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

LOCAL FUEL PLC

SHOREHAM OIL TERMINAL

OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MANAGEMENT MANUAL

Contents

P & I Design Ltd
2 Reed Street, Thornaby, UK, TS17 7AF
Tel: 00 44 (0)1642 617444
Fax: 00 44 (0)1642 616447
www.pidesign.co.uk

P & I Design Ltd

Process Instrumentation Consultancy & Design

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

LOCAL FUEL PLC

SHOREHAM OIL TERMINAL

SAFETY INSTRUMENTED SYSTEMS

POLICY AND LIFECYCLE ACTIVITIES

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	15.12.14	D.R. Ransome	DSR	L. Salvidge	Original Issue	
B	26.03.15	D. R. Ransome	DSR	L. Salvidge	Updated following HSE review	
C	12.06.15	D. R. Ransome	DSR	L. Salvidge	Minor typographical errors corrected	Document Number **LF364003_RPT**

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

References

The following standards and guidance are relevant to Managing Functional Safety of Safety Instrumented Systems in the Oil Storage Sector of the Process Industry.

1. BS EN 61508 Parts 1 – 7: 2010
   Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.
2. BS EN 61511 Parts 1 – 3: 2004
   Functional Safety – Safety Instrumented Systems for the Process Industry Sector.
3. EEMUA Publication 222 – Guide to the Application of IEC 61511 to Safety Instrumented Systems.
4. PSLG Final Report – Safety and Environmental Standards for Fuel Storage Sites.
5. API 2350 – Overfill Protection for Storage Tanks in Petroleum Facilities.
6. HSE Managing Competence for Safety-Related Systems Parts 1 & 2.
7. HSE Guidance OG54 – Proof Testing of Safety Instrumented Systems in the Onshore Chemical/Specialist Industry.
8. HSE Guidance OG46 – Management of Instrumented Systems Providing Safety Functions of Low/Undefined Safety Integrity.
9. HSE 428/2002 – Principles for Proof Testing of Safety Instrumented System in the Chemical Industry.
10. CDOIF – Demonstrating Prior Use of Elements of a Safety Instrumented Function in support of BS EN 61511.

1 REVISION HISTORY

Rev	Description
A	Original Issue.
B	References: Ref 7 updated to OG54, Ref 7 updated to OG46. 5.2 Systematic Capability and Failure statement added. Remaining Section 5 items incremented by .1 5.5 Note added regarding the full requirements of the SRS. 5.8 Operation and Maintenance added. Remaining Section 5 items incremented by .1 5.11 Functional Safety Assessments statement added. 7.4 Inspection activities added Appendix removed
C	Minor typographical errors corrected.
D	

2 INTRODUCTION

Local Fuel plc own and operate a fuel storage facility at Shoreham. The terminal is classified as a low tier COMAH site. Local Fuel plc manage and employ operators and maintenance personnel for the day to day running of the terminal. As and when necessary Local Fuel plc employ the services of outside organisations to assist in specialist advice and services.

In the case of Management of Functional Safety related to the terminal's SIL rated overfill protection system, Local Fuel plc have engaged P & I Design Ltd to assist and support the company in ensuring compliance to BS EN 61511.

3 POLICY

The objective of Local Fuel plc's management is to conduct its business in a manner which fully conforms to the Clients' Contractual Requirements, together with ensuring that Operational, Environmental, Safety and Regulatory requirements are adhered to.
In order to achieve this objective relevant to Safety Instrumented Systems (SIS), it is the policy of this company to ensure that an effective and efficient Functional Safety Management system is established, maintained and improved upon. This is achieved through each member of the Company accepting that they are responsible for whatever part they play in the organisation, together with managing all lifecycle phases relevant to the SIS.
This Policy section gives an overview of how Local Fuel plc will manage the requirements of BS EN 61511 – Functional Safety – Safety Instrumented Systems for the Process Sector.

Management of Functional Safety

Management of Functional Safety applies across all safety lifecycle phases. Local Fuel plc utilises the services of external organisations to assist in certain lifecycle phases. However, Local Fuel plc ensure that all external organisations are aware of their responsibilities and the deliverables required of them.

Roles, Responsibilities and Competence

The Managing Director will adopt the role of Functional Safety Manager (FSM) and be responsible for ensuring compliance to this procedure. He is also responsible in ensuring the competence of both employees and external contractors and consultants who carry out all activities associated with the SIS. Specific required competencies are identified in this Policy and Lifecycle Activities document.

Planning

Local Fuel plc will utilise the BS EN 61511 lifecycle as a methodology and will plan for all lifecycle phases of the SIS by creating a Safety Plan. The Safety Plan will define the applicable tasks required at each lifecycle phase and identify those responsible in carrying out the relevant activities.

Verification and Validation

Local Fuel plc will ensure Verification is performed by review, analysis and/or testing and that the required deliverables satisfy the defined requirements for the appropriate phases of the safety life cycle. Procedures will be developed to provide for Validation through inspection and testing, that the installed and commissioned safety instrumented system and its associated safety instrumented functions achieve the requirements as stated in the safety requirement specification.

Functional Safety Assessments

Functional Safety Assessments (FSA) will be conducted at relevant lifecycle phases, the Safety Plan will identify when and what Stage FSA is to be conducted.

4 BS EN 61511 LIFECYCLE

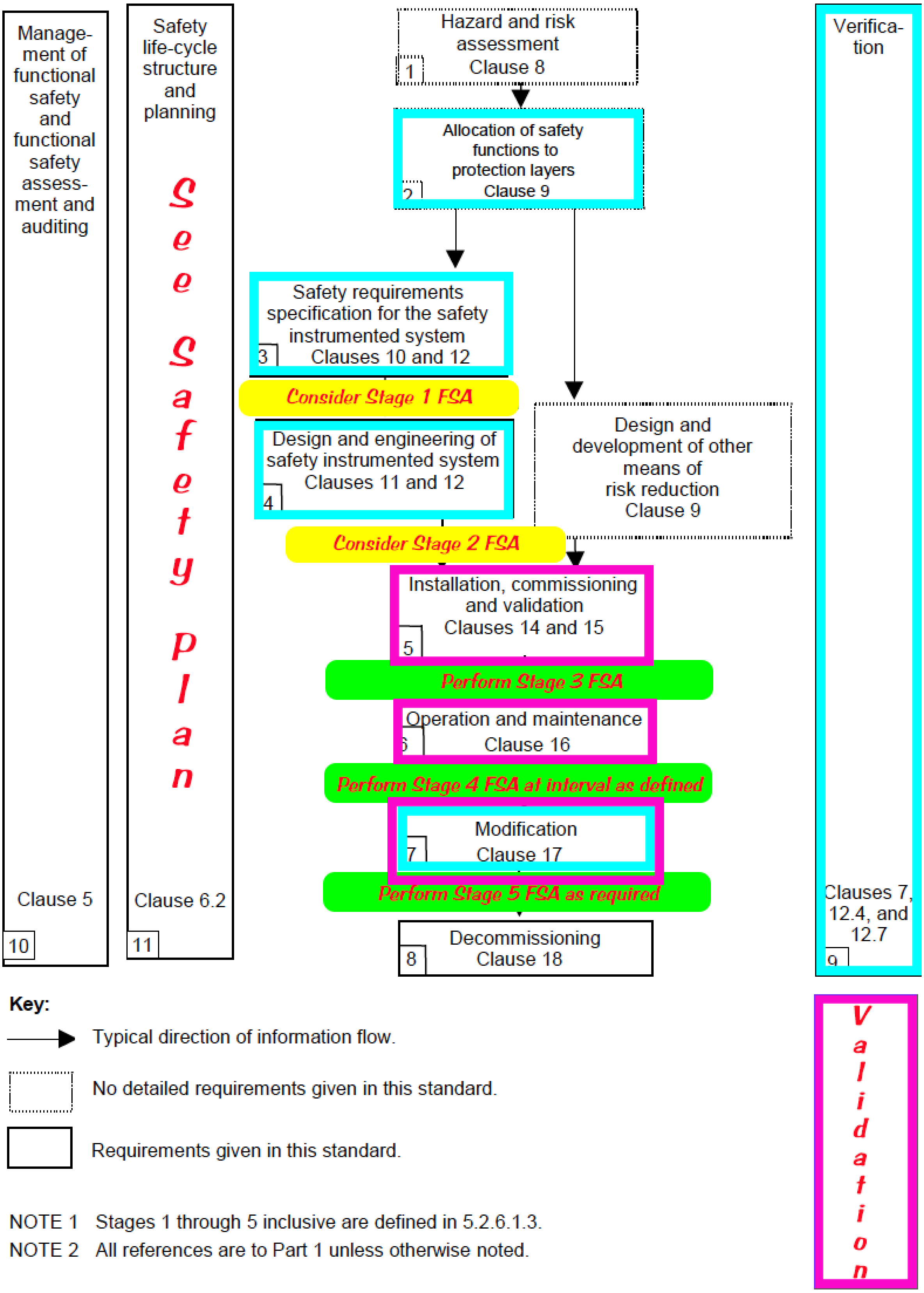


Figure 1: BS EN 61511 Lifecycle with Verification, Validation and FSA processes.

5 ACTIVITIES THROUGHOUT THE LIFECYCE

5.1 Safety Plan

Local Fuel plc will open a Safety Plan when it is anticipated that a Safety Instrumented System is required. The Safety Plan will be updated with the lifecycle documentation, starting at the Hazard and Risk Assessment stage of the lifecycle. The Safety Plan will identify for each lifecycle activity the criteria, techniques, measures and procedures together with roles and responsibilities of employees and external organisations to ensure the activity is correctly administered.

5.2 Systematic Capability and Failure

Local Fuel plc appreciate that by the nature of a systematic failure that a potential failure could be present in the Safety Instrumented System and be dormant until a unique set of circumstances occur. Systematic failures, together with dangerous undetected random hardware failures are difficult to identify. In order to reduce the likelihood of Systematic failures occurring checking, verification and validation is carried out throughout the lifecycle.

5.3 Hazard and Risk Assessment

The Functional Safety Manager is responsible for ensuring that Hazard and Risk Assessment (HRA) is conducted and for the appointment of an appropriate multi-disciplined team.
All HRA studies will be conducted by a multi-disciplined team with the relevant knowledge and skills appropriate to the terminal, the process and operations, together with control and instrumentation systems.

The objective of a HRA is to review the process and identify hazardous events arising from possible failures, including failures of the process, operations and control systems, where the consequence of a failure may lead to cause a harmful event to people, the environment or the business of Local Fuel plc.

Local Fuel plc utilise the most appropriate of the following techniques to perform HRA:
Hazard Identification (HAZID), Hazard and Operability Studies (HAZOP), Risk Graphs, Fault Trees Analysis, Layer of Protection Analysis (LOPA) or Quantitative Risk Assessments (QRA).

5.4 Allocation of Safety Functions

When the HRA derives that a SIS is required the Safety Integrity Level (SIL) Determination is conducted utilising Risk Graphs, LOPA or QRA. Local Fuel plc policy is that if a Risk Assessment deems a Safety Instrumented Function (SIF) is required with a Safety Integrity Level SIL 1 or greater then a LOPA study or QRA will be employed to ensure that the study is neither over conservative nor over pessimistic.

As shown in Figure 1, verification of the allocation of Safety Functions are required at this lifecycle phase. The Functional Safety Manager is responsible to ensure that this verification is completed as defined in the Safety Plan. Local Fuel plc will develop checklists to record the verification process.

5.5 Safety Requirement Specification

Local Fuel plc will produce or have produced for them a Safety Requirement Specification, the purpose of which is to:

- Define Safety Instrumented Functions and Safety Integrity Levels.

- Provide information to fully define the intended SIS, by defining: [1]
  - The Process and the Process Safe State.
  - System Architecture.
  - Time of response.
  - The demand on the System.
  - Settings, Calibrated Ranges and Levels of Concerns.
  - Process and Environmental Limitations.
  - Interface with other control systems and protection layers.
  - Manual Shutdown methods.
  - Override facilities if required. (Overrides are avoided unless absolutely necessary).
  - Spurious Trip acceptability.
  - Proof Test Requirements.

- Provide the System Integrator and or suppliers the Basis of Design for development of the SIS.

As shown in Figure 1, verification of the Safety Requirement Specification is required at this lifecycle phase. The Functional Safety Manager is responsible to ensure that this verification is completed as defined in the Safety Plan. Local Fuel plc have developed checklists to record the verification process.

The Safety Plan will have identified if a Functional Safety Assessment (FSA) Stage 1 is to be performed. If it is required then the Functional Safety Manager will arrange for an assessment to be conducted.

[1] A full list of requirements to be detailed within the SRS can be found in BS EN 61511 - 2004 Clause 10.3

5.6 Design and Engineering of the Safety Instrumented System

Local Fuel plc will utilise the services of suitable competent consultants, suppliers and sub-contractors for the realisation phase of the BS EN 61511 lifecycle. The Functional Safety Manager is responsible to ensure that all external organisations are aware of what is required of them and he will liaise with them in providing the necessary design input and ensure that the deliverables received by them comply with the company's requirements.

The design shall meet the requirements of BS EN 61511 with respect to system architecture, hardware fault tolerance, common cause failures, random hardware failures and Probability of Failing in Demand PFD_{AVG} calculations together with system capability and systematic failures.

The design will include all necessary documentation to provide for the specification, implementation, procurement, installation, verification testing including Factory Acceptance Test (FAT) and Site Acceptance Tests (SAT) together with Validation documentation for initial and on-going proof testing of the SIS.

SIL Verification calculations shall be included using failure rate data, preference in the selection of hardware will be given to SIL Certified to BS EN 61508 components.

As shown in Figure 1, verification of the Design is required at this lifecycle phase. The Functional Safety Manager is responsible to ensure that this verification is completed as defined in the Safety Plan. Local Fuel plc have developed checklists to record the verification process.

The Safety Plan will have identified if a Functional Safety Assessment (FSA) Stage 2 is to be performed. If it is required then the Functional Safety Manager will arrange for an assessment to be conducted.

5.7 Installation, Commissioning and Validation

Local Fuel plc or the System Integrator will employ sub-contractors to install the SIS. All installation work will be carried out by technicians who are competent in both SIS and hazardous areas working and will be undertaken by CompEx certified technicians, or at a minimum the final inspections, prior to energising the system, must be carried out and documented by a CompEx certified technician.

Local Fuel plc will ensure that the Installation Contractor has all required documentation in order that the installation will comply with the design. It is the Installation Contractor's responsibility to ensure that any changes during the installation are advised and agreed with the designer and supported with information to allow As Built documentation.

Installation testing documentation is to be provided by the Installation Contractor to Local Fuel plc or their representative for inclusion into the Safety Instrumented System Manual.

On completion of the installation the full system will be pre-commissioned and validated to ensure the installed SIS meets the requirement of the design for both functional safety and in compliance with BS EN 61511.

Full and comprehensive records will be produced and retained of the installation, commissioning and validation detailing test results, instrumentation calibration, procedures used and any discrepancies between actual and expected results. This documentation will be included in the Safety Instrumented System Manual.

As shown in Figure 1, validation of the Installation and Commissioning is required at this lifecycle phase. The Functional Safety Manager is responsible to ensure that this validation is completed as defined in the Safety Plan. Local Fuel plc have developed checklists to record the verification of the validation process.

