FUNCTIONAL SAFETY ASSESSMENT REPORT

K-Series Valvetop Indicators

By:

TOPWORX

Assessor:	DKilshaw	**David Kilshaw** **BSc (Hons) MIET** Functional Safety Engineer CSA Group UK Ltd – Sira
Verified By:		**James Lynskey** **BEng (Hons) MIET MInstMC MSaRS** Functional Safety Team Lead CSA Group UK Ltd - Sira
Date of issue:		**03 January 2019**
Customer:		**Topworx**
Report Number:		**R70198140A v0.1**

Commercially in Confidence

Table of Contents

Revision History

REV	DATE	PROJECT REF.	COMMENT	VERIFIED BY
0.1	03/01/2019	70198140	Interim draft hardware assessment report	JL
1.0	04/01/2019	70198140	Final hardware assessment report	JL

1 Introduction

1.1 References

Carried out by:	CSA Group Testing UK Ltd - Sira Unit 6 Hawarden Industrial Park Hawarden CH5 3US UK
For:	Topworx Inc 3300 Fern Valley Road Louisville Kentucky 40213 USA
Equipment assessed:	K-Series Valvetop Indicators
Date of Request for Assessment:	September 2018
Assessment standards:	IEC 61508-2:2010 Requirements for electrical/electronic/ programmable electronic safety-related systems.
Certificate number:	FSP 19001
Assessment conducted:	September 2018

1.2 Scope of this Document

The objective of this report is to assess the suitability of the K-Series Valvetop Indicators for use in safety related systems that perform a safety function with a specified safety integrity level (SIL).

System integrators that design safety related systems require verified information for the elements that will be used to form the safety instrumented system. The purpose of this report is to assess the failure data and examine the relevant information of the K-Series Valvetop Indicators in order to assist system designers in achieving the required functional safety of the system.

This report is concerned with the hardware safety integrity assessment of the K-Series Valvetop Indicators. The manufacturer's generic quality management system and product lifecycle have been assessed during the course of this product assessment; see APPENDIX 3. Certification of this product is based on satisfactory assessment of both the hardware and systematic capability of Topworx. The relevant requirements from IEC 61508 that apply to an element / subsystem and how these are divided between the separate reports are shown below.

Table 1: Requirements from IEC 61508

Sira report	Scope	IEC 61508:2010 reference
R70198140A (This Report)	General requirements	Part 2: 7.4.2
	Architectural constraints	Part 2: 7.4.4
	Random hardware failures	Part 2: 7.4.5, Annex C
	Avoidance of systematic faults	Part 2: 7.4.6
	T & M to control failures during operation (systematic faults)	Part 2: 7.4.7, Annex A
	System behaviour on fault detection	Part 2: 7.4.8
	Verified documentation	Part 2: 7.4.9, Annex D
	~~Proven in Use elements~~	~~Part 2: 7.4.10~~
	~~Additional requirements for data communication~~	~~Part 2: 7.4.11~~
APPENDIX 3	Manufacturer's product development lifecycle, including evidence of traceability for the product being assessed	Part 2: 7.1
topworx_FSM_70 005301	T & M to avoid systematic failures during the lifecycle	Part 2: 7.4.6, Annex B
	Management of functional safety	Part 1: 6.2

1.3 Summary of Assessment

As part of the product assessment and supporting evidence of conformity in with respect to *'hardware safety integrity'* against the requirements of IEC 61508-2; Topworx have submitted the K-Series Valvetop Indicators for FMEA assessment to attain SIL capability. The component failure rates and modes for the K-Series Valvetop Indicators have been extracted from or calculated using Quanterion Automated Databook, Item Toolkit and Faradip 3.0. Table 2 summarises the FMEA assessment for the K-Series Valvetop Indicators.

