



SAFETY MANUAL

FCX-AII VG PRESSURE TRANSMITTERS

Models : FKC, FKG, FKA...G FKP, FKH...G FKD,FKM, FKB...G FKP, FKH...G

(standard process cover) (direct mounting) (with remote seal) (with remote seal)



-Fuji Electric France S.A.S. –



CERTIFICATE

Z10 16 08 96769 001 No.

Holder of Certificate:	Fuji Electric France SAS 46 rue Georges Besse - ZI du Brézet 63039 Clermont-Ferrand FRANCE
Factory(ies):	96769
Certification Mark:	



Product:

Model(s):

Sensors

FCX-All VG Series Transmitter For nomenclature see attachment

Parameters: Systematic Capability: Safety Integrity Level (SIL): Rated Input Voltage: Rated Output Current: Protection Degree:

Tested according to: IEC 61508-1(ed.2) IEC 61508-2(ed.2) IEC 61508-3(ed.2) IEC 61508-4(ed.2) IEC 61511(ed.1) IEC 61010-1(ed.3) IEC 61326-3-2(ed.1) SC3 SIL2 (HFT=0), SIL3 (HFT=1) 10.5 ... 45VDC 4 ... 20mA IP66 / IP67

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.:

FC89017T

Valid until:

2021-08-30

Date, 2016-08-31

Page 1 of 2





TÜV SÜD Product Service GmbH + Zertifizierstelle + Ridlerstraße 65 + 80339 München + Germany

TUV®

A1 / 04.11

TABLE OF CONTENT

1. ABBREVIATIONS AND DEFINITIONS	6
2. INTRODUCTION	7
	_
3. USING FCX-AII VG FOR A SIS APPLICATION	8
	0
4. SAFETT RELATED FARAMETERS	9
5. HARDWARE FAULT TOLERANCE	10



Abbreviation	Definition	
MooN	"M out of N" architecture	
FIT	Frequency unit: 10-9 h-1	
λ_{S}	Safe (detected and undetected) failure rate [1/h]	
λ_{DD}	Dangerous detected failure rate [1/h]	
λ _{DU}	Dangerous undetected failure rate[1/h]	
PFDAVG	Average Probability of failure on demand	
PFH	Probability of dangerous failure per hour (IEC 61508-6)	
SFF	Safe failure fraction (IEC 61508)	
HFT	Hardware Fault Tolerance	
T ₁	Proof test interval [h]	
MTTR	Mean time to repair [h]	
MTBF	Mean time between failure	
SIS	Safety Instrumented System	
FMEDA	Failure Mode, Effects and Diagnosis Analysis	

Note : The MTTR is assumed to be 8 hours



FCX-All VG series of pressure transmitters have been evaluated by TÜV-SÜD Rail GmbH as per ISO/IEC 61508 standard and according to the following functional testing operations :

- Functional safety management (FSM) and safety lifecycle
- Analysis of the system structure (System-FMEA)
- Analysis of the hardware (FMEDA)
- Analysis of the software
- Error simulations and software tests
- Test of the error prevention measures
- Functional tests

Related standards :

Standard	Title
2006/42/EC	Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC
IEC 61508-1: 2010 (SIL3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
IEC 61508-2: 2010 (SIL3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/ programmable electronic safety- related systems
IEC 61508-3: 2010 (SIL3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements
IEC 61508-4: 2010 (SIL3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations
IEC 61511: 2004	Functional safety: Safety Instrumented Systems for the process industry sector

The Fig.1 below shows a typical configuration of a Safety Instrumented Function using the FCX-AII VG pressure transmitter.



Fig.1: Example of Safety Instrumented Function with FCX-AII VG

The FCX-All VG is supposed for use in a low demand operating mode. The Safety Integrity Level of the SIF must be evaluated taking into account the entire safety function i.e. including the FCX-All VG, the safety logic solver, the actuator and their respective PFD_{AVG} value.

