



FUNCTIONAL SAFETY CERTIFICATE

This is to certify that the

Programmable Interlock Board

manufactured by

MKS CIT

*Yodfat st. 2
Lod
Israel
71291*

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

IEC 61508-2:2000

The certified failure data, which is subject to the conditions and scope herein, may be used in the design of safety functions up to and including safety integrity level 3 (SIL3)

Certification Manager:

A handwritten signature in black ink, appearing to read "D R Stubbings".

D R Stubbings

Initial Certification: 03 September 2009
This certificate issued: 03 September 2009
Renewal date: 02 September 2014

This certificate may only be reproduced in its entirety without any change.



Certificate No.: Sira FSP 08005/01
Form 7016 issue 1
Page 1 of 6



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 function of the Programmable Interlock Board (the 'certified equipment') is to provide a trip function in the event of a specific combination of input states not being met. The certified equipment is a sub-system performing a 'logic solver' function, according to IEC 61508-2.

There are 65 digital input channels operating at 24 volts which support 47 interlock functions. Any combination of input states can be configured to energize any of the 32 pairs of output relays. In addition there are 15 dummy functions available to extend the complexity of the interlock logic. The output relays are connected in series (for redundancy) such that there are up to 32 independent output channels available.

This certificate covers both the hardware and systematic safety integrity requirements from IEC 61508.

Use in safety functions

The product's functionality which has been assessed for use in safety functions is:

- For each output channel, to de-energize both relays and hence open the relay contacts unless a valid combination of input states is met.

Hardware safety integrity

Avoidance and control of equipment failures is achieved by the following measures:

- high diagnostic coverage
- fault tolerance
- fail-safe design
- diversity in FPGA device programming



Certificate No.: Sira FSP 08005/01
Form 7016 issue 1
Page 2 of 6



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 identification and configuration

The certified equipment and its 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
ES00675-01 ES00675-02	1-43	02 01	28-Aug-08 28-Aug-08	Programmable Interlock for ECM - Circuit diagram.
BOMforAS00675-01 BOMforAS00675-02	-	02 01	-	Parts List
AS00675-01 Prg_Intlk UM	1-22	1.X	09-Jul-09 (or later)	Ethernet Control Module™ Programmable Interlock User Manual

"X" = minor revision that does not affect functional safety information in the Instruction Manual

Certified Data Set in support of use in safety functions

The assessment has been carried out with reference to the *Conformity Assessment of Safety-related Systems (CASS)* methodology.

A Failure Mode and Effect Analysis (FMEA) has established the failure modes and predicted the random hardware failure rates. Summary details are shown below.

Probabilistic failure rates and their allocations to safe or dangerous have been modelled using the FARADIP.THREE failure rate database and shown on Table 2 below for the following failure mode: **Fail to open circuit an output channel (using redundant relays) in response to an invalid combination of input states**

Table 2: Failure data

Probability of failure total (λ_{TOTAL})	Probability of spurious failures ($\lambda_{SPURIOUS}$)	Probability of dangerous diagnosed failures (λ_{DD})	Probability of dangerous undiagnosed failures (λ_{DU})	Safe Failure Fraction (SFF)	Probability of Failure on Demand (PFD_{AVG})
8.20E-06	6.55E-06	1.58E-06	7.28E-08	90-<99%	3.16E-04

Notes on the failure data:

- 1) Failure rates (symbol: λ) are stated are in units of failures per hour.
- 2) Safe detected failures (λ_{SD}) and safe undetected failures (λ_{SU}) are included in $\lambda_{SPURIOUS}$
- 3) Calculation of λ_{DU} and PFD assumes a proof test interval of 8,760 hours and MTTR of 24 hours (refer to User Manual)



Certificate No.: Sira FSP 08005/01
Form 7016 issue 1
Page 3 of 6



011

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

The failure data (above) is supported by the 'Base Information' given in Table 3 below.

Table 3: Base information table

Product ID:	Programmable Interlock Board, AS00675-01/02
Functional specification:	Safety Functions Requirements for Programmable Interlock AS00675-01, rev 02, AS00675-02, rev 01 and published specification in User Manual.
Environment / stress criteria:	Failure rates modelled using normal component quality control processes and control room environments.
Environment limits:	<ul style="list-style-type: none"> • Temperature range: -20°C to +55 °C • Humidity : 0 – 95% non-condensing • Vibrations: 2.5g acceleration over 5-300Hz sine wave. • Shock: 30g, 11ms duration, half sine shock pulse. • EMC: FCC Class B requirements; 89/336/EEC Emission EN 55011 class A; 89/336/EEC Immunity EN 50082-1
Lifetime limit:	10 years
Maintenance requirements:	Refer to manufacturer's User Manual: Ethernet Control Module™ Programmable Interlock User Manual Rev. 1.0
Repair constraints:	Refer to manufacturer's User Manual (above)
Hardware fault tolerance:	1 (architecture: 1oo2)
Systematic failure constraints:	Refer to manufacturer's User Manual (above)
Highest SIL (systematic):	SIL 3
Systematic fault avoidance measures:	Conforms with IEC 61508-2, 7.4.4, including: <ul style="list-style-type: none"> • diversity in FPGA device programming
Systematic fault tolerance measures:	Conforms with IEC 61508-2, 7.4.5, including: <ul style="list-style-type: none"> • high diagnostic coverage • fault tolerance • fail-safe design
Validation records:	<ul style="list-style-type: none"> • Programmable Interlock For ECM – HW Design Verification Test AS00675-01 (DVT), rev 01. • Programmable Interlock For ECM - Hardware Fault Verification Test P/N: AS00675-01, rev 01
Type A / Type B:	Type B

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 61508-1:1998 clause 6.



Certificate No.: Sira FSP 08005/01
Form 7016 issue 1
Page 4 of 6



011

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

Conditions of Certification

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

1. The manufacturer shall analyze 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. (Where possible, a process to rate the validity of field data should be used. To this end, the manufacturer should encourage 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 are carried out. Sira may need to re-assess the product if modifications are judged to affect the certified data.
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 data is conditional on the user complying with the following conditions:

1. The user shall comply with the requirements given in the Manufacturer's user documentation (referred to in Table 1 above) in regard to all relevant functional safety aspects such as application of use, installation, operation, maintenance, proof tests, maximum ratings, environmental conditions, repair, etc;
2. Selection of this equipment for use in safety functions 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 instructions.
3. 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.
4. 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.



Certificate No.: Sira FSP 08005/01
Form 7016 issue 1
Page 5 of 6



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

General Conditions and Notes

1. This certificate is based upon a functional safety assessment of the product described in Sira Test & Certification Assessment Report R56A18067A;
2. If certified product is found not to comply, Sira Certification Service shall be notified immediately at the address shown on this certificate;
3. The use of this Certificate and the Certification Marks that can be applied to the product or used in publicity material are defined in '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.



Certificate No.: Sira FSP 08005/01
Form 7016 issue 1
Page 6 of 6



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