A Functional Safety Assessment (FSA) Stage 3 is to be performed. The Functional Safety Manager will arrange for an assessment to be conducted.

5.8 Operation & Maintenance

To ensure that the functional safety of the SIS is maintained during operation and maintenance Local Fuel plc. ensure that SIS/SIF are maintained, tested and inspected.

Inspection, maintenance and test procedures will be produced for the SIS. All testing will be fully documented and analysed. Inspection, maintenance and test procedures should be approved by the FSM.

The test procedures should address the following:

- A statement of the "purpose and scope".
- Consideration and documentation of all precautions that must be observed whilst performing the tests in order to avoid potential hazards.
- Identification of any special tools or equipment required and evidence that the personnel are competent to use such equipment.

- Any initial conditions which must be satisfied prior to undertaking the test.
- Adequate cross references to any other documents, manuals etc.
- Clear and concise procedural steps which adequately define the tasks necessary to perform the test safely and efficiently.

Proof test procedures should be designed in order to detect dangerous undetected failures by, where possible, providing realistic end to end testing. Where full testing cannot be conducted, partial testing will be utilised, but the testing plan will identify when a full test is required to ensure the PFD of the component and system is not compromised.

Any warnings or specific issues that should be drawn to the attention of the tester should be clearly and conspicuously stated.

The FSM will schedule the inspection, maintenance and test routines utilising the site competent personnel or an organisation to carry out the inspection, maintenance and test routines.

Full documentation of the findings of every inspection, maintenance and test routine, including any failures or faults will be produced by, or on behalf of Local Fuel plc. The documentation associated with proof testing and inspection should a minimum contain:

- SIF tag number.
- Inspection, maintenance and test procedure tag number.
- Brief description of inspection, maintenance and test.
- Date carried out.
- Name/s of person/s carrying out inspection, maintenance and test routine.
- Results of inspection and test routine including “as found” and “as left” condition.
- Any critical steps which following the tests may leave the system in-operable.
    - If critical steps are identified then independent checks of that task should be identified and recorded on the test procedure.

Any reports of overdue tests, demands upon the SIF, or spurious operation and failures during operation or under test, shall be investigated and documented by the FSM.

Periodically the FSM shall ensure that a review of the data from demands, mean time to restore, spurious trips and testing is performed to verify that assumptions made during the SIL Determination and design activities were accurate and complete.

Local Fuel plc ensure that terminal operating personnel understand what is required of them in the case of activation of the SIS. The FSM will ensure that operators log and record all SIS activities, such as activations, spurious events and failures using a dedicated SIS failures report.

The FSM will review each and every report to ensure Functional Safety is maintained.

All terminal operations and procedures are conducted utilising Standard Operating Procedures (SOP’s) to which operators are trained and competent in carrying out.

5.9 Modification

Local Fuel plc appreciate that modifications to the originally installed SIS may be required from time to time. This may result from operational changes at the terminal requiring changes to the SIS, enhancements to the SIS or corrections to shortfalls in the operation of the SIS.

Any modification to the SIS can only be authorised by the Functional Safety Manager and must be controlled utilising the company's Management of Change Procedure.

Before any modification is authorised, consideration will be given to the requirement of a FSA Stage 5. This will then decide at what stage of the Safety Lifecycle the modification process requires to be reviewed.

The Safety Plan will be utilised to manage the modification.

Local Fuel plc have developed checklists to record the verification of the validation process.

5.10 Decommissioning

Local Fuel plc will utilise its Management of Change Procedure to instigate the decommissioning of the SIS.

The Functional Safety Manager will arrange for a FSA 5 to be conducted on the proposed decommissioning of the SIS and the FSA will be conducted as for a modification to the SIS, with emphasis that the decommissioning of the SIS cannot put a further demand on any other remaining protection systems.

Local Fuel plc have developed checklists to record the verification of the validation process.

5.11 Functional Safety Assessments

The Functional Safety Manager will arrange for FSAs to be conducted in accordance with the Safety Plan.

The following will be considered when planning a FSA.

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

6 ROLES AND RESPONSIBILITIES

Local Fuel plc ensures that all its employees who are involved in the management, operation or maintenance of the SIS are aware of their responsibilities related to the SIS. All such employees will undergo BS EN 61511 awareness training and where necessary more specific on the job or other specialist training.

6.1 Roles and responsibilities include:

6.1.1 Managing Director

The Managing Director assumes the role of Functional Safety Manager and is responsible for the management and control of the SIS:

- He ensures that the hazard and risk assessments are carried out.
- Arranges for a multi-discipline team to carry out HRA, SIL Determination and FSA studies, and to arrange external expertise when required.
- Ensures that the design of the SIS fulfils the safety requirement for functional safety and target SIL/ PFD_{AVG}.
- Ensures that all SIFs are correctly installed, tested and commissioned according to the design.
- Ensures that the SIS is maintained, tested and inspected as detailed in the inspection, maintenance and test procedures.
- Performs Analysis and Approval of all data from demands, spurious trips and testing to verify that assumptions made during the SIL Determination and design activities were accurate and complete.
- Arranges for all necessary training to ensure employees are competent to carry out their responsibilities.
- Selects competent personnel or an organisation to carry out the design and installation of SIS.
- Ensures any SIS modifications are controlled and managed as per the modifications procedure.

6.1.2 Operations Manager - SIS

- To manage SIS inspection, maintenance and test procedures.
- To maintain the inspection, maintenance and test procedures and results of all activities.
- Schedules the inspection, maintenance and proof test.
- Selects competent personnel or an organisation for inspection, maintenance and proof test.
- Participation in SIS risk assessments, installation, commissioning and validation planning.

6.1.3 Maintenance Technicians

- Carries out inspection, maintenance, testing and reinstatement of the SIS (in co-operation with specialist SIS Technicians).
- Ensures any faults detected during inspection, maintenance and testing are fully documented in the inspection and testing report.

6.1.4 Operations Personnel

- Be knowledgeable with the operation of the SIS.
- Know how to react to an activation of the SIS without having to refer to any additional guidance.
- Log and report any activations, spurious trips or other faults with the SIS.
- Know how and when to activate a manual shutdown of the system.
- Be aware of other employees or sub-contractors responsibilities when they request to work on the SIS.

7 COMPETENCE

Local Fuel plc utilise the guidelines of EEMUA 222 to define the competencies required to perform each of the lifecycle phases. These are detailed below in a simplified form, for more information refer to EEMUA 222.

7.1 HRA and Allocation of Safety Functions

Safety lifecycle phase	Activity	Required Competencies
Hazard and Risk Analysis	HAZID studies HAZOP studies SIL determination	• Understands principles of hazard identification, analysis and HAZOP studies • Understands where hazards may be introduced by the SIS. • Has experience of participating in HRA studies.
Allocation of Safety Functions to protection layers	SIL determination	• Understands the effectiveness of different types Of protection layers, • Has experience of allocating safety functions to layers. • Has experience of participating in or leading SIL determination.
Safety requirement specification	SRS preparation or approval of SRS	• Knows and understands how to develop specifications. • Has experience of developing role statements functional and integrity specifications for SIS.

7.2 Design & Engineering of the SIS

Safety lifecycle Phase	Activity	Required Competencies
Design and engineering of SIS	Design Engineering	• Knows and understands how to select the most appropriate sensors and final elements to meet the process conditions and safety integrity requirements. • Knows and understands how to select an appropriate logic solver to meet the safety requirements. • Has experience of selecting sensors and final elements for SIS applications at the required SILs. • Has experience of specifying a logic solver for SIS application at the required SILs. • Has experience of configuring a logic solver for SIS application at the required SILs. • Has experience of integrating and factory testing a logic solver to meet specified functional requirements. • Has experience of developing documentation for SIS including Factory and Site Acceptance Test procedures.
	Software Development	• Understands the requirements of BE EN 61511 for Software. • Is familiar with the Safety Manual for the programmable logic solver and how to comply with all its requirements.
	Project Management	• Knows and understands principles of BS EN 61508 and BS EN 61511 and their application to the process sector. • Knows and understands company's project lifecycle and associated procedures. • Knows and understands the companies quality system.
	Functional Safety	• Knows and understands details of BE EN 61511 and its application to the process sector. • Knows and understands company's project lifecycle and associated procedures. • Knows and understands company's quality system • Knows, understands and has experience of SIS software and hardware technology in a similar application. • Experience of participating in at least one Safety Integrity Level Assessment. • Experience of performing SIL verification (achieved PFD) calculations.

7.3 Installation, Commissioning and Validation

Safety lifecycle Phase	Activity	Required Competencies
Installation, commissioning and validation	Installation and commissioning	• Knows and understands installation and commissioning issues with SIS field equipment and logic solvers. • Has managed site installation of SIS equipment and systems.
	Testing and validation	• Knows and understands Site Acceptance Testing issues with SIS field equipment and logic solvers. • Has managed site commissioning and acceptance testing activities against test procedures. • Understands requirements of BE EN 61511 for Verification.

7.4 Operation and Maintenance

Safety lifecycle Phase	Activity	Required Competencies
Operation and Maintenance	Operation and Maintenance Management	• Knows and understands how to manage SIS to ensure functional and integrity requirements are achieved. • Has developed procedures for maintenance and testing of SIS. • Has reviewed testing results to ensure that functional and integrity requirements are achieved and amended, testing scopes and test intervals as necessary. • Has developed and implemented procedural controls for management of overrides and inhibits.
	Routine Proof Testing	• Knows and understands Proof Testing issues with SIS field equipment and logic solvers. • Has managed site commissioning and acceptance testing activities against test procedures. • Understands requirements of BE EN 61511 for Verification.
	SIS Inspection	• Knows and understands how to manage SIS to ensure functional and integrity requirements are achieved. • Knows and understands maintenance issues with SIS field equipment and logic solvers. • Compex certification if SIS is located in electrical hazardous area.

7.5 Modification

Safety lifecycle Phase	Activity	Required Competencies
Modification	Management of Change Control	• Knows and understands site procedures for management of change. • Has carried out a risk assessment for management of change. • Knows how to modify SIS to achieve required revised functionality and integrity and implications of the changes. • Has managed and/or developed revised documentation and procedures associated with SIS modifications.
	Specification, Design, Implementation and Testing of Modification	• For any activities included in Design and Engineering, Installation Commissioning and Validation or Operation and Maintenance above, the same competencies are required for modifications.

7.6 Decommissioning

Safety lifecycle Phase	Activity	Required Competencies
Decommissioning	Decommissioning	• Knows and understands how to decommission SIS while ensuring hazards are managed. • Has experience of decommissioning SIS in a safe manner.

7.7 Verification

Safety lifecycle Phase	Activity	Required Competencies
Verification	Checking and approval of lifecycle documentation	• Knows how to carry out verification reviews. • Has experience of verifying two or more lifecycle activities.

7.8 Management of Functional Safety

Safety lifecycle Phase	Activity	Required Competencies
Management of Functional Safety	Management of SIS Lifecycle	• Knows and understands details of BE EN 61511 and its application to the process sector. • Knows and understands company's project lifecycle and associated procedures • Has experience of project management involving people, and resources including financial resources. • Has experience of carrying out audits and incorporating recommendations into action plans. Has experience of managing clients, suppliers or sub-contractors.
	Functional Safety Assessment	• Knows and understands details of BE EN 61511 and its application to the process sector. • Has experience of carrying out functional safety assessment or audit of SIS.
Safety Lifecycle Structure and Planning		• Knows and understands how to create a lifecycle structure and planning process with defined inputs, outputs and verification requirements for each activity. • Has experience of creating a SIS lifecycle structure for planning and project management purposes. • Has experience of successfully implementing a lifecycle planning process.

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

LOCAL FUEL PLC

THE SHOREHAM OIL TERMINAL

SAFETY INSTRUMENTED SYSTEM

MANAGEMENT OF FUNCTIONAL SAFETY

SAFETY PLAN

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	23.12.14	D R Ransome	D S Regan	L Salvidge	Original Issue	
B	27.03.15	D R Ransome	D S Regan	L Salvidge	Typographical errors corrected and action history updated	
C	27.05.15	D R Ransome	D S Regan	L Salvidge	Updated for latest documentation	Document No. **LF364004_RPT**

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION CONTROL

Rev	Description
A	Original Issue
B	Typographical errors corrected. Action History Updated for revised LOPA and new SRS
C	Action History Updated for revised LOPA, SRS, SIL verification and testing
D	

2 SCOPE

This safety plan details the Management of the Safety Instrumented Overfill Protection System at Local Fuel plc's Shoreham Terminal. It is intended to reflect the life cycle of the SIS in accordance with BS EN 61511 and to be a working document throughout the life cycle of the Safety System.

The objective of this document is to identify the various lifecycle phases of the SIS and the management activities, together with the inputs and outputs required to ensure that the appropriate deliverables are achieved at the various lifecycle phases to ensure the functional safety objectives are met.

This document is to be read in conjunction with Local Fuel plc Policy and Lifecycle Activities Document Ref: LF364003_RPT

3 ORGANISATIONS AND RESOURCES

Persons, departments and organisations who 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.

Local Fuel plc Management Procedures identify the responsibility of persons assigned to this Safety Instrumented System and ensure the competence of such persons.

Local Fuel plc Management Procedures include the following elements specific to the Safety Instrumented 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 is controlled by Local Fuel plc's Functional Safety Manager.

		Date
Functional Safety Manager	………………………………………….	…………………

4 SAFETY POLICY & LIFECYCLE ACTIVITIES

Local Fuel plc have a Safety Policy for the implementation and management of Safety Instrumented Systems, this is detailed in document LF364003_RPT – Safety Policy & Lifecycle Activities Document.

That document and this Safety Plan refer to the Safety Instrumented System detailed in Section 5 of this document.

4.1 Safety Instrumented System Lifecycle

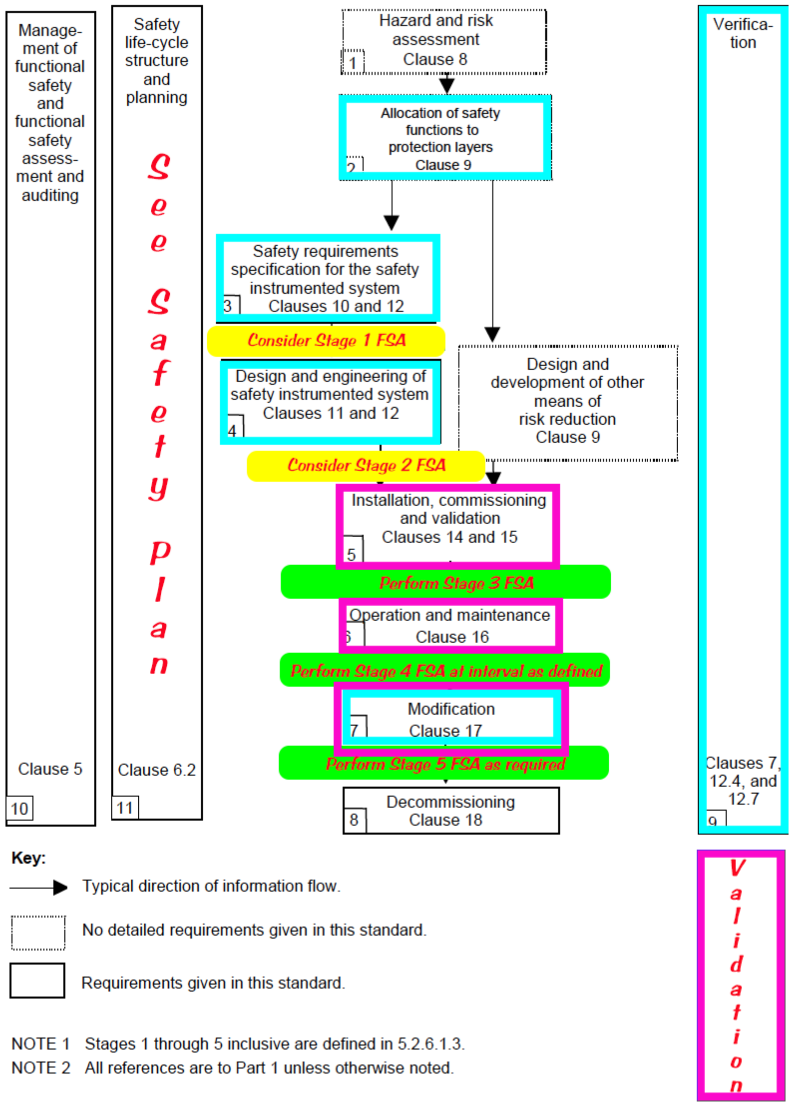


FIGURE 1 – SIS LIFECYCLE

4.2 Safety Plan

Throughout this Safety Plan each section is prefaced with a Table depicting the activity together with the objectives, inputs, outputs, deliverables and responsible persons/organisations. This plan follows the guidance of EEMUA 222 – Application of IEC 61511 to safety instrumented systems.

