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

NUSTAR TERMINALS

BELFAST TERMINAL

STORAGE TANK OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

MANAGEMENT MANUAL

Contents

Please click on link below to access document:

https://cld.bz/nemZrHu/1

Intentionally Left Blank

Not Included In This Issue

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

NUSTAR TERMINALS

BELFAST TERMINAL

GASOLINE IHLA OVERFILL PROTECTION

SAFETY INSTRUMENT SYSTEM

FUNCTIONAL SAFETY ASSESSMENT

STAGE 4

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	30.09.11	D R Ransome	DSR	Client	Original Issue	
B	01.11.11	D R Ransome	DSR	Client	Incorporating Client Comments	Document No. NU271001_RPT
C	01.10.12	D R Ransome	DSR	Client	Following Functional Safety Meetings	
D	20.02.14	D R Ransome	DSR	Client	Reviewed prior to 2014 Functional Safety Committee meeting	Page 1 of 72
E	05.03.15	D R Ransome	DSR	Client	Action 8 Completed	
F	30.06.17	D R Ransome	DRR	NuStar Safety Committee	Actions confirmed completed and FSA CLOSED	

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

Appendices

1 REVISION HISTORY

Rev	Description
A	Original Issue – Issued following the FSA with actions part complete.
B	Incorporating Client Comments: Nustar Terminals instead of Nustar Energy Section 4.3: Comment added *"The valves are not operational and are left open at all times. They are tested and monitored for closure during weekly SIS testing."* *Tank 47 is fitted with a micropilot radar level transmitter*
C	Actions Updated following Functional Safety Committee meetings
D	Actions Updated following Functional Safety Committee meetings and reviewed prior to 2014 Functional Safety Committee meeting
E	Action 8 Completed
F	Actions confirmed completed and FSA CLOSED

2 SCOPE

Nustar Terminals have had installed an Independent High Level Alarm system to provide a SIL 2 rated automatic shutdown system to prevent 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. Prior to this FSA no previous FSA's have been conducted.

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

3 INTRODUCTION

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

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

3.1 Assumptions and Constraints

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

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

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

4. This document is to be read in conjunction with document NU211002_RPT – SIS Compliance Document.

3.2 Team Membership

Date of Review – Wednesday 7th September 2011 at Nustar Terminals, Belfast Terminal

The FSA review team:-

Nustar Terminals Ltd.:
The FSA review team:-

Andy Bann – Terminal Manager
Dean Bannon – Electrical Technician
Neil Mearms – Terminal Engineer
Yvette Davis – Nustar Terminals HSE Department
Nigel Houghton – EC&I Engineer
Darren Peck – EC&I Engineering Manager

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

Andy Bann , Terminal Manager
14 years experience at Belfast Terminal; with a background in operations as a Terminal Controller, Senior Terminal Controller and Terminal Manager. Previous experiences in the aerospace and transport industries, as an electrical technician, and in junior management roles. Time served aircraft electrician. *Currently holds a NEBOSH Managing Safety Certificate (Level 3)*

Neil Mearns, Terminal Engineer
Graduated from The Queen's University of Belfast in 1999 with a BEng in Mechanical and Manufacturing Engineering, joining the Stocks team at BP Oil UK Ltd in the same year. He progressed to Operations Controller at the company in 2001, before joining Belfast Terminal in 2003 as a Terminal Controller. He was promoted to Terminal Engineer in 2007. *Currently holds a Postgraduate Diploma in Safety and Risk Management (Level 7) from the University of Strathclyde, and has current GradIOSH professional status.*

Dean Bannon, Electrical Technician
Joined the Nustar team at Belfast in October 2010
Previous experience includes working for a leading local electrical contractor in the petrol forecourt industry for 10 years as senior electrical technician and contracts manager.
Time served electrician and qualified in 'Comp Ex Modules':
EX01 & EX02 Installation, inspection & maintenance of EEx d,e,n and p Systems
EX03 & EX04 Installation inspection & maintenance of EEx ia and EEx ib Systems
EX07 & EX08 Preparation, Installation, Testing & maintenance of Electrical Installations at Petrol Filling Stations
Currently holds a BTEC HNC – Building Services (Electrical)

Yvette Davis, Senior Manager for HSE - UK
Over 15 years' experience in managing HSE in TT COMAH sites, 5 years' experience in Fuel Storage Terminals, managing both Process and Occupational safety aspects

Nigel Houghton – EC&I Engineer
City and Guilds in Electrical Installation, City and Guilds In IEE wiring regulations, Compex trained. Over 20 years' experience in storage and handling of petroleum liquids.

Darren Peck, EC&I Engineering Manager - UK
Over 20 years' experience in the petrochemical process industry ranging from design through to installation and commissioning.

P&I Design Ltd.

D.R. Ransome	FSA Chair
D. Regan.	Project Designer

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

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.

David Regan is a Process Engineer with a degree in Chemical Engineering. He has specialised in Process Instrumentation for over 25 years and is a Certified Functional Safety Expert.

The FSA actions were reviewed at the Safety Committee meetings held on 6th March 2012 and attended by the following:

Yvette Davis - Nustar Energy, Senior Manager for HSE - UK
George Reeves – Nustar Energy, General Manager of Engineering
Darren Peck – Nustar Energy, EC&I Engineering Manager - UK
David Ransome – P&I Design, Consultant
David Regan - P&I Design, Certified Functional Safety Expert

A further review was held on 18th September 2012

The FSA action list has been updated following these meeting, Revision C of this document.

4 FUNCTIONAL SAFETY ASSESSMENT – DEFINITIONS AND STAGES

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

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

Stage 1: After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed.

Stage 2: After the safety instrumented system has been designed.

Stage 3: After the installation, pre-commissioning and final validation of the safety instrumented system has been completed and the operation and maintenance procedures have been developed.

Stage 4: After gaining experience in operating and maintenance.

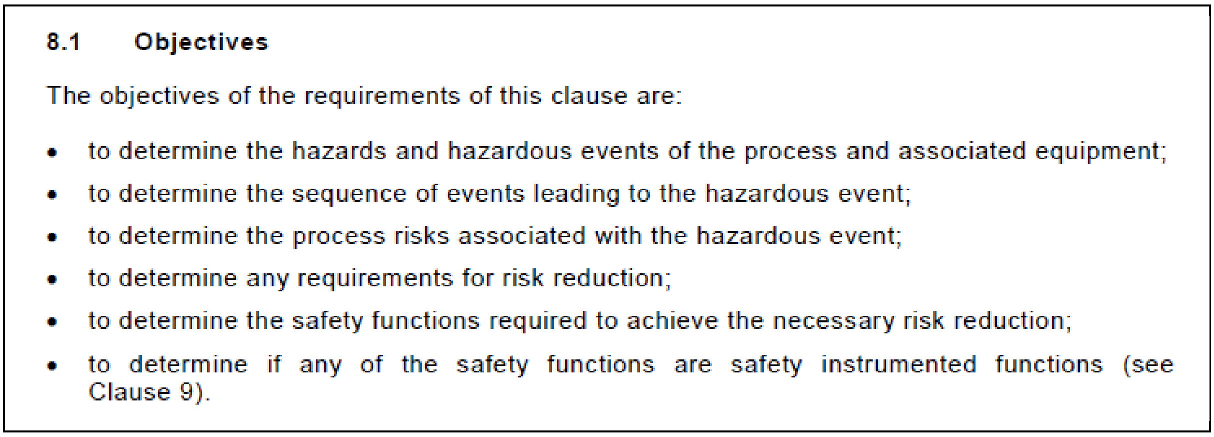
Stage 5: After modification and prior to decommissioning of a safety instrumented system.

BS EN 61511-1 Clause 5.2.6.1.4 states that "as a minimum the assessment shall be carried out prior to the identified hazards being present (i.e. stage 3)". This project is a modification of an existing facility and the hazards are already potentially present. This document details stage 4 Functional Safety Assessment. Document NU271002_RPT " Safety Instrument System Compliance Document" is part of this FSA for the purposes of ensuring compliance to BS EN 61511.

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

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

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



8.1 Objectives

The objectives of the requirements of this clause are:

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

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

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

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

- The hazards and hazardous events of the process and associated equipment were determined in a LOPA review.
  - o The LOPA was conducted by a team of NuStar personnel each with different roles and responsibilities, the LOPA was independently chaired and facilitated by D. O. Jones – Risk Assessor of BCS Chester Ltd.
  - o Although the LOPA report is undated it is believed that it was compiled following the revised requirements for LOPA by the HSE, and after the issue of the PSLG final report.

- The following sequence of events leading to the following hazardous events were considered from both ship and pipeline imports
  - o Vapour Cloud explosion followed by a pool fire
  - o Flash fire followed by a pool fire
  - o An un-ignited release

  the following Initiating Events were identified:

  - IE1 Ship/Pipeline discharged when there is insufficient ullage in the receiving tank
  - IE2 Ships cargo greater than receipt at terminal (Ship only)
  - IE3 Tank changeover failure
  - IE4 Discharge into wrong tank
  - IE5 ATG failure

- The process risks and consequences were determined as:
    - Overfill leading to VCE – Safety & Environmental Issues
    - Overfill leading to a Flash fire and Bund fire with both safety and environmental Issues
    - Overfill leading to un-ignited spill leading to environmental issues

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

    - PL1 ATG with alarms
        - As part of the required protection layers, NuStar realise that this layer, although not SIL rated, requires to be independent, auditable and effective and to maintain this, they are managing this protection layer within their 61511 SFAIRP. (So far as reasonably practicable).

    - PL2 An automated independent high level trip rated to SIL 2 in accordance with BS EN 61511.

      An activation of an independent high level on any of the storage tanks will cause the Emergency Shutdown valves on all of the transfer lines/docklines to close.

    - ML1 A mitigation layer utilising liquid level detection in the bund providing an early warning of overfill. This, to date, has not been installed, but is expected to be operational by end of 2012. In addition there are CCTV facilities. Although it is claimed the instrumentation associated with this ML is SIL1. NuStar realise that the final element response to this relies on an operator and within their claim of 0.1, they have put into place a robust maintenance procedures and hourly site walkabouts.
    - ML2 Secondary and tertiary containment. No credit is claimed for this layer as further action is required.
    - Emergency Warning and evacuation. No credit is claimed for this layer as further action is required.

From the original LOPA, the residual risk following the inclusion of all PL & ML's was 4.2 x 10^{-8} against a risk tolerance criteria (RTC) of 1.00 x 10^{-5} the SIS PL2 having a SIL 2 rating with an estimated PFD of 4.0 x 10^{-3}.

Actual Calculated PFD of PL2 SIF as detailed in:
Document Number NuStar_SIL_Report_Belfast_20110128 Version 2.3, dated 8th February 2011 for the safety Instrument System is: SIL 2 with pfd of 7.74 x 10^{-3} PFD to be added in to the LOPA calculation to confirm suitability of risk reduction.
(Action 1 completed. The LOPA recommendations remain suitable)

As part of this FSA the LOPA calculation is to be re-worked to consider the mitigated risk whilst the bund liquid level detectors are not installed. If their installation is delayed beyond 2012, then it may be advisable to re-work the LOPA to ensure the total removal of this mitigation layer does not affect functional safety.(Action 2 completed. The LOPA recommendations remain suitable)

4.2 Suitability of the Proposed Protection Layer

The purpose of the SIL 2 SIS protection layer is to prevent an overfill and overflow of a storage tank leading to a release of product capable of being ignited and possibly causing a vapour cloud explosion.

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

The level measurement is performed in tank so it is unlikely then any external devices can interfere with the correct operation of the instrument and also it should be able to detect actual level not inferred level, for example had it been located in an external pot or chamber where the change in level may not fully reflect the change of state in the tank.

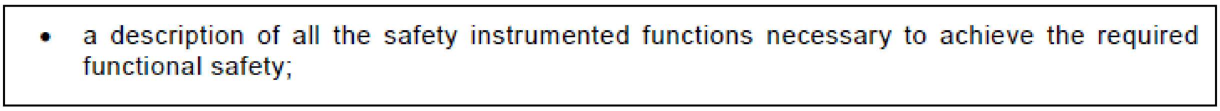
Operation against ships pressure and flow was raised in the FSA i.e. have the valves been operated against full ship pressure and flow to check the operation and effects of any surge on the pipeline and the ship. The Terminal reported this had not be carried out as part of the testing procedure, the system has operated on a spurious trip, however. Surge calculations have been carried out for the terminal and are available in the COMAH report.
At the FSA it was indicated that the surge calculations show that a valve closure time of less than 7 seconds could lead to dangerous surge conditions. The actual valve closure times are approx. 90 seconds.

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

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

It appears that no specific SRS has been produced for this project. There is a Functional Specification document Version 5.0 which provides quite a detail of functionality of the system. NuStar may decide to add to the Functional Specification details that are required within a SRS, but not currently in the Functional Specification. (Action 3 completed. SRS document NU271003_RPT)

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



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

The Functional Specification details the requirements of the SIF from an instrumentation point. Additional information should be included regarding functional safety.
This to include flowrates, operating pressure, closure times of the valves and ullage available etc.
Items 2 & 3 of the Functional Specification to be further developed to indicate how the valves are operated i.e. are they closed after each import or are they left open and if necessary is there any partial stroke testing carried out. (Action 3 completed. SRS document NU271003_RPT, Section 2.2 and 4.5) The valves are not operational and are left open at all times. They are tested and monitored for closure during weekly SIS testing.

Document Number NuStar_SIL_Report_Belfast_20110128 Version 2.3 Dated 8th February 2011 Title Safety Integrity Level (SIL) Verification Report Section 2.0 Scope details the SIF.

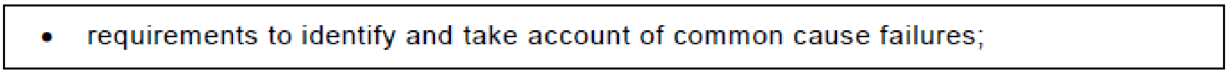
The functional Specification details Micropilot level transmitters on tanks 4, 5, 11, 12, 45 & 46 with the analogue signals fed direct to the analogue card in the PSS within the safety PLC. Tank 47 will also have a Micropilot level transmitter which will feed to an E&H RMA422 which will act as a trip amplifier.

The functional Specification details E&H Liquiphant level switches on tanks 1, 2, 3, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 26, 27, 28, 29, 30, 31, 32, 33, 34, 38, 39, 40, 41, 48, 49 & 50.

The ESV's are installed on 3 dock-lines and 4 transfer lines (5 in future).
Dock-line Valve 1
Dock-line Valve 2
Dock-line Valve 3
Gasoline Transfer Shutdown Valve (PU10 Gasoline Valve)
Diesel Transfer Shutdown Valve

Gas Oil Transfer Shutdown Valve
Kerosene Transfer Shutdown Valve
(Future Kerosene line Valve) – not included in system at present

It will be necessary to provide, within the SRS, a block diagram showing functionality of the various SIF’s. (Action 4 completed, SRS document NU271003_RPT, Section 2.3)



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

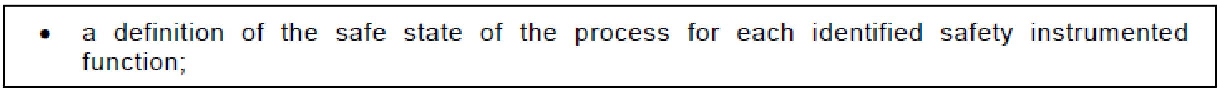
There is no reference to common cause failure. Again confirmation is required if all valves are required to operate to stop product flow i.e. 7oo7 or if only one supply line will be used at any one time. If 1oo1 then common cause failure may not be applicable.

Response in FSA meeting:

Activation of any high level causes all valves to close. In normal operation, up to two lines with ESV’s can be feeding a single tank at any one time. This is never done with gasoline import.

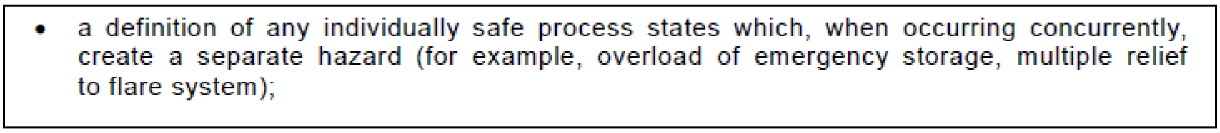
The terminal utilises Nitrogen for the actuator. The valves are all ball valves of Pekos manufacture. All actuators are Actreg and the solenoid valves are Norgren.

Common cause failure may be an issue with 2oo2 system operation. To be covered in the SRS and in the PFD verification calculations. (Action 3 completed, SRS document NU271003_RPT, Section 2.2) (Action 9)



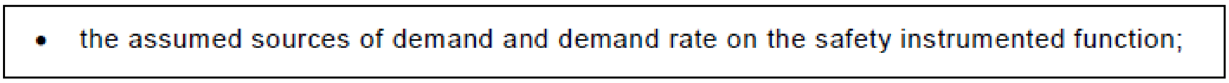
- a definition of the safe state of the process for each identified safety instrumented function;

The Functional Specification details the fails safe state of the SIF. The SRS should also include more details of the safe state of the process and actions on shutting down against a ship import. (Action 3 completed, SRS document NU271003_RPT, Section 4.5)



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

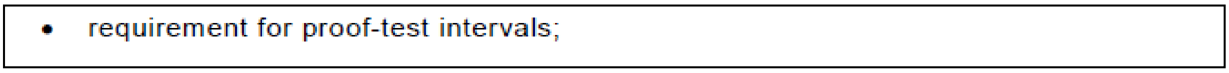
No reference. (Action 3 completed, SRS document NU271003_RPT. There are no safe process states which, when occurring concurrently create a separate hazard)



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

Document Number NuStar_SIL_Report_Belfast_20110128 Version 2.3 Dated 8th February 2011 Title Safety Integrity Level (SIL) Verification Report Section 4 Demand Mode.

It is stated that the demand on the system is less than once a year and as such is classified as low demand mode.

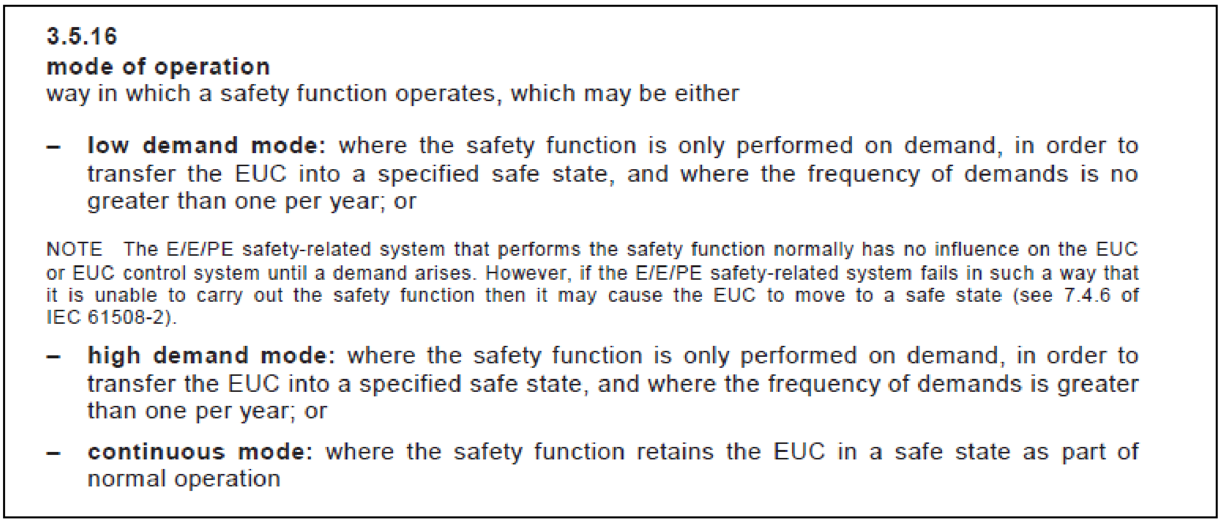


- requirement for proof-test intervals;

Document Number NuStar_SIL_Report_Belfast_20110128 Version 2.3 Dated 8th February 2011 Title Safety Integrity Level (SIL) Verification Report Section 4 Demand Mode.

It is stated that the proof test interval will be annually.

However, BS EN 61508 – 4: 2010 Section 3.5.16 redefines low demand as detailed below:



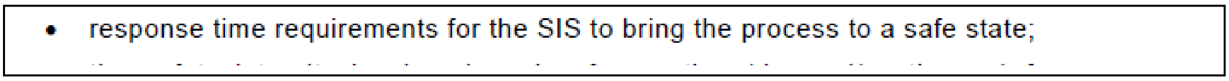
3.5.16
mode of operation
way in which a safety function operates, which may be either

– **low demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or

NOTE The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508-2).

– **high demand mode:** where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or

– **continuous mode:** where the safety function retains the EUC in a safe state as part of normal operation



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

No reference in NuStar documentation.

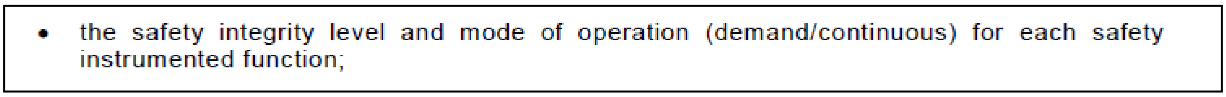
At FSA meeting:

Operators do the testing, Liquiphants are tested (1 tank per week) more often than annually. Testing is recorded.

Monthly tests on valves will be continued with recording of times to open and close.

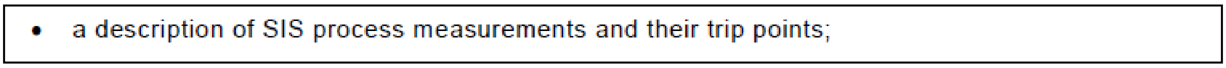
Annual testing on the radar transmitters by a controlled fill to activation point using a tank to tank transfer. It was pointed out at the FSA that this method of test resulted in taking the process into a dangerous state. Terminal Management explained that this is conducted using tank to tank transfers at lower rates and is fully monitored during the operation.

At the FSA it was indicated that the surge calculations show that a valve closure time of less than 7 seconds could lead to dangerous surge conditions. The actual valve closure times are approx. 90 seconds.
Response time to be included in the SRS. (Action 3 completed, SRS document NU271003_RPT, Section 4.5)



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

Document Number NuStar_SIL_Report_Belfast_20110128 Version 2.3 Dated 8th February 2011 Title Safety Integrity Level (SIL) Verification Report details the demand mode and the SIL.



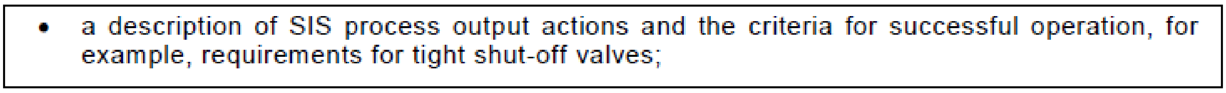
- a description of SIS process measurements and their trip points;

No reference to these settings could be identified.

In FSA meeting the following points were confirmed:

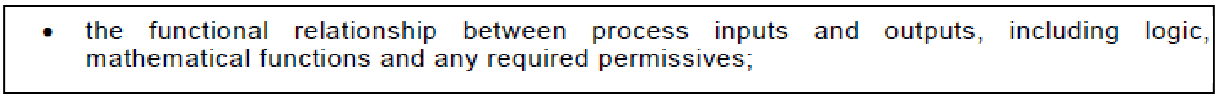
A time of 4.5 minutes from high level activation point to tank overfill. Flowrate 400 Te/hr. Action on failure of SIS, can action be taken to stop import. Procedure Reference: Operation, Override, Testing Procedures and records.

Trip points to be included in SRS. (Action 3 completed, SRS document NU271003_RPT, Section 4.5)



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

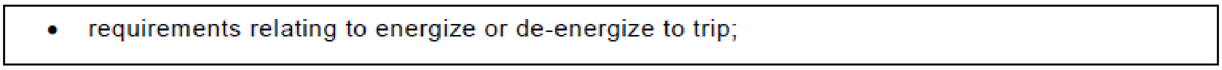
No reference. (Action 3 completed, SRS document NU271003_RPT, Section 3)



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

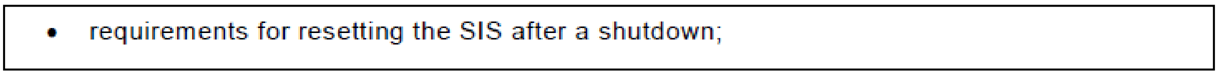
No method of manually shutting down the SIS. Independent ROSOVs can be used to shutdown specific tanks. Manual valves are used and there is a ship shutdown procedure. There is a fire alarm which will also alert the ship. The ESV's are left open but are currently stroke stroked once a week. It was suggested that the record sheet for stroke testing be modified to include closure times of the valve on each test.

SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Sections 2.2 & 4.5)



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

No reference. (Action 3 completed, SRS document NU271003_RPT, Section 3)

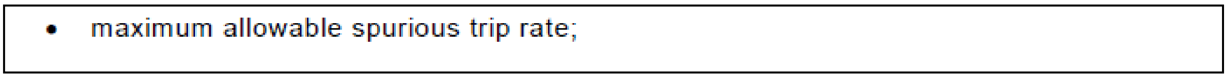


- requirements for resetting the SIS after a shutdown;

Reset procedure requires defining.

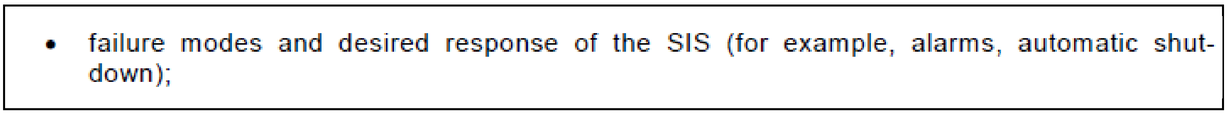
Response in FSA meeting: Procedures for the reset of the SIS are included in IHLA Operation, Override, Testing Procedures and records. Reset can be only performed from the switchroom panel.

SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 2.2)



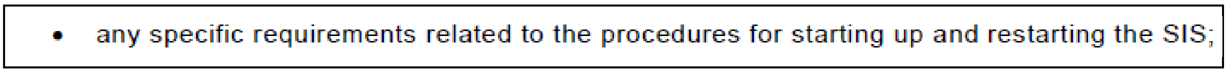
- maximum allowable spurious trip rate;

No Reference. SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 2.3)



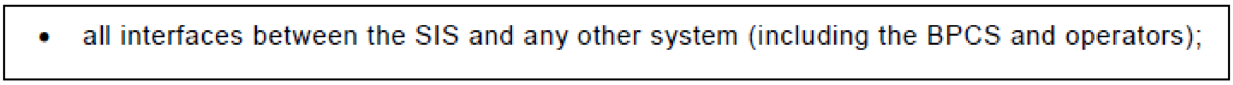
- failure modes and desired response of the SIS (for example, alarms, automatic shut-down);

Needs further clarification, SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 4.5)



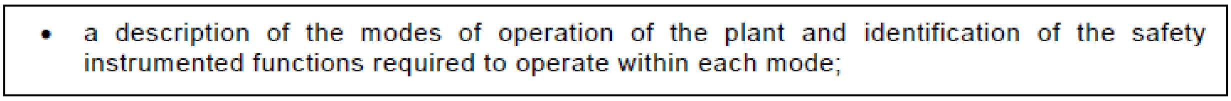
- any specific requirements related to the procedures for starting up and restarting the SIS;

Needs further clarification. SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 2.2)



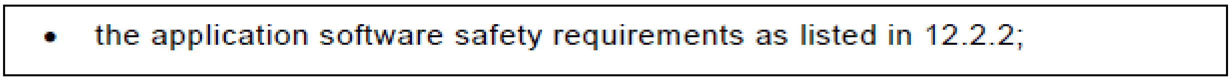
- all interfaces between the SIS and any other system (including the BPCS and operators);

Further clarification is required on interface between the BPCS and SIS. SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 4.4)



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

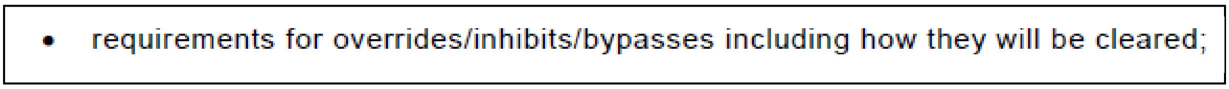
SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 4.5)



- the application software safety requirements as listed in 12.2.2;

The logic solver is a PILZ Safety PLC. Document Safety Check - Validation provides information on software installed at the time of testing.

PILZ performed both the FAT and SAT, NuStar have received the validation documents. Software verification to be included with these documents for Grangemouth Terminal so it assumed it would be similar for Belfast. (Action 5)



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

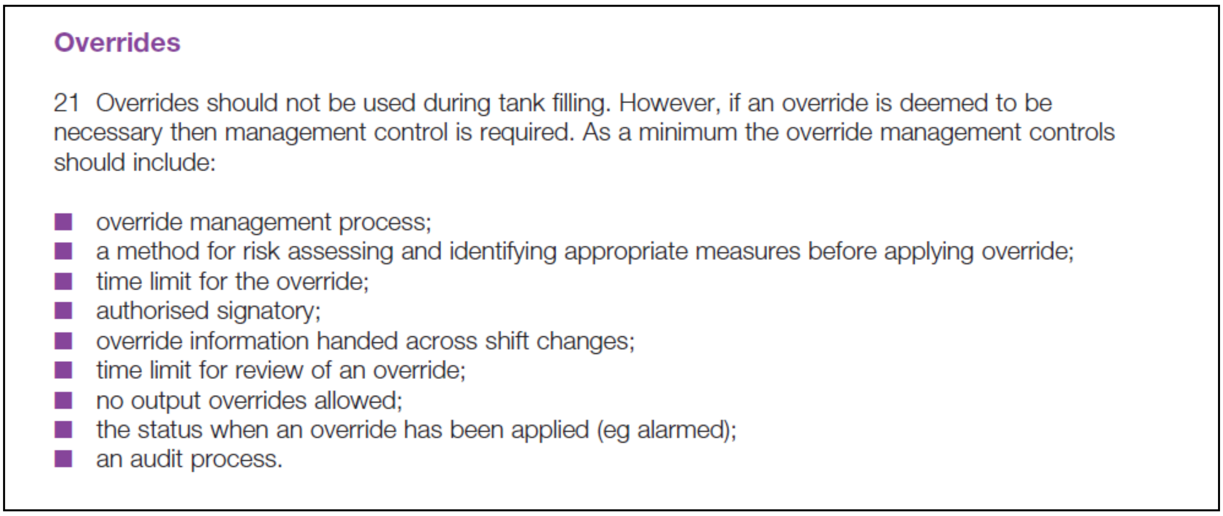
The Functional Specification provides details of overrides. It is noted that the overrides may appear to operate on the final elements which is against the advice given in PSLG – Safety and environmental standards for fuel storage sites: Appendix 4 Section 21:

Review of override control to be assessed to above and as detailed below:

Response in FSA meeting:

If a tank level device goes into fault, the tank is normally isolated. The tank (or other tanks) can still be filled under management procedures. A key is used to override the input to the logic solver which allows further operation of valves. The system continues to indicate a fault. In the event of any further activation of a level switch, the valves will close. Before any override is initiated, a TORA (Trip override risk assessment) is completed and recorded in "IHLA Operation, Override, Testing Procedures and Records". SRS to incorporate Override philosophy (Action 3 completed, SRS document NU271003_RPT, Section 2.2)

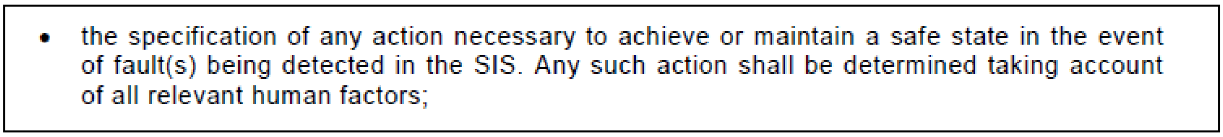
Review of override control to be assessed against PSLG guidance (Action 6 completed, See above)



Overrides

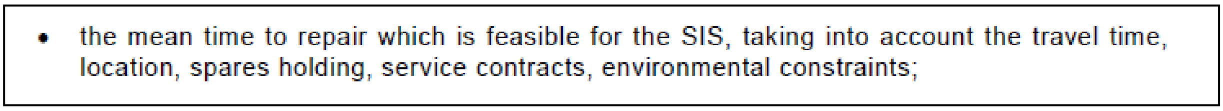
21 Overrides should not be used during tank filling. However, if an override is deemed to be necessary then management control is required. As a minimum the override management controls should include:

- override management process;
- a method for risk assessing and identifying appropriate measures before applying override;
- time limit for the override;
- authorised signatory;
- override information handed across shift changes;
- time limit for review of an override;
- no output overrides allowed;
- the status when an override has been applied (eg alarmed);
- an audit process.



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

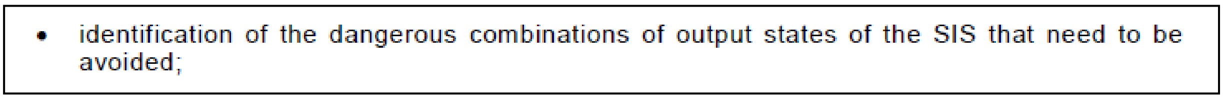
SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 4.5)



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

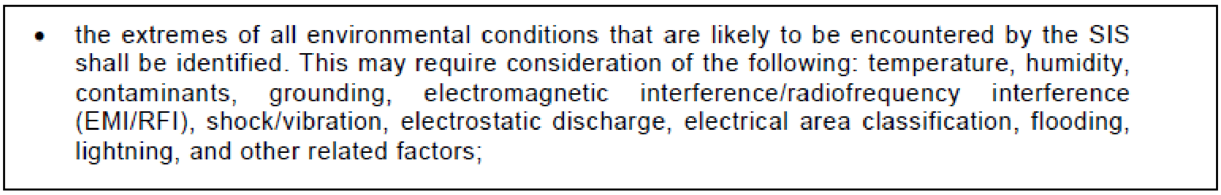
SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 3)

Response in FSA meeting: From a sensor point of view multiple tanks are used for each product. However, Belfast currently carrier a spare radar transmitter and a spare vibronics switch which could be utilised within the MTTR.



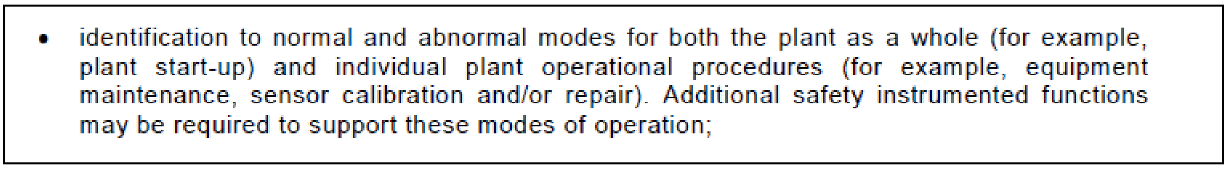
- identification of the dangerous combinations of output states of the SIS that need to be avoided;

SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 3)



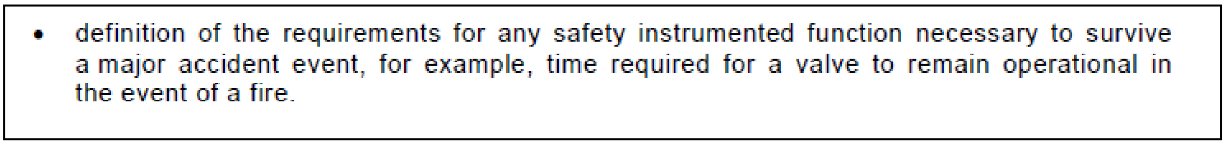
- the extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock/vibration, electrostatic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

SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 3)



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

SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 3)



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

The ESV solenoid valves have nylon nitrogen lines which will act as fusible links to close the valves in the event of a fire and the ESV's are specified as firesafe.

SRS to include details. (Action 3 completed, SRS document NU271003_RPT, Section 3)

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

Design changes appear to have been conducted. There appear anomalies between the documentation as to what is the current status of the installed system. NuStar to confirm how they will provide management of change now the system is operational. Some documents do not carry unique document numbers. NuStar should incorporate these documents into the system and provide document numbers. (Action 7).

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

No previous functional Safety Assessments have been carried out.

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

This was reviewed and discussed at the FSA meeting held on 7th September 2011 at NuStar Belfast.

Hardware Fault Tolerances to be checked. (See Action 9)

The wiring and installation has been independently verified by Stuart Robinson from PILZ (on 8th Jan 2009 & 1st December 2010). The system has now been operational since 2009 and there have been the following issues:

Tank 4 radar had to be replaced (Prior to full SIS implementation)
A batch of radar devices were installed on the floating deck tanks. Spurious trips and failures have occurred. The radar devices have activated during heavy rain, snow and windy conditions. Consideration is being given to an change of level device in the external floating roof tanks.
Tank 41 has a recorded spurious activation. This is under investigation and no fault has been identified. This happened during heavy rain conditions.

The following documentation was available for review.

Drawings:

Drawing Number	Title	No of Sheets	Revision
10041/250	Marine Offloading P&I Diagram	1	A
10041/252	Kerosene P&I Diagram	2	B
54/70/340	ECV Valve Connections Safety PLC	1	A
54/70/341	IHLA Panel Fault Relay Digital Outputs for Tanks 1, 2. 13, 16-19, 21,22, 27, 29, 30 & 38	1	B
54/70/347	IHLA Panel Digital Outputs	1	D
54/70/348	IHLA Power Supply Arrangement	1	A
54/70/349	IHLA Panel Digital Inputs	1	B
54/70/350	IHLA Panel Digital Inputs	1	C
54/70/356	Independent High Level Alarm Cable Layout Tanks 3, 6, 9, 15, 26, 28, 32, 33, 34, 39, 40, 41, 47 & 48	1	A
54/70/357	ECV Valve Connections for Site 3 & Site 1 Transfer System	1	O
54/70/358	IHLA Panel Fault Relay Digital Outputs for Ttanks 3, 6, 9, 15, 26, 28, 32, 33, 34, 39, 40, 41 & 48	1	A
54/70/408	IHLA Connections Tanks 1, 2, 13, 16-22 Safety PLC Connections	1	A
54/70/389	IHLA System Layout and Control Philosophy Tank 50	1	A
54/70/390	IHLA System Layout and Control Philosophy Tank 3	1	O
54/70/391	IHLA System Layout and Control Philosophy Tank 6	1	O
54/70/392	IHLA System Layout and Control Philosophy Tank 9	1	O
54/70/393	IHLA System Layout and Control Philosophy Tank 15	1	O
54/70/394	IHLA System Layout and Control Philosophy Tank 26	1	O

54/70/395	IHLA System Layout and Control Philosophy Tank 28	1	O
54/70/396	IHLA System Layout and Control Philosophy Tank 32	1	O
54/70/397	IHLA System Layout and Control Philosophy Tank 33	1	O
54/70/398	IHLA System Layout and Control Philosophy Tank 34	1	O
54/70/399	IHLA System Layout and Control Philosophy Tank 39	1	O
54/70/400	IHLA System Layout and Control Philosophy Tank 40	1	O
54/70/401	IHLA System Layout and Control Philosophy Tank 41	1	O
54/70/402	IHLA System Layout and Control Philosophy Tank 47	1	O
54/70/403	IHLA System Layout and Control Philosophy Tank 48	1	O
54/70/374	IHLA System Layout and Control Philosophy Tank 20	1	A
54/70/375	IHLA System Layout and Control Philosophy Tank 21	1	A
54/70/376	IHLA System Layout and Control Philosophy Tank 22	1	A
54/70/377	IHLA System Layout and Control Philosophy Tank 27	1	A
54/70/378	IHLA System Layout and Control Philosophy Tank 29	1	A
54/70/379	IHLA System Layout and Control Philosophy Tank 30	1	A
54/70/380	IHLA System Layout and Control Philosophy Tank 31	1	A
54/70/381	IHLA System Layout and Control Philosophy Tank 38	1	A
54/70/382	IHLA System Layout and Control Philosophy Tank 45	1	A
54/70/383	IHLA System Layout and Control Philosophy Tank 46	1	A
54/70/384	IHLA System Layout and Control Philosophy Tank 49	1	A
54/70/366	IHLA System Layout and Control Philosophy Tank 11	1	A
54/70/367	IHLA System Layout and Control Philosophy Tank 12	1	A
54/70/368	IHLA System Layout and Control Philosophy Tank 13	1	A
54/70/369	IHLA System Layout and Control Philosophy Tank 14	1	A
54/70/370	IHLA System Layout and Control Philosophy Tank 16	1	A
54/70/371	IHLA System Layout and Control Philosophy Tank 17	1	A
54/70/372	IHLA System Layout and Control Philosophy Tank 18	1	A
54/70/373	IHLA System Layout and Control Philosophy Tank 19	1	A
54/70/359	IHLA System Layout and Control Philosophy Tank 5	1	A
54/70/360	IHLA System Layout and Control Philosophy Tank 1	1	A
54/70/361	IHLA System Layout and Control Philosophy Tank 2	1	A
54/70/362	IHLA System Layout and Control Philosophy Tank 4	1	A
54/70/363	IHLA System Layout and Control Philosophy Tank 7	1	A
54/70/364	IHLA System Layout and Control Philosophy Tank 8	1	A
54/70/365	IHLA System Layout and Control Philosophy Tank 10	1	A
54/70/409	ECV Valve Connections Safety PLC	1	A
54/70/411	IHLA Cable Layout Overview	1	O
54/70/412	IHLA Connections Tanks 27, 29, 30, 31 & 38 plus Tanks 26, 28, 32, 33, 34, 39, 40 & 41 Safety PLC Connections	1	O

Reports:

Report Number	Title	No of Sheets	Revision
	Functional Spec for the Design and operation of the SIL Rated PLC Monitoring the IHLA on Specific Storage tanks.	7	4
	Proof Testing of the IHLA System	6	2
	Safety Integrity Level Verification Report (Pilz)	17	2.3
200806041_01_CSC	Safety Check - Validation	28	1.3
20101128_01_CSC	Safety Check - Validation	32	1.0

At the FSA meeting there were discrepancies in the documentation as to the operation of the system since certain additions have been incorporated.

NuStar have current P&I Drawings which reflect the installed system. These will be issued to P&I Design Ltd, on completion, for review. It was noted that currently the numbering system is not continued throughout all drawings and documentation. The equipment numbering system is under review and a new asset management system is in progress. Final tag numbers to be added to the P&I Diagrams for re-issue and following this, all SIS documentation will be updated. (Action 14)

It was decided at the FSA that all SIS documentation will be brought up to an AS BUILT status, ensuring that it agrees with the P & I Diagrams and the installed system. (After Asset Management System change) (Action 15)

The documentation for the logic solver was incomplete. Ensure that PILZ provide the up to date software documentation and software verification reports. On receipt of this information, the verification will be reviewed. (Action 5)

NuStar to develop a process for controlling modifications to the SIS to ensure that functional safety is not compromised. It was therefore decided not to review the documentation listed, in detail, at this stage and that a further review be conducted. (Action 16)

Further to some inconsistencies, NuStar provided a brief summary of each of the systems is as follows:

ESVs on 3 dock-lines and 4 transfer lines (5 in future).
Dock-line Valve 1
Dock-line Valve 2
Dock-line Valve 3
Gasoline Transfer Shutdown Valve (PU10 Gasoline Valve)
Diesel Transfer Shutdown Valve
Gas Oil Transfer Shutdown Valve
Kerosene Transfer Shutdown Valve
(Future Kerosene line Valve) – not included in system at present

41 tanks can receive product from any of the above lines.

Tanks are normally dedicated to a particular product, but this can be subject to change at short notice.
The activation of the SIS level device on any of the 41 tanks will shut down the ESVs on all the above lines.

In normal operation, up to two lines with ESV's can be feeding a single tank at any one time. This is never done with gasoline import. No calculation for this 2oo2 system is provided in the design dossier.

There are only 3 dock-lines which can be used for import. These lines can all be in operation simultaneously. In this case there would be no transfer operations being carried out.

No tank to tank transfers have been included in the LOPA and are not accounted for. Review LOPA for the addition of gasoline tank to tank transfers (Action 8).

There is consideration for a further independent layer of protection which will utilise independent level devices to close the tank–side import valves. This will primarily protect the tanks during tank to tank transfers. See above regarding LOPA (Expected end 2012).

VRU lines are not included in the SIS.

4.6.1 SIL Verification

Review of SIL Verification document including check of PFD and hardware fault tolerance calculations. (ACTION 9).

Document: Pilz Safety Integrity Level (SIL) Verification was reviewed and calculations verified.

Pilz Safety Integrity Level (SIL) Verification calculated the following combination of SIL and PFD:

a. 1oo1 Radar Level Sensor fed direct to analogue input module, Logic Solver and 1oo1 ROSOV final element:
    i. Calculated at SIL 2 with a PFD of 4.04 x 10^{-3}.

b. 1oo1 Vibronics Level Switch Sensor, Logic Solver and 1oo1 ROSOV final element:
    i. Calculated at SIL 2 with a PFD of 2.17 x 10^{-3}.

c. 1oo1 Radar Level Switch Sensor, Logic Solver and 1oo2 Sounder final element (Calculation is part final element only as no pfd value has been included for the response of the operator).
    i. Calculated at SIL 2 capable with a PFD of 4.28 x 10^{-3}.
    ii. FSA Not verified as no operator data available. However, not an independent protection layer from a above and maximum credit that can be taken for operator prevents any SIL claim.

d. 1oo1 Vibronics Level Switch Sensor, Logic Solver and 1oo2 Sounder final element (Calculation is part final element only as no pfd value has been included for the response of the operator).
    i. Calculated at SIL 2 capable with a PFD of 2.41 x 10^{-3}.
    ii. FSA Not verified as no operator data available. However, not an independent protection layer from b above and maximum credit that can be taken for operator prevents any SIL claim.

e. 1oo1 Radar Level Sensor with Trip amplifier, Logic Solver and 1oo1 ROSOV final element:
    i. Calculated at SIL 2 with a PFD of 4.43 x 10^{-3}

f. 1oo1 Vibronics Level Sensor connected by SafetyBUS, Logic Solver and 1oo1 ROSOV final element:
    i. Calculated at SIL 2 with a PFD of 2.40 x 10^{-3}.

It must also be confirmed that c and d above are not intended as additional protection layers as firstly they are incomplete in the fact that no value has been included in the calculations for operator response. If operator response was included then the PFD and SIL would not achieve SIL 1.
Also, if they are intended as an additional layer of protection, then they would not qualify as they are utilising the same sensor and possibly logic solver as detailed in a and b.
If it is intended that the purpose c and d is to advise the operator of the activation of the SIS then the operators response must be defined.

Verification Calculations

1. PILZ Safety data available within the design manual, the Safe Fail Fraction could not be found, however the verification calculation assumes a SFF of 0.9 for these devices.
2. The original generic value of 2.07 x 10^{-4} used in the Pilz calculation for the ball valve has now been substituted by the Pekos data certified by Exida which is less conservative. See Appendix 1. The new PFD has been used for the verification calculation.
3. A PFD of 1 x 10^{-6} has been used for the Norgren Solenoid valve. However, it was noted that the TüV second page to the certificate appears to have several errors on it. Namely there is confusion as the PFD, it is quoted at the top as 2.00 x 10^{-7} with an adjusted figure at the bottom as the impact to test interval as 1 x 10^{-6}. Also, it would appear that they have miss-referenced the safe and dangerous failures as it states dangerous detected failures are 0 and dangerous undetected failures are 2.28 x 10^{-10} with safe detected failures as 0 and safe undetected failures as 2.28 x 10^{-12}. This would infer a SFF of 0.01 when it states 0.99.

4.6.1.1 SIL and PFD Verification Summary

The following show the revised calculations for the SIF for each system.