Table 2: FMEA Summary for the K-Series Valvetop Indicators without GO switch

Safety Function: *To provide an indication of the monitored valve position via 2 outputs via:* *1- 4-20mA output using 5337D module* *2- GO – switches, reed or standard switches.* Output current signal will be as follows: • Valve fully open = 20mA • Valve fully closed = 4mA • Faults 0 mA.					
Summary of IEC 61508-2 Clauses 7.4.2 and 7.4.4		K-Series Valvetop Indicators			
Architectural constraints & Type of product A/B		HFT = 0 Main parts: Type A	HFT = 1 Magnet & SW1&2,Type A	HFT = 0, 5337D 4-20mA module Type B	Overall output, magnet+ 5337D Overall Indicator K-Series
Safe Failure Fraction (SFF)		SFF : (73%) SIL 2 (1oo1)	SFF: 20% SIL 2 (1oo2)	SFF: 75.6% SIL 1 (1oo1)	SIL 2
Random hardware failures: [h^{-1}]	λ_{DD} λ_{DU}	0.0 4.5E-09	0.0 6.55E-09	0.0 1.04E-07	0.0 1.74E-07
Random hardware failures: [h^{-1}]	λ_{SD} λ_{SU}	0.0 1.23E-08	0.0 8.06E-08	0.0 3.23E-07	0.0 3.51E-07
Diagnostic coverage (DC) Common Cause Failures		0.0%	0.0% β : 10%	0.0%	0.0%
PFD @ PTI = 8760 Hrs. MTTR = 8 Hrs.					7.62E-04
Probability of Dangerous failure, High Demand, PFH h^{-1}]		4.5E-09	6.55E-09	1.04E-07	1.74E-07
Hardware safety integrity		Route 1_H			
Systematic safety integrity		Route 1_S			
Systematic Capability (SC1, SC2, SC3, SC4)		**SC 3**			
Hardware safety integrity achieved		**SIL 2 (Low Demand)** **SIL 2 (High Demand)**			

2 Terms and Definitions

For a full definition of terms used in functional safety, refer to IEC 61508-4. For convenience, some of the commonly used terms are given below.

1oo1, 1oo2, etc.	Nomenclature to indicate voting of channels
E/E/PES	Electrical/Electronic/Programmable-Electronic safety-related Systems
ESD	Emergency shutdown
FMEDA	Failure modes, effects and diagnostics analysis
FSM	Functional safety management
HFT	Hardware fault tolerance
MTTR	Mean time to repair
NCR	Non-Conformity Report
PFD_{AVG}	Probability of failure on demand (average)
PLC	Programmable Logic Controller
PTI	Proof test interval
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TOE	Target of Evaluation (used in CASS methodology)
Type A	Non-complex component or sub-system (e.g., switch, mechanical device)
Type B	Complex component or sub-system (e.g. programmable device)
UKAS	United Kingdom Accreditation Service

3 Overview of Equipment Submitted for Assessment

The TopWorx™ K-Series switchbox gives you a compact, robust product that conforms to the latest European Directives. The use of quality materials and attention to detail in the design and manufacturing processes has resulted in an excellent reputation for reliability. The requirement for maintenance has been virtually eliminated.

Figure 1: Typical Assembly of the K-Series Valvetop Indicators

3.1 Hardware Functional Description

The K-Series Valvetop Indicators implements its safety function as an element as defined according to IEC 61508-2 clause 7.4.2.11. Furthermore, with reference to IEC 61508-2 clause 7.4.4.1.3, the full assembly can be classified as a Type B element.

A functional wiring diagram of the K-Series Valvetop Indicators is shown in Figure 2 below.

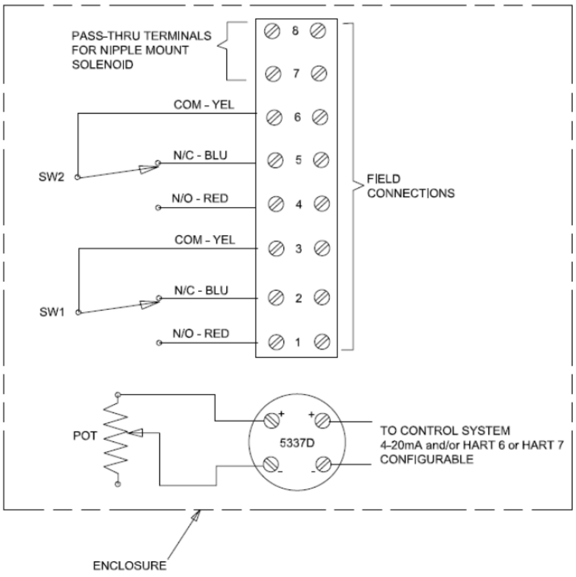
PASS-THRU TERMINALS FOR NIPPLE MOUNT SOLENOID
8
7
COM - YEL
6
N/C - BLU
5
SW2
N/O - RED
4
FIELD CONNECTIONS
COM - YEL
3
N/C - BLU
2
SW1
N/O - RED
1
POT
+
+
5337D
-
-
TO CONTROL SYSTEM 4-20mA and/or HART 6 or HART 7 CONFIGURABLE
ENCLOSURE

Figure 2: Wiring illustration of the internal configuration of K-Series.

