SIL Declaration of Conformity

Functional safety according to IEC 61508

Manufacturer: PCB Piezotronics
3425 Walden Avenue
Depew, NY 14043 USA

PCB Piezotronics declares as manufacturer, that the DIN Rail Differential Charge Amplifiers:

- 682 Series - (XX)682yzzz/aaa

(XX) Options include one or more of the following:

EX – Approved for Hazardous Locations
M – Metric Mounting Hardware

Are suitable for use in safety-instrumented systems according to IEC 61508, if the safety instructions and the following parameters are observed:

Parameter	**682x Series**	**EX or M Series**
SIL	2	2
Proof Test Interval (Annual)	8,760 h	8,760 h
Device Type	B	B
HFT	0	0
SFF	98%	98%
PFD_{AV}[1]	1.58×10^{-8}	1.58×10^{-8}
$\lambda_{du} \times 10^{-9}$	0.03	0.03
SIL Capability (Low Demand Mode)	2	2
SIL Capability (Continuous Demand Mode)	2	2
MTTF[2]	10 y	10 y
1. The values comply with SIL2 according to ISA S84.01 2. According to Siemens SN29500 and Proven In Use data		

The PCB sensor hardware is suitable for inclusion in Safety Instrumented Systems (SIS) that are designed using IEC 61511 (for the process industry sector), IEC 62061 (safety of machinery), EN 50129 (railway applications), and ISO 26262 (automotive industry).

Note: The use of SIL Hardware in specific safety standard application may apply different number of sequences or definitions to those in IEC 61508.

May 20, 2021

PCB Piezotronics Authorized Representative:

Carrie Termin
Regulatory Affairs and Product Certification Specialist

PCB PIEZOTRONICS, INC. — CORPORATE HEADQUARTERS
3425 Walden Avenue, Depew, New York 14043-2495 USA
Phone: 716-684-0001 Fax: 716-684-0987
E-mail: info@pcb.com
Web site: www.pcb.com

intertek
Total Quality. Assured.

INTERTEK ASSURANCE FUNCTIONAL SAFETY CERTIFICATE REPORT

XX682YYY SENSOR SERIES FMEA REPORT

CLIENT NAME
PCB PIEZOTRONICS INC
3425 Walden Ave
Depew, NY 14043-2417USA

REPORT NO
104324913CSLT-002

COMPILED BY
Ashton D. Hainge, CFSP, PMP

PROJECT NAME
G104324913

DATE
07 May 2021


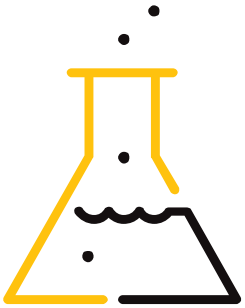

TABLE OF CONTENTS

1 XX682YYY SERIES SENSOR DOCUMENTATION AND RESULTS

1.1 Documentation for XX682YYY Series Sensor

This report details the results of the reliability analysis performed on the PCB Piezotronics 4-20 mA Output Sensor model XX682YYY series. These results are based on the following PCB Piezotronics documentation. Design changes from this documentation package would need to be evaluated for the impact on the reliability characteristics.

- Spec Sheet 55856-B.pdf
- 682 series returns 3-10-21.xlsx
- 682 series shipments 3-10-21.xlsx
- Manual 682c05.pdf

Reliability calculations were conducted using component and circuit level information. Product level failure parameters were then calculated in accordance with the functional safety approach of IEC 61508.

1.2 Overall Component Results SIL and PLr

The results from the FMEA are given below for 4-20 mA Output Sensor model XX682YYY with terminal block (worst case):

Name		Result
Component Performance Level	PLr	**PLr d**
Safety Integrity Level	SIL	**SIL 2**
Safe Failure Fraction	SFF	**0.98**
Hardware Fault Tolerance	HFT	**0**
Proof test interval	Annual	**8,760 h**
Probability of Failure On Demand	PFD_{avg}	**$1.58x10^{-8}$**
Safe Detected failure rate	λ_{SD} x 10^{-9} (FIT)	**0.99**
Safe Undetected failure rate	λ_{SU} x 10^{-9} (FIT)	**0.25**
Dangerous Detected failure rate	λ_{DD} x 10^{-9} (FIT)	**0.11**
Dangerous Undetected failure rate	λ_{DU} x 10^{-9} (FIT)	**0.03**
Average frequency of a dangerous failure on demand	PFH x 10^{-9} (FIT)	**0.03**