SIL & PFD Verification Summary

a. Tanks 4, 5, 11, 12, 45 & 46
1oo1 Radar Level Sensor connected direct to Analogue Input Card, Logic Solver and 1oo1 actuated valve final element:
Calculated at SIL 2 with a PFD of 6.76 x 10^{-3}.
Spurious Trip 25.2 years

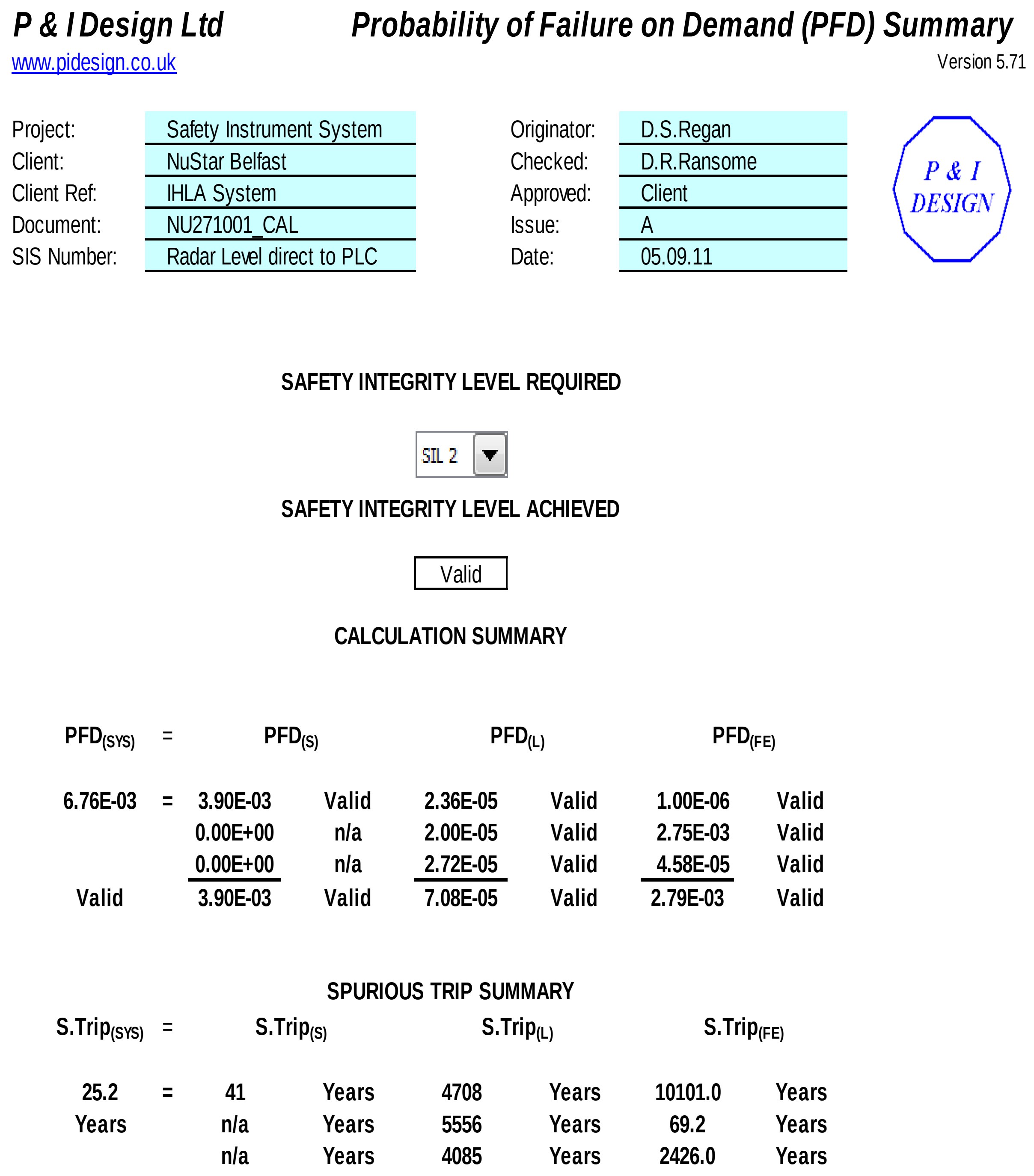
b. Tanks 1, 2, 13, 16, 17, 18, 19, 20 & 21 + Tanks 7, 8, 10, 14, 20, 49, 50 & 48
1oo1 Vibronics Level Sensor, Logic Solver and 1oo1 actuated valve final element:
Calculated at SIL 2 with a PFD of 4.9 x 10^{-3}.
Spurious Trip 29.5 years

c. Tank 47
1oo1 Radar Level Sensor with Trip amplifier, Logic Solver and 1oo1 ROSOV final element:
Calculated at SIL 2 with a PFD of 7.74 x 10^{-3}.
Spurious Trip 20.8 years

d. Tanks 3, 6, 9 & 15
1oo1 Vibronics Level Sensor connected by SafetyBUS, Logic Solver and 1oo1 ROSOV final element:
Calculated at 2 with a PFD of 5.11 x 10^{-3}.
Spurious Trip 23.2 years

e. Tanks 1, 2, 13, 16, 17, 18, 19, 20 & 21 + Tanks 7, 8, 10, 14, 20, 49, 50 & 48
1oo1 Vibronics Level Sensor, Logic Solver and 2oo2 actuated valve final element:
Calculated at SIL 2 with a PFD of 7.69 x 10^{-3}.
Spurious Trip 29.9 years

Tanks 4, 5, 11, 12, 45 & 46



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

www.pidesign.co.uk

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

P & I DESIGN

SAFETY INTEGRITY LEVEL REQUIRED

SIL 2 ▼

SAFETY INTEGRITY LEVEL ACHIEVED

Valid

CALCULATION SUMMARY

PFD$_{(SYS)}$	=	PFD$_{(S)}$		PFD$_{(L)}$		PFD$_{(FE)}$	
6.76E-03	=	3.90E-03	Valid	2.36E-05	Valid	1.00E-06	Valid
		0.00E+00	n/a	2.00E-05	Valid	2.75E-03	Valid
		0.00E+00	n/a	2.72E-05	Valid	4.58E-05	Valid
Valid		3.90E-03	Valid	7.08E-05	Valid	2.79E-03	Valid

SPURIOUS TRIP SUMMARY

S.Trip$_{(SYS)}$	=	S.Trip$_{(S)}$		S.Trip$_{(L)}$		S.Trip$_{(FE)}$	
25.2	=	41	Years	4708	Years	10101.0	Years
Years		n/a	Years	5556	Years	69.2	Years
		n/a	Years	4085	Years	2426.0	Years

P & I Design Ltd

www.pidesign.co.uk

PFD - Sensor Subsystem Calculation Sheet 1

Sheet Title:- Sensor E&H Micropilot FMR240

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

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

System Architecture

1oo1 ▼

Data Type

2

Failure Rate/hr (λ)

Sub System Item	E&H Radar
FAILURE DATA	
Failures - Safe, Detected (λSD)	1.05E-07
Failures - Safe, Undetected (λSU)	1.69E-06
Failures - Dangerous, Detected (λDD)	9.57E-07
Failures - Dangerous, Undetected (λDU)	8.86E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	3.64E-06
Safe Fail Fraction	0.76
Total Dangerous Failures (λ_D)	1.84E-06
Calculated Diagnostic Coverage (%)	51.93

SUB-SYSTEM DATA	
Mean Time to Repair (hrs)	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	1.84E-06
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	9.57E-07
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	8.86E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	2113.6
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	51.9

LOOP CRITERIA ACHIEVED	
PFD Total	**3.90E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**41**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES ▼

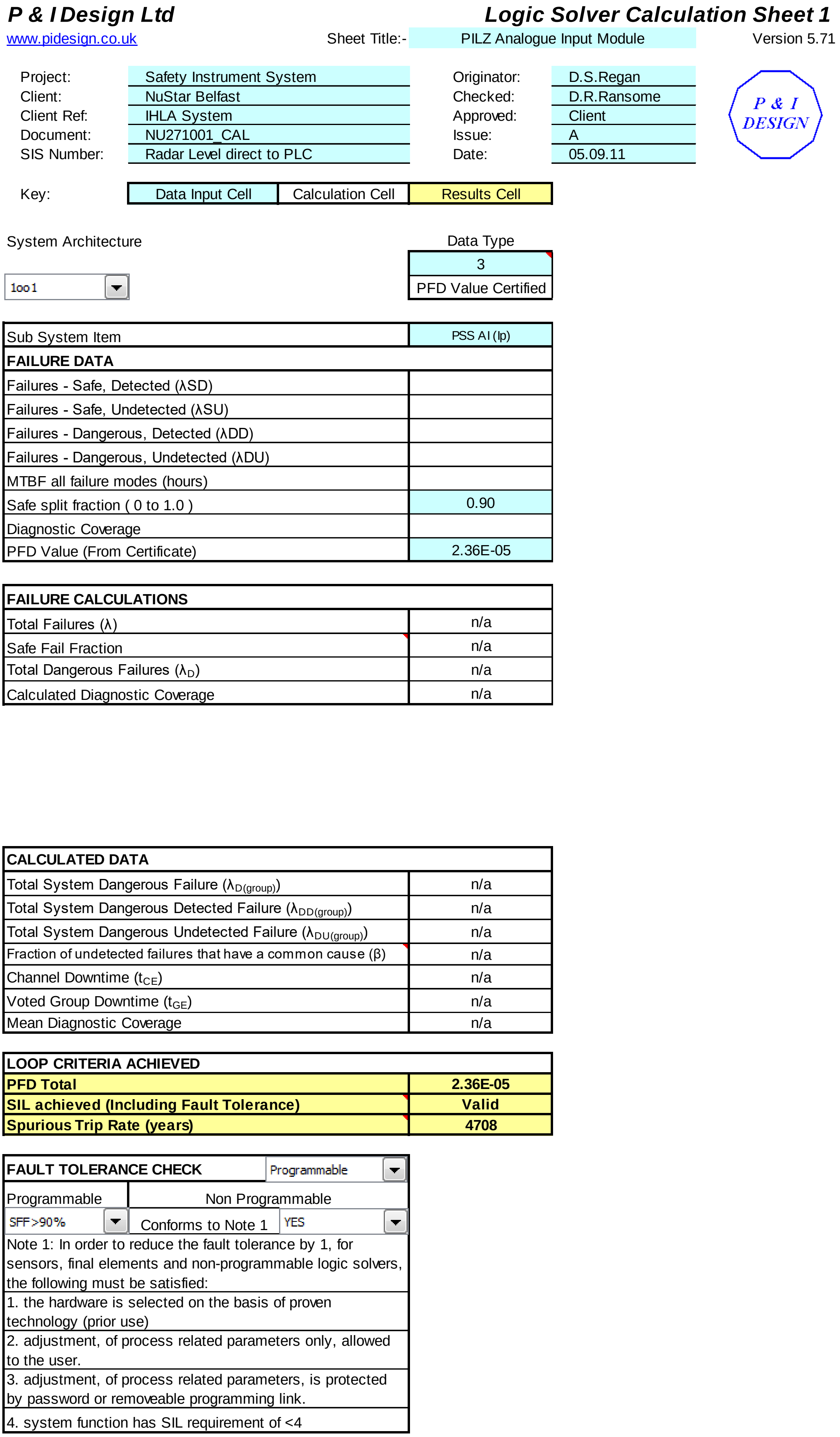
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Logic Solver Calculation Sheet 1

www.pidesign.co.uk

Sheet Title:- PILZ Analogue Input Module

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture

1oo1

Data Type
3
PFD Value Certified

Sub System Item	PSS AI (Ip)
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.36E-05

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

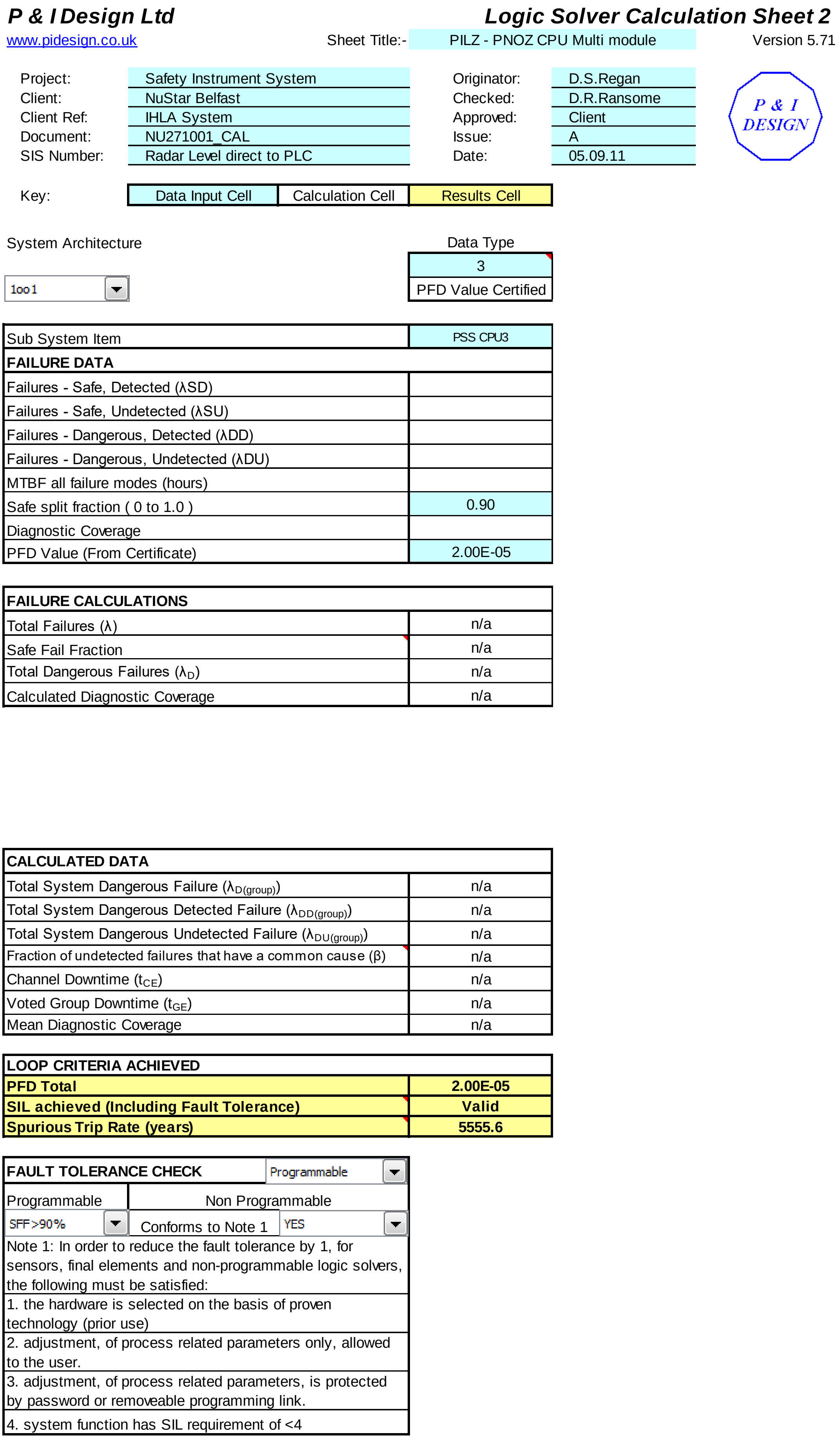
CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.36E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**4708**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4



P & I Design Ltd — ***Logic Solver Calculation Sheet 2***

www.pidesign.co.uk — Sheet Title:- PILZ - PNOZ CPU Multi module — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS CPU3
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.00E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.00E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**5555.6**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

P & I Design Ltd

Logic Solver Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- PILZ - PNOZ multi single pole DO

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

Key:	Data Input Cell	Calculation Cell	Results Cell

System Architecture

1oo1

Data Type
3
PFD Value Certified

Sub System Item	PSS DOS
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.72E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.72E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**4085.0**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

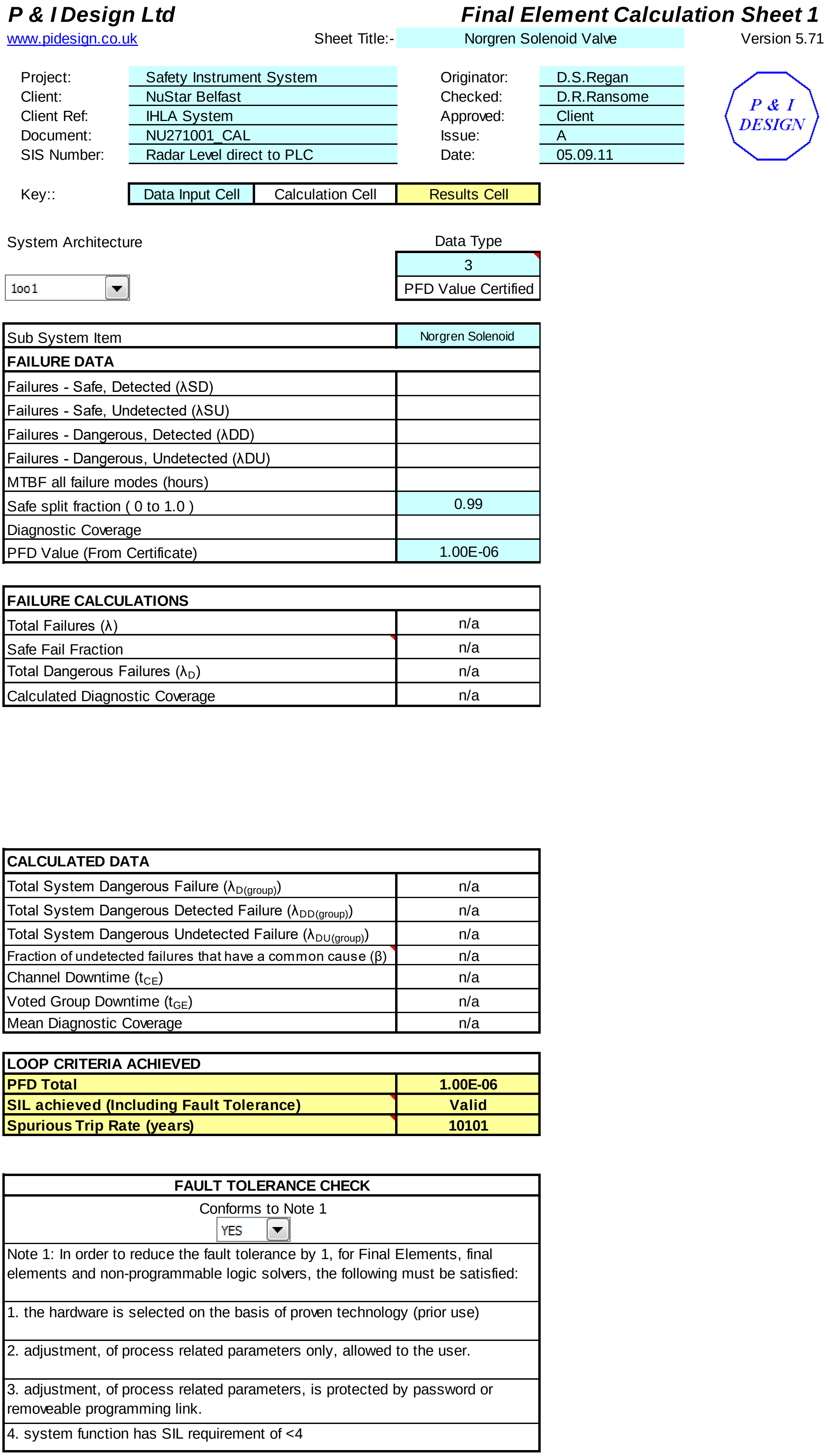
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



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

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

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

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

System Architecture

1oo1 ▼

Data Type

3

PFD Value Certified

Sub System Item	Norgren Solenoid
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.99
Diagnostic Coverage	
PFD Value (From Certificate)	1.00E-06

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**1.00E-06**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**10101**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES ▼

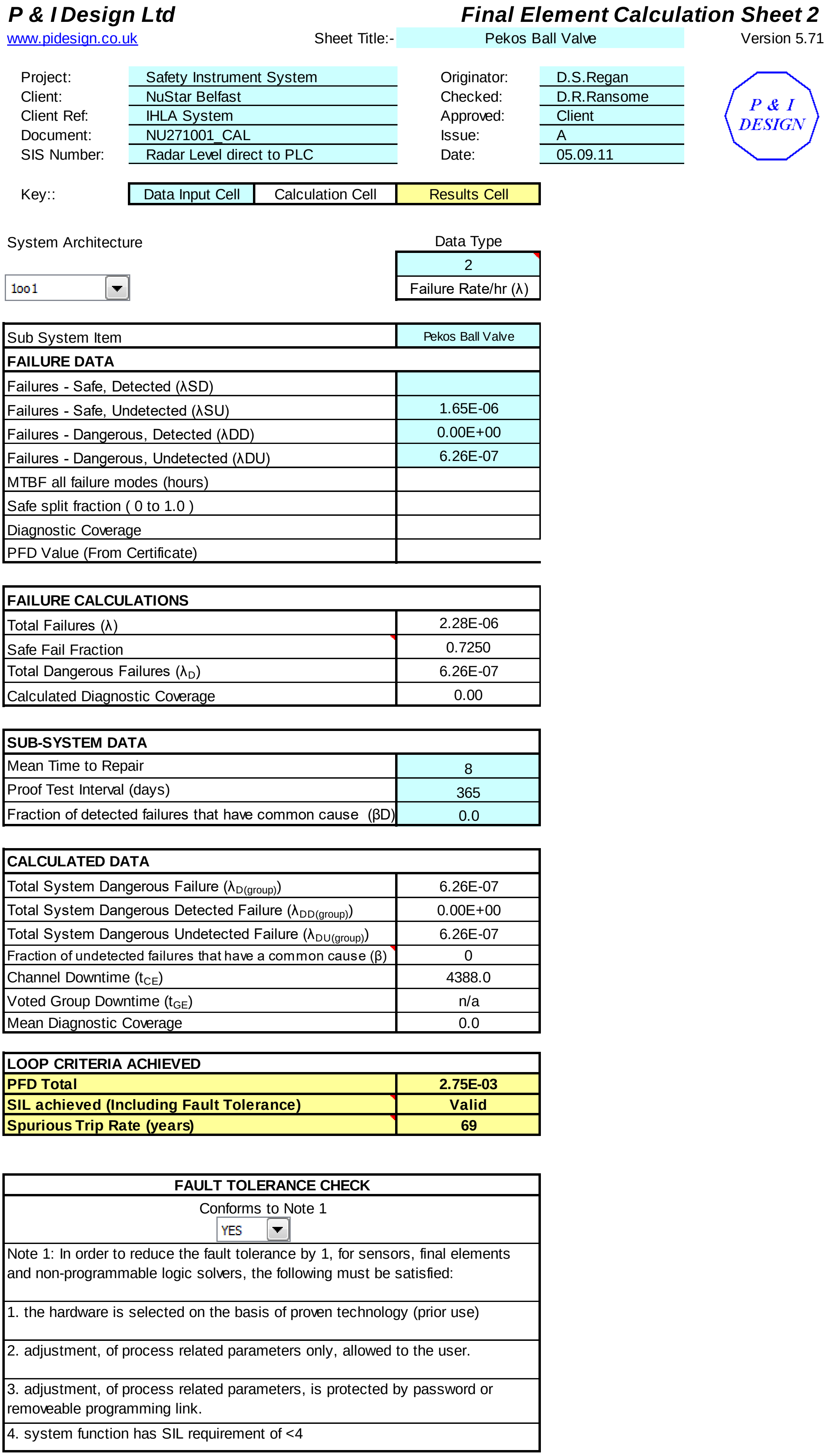
Note 1: In order to reduce the fault tolerance by 1, for Final Elements, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

www.pidesign.co.uk

Final Element Calculation Sheet 2

Sheet Title:- Pekos Ball Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

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

System Architecture: 1oo1

Data Type: 2 — Failure Rate/hr (λ)

Sub System Item	Pekos Ball Valve
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	1.65E-06
Failures - Dangerous, Detected (λDD)	0.00E+00
Failures - Dangerous, Undetected (λDU)	6.26E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	2.28E-06
Safe Fail Fraction	0.7250
Total Dangerous Failures (λ_D)	6.26E-07
Calculated Diagnostic Coverage	0.00

SUB-SYSTEM DATA	
Mean Time to Repair	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	6.26E-07
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	0.00E+00
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	6.26E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	4388.0
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	0.0

LOOP CRITERIA ACHIEVED	
PFD Total	**2.75E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**69**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

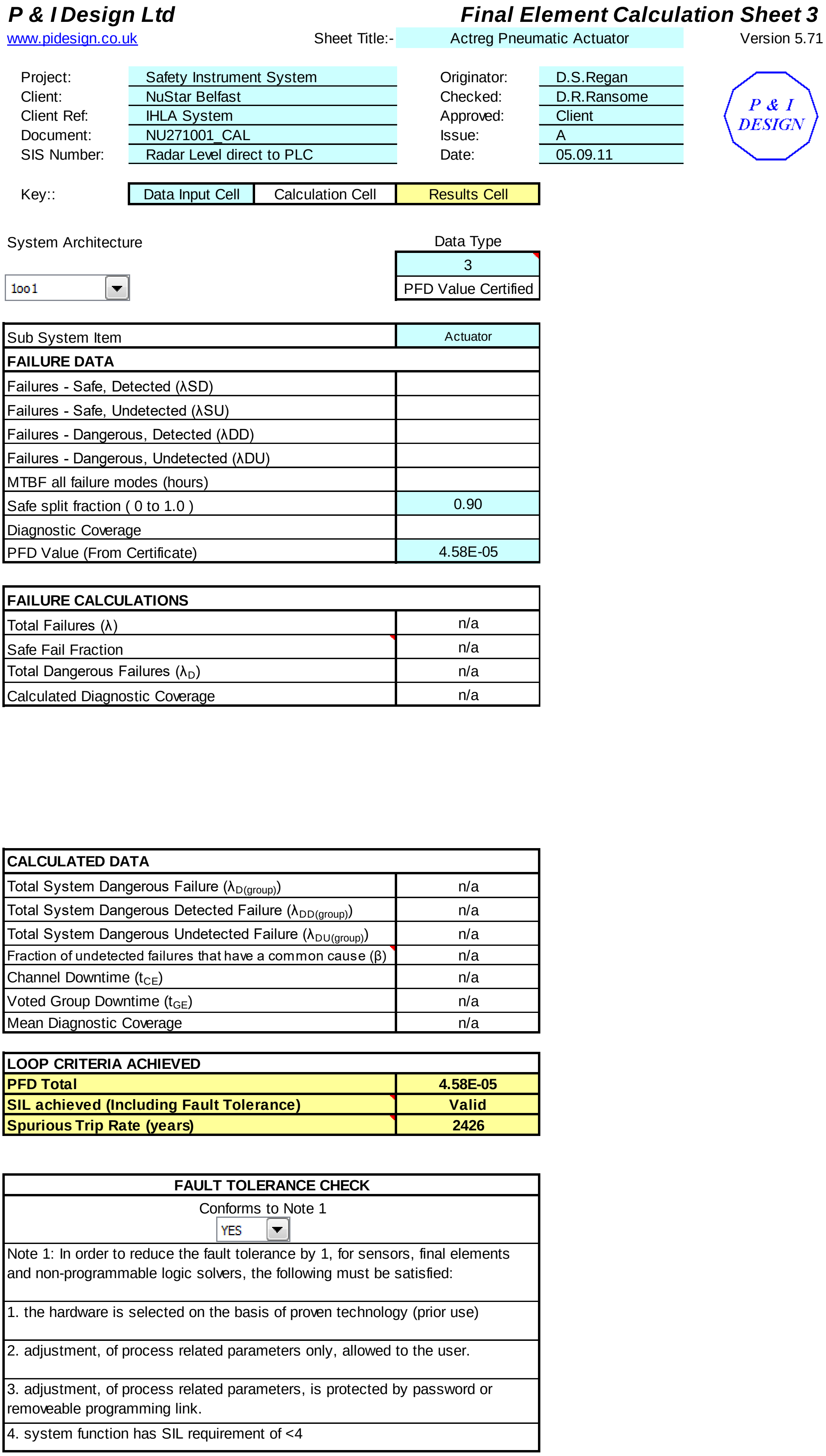
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- Actreg Pneumatic Actuator

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271001_CAL	Issue:	A
SIS Number:	Radar Level direct to PLC	Date:	05.09.11

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

System Architecture

1oo1

Data Type

3

PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

Tanks 1, 2, 13, 16, 17, 18, 19, 20 & 21 + Tanks 7, 8, 10, 14, 20, 49, 50 & 48

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

www.pidesign.co.uk

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

SAFETY INTEGRITY LEVEL REQUIRED

SIL 2 ▼

SAFETY INTEGRITY LEVEL ACHIEVED

Valid

CALCULATION SUMMARY

PFD$_{(SYS)}$	=	PFD$_{(S)}$		PFD$_{(L)}$		PFD$_{(FE)}$	
4.90E-03	=	1.50E-03	Valid	5.55E-04	Valid	1.00E-06	Valid
		0.00E+00	n/a	2.00E-05	Valid	2.75E-03	Valid
		0.00E+00	n/a	2.72E-05	Valid	4.58E-05	Valid
Valid		1.50E-03	Valid	6.02E-04	Valid	2.79E-03	Valid

SPURIOUS TRIP SUMMARY

S.Trip$_{(SYS)}$	=	S.Trip$_{(S)}$		S.Trip$_{(L)}$		S.Trip$_{(FE)}$	
29.5	=	74	Years	200	Years	10101.0	Years
Years		n/a	Years	5556	Years	69.2	Years
		n/a	Years	4085	Years	2426.0	Years

P & I Design Ltd

www.pidesign.co.uk

PFD - Sensor Subsystem Calculation Sheet 1

Sheet Title:- Sensor E&H Liquiphant +FTL325P

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

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

System Architecture

1oo1

Data Type

3

PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

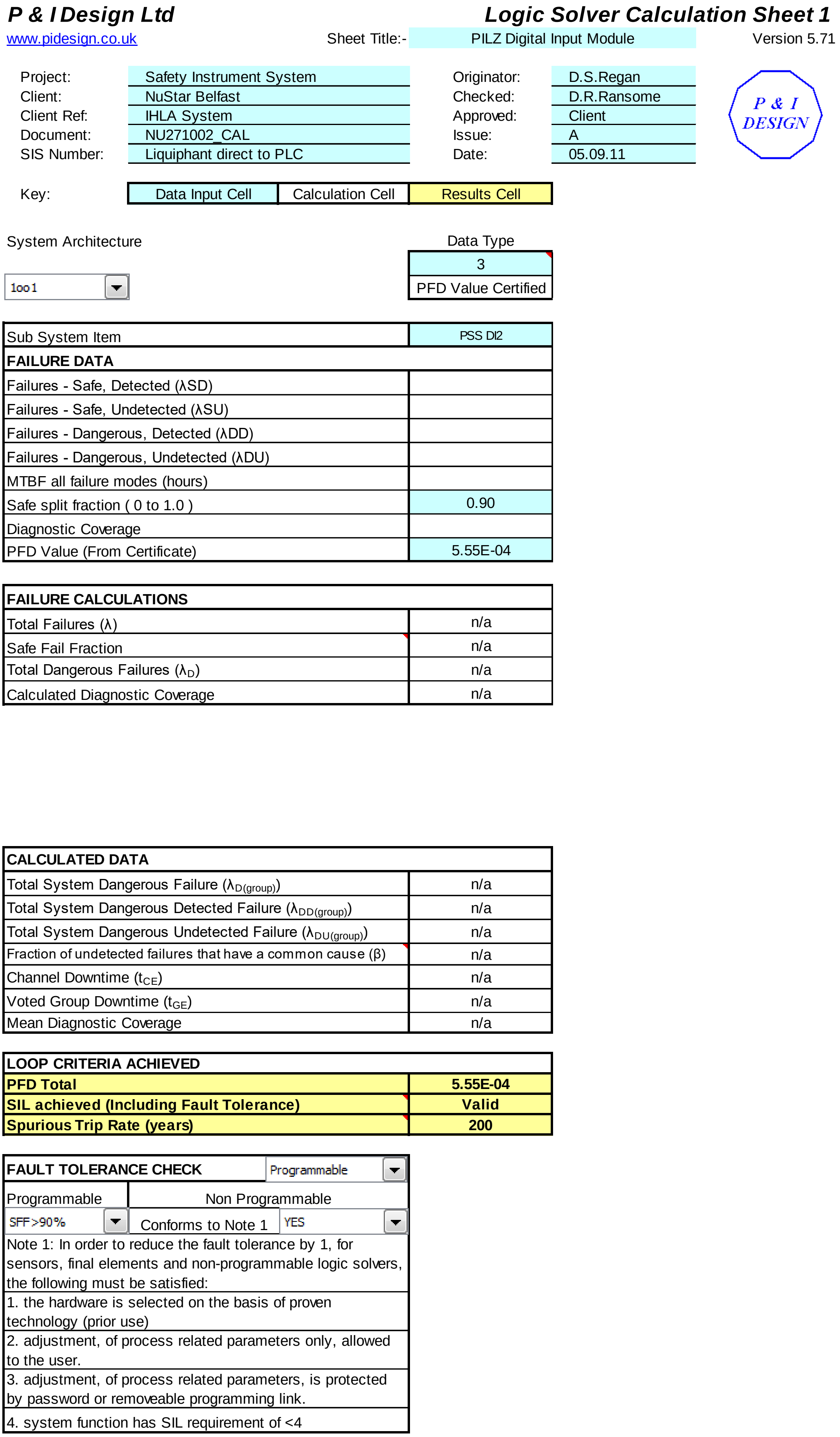
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



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

www.pidesign.co.uk

Sheet Title:- PILZ Digital Input Module | Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS DI2
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	5.55E-04

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**5.55E-04**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**200**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4

P & I Design Ltd

Logic Solver Calculation Sheet 2

www.pidesign.co.uk Sheet Title:- PILZ - PNOZ CPU Multi module Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS CPU3
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.00E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.00E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**5555.6**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

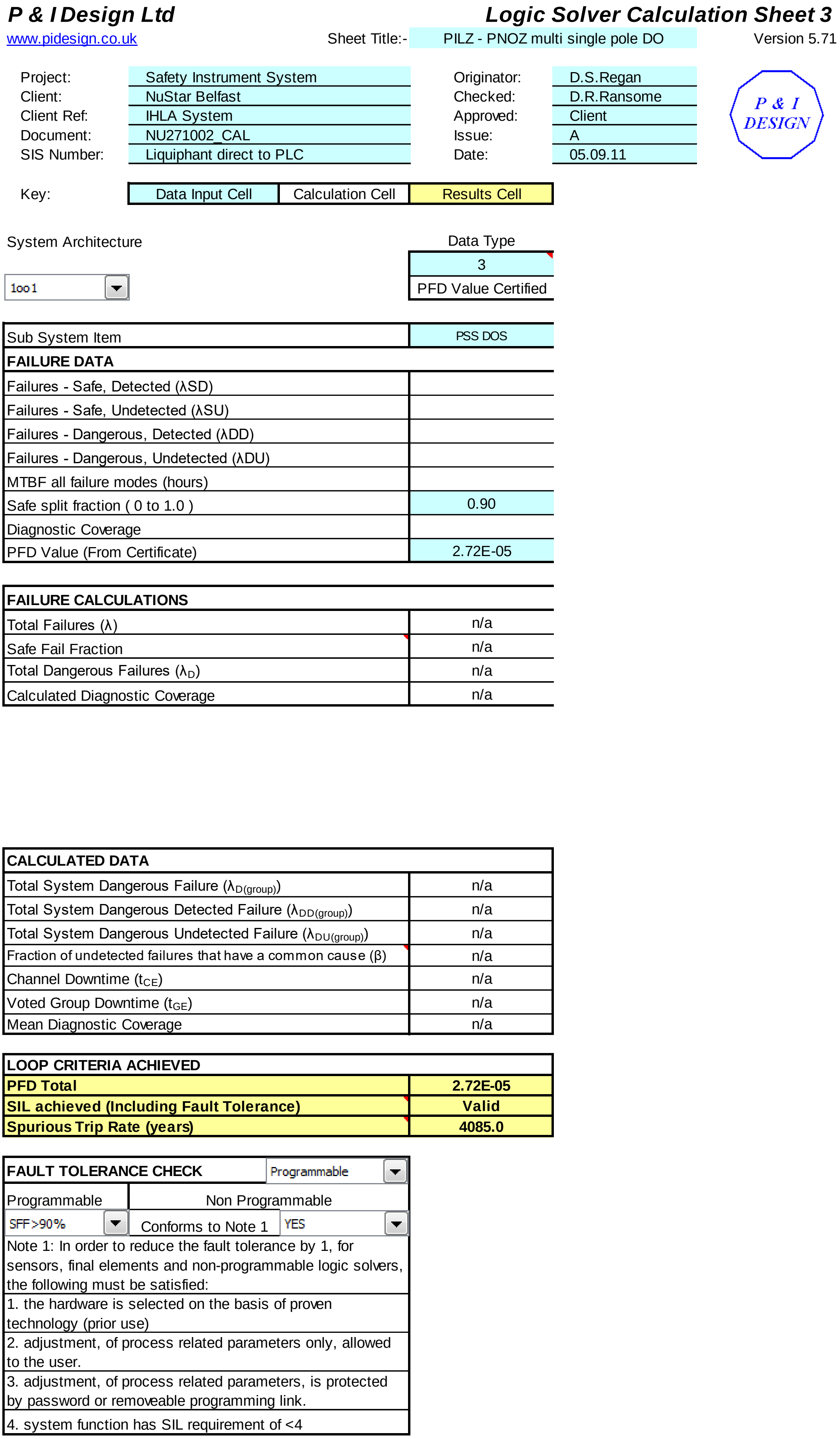
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Logic Solver Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- PILZ - PNOZ multi single pole DO

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS DOS
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.72E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.72E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**4085.0**

FAULT TOLERANCE CHECK Programmable

Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

P & I Design Ltd

Final Element Calculation Sheet 1

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

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

P & I DESIGN

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

System Architecture

1oo1

Data Type
3
PFD Value Certified

Sub System Item	Norgren Solenoid
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.99
Diagnostic Coverage	
PFD Value (From Certificate)	1.00E-06

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**1.00E-06**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**10101**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

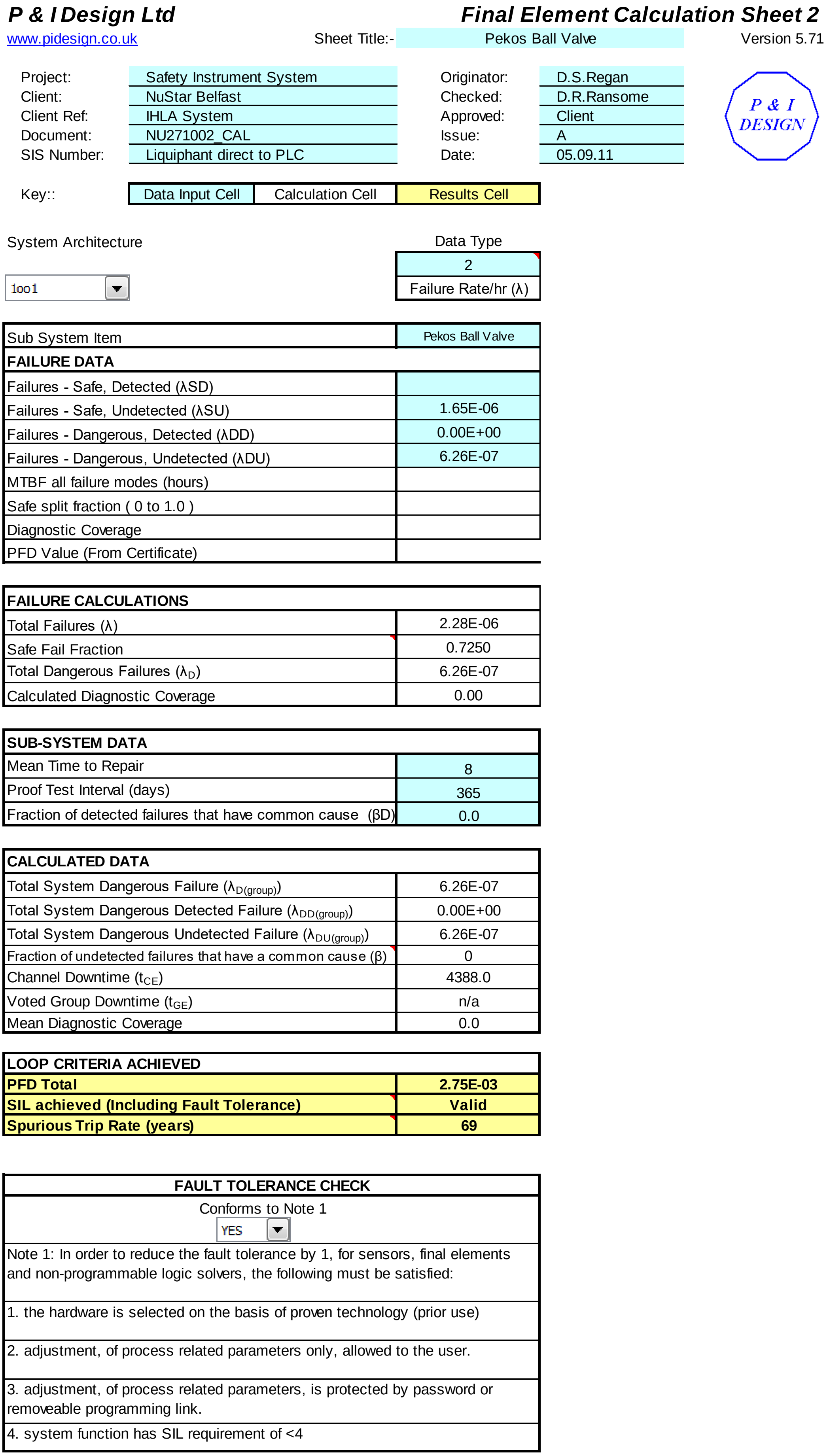
Note 1: In order to reduce the fault tolerance by 1, for Final Elements, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 2

www.pidesign.co.uk

Sheet Title:- Pekos Ball Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

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

System Architecture

1oo1

Data Type

2

Failure Rate/hr (λ)

Sub System Item	Pekos Ball Valve
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	1.65E-06
Failures - Dangerous, Detected (λDD)	0.00E+00
Failures - Dangerous, Undetected (λDU)	6.26E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	2.28E-06
Safe Fail Fraction	0.7250
Total Dangerous Failures (λ_D)	6.26E-07
Calculated Diagnostic Coverage	0.00

SUB-SYSTEM DATA	
Mean Time to Repair	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	6.26E-07
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	0.00E+00
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	6.26E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	4388.0
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	0.0

LOOP CRITERIA ACHIEVED	
PFD Total	**2.75E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**69**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

P & I Design Ltd

Final Element Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- Actreg Pneumatic Actuator

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271002_CAL	Issue:	A
SIS Number:	Liquiphant direct to PLC	Date:	05.09.11

P & I DESIGN

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

System Architecture

1oo1 ▼

Data Type

3

PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES ▼

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

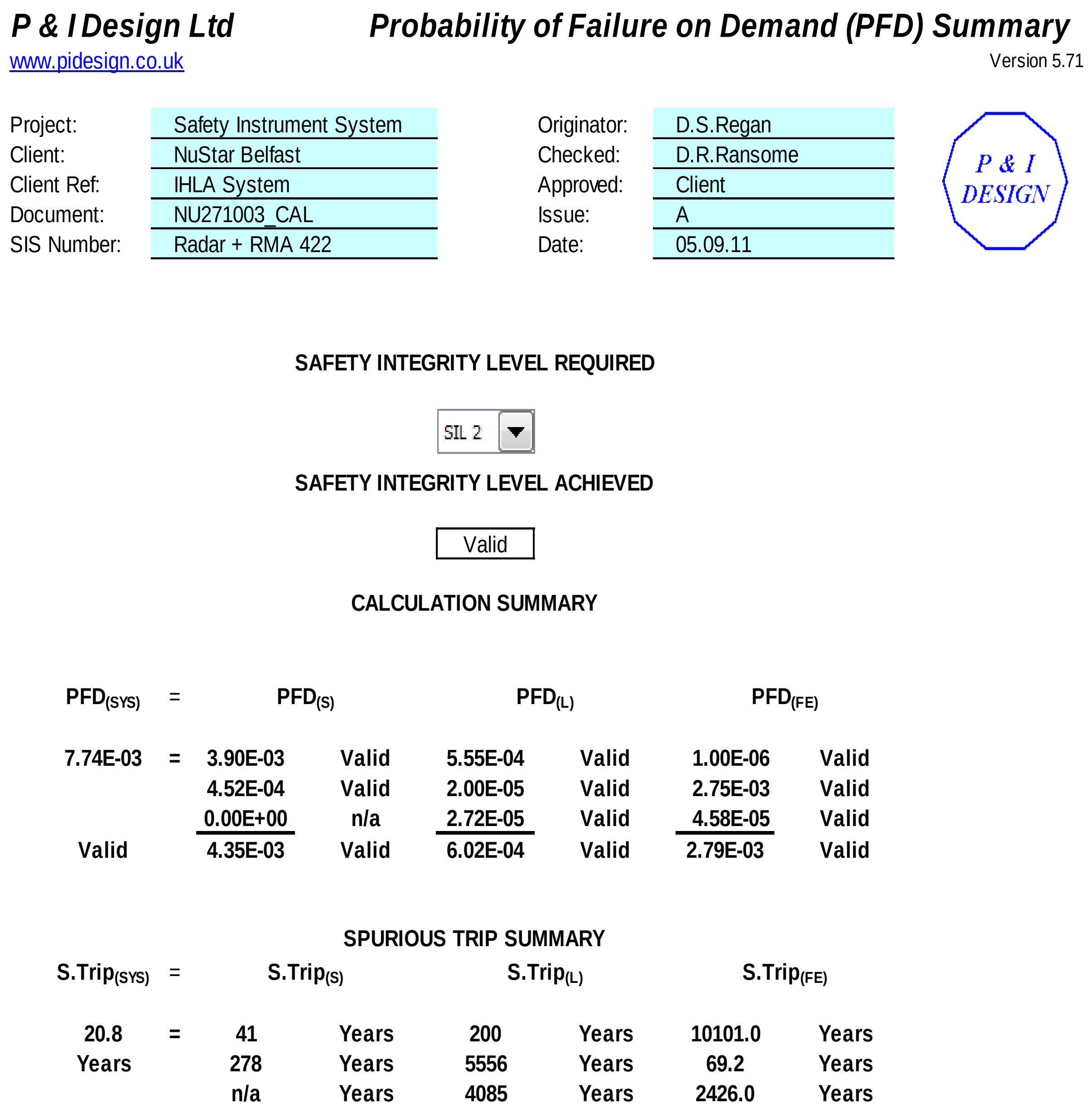
1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

Tank 47



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

www.pidesign.co.uk

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

SAFETY INTEGRITY LEVEL REQUIRED

SIL 2 ▼

SAFETY INTEGRITY LEVEL ACHIEVED

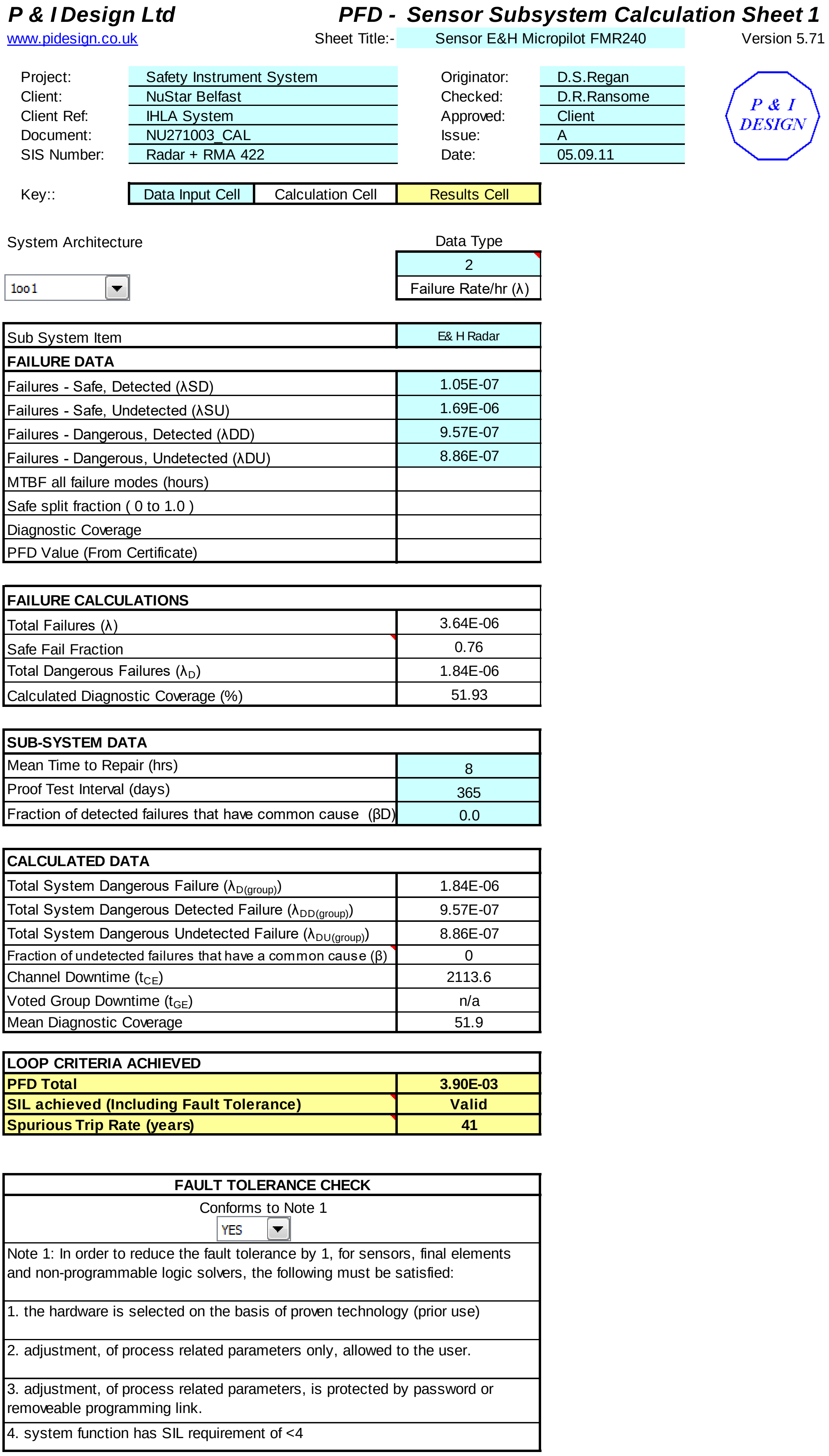
Valid

CALCULATION SUMMARY

$PFD_{(SYS)}$	=	$PFD_{(S)}$		$PFD_{(L)}$		$PFD_{(FE)}$	
7.74E-03	=	3.90E-03	Valid	5.55E-04	Valid	1.00E-06	Valid
		4.52E-04	Valid	2.00E-05	Valid	2.75E-03	Valid
		0.00E+00	n/a	2.72E-05	Valid	4.58E-05	Valid
Valid		4.35E-03	Valid	6.02E-04	Valid	2.79E-03	Valid

SPURIOUS TRIP SUMMARY

$S.Trip_{(SYS)}$	=	$S.Trip_{(S)}$		$S.Trip_{(L)}$		$S.Trip_{(FE)}$	
20.8	=	41	Years	200	Years	10101.0	Years
Years		278	Years	5556	Years	69.2	Years
		n/a	Years	4085	Years	2426.0	Years



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

www.pidesign.co.uk

Sheet Title:- Sensor E&H Micropilot FMR240 — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

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

System Architecture: 1oo1

Data Type: 2 — Failure Rate/hr (λ)

Sub System Item	E& H Radar
FAILURE DATA	
Failures - Safe, Detected (λSD)	1.05E-07
Failures - Safe, Undetected (λSU)	1.69E-06
Failures - Dangerous, Detected (λDD)	9.57E-07
Failures - Dangerous, Undetected (λDU)	8.86E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	3.64E-06
Safe Fail Fraction	0.76
Total Dangerous Failures (λ_D)	1.84E-06
Calculated Diagnostic Coverage (%)	51.93

SUB-SYSTEM DATA	
Mean Time to Repair (hrs)	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	1.84E-06
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	9.57E-07
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	8.86E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	2113.6
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	51.9

LOOP CRITERIA ACHIEVED	
PFD Total	**3.90E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**41**

FAULT TOLERANCE CHECK

Conforms to Note 1: YES

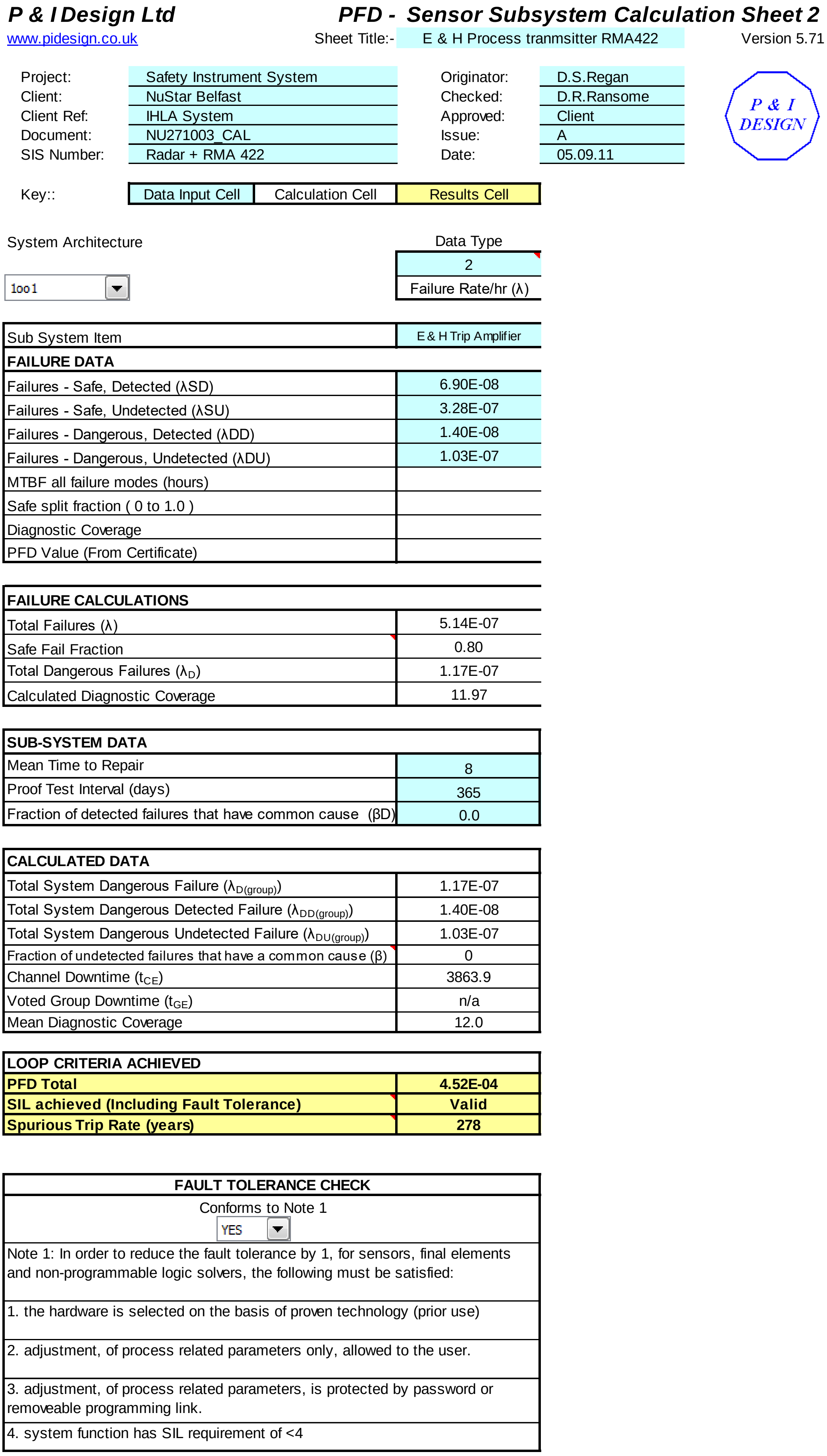
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd — **PFD - Sensor Subsystem Calculation Sheet 2**

www.pidesign.co.uk — Sheet Title:- E & H Process tranmsitter RMA422 — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

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

System Architecture: 1oo1

Data Type: 2 — Failure Rate/hr (λ)

Sub System Item	E & H Trip Amplifier
FAILURE DATA	
Failures - Safe, Detected (λSD)	6.90E-08
Failures - Safe, Undetected (λSU)	3.28E-07
Failures - Dangerous, Detected (λDD)	1.40E-08
Failures - Dangerous, Undetected (λDU)	1.03E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	5.14E-07
Safe Fail Fraction	0.80
Total Dangerous Failures (λ_D)	1.17E-07
Calculated Diagnostic Coverage	11.97

SUB-SYSTEM DATA	
Mean Time to Repair	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	1.17E-07
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	1.40E-08
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	1.03E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	3863.9
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	12.0

