FSC

FUNCTIONAL SAFETY CONSULTANCY

SCIENCE AND TECHNOLOGY FACILITIES COUNCIL

HYDROGEN DELIVERY SYSTEM

SAFETY INTEGRITY LEVEL ASSESSMENT

Document Identifier: X589 TR 002 (1.0)			
Issue	Date	Author	Approved
Draft A	Aug 2011	D Chauhan	K J Kirkcaldy
1	Sept 2011	D Chauhan	K J Kirkcaldy
DCD Date		D Chauhan	K Kirkcaldy

CHANGE HISTORY

Issue	Date of Issue	CR/DR Numbers	No. of Pages	Pages Changed and Reasons for Change
Draft A	Aug 2011	N/A	28	Draft Issue
Issue 1	Sept 2011	N/A	28	Formal issue with client comments from draft issue incorporated

DISTRIBUTION LIST

Copy	Registered Holder
Master	Functional Safety Consultancy
Copy 1	Science and Technology Facilities Council

© Copyright 2011. FUNCTIONAL SAFETY CONSULTANCY. All Rights Reserved.

No part of this document may be used, translated into another language, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of FUNCTIONAL SAFETY CONSULTANCY.

The information and statements contained in this document are opinions only and reflect Functional Safety Consultancy's best judgement based on the available information. Functional Safety Consultancy shall not be responsible whatsoever for loss or damage (including, without limitation, loss of profits or any indirect loss), if any, suffered by any party as a result of decisions made or actions taken in reliance upon or in connection with the information contained in this report.

FUNCTIONAL SAFETY CONSULTANCY reserves the right to revise any information contained in this document without prior notice.

Questions or comment regarding this document or the product to which it relates should be directed to:

Functional Safety Consultancy
Holmwood
Broadlands Business Campus
Langhurstwood Road
Horsham
West Sussex
RH12 4PN

CONTENTS

ABBREVIATIONS

λ	Failure rate, the ratio of the total number of failures occurring in a given period of time.
λ_D	failure rate of dangerous failures.
λ_{DD}	failure rate of dangerous failures detected by diagnostics.
λ_{DU}	failure rate of dangerous failures undetected by diagnostics.
λ_S	failure rate of safe failures.
CCF	Common Cause Failure.
CPU	Central Processing Unit
Dangerous failure	This is a failure mode that has the potential to put the safety-related system into a hazardous or fail-to-function state.
DD	Dangerous Detected
DU	Dangerous Undetected
E/E/PE	Electrical/Electronic/Programmable Electronic
f/hr	Failures per hour.
FMEDA	Failure Modes Effects and Diagnostics Analysis
FSC	Functional Safety Consultancy
HDS	Hydrogen Delivery System
HFT	Hardware Fault Tolerance
Hrs	Hours.
LEL	Lower Explosive Limit
LOPA	Layers of Protection Analysis
MDT	Mean Down Time
MICE	Muon Ionisation Cooling Experiment
Mths	Months.
MTTR	Mean Time to Repair
N/a	Not applicable.
PFD	Probability of failure on demand.
PTI	Proof Test Interval
RBD	Reliability Block Diagram
S	Safe
Safe failure	This is a failure mode which does not have the potential to put the safety-related system in a hazardous or fail-to-function state.
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level.
STFC	Science and Technology Facilities Council
Tp	Proof Test Interval

SUMMARY

This report provides a Safety Integrity Level (SIL) Assessment in accordance with IEC61508 [1.3.1] in order to demonstrate that the Safety Instrumented Functions (SIFs) proposed as part of the Hydrogen Delivery System (HDS) associated with the Muon Ionisation Cooling Experiment (MICE) provide adequate levels of risk reduction consistent with industry standards and the SIL targets identified by Layer of Protection Analysis (LOPA).

The analysis has been carried on the SIFs proposed by Science and Technology Facilities Council (STFC) and assumes a mean down time (MDT) of 24 hours. The Probability of Failure on Demand (PFD) performance of the SIFs is founded on the assumption that end-to-end proof tests will be performed at an interval not exceeding 1 year. The results of the assessment are summarised in Table 1.

TABLE 1. SUMMARY OF PFD AND ARCHITECTURE RESULTS

Hazard ID	Description	Required PFD	Required SIL	Achieved PFD	Achieved SIL (based on PFD only)	Achieved SIL (based on Arch only)	Pass / Fail
17-18	Buffer Tank Over Pressure	1.00E-01	SIL 1	1.51E-02	SIL 1	SIL 1	Pass
27-29	Build up of Impurities in the Test Cryostat	6.73E-03	SIL 2	3.76E-03	SIL 2	SIL 2	Pass

The analysis shows that the SIFs meet their respective PFD and architectural requirements identified from LOPA.

1. INTRODUCTION

1.1. Objectives

A SIL assignment study carried out for the HDS identified two hazards which required a SIF in order to reduce the risk to an acceptable level.

