FUNCTIONAL SAFETY CERTIFICATE

This is to certify that the

SI3 & SI4,
Skilmatic Range of Electro-Hydraulic Actuators

manufactured by

Rotork (UK) Ltd.
9 Brown Lane West
Leeds
LS12 6BH

has been assessed by Sira Certification Service with reference to the CASS methodologies and found to meet the requirements of

IEC 61508-2:2010
Routes 1_H & 1_S
Systematic Capability (SC3)

as an element/subsystem suitable for use in safety related systems performing safety functions up to and including

SIL 2 capable without diagnostics
SIL 3 capable with diagnostics

when used in accordance with the scope and conditions of this certificate.

* This certificate does not waive the need for further functional safety verification to establish the achieved Safety Integrity Level (SIL) of the safety related system

Certification Decision:

James Lynskey

Initial Certification : 26/07/2019
This certificate re-issued : 09/02/2021
Renewal date : 25/07/2024

Certificate No.: Sira FSP 19008/02
Form 7016 issue 4

0011

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

Product description and scope of certification

The SI3 and SI4 are self-contained, electro-hydraulic, fail-safe actuators. The actuators operate on a pump and bleed principle with two basic configurations as described below:

Configuration 1
Closing the bleed solenoid valve(s) and pumping hydraulic fluid under pressure will drive the spring opposed piston within the hydraulic actuator, causing it to move away from its fail-safe position.

Configuration 2
Hydraulic fluid is first pumped into an accumulator under pressure thus charging the accumulator. Closing the bleed solenoid valve(s) and opening the accumulator solenoid valve will drive the spring opposed piston within the hydraulic actuator, causing it to move away from its fail-safe position.

When the bleed solenoid valve(s) are opened the pressure will be released and the spring will drive the piston/actuator back to the fail-safe position. In a fail-safe actuator the bleed solenoid valve(s) will be normally open (de-energised) and the accumulator solenoid valve, where applicable, will be normally closed (de-energised).

There is also a by-pass solenoid valve fitted which allows the motor to start under no load by remaining open and allowing the oil to circulate around the tank before being closed and diverting the flow to the actuator or accumulator.

When the actuator is stopped in position away from the fail-safe limit then the hydraulic pressure is maintained by the bleed solenoid valves, check valve and pressure relief valve. If an accumulator is fitted and is fully charged then the hydraulic pressure in the accumulator is maintained by the accumulator solenoid valve, check valve and pressure relief valve.

Flow control valves will be used to adjust the operating speed in both the spring direction and hydraulic direction. The control unit will also be continually monitoring the position and pressure and making adjustments to maintain the demanded position or to issue various alarms if the actuator is unable to carry out the given command. Where applicable the control unit will also be continually monitoring the pressure in the accumulator making adjustments to maintain the correct level or to issue various alarms if the
actuator is unable to carry out the given command.

Both the SI3 & SI4 can incorporate either of three actuator options. The GH or RH range of quarter turn actuators or the LH range of linear actuators.

Fail-Safe on Loss of ESD Signal or Power Supply
The actuator will accept an ESD input signal of 20-60 VDC or 60-120 VAC with the following functionality:
- Fail-safe on loss of ESD signal
- Fail-safe on loss of power supply

Fail-Safe on Loss of ESD Signal only
The actuator will accept an ESD input signal of 24 VDC as standard with the option of 20-60 VDC through
the Wide Input ESD Board with the following functionality:
- Fail-safe on loss of ESD signal
- Stayput on loss of power supply

Fail-Safe on Loss of Power Supply only
The actuator will not require an ESD input signal and will only have the following functionality:
- Fail-safe on loss of power supply

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

Additional ESD Input

The standard fail-safe configuration of the SI Actuator Range will accept a single ESD input. The SI offers the option of a second ESD input by using an additional ESD option card with the following functionality:

- Two ESD signals operate common solenoid valve(s). If either ESD signal is removed the actuator will perform the safety function by operating the same solenoid valve(s).
- Two ESD signals operating independent solenoid valve(s). If either ESD signal is removed then the actuator will perform the safety function by operating the associated solenoid valve. This is available for configuration 1 only.

Figure 1: Typical Assembly of the SI Actuator Range

Element Safety Function

The element safety functions of the SI range of Actuators are defined as follows:

Fail-Safe on Loss of ESD Signal or Power Supply (Standard ESD)

- *The safety function shall operate on the removal of the Emergency Shut Down signal or Mains Power Supply to the actuator and shall cause the actuator to move to the end position* by means of a spring.*

Fail-Safe on Loss of ESD Signal only (Hardwired ESD)

- *The safety function shall operate on the removal of the Emergency Shut Down signal to the actuator and shall cause the actuator to move to the end position* by means of a spring.*

Fail-Safe on Loss of Power Supply only

- *The safety function shall operate on the removal of the Mains Power Supply to the actuator and shall cause the actuator to move to the end position* by Means of a spring.*

*The end position depends on the fail-safe requirement (closed or open).