5 SAFETY INSTRUMENTED SYSTEM

The Safety Instrumented Functions of the Safety Instrumented Systems are:

Gasoline Tank Overfill Protection at Local Fuel plc's Shoreham Terminal.

6 FUNCTIONAL SAFETY ASSESSMENTS

In addition to roles, responsibilities, inputs, outputs and deliverables this document will provide the control of the Functional Safety Assessment through the lifecycle of the SIS to ensure the necessary objectives of functional safety are met. Functional Safety Assessments (FSA) will be documented in separate documents but referenced within this document.

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 circumstances and 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 one FSA shall be undertaken before the hazards are present.

6.1 Functional Safety Assessment Plan

It is envisaged that the following FSA's will be conducted for this SIS:

- Stage 3
- Stage 4
- Stage 5

7 RISK ANALYSIS AND ALLOCATION OF SAFETY FUNCTIONS

7.1.1 Risk Analysis Requirements

Lifecycle phase in Figure 1	Activity			
1	Hazard and Risk Analysis			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To determine the hazards and hazardous events of the process and associated equipment. The sequence of events leading to the hazardous event and the process risks associated with the hazardous event. The requirements for risk reduction and the safety functions required to achieve the necessary risk reduction.	Process design Safety and Environmental targets	Description of Hazards Required Safety Functions Required risk reduction for each safety function	HAZOP Report Risk Graphs LOPA QRS	Functional Safety Manager Designers Operators
Lifecycle phase in Figure 1	Verification Plan			
9	Utilise QSF022_SIS – Stage 1 – Hazard & Risk Assessment - Checklist A			

7.1.2 Risk Analysis Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
25.01.07	SI087007_RPT Revision A	An original LOPA was performed for and on behalf of the original owners of the Terminal – Chevron.	**LOPA Team** Chair Member Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd I Goldsworthy – Facility Engineer – Simon Management Ltd Miss L Dixon – H&S Department – Chevron Ltd D Crook – Terminal Manager – Simon Management Ltd D S Regan BEng – Process Engineer – P & I Design Ltd
20.10.10	SI087007_RPT Revision B	LOPA study re-conducted following CA request and PSLG Guidance.	**LOPA Team** Chair Member Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd I Goldsworthy – Facility Engineer – Chevron Ltd Miss L Dixon – H&S Department – Chevron Ltd D Crook – Terminal Manager – Chevron Ltd D S Regan BEng – Process Engineer – P & I Design Ltd
20.10.10	SI087007_RPT Revision C	Chevron comments added and LOPA re-issued.	**LOPA Team** Chair Member Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd I Goldsworthy – Facility Engineer – Chevron Ltd Miss L Dixon – H&S Department – Chevron Ltd D Crook – Terminal Manager – Chevron Ltd D S Regan BEng – Process Engineer – P & I Design Ltd
20.10.10	SI087007_RPT Revision D	LOPA re-written following Chevron discussions with HSE.	**LOPA Team** Chair Member Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd I Goldsworthy – Facility Engineer – Chevron Ltd Miss L Dixon – H&S Department – Chevron Ltd D Crook – Terminal Manager – Chevron Ltd D S Regan BEng – Process Engineer – P & I Design Ltd
20.10.10	SI087007_RPT Revision E	Details of Societal Risk Added.	**LOPA Team** Chair Member Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd I Goldsworthy – Facility Engineer – Chevron Ltd Miss L Dixon – H&S Department – Chevron Ltd D Crook – Terminal Manager – Chevron Ltd D S Regan BEng – Process Engineer – P & I Design Ltd

Activity History – Terminal in Local Fuel PLC ownership				
Date	Reference	Description	Roles	Persons assigned
08.12.14	LF364002_RPT Revision A	Valero LOPA re-visited and revised to reflect current practices and procedures of Local Fuel plc.	**LOPA Team** Chair Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd L Salvidge – Managing Director – Local Fuel plc D Winser – Operations Manager – Local Fuel plc D S Regan BEng – Process Engineer – P & I Design Ltd
11.02.15	LF364002_RPT Revision B	Local Fuel LOPA re-visited and revised to reflect HSE Comment.	**LOPA Team** Chair Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd L Salvidge – Managing Director – Local Fuel plc D Winser – Operations Manager – Local Fuel plc D S Regan BEng – Process Engineer – P & I Design Ltd
30.03.15	LF364002_RPT Revision C	Local Fuel LOPA re-visited and revised to reflect HSE and Local Fuel comments	**LOPA Team** Chair Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd L Salvidge – Managing Director – Local Fuel plc D Winser – Operations Manager – Local Fuel plc D S Regan BEng – Process Engineer – P & I Design Ltd
01.04.15	LF364002_RPT Revision D	Local Fuel LOPA re-visited and revised to reflect Local Fuel comments	**LOPA Team** Chair Member Member Member	D R Ransome BA CEng FInstMC – P & I Design Ltd L Salvidge – Managing Director – Local Fuel plc D Winser – Operations Manager – Local Fuel plc D S Regan BEng – Process Engineer – P & I Design Ltd

7.2.1 Allocation of Safety Functions Requirements

Lifecycle phase in Figure 1	Activity			
2	Allocation of safety functions to protection layers			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level.	Required safety functions and associated integrity levels	Description of safety functions allocation to different systems	SIL Determination	Functional Safety Manager Designers
Lifecycle phase in Figure 1	Verification Plan			
9	Utilise QSF022_SIS – Stage 1 – Hazard & Risk Assessment - Checklist A			

7.2.2 Allocation of Safety Functions Action History

Activity History – Terminal in Chevron/Valero ownership		
Date	Reference	Description
25.01.07	SI087007_RPT Revision A	The LOPA concluded that an additional layer of protection was required and that a Safety Instrumented System with integrity of SIL 2 be designed and installed. The Safety Instrumented Function being that if any gasoline tank level was above the existing high level alarm then it would activate the closure of the jetty import line valve and stop the gasoline flow to the terminal.

7.3 Risk Analysis and Allocation of Safety Functions Verification History

Lifecycle phase in Figure 1	Verification -Terminal in Chevron/Valero ownership
9	Utilise QSF022_SIS – Stage 1 – Hazard & Risk Assessment - Checklist A
Verification Checklist	Notes
SI157105_RPT Revision A – Compliance Document - Section 4	QSF022 did not exist under Chevron ownership, all checklists were contained in a compliance document. Section 4 was a combined HRA – SRS Checklist

8 SPECIFICATION OF SAFETY INSTRUMENT SYSTEM

8.1 Safety Requirement Specification Requirements

Lifecycle phase in Figure 1	Activity			
3	SIS safety requirement specification			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, to achieve the required functional safety.	Description of safety functions allocation to different systems	SIS functional and integrity requirements by system software safety requirements.	Safety Requirement Specification Software Requirement Specification	Functional Safety Manager Designers SIS Supplier
Lifecycle phase in Figure 1	Verification Plan			
9	Utilise QSF010_SIS – Stage 1 – Safety Requirement Specification - Checklist 1			

8.2 Safety Requirement Specification Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
18.08.08	SI157007_RPT Revision A	SRS included as Section 6 in SIS Design document Original Issue.	P&I Design Ltd Simon Management Ltd	D S Regan BEng I Goldsworthy
23.03.10	SI157007_RPT Revision B	SRS included as Section 6 in SIS Design document Revised Post Installation.	P&I Design Ltd Chevron Ltd	D S Regan BEng I Goldsworthy
20.02.14	SI157007_RPT Revision C	SRS included as Section 6 in SIS Design document Revised for new panel trip amplifiers.	P&I Design Ltd Chevron Ltd	D S Regan BEng I Goldsworthy

Activity History – Terminal in Local Fuel PLC ownership				
Date	Reference	Description	Roles	Persons assigned
11.02.15	LF364005_RPT Revision A	Original Issue	P&I Design Ltd Local Fuel	D S Regan BEng L Salvidge
05.05.15	LF364005_RPT Revision B	Revised following SIS Design	P&I Design Ltd Local Fuel	D S Regan BEng L Salvidge

8.3 Safety Requirement Specification Verification History

Lifecycle phase in Figure 1	Verification - Terminal in Chevron/Valero ownership
9	Utilise QSF010_SIS – Stage 1 – Safety Requirement Specification - Checklist 1
Verification Checklist	Notes
SI157105_RPT Revision A – Compliance Document - Section 4	QSF010 did not exist under Chevron ownership, all checklist were contained in a compliance document

9 FUNCTIONAL SAFETY ASSESSMENT – STAGE 1

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.

9.1 Functional Safety Assessment Stage 1 Requirements

Lifecycle phase in Figure 1	Activity			
10	Functional Safety Assessment Stage 1			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To investigate and arrive at a judgement on the functional safety achieved by the SIS.	Planning for SIS functional safety assessment LOPA SRS	Results of SIS functional safety assessment	Functional Safety Assessment Stage 1 Document	Functional Safety Manager FSA Chairperson FSA Team
Functional Safety Assessment				

Proposed Agenda:
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 defined in the SRS.
- The SRS fully defines the Safety Instrumented System and the safety instrumented functions necessary to achieve the required functional safety;
- That a software safety requirements specification shall be derived from the SRS;
- That project design change procedures are in place and properly implemented.
- Plans or strategies for implementing further FSA's are in place

9.2 Functional Safety Assessment Stage 1 Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership		
Date	Reference	Description
		A Functional Safety Assessment Stage 1 was not conducted.

10 DESIGN & DEVELOPMENT OF SIS

10.1 Design and Engineering Requirements

Lifecycle phase in Figure 1	Activity				
4	SIS design and engineering				
Objectives		Inputs	Outputs	Deliverables	Responsible persons and or organisations
To design the SIS to meet the requirements for safety instrumented functions and safety integrity.		SIS functional and integrity requirements by system. Software safety requirements. Subsystem failure rates.	Design of SIS to functional and integrity requirements. SIS integration test plan. SIF reliability calculations and HFT report. SIS operations & maintenance plan including proof test intervals.	Safety Instrumented System. Safety Instrumented System Manual.	Functional Safety Manager Designers SIS Supplier
Lifecycle phase in Figure 1	Verification Plan				
9	Utilise QSF011_SIS – Stage 2 – Safety Instrument Design - Checklist 2 - General				
9	Utilise QSF012_SIS – Stage 2 – Safety Instrument Design - Checklist 3 – Components & Sub-Systems				
9	Utilise QSF013_SIS – Stage 2 – Safety Instrument Design - Checklist 4 – Interfaces				
Lifecycle phase in Figure 1	Validation Verification Plan				
9/9a	Utilise QSF014_SIS – Stage 3 – SIS Validation - Checklist 5 – Factory Acceptance Test – Planning				
9/9a	Utilise QSF015_SIS – Stage 3 – SIS Validation - Checklist 6 – Factory Acceptance Test				
9/9a	Utilise QSF016_SIS – Stage 2 – SIS Validation - Checklist 7 – Installation & Pre-Commissioning (Prior to SAT)				

10.2 Design and Engineering Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
18.08.08	SI157007_RPT Revision A	Gasoline Overfill Protection Safety Instrument System Manual Original Issue	P&I Design Ltd Simon Management Ltd	D S Regan BEng I Goldsworthy
23.03.10	SI157007_RPT Revision B	Gasoline Overfill Protection Safety Instrument System Manual Revised Post Installation	P&I Design Ltd Chevron Ltd	D S Regan BEng I Goldsworthy
20.02.14	SI157007_RPT Revision C	Gasoline Overfill Protection Safety Instrument System Manual Revised for new panel trip amplifiers	P&I Design Ltd Chevron Ltd	D S Regan BEng I Goldsworthy

Activity History – Terminal in Local Fuel PLC ownership				
Date	Reference	Description	Roles	Persons assigned
27.05.14	LF364006_RPT Revision A	Original Issue	P&I Design Ltd Local Fuel	D S Regan BEng L Salvidge

10.3 Design and Engineering Verification History

Lifecycle phase in Figure 1	Verification	
9	Utilise QSF011_SIS – Stage 2 – Safety Instrument Design - Checklist 2 - General	
9	Utilise QSF012_SIS – Stage 2 – Safety Instrument Design - Checklist 3 – Components & Sub-Systems	
9	Utilise QSF013_SIS – Stage 2 – Safety Instrument Design - Checklist 4 – Interfaces	
SI157105_RPT Revision A – Compliance Document - Section 5 – Checklist 2 - General		QSF011 did not exist under Chevron ownership, all checklist were contained in a compliance document
SI157105_RPT Revision A – Compliance Document - Section 5 – Checklist 3 – Components & Sub Systems		QSF012 did not exist under Chevron ownership, all checklist were contained in a compliance document
SI157105_RPT Revision A – Compliance Document - Section 5 – Checklist 4 – Interfaces		QSF013 did not exist under Chevron ownership, all checklist were contained in a compliance document

10.4 Design and Engineering Validation Verification History

Lifecycle phase in Figure 1	Validation - Terminal in Chevron/Valero ownership	
9/9a	Utilise QSF014_SIS – Stage 3 – SIS Validation - Checklist 5 – Factory Acceptance Test – Planning	
9/9a	Utilise QSF015_SIS – Stage 3 – SIS Validation - Checklist 6 – Factory Acceptance Test	
9/9a	Utilise QSF016_SIS – Stage 2 – SIS Validation - Checklist 7 – Installation & Pre-Commissioning (Prior to SAT)	
SI157105_RPT Revision A – Compliance Document - Section 6 – Checklist 5 – FAT - Planning		QSF014 did not exist under Chevron ownership, all checklist were contained in a compliance document
SI157105_RPT Revision B – Compliance Document - Section 6 – Checklist 6 – FAT		QSF015 did not exist under Chevron ownership, all checklist were contained in a compliance document
SI157105_RPT Revision B – Compliance Document - Section 6 – Checklist 7 – Installation & Pre-Commissioning (Prior to SAT)		QSF016 did not exist under Chevron ownership, all checklist were contained in a compliance document

11 FUNCTIONAL SAFETY ASSESSMENT – STAGE 2

Stage 2 - After the SIS has been designed

11.1 Functional Safety Assessment Stage 2 Requirements

Lifecycle phase in Figure 1	Activity				
10	Functional Safety Assessment Stage 2				
Objectives		Inputs	Outputs	Deliverables	Responsible persons and or organisations
To investigate and arrive at a judgement on the functional safety achieved by the SIS.		Planning for SIS functional safety assessment SRS Design Manual PFD & SIL Verification Calculations	Results of SIS functional safety assessment	Functional Safety Assessment Stage 2 Document	Functional Safety Manager FSA Chairperson FSA Team
Functional Safety Assessment					
Proposed Agenda: The FSA will address the following as a minimum: • The recommendations and actions arising from the Stage 1 FSA have been resolved and completed; • That project design change procedures are in place and properly implemented. • The SIS is designed in accordance with the SRS, any differences to be identified and resolved. • Plans or strategies for implementing further FSA's are in place.					