1. K1*-0H* - K1 size enclosure with HART output
2. K1*-0X* - K1 size enclosure with 4-20mA output
3. K2*-0H* - K2 size enclosure with HART output
4. K2*-0X* - K2 size enclosure with 4-20mA output
5. K2*-LH* - K2 size enclosure with HART and pre-certified model 35 GO switch output
6. K2*-LX* - K2 size enclosure with 4-20mA output and pre-certified model 35 GO switch output

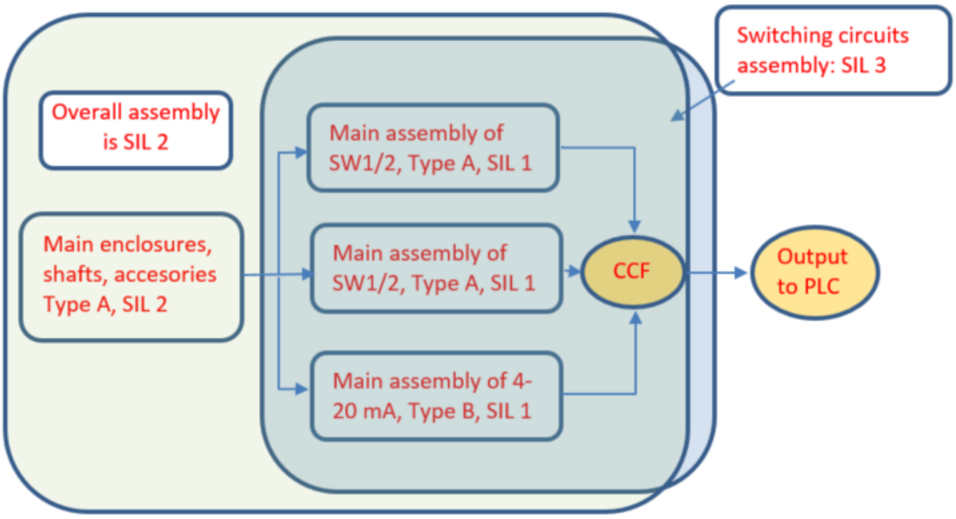
Switching circuits assembly: SIL 3
Overall assembly is SIL 2
Main enclosures, shafts, accesories Type A, SIL 2
Main assembly of SW1/2, Type A, SIL 1
Main assembly of SW1/2, Type A, SIL 1
Main assembly of 4-20 mA, Type B, SIL 1
CCF
Output to PLC

Figure 3: a reliability block diagram of the K-Series Topvalve indicators.

3.2 Element Safety Function

The element safety functions of the K-Series Valvetop Indicators are defined as follows:

To provide an indication of the monitored valve position via 4-20mA output and any combinations of Go – Switches.

4-20mA output will be as follows:

- Valve fully open = 20mA
- Valve fully closed = 4mA
- Hardware fault : 0 mA

3.2.1 No Fault (normal) Conditions

Under normal operating conditions the K-Series Valvetop will monitor the position of the attached valve and show the correct position on the beacon assembly. The electrical signal provided by the switch assembly will match the position of the bacon. The K-series includes a 2-wire 4-20mA/HART output which is used as an indication of the valve position. When the valve is fully open, the output will be 20mA and when the valve is fully closed the output will be 4mA. This is achieved using a potentiometer which is connected to the shaft. As the valve rotates, the output voltage of the pot will change. This signal is the processed by the 5773D module which will output the relevant 4-20mA signal.

At the same time, the K-Series can also be fitted with G-Switches as logic outputs to provide open and close diagnostics.

3.2.2 Self-Diagnosed Fault Conditions

The K-Series can claim a form of diagnostics. If a failure occurs that results in the two outputs (mechanical beacon and electrical switch signal) begin different, the operator can identify that a fault has occurred. This claim has allowed for some dangerous undetectable failures to become detectable and this is considered as such in the FMEA.

Some models of the K-series include both the 4-20mA output and the GO switch configuration. Improved diagnostics can be achieved if both of these redundant signals are monitored. The integrity of the 4-20mA output can be verified by the pre-certified GO switches. In the event that there is discrepancy between the 4-20mA signal and the GO switches, the external controller shall ensure that an operator is made aware that there is a failure.

3.2.3 Alarm Conditions (clause 7.4.2.2-d)

Due to the type of product, the K-Series Valvetop has no formal alarm system in place.

4 Existing Certification Relevant to This Assessment

The manufacturer has the other certificates which may be relevant to this assessment detailed in Table 3 below.

Table 3: Existing Certifications

Certificate Number	Document Description	Date
10108795	ISO 9001:2015 Certificate Cert. Body: Lloyd's Register Scope: Design and Manufacture of Valve Controllers and Position Sensors Issued: 23 July 2018 Expiry: 28 February 2021	23 July 2018

5 Assessment Route

Based on the above hardware description the K-Series Valvetop Indicators will be assessed as per the following:

a) The requirements for hardware safety integrity which consists of architecture constrains (clause 7.4.4) and quantifying the effect of random failures (clause 7.4.5).

