



FUNCTIONAL SAFETY ASSESSMENT REPORT
For the Topworx
ESD VALVE CONTROLLER

Author:

A handwritten signature in blue ink, appearing to read "P. Reeve", written over a dotted horizontal line.

Paul Reeve BEng CEng MIET MInstMC
Consultant Engineer,
Sira Test & Certification

Report checked:

A handwritten signature in blue ink, appearing to read "Dr D J Smith", written over a dotted horizontal line.

Dr D J Smith BSc PhD CEng FIEE HonFSaRS MIGasE
Sira Associate,
Sira Certification Service

Date of issue:

19th March 2008

Customer:

TopWorx Inc.

Report Number:

R56A16648A

COMMERCIALLY IN CONFIDENCE

**THIS DOCUMENT MAY BE NOT BE REPRODUCED WHOLE, OR IN PART,
WITHOUT WRITTEN PERMISSION FROM SIRA TEST & CERTIFICATION**

CONTENTS

1	INTRODUCTION.....	3
1.1	References.....	3
1.2	Scope of this report.....	3
1.3	Terms and abbreviations used.....	4
1.4	Overall description of the equipment	4
1.5	Safety function(s).....	5
2	SCOPE OF THE ASSESSMENT.....	6
2.1	Equipment and documentation assessed.....	6
2.2	Assessment procedures, tools and techniques used	7
2.3	Existing certification relevant to this assessment	7
3	RELIABILITY ANALYSIS	8
3.1	Functional diagram.....	8
3.2	Failure mode.....	8
3.3	Architecture	8
3.4	Diagnostic coverage	8
3.5	Reliability modelling.....	9
3.6	Failure rates.....	10
3.7	Probability of Failure on Demand (PFD) calculations	10
3.8	Proof test interval.....	11
3.9	Calculation of Safe failure fraction	11
3.10	Summary of failure rate data.....	12
3.11	Use of recommended techniques and measures	12
3.12	Operating environment/constraints.....	12
3.13	Verification and Validation.....	12
3.14	E/E/PES lifecycle	13
3.15	Management of functional safety.....	13
3.16	Summary of base information which may be certified	13
3.17	Conditions of Certification	14
3.18	Conditions of Safe Use.....	14
4	CONCLUSIONS AND RECOMMENDATIONS.....	14
	APPENDIX 1 – FMEA OF THE DIAGNOSTICS CIRCUITS.....	15
	APPENDIX 2 – ASSESSMENT OF USE OF TECHNIQUES AND MEASURES (IEC 61508 –2, ANNEX A)	17
	APPENDIX 3 – ASSESSMENT OF THE E/E/PES SUB-SYSTEM (IEC 61508 –2)	24

FUNCTIONAL SAFETY ASSESSMENT REPORT

1 INTRODUCTION

1.1 References

Carried out by:	Sira Test & Certification, Rake Lane, Eccleston, Chester, CH4 9JN
On behalf of:	TopWorx Inc. 3300 Fern Valley Road Louisville Kentucky 40213 USA
Equipment assessed:	ESD Valve Controller
Date of Request for Assessment:	20-August-2007
Assessment standards:	IEC 61508-2:2000
Certificate number:	Sira FSP 08001/01
Assessments conducted between:	September 2007 and March 2008

1.2 Scope of this report

This assessment covers the hardware safety integrity of the ESD valve controller against the requirements of IEC 61508-2 in order to approve its capability for use in SIL3 safety functions. The scope of this report covers the probability of random hardware failures, safe failure fraction, architecture, proof test interval and diagnostic capability.

Some qualitative assessment against systematic failures is also included:

- product specification (with respect to functional safety)
- verification and validation plan/results
- functional safety aspects of the installation, operation and maintenance manual (I,O&M manual)

For certification purposes, the safety-related data that may be stated is summarised in Tables 1, 4, 6 and 7 of this report.

1.3 Terms and abbreviations used

E/E/PES	Electrical/Electronic/Programmable-Electronic safety-related Systems
PLC	Programmable Logic Controller
SIL	Safety Integrity Level
UKAS	United Kingdom Accreditation Service
PFD	Probability of failure on demand
SIS	Safety Instrumented System
SCS	Sira Certification Services
ROSOV	Remotely operated shut off valve
HSE	Health and Safety Executive
FSM	Functional safety management
SIF	Safety instrumented function
HLA	High level alarm
T	Proof test interval
HFT	Hardware fault tolerance
SFF	Safety failure fraction
FMEA	Failure modes and effects analysis
MTTR	Mean time to repair

1.4 Overall description of the equipment

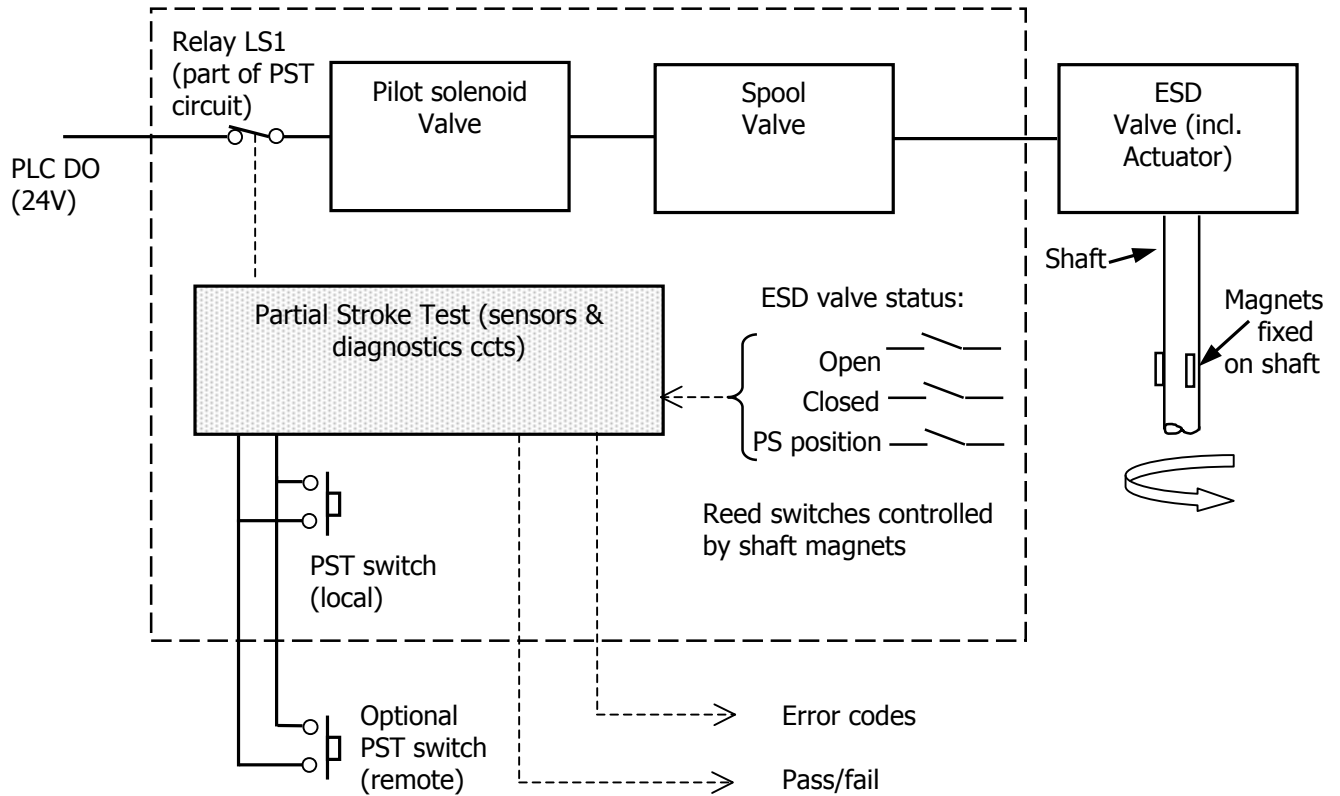
The Topworx 'Valvetop' ESD Valve Controller is intended to be used with emergency shut-down (ESD) valves in order to improve their PFD and availability by virtue of increased diagnostic coverage, particularly when such valves are used in safety functions.