LOOP CRITERIA ACHIEVED	
PFD Total	**4.52E-04**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**278**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

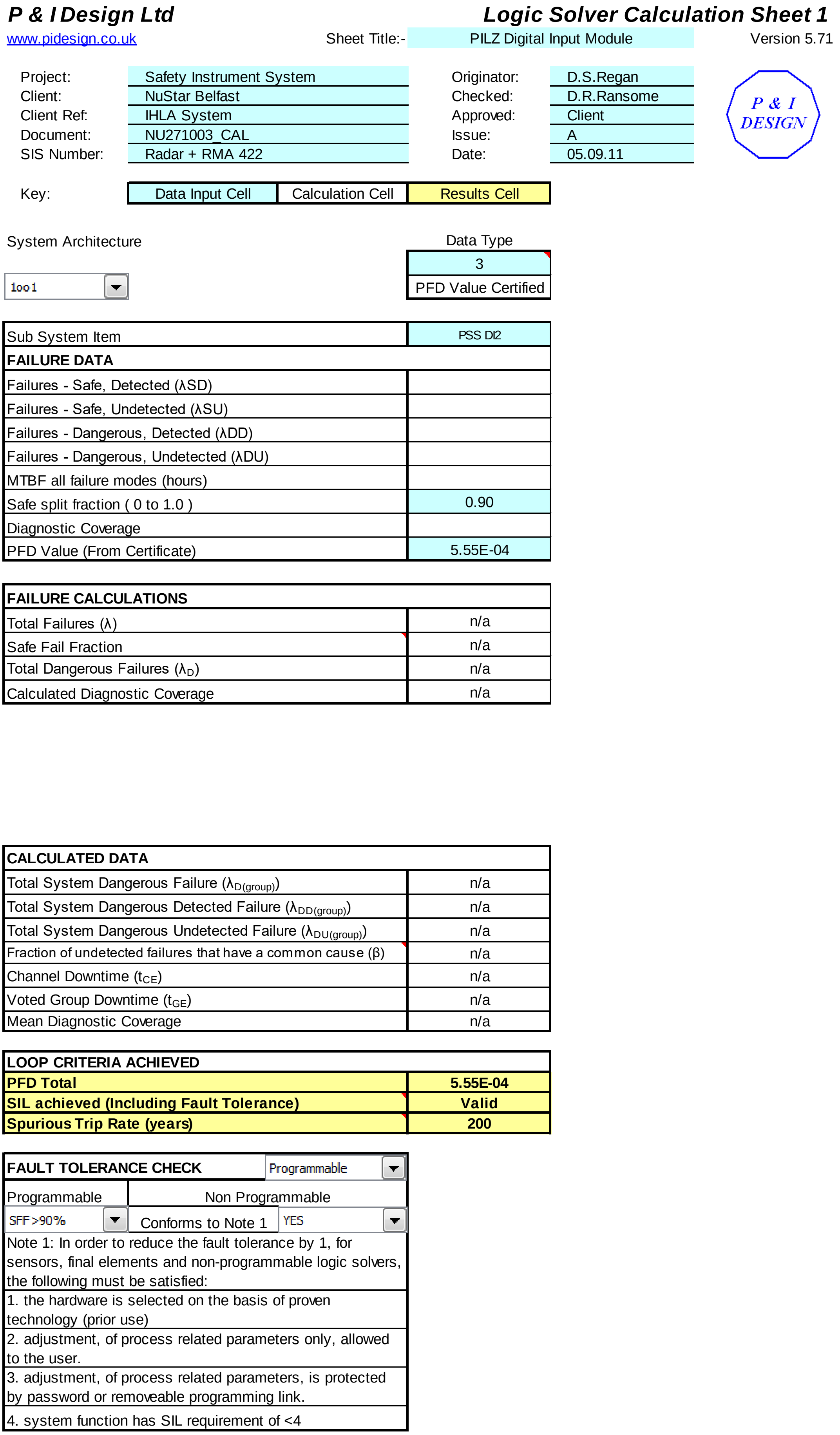
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

www.pidesign.co.uk

Logic Solver Calculation Sheet 1

Sheet Title:- PILZ Digital Input Module

Version 5.71

P & I DESIGN

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS DI2
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	5.55E-04

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

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

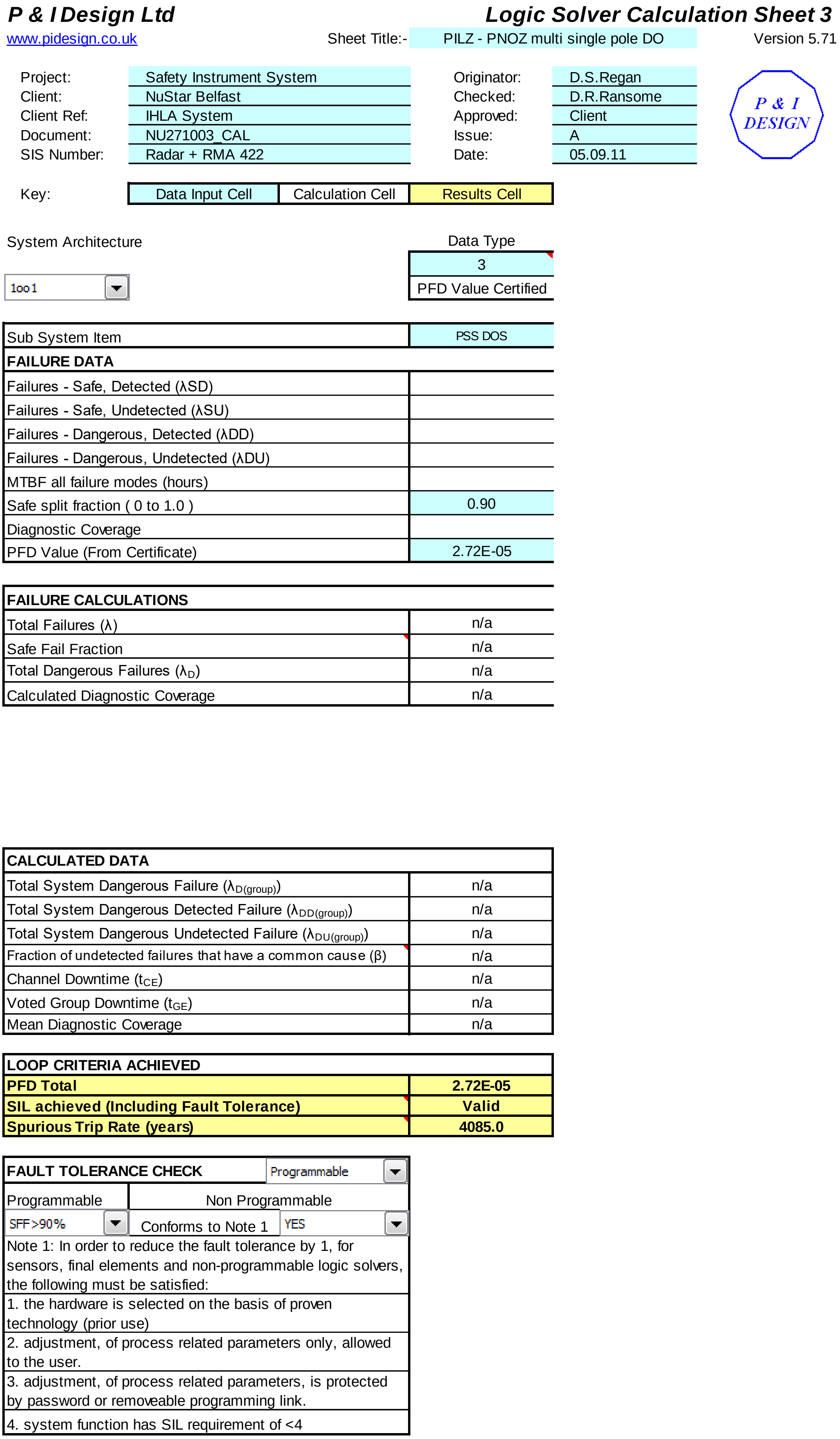
LOOP CRITERIA ACHIEVED	
PFD Total	**5.55E-04**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**200**

FAULT TOLERANCE CHECK Programmable

Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4



P & I Design Ltd

Logic Solver Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- PILZ - PNOZ multi single pole DO

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS DOS
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.72E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.72E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**4085.0**

FAULT TOLERANCE CHECK Programmable

Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

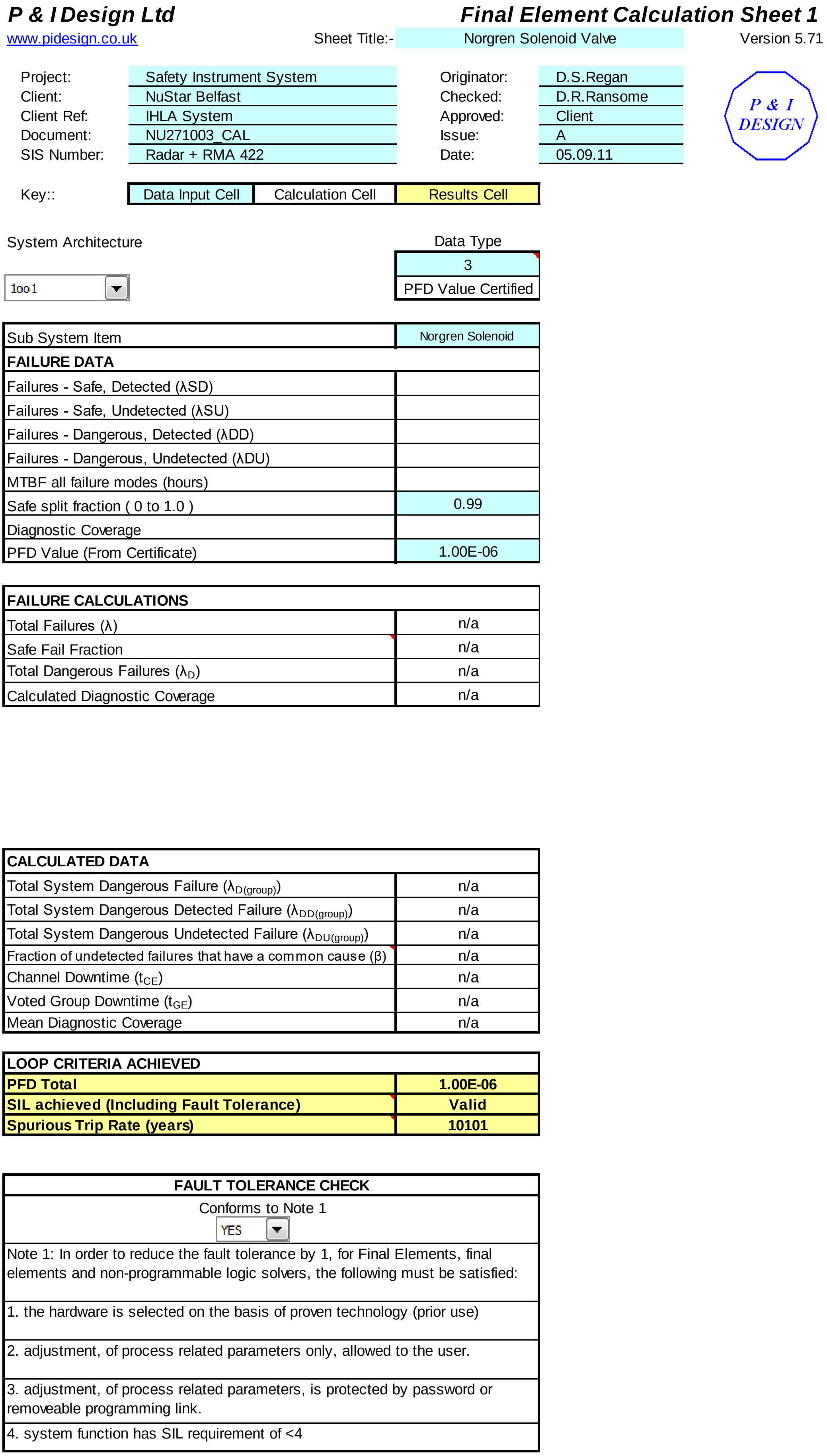
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 1

www.pidesign.co.uk

Sheet Title:- Norgren Solenoid Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

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

System Architecture

1oo1

Data Type
3
PFD Value Certified

Sub System Item	Norgren Solenoid
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.99
Diagnostic Coverage	
PFD Value (From Certificate)	1.00E-06

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**1.00E-06**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**10101**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

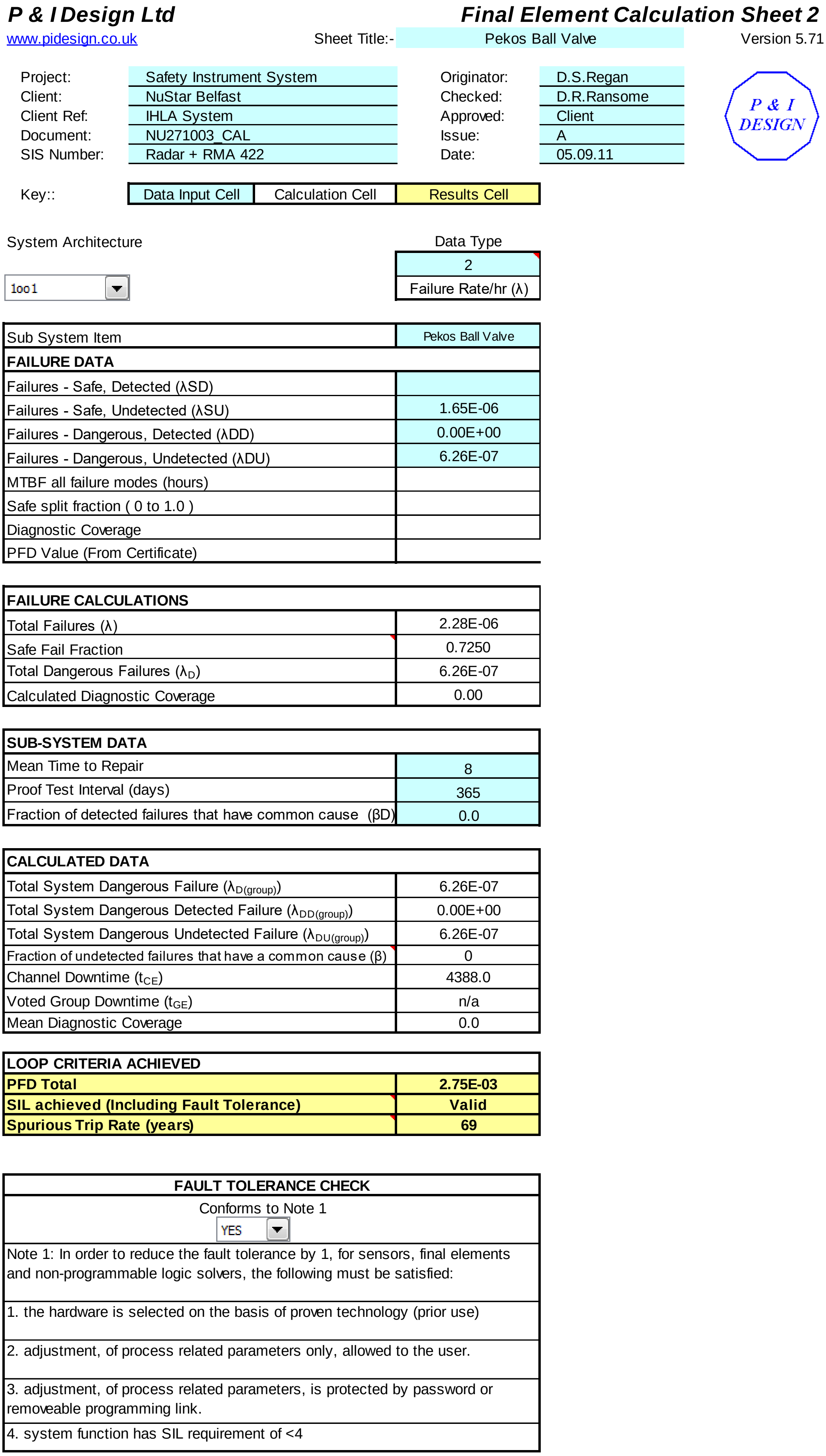
Note 1: In order to reduce the fault tolerance by 1, for Final Elements, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



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

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

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

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

System Architecture: 1oo1

Data Type: 2 — Failure Rate/hr (λ)

Sub System Item	Pekos Ball Valve
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	1.65E-06
Failures - Dangerous, Detected (λDD)	0.00E+00
Failures - Dangerous, Undetected (λDU)	6.26E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	2.28E-06
Safe Fail Fraction	0.7250
Total Dangerous Failures (λ_D)	6.26E-07
Calculated Diagnostic Coverage	0.00

SUB-SYSTEM DATA	
Mean Time to Repair	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	6.26E-07
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	0.00E+00
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	6.26E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	4388.0
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	0.0

LOOP CRITERIA ACHIEVED	
PFD Total	**2.75E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**69**

FAULT TOLERANCE CHECK

Conforms to Note 1: YES

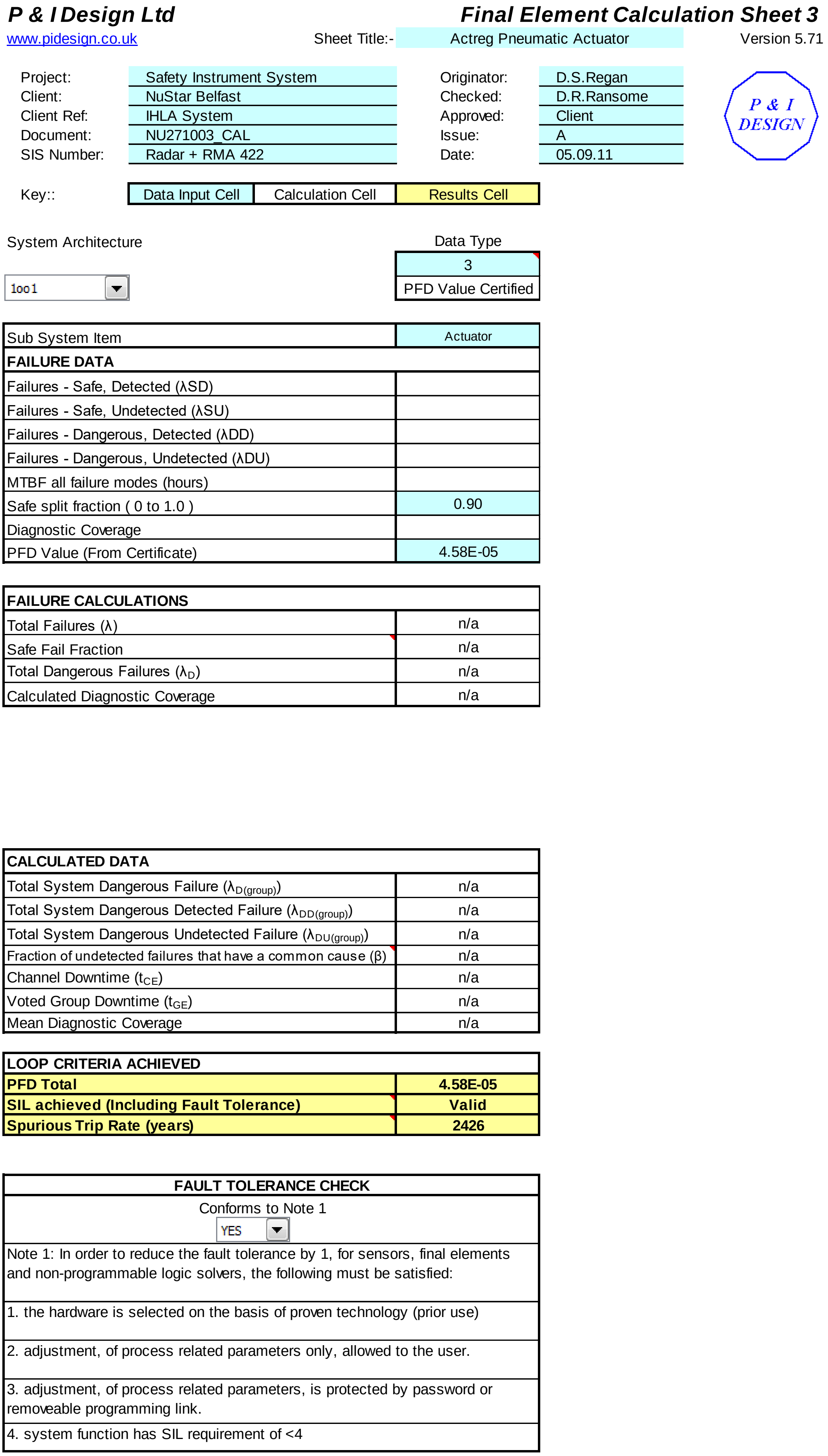
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

www.pidesign.co.uk

Final Element Calculation Sheet 3

Sheet Title:- Actreg Pneumatic Actuator

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271003_CAL	Issue:	A
SIS Number:	Radar + RMA 422	Date:	05.09.11

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

System Architecture

1oo1

Data Type

3

PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

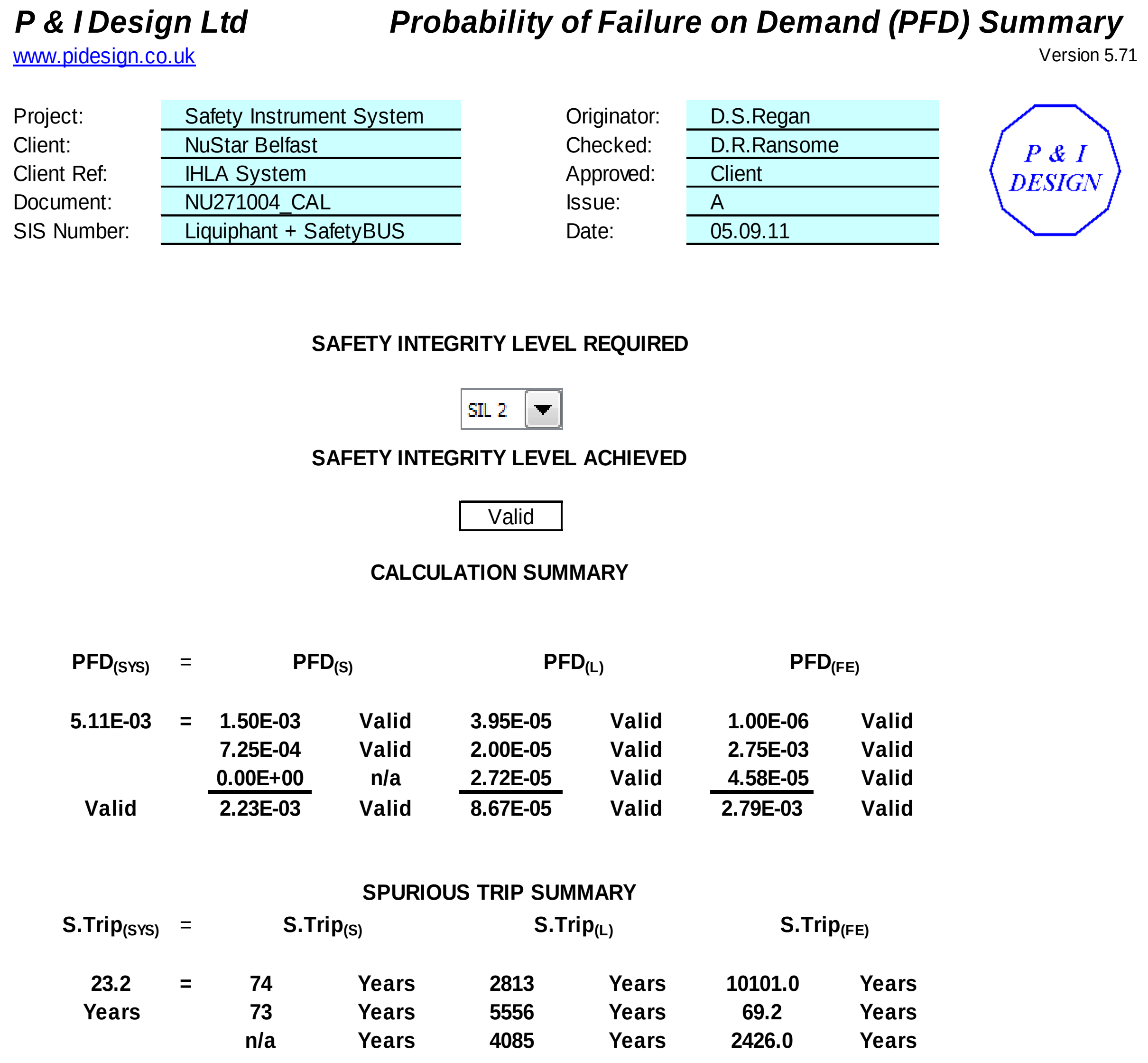
1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

Tanks 3, 6, 9 & 15



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

www.pidesign.co.uk

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

SAFETY INTEGRITY LEVEL REQUIRED

SIL 2

SAFETY INTEGRITY LEVEL ACHIEVED

Valid

CALCULATION SUMMARY

PFD$_{(SYS)}$	=	PFD$_{(S)}$		PFD$_{(L)}$		PFD$_{(FE)}$	
5.11E-03	=	1.50E-03	Valid	3.95E-05	Valid	1.00E-06	Valid
		7.25E-04	Valid	2.00E-05	Valid	2.75E-03	Valid
		0.00E+00	n/a	2.72E-05	Valid	4.58E-05	Valid
Valid		2.23E-03	Valid	8.67E-05	Valid	2.79E-03	Valid

SPURIOUS TRIP SUMMARY

S.Trip$_{(SYS)}$	=	S.Trip$_{(S)}$		S.Trip$_{(L)}$		S.Trip$_{(FE)}$	
23.2	=	74	Years	2813	Years	10101.0	Years
Years		73	Years	5556	Years	69.2	Years
		n/a	Years	4085	Years	2426.0	Years

P & I Design Ltd

PFD - Sensor Subsystem Calculation Sheet 1

www.pidesign.co.uk

Sheet Title:- Sensor E&H Liquiphant +FTL325P

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

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

System Architecture

1oo1

Data Type
3
PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

P & I Design Ltd | **PFD - Sensor Subsystem Calculation Sheet 2**

www.pidesign.co.uk | Sheet Title:- Pilz SafetyBUS | Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

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

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSSu EF 4DI
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.95
Diagnostic Coverage	
PFD Value (From Certificate)	7.25E-04

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**7.25E-04**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**73**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

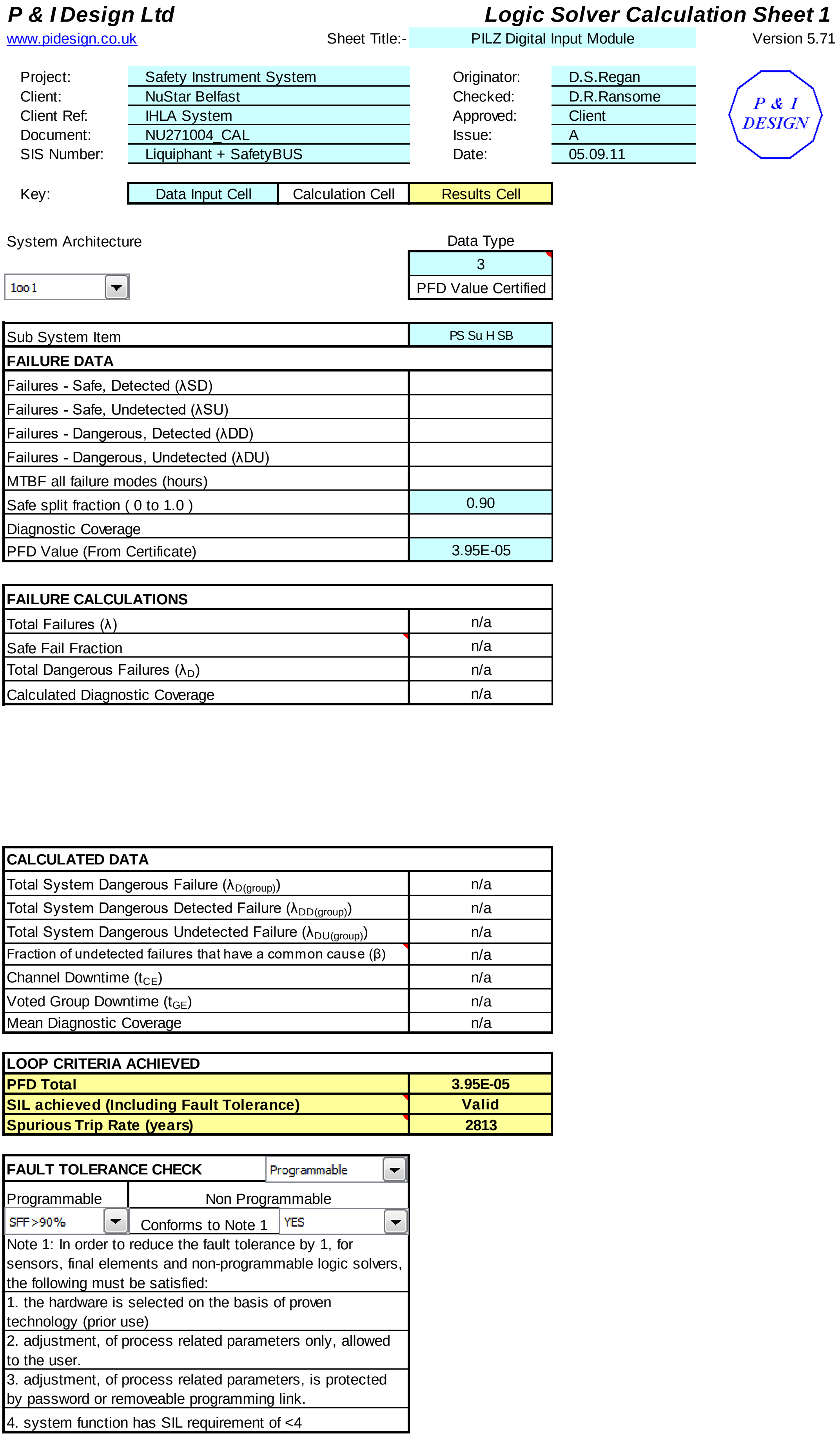
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Logic Solver Calculation Sheet 1

www.pidesign.co.uk

Sheet Title:- PILZ Digital Input Module

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PS Su H SB
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	3.95E-05

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

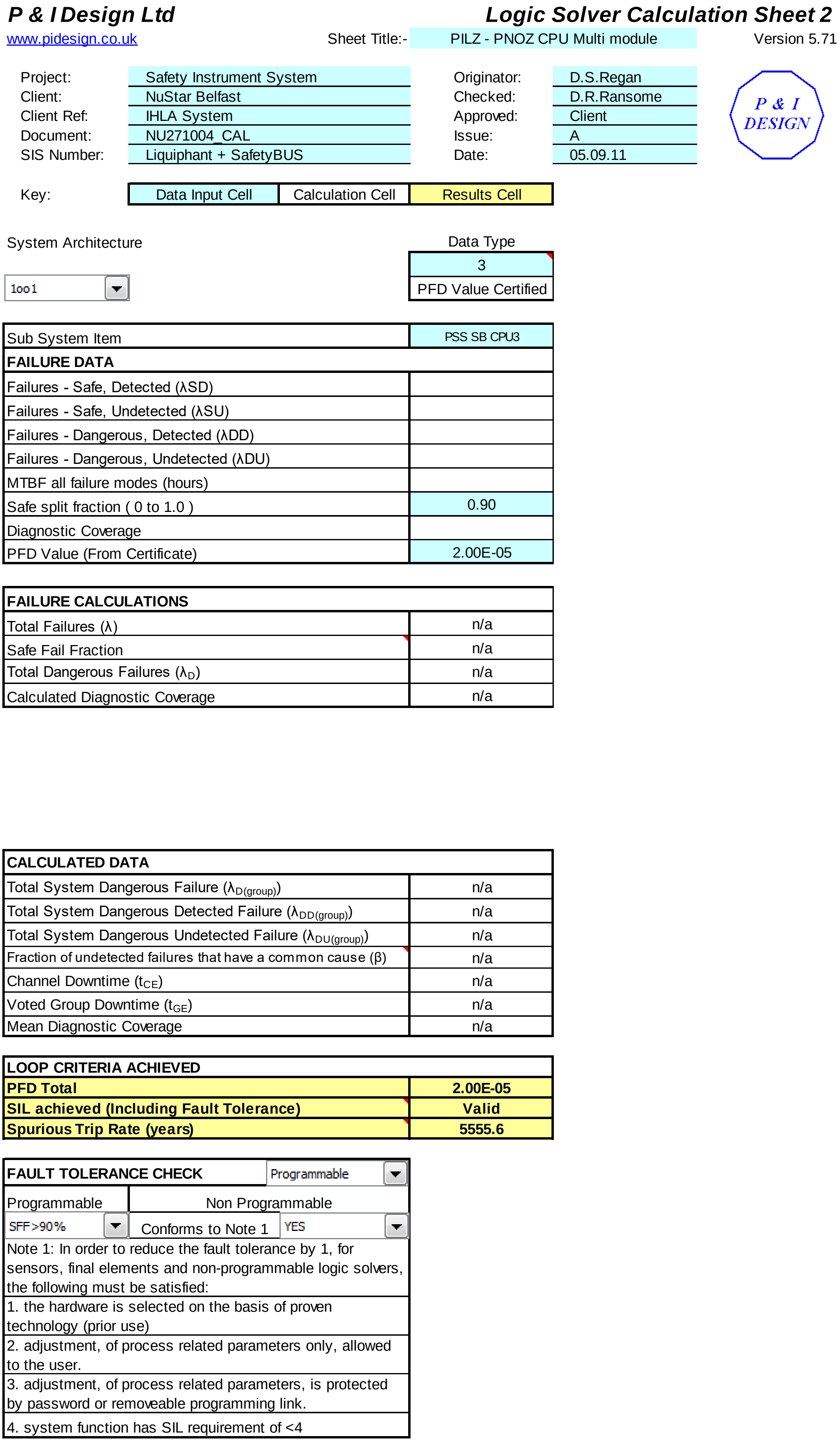
CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})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

LOOP CRITERIA ACHIEVED	
PFD Total	**3.95E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**2813**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4



P & I Design Ltd

www.pidesign.co.uk

Logic Solver Calculation Sheet 2

Sheet Title:- PILZ - PNOZ CPU Multi module

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS SB CPU3
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.00E-05

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

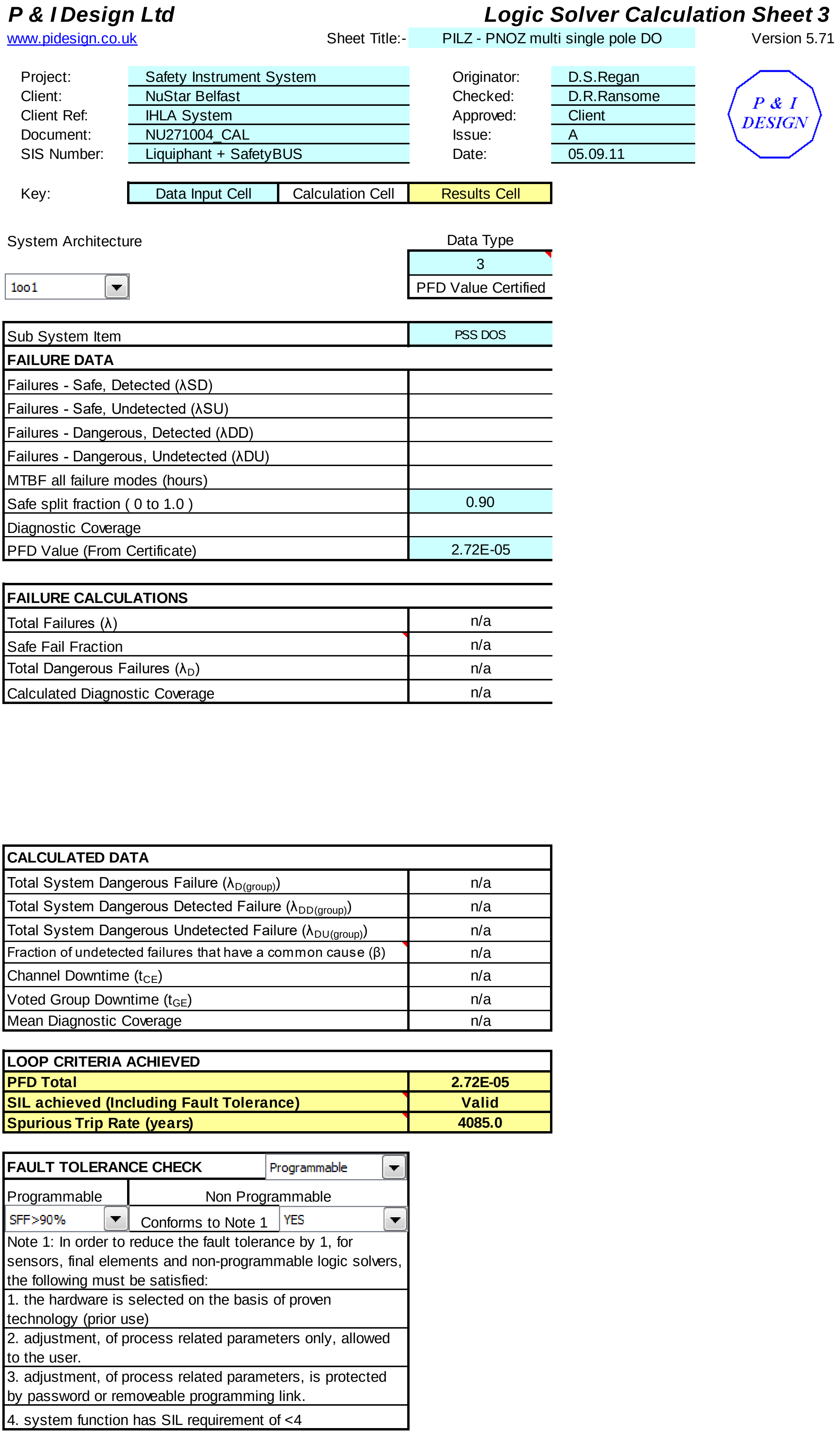
CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.00E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**5555.6**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4



P & I Design Ltd — **Logic Solver Calculation Sheet 3**

www.pidesign.co.uk — Sheet Title:- PILZ - PNOZ multi single pole DO — Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS DOS
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.72E-05

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

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

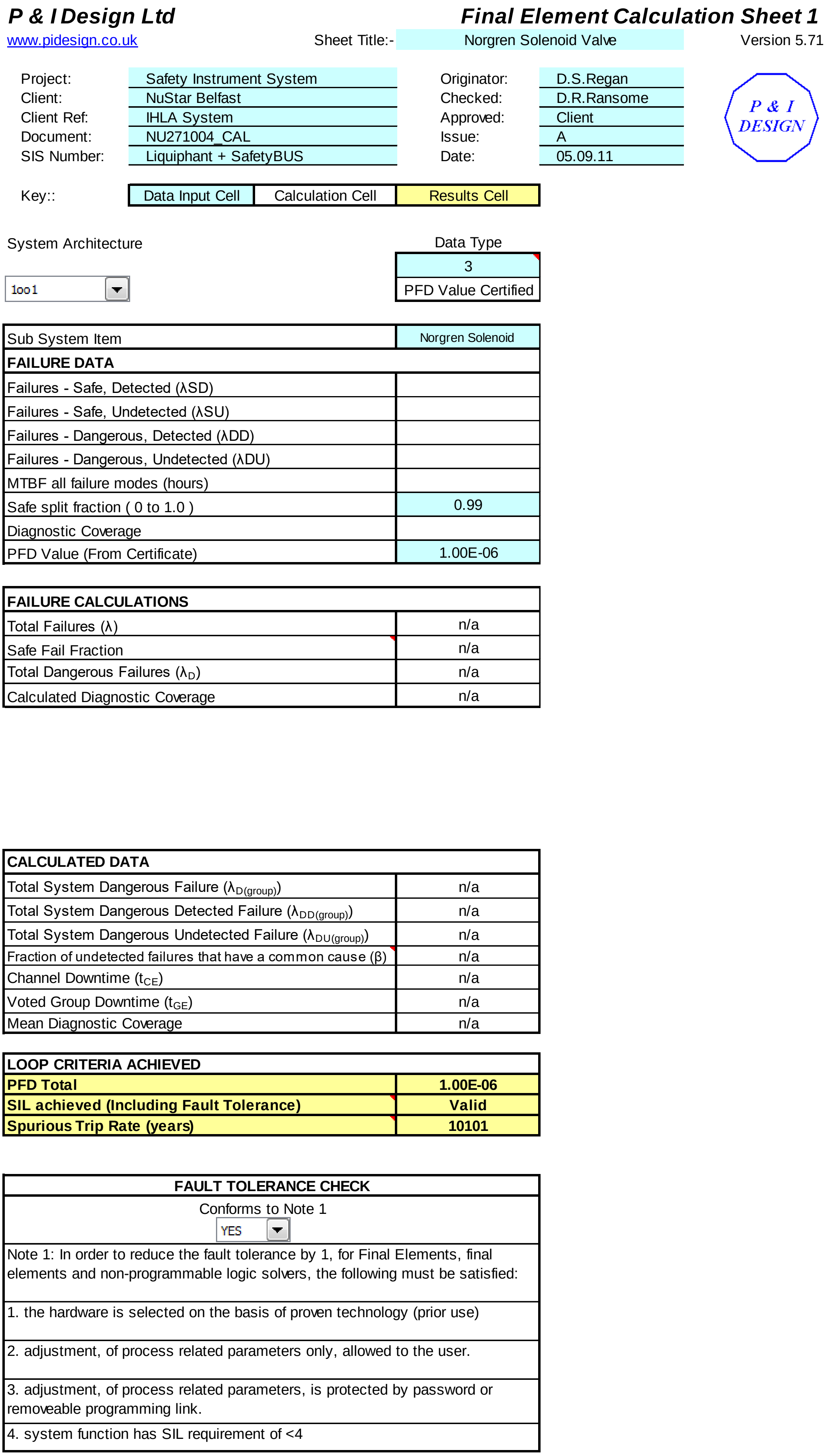
LOOP CRITERIA ACHIEVED	
PFD Total	**2.72E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**4085.0**

FAULT TOLERANCE CHECK — Programmable

Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 1

www.pidesign.co.uk

Sheet Title:- Norgren Solenoid Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

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

System Architecture

1oo1

Data Type

3

PFD Value Certified

Sub System Item	Norgren Solenoid
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.99
Diagnostic Coverage	
PFD Value (From Certificate)	1.00E-06

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**1.00E-06**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**10101**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

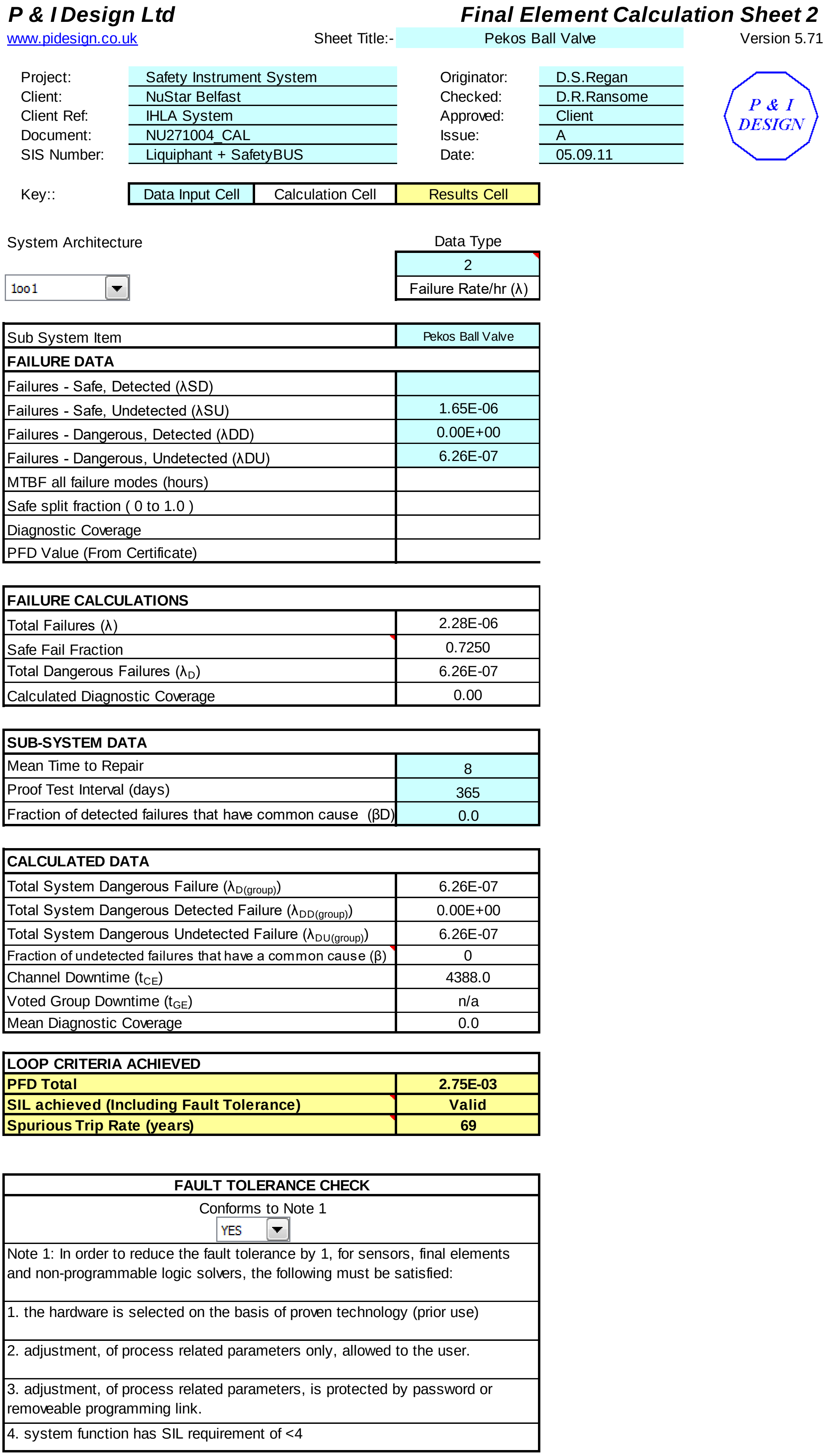
Note 1: In order to reduce the fault tolerance by 1, for Final Elements, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 2

www.pidesign.co.uk

Sheet Title:- Pekos Ball Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

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

System Architecture

1oo1

Data Type

2

Failure Rate/hr (λ)

Sub System Item	Pekos Ball Valve
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	1.65E-06
Failures - Dangerous, Detected (λDD)	0.00E+00
Failures - Dangerous, Undetected (λDU)	6.26E-07
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	
Diagnostic Coverage	
PFD Value (From Certificate)	

FAILURE CALCULATIONS	
Total Failures (λ)	2.28E-06
Safe Fail Fraction	0.7250
Total Dangerous Failures (λ_D)	6.26E-07
Calculated Diagnostic Coverage	0.00

SUB-SYSTEM DATA	
Mean Time to Repair	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	0.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	6.26E-07
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	0.00E+00
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	6.26E-07
Fraction of undetected failures that have a common cause (β)	0
Channel Downtime (t_{CE})	4388.0
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	0.0

LOOP CRITERIA ACHIEVED	
PFD Total	**2.75E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**69**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

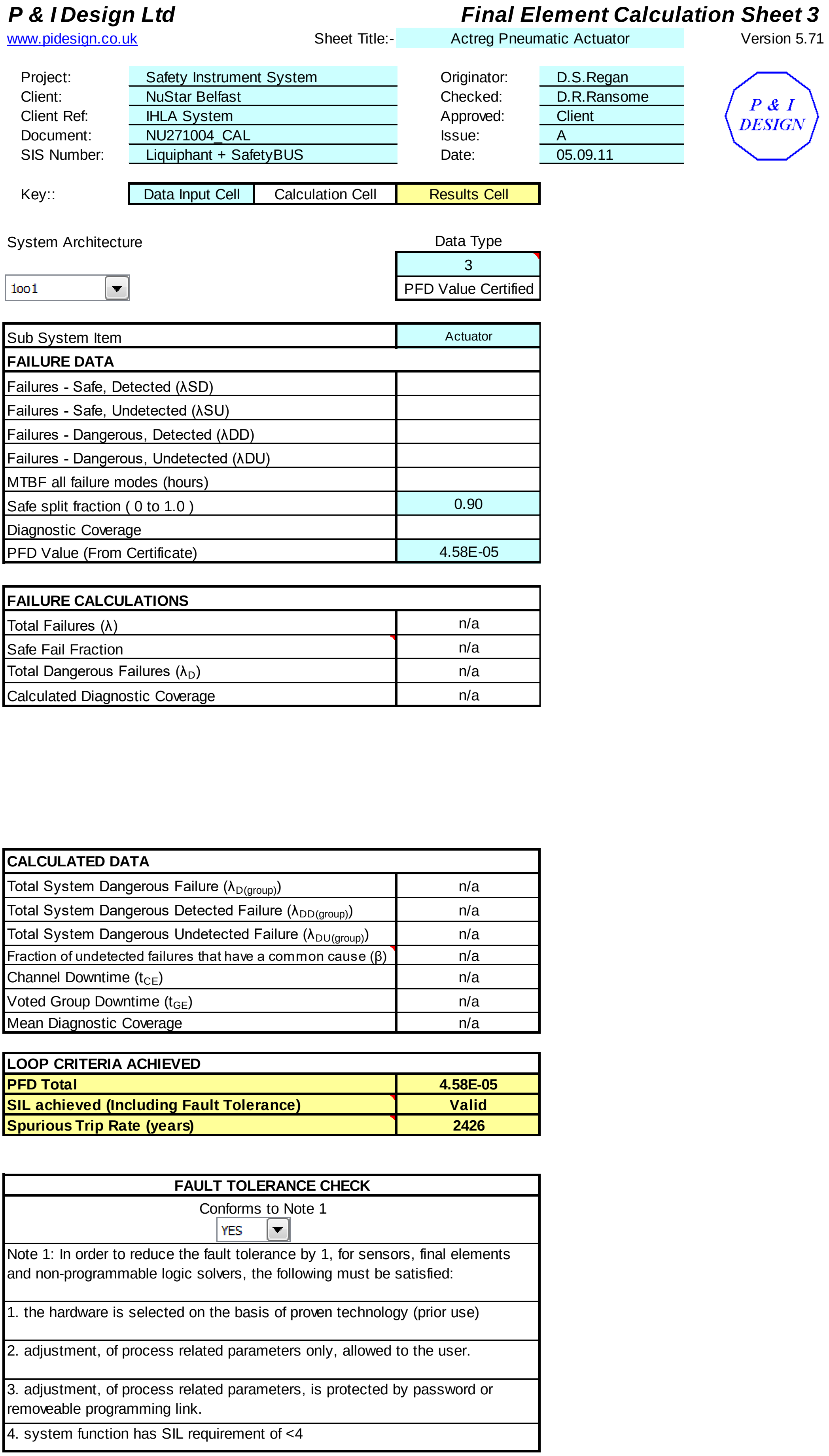
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- Actreg Pneumatic Actuator

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271004_CAL	Issue:	A
SIS Number:	Liquiphant + SafetyBUS	Date:	05.09.11

P & I DESIGN

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

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

Tanks 1, 2, 13, 16, 17, 18, 19, 20 & 21 + Tanks 7, 8, 10, 14, 20, 49, 50 & 48 with 2oo2 Valves

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

www.pidesign.co.uk

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

SAFETY INTEGRITY LEVEL REQUIRED

SIL 2

SAFETY INTEGRITY LEVEL ACHIEVED

Valid

CALCULATION SUMMARY

$PFD_{(SYS)}$	=	$PFD_{(S)}$		$PFD_{(L)}$		$PFD_{(FE)}$	
7.69E-03	=	**1.50E-03**	**Valid**	**5.55E-04**	**Valid**	**2.00E-06**	**Valid**
		0.00E+00	**n/a**	**2.00E-05**	**Valid**	**5.49E-03**	**Valid**
		0.00E+00	**n/a**	**2.72E-05**	**Valid**	**9.16E-05**	**Valid**
Valid		**1.50E-03**	**Valid**	**6.02E-04**	**Valid**	**5.59E-03**	**Valid**

SPURIOUS TRIP SUMMARY

$S.Trip_{(SYS)}$	=	$S.Trip_{(S)}$		$S.Trip_{(L)}$		$S.Trip_{(FE)}$	
29.9	=	**74**	**Years**	**200**	**Years**	**10101.0**	**Years**
Years		**n/a**	**Years**	**5556**	**Years**	**69.2**	**Years**
		n/a	**Years**	**4085**	**Years**	**5885509.0**	**Years**