This report provides a SIL Assessment for the SIFs identified by STFC in order to demonstrate that the PFD and Architectural Requirements are met in accordance with IEC61508 [1.3.1].

The objectives are to provide:

- an analysis of the identified safety functions to confirm that the configurations meet the reliability and architectural requirements;
- details of any shortcomings and where possible, recommendations for improvement;
- a clear and traceable assessment which presents all data used, with references to appropriate sources, and lists all assumptions and limitations in terms of sensitivity of data.

1.2. Scope

The hardware reliability and minimum architecture requirements of IEC61508 [1.3.1] are addressed.

The analysis does not address measures adopted for the avoidance and control of systematic failures.

1.3. Related Documents

1.3.1. IEC 61508 2010, Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety Related Systems.

1.3.2. FSC Report, Science and Technology Facilities Council, Hydrogen Delivery System, Safety Integrity Level Assignment, Document Number X589 TR 001 (2.0), dated January 2011.

1.3.3. Mice Hydrogen System, Hydrogen System Safety Instrumented Functions, Document Number MICCEH2-TN-110801 Issue 1, dated 04/08/2011.

1.3.4. BETAPLUS Common Mode Failure Assessment Program, version 3.0. Technis, 26 Orchard Drive, Tonbridge, Kent TN10 4LG, ISBN 0-951-65625-2.

1.3.5. Exida.com Safety Equipment Reliability Handbook, 2007, 3rd Edition Volume 1 – Sensors, ISBN 978-0-9727234-3-5

1.3.6. Exida.com Safety Equipment Reliability Handbook, 2007, 3rd Edition Volume 2 – Logic Solvers and Interface Modules, ISBN 978-0-9727234-4-2

1.3.7. Exida.com Safety Equipment Reliability Handbook, 2007, 3rd Edition Volume 3 – Final Elements, ISBN 978-0-9727234-5-9

1.3.8. FARADIP-THREE V6.4, Reliability Data Base. Technis, 26 Orchard Drive, Tonbridge, Kent TN10 4LG, ISBN 0-951-65623-6.

1.3.9. Failure Modes of Armature Relays, Report T219, issue 2, January 2006, Technis, 26 Orchard Drive, Tonbridge, Kent TN10 4LG, ISBN 0-951-65625-2.

2. SYSTEM DESCRIPTION

2.1. General

Buffer Tank Over-Pressure

A SIF to protect against the over-pressurisation of the Buffer-Tank has been designed to provide the required SIL 1 risk reduction as identified from LOPA.

The over-pressure results from liquid boil-off caused by the failure of the cryo-cooler and an associated failure of the mechanical relief systems.

In order to mitigate the risk, an additional hydrogen sensor will be installed in the MICE Hall into the HDS. This will provide both visible and audible warnings on detection of hydrogen at a fraction of the lower explosive limit (LEL).

The safety function consists of redundant hydrogen sensors, an Oliver Tocsin 920 gas detector control panel and beacons / alarm sirens.

Build up of Impurities in the Test Cryostat

A second SIF provides an interlock, whereby the operation of the heaters, which could act as an ignition source, is prevented if a potentially explosive atmosphere is present.

The Cryostat Vacuum rising above a vacuum level of 10^{-3}mbar, could be an indication that there is a possibility of a hydrogen-air mixture formed in the vacuum space. This interlock stops the absorber heaters working, while the Cryostat Vacuum is 'not good'.

The safety function consists of redundant pressure gauges, gauge controllers and relays.

2.2. SIL Targets

The SIL targets were defined within FSC Report X589 TR 001 (2.0) [1.3.2] and information defining the SIFs was supplied by STFC via a Hydrogen Safety Instrumented Functions Report [1.3.3].

Table 2 defines the SIFs and their targets:

TABLE 2. SAFETY INSTRUMENTED FUNCTIONS AND TARGETS

Hazard ID	Node	Node Description	Event (Hazard) Description	Consequence	SRS Requirement (PFD)	SRS required SIL
17-18	4	Buffer Tank	Over pressure of buffer tank	Increase pressure leading to a release of hydrogen and ignition leading to multiple deaths	1.00E-01	SIL1
27-29	7	Test Cryostat and Mass Spectrometer Port to Vent and Exhaust Vent	Build up of impurties over a period of time, pressurisation and heating of hydrogen leading to a rupture	Explosion leading to multiple deaths	6.73E-03	SIL2

3. QUANTITATIVE SIL ASSESSMENT

3.1. Introduction

The SIL Assessment has been carried out in line with IEC 61508, Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety Related Systems [1.3.1].

The identified SIFs were assessed in order to demonstrate that they meet the hardware reliability requirements, in terms of PFD and the architectural requirements against the targets identified by LOPA, shown in Table 2.

3.2. SIL Target Reliability Requirements

The PFD for each SIL depends upon the mode of operation in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it. These are defined in IEC 61508-4, 3.5.12 and may be either:

- low demand, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency;
- high demand or continuous mode, where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof test frequency.

