SRD991 Intelligenter Stellungsregler

SRD960 Universeller Stellungsregler

Funktionale Sicherheit

Safety **I**ntegrity **L**evel

SIL certified

acc. to IEC 61508 / IEC 61511

Der Intelligenter Stellungsregler SRD991 und der Universelle Stellungsregler SRD960 dienen zur Ansteuerung pneumatischer Stellantriebe durch Leitsysteme und elektrische Regler, welche den besonderen Anforderungen der Sicherheitstechnik nach IEC 61508 / IEC 61511-1 genügen sollen. Die sicherheitsgerichtete Funktion des Stellungsreglers bezieht sich dabei auf einfachwirkende Stellungsregler für pneumatische Antriebe mit Federrückstellung.

MERKMALE

- Beurteilung der funktionalen Sicherheit gemäß IEC 61508 / IEC 61511-1durch *exida.com* ®
- Einsetzbar bis SIL 3
- Permanente Selbstüberwachung
- Explosionsschutz (je nach Version)
- Elektromagnetische Verträglichkeit nach EN 61326 und NAMUR-Empfehlung NE21

FOXBORO ECKARDT

INHALTSVERZEICHNIS

1 ANWENDUNGSBEREICH

1.1 Allgemein

Der Anwendungsbereich erstreckt sich auf intelligente Stellungsregler vom Typ SRD991 ab Geräterevision 3.3 (HART und 4-20mA ohne Kommunikation) mit einfachwirkendem pneumatischen Leistungsverstärker (Modelcode SRD991-BHxxx und SRD991-BDxxx) und auf universelle Stellungsregler vom Typ SRD960 mit einfachwirkendem pneumatischen Leistungsverstärker (Modelcode SRD960-BHxxx und SRD960-BDxxx) zur Ansteuerung pneumatischer Stellantriebe mit Federrückstellung.

Bei Ausfall der elektrischen und/oder pneumatischen Hilfsenergie wird automatisch der Ausgang Y1 des Stellungsreglers drucklos geschaltet. Durch die damit verbundene Entlüftung wird der Stellantrieb in die, durch die Federn vorbestimmte, sichere Endlage gefahren. Im Falle eines Fehlers innerhalb des Stellungsreglers selbst wird der Ausgang Y1 ebenfalls drucklos geschaltet.

Der Einsatz des Stellungsreglers unter den besonderen Anforderungen der Sicherheitstechnik kann auf drei verschiedene Arten geschehen.

All diese drei Einsatzarten basieren auf einer hardwaremäßigen Abschaltung der pneumatischen Ausgangsstufe mit dem zuvor genannten Verhalten. Dadurch ist gewährleistet, dass die Abschaltung unabhängig von allen softwaremäßigen Einstellungen und Parameterkonfigurationen (z.B. Dichtschließen, Ventilkennlinie, Invertierung, Hubbegrenzung, usw.) stattfinden kann. Somit sind alle softwaremäßigen Einstellungen und Parameterkonfigurationen für die sicherheitsgerichtete Funktion des Stellungsreglers nicht relevant.

1.1.1 Stromabschaltung unter Schwelle 0,2mA

Der Stellungsregler wird in diesem Fall derart betrieben, dass im Anforderungsfall zumindest die elektrische Hilfsenergie unter einen Schwellwert von 0,2mA abgeschaltet wird. Für diesen Fall kommen die sicherheitstechnischen Kenndaten nach Kapitel 5.2 zur Anwendung.

1.1.2 Stromabschaltung unter Schwelle 2mA

Der Stellungsregler wird in diesem Fall derart betrieben, dass im Anforderungsfall die elektrische Hilfsenergie unter einen Schwellwert von 2mA geschaltet wird. Für diesen Fall kommen die sicherheitstechnischen Kenndaten nach Kapitel 5.3 zur Anwendung.

