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

PIPELINE OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM BRM-SIS1

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

CONOCO PHILLIPS

BRAMHALL TERMINAL

OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

FUNCTIONAL SAFETY ASSESSMENT

STAGE 4

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	22.02.12	D R Ransome	DSR	Client	Original Issue	
B	15.08.12	D R Ransome	DSR	Client	Action List Updated	Document No. **SI297020_RPT**
C	30.03.17	D S Regan	DBF	Client	FSA Closed	
						Page 1 of 20

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

Appendix

1. E-mail trail justifying SIL 1.

1 REVISION HISTORY

Rev	Description
A	Original Issue
B	Actions Updated
C	FSA Closed, all actions complete
D	

2 SCOPE

Conoco Phillips have installed an Independent High Level Alarm system to provide a SIL 1 rated automatic shutdown system to prevent storage tank overfills.
Although the risk assessment called for risk reduction to SIL 1, the Safety Instrumented System has actually been designed to SIL 2.

The overfill protection systems are 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 Conoco Phillips 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 Conoco Phillips, Bramhall terminal for overfill protection on the tanks.

3 All documents are to be made available including 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 will determine what additional documentation should be retrospectively produced.

4 This document is to be read in conjunction with document SI297021_RPT – SIS Compliance Document.

3.2 Team Membership

Date of Review – Wednesday 22nd February 2011 at Conoco Phillips, Bramhall Terminal

The FSA review team:-

px:
The FSA review team:-
Peter Lee – Terminal Manager
Mark Reading – Terminal Engineer
Keith Mason – Terminal Operations Superintendent

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

PETER LEE is the Terminal Manager, he has BSc in Chemistry, with over 13 years' experience in plant and terminal operations.

MARK READING is the Terminal Engineer. He has over 20 years' experience in refinery and terminal operations.

KEITH MASON is the Terminal Operations Superintendent. He has over 32 years' experience terminal operations at this terminal.

P&I Design Ltd.

D.R. Ransome	Facilitator
D. Regan.	Project Designer

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 SI297002_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).

- The hazards and hazardous events of the process and associated equipment were determined in a LOPA review (Reference LOP-D426-06 Overfill of Storage Tanks at Bramhall dated 9th February 2007.

- The sequence of events leading to the hazardous event were also determined in the LOPA review.

- The process risks were determined.

- The LOPA considered that additional risk reduction was required by the inclusion of an additional Safety Instrumented Protection Layer.

- From the LOPA, risk reduction is to be achieved by the inclusion of a SIL 1 rated Layer of Protection comprising of a common gasoline supply line valve activated via a logic solver from level switches on all tanks.

The LOPA referenced above was carried out in 2007. During the FSA it was noted that an updated LOPA has been produced. This assessment was not available and as such could not be reviewed. The new assessment will be made available.

See e-mail trail justifying SIL 1 (Appendix 1).

(Action 1 confirm SIL requirement) - Closed

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 storage tank leading to a release of product capable of being ignited and possibly causing an explosion and/or fire.

This is achieved by use of an independent, to the normal tank level measurement, separate independent level switch in the storage tank. A logic solver provides monitoring of this level and on reaching a predefined value will initiate the closure of valve independent of the process control. This valve is under the control of ConocoPhillips.

The level measurement is performed in tank 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 valve is set to slow close at around 90 seconds to prevent surge problems in the lines and to prevent the overfill from the tank occurring before the flow is shut down. This timing has been advised by ConocoPhillips, Bramhall.

The valve has not been closed against process pressure to confirm the speed of closure of the valves against the full pipeline pressure and flow.

The valve has a manual method of override which is contrary to the PSLG guidance. However, the override is locked and under management control. The override has never been activated. (Action 2 – SIS design to include reference to this override and confirm action of override and shutdown) – Closed.

There has been a problem on tank 1 rotork valve where it was not confirmed as fully open when required. This caused a pipeline shutdown. This has been investigated by Rotork. This is not part of the Safety Instrumented System.

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

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 specific SRS has been produced for this project. SI297013_RPT

This FSA has reviewed the available documentation against what the standard details should be within a SRS.

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

Safety Requirement Specification Document SI297013_RPT , Section 4, details all the SIFs.

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

Common cause failures are not specifically considered in the SRS. However, for a 1oo1 configuration, common cause failures are not normally an issue.

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

Document SI297013_RPT, Section 4, details the safe state of the process for each SIF. The system is designed such that all components are energise to operate and the safe states is de-energised with flow to all the tanks isolated.

- 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);

There are not considered to be any individually safe process states which, when occurring concurrently create a separate hazard.

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

The sources of demand were detailed in the LOPA referenced in section 4.1 and the SIF shall operate as a low demand mode system with demands placed on the system from operations no more frequently than once every two years. Ref: Document SI297013_RPT, section 2.

- requirement for proof-test intervals;

Document SI297013_RPT, Section 4, details the annual proof test interval.

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

Document SI297013_RPT, Section 4, details the response times.

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

The SIF shall operate as a low demand mode system.
Ref: Document SI297013_RPT, section 2.

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

Document SI297013_RPT, Section 4, details the trip points for the SIFs.

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

Document SI297013_RPT, Section 4, details the SIS output actions and SI297013_RPT, Section 4 details the criteria for successful operation.

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

Document SI297013_RPT, Section 1.4.1, details the relationships between process inputs and outputs.
.

- requirements for manual shutdown;

Document SI297013_RPT, Section 4, details the requirements for manual shutdown.

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

Document SI297013_RPT, Section 4, details the requirement to de-energise to trip.

- requirements for resetting the SIS after a shutdown;

Document SI297013_RPT, Section 1.3 details the requirements for resetting after a shutdown.

- maximum allowable spurious trip rate;

The maximum allowable spurious trip rate is not specifically defined in the SRS and the design calculation has no spurious trip calculation. SIL calculation to be redone to include spurious trips (Action 3 - SIL Calculation to be redone) – Closed. Sensor referenced as Magnetrol, this is incorrect.

This was discussed in the FSA and it was considered that 1 in 20 years would be acceptable

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

Document SI297013_RPT, Section 2 details the failure safe mode of the SIS.

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

The SIS is in operation at all times unless the logic panel is de-energised. In which case the pipeline isolation valve would be closed. The operation of the terminal is essentially a batch process with parcels of fuel being imported to the terminal. The Safety Instrumented system requires no procedures for start up.

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

Document SI297013_RPT, Section 3.3 details the interface between the SIS and BPCS.

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

The plant operation is a single mode of operation only. The operation of the terminal is essentially a batch process with parcels of fuel being imported to the terminal.

- the application software safety requirements as listed in 12.2.2;

There are no requirements for application software the system uses solid state relays for the logic solver function.

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

The SRS states is no requirement for overriding or bypassing the SIS. Document SI297013_RPT, Section 1.3. The valve, however, has been fitted with a manual hydraulic override, this is locked to prevent unauthorised operation. The operation of this manual override is controlled by management procedures with the key being available from the terminal manager. It has been confirmed during the FSA that, if the valve has been opened manually, the valve will not automatically close on activation of the Safety Instrumented System.

- 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;

There are no actions necessary to achieve or maintain a safe state in the event of a fault being detected in the SIS. The system is designed to fail safe on any fault being detected in the SIS. No reset would be available. The closure time of the valve has been physically set to prevent damage to the upstream pipeline.

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

Document SI297013_RPT, section 2 details the MTTR.