P & I Design Ltd

www.pidesign.co.uk

PFD - Sensor Subsystem Calculation Sheet 1

Sheet Title:- Sensor E&H Liquiphant +FTL325P

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

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

System Architecture

1oo1

Data Type
3
PFD Value Certified

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

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

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

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

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

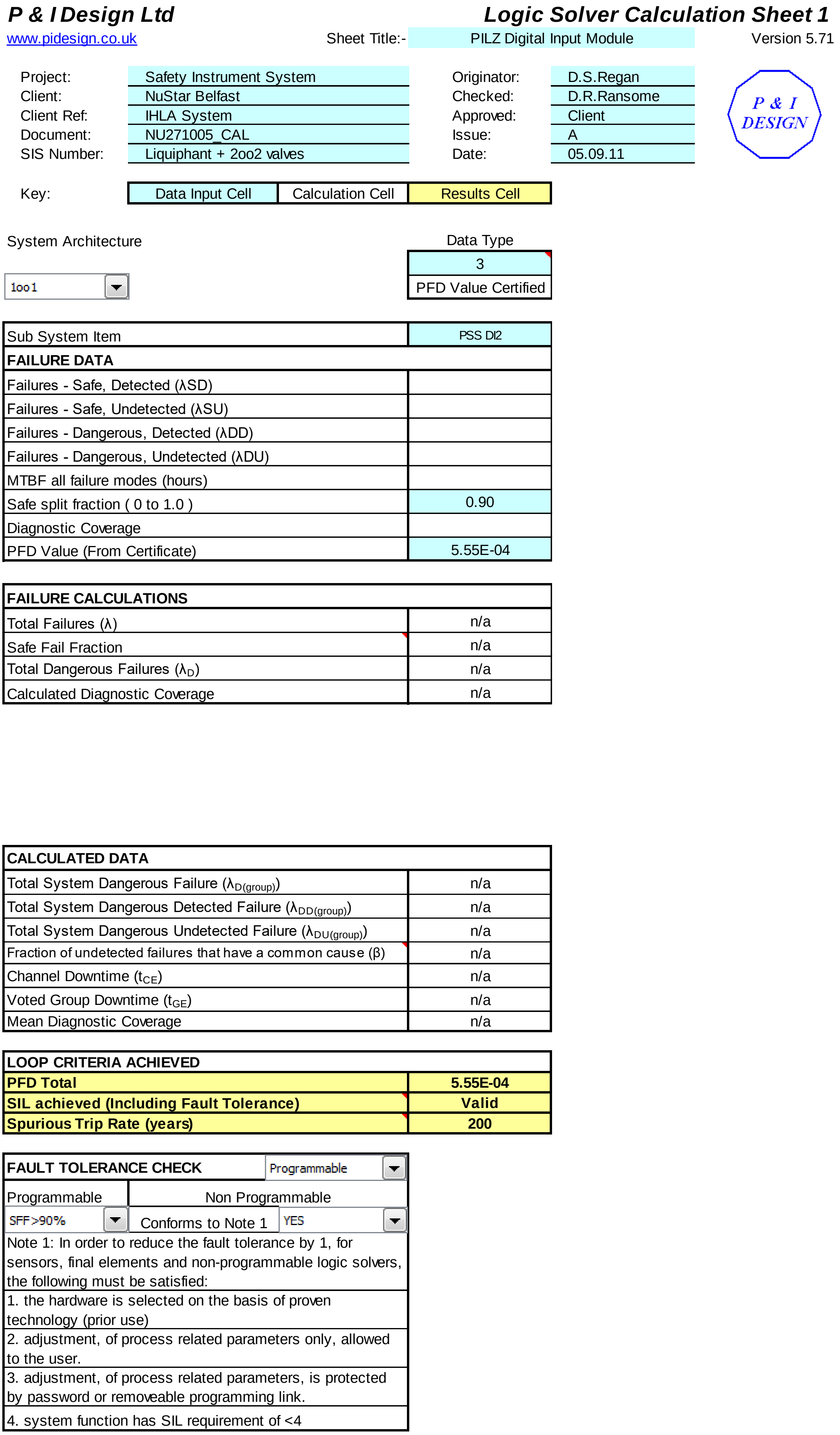
Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

www.pidesign.co.uk

Logic Solver Calculation Sheet 1

Sheet Title:- PILZ Digital Input Module

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS DI2
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	5.55E-04

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**5.55E-04**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**200**

FAULT TOLERANCE CHECK Programmable

Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

P & I Design Ltd

Logic Solver Calculation Sheet 2

www.pidesign.co.uk

Sheet Title:- PILZ - PNOZ CPU Multi module

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture: 1oo1

Data Type: 3 — PFD Value Certified

Sub System Item	PSS CPU3
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.00E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.00E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**5555.6**

FAULT TOLERANCE CHECK	Programmable	
Programmable	Non Programmable	
SFF>90%	Conforms to Note 1	YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4

P & I Design Ltd

Logic Solver Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- PILZ - PNOZ multi single pole DO

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

P & I DESIGN

Key: Data Input Cell | Calculation Cell | Results Cell

System Architecture

1oo1 ▾

Data Type
3
PFD Value Certified

Sub System Item	PSS DOS
FAILURE DATA	
Failures - Safe, Detected (λSD)	
Failures - Safe, Undetected (λSU)	
Failures - Dangerous, Detected (λDD)	
Failures - Dangerous, Undetected (λDU)	
MTBF all failure modes (hours)	
Safe split fraction (0 to 1.0)	0.90
Diagnostic Coverage	
PFD Value (From Certificate)	2.72E-05

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

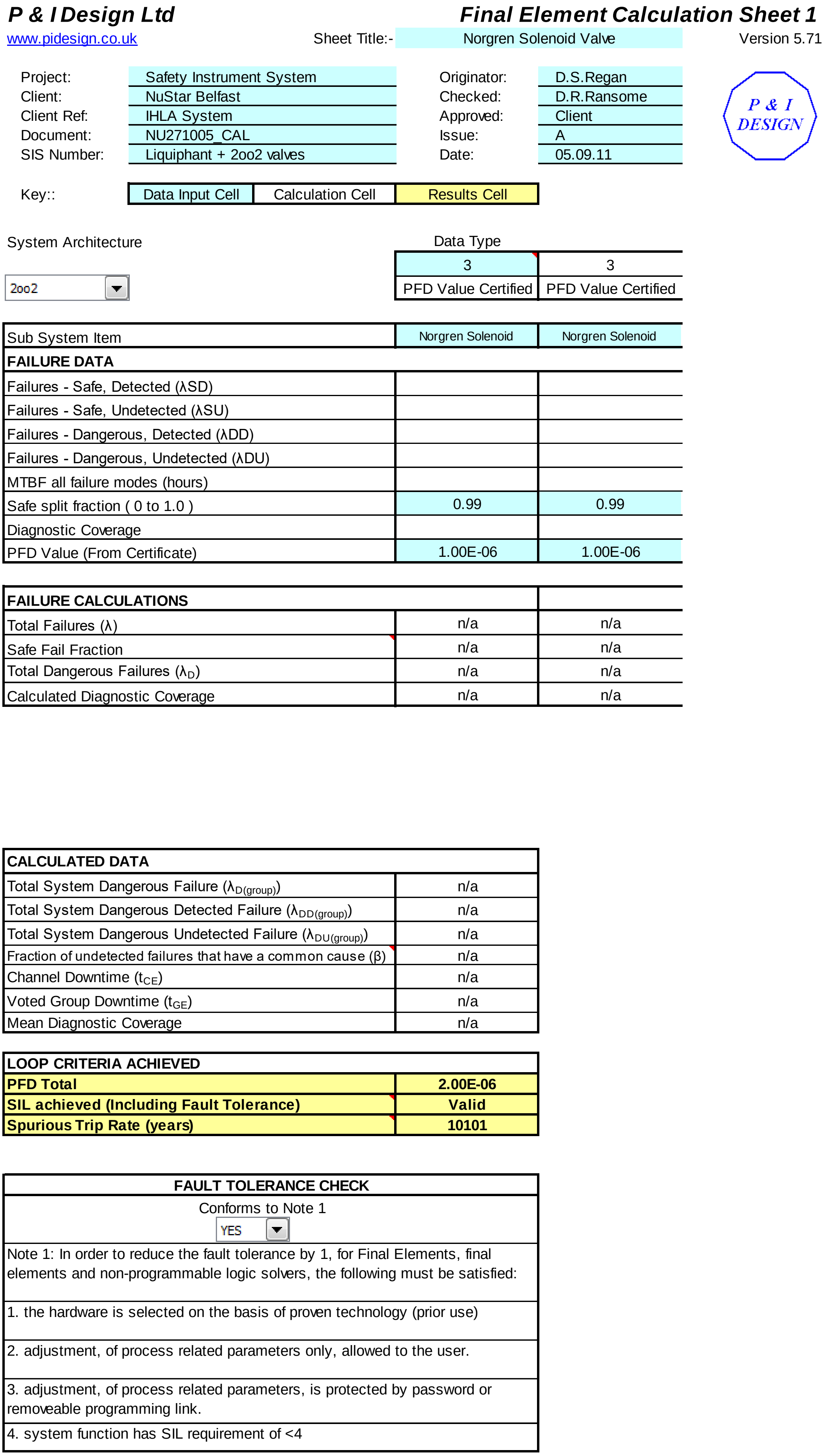
CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	n/a
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	n/a
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	n/a
Fraction of undetected failures that have a common cause (β)	n/a
Channel Downtime (t_{CE})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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.72E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**4085.0**

FAULT TOLERANCE CHECK	Programmable ▾	
Programmable	Non Programmable	
SFF>90% ▾	Conforms to Note 1	YES ▾

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)
2. adjustment, of process related parameters only, allowed to the user.
3. adjustment, of process related parameters, is protected by password or removeable programming link.
4. system function has SIL requirement of <4



P & I Design Ltd

Final Element Calculation Sheet 1

www.pidesign.co.uk

Sheet Title:- Norgren Solenoid Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

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

System Architecture

2oo2

Data Type	
3	3
PFD Value Certified	PFD Value Certified

Sub System Item	Norgren Solenoid	Norgren Solenoid
FAILURE DATA		
Failures - Safe, Detected (λSD)		
Failures - Safe, Undetected (λSU)		
Failures - Dangerous, Detected (λDD)		
Failures - Dangerous, Undetected (λDU)		
MTBF all failure modes (hours)		
Safe split fraction (0 to 1.0)	0.99	0.99
Diagnostic Coverage		
PFD Value (From Certificate)	1.00E-06	1.00E-06

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**2.00E-06**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**10101**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

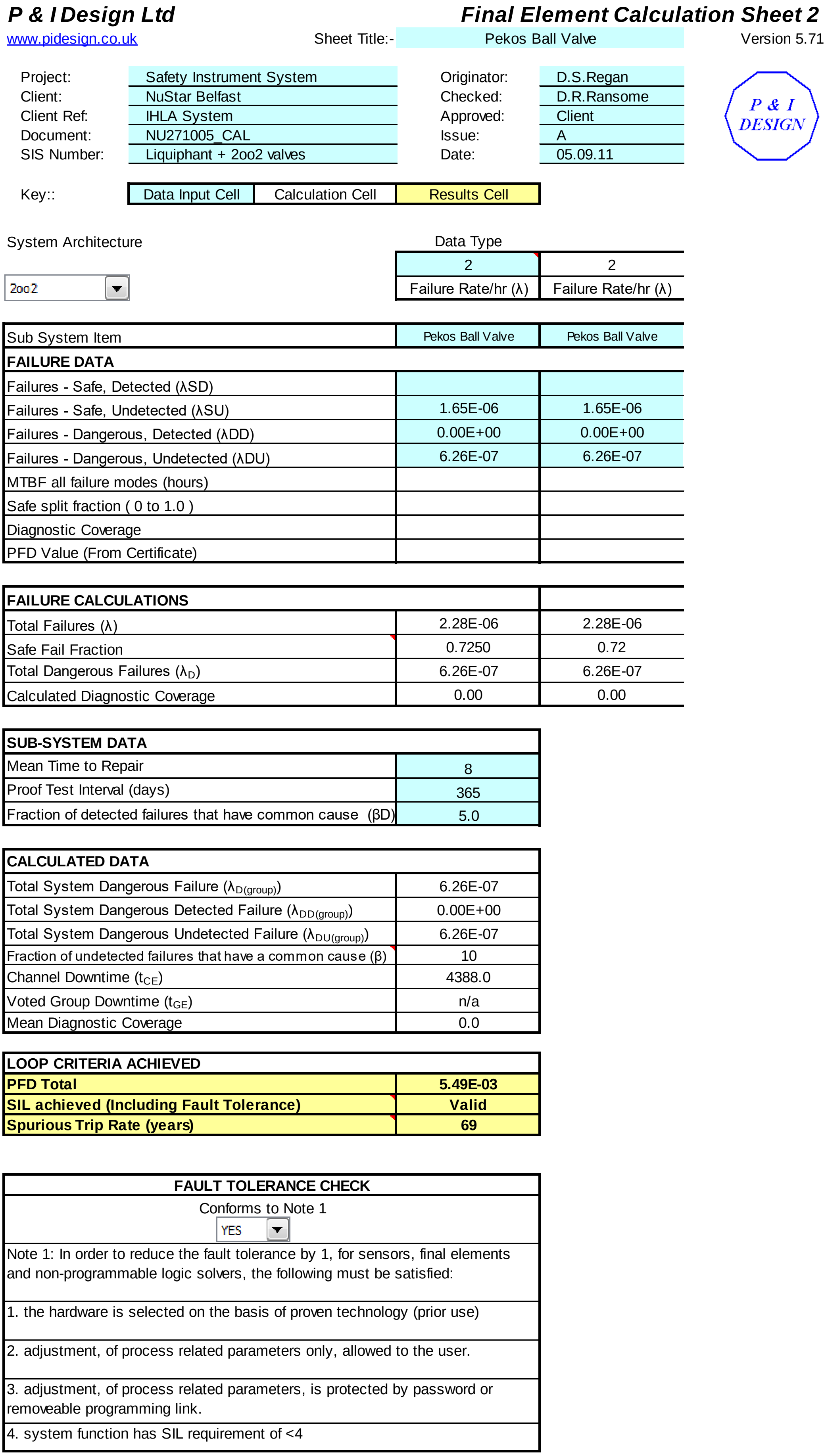
Note 1: In order to reduce the fault tolerance by 1, for Final Elements, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4



P & I Design Ltd

www.pidesign.co.uk

Final Element Calculation Sheet 2

Sheet Title:- Pekos Ball Valve

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

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

System Architecture: 2oo2 ▼

Data Type	
2	2
Failure Rate/hr (λ)	Failure Rate/hr (λ)

Sub System Item	Pekos Ball Valve	Pekos Ball Valve
FAILURE DATA		
Failures - Safe, Detected (λSD)		
Failures - Safe, Undetected (λSU)	1.65E-06	1.65E-06
Failures - Dangerous, Detected (λDD)	0.00E+00	0.00E+00
Failures - Dangerous, Undetected (λDU)	6.26E-07	6.26E-07
MTBF all failure modes (hours)		
Safe split fraction (0 to 1.0)		
Diagnostic Coverage		
PFD Value (From Certificate)		

FAILURE CALCULATIONS		
Total Failures (λ)	2.28E-06	2.28E-06
Safe Fail Fraction	0.7250	0.72
Total Dangerous Failures (λ_D)	6.26E-07	6.26E-07
Calculated Diagnostic Coverage	0.00	0.00

SUB-SYSTEM DATA	
Mean Time to Repair	8
Proof Test Interval (days)	365
Fraction of detected failures that have common cause (βD)	5.0

CALCULATED DATA	
Total System Dangerous Failure ($\lambda_{D(group)}$)	6.26E-07
Total System Dangerous Detected Failure ($\lambda_{DD(group)}$)	0.00E+00
Total System Dangerous Undetected Failure ($\lambda_{DU(group)}$)	6.26E-07
Fraction of undetected failures that have a common cause (β)	10
Channel Downtime (t_{CE})	4388.0
Voted Group Downtime (t_{GE})	n/a
Mean Diagnostic Coverage	0.0

LOOP CRITERIA ACHIEVED	
PFD Total	**5.49E-03**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**69**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES ▼

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

P & I Design Ltd

Final Element Calculation Sheet 3

www.pidesign.co.uk

Sheet Title:- Actreg Pneumatic Actuator

Version 5.71

Project:	Safety Instrument System	Originator:	D.S.Regan
Client:	NuStar Belfast	Checked:	D.R.Ransome
Client Ref:	IHLA System	Approved:	Client
Document:	NU271005_CAL	Issue:	A
SIS Number:	Liquiphant + 2oo2 valves	Date:	05.09.11

Key::	Data Input Cell	Calculation Cell	Results Cell

System Architecture

2oo2

	Data Type	
	3	3
	PFD Value Certified	PFD Value Certified
Sub System Item	Actuator	Actuator
FAILURE DATA		
Failures - Safe, Detected (λSD)		
Failures - Safe, Undetected (λSU)		
Failures - Dangerous, Detected (λDD)		
Failures - Dangerous, Undetected (λDU)		
MTBF all failure modes (hours)		
Safe split fraction (0 to 1.0)	0.90	0.90
Diagnostic Coverage		
PFD Value (From Certificate)	4.58E-05	4.58E-05

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

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

LOOP CRITERIA ACHIEVED	
PFD Total	**9.16E-05**
SIL achieved (Including Fault Tolerance)	**Valid**
Spurious Trip Rate (years)	**5885509**

FAULT TOLERANCE CHECK

Conforms to Note 1

YES

Note 1: In order to reduce the fault tolerance by 1, for sensors, final elements and non-programmable logic solvers, the following must be satisfied:

1. the hardware is selected on the basis of proven technology (prior use)

2. adjustment, of process related parameters only, allowed to the user.

3. adjustment, of process related parameters, is protected by password or removeable programming link.

4. system function has SIL requirement of <4

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

This was reviewed and discussed at the FSA meeting held on 7th September 2011 at NuStar Belfast. (ACTION 10). FSA Meeting:

Operating procedures associated with the SIS are in place. See Appendix 2.
Maintenance and testing procedures are in place and are carried out internally. See Appendix 2.
Procedures detailing the actions required in an emergency are in place. See Appendix 2.

4.8 Are the safety instrument system validation planning appropriate and have the validation activities been completed?

This was reviewed and discussed at the FSA meeting held on 7th September 2011 at NuStar Belfast. (ACTION 11).
FSA Meeting: NuStar appreciate that they are ultimately responsible for the testing and safe operation of the system as system owners.
It is felt that Proof Testing procedures may need to be further developed to include planning, testing, analysis and approval. ACTION 17
Operators do the testing, Liquiphants are tested (1 tank per week) - more often than annually. Testing is recorded. The closure times of the valves during this test will also be recorded on the modified procedure.

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

This was reviewed and discussed at the FSA meeting to be held on 7th September 2011 at NuStar Belfast. (ACTION 12).
FSA Meeting: Training presentations have been produced, as yet this has not been formalised. (ACTION 18).

4.10 Are plans or strategies for implementing further safety assessments in place?

Any further safety assessments will be carried out as required. At present no further assessments are planned.
However, it will be necessary to review all the Actions and their results arising from this FSA, together with a review of all documentation.

4.11 Compliance to BS EN 61511

As part of P&I Design Ltd. review procedures and forming part of this FSA is a checklist to confirm that all the relevant clauses from the standard have been complied with. See Document NU271002_RPT – SIS Compliance Document. (ACTION 13).
FSA Meeting: The compliance document is to be completed following the conclusion of all other Actions and following review of documentation.

5 CONCLUSIONS

5.1 FSA meeting

The Safety Lifecycle documentation reviewed at Revision A of this FSA was provided by NuStar.

Following this FSA assessment it appears that there is lifecycle documentation incomplete, missing or not available at this time.

Life-cycle documentation:

- Management of Functional Safety Document (Not available for FSA – to be compiled)
- LOPA Report (To be reviewed and reworked to include calculated PFD and possibility of the continued lack of Mitigation Layer 1) including:
  - Allocation of Safety Functions
  - Required Integrity Level of Safety Functions
  - Tank to tank Transfers
- Safety Requirement Specification (Not available for FSA – to be compiled. A functional Specification was available but lacked some detail required by the standard)
- SIF Calculations (To be revised to include installed system and comments from FSA)
- Process & Instrumentation Drawings (Not available for FSA – to be completed and reviewed)
- SIS Design Dossier
  - Equipment Specifications (None provided, normal procedure to identify instrumentation by specific loop sheet and included on plant equipment register)
  - Interface with BPCS Document (None provided, to be included in SRS and SIL Assessment)
  - Software Schematics and Program (None provided, to be provided and reviewed by Functional Safety Committee)
  - System Overview and Loop Drawings (To be revised to include installed system and comments from FSA)
- Proof Testing Documentation (New end to end Proof Testing and equipment failure testing procedures will be developed to include planning, testing, analysis and approval. These procedures will include for non-disturbed tests as well as for current injection tests (high mA range, low mA range or multiple mid-range), valve closure time tests or actual functional tests. There will be recording documents as part of the procedure and an approval system.)
- Modification and Management of Change Procedures (Not available for FSA – to be completed and reviewed)

This Functional Safety Assessment concludes that the Probability of Failure on Demand calculation and hardware fault tolerance meet the requirements of a SIL 2 Safety Instrumented System.

As a result of this FSA, Nustar Terminals are modifying some of their management procedures and documentation to ensure that all aspects of the safety lifecycle, see Action list, are in line with BS EN 61511.

Subsequent developments have led to NuStar engaging P&I Design Ltd. to assist in the management of the Functional Safety Aspects of the Safety Instrument Systems at all five of the NuStar terminals and as such a Safety Committee will be set up comprising of NuStar and P&I Design Ltd. Personnel. The purpose will be to ensure compliance with all aspects of the BS EN 61511 standard in respect of the Safety Instrument Systems installed. As such Functional Safety Assessments have been carried out on all the terminals and action lists compiled to ensure that the systems comply with the standard.

6 ACTIONS

Action No.	Action	By	Expected Completion	Completion Date
1	PFD to be added in to the LOPA calculation to confirm suitability of risk reduction	Nustar Terminals	End October 2011	30/09/11
2	LOPA calculation is to be re-worked to consider the mitigated risk whilst the bund liquid level detectors are not installed.	Nustar Terminals	End October 2011	30/09/11
3	NuStar may decide to add to the Functional Specification details that are required within a SRS, but not currently in the Functional Specification.	Nustar Terminals	End October 2011	30/09/11
4	Provide a block diagram showing functionality of the various SIF's	Nustar Terminals	End October 2011	30/09/11
5	Software or software validation to be provided to complete FSA	Nustar Terminals	End November 2011	End November 2011
6	Review of override control to be assessed against PSLG guidance	Nustar Terminals & FSA	End October 2011	30/09/11
7	NuStar to confirm how they will provide management of change now the system is operational. Also include unique document numbers to documentation, at present, un-numbered.	Nustar Terminals	End November 2011	April 2012
8	Review LOPA for the addition of gasoline tank to tank transfers. Still incomplete	Nustar Terminals	End November 2013	March 2015
9	Review of SIL Verification document including check of PFD and hardware fault tolerance calculations.	P & I Design Ltd	End November 2011	End November 2011
10	Safety, Operating and maintenance Procedures to be reviewed.	FSA	07/09/11	30/09/11
11	Review of validation and Testing plans and procedures.	FSA	07/09/11	30/09/11
12	Review training, maintenance and operation procedures.	FSA	07/09/11	30/09/11

13	Complete Compliance Document against BS EN 61511	P & I Design Ltd	n/a	Compliance docn. will form part of FSA stage 4
14	Final tag numbers to be added to the P&I Diagrams for re-issue. Still incomplete	NuStar	End November 2013	Confirmed complete by NuStar
15	SIS Instrumentation and Documentation to reflect tag numbering of P & I Drawings also Instrument Tagging should be consistent with P & I Drawings Still incomplete awaiting action 14	NuStar	End November 2013	Confirmed complete by NuStar
16	All SIS documentation to be reviewed and ensure that it reflects P& I Drawings and installed system. Still incomplete awaiting action 14	NuStar	End November 2013	Confirmed complete by NuStar
17	Proof Testing procedures need to be further developed to include planning, testing and analysis and approval. This is in addition to the test conducted by E & H. NU271006, NU271007, NU271008, NU271009 & NU271010	P&I Design Ltd.	February 2013	Proof Test Procedures completed. These will need to be updated for modifications
18	Training is to be formalised, conducted and recorded. Webex presentations may be used for future training of new employees.	NuStar	End April 2012	All training now completed

Appendices

1. Certification
2. Operating Procedures
3. P & I Drawings
4. LOPA Calculation with revised PL pfd and removal of ML

Appendix 1

Certification

Appendix 1

Certification

exida®
CERTIFICATION

CERTIFICATE

PEKOS 090168 P0006 C02

exida Certification S.A. hereby confirms that the

PEKOS Full Trunnion Ball Valves

PEKOS group

Montmeló (Barcelona), Zaratamo (Vizcaya), Spain

Has been assessed according to the relevant requirements of

IEC 61508

Parts 1 - 2, and meets requirements providing a level of integrity to

Systematic Integrity : SIL 3 Capable

Random Integrity : Type A device, PFD_{AVG} and architecture constraints must be verified for each application

Safety Function

The valve will move to the designed safe position within the specified safety time.

Application Restrictions

The unit must be properly designed into a Safety Instrumented Function per the requirements in the Installation, Operations and Maintenance and Safety Manuals for the respective valve type.

Assessor

Certifying Assessor

Date: 8 September 2009

exida Certification SA, Nyon, Switzerland

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 認証

exida®
CERTIFICATION

Systematic Integrity: SIL 3 Capable

SIL 3 Capability

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

For a Full Trunnion Ball Valve used in final element assembly, SIL must also be verified for the specific application using the following failure data:

Summary for the Full Trunnion Ball Valves :

V1 - Full Trunnion Ball valves with soft seat up to 20" / DN500
V2 - Full Trunnion Ball valves with metal-to-metal seat up to 20" / DN500
V3 - Full Trunnion Ball valves with soft seat 3-way up to 12" / DN300

	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

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory parts this certificate:

PEKOS 0901-68-C R004 V1R1 Assessment report.
Safety manual PEKOS group DC 77-02-04 Rev 0

The holder of this certificate may use this mark.

EXIDA FS CERTIFIED

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 認證

ACTREG

ACTREG, S.A.
Cantabria, 2 – Pol Ind. Les Salines
08830 Sant Boi de Llobregat (Barcelona) - SPAIN
Tel. +(34) 936 61 44 10 – Fax +(34) 936 54 33 93
e-mail: sales@actreg.com – http://www.actreg.com

ISO 9001
BUREAU VERITAS
Certification
1828

CERTIFICATE OF CONFORMITY: IEC 61508

ACTREG, S.A. certifies that the ACTREG actuators are suitable for use in safety related systems up to and including SIL 3 according to IEC EN 61508.

The reachable results from internal assessment carried out by the notified company Bureau Veritas (*Ref.: 859-1985759/09/R/058/0 and 859-1985759/09/R/057/0)* and based on the field experience obtained from ACTREG are as follows:

Acronym	**Description**	**Values**
λ_D	Dangerous Failure Rate	1,04E-08
PFD	Probability of Failure on Demand	4,58E-05
PFH	Probability of Failure per Hour	1,04E-08
SFF	Safe Failure Fraction	0.9
MTBF	Mean Time Between Failure (year)	10928
MTTR	Mean Time To Repair	8 hours

According to the field experience and the technical documents of ACTREG, the actuators systems have PFD & PFH suitable to use in safety loops SIL 3.

Sant Boi de Llobregat (Barcelona) Spain
4th March 2009
Quality Assurance Manager

ACTREG ACTREG, S. A.
Cantabria, 2
Polígono Industrial Les Salines
08830 SANT BOI DE LL. (Barcelona)
Tel. +(34) 93 661 44 10
Fax +(34) 93 654 33 93
e-mail: sales@actreg.com

Ref.: ACTREG-SIL rev. 0

TÜVRheinland®

Certificate

No. V 37 2009 C1

Manufacturer **Norgren GmbH**
Stuttgarter Straße 120
70736 Fellbach

Product: **3/2 way-solenoid valves**

Type: **series**
24010XX, 24011XX

Use: **solenoid valve with safety function**

test result: **The above mentioned valves are suitable for use in safety related systems up to and including SIL 4 according to IEC 61508**

For detailed results see test reports
V 37 2004 S1 dated 2004-01-20
V 37 2005 Z2 dated 2005-12-06
V 37 2009 Z1 dated 2009-04-03
A short summary of test results is filed up on the back side of this certificate.

The suitability for certain fields of application can only be assessed by additional evaluation of further components of the subsystem.

This certificate remains valid until 04/2014

Cologne, 2009-04-03

Test laboratory
for energy appliances
Head of Laboratory

Rick

Dipl.-Ing. F. Rick

second page to certificate V 37 2009 C1

Appliance-specific values determined:

Probability of failure on demand	PFD	Failure/demand	**2,00E-07**
Confidence level	1-α		95
Safe failure fraction	SFF	%	0,99
Hardware fault tolerance		HFT	0
Diagnostic coverage		DC	0
Type of sub systems according IEC 61508-2, 7.4.3.1.2			type A
assumed operation conditions			
10 cycles/year (10/8760)/h	Fnp	1/h	1,14 E-03
calculated values:			
Dangerous failure rate $\lambda_{D=}$ PFD x Fnp	λ_D	1/h	**2,28E-10**
		FIT	0,23
MTBFd dangerous failures MTBFd=1/ λ_D		h	**4,38E+09**
	years	y	500000
safe failure rate $\lambda s_= \lambda_D$*SFF/100/(1-SFF/100)	λ_S	1/h	**2,28E-12**
		FIT	0,00
total failure rate	$\lambda_S + \lambda_D$	1/h	**2,31E-10**
		FIT	0,23
MTBF total MTBF=1/ $\lambda_{S+}\lambda_D$		h	**4336638000**
MTBF total	years	y	495050
dangerous detected	λ_{DD}	1/h	0,00E+00
dangerous undetected	λ_{DU}	1/h	2,28E-10
safe detected	λ_{SD}	1/h	0,00E+00
safe undetected	λ_{SU}	1/h	2,28E-12

impact of test interval (full stroke)

test intervall	Ti	y	1	5
av. PFD			1,00E-06	5,00E-06

The results are valid for 3/2-way solenoid valves optionally equipped with a volatile manual override according to report V 37 2009 Z1

Remarks: This statement applies to new appliances and for deployment thereof for a period of time of maximum 6 years plus a maximum of 2 years storage time before being used for the first time and provided that all safety-relevant operating conditions as stated by the manufacturer are complied with.

These statements are bound to the proven and verified deployment of safety-related quality management of the manufacturer.

Appendix 2

Operating Procedures

Testing of IHLA System - 'RADAR'

		Tank 04	Tank 05	Tank 11	Tank 12	Tank 45	Tank 46	Tank 47
Check Dip recorded before transfer								
Difference between manual and auto tank gauge dip								
Calculated Amount to be added, to get level to 'Normal Fill Level'								
Manual Check dip tank (after initial transfer)								
Recorded Reading of ATG and IHLA (after initial transfer)	ITG							
	IHLA							
Difference between manual and auto tank gauge dip								
Calculated amount to be added to get to IHLA activation set point								
Calculations checked by?								
Tankside valve operation checked before transfer (Yes/No)								
Transfer System 'By-Pass' enabled by?								
IHLA activation point recorded at?								
Did all ESV's shut down? (Yes/No)								
Did 'Klaxons' and 'Jetty Warning System' operate?								
IHLA system reset by and product lowered in tank by?								
Transfer system 'By-Pass' disabled and key removed by?								
Test carried out by and date?								

Extreme caution is required when filling tanks to IHLA set point, to ensure no spillage occurs or damaged is caused to floating roofs. Ensure no other product movement is occurring. Report any faults immediately to Terminal Management.

Testing of ‘Liquiphant’ IHLA’s

All tanks except 04, 05, 11, 12, 45, 46 and 47 are fitted with Endress+Hauser Liquiphant IHLA’s. These are designed to operate when product either touches it; it goes into fault mode or fails to communicate with the IHLA PLC.

Each Liquiphant must be checked at least once per annum, to ensure it operates. This is done by pressing the test button on the ‘Nivotester’ for each tank within the IHLA panel located in the main switch room ‘IHLA Control Panel’.

The test will activate the appropriate liquiphant, which should then close all ‘Emergency Shutdown Valve’s or ESV’s’ (after approx 2.5mins).
There are 7 of these, which are located at:

- **Dockline No.01 – No.01 Pump Bay**
- **Dockline No.02 – No.01 Pump Bay**
- **Dockline No.03 – No.01 Pump Bay**
- **Gasoline Transfer Line – At Tk 20**
- **Kero Transfer Line – At Pump 45 (Site 3)**
- **Gas Oil Transfer Line – At Pump 47 (Site 3)**
- **Diesel Transfer Line – At Pump 50 (No.01 Pump Bay)**

It should also activate the two klaxons located on the switch room wall, the jetty warning system and display the activated IHLA in the control room.

This test can only be carried out when no shipping or transfer operations are in progress, and is advisable when the terminal is quiet (i.e. Sat/Sun PM).

1. Using the ‘Testing of IHLA’s – Liquiphant and ESV’s test sheet, select the next tank to be tested from the list.
2. Go to the main switch room and open the ‘IHLA Control Panel’
3. At the bottom of the panel, select the appropriate ‘Nivotester’ for the tank to be tested.
4. Pull the ‘blue’ cover towards you and press in the test button (Do Not use anything metal, i.e. screwdriver etc).
5. Ensure main Klaxons activate (at switch room), Klaxon and warning light at jetty operates and all ESV’s close. Also, check that appropriate IHLA has indicated on control room PC.
6. Once confirmed, system can be muted.
7. Confirm tests have been completed and that system has operated OK.
8. When all checks have been done and test sheet has been completed, the system should be reset.
9. At the main IHLA Control Panel Press and hold the reset button. System should now reset and ESV’s should open.
10. In control room, ensure all valves are indicting that they are open.
11. Reset PC by pressing and holding on the ‘Alarm Accept and Reset’ icon (5 secs).
12. When completed, check the ‘Jetty PLC and IHLA Status’ are indicated as being ‘Healthy’ on control room PC.

If there are any faults ensure to advise Terminal Management at once.

Check over paper work, ensuring all information has been obtained and file.

Testing of 'Radar' IHLA's

Tanks 04, 05, 11, 12, 45, 46 & 47 have Endress+Hauser Radar IHLA's fitted, and are set to activate when the floating roofs comes within a predetermined set point. When any one of these alarms activates the shipping docklines and transfer shutdown valves should close, stopping all product flow.

Under controlled conditions, these alarms are required to be tested annually by carrying out a 'Wet Test' to ensure they are functional and operate at their predetermined alarm set point. For all tanks this will mean transferring product into the tank, to actually bring the roof up to the alarm set point, to ensure the system activates.

Therefore to ensure these checks are carried out correctly and without compromising safety the following procedure must be followed, **at no time should it be deviated from unless written permission has been obtained from Terminal Management.**

This operation should be carried out for each tank (04, 05, 11, 12, 45, 46 & 47), **and can only be done in consultation between Terminal Engineer and Operations Manager.**

1. Ensure no shipping or transfer activities are occurring or due
2. Lock out tank from road loading (if applicable)
3. Manually check dip 'test' tank and compare to 'Tank Gauge', ensuring the level in the tank is within acceptable limits (+-3mm)
4. Calculate amount of product that can be transferred to bring tank to maximum/normal fill level.
5. Check line settings and start to transfer product. Monitor transfer as per normal procedure, ensuring flow rates are correct and product is going to correct tank.
6. Following completion of transfer, check amount transferred to receipt tank, to confirm the correct volume has been transferred, and that tank is at maximum/normal fill level.
7. Manually check dip tank again and check against 'tank gauge' to confirm the gauge is within acceptable levels. Also record ITG against IHLA readings.
8. Calculate amount of product it will take to bring tank to IHLA set point (as indicated below). Get these figures checked by another to confirm amounts calculated are correct.
9. Obtain 'key No10' from the 'Over- Ride' box located in the Operations Managers office. This will allow the 'Transfer Pump' trip to be by-passed. Red light on Tank Gauging panel should illuminate.
10. Ensuring you have control of tankside valve to close if required, start to transfer calculated volume into tank. Monitor the volume at all times, ensuring it does not go more that 20mm above IHLA set point.
    NOTE – during this operation tank gauge alarms will activate, the activation of these should be noted and silenced as required.
11. Ensure IHLA activates at set point. Record this level and ensure transfer is stopped immediately.
12. Ensure correct IHLA on 'test' tank has indicated on the control room display PC and that all Klaxons and Beacon activated (Switch room and Jetty).

Trip Over-Ride Risk Assessment – 'TORA'

Introduction

The objective of this procedure is to highlight the potential dangers of overriding SIS functions, to identify those circumstances where this may be permitted and to provide a mechanism for controlling this operation.

The Trip Override Risk Assessment (TORA) described in this procedure is a decision support process which when complete is intended to provide clear guidance on the boundaries in which any authorised person is permitted to apply trip overrides.

Scope

This procedure will be applied to safety related instrumented protection systems or SIS, (i.e. SIL 1-4). However it is recommended that the same procedure be followed for the application of overrides for all categories' or integrity levels of instrumented protection system.

Wherever possible, overrides should not be applied during SIS proof testing. Where it is considered necessary, overrides applied during SIS proof testing should be controlled either by using this procedure or through an equivalent specific risk assessment procedure.

Responsibilities

The responsibility for overrides for whatever reason will be with the Terminal Management. The Terminal Manager or his deputy has the ultimate responsibility for the current status of any overrides.

Terminal Management is responsible for leading the TORA and will seek the assistance of appropriate discipline experts when required.

Basic Principles of Manual Overrides

The need for the override of any system involving safety should be avoided but should the need arise then it should be covered by this procedure.

The application of an override to a safety instrumented system will prevent such system from acting on demand and is likely to increase the risk of serious consequences. The application of an override on a SIL rated system would be considered to generate an abnormal condition and should be minimised.

Before any override is applied it is of utmost importance that the implications of doing so are fully understood and that adequate measures have been taken to reduce the consequential risk of operating without the safety protection. This should be as per individual terminals procedures.

It should be noted that this procedure requires a specific risk assessment be carried out on each override and should be done so by using TORA Form.

Trip Override Risk Assessment (TORA)

A “Trip Override Risk Assessment” (TORA) shall be carried out before the application of ANY SIS override. This will:

- Identify the consequence and risk associated with the failure of the trip to act on demand through the application of that particular override
- Identify the consequence and risk of any spurious trip
- Identify the situation where it may be necessary to apply the override
- Identify any restrictions, control measures or actions that may be taken to reduce the risk to an acceptable level
- Define whether or not it is permissible to apply the override
- Specify whether any timescale needs to be applied to the override
- Specify whether any further actions need to be taken.

Control of overrides

Whilst a TORA determines the circumstances under which an override may be applied, the application of the override shall be controlled through the individual terminals procedures.

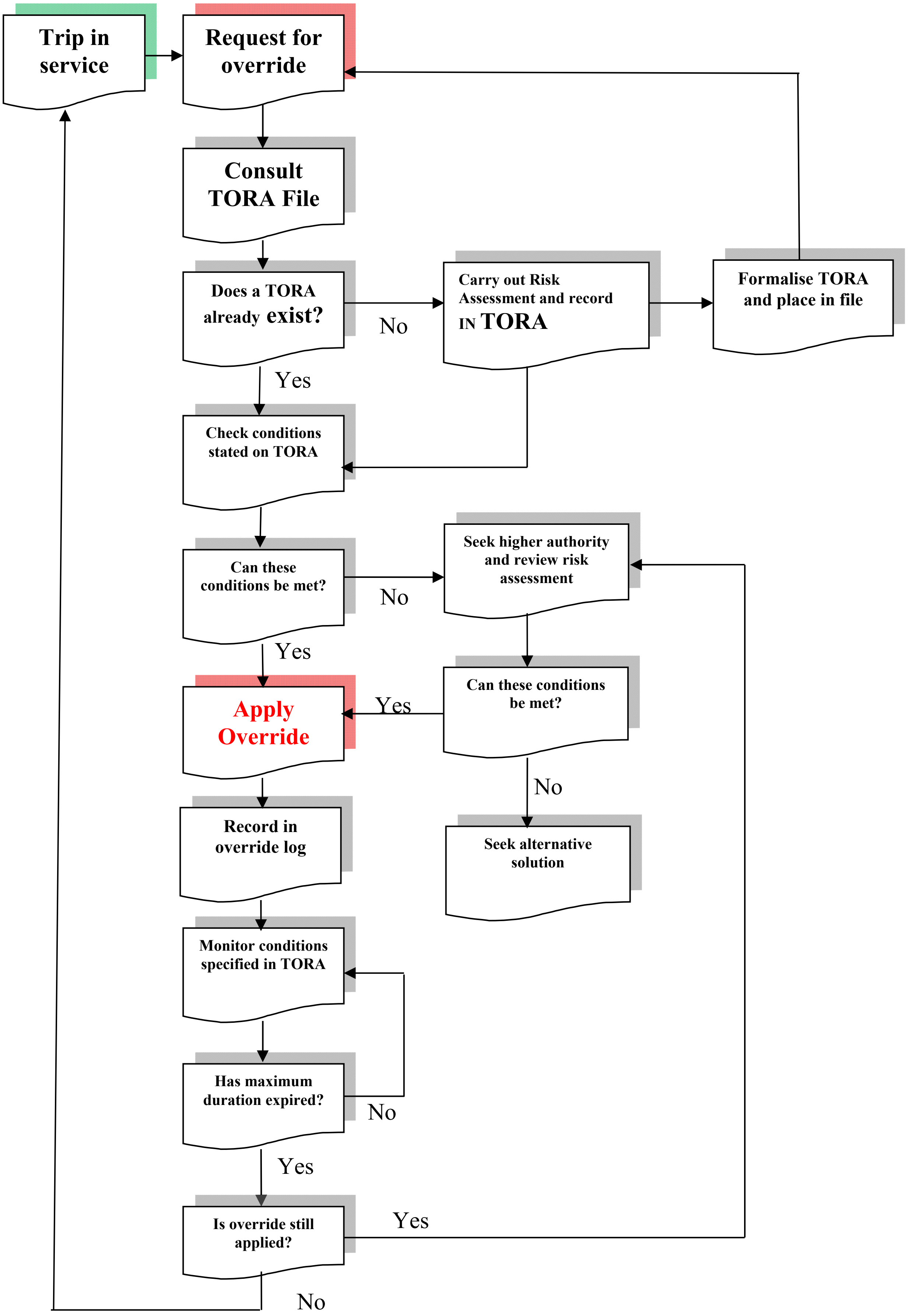
Each terminal shall have a clear Operating Procedure or Instruction specifying the process to be used when applying an override on a critical system. These procedures or instructions should make reference to the TORA.

Any overrides required for testing or maintenance shall be carried out in conjunction with the TORA and any observations should be entered in the appropriate procedure or method statement.

The control of the overrides for maintenance purposes still remains with the Terminal Manager or his deputy who should witness the application and removal of such an override.

Regular audits (using TORA audit check sheet) and reviews of this procedure should be carried out to ensure compliance and improvement of the system.

TORA Flow Chart


Trip in service
Request for override
Consult TORA File
Does a TORA already exist?
No
Carry out Risk Assessment and record IN TORA
Formalise TORA and place in file
Yes
Check conditions stated on TORA
Can these conditions be met?
No
Seek higher authority and review risk assessment
Yes
Apply Override
Yes
Can these conditions be met?
No
Seek alternative solution
Record in override log
Monitor conditions specified in TORA
Has maximum duration expired?
No
Yes
Is override still applied?
Yes
No

TORA No. - _______

Trip Override Risk Assessment (TORA)

Identity of Critical Device: ________________________________

Where is it to be applied: ______________________________________

Risk of Applying Override:

(What are the consequences if this trip fails to act on demand)

What are the consequences of not applying the override:

Reasons for Applying Override:

(Critical Maintenance, Fault, Overfill)

Control Measures and Mitigation:

(What actions should be taken to minimise the risk whilst trip is overridden?)

Maximum Duration of Override:

Less than 1 hour/Up to 4 hours/Up to 8 hours/Up to 12 hours/Up to 24 hours/Maximum 96 hours*

***Delete where applicable – (How long can override remain applied?)**

Observations:

(Detail any additional monitoring or precautions required)

Assessment carried out by:

Date:

Time

Signature

Authorisation

	Signature	Date	Time
Operations Manager/Terminal Manager			

Trip Override Log -

Override No.	Key/Tag/ Lock Out No.	Description	Reason for Override	TORA No.	Applied by	Date	Time	Restored by	Date	Time
111										
112										
113										
114										
115										
116										
117										
118										
119										
120										

Trip Override - Shift Handover Acceptance Sheet

By signing below all signatories confirm knowledge and acceptance of the outstanding overrides listed on the ‘Trip Over-Ride Log’. All overrides must be acknowledged and signed off at each shift handover.

Override No.	Reason for override explained and understood?	TORA No.	Signature oncoming shift	Signature outgoing shift	Date	Time	Comments
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						
	Yes/No						

TORA Audit Check Sheet

Check	Details	Pass/Fail	Comments
Current Override Status	Check for active overrides. Are they clearly stated and are the Terminal Controllers aware of their existence.		
TORA Status	Check that the adequate Trip Override Risk Assessments exist for every active override identified above. Is it clear which TORA has been used and are they available to Terminal Controllers.		
Override Conditions	Check that the specific circumstances under which each override was applied are covered by the TORA risk assessment.		
Override Control Measures	Check that the control measures specified in the TORA for each active override have been applied.		
Trip Override Log and Activity Level	Check that all active overrides have been recorded in the Trip Override Log and if this is acknowledge during each shift handover. Note the number of overrides applied and removed during the audit period.		

Audit carried out by: ________________________________ Date: __________________________

Signature: ____ Time: __________________________

13. Check that all ‘Shutdown’ valves have closed and are indicating this on the control room display screen. Manually ‘check dip’ test tank and compare level to Auto Tank Gauge.
14. Ensure all dips and checks are recorded on ‘Testing of IHLA – Radar’ report sheet.
15. Lower product in tank, to a level below maximum fill level. Reset system and ensure all valves open and that IHLA activated is displayed as ‘Healthy’ on control room PC.
16. To test another tank, return to step 01.
17. When all tests have been completed, remove ‘By-Pass Key No.10’ from tank gauging panel, ensuring red light extinguishes and lock away.

If there are any faults ensure to advise Terminal Management at once.

Check over paper work, ensuring all information has been obtained and file.

Dockline Shutdown System

Dockline 'shutdown' valves are fitted in the terminal and will close if an 'Independent High Level Alarm' (IHLA) activates or if there is an electrical/mechanical failure of the equipment or services.

The time taken to close these valves is approx **90 seconds (or 1min, 30 secs),** which has been calculated to ensure there will be no 'Hydraulic Shock' on the docklines caused by the closure of the valves.

A 'Jetty Warning' system has been installed to warn when the system activates and that the valves are closing, therefore I would advise that your vessel takes the appropriate action to ensure immediate suspension of discharge operations.

The activation of the system will consist of a warning Klaxon, which will sound continuously and a flashing beacon. All of which is located beside the jetty hut and is clearly identified.

Therefore, I would appreciate if you would sign below to ensure you have read and understand the above information and that you will explain this to your crew, to ensure they are aware of what action to take should the system activate.

______________________________	______________________________
Signed for on behalf of discharging vessel	Signed for on behalf of NuStar

Date: ______________________________

Thanks and Regards

Andrew Bann

Andrew Bann
Terminal Manager

Testing of IHLA's - 'Liquiphant' and ESV's

Tank	Main Klaxons Activated? Yes/No	Dockline Valves (1,2&3) Closure? Yes/No	Transfer Valves Kero/Gas Oil /Diesel/Gasoline) Closure? Yes/No	Correct Tank Indicated in Control Room Yes/No?	Jetty Alarm System Operational Yes/No?	Date
01						
02						
03						
06						
07						
08						
09						
10						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
26						
27						
28						
29						
30						
31						
32						
33						
34						
38						
39						
40						
41						
48						
49						
50						

Weekly check of IHLA System and to ensure all ESV's operate. When checks are completed, system to be reset.Tests can only be done when 'NO' product movement is occurring. Report any faults immediately to Terminal Management.

Testing of IHLA's - 'Liquiphant' and ESV's

Test carried out and system reset by?

Weekly check of IHLA System and to ensure all ESV's operate. When checks are completed, system to be reset.Tests can only be done when 'NO' product movement is occurring. Report any faults immediately to Terminal Management.

