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

inter terminals

INTER TERMINALS IMMINGHAM LTD

EAST TERMINAL

GASOLINE OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM IMMEAS-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

IMMINGHAM STORAGE COMPANY

EAST TERMINAL

GASOLINE TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MANAGEMENT OF FUNCTIONAL SAFETY

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	20/12/10	DSR	DRR	Client	Issued for FSA Stage 1	
B	10/10/12	DSR	DBF	Client	Following FSA Stage 2/3	Document No. **SI277102_RPT**
						Page 1 of 22

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION HISTORY

Rev	Description
A	Original Issue
B	Following FSA Stage 3: Stage 3 FSA added Documentation references added
C	
D	
E	

2.0 SCOPE

This document has been prepared for the Safety Instrument System (SIS) Management System. It is intended to reflect the life cycle of the SIS in accordance with BS EN 61508 & BS EN 61511 and to be a working document throughout the life cycle of the Safety System. This objective of this document is to identify the management activities that are necessary to ensure the functional safety objectives are met.

3.0 ORGANISATIONS AND RESOURCES

Persons, departments, organisations or other units which are responsible for carrying out and reviewing each of the safety lifecycle phases shall be identified and be informed of the responsibilities assigned to them.

Persons, departments or organisations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

Immingham Storage Ltd Management Procedures identify the responsibility of persons assigned to this Safety Instrument System and ensure the competence of such persons.

Immingham Storage Ltd Management Procedures include the following elements specific to the Safety Instrument System.

- Safety Planning, organisation and procedures.
- Identification of roles and responsibilities.
- Competence of persons and accountability.
- Implementation and monitoring of procedures.
- Management of Change.

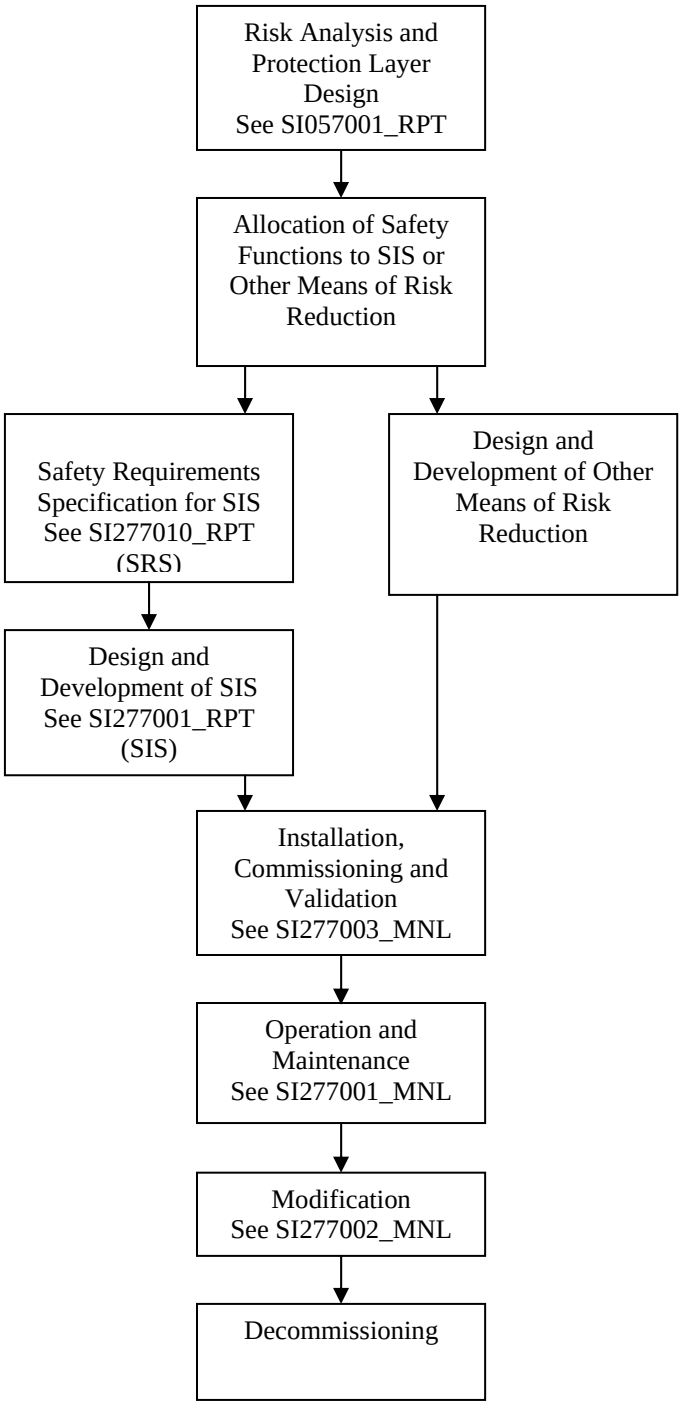
This document details the persons, departments and organisations who will be responsible in this Safety Instrument System.

P&I Design Ltd are responsible for the design of the SIS and also are involved with Immingham Storage Ltd in the Risk Assessment Process (LOPA) study.

P&I Design Ltd Quality System ensures the competence of persons assigned to this Safety Instrument System.

4.0 SAFETY LIFE CYCLE

A SIS requires being auditable throughout each stage of its cycle. It is necessary not just at the conceptual and design stage but also at operational and maintenance stages.



5.0 SAFETY INSTRUMENT SYSTEM

The Safety Instrument Functions of the Safety Instrumented Systems are:

1. Tank Overfill Protection – SIL 2

6.0 FUNCTIONAL SAFETY

This document will provide the control of the design review assessments and Functional Safety Assessment through the lifecycle of the SIS to ensure the necessary objectives of functional safety are met. It will identify the means of evaluating the system together with all stages of the review process. Design reviews and Functional Safety Assessments (FSA) will be documented in separate documents but referenced within this document.

As part of the continuous assessment process a Compliance Document Ref SI277101_RPT will be completed at various lifecycle phases. The purpose of this document is to ensure compliance to the standard at each phase.

In accordance with BS EN 61511 the defined stages for FSA are:

- Stage 1 – After the HAZOP and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification (SRS) has been developed.
- Stage 2 - After the SIS has been designed.
- Stage 3 After the installation, pre-commissioning and final validation of the SIS has been completed and operating and maintenance procedures have been developed.
- Stage 4 – After gaining experience in operating and maintenance.
- Stage 5 – After modification and prior to decommissioning of the SIS.

The number, size and scope of Functional Safety Assessments is decided upon specific circumstance considering the following:

- Size of project;
- Degree of complexity;
- Safety integrity Level;
- Duration of Project;
- Consequence in the event of failure;
- Degree of standardisation of design features;
- Safety regulatory requirements;
- Previous experience with a similar design.

The constitution of the FSA team is based upon the following:

- The scope of the FSA;
- Who is to participate in the FSA;
- The skills, responsibilities and authorities of the FSA team
- The information that will be generated as a result of the FSA;
- The identity of any safety bodies if required;
- The resources required to complete the FSA;
- The level of independence of the FSA team;
- The means by which the FSA will be revalidated after modifications.

BS EN 61511 states that at least on FSA shall be undertaken before the hazards are present.

For this project it is envisaged that the following FSA's will be carried out;

- Stage 1
- Stage 3
- Stage 4
- Stage 5

Based upon the criteria of this SIS detailed above it has been decided that for Stage 1 and 3 the senior competent person to lead the FSA will be independent from the design team.

Roles and Responsibilities:

Senior Independent competent person not involved in the design team and chair of the FSA team:

Mr D. Ransome – P&I Design Ltd.

7.0 RISK ANALYSIS AND ALLOCATION OF SAFETY FUNCTIONS

Layer of Protection Analysis (LOPA) was used as a technique to establish the initiating events, and protection layers to establish if further risk reduction was required.

Roles and Responsibilities:

Immingham Storage Ltd:

Agree Scope of LOPA
Provide LOPA team of competent persons in accordance with Management Procedures

Personnel assigned to this phase:

Meeting 1 – 31.01.2007 June 2010 – Tank Overfill Protection LOPA

Immingham Storage Ltd.
Mr C. Newstead
Allan Hall
Paul Jobling
Andy Drayton

P&I Design Ltd:
D.R.Ransome – Consultant
D. S. Regan – Facilitator and Secretary

Roles and Responsibilities:

P&I Design Ltd:

Agree Scope of LOPA
Provide personnel to facilitate and record LOPA study, allocate Safety Functions to SIS (or other Means of Risk Reduction) and produce report.
The LOPA review Document will be updated to reflect the final SIS calculated figure

Personnel assigned to this phase:
D. S. Regan
D. R. Ransome

LOPA Document Reference – SI057001_.RPT
Note: The LOPA Document is currently at Issue D 08.07.2010. Issue D included an Environmental Statement. It should be noted that this LOPA was not conducted against PSLG guidelines, and was not updated in accordance with these guidelines, as the facility, at present, does not have a gasoline facility.

8.0 SPECIFICATION OF SAFETY INSTRUMENT SYSTEM

The requirement for a Safety Instrument System was confirmed from the LOPA assessments and a Safety Requirement Specification is to be produced by P&I Design Ltd. Reference Document SI277010_RPT

Roles and Responsibilities:

Immingham Storage Ltd:

Competent person to Check and Confirm Safety Requirement Specification represents the design intent of the Safety Instrument System and LOPA study.