The ESD Valve Controller contains a solenoid pilot valve operating a spool valve, which either admits or relieves pneumatic pressure to the actuator of an ESD process valve. The safe state of the ESD process valve is the closed position, which is achieved by the spool valve diverting pneumatic pressure away from the ESD actuator.

The failure mode of interest in this assessment is therefore defined as: failure of the spool valve to close when the PLC DO signal is removed.

The ESD Valve Controller enables the process valve to be exercised (either from a local switch or by remote command) by partially closing it (typically to 80 - 85% of full stroke) and monitoring the time the valve takes to reach this position. This time is compared with the calibrated time for the specific valve. Any differences (outside a tolerance band) can indicate a variety of conditions such as a damaged shaft, actuator spring fatigue, solenoid pilot exhaust blockage, solenoid spring failure, etc. In this way, 'partial stroke testing' (PST) serves as an effective diagnostic without interrupting the process.

The overall system can be represented by the functional block diagram shown in Figure 1. The ESD Valve Controller is shown in the dotted box. An allowance for the ESD process valve and actuator has been included in the reliability assessment:



Notes: The PST (sensors & diagnostics ccts) shaded box is the subject of the FMEA in Appendix 1
 PLC DO is the (fail safe) control signal:
 Hi = ESD Valve open
 Lo = ESD Valve closed

Figure 1: Functional Diagram

The increased reliability afforded by the ESD Valve Controller relies on the partial stroke test being performed automatically (or by an operator) at no longer than the prescribed intervals, and the operator taking appropriate action in the event of a failure.

1.5 Safety function(s)

The safety function for the ESD Valve Controller is defined as:

- The spool valve to remove pneumatic pressure when the pilot solenoid valve control signal (e.g., PLC DO) is removed

It is expected that this safety function will be used in 'low demand' mode applications. (Refer to IEC 61508-4 for definition of 'low demand').

The ESD Valve Controller is intended to work with ESD valves which, when benefiting from the additional reliability of the Partial Stroke Test, are suitable for safety functions up to and including SIL3.

2 SCOPE OF THE ASSESSMENT

2.1 Equipment and documentation assessed

The equipment assessed is defined in the drawings and identifiers stated in the Tables below.

2.1.1 Product Drawings

The following documents define the equipment that is assessed and should be stated in any certificate that is supported by this assessment. Any changes to these drawings will require a re-assessment.

Table 1: Product Documents

Document no.	Pages	Rev	Date	Document description
ES-00928-1	1 of 6	03	01-FEB-08	Circuit diagram, upper board
ES-00928-1	2 of 6	03	01-FEB-08	Circuit diagram, lower board
ES-00928-1	3 of 6	03	01-FEB-08	PCB layout, upper board
ES-00928-1	4 of 6	03	01-FEB-08	PCB layout, lower board
ES-00928-1	5 of 6	03	01-FEB-08	Parts list, upper board
ES-00928-1	6 of 6	03	01-FEB-08	Parts list, lower board
S-AV1-0001	1 of 1	08	05-MAR-08	SMC Pilot assembly *
S-A01-0027	1 of 1	22	14-JUN-07	DXP Master assembly *
S-AV1-0003	1 of 1	13	13-MAR-08	Cold temp valve assembly *
ES-01309-1	-	01	20-MAR-08	ESD Master Nomenclature *
ES-00936-1	-	03	-	Install, Ops and Maintenance Manual

* only the options shown on the ESD Master Nomenclature ES-01309-1 (R1) are valid

2.1.2 Documentation provided in support of the assessment

The following drawings were referred to during the assessment but do not require to be stated in any certificate that this is supported by this assessment.

Table 2: Supporting Documents

Document number	Rev	Date	Document description
FRM-VTPR	-	27-FEB-08	Validation test plan & results
080118A	A	18-JAN-08	ESD Functional Diagram
Test Report 644		09-DEC-07	Validation extremes of temperature DXP ESD conventional
Test Report 645		09-DEC-07	Validation of over-pressure of ESD pushbutton
Test Report 646		09-DEC-07	Validation life test of ESD conventional
Test Report 655		06-MAR-08	Software/Hardware V&V test procedure & results
DXP/DXS ESD		27-FEB-08	Validation test plan & results
MTBF calculations.xls		09-DEC-07	Failure rate calculations
MTBF Plan 4_07.pdf		26-NOV-07	Failure rate test plan

2.2 Assessment procedures, tools and techniques used

During examination of the product and process documentation, the following procedures, tools and techniques were used:

- Use was made of the relevant schedule of TOEs in The CASS Templates for Sub-Systems, rev 0, and the CASS Scheme Common Schedules in The CASS Guide, rev 2.a,
- The SCS procedures manual for functional safety assessment
- FARADIP.THREE, ver 6.2 was used for the FMEA

FARADIP.THREE, version 6.2, is a failure rate and failure mode data bank linked with a failure mode analysis program. The failure rates are to be regarded as credible as they are selected from the most relevant figures from a number of diverse industrial sources (over 30), taking into account environmental and quality factors. The failure rates are constantly updated by Technis with recent experience and therefore benefit from new data that becomes available from field reliability growth programmes.

2.3 Existing certification relevant to this assessment

TopWorx have an accredited ISO 9001:2000 quality management system with relevant scope.

In addition, TopWorx operate an approved quality system that complies with EN 13980:2002 for production of explosion protection products sold under the European ATEX directive.

These two approvals are relevant to some aspects of the management of functional safety (IEC 61508 Part 1 clause 6) and the hardware development lifecycle (IEC 61508 Part 2 clause 7), although a full audit of these activities was not carried out during this assessment.

3 RELIABILITY ANALYSIS

3.1 Functional diagram

Refer to Figure 1 above for a functional block diagram of the ESD Valve Controller. The device consists of a relay (LS1), a pilot solenoid and a spool valve. These components can be regarded as 'Type A' as defined by IEC 61508-2 clause 7.4.3.1.2. Diagnostics are used to reveal dangerous failures in these components (and the final element ESD valve).