Maintenence of Independant High Level Alarm System

Item	Tank No.	Part No.	Serial No.	Details of Work Carried Out	Did Device/Replaced Unit need reset?	Maintenence Carried Out By	System Tested	Date

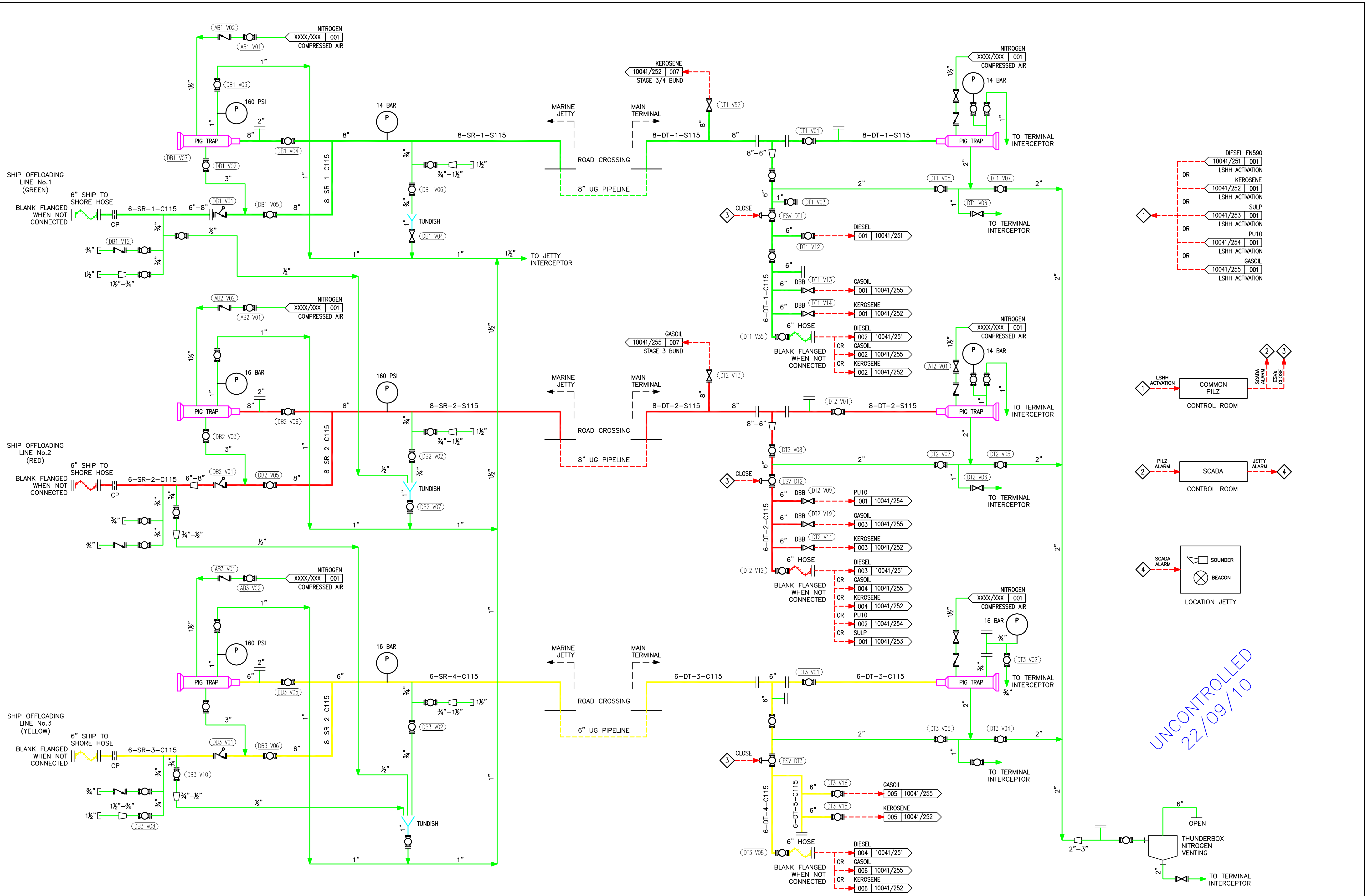
Appendix 3

P & I Drawings

Not included at this revision

Appendix 3

P & I Drawings



UNCONTROLLED
22/09/10

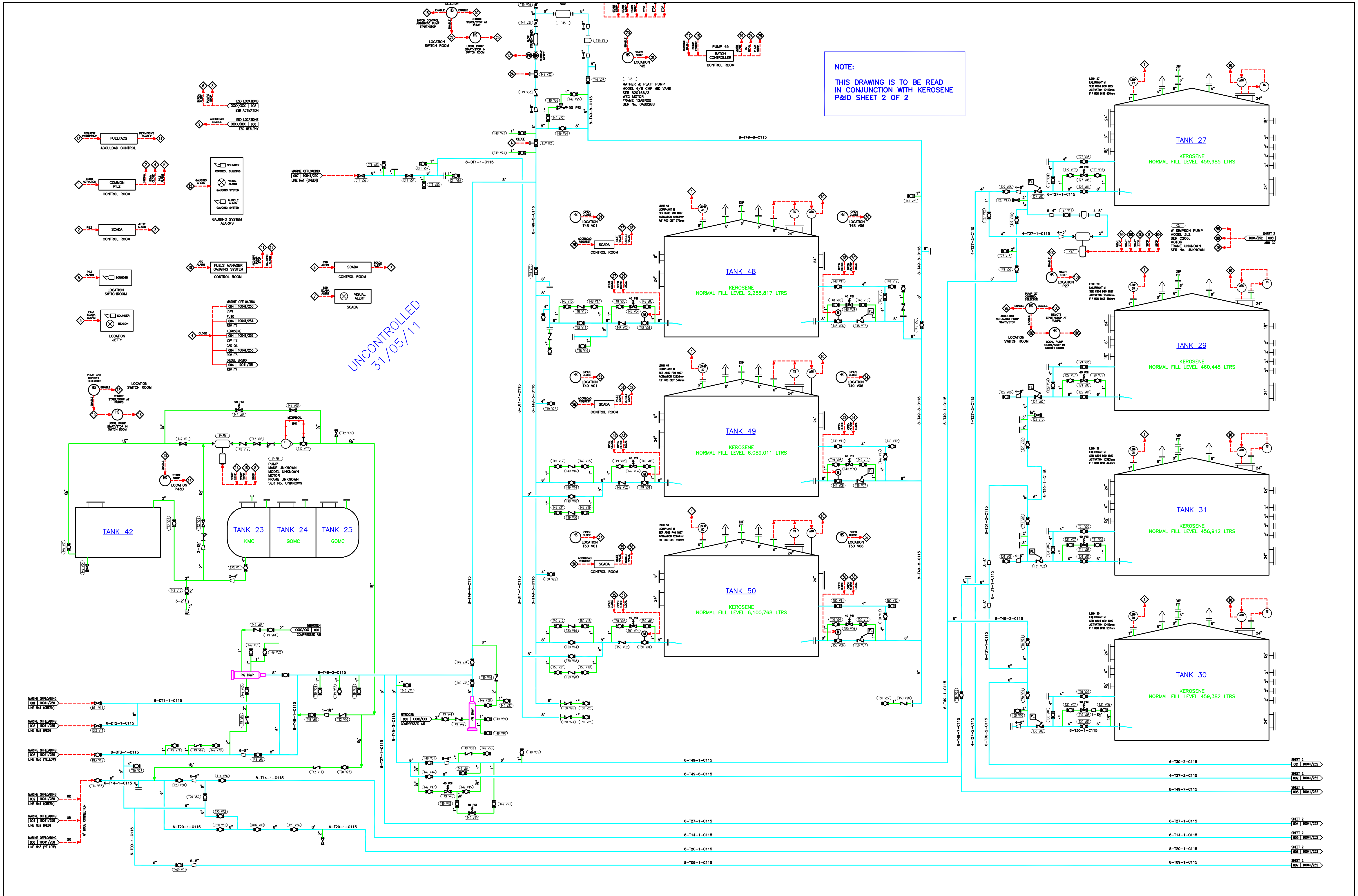
	DRAWN	DATE	DESCRIPTION
A	IPH	22/09/10	FIRST ISSUE BY EPM SOLUTIONS LTD

MODIFICATIONS

DRAWN	DATE	DESCRIPTION

DRAWN BY	IPH	16/08/10	TITLE	MARINE OFFLOADING PIPING AND INSTRUMENTATION DIAGRAM
CHECKED	GK	16/08/10		
APPROVED	NM	22/09/10		
TRACED	***	***	SCALE NTS	INSTALL'N BELFAST PROJECT No. 10041
1st ISSUED	EPM	22/09/10	NUSTAR TERMINALS LTD	DRAWING No. 10041/250 ISSUE A
FILENAME	10041-250	DATE		

NUSTAR TERMINALS Ltd
Chatsworth House
29 Broadway
Maidenhead
Berkshire SL6 1LY



NOTE:

THIS DRAWING IS TO BE READ IN CONJUNCTION WITH KEROSENE P&ID SHEET 2 OF 2

UNCONTROLLED
31/05/11

MODIFICATIONS		DRAWN	DATE	DESCRIPTION
	A	IPH	22/09/10	FIRST ISSUE BY EPM SOLUTIONS LTD
	B	NM	31/05/11	IHLAs and transfer ESVs added

MODIFICATIONS		DRAWN	DATE	DESCRIPTION

MODIFICATIONS		DRAWN	DATE	DESCRIPTION

DRAWN BY	NM	31/05/11
CHECKED		
APPROVED		
TRACED	***	***
1st ISSUED	EPM	22/09/10
FILENAME	10041-252	DATE

TITLE

KEROSENE
PIPING AND INSTRUMENTATION
DIAGRAM - SHEET 1 OF 2

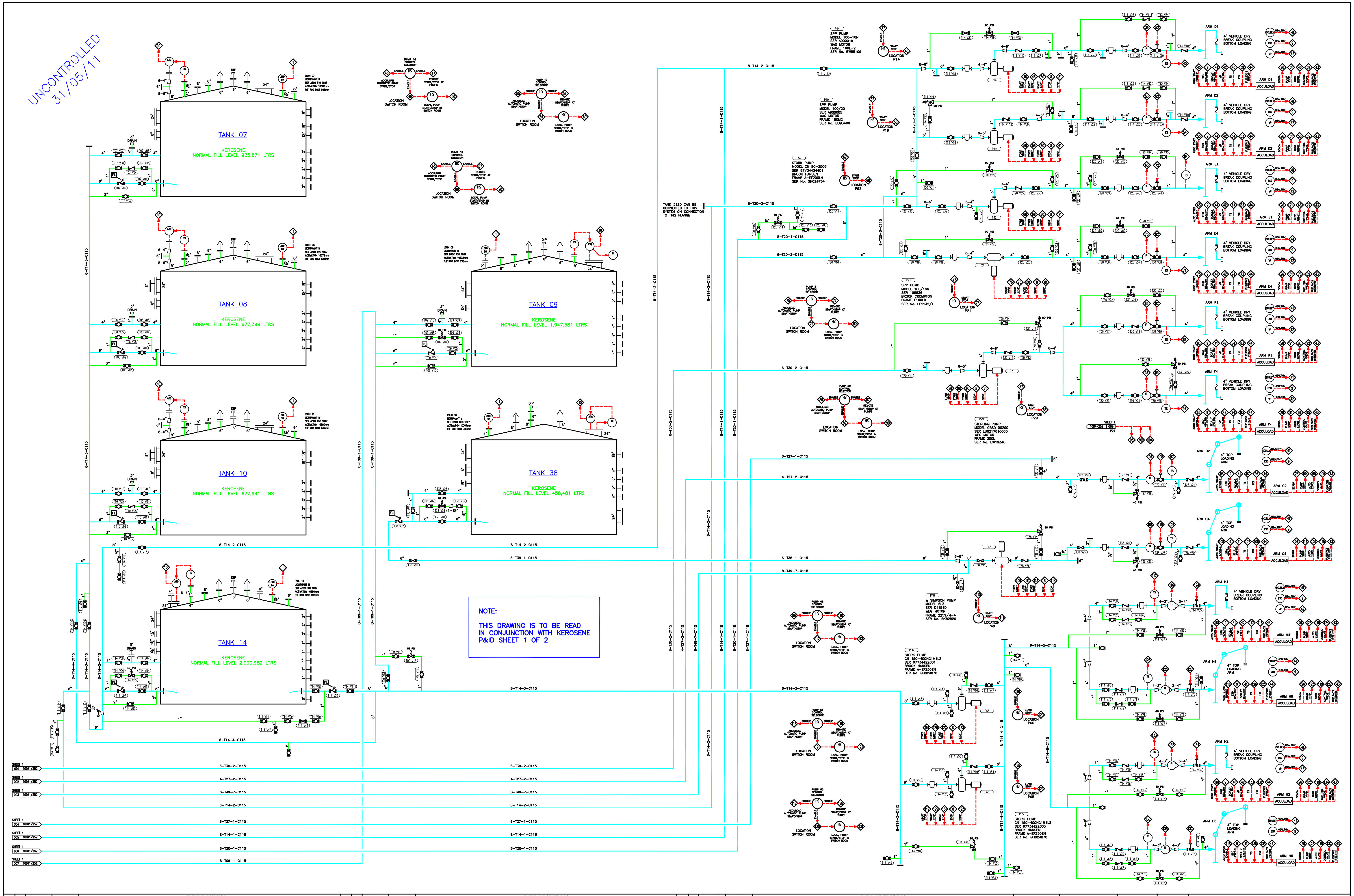
SCALE NTS | INSTALL'N BELFAST | PROJECT No. 10041

NUSTAR TERMINALS LTD

NUSTAR TERMINALS Ltd
Chatsworth House
29 Broadway
Maidenhead
Berkshire SL6 1LY

DRAWING No. 10041/252 | ISSUE B

UNCONTROLLED
31/05/11



NOTE:

THIS DRAWING IS TO BE READ IN CONJUNCTION WITH KEROSENE P&ID SHEET 1 OF 2

MODIFICATIONS		DRAWN	DATE	DESCRIPTION
	A	IPH	22/09/10	FIRST ISSUE BY EPM SOLUTIONS LTD
	B	NM	31/05/11	IHLAs and transfer ESVs added

MODIFICATIONS		DRAWN	DATE	DESCRIPTION

MODIFICATIONS		DRAWN	DATE	DESCRIPTION

DRAWN BY	NM	31/05/11	TITLE	KEROSENE PIPING AND INSTRUMENTATION DIAGRAM - SHEET 2 OF 2			
CHECKED							
APPROVED							
TRACED	***	***	SCALE	NTS	INSTALL'N	BELFAST	PROJECT No. 10041
1st ISSUED	EPM	22/09/10	NUSTAR TERMINALS LTD	NUSTAR TERMINALS Ltd Chatsworth House 29 Broadway Maidenhead Berkshire SL6 1LY		DRAWING No. 10041/252	ISSUE B
FILENAME	10041-252	DATE					

Appendix 4

LOPA Calculation

Frequencies are in events per year, other numerical values are probabilities.

1	2	3	4	5	6	7	8	9	10	11
	Select severity cell below and choose a severity level from the drop down list		Enter 1 if none or if constantly present. Note: enter description of enabling event in comments box	Enter nothing if no IE	Enter 1 if no credit claimed. BPCS includes all equipment and people required to perform basic process control. This may vary with each scenario	Enter 1 if CM not relevant or always present for associated IE. CM values are probability of success therefore care is needed in how CM is worded				
Scenario Description	***Select Severity Level (company specific) from pull down lis below***	***Initiating Event identifier***	***Enabling Events (e.g. fill operations per year or % of yr present)***	***Initiation Event Frequency (freq / yr)***	***BPCS dangerous failure rate per hour***	***CM1 probability of ignition***	***CM2 proability of explosion (instead of flash fire)***	***CM3 probability of calm weather***	***CM4 proability operator is in hazard zone***	***CM5 proability of fatality***
Gasoline bulk storage tank overfill leading to vapour cloud explosion.	**(S) Serious**	***IE1***								
		IE2								
		IE3								
		IE4								
		IE5								
Company Risk Target	**1.00E-06**									
Inputs										

3	13	14	15	16	17	18	19	20
	Protection layers (PL**s**) and Mitigation layers (MLs) PFD Enter 1 if no credit is claimed for IPL or IML relevant to each IE. **Figures represent PFD**			IE frequency /yr multiplied by the enabling event and any conditional modifiers ((5*(4*7*8*9*10*11))	LOPA ratio Risk target frequency divided by residual risk frequency	User proposed SIF value must be entered as a PFD Enter 1 if non chosen	**Residual risk without proposed SIL .** This columns equates to the scenario frequency multiplied by the existing protection layers (16*(4*5*6*13*14*15))	**Residual risk including the user proposed SIL .** This columns equates to (18*19)
Initiating Event identifier	***IPL 1 Independent Alarm***	***IPL 2 e.g. existing shutdown system***	***IMLs e.g. Overfill detection fails***	***Frequency of unmitigated consequence***	***Level of risk reduction required to meet stated risk target***	***User Proposed SIF Integrity Level (PFD)***	***Intermediate Event frequency (events/yr)***	***Frequency of mitigated consequence***
IE1				0.00E+00	**#DIV/0!**	**1.00E+00**	0.00E+00	0.00E+00
IE2				0.00E+00			0.00E+00	0.00E+00
IE3				0.00E+00			0.00E+00	0.00E+00
IE4				0.00E+00		**CHOSEN PFD NOT IN SIL RANGE**	0.00E+00	0.00E+00
IE5				0.00E+00	**#DIV/0!**		0.00E+00	0.00E+00
				0.00E+00			**0.00E+00**	**0.00E+00**
				Outputs				

Notes

1. If more than 5 Conditional Modifiers are present, combine them for the purpose of calculation. State how the CM's were combined in the "Comments" below.
2. If more than 3 Independent Layers of Protection/mitigation (IPL/IML) are present, combine them for the purpose of calculation. State how the IPL's and IML's were combined in the "Comments" below.

The suggested risk targets below may be considered conservative but may be used; alternativly the company can enter their own risk targets.

Severity Level	**Safety Consequence**	**Maximum Frequency of Mitigated Event Likelihood per year**
(M) Minor	Consequence limited to serious injury.	**1.00E-04**
(S) Serious	Impact Event could cause a fatality.	**1.00E-06**
(E) Extensive	Impact Event includes up to 50 fatalities (greater than 50 is intolerable)	**1.00E-08**
(U) User Defined	Enter user target frequency in the next cell and select U from drop down menu above	**1.00E-07**

	Low demand SIL ranges		**High demand SIL ranges**	
Target SIL	**Max**	**Min**	**Max**	**Min**
SIL1	1.00E-01	1.00E-02	1.00E-05	1.00E-06
SIL2	1.00E-02	1.00E-03	1.00E-06	1.00E-07
SIL3	1.00E-03	1.00E-04	1.00E-07	1.00E-08
SIL4	1.00E-04	1.00E-05	1.00E-08	1.00E-09
Select SIL Demand Rate (high/low) from cell below				
Low				

Output Summary		**Column**
Frequency of unmitigated consequence	**0.00E+00**	16 (sum)
Frequency of intermediate event	**0.00E+00**	19 (sum)
Frequency of mitigated consequence	**0.00E+00**	20 (sum)
PFD Target (Gap to Fill)	**#DIV/0!**	17
Required SIF SIL	#DIV/0!	17

Comments

Company Name: ***Name of LOPA Site***
LOPA Overview: ***Why the LOPA has to be verified.***
Date:
Assessor:

Combiner tool.			
This is **not** part of the LOPA calculation. It is a **tool to help** combine CM OR IPL values.			
CM Combiner		**IPL Combiner**	
CM1	1	IPL1	1.00E+00
CM2	1	IPL2	1.00E+00
CM3	1	IPL3	1.00E+00
CM4	1	IPL4	1.00E+00
CM5	1	IPL5	1.00E+00
Product CM	**1.00E+00**	**Product IPL**	**1.00E+00**
Set unused CM to 1		Set unused IPL to 1	

$$\textbf{Target PFD (Gap to fill)} = \frac{\textbf{Risk Tolerance Criterion}}{\textbf{Frequency of Mitigated Consequence}}$$

Frequencies are in events per year, other numerical values are probabilities.

1	2	3	4	5	6	7	8	9	10	11	13	14	15	16	17	18	19	20
	Select severity cell below and choose a severity level from the drop down list		Enter 1 if none or if constantly present. Note: enter description of enabling event in comments box	Enter nothing if no IE	Enter 1 if no credit claimed. BPCS includes all equipment and people required to perform basic process control. This may vary with each scenario	Enter 1 if CM not relevant or always present for associated IE. CM values are probability of success therefore care is needed in how CM is worded					Protection layers (PL**s**) and Mitigation layers (MLs) PFD Enter 1 if no credit is claimed for IPL or IML relevant to each IE**.** **Figures represent PFD**			IE frequency /yr multiplied by the enabling event and any conditional modifiers ((5*(4*7*8*9*10*11))	LOPA ratio Risk target frequency divided by residual risk frequency	User proposed SIF value must be entered as a PFD Enter 1 if non chosen	**Residual risk without proposed SIL**. This columns equates to the scenario frequency multiplied by the existing protection layers (16*(6*13*14*15))	**Residual risk including the user proposed SIL**. This columns equates to (18*19)
Scenario Description for SCENARIO A	***Select Severity Level (company specific) from pull down list below***	***Initiating Event identifier***	***Enabling Events (e.g. fill operations per year or % of yr present)***	***Initiation Event Frequency (freq / yr)***	***BPCS dangerous failure rate per hour***	***CM1 probability of ignition***	***CM2 probability of person on site raising alarm***	***CM3 probability of calm weather***	***CM4 probability operator is in hazard zone***	***CM5 probability of fatality***	***IPL 1 ATG Alarm***	***IPL 2 e.g. existing shutdown system***	***IMLs e.g. Overfill detection fails***	***Frequency of unmitigated consequence***	***Level of risk reduction required to meet stated risk target***	***User Proposed SIF Integrity Level (PFD)***	***Intermediate Event frequency (events/yr)***	***Frequency of mitigated consequence***
Gasoline bulk storage tank overfill leading to vapour cloud explosion.	**(S) Serious**	***IE1***	1	1	1.00E-05	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E+00	**8.00E-02**	**7.02E+00**	**7.74E-03**	**8.00E-08**	**6.19E-10**
		IE2	1	1	1.00E-03	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E+00	**8.00E-02**			**8.00E-06**	**6.19E-08**
		IE3	1	20	1.00E-03	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E+00	**1.60E+00**			**1.60E-04**	**1.24E-06**
		IE4	1	0.05	1.00E-02	0.8	1	0.1	1	1	1.00E-01	1.00E+00	1.00E+00	**4.00E-03**		**SIL2**	**4.00E-06**	**3.10E-08**
		IE5	1	0.15	1.00E-03	0.8	1	0.1	1	1	1.00E+00	1.00E+00	1.00E+00	**1.20E-02**	**NO SIL REQUIRED**		**1.20E-05**	**9.29E-08**
Company Risk Target	**1.00E-05**													**1.78E+00**			**1.84E-04**	**1.42E-06**
Inputs														**Outputs**				

Notes

1. If more than 5 Conditional Modifiers are present, combine them for the purpose of calculation. State how the CM's were combined in the "Comments" below.
2. If more than 3 Independent Layers of Protection/mitigation (IPL/IML) are present, combine them for the purpose of calculation. State how the IPL's and IML's were combined in the "Comments" below.

The suggested risk targets below may be considered conservative but may be used; alternatively the company can enter their own risk targets.

Severity Level	**Safety Consequence**	**Maximum Frequency of Mitigated Event Likelihood per year**
(M) Minor	Consequence limited to serious injury.	**1.00E-04**
(S) Serious	Impact Event could cause a fatality.	**1.00E-06**
(E) Extensive	Impact Event includes up to 50 fatalities (greater than 50 is intolerable)	**1.00E-08**
(U) User Defined	Enter user target frequency in the next cell and select U from drop down menu above	**1.00E-07**

	Low demand SIL ranges		**High demand SIL ranges**	
Target SIL	**Max**	**Min**	**Max**	**Min**
SIL1	1.00E-01	1.00E-02	1.00E-05	1.00E-06
SIL2	1.00E-02	1.00E-03	1.00E-06	1.00E-07
SIL3	1.00E-03	1.00E-04	1.00E-07	1.00E-08
SIL4	1.00E-04	1.00E-05	1.00E-08	1.00E-09
Select SIL Demand Rate (high/low) from cell below				
Low				

Output Summary		**Column**
Frequency of unmitigated consequence	**1.78E+00**	16 (sum)
Frequency of intermediate event	**1.84E-04**	19 (sum)
Frequency of mitigated consequence	**1.42E-06**	20 (sum)
PFD Target (Gap to Fill)	**7.02E+00**	17
Required SIF SIL	NO SIL REQUIRED	17

Comments

(U) User Defined
(E) Extensive
(S) Serious
(M) Minor
Validation list for severity level

Low
High

Validation list for Demand rate value

Combiner tool.

This is **not** part of the LOPA calculation. It is a **tool to help** combine CM OR IPL values.

CM Combiner		**IPL Combiner**	
CM1	1	IPL1	1.00E+00
CM2	1	IPL2	1.00E+00
CM3	1	IPL3	1.00E+00
CM4	1	IPL4	1.00E+00
CM5	1	IPL5	1.00E+00
Product CM	**1.00E+00**	**Product IPL**	**1.00E+00**
Set unused CM to 1		Set unused IPL to 1	

Checking Stats

Product of CM for IE1	0.08
Product of CM for IE2	0.08
Product of CM for IE3	0.08
Product of CM for IE4	0.08
Product of CM for IE5	0.08

Total PFD for all PL		**Incident Frequency**
Product for IE1	1.00E-01	1.00E-01
Product for IE2	1.00E-01	1.00E-01
Product for IE3	1.00E-01	2.00E+00
Product for IE4	1.00E-01	5.00E-03
Product for IE5	1.00E+00	1.50E-01
		2.36E+00 per year

$$\textbf{Target PFD (Gap to fill)} = \frac{\textbf{Risk Tolerance Criterion}}{\textbf{Frequency of Mitigated Consequence}}$$

Layers of Protection Analysis (LOPA) Report

Gasoline tank overfill

NuStar Belfast (Version 2 September 2011)

A team was formed to undertake the LOPA study and comprised:

George Reeves, General Manager Engineering
Yvette Davis, Senior Manager HSE
Andrew Bann, Terminal Manager
Paul McGreevy, Operations Manager
Neil Mearns, Terminal Engineer
Charles Stuart, Process Safety and Environment Coordinator
D O Jones, Risk Assessor (BCS Chester Ltd)

1. Summary

The site receives petroleum products from ships which berth at Oil Berth No.01 berthed in Musgrave Channel, within Belfast Lough and stores them in dedicated bulk storage tanks in the three Tank Farms. All the dangerous substances are petroleum products. The products are pumped to road tankers using proprietary loading bays in three locations.

The ships discharge using their own pumps and connect to shore using flexible hoses supplied by NuStar.

The terminal is housed within a single security fence and is divided into three storage areas.

The site occupies approximately 5.3 hectares and employs 10 staff.

2. Terminal Overview

2.1 Terminal Description

Storage tanks range in size from 492m^3 to 6,072m^3 and are of fixed roof construction, some of which are fitted with internal floating blankets. Three tanks with external floating roof construction.

All tanks are constructed to British Standards 2654 (BSEN14015-2004) or API650 and fabricated from Mild Steel and vary in age from 10 to 40 years).

All tanks are calibrated by external contractors to accurately establish product volumes this is done either by Automatic Tank Gauging (ATG) or by manual dipping.

Non-return valves are fitted at tank-side locations in both shipping and road loading lines.

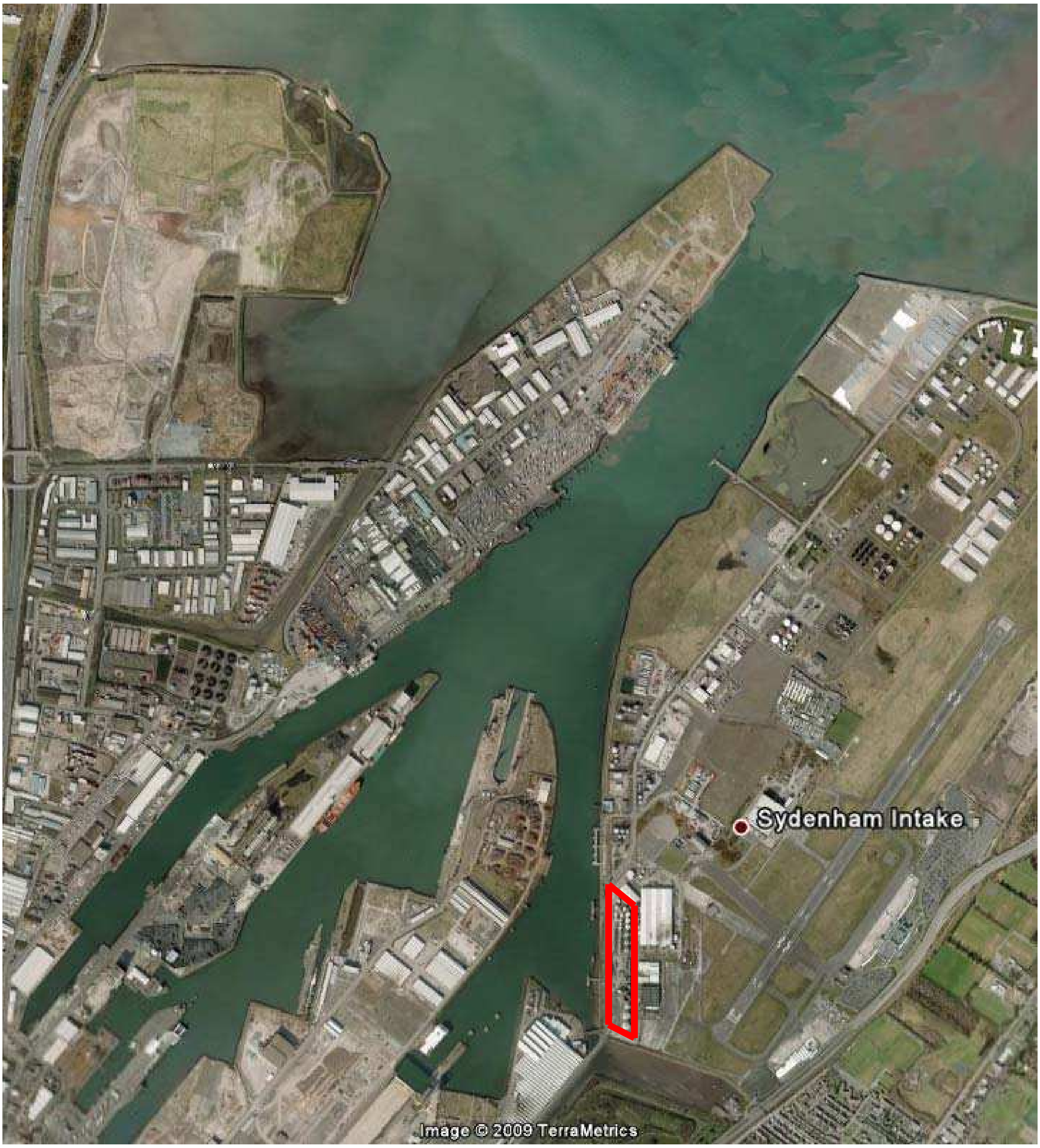
Bunding is constructed to at least contain a 110% spill of the largest tank.

The three pipelines used for shipping purposes (one Mild Steel and two Stainless Steel) are maintained in an empty condition when not in use and are “pigged” using nitrogen gas. Transfer and delivery lines in use are maintained in a full condition, typically from tank to road loading rack.

2.2 Location

The site is a flat area alongside Musgrave Channel (southwest of the site) and occupies approximately 5.3 hectares west of George Best City airport in Belfast.

Figure 1: Establishment Location



2.3 Normal operating procedures

Prior to import

The site has formal written procedures that include product imports from ship. All procedures clearly define site personnel actions during normal import conditions. These procedures have been reviewed and revised by the Senior Manager HSE, along with input from those carrying out the activities to ensure the procedures are correct, complete and unambiguous and that errors and recovery options have been considered.

The imported volumes, the exported volumes and the tank contents are reconciled by the Terminal staff to identify any losses and gains. These are compared to acceptable tolerance settings and this process is used to highlight failures of the Automatic Tank Gauging (ATG). Prior to the ship discharge, the independent cargo surveyor dips the receipt tank.

The product owner (client) determines the number of receipts from ship & discharges to road vehicle for each tank. Prior to a ship arriving to discharge gasoline, the client (product owner) provides a 'pre-authorisation form' that is a system agreeing the cargo details (including quantity) and the tanks designated for its receipt. The NuStar Terminal Controller, and also Terminal Management use this data to produce a 'pre discharge plan' for the ship that can identify some types of gauge failure and any errors in the ullage calculation.

Once the ship has berthed there is a recorded checklist agreed between the ship's crew and the terminal. This includes confirmation that the correct cargo is to be discharged to the correct tank or tanks.

The Cargo Surveyor is an independent third party, appointed by the owner of the cargo, who confirms the cargo identity and quantity to be discharged and compares it to the ullage in the receiving tank or tanks. The physical dips of the ship and receiving tanks are taken as part of this confirmation.

Importing

Once the import has commenced, there is a formal written procedure whereby the storage tank level is recorded every hour (taken from the ATG) and the quantity received compared to the quantity discharged from the ship (based on ship's cargo tank gauging). This is to ensure that the rate of rise of the tank level agrees with the agreed ship discharge rate, which will highlight both whether the import is being received into the correct tank and also highlight any errors on the initial ullage calculation. This procedure would also detect failure or gross errors in the ATG reading. Site management (post discharge), subsequently checks these import control sheets and non-conformities in completing these sheets are recorded and submitted to senior management as part of the established 'Impact System' that records non-conformities and is an audited system. The Process Safety Performance Indicators are based on this system.

All the relevant data for ship discharges are recorded within an audited 'shipping file'. This forms part of the QA system and non-conformances recorded through the 'Impact System'.

The ATG readings are compared to the book stock level at regular times during the month and at month end and any discrepancies rectified.

During discharge the storage tank level is recorded every hour and the quantity received compared to the quantity discharged from the ship (based on ship's cargo tank gauging).

The storage tank ATG has a high-level alarm (set at normal fill level) and a high high-level alarm. There is also an independent high-level alarm that trips the ESV on the ship's discharge line, designed to SIL 2 standard.

The site also has clear written procedures that define site personnel actions in the event of an abnormal situation. All onsite personnel are empowered and instructed to immediately stop the import. In the event that an import needs to be stopped then site personnel are able to undertake a range of different options (such as manually closing valves or instructing the ship to stop pumping – also, Operators can close the tank side ROSOV; however they cannot activate the ESV system). The additional time to carry out these actions has been taken into account when defining the tank fill levels. All procedures are part of the QA system and audited by a quality systems specialist. In addition there is an annual SHE audit of the procedures and legislative compliance by the SHE department.

3. Potential Consequences and Target Frequencies

There are three key consequences that can be considered for a gasoline tank overfill:

- Vapour Cloud Explosion (VCE) followed by a pool fire
- Flash Fire followed by a pool fire
- Unignited Release

It has been assumed that the worse case consequences will be associated with the Vapour Cloud Explosion, and this is the base case for this assessment. However the other consequences have been considered separately.

Flow rates, duration of overfill etc. could be similar to that seen at Buncefield. There are no features of site topography that can be relied upon to prevent the formation of a large vapour cloud. Therefore the zones identified within the PSLG report have been adopted as conservative assumptions and the population with these zones are shown below:

Table 1: Populations

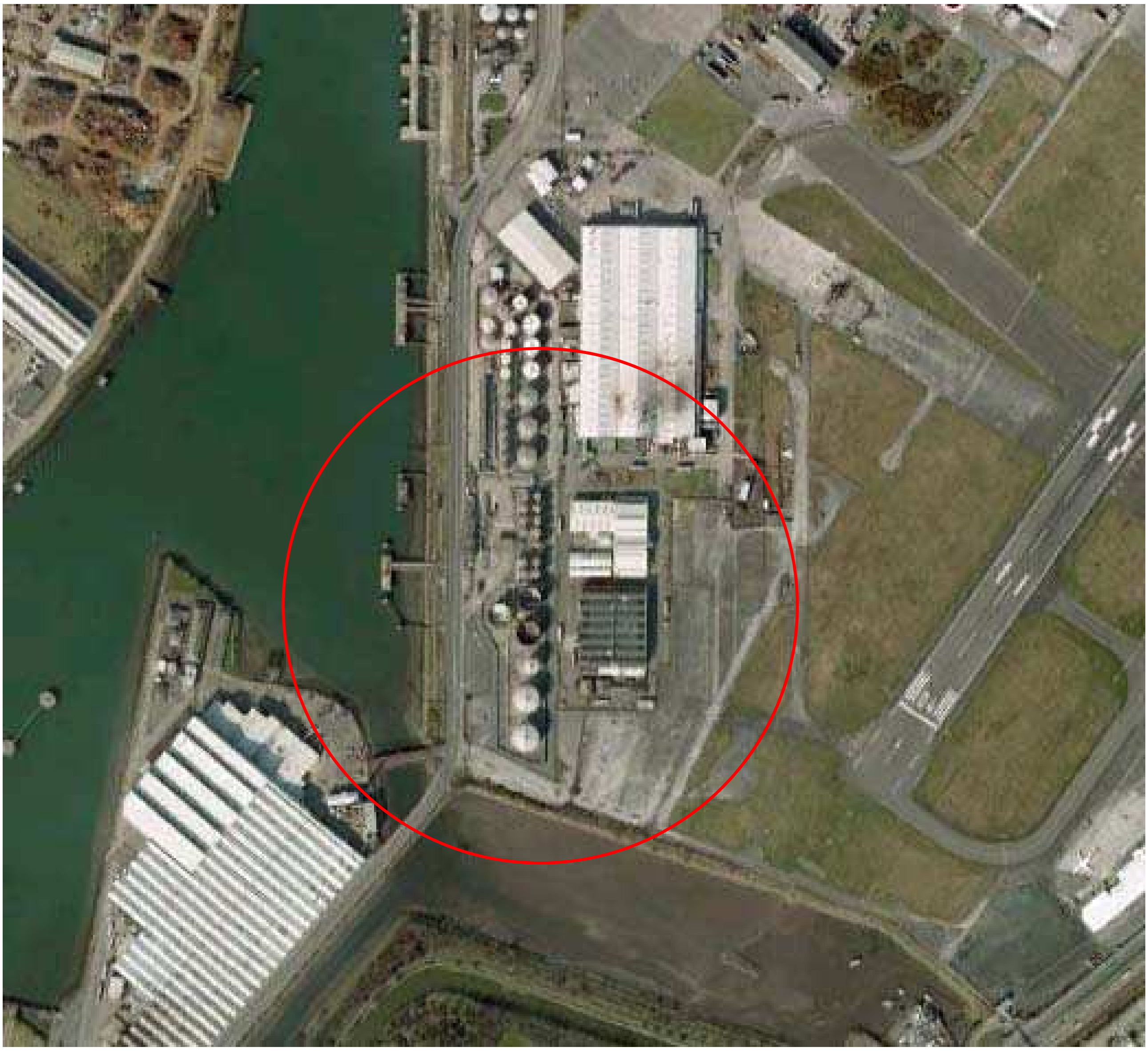
Time of day	Estimated number of fatalities

Day time within 250m	On-site = 10 NuStar
	Off-site = 10 Bombardier Aerospace)
	Total = 20

Night time within 250m	On-site = 5
	Off-site = 10
	Total = 15

Figure 2 below shows the 250m radius from Tanks 5045 & 5046 that contain gasoline.

Figure 2: 250m Radius from Gasoline tanks



Ship imports occur during both the day and night. In line with the PSLG guidance, this LOPA has therefore been based on both nightime and daytime occupancies for weather conditions suitable for a VCE. A simple uncertainty/sensitivity analysis was also performed (see section 9) as well as an estimate of Individual risk (section 10).

There is potential for escalation of a fire to adjacent bunds but the only toxic material is gasoline and no significant toxic plume is created by their release (see COMAH Safety Report).

With regard to environmental consequences, the site has concrete bund walls and as such a VCE is assumed to significantly damage the bunds. Therefore it is credible for there to be pathways for product, foam and firewater to reach the soil and groundwater and, if this were to occur, then there could be major off-site pollution of the groundwater and Musgrave Channel.

Based on the PSLG final report, the following target frequencies have therefore been used:

Table 2: Target Frequencies

Scenario	Consequences	Target likelihood
Vapour Cloud Explosion and subsequent bund pool fire	**Safety** Based on 100% fatality within 250m plus a low risk of further fatalities up to 400m. Estimations based on 17 daytime fatalities.	1×10^{-5} Tolerable if ALARP for scenario
	Environmental Major off-site pollution of groundwater and/or watercourse by product / foam / fire water from subsequent bund fires.	1×10^{-5} Acceptable for establishment

Safety

Based on Table 8 of the PSLG final report for 11-50 fatalities then 'tolerable if ALARP' ranges from 1×10^{-4} y^{-1} to 1×10^{-7} y^{-1} and so less than 1×10^{-5} y^{-1} was chosen as the target frequency for the VCE.

Environmental

The COMAH safety report estimates the effects of a release of hydrocarbons or firewater at the establishment as having limited effects at the site that most closely resemble 'Category 3, Significant' from Table 10 of the PSLG final report. The relevant described is "Severe and sustained nuisance e.g. strong offensive odours or noise disturbance; major breach of permitted emissions limits with possibility of prosecution; numerous public complaints". This 'acceptable' risk criterion from Table 9 of the PSLG final report is 1×10^{-4} y^{-1} for the establishment.

The VCE scenario criterion was taken as 1×10^{-5} y^{-1} to conservatively allow for the environmental risk from other Major Accident Hazards detailed in the Safety Report.

4. Initiating Events

4.1 Introduction

The FMEA approach used for hazard identification in the COMAH Safety Report identified initiating events, including human error and equipment failure that could lead to a tank overfilling.

Each was then considered by the LOPA team to see if they present credible mechanisms by which a gasoline tank at the establishment could be overfilled from imports.

Table 3: Initiating Events

Initiating Event	IE
Initiating event 1 is a ship discharge arranged when there is insufficient ullage in the designated receiving tank (Human Error)	IE1
Ship arrives with sufficient ullage available in designated tank but cargo greater than the agreed quantity because ship will subsequently discharge at another terminal (Human Error)	IE2
Ship arrives to discharge into two receiving tanks & the switch between tanks fails, overfilling the first tank (Human Error)	IE3
Ship discharge progresses normally but load transferred into wrong tank. Valves are correctly set to the tank but when instructed, opens the wrong last valve & allows the load into the wrong tank (Human Error)	IE4
ATG fails to danger (Equipment failure)	IE5

4.2 Data and assumptions

In order to calculate the likelihood of each of the initiating events the following site data was used:

Table 4: Site Data

Data / Assumptions	Values
Total number of ship receipts per year for gasoline	100 per year
Number of ship receipts per year for gasoline requiring a split discharge to more than one tank	20 per year
Average time ship discharge time	10-15 hours

4.3 Initiating Event Calculations

Table 5: IE1

Initiating Event 1 is a ship discharge arranged when there is insufficient ullage in the designated receiving tank				
Number of ship discharges per year	**Probability of failure for initial calculation**	**Probability of failure for start checks**	**Probability of failure for not detecting errors on hourly ullage cross-checks**	**Probability errors would lead to filling above maximum working level**
A ship discharges gasoline 100 events per year Initiating event 1 is a ship discharge arranged when there is insufficient ullage in the designated receiving tanks. This does occur (e.g. caused by delays in road loading) and is part of the normal procedures for managing ship discharges. Ship rarely berth with insufficient ullage in the tank say 1 time per year	Cargo Surveyor appointed by cargo owner fails to check cargo. This is a trained professional who is intimately involved in determining the minor discrepancies between ship contents measurements & tank measurements. Such an error unknown in last 5,000 discharges, assume 0.001 (consistent with Kletz No 1 in Annex A).	Shipping Supervisor checks the ship's paperwork and the Terminal paperwork compares tank ATG with bill of laden. Assume 0.1 (conservative use of HEARTS task D in Annex A).	Hourly dips taken & recorded by operators but fails to notice tank levels incorrect & overfill possible (conservative use of HEARTS task D in Annex A)	Not relevant for this scenario
1 y^{-1}	0.001	0.1	0.1	1

Table 6: IE2

Initiating Event 2 is a ship arriving with sufficient ullage available in designated tank but cargo greater than the agreed quantity because ship will subsequently discharge at another terminal				
Number of ship discharges per year	**Probability of failure for initial calculation**	**Probability of failure for start checks**	**Probability of failure for not detecting errors on hourly ullage cross-checks**	**Probability errors would lead to filling above maximum working level**
Ship arrives with sufficient ullage available in designated tank but cargo greater than the agreed quantity because ship will subsequently discharge at another terminal. Based on terminal experience, up to 1 ship per year - (part discharged)	Cargo Surveyor checks are irrelevant for this scenario	Shipping Supervisor checks the ship's paperwork and the Terminal paperwork, irrelevant for this scenario	Supervisor in control room fails to advise when tank full and time to terminate transfer. This is a trained professional who is intimately involved in determining the minor discrepancies between ship contents measurements & tank measurements. Such an error unknown in last 1,400 discharges, assume 0.001 (consistent with Kletz No 1 in Annex A).	Not relevant for this scenario
$1\ y^{-1}$	1	1	0.001	1

Table 7: IE3

Initiating Event 3 Ship arrives to discharge into two receiving tanks & the switch between tanks fails, overfilling the first tank				
Number of ship discharges per year	**Probability of failure for initial calculation**	**Probability of failure for start checks**	**Probability of failure for not detecting errors on hourly ullage cross-checks**	**Probability errors would lead to filling above maximum working level**
Scenario 3: ship arrives to discharge into two receiving tanks & the switch between tanks fails, overfilling the first tank. Up to 20 loads per year are split.	Supervisor in control room fails to advise when first tank full and time to switch to second tank. This is a trained professional who is intimately involved in determining the minor discrepancies between ship contents measurements & tank measurements. Such an error unknown in last 5,000 discharges, assume 0.001 (consistent with Kletz No 1 in Annex A).	Not relevant for this scenario	Conservatively assumed not relevant for this scenario	Not relevant for this scenario
20 y^{-1}	0.001	1	1	1

Table 8: IE4

Initiating Event 4 Ship discharge progresses normally but load transferred into wrong tank. Valves are correctly set to the tank but when instructed, opens the wrong last valve & allows the load into the wrong tank				
Number of ship discharges per year	**Probability of failure for initial calculation**	**Probability of failure for start checks**	**Probability of failure for not detecting errors on hourly ullage cross-checks**	**Probability errors would lead to filling above maximum working level**
Ship discharge progresses normally but load transferred into wrong tank. Valves are correctly set to the tank but when instructed, operator opens the wrong last valve & allows the load into the wrong tank. Never happened in over 20 years (1,500 ships) so assume 0.05 y^{-1}	Ship takes about 5 minutes to fill the line & operator fails to check correct tank entry (not independent). Initial filling rate low to facilitate this check.	Supervisor fails to check the lack of rise in level on ATG & ignores rise in wrong tank (consistent with Kletz No 1 in Annex A but conservatively downgraded)	Conservatively assumed not relevant for this scenario	Not relevant for this scenario
0.05 y^{-1}	1	0.01	1	1

Table 9: IE5

Initiating Event 5 ATG fails to danger during ship discharge into two receiving tanks				
Number of ship discharges per year	**Probability of failure for initial calculation**	**Probability of failure for start checks**	**Probability of failure for not detecting errors on hourly ullage cross-checks**	**Probability errors would lead to filling above maximum working level**
Overfilling due to ATG failure is a function of the time tank being filled, rather than the number of times the tank is filled. There are 100 ship imports per year for less than 1,500 hours per year, hence assume import pumping is 0.15 of the year	ATG (non-SIL rated) will be managed in line with IEC 61511 SFAIRP (including robust maintenance arrangements with manufacturer). Currently no history of failure to danger. Although equipment reliability is likely to be in better than 0.1, IEC 61511 requires non-SIL equipment to have maximum reliability of 10^{-5} dangerous failures per hour	Not relevant for this scenario	NuStar Terminal Controller fails to compare tank level with dipping plan. Hourly dips taken & recorded by operators but fail to terminate the transfer at agreed quantity (consistent with Kletz No 1 in Annex A but conservatively downgraded) Usually the ship discharge occurs across shifts allowing a different person to notice the error.	Not relevant for this scenario
0.15 y^{-1}	0.1	1	0.01	1

5. Independent Layers of Protection

Table 10: Protection Layers

Name		Description	Failure on demand
PL 1	High Level (from ATG)	The gasoline tanks have servo gauges providing the ATG & the real-time contents are displayed in the Control Room Audible (inside and outside control room) and visible alarm in control room that will require operator action. During import there is a minimum of one person in the control room at all times who could react to high level alarms, and although there could be a common cause failure (such as a major distraction), this is considered to be very unlikely. There are only a few alarm activations within the control room and as such there is little risk of alarm flooding. Audible and visible High level alarm (inside and outside the control room) This system is not SIL rated but will be managed to 61511 SFAIRP.	0.1
PL 2	High High (automated independent trip)	SIL 2 rated independent High High trip These are radar sensors with a safety PLC logic solver Failsafe and firesafe ROSOVs for imports	4 x 10^{-3}

6. Mitigation Layers

Table 11: Mitigation Layers

Name		Description	Safety Failure on demand	Environmental Failure on demand
ML 1	Overflow detection & effective action	Level detection in the bund will alarm in the control room if there is a tank overfill scenario. Early detection of the overflow will enable the supervisor/operator to stop the import. The system requires operator response to stop the import e.g. close a valve. Robust maintenance process is in place with equipment suppliers. In addition existing CCTV (but not specifically designed to monitor tank farm) There are many different final elements by which the import can be stopped including powered and manual valves & stopping the ship's pump. Manual response relies on the actions of one of several supervisors or operators, with alarms sounding both inside the control room. All personnel, including the ship, are in constant communication via the two-way radios. Therefore overall conservative figure of 0.1 taken.	0.1	0.1

ML 2	Secondary and Tertiary containment	Bunds / tertiary containment does not prevent loss of vapour and therefore will not stop a VCE, but is likely that these will provide significant protection against environmental impacts. Concrete bund walls with a capacity well over 110% of the largest tank volume and it is therefore possible that these walls will be adversely affected by the VCE and as such the protection provided by the bunds may in some cases be compromised. The bund meets the permeability criteria. There does not exist tertiary containment that fully complies with the requirements identified within PSLG although an action plan will be agreed to address this. Therefore overall a conservative figure of 1 has been taken.	1	1
ML 3	Emergency warning and evacuation	If people can be moved outside of 250m radius from overfilling tank, the likelihood of fatalities falls rapidly. Will only be effective if overfill is detected with sufficient notice to allow evacuation outside of 250m radius in order to significantly reduce consequences. Site only has a fire alarm system therefore adopt conservative approach and assume 250m radius cannot be evacuated in time. No further credit to be taken over that in ML 1, which may involve some degree of evacuation.	1	1

7. Conditional Modifiers

Table 12: Conditional Modifiers

Title	Description	H&S (Probability of occurrence)	Environmental (Probability of occurrence)
CM 1	Probability of delayed ignition based on 0.1 for immediate ignition (TNO Purple Book) assume the same for no ignition & remainder is delayed ignition	0.8	0.8
CM 2	Probability of calm weather (less than 2.6m/s windspeed = 0.1) from site weather data	0.1	0.1
CM 3	Periodic walk rounds by operators may detect an overfill but this is ignored	1	1
CM 4	The likelihood of a significant explosion depends on factors such as whether there is a high-energy ignition source, the amount of congestion etc. However as Buncefield explosion mechanism not fully understood, adopt a conservative figure of 1	1	1
CM 5	Probability of fatality. This has been taken account of in the predicted consequences No credit to be taken	1	1
CM 6	Probability of environmental consequence has been taken account of in the predicted consequences No credit to be taken	1	1

8. Tank overfill leading to Vapour Cloud Explosion and subsequent bund fire

Table 13: Frequencies

SAFETY	Residual risk	Target likelihood	Further layers required
Gasoline tanks overfill & VCE	$7.36 \times 10^{-8}\ y^{-1}$	$1 \times 10^{-5}\ y^{-1}$	No
ENVIRONMENTAL	**Residual risk**	**Target likelihood**	**Further layers required**
Gasoline tanks overfill & VCE	$7.36 \times 10^{-8}\ y^{-1}$	$1 \times 10^{-5}\ y^{-1}$	No

9. Uncertainty & Sensitivity

There is uncertainty in any LOPA estimation and the sensitivity to the input data was addressed by using pessimistic data. Using this approach, the overall frequency of a gasoline tank being filled to reaching the Independent High level is calculated as 2.3 x 10^{-3} per year (without the SIL 2 trip system), hence about once every 435 years or 43,500 gasoline ship discharge operations. Site personnel have experience of 2,000 ship discharges of various ship products over the last 20 years without any tank-overfilling incident. If the other four NuStar terminals were also included then this value would increase significantly to over 10,000 without overfilling.

Therefore, the assumptions made within this analysis appear to be reasonable and believable.

The numerical results are most sensitive to IE3 that is consistent with site operational judgement. The main contribution to the risk comes from human error & failures of the trip system.

LOPA is not normally used to assess societal risk, however a coarse review has been considered to see is more detailed analysis needs to be undertaken at this stage. R2P2 suggests that the risk of an accident causing the death of 50 people or more in a single event should be regarded as intolerable if the frequency is estimated to be more than one in five thousand per annum. The estimated maximum number of fatalities and the frequency are well below this value.

There may also be other scenarios, which have off-site risks but none of the major accident hazards identified in the safety report have significant off-site safety hazard. By far the largest societal impact will be caused by a VCE.

10. Individual Risk

The Safety Report estimates a conservative Individual Risk by simply summating all the fatal accident frequencies, although no individual can be exposed to all these risks at the same time due to the distances between the locations of the Major Accident Hazards. This gave a value of less than 600 cpm (tolerable if ALARP) and the VCE is a small contributor to this value.

Looking at the guidance given in R2P2 (Reducing Risks Protecting People), this gives a maximum tolerable risk for an individual on site of 1 x 10^{-3} y^{-1} and identifies that risks become broadly acceptable from 1 x 10^{-6} y^{-1}. Therefore the risk to an individual on site from all risks falls within the 'Tolerable if ALARP' range.

11. Improvement Plan

The recent and proposed risk reduction measures are listed below:

- SIL 2 rated high level alarms that trip the importing ROSOVs were fitted in 2010
- A training programme on IEC61511 part 3 and the general principles of IEC61511/08 was delivered to all senior staff at the Terminal in 2010.
- Gasoline bund liquid high level alarms to warn of potential loss of containment will be completed in by end 2012
- An additional high level alarm is proposed for the gasoline tankers vapour return line to trip the filling system
- There is a current NuStar Terminals Ltd review of all core skills, training and competency
- A CDIT qualified auditor is currently reviewing all operational procedures at the terminal.
- The detailed review of tertiary containment is currently progressing
- The pre-fire plan is in progress

12. Other consequences

Two further consequences were considered:

- Flash Fire followed by a pool fire
- Unignited tank overfill

12.1 Summary of flash fire LOPA

See full details in Annex C.

Table 14: Summary of Flash Fire & Bund fire LOPA

	Safety Residual risk	Target likelihood	Further layers required
Flash Fire & Bund fire	1.5×10^{-9}	1×10^{-5}	No
	Environment Residual risk	**Target likelihood**	**Further layers required**
Flash Fire & Bund fire	4.6×10^{-9}	1×10^{-5}	No

Safety

Based on Table 8 of the PSLG final report for 1 fatalities then 'tolerable if ALARP' ranges from 1×10^{-4} y^{-1} to 1×10^{-5} y^{-1} and so less than 1×10^{-5} y^{-1} was chosen as the target frequency for the VCE.

Environmental

The COMAH safety report estimates the effects of a release of hydrocarbons or firewater at the establishment as having limited effects at the site that most closely resemble 'Category 3, Significant' from Table 10 of the PSLG final report. The relevant described is "Severe and sustained nuisance e.g. strong offensive odours or noise disturbance; major breach of permitted emissions limits with possibility of prosecution; numerous public complaints". This 'acceptable' risk criterion from Table 9 of the PSLG final report is 1×10^{-4} y^{-1} for the establishment.