Based on these criteria, the SIFs are assumed to be low demand systems and therefore the LOW DEMAND PFD targets presented in Table 3 have been applied in this analysis.

TABLE 3 SIL SPECIFIED PFD AND FAILURE RATES

SIL Level	LOW DEMAND Probability of failure on demand	HIGH DEMAND Failure rate per hour
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

3.3. Probability of Failure on Demand

The calculation of PFD is presented in Appendix 1 and summarised in section 4.

The calculations are performed using the Reliability Block Diagram (RBD) technique. In RBDs, the diagrams show the items or components required for a reliable system and do not necessarily represent physical layout or connections. Failure of a series element results in failure of the system, whereas failure of more than one element in parallel is required for system failure. RBD modelling is a valid technique described in IEC61508-6, Annex B, 4.2.

3.4. Proof Test Period (PTI) and Mean Down Time (MDT)

The probability of failure on demand relates to dangerous failures that prevent the safety function from operating when required. These failure modes are either classified as detected failures, in that they are detected by diagnostics, or undetected failures that are not detected except by proof tests, which are typically performed annually.

The analysis assumes that failure modes not detected by diagnostics or by failing to the safe state, will be found at proof test and therefore maintenance procedures should ensure that this is achieved in practice.

If a failure occurs, it is assumed that on average it will occur at the mid point of the test interval. In other words, the fault will remain undetected for 50% of the test period.

For both detected and undetected failures the Mean Down Time (MDT) depends upon the test interval and also the repair time, or Mean Time to Repair (MTTR).

The MDT used in the analysis, is calculated from:

$$MDT = \frac{\text{test interval}}{2} + MTTR$$

The MDT for detected failures therefore approximates to the repair time, since the test interval (autotest) is generally short compared to the MTTR. For undetected failures the repair time is short compared to the test interval, the PTI (Tp), and therefore MDT for undetected failures approximates to Tp/2.

The MDT and PTI initially assumed for the analysis are shown in Table 4.

TABLE 4. MEAN DOWN TIME AND PROOF TEST INTERVAL

MDT	24 hours
PTI	8760 hours (1 year)

3.5. Accounting for Common Cause Failures

Common cause failures (CCF) are failures that may result from a single cause but simultaneously affect more than one channel. They may result from a systematic fault for example, a design specification error or an external stress such as an excessive temperature that could lead to component failure in both redundant channels. It is the responsibility of the system designer to take steps to minimise the likelihood of common cause failures by using appropriate design practices. The contribution of CCFs in parallel redundant paths is accounted for by inclusion of a β factor. The CCF failure rate that is included in the calculation is equal to β x the total failure rate of one of the redundant paths.

The contribution of CCF in parallel redundant paths is accounted for by inclusion of a β factor. The CCF failure rate that is included in the calculation is equal to β x the total failure rate of one of the redundant paths.

The BETAPLUS [1.3.4] model has been used to estimate the β-factor. The model is the preferred technique because it is objective and provides traceability in the estimation of β. The model has been compiled to ask a series of specific questions, which are then scored using objective engineering judgement [refer to Appendix 2]. The maximum score for each question has been weighted in the model by calibrating the results of various assessments, against known field failure data.

Two columns are used for checklist scores. Column A contains the scores for those features of CCF protection that are perceived as being enhanced by an increase of diagnostic frequency (auto-test or proof test). Column B contains the scores for those features thought not to be enhanced by an improvement in diagnostic frequency.

The model allows the scoring to be modified by the frequency and coverage of diagnostic test. Column A scores are multiplied by a factor C, which is derived from diagnostic related considerations. The final β factor is then estimated from the raw score total:

Raw score = (A * C) + B

The relationship between β and the raw score is essentially a negative exponential function, since there is no data to justify departure from the assumption that as β decreases (improves) then successive improvements become increasingly more difficult to achieve.

Where a particular question may not apply to the system being evaluated, a score of either 100% or 0% is entered depending upon which is appropriate for the system.

3.6. Estimation of Common Cause Failure Contribution

For the parallel redundant configurations, a CCF factor has been estimated based on the BETAPLUS model [1.3.4], judgement tables in Appendix 2. This assesses the degree of channel separation, design with common cause awareness, diagnostic cover and self-test frequency and the fact that the operating environment will be controlled to limit common cause failure risk.

The following assumptions have been made for the purposes of estimating CCF contribution:

- alarms, beacons and gauges are physically separated and at least 1 metre apart;
- programmable channels are on separate modules;
- written system of work on site should ensure that failures are investigated and checked in other channels (including degredation);
- written maintenance procedures should prevent re-routing of cable runs;
- up to 25% of installers and 50% of maintainers understand CCFs;
- personnel access is limited;
- the operating environment is controlled and the equipment has been rated over the full environmental range;
- maintenance of the redundant channels will be staggered.