11.2 Functional Safety Assessment Stage 2 Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership		
Date	Reference	Description
		A Functional Safety Assessment Stage 2 was not conducted.

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

12 INSTALLATION, COMMISSIONING AND VALIDATION

12.1 SIS Installation, Commissioning and Validation Requirements

Lifecycle phase in Figure 1	Activity			
5	Installation, Commissioning and Validation			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity	SIS design SIS integration test plan SIS safety requirements Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS design Results of SIS integration tests Results of the installation, commissioning and validation activities	Fully functioning SIS Safety Instrumented System Manual with all testing documentation included	Functional Safety Manager Designers SIS Supplier
Lifecycle phase in Figure 1	Validation Verification Plan			
9/9a	Utilise QSF017_SIS – Stage 3 – SIS Validation - Checklist 8 – Site Acceptance Test			

12.2 SIS Installation, Commissioning and Validation Action History

12.2.1 SIS Test Procedures

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
10.04.08	SI157035_RPT Revision A	SIS Panel FAT Procedure - Original Issue	P&I Design Ltd	D S Regan BEng D R Ransome
09.07.08	SI157035_RPT Revision B	SIS Panel FAT Procedure – Panel Test	P&I Design Ltd	D S Regan BEng D B Faulkner
22.10.13	SI157035_RPT Revision C	SIS Panel FAT Procedure	P&I Design Ltd	D S Regan BEng D B Faulkner
26.03.08	SI157036_RPT Revision A	SIS Shutdown Conditions Functional Test Procedure – Original Issue	P&I Design Ltd	D S Regan BEng D R Ransome
17.11.08	SI157036_RPT Revision B	SIS Shutdown Conditions Functional Test Procedure – Tankside Valves Removed	P&I Design Ltd	D S Regan BEng D R Ransome
27.07.12	SI157036_RPT Revision C	SIS Shutdown Conditions Functional Test Procedure – Wet Testing Added	P&I Design Ltd	D S Regan BEng D B Faulkner
30.07.12	SI157036_RPT Revision D	SIS Shutdown Conditions Functional Test Procedure – Wet Testing Corrected	P&I Design Ltd	D S Regan BEng D B Faulkner
28.04.08	SI157037_RPT Revision A	SIS Documentation & Hardware Verification Test Procedure – Original Issue	P&I Design Ltd	P Lynch D R Ransome
09.05.11	SI157037_RPT Revision B	SIS Documentation & Hardware Verification Test Procedure – 2011 Testing Update	P&I Design Ltd	P Lynch D S Regan BEng
08.06.12	SI157037_RPT Revision C	SIS Documentation & Hardware Verification Test Procedure – 2012 Testing Update	P&I Design Ltd	P Lynch D S Regan BEng
26.03.08	SI157038_RPT Revision A	SIS Power Failure Functional Testing Procedure – Original Issue	P&I Design Ltd	D S Regan BEng D R Ransome
17.11.08	SI157038_RPT Revision B	SIS Power Failure Functional Testing Procedure – Tankside Valves Removed	P&I Design Ltd	D S Regan BEng D R Ransome
23.07.12	SI157038_RPT Revision C	SIS Power Failure Functional Testing Procedure – Tank 3 Relay No Corrected	P&I Design Ltd	D S Regan BEng D R Ransome

09.05.11	SI157211_RPT Revision A	SIS Drexelbrook PCB Replacement & Testing Procedure – Original Issue	P&I Design Ltd	P Lynch D S Regan BEng

Activity History – Terminal in Local Fuel PLC ownership				
Date	Reference	Description	Roles	Persons assigned
20.05.15	LF364011_RPT Revision A	LFS-SIS1 Documentation Verification	P&I Design Ltd	D B Faulkner M Morgan
20.05.15	LF364012_RPT Revision A	LFS-SIS1 Shutdown Conditions Proof Testing	P&I Design Ltd	D B Faulkner M Morgan

12.2.2 SIS Panel Factory Acceptance Tests

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
09.07.08	SI157035_RPT Revision B Controlled Copy 09.07.08	SIS Panel FAT	P&I Design Ltd	S Micklewright
25.10.13	SI157035_RPT Revision C Controlled Copy 23.10.13	SIS Panel FAT	P&I Design Ltd	D B Faulkner

12.2.3 SIS Shutdowns Conditions Functional Testing

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
11.09.08	SI157036_RPT Revision B Controlled Copy 17.11.08	SIS Shutdown Conditions Functional Testing	P&I Design Ltd	P Lynch
11.09.08	SI157037_RPT Revision A Controlled Copy 17.11.08	SIS Documentation & Hardware Verification	P&I Design Ltd	P Lynch
11.09.08	SI157038_RPT Revision B Controlled Copy 17.11.08	SIS Power Failure Testing	P&I Design Ltd	P Lynch
19.05.11	SI157211_RPT Revision A Controlled Copy 11.05.11	SIS PCB Replacement Testing	P&I Design Ltd	P Lynch
19.05.11	SI157037_RPT Revision B Controlled Copy 11.05.11	SIS Documentation & Hardware Verification	P&I Design Ltd	P Lynch
19.05.11	SI157036_RPT Revision B Controlled Copy 11.05.11	SIS Shutdown Conditions Functional Testing	P&I Design Ltd	P Lynch
15.06.12	SI157037_RPT Revision C Controlled Copy 08.06.12	SIS Documentation & Hardware Verification	P&I Design Ltd	P Lynch

15.06.12	SI157036_RPT Revision B Controlled Copy 08.06.12	SIS Shutdown Conditions Functional Testing	P&I Design Ltd	P Lynch
18.11.13	SI157037_RPT Revision C Controlled Copy 15.11.13	SIS Documentation & Hardware Verification Test Procedure	P&I Design Ltd	D R Pearson D B Faulkner
19.11.13	SI157036_RPT Revision D Controlled Copy 08.11.13	SIS Shutdown Conditions Functional Testing	P&I Design Ltd	D R Pearson D B Faulkner

12.3 Post Installation

Upon Completion of the installation, commissioning and validation, and prior to wet commissioning, the installation is to be tested and the design to be verified and all completed documentation is to be reviewed.

12.3.1 Installation and Commissioning Verification History

Lifecycle phase in Figure 1	Validation - Terminal in Chevron/Valero ownership	
9/9a	Utilise QSF017_SIS – Stage 3 – SIS Validation - Checklist 8 – Site Acceptance Test	
SI157105_RPT Revision A – Compliance Document - Section 6 – Checklist 8 – Site Acceptance Test		QSF017 did not exist under Chevron ownership, all checklist were contained in a compliance document

13 TRAINING

Local Fuel plc 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

13.1 Training Requirements

Lifecycle phase in Figure 1	Activity			
	Training			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To ensure all operations and maintenance staff are aware of BS EN 61511 and to carry out there responsibilities competently.	SIS design BS EN 61511 awareness training Site specific toolbox training	Awareness training package On the job training	Operators and maintenance staff competent in their roles within the SIS	Functional Safety Manager

13.2 Training History

Activity History – Terminal in Texaco/Chevron/Valero ownership			
Date	Description	Trainer	Trainees
17-18/11/2008	Training Course on Brighton Terminal Tank Overfill Safety Instrumented System	D S Regan	Dave Crook Dan Newman Neil Perry Ian Goldsworthy Lawrence Wade Dave Winser Dan Parsons

14 FUNCTIONAL SAFETY ASSESSMENT – STAGE 3

Stage 3 FSA - After the installation, pre-commissioning and final validation of the SIS has been completed and operating and maintenance procedures have been developed.

14.1 Functional Safety Assessment Stage 3 Requirements

<table>
<tr><td>Lifecycle phase in Figure 1</td><td colspan="5">Activity</td></tr>
<tr><td>10</td><td colspan="5">Functional Safety Assessment Stage 3</td></tr>
<tr><td colspan="2">Objectives</td><td>Inputs</td><td>Outputs</td><td>Deliverables</td><td>Responsible persons and or organisations</td></tr>
<tr><td colspan="2">To investigate and arrive at a judgement on the functional safety achieved by the SIS</td><td>Planning for SIS functional safety assessment

SRS

Design Manual

As Built Documentation

PFD & SIL Verification Calculations</td><td>Results of SIS functional safety assessment</td><td>Functional Safety Assessment Stage 3 Document</td><td>Functional Safety Manager

FSA Chairperson

FSA Team</td></tr>
<tr><td colspan="6">Functional Safety Assessment</td></tr>
<tr><td colspan="6">Proposed Agenda:
The FSA will address the following as a minimum:
• The recommendations and actions arising from the Stage 1 & 2 FSA have been resolved and completed;
• That 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;</td></tr>
</table>

14.2 Functional Safety Assessment Stage 3 Action History

<table>
<tr><td colspan="5">Activity History – Terminal in Texaco/Chevron/Valero ownership</td></tr>
<tr><td>Date</td><td>Reference</td><td>Description</td><td>Roles</td><td>Persons Assigned</td></tr>
<tr><td>27.06.08</td><td>SI157001.RPT</td><td>A Functional Safety Assessment Stage 3 was conducted for all terminals in a joint assessment.</td><td>Chair
FSA Team
FSA Team</td><td>D R Ransome BA CEng FInstMC – P & I Design Ltd
I Goldsworthy – Facility Engineer – Chevron Ltd
D S Regan BEng – Process Engineer – P & I Design Ltd</td></tr>
</table>

15 OPERATION AND MAINTENANCE

Local Fuel plc are responsible for operating and maintaining the SIS in order that it's performance does not degrade.

15.1 Operation and Maintenance Requirements

Lifecycle phase in Figure 1	Activity			
6	Operation and Maintenance			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To ensure that the functional safety of the SIS is maintained during operation and maintenance.	SIS functional and integrity requirements SIS operations and maintenance plan including proof test intervals	SIFs actual functionality and integrity Any required changes to testing Scope of any required modifications to maintain integrity	Proof Testing Reports Fully functioning SIS	Functional Safety Manager
Lifecycle phase in Figure 1	Verification Plan			
9	Utilise QSF018_SIS – Stage 4 – Safety Instrument Operation & Maintenance Checklist 9 - Operation & Management			
9	Utilise QSF019_SIS – Stage 4 – Safety Instrument Operation & Maintenance Checklist 10 – Proof Testing & Maintenance			

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

15.2 Operation and Maintenance Action History

15.2.1 SIS Testing Plan

Activity History – Terminal in Local Fuel PLC ownership				
Date	Reference	Description	Roles	Persons assigned
20.05.15	LF364013_RPT Revision A	SIS Operation, Maintenance and Modification Lifecycle	P&I Design Ltd	D B Faulkner M Morgan

15.2.2 SIS Shutdown Conditions Functional Test

Activity History - Terminal in Local Fuel plc ownership				
Date	Reference	Description	Roles	Persons assigned
02.11.14	SI157037_RPT Revision C Controlled Copy 25.11.14	SIS Documentation and Hardware Verification Procedure	P&I Design Ltd Local Fuel plc	D R Pearson M Morgan L Salvidge
03.11.14	SI157036_RPT Revision D Controlled Copy 25.11.14	SIS Shutdown Conditions Functional Test Procedure	P&I Design Ltd Local Fuel plc	D R Pearson M Morgan L Salvidge

15.3 Operation and Maintenance Verification History

Lifecycle phase in Figure 1	Verification
9	Utilise QSF018_SIS – Stage 4 – Safety Instrument Operation & Maintenance Checklist 9 - Operation & Management
9	Utilise QSF019_SIS – Stage 4 – Safety Instrument Operation & Maintenance Checklist 10 – Proof Testing & Maintenance
SI157105_RPT Revision A – Compliance Document - Section 7 – Checklist 9 - Operation & Management	QSF018 did not exist under Chevron ownership, all checklist were contained in a compliance document
SI157105_RPT Revision A – Compliance Document - Section 7 – Checklist 10 – Proof Testing & Maintenance	QSF019 did not exist under Chevron ownership, all checklist were contained in a compliance document

16 FUNCTIONAL SAFETY ASSESSMENT – STAGE 4

Stage 4 – After gaining experience in operating and maintenance.

16.1 Functional Safety Assessment Stage 4 Requirements

Lifecycle phase in Figure 1	Activity			
10	Functional Safety Assessment Stage 4			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To investigate and arrive at a judgement on the functional safety achieved by the SIS	Planning for SIS functional safety assessment SRS Design Manual Testing Records Report of all activations, spurious trips, failures and maintenance activities	Results of SIS functional safety assessment	Functional Safety Assessment Stage 4 Document	Functional Safety Manager FSA Chairperson FSA Team
Functional Safety Assessment				

Proposed Agenda:
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;

16.2 Functional Safety Assessment Stage 4 Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership		
Date	Reference	Description
		A Functional Safety Assessment Stage 4 was not conducted. Discussions on the management of functional safety and review of each terminal was conducted by the SIS Safety Committee.

17 MODIFICATION

17.1 Modification Requirements

Lifecycle phase in Figure 1	Activity			
7	Modification			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained.	Scope of any required modifications to maintain integrity	As-built documentation, records and back-ups.	Modified SIS.	Functional Safety Manager
Lifecycle phase in Figure 1	Verification Plan			
9	Utilise QSF020_SIS – Stage 5 – Safety Instrument System Modification Checklist 11 - Modifications			

17.2 Modification Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons assigned
09.05.11	SI157211_RPT Revision A	Drexelbrook Level Switch PCB Replacement Test Procedure	P&I Design Ltd Simon Management Ltd	D S Regan BEng I Goldsworthy
11.05.11	SI157211_RPT Revision A Controlled Copy	Drexelbrook Level Switch PCB Replacement Test Procedure Results	P&I Design Ltd Simon Management Ltd	P Lynch I Goldsworthy
16.01.12	SI157052_RPT Revision A	Trip Amplifier Wiring Modifications	P&I Design Ltd Chevron Ltd	P Lynch I Goldsworthy

17.3 Modification Verification History

Lifecycle phase in Figure 1	Verification
9	Utilise QSF020_SIS – Stage 5 – Safety Instrument System Modification Checklist 11 - Modifications
SI157105_RPT Revision A – Compliance Document - Section 8 – Checklist 11 – Modifications	QSF020 did not exist under Chevron ownership, all checklists were contained in a compliance document.

18 FUNCTIONAL SAFETY ASSESSMENT – STAGE 5 MODIFICATION

Stage 5 – After modification and prior to decommissioning of the SIS.