3.2 Failure mode

The failure mode of interest in this assessment is failure of the spool valve to close when the PLC DO signal is removed.

3.3 Architecture

The architecture is 1oo1D (refer to the reliability block diagram below). Hence there is no fault tolerance afforded by redundancy, but random hardware faults in the relay, solenoid and spool valves are diagnosed by the partial stroke test facility.

For 'Type A' components used in SIL3 safety functions, a zero-fault tolerant architecture is permitted if the safe failure fraction is $\geq 90\%$. (See IEC 61508-2 Table 2).

3.4 Diagnostic coverage

The diagnostics perform the following actions:

- Respond to the remote PST command (or local operator pushbutton switch) by temporarily interrupting the PLC drive signal to the valve
- Detect the valve position (open, partially closed and closed) via internal reed switches
- Measure the time to travel from open to the partial stroke position
- Calculate any difference between this measured time and a previously calibrated time (stored in memory) for the specific valve
- Provide an indication via flashing LEDs and switching relay contacts of the status of calibration, PST (pass/fail), ability to fully open, memory error.

It should be realised that the electronics in the ESD Valve Controller are performing diagnostics for the relay (LS1) on the PCB, the pilot solenoid, spool valve and the external ESD valve. Diagnostic coverage is assessed in the FMEA according to the approach given in IEC 61508-2 Annex C and is shown to be $>90\%$ which satisfies the requirement for SIL3 applications. Reference has been made to IEC 61508-2, Table A.1 (faults or failures to be detected during operation or to be analysed in the derivation of safety failure fraction).

3.5 Reliability modelling

The overall system block diagram for failure of the ESD Valve to close can be represented by the following Reliability Block Diagram. The ESD Valve Controller is formed by the items in the dotted box. The PST (sensors & diagnostics ccts) shaded box is the subject of the FMEA in Appendix 1.

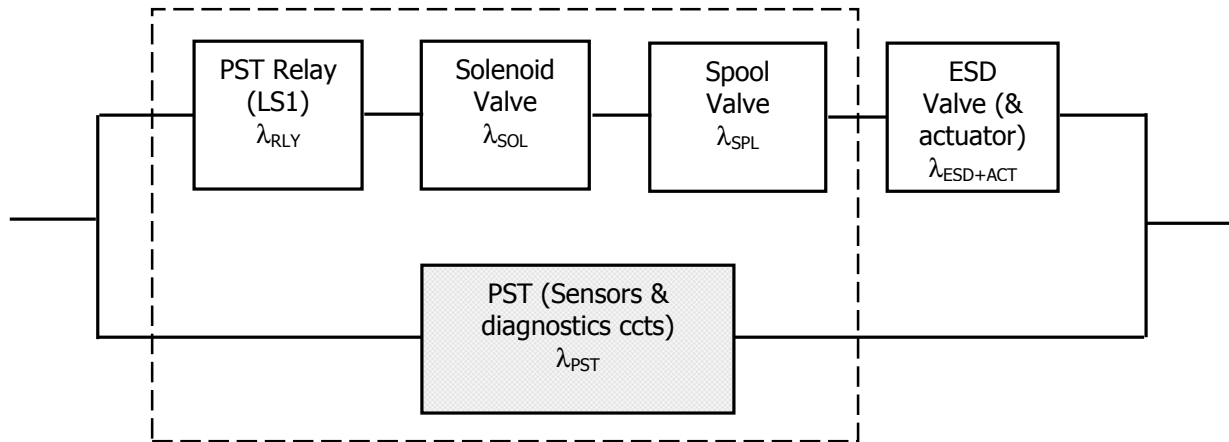


Figure 2: Reliability Block Diagram

The system does not have redundancy, however, the PST circuit effectively performs diagnostics of the relay ('LS1'), solenoid, spool and ESD valves, as the PST is performed at relatively frequent intervals. As the actual failure parameters of the specific ESD Valve (and any associated actuator) are unknown, an allowance is used in the PFD calculations, assuming the failure mode of the ESD valve and it's associated actuator is 'fail to close' (e.g., "sticking valve"). The reliability block diagram can be reduced to:

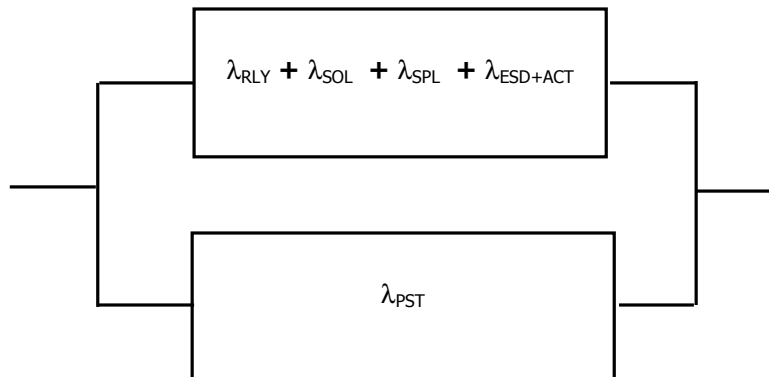


Figure 3: Reduced Reliability Block Diagram

3.6 Failure rates

For the failure rate calculations, it is assumed:

- Repair time is small (manufacturer has quoted 4 hours) compared to the proof test interval
- The MTTR is much greater than the proof test interval

IEC 61508 does not state safety integrity requirements for diagnostic functions, however, these have been assessed anyway to ensure they are of an appropriate integrity to support a SIL3 safety function. An estimated failure rate for the diagnostics circuits is calculated using the Technis FARADIP.THREE package version 6.2 and shown in the table below.

Refer to Appendix 1 for details of the FMEA for the diagnostics circuit. The failure mode for the diagnostics circuits FMEA was defined as failure to perform a partial stroke test and report the result via the relay signals and local LEDs.

Estimated failure rates for the components in the ESD Valve Controller are taken from Technis FARADIP.THREE database and are shown in the table below.

The dominant factor in calculating the total PFD will be the failure rate of the ESD valve and it's associated actuator. As these items are not known at this stage, calculations are based on an allowance for a minimum and maximum value from the FARADIP.THREE database.