~~b) Architecture requirements for ICs with on chip redundancy.~~

c) Requirements for systematic safety integrity (systematic capability). Identify which software route is selected from the list (1_S, 2_S or 3_S). See (7.4.6 or 7.4.7, 7.4.20 or 7.4.2.12)

d) Identify the system behavior on detection of a fault (7.4.8).

~~e) Requirements for data communication process (7.4.11).~~

The assessment has used the CASS (Conformity Assessment of Safety-related Systems, www.61508.org) methodology as a framework. See Appendix 1 for more details of the CASS methodology. For product assessments, the methodology uses the following 'Targets of Evaluation' (TOEs):

TOEs 1-16 are common targets that apply to all products / sub-system assessments

~~*TOEs 17-20 apply to proven in use assessments*~~

TOEs 21-24 apply to proven by design assessments

This assessment is of the proven by design type.

IEC 61508-2 references: 2/7.4.4, and 7.4.5

5.1 Sub-System/Element Identification for Hardware and/or Software (TOE1)

IEC 61508-2 references: 2/7.4.9.3 (d)

This assessment is based on the K-Series Valvetop Indicators. The following documents define the equipment that is assessed and should be stated in any future certificate that is supported by this assessment. Any changes to these documents will require a re-assessment.

Table 4: Equipment Documents

Document no.	Rev	Date	Document description
K1P-0HCGNPS-180912123246	-	12/09/2018	Schematic for the K1P-0HCGNPS
K1P-0XCGNPS-180912123402	-	12/09/2018	Schematic for the K1P-0XCGNPS
K2P-LHCGNPS-180912123503	-	12/09/2018	Schematic for the K2P-LHCGNPS
K2P-LXCGNPS-180912123550	-	12/09/2018	Schematic for the K2P-LXCGNPS
K1P-0X0FBMS	-	-	Bill of Materials for K1
K2P-LHCBNMS	-	-	Bill of Materials for K2

5.2 Functional Specification (TOE2)

IEC 61508-2 references: 2/7.4.9.3 (a)
2/7.4.9.5
2/7.4.10.5

Table 5: Functional Specification Documents

Document no.	Rev	Date	Document description
ES-06033-1	-	11.01.2018	IOM for the K-Series 4-20 HART IOM
ES-06079-1	-	-	K-Series K2P/K2S IOM
ES-06080-1	-	-	K-Series K1P/K1S IOM

The above documents have been reviewed along with the datasheets and product specifications. Methods of use, installations, maintenance, proof test intervals, safety functions and diagnostics are described in the safety manual with a failure log.

5.3 The Estimated Rates of Failure (due to random hardware failures) in Any Modes (TOE3)

IEC 61508-2 references:
2/7.4.9.4 (c)
2/7.4.9.4 (l)
2/7.4.9.4 (j) (failure rates of the diagnostics should be included in the FMEDA)
2/7.4.9.5
2/7.4.5 for PFD context
2/Annex A
2/Annex C
7/B.6.6.1

Refer to Table 6 below for further illustration.

The failure rate of any diagnostics functions has been included in the FMEDA.

The failure modes applied during the FMEDA analysis for the K-Series Valvetop Indicators can be defined as follows:

Failure	Termination of the ability of the equipment to provide a required function or operation of the equipment in any way other than as required. This failure could be either random hardware failure or systematic failure – refer to IEC 61508-4:2010 for further definition. Sub-divisions of random hardware failure used in the FMEDA section of this report follow below.
Dangerous Failure, λ_D	Failure of an equipment that plays a part in implementing the safety function that: a) Prevents a safety function from operating when required, OR causes a safety function to fail, such that the EUC is put into a hazardous or potential hazardous state. Or, b) Decreases the probability that the safety function operates correctly when required. If the equipment has self-diagnostics, dangerous failures can be further sub-divided into: • Dangerous Detected Failures, (λ_{DD}); Dangerous Undetected Failures, (λ_{DU})
Safe Failure, λ_S	A failure in the equipment that: a) Results in the spurious operation of the safety function to put the EUC into a safe state or *maintain safe state*. Or, b) Increases the probability of the spurious operation of the safety function to put the EUC into a safe state, or *maintain a safe state.* If the equipment has self-diagnostics, safe failures can be further sub-divided into: • Safe Detected Failures, (λ_{SD}); Safe Undetected Failures, (λ_{SU})
'No Effect' Failure or 'No Part' Failure	A failure in the equipment that plays not part in implementing the safety function, or has no direct effect on the safety function. These failures do not contribute to the SFF calculation.

Note 1: there are important differences in the definitions between edition 1 and 2 of IEC 61508 for safe and dangerous failures. Refer to the two editions of Part 4 of the Standard for details.