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

No dangerous combinations of output states of the SIS 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;

Document SI297013_RPT, section 2 states: This system will be installed in mainland UK where it will not be subjected to extremes of temperature or humidity. The individual elements of the system shall be designed for the process and operating conditions, the environment and the site electrical area classification. Specifically, all wetted parts should be suitable for Petroleum Spirits and Distillates (Gasoline, Diesel, Kerosene etc.).

> • 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 operates in a single mode. The operation of the terminal is essentially a batch process with parcels of fuel being imported to the terminal. The SIS is in operation at all times unless the logic panel is de-energised. In which case the pipeline isolation valve would be closed.

> • 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.

Document SI297013_RPT, section 2, states that isolation valves must conform fire safe requirements.

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

Design changes appear to have been conducted See Manual Document SI297002_MNL.

This FSA was conducted at Stage 4 and not stage 2. Design changes have been conducted directly between ConocoPhillips and P&I Design Ltd. 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 once 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.

Drawings:

SI297001	C	Tank Overfill Protection Safety Instrument System Cable Overview
SI297003	B	Tank Overfill Protection SIS Tank Level JB No.1 Connection Details
SI297004	B	Tank Overfill Protection SIS Tank Level JB No.2 Connection Details
SI297005	D	Tank Overfill Protection SIS Local Valve Control Panel Connection
SI297006	D	Tank Overfill Protection SIS Local Valve Control Panel Layout
SI297007	C	Control Room Panel/Switchroom High Level Panel ESD Connections
SI297008	E	Manifold Valve V14 Wiring Modifications
SI297009	A	ESD Valve V1 Status Telemetry Wiring Details
SI297010	G	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 1
SI297011	D	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 2
SI297012	D	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 3
SI297013	E	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 4
SI297014	E	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 5
SI297015	E	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 6
SI297016	E	Tank Overfill Protection SIS Monitoring Panel Logic Drawing 7
SI297018	D	Tank Overfill Protection SIS Tank Monitoring Panel External Layout
SI297019	C	Tank Overfill Protection SIS Tank Monitoring Panel Internal Layout
SI297022	B	Alarm Annunciator Window Engraving Details
SI297023	E	Alarm Annunciator Connection Details
03/67411/11631/G0003	I	Site Cable Routing Drawing
SI297001.SCH	B	Cable Schedule

Reports:

SI297001_RPT	H	04.11.08	Design Basis Memorandum
SI297002_RPT	B	12.07.10	Tank Overfill Protection SIS
SI297013_RPT	A	12.07.10	Tank Overfill Protection SIS Requirement Spec
SI297004_RPT	A	07.07.08	SIS Factory Acceptance Test Procedure
SI297005_RPT	B	09.11.10	SIS Testing Procedure
SI297006_RPT	C	09.11.10	SIS Shutdown Conditions Testing Procedure
SI297007_RPT	D	19.11.10	SIS Documentation & Hardware Verification Testing
SI297008_RPT	C	09.11.10	SIS Equipment Failure Testing Procedure
SI297009_RPT	C	10.11.10	SIS Process Conditions Functional Testing Procedure
SI297010_RPT	C	11.11.10	SIS Analysis & Approval
SI297011_RPT	B	16.11.08	SIS Loop Testing & Commissioning Method
SI297014_RPT	A	15.11.10	SIS Modification Sheet
SI389001_RPT	A	17.11.09	Annual Testing Method Statement

Design

The system is generally in accordance with the Safety Requirement Specification and the Design Basis Memorandum. There are a few discrepancies as previously noted.

There is a VRU system which is connected to tanks 1, 6, 7 & 8. The vents for these tanks are connected to the VRU at all times. The VRU return can be connected to any of the 4 tanks. There is a risk that the VRU return could overfill a tank which is already at high level. The VRU return valves are manual valves. The VRU return rate needs to be confirmed and the ullage above the SIS high high high level is to be confirmed. Then the time available before overfill can be calculated. (Action 4) – Closed.

There is no protection from the SIS on tank to tank transfers or VRU return. A modification of the SIS is to be considered. (Action 5) – Closed.

The duties of the tanks are not as per detailed in the SRS. Changes in SRS to confirm and document. (Action 6) - Closed

Current Tank Duties are as follows:

Tank 1 Gasoline (normally Derv)
Tank 2 Derv (Gas Oil)
Tank 3 Kero
Tank 4, 5 Derv
Tank 6 Gasoline
Tank 7 Slops
Tank 8 Currently out of service but normally Gasoline

Installation and Testing of the Installed System

The wiring and installation was carried out, on behalf of Conoco Phillips, by an approved contractor and this was verified by P&I Design Ltd during the SAT. The system has now been operational since 2008 and no problems or demands have been encountered.

There has been a problem on ESD V1 rotork valve where it was not confirmed as fully open at the proximity sensors when the valve was fully open and fully closed This has been investigated by Rotork. A report has been promised by Rotork. (Action 7 – Follow up to obtain report from Rotork) – Closed.

The Safety Instrumented System has been modified, since the initial SAT, with the removal of tanks 12, 12 & 13. A modification assessment was carried out. However the modification assessment has not been signed off by the terminal, neither has the Analysis and Approval documentation. The Analysis and Approval document has not been updated for the 2011 testing. (Action 8 – Ensure documentation completed and ensure Bramhall terminal management sign off documentation) – Closed.
The system has been inspected and tested annually by P&I Design Ltd..

For this FSA stage 4, an inspection of the installation was carried out.

Safety Check – Validation Customer Document

Function testing documentation is included, completed testing documentation has been included in the manual. See above for comments on Analysis and Approval.

There is a site procedure for taking a tank out of service which includes an ‘as found’ test, as well as an ‘as left’ test after the tank comes back into service. These tests are documented. (See TANK ISOLATIONS REQUEST SHEET).

There should be a site procedure for any actions on equipment involved in the Safety Instrumented System which shall include an ‘as found’ test, as well as an ‘as left’ test after the action is complete. These tests must be documented. Terminal to ensure that any demand, spurious trips or actions that involve the SIS as well as ‘as found’ and ‘as left’ tests are documented and auditable. These can then be included in the Analysis and Approval Documentation.
(Action 9 – Ensure Bramhall terminal have record of SIS actions, tests etc.) – Closed.
(Action 10 – P&I Design Ltd. To produce basis of documentation to px as part of the Safety Committee.) – Closed.
Data collection for both SIF and ISF failure, activations, replacements etc will be carried out.

SIL Verification

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

Document Number SI297002_RPT was reviewed and calculations verified.

The original calculated SIL 2, with a PFD of 2.73 x 10^{-4}, has been reviewed and the following noted:

The calculation for the PFD for the valve is not based on the actual valve body manufacturer as at that time Perar valves had not produced a Safety Manual. (Action 11 – PFD Documentation on valve body to be obtained) - Closed.

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 22nd February 2011 at ConocoPhillips Bramhall.

Operator response to high level activation confirmed on BRM023 Appendix A.

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 22nd February 2011 at ConocoPhillips, Bramhall.

The system validation documentation has been issued. The FSA identified that testing has been carried out and revalidated in 2009, 2010 and 2011 and the SIS independently inspected and tested by P&I Design Ltd in 2011. Tighter control over validation and inspection will be maintained. (Action 12 - Validation Dates to be brought forward to November.) – Closed.

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 March 2012 and documented.

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

Any 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 SI297021_RPT – SIS Compliance Document.

5 CONCLUSIONS

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

Following this FSA assessment there is lifecycle documentation missing.

