E-03	Valid	2.13E-05	Valid	8.80E-05	Valid

SPURIOUS TRIP SUMMARY

$S.Trip_{(SYS)}$	=	$S.Trip_{(S)}$		$S.Trip_{(L)}$		$S.Trip_{(FE)}$	
68.9	=	74	Years	2471	Years	50505.1	Years
Years		n/a	Years	n/a	Years	5585.0	Years
		n/a	Years	n/a	Years	2426.0	Years

P & I Design Ltd — **PFD - Sensor Subsystem Calculation Sheet 1**

www.pidesign.co.uk — Sheet Title:- Sensor FTL51 + FEL57 + FTL325P — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	Simon - Bramhall	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	SI181001_CAL	Issue:	A
SIS Number:		Date:	03.08.11

P & I DESIGN

Key:: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	E&H Liquiphant
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	1.50E-03

FAILURE CALCULATIONS	
Total Failures (λ)	n/a
Safe Fail Fraction	n/a
Total Dangerous Failures (λ_D)	n/a
Calculated Diagnostic Coverage (%)	n/a

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})	n/a
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	n/a

LOOP CRITERIA ACHIEVED	
PFD Total	**1.50E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**74**

FAULT TOLERANCE CHECK
Conforms to Note 1: YES
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:
1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4

P & I Design Ltd — **Logic Solver Calculation Sheet 1**

www.pidesign.co.uk — Sheet Title:- Safety Relay — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	Simon - Bramhall	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	SI181001_CAL	Issue:	A
SIS Number:		Date:	03.08.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PILZ PNOZ S2
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.95
Diagnostic Coverage	
PFD Value (From Certificate)	2.13E-05

FAILURE CALCULATIONS	
Total Failures (λ)	n/a
Safe Fail Fraction	n/a
Total Dangerous Failures (λ_D)	n/a
Calculated Diagnostic Coverage	n/a

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})	n/a
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	n/a

LOOP CRITERIA ACHIEVED	
PFD Total	**2.13E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**2471**

FAULT TOLERANCE CHECK	Programmable
Programmable	Non Programmable
SFF>90%	Conforms to Note 1 — YES
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:	
1. the hardware is selected on the basis of proven technology (prior use)	
2. adjustment, of process related parameters only, allowed to the user.	
3. adjustment, of process related parameters, is protected by password or removeable programming link.	
4. system function has SIL requirement of <4	

P & I Design Ltd — ***Final Element Calculation Sheet 1***

www.pidesign.co.uk — Sheet Title:- Seitz Solenoid Valve — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	Simon - Bramhall	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	SI181001_CAL	Issue:	A
SIS Number:		Date:	03.08.11

Key:: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	Seitz SOV
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.99
Diagnostic Coverage	
PFD Value (From Certificate)	2.00E-07

FAILURE CALCULATIONS	
Total Failures (λ)	n/a
Safe Fail Fraction	n/a
Total Dangerous Failures (λ_D)	n/a
Calculated Diagnostic Coverage	n/a

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})	n/a
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	n/a

LOOP CRITERIA ACHIEVED	
PFD Total	**2.00E-07**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**50505**

FAULT TOLERANCE CHECK
Conforms to Note 1: YES
Note 1: In order to reduce the fault tolerance by 1, for Final Elements, final elements and non-programmable logic solvers, the following must be satisfied:
1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4

P & I Design Ltd — ***Final Element Calculation Sheet 2***

www.pidesign.co.uk — Sheet Title:- Butterfly Valve — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	Simon - Bramhall	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	SI181001_CAL	Issue:	A
SIS Number:		Date:	03.08.11

Key:: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	Butterfly valve
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.81
Diagnostic Coverage	
PFD Value (From Certificate)	4.20E-05

FAILURE CALCULATIONS	
Total Failures (λ)	n/a
Safe Fail Fraction	n/a
Total Dangerous Failures (λ_D)	n/a
Calculated Diagnostic Coverage	n/a

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})	n/a
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	n/a

LOOP CRITERIA ACHIEVED	
PFD Total	**4.20E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**5585**

FAULT TOLERANCE CHECK
Conforms to Note 1: YES
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:
1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4

P & I Design Ltd — ***Final Element Calculation Sheet 3***

www.pidesign.co.uk — Sheet Title:- Actreg Pneumatic Actuator — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	Simon - Bramhall	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	SI181001_CAL	Issue:	A
SIS Number:		Date:	03.08.11

Key:: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	Actuator
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	4.58E-05

FAILURE CALCULATIONS	
Total Failures (λ)	n/a
Safe Fail Fraction	n/a
Total Dangerous Failures (λ_D)	n/a
Calculated Diagnostic Coverage	n/a

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})	n/a
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	n/a

LOOP CRITERIA ACHIEVED	
PFD Total	**4.58E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**2426**

FAULT TOLERANCE CHECK
Conforms to Note 1: YES
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:
1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4

4.7 The safety, operating, maintenance and emergency procedures pertaining to the safety instrument system are in place.

This was reviewed and discussed at the FSA meeting to be held on 15th December 2011 at ConocoPhillips Bramhall.
It was not apparent whether the full daily, weekly, six monthly and annual testing is being carried out and recorded as per the SIS testing documentation.

