

# SRI990 Analoger Stellungsregler

## Funktionale Sicherheit



Der Analoge Stellungsregler SRI990 dient 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 61511-1 durch *exida.com*®
- Einsetzbar bis SIL 3
- Pneumatiktest-Funktion
- Explosionsschutz (je nach Version)
- Elektromagnetische Verträglichkeit nach EN 61326 und NAMUR-Empfehlung NE21

---

**INHALTSVERZEICHNIS**

<b>1 ANWENDUNGSBEREICH</b>	<b>3</b>
1.1 Allgemein	3
1.1.1 Stromabschaltung unter Schwelle 0,6mA	3
1.2 Voraussetzungen	4
<b>2 ALLGEMEIN</b>	<b>5</b>
2.1 Relevante Normen	5
2.2 Begriffe	5
2.3 Abkürzungen	6
2.4 Auslegungstabellen	7
2.4.1 Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung ( $PFD_{avg}$ )	7
2.4.2 Sicherheitsintegrität der Hardware	7
2.4.3 Sicherheitsbezogenes System	9
<b>3 VERHALTEN IM BETRIEB UND BEI STÖRUNG</b>	<b>10</b>
<b>4 WIEDERKEHRENDE PRÜFUNGEN DES STELLUNGSREGLERS</b>	<b>10</b>
4.1 Sicherheitsüberprüfung	10
4.2 Funktionsüberprüfung	10
4.3 Reparaturen	10
<b>5 SICHERHEITSTECHNISCHE KENNGRÖßEN</b>	<b>11</b>
5.1 Annahmen	11
5.2 Stromabschaltung unter Schwelle 0,6mA	11
<b>6 LITERATURVERZEICHNIS</b>	<b>12</b>
<b>7 KONFORMITÄTSERKLÄRUNG</b>	<b>13</b>
<b>8 MANAGEMENT SUMMARY</b>	<b>14</b>

# 1 ANWENDUNGSBEREICH

## 1.1 Allgemein

Der Anwendungsbereich erstreckt sich auf analoge Stellungsregler vom Typ SRI990 mit einfachwirkendem pneumatischen Ausgangsverstärker (Modelcode SRI990-BIxxx) 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 die Art „Stromabschaltung unter Schwelle 0,6mA“ geschehen.

Diese Einsatzart basiert auf einer hardwaremäßigen Abschaltung der pneumatischen Ausgangsstufe mit dem zuvor genannten Verhalten. Dadurch ist gewährleistet, dass die Abschaltung unabhängig von allen Einstellungen und Parameterkonfigurationen (z.B. Nullpunkt, Spanne, Verstärkung, Dämpfung, Invertierung, usw.) stattfinden kann. Somit sind alle Einstellungen und Parameterkonfigurationen für die sicherheitsgerichtete Funktion des Stellungsreglers nicht relevant.

### 1.1.1 Stromabschaltung unter Schwelle 0,6mA

Der Analoge Stellungsregler wird in diesem Fall derart betrieben, dass im Anforderungsfall zumindest die elektrische Hilfsenergie unter einen Schwellenwert von 0,6mA abgeschaltet wird. Für diesen Fall kommen die sicherheitstechnischen Kenndaten nach Kapitel 5.2 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, insbesondere 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 SRI990 wird nur in Anwendungen mit niedriger Anforderungsrate eingesetzt.
- 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 SRI990-BIxxx den Wert 6V 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/elektronischer/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.
Diagnosedeckungsgrad	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 unvermeidbaren 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.
Sicherheitstechnisches System (SIS)	Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktor(en).
Ungefährlicher Ausfall	Ausfall ohne das Potential, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu versetzen.

## 2.3 Abkürzungen

Abkürzung	Beschreibung (Englisch)	Beschreibung (Deutsch)
$\lambda$	Failure rate per hour	Ausfallrate pro Stunde
$\lambda_D$	Dangerous failure rate per hour	Rate gefährbringender Ausfälle je Stunde
$\lambda_{DD}$	Detected Dangerous failure rate per hour	Rate erkannter gefährbringender Ausfälle je Stunde
$\lambda_{DU}$	Undetected Dangerous failure rate per hour	Rate unerkannter gefährbringender Ausfälle je Stunde
$\lambda_S$	Safe failure rate per hour	Rate ungefährlicher Ausfälle je Stunde
$\lambda_{SD}$	Detected Safe failure rate per hour	Rate erkannter ungefährlicher Ausfälle je Stunde
$\lambda_{SU}$	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 ( $1 \times 10^{-9}$ per h)	Fehler pro Zeit ( $1 \times 10^{-9}$ 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 und 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%	<b>SIL 3</b>	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) <sup>1</sup>	2
< 60%	Nicht erlaubt	SIL 1	SIL 2
60% - < 90%	SIL 1	<b>SIL 2</b>	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