Additional Life-cycle documentation to be produced:

- Management of Functional Safety Document. (Action 14 - Safety Committee to agree Management of Functional Safety.) – Closed.

Life-cycle documentation to be updated:

- LOPA
- Safety Requirement Specification
- Safety Instrumented System Design and SIL Verification
- Compliance Document

(Action 13 – Update SIS documentation as required.) – Closed.

This will be assessed at the Safety Committee meetings.

6 ACTIONS

Action No.	Action	By	Expected Completion	Completion Date
1	Confirm SIL requirement from LOPA. **ACTION COMPLETE, SIL 1 SIS required and installed.**	px	End June 2012	Action Complete June 2014
2	SIS design to include reference to the manual override and confirm action of override and shutdown	P & I Design Ltd.	End June 2012	Action Complete SRS Updated 29/05/12
3	SIL Calculation to be redone, sensor referenced as Magnetrol, this is incorrect.	P & I Design Ltd.	End June 2012	Action Complete PFD Calc Updated 29/05/12
4	The VRU return rate needs to be confirmed and the ullage above the SIS high high high level is to be confirmed. Then the time available before overfill can be calculated. **June 2014 – ACTION COMPLETE, ~2 hrs 30 minutes to overfill at VRU rate and VRU pumps shut down on high high alarms**.	px / P & I Design Ltd.	End June 2012	Action Complete June 2014
5	There is no protection from the SIS on tank to tank transfers or VRU return. A modification of the SIS is to be considered. **June 2014 – ACTION COMPLETE (email from Matt Dearnley, dated 4/8/12, stating that there is protection provided through the ROSOVs, and pump shutdowns, that are linked to the independent alarms.)**	px / P & I Design Ltd.	End June 2012	Action Complete June 2014
6	The duties of the tanks are not as per detailed in the SRS. Changes in SRS to be documented.	P & I Design Ltd.	End June 2012	Action Complete SRS Updated 14/06/12

7	Follow up to obtain report from Rotork on problem with SIS valve ESD-V1. *(There has been a problem on ESD V1 rotork valve where it was not confirmed as fully open at the proximity sensors when the valve was fully open and fully closed This has been investigated by Rotork. A report has been promised by Rotork.)*	px	End June 2012	Action Complete Report issued, no fault found.
8	Ensure documentation completed and ensure Bramhall terminal management sign off documentation. Reviewed 2014, to be issued to D. Williams for sign off	px / P & I Design Ltd.	End June 2012	Action Closed, documentation issued on cloud based system
9	Ensure Bramhall terminal have record of SIS actions, tests etc.	px / P & I Design Ltd.	End June 2012	Action Complete Issued June 2012
10	To produce basis of documentation to px as part of the Safety Committee.	P & I Design Ltd.	End June 2012	Action Complete 23/04/12
11	PFD Documentation on valve body to be obtained if possible. Now included in PFD Calculation	P & I Design Ltd.	End June 2012	Action Complete September 2014
12	Validation Dates to be brought forward to November.	px / P & I Design Ltd.	End June 2012	Action Complete October 2012
13	Update SIS documentation as required.	P & I Design Ltd.	End June 2012	Action Complete SRS &SIS Updated 14/06/12
14	Safety Committee to agree Management of Functional Safety.	px / P & I Design Ltd.	End June 2012	Action Complete 23/04/12

Appendix 1

Appendix 1.

From: De Halle, D J [mailto:DAVE.J.De-Halle@conocophillips.com]
Sent: 13 May 2007 11:02
To: Les Proud, Tyne
Cc: Chris Swinden, Bramhall; Thoo, Chee Hing; De Halle, D J
Subject: FW: Bramhall LOPA

Just tidying up,

Re Bramhall Level Gauging, I think we have agreed the scope as follows.

1) Link 11/12/13 together

2)Achieve SIL 1 for Slops tanks and all Gasoline tanks

3)Include distillate tanks in design of SIL1 if practicable

4)Provide for an independent shut down valve to operate at a level above the pipeline shutdown system setting.

Other

Include for emergency venting of 11/12/13

With access to cater for maintenance of level instruments and vents etc.

Regards Dave

From: Tinkler, Richard
Sent: 12 April 2007 09:26
To: De Halle, D J; Smith, John A
Cc: les.proud@simstor.co.uk; Turk, Andrew; drr@pidesign.co.uk; Ellis, Jon R.; Ali, S. Mohammad (Humber)
Subject: RE: Bramhall LOPA

Some initial thoughts .....

The Bramhall tanks are outside of the Buncefield scope due to tank height - I would have thought that the most plausible outcome is a pool fire, not an explosion, this may alter the consequence (and therefore RTC) that is selected (although I'm not familiar with the site).

IEF3 seems high at 1 in 2 years - does this feel right compared to recent experience

IPL1 of 0.02 for ATG PFD is inappropriate - it is a BPCS, which is generally accepted to have a PFD no lower than 0.1, claiming 0.02 makes it a SIL 1 SIS and it would therefore need to comply with the management system requirements of 61511.

A new SIL 2 SIS doesn't feel right to me, as the Bramhall tanks are probably lower current risk than, for example, the IPC gasoline tanks and we're not looking at installing new instrumentaion there (other than hydrocarbon detectors). Unless the IEFs are much higher at Bramhall ??? Probably worth reviewing the Plymouth, IPC and Humber T830 LOPAs, along with the latest WG5 guidance (attached) to calibrate the basis - I spoke with Jon about this recently.

Remember that the RTC does not necessarily have to be met to demonstrate ALARP.

Regards Richard

From: De Halle, D J
Sent: Tuesday, April 10, 2007 2:36 PM
To: Smith, John A
Cc: les.proud@simstor.co.uk; Tinkler, Richard
Subject: FW: Bramhall LOPA

John Re the Bramhall LOPA the site have been reviewing SIL 2 shutdown to try and achieve the risk tolerance. Bramhall as you may recall we (Mark Foster, Myself and Site Representative) set the tolerable criteria at 1 in 100,000,000 due to the close proximity of residential housing. Intuitively it feels correct to be more conservative than at the more remote sites.

It does of course make the solutions more difficult/costly

The attached is based on our own LOPA study but with improved shutdown system factored in. If we accept the risk tolerance we should finalise with a cost for the modifications to achieve SIL 2 to complete ALARP/cost benefit demonstration. Your previous analysis indicated that spending $150,000 (£80,000) would be justified.

If you or Richard believe the 1/100,000,000 should be changed please advise.

Regards Dave

From: Les Proud, Tyne [mailto:Les.Proud@simonstorage.com]
Sent: 23 March 2007 14:02
To: De Halle, D J
Subject: FW: Bramhall LOPA

Dave,

Dave Ransome has been to site and carried out a new LOPA based on installing a separate SIL 2 rated level alarm on the tanks and you can see that it still does not satisfy the risk tolerance criteria. He also indicated that even if we installed a SIL3 unit we still would just be outside the criteria. Would it be worth speaking to Richard for his comments or do you want to hold a meeting with Dave to discuss. I have asked him to hold off until we determine what we are to do.

Regards,

Les Proud

From: Dave Ransome [mailto:drr@pidesign.co.uk]
Sent: 23 March 2007 13:02
To: Les Proud, Tyne
Subject: Bramhall LOPA

Les

Please find enclosed a new LOPA for Bramhall with a mid-range SIL2 SIS fitted.

As you will see it does not satisfy the Risk Tolerance Criteria .