Table 3: Failure Rates

Element	Symbol	Failure rate (per hr)	Data source / comments
PST Relay (LS1)	λ_{RLY}	1×10^{-6}	Technis FARADIP.THREE database, version 6.2, (middle figure in range)
Solenoid Valve	λ_{SOL}	1×10^{-7}	Technis FARADIP.THREE database, version 6.2, (geometric mean of minimum and maximum values in range)
Spool Valve	λ_{SPL}	1×10^{-7}	Technis FARADIP.THREE database, version 6.2, (geometric mean of minimum and maximum values in range)
PST (Sensors & diagnostics ccts)	λ_{PST}	2.738×10^{-6}	Calculated from FMEA using Technis FARADIP.THREE database, version 6.2. Refer to Appendix 1 in this report.
ESD Valve & actuator)	$\lambda_{ESD+ACT}$	2×10^{-5}	Technis FARADIP.THREE database, version 6.2, (geometric mean of <u>worst case</u> figures in the range for all valve types)
		2×10^{-6}	Technis FARADIP.THREE database, version 6.2, (geometric mean of <u>best case</u> figures in the range for all valve types)

3.7 Probability of Failure on Demand (PFD) calculations

Considering the reliability block diagrams in Figures 2 and 3 above, the probability of failure on demand (PFD_{ave}) for unrevealed failures is given by:

$$\begin{aligned}
 PFD_{ave} &= (\lambda_{RLY} + \lambda_{SOL} + \lambda_{SPL} + \lambda_{ESD+ACT}) \times \lambda_{PST} \times T^2 / 3 \\
 &= [(1.2 \times 10^{-6} + \lambda_{ESD+ACT}) \times 2.738 \times 10^{-6}] \times T^2 / 3
 \end{aligned}$$

Where T is the proof test interval.

IEC 61508-1 Table 2 states that the probability of failure on demand for SIL3 safety functions shall be in the range 10^{-4} to 10^{-3} . A typical allowance for the final element is 50% of this figure, 5×10^{-4} to leave a

sufficient allowance for the other items in the safety instrumented system. Using the formula above, PFD can be calculated for given values of the ESD valve+actuator failure rates and proof test intervals.

3.8 Proof test interval

For an ESD valve failure rate of 2×10^{-5} failures per hour (worst case from Table 3) the proof test interval T to achieve a PFD of 5×10^{-4} can be calculated as follows:

$$T = \sqrt{\frac{3 \times \text{PFD}_{\text{SYS}}}{(\lambda_{\text{RLY}} + \lambda_{\text{SOL}} + \lambda_{\text{SPL}} + \lambda_{\text{ESD}}) \times \lambda_{\text{PST}}}} = \sqrt{\frac{3 \times 5 \times 10^{-4}}{2.12 \times 10^{-5} \times 2.738 \times 10^{-6}}} = 5,083 \text{ hours}$$

As the PFD figures are dominated by the failure rate of the ESD valve, the following table represents the proof test interval for given failure rates of ESD valves when used in low demand SIL3 applications.

Table 4: Proof Test Intervals to achieve 50% of SIL3 PFD

Failure rate of ESD valve + actuator (per hour)	Proof test interval required to meet 50% of SIL3 PFD allowance
2×10^{-4}	1,650 hours
2×10^{-5}	5,083 hours
2×10^{-6}	13,084 hours
2×10^{-7}	19,782 hours

3.9 Calculation of Safe failure fraction

The failure rates from Table 4 are replicated below together with their contributions to the ESD Valve Controller failure mode and diagnostic coverage in order to calculate the safe failure fraction (SFF).

Table 5: Safe Failure Fraction data

Component	Failure rate (all failures) λ	Contribution leading to dangerous failure mode [NOTE 1]	Failure rate leading to dangerous failure mode [NOTE 1] λ_D	% diagnosed (by PST or other means)	Diagnosed dangerous failures λ_{DD}	Undiagnosed dangerous failures λ_{DU}
1A, 24V, relay (LS1)	1.00E-06	60%	6.00E-07	100%	6.00E-07	0.00E+00
Solenoid Valve	1.00E-07	80%	8.00E-08	50%	4.00E-08	4.00E-08
Spool Valve	1.00E-07	80%	8.00E-08	50%	4.00E-08	4.00E-08
ESD Valve + actuator	2.00E-05 [NOTE 2]	90%	1.80E-05	100%	1.80E-05	0.00E+00
PST (sensors & diagnostics cct)	2.74E-06	10%	2.74E-07	50%	1.37E-07	1.37E-07
TOTALS	2.3938E-05		1.9034E-05		1.8817E-05	2.1690E-07

NOTE 1: failure mode is failure of the spool valve to remove pneumatic pressure on demand

NOTE 2: or, $\lambda = 2 \times 10^{-6}$ using minimum figures from Technis FARADIP.THREE database.

The safe failure rate, λ_S , is calculated from the total values of $\lambda - \lambda_D = 4.904 \times 10^{-6}$

$$\text{Safe failure fraction (SFF)} = \frac{\lambda - \lambda_{DU}}{\lambda} = \mathbf{99\%} [\lambda_{ESD} = 2 \times 10^{-5}] \text{ or } \mathbf{96\%} [\lambda_{ESD} = 2 \times 10^{-6}]$$

For all practical values of failure rate for an ESD valve and actuator the range of SFF lies between 90 to 99%. This meets the requirements for use in SIL3 safety functions.

3.10 Summary of failure rate data

From the previous section, the following summary failure rates are obtained which may be stated on a certificate of conformity.

Table 6: Summary failure rate data

Failure mode	Failure rates	Safe Failure Fraction (SFF)
Fail to close the spool valve when the PLC DO control signal is removed	$\lambda_{DU} = 2.17 \times 10^{-7}$ $\lambda_{DD} = 1.88 \times 10^{-5}$ $\lambda_S = 4.90 \times 10^{-6}$	90% - <99%

3.11 Use of recommended techniques and measures

An appropriate use of the recommended techniques and measures from IEC 61508-2 Annex A have been used in the design for the control of failures during operation. Most of the techniques and measures are not relevant to the safety function of the ESD valve controller (assuming diagnostics functions are support functions and not safety-related functions), but some aspects of Tables A.1, A.2, A.14 and A.15 do apply. Refer to Appendix 2 for details of the assessment.

3.12 Operating environment/constraints

The equipment is designed for use in ambient temperatures of -40 to +60°C. References to environmental constraints of operation are detailed in Appendix 2, TOE 6.

The ESD Valve Controller requires a suitable power source (outside scope of this assessment), however, the ESD Valve Controller is fail-safe in the event of a power loss.

The ESD Valve Controller uses embedded software to carry out the diagnostic functions. This software is outside the scope of this assessment, however, diagnostics are not themselves the object of reliability assessment.

3.13 Verification and Validation

Details of the manufacturer's verification and validation activities are recorded in the following documents:

- FRM-VTPR Validation test plan & results, 27-FEB-08
- Test Report 644 Validation extremes of temperature DXP ESD conventional, 09-DEC-07
- Test Report 645 Validation of over-pressure of ESD pushbutton, 09-DEC-07
- Test Report 646 Validation life test of ESD conventional, 09-DEC-07
- Test Report 655 Software/Hardware V&V test procedure & results, 06-MAR-08
- MTBF calculations.xls MTBF calculations, 09-DEC-07
- MTBF Plan 4_07.pdf MTBF test plan, 26-NOV-07

These activities included the testing of 24 pilot valves and 24 spool valves, both mounted in ESD Valve Controllers, and tested to over 3 million and 5 million cycles respectively.

3.14 E/E/PES lifecycle

To claim compliance with *all* the requirements of IEC 61508, TopWorx must demonstrate the ESD Valve Controller was realised using a lifecycle that conforms to the relevant requirements of IEC 61508-2 clause 7. Some of these requirements are addressed by the TopWorx accredited ISO 9001:2000 quality management system.