18.1 Functional Safety Assessment Stage 5 Requirements

<table>
<tr><td>Lifecycle phase in Figure 1</td><td colspan="5">Activity</td></tr>
<tr><td>10</td><td colspan="5">Functional Safety Assessment Stage 5</td></tr>
<tr><td colspan="2">Objectives</td><td>Inputs</td><td>Outputs</td><td>Deliverables</td><td>Responsible persons and or organisations</td></tr>
<tr><td colspan="2">To investigate and arrive at a judgement on the functional safety achieved by the SIS</td><td>Planning for SIS functional safety assessment

SRS

Design Manual

Management of Change procedure for modification</td><td>Results of SIS functional safety assessment</td><td>Functional Safety Assessment Stage 5 Document</td><td>Functional Safety Manager

FSA Chairperson

FSA Team</td></tr>
<tr><td colspan="6">Functional Safety Assessment</td></tr>
<tr><td colspan="6">Proposed Agenda:
The FSA will address the following as a minimum:
The recommendations and actions arising from the Stage 1, 2, 3 & 4 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;</td></tr>
</table>

18.2 Functional Safety Assessment 5 Action History

<table>
<tr><td colspan="3">Activity History</td></tr>
<tr><td>Date</td><td>Reference</td><td>Description</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

19 DECOMMISSIONING

19.1 Decommissioning Requirements

Lifecycle phase in Figure 1	Activity			
8	Decommissioning			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To ensure that safety instrumented functions remain appropriate during decommissioning and that safety integrity of interfacing systems is not compromised.	Decommissioning plan. As-built SIS and process information	SIS and SIFs placed out of service	Decommissioned SIS.	Functional Safety Manager
Lifecycle phase in Figure 1	Verification Plan			
9	Utilise QSF021_SIS – Stage 5 – Safety Instrument System Decommissioning Checklist 12 - Decommissioning			

19.2 Decommissioning Action History

Activity History				
Date	Reference	Description	Roles	Persons assigned

19.3 Decommissioning Verification History

Lifecycle phase in Figure 1	Verification
9	Utilise QSF020_SIS – Stage 5 – Safety Instrument System Modification Checklist 12 - Decommissioning
SI157105_RPT Revision A – Compliance Document - Section 8 – Checklist 12 – Decommissioning	QSF021 did not exist under Chevron ownership, all checklist were contained in a compliance document

20 FUNCTIONAL SAFETY ASSESSMENT – STAGE 5 DECOMMISSIONING

Stage 5 – Prior to decommissioning of the SIS.

20.1 Functional Safety Assessment Stage 5 Requirements

Lifecycle phase in Figure 1	Activity			
10	Functional Safety Assessment Stage 5			
Objectives	Inputs	Outputs	Deliverables	Responsible persons and or organisations
To investigate and arrive at a judgement on the functional safety achieved by the SIS	Planning for SIS functional safety assessment SRS Design Manual Management of Change procedure for modification	Results of SIS functional safety assessment	Functional Safety Assessment Stage 5 Document	Functional Safety Manager FSA Chairperson FSA Team
Functional Safety Assessment				

Proposed Agenda:
The FSA will address the following as a minimum:

- The recommendations and actions arising from the Stage 1, 2, 3 & 4 FSA have been resolved and completed;
- The FSA will address the following as a minimum:
  - Review of functional safety during the decommissioning
  - Review the impact of decommissioning

20.2 Functional Safety Assessment 5 Action History

Activity History – Terminal in Texaco/Chevron/Valero ownership				
Date	Reference	Description	Roles	Persons Assigned
02.12.12	SI157301.RPT	A Functional Safety Assessment Stage 5 was conducted on 03.12.2012 due to the anticipated decommissioning of the Brighton Terminal. The decommissioning was later revoked, so some the actions of the FSA remain un-completed and unnecessary.	Chair FSA Team FSA Team	D R Ransome BA CEng FInstMC – P & I Design Ltd I Goldsworthy – Facility Engineer – Chevron Ltd D S Regan BEng – Process Engineer – P & I Design Ltd

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

LOCAL FUEL PLC

SHOREHAM OIL TERMINAL

SAFETY INSTRUMENTED SYSTEM

FUNCTIONAL SAFETY ASSESSMENT STAGE 5

LFS-SIS1

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	15.06.15	D.R. Ransome	Les Salvidge	Client	Prepared for FSA 5 Meeting	
						Document No. **LF364100_RPT**

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION CONTROL

Rev	Description
A	Original Issue prior to FSA Meeting and initial review

2 SCOPE & DEFINITIONS

2.1 Scope

Local Fuel plc – Shoreham Terminal has an Independent High Level Alarm system to provide a SIL 2 rated automatic shutdown system 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 5 "Modification".

2.2 Definitions

The following abbreviations and symbols may be used within this document:

ALARP As low as reasonably practicable
BPCS Basic process control system
BSTG Buncefield Standards Task Group
CCF Common cause failure
COMAH Control of Major Accident Hazards Regulations
DC Diagnostic coverage
EC&I Electrical, Control and Instrumentation
E/E/PE Electrical/electronic/programmable electronic
E/E/PES Electrical/electronic/programmable electronic system
EMC Electro-magnetic compatibility
ESV Emergency Shutdown Valve
FAT Factory acceptance testing
FIT Failure in Time expressed as failures that can be expected in 10^9 device hours of operation
FMEA Failure mode and effects analysis
FMEDA Failure mode effects and diagnostic analysis
FSA Functional Safety Assessment
FPL Fixed program language
FTA Fault tree analysis
FVL Full variability language
HAZOP Hazard and Operability Study
HFT Hardware fault tolerance
HMI Human machine interface

HSE Health & Safety Executive
HSL Health & Safety Laboratories
HRA Hazard risk assessment
HRA Human reliability analysis
IHLA Independent High Level Alarm
LOPA Layer of Protection Analysis
LVL Limited variability language
MIIB Major Incident Investigation Board
MOC Management of Change
MODBUS a serial communications protocol originally published by Modicon
MooN “M” out of “N”
MTBF Mean Time Between Failure
MTTR Mean Time to Repair
P&I Process and Instrumentation
PE Programmable electronics
PES Programmable electronic system
PFD Probability of failure on demand
PFD_{avg} Average probability of failure on demand
PFD_{g} Group probability of failure on demand
PLC Programmable logic controller
PSLG Process Safety Leadership Group
ROSOV Remotely Operated Shutoff Valve
RTC Risk Tolerance Criteria
PVST Partial Valve Stroke Testing
SAT Site acceptance test
SCADA Supervisory Control & Data Acquisition
SFF Safe failure fraction
SIF Safety instrumented function
SIL Safety integrity level
SIS Safety instrumented system
SMS Safety Management System
SRS Safety requirement
T_1 Proof Test Interval
TORA Trip Override Risk Assessment
UPS Uninterruptible Power Supply
β = Common Cause Failure Fraction
β_D = Detected Common Cause Failures
λ = Failure rate (per hour)
λ_D = Dangerous Failure Rate
λ_{DD} = Dangerous Detected Failures
λ_{DU} = Dangerous Undetected Failures
λ_{SD} = Safe Detected Failures
λ_{DU} = Safe Undetected Failures

3 INTRODUCTION

The fuel storage depot is owned and managed by Local Fuel plc and classified as a low tier site under the COMAH Regulations.

In 2014 Local Fuel plc acquired the Shoreham Terminal from Valero Energy. The existing SIS system has been in operation for a number of years, with various reviews and assessments conducted by or on behalf of Valero.

As part of Local Fuel plc responsibility and following reviews of the SIS by the Health & Safety Executive it was decided to update all documentation to reflect the new ownership. As part of these reviews it was also decided to implement a modification on components within the SIS which were not SIL rated to BS EN 61508.

This Functional Safety Assessment builds upon functional safety and lifecycle planning and management by assessing the proposed modifications to the system. It will also review all documentation of the SIS following documentation update to reflect change of ownership as well as the modification.

3.1 Proposed Modification

3.1.1 To replace the final element actuator on valve XV 162 and to update all documentation to reflect the new system owner.

3.1.2 To change the duty on two of the existing gasoline tanks to Marine Oil duty.

3.2 Team Membership

Date of Initial Review – 4th June 2015 at Local Fuel plc, Shoreham Terminal.

The FSA review team:-

Local Fuel plc

Les Salvidge is a Chartered Engineer and a Member of the Energy Institute and a Member of the Institute of Energy Technology. He is the Managing Director of Locals Fuel and has extensive experience in the petroleum industry. He has been acting in an advisory role on HSE at the Shoreham Oil Terminal due to his experience in Health and Safety management.

FSA Chair
D.R. Ransome

David Ransome is a Chartered Engineer and a Fellow of the Institute of Measurement and Control with over 40 years' experience in the Chemical and Process Industry. Formerly the Managing Director of P & I Design Ltd he know has no involvement in projects or day to day running in the business. He served on the Buncefield Standards Task Group and Process Standards leadership Group, together with contributing to the guidance produced for the PSLG final report and CDOIG guidance.

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)".

4.1 Stage 5 Functional Safety Assessment - Modification

Primarily this assessment is to review the changes made by a modification to ensure that the SIS is not compromised by the modification. However, as the system has been in use for several years under Valero ownership and latterly under Local Fuel ownership elements that would have been reviewed in a FSA1, 2 & 4 will be included, as far as practicable.

The FSA will address the following:

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, i.e;

- LOPA
- SRS
- Design
- Installation
- Testing
- Operation
- Maintenance

Review the status of operating manuals and documentation in respect to the implemented modification;
Plans or strategies for implementing further FSA's are in place;

4.2 Actions from Previous FSA and Competent Authority Reports

A FSA Stage 2 was conducted on 19th June 2008 by Chevron (previous company name of Valero). This assessment of the design was conducted for all Valero terminals as the design intent was identical. No actions remain open from this assessment.

A FSA Stage 3 was conducted by way of a compliance document between March 2009 and March 2010 the final issue being revised post installation. No actions remain open from this assessment.

With regard to FSA Stage 4, Valero were in the process of conducting Stage 4 assessments when the decision was taken to either sell or de-commission the terminal, so a FSA Stage 4 has not be conducted at the Shoreham Terminal.

In December 2012 a FSA Stage 5 was initiated for the de-commissioning of the SIS, this FSA was only partly completed as Valero then sold the terminal as opposed to de-commissioning. No actions are therefore relevant to the SIS.

On 30th July 2014 an assessment was conducted by the COMAH Competent Authority.
Nine actions were raised from the assessment of which:

- actions one to seven were related to functional safety,
- action eight related to Automatic Tank Gauging system which provides a layer of protection albeit the system is providing a safety function of low/undefined safety integrity as defined in HSE/SPC/Technical/General/51.
- Action nine related to DSEAR.

The functional safety actions are detailed below, however, not to duplicate with other control documents the action history is not detailed in the assessment, other than showing action status.

Action control for this FSA is conducted utilising a live action tracker called ASANA. This allows up to date status of all actions. A snapshot from ASANA will be appended to this FSA for the status of each action relevant to the issue of the FSA.

HSE Visit Actions

No.	Action	Status
300714/1	**Functional Safety Implementation Plan**	Closed
	Description	
	Gaps were identified against recommended good practice and these have been raised as individual actions (2 through 8). A Functional Safety implementation plan should be produced which identifies how and when these gaps will be closed. The plan should include all the stages of the FS safety lifecycle.	

No.	Action	Status
300714/2	**Management of Functional Safety**	Closed
	Description	
	The Company does not have SIS management policies and procedures in place that describe how the Shoreham Terminal plan, specify, design, install, commission, operate and test SIS. The Company should therefore produce and implement suitable Functional Safety management policies and associated procedures for the Shoreham Terminal. These documents should detail how all the safety lifecycle stages are managed and implemented including defined roles and responsibilities, SIS asset register, obsolescent equipment (end of life), logging true demands, spurious trips, management of change (modification of SIS) and decommissioning.	

No.	Action	Status
300714/3	**Hazard Analysis, SIL Assessment & Safety Requirements Specifications**	Closed
	Description	
	The Company should complete the hazard analysis and SIL assessments for the Shoreham Terminal operations including MLA's, Tanker Loading and Jetty operations. The HA activities should include all credible Major Accident Scenarios and result in the identification of all safety functions. The Company should determine SIS integrity using a suitable SIL assessment technique (stated to be the LOPA). The assessments should consider Human Response, utility failure and IPL's should be independent and reliability data justified and referenced (traceable). Safety Requirements Specifications for each SIS should be produced to include (but not be limited to) documented Safety function, integrity, architecture, response times, operation, diagnostics, inhibits, interfaces, test frequency and MTTR.	

No.	Action	Status
300714/4	**SIS Design and Engineering**	Ongoing
	Description	
	The Company should use the results of the HA and SIL assessment work (Action 300714/3) to; 1. Design new SIS as necessary in alignment with the SIF and SIL requirements identified and documented from the HA and SIL assessment activities. New SIS should conform to benchmark standard BS EN 61511 or equivalent. 2. Perform gap analysis of existing (legacy) systems against the SIF and SIL requirements identified and documented from the HA and SIL assessment activities. The analysis should be used to re-engineer the existing systems where necessary to fulfil the SIS requirements and conform to BS EN 61511 or equivalent as far as is reasonably practicable.	

No.	Action	Status
300714/5	**Installation, Commissioning and Verification**	Ongoing
	Description	
	The Company should use the design and engineering documentation (Action 300714/4) to complete the installation of new and modification (re-engineering) of existing systems where necessary. All SIS should be verified through commissioning and validation activities as appropriate. This should include identification and as-built drawings.	

No.	Action	Status
300714/6	**Operation and Maintenance**	Ongoing
	Description	
	The Company should develop written operating, inspection and maintenance procedures for the SIS on the Shoreham Terminal. Operating procedures should include logging demands, resets and inhibits. Proof testing procedures should be developed to reveal all undiagnosed dangerous failures specific for each SIF, end-to-end, unauthorised modifications, labelling, weathering, erosion, corrosion, security, diagnostics, pass/fail criteria, approvals, defects and follow-up. Consideration should be given to the inspection of the Drexelbrook and Rotork valve ('XV162') in alignment with the manufacturers recommendations. Training should be provided to personnel involved with SIS at the Shoreham Terminal (BS EN 61511, clause 5.2.2).	

No.	Action	Status
300714/7	**Functional Safety Assessment**	Ongoing
	Description	
	The Company should perform a suitable (including suitable independence) Functional Safety Assessment on all SIS on the Shoreham Terminal. For new systems this will be at minimum stage 3 (before the identified hazard is introduced), for legacy systems this may need to be a stage 4 assessment.	

4.3 Proposed Modification

The FSA Meeting was held at the terminal on 4th June 2015. The purpose of the meeting was to review the proposed modification and identify all requirements to ensure the modification was performed in accordance with BS EN 61511 and did not compromise functional safety.

4.4 Description of the Modification

a). Replacement of a non SIL certified component with a BS EN 61508 certified component and update of all appropriate lifecycle documentation. This involves replacement of the electro-hydraulic actuator on XV 162.
b). Currently gasoline is imported to Tanks 1, 2, 3 & 4. It is intended that gasoline in future will only be imported into Tanks 1 & 3 and that Tanks 2 & 4 will be converted to Marine Gas oil service. As a result of this the SIS requires modifying to remove Tanks 2 & 4 from operating XV 162. Tanks 2 & 4 will retain their sensors and become alarm only, they will however, be proof tested in line with the SIS.