A lot of discussion took place at WG5 regarding Conditional Modifiers and RTC, debating if the figure of fatality was relatively high due to VCE then the figure of occupancy would be extremely low as everybody would probably smell the large release and evacuated the area.

- 1. Dave may want to discuss these figures with Richard Tinkler Richard.Tinkler@conocophillips.com Richard is also on WG5 and also the LOPA sub group with me.

Dave Ransome BA FInstMC

Managing Director

www.pidesign.co.uk

Phillips 66

Bramhall Terminal

BRM-SIS1 Annunciator Relay Replacement

Functional Safety Assessment

Stage 5

Document Number: 16089RPT205

Revision: B

Date: 21/11/2016

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

Contents

1. REVISION CONTROL

Revision	A
Date of Revision	21/10/2016
Description	Original Issue for Review
Created By	D.B.Faulkner
Checked By	M.Morgan
Approved For Issue By	M.Morgan

Revision	B
Date of Revision	21/11/2016
Description	Update following Modification
Created By	D.B.Faulkner
Checked By	D.S.Regan
Approved For issue By	D.S.Regan

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

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

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

2 INTRODUCTION

2.1 Scope

A Functional Safety Assessment (FSA) 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 (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.

IEC 61511-1 Clause 5.2.6.1.4 Ed 2: states that: A FSA team shall review the work carried out on all phases of the safety life cycle prior to the stage covered by the assessment that have not been already covered by previous FSA's.

2.2 Functional Safety Assessment Stage 5

IEC 61511-1 Ed 2 specifically defines the following in respect to SIS modifications and FSA 5.

Clause 5.2.6.2.4: Management of change procedures shall be in place to initiate, document, review, implement and approve changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed).

Clause 5.2.6.1.9: In cases where a FSA is carried out on a modification the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

Clause17.2.3: Prior to carrying out any modification to a SIS (including the application program) an analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification could impact safety then there shall be a return to the first phase of the SIS safety life-cycle affected by the modification.

Clause 17.2.6: Modification activity shall not begin until a FSA is completed in accordance with 5.2.6.1.9 and after proper authorisation.

2.3 Action Control

Actions within this report will be controlled in section 10

2.4 Team Membership

Date of Assessment	21/10/2016	
Location	No formal meeting, documentation circulation only	
FSA Team		
Name	**Company & Position**	**Competence**
D.B.Faulkner	P&I Design Ltd Instrument Engineer	ISA84 Functional Safety Specialist 30 Years Instrumentation Experience 15 Years Safety Instrument Systems
S.Joyce	px Ltd Maintenance Supervisor	

3 FUNCTIONAL SAFETY ASSESSMENT STAGE 5 REQUIREMENTS

3.1 FSA 5 Modification

This FSA is for a modification to an existing Safety Instrumented System.

3.2 Agenda

This FSA will address the following:

- The recommendations and actions arising from previous FSA have been resolved and completed;

- Project design change procedure;

- Review of the following;
  - Description of the modification;
  - Reason for the modification
  - Hazards which may be affected by the modification;
  - An analysis of the impact on functional safety as a result of the proposed modification;
  - Approvals for the modification;
  - Test used to verify that the change was properly implemented and the SIS performs as required.

- Assess how far within the SIS lifecycle to go back and review the impact of the modification;
  - LOPA
  - SRS
  - Design
  - Installation
  - Testing
  - Operation
  - Maintenance

- Review the status of operating manuals and documentation in respect to the implemented modification;

- Plans or strategies for implementing further FSA's are in place;

4 SAFETY INSTRUMENTED SYSTEM TO BE REVIEWED

4.1 Existing System

The following, details the Safety Instrumented System (SIS) being assessed by this FSA.

SIS Unique Identifier	BRM-SIS1	
Title	Pipeline Import Overfill Protection	
Location	Bramhall Terminal	
Existing Safety Integrity Level & Systematic Capability	SIL 2	SC 2

SIS Description	Import pipeline to bulk storage tank overfill protection.
SIF Description	Tanks 1 to 8 High High High Levels close XVESD-V1

4.2 Proposed Modification

Description	Replace annunciator alarm repeat relays with units from a different supplier
Proposed Safety Integrity Level	Not Applicable, Status signal only
Reason for the Modification	The terminal has been experiencing failures of the annunciator repeat relay during Nivotester pushbutton simulation testing. The Nivotester simulation test cycles the relay twice before returning healthy, several units have failed to return healthy leaving a high high high level alarm active. The relay is not part of the safety instrumented system, safety integrity level (SIL) calculations and does not affect the safety instrument function (SIF) of high high high level closing V1 ESD valve.
Hazards which may be affected by the modification	None
Impact on functional safety as a result of the proposed modification	None, units not SIL rated

5 PREVIOUS FUNCTIONAL SAFETY ASSESSMENTS

Details of previous FSA's conducted on this SIS.

5.1 Previous Functional Safety Assessments

FSA Stage	FSA 4
Document Number and Revision of previous FSA	SI297020_RPT SIS Functional Safety Assessment
Date of FSA	22/02/2011
Are there any actions outstanding from the assessment	Any Outstanding actions: ☒Yes ☐No If No go to Section 6
Where are outstanding actions controlled	Outstanding actions controlled by the Safety Committee

5.2 Functional Safety Assessments Outstanding Actions

FSA Stage and Date	FSA 4	22/02/2011
Action Number	See Safety Committee Report	
Description of status of Action	See Safety Committee Report	

6 MANAGEMENT OF CHANGE

6.1 Project Design Change Procedures

Project Design Changes	MOC Number 152
Description of Procedure employed	Management of Change Procedure detailing the following: Description of the modification, Reason for modification, Identified hazards during modification, Impact on FS, Design of the modification, SIS documentation impacted by the modification, Implementation Plan, Testing Plan, approvals and responsibilities
Does the procedure satisfy the requirements	☒Yes ☐No If No, then detail below what actions are required;

6.2 Approvals for the Modification

Originator of modification; **Name - Position**	S.Joyce	Maintenance Supervisor
Modification request approved by; **Name - Position**	Name	Position
Responsibility for design by; **Name - Position**	D.B.Faulkner	P&I Design Ltd Instrument Engineer
Responsibility for implementation by; **Name - Position**	D.B.Faulkner	P&I Design Ltd Instrument Engineer
Responsibility for validation by; **Name - Position**	D.B.Faulkner	P&I Design Ltd Instrument Engineer

6.3 Verification and Validation

To ensure verification of the proposed modification through the implementation phase and validation of the installed modification the following procedure will be utilised.