1.1.3 Normalabschaltung

Der Stellungsregler wird in diesem Fall derart betrieben, dass im Anforderungsfall das Einheitssignal auf einen Wert <= 3,8mA (siehe hierzu auch [Ref. 6]) gestellt wird. Für diesen Fall kommen die sicherheitstechnischen Kenndaten nach Kapitel 5.4 zur Anwendung.

1.2 Voraussetzungen

Für den Einsatz unter den besonderen Anforderungen der Sicherheitstechnik nach IEC 61508 / IEC 61511-1 sind folgende Voraussetzungen zu beachten:

- Beim Einsatz des Stellungsreglers ist darauf zu achten, dass die in [Ref. 4] spezifizierten technischen Daten, insbesodere bzgl. Einsatz- und Umgebungsbedingungen, eingehalten werden.
- Einsatz nur in Verbindung mit einfachwirkenden pneumatischen Stellantrieben.
- Der Stellantrieb muss hierbei derart ausgelegt sein, dass er im drucklosen Betrieb mit Hilfe von Federn die sichere Stellung anfährt.
- Die pneumatische Hilfsenergie (Zuluft) muß frei von Wasser, Öl und Staub gemäß ISO 8573-1, Feststoffpartikelgröße und –dichte Klasse 2 und Ölgehalt Klasse3, ausgeführt sein.
- Die mittlere Einsatztemperatur über einen längeren Zeitraum ist nicht größer als 40°C
- Der Stellungsregler SRD991 / SRD960 wird nur in Anwendungen mit niedriger Anforderungsrate eingesetzt.
- Der Sollwert ist ausschließlich durch den analogen Stromwert definiert. Damit wird die HART-Kommunikation als nicht sicherheitsrelevant eingestuft.
- Nach der Montage, Anschluss und Inbetriebnahme des Stellungsreglers gemäß [Ref. 5] ist eine Funktionsprüfung durchzuführen:
  - Als Sollwert 4mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination in die korrekte Endlage fährt.
  - Als Sollwert 20mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination in die korrekte Endlage fährt.
  - Als Sollwert 12mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination die korrekte Ventilposition (z.B. 50% bei linearer Kennlinie) anfährt.
  - Überprüfen der Klemmenspannung bei 20mA Eingangsstrom. Diese sollte für ein Gerät vom Typ SRD991-BDxxx den Wert 6V DC und für ein Gerät vom Typ SRD991-BHxxx den Wert 8V DC nicht überschreiten.
- Die regelmäßige Funktionsprüfung (siehe Kapitel 4.2) ist durchzuführen.

2 ALLGEMEIN

2.1 Relevante Normen

- DIN EN 61508 Teil 1 bis 7: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektonischer/programmierbarer elektronischer Systeme
- DIN IEC 61511 Teil 1 bis 3: Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

2.2 Begriffe

Die hier aufgeführten Begriffe sind gemäß [Ref. 1], Teil 4 und [Ref. 2], Teil 1 definiert.

Name	Beschreibung
Aktor	Teil eines sicherheitstechnischen Systems, das die Eingriffe in den Prozess ausführt, um einen sicheren Zustand zu erreichen.
Ausfall	Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen.
Diagnosedeckungs-grad	Verhältnis der Ausfallrate der durch Diagnosetests erkannten Fehler zur Gesamtausfallrate der Komponente oder Teilsystems. Der Diagnosegrad beinhaltet keine bei Wiederholungsprüfungen festgestellten Fehler.
Fehler	Anomaler Zustand, der eine Verminderung oder Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen.
Funktionale Sicherheit	Teil der Gesamtsicherheit, der sich auf den Prozess und das BPCS bezieht und der von der bestimmungsgemäßen Funktion des SIS und anderer Sicherheitsebenen abhängt.
Funktionseinheit	Einheit aus Hardware oder Software oder beidem, die zur Durchführung einer festgelegten Aufgabe geeignet ist.
Gefährlicher Ausfall	Ausfall mit dem Potential, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu versetzen.
Sicherheit	Freiheit von unvertretbaren Risiken
Sicherheitsfunktion	Funktion, die von einem SIS, einem sicherheitsbezogenen System anderer Technologie oder von externen Einrichtungen zur Risikominderung ausgeführt wird, mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für den Prozeß zu erreichen oder aufrecht zu erhalten.
Sicherheitsintegrität	Mittlere Wahrscheinlichkeit, dass ein sicherheitstechnisches System die geforderten sicherheitstechnischen Funktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt.
Sicherheits-Integritätslevel (SIL)	Eine von vier diskreten Stufen zur Spezifikation der Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem sicherheitstechnischen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 den höchsten Grad der Sicherheitsintegrität, der Sicherheits-Integritätslevel 1 den niedrigsten darstellt.
Sicherheitstech-nisches System (SIS)	Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheits-technischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktor(en).
Ungefährlicher Ausfall	Ausfall ohne das Potential, das sicherheitstechnische System in einen gefahr-bringenden oder funktionsunfähigen Zustand zu setzen.