Certified Data in support of use in safety functions

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, Rotork (UK) Ltd have submitted the SI Actuator range for FMEA assessment to attain SIL capability. The component failure rates and modes for the SI Actuator Range have been extracted from or calculated using Quanterion Automated Databook, Item Toolkit and Faradip 3.0. Tables 1.1 and 1.2 summarise the FMEA assessment for the SI actuator range.

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

Table 1.1: FMEA Summary for the SI3 & SI4 Actuators

Safety Function:
The safety function used in the SI actuator range is defined as follows:
Fail-Safe on Loss of ESD Signal or Power Supply (Standard ESD)
• The safety function shall operate on the removal of the Emergency Shut Down signal or Mains Power Supply to the actuator and shall cause the actuator to move to the end position by means of a spring.*
Fail-Safe on Loss of ESD Signal only (Hardwired ESD)
• The safety function shall operate on the removal of the Emergency Shut Down signal to the actuator and shall cause the actuator to move to the end position by means of a spring.*
Fail-Safe on Loss of Power Supply only
• The safety function shall operate on the removal of the Mains Power Supply to the actuator and shall cause the actuator to move to the end position by means of a spring.*
**The end position depends on the Fail-Safe requirement (closed or open).*

Summary of IEC 61508-2 Clauses 7.4.2 and 7.4.4		**Manifold Configuration 1**			
Architectural constraints & Type of product A/B		**Overall HFT = 0 (1oo1) Type A**			
Solenoid Valve Option		**Single mode (1oo1)**		**Dual mode (1oo2)**	
Diagnostic Capability (Partial stroke)		**No**	**Yes**	**No**	**Yes**
Safe Failure Fraction (SFF)		**63%**	**92%**	**62%**	**91%**
Random hardware failures: [h^{-1}]	λ_{DD} λ_{DU}	0.00E+00 4.82E-07	3.75E-07 1.07E-07	0.00E+00 4.07E-07	3.08E-07 9.99E-08
Random hardware failures: [h^{-1}]	λ_{SD} λ_{SU}	0.00E+00 8.08E-07	2.81E-07 5.27E-07	0.00E+00 6.57E-07	1.35E-07 5.24E-07
PFD @ PTI = 8760 Hrs. MTTR = 8 Hrs.		2.11E-03	4.72E-04	1.79E-03	4.41E-04
Probability of Dangerous failure (High Demand - PFH) [h^{-1}]		4.82E-07	4.82E-07	4.07E-07	4.08E-07
Hardware safety integrity compliance		Route 1_H		Route 1_H	
Systematic safety integrity compliance		Route 1_S **R70214587B**		Route 1_S **R70214587B**	
Systematic Capability (SC1, SC2, SC3, SC4)		**SC 3**			
Hardware safety integrity achieved		**SIL 2**	**SIL 3**	**SIL 2**	**SIL 3**

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

Table 1.2: FMEA Summary for the SI3 & SI4 Actuators

Safety Function:
The safety function used in the SI actuator range is defined as follows:
Fail-Safe on Loss of ESD Signal or Power Supply (Standard ESD)
• The safety function shall operate on the removal of the Emergency Shut Down signal or Mains Power Supply to the actuator and shall cause the actuator to move to the end position by means of a spring.*
Fail-Safe on Loss of ESD Signal only (Hardwired ESD)
• The safety function shall operate on the removal of the Emergency Shut Down signal to the actuator and shall cause the actuator to move to the end position by means of a spring.*
Fail-Safe on Loss of Power Supply only
• The safety function shall operate on the removal of the Mains Power Supply to the actuator and shall cause the actuator to move to the end position by means of a spring.*
**The end position depends on the Fail-Safe requirement (closed or open).*