2 GENERAL FUNCTIONAL SAFETY CONSIDERATIONS

2.1 Diagnostic Coverage

For connections such as welding, connectors, and solders, the diagnostic coverages are based on inspection (reviews and analysis). Specified functions of the safety-related system are examined and evaluated to ensure that the safety-related system conforms to the requirements given in the specification. Any points of doubt concerning the implementation and use of the product are documented so they may be resolved. In contrast to a walk-through, the author is passive, and the inspector is active during the inspection procedure. – 60 % detection (IEC 61508-7 B.3.7 & IEC 61508-2 Table B.2)

All complex components are based on analogue signal monitoring technique. Wherever there is a choice, analogue signals are used in preference to digital on/off states. For example, trip or safe states are represented by analogue signal levels, usually with signal level tolerance monitoring. The technique provides continuity monitoring and a higher level of confidence in the transmitter, reducing the necessary proof-test frequency of the transmitter sensing function. External interfaces, for example impulse lines, will also require testing. – 60 % detection (IEC 61508-7 A.2.7 & IEC 61508-2 Table A.3)

All simple components are based on IEC 61508-2 Annex C.2. It is possible that open-circuit or short-circuit failures for simple components (resistors, capacitors, transistors) can be detected with a coverage of 100 %.

2.2 Safe and Dangerous Failure

Based on IEC 61508-6 Annex C. The division between safe (1) and dangerous (0) failures may be deterministic for simple components but is otherwise based on engineering judgement. Dangerous failure is any failure when the sensor does not detect any vibration when there is vibration or detects vibration when there is not. For complex components, where a detailed analysis of each failure mode is not possible, a division of failures into 50 % safe, 50 % dangerous is generally accepted. 50/50 were given to complex component that did not have manufactured reliability data.

2.3 Hardware Fault Tolerance

Hardware fault tolerance of “0” was used in this FMEA. Below is the SIL table from IEC 61508-2

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

According to IEC 61508-2 SFF of 90% or greater can be considered to have SIL 2 capability with a HFT of 0.

2.4 General FMEA Calculations (IEC 61508-2, 6)

Safe Failure Fraction:

$$SFF = \frac{\Sigma\lambda_S + \Sigma\lambda_{Dd}}{\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du}}$$

Average frequency of a dangerous failure on demand (*PFH)*:

$$PFH = \sum \lambda_{DU}$$

PFD_{avg} calculations:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$

For 1oo1:

- MRT = 8 hours
- MTTR = 8 hours
- Assumption one year for T1 = 8,760 h

$$PFD_{avg} = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

3 PLR MACHINE SAFETY IEC 62061 AND EN/ISO 13849-1

The EN/ISO 13849-1 machine safety standard uses a qualitative risk graph, or flow chart, to assign a performance level (PL), based on three criteria:

- severity of injury
- frequency and/or exposure time to the hazard
- possibility of avoiding the hazard or limiting the harm

The performance level (PL) is designated by an alphabetic character, a thru e, with PLe being the highest risk level.

Once the performance level has been determined, the architecture that facilitates the defined performance level is classified into one of six categories ("B" and 1 thru 5, with B being the least safe and 5 being the safest). The architecture category is determined by combining the performance level (PL) with quantitative measures of diagnostic coverage (DC) and mean time to dangerous failure (MTTFd).

3.1 EN/IEC 62061 Machine Safety

The EN/IEC 62061 machine safety standard (often written as just EN 62061) assigns a safety integrity level (SIL) to each function based on the severity of the potential harm (Se) and the probability of the harm occurring.

The severity of potential harm is given a score from 1 to 4, with 4 being the most severe. The probability of harm occurring is broken down into three parameters:

- frequency and duration of exposure (Fr)
- probability of an event occurring (Pr)
- probability of avoiding or limiting the harm (Av)

Each of these parameters is scored from 1 to 5, with 5 being the "worst," or least safe situation, and their scores are summed to determine a class (Cl). The SIL rating is then chosen from a matrix that plots the severity scores (Se) and classes (Cl).

3.2 EN/ISO 13849-1 Machine Safety

Note that performance level (PL) ratings under EN/ISO 13849-1 are also correlated with probability of dangerous failures per hour (PFHd) values, so direct comparisons can be made between EN/ISO 13849-1 performance levels and EN 62061 safety integrity levels.

3.3 Performance Level PLr

Once the safety integrity level (SIL) has been assigned, the system is broken into subsystems, whose architectures are classified as a, b, c, or d, with d being the "highest," or safest. Each architecture is associated with a formula to determine the probability of dangerous failure per hour (PFHd) of the subsystem.

PL (Performance Level)	PFH_D (Probability of Dangerous Failure per Hour)	SIL
a	$\geq 10^{-5}$ to $<10^{-4}$	None
b	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
c	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $<10^{-6}$	2
e	$\geq 10^{-8}$ to $<10^{-7}$	3

Figure 3-1 – Performance Level Chart