3.15 Management of functional safety

To claim compliance with *all* the requirements of IEC 61508, TopWorx must demonstrate the ESD Valve Controller was realised under a formal management system for functional safety that conforms to the relevant requirements of IEC 61508-1 clause 6. Some of these requirements are addressed by the TopWorx accredited ISO 9001:2000 quality management system.

3.16 Summary of base information which may be certified

Table 7: Base information

Product ID:	ESD valve controller, according to product variants specified in Topworx ES-01059-1.
Functional specification:	To close spool valve in response to removal of the pilot valve control signal
Environment / stress criteria:	Non-aggressive environments / normal quality specifications
Environment limits:	-40°C to +60°C
Lifetime limit:	10 years
Maintenance requirements:	Specified in manufacturer's user's manual
Repair constraints:	Specified in manufacturer's user's manual
Hardware fault tolerance:	0
Highest SIL (systematic):	SIL 3
Systematic fault tolerance measures:	High diagnostic coverage and fail-safe design
Validation records:	Assessed in Sira Report R56A16648A
Type A / Type B:	Type A
Proof test interval:	Refer to paragraph 3.8
Mean time to restoration (MTTR):	<4 hours

3.17 Conditions of Certification

The manufacturer of the certified equipment shall observe the following conditions of certification:

1. The manufacturer is required to collect and analyse failure data from returned products on an on-going basis. Sira Certification Service shall be informed in the event of any trend that could affect reliability of the safety function(s);

3.18 Conditions of Safe Use

The following conditions apply to the installation, operation and maintenance of the certified equipment. Failure to observe these may compromise the safety integrity of the certified equipment:

1. The probability of failure on demand (PFD) figure stated in this certificate is dependent on the stated Proof Test Interval and Mean time to restoration (MTTR) figures not being exceeded;
2. It is essential that the operator follow the calibration instructions correctly to make sure the valve functions properly during calibration and at each subsequent partial stroke test.
3. The user shall ensure that appropriate actions are taken to maintain the required risk reduction in the event that the diagnostics reveal a potential failure.

4 CONCLUSIONS AND RECOMMENDATIONS

The assessment of the evidence submitted by the applicant has shown that the equipment complies with the requirements of IEC 61508 Part 2 in respect of random hardware failure, Safe Failure Fraction (SFF) and architecture for use in safety instrumented functions up to and including SIL3.

It is therefore recommended that the ESD Valve Controller can be considered for certification to IEC 61508-2:2000 for the specified safety function(s), in respect of random hardware failure, Safe Failure Fraction (SFF) and architecture within the constraints given in the summary tables above.

APPENDIX 1 – FMEA OF THE DIAGNOSTICS CIRCUITS

This is the Partial Stroke Test (sensors & diagnostics circuit) shaded box in Fig 1 and Fig 2. Mode 1 below refers to failure to perform a partial stroke test and report the result via the relay signals and local LEDs

FARADIP3 6.2 Data output 18/03/2008
 Data file: Topworx ESD.FDP
 Topworx ESD
 Mode 1
 Environment factor 1.00 Quality factor 1.00

Component Ref	Component Name	Component Failure Rate	Total Failure Rate	Failure Mode	Mode 1 Factor	Failure Rate Mode 1	Diagnostic Coverage Mode 1
D21	LED	.3000	.3000	O/C	1.000	.3000	100.0
D2	LED	.3000	.3000	O/C	1.000	.3000	100.0
U1	OPTO	.2000	.2000	O/C	.3000	.0600	100.0
D3	LED	.3000	.3000	O/C	1.000	.3000	100.0
U4	OPTO	.2000	.2000	O/C	.3000	.0600	100.0
SW1	SWITCH	.1000	.1000	O/C	.3000	.0300	100.0
SW2	REED SWI	.2500	.2500	INTERM	.5000	.1250	50.00
SW3	REED SWI	.2500	.2500	INTERM	.5000	.1250	50.00
D4-8	DIODE	.0250	.0250	O/C	.1000	.0025	.0000
D9-12	DIODE	.0200	.0200	O/C	.1000	.0020	.0000
R4	FILM RES	.0010	.0010	O/C	.8000	.0008	100.0
R2	FILM RES	.0010	.0010	O/C	.8000	.0008	.0000
R3	FILM RES	.0010	.0010	O/C	.8000	.0008	100.0
R10	FILM RES	.0010	.0010	O/C	.8000	.0008	100.0
D22	DIODE	.0050	.0050	O/C	.1000	.0005	100.0
C2-3	CERAMIC	.0008	.0008	S/C	.5000	.0004	100.0
U3	REGULATO	.0200	.0200	O/P S/	.8000	.0160	100.0
C4-6	CERAMIC	.1500	.1500	S/C	.5000	.0750	100.0
R7	FILM RES	.0010	.0010	O/C	.8000	.0008	100.0
R6,8,1	FILM RES	.0030	.0030	O/C	.8000	.0024	100.0
C1	CERAMIC	.0500	.0500	S/C	.5000	.0250	100.0
D23-25	DIODE	.0150	.0150	S/C	.7500	.0112	100.0
R9	FILM RES	.0010	.0010	O/C	.8000	.0008	.0000
D17-20	DIODE	.0050	.0050	O/C	.1000	.0005	.0000
R5	FILM RES	.0010	.0010	O/C	.8000	.0008	.0000
D13-16	DIODES	.0200	.0200	O/C	.1000	.0020	.0000
U4	FET	.0600	.0600	S/C	.3000	.0180	.5000
U5	FET	.0600	.0600	S/C	.3000	.0180	.5000
U6	FET	.0600	.0600	S/C	.3000	.0180	.5000
U2	MICRO	.0700	.0700	ALL	.5000	.0350	.5000
LS2	RELAY PC	1.000	1.000	CONTAC	.6000	.6000	.5000
LS3	RELAY PC	1.000	1.000	CONTAC	.6000	.6000	.5000
J13	CONNECTO	.0010	.0010	ALL	.5000	.0005	.5000
J12	CONNECTO	.0010	.0010	ALL	.5000	.0005	.5000
J1-11	CONNECTO	.0100	.0100	ALL	.5000	.0050	.5000

Parts count
 Failure rate 4.483 per million hours
 MTBF 25.47 years

Mode 1
 Mode 1 failure rate 2.738 per million hours
 Mode 1 MTBF 41.69 years
 Mode 1 diagnostic cover 48.03 %
 Mode 1 safe failure fraction 68.26 %

Failure rate data used from FARADIP.THREE

Refer to table above for % contribution to the ESD Valve Controller failure mode.