Personnel assigned to this phase:

M.Cook – Environmental & Technical Assistant
C. Newstead – Environmental & Technical Manager
P. Jobling – Group Safety Compliance Manager
A.Dixon - Group SHE officer
A. Rhodes – Terminal Manager

Any of the above may perform the checking.

P&I Design Ltd:

Produce Safety Requirement Specification and ensure that it meets the requirements of the LOPA report as well as the requirements of BS EN 61511.

Personnel assigned to this phase:

Production of SRS	D.S. Regan
Review	P.J. Parkin
	M. Morgan
	D.R. Ransome

At this stage, a functional Safety assessment Stage 1 will be carried out as per the requirements of BS EN61511. Reference

9.0 FUNCTIONAL SAFETY ASSESSMENT – STAGE 1

This assessment is to ensure that the SRS conveys the requirements of the SIS together with confirming the SRS complies with the requirements of the LOPA.

The FSA will address the following as a minimum:

- That the hazard and risk assessment considers the following:
  - Determined the hazards and hazardous events of the process and associated equipment;
  - Determined the sequence of events leading to the hazardous event;
  - Determined the process risk associated with the hazardous event;
  - Determined the requirements for risk reduction;
  - Determined the safety functions required to achieve the necessary risk reduction;
  - Determined the safety instrumented functions and Safety integrity level
- The recommendations from the hazard and risk assessment are in place and have been properly implemented.
- Plans or strategies for implementing further FSA's are in place.

Date of Review – Thursday 9th December 2010 at Immingham Storage East

Roles and Responsibilities:

P&I Design Ltd
Provide an independent assessment to ensure that the findings of the LOPA have been interpreted into the SRS and that the SRS details the full requirements of the intended SIS to proceed to detailed design. Document the FSA sand produce an outstanding action list with competition deadlines.

D.R.Ransome - Consultant

Immingham Storage Ltd:

Attendance of competent personnel relevant to the required disciplines to participate in the FSA.

Personnel assigned to this phase:

P. Jobling – Group Safety Compliance Manager
Andy Rhodes - Terminal Manager
Steve Waterman - Plant Engineer
Alan Hall - Project Engineering Manager

P&I Design Ltd:
Attendance of competent personnel relevant to the design of the SIS. Provide the FSA team with all necessary documentation. Update this Management of Functional Safety Document.

Personnel assigned to this phase:
D.S.Regan - Engineer

10.0 DESIGN & DEVELOPMENT OF SIS

The design for a Safety Instrument System will be produced by P&I Design Ltd. Reference Document SI277001.RPT.

Roles and Responsibilities:

Immingham Storage Ltd:

Competent person to review Design Documentation in conjunction with P&I Design Ltd.
Competent person(s) to participate in design reviews.

Personnel assigned to this phase: From

M.Cook – Environmental & Technical Assistant
C. Newstead – Environmental & Technical Manager
P. Jobling – Group Safety Compliance Manager
A.Dixon - Group SHE officer
A. Rhodes – Terminal Manager

Any of the above may carry out the checking.

P&I Design Ltd:

Produce SIS Design Documentation and ensure that it meets the requirements of the Safety Requirements Specification as well as the requirements of BS EN 61511.

The SIS Specification and Design will include manufacturer's certification for PFD data and SIS calculation.

Document design review meetings.

Personnel assigned to this phase:

Production of Design Document	D.S.Regan
Review	P.J. Parkin
	M. Morgan

On completion of the Design and Development or at various stages during the design, a design review will be carried out as per P&I Design Ltd. Quality Procedures.

11.0 INSTALLATION, COMMISSIONING AND VALIDATION

11.1 Pre-Installation

Prior to any installation, the following documentation for the installation, commissioning and validation are to be produced by P&I Design Ltd. The documentation is as follows:

Title	**Document Ref.**
SIS Panel Factory Acceptance Test Document	SI277002_RPT
Documentation and Hardware Verification Document	SI277004_RPT
SIS Test Procedure Document	SI277003_RPT
Analysis and Approval Document	SI277009_RPT
Shutdown Conditions Functional Test Document	SI277005_RPT
Process Conditions Functional Test Document	SI277007_RPT
Equipment Failure Testing Document	SI277006_RPT

Roles and Responsibilities:

Immingham Storage Ltd:

Competent person to Review Documents.

Personnel assigned to this phase: From

M.Cook – Environmental & Technical Assistant
C. Newstead – Environmental & Technical Manager
P. Jobling – Group Safety Compliance Manager
A.Dixon - Group SHE officer
A. Rhodes – Terminal Manager
S. Waterman – Terminal Engineer

Any of the above may carry out the checking.

P&I Design Ltd:

Produce Documentation and ensure that they meet the requirements of the SIS Design as well as the requirements of BS EN 61511.

Personnel assigned to this phase:

Production of Design Documentation	D.S.Regan
Development of Design	P. Potter
Review	P.J.Parkin

11.2 Post Installation

Upon Completion of the installation, commissioning and validation, all completed documentation is to be reviewed.

Roles and Responsibilities:

P&I Design Ltd competent person(s) to check the installation against the following documentation to ensure that the installation was complete and in accordance with the SIS design and that any modifications necessary were documented, reviewed and the documentation revised.

	Responsible Person(s)
SIS Panel Factory Acceptance Test	D.B. Faulkner
SIS Installation Specification	D.B. Faulkner
Shutdown Conditions Functional Test Document	D.B. Faulkner
Documentation and Verification Document	D.B. Faulkner
Process Conditions Functional Test Document	D.B. Faulkner
Analysis and Approval Document	D.B. Faulkner
Installation Approval and Inspection Document	D.B. Faulkner
Equipment Failure Testing Document	D.B. Faulkner

On completion of the installation and testing a functional safety assessment Stage 3 should be carried out to ensure the installed SIS meets the requirements of the design and BS EN 61511.

12.0 FUNCTIONAL SAFETY ASSESSMENT – STAGE 3

This assessment is to ensure that the installed SIS meets the requirement of the SRS and the design complies with BS EN 61511.

The FSA will address the following as a minimum:

- The recommendations and actions arising from the Stage 1 and 2 FSA have been resolved and completed;
- Project design change procedures are in place and properly implemented;
- The SIS is installed and pre-commissioned in accordance with the design and the SRS, any differences to be identified and resolved;
- The safety, operating, maintenance and emergency procedures pertaining to the SIS are in place;
- The employee training has been completed and appropriate information about the SIS has been provided to the maintenance and operating personnel;
- Plans or strategies for implementing further FSA's are in place;

Roles and Responsibilities:

P&I Design Ltd.

Provide an independent assessment of the SIS installation and pre-commissioning and that it meets the requirements of the design and the SRS. That it complies to BS EN 61511. Document the FSA produce an outstanding action list with competition deadlines.

D.B. Faulkner – Project Manager

Immingham Storage Ltd:

Attendance of competent personnel relevant to the required disciplines to participate in the FSA.

Personnel assigned to this phase: From

M.Cook – Environmental & Technical Assistant
P. Jobling – Group Safety Compliance Manager
A.Dixon - Group SHE officer
C. Newstead – Environmental & Technical Manager
Chris Pearson – Senior Terminal Engineer
Andy Rhodes – Terminal manager
Steve Waterman – Terminal Engineer
Alan Hall - Project Engineering Manager

Any of the above may attend.

P&I Design Ltd:

Attendance of competent personnel relevant to the design, installation and pre-commissioning of the SIS. Provide the FSA team with all necessary documentation. Update this Management of Functional Safety Document.

Personnel assigned to this phase:
M. Morgan – Project Manager
D.S.Regan – Engineer
D.R Pearson – Commissioning Engineer
D.B. Faulkner – Project Manager

Any of the above may attend.

Date of Review – Thursday 16th February 2012 at Immingham Storage Company, East Terminal.

The FSA review team:-

Immingham Storage Company East Terminal:
The FSA review team:-
Chris Newstead
Mike Cook
Alan Hall
Andrew Rhodes
Paul Jobling
Phil Dyson
Mike Plaskitt

The competency of the ISCo personnel above can be demonstrated from the individuals job description and training files as well as the Simon Storage Competency Matrix.

Dave Regan – Facilitator and Functional Safety Expert
David Faulkner – Project Manager

The competency of the P&I Design personnel is detailed in the P&I Design Ltd. quality system and described below.

David Faulkner – Project Manager
DAVID FAULKNER is a Project Manager and Commissioning Engineer of P & I Design Ltd. He has been involved in the maintenance and commissioning of Process Plants, Storage Facilities and Safety Instrumented Systems for over 20 years. His experience includes on-shore systems, including high integrity protection systems.

David Regan – SIS Designer and LOPA Team Leader
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.

13.0 OPERATION AND MAINTENANCE

13.1 Documentation Manuals

The final SIS Manuals are to be completed and issued by P&I Design Ltd to Immingham Storage Ltd to ensure that the operation and maintenance of the Safety Instrument System can be continued.

Reference Document:

Roles and Responsibilities:

Immingham Storage Ltd:

Assign competent person to manage the control of and distribution of the manuals to all relevant competent persons..

Personnel assigned to this phase

Steve Waterman – Terminal Engineer

P&I Design Ltd:

Complete final SIS manual and issue to Immingham Storage Ltd ensuring it meets the requirements of BS EN 61511.

The SIS Manual includes all manufacturer's installation and maintenance documentation along with all testing and as built documents.

Personnel assigned to this phase:

Production of Manual	D. Smith
Checking	M. Morgan

13.2 Operation and Maintenance

Immingham Storage Ltd are responsible for operating and maintaining the SIS in order that it's performance does not degrade.