Management of Functional Safety Procedure	MOC Form SHE/PX/M/F/4.11.1
Verification Procedures to be utilised for the modification	MOC Form SHE/PX/M/F/4.11.1
Validation Procedures to be utilised for the modification	MOC Form SHE/PX/M/F/4.11.1

7 LIFECYCLE DOCUMENTATION

Considering the proposed modification, it is felt that the modification will require the following lifecycle documentation to be reviewed and possibly modified:

Hazard and Risk Analysis	**HAZOP** Yes ☐ No ☒	Not applicable, no change to hazard
	LOPA Yes ☐ No ☒	Not applicable, no change to protection layers
Safety Requirement Specification	Yes ☐ No ☒	Not applicable, no changes
Software Requirement Specification	Yes ☐ No ☒	Not applicable, hardwired system
FSA Stage 1	Yes ☐ No ☒	Not required

Design Documentation		
Process & Instrumentation Drawing	Yes ☐ No ☒	Not applicable, no plant changes
Schematic overview Drawing	Yes ☐ No ☒	Not applicable, no plant changes
Equipment Specifications	Yes ☐ No ☒	No specific specification, relay type listed on drawings.
Loop and Hook Up Diagrams	Yes ☒ No ☐	See MOC
Logic and Panel Drawings	Yes ☒ No ☐	See MOC
SIL Verification Document	Yes ☐ No ☒	Not applicable, non SIL rated
Software Documentation	Yes ☐ No ☒	Not applicable, hardwired
Cause & Effect Matrix	Yes ☐ No ☒	Not applicable, unaffected
FSA Stage 2	Yes ☐ No ☒	Not required

Installation Documentation		
Scope of Work	Yes ☒ No ☐	Drawing revisions
Construction Drawings	Yes ☐ No ☒	Not applicable, no changes

Operation & Maintenance		
Operational Procedures	Yes ☐ No ☒	Not applicable, no changes to procedures
Maintenance Procedures	Yes ☐ No ☒	Not applicable, no changes to procedures

Testing Documentation		
Testing Plan	Yes ☒ No ☐	Re test during proof test
FAT	Yes ☐ No ☒	Not applicable, system installed on site. See SAT
Documentation & Hardware Verification	Yes ☐ No ☒	Not applicable, non SIL rated.
ATEX Certification	Yes ☐ No ☒	Not applicable, safe area
SAT	Yes ☒ No ☐	Qsf2058 - Method Statement Instrument Proof testing procedures
FSA Stage 3	Yes ☐ No ☒	Not required

Management of Functional Safety		
Safety Instrumented Systems Policy Document	Yes ☐ No ☒	Not applicable, policy unaffected
Safety Instrumented System Procedures	Yes ☐ No ☒	Not applicable, proof testing procedures unchanged
Safety Instrumented System Safety Plan	Yes ☒ No ☐	Plan to update
Training	Yes ☐ No ☒	Not applicable, no change to operation or testing
External Considerations	Yes ☐ No ☒	Not applicable, none identified

8 FUNCTIONAL SAFETY ASSESSMENT

The following provides details of this assessment, any non-compliances or observations found requiring further action are detailed, and an FSA Action created. As stated in Section 2.2 action history is controlled within ASANA and a snapshot of the action status will be appended to this document relevant to the time of the issue of the revision of this document.

8.1 Risk Analysis & Allocation of Safety Functions

8.1.1 Hazard & Operability Study

Was Assessment Required	Yes ☐ No ☒ If yes continue below:

8.1.2 Risk Graph or Layer of Protection Analysis

Was Assessment Required	Yes ☐ No ☒ If yes continue below:

8.1.3 HAZARD Impact Assessment

Was Assessment Required	Yes ☐ No ☒ If yes continue below:

8.2 Allocation of Safety Functions

Are the Safety Instrumented Functions (SIF) defined	Yes ☐ No ☒ Not applicable

8.3 Safety Requirement Specification

The following provides details of this assessment of the Safety Requirement Specification, any non-compliances or observations found requiring further action are detailed and an FSA Action created.

Document Number	SI297013_RPT Bramhall SIS Safety Requirement Specification – Not affected

8.4 Software Requirement Specification

The following provides details of this assessment of the Software Requirement Specification, any non-compliances or observations found requiring further action are detailed and an FSA Action created.

8.5 Design Documentation Review

Process & Instrumentation Drawing	Yes ☐ No ☒	Not affected by modification

SI297002_DWG_A - BRM-SIS1 Schematic Overview	Yes ☐ No ☒	Not affected by modification

Equipment Specifications	Yes ☐ No ☒	Not affected by modification. Not SIL rated so no specification required

Loop and Hook Up Diagrams	Yes ☒ No ☐	The following drawings have been revised, check and approved – SI297001_DWG – E to F SI297003_DWG – C to D SI297004_DWG – B to C SI297040_DWG – A to B SI297041_DWG – A to B SI297042_DWG – A to B SI297043_DWG – A to B SI297044_DWG – A to B SI297045_DWG – A to B SI297046_DWG – A to B SI297047_DWG – A to B SI297048_DWG – A to B SI297049_DWG – A to B SI297050_DWG – A to B

Logic and Panel Drawings	Yes ☒ No ☐	The following drawings have been revised, check and approved – SI297011_DWG – D to E SI297012_DWG – D to E SI297013_DWG – F to G SI297014_DWG – E to F SI297016_DWG – F to G SI297019_DWG – D to E

SI297002_RPT Bramhall Safety Instrument System	Yes ☐ No ☐	Not affected by modification. Not SIL rated

Software Documentation	Yes ☐ No ☒	No software

Cause & Effect Matrix **Enter Doc reference**	Yes ☐ No ☒	Not affected by modification

8.6 Testing Documentation Review

16089HDR001A - Method Statement Instrument	Yes ☒ No ☐	Installation Inspection – No faults reported

16089HDR002A - Instrument Installation Conformance Control	Yes ☒ No ☐	Functional test – No faults reported

SI297006_RPT_D_CC20161111_16089 - BRM-SIS1 Shutdown Conditions Proof Testing	Yes ☒ No ☐	Re Proof Test – No Faults Reports associated with relay replacement

8.7 Management of Functional Safety Documentation Review

TBC	Yes ☐ No ☒	Safety Committee Action

8.8 Functional Safety Review

Does it appear that the modification provides the functional safety required of it	Yes ☒ No ☐
Enter details	No change in safety function

9 CONCLUSIONS

Project complete

10 Actions

No actions associated with the modification

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

CONOCO PHILLIPS ENERGY

BRAMHALL TERMINAL

GASOLINE OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

COMPLIANCE DOCUMENT

STAGE 4 FSA

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	30.06.11	D.R. Ransome	DSR	Client	Original Issue	
						Document No. **SI297021_RPT**
						Page 1 of 15

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION HISTORY

Rev	Description
A	Original Issue and Pre-Assessment prior to Stage 4 FSA
B	
C	
D	

2 INTRODUCTION

This document provides a checklist to ensure that the Safety Instrument System Life Cycle complies with the requirements of the standard BS EN 61511.

BS EN 61511 details that functional assessments should be carried out in line with the following stages:

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 – Following **Safety Instrument System Design.**

Stage 3 – After the **installation, pre-commissioning and final validation of the Safety Instrument System** has been completed and operation and maintenance procedures have been developed.

Stage 4 – After gaining experience in **operating and maintenance**.

Stage 5 – After **modification and prior to decommissioning**.

The items in bold underline type above reflect the items covered by the BS EN 61511.

In order to conduct the functional assessments the following checklists have reference to the clauses within the standard and the relevant assessment stage.

Depending on the complexity of the Safety Instrument System, some of the following checklists may not be appropriate, if this is the case then N/A should be entered into the appropriate box.

3 SUMMARY

This document at Revision A has been completed as a pre-assessment for a Functional Safety Assessment.

It may be that some lifecycle documentation was not supplied for the pre-assessment or that it has not been created.

4 DEFINITIONS AND ABBREVIATIONS

The following definitions and abbreviations apply to this document.