2.3 Abkürzungen

Abkürzung	Beschreibung (Englisch)	Beschreibung (Deutsch)
λ	Failure rate per hour	Ausfallrate pro Stunde
λ_D	Dangerous failure rate per hour	Rate gefahrbringender Ausfälle je Stunde
λ_{DD}	Detected Dangerous failure rate per hour	Rate erkannter gefahrbringender Ausfälle je Stunde
λ_{DU}	Undetected Dangerous failure rate per hour	Rate unerkannter gefahrbringender Ausfälle je Stunde
λ_S	Safe failure rate per hour	Rate ungefährlicher Ausfälle je Stunde
λ_{SD}	Detected Safe failure rate per hour	Rate erkannter ungefährlicher Ausfälle je Stunde
λ_{SU}	Undetected Safe failure rate per hour	Rate unerkannter ungefährlicher Ausfälle je Stunde
BPCS	Basic process control system	Betriebs- und Überwachungseinrichtungen als ein System
DC	Diagnostic coverage	Diagnose-Deckungsgrad
FIT	Failure in Time (1×10^{-9} per h)	Fehler pro Zeit (1×10^{-9} pro h)
HFT	Hardware fault tolerance	Hardware-Fehlertoleranz
PFD	Probability of failure on demand	Wahrscheinlichkeit eines Ausfalls bei Anforderung
PFD_{avg}	Average probability of failure on demand	Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung
MooN	Architecture with M out of N channels	Architektur mit M aus N Kanälen
MTBF	Mean Time Between Failures	Mittlere Zeitdauer zwischen zwei Ausfällen
MTTR	Mean Time To Repair	Mittlere Zeitdauer zwischen dem Auftreten eines Fehlers und der Reparatur
SFF	Safe failure fraction	Anteil ungefährlicher Ausfälle
SIL	Safety integrity level	Sicherheits-Integritätslevel
SIS	Safety instrumented system	Sicherheitstechnisches System

2.4 Auslegungstabellen

Die nachfolgenden Tabellen dienen zur Bestimmung des Sicherheits-Integritätslevels (SIL).

2.4.1 Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFD_{avg})

Diese Tabelle gibt den erreichbaren Sicherheits-Integritätslevel (SIL) in Abhängigkeit von der mittleren Wahrscheinlichkeit eines Ausfalls bei Anforderung wieder. Die angegebenen Ausfallgrenzwerte sind hierbei gültig für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird (siehe [Ref. 1] Teil 1, Kapitel 7.6.2.9).

Sicherheits-Integritätslevel (SIL)	PFD_{avg} mit niedriger Anforderungsrate
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

2.4.2 Sicherheitsintegrität der Hardware

Nach [Ref. 1] Teil 2, Kapitel 7.4.3.1.2 udn 7.4.3.1.3. ist zwischen Systemen vom Typ A und Systemen vom Typ B zu unterscheiden.

Für Typ A –Systeme gilt:

- Das Ausfallverhalten aller eingesetzter Bauteile ist ausreichend definiert und
- das Verhalten des Teilsystems unter Fehlerbedingungen vollständig bestimmt werden kann und
- verlässliche Ausfalldaten durch Felderfahrungen für das Teilsystem existieren um zu zeigen, dass die angenommenen Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle erreicht werden.