Actual in-service performance however, will depend upon the specific installation and the design, operating and maintenance practices that are adopted but provided that all appropriate good engineering practices are adopted, then the model will provide a reasonable estimation of CCF contribution.

The estimated CCF values used in the analysis are shown in Table 5.

TABLE 5. CCF CONTRIBUTION

Device	Configuration	β-Factor	Justification
Buffer Tank Over Pressure	1oo2	5%	BETAPLUS model [1.3.4] estimated 4.95% [Appendix 2].
Build up of Impurities in the Test Cryostat	1oo2	5%	BETAPLUS model [1.3.4] estimated 4.64% [Appendix 2].

3.7. Safe Failure Fraction (SFF)

In the context of hardware safety integrity, the highest SIL that can be claimed for a safety function is limited by the hardware fault tolerance and the SFF, of the sub-systems that carry out that safety function.

With respect to these requirements, IEC61508, [1.3.1] gives the following additional guidance:

- a hardware fault tolerance of N means that N+1 faults could cause the loss of the safety function. In determining the hardware fault tolerance, no account shall be taken of other measures that may control the effects of faults such as diagnostics;
- where one fault directly leads to the occurrence of one or more subsequent faults, these are considered as a single fault;
- in determining hardware fault tolerance, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem. Any such fault exclusions shall be justified and documented.

Within IEC 61508, [1.3.1] subsystems are divided into two categories, A and B. The SFF and device type categorisation is presented in Table 7.

The relays, beacons and alarm sirens, were considered to be Type A, in that they are not complex programmable devices, the failure modes and behaviour under fault conditions are well defined and failure rate data is available.

All sensors, Logic Solvers and controllers were Type B in that they contain some processing capability and as such, their behaviour under fault conditions may not be completely determined.

3.8. Architectural Constraints

The architectural constraints for a SIF are summarised in Table 6. This has been used to access the architectural performance of the specified safety function.

TABLE 6. ARCHITECTURAL CONSTRAINTS

Type A subsystems definition: Failure modes of all constituent parts well defined, and Behaviour of the subsystem under fault conditions completely determined, and Sufficient dependable data from field experience to show that the claimed failure rates for detected and undetected dangerous failures are met			
Safe Failure Fraction	Hardware Fault Tolerance (N)		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% - <90%	SIL 2	SIL 3	SIL 4
90% - <99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4
Type B subsystems definition: Failure mode of at least one constituent component is not well defined, or The behaviour of the subsystem under fault conditions cannot be completely determined, or There is insufficient dependable data from field experience to support the claimed failure rates for detected and undetected dangerous failures			
Safe Failure Fraction	Hardware Fault Tolerance (N)		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% - <90%	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Note: A hardware fault tolerance of N means that N+1 faults could cause the loss of the safety function.

3.9. Detected and Undetected Failures

The probability of failure on demand relates to dangerous failures that prevent the SIF from operating when required. These failure modes are either classified as detected failures, in that they are detected by diagnostics, or undetected failures that are not detected except by manual proof tests, which are provisionally performed annually.

The analysis assumes that failure modes not detected by diagnostics, will be found at proof test and therefore maintenance procedures should ensure that this is achieved in practice.

3.10. Calculations

The following general relationships were used in the analysis.

SFF	=	$(\Sigma \lambda_{DD} + \Sigma \lambda_S) / (\Sigma \lambda_S + \Sigma \lambda_{DD} + \Sigma \lambda_{DU})$	Ref. IEC61508-2, C.1
λ_D	=	$\lambda_{DU} + \lambda_{DD}$	Ref. IEC61508-6, B.3.2.2.1
For detected failures:			Ref. IEC61508-6, B.3.2.2
PFD_{1oo1}	=	$\lambda_{DD} . MDT$	
PFD_{1oo2}	=	$\lambda_{DD}^2.MDT^2 + \beta.\lambda_{DD}.MDT$	
For undetected failures:			Ref. IEC61508-6, B.3.2.2
PFD_{1oo1}	=	$\lambda_{DU}.T_p / 2$	
PFD_{1oo2}	=	$\lambda_{DU}^2.T_p^2 / 3 + \beta.\lambda_{DU}.T_p / 2$	

Where λ_{DD} is the dangerous detected failure rate, λ_{DU} is the dangerous undetected failure rate and β is the contribution from common cause failures section [3.5]. T_p is the proof test interval and MDT is the Mean Down Time.

