SENSOR TECHNIK

Application Note

SIL2 IEC 61508
ADZ PERFORMANCE

Pressure Transducers for Applications with **Safety Integrated Level or Performance Level** Requirements

SIL 2, PL: d

Exemplary, typical configuration

EI-000024-C.DOCX

ADZ NAGANO GmbH
Gesellschaft für Sensortechnik
Bergener Ring 43 • D-01458 Ottendorf-Okrilla
Tel.: +49 (0) 35 205 / 59 69-30 • Fax: -59
eMail: info@adz.de
Internet: www.adz.de

PRODUCT CONFIGURATION

Product series: **SMO**
Output Signal configuration: **18.0**

SIL2 IEC-61508 ADZ PERFORMANCE

PERFORMANCE LEVEL INFORMATION

The sensor enables an EC-controlled safety system to perform as follows.
These values have been calculated in accordance to

[1] DIN EN ISO 13849-1
[2] EN61508-6
[3] IEC-TR62380
[4] EPB-000110 & EPB-000206
[5] FSM ZSC31050 Rev. 1.00 / April 2015

Output Signal Safety Limits / diagnostic range:

The electronic circuity and signal conditioner are providing defines safety limits for the output signal.
These limits must be considered in the System ECU to enable the system to go into a safe state upon detecting these.
The ***low*** diagnostic range is **<3,85mA**
The ***high*** diagnostic range is **>22mA**
Depending on the detected failure, the output signal will go *below* or *above* these limits.

Detected internal failures:

The following internal failures are detected by the signal conditioner and will actively lead to an output signal *below* or *above* the defined safety limits

- Broken bond wires (connection to the sensing element, in operation) **RESULT: >22mA**
- Broken bond wires (connection to the sensing element, before power on) **RESULT: <3,85mA**
- Internal EEPROM errors caused by CRC **RESULT: <3,85mA**
- Internal Watchdog (will trigger for different internal failures) **RESULT: <3,85mA**

Startup time / power on:

- Startup time / power on = **max 40 ms**

During the defined startup period the output signal may vary between the diagnostic ranges.
The Signal **must not** be used in the ECU to determine sensor or system status.

MTTFd Values / Performance Level:

The following performance level values have been determined (ref [4] and [5])

- $MTTF_d$ = **228 (100*) years**
- Failure Rate (λ_F) = **0,832310 $10^{-6}H^{-1}$**
- DC (diagnostic coverage, dangerous failures) = **72,17% (considered *low*)**
- CCF (common cause failures) = **65% ("use of proven component" [5])**
- PERFORMANCE LEVEL = **d, for a category 2 system, acc. Table K1 of [1]**

** According to [1] the $MTTF_d$ is limited to 100 years.*

The following values are not used for performance level rating, but may be used for system evaluation.

- PFH = **1,392*$10^{-7}H^{-1}$**
- SFF = **83,27%**

The hardware architecture is defined as: **1001**
Considered mission profile for failure rate calculation: *Automotive, Motor control cycling of [3]*

ADZ NAGANO GmbH
Gesellschaft für Sensortechnik
Bergener Ring 43 • D-01458 Ottendorf-Okrilla
Tel.: +49 (0) 35 205 / 59 69-30 • Fax: -59
eMail: info@adz.de
Internet: www.adz.de

Anwendungshinweis

SIL2 IEC 61508
ADZ PERFORMANCE

Drucktransmitter für Anwendungen mit der Forderung nach einem

Sicherheits-Integritätslevel oder Performance Level

SIL 2, PL: d

Beispielhafte Darstellung, typische Konfiguration

ADZ NAGANO GmbH
Gesellschaft für Sensortechnik
Bergener Ring 43 • D-01458 Ottendorf-Okrilla
Tel.: +49 (0) 35 205 / 59 69-30 • Fax: -59
eMail: info@adz.de
Internet: www.adz.de

PRODUKT KONFIGURATION
Produktreihe: **SMO**
Ausgangssignalkonfiguration: **18.0**