Für Typ B – Systeme gilt:

- Das Ausfallverhalten von mindestens einem eingesetzten Bauteil nicht ausreichend definiert ist oder
- das Verhalten des Teilsystems unter Fehlerbedingungen nicht vollständig bestimmt werden kann oder
- keine ausreichend zuverlässigen Ausfalldaten aus Felderfahrung für das Teilsystem vorliegen, um die in Anspruch genommenen Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle zu unterstützen.

Diese folgenden Tabellen geben den erreichbaren Sicherheits-Integritätslevel (SIL) in Abhängigkeit vom Anteil der ungefährlichen Ausfälle (SFF) und der Fehlertoleranz der Hardware (HFT) für sicherheitsbezogene Typ A- und Typ B-Teilsysteme (siehe [Ref. 1] Teil 2, Kapitel 7.4.3.1.4) an.

Anteil ungefährlicher Ausfälle (SFF)	**Fehlertoleranz der Hardware (HFT) für Typ A**		
	0	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3
60% - < 90%	SIL 2	SIL 3	SIL 4
90% - < 99%	**SIL 3**	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Anteil ungefährlicher Ausfälle (SFF)	**Fehlertoleranz der Hardware (HFT) für Typ B**		
	0	**1 (0)[1]**	**2**
< 60%	Nicht erlaubt	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

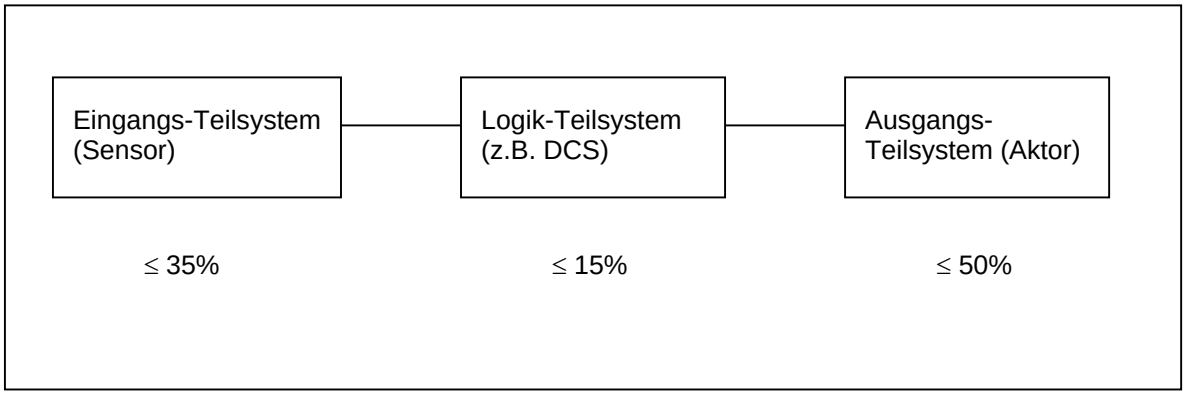
1) Nach [Ref. 2] Teil 1, Kapitel 11.4.4 dürfen bei Teilsystemen wie z.B. Sensoren und Aktoren die Fehlertoleranz der Hardware (HFT) um eins reduziert werden (Werte in Klammern), wenn das verwendete Gerät alle folgenden Bedingungen erfüllt:

- Das Gerät ist betriebsbewährt
- Am Gerät können nur prozessrelevante Parameter geändert werden
- Die Veränderung der prozessrelevanten Parameter ist geschützt (z.B. Passwort, Jumper, usw.)
- Die Funktion hat einen geforderten Sicherheits-Integritätslevel von weniger als SIL 4.

Diese genannten Bedingungen treffen auf die Stellungsregler SRD991 / SRD960 zu.