BPCS	Basic Process Control System
Logic Solver	Part of the SIS that performs one or more logic functions, e.g. safety relay, trip amplifier
Proof Test	Periodic testing to detect failures in a safety instrumented system
Protection Layer	A mechanism that reduces risk by control, prevention or mitigation
Sensor	Part of the SIS which measures the process condition
SIF	Safety Instrumented Function – A function with a specified safety integrity level which is necessary to achieve functional safety
SIL	Safety integrity level – A numerical number, 1 to 4 stipulating the level of integrity the system shall perform to, 1 being the lowest 4 the highest
SIS	Safety Instrument System – A SIS comprises of sensors, logic solvers and final elements
1ooN	SIS made up of N independent channels, which are so connected, that any single channel is sufficient to perform the correct safety instrumented function
2ooN	SIS made up of N independent channels, which are so connected, that any two of the channels are required to perform the correct safety instrumented function
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PFD	Probability of Failing on Demand

5 STAGE 1 - SAFETY REQUIREMENT SPECIFICATION CHECKLIST

Stage 1 – Safety Requirement Specification Checklist 1				
Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
1.1	8 & 9	Do the Safety Instrumented Functions (SIF) derive from a HAZOP or LOPA study, if not where are they derived from.	Yes	
1.2	9	Has the Safety Integrity Level (SIL) for each SIF been allocated.	SIL 2	
1.3	10	Has the demand on the SIF been specified (demand or continuous).	Yes	
1.4	10	Is each SIF described adequately, together with a definition of the safe state.	Yes	
1.5	10	Have common cause failures been considered.	Yes	
1.6	10	Have process conditions been considered which could have an effect on the limitations of sensors or final elements. (e.g corrosion, plugging, coating).	Yes	
1.7	10	Are performance requirements defined. (e.g speed of closure of valve).	Yes	
1.8	10	Are sensor inputs defined with respect to range, accuracy etc.	No	
1.9	10	Have the process setpoints and trips been defined.	Yes	
1.10	10	Is there a description of the relationship between inputs, logic solver and outputs and any specific requirements requiring 1oo2, 2oo2 systems or specific requirements regarding nuisance tripping.	Yes	
1.11	10	Has the mean time to repair been specified with consideration to availability of spares and labour	Yes	
1.12	10	Have manual shutdowns been considered.	Yes	
1.13	10	Is there a requirement for overrides and if so has the effect on the SIF been considered.	No	
1.14	10	Have the interfaces with the Basic Process Control System (BPCS) been defined.	Yes	
1.15	10	Can the BPCS interfere with the safe operation of the SIF.	No	
1.16	10	Has the method of resetting the system been defined.	Yes	
1.17	10	Have environmental and abnormal events been considered. (e.g. temperature, humidity, fire etc.)	Yes	
1.18	10 & 12	If the SIS logic solver is software based have the application software requirements been specified.	Yes	

6 STAGE 2 - SAFETY INSTRUMENT SYSTEM DESIGN CHECKLIST

Stage 2 – Safety Instrument Design
Checklist 2 - General

Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
2.1	5	Are design documents within a formal revision and control process.	Yes	
2.2	11.2.1 & 11.9.2	Has the Probability of Failure on Demand (PFD) been calculated for the SIF and does it meet the Safety Specification requirements.	Yes	
		Has nuisance tripping being considered.	Yes	
	11.4	Has the system hierarchy been derived (e.g. 1oo1, 1oo2, 2oo2 etc) on the basis of PFD, Hardware Fault tolerance and nuisance tripping to provide the most appropriate solution.	Yes	
2.3	11.2.2	If the SIS implements both SIS and non SIS functions can the non SIS system interfere with the safe operation of the SIS.	n/a	
2.4	11.2.3	If SIF's with different SIL share the same hardware or software does it comply to the highest safety level.	No	
2.5	11.2.4	Is the design of the BPCS to BS EN 61511. If answer is no then:	No	
	11.2.9	Is there independence in the function of the BPCS and the SIS.	Yes	
	11.2.10	Can any interface with non SIS systems such as BPCS adversely effect the operation of the SIS.	No	
2.6	11.2.5	Is there any bypass systems provided and if so are their operating procedures well documented	No	
2.7	11.2.5	Have testing procedures been developed.	Yes	
2.8	11.2.7	Once the SIF has initiated putting the plant into a safe state does it remain in a safe state until after the system has been manually reset.	Yes	
2.9	11.2.8	Is there a manual means of initiating the SIF e.g ESD pushbutton.	Yes	
2.10	11.2.11	Is the system designed as fail safe on loss of power or air. If the answer is no then: Is loss detected Is there back up supply to ensure system operation.	Yes	
2.11	11.3	Has consideration been given to SIF behaviour on detection of a fault and has sufficient time and spares been allowed for in MTTR.	Yes	
2.12	11.4	Has hardware fault tolerance been considered in deriving the SIL.	Yes	

Stage 2 – Safety Instrument Design **Checklist 3 – Components & Sub-Systems**				
Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
3.1	11.5.2 11.5.3	Have equipment vendors provided failure rate data in accordance with BS EN 61508 If not Is evidence of proven in use satisfied.	Yes	
3.2	11.9.2	Have equipment vendors provided proof test methodology and frequency data in accordance with BS EN 61508. If not On what basis is proof testing performed.	Yes	
3.3	11.5.4	Do components selected on prior use have a fixed programming language. If the answer is yes then: Can any unused features jeopardize the SIF. Have all settings being recorded e.g ranges, modes of operation, etc	n/a	
3.4	11.5.5 11.5.6	Is the logic solver programmable. If yes fully consult BS EN 61511-1 Section 11.5.5, 6 and Section 12.	No	
3.5	11.6 & 11.9.2	Have the following conditions been considered for the field devices: Common Cause failures Material of construction Plugging Dirt Corrosion Foreign bodies Freezing Temperature effects Pressure EMC	Yes	
3.6	11.6	Have the following conditions been considered for the final elements: Shutoff differential Opening & Closing speed of valves Leakage Fire resistance	Yes	
3.7	11.6.3	Does each device have its own dedicated wiring.	Yes	
3.8	11	Are SIS components identified uniquely.	Yes	

Stage 2 – Safety Instrument Design
Checklist 4 – Interfaces

Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
4.1	11.7.1 11.7.1	Can the operator influence the action of the SIS from the BPCS. If yes: Is this by a bypass facility, is the bypass either key protected or if BPCS, password protected.	No	
4.2	11.7.1	Does the SIS operate without any intervention of the operator. If no: Is the operator has actions then is there a confirmation step.	Yes	
4.3	11.7.1 & 11.7.2	The status of the SIS should be available to the operator and the maintenance technician. Have the following been provided, if no then add comments as to why not: • Indication that the SIS protective action has occurred. • Where the SIS process is in its sequence. • Indication the SIF is bypassed • Status of sensors and final elements. • Status of elements in voting systems. • Loss of power or air when it would impact on safe operation. • Diagnostics for fault finding.	Yes	
4.4	11.7.3	Can communication failures have an adverse affect on the SIS.	No	
4.5	11.7.3	Are communication signals isolated from other energy sources.	Yes	

7 STAGE 3 - SAFETY INSTRUMENT SYSTEM VALIDATION CHECKLIST

Stage 3 – Safety Instrument System Validation
Checklist 5 – Factory Acceptance Tests - Planning

Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
5.1	13.2.2	Has a FAT procedure been defined prior to FAT	Yes	
5.2	13.2.2	Does the FAT identify the number and issue of drawings to which the tests are to be conducted	Yes	
5.3	13.2.2	Is the test engineer competent to perform the checks and does he have an understanding of the system functionality	Yes	
5.4	13.2.2 13.2.5	Does the FAT identify any special tools or equipment needed to conduct the FAT	No	
5.5	13.2.5	Is the FAT test plan issued at a auditable revision	Yes	
5.6	13.2.5	Is the Safety Instrument Specification available to the test engineer	Yes	
5.7	13.2.2	Does the FAT provide a methodical approach to the testing	Yes	
5.8	13.2.2	Can the test be conducted without dependency on other systems	Yes	
5.9	13.2.2	Does the location of the test provide a suitable environment for the FAT	Yes	

Stage 3 – Safety Instrument System Validation
Checklist 6 – Factory Acceptance Tests

Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
6.1		Is the system constructed in accordance with the design	Yes	
6.2	13.2.5	Did the tests verify the functionality of the system in accordance with the design	Yes	
6.3	13.2.6	Have the test results been recorded	Yes	
6.4	13.2.6	Were there any failures during the test	Yes	
6.5	13.2.6	Were any modifications required during the FAT If the answer to this question is yes: Have the modifications been reviewed with the design engineers to review the impact on the SIS and Have any associated modifications to the documentation been carried out	Yes	
6.6	13.2.6	Is there any requirement for a re-test	No	
6.7	13.2.6	For any retest, state what has been retested	N/A	

Stage 3 – Safety Instrument System Validation **Checklist 7 – Installation & Pre-Commissioning (Prior to SAT)**				
Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
7.1	14.1.1	Has the installation been installed in accordance with the design Including: Segregation of cabling from the BPCS Identification of all aspects of the system including: Cable identification Junction Box identification Logic Solver Identification Sensor Tag or Asset Number identification Final Element Tag or Asset Number identification Identification that all equipment is part of an SIS	Yes	
7.2	14.1.1	Have test sheets been issued by the installation contractor that the system has been checked in accordance with all national electrical requirements and standards and is ready for commissioning	Yes	
7.3	14.2.2	Does the component comply with the Design Specification	Yes	
7.4	14.2.2	Are all SIS components installed in accordance with the design and any special manufacturers requirements	Yes	
7.5	16.3.2	Has consideration been given to some form of security system to prevent unauthorised access to instruments and also to assist in periodic visual inspections	Yes	
7.6	14.2.3	Are the following acceptable prior to the system being energised for testing: Earthing Any transportation stops removed No evidence of physical damage All instrument calibrated where necessary Power supply available Air supply available Interfaces with non SIS systems available	Yes	
7.7	14.2.5	Have any modifications been necessary throughout the installation phase and if so: Have the modifications been reviewed with the design engineers to review the impact on the SIS and Have any associated modifications to the documentation been carried out	No	

Stage 3 – Safety Instrument System Validation **Checklist 8 – Site Acceptance Test**				
Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
8.1	15.2.1	Has a test plan been produced to cover the following: Responsibilities for testing Testing Criteria Special requirements for start up, shutdown & maintenance Component failure testing Any special preparations or effects on operating plant during the test Partial testing if it not possible to complete the full testing Testing Schedule Testing Procedures	Yes	
8.2	15.2.3	Where the SIS components require measurement calibration: Has this been completed Are the results within the required tolerance	N/A	
8.3	15.2.4	Is the SIS documentation as the installed system	Yes	
8.4	15.2.4	Does the SAT testing include for the following: Checks to ensure the SIS performs during: Start up/Shut down Loss of power/Loss of air	Yes	
8.5	15.2.4	Does the SAT testing include for the following: That the SIF performs as specified That any external manual shutdown or non SIS functions cannot impair the operation of the SIS	Yes	
8.6	15.2.4	Does the SAT testing include external interfaces: BPCS Annunciation Diagnostics	Yes	
8.7	15.2.4	Have the following been checked for correct operation: Reset Bypass facilities Start up overrides	N/A	
8.8	15.2.4	Following the SAT have: All test results been recorded	Yes	
8.9	14.2.5	Have any modifications been necessary throughout the SAT phase and if so: Have the modifications been reviewed with the design engineers to review the impact on the SIS and Have any associated modifications to the documentation been carried out	No	

8 STAGE 4 - SAFETY INSTRUMENT SYSTEM OPERATION & MAINTENANCE

Stage 4 – Safety Instrument System Operation & Maintenance
Checklist 9 – Operation & Management

Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
9.1	16.2.1	Have manuals been issued for use by end user And is there sufficient information to enable operation, proof testing and maintenance of the SIS	Yes	
9.2	16.2.4	Have operators and management been trained and understand: How the SIS functions The hazards the SIS is protecting against The operation of and consequences of: Override facilities Reset functions Manual shutdown facilities Interpretation of Alarms Interpretation of diagnostics	Yes	
9.3	16.2.2 16.2.6	Do management have procedures in place for: Proof testing Record keeping of: Proof testing activation of SIS failure of SIS analysis of reliability of SIS	Yes	
9.4	16.2.7	Do management understand the life cycle requirements BS EN 61511 relevant to the SIS	Yes	

Stage 4 – Safety Instrument System Operation & Maintenance
Checklist 10 – Proof Testing & Maintenance

Item No	BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
10.1	16.2.5	Are the maintenance and proof testing engineers familiar with and competent to work on the SIS	Yes	
10.2	16.3.1	Are test procedures available and do they reflect the appropriate methods of tests with consideration to site operating conditions	Yes	
10.3	16.3.1	All aspects of the SIS, sensors logic solver and final elements should be proof tested. If it is not possible to test all elements in a single proof test does the proof test plan indicate how the test should be conducted	Yes	
10.4	16.3.2	Following proof testing are the following available: Description of the tests performed Dates of inspections and tests Name of person conducting the tests Identification of the equipment tested Results of the tests	Yes	
10.5	17.2.5	Following any repair or replacement of an SIS component is a modification sheet available together with analysis of the repair or replacement	Yes	

9 STAGE 5 - SAFETY INSTRUMENT SYSTEM MODIFICATION

Intentionally Left Blank

10 ACTIONS

ACTION STATUS			
Action No.	**Action By**	**Description**	**Completed**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

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

px LTD

PHILLIPS 66 BRAMHALL TERMINAL

TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MODIFICATION REPORT

COMPEX RECTIFICATION

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	08.03.13	D.B.Faulkner	D.S.Regan	Client	Original Issue	
						Document No. **PX232003_RPT**
						Page 1 of 5

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

P & I Design Ltd
2 Reed Street, Thornaby, UK, TS17 7AF
Tel: + 44 (0)1642 617444
Fax: + 44 (0)1642 616447
www.pidesign.co.uk

1 REVISION HISTORY

Rev	Description
A	Original Issue – Modification requested, assessed and initiated
B	
C	
D	

2 SCOPE

This document has been prepared to control a modification to the Phillips 66, Bramhall Terminal, Tank Overfill Safety Instrument System.

The modification is necessary due to a failure of a JB1, LEHHH03 and LEHHH04 during CompEx inspection.

The purpose of this report is to ensure that the proposed modifications are planned, reviewed and approved prior to implementation. Also to highlight the necessary changes to all documentation.

A stage 5 Functional Safety Assessment would normally be initiated at this stage. However as the replacement is a like for like replacement of a certified component, no stage 5 FSA is considered necessary.

3 MODIFICATION PLAN

3.1 Description of the modification or change

LEHHH03 and LEHHH04 replaced with identical units.

JB3 to be added to installation.

3.2 Reason for the modification or change

LEHHH03 and LEHHH04 water ingress in original units due to cracked housings.