Maintenance personnel must be aware that all work on the SIS must be recorded and that no unauthorised modifications are performed. All modifications must be reviewed prior to installing.

Personnel assigned to this phase

A. Rhodes – Terminal Manager
S. Waterman – Terminal Engineer

.

13.3 Training

Immingham Storage Ltd are responsible for ensuring that all personnel involved in the operation and maintenance of the facility are aware of their responsibilities and are trained in operation and maintenance with respect to the SIS.

Training is to be completed to ensure that management operators and maintenance personnel understand the following:

- 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
- Management understand the life cycle requirements BS EN 61511 relevant to the SIS

Reference Document – Training presentations

Roles and Responsibilities:

Immingham Storage Ltd:

A. Rhodes – Terminal Manager
S. Waterman – Terminal Engineer

Assign competent persons to be trained and complete training records completion.

P&I Design Ltd:

Prepare training presentation and test sheets:.

Personnel assigned to this phase:

D.R. Ransome – Consultant

13.4 Procedures

Management Procedures are to be compiled to ensure that the proof testing as required for in the Safety Instrument System Manual is carried out in accordance with the testing schedule and to ensure the record keeping of the following:

- Proof testing.
- Activation of SIS.
- Failure of SIS.
- Analysis of reliability of SIS.

The following Records are to be available after proof testing is complete

- 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.

Roles and Responsibilities:

Immingham Storage Ltd:

Assign competent persons to be responsible for the proof testing and record keeping.

Personnel assigned to this phase:

Proof Testing:

S. Waterman – Terminal Engineer

Record Keeping:

S. Waterman –Terminal Engineer

Following a period of operation, testing and maintenance:

A further FSA meeting Stage 4 should be held

14.0 FUNCTIONAL SAFETY ASSESSMENT – STAGE 4

This assessment is to ensure that SIS is performing as intended and to identify any problems in respect to operation and maintenance of the system.

The FSA will address the following as a minimum:

- The recommendations and actions arising from the Stage 1, 2 & 3 FSA have been resolved and completed;
- Review all proof testing, activation and false alarms of the SIS;
- Review any issues in operation, maintenance and proof testing of the SIS;
- Review the status of operating manuals and documentation;
- Plans or strategies for implementing further FSA's are in place;

Roles and Responsibilities:

Immingham Storage Ltd:

Attendance of competent personnel relevant to the required disciplines to participate in the FSA.

Personnel assigned to this phase:

S. Waterman – Terminal Engineer

P&I Design Ltd:

Attendance of competent personnel relevant to the design of the SIS. Provide the FSA team with all necessary documentation. Update this Management of Functional Safety Document.

Personnel assigned to this phase:

M. Morgan
D.S. Regan
P.J. Parkin

15.0 MODIFICATION

Management Procedures must include for any modifications of the Safety Instrument System. These should follow the Management of Change Procedure but should also include, that following the requirement for a modification of the SIS the following have been considered and implemented:

- Description of the modification
- Reason for the modification
- Identified hazards which may be affected
- Analysis of the impact of the modification
- Approval for the modification

Following any modification the following should be documented:

- Have all documentation affected by the modification been revised
- Have the modification been fully proof tested
- Has a detailed modification sheet been completed

Roles and Responsibilities:

Immingham Storage Ltd:

Assign competent persons to be responsible for any modification to the Safety Instrument System.

Personnel assigned to this phase to be detailed on competition of stage 4 Review.

A FSA meeting Stage 5 should be held to confirm that any modifications does not impede on the safe operation of the SIS and that the original intent is maintained.

16.0 FUNCTIONAL SAFETY ASSESSMENT – STAGE 5 MODIFICATION

This assessment is to review the changes made by a modification to ensure that the SIS is not compromised by the modification.

The FSA will address the following as a minimum:

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

Roles and Responsibilities:

Immingham Storage Ltd:

Attendance of competent personnel relevant to the required disciplines to participate in the FSA.

Personnel assigned to this phase to be detailed on completition of stage 4 Review

Design Consultant.

Attendance of competent personnel relevant to the design of the SIS. Provide the FSA team with all necessary documentation. Update this Management of Functional Safety Document.

Personnel assigned to this phase to be detailed on competition of stage 4 Review

17.0 DECOMMISSIONING

Management Procedures must include for the decommissioning of the Safety Instrument System. These should follow the Management of Change Procedure but should also include that, on decommissioning of the system have the following been considered:

- Functional safety during decommissioning
- The impact on systems interfacing with the SIS

Has a decommissioning plan been implemented and approved
Following any modification the following should be documented:

- Has all documentation affected by the modification been revised
- Has the modification been fully proof tested
- Has a detailed modification sheet been completed

Roles and Responsibilities:

Immingham Storage Ltd:

Assign competent persons to be responsible for the implementation and approval of a decommissioning plan.

Following decommissioning, assign competent person(s) to be responsible for ensuring that all documentation has been archived

Personnel assigned to this phase to be detailed at the time of de-commissioning.

18.0 FUNCTIONAL SAFETY ASSESSMENT – STAGE 5 DECOMMISSIONING

This assessment is to review the impact of decommissioning the SIS.

The FSA will address the following as a minimum:

- Review of functional safety during the decommissioning
- Review the impact of decommissioning

Roles and Responsibilities:

Immingham Storage Ltd:

Attendance of competent personnel relevant to the required disciplines to participate in the FSA.

Personnel assigned to this phase to be detailed at the time of de-commissioning.

Design Consultant.

Attendance of competent personnel relevant to the decommissioning of the SIS. Provide the FSA team with all necessary documentation. Update this Management of Functional Safety Document.

Personnel assigned to this phase to be detailed at the time of de-commissioning.

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

IMMINGHAM STORAGE COMPANY

EAST TERMINAL

GASOLINE TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

STAGE 1 FUNCTIONAL SAFETY ASSESSMENT

Rev	Date	By	Checked	Approved	Description
A	13.12.10	D.S. Regan	DRR	Client	Stage 1 FSA
B	22.02.11	D.S. Regan	DRR	Client	Updated Post Stage 1 FSA. Actions status revised
C	16.02.12	D.S. Regan	DRR	Client	Updated Post Stage 3 FSA. Actions status revised

Client Ref.

Document No.
SI277014_RPT

Contents

1.0 SCOPE

To review a risk assessment and design package for automatic overfill protection systems to the gasoline storage tanks installed at the East terminal operated by Immingham Storage Company Ltd.

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. This report has been prepared as a Functional Safety Assessment of the risk assessment and Safety Requirement Specification available in December 2010, for the project to provide overfill protection systems for Immingham Storage Co. Ltd., East Terminal.

The overall conclusion of this FSA is that the storage installation has been risk assessed see (section3.1) and the automatic overfill protection system specified to provide a defined level of functional safety. A number of detailed recommendations have been made where either relevant elements of the overall BS EN 61511 lifecycle have not yet been completed, or where improvements could be made to the information package that has been prepared to support the project.

2.0 INTRODUCTION

The storage facility is managed by Immingham Storage 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, two joint Industry/HSE bodies BSTG and PSLG have produced guidance associated with gasoline storage. The Immingham East facility is 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.

2.1 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 in ten years. (LOPA (SI157001 Rev D) calculated demand on system without SIS layer of protection = 1.92×10^{-3})

2 The information made available to the FSA is a fair and valid representation of the 'proposed' operations of the Immingham East Storage Facility and the proposals for overfill protection on the tanks. It should be noted that no gasoline is currently imported or stored at the facility.

3 The primary documents made available were the "LOPA study report (SI157001 Rev D dated 08/07/10)" and the "Safety Requirements Specification" (SI277010 Rev B dated 03/12/10) including all design specifications and drawings. Also available were the "Management of Functional Safety" and "SIS Compliance Document"

4 Mr Dave Ransome, who chaired the meeting, was involved in the hazard and risk analysis but not in the development of the Safety Requirement Specification or the design of the Safety Instrument System and will be treated as the independent competent person for the purposes of this FSA.

5 P&I Design Ltd. have previous experience with similar designs. This system design has no greater degree of complexity than any of the other designs. There is no greater degree of novelty of design or of the technology used and standardisation of design features from previous systems can be well demonstrated.

2.2 Team Membership

The FSA review team was:-

Date of Review – Thursday 9th December 2010 at Immingham Storage East

Immingham Storage
Andy Rhodes - Terminal Manager
Paul Jobling - Group Safety Compliance Manager
Steve Waterman - Plant Engineer
Alan Hall - Project Engineering Manager

The competency of the personnel above can be demonstrated from the individual's job description and training files. The required knowledge of the operational requirements and the possible risks associated with the operation can be readily demonstrated by Immingham Storage.

P&I Design Ltd
Dave Ransome – Competent Safety Consultant
Dave Regan – SIS Designer

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

2.3 Competency

Functional Safety Management is to be addressed with the intent to improve the defined competency of the Immingham Storage personnel.

Functional Matrix to be reviewed and produced by Immingham Storage to link job titles to named individuals for the Management of Functional Safety Document.

The Management of Functional Safety Document to be updated to show Immingham Storage personnel for all phases.

2.4 Definitions and Abbreviations

The following details the definitions and abbreviations used in this document.