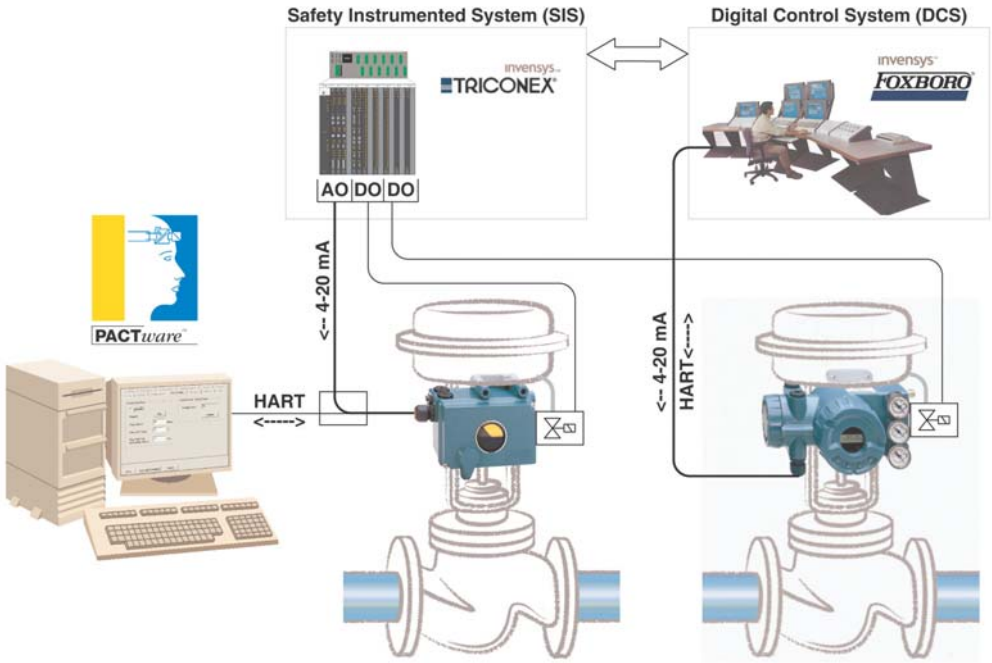
2.4.3 Sicherheitsbezogenes System

Ein sicherheitsbezogenes System besteht üblicherweise aus de drei Teilsystemen Eingangs-Teilsystem (Sensor), Logik-Teilsystem (SPS oder Leitsystem) und Ausgangs-Teilsystem (Stellgerät bestehend aus Stellungsregler, Antrieb und Ventil). Die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung wird dabei üblicherweise wie folgt aufgeteilt:



Beispiel für eine Ankopplung des Stellungsreglers SRD mit HFT=1

- in ein sicherheitsgerichtetes System über AO-Module mit energetischer Entkopplung der HART-Kommunikation z.B. über HART-Multiplexer und zusätzlicher Ansteuerung des Magnetventils über DO-Module
- in eine Leitsystemumgebung mit Stromversorgung sowie HART-Kommunikation und zusätzlicher Ansteuerung des Magnetventils über DO-Module



3 VERHALTEN IM BETRIEB UND BEI STÖRUNG

Das Verhalten im Betrieb und bei Störungen ist in der Inbetriebnahme- und Wartungsanleitung MI EVE0105 E [Ref. 5] für SRD991 bzw. MI EVE0109 A [Ref. 9] für SRD960 beschrieben.

4 WIEDERKEHRENDE PRÜFUNGEN DES STELLUNGSREGLERS

4.1 Sicherheitsüberprüfung

Gemäß IEC 61508/61511 ist die Sicherheitsfunktion des gesamten Sicherheitskreises regelmäßig zu überprüfen. Die hierfür notwendigen Testintervalle werden bei der Berechnung des jeweiligen Sicherheitskreises bestimmt.