Note 2: IEC 61508-2 is primarily addressing the overall safety function. Typically, the Sira FMEDA is only concerned with an instrument or sub-system intended for use (with other such devices) by one or more engineered safety functions. Sira's FMEDA can only evaluate each failure mode against the resultant effects on the equipment's stated functionality (as the overall safety function is not known at this stage).

The requirements for target failure measures for the safety integrity levels with respect to the probability of failure on demand for a low demand or high demand safety function, where dormant failures can be revealed by proof testing, are given in IEC 61508-1 Table 2 and 3. Calculating the proof test interval (T) will be aiming to achieve the target PFD for an overall safety-related system working in the low demand mode.

Summary of Table 2 and 3 of IEC 61508-1

Safety Integrity Level (SIL)	LOW DEMAND	HIGH DEMAND

	Average probability of failure on demand (PFD_{AVG})	**Failure Rate, hr^{-1}**
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 $< 10^{-5}$

5.4 Diagnosed (dangerous) Failure Rates (TOE4)

IEC 61508-2 references:	2/7.4.9.4 (c) 2/7.4.9.5 2/7.4.9.4 (l) 2/Annex A

The calculated failure rates of the K-Series Valvetop Indicators were based on the worst-case configuration of the highest maximum possible option which counts for the maximum number of components. The failure rate figures shown in the FMEDA were extracted from or calculated using Quanterion Automated Databook, Item Toolkit, and Faradip 3.0.

The calculated failure rates of the K-Series Valvetop Indicators for a single product (1oo1) are summarised as shown in Table 6. Note that in the table below, the hardware safety integrity is limited by the architectural constraints (SFF, HFT and Type B) rather than the failure data.

Table 6: FMEDA Analysis Results of the K-Series Valvetop Indicators with GO Switch (1oo2)

1oo2 EQUATIONS

Parameter name	Symbol	Equation / source	Value/Result
Proof Test Interval	T1	IEC 61508-4 clause 3.8.5	8760
Common cause factor	β	IEC 61508-6 Annex D Table D.1	0.2
Common Cause Factor (Detected)	β_D	IEC 61508-6 Annex D Table D.1	0.1
Mean Time To Restoration	MTTR	IEC 61508-4 clause 3.6.21	8
Hardware Fault Tolerance	HFT	IEC 61508-4 clause 3.6.3	1
Type A/B	Type	IEC 61508-2 clause 7.4.4.1.2 & 7.4.4.1.3	Type A
Total failures:	λ	IEC 61508-4 clause 3.6.4	4.08E-08
Safe diagnosed failures:	λ_{SD}	IEC 61508-4 clause 3.6.8	0.00E+00
Safe undiagnosed failures:	λ_{SU}		8.06E-09
Dangerous diagnosed failures:	λ_{DD}	IEC 61508-4 clause 3.6.7	0.00E+00
Dangerous undiagnosed failures:	λ_{DU}		3.27E-08
Diagnostic coverage:	DC	$\lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$	0%
Safe Failure Fraction:	SFF	$(\lambda_{SD} + \lambda_{SU} + \lambda_{DD}) / \lambda$	**20%**
System equivalent down time	t_{GE}	$(\lambda_{DU} / \lambda_D)(T/3 + MRT) + \lambda_{DD} / \lambda_D\, MTTR$	2.92E+03
PFDAVG (using 61508-6 equation)	$PFD_{AVG\ 1oo2}$	$2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2\, t_{CE}\, t_{GE} + \beta_D\lambda_{DD}\, MTTR + \beta\lambda_{DU}\, ((T/2)+MRT)$	**2.87E-05**
PFH (using 61508-6 equation)	PFH 1oo2	$2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}](1-b)\lambda_{DU}t_{CE} + \beta\lambda_{DU}$	**6.5496E-09**
SIL capability (Low demand mode)	**SIL**	□	**SIL 2**

Table 7: FMEDA Final Analysis Results of the K-Series Valvetop Indicators with GO Switch

Product Name	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Main parts of K, D-T series	0.00E+00	1.23E-08	0.00E+00	4.50E-09
Manet+SW1&SW2	0.00E+00	8.06E-09	0.00E+00	3.27E-08
1oo2 SW//SW2	0.00E+00	8.06E-09	0.00E+00	3.27E-08
4-20 mA module 5337D	0.00E+00	3.23E-07	0.00E+00	1.04E-07
Overall failure rates.	0.00E+00	3.51E-07	0.00E+00	1.74E-07

PFDavg : 1.75E-07 * 8760 /2 7.62E-04

5.5 Un-Diagnosed Dangerous Failure Rates (TOE5)

IEC 61508-2 references:	2/7.4.9.4 (a) 2/7.4.7.5 2/7.4.9.4 (l)

Refer to information in previous TOEs above, section 5.4.