AICHE	American Institute of Chemical Engineers
BPCS	Basic Process Control
BSTG	Buncefield Standards Task Group
E/E/PE	Electrical Electronic and Programmable Electronic
ESD	Emergency Shutdown
FSA	Functional Safety Assessment
HMI	Human Machine Interface
HSE	Health and Safety Executive
LOPA	Layers of Protection Analysis
MTBF	Mean Time Between Failures
OPRT	Overfill Protection Regulatory Team
PLC	Programmable Logic Controller
PSLG	Process Safety Leadership Group
PFD	Probability of Failing on Demand
PSLG	Process Safety Leadership Group
SIF	Safety instrumented function – An E/E/PE 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
SRS	Safety Requirement Specification
TSA	Tank Storage Association
UKPIA	United Kingdom Petroleum Industry Association

3.0 FUNCTIONAL SAFETY ASSESSMENT

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 a stage 1 Functional Safety Assessment.

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

The hazards and hazardous events of the process and associated equipment were determined in a LOPA review (Reference SI057001.RPT). The LOPA study was based on the principles in the AICHE book, BS EN 61511 part 3 and the BSTG Guidelines. The sequence of events leading to the hazardous event were also determined in the LOPA review and process risks were estimated.

It was noted that the site does not operate with gasoline. The original LOPA produced an estimated throughput and storage capability and this FSA reviewed the intent of the LOPA against the new Safety Requirement Specification.

Following the issue of the PSLG guidelines on LOPA, it was decided that there was no point in revisiting the LOPA and revising it in accordance with PSLG, as it would not be possible to provide the data in sufficient detail as the facility currently does not store gasoline. However, as part of a terminal upgrade in overfill protection, it was decided to design, procure and install all instrument equipment/items on their ability to demonstrate suitability for a SIL2 system design.

A number of issues have been notified by the Competent Authority as necessary in any new or revised LOPA and will need to be addressed as follows:

- Domino effects have been not been examined. Onsite and Offsite domino effects could lead to an expansion of a possible fire or to an environmental release.
- A full assessment of Environmental risk was not carried out
- A plan view showing the 250m and 400m radii from the gasoline tanks was not included.
- Weather data was not included.

The original LOPA Review concluded that a revised Independent Protection Layer, was required to provide a mid-range SIL1 Safety Instrumented Function. This will be designed and installed to ensure that import fail safe actuated valves will close on initiation of any of 10 tank high high level switches. Two techniques will be used, the first utilising a weighted mechanical switch for floating deck roof tanks, the second a vibronics level switch for fixed roof tanks. The logic solver and final elements being similar for both systems.

Since the LOPA was originally carried out, the tanks that would possibly be used for gasoline storage, in the future, have been reviewed and the number of possible tanks increased to a total of 20 tanks.

The FSA discussed the original LOPA and confirmed that the SIF derived from high high level in a storage tank to close the inlet to the storage tank would be implemented with an integrity requirement of SIL2. Also, that a further LOPA study would be conducted, prior to utilising the facility for gasoline, in order that adequate protection could be confirmed.

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

The Safety Requirement Specification (SI277010_RPT rev B 03/12/10) was reviewed with the following points noted.

The Safety Requirement Specification has allowed for a mid-range IPL SIL2 SIF, which would close new tank-side import fail safe actuated valves for 600 Series tanks 601, 602 & 603 on activation of the gasoline tank high high level switch and common pipeline import fail safe actuated valves which will close on activation of any one of No. 4 East tanks 552, 553, 554, 557, 558, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572. This modification to include the provision of new instrumentation designed and installed to provide the required PFD. See Safety Requirements Specification SI277010_RPT

A paragraph should be added to the SRS regarding other possible routes.
"There are also 2 other possible jetty routes that could feed to the tanks. East Jetty 14" Bridge Line and JP24 Jetty Import Line. The East Jetty line will be locked at the 600 hose exchange and will only be connected under management control. JP24 Jetty line is unused at present and terminates adjacent to tank 566."

Operation of reset facility was discussed, it was reiterated that the activation of a high high switch on any of the No 4 East Tanks would lead to all four of the common import valves closing and that they would not be able to be opened until the high high level was cleared and the Safety Instrument Function reset. It was recognised that whilst this was not ideal for operational purposes, the design is to allow for individual tank side valves for the future.

Lack of any over-ride facility was discussed, it was reiterated that no over-ride facilities are available and that operational procedures to bypass the import valves are unavailable. For a level transmitter fault the fault would have to be corrected before any of the common import valves could be opened. On activation of a high high level, the high high level must be cleared and the system reset before any of the common import valves could be opened.

For the Series 600 tanks the method of clearing any high high level was discussed and ISCo confirmed that this would be done, under full management control, by the temporary installation of a fixed spool (or hose) around the tankside import/export valve.

The SRS detailed that the valves would be opened and closed on each batch. Immingham Storage Management considered it was not practical to cycle the common import valves before each import operation and an auditable maintenance and testing procedure will be put in place by Immingham Storage to test the operation of each valve monthly. This will confirm that the valve is operational and the limit switches correctly prove the valve open and closed. It was stated that the basis of design was a 1oo1 system based on partial stroke testing. If ISCo feel that this cannot be managed then system redundancy will need to be reconsidered.

System checks after operation were discussed, it will be necessary to incorporate new auditable actions in the operating procedures to ensure that on activation of the SIS, the import from ship or pipeline is immediately stopped. It will also be necessary to check that the correct valves have closed, and flow has ceased as required by the Safety Instrument System

The Safety Requirement specification states that the final element is arranged as a 1oo1 system even though there are four possible import routes. This was discussed and the FSA team were assured that due to the import and manifold arrangements, it was not possible to utilise more than one import line to a tank simultaneously.

The requirements for diagnostics was discussed and it was confirmed that the proposed Endress and Hauser vibronics level switches to be installed on the No. 4 Series tanks can be considered analogue devices with diagnostics. No diagnostics are available from the magnetrol level switches which will be installed on the Series 600 tanks.

There were a number of issues on the current volumes and high high switch setpoints to be used for Safety Instrument System Design. Immingham Storage are to provide information for level switch settings on all tanks in the SIS.

It was confirmed that the Safety Instrument System will be hardwired logic system utilising analogue and digital switches and safety relays.

The proof testing philosophy was discussed and it was confirmed that the functional test will be an end to end test with a simulated high high level derived from the level switch. The switches cannot be fixed in the override position.

It was confirmed that there was no requirement for any additional SIFs to support abnormal modes of operation (Start-up, maintenance, testing etc.)

The Compliance Documentation will be completed up to stage 1

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

The project design procedures are in place and an audit trail is available for the lifecycle of the system. At this FSA the documentation was at the following revisions.

LOPA Study	SI057001_RPT	D (08/07/10)
SIS Safety Requirements Specification	SI277010_RPT	B (03/12/10)
SIS Management of Functional Safety	SI277102_RPT	A (09/12/10)
SIS Compliance Document	SI277101_RPT	B (27/11/10)

Safety Instrument System Design package is to be reviewed at FSA Stage 2/3.

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

No formal functional Safety Assessments have previously been carried out.

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

To be confirmed by an FSA Stage 3

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

To be confirmed by an FSA Stage 3

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

To be confirmed by an FSA Stage 3

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

To be confirmed by an FSA Stage 4

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

The next functional safety Assessment will be carried out a Stage 3.

3.10 Compliance to BS EN 61511

As part of the SIS reviews, and included as part of this FSA, a checklist has been produced to confirm that all the relevant clauses from the standard have been complied with. See Document SI277101_RPT – Compliance Document.

4.0 CONCLUSIONS

The overall conclusion of this FSA is that the storage installation had been risk assessed and the automatic overfill protection system specified to provide an appropriate level of functional safety. A further LOPA along the PSLG guidelines will need to be conducted prior to any change of use to allow gasoline storage. A number of detailed recommendations have been made where either relevant elements of the overall BS EN 61511 lifecycle have not yet been completed, or where improvements could be made to the information package that has been prepared to support the project.

Comments noted above will be incorporated Safety Requirement Specification and the system will be revised to Stage 1 FSA Status.

Actions, listed below, arising from this FSA will be completed within 2 weeks

Action	By	Expected Completion	Completion Date
1. Modify SRS as discussed in the FSA	DSR	21/12/10	21/12/10
2. Confirm level switch lengths and high high level activation point for all tanks.	SW	21/12/10	04/05/11
3. Complete Compliance Document up to FSA Stage 1.	DSR	21/12/10	21/12/10
4. FSA, Compliance Document, Management of Functional safety, SRS & LOPA to be issued to Immingham Storage	DSR	21/12/10	21/12/10
5. Review and Modify LOPA in line with PSLG guidelines.	ISCo/P&I Design Ltd.	Prior to any Gasoline Storage on site	31/08/11

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

IMMINGHAM STORAGE CO LTD

EAST TERMINAL

GASOLINE STORAGE TANKS OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

FUNCTIONAL SAFETY ASSESSMENT

STAGE 2/3

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	16.02.12	D S Regan	D.B.Faulkner	Client	Original Issue	
B	16.04.12	D S Regan	D.B.Faulkner	Client	Following Client Comments	
C	28.03.13	D S Regan	D.B.Faulkner	Client	Action Status Updated	Document No. SI277016_RPT
D	25.04.13	M.Morgan	D.B.Faulkner	Client	Action Status Updated	

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

Appendices

Not Included at Revision D

1 REVISION HISTORY

Rev	Description
A	Original Issue
B	Following Client Comments Typographical errors corrected (pages 5, 6 & 8). References to levels in tanks for PL1 in section 4.1 removed References to SCADA removed Times from high high level switch activation to overfill added in section 4.1 Comment regarding LOPA corrected to *"HSE have reviewed the LOPA and accepted the requirement for a SIL 2 protection system. See letter from HSE regarding COMAH; 3rd November 2011."* Reference to SIS design document SI277001_RPT added on page 19
C	Page 15 – MTTR corrected to 72 hours Action status updated
D	Action 17 completed

2 SCOPE

Immingham Storage Company East Terminal have installed Independent High Level Shutdown systems to provide SIL 2 rated automatic shutdown systems to prevent gasoline storage tank overfills.