Driver inductions include locations of the ESD.

Operator response to high level activation to be confirmed.

px have the responsibility and ownership of the safety Instrument System. During this FSA the testing and maintenance of the SIS was discussed. A Safety Committee may be set up to ensure that the safety instrument system(s) are controlled and maintained.

The following will be considered:

- SIS Performance including any activations and false alarms.
- SIS Testing, planning, results and analysis.
- Training requirements and roles and responsibilities of employees and contractors.
- Review of organisation and resources.
- Outcome of Functional Safety Assessments and Outstanding Action status.
- Review of any management of change or modifications to the systems.
- Review of any HSE or other agency visits.
- Review of any changes in the standard or competent authority guidelines.

The system will be proof tested independently and will be maintained by px. As detailed previously, px are to consider essential spares for the SIS.

Emergency procedures are covered under site operation procedures for a COMAH site.

4.8 The safety instrument system validation planning is appropriate and the validation activities have been completed.

This was reviewed and discussed at the FSA meeting to be held on 15th December 2011 at ConocoPhillips, Bramhall. (ACTION 8).

The system validation documentation has been issued. The FSA identified that testing has been carried out and revalidated in 2010/2011 and the SIS will be independently inspected and tested by P&I Design Ltd in 2012. See above. Tighter control over validation and inspection will be maintained.

4.9 The employee training has been completed and appropriate information about the safety instrumented system has been provided to the maintenance and operating personnel

SIS functional operator training is complete but is not formally documented at present.
Further specific appreciation training on Safety Instrument Systems will be completed in 2012 and documented. px have their own competency matrix and have been undergoing training on Functional Safety to improve and demonstrate competency.

4.10 Plans or strategies for implementing further safety assessments are in place.

Further safety assessments will be carried out as required.
Reviews of the actions arising from this FSA will be carried out as part of the Safety Committee meetings.

4.11 Compliance to BS EN 61511

As part of P&I Design Ltd. review procedures and forming part of this FSA is a checklist to confirm that all the relevant clauses from the standard have been complied with. See Document SI181002_RPT – SIS Compliance Document. Compliance document to be completed. Action Closed, Committee set up to monitor Functional Safety.

5 CONCLUSIONS

The Safety Lifecycle documentation reviewed at Revision A of this FSA was provided by BC & T. They have produced design, validation and verification documentation.

Following this pre-FSA assessment it appears that there could be lifecycle documentation missing.

Additional Life-cycle documentation to be produced:

- Management of Functional Safety Document

This will be assessed at the Safety Committee meetings.

6 ACTIONS

Action No.	Action	By	Expected Completion	Completion Date
1	Liquid Level/quantity in vapour line at activation point to be confirmed. June 2014 - Confirmed as 30 litres. ACTION COMPLETE	BC&T	March 2012	June 2014
2	Operating Procedure for loss of Safety System BRM-POL-010 (This may be revised to a px document) is to be issued. June 2014, ACTION COMPLETE, new procedure BRM-OP-014 issued. Copy to be issued to P&I Design Ltd. for reference.	px	March 2012	June 2014
3	The system appears to be designed in accordance with the Safety Requirement Specification and the Design Basis Memorandum. DBF to confirm and document. June 2014, Documentation issued to P&I Design Ltd.	P&I Design Ltd.	September 2015	Completed. October 2015
4	The installed system will be independently inspected and tested by P&I Design. Due 23rd October 2012	P&I Design Ltd.	March 2012	Completed. October 2012
5	Design documentation is to be reviewed independently by D. R. Ransome. June 2014, Documentation issued to P&I Design Ltd.	P&I Design Ltd.	September 2015	Complete June 2016
6	BC&T to send the completed testing documentation for inclusion in this FSA. Testing implemented as a procedure in Q4	BC&T	March 2012	16/12/11 (Appendix3)
7	Compliance document to be completed. June 2014, Documentation issued to P&I Design Ltd.	P&I Design Ltd.	September 2015	Closed

8	Further specific appreciation training on Safety Instrument Systems will be completed and documented. px have their own competency matrix and have been undergoing training on Functional Safety to improve and demonstrate competency.	P&I Design Ltd. / px	End 2012	Closed
9	Gantry LOPA to be reviewed following re-write of COMAH report. LOPA now supplied to P&I Design Ltd. Review ongoing to be completed by end September 2014.	P&I Design Ltd.	September 2015	June 2016 Complete. LOPA is up to date and conclusions are acceptable.
10	Road Loading SIS Documentation to be reviewed following LOPA review. June 2014, Documentation issued to P&I Design Ltd.	P&I Design Ltd.	September 2015	Complete June 2016