The scenario criterion was taken as 1×10^{-5} y^{-1} to conservatively allow for the environmental risk from other Major Accident Hazards detailed in the Safety Report.

Therefore proposed Environmental Integrity Level achieves the target frequency.

12.2 Unignited tank overfill

See full details in Annex D

Table 15: Summary of Unignited Spill LOPA

	Environment Residual risk	Target likelihood	Further layers required
Unignited Spill	8.6×10^{-8}	1×10^{-5}	No

Therefore proposed Environmental Integrity Level achieves the target frequency.

ANNEX A
HUMAN ERROR DATA

From 'Methods for Determining and Processing Probabilities' CPR 12E Committee for the prevention of Disasters (Red Book) ISBN 90 12 08543 8, Appendix 14-A:

Table 14-A-1: Human Reliability Data (HEART values)

TASK	DESCRIPTION OF TASK	HUMAN ERROR PROBABILITY	BOUNDS (5th TO 95 th)
A	Totally unfamiliar; performed at speed; with no real idea of likely consequences	0.55	0.35-0.97
B	Shift or restore system to a new original state without supervision or procedure	0.26	0.14-0.42
C	Complex task requiring high level of comprehension and skill	0.16	0.12-0.28
D	Fairly simple task performed rapidly or given scant attention	0.09	0.06-0.13
E	Routine, highly practiced, rapid task involving relatively low level of skill	0.02	0.007-0.045
F	Restore or shift a system to original or new state following procedures, with some checking	0.003	0.0008-0.007
G	Completely familiar, well designed, highly practised routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential error but without the benefit of significant job aids	0.0004	0.00008-0.009
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002	0.00006-0.0009
M	Miscellaneous task for which no description can be found	0.03	0.008-0.11

Tasks are listed with least reliable first & improving on descending the table (apart from M)

Table 14-A-2: Operator Error Estimates (Kletz)

NO	DESCRIPTION OF TASK	HUMAN ERROR PROBABILITY
1	Omission or incorrect execution of step in a familiar startup routine	0.001
2	Failure to respond to audible alarm in quiet control room by pressing single button	0.001
3	Failure to respond to audible alarm in quiet control room by some more complex action such as going outside and selecting correct valve among many	0.01
4	Failure to respond to audible alarm in busy control room within 10 minutes	0.1
5	Failure to carry out rapid and complex actions to avoid serious incident such as an explosion	0.5

IEC 61511-3: 2003 Annex F LOPA
Table F3 (PfD)

Human Performance (trained, no stress) 10^{-2} to 10^{-4}

Human Performance (under stress) 1 to 0.5

ANNEX B

HSE LOPA SPREADSHEET DATA

ANNEX C
FLASH FIRE & BUND FIRE

Consequences

The worst-case consequence of an ignited large vapour cloud from a gasoline tank-overfilling scenario is that it will lead to a VCE. A flash fire is an alternative scenario that is expected to occur for smaller vapour clouds or if there is early ignition. Within a flashfire, it is assumed that anyone within the vapour cloud will be killed.

In the event that the flash fire is restricted to the bund then it is expected that there would not be any personnel present. However, if the vapour cloud and subsequent flash fire extended outside the bund then personnel could be present, although in most cases there would not be anyone within the flash fire. Conservatively assume 1 fatality for an operator conducting the regular tours.

The consequential bund fire creates a thermal radiation hazard that is considered in the Safety Report and no further fatalities are expected because no other persons will be affected.

The environmental consequences will be less than for a VCE as the flash fire will not cause the same level of damage to the other structures and the scale of the fire and environmental release much lower. In addition, early ignition will result in a smaller volume being released before the ignition. However assume small-scale pollution caused by product / foam / firewater reaching the river by surface drainage.

Based on the PSLG final report, the following target frequencies for this scenario have therefore been used:

Table C.1: Target Frequencies

Scenario	Consequences	Target likelihood
Flash fire and subsequent significant bund pool fire	**Safety** One Fatality within vapour cloud.	1 x 10^{-5} Broadly acceptable for scenario
	Environmental Significant pollution caused by hydrocarbons, foam & firewater reaching the Musgrave Channel from subsequent bund fires.	1 x 10^{-4} Acceptable for establishment

Safety

Based on Table 8 of the PSLG final report for 1 fatalities then 'tolerable if ALARP' ranges from 1 x 10^{-4} y^{-1} to 1 x 10^{-5} y^{-1} and so less than 1 x 10^{-5} y^{-1} was chosen as the target frequency for the VCE.

Environmental

The COMAH safety report estimates the effects of a release of hydrocarbons or firewater at the establishment as having limited effects at the site that most closely resemble 'Category 3, Significant' from Table 10 of the PSLG final report. The relevant described is "Severe and sustained nuisance e.g. strong offensive odours or noise disturbance; major breach of permitted emissions limits with possibility of prosecution; numerous public complaints". This 'acceptable' risk criterion for the establishment from Table 9 of the PSLG final report is 1 x 10^{-4} y^{-1}.

Initiating Events

As before

Independent Layers of Protection

As before

Mitigation Layers

Table C.2: Mitigation Layers

	Name	Description	Safety (Probability of failure)	Environment (Probability of failure)
ML 1	Overflow detection & effective action	As before	0.1	0.1
ML 2	Secondary and Tertiary containment	Bunds with a capacity of over 110% of largest tank volume. The spot tests done meet the permeability criteria for earth bund floors but a more detailed analysis by an external competent person identified discontinuities that has created a detailed improvement plan. Although there is some existing tertiary containment this does not yet fully comply with the requirements identified within PSLG although an action plan will be agreed to address this. Bunds / tertiary containment does not prevent loss of vapour and therefore will not stop a flash fire and therefore will not prevent the H&S consequences. However, the bunds and tertiary containment will significantly mitigate the environmental consequences.	1	0.1
ML 3	Emergency warning and evacuation	As before	1	1

Conditional Modifiers

Table C.3: Conditional Modifiers

	Title	Description	H&S (Probability of occurrence)	Environmental (Probability of occurrence)
CM1	Probability of ignition	As before, probability of ignition based on 0.1 (TNO Purple Book) for immediate ignition	0.1	0.1
CM2	Probability of calm and stable weather	Data as before but a flash fire may require a smaller vapour cloud than was the case for the VCE, and as such relevant weather conditions may be present more of the time than for VCE. Therefore take a more conservative figure of 0.5	0.5	0.5
CM3	Probability that a person is present within the hazard zone	Periodic walk rounds by persons are for 5 minutes within the 250m zone around the gasoline tanks for up to 10 tours per day = 0.035 of the time. No credit taken for environmental scenario	0.035	1
CM4	The likelihood of a significant explosion	Not relevant for a flashfire	1	1
CM5	Probability of fatality	This has been taken account of in the predicted consequences No credit to be taken	1	1
CM6	Probability of the environmental consequence	This has been taken account of in the predicted consequences No credit to be taken	1	1

Summary of Flash Fire & Bund fire LOPA

Table C.4: Summary of Flash Fire & Bund fire LOPA

	Safety Residual risk	Target likelihood	Further layers required
Flash Fire & Bund fire	1.5 x 10^{-9}	1 x 10^{-5}	No
	Environment Residual risk	**Target likelihood**	**Further layers required**
Flash Fire & Bund fire	4.6 x 10^{-9}	1 x 10^{-5}	No

Safety

Based on Table 8 of the PSLG final report for 1 fatalities then ‘tolerable if ALARP’ ranges from 1 x 10^{-4} y^{-1} to 1 x 10^{-5} y^{-1} and so less than 1 x 10^{-5} y^{-1} was chosen as the target frequency for the VCE.

Environmental

The COMAH safety report estimates the effects of a release of hydrocarbons or firewater at the establishment as having limited effects at the site that most closely resemble ‘Category 3, Significant’ from Table 10 of the PSLG final report. The relevant described is “Severe and sustained nuisance e.g. strong offensive odours or noise disturbance; major breach of permitted emissions limits with possibility of prosecution; numerous public complaints”. This ‘acceptable’ risk criterion from Table 9 of the PSLG final report is 1 x 10^{-4} y^{-1} for the establishment.

The VCE scenario criterion was taken as 1 x 10^{-5} y^{-1} to conservatively allow for the environmental risk from other Major Accident Hazards detailed in the Safety Report.

Therefore proposed Environmental Integrity Level achieves the target frequency.

ANNEX D

UNIGNITED SPILLAGE

Consequences

As the bund is sized for over 110% of the largest tank's maximum working level, an overfill scenario at the maximum flow rate would take many hours to fill the bund. In addition, as the imports from ship are fixed parcels, the size of the parcel is less than the volume that could be contained within the bund. As such, in the event of an unignited spill it is assumed that the volume of the spill can be contained within the bund.

There could be a substantial spillage into the bund but the environmental consequences will be much less than for a VCE or flash fire as there will not be any overpressure or pool fire. However, it is assumed that there may be some minor pollution caused by product or foam (from vapour suppression to prevent ignition) reaching the site drainage system and interceptors.

Based on the PSLG final report, the following target frequencies for this scenario have therefore been used:

Table D.1: Target Frequencies

Scenario	Consequences	Target likelihood
Release of gasoline from overfilling a tank but no ignition	**Environmental** Significant pollution caused by severe and sustained nuisance due to odours. Possible but unlikely that some foam may reach the River Thames.	1×10^{-4} Acceptable for establishment

Initiating Events

As before

Independent Layers of Protection

As before

Mitigation Layers

Table D.2: Mitigation Layers

	Name	Description	Environment (Probability of failure)
ML 1	Overflow detection & effective action	As before	0.1
ML 2	Secondary and Tertiary containment	Bunds with a capacity of over 110% of largest tank volume. The spot tests done meet the permeability criteria for earth bund floors but a more detailed analysis by an external competent person identified discontinuities that has created a detailed improvement plan. Although there is some existing tertiary containment this does not yet fully comply with the requirements identified within PSLG although an action plan will be agreed to address this. Bunds / tertiary containment does not prevent loss of vapour and therefore will not stop a flash fire and therefore will not prevent the H&S consequences. However, the bunds and tertiary containment will significantly mitigate the environmental consequences.	0.1
ML 3	Emergency warning and evacuation	As before	1

Conditional Modifiers

Table D.3: Conditional Modifiers

	Title	Description	Environmental (Probability of occurrence)
CM1	Probability of ignition	Not relevant for this scenario	1
CM2	Probability of calm and stable weather	Not relevant for this scenario	1
CM3	Probability that a person is present within the hazard zone	Not relevant for this scenario because an evaporating pool of gasoline would not cause harm (see Safety Report)	1
CM4	The likelihood of a significant explosion	Not relevant for this scenario	1
CM5	Probability of fatality	Not relevant for this scenario	1
CM6	Probability of the environmental consequence	This has been taken account of in the predicted consequences No credit to be taken	1

Summary of Unignited Spill LOPA

Table D.4: Summary of Flash Fire & Bund fire LOPA

	Environment Residual risk	Target likelihood	Further layers required
Unignited Spill	8.6 x 10^{-8}	1 x 10^{-5}	No

Therefore proposed Environmental Integrity Level achieves the target frequency.

Signature Certificate

Document Reference: 5XPF3PIHMIGD9LWHLXW4JZ

RightSignature
Easy Online Document Signing

David Ransome
Party ID: BVH7GMJ6WICJNYHSCCZ3CD
IP Address: 86.14.218.30
VERIFIED EMAIL: drr@pidesign.co.uk

Electronic Signature:

Multi-Factor
Digital Fingerprint Checksum 94600ad33143872576526222709d82466af85793

Timestamp	Audit
2017-06-30 05:24:07 -0700	All parties have signed document. Signed copies sent to: David Ransome and David Ransome.
2017-06-30 05:24:07 -0700	Document signed by David Ransome (drr@pidesign.co.uk) with drawn signature. - 86.14.218.30
2017-06-30 05:23:25 -0700	Document viewed by David Ransome (drr@pidesign.co.uk). - 86.14.218.30
2017-06-30 05:23:25 -0700	Document created by David Ransome (drr@pidesign.co.uk). - 86.14.218.30

This signature page provides a record of the online activity executing this contract.

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

NUSTAR

BELFAST TERMINAL

STORAGE TANKS OVERFILL

SAFETY INSTRUMENT SYSTEM

FUNCTIONAL SAFETY ASSESSMENT

STAGE 5 – MODIFICATION

Rev	Date	By	Checked	Approved	Description	Client Ref.
A	24.02.14	D.R. Ransome	DSR	DRR	For Client Comments	
B	28.04.14	D. R. Ransome	DSR	Client	Following Installation	
C	15.09.14	D. R. Ransome	DSR	Client	Actions Updated	Document No. **NU271011_RPT**
D	25.03.15	D. R. Ransome	DSR	Client	Actions Updated	
E	14.11.16	D. R. Ransome	DRR DRansome	Client	Actions Updated and FSA Closed	

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION CONTROL

Rev	Description
A	Original Issue following FSA Meeting and initial review
B	Revised following Installation and documentation update
C	Revised following Actions update
D	Revised following Actions update
E	Actions Updated and FSA closed

2 SCOPE & DEFINITIONS

2.1 Scope

NuStar Energy – Belfast Terminal have an Independent High Level Alarm system to provide a SIL 2 rated automatic shutdown system to prevent 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
= Common Cause Failure Fraction
$_{D}$ = Detected Common Cause Failures
= Failure rate (per hour)
$_{D}$ = Dangerous Failure Rate
$_{DD}$ = Dangerous Detected Failures
$_{DU}$ = Dangerous Undetected Failures
$_{SD}$ = Safe Detected Failures
$_{DU}$ = Safe Undetected Failures

3 INTRODUCTION

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

3.1 Assumptions and Constraints

The existing SIS system has been in operation for a number of years, with various reviews and assessments having been previously conducted. This Functional Safety Assessment builds upon functional safety and lifecycle planning and management by assessing the proposed modifications to the system.

3.2 Proposed Modification

There is a requirement to perform several enhancements to the SIS. The elements of the modification are detailed below

3.2.1 Change Radar level sensor to Magnetrol on Tank 46 & 47.

3.2.2 Addition of two ESV for Ethanol system.

3.2.3 To provide for opening and closing of the Tank 6 Road Tanker offload ESV from the SCADA.

3.2.4 Replace Tank 11 radar for a liquiphant.

3.2.5 Install MODBUS transfer of Data from safety PLC to BPCS – Not SIL Rated

3.3 Team Membership

Date of Initial Review –18th September 2013 updated 9th October 2013 & 24th January 2014 at NuStar Terminals, Belfast Terminal.

The FSA review team:-
NuStar Terminals:
Andy Bann. Terminal Manager
Paul McGreevy
Neil Mearns
Darren Peck – EC&I Engineering Manager

P&I Design Ltd.
D.R. Ransome - FSA Chair

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

Andy Bann, Terminal Manager

15 years experience at Belfast Terminal; with a background in operations as a Terminal Controller, Senior Terminal Controller and Terminal Manager. Previous experiences in the aerospace and transport industries, as an electrical technician, and in junior management roles. Time served aircraft electrician. Currently holds a NEBOSH Managing Safety Certificate (Level 3).

Paul McGreevy

Neil Mearns, Terminal Engineer
Graduated from The Queen's University of Belfast in 1999 with a BEng in Mechanical and Manufacturing Engineering, joining the Stocks team at BP Oil UK Ltd in the same year. He progressed to Operations Controller at the company in 2001, before joining Belfast Terminal in 2003 as a Terminal Controller. He was promoted to Terminal Engineer in 2007. Currently holds a Postgraduate Diploma in Safety and Risk Management (Level 7) from the University of Strathclyde, and has current GradIOSH professional status.

Darren Peck, EC&I Engineering Manager - UK
Over 20 years' experience in the petrochemical process industry ranging from design through to installation and commissioning.

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. A Registered Functional Safety Engineer.

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

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

The FSA will address the following:

The recommendations and actions arising from previous FSA have been resolved and completed;
Review of the following;

- o Description of the modification;
- o Reason for the modification
- o Hazards which may be affected by the modification;
- o An analysis of the impact on functional safety as a result of the proposed modification;
- o Approvals for the modification;
- o 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;

- o LOPA
- o SRS
- o Design
- o Installation
- o Testing
- o Operation
- o 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 4 was held on Wednesday 7th September 2011 at Belfast Terminal. It has been issued at Revisions A through to D. It is noted that the following actions are still incomplete.

Action 8: Review LOPA for the addition of gasoline tank to tank transfers.

Action 14: Final tag numbers to be added to the P&I Diagrams for re-issue.

Action 15: SIS Instrumentation and Documentation to reflect tag numbering of P & I Drawings also Instrument Tagging should be consistent with P & I Drawings.

Action 16: All SIS documentation to be reviewed and ensure that it reflects P& I Drawings and installed system.

These actions need to be reviewed and updated as to their current status. It is not intended to record the status of these actions in this FSA as this could cause confusion and difficulty in action control.

4.3 Proposed Modification

A FSA Meeting was held at the terminal on 18th September 2013. 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.

Document NU343001_MIN details this meeting. Detailed below are the conclusions of the meeting.

4.4 Description of the Modification

4.4.1 Change Radar level sensor to Magnetrol on Tank 46 & 47.

4.4.2 Addition of two ESV's for Ethanol system.

4.4.3 To provide for opening and closing of the Tank 6 Road Tanker offload ESV from the SCADA.

4.4.4 Replace Tank 11 radar for a liquiphant.

4.4.5 MODBUS transfer of Data from safety PLC to BPCS – Not SIL Rated

4.5 Reason for the Modification

4.5.1 Change Radar level sensor to Magnetrol on Tank 46 & 47.
The existing radar transmitters on floating roof tanks have suffered from numerous spurious activations, Magnetrol displacer switches are to be utilised in place of the radar transmitters with a view of the different technology providing less false activations.

4.5.2 Addition of two ESV's for Ethanol system.
New transfer system and road receipt system. One ESV on Road Tanker offload at Tank 6, activation of any tank IHLA will close this ESV. The second is the Ethanol tank transfer system for tank 6 to tank 11. Any IHLA (all tanks) will close the ESV.

4.5.3 To provide for opening and closing of the Tank 6 Road Tanker offload ESV from the SCADA.
This is to allow for remote operation of the valve.

4.5.4 Replace Tank 11 radar for a liquiphant.
The floating roof has been removed from tank 11, thus the radar can be removed and the preferred technology of vibronics switch can be installed for liquid level detection.

4.5.5 MODBUS transfer of Data from safety PLC to BPCS – Not SIL Rated
This is to provide data exchange between the Safety PLC and the BPCS. It has no impact on safety and is for diagnostics. It is not considered as SIL rated.

4.6 Hazards Which May Be Affected By The Modification

4.6.1 Change Radar level sensor to Magnetrol on Tank 46 & 47.

No change in the hazard, just the method of detection. There will be a requirement to also install a signal conditioner. The use a four core (2 pair) cable from each switch to a P&F signal conditioner is to be installed to provide short and open circuit protection.

The logic solver and final elements are as original for Tanks 46 & 47.

4.6.2 Addition of two ESV's for Ethanol system.

This is a new system, but presents the same hazard of tank overfill and overspill, rates are considerably less than ship import so this modification has no additional requirements than those already employed on tank overfill protection.

4.6.3 To provide for opening and closing of the Tank 6 Road Tanker offload ESV from the SCADA.

This facility is to provide remote operation of opening and closing the valves. It is not intended as a control system to be independent from the SIS. It must be ensured that the SCADA/PLC opening and closing of the valves cannot influence on the safe operation of the IHLA.

4.6.4 Replace Tank 11 radar for a liquiphant.

No change in hazard just the method of detection. The operating height to be determined in the fact that activation point may be different from that of the floating roof activation point.

4.6.5 MODBUS transfer of Data from safety PLC to BPCS.
Not SIL Rated, to provide better diagnostics and operator information.

4.7 The Impact On Functional Safety

There was nothing identified as impacting on functional safety

4.8 Approvals For The Modification and Competencies

For all of the modifications, NuStar 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

At the FSA meeting it was stated that the design was to commence immediately with a view to installation commissioning in November/December 2013.

The Magnetrol switches are on a reasonably long delivery, so it is important for specification and order to be expedited.

4.10 Verification Process To Ensure Proper Implementation

Utilise normal lifecycle approach procedures with SAT and test procedures to ensure the modifications have not had any influence on the existing SIS. Following design the design to be reviewed as part of this FSA. The completed installation to be validated by proof testing.

4.11 SIS Lifecycle Requirements Of The Modification

It is felt there is no requirement to re LOPA or Risk Assess the process however, it may be prudent to update the LOPA at the next issue and include theses additional items.

4.12 Documentation That Will Require Updating:

Safety Requirement Specification
SIL Verification Document
Software Design
Loop Drawings
Cable & Wiring Drawings
Verification Documentation
Management of Functional Safety Document
P & I D’s

4.13 Operating Manuals And Documentation

Operating Procedures and TORA require updating together with new procedures for the Ethanol Transfer System.

4.14 Training Requirements Following Modification

As the system will operate as it does at present, no specific training is necessary other that ensuring operators are aware of the changes and the additional operation of Tank 6 valves.

5 REVIEW OF REVISED LIFECYCLE DOCUMENTATION

5.1 Safety Requirement Specification

The Safety Requirement Specification, NU271003_RPT, prior to this FSA was issued at Revision A - 13.09.11 and Issue B - 01.11.11. Originally a Functional Specification had been produced as part of the original design documentation. The SRS was created retrospectively resulting from an Action from FSA 4.

The SRS has been revised to Revision C to include the modifications detailed in this FSA, with a further Revision D on 14.10 13 which included client comments.

The SRS has been revised as follows:
2.2 Description of Operation revised to reflect the addition of the Ethanol system.
2.3 Revised to reflect new system models.
4.1 Revised for new sensor inputs
4.3 Revised for final elements.
4.4 Revised for SIS BPCS Interface.
4.5 Revised for SIF requirements.

As FSA 4 did not formally review the SRS the following checklist has been used to ensure the SRS complies with the Clauses of BS EN 61511.

5.1.1 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 details that a LOPA was conducted in September 2011 and that a SIL 2 Independent High Level Alarm (IHLA) SIS was to be designed and installed.

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

All Safety Instrumented Functions (SIF) within the Safety Instrumented System (SIS) are to SIL 2. This is detailed in Section 2.1 and in Section 4.5 - SIF Requirements.

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

Section 3 of the SRS details that the SIS shall operate in a low demand mode, but no reference to the demand rate could be found.

ACTION 1 - Define the actual demand rate derived from the LOPA to Section 2 of the SRS.

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

Section 2.2 provides a description of operation of the SIF's and Section 4.5 defines the safe state.

5.1.5 Have common cause failures been considered. BS EN Clause 10.

Each SIF is effectively a 1oo1 so common cause fail is not a real issue. However, Section 2.2 does define this and details common failures which could affect the SIS.

5.1.6 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 2.2 does detail that surge calculations have been carried out, Section 3 details process materials but process conditions are not specifically defined in the SRS.

ACTION 2: Process Conditions require to be added to the SRS to identify any issues the process or process conditions could have on the SIS.

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

Section 2.2 derives that slow closing valves of approximately 90 seconds are required to prevent pipeline surge.

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

Section 4.5 defines response times and the time required for activation at maximum flow. However, there is no reference to the Level of Concerns document detailing the range of the radar instruments, activation point of point sensors. These are all detailed in a separate NuStar document.

ACTION 3: A reference in the SRS to the document detailing Levels of Concerns and tank details should be added.

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

See 5.1.8 above and ACTION 3.

5.1.10 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 2.3 provides a system model of the SIF's.

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

Section 3 details that the MTTR is 8 hours.

5.1.12 Have manual shutdowns been considered. BS EN 61511 Clause 10.

Section 2.2 details that the new Ethanol valves can be remotely operated from the SCADA. The dockline valves are stated as being left open. Section 4.5 states that manual operation is via manual isolation valves.

ACTION 4: Add a description to the SRS as to how the ESV's can be operated manually in the event of an emergency.

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

Section 2.2 details the operation of the override system and the Management actions to be taken to maintain Functional Safety.

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

Section 4.4 details the interfaces between the BPCS and the SIS.

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

Section 4.4 states that the BPCS cannot interfere with the safe operation of the SIS. This is effectively achieved by a separate SCAP/PLC and Safety PLC.

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

Section 2.2 details the rest procedure.

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

Section 3 details requirements for anti-static and fire safe valves together with the anticipated effects of environmental and other considerations.

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

Section 4.2 details that the logic solver is a safety PLC but no reference to the requirements of Clause 12 of BS EN 61511.

ACTION 5: Add details to the SRS regarding the application software requirements.

FSA Revision B – The SRS has now had further revisions and was again reviewed at Revision E. See Section 7 of this FSA for progress of Actions.

FSA Revision C – The SRS has now had further revisions and was again reviewed at Revision F. See Section 7 of this FSA for progress of Actions.

5.2 SIL Verification

PILZ have been commissioned by NuStar Energy to provide the SIL Verification document.

This document requires to be modified to reflect the Probability of Failure on Demand (PFD) value for the revised SIF's.

ACTION 6: PILZ to revise their SIL Verification document to reflect revised and new SIF's. SIL Verification document revised to Version 3.

The SIL Verification Document has been reviewed by the FSA with the following comments:

SECTION 2:

Scope – The FSA now details Tanks 46 & 47 as having Magnetrol Displacer sensing elements, and Tank 11 has been added to the tanks with vibronic sensors.

There is no mention in this document as to the modifications for the Ethanol System as defined in Section 4.4 of this FSA.

ACTION 19: SIL Verification and design documentation for the Ethanol System to be provided for review by the FSA.

ACTION 20: There is a minor typographical error in the seventh paragraph the word "apmlifire" should read "amplifier"

SECTION 3:

The Executive Summary defines the basic operation and confirms the SIF's are to a SIL 2 integrity.

SECTION 4:

The demand mode is confirmed as a low demand mode.

SECTION 5:

This section of the SIL Verification document defines the calculations used in the SIL Verification.

ACTION 21: Section 5.2.3 and 5.2.4 details the common cause fraction and detected common cause failures, which have been defined as and $_{D}$ of 20% and 10% respectively. However, in the actual calculations the values used are 10% and 5 % respectively.

SECTION 6:

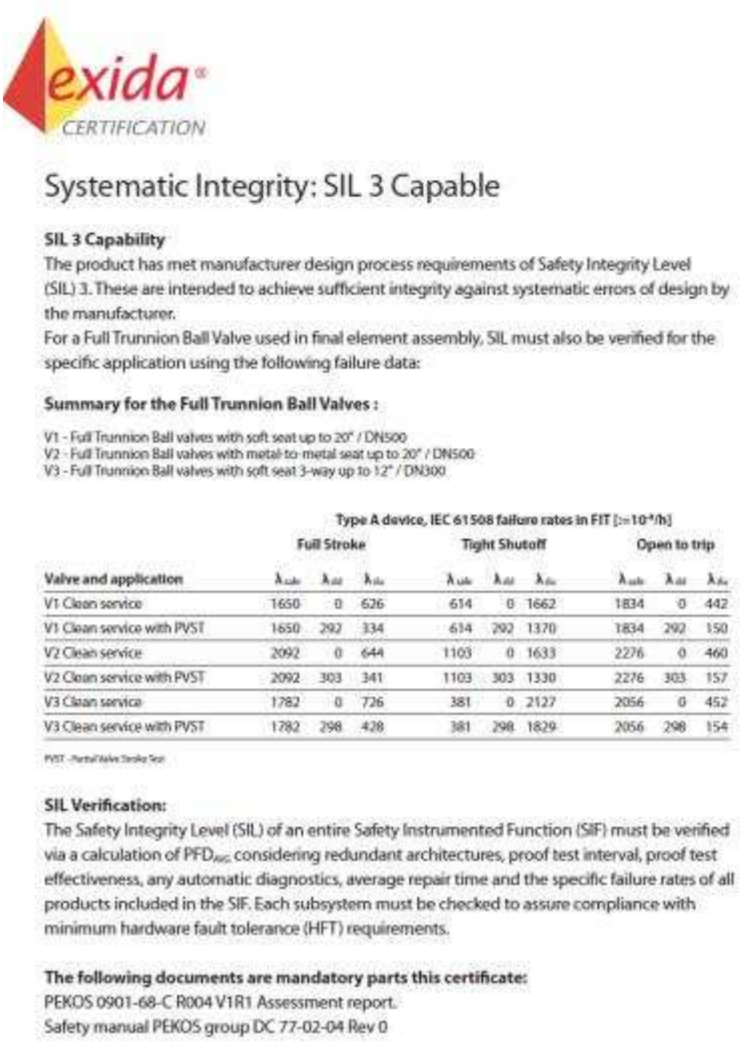
This section details the Safety Related Components and provides the PFD of the components employed in the SRS.

As detailed above, Action 21 there is a discrepancy in the value used for the common cause fraction.

If a figure of and $_{D}$ of 20% and 10% were used in the calculations, this would change the PFD$_{G}$ from 2.06 x 10^{-5} to 4.13 x 10^{-5}.

The SIL verification states that the calculation uses a simplistic approach and consideration should be given to a failure mode analysis. As the PFD value is low it is felt there is sufficient safety margin without further analysis being required.

ACTION 22: The failure data used in the calculation of the Pekos valve body Section 6.7.1 is not the latest data available. The calculation requires revising utilising the newer less conservative data.



exida® CERTIFICATION

Systematic Integrity: SIL 3 Capable

SIL 3 Capability
The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
For a Full Trunnion Ball Valve used in final element assembly, SIL must also be verified for the specific application using the following failure data:

Summary for the Full Trunnion Ball Valves :

V1 - Full Trunnion Ball valves with soft seat up to 20" / DN500
V2 - Full Trunnion Ball valves with metal-to-metal seat up to 20" / DN500
V3 - Full Trunnion Ball valves with soft seat 3-way up to 12" / DN300

	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

SIL Verification:
The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD$_{AVG}$ considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory parts this certificate:
PEKOS 0901-68-C R004 V1R1 Assessment report.
Safety manual PEKOS group DC 77-02-04 Rev 0

Using the new data increases the PFD from 2.60 x 10^{-5} with a SFF of 92% to 1.46 x 10^{-3} with a SFF of 85%.

Section 6.7.4 ROSOV Assembly, using the above data in the PFD_G calculation increases the failure from PFD_G - 7.28 x 10^{-5} to 1.52 x 10^{-3}.

SECTION 7

ACTION 23: Section 7 SIF PFD calculations need to be revised as a result of Actions 21 & 22.

5.3 Design Documentation

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

5.3.1 Safety Requirement Specification

This is detailed in Section 5.1.

5.3.2 SIL Verification Document

This is detailed in Section 5.2.

5.3.3 Equipment Specifications

The following specifications have been produced and reviewed:

NU271001_SPC - Tank 46 Level Switch.

The specification reviewed at the FSA was at Revision E. It was observed that the instruments were ordered against an earlier revision and specified with a 5m cable. Revision E of the document details the activation and cable length required to achieve the correct activation point.

ACTION 7: During installation it is essential that the calculated length of activation be checked and confirmed and that the cable length be set accordingly.

ACTION 8: Tag Number to be issued and added to specification.

NU271002_SPC - Tank 47 Level Switch.

The specification reviewed at the FSA was at Revision E. It was observed that the instruments were ordered against an earlier revision and specified with a 5m cable. Revision E of the document details the activation and cable length required to achieve the correct activation point.

ACTION 7: During installation it is essential that the calculated length of activation be checked and confirmed and that the cable length be set accordingly.

ACTION 8: Tag Number to be issued and added to specification.
NU271003_SPC - Interface Relay Barrier.

This specification details the switch interface unit and was reviewed at Revision B.

There were no specifications for the new valves or solenoid valves to be reviewed. It is presumed that NuStar Energy have a generic specification for valves, actuators and solenoid valves.

ACTION 9: To be confirmed that the final element assembly is specified to ensure that there is sufficient oversizing allowance. Also NuStar to produce their generic specification for final elements for review.

5.3.4 IHLA Calculation Sheet

NuStar Energy have produced and maintain a document which details the Levels of Concerns for all tanks together with the activation point of high alarms and Independent High level Alarms (IHLA).

ACTION 10: The Level of Concerns document to be updated to reflect changes from Radar to Magnetrol and Liquiphant.

5.3.5 Design Drawings

Tank 46 & 47

New loop drawings NU271002_DWG - Tank 46 & NU271003_DWG - Tank 47 have been produced. Following a review of the loop drawings it can be seen that the SIF utilises the two switches within the Magnetrol and also provides open circuit and short circuit lead protection. It would assist if the functions of the relay outputs from the P&F to the safety PLC were added i.e. What is the function of relay 1 and relay 2 outputs.

ACTION 11: Update the loop drawings with descriptors of the P&F relay outputs.

Ethanol

At Revision A and B of this FSA there were no drawings to review for the Ethanol modifications.

ACTION 12: NuStar to provide drawings for review of the Ethanol SIF’s.

Tank 11

At Revision A and B of this FSA there were no drawings to review for Tank 11 modifications

ACTION 13: NuStar to provide drawings for review of the Tank 11 SIF.

MODBUS

This non-SIL function is to be incorporated into the Software documentation by PILZ See Section 5.3.6.

5.3.6 Software Specification

PILZ produced the software for the SIS logic solver.

ACTION 14: PILZ to update and issue for review their software design and testing documentation to reflect the changes.

5.3.7 Testing and Inspection Documentation

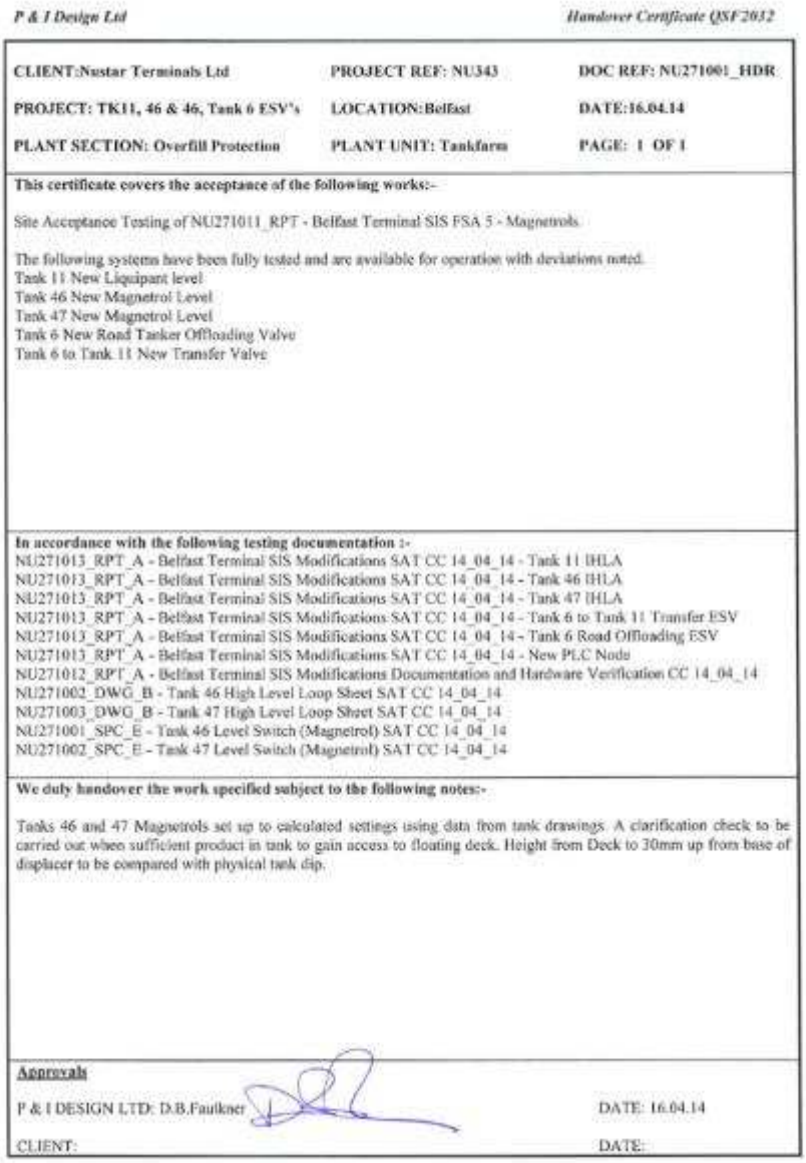
In addition to the software testing documents detailed in 5.3.6 there is a series of testing documentation:

NU271004_RPT Testing Procedure
NU271005_RPT Documentation and Hardware Verification
NU271006_RPT Radar Functional Test Procedure
NU271007_RPT Analysis and Approval
NU271008_RPT Equipment Failures Test Procedure
NU271009_RPT Test Procedure
NU271010_RPT Vibronics Functional Test Procedure
NU271101_RPT Testing Witness Report

At Revision A of this FSA this documentation had not been updated for the modifications so could not be reviewed.

ACTION 15: Testing documentation to be revised and additional documentation as required to be produced and issued for review.

The SAT was conducted on 16.04.14 – See below



P & I Design Ltd *Handover Certificate QSF2032*

CLIENT:Nustar Terminals Ltd	**PROJECT REF: NU343**	**DOC REF: NU271001_HDR**
PROJECT: TK11, 46 & 46, Tank 6 ESV's	**LOCATION:Belfast**	**DATE:16.04.14**
PLANT SECTION: Overfill Protection	**PLANT UNIT: Tankfarm**	**PAGE: 1 OF 1**

This certificate covers the acceptance of the following works:-

Site Acceptance Testing of NU271011_RPT - Belfast Terminal SIS FSA 5 - Magnetrols

The following systems have been fully tested and are available for operation with deviations noted.
Tank 11 New Liquipant level
Tank 46 New Magnetrol Level
Tank 47 New Magnetrol Level
Tank 6 New Road Tanker Offloading Valve
Tank 6 to Tank 11 New Transfer Valve

In accordance with the following testing documentation :-
NU271013_RPT_A - Belfast Terminal SIS Modifications SAT CC 14_04_14 - Tank 11 IHLA
NU271013_RPT_A - Belfast Terminal SIS Modifications SAT CC 14_04_14 - Tank 46 IHLA
NU271013_RPT_A - Belfast Terminal SIS Modifications SAT CC 14_04_14 - Tank 47 IHLA
NU271013_RPT_A - Belfast Terminal SIS Modifications SAT CC 14_04_14 - Tank 6 to Tank 11 Transfer ESV
NU271013_RPT_A - Belfast Terminal SIS Modifications SAT CC 14_04_14 - Tank 6 Road Offloading ESV
NU271013_RPT_A - Belfast Terminal SIS Modifications SAT CC 14_04_14 - New PLC Node
NU271012_RPT_A - Belfast Terminal SIS Modifications Documentation and Hardware Verification CC 14_04_14
NU271002_DWG_B - Tank 46 High Level Loop Sheet SAT CC 14_04_14
NU271003_DWG_B - Tank 47 High Level Loop Sheet SAT CC 14_04_14
NU271001_SPC_E - Tank 46 Level Switch (Magnetrol) SAT CC 14_04_14
NU271002_SPC_E - Tank 47 Level Switch (Magnetrol) SAT CC 14_04_14

We duly handover the work specified subject to the following notes:-

Tanks 46 and 47 Magnetrols set up to calculated settings using data from tank drawings. A clarification check to be carried out when sufficient product in tank to gain access to floating deck. Height from Deck to 30mm up from base of displacer to be compared with physical tank dip.

Approvals

P & I DESIGN LTD: D.B.Faulkner DATE: 16.04.14

CLIENT: DATE:

5.3.8 Management of Functional Safety Document

This document was not available for review at Revision A and B of this FSA.
P & I D's

ACTION 16: Provide Management of Functional Safety Document for review.

5.4 Validation and Testing Documentation

Section 5.3 details the testing documentation currently available for the SIS.

This FSA will review the completed testing documentation following installation and validation.

ACTION 17: On completion of testing, completed testing documentation to be issued for review by the FSA.

5.5 Software Validation

Following software modification by PILZ a software validation document will be produced and issued to this FSA for review.

ACTION18: On completion of testing, completed testing documentation to be issued for review by the FSA.

FSA Rev B – PILZ have produced several documents following the successful installation and testing of the modifications.

Document No: 100447.02_20140416_01_CSVS – Verification of Software for SI Projects (CSVS).

This document has been revised to reflect the program structure including the modified tanks and valves.

Document No: 100447.02_20140423_02_CSCC – Change Control Customer Document.

This document builds on the requirements of the SRS and defines the changes and procedures for change to incorporate the modification.

Document No: 100447.02_20140411_0A_CSSC – Safety Check – Validation.

This document shows the Software and version as V2.3.0 Build 138 and details the tests conducted to ensure correct operation. A sync fault between the two inputs was added to the software as part on the testing.

The above document, used at the test, has now been updated, which also includes Tank 6 checks.

Document No: 100447.02_20140416_01_CSSC – Safety Check – Validation.

Sections 8 & 9 of the document were not completed, these sections were for Additional Test Requirements and Customer Comments, this may be as no for test and comments were required.

5.6 Operation

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.

6 CONCLUSION

6.1 FSA Status

Revision A of this document was issued following changes to the SRS and before the modifications were completed. It serves as a request for the documentation required for review.

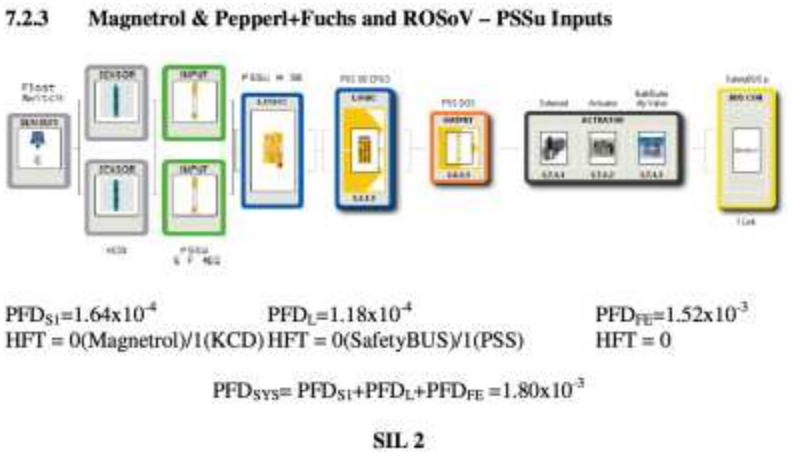
Revision B of this document concludes that, other than for some in-complete documentation, that the modifications have not impacted on Functional Safety and for the Tank Overfill SIF’s of SIL 2 has been maintained.

Revisions C & D were updates of the actions arising from the FSA.

Revision E was confirmation that all actions have been completed and closing of the FSA.

6.2 PFD & SIL

The SIL & PFD values of the modified sensor system on tanks 46 & 47 remain within the SIL 2 capability:



7.2.3 Magnetrol & Pepperl+Fuchs and ROSoV – PSSu Inputs

PFD_{S1}=1.64x10^{-4}
HFT = 0(Magnetrol)/1(KCD)

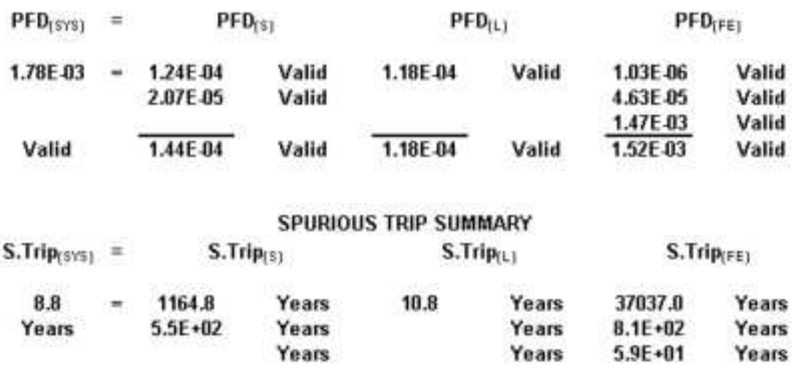
PFD_{L}=1.18x10^{-4}
HFT = 0(SafetyBUS)/1(PSS)

PFD_{FE}=1.52x10^{-3}
HFT = 0

PFD_{SYS}= PFD_{S1}+PFD_{L}+PFD_{FE} =1.80x10^{-3}

SIL 2

Independent Validation check – NU271008_CAL



$PFD_{(SYS)}$	=	$PFD_{(S)}$		$PFD_{(L)}$		$PFD_{(FE)}$	
1.78E-03	=	1.24E-04	Valid	1.18E-04	Valid	1.03E-06	Valid
		2.07E-05	Valid			4.63E-05	Valid
						1.47E-03	Valid
Valid		1.44E-04	Valid	1.18E-04	Valid	1.52E-03	Valid

SPURIOUS TRIP SUMMARY

$S.Trip_{(SYS)}$	=	$S.Trip_{(S)}$		$S.Trip_{(L)}$		$S.Trip_{(FE)}$	
8.8	=	1164.8	Years	10.8	Years	37037.0	Years
Years		5.5E+02	Years		Years	8.1E+02	Years
			Years		Years	5.9E+01	Years

6.3 Detection of Dangerous Undetected Failures

For the sensor replacement, although the detection of DU failures is difficult, as this device contains no electronic components, most failures can be eliminated by proof testing. The device contains dual switches and defines the method of wiring back to the logic solver. It is noted from the design employed, that an additional detection has been designed into the system with the use of open circuit and cable short circuit detection, utilised on both channels, with each channel monitored by the logic solver.

In addition, another un-detected failure of these devices is the puncturing of the displacer, for this application the designers have specified a ptfe displacer which totally eliminates this DU failure mode.

The provision of the proofer allows simulated testing and avoids the dangerous testing required in taking the process into a dangerous state.

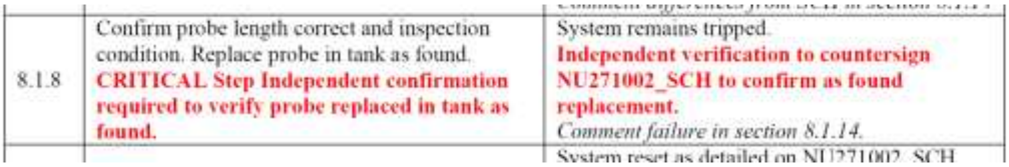
The operation of the proofer is such that it cannot be left in a dangerous undetected failure mode.

6.4 Elimination of Systematic Failures

Original systematic failures utilising radar technology revolved around incorrect calibration and sensor detection of the level. The systematic failures that can be expected form the use of the Magnetrol displacer switch technology revolve around miss-specification of the installed length, incorrect installation or maintenance activity were the switch is installed in the wrong location or at the wrong insertion length.

Action 7 of this FSA re-checked the installed length of the Magnetrol probe to ensure the insertion length is at the correct level of concern position.

NU271006_RPT - Shutdown Conditions SIF Proof Testing Procedure includes critical tasks that require independent checking when items that require to be removed from the tank for wet testing are replaced correctly.



		Comment differences from SCH in section 8.1.1
8.1.8	Confirm probe length correct and inspection condition. Replace probe in tank as found. **CRITICAL Step Independent confirmation required to verify probe replaced in tank as found.**	System remains tripped. **Independent verification to countersign NU271002_SCH to confirm as found replacement.** *Comment failure in section 8.1.14.*
		System reset as detailed on NU271002_SCH

6.5 Provision of Functional Safety

It is felt that functional safety has not be comprised by this modification. In fact it has probably improved the operator belief in the SIS as previously the original SIF was providing far too many spurious trips. To date this modification has almost eradicated spurious trips and maintained the functionality of the SIS. This has been achieved by changing from radar to vibronics on Tank 11 and radar to displace on the floating roof tanks 46 & 47.

With regard to the additional valves, as operation of any tank high level closes all SIS valves then the functionality remains unchanged.

7 ACTIONS

No.	Action	Action By	Status
1	Define the actual demand rate derived from the LOPA to Section 2 of the SRS	DSR	Complete
	Date	**Action History**	
	21/02/14	Revision E of SRS - Added to Section 3	

No.	Action	Action By	Status
2	Process Conditions require to be added to the SRS to identify any issues the process or process conditions could have on the SIS.	DSR	Complete
	Date	**Action History**	
	21/02/14	Revision E of SRS - Added to Section 3	

No.	Action	Action By	Status
3	A reference in the SRS to the document detailing Levels of Concerns and tank details should be added.	DSR	Complete
	Date	**Action History**	
	21/02/14	No reference to LoC document.	
	08/08/14	SRS Revision F includes references.	

No.	Action	Action By	Status
4	Add a description to the SRS as to how the ESV's can be operated manually in the event of an emergency.	DSR	Complete
	Date	**Action History**	
	21/02/14	Revision E of SRS - Added to Section 3	

No.	Action	Action By	Status
5	Add details to the SRS regarding the application software requirements.	DSR	Complete

Date	Action History
21/02/14	Revision E of SRS – Section 4.4.1 added. However, Revision History states it is Section 4.5.1, this requires correcting.
08/08/14	SRS Revision F now corrected.

No.	Action	Action By	Status
6	PILZ to revise their SIL Verification document to reflect revised and new SIF’s.	Pilz	Complete

Date	Action History
02/04/14	Version 3 of SIL Verification Report issued on 22.04.14

No.	Action	Action By	Status
7	During installation it is essential that the calculated length of activation be checked and confirmed and that the cable length be set accordingly.	NuStar	Complete

Date	Action History
16/04/14	From the SAT handover note the following was commented “Tanks 46 and 47 Magnetrols set up to calculated settings using data from tank drawings. A clarification check to be carried out when sufficient product in tank to gain access to floating deck. Height from Deck to 30mm up from base of displacer to be compared with physical tank dip.”
25.03.15	To be conducted during 2015 proof test
14.11.16	April 2016, confirmed that all lengths have been checked.

No.	Action	Action By	Status
8	Tag Number to be issued and added to specification.	DSR	Complete

Date	Action History
28/04/14	FSA Rev B – Still incomplete.
08/08/14	FSA Rev C – Specifications updated at revision F

No.	Action	Action By	Status
9	To be confirmed that the final element assembly is specified to ensure that there is sufficient oversizing allowance. Also NuStar to produce their generic specification for final elements for review.	NuStar	Complete

Date	Action History
08/08/14	FSA Rev C – Still incomplete
25.03.15	Reply from Neil Woodley "Presumably, although the main criteria for the 4” transfer line and 4” ESV was the transfer pump with a 4” outlet I’m not sure if the operation of the ESV against the full discharge pressure was a consideration (the system was well on its way to completion before I started coming back over), but the output pressure of a 4” pump can’t be too high, so I would think it is appropriately sized" Regards, Neil

No.	Action	Action By	Status
10	The Level of Concerns document to be updated to reflect changes from Radar to Magnetrol and Liquiphant.	NuStar	Complete

Date	Action History
08/08/14	FSA Rev C – Now complete, revised April 2014

No.	Action	Action By	Status
11	Update the loop drawings with descriptors of the P&F relay outputs	DBF	Complete

Date	Action History
08/08/14	Drawings have been revised to Rev C, but descriptions of output still incomplete. Drawings to be checked and approved with correct information
25.03.15	Revision D of drawings description added 28.08.14

No.	Action	Action By	Status
12	NuStar to provide drawings for review of the Ethanol SIF's.	NuStar	Complete

Date	Action History
08/08/14	FSA Rev C – Still incomplete
25/03/15	Drawings 54/70/432 Rev E, 54/70/357 F, 54/70/366 Rev B received and reviewed.