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.

This report has been prepared as a Functional Safety Assessment Stage 2/3 "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". A previous assessment at stage 1 has been completed. Reference document SI277014_RPT Revision C.

3 INTRODUCTION

The fuel storage depot is owned and managed by Immingham Storage Company 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 Immingham East terminal is 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 Immingham Storage Company East 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.

3.2 Team Membership

Date of Review – Thursday 16th February 2012 at Immingham Storage Company, East Terminal.

The FSA review team:-

Immingham Storage Company East Terminal:
The FSA review team:-
Chris Newstead
Mike Cook
Alan Hall
Andrew Rhodes
Paul Jobling
Phil Dyson
Mike Plaskitt

The competency of the ISCo personnel above can be demonstrated from the individuals job description and training files as well as the Simon Storage Competency Matrix.

Dave Regan – Facilitator and Functional Safety Expert
David Faulkner – Project Manager

The competency of the P&I Design personnel is detailed in the P&I Design Ltd. quality system and described below.

David Faulkner – Project Manager
DAVID FAULKNER is a Project Manager and Commissioning Engineer of P & I Design Ltd. He has been involved in the maintenance and commissioning of Process Plants, Storage Facilities and Safety Instrumented Systems for over 20 years. His experience includes on-shore systems, including high integrity protection systems.

David Regan – SIS Designer and LOPA Team Leader
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.

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 2/3 Functional Safety Assessment.

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, a Stage 1 FSA has been conducted. During the FSA it was agreed that the existing LOPA would be updated when gasoline storage was due to commence.

An updated LOPA Review has been produced by Immingham Storage Company East and updated following the guidelines of PSLG.

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 Immingham Storage Company East and P&I Design Ltd. personnel each with different roles and responsibilities,
  - The LOPA report – SI057001_RPT, Revision F - Dated 31/08/11, is available and it has been updated following the revised requirements for LOPA by the HSE, and after the issue of the PSLG final report.

- The following sequence of events leading to the following hazardous events were considered from ship imports and tank to tank transfers

    - Overfill of gasoline tank during import from a ship leading to a potential open vapour cloud explosion

    - Overfill of gasoline tank during import from a ship leading to a potential flash fire.

    - Overfill of gasoline tank during import from a ship leading to a potential open vapour cloud explosion, fire with significant smoke; together with a release to the River Humber corresponding to a potential short-term major environmental consequence to the River Humber which could constitute a threat to the environment. This might constitute a short-term MATTE, subject to the volume, components and duration of the release actually reaching the river.

- the following Initiating Events were identified:

Overfill of a gasoline storage tank

- IE1 Whilst importing from a ship, overfill of Gasoline Tank due to incorrect line up.
- IE2 Whilst importing from a ship, overfill of Gasoline Tank with correct line up due to the capacity of the tank being less than expected.
- IE3 Failure of Level Instrument on the Gasoline Tank. Radar gauge reads low.

- The LOPA considered the requirement for Instrumented Protection and Mitigation Layers with the following being identified:

Protection Layer 1
BPCS with Level Indication and alarms monitored by Operator
A VTW (Virtual Tank for Windows) system enables the operator to view the tank levels. The normal fill level and high alarms are software derived from the VTW. The alarms are audible within the control room and transmitted by radio.

Protection Layer 2
High High Level alarm and automatic closure of import valve Mid-Range SIL 2 SIS
The protection layer will be auditable via the SIS maintenance and testing records. This consists of an independent high high level switch using a different measurement technology from the ATG (Automatic Tank Gauging) system**,** operating through a hard wired and independent electronic protection system to close remotely operated shut off valves that will shut off a tank side valve. The valve will close quickly, at a speed commensurate with any surge constraints in the pipelines.

LOPA study Results

Scenario 1 - Overfill of gasoline tank during import from a ship leading to a potential open vapour cloud explosion causing up to 3 on-site fatalities and up to 6 off-site fatalities.

Risk Tolerance Criteria = 1.0×10^{-6} per year

Frequency of Mitigated Consequence = 7.58×10^{-7} per year

The risk tolerance criteria is within the Broadly Acceptable region for up to 10 fatalities (Table 2 - Tolerable Risk Criteria). The frequency of Mitigated Consequence with a mid-range SIL 2 SIS is well within the "Broadly Acceptable" region.

Scenario 2 - Overfill of gasoline tank during import from a ship leading to a potential flash fire causing up to 1 on-site fatality and no off-site fatalities.

Risk Tolerance Criteria = 1.0×10^{-5} per year

Frequency of Mitigated Consequence = 8.81×10^{-7} per year

The risk tolerance criteria is within the Broadly Acceptable region for up to 1 fatality (Table 2 - Tolerable Risk Criteria). The frequency of Mitigated Consequence with a mid-range SIL 2 SIS is well within the "Broadly Acceptable" region.

Scenario 3 - Overfill of gasoline tank during import from a ship leading to a potential open vapour cloud explosion and a release to the River Humber corresponding to a potential short-term major environmental consequence to the River Humber which could constitute a threat to the environment. (Consistent with Table 4 - Environmental Tolerable Risk Frequency).

Risk Tolerance Criteria = 1.0×10^{-6} per year

Frequency of Mitigated Consequence = 6.06×10^{-7} per year

The risk tolerance criteria is within the Acceptable region for a severe environmental consequence (Table 4 - Environmental Tolerable Risk Frequency). The frequency of Mitigated Consequence with a mid-range SIL 2 SIS is well within the "Broadly Acceptable" region.

The envelope that the LOPA was based on has not changed.

HSE have reviewed the LOPA and accepted the requirement for a SIL 2 protection system. See letter from HSE regarding COMAH; 3rd November 2011.

The operational basis of the LOPA was confirmed at the FSA.

Sections from the LOPA was discussed.

"The number of people on-site within the 250m zone is stated as 10 during the day and 3 on the night. Off-site personnel within the 250m zone has been stated, typically as 20 during the day and 0 on a night time (see Appendix 5). A worst case of Off-site personnel of 35 during the day and 20 during the night is quoted, however the night time case has been discussed as being drivers arriving and leaving overnight and it is considered likely that no more than 6 will be within the 250m zone at any one time"

It was considered that the number of people on-site should be stated as typically up to 20-30 during the day and unchanged overnight.

In section 4.1.2,

Information has been supplied from the Competent authority which states that:
For fire / un-ignited events
Concrete or earth bunds, PFD = 0.1 (this may increase, e.g. to 0.25 if the bund is not upgraded due to the operator demonstrating it meets requirements SFAIRP – e.g. if it includes a gravity drain system)
Tertiary containment = 0.1
Thus the maximum credit claimed by operators for fully upgraded secondary and independent tertiary containment is a combined PFD of 0.01 for un-ignited and fire scenarios.

It was discussed that no tertiary containment was available. In the LOPA no credit has been taken for the Environmental case, Scenario 3.

The operating procedures were discussed and it was confirmed that the independent checks were auditable and that the actuated import valves were being tested regularly and stroked closed/open prior to operational use.

Section 5.1.2

"For ship imports, the pumps are under the control of the ship. Simon operational procedures are that all import operations are stopped on any high level alarm. The jetty operator can stop the import by instructing the ship to stop pumping or by closing the jetty manual valve. The jetty operator can also set off the fire alarm using the site phone system which will close the jetty line actuated import valves. Radio communications are constant between the ship and Simon Operations"

It was noted that the jetty line actuated import lines will not close on activation the fire alarm. However, the actuated tank import valves will close.

ATG Alarms via VTW System
Topping Off Alert (Facility available, % to be set 60 minutes from predicted finish time)
Normal Fill Level Alert (Set at 95% at present)
High Level Alarm (Set at 96% at present)
The normal fill level alert and high alarms are purely audible alarms within the control room and transmitted through the radio system.

It was confirmed:
The TOA is set at 60 minutes from predicted finish time.
Normal Fill Level Alert (Set at 95%).
High Level Alarm (Set at 96%).

There is an independent high high level switch and shutdown system which closes the Automated Shutdown valve on the receiving tank inlet. The activation of the switch is transmitted to a control room annunciator and repeated to the radio system. (Set at 97% at present)

It was confirmed that the high high level switch activation point is 97%
(For tank 561 = 6931mm, time to overfill after high high level activated: 5.4 minutes)
(For tank 564 = 8682mm, time to overfill after high high level activated: 9.9 minutes)
(For tank 568 = 8662mm, time to overfill after high high level activated: 9.9 minutes)

Section 2.2.

"The above were achieved with the following:
A mid-range SIL2 protection layer which would close the two common jetty pipeline fail-safe actuated valves (as well as the two common APT pipeline valves) on initiation of any tank's high high level switch. This protection layer has been installed and commissioned and full SIS documentation is available. The actual credit available from the SIS is calculated as: 2.5 x 10^{-3}. See SIS Design Report SI277001_RPT. The protection layer is auditable via the SIS maintenance and testing records."