4.5 Reason for the Modification

a). As part of the HSE inspection visit see Action 4 above. The fact that a single valve is installed on a SIL 2 system requires further justification for a non BS EN 61508 certified component. This requires specific consideration (hardware fault tolerance) which was justified under Valero ownership by ‘proven in use’ data i.e. extensive use of that type of valve across their terminals worldwide for many years. Local Fuel can not use that justification and this means that either a second valve is required or use equipment having an BS EN 61508 certificate. For the final element components, the PEKOS ball valve does have certification, although the current actuator is not SIL certified the new equivalent Rotork actuator has obtained certification. Following discussions with Rotork they advise that it does not apply retrospectively and as such it has been decided that a replacement of the actuator will be necessary to gain compliance of the overall system in providing SIL 2 capability with HFT = 0. In addition Valero has a spare actuator in their UK facilities. Local Fuel do not have a spare actuator and as such, the lack of a spare could result in the MTTR being unacceptable. This could further impact on terminal operations effectively shutting down the terminal due to a single failure. In order to satisfy all of these constraints it is intended to replace the actuator and utilise the non-SIL rated actuator as a spare in the unlikely event of the SIL rated actuator failing and not being able to be repaired by the UK facility of the manuafacturer. Local Fuel appreciate that additional management procedures may need to be implemented should the change over be required until the SIL rated actuator is returned to service. This should produce a MTTR in accordance with the SIL verification of within 24 hours.

b). Current company strategy is diversity in the Terminal and as the quantities of gasoline have reduced the extra storage capacity will be utilised for Marine Gas oil because recent legislation has increased the demand for MGO in the location.

4.6 Hazards Which May Be Affected By The Modification

No change in the hazard perceived.

a). The Rotork actuator should perform identically to the existing installed device. However, there may be subtle differences within the actuators firmware and as such the complete system is to be proof tested following completion of the installation.

The sensors and logic solver are as original for Tanks 1, 2, 3 & 4 gasoline tanks.

Distillate tanks 5, 6, 7, 8, 9, 10, 11, 18. 18A, 21 & 22 utilise RF technology sensors but are alarm only.

b). The change of Tank duty will reduce the terminals current capacity for the storage of gasoline from four to two tanks. This was addressed in the LOPA report LF364002_RPT.

4.7 The Impact On Functional Safety

a). As this is a change of actuator it is essential that it performs as specified. Checks must be completed to ensure that systematic failures are not induced through the design phase, and manufacturing phases, including:

- Ensure sufficient oversizing and torque to close against ships pumps
- Ensure slow closing not to induce pressure surge issues in import line
- Confirm failures mode operation including loss of power

b). No impact on functional safety is perceived from the reduction in gasoline storage.

4.8 Approvals For The Modification and Competencies

For the modification, Local Fuel MOC's will be completed and this FSA Stage 5 will be conducted to ensure compliance to functional safety and to BS EN 61511 lifecycle.

4.9 Timescale and Timelines

a). At the FSA meeting it was advised that the Rotork is on a long delivery. However, design has commenced with the Safety Requirement Specification having been updated.
The documentation has been revised with the references to Chevron/Valero being removed and creating new issue drawings for Local Fuel plc. These drawings at Revision A will be reviewed by this FSA. It may become necessary to revise them further for the modifications.

4.10 Verification Process To Ensure Proper Implementation

The design is to be verified by the designer in accordance with the quality and management of functional safety policies and in accordance with BS EN 61511. At the design stage testing documentation is to be produced the purpose of which is to provide a series of testing procedures which will ensure that the probability of failure on demand figure of the installed system is maintained through the operating life of the SIS. Where known, dangerous undetected failures should be identified and a method of detecting for these included within the testing regime.

In addition necessary FAT and SAT are to be conducted to ensure the installed system performs in the required manner.

All testing documentation to be reviewed as part of this FSA on completion of the modification.

Local Fuel plc will also utilise their documents LF363003_RPT – Policy & Lifecycle Activities and LF363004_RPT – SIS Safety Plan for Management of Functional safety purposes.

4.11 SIS Lifecycle Requirements Of The Modification

As stated previously all lifecycle documentation is being updated and as such is to be reviewed as part of this FSA.

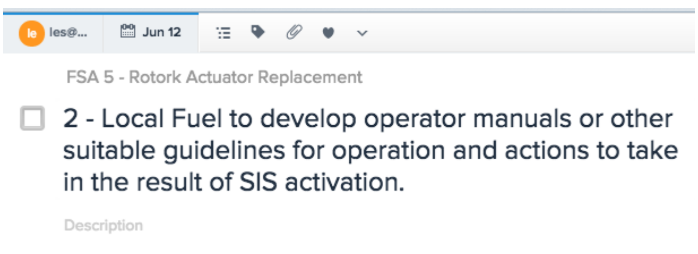
4.12 Documentation That Will Require Updating:

Layer of Protection Analysis – depending on outcome of Action 1.
Safety Requirement Specification
System Verification Document
Loop Drawings
Cable & Wiring Drawings
Testing Documentation
Management of Functional Safety Document

4.13 Operating Manuals And Documentation

All design documentation is to be re-issued together with manufacturers maintenance manuals. Local Fuel to develop operator manuals or other suitable guidelines for operation and actions to take in the result of SIS activation.

Action 2:



4.14 Training Requirements Following Modification

Local Fuel employees who were originally employed by Valero have already been provided with SIS awareness and on the job training.

Additional awareness training was conducted on 4th June 2015 to Local Fuel plc employees with further on the job training following installation of the modified system.

5 REVIEW OF REVISED LIFECYCLE DOCUMENTATION

5.1 Layer of Protection Analysis

The LOPA has been reviewed and accepted by the HSE. The SIL 2 Overfill Protection System within the LOPA was estimated with a PFD of 0.005.

5.2 Safety Requirement Specification

Although this FSA is a Stage 5, it was decided to fully review all documentation, not just that required as part of the modification. This was decided upon as all documentation has been re-issued for Local Fuel plc and is effectively new issues.

In order to ensure compliance to BS EN 61511 the SRS was reviewed as follows:

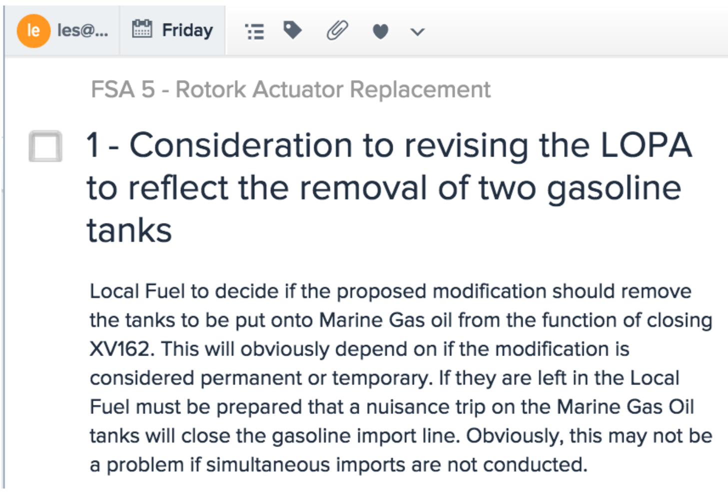
5.2.1 *Do the Safety Instrumented Functions (SIF) derive from a HAZOP or LOPA study, if not where are they derived from. BS EN Clause 8 & 9.*

Section 2.1 of the SRS references the LOPA and the requirements for a SIL 2 SIS to be installed on the gasoline tanks.

5.2.2 *Has the Safety Integrity Level (SIL) for each SIF been allocated. BS EN Clause 9.*

Section 4.6 of the SRS details the SIF requirements for Tanks 1, 2, 3 & 4, which prior to the proposed Marine Gas Oil modification were all available for gasoline. As stated previously the LOPA considered that only two of these tanks would be utilised.

ACTION 1:



5.2.3 *Has the demand on the SIF been specified (demand or continuous). BS EN Clause 10.*

Section 3 of the SRS confirms that the system is a low demand SIS with a demand on the SIF of no more frequently that one in every ten years.

5.2.4 *Is each SIF described adequately, together with a definition of the safe state. BS EN Clause 10.*

Section 4.6 of the SRS provides information of the function and safe state.

5.2.5 *Have common cause failures been considered. BS EN Clause 10.*

Section 2.3 of the SRS details that the SIF's are non-redundant and as such common cause failure should not be an issue. However, although not really a common cause failure as such, the failure of XV162 is common to all gasoline tanks and as such a total failure of this valve will have the effect of preventing gasoline imports to both tanks.

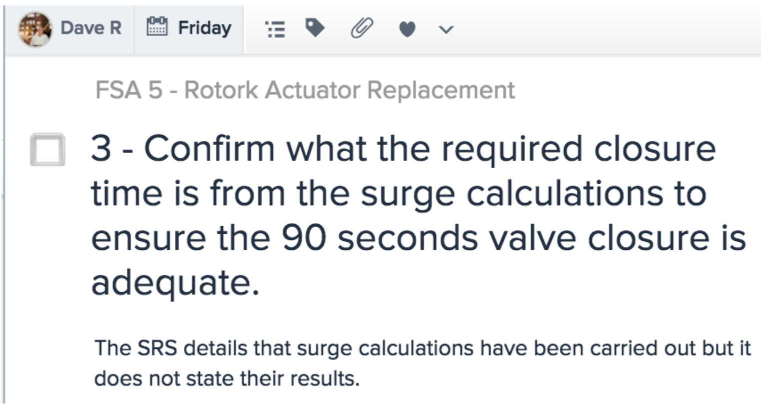
5.2.6 *Have process conditions been considered which could have an effect on the limitations of sensors or final elements. (e.g corrosion, plugging, coating). BS EN Clause 10.*

Section 3 of the SRS defines the conditions likely to have an effect of the SIS.

5.2.7 *Are performance requirements defined. (e.g speed of closure of valve). BS EN Clause 10.*

Section 4.6 of the SRS defines the requirements of slow closure of the final element to prevent pipeline surge. As the actuator is electrically operated there should be no difficulty in achieving the stated 90 seconds closure time. Section 2.3 defines that surge calculations have been carried out but it does not define what the actual safe closure time is.

Action 3:



5.2.8 *Are sensor inputs defined with respect to range, accuracy etc. BS EN Clause 10.*

The SIF operates at a selected location in the tanks and as such is a switch, so no range is required.

5.2.9 *Have the process setpoints and trips been defined. BS EN Clause 10.*

The process setpoint is provided in Section 4.6 of the SRS.

5.2.10 *Is there a description of the relationship between inputs, logic solver and outputs and any specific requirements requiring 1oo2, 2oo2 systems or specific requirements regarding nuisance tripping. BS EN Clause 10.*

Section 2.4 of the SRS provides a simplified system model of the SIF, this together with Section defines the inputs, logic solver and outputs of the SIS.

5.2.11 *Has the mean time to repair been specified with consideration to availability of spares and labour. BS EN 61511 Clause 10.*

Section 3 of the SRS defines a MTTR of 24 hours, it further states that the filling of the tanks are on a batch process with extremely long intervals between imports providing for proof testing and other maintenance to be carried out in these time intervals. Section 4.5 of this FSA defines further the proposed intention of a spare valve.

5.2.12 *Have manual shutdowns been considered. BS EN 61511 Clause 10.*

Section 4.6 of the SRS states that manual shutdown is available by manual control of the valve and also on operation of the ESD pushbutton.

5.2.13 *Is there a requirement for overrides and if so has the effect on the SIF been considered. BS EN Clause 10.*

Section 2.3 of the SRS states that there are no facilities for overriding the SIF.

5.2.14 *Have the interfaces with the Basic Process Control System (BPCS) been defined. BS EN Claus 10.*

Section 4.4 of the SRS defines BPCS interface.

5.2.15 *Can the BPCS interfere with the safe operation of the SIF. BS EN 61511 Clause 10.*

Section 4.4 that the BPCS can have no effect on the operation of the SIS.

5.2.16 *Has the method of resetting the system been defined. BS EN Clause 10.*

Section 3 of the SRS states that automatic reset of the final element shall not be possible.

5.2.17 *Have environmental and abnormal events been considered. (e.g. temperature, humidity, fire etc.) BS EN Clause 10.*

Section 3 of the SRS provides information on the environmental operating parameters of the SIS.

5.2.18 *If the SIS logic solver is software based have the application software requirements been specified. BS EN Clause 10 & 12.*

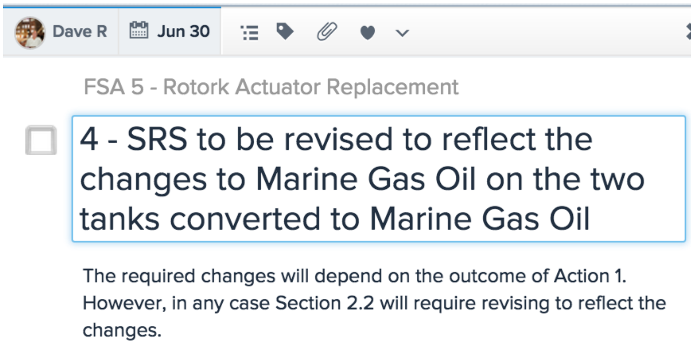
The logic solver is not software based.

5.2.19 SRS Review

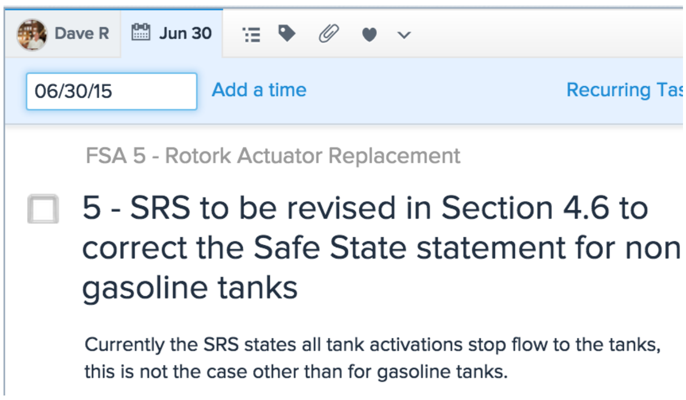
Sections 5.2.1 to 5.2.18 of this FSA review the SRS with respect to it providing the required information to comply with the relevant clauses of BS EN 61511.
The following details are more general review of the SRS in respect to the requirements of the functionality of the SIS.

- Section 2.2 of the SRS details that activation of a high level in any of the four gasoline tanks Tank 1, 2, 3 & 4 will close the common import valve XV162. Activation of any of the remaining Tank high level sensors will provide an alarm. However, Section 4.6 of the SRS contradicts this is stating in the section “Safe State” that they also stop the flow to all tanks.
    - Action 1 previously requires Local Fuel plc to consider if the Tanks to be converted to Marine Gas Oil should operate on the gasoline import valve. The conclusion to this will also have an impact in modifying the SRS to reflect how the modified system is to operate.