No.	Action	Action By	Status
13	At Revision A of this FSA there were no drawings to review for Tank 11 modifications	NuStar	Complete

Date	Action History
15/09/14	FSA Rev C – Still incomplete
25/03/15	Covered in Action 12

No.	Action	Action By	Status
14	PILZ to update their software design and testing documentation to reflect the changes.	PILZ	Complete

Date	Action History
28/04/14	FSA Rev B

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td rowspan="3">15</td><td colspan="2">Testing documentation to be revised and additional documentation as required to be produced and issued for review.</td><td>P&I Design Ltd</td><td>Complete</td></tr>
<tr><th>Date</th><th colspan="3">Action History</th></tr>
<tr><td>15/09/14
14/11/16</td><td colspan="3">Revision C of FSA – Documents still require updating.
NU271006_RPT_C - BF-SIS1 Shutdown Conditions SIF Proof Testing.pdf
NU271002_SCH_A - BF-SIS1 SIF Testing Matrix.pdf
NU271003_SCH_A - BF-SIS1 SIF Instrument Schedule.pdf
Testing documents revised, critical task independent checking added.</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td rowspan="3">16</td><td colspan="2">Provide Management of Functional Safety Document for review.</td><td>P&I Design Ltd</td><td>Complete</td></tr>
<tr><th>Date</th><th colspan="3">Action History</th></tr>
<tr><td>15/09/14
14/11/16</td><td colspan="3">Revision C of FSA – Documents still require updating.
Reviewed at Safety Committee meeting October 2015.
This action is a continually running lifecycle activity and will in future be managed by the Safety Panel.</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td rowspan="3">17</td><td colspan="2">On completion of testing, completed testing documentation to be issued for review by the FSA.</td><td>NuStar Energy / P&I Design Ltd</td><td>Complete</td></tr>
<tr><th>Date</th><th colspan="3">Action History</th></tr>
<tr><td>28/04/14</td><td colspan="3">FSA Rev B</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td rowspan="3">18</td><td colspan="2">On completion of testing, completed testing documentation to be issued for review by the FSA.</td><td>PILZ</td><td>Complete</td></tr>
<tr><th>Date</th><th colspan="3">Action History</th></tr>
<tr><td>28/04/14</td><td colspan="3">FSA Rev B</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td>19</td><td colspan="2">SIL Verification and design documentation for the Ethanol System to be provided for review by the FSA.</td><td>PILZ / NuStar</td><td>Complete</td></tr>
<tr><td></td><td><b>Date</b></td><td colspan="3"><b>Action History</b></td></tr>
<tr><td></td><td>15/09/14</td><td colspan="3">FSA Rev C – Still incomplete</td></tr>
<tr><td></td><td>25/03/15</td><td colspan="3">SIL Verification document reviewed for Magnetrol and Ethanol Tank 11 additions, SIL 2 capability maintained.</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td>20</td><td colspan="2">There is a minor typographical error in the seventh paragraph the word apmlifire” should read “amplifier”</td><td>PILZ</td><td>Complete</td></tr>
<tr><td></td><td><b>Date</b></td><td colspan="3"><b>Action History</b></td></tr>
<tr><td></td><td>15/09/14</td><td colspan="3">FSA Rev C – Still incomplete</td></tr>
<tr><td></td><td>25/03/15</td><td colspan="3">Completed</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td>21</td><td colspan="2">Section 5.2.3 and 5.2.4 details the common cause fraction and detected common cause failures, which have been defined as and $_{D}$ of 20% and 10% respectively. However, in the actual calculations the actual values used are 10% and 5 % respectively.</td><td>PILZ</td><td>Complete</td></tr>
<tr><td></td><td><b>Date</b></td><td colspan="3"><b>Action History</b></td></tr>
<tr><td></td><td>15/09/14</td><td colspan="3">FSA Rev C – Still incomplete</td></tr>
<tr><td></td><td>25/03/15</td><td colspan="3">Calculations revised</td></tr>
</table>

<table>
<tr><th>No.</th><th colspan="2">Action</th><th>Action By</th><th>Status</th></tr>
<tr><td>22</td><td colspan="2">The failure data used in the calculation of the Pekos valve body Section 6.7.1 is not the latest data available. The calculation requires revising utilising the newer less conservative data.</td><td>PILZ</td><td>Complete</td></tr>
<tr><td></td><td><b>Date</b></td><td colspan="3"><b>Action History</b></td></tr>
<tr><td></td><td>15/09/14</td><td colspan="3">PILZ SIL Verification Report - Version 5, 08/09/2014. Now corrected.</td></tr>
</table>

No.	Action	Action	Status

		By	
23	Section 7 SIF PFD calculations need to be revised as a result of Actions 21 & 22.	PILZ	Complete
	Date	**Action History**	
	15/09/14	Action 21, Still outstanding	
	25/03/15	Completed – See Action 21	

Signature Certificate

Document Reference: 6TP3LZIAH276W8JU66JCEA

RightSignature
Easy Online Document Signing

David Ransome
Party ID: CVTDKTITR28J5VJXWFXDKR
IP Address: 86.14.218.30
VERIFIED EMAIL: drr@pidesign.co.uk

Electronic Signature:

Multi-Factor
Digital Fingerprint Checksum 826ad94f640f1e25acebfac42d67efd1040b7b11

Timestamp	Audit
2016-11-14 04:29:14 -0800	All parties have signed document. Signed copies sent to: David Ransome and P I Design Ltd.
2016-11-14 04:29:14 -0800	Document signed by David Ransome (drr@pidesign.co.uk) with drawn signature. - 86.14.218.30
2016-11-14 04:28:36 -0800	Document viewed by David Ransome (drr@pidesign.co.uk). - 86.14.218.30
2016-11-14 04:28:13 -0800	Document created by P I Design Ltd (signature@pidesign.co.uk). - 86.14.218.30

This signature page provides a record of the online activity executing this contract.

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

NUSTAR

BELFAST TERMINAL

STORAGE TANKS OVERFILL

SAFETY INSTRUMENT SYSTEM

FUNCTIONAL SAFETY ASSESSMENT

STAGE 5

MODIFICATION OF SENSORS ON TANKS 4, 5 & 12

Rev	Date	By	Checked	Approved	Description
A	20.05.15	D.R. Ransome	DSR	DRR	FSA 5 Meeting
B	06.12.16	D.R. Ransome	DRansome	NuStar Safety Committee	Actions Updated and FSA CLOSED

Client Ref.

Document No.
NU271014_RPT

IF NOT SIGNED THIS DOCUMENT IS UNCONTROLLED

Contents

1 REVISION CONTROL

Rev	Description
A	Original Issue following FSA Meeting and initial review
B	Actions Updated and FSA CLOSED

2 SCOPE & DEFINITIONS

2.1 Scope

NuStar Energy – Belfast Terminal have an Independent High Level Alarm system to provide a SIL 2 rated automatic shutdown system to prevent 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
= Common Cause Failure Fraction
$_{D}$ = Detected Common Cause Failures
= Failure rate (per hour)
$_{D}$ = Dangerous Failure Rate
$_{DD}$ = Dangerous Detected Failures
$_{DU}$ = Dangerous Undetected Failures
$_{SD}$ = Safe Detected Failures
$_{DU}$ = Safe Undetected Failures

3 INTRODUCTION

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

3.1 Assumptions and Constraints

The existing SIS system has been in operation for a number of years, with various reviews and assessments having been previously conducted. This Functional Safety Assessment builds upon functional safety and lifecycle planning and management by assessing the proposed modifications to the system.

3.2 Proposed Modification

There is a requirement to perform an enhancement to the SIS. The elements of the modification are detailed below

3.2.1 Change Radar level sensor to Magnetrol on Tank 4, 5 & 12.

3.3 Team Membership

Date of Initial Review –20th May 2015 at NuStar Terminals, Belfast Terminal.

The FSA review team:-
NuStar Terminals:
Paul McGreevy - Terminal Manager
Davy Gamble – Operations Manager
Neil Woodley – Terminal Engineer
Dean Bannon – Electrical Technician
Darren Peck – EC&I Engineering Manager

P&I Design Ltd.
D.R. Ransome - FSA Chair

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

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. 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

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

The FSA will address the following:

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 4 was held on Wednesday 7th September 2011 at Belfast Terminal. It has been issued at Revisions A through to E. It is noted that the following actions are still incomplete.

Action 14: Final tag numbers to be added to the P&I Diagrams for re-issue.
NOW COMPLETE (Rev B of this FSA).

Action 15: SIS Instrumentation and Documentation to reflect tag numbering of P & I Drawings also Instrument Tagging should be consistent with P & I Drawings.
ALL DOCUMENTATION COMPLETED WITH THE EXCEPTION OF ETHANOL TANKS (Rev B of this FSA)

Action 16: All SIS documentation to be reviewed and ensure that it reflects P& I Drawings and installed system.
ALL DOCUMENTATION COMPLETED WITH THE EXCEPTION OF ETHANOL TANKS (Rev B of this FSA)

The above actions were discussed at this FSA meeting and Safety Panel meeting on 30th November 2016. NuStar Energy advised that they were still outstanding but progressing.

A FSA 5 modification of level sensors, was held 18th September 2013 at Belfast Terminal. It has been issued from Revisions A to D (25.03.2015). It is noted that the following actions are still incomplete.
NOW COMPLETE (Rev B of this FSA).

4.3 Proposed Modification

The FSA Meeting was held at the terminal on 20th May 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

Change Radar level sensor to Magnetrol on Tank 4, 5 & 12.

This is a further enhancement of the SIS, essentially the same as the modification conducted on Tanks 46 & 47.

4.5 Reason for the Modification

The existing radar transmitters on floating roof tanks have suffered from numerous spurious activations, Magnetrol displacer switches are to be utilised in place of the radar transmitters with a view of the different technology providing less false activations as demonstrated by the previous modification to Tanks 46 & 47.

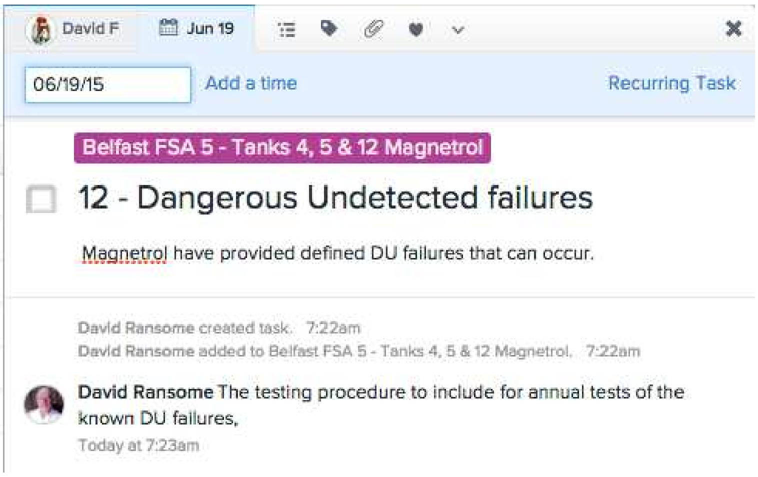
4.6 Hazards Which May Be Affected By The Modification

No change in the hazard perceived, just the method of detection.

The Magnetrol is in effect a simple device, as such it does not have any self diagnostics. However, they are fitted with two independent switch assemblies and as such require a signal conditioner. In order to accommodate this a four core (2 pair) cable from each switch will be wired to a P&F signal conditioner, together with the fitting of resistors to provide short and open circuit detection.

Unlike more sophisticated electronic sensors, the dangerous undetected failures can be defined and checks for these known failures are to be added to the testing procedures.

Action 12 – Dangerous Undetected Failures



06/19/15

Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

□ 12 - Dangerous Undetected failures

Magnetrol have provided defined DU failures that can occur.

David Ransome created task. 7:22am
David Ransome added to Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 7:22am

David Ransome The testing procedure to include for annual tests of the known DU failures,
Today at 7:23am

The logic solver and final elements are as original for Tanks 4, 5 & 12. Albeit the radar where analog inputs and the magnetrols will be digital.

The modification will involve a revision to the safety PLC Logic Solver program, checks must be performed on the complete SIS to ensure that no induced systematic failures have been introduced during the modification.

4.7 The Impact On Functional Safety

There was nothing identified as impacting on functional safety

4.8 Approvals For The Modification and Competencies

For the modification, NuStar 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.

Action 10 – NuStar Energy to complete MOC document.

4.9 Timescale and Timelines

At the FSA meeting it was stated that the design was nearing completion, installation underway and procurement and delivery of new sensor imminent. Commissioning is expected to take place at the end of June 2015.

4.10 Verification Process To Ensure Proper Implementation

Utilise normal lifecycle approach procedures with SAT and test procedures to ensure the modifications have not had any influence on the existing SIS. Following completion of the design it is to be reviewed as part of this FSA. The completed installation to be validated by proof testing.

4.11 SIS Lifecycle Requirements Of The Modification

It is felt there is no requirement to re LOPA or Risk Assess the process.

4.12 Documentation That Will Require Updating:

Safety Requirement Specification
SIL Verification Document
Software Design
Loop Drawings
Cable & Wiring Drawings
Verification Documentation
Management of Functional Safety Document
P & I D's

4.13 Operating Manuals And Documentation

Operating Procedures and TORA require updating together with new procedures for the Ethanol Transfer System.

4.14 Training Requirements Following Modification

As the system will operate as it does at present, no specific training is necessary.

5 REVIEW OF REVISED LIFECYCLE DOCUMENTATION

5.1 Safety Requirement Specification

The Safety Requirement Specification, NU271003_RPT, prior to the FSA for Tanks 46 & 47 was issued at Revision A - 13.09.11 and Issue B - 01.11.11. Following that modification it was issued at Revisions C – 18.09.13, D - 14.10.14, E – 21.02.14, F – 08.08.14.

The SRS has been revised to Revision G – 03.04.15 to include the modifications detailed in this FSA.

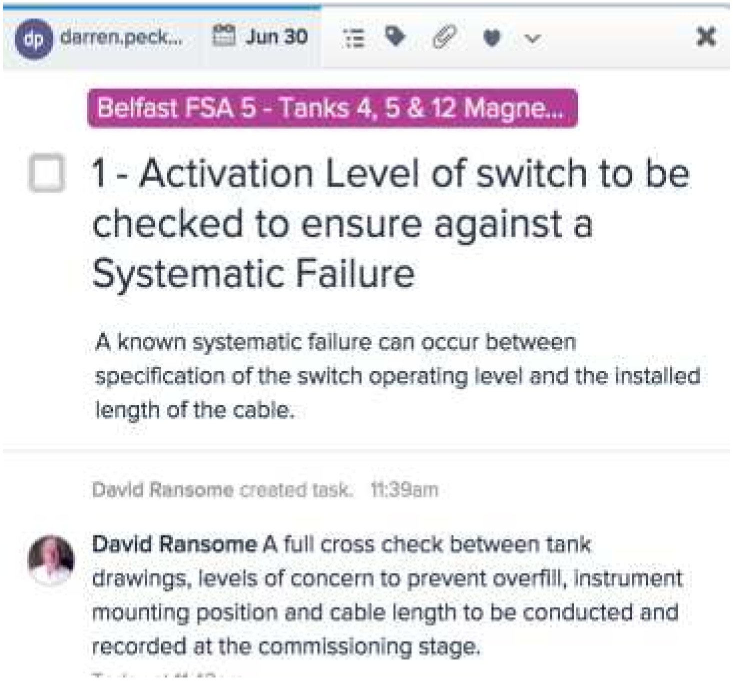
The Revision G of the SRS has been revised as follows:

Section 2.3.1 Revised to Magnetrol sensors for Tanks 4, 5 & 12 – system structure diagram.
Section 4.1 Revised for new sensor inputs

The previous FSA 5 (NU271011_RPT) conducted a full detailed review of the SRS as the FSA 4 did not formally review the SRS. The only changes to the SRS from that detailed review are as detailed above.

Sections 2.3.1 and 4.1 were reviewed at the FSA meeting and it was not considered necessary to perform a further detailed review of the SRS as this modification is identical to that of the previous FSA in relationship to the change of tank sensors.

However, in order to protect against a known systematic failure, the length of the magnetrol cable, hence the operating level of the switch was discussed and Action 1 raised to perform a check of the operating level in relationship to tank level. This to be conducted at the time of final commissioning.



□ 1 - Activation Level of switch to be checked to ensure against a Systematic Failure

A known systematic failure can occur between specification of the switch operating level and the installed length of the cable.

David Ransome created task. 11:39am

David Ransome A full cross check between tank drawings, levels of concern to prevent overfill, instrument mounting position and cable length to be conducted and recorded at the commissioning stage.

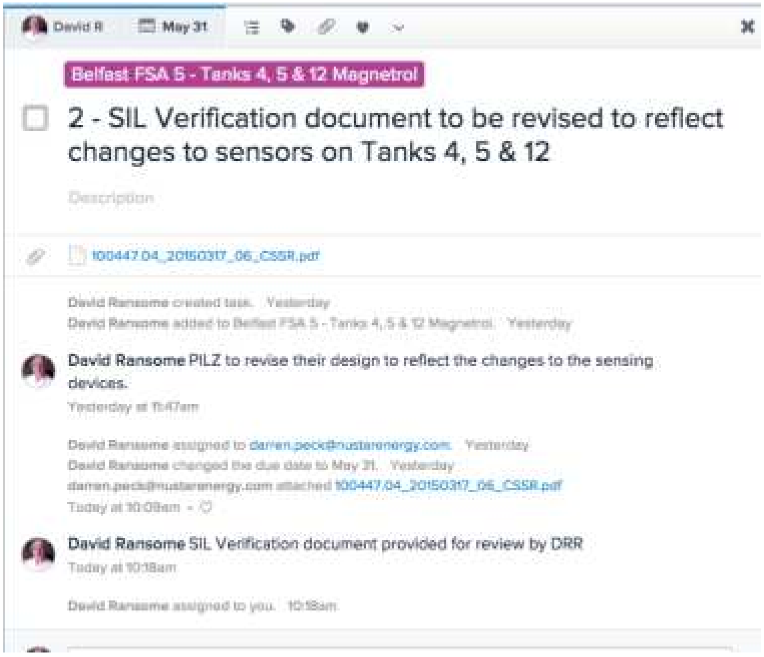
5.2 SIL Verification

PILZ have been commissioned by NuStar Energy to provide the SIL Verification document.

This document requires to be modified to reflect the changes to Tanks 4, 5 & 12.

ACTION 2: PILZ to revise their SIL Verification document to reflect revised SIF’s.

At the FSA meeting NuStar Energy provided the SIL verification document for review.



Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

□ 2 - SIL Verification document to be revised to reflect changes to sensors on Tanks 4, 5 & 12

Description

100447.04_20150317_06_CSSR.pdf

David Ransome created task. Yesterday
David Ransome added to Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. Yesterday

David Ransome PILZ to revise their design to reflect the changes to the sensing devices.
Yesterday at 11:47am

David Ransome assigned to darren.peck@nustarenergy.com. Yesterday
David Ransome changed the due date to May 31. Yesterday
darren.peck@nustarenergy.com attached 100447.04_20150317_06_CSSR.pdf
Today at 10:08am - ♡

David Ransome SIL Verification document provided for review by DRR
Today at 10:18am

David Ransome assigned to you. 10:18am

5.3 Design Documentation

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

5.3.1 Safety Requirement Specification

This is detailed in Section 5.1.

5.3.2 SIL Verification Document

This is detailed in Section 5.2.

5.3.3 Equipment Specifications

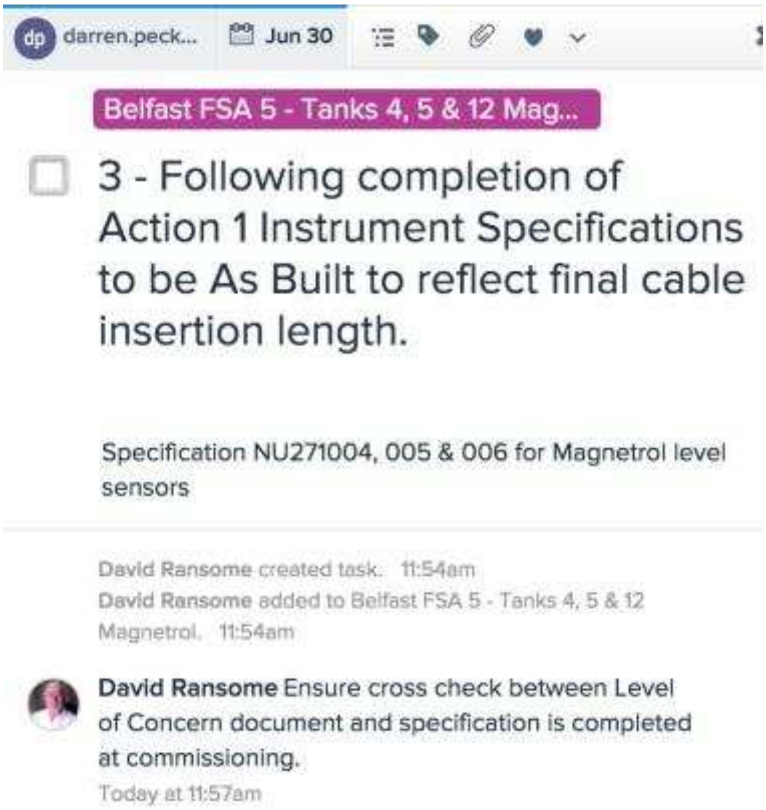
The following specifications have been produced and reviewed:

NU271004_SPC - Tank 4 Level Switch.
NU271005_SPC - Tank 5 Level Switch.
NU271006_SPC - Tank 12 Level Switch.

The specifications reviewed at the FSA were at Revision A. It was observed that the instruments were ordered with a 5m cable and at Revision A the final cable length and operating levels were not recorded on the specification.

See Previous ACTION 1: During installation it is essential that the calculated length of activation be checked and confirmed and that the cable length be set accordingly.

ACTION 3: Specifications to be updated AS BUILT with the correct cable length following ACTION 1.



Belfast FSA 5 - Tanks 4, 5 & 12 Mag...

☐ 3 - Following completion of Action 1 Instrument Specifications to be As Built to reflect final cable insertion length.

Specification NU271004, 005 & 006 for Magnetrol level sensors

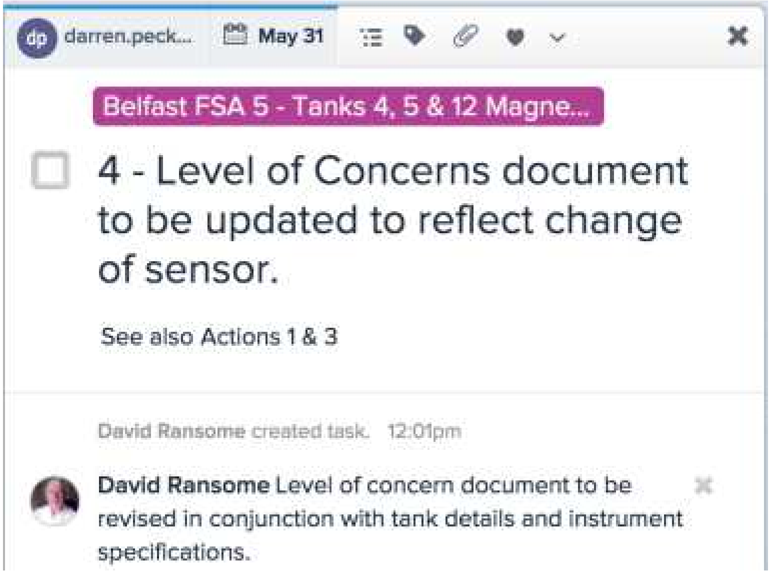
David Ransome created task. 11:54am
David Ransome added to Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 11:54am

David Ransome Ensure cross check between Level of Concern document and specification is completed at commissioning.
Today at 11:57am

5.3.4 IHLA Calculation Sheet

NuStar Energy have produced and maintain a document which details the Levels of Concerns for all tanks together with the activation point of high alarms and Independent High level Alarms (IHLA).

ACTION 4: The Level of Concerns document to be updated to reflect changes from Radar to Magnetrol.



Belfast FSA 5 - Tanks 4, 5 & 12 Magne...

□ 4 - Level of Concerns document to be updated to reflect change of sensor.

See also Actions 1 & 3

David Ransome created task. 12:01pm

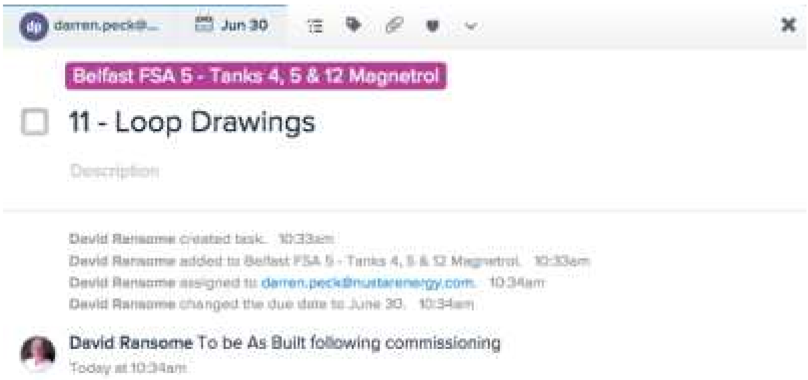
David Ransome Level of concern document to be revised in conjunction with tank details and instrument specifications.

5.3.5 Design Drawings

Tank 4, 5 & 12

New loop drawings NU271004_DWG - Tank 4, NU271005_DWG - Tank 5 & NU271006_DWG - Tank 12 have been produced and reviewed.

Action 11 – Loop drawings to be updated to As Built following commissioning.



Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

□ 11 - Loop Drawings

Description

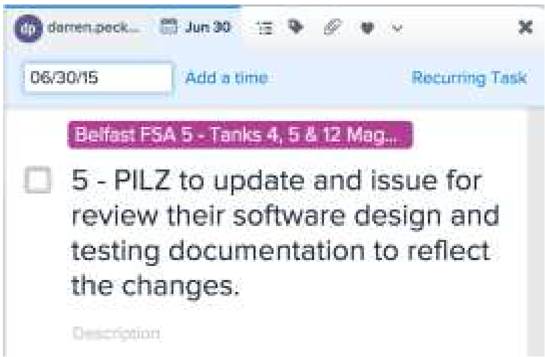
David Ransome created task. 10:33am
David Ransome added to Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 10:33am
David Ransome assigned to darren.peck@nustarenergy.com. 10:34am
David Ransome changed the due date to June 30. 10:34am

David Ransome To be As Built following commissioning
Today at 10:34am

5.3.6 Software Specification

PILZ produced the software for the SIS logic solver.

ACTION 5: PILZ to update and issue for review their software design and testing documentation to reflect the changes.



06/30/15

Belfast FSA 5 - Tanks 4, 5 & 12 Mag...

□ 5 - PILZ to update and issue for review their software design and testing documentation to reflect the changes.

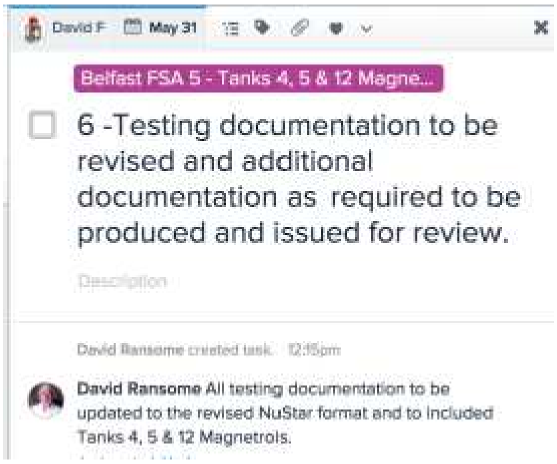
5.3.7 Testing and Inspection Documentation

In addition to the software testing documents detailed in 5.3.6 there is a series of testing documentation:

NU271004_RPT Testing Procedure
NU271005_RPT Documentation and Hardware Verification
NU271006_RPT Radar Functional Test Procedure
NU271007_RPT Analysis and Approval
NU271008_RPT Equipment Failures Test Procedure
NU271009_RPT Test Procedure
NU271010_RPT Vibronics Functional Test Procedure
NU271101_RPT Testing Witness Report

At Revision A of this FSA this documentation had not been updated for the modifications so could not be reviewed.

ACTION 6: Testing documentation to be revised and additional documentation as required to be produced and issued for review.



Belfast FSA 5 - Tanks 4, 5 & 12 Magne...

□ 6 -Testing documentation to be revised and additional documentation as required to be produced and issued for review.

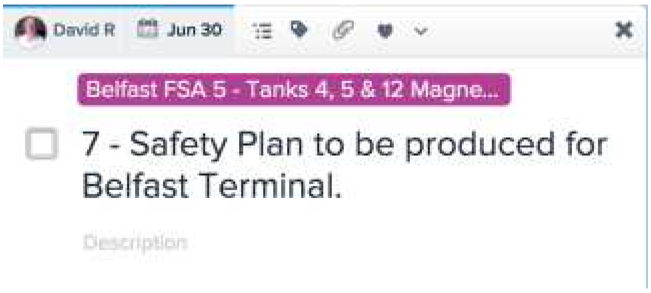
David Ransome created task. 12:15pm

David Ransome All testing documentation to be updated to the revised NuStar format and to included Tanks 4, 5 & 12 Magnetrols.

5.3.8 Management of Functional Safety Document

NuStar Energy Safety Committee have produced a new Policy Document and Safety Plan for each SIS.

ACTION 7: Safety Plan to be produced for Belfast Terminal.



Belfast FSA 5 - Tanks 4, 5 & 12 Magne...

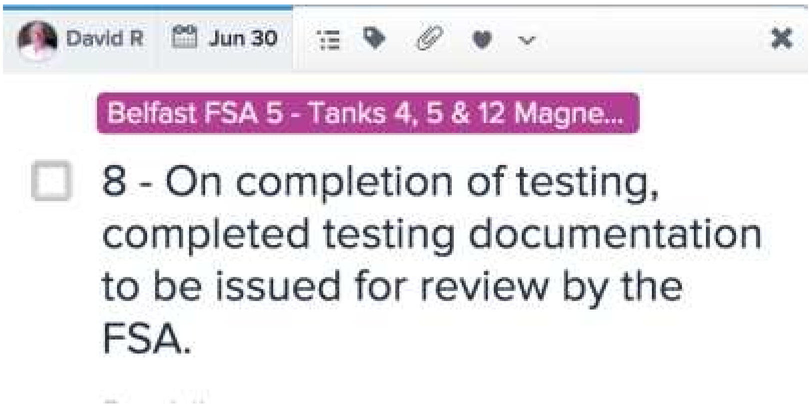
□ 7 - Safety Plan to be produced for Belfast Terminal.

5.4 Validation and Testing Documentation

Section 5.3 details the testing documentation currently available for the SIS.

This FSA will review the completed testing documentation following installation and validation.

ACTION 8: On completion of testing, completed testing documentation to be issued for review by the FSA.



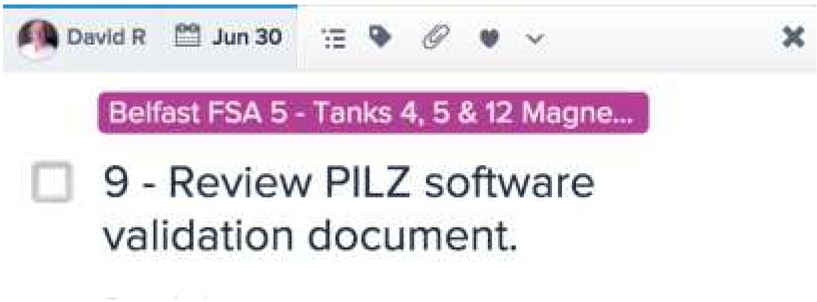
Belfast FSA 5 - Tanks 4, 5 & 12 Magne...

□ 8 - On completion of testing, completed testing documentation to be issued for review by the FSA.

5.5 Software Validation

Following software modification by PILZ a software validation document will be produced and issued to this FSA for review.

ACTION 9: Review PILZ software validation document.



Belfast FSA 5 - Tanks 4, 5 & 12 Magne...

□ 9 - Review PILZ software validation document.

5.6 Operation

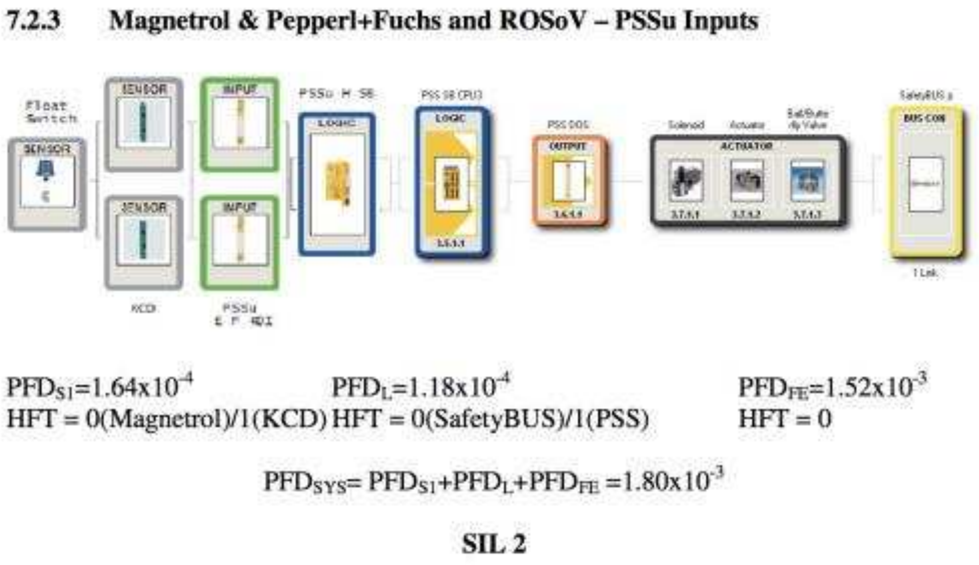
During the installation phase, operators are to be made familiar of the changes to the SIS. It is not envisaged that any additional training, other than on the job familiarisation will be required.

6 CONCLUSION

Revision A of this document was issued following changes to the SRS and before the modifications were completed. It serves as a request for the documentation required for review.

Revision B of this document was issued following implementation and testing of the SIS modification and with a suitable period of operational experience. The reason for the modification was as a result of spurious activations from radar sensing level instruments. This modification changed these sensors to displacer switch sensors. Since the original modification of Tanks 46 & 47 and this modification on Tanks 4, 5 & 12 the number of spurious activations as reduced significantly and much more in line with what would be expected.

As for the SIL and pfd, the modification has not comprised these figures as seen below:



7.2.3 Magnetrol & Pepperl+Fuchs and ROSoV – PSSu Inputs

$PFD_{S1}=1.64x10^{-4}$ $PFD_{L}=1.18x10^{-4}$ $PFD_{FE}=1.52x10^{-3}$
HFT = 0(Magnetrol)/1(KCD) HFT = 0(SafetyBUS)/1(PSS) HFT = 0

$$PFD_{SYS}= PFD_{S1}+PFD_{L}+PFD_{FE} =1.80x10^{-3}$$

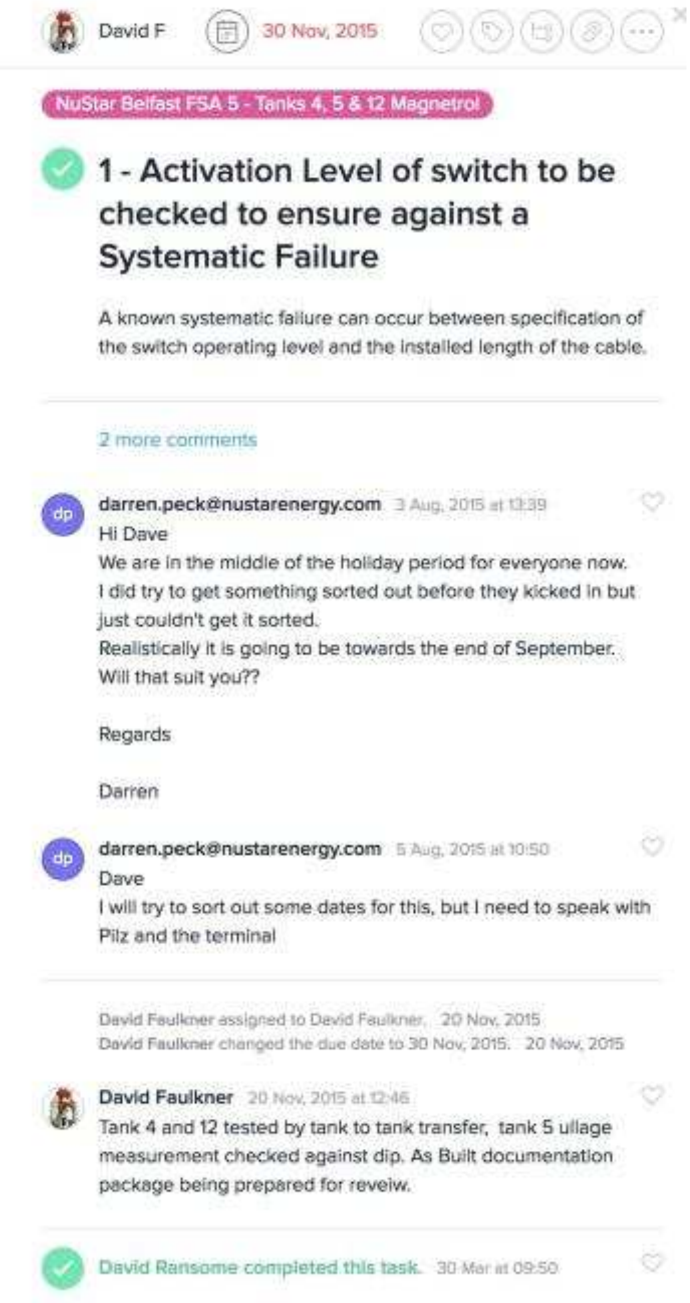
SIL 2

It is therefore considered that the modification was a success in not compromising functional safety, preserving a SIL 2 protection and becoming more reliable as a result of decreasing unwanted spurious activations.

Section 7 details the progress of all actions.

7 ACTIONS

Detailed below are details of all actions raised during this FSA.



David F 30 Nov, 2015

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

1 - Activation Level of switch to be checked to ensure against a Systematic Failure

A known systematic failure can occur between specification of the switch operating level and the installed length of the cable.

2 more comments

darren.peck@nustarenergy.com 3 Aug, 2015 at 13:39
Hi Dave
We are in the middle of the holiday period for everyone now.
I did try to get something sorted out before they kicked in but just couldn't get it sorted.
Realistically it is going to be towards the end of September.
Will that suit you??

Regards

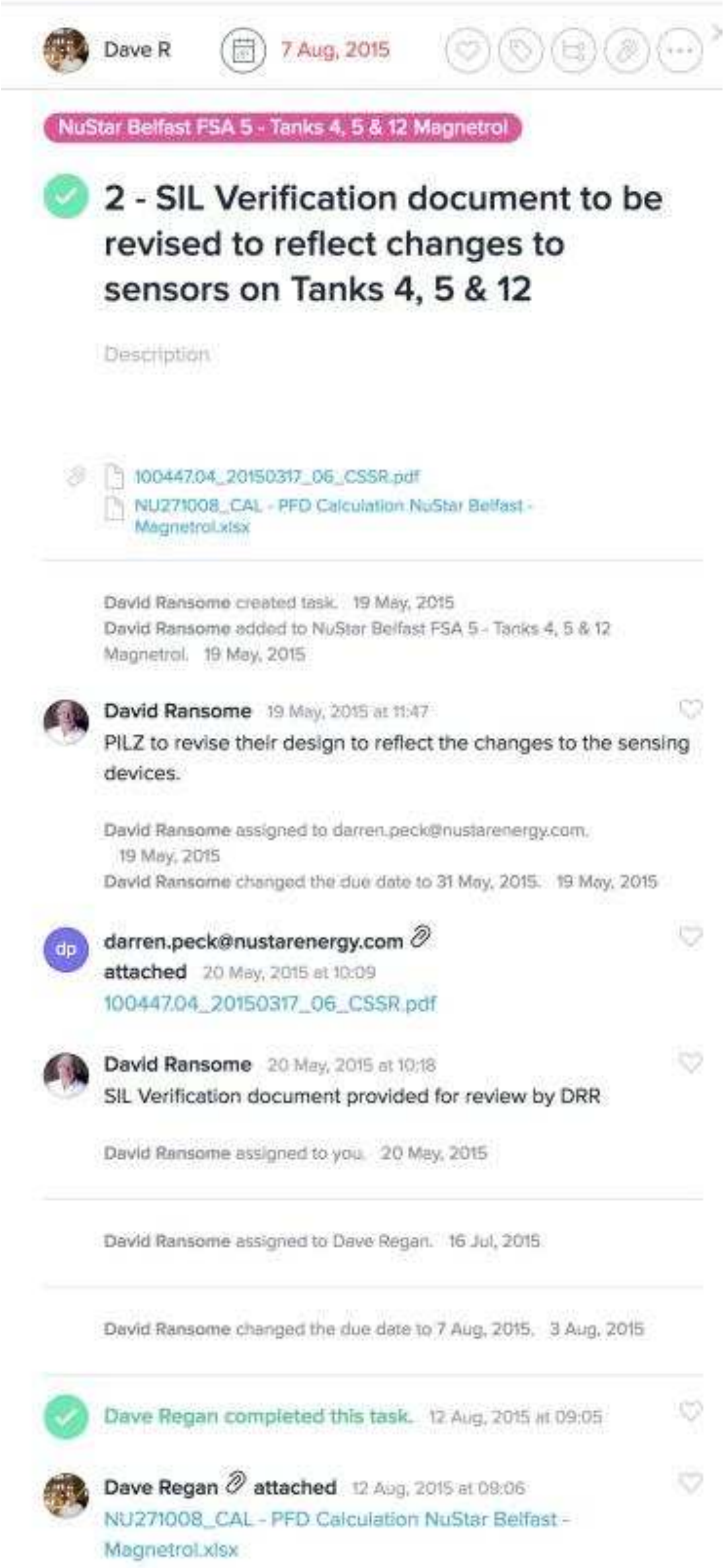
Darren

darren.peck@nustarenergy.com 5 Aug, 2015 at 10:50
Dave
I will try to sort out some dates for this, but I need to speak with Pilz and the terminal

David Faulkner assigned to David Faulkner. 20 Nov, 2015
David Faulkner changed the due date to 30 Nov, 2015. 20 Nov, 2015

David Faulkner 20 Nov, 2015 at 12:46
Tank 4 and 12 tested by tank to tank transfer, tank 5 ullage measurement checked against dip. As Built documentation package being prepared for reveiw.

David Ransome completed this task. 30 Mar at 09:50



Dave R 7 Aug, 2015

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 2 - SIL Verification document to be revised to reflect changes to sensors on Tanks 4, 5 & 12

Description

100447.04_20150317_06_CSSR.pdf
NU271008_CAL - PFD Calculation NuStar Belfast - Magnetrol.xlsx

David Ransome created task. 19 May, 2015
David Ransome added to NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 19 May, 2015

David Ransome 19 May, 2015 at 11:47
PILZ to revise their design to reflect the changes to the sensing devices.

David Ransome assigned to darren.peck@nustarenergy.com. 19 May, 2015
David Ransome changed the due date to 31 May, 2015. 19 May, 2015

darren.peck@nustarenergy.com attached 20 May, 2015 at 10:09
100447.04_20150317_06_CSSR.pdf

David Ransome 20 May, 2015 at 10:18
SIL Verification document provided for review by DRR

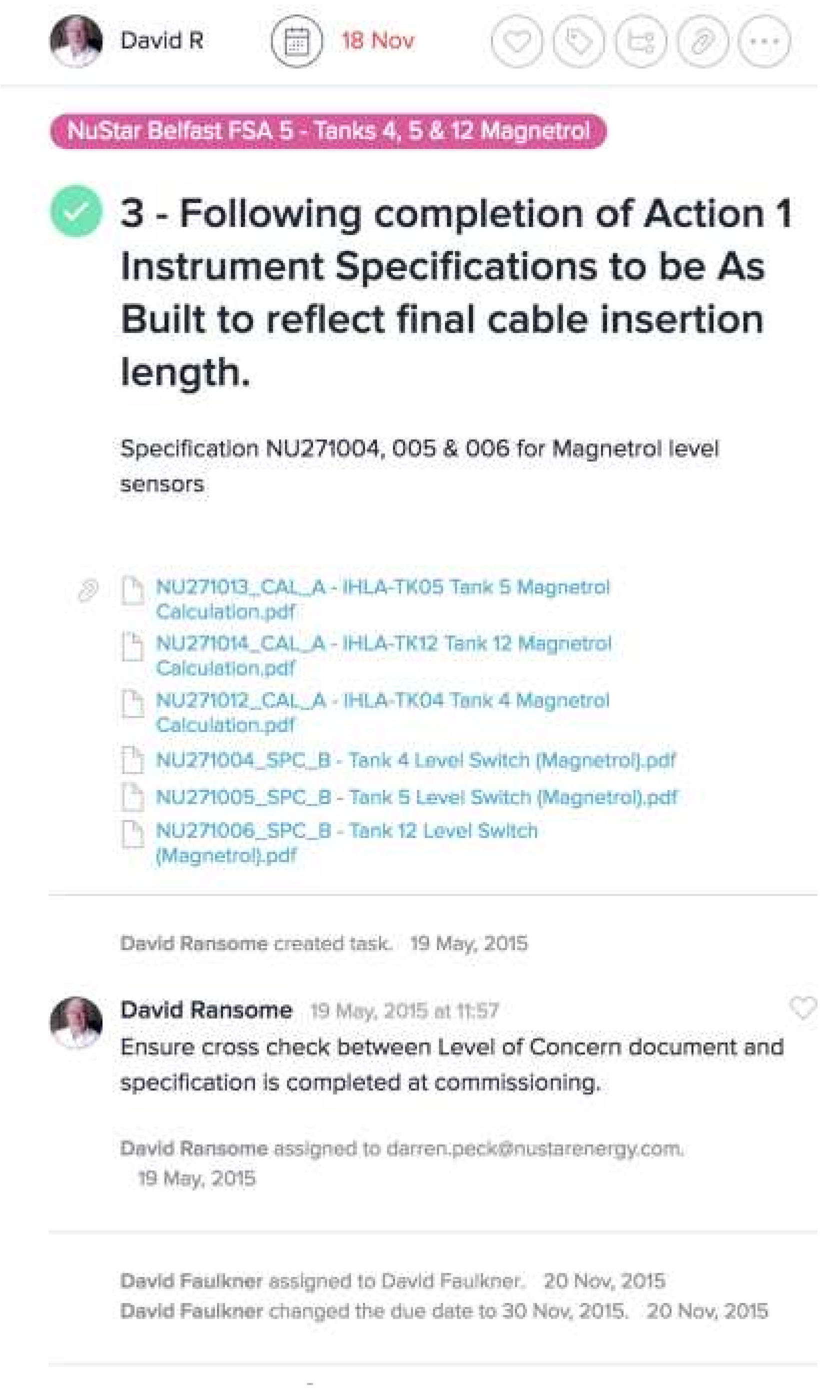
David Ransome assigned to you. 20 May, 2015

David Ransome assigned to Dave Regan. 16 Jul, 2015

David Ransome changed the due date to 7 Aug, 2015. 3 Aug, 2015

✓ Dave Regan completed this task. 12 Aug, 2015 at 09:05

Dave Regan attached 12 Aug, 2015 at 09:06
NU271008_CAL - PFD Calculation NuStar Belfast - Magnetrol.xlsx



David R 18 Nov

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 3 - Following completion of Action 1 Instrument Specifications to be As Built to reflect final cable insertion length.

Specification NU271004, 005 & 006 for Magnetrol level sensors

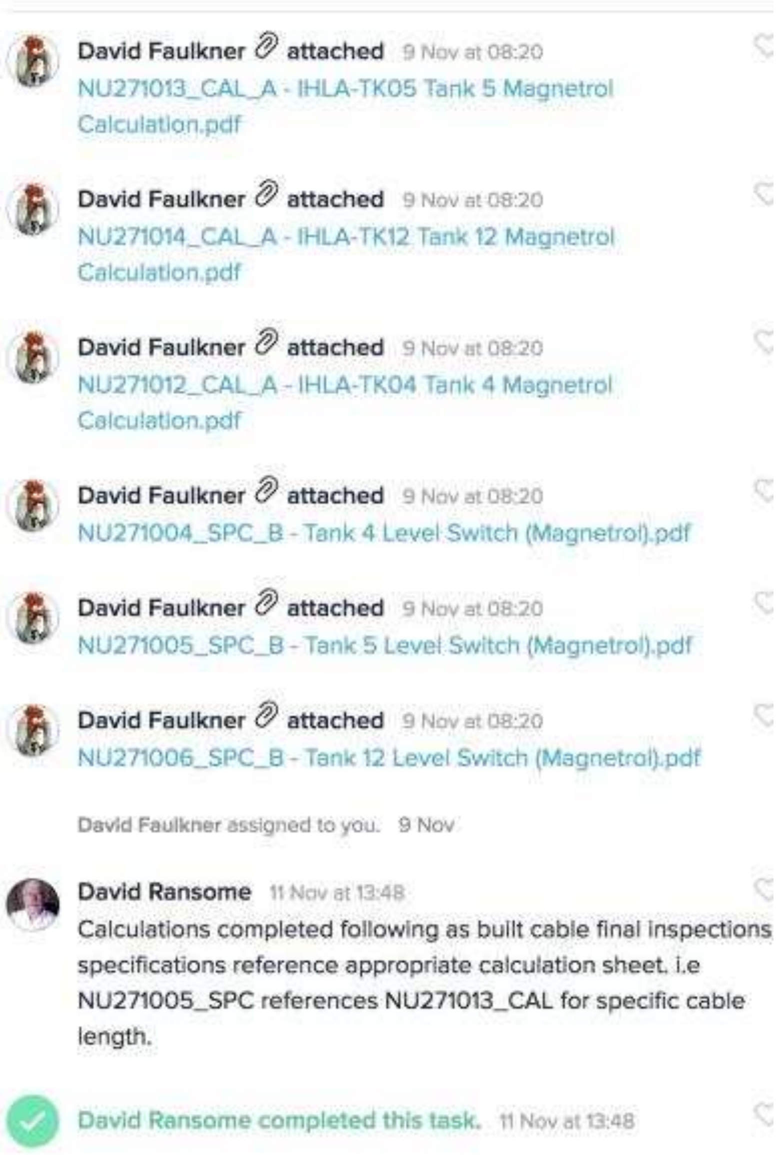
- NU271013_CAL_A - IHLA-TK05 Tank 5 Magnetrol Calculation.pdf
- NU271014_CAL_A - IHLA-TK12 Tank 12 Magnetrol Calculation.pdf
- NU271012_CAL_A - IHLA-TK04 Tank 4 Magnetrol Calculation.pdf
- NU271004_SPC_B - Tank 4 Level Switch (Magnetrol).pdf
- NU271005_SPC_B - Tank 5 Level Switch (Magnetrol).pdf
- NU271006_SPC_B - Tank 12 Level Switch (Magnetrol).pdf

David Ransome created task. 19 May, 2015

David Ransome 19 May, 2015 at 11:57
Ensure cross check between Level of Concern document and specification is completed at commissioning.

David Ransome assigned to darren.peck@nustarenergy.com. 19 May, 2015

David Faulkner assigned to David Faulkner. 20 Nov, 2015
David Faulkner changed the due date to 30 Nov, 2015. 20 Nov, 2015



David Faulkner attached 9 Nov at 08:20
NU271013_CAL_A - IHLA-TK05 Tank 5 Magnetrol Calculation.pdf

David Faulkner attached 9 Nov at 08:20
NU271014_CAL_A - IHLA-TK12 Tank 12 Magnetrol Calculation.pdf

David Faulkner attached 9 Nov at 08:20
NU271012_CAL_A - IHLA-TK04 Tank 4 Magnetrol Calculation.pdf

David Faulkner attached 9 Nov at 08:20
NU271004_SPC_B - Tank 4 Level Switch (Magnetrol).pdf

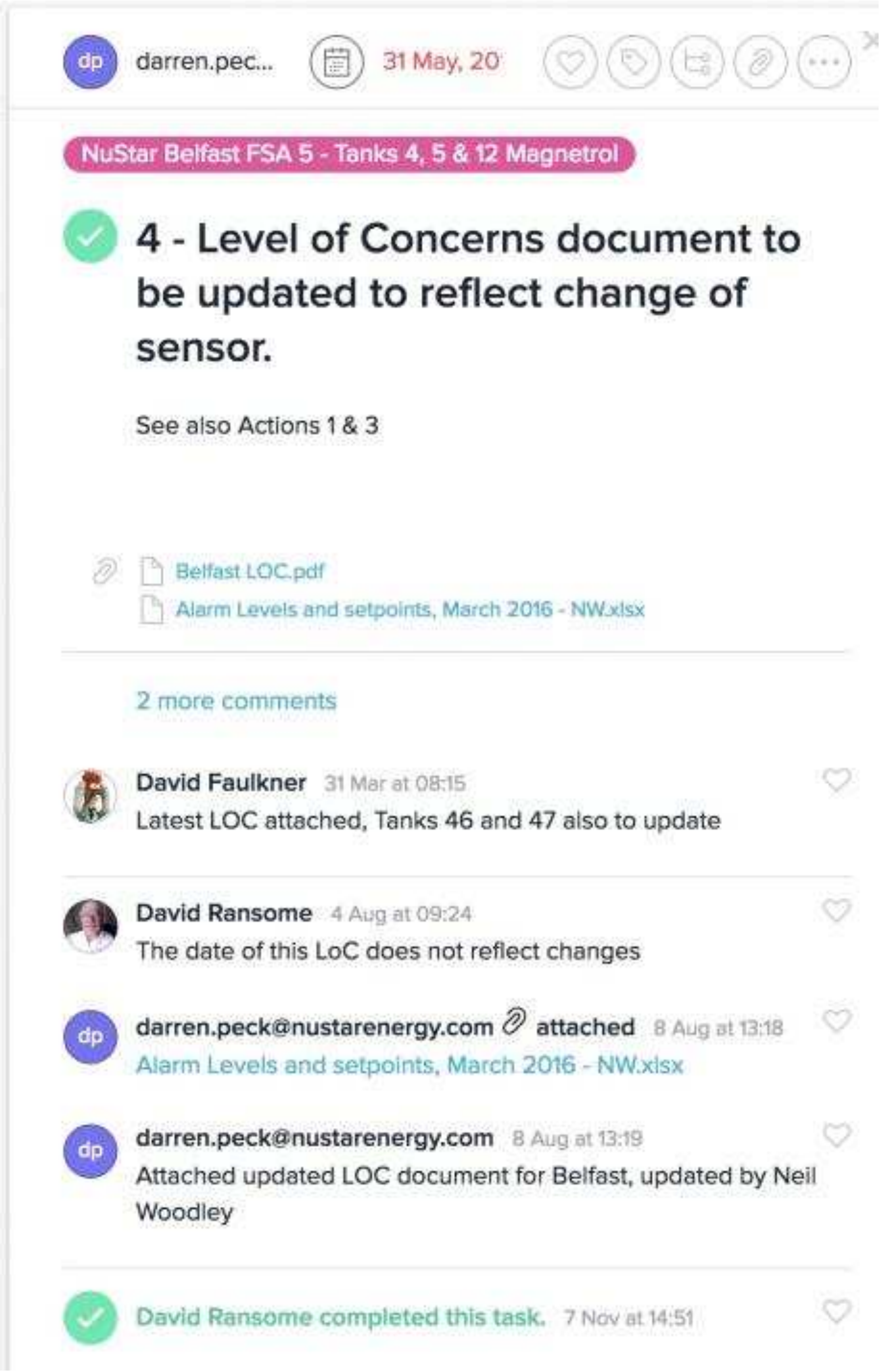
David Faulkner attached 9 Nov at 08:20
NU271005_SPC_B - Tank 5 Level Switch (Magnetrol).pdf

David Faulkner attached 9 Nov at 08:20
NU271006_SPC_B - Tank 12 Level Switch (Magnetrol).pdf

David Faulkner assigned to you. 9 Nov

David Ransome 11 Nov at 13:48
Calculations completed following as built cable final inspections specifications reference appropriate calculation sheet. i.e NU271005_SPC references NU271013_CAL for specific cable length.