Water Ingress found in JB1, JB3 to be added to installation to relieve tension on JB1 cables (suspected water ingress route).

3.3 Identified hazards affected

None.

3.4 Impact on functional safety

It is considered that there will be no impact on functional safety from this modification.

Note: If by performing this modification, there is an impact on functional safety, then the impact must be analysed by returning to the first part of the safety system lifecycle documentation and review the effect of this change, ensuring that the Safety Integrity Level and other protection layers are adequate for functional safety.

3.5 Design of the modification

3.5.1 SIS Documentation impacted by the modification

SI297001_DWG
SI297003_DWG
SI297001_SCH
SI297007_RPT

3.6 Implementation plan

LEHHH03 to be replaced and retested when tank 3 back in service.
LEHHH04 to be replaced when tank 4 removed from service, retested when tank 4 back in service.
JB3 to be added when tank 4 removed from service.

3.7 Testing plan

The Safety Instrument System Panel will require re-testing prior to and following the modifications.

3.8 Approvals, Roles and Responsibilities

This modification was requested by: Paul Lynch

This modification request approved by: Dave Regan, CSFE

Hazard and Impact assessment conducted by: Dave Regan, CSFE

Design incorporation by: David Faulkner

Design Reviewed by: Dave Regan CSFE

Modifications by: Mark Jones, E&I Engineer px Ltd.

Modifications proof tested by: ………………..

Modification completed – date ………………

Documentation updated and re-issued: ………………

P & I DESIGN

P & I Design Ltd
2 Reed Street, Thornaby, UK, TS17 7AF
Tel: + 44 (0)1642 617444
Fax: + 44 (0)1642 616447
www.pidesign.co.uk

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

px LTD

CONOCO PHILLIPS BRAMHALL TERMINAL

TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MODIFICATION REPORT

SAFETY RELAY REPLACEMENT

Rev	Date	By	Checked	Approved	Description	
A	10.07.12	D.S.Regan	D.R.Ransome	Client	Original Issue	Client Ref.
						Document No. **PX232001_RPT**
						Page 1 of 5

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION HISTORY

Rev	Description
A	Original Issue – Modification requested, assessed and initiated
B	
C	
D	

2 SCOPE

This document has been prepared to control a modification to the Conoco Phillips, Bramhall Terminal, Tank Overfill Safety Instrument System.

The modification is necessary due to a failure of a safety relay in the Safety Instrumented System for tank 1

The purpose of this report is to ensure that the proposed modifications are planned, reviewed and approved prior to implementation. Also to highlight the necessary changes to all documentation.

A stage 5 Functional Safety Assessment would normally be initiated at this stage. However as the replacement is a like for like replacement of a certified component, no stage 5 FSA is considered necessary.

3 MODIFICATION PLAN

3.1 Description of the modification or change

The Pilz S2 relay in the Safety Instrumented system logic for tank 1 will be replaced with an identical unit supplied by Pilz.

3.2 Reason for the modification or change

Tank 1 was out of service so before it was re-instated the Hi Hi Hi alarm was tested, everything worked fine but the annuciator panel could not be reset.

The panel was checked l & all seemed to be ok, all relays were energised as they should be.

It would appear that R128 was energised & all the lights were correct but none of the contacts had changed over.
The power was cycled a couple of times but this made no difference.
The relay was removed to test on the bench, this time it worked.
The relay was then put back & worked.

Due to the failure it was recommended that the relay be replaced and the faulty relay returned to the manufacturer for evaluation and report.

3.3 Identified hazards affected

None.

3.4 Impact on functional safety

It is considered that there will be no impact on functional safety from this modification.

Note: If by performing this modification, there is an impact on functional safety, then the impact must be analysed by returning to the first part of the safety system lifecycle documentation and review the effect of this change, ensuring that the Safety Integrity Level and other protection layers are adequate for functional safety.

3.5 Design of the modification

3.5.1 SIS Documentation impacted by the modification

None

3.6 Implementation plan

A replacement relay will be obtained.

Once the new relay is available, the following procedure should be followed.

- Full test carried out on tank 1, and documented, to confirm that the SIS was available and operational prior to the modification.
- Removal of faulty relay.
- Replacement of relay.
- Full test carried out on tank 1, and documented, to confirm that the SIS is available and operational after to the modification.
- Relay to be despatched to the manufacturer with a detailed explanation of the fault and a request for a full evaluation and report.
- Report from manufacturer to be evaluated to determine if any further action is necessary.

3.7 Testing plan

The Safety Instrument System Panel will require re-testing prior to and following the modifications.

3.8 Approvals, Roles and Responsibilities

This modification was requested by:	Mark Jones, E&I Engineer px Ltd.
This modification request approved by:	Dave Regan, CSFE
Hazard and Impact assessment conducted by:	Dave Regan, CSFE
Design incorporation by:	n/a
Design Reviewed by:	n/a
Modifications by:	Mark Jones
Modifications proof tested by:	………………..
Modification completed – date	………………
Documentation updated and re-issued:	n/a

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

SIMON STORAGE

CONOCO PHILLIPS BRAMHALL TERMINAL

TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MODIFICATION SHEET

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	15/11/10	D.S.Regan	PJP	PJP	Original Issue	
						Document No. **SI297014_RPT**
						Page 1 of 2

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

From the Standard BS EN 61511, and following the requirement for a modification of the SIS have the following been considered and implemented:

Description of the modification – See Below
Reason for the modification - See Below
Identified hazards which may be affected – See Below
Analysis of the impact of the modification – See Below
Approval for the modification
Has all documentation affected by the modification been revised - Yes
Has the modification been fully proof tested - Yes
Has a detailed modification sheet been completed – See below

SIS Modification Sheet		
<u>Describe The Proposed Change & Objective</u> Slops Tanks 11, 12 & 13 removed permanently from Safety Instrument System.	***Note*** *What is it you are proposing to modify?* *What is the objective of the modification?* *What are the benefits of the modification?* *If temporary change, how long will it be in effect for?*	
<u>Reason for the modification</u> Following the implementation of facilitate blending of ethanol with gasoline. The existing slops tanks 11,12 & 13 were modified to store ethanol. Tanks 11, 12 & 13 will now be filled from road tankers and as such are outside the PSLG guidelines and have been permanently removed for the site gasoline Safety Instrument System.	***Note*** *Why is the modification being proposed?*	
<u>Options Available & Risks</u> The new risks will be the possible overflow of tanks 11, 12 & 13 and release of ethanol. The tanks will have their own independent overfill protection system. There will be a separate Safety system to prevent overfill of tanks 12, 12 & 13 by shutting down the Road Tanker Offloading Pump in the event of an activation of any of the high high level switches in tanks 11, 12 & 13. There is no impact on the existing Safety Instrument System with the removal of the three tanks 11, 12 & 13 apart form that stated above	***Note*** *What options are there to make the change?* *What are the risks of not doing the change, what new risks does the change potentially introduce and how are these risks to be managed?*	
<u>Outline Plan To Introduce Change</u> The existing SIS Monitoring panel will be modified to incorporate the logic for the removal of the tanks. The SIS design and Lifecycle documentation has been modified to exclude the three tanks.	***Note*** *Identify the requirements to introduce and manage the change* *Any suggestions to improve the proposed change?*	
<u>Has all documentation affected by the modification been revised</u> SIS Designer:___________________________		
Approvals (Note: Signature Indicates Acceptance Of Modification With Actions/Comments Noted)	**Sign**	**Date**
Approved by Conoco Phillips		