Action 4:

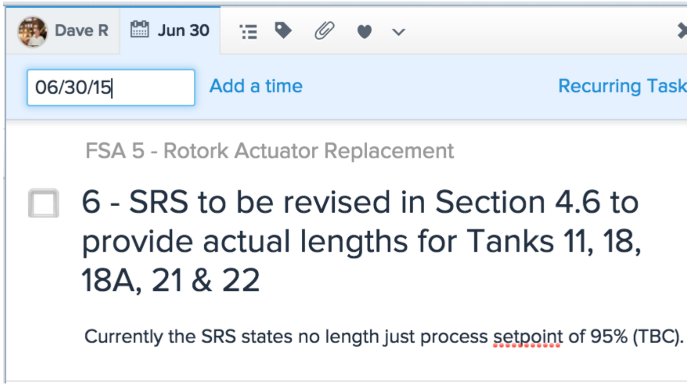


Action 5:



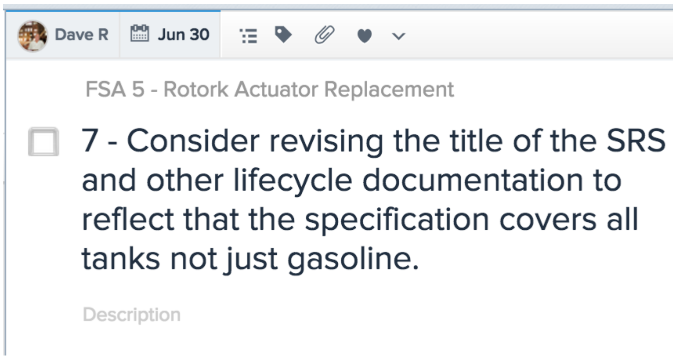
- Section 4.6 details the individual tank activation point for all tanks with the exception of tanks 11, 18, 18A, 21 & 22 were it states 95% (TBC).

Action 6:

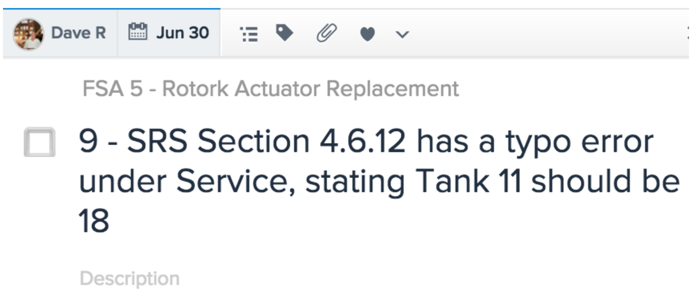


- The title of the SRS and other lifecycle documentation is confusing as it is specific in stating Gasoline Import Safety Instrumented System yet the documents are written for all tanks not just gasoline. The SRS also provides for future individual tankside valves. This obviously derives from the previous owner with future plans to provide individual tank isolation in addition to or opposed to common pipeline isolation.

Action 7:



- Section 4.6.12 – there is a typo error should be Tank 18 not Tank 11 as described in the Service section.



5.3 SIL Verification

Document LF364006_RPT Revision A was reviewed as part of this FSA. It was noted that it has been written for inclusion of the new SIL rated XV162 actuator but not for the later modification for the change of two gasoline tanks to Marine Oil tanks. Again, depending on the outcome of Action 1, this document may also need revising, see also Action 7 regarding the title.

As part of the FSA SIL Verification, the data used to calculate the pfd was reviewed and detailed below:

Sensor:
The sensors employed within the SIS are Drexelbrook Intellipoint RF transmitters providing a 4 – 20mA signal, although this is not analog in normal understanding of analog. The devices utilises this as a carrier signal and depending on the status of the sensor provides a corresponding mA signal: 8mA - Alarm, 16mA - Normal, 22mA – Fault.

The failure data is provided as:

Table 1: Failure rates according to IEC 61508

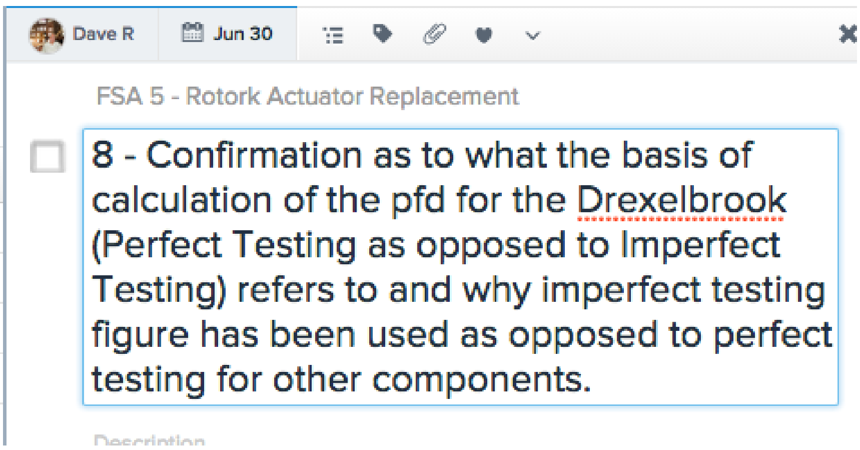
Safety IntelliPoint RF™ Series Point Level Switch	λ^{sd}	λ^{su2}	λ^{dd}	λ^{du}	SFF
High Level Fail Safe application	0 FIT	300 FIT	686 FIT	73 FIT	93.2%

These failure rates are valid for the useful lifetime of the product, see Appendix A.

A user of the Safety IntelliPoint RF™ Series Point Level Switch can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full set of failure rates is presented in section 4.5 along with all assumptions.

The calculation within the SIL Verification document Section 6.5 utilises the above data and confirms that a PFD = $3.38\text{x}10^{-4}$ it is noted that the calculation refers to this pfd being for perfect testing and imperfect testing provides a pfd of $8.57\text{x}10^{-4}$. The device has a SFF of 0.93 and as such satisfies HFT = 0 in accordance with BS EN 61508.

Action 8:



Logic Solver:

As stated in the above section that the sensor provides a 4 – 20mA signal which changes relevant to its status. The safety manual for the sensor requires a logic solver which can monitor and act upon this change of mA signal, it further states that it the signal should be monitored for a 1mA change.

This is provided for within the logic solver by utilising a trip amplifier which is set at 15mA falling and 17mA rising, mA signal outside this range will result in the de-energising of the trip amplifiers relay output which is fed into the coil of a PILZ safety relay.

The pfd data on the Trip Amplifier is:

Acc. Table 3: Summary for the Transmitter Supply Isolators KF-CRG2-*** (relay output)**

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF	DC_S	DC_D
PFD_{AVG} = 3.94E-04	PFD_{AVG} = 7.88E-04	PFD_{AVG} = 1.97E-03	> 83%	3%	50%

λ_{sd} = 9,00E-09 1/h = 9 FIT

λ_{su} = 3,47E-07 1/h = 347 FIT

λ_{dd} = 8,90E-08 1/h = 89 FIT

λ_{du} = 9,00E-08 1/h = 90 FIT

The calculation within the SIL Verification document Section 6.5 utilises the above data and confirms that a $PFD_S = 3.98 \times 10^{-4}$ it is noted that the calculation refers to this pfd being for perfect testing and imperfect testing provides a pfd of 3.94×10^{-4}. The device has a SFF of 0.83 and as such would not satisfy HFT = 0 in accordance with BS EN 61508. However, the device has been assessed and certified by Exida Prior Use against the requirements of BS EN 61511 and is certified as appropriate for a single device in a SIL 2 system.

The second part of the logic solver is a PILZ PNOZ s2 safety relay. The device has internal architecture providing a 1oo2D with internal diagnostic coverage of 99% and providing a SFF of 0.99. In accordance with BS EN 61508 the device can be utilised in a SIL 3 system. However, in accordance with BS EN 61511 the device is limited to SIL 2 for a single device. The pfd is certified as 2.13×10^{-5}.

pilz
more than automation
safe automation

Pilz Automation Technology
Willow House, Medlicott Close
Oakley Hay Business Park, Corby, Northants NN18 9NF
Telephone (01536) 460766 Fax (01536) 460866

Safety Relay Type PNOZ s2
Internal Safety Integrity Details

Description	Type A Logic Subsystem (pre-designed)
Device	Safety Relay
Manufacturer	Pilz Automation
Model	PNOZ s2
BSEN 61508 internal architecture	1oo2D*
Internal Diagnostic Coverage...DC	99%
Safe Failure Fraction..............SFF	99%
Common Cause Failure...........CCF	2%
Sensor Sub-System input	1oo1
$MTTF_L$	5.0E-07
Probability of Dangerous failure on Demand	
BSEN 61508.......PFD	2.13E-05
BSEN61508 Sil claim limit for relay..*SILCL*	3
BSEN61511 Sil claim limit for relay..*SILCL*	3
Probability of Dangerous Failure per Hour	
BSEN61508 .... PFH_D	2.5E-09
BSEN62061 Sil claim limit for relay..SILCL	3
BSEN 954-1 category	4
BSENISO 13849-1performance level.. PL	e
BSENISO 13849-1 category..	4
Proof Test Interval ....T (yrs)	20

Final Element:

The PILZ safety relay provides normally open volt free contacts. A 24V dc supply originating in the Rotork actuator is fed through these contacts and back to the hardwired ESD circuit contained with the actuator. The actuator is capable of being operated remotely, however, without the 24V dc input to the ESD circuit the actually will fail closed.

It is certified to BS EN 61508 by SIRA for use in a SIL 2 SIS with HFT = 0. As it has fairly recently being certified it also has a Systematic Capability assessment with a resulting SC3.

Safety Function: ***'To move the actuator to the end position by means of a spring when the ESD signal is removed'.***					
Summary of clauses 2/7.4.2&2/7.4.4		Best Config Value	Worst Config Value	Average Value	Verdict
Architectural constraints		**HFT=0**			Type A
Safe Failure Fraction (SFF)		**83%**	**87%**	**85%**	SIL 2
Random hardware failures: $[h^{-1}]$	λ_{DD} λ_{DU}	0.00×10^{0} 1.20×10^{-7}	0.00×10^{0} 2.69×10^{-7}	0.00×10^{0} 1.85×10^{-7}	
Random hardware failures: $[h^{-1}]$	λ_{SD} λ_{SU}	0.00×10^{0} 5.80×10^{-7}	0.00×10^{0} 1.80×10^{-6}	0.00×10^{0} 1.07×10^{-6}	
PFD @ PTI = 8760Hrs[1] MTTR = 8 Hrs[1]		**5.27×10^{-4}**	**1.18×10^{-3}**	**8.11×10^{-4}**	SIL 2
Hardware safety integrity compliance		Route 1_H			
Systematic safety integrity compliance		Route 1_S			
Systematic capability		*SC3* (See report 56A28091B)*			
Overall SIL achieved		**SIL 2 due to architectural constraints (SFF)**			

Table 1a: Summary of Failure Data of SI 10

The value used for the actuator in LF364006_RPT utilises the average value from the certified data. This FSA checked what the overall pfd of the SIS would be if the worst case value was used, this changed the PFD_{SYS} form 3.57×10^{-3} to 3.94×10^{-3} which is still within the required 5.00×10^{-3} required from the LOPA.

The second part of the final element sub-system is a PEKOS ball valve. Exida have certified this component as SIL 3 capable. In accordance with BS EN 61511 the device can be used in a SIL 3 with HFT = 1 and SIL 2 with HFT = 0.

	Type A device, IEC 61508 failure rates in FIT $[:=10^{-9}/h]$								
	Full Stroke			Tight Shutoff			Open to trip		
Valve and application	λ_{safe}	λ_{dd}	λ_{du}	λ_{safe}	λ_{dd}	λ_{du}	λ_{safe}	λ_{dd}	λ_{du}
V1 Clean service	1650	0	626	614	0	1662	1834	0	442
V1 Clean service with PVST	1650	292	334	614	292	1370	1834	292	150
V2 Clean service	2092	0	644	1103	0	1633	2276	0	460
V2 Clean service with PVST	2092	303	341	1103	303	1330	2276	303	157
V3 Clean service	1782	0	726	381	0	2127	2056	0	452
V3 Clean service with PVST	1782	298	428	381	298	1829	2056	298	154

PVST - Partial Valve Stroke Test

Calculation Summary:

From the supplied components and BS EN 61508 certification it confirms that the system does comply to the requirements of a PFD and HFT for a SIL 2 SIS, with a PFD_{SYS} of 3.57×10^{-3}.

5.4 Design Documentation

As stated in Section 4.12 the following documentation requires to be modified to reflect the modifications.

5.4.1 Safety Requirement Specification

This is detailed in Section 5.2.

5.4.2 SIL Verification Document

This is detailed in Section 5.3.

5.4.3 Equipment Specifications

Specification Number	Title	Revision
LF364001_SPC	Level Switch – Floating Deck Switching points to be checked with LOC document when received see Action 10.	A
LF364002_SPC	Level Switch – Fixed Roof Switching points to be checked with LOC document when received see Action 10. Actual insertion lengths for Tanks 11, 18, 18A 21 and 22 to be added following Action 10.	A
LF364005_SPC	Annunciator	A
LF364006_SPC	Pipeline Import Valve There is no mention of the valve slow closing on the specification. Reference is made to actuator details appearing on sheet 2, yet sheet 2 is Documentation Requirements, it should say see specification LF364021_SPC	A
LF364007_SPC	Overfill protection/ESD Safety Relays	A
LF346008_SPC	Isolating units	A
LF346009_SPC	Isolating units	A
LF364021_SPC	Valve Actuator Add reference to valve details on LF364006_SPC	A
LF364056_SPC	East Bund SIS AC JB	A
LF364057_SPC	West Bund SIS AC JB	A
LF364058_SPC	East Bund SIS DC JB	A
LF364059_SPC	West Bund SIS DC JB	A
LF364060_SPC	East Bund SIS IS JB	A
LF364061_SPC	West Bund SIS IS JB	A
LF364062_SPC	Additive Tanks SIS IS JB	A

Action 14:

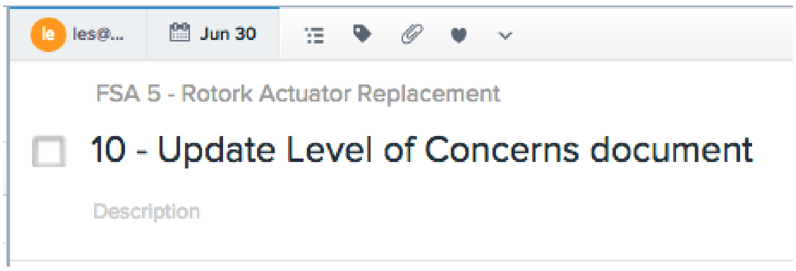
5.4.4 Reports

Report Number	Title	Revision
LF364001_RPT	Functional Safety Implementation Plan This document was specific to Local Fuel implementing improvements to their management and operation of SIS. It is not a lifecycle document and has not been reviewed by this FSA.	B
LF364002_RPT	Layer of Protection Analysis See Action 1.	D
LF364003_RPT	Policy & Lifecycle Activities To be updated.	B
LF364004_RPT	Safety Plan To be updated.	C
LF364005_RPT	Safety Requirement Specification See Section 5.2	B
LF364006_RPT	SIL Verification See Section 5.3	A

5.4.5 IHLA Calculation Sheet

As the products and Tanks are changing there is a requirement to up date the Level of Concerns document which details the Tanks, associated products, alarm activation point and high high alarm setting.

