FUNCTIONAL SAFETY CERTIFICATE

This is to certify that the hardware safety integrity of the

Valvetop ESD Valve Controller

manufactured by

TopWorx Inc.
3300 Fern Valley Road
Louisville
Kentucky 40213
USA

has been assessed by Sira Certification Service
and found to meet the requirements of

IEC 61508-2:2000

The certified data set herein may be used in the design of safety functions up to and including safety integrity level 3 (SIL3), subject to the stated conditions and scope in this certificate.

Certification Manager:

D R Stubbings

Initial Certification:	25 March 2008
This certificate issued:	14 November 2011
Renewal date:	25 March 2013

Sira Certification Service
Rake Lane, Eccleston, Chester, CH4 9JN, England
Tel: +44 (0) 1244 670900
Fax: +44 (0) 1244 681330
Email: info@siracertification.com
Web: www.siracertification.com

Product description and scope of certification

The Valvetop ESD 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 instrumented functions.

The ESD Valve Controller enables the ESD process valve to be exercised by partially closing (typically to 80 - 85% of full stroke) and monitoring the time the valve takes to reach this position. This time is compared with the pre-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.

Safety function(s)

The safety function of the certified equipment is:

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

Hardware safety integrity

Control of dangerous failures during operation is achieved by:

- high diagnostic coverage
- fail-safe design

Identification of certified equipment

The certified equipment and it's safe use is defined in the manufacturer's documentation listed in Table 1 below.

Table 1: Certified 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 *[1]
S-AV1-0003	1 of 1	13	13-MAR-08	Cold temp valve assembly *
ES-01309-1	-	02	17-Oct-11	ESD Master Nomenclature *
ES-00936-1	-	03	-	Install, Ops and Maintenance Manual
ES-006891	1 of 1	12	16-Sept-11	Assembly, Lower Housing, DXP[1]

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

[1] The DXP and DXR enclosure are a no part failure effect and do not contribute to the safe failure fraction or failure rate of the ESD valve controller.

Sira Certification Service
Rake Lane, Eccleston, Chester, CH4 9JN, England
Tel: +44 (0) 1244 670900
Fax: +44 (0) 1244 681330
Email: info@siracertification.com
Web: www.siracertification.com

Certified Data Set in support of use in safety functions

The following failure modes and probabilities have been calculated for the certified equipment by a failure modes and effect analysis (FMEA).

Table 2: Failure rate data

Failure mode	Failure rates	Safe Failure Fraction (SFF)
Fail to remove pneumatic pressure when the pilot valve control signal (e.g., PLC DO) is removed	λ_{DU} = 2.17 x 10^{-7} λ_{DD} = 1.88 x 10^{-5} λ_{S} = 4.90 x 10^{-6}	90% - <99%

The PFD_{ave} for the ESD valve controller may be calculated from it's component failure rates, the dangerous failure rate of the ESD valve (and actuator) and the proof test interval (T). The following formula may be used:

$$PFD_{ave} = [(1.2 \times 10^{-6} + \lambda_{VALVE} + \lambda_{ACTUATOR}) \times 2.738 \times 10^{-6}] \times T^2 / 3$$

The following table gives proof test intervals for sample failure rates of ESD valves (+ actuator) that will achieve 50% of the permitted allowance of PFD_{ave} for SIL3 safety functions. (Figures assume the Topworx ESD valve controller is used to diagnose residual failures of the ESD valve and actuator which are not diagnosed by any other means).

Table 3: Proof test intervals for sample ESD valve + actuator failure rates

$\lambda_{VALVE} + \lambda_{ACTUATOR}$ (per hr)	Proof test interval to meet 50% of SIL3 PFD
1 x 10^{-4}	2,327
1 x 10^{-5}	6,994
1 x 10^{-6}	15,780
1 x 10^{-7}	20,528

Notes on the certified data set:

1) The formula above to calculate PFD_{ave} assumes the value of MTTR shown in Table 4 is used which is insignificant.
2) SFF of the certified equipment assumes the following application context:
    - the safety function of the process ESD valve (via it's associated actuator) is to perform it's safety function on removal of pneumatic drive
    - no further external diagnostics are used
3) Attention is drawn to the conditions for safe use in this certificate when using the certified data set in the design of safety functions.

Sira Certification Service
Rake Lane, Eccleston, Chester, CH4 9JN, England
Tel: +44 (0) 1244 670900
Fax: +44 (0) 1244 681330
Email: info@siracertification.com
Web: www.siracertification.com

Table 4: Base information table

Product ID:	ESD valve controller, according to product variants specified in Topworx ES-01059-1.
Functional specification:	The spool valve to remove pneumatic pressure when the pilot solenoid valve control signal (e.g., PLC DO) is removed
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 (T):	See values in Table 3
Mean time to restoration (MTTR):	<4 hours

Conditions of Certification

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

1. The manufacturer is required to collect and analyze 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).
2. Sira shall be notified in advance before any modifications to the certified equipment are carried out.

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 Proof Test Interval (T) and Mean Time To Restoration (MTTR) figures shown in Table 4 not being exceeded;

Sira Certification Service
Rake Lane, Eccleston, Chester, CH4 9JN, England
Tel: +44 (0) 1244 670900
Fax: +44 (0) 1244 681330
Email: info@siracertification.com
Web: www.siracertification.com

2. When integrating the certified equipment into an overall safety system whose function is intended to mitigate or prevent the occurrence of a hazard, users should make use of the failure probability data quoted to determine the level of risk-reduction required of the certified equipment within the overall safety integrity target for the entire function.
3. Strict adherence to all the requirements, ratings and conditions stated in the manufacturer's user documentation;
4. Installation, calibration and maintenance activities shall be carried out by competent personnel, observing all stated manufacturer's recommendations;
5. Only the manufacturer's recommended replacement parts shall be used;
6. 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.

General Notes

1. This certificate is based upon a functional safety assessment of the certified equipment described in Sira Test & Certification confidential assessment report number R56A16648A.
2. If certified product or system is found not to comply, Sira Certification Service should be notified immediately at the address shown on this certificate.
3. This Certificate and the Sira Certification Mark are subject to the 'Regulations Applicable to the Holders of Sira Certificates' and 'Supplementary Regulations Specific to Functional Safety Certification'.
4. This document remains the property of Sira and shall be returned when requested by the company.

Sira Certification Service
Rake Lane, Eccleston, Chester, CH4 9JN, England
Tel: +44 (0) 1244 670900
Fax: +44 (0) 1244 681330
Email: info@siracertification.com
Web: www.siracertification.com