4.2 Funktionsüberprüfung

Die ordnungsgemäße Funktionsfähigkeit des Stellungsreglers regelmäßig einmal pro Jahr zu überprüfen. Hierbei sind folgende Funktionen auszuführen:

- Überprüfen der angezeigten Status- und Diagnosemeldungen via LED, LCD oder HART-Kommunikation.
- Überprüfen des Zuluftfilters und ggfs. Tausch gemäß MI EVE 0105 E Kap. 10.2 ([Ref. 5]) bzw. MI EVE0109 A Kap. 10.2 ([Ref. 9]).
- Neustart (Reset) des Stellungsreglers durch gleichzeitiges Drücken aller 3 Tasten (4 Tasten beim SRD960) oder kurzzeitiges Unterbrechen des Eingangsstromes.
- Ausführen eines Kurzautostarts zur Neubestimmung der Ventilanschläge.
- Als Sollwert 4mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination in die korrekte Endlage fährt.
- Als Sollwert 20mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination in die korrekte Endlage fährt.
- Als Sollwert 12mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination die korrekte Ventilposition (z.B. 50% bei linearer Kennlinie) anfährt.
- Überprüfen der Klemmenspannung bei 20mA Eingangsstrom. Diese sollte für ein Gerät vom Typ SRD991/SRD960-BDxxx den Wert 6V DC und für ein Gerät vom Typ SRD991/SRD960-BHxxx den Wert 8V DC nicht überschreiten.

Der Stellungsregler selbst bedarf keiner turnusmäßigen Wartung. Bei Instandhaltung- oder Instandsetzungsarbeiten ist das Kapitel 10 der Inbetriebnahme- und Wartungsanleitung MI EVE0105 E ([Ref. 5]) bzw MI EVE0109 A ([Ref. 9]) zu beachten.

4.3 Reparaturen

Defekte Geräte sollten unter Angabe der genauen Störung bzw. Ursache an die Reparaturabteilungvon Foxboro Eckardt gesandt werden

5 SICHERHEITSTECHNISCHE KENNGRÖßEN

Bei den sicherheitstechnischen Kenngrößen ist zwischen den beiden in Kapitel 1.1 erläuterten Einsatzarten „Stromabschaltung“ und „Normalabschaltung“ zu unterscheiden. Weitere, über diese Zusammenfassung hinausgehende Informationen, sind in Kapitel 8 beinhaltet.

5.1 Annahmen

Die in den folgenden Unterkapiteln angegebenen Kenngrößen gelten unter folgenden Annahmen:

- Die Voraussetzungen aus Kapitel 1.2 sind erfüllt.
- Die Reparaturzeit (MTTR) nach einem Gerätefehler beträgt 8 Stunden.
- Prüfinterval: ≤ 1 Jahr.
- Die Diagnosezeit der internen Tests beträgt ≤ 20 Minuten.
- Ein gefahrbringender Ausfall für beide Einsatzarten der Stromabschaltung ist definiert als ein Fehler, bei dem das Gerät auf die Anforderung des Abschaltens unter die jeweilige Schwelle nicht reagiert.
- Ein gefahrbringender Ausfall für die Einsatzart Normalabschaltung ist definiert als ein Fehler, bei dem das Gerät auf die Anforderung des Abschaltens (Eingangsstrom ≤ 3,8mA) nicht reagiert.

5.2 Stromabschaltung unter Schwelle 0,2mA

Gerätetyp	Kategorie	HFT	SFF	PFD_{avg}	λ_{du}	λ_{dd}	λ_{su}	λ_{sd}
A	SIL 3	0	94%	$8{,}8x10^{-5}$	20 FIT	0 FIT	327 FIT	0 FIT

5.3 Stromabschaltung unter Schwelle 2mA

Gerätetyp	Kategorie	HFT	SFF	PFD_{avg}	λ_{du}	λ_{dd}	λ_{su}	λ_{sd}
A	SIL 2	0	93%	$1{,}2x10^{-4}$	27 FIT	1 FIT	342 FIT	0 FIT

5.4 Normalabschaltung

Gerätetyp	Kategorie	HFT	SFF	PFD_{avg}	λ_{du}	λ_{dd}	λ_{su}	λ_{sd}
B	SIL 2	0	90%	$3{,}2x10^{-4}$	73 FIT	73 FIT	572 FIT	43 FIT