3.11. Assumptions

This section summarises the general assumptions used in the analysis and provides cross-references to the sections in the report where they occur.

a) The SIFs are assumed to be low demand systems and therefore the LOW DEMAND PFD targets apply, section [3.1];

b) The MDT and PTI assumed for the analysis are shown in Table 4, section [3.4];

c) In determining the contribution of common cause failures, certain assumptions were made regarding the degree of separation of redundant elements. These are recorded in Appendix 2 and summarised in section [3.5].

d) The analysis assumes that failure modes not detected by diagnostics or by failing to the safe state, will be found at proof test and therefore maintenance procedures should ensure that this is achieved in practice, section [3.9];

e) If a failure occurs, it is assumed that on average it will occur at the mid point of the test interval. In other words, the fault will remain undetected for 50% of the test period, section [3.9].

f) Failure modes not detected by diagnostics or by fail-to-safe conditions, were assumed to be detected at proof test, section [3.9];

g) The analysis assumes constant failure rates and therefore the effects of early failures are expected to be removed by appropriate processes. It is also assumed that components are not operated beyond their useful life thus ensuring that failures due to wear-out mechanisms do not occur, section [3.12];

3.12. General Use of Failure Rates

3.12.1. General

The analysis assumes constant failure rates and therefore the effects of early failures are expected to be removed by appropriate processes. These processes include the use of mature products from approved sources, in-house testing prior to delivery and extended operation and functional testing as part of installation and commissioning. Field returns data on other similar projects indicates that early life failures do not result in a significant number of returns and therefore the techniques employed are judged to be sufficient.

It is also assumed that components are not operated beyond their useful life thus ensuring that failures due to wear-out mechanisms do not occur.

3.12.2. Data Sources

The failure rates used and their sources are presented in Table 7. Where possible, the analysis makes use of available field data but refers to industry sources to ensure that the values used provide a conservative approach in terms of reliability modelling. This approach gives confidence that the calculated reliability performance should be achievable in service.

TABLE 7. FAILURE RATES AND SFF

Device	Part No.	λDU	λDD	λS	SFF	Type	Data Source
Hydrogen Sensor	Generic Catalytic Hydrocarbon Gas Detector	1.8E-06	0.0E+00	3.8E-06	0.68	B	Exida 2007 - Volume 1 Item No 1.2.1 [1.3.5]
Analogue Input Module	Generic AI	2.88E-07	7.63E-07	1.05E-06	0.86	B	Exida 2007 - Volume 2 Item No 2.3.1 [1.3.6]
CPU Module	Generic CPU	1.50E-06	3.50E-06	5.00E-06	0.85	B	Exida 2007 - Volume 2 Item No 2.3.1 [1.3.6]
Data Hub	Generic	1.20E-06	0.00E+00	1.80E-06	0.60	B	Faradip [1.3.8]
Beacon	Generic	1.0E-06	0.0E+00	0.0E+00	0.00	A	Exida 2007 - Volume 3 Item No 3.7.3 [1.3.7]
Alarm Siren	Generic	4.2E-06	0.0E+00	1.8E-06	0.30	A	Exida 2007 - Volume 3 Item No 3.7.2 [1.3.7]
Pressure Gauge	Generic Pressure Gauge and Input Converter	4.00E-06	0.00E+00	6.00E-06	0.60	B	Faradip [1.3.8]
Pressure Gauge Controller	Generic Pressure Controller with Processor	4.60E-06	0.00E+00	6.90E-06	0.60	B	Faradip [1.3.8]
Relay (Normally Energised, Normally Open)	Generic	9.00E-08	0.00E+00	2.10E-07	0.70	A	Technis Report T219 [1.3.9]

4. RESULTS OF QUANTITATIVE SIL ASSESSMENT

4.1. Results of Safety Function PFD Calculation

The results of the Safety Function PFD calculation are summarised in Table 8. The allowable SIL category is based only on the calculated PFD for the assumed annual proof test interval and does not take the architectural constraints into account.

TABLE 8. SUMMARY OF PFD RESULTS

Hazard ID	Description	Required PFD	Required SIL	Achieved PFD	Achieved SIL (based on PFD only)	Pass / Fail
17-18	Buffer Tank Over Pressure	1.00E-01	SIL 1	1.51E-02	SIL 1	Pass
27-29	Build up of Impurities in the Test Cryostat	6.73E-03	SIL 2	3.76E-03	SIL 2	Pass

4.2. Performance against Architectural Constraints

Table 9 summarises the performance of the safety functions against the architectural constraints.

TABLE 9. SUMMARY OF ARCHITECTURAL CONSTRAINTS

Hazard ID	Sub-system	Modules	SFF	HFT	Type	Subsystem SIL Category	Allowable SIL (based on Arch only)
17-18	Inputs	Hydrogen Sensor	0.68	1	B	SIL 2	SIL 1
	Logic Solver	Analogue Input	0.83	0	B	SIL 1	
		CPU	0.85	0	B	SIL 1	
		Data Hub	0.60	0	B	SIL 1	
		Relay	0.70	0	A	SIL 2	
	Outputs	Beacon	0.00	1	A	SIL 2	
		Alarm Siren	0.30	1	A	SIL 2	
27-29	Inputs	Pressure Gauge	0.60	1	B	SIL 2	SIL 2
	Logic Solver	Gauge Controller	0.60	1	B	SIL 2	
		Set-Point Relay	0.70	1	A	SIL 3	
	Outputs	Output Relay	0.70	1	A	SIL 3	

4.3. SIL Assessment Results

The SIL category that is allowed overall is the lower of its PFD performance (Table 8) and its architectural performance (Table 9). The results of the Safety Function PFD calculation and the overall allowable SILs are summarised in Table 10.