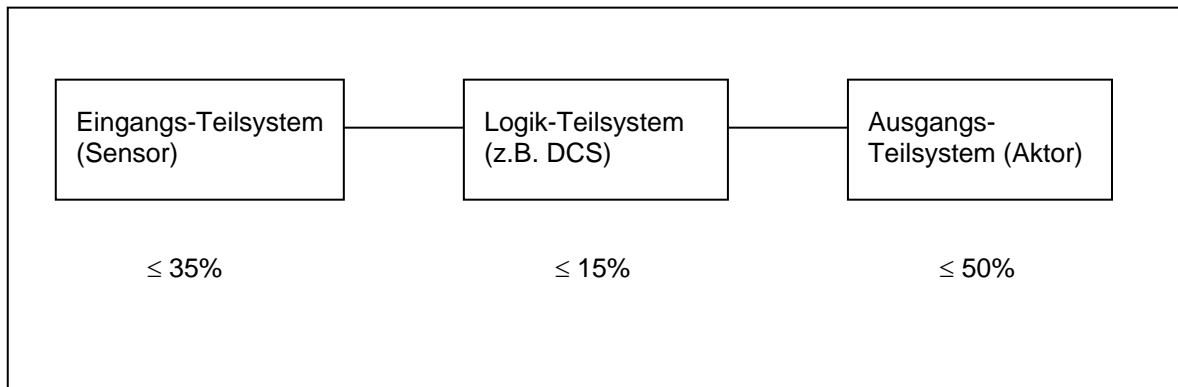
1) Nach [Ref. 2] Teil 1, Kapitel 11.4.4 dürfen bei Teilsystemen wie z.B. Sensoren und Aktoren die Fehlertoleranz der Hardware (HFT) um eins reduziert werden (Werte in Klammern), wenn das verwendete Gerät alle folgenden Bedingungen erfüllt:

- 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 den Stellungsregler SRI990 zu.

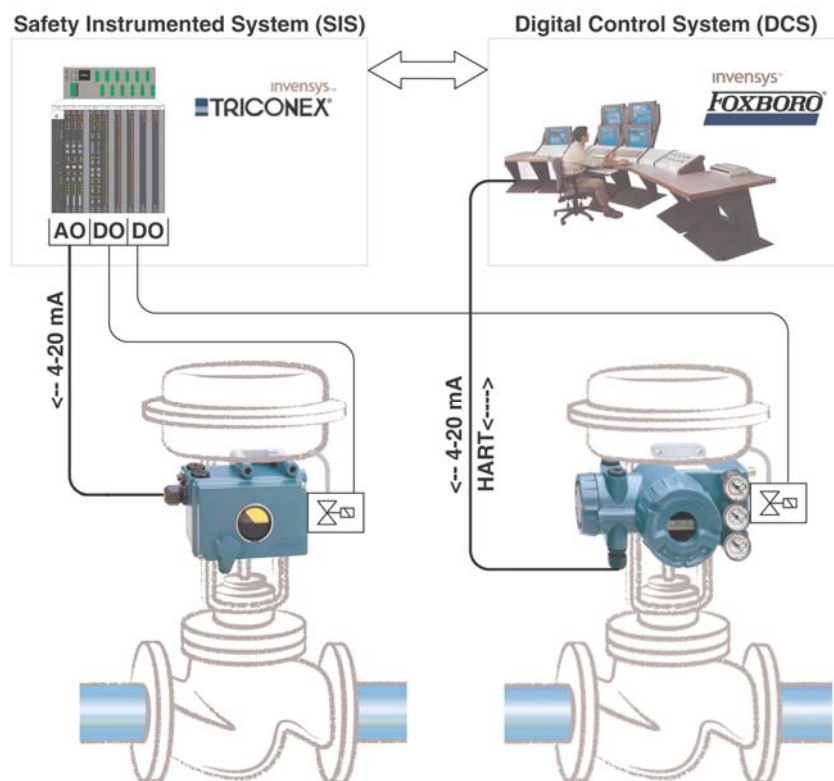
**2.4.3 Sicherheitsbezogenes System**

Ein sicherheitsbezogenes System besteht üblicherweise aus drei Teilsystemen: Eingangsteilsystem (Sensor), Logik-Teilsystem (SPS oder Leitsystem) und Ausgangsteilsystem (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 SRI990 mit HFT=1

- in ein sicherheitsgerichtetes System über AO-Module und zusätzlicher Ansteuerung des Magnetventils über DO-Module
- in eine Leitsystemumgebung mit Stromversorgung 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 EVE0107 A [Ref. 5] 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 des Zuluftfilters und ggfs. Tausch gemäß MI EVE0107 A Kap. 10.2 ([Ref. 5]).
- Als Sollwert 4mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination in die korrekte Endlage fährt, ggfs. Nullpunkt neu einstellen.
- Als Sollwert 20mA vorgeben und überprüfen, ob die Ventil-/Antriebskombination in die korrekte Endlage fährt, ggfs. Spanne neu einstellen.
- 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 SRI990-BDxxx den Wert 6V DC nicht überschreiten.