Component	Failure rate (x 10⁻⁶ per hour)	Failure mode
LED	0.3	O/C
Opto-coupler	0.2	O/C
Pushbutton witch	0.1	O/C
Reed switch	0.25	Intermittent
Signal diode	0.005	O/C
Film resistor	0.001	O/C
Ceramic capacitor	0.004	S/C
Regulator IC	0.02	S/C
FET	0.06	S/C
PIC micro	0.07	All
PCB Relay	1.0	Contact & coil
Connector	0.001	All

APPENDIX 2 – ASSESSMENT OF USE OF TECHNIQUES AND MEASURES (IEC 61508 –2, ANNEX A)

Table A.1 - Faults or failures to be detected during operation or to be analysed in the derivation of safe failure fraction

Component	See table(s)	Requirements for diagnostic coverage or safe failure fraction claimed			Evidence/Comments
		Low (60 %)	Medium (90 %)	High (99 %)	
Electromechanical devices	A.2	Does not energize or de-energize	Does not energize or de-energize	Does not energize or de-energize	<p>Faults in the relay coil (LS1) or pilot coils will be revealed by the lack of response from the ESD valve during partial stroke test (PST).</p> <p>Faults in the relay coil (LS2 and LS3) will be revealed during partial stroke test (PST) and can also be cross-checked against the LED flashes.</p>
		Welded contacts	Individual contacts welded	Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent)	<p>Faults in the relay contacts (LS1) will be revealed by the lack of response from the ESD valve during partial stroke test (PST).</p> <p>Faults in the relay contacts (LS2 and LS3) will be revealed during partial stroke test (PST) and can also be cross checked against the LED flashes</p>
				No positive opening (for position switches this failure is not assumed if they are built and tested according to EN 60947-5-1, or equivalent)	Position switches have been tested to over 50 million cycles with less than 10 failures per billion hours (FITs).
Discrete hardware	A.3, A.7, A.9, A.11				There only electrical components performing the safety function are the interrupting relay (LS1) and pilot valve coils. These can only fail-safe, and faults are identified during PST.
Digital I/O		Stuck-at	DC fault model	DC fault model drift and oscillation	
Analogue I/O		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation	
Power supply		Stuck-at	DC fault model drift and oscillation	DC fault model drift and oscillation	

Component	See table(s)	Requirements for diagnostic coverage or safe failure fraction claimed			Evidence/Comments
		Low (60 %)	Medium (90 %)	High (99 %)	
Bus					N/A
General	A.3 A.7	Stuck-at of the addresses	Time out	Time out	
Memory management unit	A.8	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding	
Direct memory access		No or continuous access	DC fault model for data and addresses	All faults which affect data in the memory	
			Wrong access time	Wrong data or addresses	
				Wrong access time	
Bus-arbitration (see note 1)		Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration	
CPU	A.4,A.10				N/A
Register, internal RAM		Stuck-at for data and Addresses	DC fault model for data and addresses	DC fault model for data and addresses	
				Dynamic cross-over for memory cells	
				No, wrong or multiple addressing	
Coding and execution including flag register		Wrong coding or no Execution	Wrong coding or wrong execution	No definite failure assumption	
Address calculation		Stuck-at	DC fault model	No definite failure assumption	
Program counter, stack pointer		Stuck-at	DC fault model	DC fault model	
Interrupt handling	A.4	No or continuous Interrupts	No or continuous interrupts	No or continuous interrupts	
			Cross-over of interrupts	Cross-over of interrupts	
Invariable memory	A.5	Stuck-at for data and	DC fault model for data and addresses	All faults which affect data in the memory	N/A

Component	See table(s)	Requirements for diagnostic coverage or safe failure fraction claimed			Evidence/Comments
		Low (60 %)	Medium (90 %)	High (99 %)	
		addresses			
Variable memory	A.6	Stuck-at for data and addresses	DC fault model for data and addresses	DC fault model for data and addresses	N/A
			Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher	Dynamic cross-over for memory cells	
				No, wrong or multiple addressing	
				Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher	
Clock (quartz)	A.12	Sub- or super-harmonic	Sub- or super-harmonic	Sub- or super-harmonic	N/A
Communication and mass storage	A.13	Wrong data or addresses	All faults which affect data in the memory	All faults which affect data in the memory	N/A
		No transmission	Wrong data or addresses	Wrong data or addresses	
			Wrong transmission time	Wrong transmission time	
			Wrong transmission sequence	Wrong transmission sequence	
Sensors	A.14	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation	Position switches have been tested to over 50 million cycles with less than 10 failures per billion hours (FITs).
Final elements	A.15	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation	The ESD valve controller is not a final element, however, it's function is to detect the fault modes stated opposite.

NOTE 1 Bus-arbitration is the mechanism for deciding which device has control of the bus.

NOTE 2 "Stuck-at" is a fault category which can be described with continuous "0" or "1" or "on" at the pins of a component.

NOTE 3 "DC fault model" (DC = direct current) includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines.

Table A.2 - Electrical subsystems

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes	Evidence/Comments
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection	PST can be an on-line method. Frequency of on-line tests can be set by the user.
Monitoring of relay contacts	A.1.2	High		Conforms, as previously stated against Table A.1.
Comparator	A.1.3	High	High if failure modes are predominantly in a safe direction	N/A
Majority voter	A.1.4	High	Depends on the quality of the voting	N/A
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC	N/A

NOTE 1 This table does not replace any of the requirements of annex C.

NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.

NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.3 – Electronic subsystems

Not used in the safety function

Table A.4 - Processing units

Not used in the safety function

Table A.5 - Invariable memory ranges

Not used in the safety function

Table A.6 - Variable memory ranges

Not used in the safety function

Table A.7 - I/O units and interface (external communication)

Not used in the safety function

Table A.8 - Data paths (internal communication)

Not used in the safety function

Table A.9 - Power supply

Not used in the safety function

Table A.10 - Program sequence (watch-dog)

Not used in the safety function

Table A.11 - Ventilation and heating system (if necessary)

Not used in the safety function

Table A.12 - Clock

Not used in the safety function

Table A.13 - Communication and mass-storage

Not used in the safety function

Table A.14 – Sensors

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes	Evidence/Comments
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection	PST can be an on-line method. Frequency of on-line tests is set by the user.
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC	Not used. Magnetic reed switches are employed for position sensing.
Analogue signal monitoring	A.2.7	Low		N/A
Test pattern	A.6.1	High		N/A
Input comparison/voting (1oo2, 2oo3 or better redundancy)	A.6.5	High	Only if dataflow changes within diagnostic test interval	N/A
Reference sensor	A.12.1	High	Depends on diagnostic coverage of failure detection	Not used.
Positive-activated switch	A.12.2	High		Not used.

- NOTE 1 This table does not replace any of the requirements of annex C.
 NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.
 NOTE 3 For general notes concerning this table, see the text preceding table A.1.

Table A.15 - Final elements (actuators)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes	Evidence/Comments
Failure detection by on-line monitoring	A.1.1	Low (low demand mode) Medium (high demand or continuous mode)	Depends on diagnostic coverage of failure detection	Used (PST). This is effected what the ESD valve controller does.
Monitoring of relay contacts	A.1.2	High		This is done and faults revealed at PST, although contacts can only fail safe.
Idle current principle	A.1.5	Low	Only for E/E/PE safety-related systems where continuous control is not needed to achieve or maintain a safe state of the EUC	Not used.
Test pattern	A.6.1	High		Not used.
Monitoring	A.13.1	High	Depends on diagnostic coverage of failure detection	Used (PST). This is effected what the ESD valve controller does.
Cross-monitoring of multiple actuators	A.13.2	High		Not used.