5.6 Environmental Limits (TOE6)

IEC 61508-2 references:	2/7.4.9.4 (e)

According to the gathered information about the product, the failure rates were taken from Quanterion Automated Databook and Item Software reliability package using Bellcore and RDF 2000K. Components failure rates were selected for a 70°C operating temperature. It is reported that the product is designed for a temperature range of -20°C to +60°C. Therefore, these failures rates can be considered to exceed the required limit specified by the product data sheet.

5.7 Lifetime Limits (TOE7)

IEC 61508-2 references:	2/7.4.9.4 (f)

With regular maintenance and inspections as recommended in the manufacturer's installation instructions, a realistic lifetime limit of approximately 20 years can be achieved.

5.8 Proof Test Requirements (TOE8)

IEC 61508-2 references:	2/7.4.9.4 (g) Annex D

The assessment of the K-Series Valvetop Indicators was completed using an example proof test interval (PTI) of 1 year (8760 hours). See Table 6 and Table 7 in section 5.4 of this report. For changes regarding the proof test interval, the end user mist ensure that the PFD is recalculated to reflect this.

5.9 Maintenance Requirements (TOE9)

IEC 61508-2 references:	2/7.4.9.4 (g) Annex D

Please refer to the IOM/Safety Manual detailed in Table 5

5.10 Diagnostic Coverage (TOE10)

IEC 61508-2 references:	2/7.4.9.4 (h) 2/Annex C 2/7.4.5.2 2/Annex A and all sub-sections

See the diagnostic method is as described in 3.2.2 and 3.2.3. In the FMEA, the random hardware failure rates of the diagnostic circuit which is used by the microcontroller as recommended by IEC 61508-2 are included in the hardware failure assessment.

Tables of techniques and measures from IEC 61508-2 Annex A, Tables A1 to A 14 are shown in 0.

5.11 Diagnostic Test Interval (TOE11)

IEC 61508-2 references:	2/7.4.9.4 (i) 2/Annex C

This product does not include any internal diagnostics. Diagnostic coverage can be claimed in the FMEA, see section 3.2.2 for details.

5.12 Other Repair Constraints (TOE12)

IEC 61508-2 references:	2/7.4.9.4 (k)

The product needs to be repaired within the MRT for the PFD value shown in Table 6 and Table 7 of this report to be deemed correct.

5.13 Safe Failure Fraction (TOE13)

IEC 61508-2 references:	2/7.4.9.4 (l) 2/Annex C

As the application context of these elements is defined it is possible to define what is 'safe' and 'dangerous' in terms of the element's hardware failure modes. The safe and dangerous failures constituent of the failure rate can therefore be used to calculate the safe failure fraction (SFF), as shown below.

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

The calculated safe failure fraction of the K-Series Valvetop Indicators is summarised in Section 1.3 and 5.4 of this report.

5.14 Hardware Fault Tolerance (TOE14)

IEC 61508-2 references:	2/7.4.9.4 (m)

This product has been analysed for single mode (1oo1) i.e. for HFT = 0. See Table 6 and Table 7 of this report.

Note: If HFT is > 0, then 5.16 (highest SIL claimed) shall be answered.

5.15 Achieved SIL (architecture) (TOE15)

IEC 61508-2 references:	2/7.4.9.4 (j) 2/7.4.9.4 (k) for Type A/B 2/7.4.4.1.2 2/7.4.4.1.3 2/7.4.4.2 (route 1_H) 2/7.4.4.3 (route 2_H)

For 'Type A' and 'Type B' sub-systems used by safety functions, the following architectural constraints apply according to IEC 61508-2, Tables 2 and 3.

Summary of Table 2 and Table 3 from IEC 61508-2

Safe Failure Fraction (SFF)	Type A Subsystem			Type B Subsystem		
	Hardware Fault Tolerance			Hardware Fault Tolerance		
	0	1	2	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3	NO SIL	SIL 1	SIL 2
60 % - < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 3	SIL 4	SIL 4	**SIL 2**	SIL 3	SIL 4
≤ 99 %	SIL 3	SIL 4	SIL 4	**SIL 3**	SIL 4	SIL 4

The K-Series Valvetop Indicators which is of Type B is targeting SIL 2 suitability. Therefore, in accordance with the above table, where HFT = 0 and as defined in IEC 61508-2 clause 7.4.4.1.2 or 7.4.4.1.3, the product was found to meet the requirements of SIL 2.

5.16 Systematic Capability Assessment to SC (N+1) (TOE16)

IEC 61508-2 references:	2/7.4.9.3 (b)

The requirements of this clause are contained in the relevant Installation, Operation and Maintenance sheet and safety manual.