It was discussed that the 4 pipeline valves are no longer used for the SIL 2 Protection layer as tank-side import valves have been installed on tanks 561 and 564 and will be installed on tank 568. This will need to be reflected on the sketch in Appendix 8 of the LOPA.

It was queried whether PL2, the SIL2 system, was applicable for Initiating event 1. To be investigated. (for all scenarios)

The operational basis of the LOPA was confirmed at the FSA. It was recommended that the above comments be incorporated in the next revision of the LOPA. This is likely to be when the COMAH report is updated. (Action 1, expected in 2012)

4.2 Suitability of the Proposed Protection Layer

The purpose of the SIL 2 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 a vapour cloud explosion.

This is achieved by use of independent, to the normal tank level measurement, magnetic or vibronic switch level instruments. A logic solver provides monitoring of this level and on reaching a predefined value will initiate the closure of valves independent of the process control. These valves are under the control of Immingham Storage Company, East and not of the supplier (ship).

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, for example had it been located in an external pot or chamber where the change in level may not fully reflect the change of state in the tank.

Operation against ships pressure and flow was raised in the FSA i.e. have the valves been operated against full ship pressure and flow to check the operation and effects of any surge on the pipeline and the ship. Surge calculations have been carried out for the terminal, for lines JP27 and JP33, and are available. Surge Calculations to be supplied and reference appended. Calculations to be based on $500m^3$/hr. (Action 2)

At the FSA it was indicated that the surge calculations show that a valve closure time of less than 60 seconds could lead to dangerous surge conditions. The actual valve closure times are approx. 120 seconds from trip. SRS and SIS Design to be updated to reflect valve closure times. (Action 3)

Process conditions testing has not been formally carried out.

4.3 Have the recommendations arising from the hazard and risk assessment that apply to the safety instrumented system 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, which covers all the tanks used for Gasoline storage SI277010_RPT Revision D, 22/02/11.

The Stage 2/3 FSA reviewed the SRS and it was required that the SRS be updated to reflect that the 4 common pipeline valves will not be used in the Safety Instrumented System. (Action 4)

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

The SRS details the requirements of the SIF from an instrumentation point. Additional information should be included regarding functional safety. This includes closure times of the valves and ullage available etc.

The SRS is written for all tanks used for the storage of gasoline

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

There is reference to common cause failure in the SRS. The system is a 1oo1 and common cause failure may not be applicable.

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

The SRS details the fails safe state of the SIF.

- 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);

The SRS details the individually safe process state of the SIF.

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

The SRS details the demand and demand rate.

- requirement for proof-test intervals;

The SRS details the proof test interval

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

The SRS details the response time to bring the process to a safe state

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

The SRS details the mode of operation.

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

The SRS contains a description of the SIS process measurements and their trip points.

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

The SRS contains a description of the SIS process output actions and criteria for successful operation.

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

The SRS contains a description of the functional relationships between process inputs and outputs.

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

The SRS contains a description of the requirements to de-energise to trip

- requirements for resetting the SIS after a shutdown;

The SRS contains a description of the requirements for reset after a shutdown.

- maximum allowable spurious trip rate;

The SRS contains a comment that the allowable spurious trip rate will be approved by Immingham Storage Company East after the spurious trip calculations are complete

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

The SRS contains the failure modes and desired response of the SIS

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

The SRS contains a description of the requirements for reset after a shutdown. There are no specific requirements for start-up and shutdown of the SIS.

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

The SRS contains details of interfaces between the SIS and the BPCS

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

There is only a single mode of operation of the plant and the SRS reflects this.

- the application software safety requirements as listed in 12.2.2;

There is no requirement for any software as the logic solver consists of individual solid state relay logic.

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

The valves are dedicated as an import valves; therefore there is no requirement to override the SIFs.

- 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;

The system is designed to fail safe on any fault being detected in the SIS. No reset would be available.

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

Mean time to repair shall be 72 hours or less. Immingham Storage Company East to approve following consideration of availability of spares and labour.

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

There are no conceivable individually safe process states which, when occurring concurrently, can create a separate hazard.

- 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;

Referenced in SRS:

This system will be installed in mainland UK where it will not be subjected to extremes of temperature or humidity. We do not consider that *grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock, vibration, electrostatic discharge, flooding or lightning* will have a detrimental effect on the SIS. The system is designed to fail safe on any loss of electrical power. 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 Spirit.

- 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;

There is only a single mode of operation of the plant and the SRS reflects this.

- 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 SRS references valves being designed as fire-safe. No additional reference is made

Valves, actuators and solenoid valve specifications required. (Action 5).

4.4 Are project Design Change Procedures in place and been properly implemented?

Design changes appear to have been conducted but no formal SIS change procedure is referenced. Immingham Storage Company East to confirm how they will provide management of change now the system is operational. All documents carry unique document numbers.

Management of change procedures to be updated to include for the requirements of BS EN 61511. (Action 6)

4.5 Have the recommendations arising from the previous functional safety assessment been resolved?

Yes, See FSA Stage 1 SI277014_RPT

It was noted that the date of the action completions were not as per the date of the document revisions. There should be some cross-referencing. (Action 7)

4.6 Is the Safety Instrument System designed in accordance with the safety requirement specification, any differences having been identified and resolved?

Stage 2 – Safety Instrument Design **Checklist 2 - General**			
BS EN 61511 Clause	Description	Checklist Yes-No-N/A	Comments and References
5	Are design documents within a formal revision and control process.	Yes	System documentation and manuals
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	Add calculated PFD and refer back to LOPA (Action 1)
	Has nuisance tripping being considered.	No	To be confirmed as acceptable. The figure acceptable for the terminal is 1 spurious trip every 10 years
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	
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.	No	
11.2.3	If SIF's with different SIL share the same hardware or software does it comply to the highest safety level.	Yes	
11.2.4	Is the design of the BPCS to BS EN 61511. If answer is no then:	No	Maintenance and testing records for the BPCS to be confirmed. Manual dips monthly. Records etc. (Action 8)
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 affect the operation of the SIS.	No	
11.2.5	Are there any bypass systems provided and if so are their operating procedures well documented	No	Bypass arrangements can be provided under management procedures.
11.2.5	Have testing procedures been developed.	Yes	Testing documentation will be used and completed.
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	Reset pushbutton is installed on the SIS panel.
11.2.8	Is there a manual means of initiating the SIF e.g ESD pushbutton.	Yes	ESD systems shutdown the SIS.
11.2.11	Is the system designed as fail safe on loss of power or nitrogen. If the answer is no then: Is loss detected Is there back up supply to ensure system operation.	Yes	
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	MTTR has been assumed as 72 hrs. Spares are available for panel equipment and a critical spares list exists. The system is operated such that no tank will normally be used for import unless the SIS is operational or under management procedures.
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	Level Switch and relay have full data to BS EN 61508. Some valves and actuators are proven in use. Site procedures include the recording of data. Data recording to be formalised. (Action 9)
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.	?	Magnetrol – Yes E&H Level Switch - Yes Pilz – No Valve – No Actuator – No SOV – No Testing procedures have been developed to ensure the individual equipment and system are tested annually.
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	All field equipment is Type A except for the Liquiphant and Nivotester, however, no adjustment of the instrument settings is available.
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 Yes Yes Yes Yes Yes Yes Yes Yes Yes	No Problems with freezing in air system during last winter with significant low ambient temperatures. Dessiccant dryers. Condensation in the enclosures of the magnetrol level switches which may lead to failure of the switch. Condensation and water in the enclosures of the E&H level switches which may lead to failure of the switch.
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 Yes Yes Yes	See above for surge calculation details.
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 Yes No Yes N/A No No	 On Annunciator and on SIS panel On/Off state Permit only management procedures On Annunciator and on SIS panel Fail closed on loss of power or air. No effective diagnostics - simple system
4.4	11.7.3	Can communication failures have an adverse effect on the SIS.	No	
4.5	11.7.3	Are communication signals isolated from other energy sources.	N/A	

Safety Instrument System Design Document: SI277001_RPT, revision C was reviewed at this FSA.

The design documentation was not reviewed at FSA stage 2/3.

Live Design documentation on the server to be confirmed. (Action 10)

4.7 Is the Safety Instrument System, constructed and installed in accordance with the safety requirement specification, any differences having been identified and resolved?

At the FSA stage 3 carried out on 9th February 2012 at Immingham Storage Company East.

As part of the FSA, a site inspection was not carried out to ensure that the installation was still maintained to the required standard. A separate inspection will be carried out and a separate report will be appended to this document. (Action 11)

It is confirmed that the installation reflects the SRS and SIL assessment documentation as discussed above.

The SIS has been designed, installed and validated by P&I Design Ltd. and Immingham Storage Company East.

Modification Report SI277001_RPT (TANK-SIDE VALVES ADDED TO T561, T564 & T568) was reviewed during the FSA and it was confirmed that no Stage 5 FSA was required as there was no detrimental effect on functional safety caused by this modification. The modification report is to be completed and updated following completion of this modification. The report will be used as a control document to ensure that all relevant documentation is updated.

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	Yes	
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	No	
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	No	
6.6	13.2.6	Is there any requirement for a re-test	Yes	See documentation
6.7	13.2.6	For any retest, state what has been retested		See documentation

The SIS had a separate FAT procedure and these have all been completed and documented.

The Factory Acceptance Tests were not reviewed at FSA stage 2/3.

The systems are installed and operational, and the completed FATs and SATs are available in the SIS manuals.