- NOTE 1 This table does not replace any of the requirements of annex C.
 NOTE 2 The requirements of annex C are relevant for the determination of diagnostic coverage.
 NOTE 3 For general notes concerning this table, see the text preceding table A.1.

APPENDIX 3 – ASSESSMENT OF THE E/E/PES SUB-SYSTEM (IEC 61508 –2)

E/E/PES SUB-SYSTEM DATA TABLE

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
1	sub-system identification	All information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management of the E/E/PE safety-related system in accordance with 1/6.2.1.	2/7.4.7.3(n)		Schematics, PCB layout and BoMs are defined and controlled by drawing part number and revision. Mechanical piece parts and assembly is defined and controlled on drawings. The matrix of options are shown on the ESD Master Nomenclature drawing ES-01309-1.
2	a functional specification	required to define those functions and interfaces of the subsystem which can be used by safety functions.	2/7.4.7.3 (a) 2/7.4.7.4 2/7.4.7.12		Technical specification is ES-01059-1 Rev 1.
3	The estimated rates of failure (due to random hardware failures) in any modes.	Required as input to the application-specific allocations of failure rates to safe and dangerous failure modes, which then permits the calculation of SFF and PFD. Proposed for these templates to be in the form of: Overall Failure Rate (all functional failures, all modes) Plus, for each failure mode: <ul style="list-style-type: none"> • % of overall Failure rate • function affected • consequence for the output signal 	2/7.4.7.3 (b) 2/7.4.7.3.(j) 2/7.4.7.4 2/7.4.3.2 for PFD context 2/ Annex A 2/ Annexe C 7/B.6.6.1 2/7.4.7.9 for PIU	Requires an environment context for the overall failure rate, or range of overall failure rates, which is relevant to the expected conditions of use. The use of an overall failure rate, and allocation of percentages to failure modes, presumes that the percentage allocation will be valid over the range of overall failure rates. Where that is not valid e.g. one failure mode becomes more dominant in certain conditions then that should be clear in the presented data.	Probability of random hardware failure (λ) has been assessed – see section 3 of this report.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
		<ul style="list-style-type: none"> externally available diagnostic indication of the failed state 			
4	diagnosed (dangerous) failure rates	Required as input to calculation of SFF and PFD. The estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are detected by diagnostic tests.	2/7.4.7.3 (b) 2/7.4.7.4 2/7.4.7.3.(j) 2/ Annex A	<p>The referenced clauses in IEC61508 require dangerous failure rates to be defined. Categorisation into safe and dangerous states can only be provided when accompanied by the assumptions for the application context</p> <p>Annex A places constraints on the claims for diagnostic techniques, and requires the diagnostic coverage claim to be justified for non-proven-in-use sub-systems</p>	Probability of diagnosed random hardware failure (λ_{DD}) has been assessed – see section 3 of this report.
5	un-diagnosed dangerous failure rates	Required as input to calculation of SFF and PFD. The estimated rates of failure (due to random hardware failures) in any modes which would cause a dangerous failure of the E/E/PE safety-related system, which are undetected by diagnostic tests (see 2/7.4.7.4)	2/7.4.7.3 © 2/7.4.7.4 2/7.4.7.3.(j)	<p>The referenced clauses in IEC61508 require dangerous failure rates to be defined. This is not valid at the generic sub-system level without an application context defining safe and dangerous states.</p> <p>The information required here is therefore described by the consequences of the failure on the critical parameters involved. (e.g. relay contact stuck closed)</p> <p>Categorisation into safe and dangerous states can be provided in addition, but only when accompanied by the assumptions for the application context</p> <p>A failure rate for each identified mode of</p>	Probability of undiagnosed random hardware failure (λ_{DU}) has been assessed – see section 3 of this report

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
				<p>failure. (see notes on 'diagnosed dangerous failures')</p> <p>Techniques for assessment of failure rate are referenced in 2/7.4.7.4, with guidance. The choice is between design assessment, or 'Proven-in-use' evidence. For 'Proven-in-use' the failure rate will include systematic failures.</p>	
6	environmental limits	any limits on the environment of the subsystem which should be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures	2/7.4.7.3 (d)		<p>Temperature specification as per the hazardous area certification code: -40 to +60°C</p> <p>Test request no. 10152007RG, ref no. 644, report date Dec 9th 2007, submitted showing test plan and results of 4 samples functionally tested from -45 to +65°C. The functional tests were manually operated once they had stabilised at temperature. All 4 samples passed.</p> <p>A humidity specification is not given.</p> <p>An EMC specification is not given/relevant</p> <p>Test request no. 11142007JA, ref no. 645, report date Dec 9th 2007, submitted showing test plan and results of 1 sample subjected to a pushbutton overpressure test. The sample passed the test, withstanding up to 2000 PSIG.</p>