TABLE 10. SUMMARY OF SIL ASSESSMENT RESULTS

Hazard ID	Description	Required PFD	Required SIL	Achieved PFD	Achieved SIL (based on PFD only)	Achieved SIL (based on Arch only)	Pass / Fail
17-18	Buffer Tank Over Pressure	1.00E-01	SIL 1	1.51E-02	SIL 1	SIL 1	Pass
27-29	Build up of Impurities in the Test Cryostat	6.73E-03	SIL 2	3.76E-03	SIL 2	SIL 2	Pass

5. CONCLUSIONS

The SIL assessment shows that based on the information provided and the stated assumptions, the identified SIFs meet the hardware reliability and architectural requirements identified in accordance with IEC61508 [1.3.1].

APPENDIX 1

Reliability Block Diagrams

Buffer Tank Over-Pressure

CCF		5%								5%
Qty	1		1	1	1	1	1	1		
Configuration	1oo2		1oo1	1oo1	1oo1	1oo2	1oo2	1oo2		
λ dd (item)	0.00E+00	0.00E+00	7.63E-07	3.50E-06	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
λ dd (branch configuration)	0.00E+00	0.00E+00				4.26E-06		0.00E+00	0.00E+00	0.00E+00
MDT	24	24				24		24	24	24
PFD dd (configuration)	0.00E+00	0.00E+00				1.02E-04		0.00E+00	0.00E+00	0.00E+00
λ du (item)	1.75E-06	8.66E-08	2.88E-07	1.50E-06	1.20E-06	9.00E-08	1.00E-06	4.20E-06	2.08E-07	
λ du (branch configuration)	1.75E-06	8.66E-08				3.08E-06	1.00E-06	4.20E-06	2.08E-07	
Tp	8760	8760				8760		8760	8760	
PFD du (configuration)	7.83E-05	3.79E-04				1.35E-02		1.07E-04	9.11E-04	
Total PFD dd	1.02E-04									
Total PFD du	1.50E-02									
Total PFD	**1.51E-02**									
Overall PFD SIL	**1**									
Type	B		B	B	B	A	A	A		
Fault Tolerance	1		0	0	0	0	1	1		
SFF	0.68		0.83	0.85	0.60	0.70	0.00	0.30		
Architectural SIL	2		1	1	1	2	2	2		
Overall Architectural SIL	**1**									

S:\fsc\Projects\X589 Sc & Tech Hydrogen\SIL Assessment\[RBD (1.1).xls]Buffer Tank Over-Pressure

Impurities in the Test Cryostat

CCF											5%
Qty	1	1	1	1	1	1	1	1	1		
Configuration	1oo2	1oo2	1oo2	1oo2	1oo2	1oo2	1oo2	1oo2	1oo2		
λ dd (item)	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00
λ dd (branch configuration)				0.00E+00				0.00E+00	0.00E+00	0.00E+00	0.00E+00
MDT									24	24	24
PFD dd (configuration)									0.00E+00	0.00E+00	0.00E+00
λ du (item)	4.00E-06	4.60E-06	9.00E-08	9.00E-08	4.00E-06	4.60E-06	9.00E-08	9.00E-08	9.00E-08	4.07E-07	
λ du (branch configuration)				8.78E-06				8.78E-06	8.78E-06	4.07E-07	
Tp									8760	8760	
PFD du (configuration)									1.97E-03	1.78E-03	
Total PFD dd	0.00E+00										
Total PFD du	3.76E-03										
Total PFD	**3.76E-03**										
Overall PFD SIL	**2**										
Type	B	B	A	A	B	B	A	A			
Fault Tolerance	1	1	1	1	1	1	1	1			
SFF	0.60	0.60	0.70	0.70	0.60	0.60	0.70	0.70			
Architectural SIL	2	2	3	3	2	2	3	3			
Overall Architectural SIL	**2**										

S:\fsc\Projects\X589 Sc & Tech Hydrogen\SIL Assessment\[RBD (1.1).xls]Impurities in the Test Cryostat

APPENDIX 2

Estimation of Common Cause Failure Contribution

BETAPLUS 3.0 Partial Beta Common Cause Model

Buffer Tank Over-Pressure

Screen 1B - SEPARATION/SEGREGATION (NON-PES)

	Maximum A	Maximum B	Input %	Actual A	Actual B
Are the sensors, actuators, pumps etc. physically separated and at least 1 metre apart?	15	52	100	15	52
If the item has some intermediate electronics or pneumatics, are the channels on separate PCBs and screened	65	35			
OR are they indoors in separate units, racks or rooms	95	65	100	95	65
Totals	110	117		110	117

Screen 2B - DIVERSITY (NON-PES)

