
Certificate of Conformity to IEC 61508 Safety Integrity Level (SIL) in terms of Random Hardware Requirements

Functional Safety of Safety-Related Programmable Electronic Systems

The **Moto Mecánica Argentina S.A., Electro-Hydraulic Assembly**, has been assessed and is considered capable for use in a low demand Safety Function up to SIL 2 (applications in non-hazardous area) and up to SIL 1 (applications in hazardous area).

The assessment was carried out to determine compliance with IEC 61508 with regards to:

- Random Hardware Failure;
- Architectural Constraint (HFT = 0).

The assessment was based on the assumptions, data provided, and recommendations given in:

- [1] **Gefran KS Series TUV Rheinland State of conformity no: 28712235, Certificate.**
- [2] **Gefran KX Series TUV Rheinland State of conformity no: 28713306, Certificate.**
- [3] **SW digiSens-F02 Technical datasheet, Page 3.**
- [4] **Danfoss DST P92S PT Safety Guide – 2017.01. IC.PS.P21.1A.02, 520B7782. Page 9.**
- [5] **Hydac Electronic Pressure Transmitter Safety Manual, Electronic Pressure Transmitter HDA 8XXN-A-XXXX-S2PD-XXX (PSI), HDA 8XX6-A-XXXX-S2PD-XXX (PSI) - Sensors for applications with increased functional safety, (SIL 2 / PL d), Part no.: 669912 / Edition: 2015/10/06 E.**
- [6] **ESC Ltd Report: L115_FM001 Rev.1.**
- [7] **ESC Ltd Report: L115_FM002 Rev.1.**
- [8] **WIKA Safety-related data, model IS-3, addition to the operating instructions, 14116671.02 02/2019 EN/DE/FR/ES**
- [9] **WIKA, Intrinsically Safe (IS) repeater power supply, data sheet AC 80.14**

The product was assessed against the following safety function:

- When the Pressure Transmitter detects the configured alarm settings the Logic Solver (PCB L03-60590-01) will cause de-energising and opening of solenoid relief valve;
- The response time of the Safety Function is of less than 1 second; this does not consider the actuation time of a well actuator/valve, as it is not part of the analysed assembly. In order to calculate the response time of a function intended to isolate a well, the response time of the well valve would have to be considered;
- The output of the Logic Solver is normally energised.

The system will also be configured to react to the following fault conditions:

- The Pressure Transmitter is to be configured in such a way that any self-detected fault or out of range (high or low) causes de-energising and opening of solenoid relief valve via Logic Solver (PCB L03-60590-01);
- Any self-detected fault in the Logic Solver will cause de-energising and opening of solenoid relief valve.

The Electro-hydraulic assembly assessed comprises the following sub-elements / functional blocks:

ENGINEERING SAFETY CONSULTANTS LTD
is ISO9001-certified by Global Group, itself a
UKAS-accredited ISO9001 certification
body

Reg: 12Q12086

ENGINEERING SAFETY CONSULTANTS LTD

2nd Floor, Exchequer Court

33 St. Mary Axe London EC3A 8AA UK

Telephone/Fax: +44 (0)20 8542 2807

E-Mail: info@esc.uk.net Web: www.esc.uk.net

Registered in England and Wales: 7006868

Registered Office: 27-37 St George's Road Wimbledon London SW19 4EU

- Acceptable Pressure Transmitters for use in the Safety Function are:

N	Brand	Model	HFT
1	Gefran [1]	KS	0
2	Gefran [2]	KX	0
3	SW [3]	DigiSens F02	0
4	Danfoss [4]	DST P92S	0
5	Hydac [5]	HDA 8700	0
6	Wika [8] [9]	IS-3	0

All these transmitters are suitable for use in the SIL 2 / SIL 1 capable Electro-Hydraulic Assembly.

- Printed Circuit Board (PCB L03-60590-01): consisting of a power supply, an analogue input, a microcontroller, an external memory and a digital output (See ESC Ltd Report: L115_FM001 Rev.1 [6]);
- Hydraulic Assembly: Assessed via FMECA technique (See ESC Ltd Report: L115_FM002 Rev.1 [7]);
- For applications in hazardous area the Wika Intrinsically Safe (IS) barrier [9] is required in conjunction with the Wika pressure transmitter [8].

The assessment results are as follows

(for applications in non-hazardous area):

System	Component	Proof Testing Period	SFF (%)	Type	HFT	Max. SIL (Arch)	Overall PFD Achieved	SIL Capability (PFD)	Achieved SIL
Electro Hydraulic Assembly	Pressure Transmitter	1 year	92	B	0	2	9.36E-04	SIL 3	SIL 2
	Power Supply / Analogue Input (PCB)		98	A	0	3			
	Microcontroller / Memory (PCB)		90	B	0	2			
	Digital Output (PCB)		83	A	0	2			
	Hydraulic Assembly		98	A	0	3			

(for applications in hazardous area):

System	Component	Proof Testing Period	SFF (%)	Type	HFT	Max. SIL (Arch)	Overall PFD Achieved	SIL Capability (PFD)	Achieved SIL
Electro Hydraulic Assembly	Pressure Transmitter	1 year	66	B	0	1	1.01E-03	SIL 2	SIL 1
	IS Barrier		90	A	0	3			
	Power Supply / Analogue Input (PCB)		98	A	0	3			

ENGINEERING SAFETY CONSULTANTS LTD
is ISO9001-certified by Global Group, itself a
UKAS-accredited ISO9001 certification
body

Reg: 12Q12086

ENGINEERING SAFETY CONSULTANTS LTD

2nd Floor, Exchequer Court

33 St. Mary Axe London EC3A 8AA UK

Telephone/Fax: +44 (0)20 8542 2807

E-Mail: info@esc.uk.net Web: www.esc.uk.net

Registered in England and Wales: 7006868

Registered Office: 27-37 St George's Road Wimbledon London SW19 4EU



ENGINEERING SAFETY CONSULTANTS

The Global Provider of Functional Safety Expertise and Technical Consultancy

System	Component	Proof Testing Period	SFF (%)	Type	HFT	Max. SIL (Arch)	Overall PFD Achieved	SIL Capability (PFD)	Achieved SIL
	Microcontroller / Memory (PCB)		90	B	0	2			
	Digital Output (PCB)		83	A	0	2			
	Hydraulic Assembly		98	A	0	3			

It must be noted that a well actuator/valve is not considered in this certificate, or in any of the calculations performed for its generation. In order to determine the achieved SIL capability of a function intended to isolate a well, the well actuator/valve would have to be considered in the calculations; the PFD of the well actuator/valve has to be added and checked that the overall SFF and PFD still meet the requirements for the SIL 2 claim (non-hazardous area) and SIL 1 claim (hazardous area).

Chairman: Kenneth G L Simpson
 Member of the IEC61508 committee
 Assessment Date: October 2021, valid to October 2023
 Certificate: L115_CT002 (Rev.1)

ENGINEERING SAFETY CONSULTANTS LTD
 is ISO9001-certified by Global Group, itself a
 UKAS-accredited ISO9001 certification
 body

Reg: 12Q12086

ENGINEERING SAFETY CONSULTANTS LTD

2nd Floor, Exchequer Court

33 St. Mary Axe London EC3A 8AA UK

Telephone/Fax: +44 (0)20 8542 2807

E-Mail: info@esc.uk.net Web: www.esc.uk.net

Registered in England and Wales: 7006868

Registered Office: 27-37 St George's Road Wimbledon London SW19 4EU