SIL2 IEC 61508
ADZ PERFORMANCE

INFORMATIONEN ZUM PERFORMANCE LEVEL
Der Sensor versetzt ein Sicherheitssystem welches über eine zentrale Steuereinheit kontrolliert wird, wie nachfolgend darstellt zu arbeiten.
Die Werte wurden in Anlehnung und nach den Vorgaben der folgenden Normen und Standards berechnet:

[1] DIN EN ISO 13849-1
[2] EN61508-6
[3] IEC-TR62380
[4] EPB-000110 & EPB-000206
[5] FSM ZSC31050 Rev. 1.00 / April 2015

Grenzen und Diagnosebereiche des Ausgangssignals:
Die elektronische Schaltung sowie der signalkonditionierende Schaltkreis stellen definierte Grenzen für das Ausgangssignal bereit. Diese Grenzwerte müssen in der Steuereinheit berücksichtigt und detektiert werden. Im Falle der Über- oder Unterschreitung der Grenzen muss das sicherheitskritische System in einen sicheren Zustand gebracht werden.
Unterer Diagnosebereich / Grenzwert: **<3,85mA**
Oberer Diagnosebereich / Grenzwert: **>22mA**
In Abhängigkeit des erkannten Fehlers, wird das Ausgangssignal *über* oder *unter* die Grenzwerte gesetzt.

Erkennbare interne Fehler
Die nachfolgenden internen Fehler können aktiv durch den Schaltkreis erkannt werden. Bei Erkennen dieser Fehler wird das Ausgangssignal aktiv *über* oder *unter* die Grenzwerte gesetzt.

❍ zerstörte / gebrochene Bonddrähte (zum Sensorelement, in Betrieb)	**SIGNAL:**	**>22mA**
❍ zerstörte / gebrochene Bonddrähte (zum Sensorelement, vor Einschalten)	**SIGNAL:**	**<3,85mA**
❍ interner EEPROM Fehler, führt zu CRC Fehler	**SIGNAL:**	**<3,85mA**
❍ interner Watchdog (kann durch diverse interne Fehler aktiviert werden)	**SIGNAL:**	**<3,85mA**

Aufstartzeit nach Einschalten:
❍ Aufstartzeit nach Einschalten = **max 40 ms**
Das Ausgangssignal kann während der Aufstartzeit schwanken und auch die Grenzwerte über- oder unterschreiten. Während dieser Zeit **darf** das Signal **nicht** zur Erkennung des System- oder Sensorstatus verarbeitet werden.

MTTFd Werte / Performance Level:
Die folgenden Werte für das Performance Level wurden bestimmt (siehe [4] und [5])

❍ $MTTF_d$	=	**228 (100*) Jahre**
❍ Gesamtfehlerrate (λ_F)	=	**0,832310 $10^{-6}H^{-1}$**
❍ DC (diagnostic coverage, gefährliche Fehler)	=	**72,17% (als *niedrig* eingestuft)**
❍ CCF (common cause failures)	=	**65% (“Einsatz bewährter Komponenten” [5])**
❍ PERFORMANCE LEVEL	=	**d, für ein System der Kat. 2 nach Table K1 aus [1]**

** Nach [1] wird der Wert für $MTTF_d$ auf 100 Jahre begrenzt.*

Nachfolgende Werte sind nicht für die Verwendung oder Bewertung des Performance Levels erforderlich, können aber für die Auslegung und Bewertung des bzw. im Gesamtsystem(s) von Relevanz sein.

❍ PFH	=	**1,392*10^{-7}H^{-1}**
❍ SFF	=	**83,27%**

Die Architektur der eingesetzten Hardware ist definiert als: **1001**
Missionsprofil zur Berechnung der Ausfallraten: *Automotive, Motor control cycling of [3]*

ADZ NAGANO GmbH
Gesellschaft für Sensortechnik
Bergener Ring 43 • D-01458 Ottendorf-Okrilla
Tel.: +49 (0) 35 205 / 59 69-30 • Fax: -59
eMail: info@adz.de
Internet: www.adz.de