	Maximum A	Maximum B	Input %	Actual A	Actual B
Do the devices employ different technologies?: e.g. 1 electronic or programmable +1 mechanical/pneumatic	100	25			
OR 1 electronic or PE, 1 relay	90	25	100	90	25
OR 1 PE, 1 electronic hardwired	70	25			
Were separate design tests applied by separate people in the case of diverse items?	32	25	100	32	25
Totals	132	50		122	50

Screen 3B - COMPLEXITY/DESIGN/APPLICATION/MATURITY (NON-PES)

	Maximum A	Maximum B	Input %	Actual A	Actual B
Does cross-connection preclude the exchange of any information other than the diagnostics?	30		100	30	
Is there > 5 years experience of the equipment in the particular environment?		10	100		10
Is the equipment simple e.g. electro/mechanical or electro/chemical sensor or single actuator field device?		20	100		20
Are devices protected from over-voltage and over-current (e.g. > 2:1) or mechanical equivalent?	30		100	30	
Totals	60	30		60	30

Screen 4 - ASSESSMENT/ANALYSIS and FEEDBACK OF DATA

	Maximum A	Maximum B	Input %	Actual A	Actual B
Has a combination of competent FMEA and design review attempted to establish multiple failure groups in the electronics?		140	50		70
Is there documentary evidence that field failures are fully analysed with feedback to design?		70	50		35
Totals		210		0	105

Screen 5 - PROCEDURES/HUMAN INTERFACE

	Maximum A	Maximum B	Input %	Actual A	Actual B
Is there a written system of work on site to ensure that failures are investigated and checked in other channels (including degradation)?	30	20	100	30	20
Is maintenance of diverse/redundant channels staggered at intervals to ensure that proof-tests operate satisfactorily between the maintenance?	60		100	60	
Do written maintenance procedures ensure redundant separations (e.g. signal cables) are separated from each other and from power cables and cannot be re-routed?	15	25	100	15	25
Are mods. forbidden without full design analysis of CCF?		20	50		10
Do different staff maintain redundant equipment?	15	20	0	0	0
Totals	120	85		105	55

Screen 6 - COMPETENCE/TRAINING/SAFETY CULTURE

	Maximum A	Maximum B	Input %	Actual A	Actual B
Have designers been trained to understand CCF?		100	100		100
Have installers been trained to understand CCF?		50	50		25
Have maintainers been trained to understand CCF?		60	25		15
Totals		210		0	140

Screen 7 - ENVIRONMENTAL CONTROL

	Maximum A	Maximum B	Input %	Actual A	Actual B
Is there limited personnel access?	40	50	100	40	50
Is there appropriate environmental control? (eg temperature, humidity)	40	50	100	40	50
Totals	80	100		80	100

Screen 8 - ENVIRONMENTAL TESTING

	Maximum A	Maximum B	Input %	Actual A	Actual B
Has full emc immunity or equivalent mechanical testing been conducted on proto-types and production units (using recognised standards)?		316	100		316
Totals		316		0	316

Screen 9B - DIAGNOSTICS AND CROSS-COMMUNICATION (NON-PES)

Input Value

Sensors and Actuators - Interval

Diagnostic Cover	<2hrs	2hrs-2days	2days-1week	>1week
98%	3.0	2.5	2.0	1.0
90%	2.5	2.0	1.5	1.0
60%	2.0	1.5	1.0	1.0

1.0

"C" > 1 may only be scored if remedial action initiated, by the diagnostic is timely enough to invalidate the effect of the second failure. (Note: In practice the majority of field devices are used in such a way that a "C" score > 1 is a possibility).

Assessment of Beta value

	A Score	B Score
Screen 1B - SEPARATION/SEGREGATION (NON-PES)	110	117
Screen 2B - DIVERSITY (NON-PES)	122	50
Screen 3B - COMPLEXITY/DESIGN/APPLICATION/MATURITY (NON-PES)	60	30
Screen 4 - ASSESSMENT/ANALYSIS and FEEDBACK OF DATA	0	105
Screen 5 - PROCEDURES/HUMAN INTERFACE	105	55
Screen 6 - COMPETENCE/TRAINING/SAFETY CULTURE	0	140
Screen 7 - ENVIRONMENTAL CONTROL	80	100
Screen 8 - ENVIRONMENTAL TESTING	0	316
Screens 1 to 8 Total	477	913

	C Score
Screen 9B - DIAGNOSTICS AND CROSS-COMMUNICATION (NON-PES)	1.0

	M out of N	
Screen 10 - TYPE OF REDUNDANCY	1	2

Beta (1 out of 2) = 4.95 %

D factor = 1.00

Beta (M out of N) = 4.95 %

BETAPLUS 3.0 Partial Beta Common Cause Model

Impurities in the Test Cryostat

Screen 1B - SEPARATION/SEGREGATION (NON-PES)