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	No effective method for this system.
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 Nitrogen 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	Yes	See documentation

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 Yes N/A Yes Yes Yes Yes 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	To be updated
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 nitrogen	 N/A 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 Yes	Documentation required. (Action 12)
8.6	15.2.4	Does the SAT testing include external interfaces: BPCS Annunciation Diagnostics	 No Yes Yes	
8.7	15.2.4	Have the following been checked for correct operation: Reset Bypass facilities Start up overrides	 Yes N/A N/A	
8.8	15.2.4	Following the SAT have: All test results been recorded	Yes	561 & 564 at present
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	

The Site Acceptance Tests was reviewed at FSA stage 2/3.

Some systems are installed and operational, and the completed SATs are available in the SIS manuals. Not available on the server. To be input to electronic data system (Action 13)

Drawings:

Drawing Number	Rev	Title
SI277001_DWG	F	Cable Overview – Import Valves & System Comms
SI277002_DWG	E	Cable Overview – Bunds L, M & O
SI277003_DWG	E	Cable Overview – Bunds G, H, I & J
SI277004_DWG	E	Cable Overview – Bunds R & T
Logic Drawings		
SI277010_DWG	F	SIS Monitoring Panel Logic Drawing 1
SI277011_DWG	F	SIS Monitoring Panel Logic Drawing 2
SI277012_DWG	F	SIS Monitoring Panel Logic Drawing 3
SI277013_DWG	E	SIS Monitoring Panel Logic Drawing 4
SI277014_DWG	F	SIS Monitoring Panel Logic Drawing 5
SI277015_DWG	F	SIS Monitoring Panel Logic Drawing 6
SI277016_DWG	F	SIS Monitoring Panel Logic Drawing 7
SI277017_DWG	F	SIS Monitoring Panel Logic Drawing 8
SI277018_DWG	E	SIS Monitoring Panel Logic Drawing 9
SI277019_DWG	E	SIS Monitoring Panel Logic Drawing 10
SI277020_DWG	F	SIS Monitoring Panel Logic Drawing 11
SI277021_DWG	F	SIS Monitoring Panel Logic Drawing 12
SI277022_DWG	F	SIS Monitoring Panel Logic Drawing 13
SI277023_DWG	F	SIS Monitoring Panel Logic Drawing 14
SI277024_DWG	F	SIS Monitoring Panel Logic Drawing 15
SI277028_DWG	F	SIS Monitoring Panel External Layout
SI277029_DWG	F	SIS Monitoring Panel Internal Layout
Junction Box Connection Drawings		
SI277030_DWG	B	JB4_80 Valve Control Junction Box Connection Details
SI277031_DWG	D	JB4_81 Valve Control Junction Box Connection Details
SI277032_DWG	D	JB4_82 Valve Control Junction Box Connection Details
SI277033_DWG	C	JB4_83 Valve Control Junction Box Connection Details

Loop Sheets

SI277050_DWG	A	Tank 552 HiHi Level Switch Loop Sheet
SI277051_DWG	A	Tank 553 HiHi Level Switch Loop Sheet
SI277052_DWG	A	Tank 554 HiHi Level Switch Loop Sheet
SI277053_DWG	A	Tank 557 HiHi Level Switch Loop Sheet
SI277054_DWG	A	Tank 558 HiHi Level Switch Loop Sheet
SI277055_DWG	A	Tank 561 HiHi Level Switch Loop Sheet
SI277056_DWG	A	Tank 562 HiHi Level Switch Loop Sheet
SI277057_DWG	A	Tank 563 HiHi Level Switch Loop Sheet
SI277058_DWG	A	Tank 564 HiHi Level Switch Loop Sheet
SI277059_DWG	A	Tank 565 HiHi Level Switch Loop Sheet
SI277060_DWG	A	Tank 566 HiHi Level Switch Loop Sheet
SI277061_DWG	A	Tank 567 HiHi Level Switch Loop Sheet
SI277062_DWG	A	Tank 568 HiHi Level Switch Loop Sheet
SI277063_DWG	A	Tank 569 HiHi Level Switch Loop Sheet
SI277064_DWG	A	Tank 570 HiHi Level Switch Loop Sheet
SI277065_DWG	A	Tank 571 HiHi Level Switch Loop Sheet
SI277066_DWG	A	Tank 572 HiHi Level Switch Loop Sheet
SI277067_DWG	B	Tank 601 HiHi Level Switch Loop Sheet
SI277068_DWG	B	Tank 602 HiHi Level Switch Loop Sheet
SI277069_DWG	B	Tank 603 HiHi Level Switch Loop Sheet
SI277101_DWG	A	XV10001 APT10 Pipeline Valve Loop Sheet
SI277102_DWG	A	XV10002 APT12 Pipeline Valve Loop Sheet
SI277103_DWG	A	XV10003 APT24 Pipeline Valve Loop Sheet
SI277104_DWG	A	XV10004 Jetty Pipeline Valve Loop Sheet
SI277105_DWG	A	XV55301 Tank 553 Import/Export Valve Loop Sheet
SI277106_DWG	A	XV55401 Tank 554 Import/Export Valve Loop Sheet
SI277107_DWG	A	XV55701 Tank 557 Import/Export Valve Loop Sheet
SI277108_DWG	A	XV55801 Tank 558 Import/Export Valve Loop Sheet
SI277109_DWG	A	XV56301 Tank 563 Import/Export Valve Loop Sheet
SI277111_DWG	A	XV56401 Tank 564 Import/Export Valve Loop Sheet
SI277112_DWG	A	XV56601 Tank 566 Import/Export Valve Loop Sheet
SI277113_DWG	A	XV56602 Tank 566 Import/Export Valve Loop Sheet
SI277114_DWG	A	XV56701 Tank 567 Import/Export Valve Loop Sheet
SI277115_DWG	A	XV56801 Tank 568 Import/Export Valve Loop Sheet
SI277116_DWG	A	XV56901 Tank 569 Import/Export Valve Loop Sheet
SI277117_DWG	A	XV57001 Tank 570 Import/Export Valve Loop Sheet
SI277118_DWG	A	XV57101 Tank 571 Import/Export Valve Loop Sheet
SI277119_DWG	A	XV57201 Tank 572 Import/Export Valve Loop Sheet
SI277120_DWG	A	XV60101 Tank 601 Import/Export Valve Loop Sheet
SI277121_DWG	A	XV60102 Tank 601 Import/Export Valve Loop Sheet
SI277120_DWG	A	XV60101 Tank 601 Import/Export Valve Loop Sheet
SI277121_DWG	A	XV60102 Tank 601 Import/Export Valve Loop Sheet
SI277122_DWG	A	XV60201 Tank 602 Import/Export Valve Loop Sheet
SI277123_DWG	A	XV60202 Tank 602 Import/Export Valve Loop Sheet
SI277124_DWG	A	XV60301 Tank 603 Import/Export Valve Loop Sheet
SI277125_DWG	A	XV60302 Tank 603 Import/Export Valve Loop Sheet

Schedules

SI277001_SCH	D	Tank Overfill SIS Cable Schedule
SI277005_SCH	B	JB/84 Tank Level Switch J/B Connection Schedule
SI277006_SCH	B	JB/85 Tank Level Switch J/B Connection Schedule
SI277007_SCH	D	JB/86 Tank Level Switch J/B Connection Schedule
SI277008_SCH	C	JB/87 Tank Level Switch J/B Connection Schedule
SI277009_SCH	D	JB/88 Tank Level Switch J/B Connection Schedule
SI277010_SCH	D	JB/89 Tank Level Switch J/B Connection Schedule

Reports:

Report Number	Title	No of Sheets	Revision
SI277001_RPT	Safety Instrument System Design Document	55	C
SI277002_RPT	SIS Factory Acceptance Test Procedure	29	B
SI277003_RPT	SIS Test Procedure	7	B
SI277004_RPT	SIS Documentation and Hardware Verification	20	B
SI277005_RPT	SIS Shutdown Condition Functional Test Procedure	41	B
SI277007_RPT	SIS Final Element Functional Test Procedure	22	B
SI277009_RPT	SIS Analysis and Approval Document	13	B
SI277010_RPT	Safety Requirement Specification	26	C
SI277101_RPT	SIS Compliance Document	14	B
SI277102_RPT	SIS Management of Functional Safety	22	A

Documents now issued with new SIS manuals, missing from this system
SIS Installation Specification Acceptance Procedure (Completed as part of first SAT)
SIS Equipment Failure Functional Test Procedure (See new FAT Procedure)

Confirm the design documentation above is at correct revision with electronic data system. (Action 14)

4.8 Are the safety, operating, maintenance and emergency procedures pertaining to the safety instrument system in place?

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		To be confirmed. (Action 13)
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	Operator awareness and familiarisation training completed and will be documented. Management have been trained. Operator SIS training on-going. (Complete end 2012)
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 Yes Yes No No	 Dangerous occurrence To be confirmed To be confirmed (Action 9)
9.4	16.2.7	Do management understand the life cycle requirements of BS EN 61511 relevant to the SIS	Yes	Management have been trained

The above were reviewed and discussed at the FSA meeting held on 16th February 2012 at Immingham Storage Company East.

4.9 Is the safety instrument system validation planning appropriate and have the validation activities been completed?

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	P&I Design competency
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	Suites of testing documentation are available in the SIS manuals.
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		Any repair or replacement is recorded and evidence is available. It is the intent to provide a report annually of failures of any SIS equipment for analysis. New Serial numbers of SIS equipment are recorded on the proof test documentation.

This was reviewed and discussed at the FSA meeting held on 16th February 2012 at Immingham Storage Company East.