5.17 Determining Maximum HW Safety Integrity Level Using (Route 1_H or 2_H) (TOE17)

IEC 61508-2	2/7.4.4.2
references:	2/7.4.4.3

The maximum hardware safety integrity level was assessed using Route 1_H (FMEA). Details of the FMEA document are provided in 5.26.

5.18 Systematic Failure Constraints (TOE18)

IEC 61508-2 references:	2/7.4.9.3 (b)

See APPENDIX 3 for systematic assessment.

5.19 Evidence of Similar Conditions in Previous Use (TOE19)

IEC 61508-2	2/7.4.10.2
references:	2/7.4.10.1
	2/7.4.10.4
	2/7.4.10.5

Proven in use is not applicable to this assessment.

5.20 Evidence Supporting the Application Under Different Conditions of Use (TOE20)

IEC 61508-2	2/7.4.10.3
references:	2/7.4.10.4
	2/7.4.10.5

Proven in use is not applicable to this assessment

5.21 Evidence of Period of Operational Use (TOE21)

IEC 61508-2	2/7.4.9.5, note (1), (2), table B.6
references:	2/7.4.7.10
	2/7.4.10.4
	2/7.4.10.5
	1/4.1

Proven in use is not applicable to this assessment

5.22 Statement of Restrictions on Functionality (TOE22)

IEC 61508-2	2/7.4.10.6
references:	2/7.4.10 to 2/7.4.10.4
	3/7.4.2.13

Proven in use is not applicable to this assessment

5.23 Highest SIL - Systematic (TOE23)

IEC 61508-2 references:	2/7.4.2.2 (c) 2/7.4.6 2/7.4.7

Topworx has achieved systematic capability of SC3.

5.24 Systematic Fault Avoidance Measures (TOE 24)

IEC 61508-2 references:	2/7.4.9.4 (l) 2/7.4.6.1 3/7.4 2/Annex B, Tables B1 to B5

Annex B tables have been completed previously, see report R70005301B.

Note: The systematic fault avoidance measures comply with the requirements of 2/7.4.9.3. In addition, the realisation lifecycle, functional safety management and techniques and measures from Part 2 Annex B.

5.25 Systematic Fault Tolerance Measures (TOE 25)

IEC 61508-2 references:	2/7.4.9.4 (m) 2/7.4.7.1 2/7.4.11 2/Annex A3 2/Tables A15, A16, A17 and A18 3/7.4.3 (no change)

The techniques and measures to avoid systematic faults have been assessed previously. See

5.26 Validation Records (TOE26)

IEC 61508-2 references:	2/ 7.4.9.3 (e); proof of document. 2/7.7 (not applicable to element). 3/7.7 (not applicable to element)

This assessment provides verification of the FMEDA. The documentation verified is stated in Table 8.

Table 8: Verified Documents

Document number	Rev	Date	Document description
Topworx – 70198140 – K Series Indicators – 4-20mA	1.0	Sept. 2018	FMEA for K-Series Valvetop

5.27 Requirements for System Behavior on Detection of a Fault (TOE27)

IEC 61508-2 references:	2/7.4.8

The system behaviour on detection of dangerous faults, abnormalities etc. are listed in 3.2.2 and 3.2.3 of this report.

5.28 Additional Requirements for Data Communications (TOE28)

IEC 61508-2 references:	2/7.4.11

There are no additional requirements for data communications, hence this clause is not applicable to this assessment.

6 Information Concerning the FMEDA

6.1 Assumptions Used in the FMEDA

1) Numerical failure data in this report based on the FMEDA assume that failure rates are constant. Infant mortalities and wear-out mechanisms are not included.

2) Figures derived from FMEDA are random hardware failures. Systematic hardware failures (such as installation or maintenance errors) are not accounted for in the FMEDA but are assessed qualitatively in this report.

3) All modules that are not part of the safety function are excluded from the FMEDA; components that play no part in the safety function and therefore whose failure does not affect the safety function (either dangerous failure or spurious trip) are classified as "no part" failures and do not therefore contribute to the SFF.

7 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 where this applies to a system and can be considered to perform safety-instrumented functions up to and including SIL 2 capability.

It is therefore recommended that the K-Series Valvetop Indicators is suitable to be certified in future to IEC 61508-2:2010 up to and including SIL 2 capability for K-series with the pre-certified GO Switches or alternative switches.

Aspect	**Procedures used**	**Tools / techniques used**
Product assessment	• Reference was made to the relevant schedule of TOEs in The CASS Templates for Sub-Systems, rev 0, and the CASS Scheme Common Schedules in The CASS Guide. • The ST&C procedures manual for functional safety assessment.	• Document inspection • Physical inspection of equipment (at client site) • Item software, and RIAC Automated Databook.
Lifecycle assessment	• Not applicable at this stage	• Not assessed at this stage.
Management of functional safety	• Not applicable at this stage.	• Not assessed at this stage.