David Ransome completed this task. 11 Nov at 13:48



dp darren.pec... 31 May, 20

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 4 - Level of Concerns document to be updated to reflect change of sensor.

See also Actions 1 & 3

Belfast LOC.pdf
Alarm Levels and setpoints, March 2016 - NW.xlsx

2 more comments

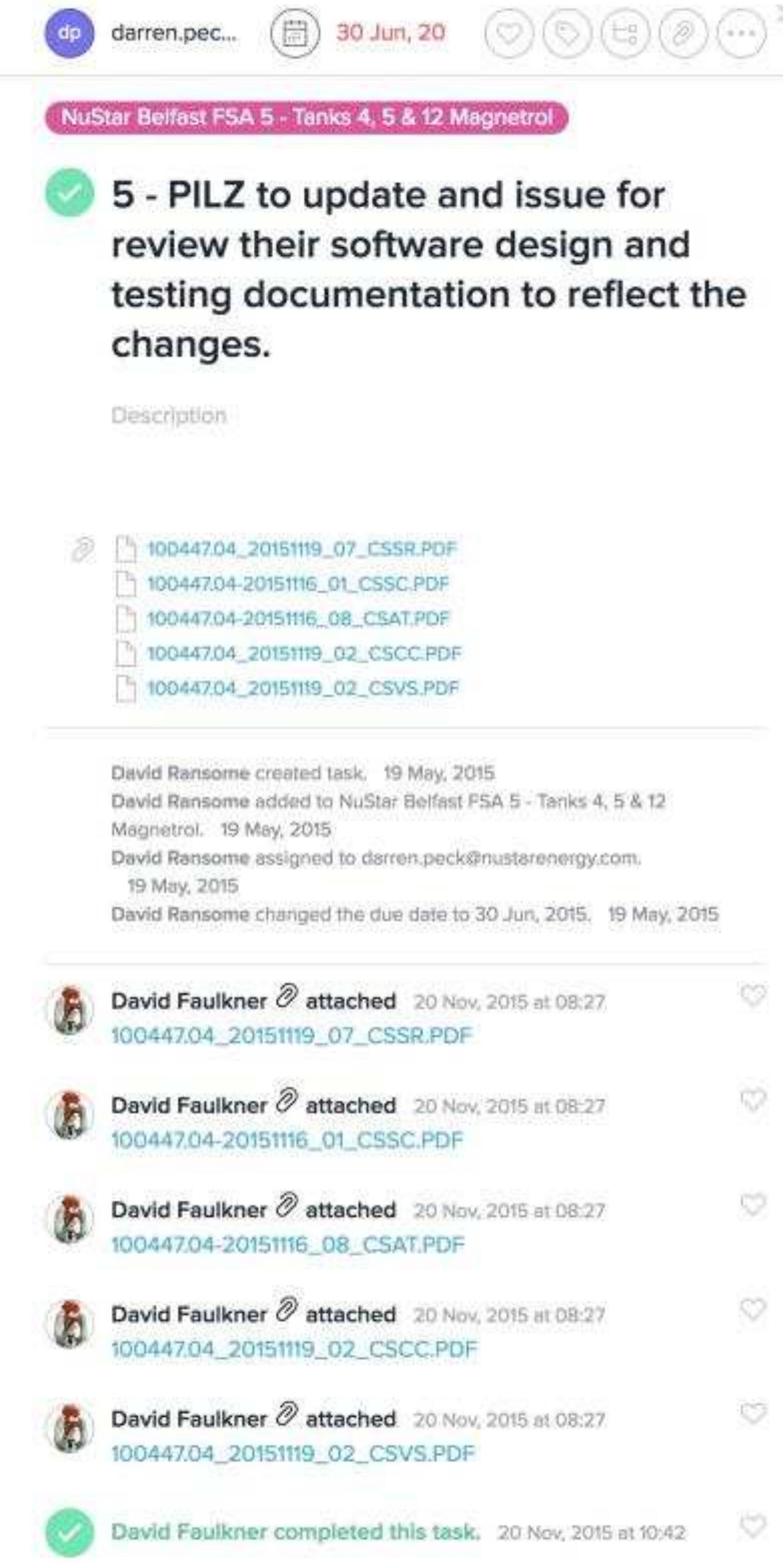
David Faulkner 31 Mar at 08:15
Latest LOC attached, Tanks 46 and 47 also to update

David Ransome 4 Aug at 09:24
The date of this LoC does not reflect changes

darren.peck@nustarenergy.com attached 8 Aug at 13:18
Alarm Levels and setpoints, March 2016 - NW.xlsx

darren.peck@nustarenergy.com 8 Aug at 13:19
Attached updated LOC document for Belfast, updated by Neil Woodley

✓ David Ransome completed this task. 7 Nov at 14:51



NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 5 - PILZ to update and issue for review their software design and testing documentation to reflect the changes.

Description

- 100447.04_20151119_07_CSSR.PDF
- 100447.04-20151116_01_CSSC.PDF
- 100447.04-20151116_08_CSAT.PDF
- 100447.04_20151119_02_CSCC.PDF
- 100447.04_20151119_02_CSVS.PDF

David Ransome created task. 19 May, 2015
David Ransome added to NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 19 May, 2015
David Ransome assigned to darren.peck@nustarenergy.com. 19 May, 2015
David Ransome changed the due date to 30 Jun, 2015. 19 May, 2015

David Faulkner attached 20 Nov, 2015 at 08:27
100447.04_20151119_07_CSSR.PDF

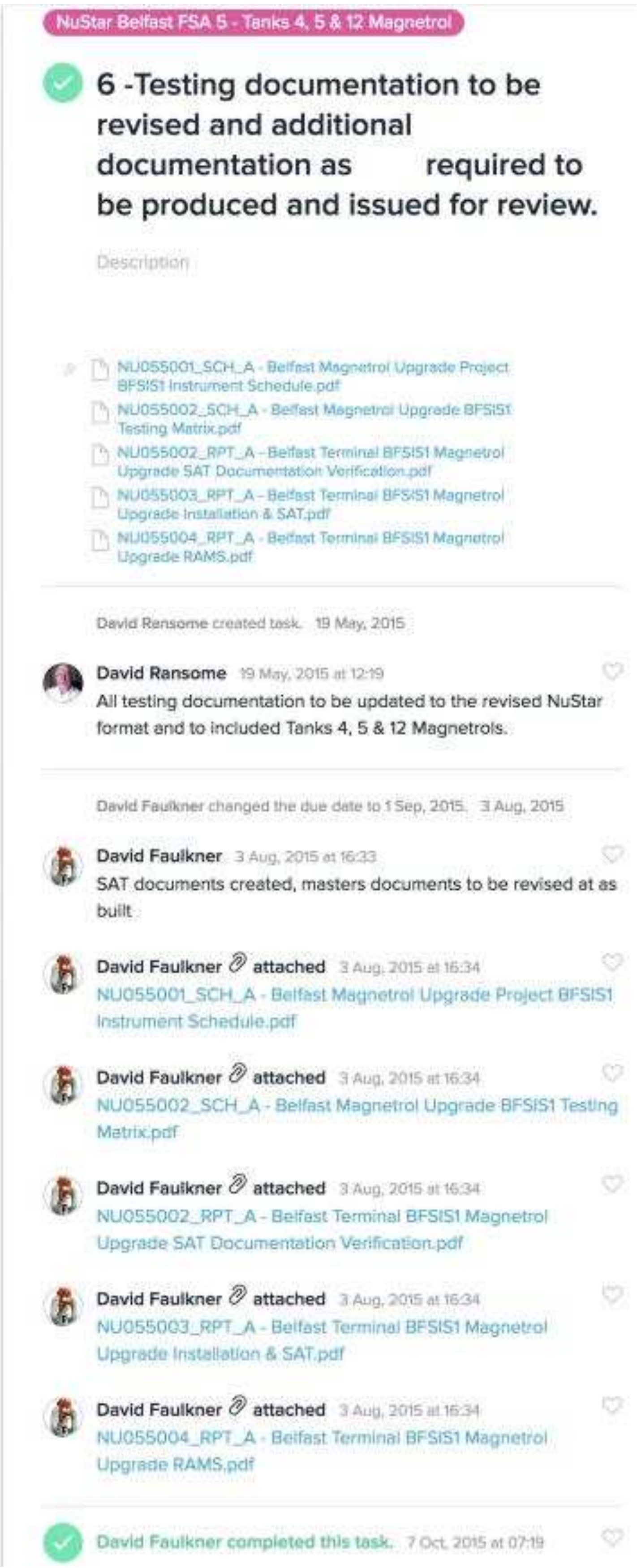
David Faulkner attached 20 Nov, 2015 at 08:27
100447.04-20151116_01_CSSC.PDF

David Faulkner attached 20 Nov, 2015 at 08:27
100447.04-20151116_08_CSAT.PDF

David Faulkner attached 20 Nov, 2015 at 08:27
100447.04_20151119_02_CSCC.PDF

David Faulkner attached 20 Nov, 2015 at 08:27
100447.04_20151119_02_CSVS.PDF

✓ David Faulkner completed this task. 20 Nov, 2015 at 10:42



NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 6 -Testing documentation to be revised and additional documentation as required to be produced and issued for review.

Description

- NU055001_SCH_A - Belfast Magnetrol Upgrade Project BFSIS1 Instrument Schedule.pdf
- NU055002_SCH_A - Belfast Magnetrol Upgrade BFSIS1 Testing Matrix.pdf
- NU055002_RPT_A - Belfast Terminal BFSIS1 Magnetrol Upgrade SAT Documentation Verification.pdf
- NU055003_RPT_A - Belfast Terminal BFSIS1 Magnetrol Upgrade Installation & SAT.pdf
- NU055004_RPT_A - Belfast Terminal BFSIS1 Magnetrol Upgrade RAMS.pdf

David Ransome created task. 19 May, 2015

David Ransome 19 May, 2015 at 12:19
All testing documentation to be updated to the revised NuStar format and to included Tanks 4, 5 & 12 Magnetrols.

David Faulkner changed the due date to 1 Sep, 2015. 3 Aug, 2015

David Faulkner 3 Aug, 2015 at 16:33
SAT documents created, masters documents to be revised at as built

David Faulkner attached 3 Aug, 2015 at 16:34
NU055001_SCH_A - Belfast Magnetrol Upgrade Project BFSIS1 Instrument Schedule.pdf

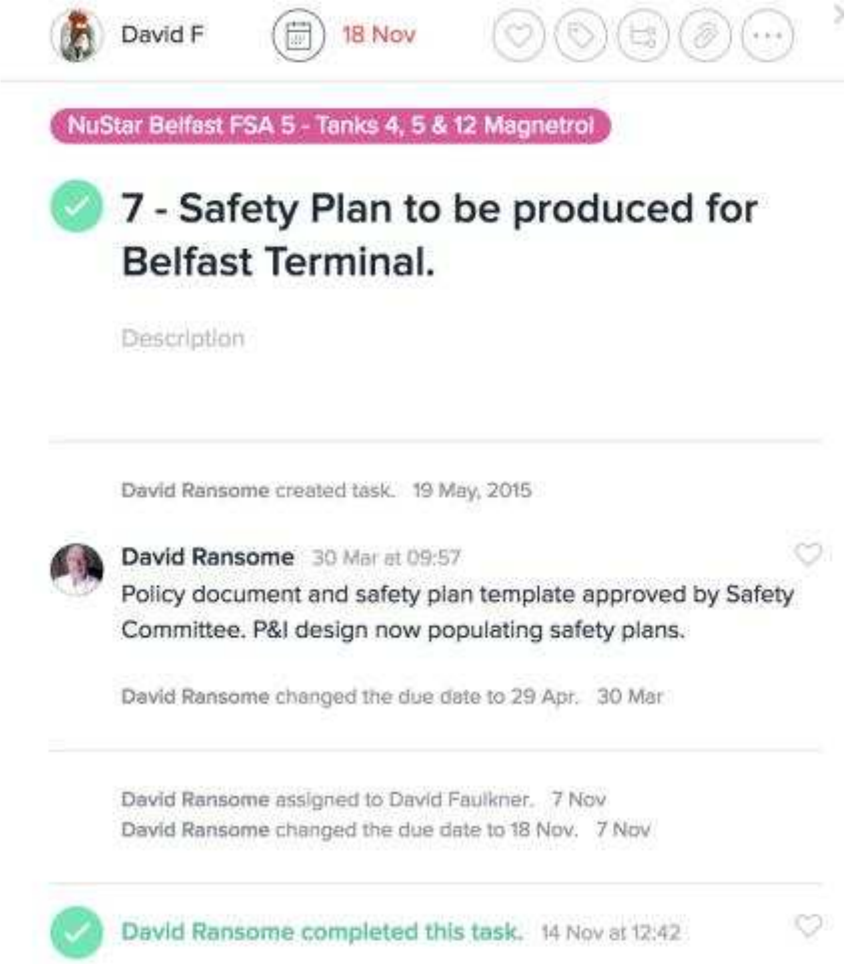
David Faulkner attached 3 Aug, 2015 at 16:34
NU055002_SCH_A - Belfast Magnetrol Upgrade BFSIS1 Testing Matrix.pdf

David Faulkner attached 3 Aug, 2015 at 16:34
NU055002_RPT_A - Belfast Terminal BFSIS1 Magnetrol Upgrade SAT Documentation Verification.pdf

David Faulkner attached 3 Aug, 2015 at 16:34
NU055003_RPT_A - Belfast Terminal BFSIS1 Magnetrol Upgrade Installation & SAT.pdf

David Faulkner attached 3 Aug, 2015 at 16:34
NU055004_RPT_A - Belfast Terminal BFSIS1 Magnetrol Upgrade RAMS.pdf

✓ David Faulkner completed this task. 7 Oct, 2015 at 07:19



David F 18 Nov

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 7 - Safety Plan to be produced for Belfast Terminal.

Description

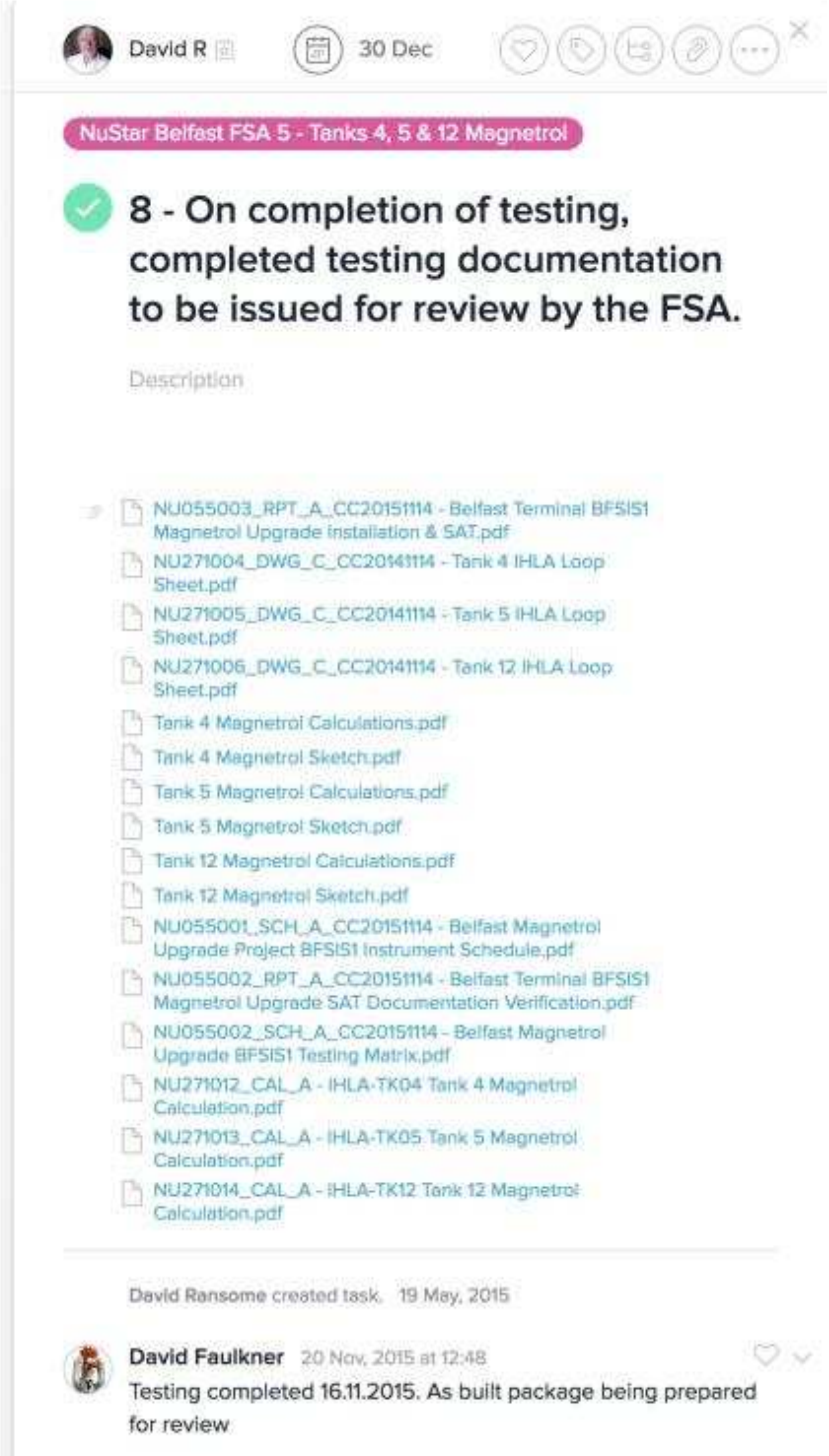
David Ransome created task. 19 May, 2015

David Ransome 30 Mar at 09:57
Policy document and safety plan template approved by Safety Committee. P&I design now populating safety plans.

David Ransome changed the due date to 29 Apr. 30 Mar

David Ransome assigned to David Faulkner. 7 Nov
David Ransome changed the due date to 18 Nov. 7 Nov

✓ David Ransome completed this task. 14 Nov at 12:42



NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

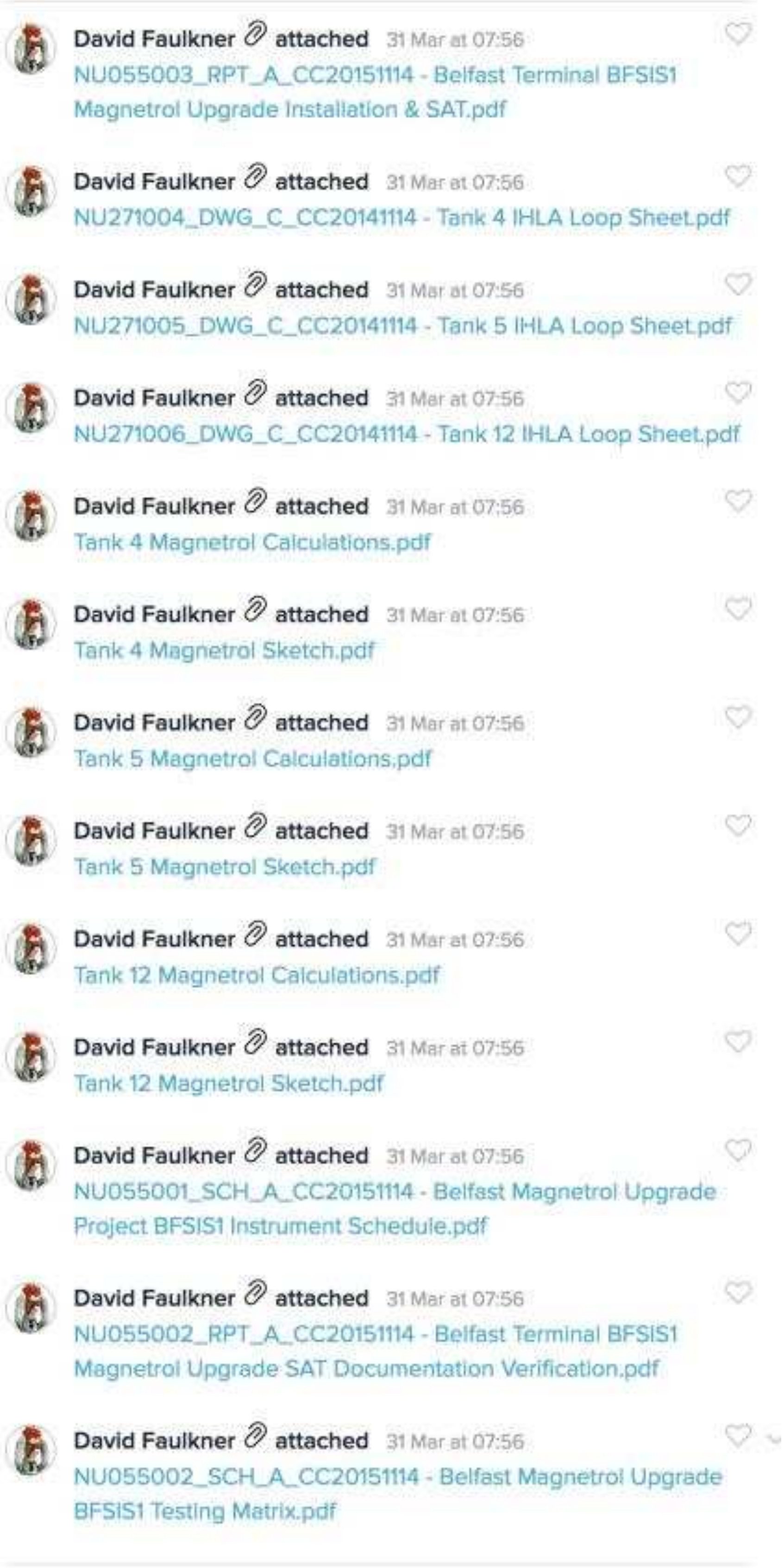
✓ 8 - On completion of testing, completed testing documentation to be issued for review by the FSA.

Description

- NU055003_RPT_A_CC20151114 - Belfast Terminal BFSIS1 Magnetrol Upgrade installation & SAT.pdf
- NU271004_DWG_C_CC20141114 - Tank 4 IHLA Loop Sheet.pdf
- NU271005_DWG_C_CC20141114 - Tank 5 IHLA Loop Sheet.pdf
- NU271006_DWG_C_CC20141114 - Tank 12 IHLA Loop Sheet.pdf
- Tank 4 Magnetrol Calculations.pdf
- Tank 4 Magnetrol Sketch.pdf
- Tank 5 Magnetrol Calculations.pdf
- Tank 5 Magnetrol Sketch.pdf
- Tank 12 Magnetrol Calculations.pdf
- Tank 12 Magnetrol Sketch.pdf
- NU055001_SCH_A_CC20151114 - Belfast Magnetrol Upgrade Project BFSIS1 Instrument Schedule.pdf
- NU055002_RPT_A_CC20151114 - Belfast Terminal BFSIS1 Magnetrol Upgrade SAT Documentation Verification.pdf
- NU055002_SCH_A_CC20151114 - Belfast Magnetrol Upgrade BFSIS1 Testing Matrix.pdf
- NU271012_CAL_A - IHLA-TK04 Tank 4 Magnetrol Calculation.pdf
- NU271013_CAL_A - IHLA-TK05 Tank 5 Magnetrol Calculation.pdf
- NU271014_CAL_A - IHLA-TK12 Tank 12 Magnetrol Calculation.pdf

David Ransome created task. 19 May, 2015

David Faulkner 20 Nov, 2015 at 12:48
Testing completed 16.11.2015. As built package being prepared for review



David Faulkner attached 31 Mar at 07:56
NU055003_RPT_A_CC20151114 - Belfast Terminal BFSIS1 Magnetrol Upgrade Installation & SAT.pdf

David Faulkner attached 31 Mar at 07:56
NU271004_DWG_C_CC20141114 - Tank 4 IHLA Loop Sheet.pdf

David Faulkner attached 31 Mar at 07:56
NU271005_DWG_C_CC20141114 - Tank 5 IHLA Loop Sheet.pdf

David Faulkner attached 31 Mar at 07:56
NU271006_DWG_C_CC20141114 - Tank 12 IHLA Loop Sheet.pdf

David Faulkner attached 31 Mar at 07:56
Tank 4 Magnetrol Calculations.pdf

David Faulkner attached 31 Mar at 07:56
Tank 4 Magnetrol Sketch.pdf

David Faulkner attached 31 Mar at 07:56
Tank 5 Magnetrol Calculations.pdf

David Faulkner attached 31 Mar at 07:56
Tank 5 Magnetrol Sketch.pdf

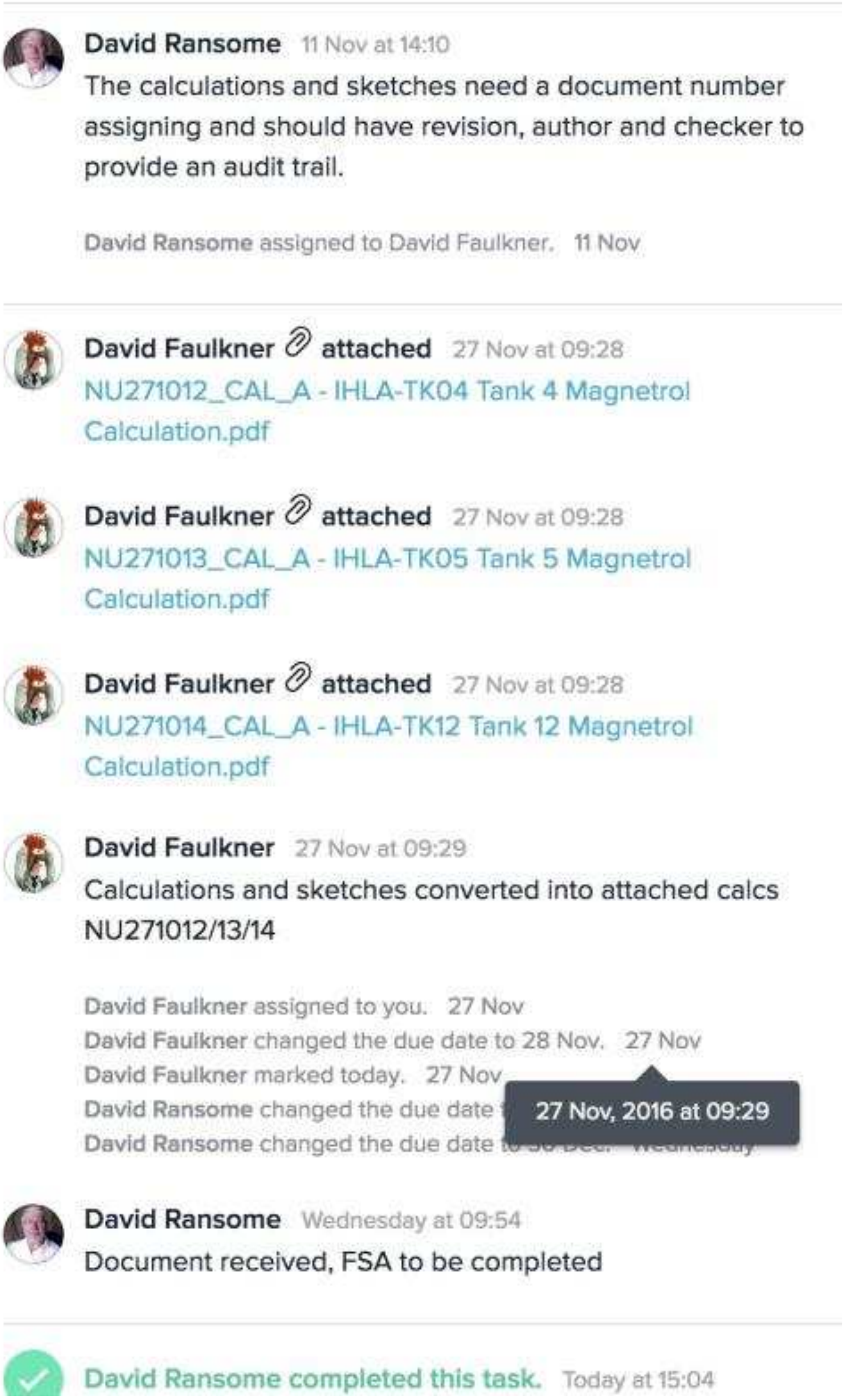
David Faulkner attached 31 Mar at 07:56
Tank 12 Magnetrol Calculations.pdf

David Faulkner attached 31 Mar at 07:56
Tank 12 Magnetrol Sketch.pdf

David Faulkner attached 31 Mar at 07:56
NU055001_SCH_A_CC20151114 - Belfast Magnetrol Upgrade Project BFSIS1 Instrument Schedule.pdf

David Faulkner attached 31 Mar at 07:56
NU055002_RPT_A_CC20151114 - Belfast Terminal BFSIS1 Magnetrol Upgrade SAT Documentation Verification.pdf

David Faulkner attached 31 Mar at 07:56
NU055002_SCH_A_CC20151114 - Belfast Magnetrol Upgrade BFSIS1 Testing Matrix.pdf



David Ransome 11 Nov at 14:10
The calculations and sketches need a document number assigning and should have revision, author and checker to provide an audit trail.

David Ransome assigned to David Faulkner. 11 Nov

David Faulkner attached 27 Nov at 09:28
NU271012_CAL_A - IHLA-TK04 Tank 4 Magnetrol Calculation.pdf

David Faulkner attached 27 Nov at 09:28
NU271013_CAL_A - IHLA-TK05 Tank 5 Magnetrol Calculation.pdf

David Faulkner attached 27 Nov at 09:28
NU271014_CAL_A - IHLA-TK12 Tank 12 Magnetrol Calculation.pdf

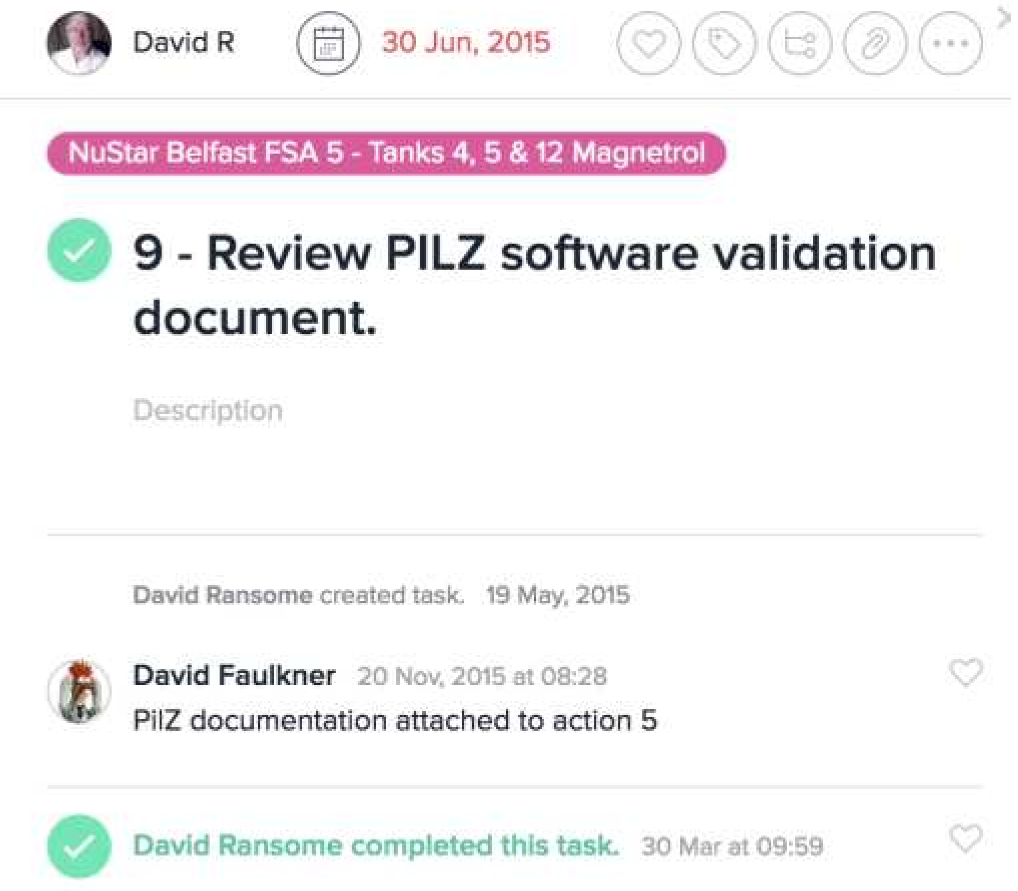
David Faulkner 27 Nov at 09:29
Calculations and sketches converted into attached calcs NU271012/13/14

David Faulkner assigned to you. 27 Nov
David Faulkner changed the due date to 28 Nov. 27 Nov
David Faulkner marked today. 27 Nov
David Ransome changed the due date t
David Ransome changed the due date to 30 Dec. Wednesday

27 Nov, 2016 at 09:29

David Ransome Wednesday at 09:54
Document received, FSA to be completed

David Ransome completed this task. Today at 15:04



David R

30 Jun, 2015

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

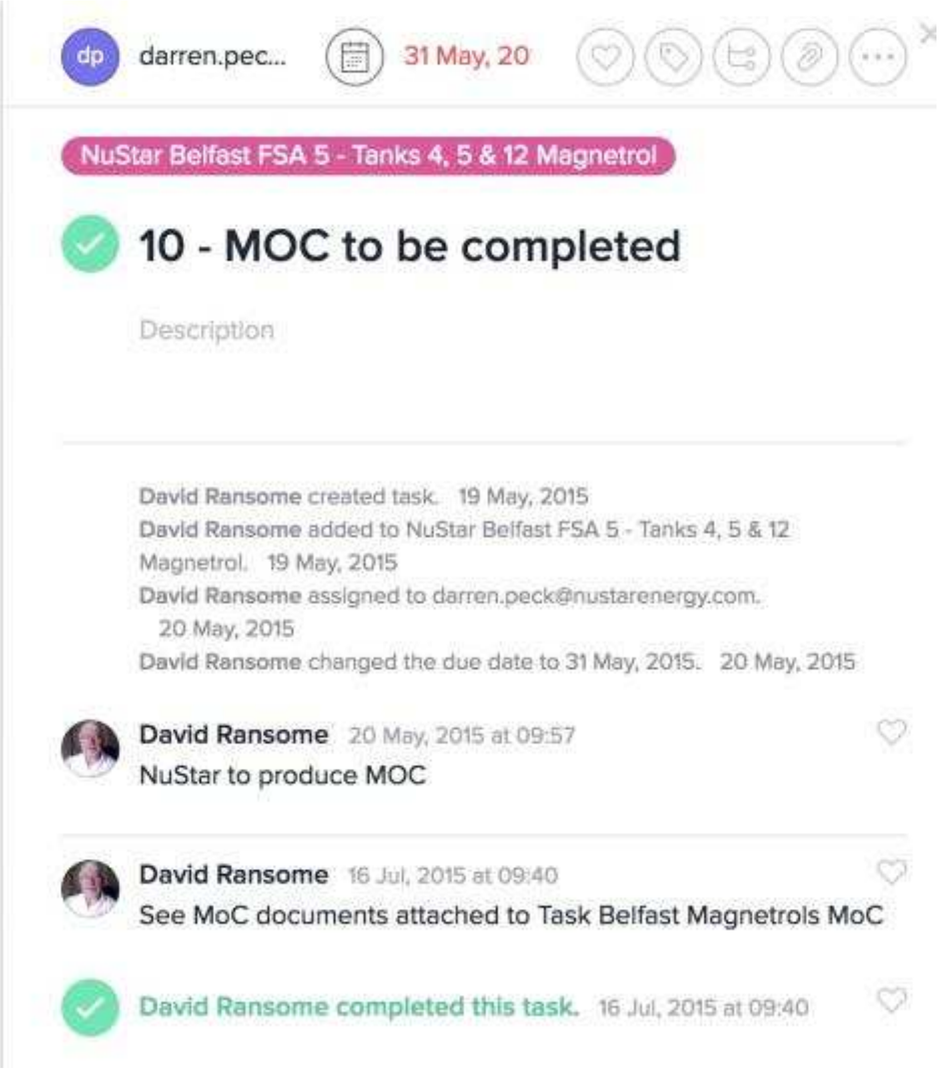
9 - Review PILZ software validation document.

Description

David Ransome created task. 19 May, 2015

David Faulkner 20 Nov, 2015 at 08:28
PilZ documentation attached to action 5

David Ransome completed this task. 30 Mar at 09:59



NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 10 - MOC to be completed

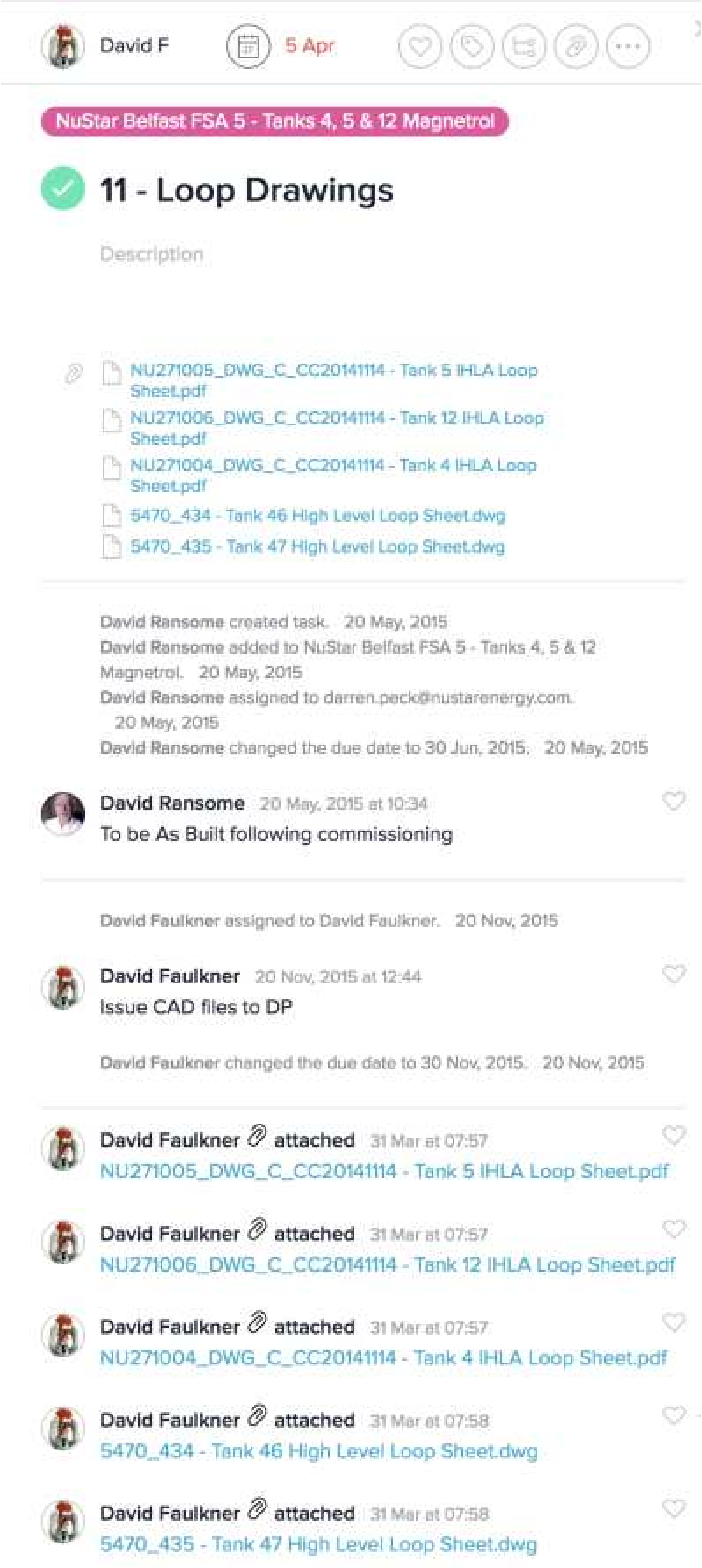
Description

David Ransome created task. 19 May, 2015
David Ransome added to NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 19 May, 2015
David Ransome assigned to darren.peck@nustarenergy.com. 20 May, 2015
David Ransome changed the due date to 31 May, 2015. 20 May, 2015

David Ransome 20 May, 2015 at 09:57
NuStar to produce MOC

David Ransome 16 Jul, 2015 at 09:40
See MoC documents attached to Task Belfast Magnetrols MoC

✓ David Ransome completed this task. 16 Jul, 2015 at 09:40



David F 5 Apr

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 11 - Loop Drawings

Description

- NU271005_DWG_C_CC20141114 - Tank 5 IHLA Loop Sheet.pdf
- NU271006_DWG_C_CC20141114 - Tank 12 IHLA Loop Sheet.pdf
- NU271004_DWG_C_CC20141114 - Tank 4 IHLA Loop Sheet.pdf
- 5470_434 - Tank 46 High Level Loop Sheet.dwg
- 5470_435 - Tank 47 High Level Loop Sheet.dwg

David Ransome created task. 20 May, 2015
David Ransome added to NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 20 May, 2015
David Ransome assigned to darren.peck@nustarenergy.com. 20 May, 2015
David Ransome changed the due date to 30 Jun, 2015. 20 May, 2015

David Ransome 20 May, 2015 at 10:34
To be As Built following commissioning

David Faulkner assigned to David Faulkner. 20 Nov, 2015

David Faulkner 20 Nov, 2015 at 12:44
Issue CAD files to DP

David Faulkner changed the due date to 30 Nov, 2015. 20 Nov, 2015

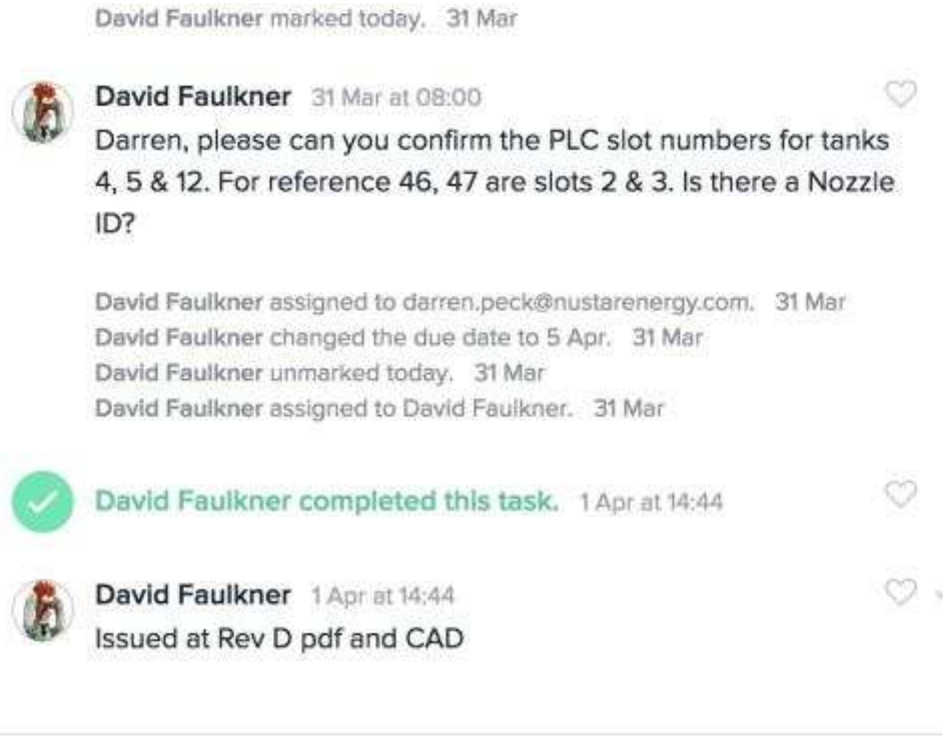
David Faulkner attached 31 Mar at 07:57
NU271005_DWG_C_CC20141114 - Tank 5 IHLA Loop Sheet.pdf

David Faulkner attached 31 Mar at 07:57
NU271006_DWG_C_CC20141114 - Tank 12 IHLA Loop Sheet.pdf

David Faulkner attached 31 Mar at 07:57
NU271004_DWG_C_CC20141114 - Tank 4 IHLA Loop Sheet.pdf

David Faulkner attached 31 Mar at 07:58
5470_434 - Tank 46 High Level Loop Sheet.dwg

David Faulkner attached 31 Mar at 07:58
5470_435 - Tank 47 High Level Loop Sheet.dwg



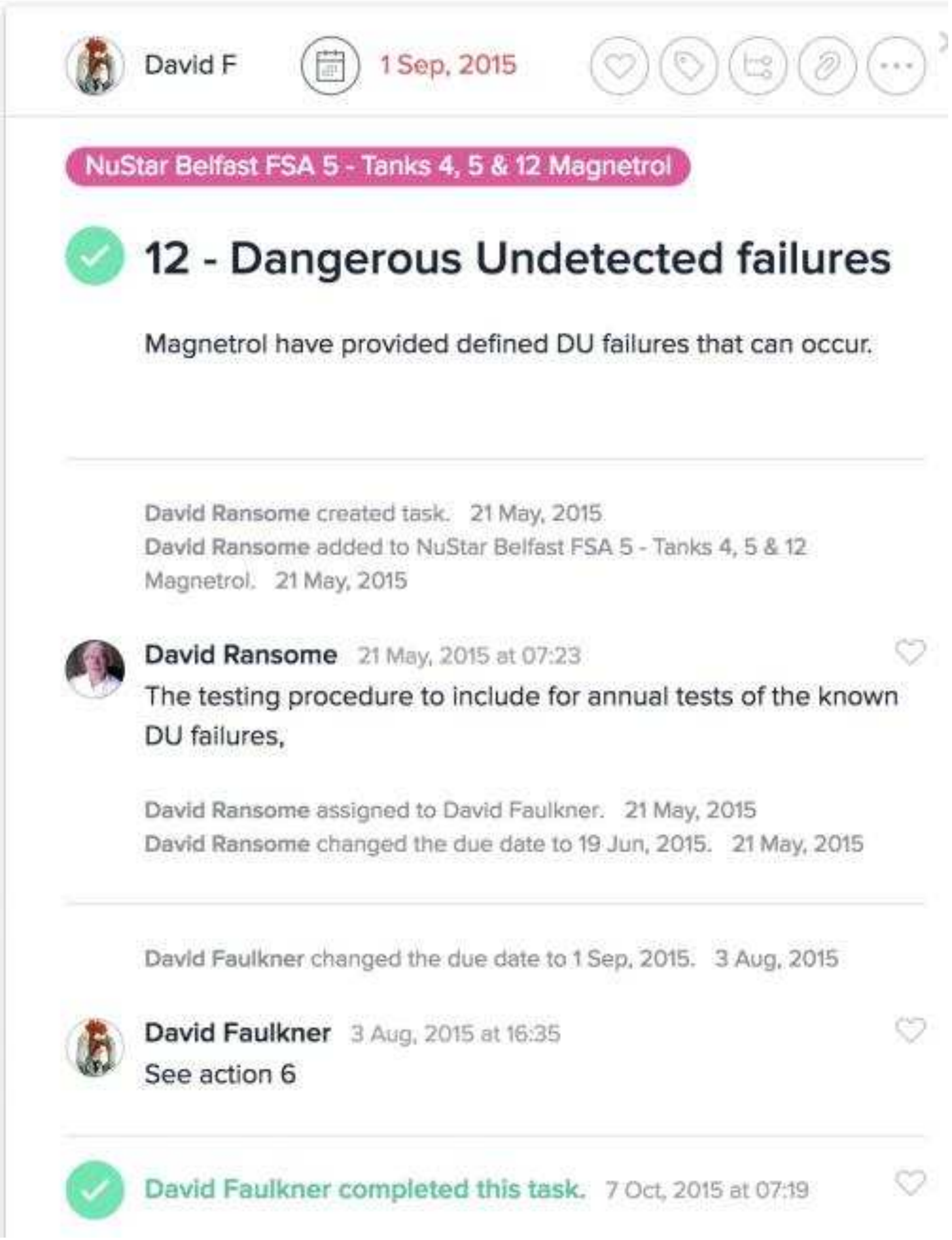
David Faulkner marked today. 31 Mar

David Faulkner 31 Mar at 08:00
Darren, please can you confirm the PLC slot numbers for tanks 4, 5 & 12. For reference 46, 47 are slots 2 & 3. Is there a Nozzle ID?

David Faulkner assigned to darren.peck@nustarenergy.com. 31 Mar
David Faulkner changed the due date to 5 Apr. 31 Mar
David Faulkner unmarked today. 31 Mar
David Faulkner assigned to David Faulkner. 31 Mar

✓ David Faulkner completed this task. 1 Apr at 14:44

David Faulkner 1 Apr at 14:44
Issued at Rev D pdf and CAD



David F 1 Sep, 2015

NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol

✓ 12 - Dangerous Undetected failures

Magnetrol have provided defined DU failures that can occur.

David Ransome created task. 21 May, 2015
David Ransome added to NuStar Belfast FSA 5 - Tanks 4, 5 & 12 Magnetrol. 21 May, 2015

David Ransome 21 May, 2015 at 07:23
The testing procedure to include for annual tests of the known DU failures,

David Ransome assigned to David Faulkner. 21 May, 2015
David Ransome changed the due date to 19 Jun, 2015. 21 May, 2015

David Faulkner changed the due date to 1 Sep, 2015. 3 Aug, 2015

David Faulkner 3 Aug, 2015 at 16:35
See action 6

✓ David Faulkner completed this task. 7 Oct, 2015 at 07:19

Signature Certificate

Document Reference: CLAEP6J6UJ9L72BT94AM6U

RightSignature
Easy Online Document Signing

David Ransome
Party ID: KC2T53J6W52Y9BEJPT9SKG
IP Address: 86.14.218.30
VERIFIED EMAIL: drr@pidesign.co.uk

Electronic Signature:
DRRansome

Multi-Factor
Digital Fingerprint Checksum 11bf3a34c02278dec9abd25d4c5da947326ac007

Timestamp	Audit
2016-12-05 07:36:19 -0800	All parties have signed document. Signed copies sent to: David Ransome and P I Design Ltd.
2016-12-05 07:36:19 -0800	Document signed by David Ransome (drr@pidesign.co.uk) with drawn signature. - 86.14.218.30
2016-12-05 07:35:57 -0800	Document viewed by David Ransome (drr@pidesign.co.uk). - 86.14.218.30
2016-12-05 07:35:34 -0800	Document created by P I Design Ltd (signature@pidesign.co.uk). - 86.14.218.30

This signature page provides a record of the online activity executing this contract.