6 LITERATURVERZEICHNIS

[Ref. 1] DIN EN 61508 Teil 1-7
Beuth-Verlag, Berlin

[Ref. 2] DIN IEC 61511 Teil 1-3
Beuth-Verlag, Berlin

[Ref. 3] Functional safety and IEC 61508 – A basic guide, November 2002
IEC

[Ref. 4] SRD991 Intelligenter Stellungsregler
Typenblatt
Foxboro Eckardt GmbH, PSS EVE0105 E

[Ref. 5] SRD991 Intelligenter Stellungsregler
Inbetriebnahme- und Wartungsanleitung
Foxboro Eckardt GmbH, MI EVE0105 E

[Ref. 6] Namur-Empfehlung NE 43
NAMUR Geschäftsstelle, Leverkusen.

[Ref. 7] Failure Modes, Effects and Diagnostics Analysis for Intelligent Positioner SRD991 and SRD960
exida, Report No. Foxboro 04/08-16 R001.

[Ref. 8] SRD960 Universeller Stellungsregler
Typenblatt
Foxboro Eckardt GmbH, PSS EVE0109 E

[Ref. 9] SRD960 Universeller Stellungsregler
Inbetriebnahme- und Wartungsanleitung
Foxboro Eckardt GmbH, MI EVE0109 E

7 KONFORMITÄTSERKLÄRUNG

SIL Konformitätserklärung
Declaration of conformity

invensys
ECKARDT

Eckardt SAS · 20, rue de la Marne · F-68360 Soultz
Foxboro Eckardt Development GmbH · Glockenstr. 52 · D-70376 Stuttgart

Stuttgart, 22.4.2005

Funktionale Sicherheit nach IEC 61508 / IEC 61511
Functional Safety according to IEC 61508 / IEC 61511

Wir erklären, dass die Geräte
We declare, that the devices

SRD991-BHxxx, SRD991-BDxxx
SRD960-BHxxx, SRD960-BDxxx

für den Einsatz in einer sicherheitsgerichteten Anwendung entsprechend der IEC 61511-1 geeignet sind, wenn die Sicherheitshinweise und die nachfolgenden Parameter beachtet werden:
are suitable for use in a safety related application according IEC 61511-1,
if the safety instructions and the following parameters are observed:

Einsatzart Usage	Stromabschaltung unter Schwelle 0,2mA Shutdown device, threshold 0,2mA	Stromabschaltung unter Schwelle 2mA Shutdown device, threshold 2mA	Normalabschaltung Smart positioner
SIL	3	2	2
Prüfintervall / Proof test interval	≤ 1 Jahr / year		
Gerätetyp / Device Type	A	A	B
HFT	0 [1] (einkanalige Verwendung / single channel usage)		
SFF	94%	93%	90%
PFG_{avg}	$8{,}8 \times 10^{-5}$	$1{,}2 \times 10^{-4}$	$3{,}2 \times 10^{-4}$
λ_{du}	20 FIT	27 FIT	73 FIT
λ_{dd}	0 FIT	1 FIT	73 FIT
λ_{su}	327 FIT	342 FIT	572 FIT
λ_{sd}	0 FIT	0 FIT	43 FIT
DC_S	0%	0%	7%
DC_D	0%	4%	50%

[1] gemäß Kapitel / according to chapter 11.4.4 of IEC 61511-1

Robert Leng
General Manager
Eckardt SAS

Gilles Annenkoff
Quality Manager
Eckardt SAS

Dr. Joachim Seckler
Development Manager Positioner
Foxboro Eckardt
Development GmbH

8 MANAGEMENT SUMMARY

Failure Modes, Effects and Diagnostics Analysis

Project:
Intelligent Positioner SRD 991 and SRD 960

Customer:
Foxboro Eckardt GmbH
Stuttgart
Germany

Contract No.: Foxboro 04/08-16
Report No.: Foxboro 04/08-16 R001
Version V1, Revision R0, April 2005
Rainer Faller

Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the intelligent positioner SRD 991 / SRD 960. The considered safety-related application of the intelligent positioner SRD 991 / SRD 960 is as a shutdown device with fail-safe single-acting (spring return) actuation.