Summary of IEC 61508-2 Clauses 7.4.2 and 7.4.4		**Manifold Configuration 2**			
Architectural constraints & Type of product A/B		**Overall HFT = 0 (1oo1) Type A**			
Solenoid Valve Option		**Single mode (1oo1)**		**Dual mode (1oo2)**	
Diagnostic Capability (Partial stroke)		**No**	**Yes**	**No**	**Yes**
Safe Failure Fraction (SFF)		**72%**	**95%**	**73%**	**96%**
Random hardware failures: [h^{-1}]	λ_{DD} λ_{DU}	0.00E+00 5.39E-07	4.19E-07 6.96E-08	0.00E+00 4.64E-07	3.52E-07 6.21E-08
Random hardware failures: [h^{-1}]	λ_{SD} λ_{SU}	0.00E+00 1.41E-06	3.71E-07 1.04E-06	0.00E+00 1.26E-06	2.22E-07 1.04E-06
PFD @ PTI = 8760 Hrs. MTTR = 8 Hrs.		2.37E-03	3.09E-04	2.04E-03	2.75E-04
Probability of Dangerous failure (High Demand - PFH) [h^{-1}]		5.39E-07	4.89E-07	4.64E-07	4.14E-07
Hardware safety integrity compliance		Route 1_H		Route 1_H	
Systematic safety integrity compliance		Route 1_S **R70214587B**		Route 1_S **R70214587B**	
Systematic Capability (SC1, SC2, SC3, SC4)		**SC 3**			
Hardware safety integrity achieved		**SIL 2**	**SIL 3**	**SIL 2**	**SIL 3**

Notes:

- The results in Tables 1.1 and 1.2 are the worst-case for the different configurations. For specific failure rate results, refer to CSA-Sira report R70214587A.
- The results with diagnostic capability in Table 1 are only valid if a PST (Partial Stroke Test) is carried out with a frequency of at least 10 times the full proof test interval. For example, if the proof test interval = 8760 hours, PST must interval must be 876 hours or less.

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

Table 2: Base information for the SI Actuator Range

1	Product identification:	SI Actuator Range
2	Functional specification:	See safety function definitions above.
3-5	Random hardware failure rates:	Refer to tables 1.1 & 1.2 of this certificate.
6	Environment limits:	Operating temperature: -50°C to +70 ºC.
7	Lifetime/replacement limits:	20 years
8	Proof Test requirements:	Refer to safety manual - STR-318
9	Maintenance requirements:	Refer to safety manual - STR-318
10	Diagnostic coverage:	Refer to tables 1.1 & 1.2 of this certificate.
11	Diagnostic test interval:	Refer to safety manual - STR-318
12	Repair constraints:	Refer to safety manual - STR-318
13	Safe Failure Fraction:	Refer to tables 1.1 & 1.2 of this certificate.
14	Hardware fault tolerance (HFT):	Refer to tables 1.1 & 1.2 of this certificate.
15	Highest SIL (architecture/type A/B):	Type A, SIL 3
16	Systematic failure constraints:	The hardware safety integrity assessment was based on a proof test interval of 1 year. For further information refer to safety manual - STR-318
17	Evidence of similar conditions in previous use:	Not applicable.
18	Evidence supporting the application under different conditions of use:	Not applicable.
19	Evidence of period of operational use:	Not applicable.
20	Statement of restrictions on functionality:	See systematic report R70214587B.
21	Systematic capability (SC1, SC2, SC3)	SC3 - See systematic report R70214587B.
22	Systematic fault avoidance measures:	Compliance with techniques and measures from IEC 61508-2 Annex B to SC3 - See systematic report R70214587B.
23	Systematic fault tolerance measures:	Compliance with techniques and measures from IEC 61508-2 Annex A to support the SFF achieved – see hardware safety integrity report R70214587A.
24	Validation records:	All documents that have been used in support of the hardware have been documented in section 5.24 of report R70214587A; this includes the FMEA document and insertion tests.

Management of functional safety

The assessment has demonstrated that the product is supported by an appropriate functional safety management system that meets the relevant requirements of IEC 61508-1:2010 clause 6, see report R70214587B.

Identification of certified equipment

The certified equipment and it's safe use is defined in the manufacturer's documentation listed in Table 3 below.

Table 3: Certified documents

Document no.	Pages	Rev	Date	Document description
MSG7003	1 of 1	00	26 Oct 12	Single acting Hydraulic Actuator "Fail to close" GH/S Series
MSG7004	1 of 1	00	26 Oct 12	Single acting Hydraulic Actuator "Fail to Open" GH/S Series
DSGA006	1 of 1	00	14 Feb 00	Centre Body (Welded Body) Assembly Drawing
DSGA001	1 of 1	00	04 Apr 05	Centre Body (Cast Body) Assembly Drawing
DSGC022	1 of 1	00	12 Jun 00	Spring Cartridge Assembly Drawing
DSGE118	1 of 1	00	08 Jan 12	Hydraulic Cylinder Assembly Drawing