APPENDIX 1 - Assessment Methodology

Sira Test & Certification has been actively involved in applying the international functional safety standard IEC 61508 since it was first published in 2010. Soon after the publication of the Standard there was a UK government funded initiative that introduced the CASS (*Conformity Assessment of Safety-related Systems*, www.cass.uk.net) scheme which was intended to provide an industry-wide approach and interpretation to IEC 61508 assessment and certification. A key aspect of the CASS methodology is the use of assessment templates (tables) to cover different aspects of conformity, for example, the safety management system, the 'lifecycle' activities and processes, the sub-system failure data, the software, etc. Each template:

- Lists a number of target subject areas that require evaluation by the assessor (each subject area is cross referred to one or more clauses from the Standard to show coverage). In the CASS terminology, these target subject areas are called 'Targets of Evaluation' (TOEs)

- enables the client's documentation to be cross referred to each TOE and hence to the clauses in the Standard

- is a procedure, prompting the assessor with guidance (criteria, comments, etc.) during the evaluation of each TOE

- provides a means for the assessor to record evidence of conformity against each TOE

The scheme also provides competence criteria to ensure that the assessors are technically competent in the areas covered by the templates they are using. One of the benefits of this methodology is that the assessment criteria, scope, guidance and approach are all open to the client as the scheme documents are all freely available in the public domain.

Sira is accredited by UKAS to carry out assessments and issue certification using this industry-recognised process.

In addition, the assessment was carried out using the procedures, tools and techniques show in Table 9 below.

Table 9: Additional Procedures, Tools and Techniques

Aspect	Procedures used	Tools / techniques used
Product assessment	• Reference was made to the relevant schedule of TOEs in The CASS Templates for Sub-Systems, rev 0, and the CASS Scheme Common Schedules in The CASS Guide. • The ST&C procedures manual for functional safety assessment.	• Document inspection • Physical inspection of equipment (at client site) • Item software, and RIAC Automated Databook.
Lifecycle assessment	• See APPENDIX 3	• See APPENDIX 3
Management of functional safety	• See topworx_FSM_70005301	• See topworx_FSM_70005301

APPENDIX 2: Assessment of the Safety Manual – IEC 61508-2 Annex D

The manufacturer’s safety manual has been verified as shown in Table 10.

Table 10: Safety Manual Verification

Client safety manual reference: ES-06033-1 HART IOM		
Revision:		**Date: 30 Oct 18**
IEC 61508-2 Annex D clause.	**Target**	**Evidence**
D.2.1		
(A.1)	Are the safety function(s) defined?	Yes, see page 22.
(A.2)	Are the normal operating conditions of the compliant item defined?	Normal operating conditions are defined in the entire IOM.
B	Is there a configuration diagram to identify the proposed interfacing of the compliant item to other safety related elements? For SW, see Annex D of part 3.	Yes, see page 4, 5 and 6.
C	Are there any operating constraints?	Yes, see operating constraints on page 4.
D.2.2		
A	Are the dangerous undetected failure modes, per safety function, of the output of the compliant item defined?	Yes, see FMEA summary on page 22.
B	For all failure modes in (a), are failure rates available?	Yes, see FMEA summary on page 22.
C	Are the failure modes of the output of the compliant item for safe detected and dangerous detected defined?	Yes, see FMEA summary on page 22.
D	On failure of the internal diagnostic, what will the outputs of the compliant item do?	Yes, see FMEA summary on page 22.
E	For all failure modes in (c) and (d), are failure rates available?	Yes, see FMEA summary on page 22.
F	Is the diagnostic test interval timing defined (cycle)?	Not applicable.
G	Is the output of the compliant item defined upon detection of a failure detected by the internal diagnostics?	Not applicable.
H	Is the proof test stated for the compliant item? Is it full or partial? Is there any procedure provided for maintenance?	Yes, see FMEA summary on page 22.
I	If the product is supported with external diagnostics such as (PST), then failure modes and failures rates shall be detailed.	Not applicable.

J	Is the hardware fault tolerance stated? If HFT>0, then D.2.3 (B) is applicable.	Yes, see FMEA summary on page 22.
K	Is the product type (A/B) defined?	Yes, see FMEA summary on page 22.
D.2.3		
A	Is the systematic capability (SC) defined?	Yes, see FMEA summary on page 22.
B	Are there any known systematic constraints (such as diversity and / or independency – as stated in clause 7.4.3)? If HFT> 0, CCF shall be conducted on the final assembly.	Not applicable.
D.2.4		
A	Is software used? If so, see 7.4.2.12 and IEC61508-3 annex D.	Not applicable.