	Maximum A	Maximum B	Input %	Actual A	Actual B
Are the sensors, actuators, pumps etc. physically separated and at least 1 metre apart?	15	52	100	15	52
If the item has some intermediate electronics or pneumatics, are the channels on separate PCBs and screened	65	35			
OR are they indoors in separate units, racks or rooms	95	65	100	95	65
Totals	110	117		110	117

Screen 2B - DIVERSITY (NON-PES)

	Maximum A	Maximum B	Input %	Actual A	Actual B
Do the devices employ different technologies?: e.g. 1 electronic or programmable +1 mechanical/pneumatic	100	25			
OR 1 electronic or PE, 1 relay	90	25			
OR 1 PE, 1 electronic hardwired	70	25	0	0	0
Were separate design tests applied by separate people in the case of diverse items?	32	25	0	0	0
Totals	132	50		0	0

Screen 3B - COMPLEXITY/DESIGN/APPLICATION/MATURITY (NON-PES)

	Maximum A	Maximum B	Input %	Actual A	Actual B
Does cross-connection preclude the exchange of any information other than the diagnostics?	30		100	30	
Is there > 5 years experience of the equipment in the particular environment?		10	100		10
Is the equipment simple e.g. electro/mechanical or electro/chemical sensor or single actuator field device?		20	100		20
Are devices protected from over-voltage and over-current (e.g. > 2:1) or mechanical equivalent?	30		100	30	
Totals	60	30		60	30

Screen 4 - ASSESSMENT/ANALYSIS and FEEDBACK OF DATA

	Maximum A	Maximum B	Input %	Actual A	Actual B
Has a combination of competent FMEA and design review attempted to establish multiple failure groups in the electronics?		140	50		70
Is there documentary evidence that field failures are fully analysed with feedback to design?		70	50		35
Totals		210		0	105

Screen 5 - PROCEDURES/HUMAN INTERFACE

	Maximum A	Maximum B	Input %	Actual A	Actual B
Is there a written system of work on site to ensure that failures are investigated and checked in other channels (including degradation)?	30	20	100	30	20
Is maintenance of diverse/redundant channels staggered at intervals to ensure that proof-tests operate satisfactorily between the maintenance?	60		100	60	
Do written maintenance procedures ensure redundant separations (e.g. signal cables) are separated from each other and from power cables and cannot be re-routed?	15	25	100	15	25
Are mods. forbidden without full design analysis of CCF?		20	50		10
Do different staff maintain redundant equipment?	15	20	0	0	0
Totals	120	85		105	55

Screen 6 - COMPETENCE/TRAINING/SAFETY CULTURE

	Maximum A	Maximum B	Input %	Actual A	Actual B
Have designers been trained to understand CCF?		100	100		100
Have installers been trained to understand CCF?		50	50		25
Have maintainers been trained to understand CCF?		60	25		15
Totals		210		0	140

Screen 7 - ENVIRONMENTAL CONTROL

	Maximum A	Maximum B	Input %	Actual A	Actual B
Is there limited personnel access?	40	50	100	40	50
Is there appropriate environmental control? (eg temperature, humidity)	40	50	100	40	50
Totals	80	100		80	100

Screen 8 - ENVIRONMENTAL TESTING

	Maximum A	Maximum B	Input %	Actual A	Actual B
Has full emc immunity or equivalent mechanical testing been conducted on proto-types and production units (using recognised standards)?		316	100		316
Totals		316		0	316

Screen 9B - DIAGNOSTICS AND CROSS-COMMUNICATION (NON-PES)

	Sensors and Actuators - Interval <2hrs	2hrs-2days	2days-1week	>1week	Input Value
Diagnostic Cover					
98%	3.0	2.5	2.0	1.0	
90%	2.5	2.0	1.5	1.0	
60%	2.0	1.5	1.0	1.0	
					1.0

"C" > 1 may only be scored if remedial action initiated, by the diagnostic is timely enough to invalidate the effect of the second failure. (Note: In practice the majority of field devices are used in such a way that a "C" score > 1 is a possibility).

Assessment of Beta value

	A Score	B Score
Screen 1B - SEPARATION/SEGREGATION (NON-PES)	110	117
Screen 2B - DIVERSITY (NON-PES)	0	0
Screen 3B - COMPLEXITY/DESIGN/APPLICATION/MATURITY (NON-PES)	60	30
Screen 4 - ASSESSMENT/ANALYSIS and FEEDBACK OF DATA	0	105
Screen 5 - PROCEDURES/HUMAN INTERFACE	105	55
Screen 6 - COMPETENCE/TRAINING/SAFETY CULTURE	0	140
Screen 7 - ENVIRONMENTAL CONTROL	80	100
Screen 8 - ENVIRONMENTAL TESTING	0	316
Screens 1 to 8 Total	355	863

	C Score
Screen 9B - DIAGNOSTICS AND CROSS-COMMUNICATION (NON-PES)	1.0

	M out of N	
Screen 10 - TYPE OF REDUNDANCY	1	2

Beta (1 out of 2) = 4.64 %

D factor = 1.00

Beta (M out of N) = 4.64 %