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

DSGE122	1 of 1	01	20 Sep 11	Hydraulic Cylinder Assembly Drawing
DSGM001	1 of 1	01	14 Feb 00	Spring cartridge adapter
ED08990	1 to 2	01	-	SI3 ESD & Solenoid
ED09535	1 to 7	02	20 Mar 19	SI3 LP AC Power Board Mk2
ED09716-2	1 of 1	02	13 Feb 19	SI3 WI ESD Adapter Board
2050773	1 of 1	01	13 Nov 20	Hydraulic schematic for SI3 & SI4 config 1
2050938	1 of 2	01	13 Nov 20	Internal arrangement for SI3 & SI4 config 1
2034573	1 of 1	02	13 Nov 20	Hydraulic schematic for SI3 & SI4 config 2
2034856	1 of 2	02	13 Nov 20	Internal arrangement for SI3 & SI4 config 2
ED08954	1 of 6	01	-	SI3 DC power board Mk1
DSL2088	1 of 5	0	09 Sep 09	LH Act Old Spring Down
DSL2089	1 of 5	0	06 Feb 03	LH Act Old Spring Up
DSRA019	1 of 1	0	-	RH Centre
DSRC001	1 of 1	0	-	RH Spring Cartridge
DSRE004	1 of 1	0	-	RH Hydraulic Cylinder
GD02601	1 of 4	0	19 Oct 20	LH Hydraulic Cylinder Spring Down
GD02602	1 of 4	0	19 Oct 20	LH Hydraulic Cylinder Spring Up

Conditions of Certification

The validity of the certified base data is conditional on the manufacturer complying with the following conditions:

1. The manufacturer shall analyse failure data from returned products on an on-going basis. Sira Certification Service shall be informed in the event of any indication that the actual failure rates are worse than the certified failure rates. (A process to rate the validity of field data should be used. To this end, the manufacturer should co-operate with users to operate a formal field-experience feedback programme).
2. Sira shall be notified in advance (with an impact analysis report) before any modifications to the certified equipment or the functional safety information in the user documentation is carried out. Sira may need to perform a re-assessment if modifications are judged to affect the product's functional safety certified herein.
3. On-going lifecycle activities associated with this product (e.g., modifications, corrective actions, field failure analysis) shall be subject to surveillance by Sira in accordance with 'Regulations Applicable to the Holders of Sira Certificates'.

Conditions of Safe Use

The validity of the certified base data in any specific user application is conditional on the user complying with the following conditions:

1. The results with diagnostic capability in Table 1 are only valid if a PST (Partial Stroke Test) is carried out with a frequency of at least 10 times the full proof test interval. For example, if the proof test interval = 8760 hours, PST must interval must be 876 hours or less.
2. The user shall comply with the requirements given in the manufacturer's user documentation in regard to all relevant functional safety aspects such as application of use, installation, operation, maintenance, proof tests, maximum ratings, environmental conditions, and repair.
3. Selection of this product for use in safety function and the installation, configuration, overall validation, maintenance and repair shall only be carried out by competent personnel, observing all the manufacturer's conditions and recommendations in the user documentation.
4. All information associated with any field failures of this product should be collected under a dependability management process (e.g., IEC 60300-3-2) and reported to the manufacturer.

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org

5. CSA-Sira suggests that the safety device is to have an independent power supply, it must not share the same power supply as non-safety devices that may cause a fault to the safety device. This is in accordance with IEC61508-1, cl. 7.6.2.7 AND IEC61508-2, cl. 7.4.2.3.
6. A proof test interval of 1 year.

General Conditions and Notes

1. This certificate is based upon a functional safety assessment of the product described in Sira Test & Certification Assessment Report R70214587A and any further reports referenced (R70214587B).
2. If the certified product or system is found not to comply with the requirements of the standards listed in this certificate, Sira Certification Service should be notified immediately at the address shown on this certificate.
3. The use of this Certificate and the Sira Certification Mark that can be applied to the product or used in publicity material 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 issuer.
5. No part of the Functional safety related aspects stated in the instruction manual shall be changed without approval of the certification body.
6. This certificate will remain valid subject to completion of two surveillance audits within the five year certification cycle, and upon receipt of acceptable response to any findings raised during this period. This certificate can be withdrawn if the manufacturer no longer satisfies scheme requirements.

Certificate History

Issue	Date	Report no.	Comment
00	26/07/2019	R70214587A R70214587B	The release of prime certificate.
01	02/08/2019	R70214587A R70214587B	Minor modifications to certificate.
02	09/02/2021	R70214587A	Updated to include new configurations 1 & 2 options with or without an accumulator

Sira Certification Service
Part of CSA Group UK
Unit 6 Hawarden Industrial Park,
Hawarden, CH5 3US, United Kingdom
Tel: +44 (0) 1244 670900
Email: ukinfo@csagroup.org
Web: www.csagroupuk.org