Der Stellungsregler selbst bedarf keiner turnusmäßigen Wartung. Bei Instandhaltung- oder Instandsetzungsarbeiten ist das Kapitel 11 der Inbetriebnahme- und Wartungsanleitung MI EVE0107 A ([Ref. 5]) zu beachten.

### 4.3 Reparaturen

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

## 5 SICHERHEITSTECHNISCHE KENNGRÖßEN

Bei den sicherheitstechnischen Kenngrößen wird die in Kapitel 1.1 erläuterte Einsatzart „Stromabschaltung“ zu Grunde gelegt. 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.
- Prüfintervall:  $\leq 1$  Jahr.
- Ein gefahrbringender Ausfall für die Einsatzart der Stromabschaltung ist definiert als ein Fehler, bei dem das Gerät auf die Anforderung des Abschaltens unter die jeweilige Schwelle nicht reagiert.
- 

### 5.2 Stromabschaltung unter Schwelle 0,6mA

Gerätetyp	Kategorie	HFT	SFF	PFD <sub>avg</sub>	$\lambda_{du}$	$\lambda_{dd}$	$\lambda_{su}$	$\lambda_{sd}$
A	SIL 3	0	94%	$8,8 \times 10^{-5}$	20 FIT	0 FIT	327 FIT	0 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] SRI990 Analoger Stellungsregler  
Typenblatt  
Foxboro Eckardt GmbH, PSS EVE0107 A
- [Ref. 5] SRI990 Analoger Stellungsregler  
Inbetriebnahme- und Wartungsanleitung  
Foxboro Eckardt GmbH, MI EVE0107 A
- [Ref. 6] Namur-Empfehlung NE 43  
NAMUR Geschäftsstelle, Leverkusen.
- [Ref. 7] Failure Modes, Effects and Diagnostics Analysis for Intelligent Positioner SRI990  
exida, Report No. Foxboro 05/03-29 R003.

## 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, 15.8.2005

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


### SRI990-BIxxx

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 to IEC 61511-1,  
if the safety instructions and the following parameters are observed:

Einsatzart	Stromabschaltung unter Schwelle 0,6mA Shutdown device, threshold 0,6mA
Usage	
SIL	3
Prüfintervall / Proof test interval	≤ 1 Jahr / year
Gerätetyp / Device Type	A
HFT	0 <sup>1)</sup> (einkanalige Verwendung / single channel usage)
SFF	94%
PFG <sub>avg</sub>	8,8x10 <sup>-5</sup>
λ <sub>du</sub>	20 FIT
λ <sub>rd</sub>	0 FIT
λ <sub>su</sub>	327 FIT
λ <sub>sd</sub>	0 FIT
DC <sub>s</sub>	0%
DC <sub>D</sub>	0%

<sup>1)</sup> gemäß Kapitel / according to chapter 11.4.4 of IEC 61511-1

  
Robert Leng  
General Manager  
Eckardt SAS

  
Giles 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:  
Positioner SRI 990

Customer:  
Foxboro Eckardt GmbH  
Stuttgart  
Germany

Contract No.: Foxboro 05/03-29  
Report No.: Foxboro 05/03-29 R003  
Version V0, Revision R2, August 2005  
Rainer Faller

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.  
© All rights on the format of this technical report reserved.



### Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the positioner SRI 990. The considered safety-related application of the positioner SRI 990 is as a shutdown device with fail-safe single-acting (spring return) actuation.

For functional safety applications, the positioner SRI 990 can be operated in 0..20 mA shutdown mode, shutdown threshold: 0,6 mA. In shutdown mode, an input current of less than the shutdown threshold (0,6mA) leads to a shutdown of the corresponding pressure output. In this mode, only the pneumatics of the positioner SRI 990 perform the shutdown action. 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 for mechanical / pneumatic components used in this analysis were obtained from experience-based *exida* data and field failure evaluations from Eckardt S.A.S. France. The pneumatics of the positioner SRI 990 are considered to be a Type A<sup>1</sup> subsystem with a hardware fault tolerance of HFT=0.

**Table 1: Summary for SRI 990 as shutdown device, threshold 0,6mA – Type A device, IEC 61508 failure rates**

$\lambda_{sd}$	$\lambda_{su}$	$\lambda_{dd}$	$\lambda_{du}$	SFF
0 FIT	327 FIT	0 FIT	20 FIT	94%

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

A user of the positioner SRI 990 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).

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.

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



Table 2: Summary for SRI 990 as shutdown device, threshold 0,6mA – PFD<sub>AVG</sub> 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<sub>AVG</sub> 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<sub>AVG</sub> 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.

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>