Action 10:



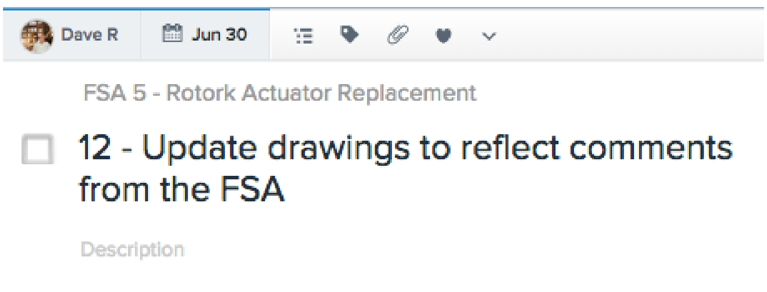
5.4.6 Design Drawings

Drawing Number	Title	Revision
LF364001_DWG	East Bund Cable Overview Drawing XV162 is shown as going to AC JB and XVa62/1 as going to DC JB. These descriptions are reversed and should be XV162 to DC JB and VX162/1 to AC JB. Arrows are shown on tankside VRU valves indicating flow direction, yet they are missing for the import and export valves, add arrows to import and export valves.	A
LF364002_DWG	West Bund Cable Overview Drawing	A
LF364003_DWG	Additive Tanks Cable Overview Drawing	A
LF364004_DWG	East Bund I.S. Junction Box Connection Details	A
LF364005_DWG	West Bund I.S. Junction Box Connection Details	A
LF364006_DWG	Additive Tanks I.S. Junction Box Connection Details	A
LF364007_DWG	East Bund DC Junction Box Connection Details – TB1	A
LF364008_DWG	East Bund DC Junction Box Connection Details – TB2	A
LF364009_DWG	West Bund DC Junction Box Connection Details	A
LF364010_DWG	Valve Power Distribution Board	A
LF364011_DWG	East Bund AC Junction Box Connection Details	A
LF364012_DWG	East Bund AC Junction Box Connection Details – TB2	A
LF364013_DWG	West Bund AC Junction Box Connection Details – TB1	A
LF364014_DWG	West Bund AC Junction Box Connection Details – TB2	A
LF364015_DWG	Site Plan – SIS Equipment	A
LF364016_DWG	Rotork Valve Control Network	A
LF364017_DWG	Alarm Annunciator Connection Details – AN001	A
LF364018_DWG	Alarm Annunciator Connection Details – AN002	A
LF364019_DWG	Alarm Annunciator Connection Details – AN003	A
LF364020_DWG	Logic Panel Drawing 1	A
LF364021_DWG	Logic Panel Drawing 2	A
LF364022_DWG	Logic Panel Drawing 3	A
LF364023_DWG	Logic Panel Drawing 4	A
LF364024_DWG	Logic Panel Drawing 5	A
LF364025_DWG	Logic Panel Drawing 6	A
LF364026_DWG	Logic Panel Drawing 7	A
LF364027_DWG	Logic Panel Drawing 8	A
LF364030_DWG	Logic Panel External Layout	A
LF364031_DWG	Logic Panel Internal Layout	A
LF364040_DWG	Loop Sheet – XV162 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364041_DWG	Loop Sheet – XV123 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364042_DWG	Loop Sheet – XV124 The title is incorrect, this is an export valve not import. There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A

LF364043_DWG	Loop Sheet – XV155 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364044_DWG	Loop Sheet – XV156 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364045_DWG	Loop Sheet – XV121 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364046_DWG	Loop Sheet – XV122 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364047_DWG	Loop Sheet – XV157 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364048_DWG	Loop Sheet – XV158 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364049_DWG	Loop Sheet – XV129 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364050_DWG	Loop Sheet – XV130 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364051_DWG	Loop Sheet – XV159 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364052_DWG	Loop Sheet – XV126 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364053_DWG	Loop Sheet – XV127 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364054_DWG	Loop Sheet – XV160 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364055_DWG	Loop Sheet – XV161 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364010_DWG.	A
LF364056_DWG	Loop Sheet – XV118 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A
LF364057_DWG	Loop Sheet – XV119 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A
LF364058_DWG	Loop Sheet – XV116 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A
LF364059_DWG	Loop Sheet – XV117 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG. The cable number VCOM24 is incorrect it is VCO23.	A
LF364060_DWG	Loop Sheet – XV114 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A

LF364061_DWG	Loop Sheet – XV115 The title does not contain the XV number as do other loop sheets, add XV115 to title. There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A
LF364062_DWG	Loop Sheet – XV110 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A
LF364063_DWG	Loop Sheet – XV111 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364013_DWG.	A
LF364064_DWG	Loop Sheet – XV108 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364014_DWG.	A
LF364065_DWG	Loop Sheet – XV109 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364014_DWG.	A
LF364066_DWG	Loop Sheet – XV106 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364014_DWG.	A
LF364067_DWG	Loop Sheet – XV107 There are two drawings referencing the power distribution to the XV's, loop sheets reference varies, add reference to LF364014_DWG.	A
LF364070_DWG	Loop Sheet – LS01	A
LF364071_DWG	Loop Sheet – LS02	A
LF364072_DWG	Loop Sheet – LS03	A
LF364073_DWG	Loop Sheet – LS04	A
LF364074_DWG	Loop Sheet – LS05	A
LF364075_DWG	Loop Sheet – LS06	A
LF364076_DWG	Loop Sheet – LS07	A
LF364077_DWG	Loop Sheet – LS08	A
LF364078_DWG	Loop Sheet – LS09	A
LF364079_DWG	Loop Sheet – LS10	A
LF364080_DWG	Loop Sheet – LS11	A
LF364081_DWG	Loop Sheet – LS18	A
LF364082_DWG	Loop Sheet – LS18A	A
LF364083_DWG	Loop Sheet – LS21	A
LF364084_DWG	Loop Sheet – LS22	A
LF364075_DWG	Loop Sheet – LS06	A
LF364076_DWG	Loop Sheet – LS07	A
LF364077_DWG	Loop Sheet – LS08	A

Action 12:



5.4.7 Schedules

Schedule Number	Title	Revision
LF364001_SCH	Trip Matrix	A
LF364002_SCH	Instrument Schedule	A
LF364003_SCH	Testing matrix	A
LF364004_SCH	Testing Lifecycle matrix	A
LF364010_SCH	Cable Schedule – Sheet 1 of 2	A
LF364010_SCH	Cable Schedule – Sheet 2 of 2	A

Not reviewed within Revision A of this FSA.

5.4.8 Testing and Inspection Documentation

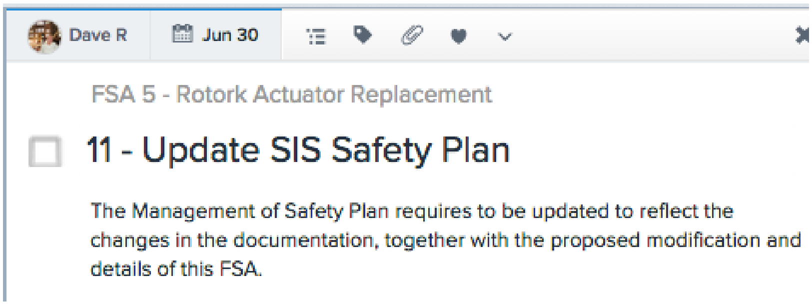
Report Number	Title	Revision
LF364011_RPT	Documentation Verification	A
LF364012_RPT	Shutdown Conditions Proof Testing	A
LF364013_RPT	Operation Maintenance and Modification Lifecycle	A

Not reviewed within Revision A of this FSA.

5.4.9 Management of Functional Safety Document

The Management of Safety Plan requires to be updated to reflect the changes in the documentation, together with the proposed modification and details of this FSA.

Action 11:



5.5 Validation and Testing Documentation

Not reviewed at Revision A of this FSA.

5.6 Operating, maintenance and emergency procedures

During the installation phase, operators are to be made familiar of the changes to the SIS. It is not envisaged that any additional training, other than on the job familiarisation will be required.

Not reviewed at Revision A of this FSA.

5.7 Suitability and Performance of the SIS

5.7.1 Description of Operation

Existing Gasoline Tanks

The SIS is a combination of four (prior to Marine Gas Oil modification) SIF's albeit they are interactive with each other in that operation of any sensor results in the final element going to its safe state. In addition there are eleven other tanks which are fitted with a similar type of SIL rated sensor and utilise the same logic solver albeit just to provide an alarm. The description below just relates to the SIF's on the gasoline tanks, the other tanks utilise the same technique, however, there is no automatic final element, the operator is warned of operation of a high high level by annunciation and on the SCADA system, he is then required to take manual intervention. Annunciation and SCADA repeats are also provided for Tanks 1, 2, 3 & 4.

Each of the four gasoline Tank sensors is connected to a trip amplifier which detects for a change in mA signal from the sensor, although the device is in effect a switch it provides an analog output equating to 8mA = Alarm, 16mA = Normal, 22mA = Fault, the trip amplifier is fitted with two relay output setpoints one at 17mA rising and the other at 15mA falling. Hence, if the sensor output is not above 15mA and below 17mA then the corresponding relay will open circuit. A 24Vdc feed is fed into the trip amplifier and through both relay contacts, the output from the trip amplifier is wired to the coil of a further safety relay via a safety relay contacts which are operated by the site ESD system. The sensor is fitted with an external test facility to simulate high level.

Tank 1:

Sensor – Drexelbrook Intellipoint – Tag Number – LE 01
Trip Amplifier – Pepperl & Fuchs KFD2 – Tag Number – LS 01
Safety Relay – PILZ PNOZ-S2 – Tag Number – R252

Tank 2:

Sensor – Drexelbrook Intellipoint – Tag Number – LE 02
Trip Amplifier – Pepperl & Fuchs KFD2 – Tag Number – LS 02
Safety Relay – PILZ PNOZ-S2 – Tag Number – R292

Tank 3:

Sensor – Drexelbrook Intellipoint – Tag Number – LE 03
Trip Amplifier – Pepperl & Fuchs KFD2 – Tag Number – LS 03
Safety Relay – PILZ PNOZ-S2 – Tag Number – R332

Tank 4:

Sensor – Drexelbrook Intellipoint – Tag Number – LE 04
Trip Amplifier – Pepperl & Fuchs KFD2 – Tag Number – LS 04
Safety Relay – PILZ PNOZ-S2 – Tag Number – R372

The final element wiring comprises a 24Vdc feed fed from XV162 Rotork actuator into Tank 1 Safety Relay which has two positively guided contacts per output, the safety function utilises channel three of the relay. The output from this relay is then fed in series through the safety relays of Tank 2, 3 and 4 all having two positively guided contacts , the output from Tank 4 safety relay is fed back to the ESD circuit of the Rotork actuator.

Each of the safety relays, R252. R292, R332 and R372 require resetting following de-energisation, this is achieved by a reset pushbutton operating onto a relay R805. This ensures that following an activation the system cannot re-open any valve without firstly all level sensors being in their normal mode.

The final element sub-system comprises of an isolator switch located in the field then to the rotork actuator. This isolator isolates the mains supply to the valve.

Gasoline Pipeline:

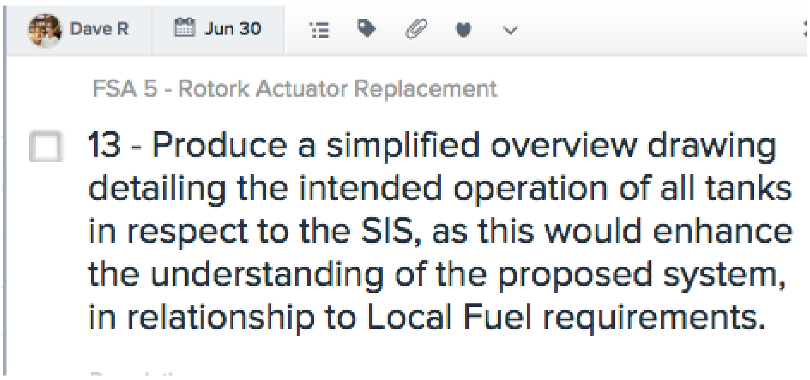
Isolator – Tag Number – HS162
Rotork Actuator and Ball Valve – XV162

There is no facility for overriding the system and it is noted that any spurious trip or sensor fault will result in total shutdown of all four tanks as any sensor activation or fault shuts down the common import valve.

In addition to the shutdown facility of the logic solver with regard to the common pipeline valve, the logic solver has future enhancement built into by the previous owners in order to provide for closing of a tankside inlet valve and return flow from the VRU. In addition the logic solver provides for closing the tankside export vanle and VRU feed valve on activation of the ESD.

It is felt that it would be unpractical to remove this enhancement, in line with the current operating methods of Local Fuel, however, it is felt that a simplified overview drawing detailing the intended operation of all tanks in respect to the SIS would enhance the understanding of the proposed system, in relationship to Local Fuel requirements.

Action 13:



5.7.2 Performance

The FSA reviewed the performance of the SIS over the 18 months that it has been in the ownership of Local Fuel, the following were considered:

Actual Activations: (Demand on System)

No activations have occurred.

Spurious Trips:

No spurious trips have occurred.

Random Hardware Failure:

No hardware failures have occurred.

Systematic Capability and Systematic Failures:

No systematic failures have been identified.

Operating Difficulties:

Local Fuel plc have taken over the operation of the Terminal and the SIS with no handover from Valero. They have now operated the system for 18 months and have had no difficulty or problems with the system.

Interface with BPCS:

The import valve is opened and closed via the HMI system. However, the BPCS can not interfere with the operation of the SIS system as this is performed on the dedicated hardwired input to the valve.

The SIS sensors are all displayed on the HMI, but again this is indication only and cannot interfere with the SIF.

Maintenance Issues:

No issues have been identified.

Functional Capability:

Not included in Revision A of this FSA.

5.8 Training

As stated previously SIS awareness training has been conducted for all operational staff of Local Fuel plc.

5.9 Further Safety Assessments

Other than for any FSA 5's due to modification, which will be conducted as and when, it is not expected to perform a further FSA 4 for approximately three years when Local Fuel plc will have approximately five years of Terminal ownership and experience in operation of these systems.

5.10 Compliance to BS EN 61511

Not Included in Revision A of this FSA.

5.11 Separate Hazards

The FSA discussed if any additional hazards were created by having the SIS. The only identified hazard is the un-expected closure of the import valve resulting in an increased back pressure to the ship. This is a know issue and the valve is specified to close slowly, typically 90 seconds, furthermore, a siren is provided at the jetty to inform the ship that the SIS has activated and the valve is closing.

5.12 Other Protection Layers

Within the LOPA a number of other protection layers, mitigation layers, enabling events and cross checks were included that were not part of the Safety Instrumented System but need to be operated and maintained as they are fundamental to the calculated SIL of the SIS. It is considered important that these non SIS protection layers are monitored to ensure they are independent, effective and auditable.

Local Fuel plc confirmed that Motherwell provide maintenance and six monthly checks on the tank gauging system. They provide full visit reports which are maintained by Local Fuel plc.

Prior to Local Fuel plc taking over the Terminal, no drawings were available for the BPCS. This has now been rectified and all documentation is available on site comprising of 48 drawings.

6 CONCLUSIONS

6.1 FSA meeting

Revision A of this FSA document details the preliminary assessment and does not include for a review of the installed modification, which at the time of issue had not been installed.

6.2 System Enhancements

There are no intended system enhancements planned or needed for the SIS at this moment in time.