The FCX-AII VG pressure transmitter generate a 4-20 mA signal proportional to the input pressure and uses the burnout current position in order to notify a failure condition to the safety logic solver. In order to monitor for faults, the safety logic solver must be able to detect either HI-alarm (output over-scale) or LO-alarm (output under-scale) burnout current values.

DANGER	FCX-All VG burnout current dir or "Output under-scale". The ' Safety Instrumented System co The FCX-All VG burnout curren •Output over-scale: •Output under-scale:	ection must be set either to "Output over-scale" Output hold" setting MUST NOT BE USED for a onfiguration. ts can be adjusted in the following ranges: [20.8 ; 22.5] mA [3.4 ; 3.8] mA
--------	---	--

The following table depicts the values from the quantitative analysis (SN 29500).

Dangerous Undetected Failure Rate	λ_{DU}	37.6 10 ⁻⁹ /h
Dangerous Detected Failure Rate	$\lambda_{ ext{DD}}$	792 10 ⁻⁹ /h
Safe Failure Rate (*)	$\lambda_{ m S}$	451 10 ⁻⁹ /h
Safe Failure Fraction	SFF	97 %
Average Probability of failure on Demand		1.71 10 ⁻⁴
(T1 = 1 year, MTTR = 8h)	PFD _{AVG}	
Probability of Failure per Hour	PFH	3.8 10 ⁻⁸ /h

 $\overline{(^*)} \lambda_{\rm S} = \lambda_{\rm SU} + \lambda_{\rm SD}$

Table 1: FCX-AIIVG Safety Data

As per the formula below, PFD_{AVG} (1001) depends upon the proof test interval T1 and the MTTR :

 $PFD_{AVG} = \lambda_{DU} (T1/2 + MTTR) + (\lambda_{DD} x MTTR)$

The proof test interval T1 is to be determined taking into account the overall safety integrated function for which the FCX-All VG is applied.

The figure below shows the FCX-All VG PFD_{AVG} values for T1 = 1 to 10 years and MTTR = 8 hours.



Fig.2 : FCX-AII VG PFD_{AVG} vs T1 (MTTR=8 hours)

The table below shows the achievable Safety Integrity Level for a type B system, depending the Safe Failure Fraction (SFF) and the Hardware Fault Tolerance (HFT).

Safe Failure Fraction	Hardware Fault Tolerance (HFT)		
(SFF)	0	1	
< 60 %	Not allowed	SIL 1	
60 % 90 %	SIL 1	SIL 2	
90 % 99 %	SIL 2	SIL 3	
> 99 %	SIL 3	SIL 4	

Table 2: SIL vs SFF and HFT

The FCX-All VG is SIL 2@HFT = 0 and SIL 3HFT = 1. To reach the SIL 3 using FCX-All VG pressure transmitters, the MooN architecture shall be implemented in order to insure a HFT = 1 (N-M=1). This can be achieved by either implementing 1002 or 2003 architectures.

The figures below show the 1002 and 2003 implementations.







Fig.3: FCX-AII VG SIL 3 HFT=1 (2003)

The choice between MooN architectures is a compromise between safety, system availability and cost. This is fully dependent of the nature of the process.



The resulting PFD_{AVG} shall be calculated taking into account the MooN architecture in order to check that $\sum_{i=1}^{n} PFD_{AVGi}$ of the safety integrated function satisfies the targeted safety integrity level.



Fuji Electric France S.A.S.

46 rue Georges Besse - Zl du brézet - 63039 Clermont ferrand Tél : 04 73 98 26 98 - Fax : 04 73 98 26 99 Mail : sales.dpt@fujielectric.fr - web : www.fujielectric.fr

Fuji Electric can accept no responsibility for possible errors in catalogues, brochures and other printed material. Fuji Electric reserves the right to alter its products without notice. This also applies to products already on order provided that such alterations can be made without subsequential changes being necessary in specifications already agreed. All trademarks in this material are property of the respective companies. All rights reseved.