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
7	lifetime limits	any limit on the lifetime of the subsystem which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failures	2/7.4.7.3 (e)	consider wear out caused by design or application, e.g. capacitor or battery life, hardening of seals, run-time of bearings etc.	10-year lifetime limit specified. Test request no. 10152007JA, ref no. 646, report date Dec 9 th 2007, submitted showing test plan and results of 3 samples which were subjected to 1,000,000 partial stroke test cycles. All 3 samples passed.
8	proof test requirements	any periodic proof test requirements	2/7.4.7.3 (f)	<ul style="list-style-type: none"> the purpose of the test, with respect to otherwise unrevealed failure modes the test procedure the typical time required to perform the test the extent to which hidden faults are revealed by the test. (see 4/ 3.8.5) the tests associated with the diagnostic functions 	Proof tests are required to reveal dangerous failures in the ESD valve. See section 3 of this report for the test interval against probability of failure.
9	maintenance requirements	any periodic maintenance requirements	2/7.4.7.3 (f)	<ul style="list-style-type: none"> the purpose of the maintenance the maintenance procedure the recommended in-service interval for maintenance. 	Some assembly diagrams are given in the IO&M manual. There are no routine maintenance instructions required other than the routine PST.
10	diagnostic coverage	the diagnostic coverage derived according to annex C. This information is required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/E/PE safety-related system.	2/7.4.7.3 (g) 2/Annex C 2/ 7.4.3.2.2 2/Annex A and all sub-sections	<p>see note 1 under 2/7.4.7.3 (h). This data is related to the internal sub-system diagnostics available with every instance of the sub-system.</p> <p>Where the defined ID of the sub-system includes an external diagnostic function, then all relevant parameters within this template related to the external diagnostic</p>	Covered in section 3 of this report.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
				<p>function must also be provided.</p> <p>Annex A places constraints on the claims for diagnostic techniques.</p> <p>Note that failure rate of any internal or external diagnostic function is required to be included in the full assessment of diagnostic coverage, and will be captured if a separate template is used for the diagnostic function as a stand-alone sub-system.</p>	
11	diagnostic test interval	the diagnostic test interval, when required. This information is required when credit is claimed for the action of the diagnostic tests performed in the subsystem in the reliability model of the E/E/PE safety-related system.	2/7.4.7.3 (h) 2/Annex C	<p>see note 1 under 2/7.4.7.3 (h). This data is related to the internal sub-system diagnostics available with every instance of the sub-system.</p> <p>Where the defined ID of the sub-system includes an external diagnostic function, then all relevant parameters within this template related to the external diagnostic function must also be provided.</p>	Partial Stroke Testing is effectively performing a background diagnostic on the hardware, without disrupting the process. This is performed automatically (by a PLC or DCS) or manually – see section 3.
12	other repair constraints	any additional information (e.g. repair times) which is necessary to allow the derivation of a mean time to restoration (MTTR) following detection of a fault by the diagnostics;	2/7.4.7.3 (i)	<p>Any maintenance, re-calibration, or other activities in addition to standard repair times and procedures should also be identified.</p> <p>Note that a standard repair time given by a sub-system supplier must be qualified by the assumed context, and will not necessarily take into account the application</p>	MTTR for the ESD Valve Controller has been stated by the manufacturer as 4 hours. A condition of safe use states that this figure could be increased by factors associated with the specific application. Also, this figure does not include the MTTR for the specific ESD valve.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
				context. Thus there may be several factors contributing to the actual MTTR as used in an application.	
13	safe failure fraction	all information which is necessary to enable the derivation of the safe failure fraction (SFF) of the subsystem as applied in the E/E/PE safety-related system, determined according to annex C. Needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints.	2/7.4.7.3 (j) 2/Annex C	The requirement is for all information related to failure rate and diagnostic coverage, placed into the application context for safe and dangerous failure modes, which are then used for calculation of SFF. The calculation of SFF cannot be done without knowledge of the safe, dangerous, and external diagnostic support context. A SFF number must always be accompanied by the application context information. This relates to the inherent architecture and fault tolerance available with every instance of the sub-system, and not application-specific combinations.	This is calculated as between 90% and <99% - see section 3 of this report.
14	hardware fault tolerance	the hardware fault tolerance of the subsystem. Needed to determine the highest safety integrity level that can be claimed for a safety function according to the architectural constraints	2/7.4.7.3 (k)	this relates to the inherent architecture and fault tolerance available with every instance of the defined sub-system, and not application-specific combinations.	The ESD Valve Controller has a zero hardware fault tolerance - see section 3 of this report.
15	Highest SIL (architecture)	the highest safety integrity level that can be claimed for a safety function according to	2/7.4.7.3 (j) 2/7.4.7.3 (k) for Type A/B	This claim depends on the selection of Type A/ Type B sub-system table, and on the SFF. The Type A/Type B classification and	SIL3 is the highest safety integrity level that can be claimed for the ESD Valve Controller on the basis of the architectural constraints.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508:2000 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
		the architectural constraints, derived from the hardware fault tolerance and SFF	2/7.4.3.1.2 2/7.4.3.1.3	<p>the SFF must always consider the application context. Consequently the Highest SIL (Architecture) is always application context dependent.</p> <p>There are also constraints imposed on the highest claimable SIL by consideration of systematic faults for Proven By Design sub-systems, and those constraints may further restrict the overall claim for the sub-system.</p>	
16	systematic failure constraints	any limits on the application of the subsystem which should be observed in order to avoid systematic failures.	2/7.4.7.3 (l)	Any requirements or constraints about the way the sub-system should be employed for safety applications, or constraints related to the extent of validity of the available data.	Refer to the section in this report on conditions of certification and safe use.

PROVEN-IN-USE SPECIFIC DATA TABLE

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
17	Evidence of similar conditions in previous use.	Demonstrates that the previous conditions of use of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/E/PE safety-related system.	2/7.4.7.7 2/7.4.7.6 2/7.4.7.10 2/7.4.7.11		Not applicable
18	Evidence supporting the application under different conditions of use.	Required to justify the use of failure rates established under different operating conditions.	2/7.4.7.8 2/7.4.7.10 2/7.4.7.11		Not applicable
19	Evidence of period of operational use	Required to support the claimed rates of failure on a statistical basis.	2/7.4.7.9 2/7.4.7.10 2/7.4.7.11 1/4.1		Not applicable
20	Statement of restrictions on functionality.	Required in order to restrict the application of a 'proven-in-use' safety-related subsystem to those functions and interfaces of the subsystem which meet the relevant requirements.	2/7.4.7.12 2/7.4.7.6 to 2/7.4.7.10 3/7.4.2.11		Not applicable

SUB-SYSTEM PROVEN BY DESIGN - SPECIFIC DATA TABLE

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
21	highest SIL - (systematic)	the highest safety integrity level that can be claimed for a safety function which uses the subsystem on the basis of the supporting evidence for control and avoidance of systematic faults	2/7.4.7.3 (m)	The systematic SIL must be related to a specified function, and the supporting evidence from TOEs 22 and 23 must relate to that same function	For the function stated for this equipment in paragraph 1.5 of this report, the systematic SIL that can be claimed is SIL3.
22	systematic fault avoidance measures (see TOE 21)	description of those measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software of the subsystem	2/7.4.7.3 (m) 2/7.4.4.1 3/7.4 2/Annexe B, Tables 2/ B2 with B6	The information here is part of the mapping process between the design and testing methodologies, and the requirement in IEC61508. Evidence that the measures and techniques have been appropriately applied, consistent with the SIL claimed. Expecting a response directly relating the techniques employed to those defined in the table, with the identification of the SIL achieved by reference to effectiveness in Table 2/B6 or the appropriate tables from Part 3 for software.	Systematic fault avoidance measures have been addressed through control of the development lifecycle, including V&V activities evaluated in this assessment as listed in paragraph 2.1.2.
23	systematic fault tolerance measures (see TOE 21)	description of the design features which make the subsystem tolerant against systematic faults	2/7.4.7.3 (m) 2/7.4.5.1 2/7.4.8 2/Annexe A3 2/Tables A16, A17, A18, in conjunction with A 19 3/7.4.3	Evidence that the features have been appropriately incorporated, consistent with the SIL claimed. Expecting a response directly relating the techniques employed to those defined in each of the tables, with the identification of the SIL achieved by reference to effectiveness in Table 2/A19, or the appropriate tables from Part 3 for software. A16 requires aspects of redundancy,	Systematic fault tolerance measures are high diagnostic coverage, frequent automatic testing and fail-safe design. Refer to section 3 of this report for more details.

	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses and Tables	Template prompts / comments	Evidence assessed / comments
				diagnostics, retry mechanisms etc. A17 requires measures against environmental hazards A18 requires consideration of operations aspects (modification, confirmation of operator action etc)	
24	validation records	documentary evidence that the subsystem has been validated according to clauses 2/7.7 and 3/7.of this standard.	2/7.4.7.3 (o) 2/7.7 3/7.7	Required as a validation statement or reference to a validation report for each parameter provided.	V&V documents evaluated as listed in paragraph 2.1.2 of this report have been evaluated. ESD valve controller has been extensively tested to several million cycles in order to establish specific failure rates of safety related components (sensors, pilot valves and spool valves).