Details of data collection for analysis and approval to be provided to Immingham Storage Company East. (Action 15)

Immingham Storage Company East appreciate that they are ultimately responsible for the testing and safe operation of the system as system owners. ISCo to discuss responsibility for the SIS on the terminal. (Action 16)

4.10 Has the employee training been completed and appropriate information about the safety instrumented system been provided to the maintenance and operating personnel.

This was reviewed and discussed at the FSA meeting held on 16th February 2012 at Immingham Storage Company East.

A package of training presentations for Safety Instrumented systems has been prepared including awareness, operation and engineering.

The relevant Immingham Storage Company East personnel have received the appropriate training and Immingham Storage Company East will continue to use the training packages as required.

Immingham Storage Company have a training matrix which includes Safety Instrumented Systems. Any contractors involved in the SIS will be trained as per Immingham Storage Company East personnel. (Action 17)

4.11 Are Plans or strategies for implementing further safety assessments in place?

Any further safety assessments will be carried out as required. At present no further assessments are planned. It is anticipated that a Stage 4 FSA will be conducted in approx. 3 years. Stage 5 FSA's will be conducted if required.

However, it will be necessary to review all the Actions and their results arising from this FSA.

4.12 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.

FSA Meeting: The compliance documentation has been incorporated into this FSA.

5 CONCLUSIONS

5.1 FSA meeting

All actions arising from the FSA are to be completed as soon as possible and by end of the 2nd quarter 2012 and a review carried out.

The Safety Lifecycle documentation reviewed at this FSA was provided by Immingham Storage Company East.

Following this FSA assessment and the comments from the HSE it appears that there may be lifecycle documentation incomplete, missing or not available at this time.

Life-cycle documentation:

- Management of Functional Safety Document to be updated following the FSA. (Action 18)
- Safety Requirement Specification to be revised to include comments from FSA. (Action 19)
- SIS Design Dossier to be issued.
- System Overview and design documentation to be revised to include comments from FSA. (Action 20)
- Modification and Management of Change Procedures to be updated and reviewed. (Action 6)

This Functional Safety Assessment concludes that the Probability of Failure on Demand calculation and hardware fault tolerance meet the requirements of a SIL 2 Safety Instrumented System and that the system has been maintained and tested to ensure functional safety.

It was agreed at the FSA that continuing field reliability data would be obtained for analysis against the calculated data.

As a result of this FSA, Immingham Storage Company East Terminal will modify some of their management procedures and documentation to ensure that all aspects of the safety lifecycle, see Action list, are in line with BS EN 61511.

6 ACTIONS

Action No.	Action	By	Expected Completion	Completion Date
1	LOPA to be reviewed and updated for next COMAH report.	D. S. Regan	End 2012	29/06/12 (SI057001_RPT Rev G)
2	Surge Calculations to be supplied and reference appended. Calculations to be based on 500m^3/hr.	A. Rhodes	End June 2012	28/3/13
3	SRS and SIS Design to be updated to reflect tankside valve closure times based on 500m^3/hr.	D. S. Regan	End June 2012	SRS SI277010_RPT Rev E SIS Design SI277001_RPT Rev D
4	SRS to be updated to reflect that the 4 common pipeline valves will not be used in the Safety Instrumented System.	D. S. Regan	End June 2012	SRS SI277010_RPT Rev E
5	Valves, actuators and solenoid valve specifications required.	D. S. Regan	End June 2013	
6	Management of change procedures to be updated to include for the requirements of BS EN 61511.	P. Jobling	End June 2013	
7	Cross referencing of actions with document revision dates required on the FSA.	D. S. Regan	End June 2012	Noted for future documentation
8	Maintenance and testing records for the BPCS to be confirmed.	A. Rhodes	End June 2013	
9	Data recording to be formalised. Record keeping of failure of SIS and analysis of reliability of SIS.	A. Rhodes	End July 2013	
10	Live Design documentation on the server to be confirmed.	D. B. Faulkner	End June 2012	16/10/12 – SI277001_MNL Rev B uploaded
11	A separate site inspection of the SIS will be carried out and a separate report will be appended to this document.	D. B. Faulkner	End June 2012	02/07/12 – SI277004_RPT 28.06.12 SI277005_RPT (Refer to SIS Manual Book 3)
12	Documentation required to confirm that any external manual shutdown or non SIS functions cannot impair the operation of the SIS.	D. B. Faulkner	End June 2012	ROSOV & ESD function tested as part of SI277005_RPT No BPCS function active on system.

13	Some systems are installed and operational, and the completed SATs are available in the SIS manuals. Not available on the server. To be input to electronic data system	D. B. Faulkner	End April 2012	17/10/12 – SIS Book 3 testing uploaded to online documentation system
14	Confirm the design documentation above is at correct revision with electronic data system.	D. B. Faulkner	End June 2012	16/10/12
15	Details of data collection for analysis and approval to be provided to Immingham Storage Company East.	D. S Regan	End June 2012	29.03.13 – added as appendix to SI277009_RPT – analysis and approval
16	ISCo to discuss responsibility for the SIS on the terminal.	A. Rhodes	End June 2012	SIS Champion nominated April 2013
17	Any contractors involved in the SIS will be trained as per Immingham Storage Company East personnel.	A. Rhodes	End June 2012	All current contractors trained to equivalent standard as ISCo personnel.
18	Management of Functional Safety Document to be updated following comments in the FSA.	D. S Regan	End June 2012	SI277102_RPT revised to B dated 10.10.12
19	Safety Requirement Specification to be revised to include comments from FSA.	D. S Regan	End June 2012	SRS SI277010_RPT Rev E
20	System Overview and design documentation to be revised to include comments from FSA.	D. S Regan	End June 2012	Covered by actions above

APPENDICES

Appendix 1

Operating Procedures

Not Included in Rev D

Appendix 2

P & I Drawings

Not Included in Rev D

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

IMMINGHAM STORAGE Co LTD

IMMINGHAM EAST TERMINAL

TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MODIFICATION REPORT

SIS RESTRUCTURING

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	04.12.13	D. B. Faulkner	D.S.Regan	Client	Original Issue	
B	06.03.15	D. B. Faulkner	D.S.Regan	ISCo	As Built	Document No. **SI483001_RPT**

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION HISTORY

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

2 SCOPE

This document has been prepared to control a modification to the ISCo East Terminal, Tank Overfill Safety Instrument System.

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 will be initiated at this stage.

3 MODIFICATION PLAN

3.1 Description of the modification or change

Remove 600 series tanks 601, 602 & 603 from the No4 East Overfill Protection SIS panel into No5 Switchroom "Arcton" SIS overfill protection panel.

Remove 500 series tanks 561, 564 & 568 from the No4 East Overfill Protection SIS Panel into a new dedicated SIS Overfill Protection Panel located at No4 East.

No4 East Overfill Protection Panel to be de-rated from SIS duty.

3.2 Reason for the modification or change

Terminal gasoline capacity not predicted to exceed current gasoline SIL rated tanks T561, T564, T568, T601, T602, T603, T615, T616, T617, T618 & T619. All other tanks currently in east terminal safety instrument system to remain protected by an independent high integrity overfill protection system, however this will not be SIL rated. Restructuring will allow SIL rated tanks to be physically segregated from non SIL rated tanks.

3.3 Identified hazards affected

None.

Field hardware to be retained. The main logic solver components, nivotesters & pilz relays, will be retained. The BPCS wiring will be modified to ease testing and diagnostics.

3.4 Impact on functional safety

It is considered that there will be no impact on functional safety form 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

Installation documentation will be created under Project SI483, the in service SI208 documentation will be as built from the project documentation on completion of the SAT, the SI483 project documentation will then be retired.

The following details the lifecycle documentation that will require reviewing / modifying as a result of the requested modification:

Document Reference	Description	Rev	Date / Sign
SI208001_MNL	No.5 Switchroom SIS Book 1	C	06.03.15 DBF
~~SI208002_MNL~~	~~No.5 Switchroom SIS Book 2~~	~~B~~	06.03.15 DBF
SI208003_MNL	No.5 Switchroom SIS Book 3	C	06.03.15 DBF
SI277001_MNL	ROSOV Documentation	D	06.03.15 DBF
~~SI277002_MNL~~	~~SIS Bk 2 of 3 Audit Trail~~	~~C~~	06.03.15 DBF
~~SI277003_MNL~~	~~SIS Bk 3 of 3 Testing~~	~~C~~	06.03.15 DBF
SI483001_MNL	No4 Switchroom SIS Manual	A	06.03.15 DBF

3.6 Implementation plan

Implementation of the modification will have no effect on the SIF and no additional protection is required to maintain functional safety.

3.7 Testing plan

The Safety Instrument System will require re-testing following the modifications.

Updated Testing Document will be provided for the on-site validation of the safety Instrument System.

3.8 Approvals, Roles and Responsibilities

This modification was requested by: A.Rhodes, ISCo East Terminal Manager

This modification request approved by: D. S. Regan, P&I Design Ltd.

Hazard and Impact assessment conducted by: D. S. Regan, P&I Design Ltd.
Design incorporation by:

Design Reviewed by: D. S. Regan, P&I Design Ltd.

Modifications by: D.B.Faulkner, P&I Design Ltd, Stark Electrical Services (ISCo Installation contractor)

Modifications proof tested by: D.B.Faulkner, P&I Design Ltd, Stark Electrical Services (ISCo Installation contractor)

Modification completed – date: 03.07.14

Documentation updated and re-issued: 06.03.15