The intelligent positioners differ by their explosion protection, SRD 991: EEx ia and SRD 960: EEx d / EEx ia. For functional safety applications, the intelligent positioner SRD 991 / SRD 960 can be operated in three modes:

- 0..20 mA shutdown mode, shutdown threshold: 0,2 mA
- 0..20 mA shutdown mode, shutdown threshold: 2 mA
- 4..20 mA positioner mode, shutdown threshold: 3,8 mA.

In shutdown mode, an input current of less than the shutdown threshold (0,2mA or 2mA) leads to a shutdown of the corresponding pressure output. The different levels of shutdown threshold are to compensate possible leakage currents of the driving output.

In positioner mode, an input current of less than 3,8 mA leads to a shutdown of the corresponding pressure output, provided the positioner is configured per the Safety Manual TI EVE 0105 S. All other possible input variants or electronics are not covered by this report.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates used in this analysis are the basic failure rates for electronic components from the Siemens standard SN 29500. For mechanical components experience-based *exida* data and field failure evaluations from Eckardt S.A.S. France were used.

The control electronics of the intelligent positioner SRD 991 / SRD 960 are considered to be a Type B[1] subsystem with a hardware fault tolerance of 0. The pneumatics of the intelligent positioner SRD 991 / SRD 960 are considered to be a Type A[2] subsystem with a hardware fault tolerance of 0.

Table 1: Summary for SRD 991 / SRD 960 as shutdown device, threshold 0,2mA – Type A device, IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S[3]	DC_D
0 FIT	327 FIT	0 FIT	20 FIT	94%	0%	0%

These failure rates do not include failures resulting from incorrect use of the intelligent positioner, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the PG inlets.

A user of the intelligent positioner SRD 991 / SRD 960 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

[3] DC means the diagnostic coverage (safe or dangerous).

The failure rates are valid for the useful life of the instrument. According to section 7.4.7.4 note 3 of IEC 61508-2, experience has shown that the useful lifetime often lies within a range of 8 to 12 years.

Table 2: Summary for SRD 991 / SRD 960 as shutdown device, threshold 0,2mA – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 years	T[Proof] = 10 years
8,8E-05	1,8E-04	4,4E-04	8,8E-04

The boxes marked in yellow (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2,0E-04. The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2,0E-04.

Table 3: Summary for SRD 991 / SRD 960 as shutdown device, threshold 2mA – Type A device, IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0 FIT	342 FIT	1 FIT	27 FIT	93%	0%	4%

Table 4: Summary for SRD 991 / SRD 960 as shutdown device, threshold 2mA – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 years	T[Proof] = 10 years
1,2E-04	2,4E-04	5,9E-04	1,2E-03

Table 5: Summary for SRD 991 / SRD 960 as smart positioner, shutdown threshold: 3,8 mA – Type B device, IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
43 FIT	572 FIT	73 FIT	73 FIT	90%	7%	50%

Table 6: Summary for SRD 991 / SRD 960 as smart positioner, shutdown threshold: 3,8 mA – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 years	T[Proof] = 10 years
3,2E-04	6,4E-04	1,6E-03	3,2E-03

The boxes marked in yellow (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2,0E-03. The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2,0E-03.

FOXBORO ECKARDT GmbH
Pragstrasse 82
D-70376 Stuttgart
Germany
Tel. + 49(0)711 502-0
Fax + 49(0)711 502-597

ECKARDT S.A.S.
20 rue de la Marne
F-68360 Soultz
France
Tel. + 33 (0)3 89 62 15 30
Fax + 33 (0)3 89 62 14 85

http://www.foxboro-eckardt.com
http://www.foxboro-eckardt.de

http://www.eckardt.fr