# SRI990 Analog Positioner

## Functional Safety

**S**afety **I**ntegrity **L**evel

## SIL certified

acc. to IEC 61508 / IEC 61511

The SRI990 Analog Positioner is designed to operate pneumatic valve actuators from control systems or electrical controllers that are consistent with the special safety requirements according to IEC 61508 / IEC 61511-1. The considered safety related application of the positioner for pneumatic actuators is as a shutdown device with fail-safe single-acting (spring return) actuation.

**Features**

- Assessment of functional safety according to IEC 61508 / IEC 61511-1 by *exida.com* ®
- Suitable for applications up to SIL 3
- Pneumatic test-Function
- Electrical classification (depending on version)
- Electro-magnetic compatibility according to EN 61326 and NAMUR-recommendation NE21

Foxboro.
by Schneider Electric

# Table of Contents

# 1 RANGE OF APPLICATION

## 1.1 General

The range of application applies to the SRI990 Analog Positioner with single-acting pneumatic amplifier (Modelcode SRI990-BIxxx) for operation of fail-safe single-acting (spring return) pneumatic actuators.

In the event of a loss of electrical- and/or pneumatic-supply the pneumatic output Y1 of the positioner will automatically be de-pressurized. In result the loss of output-pressure will automatically drive the actuator in the safe position, caused by the direction of the spring-force. If the positioner identifies any internal error, the output Y1 will also be de-pressurized and close the valve.

For functional safety applications the positioner can be operated in the shutdown mode below a threshold of 0,6 mA.

This application is based on the shutdown of the pneumatic amplifier unit by means of the positioner hardware with the before listed behavior. This ensures that the shutdown is achieved independent of any settings and/or configurations such as zero, span, amplification, damping or reverse action etc. Therefore all possible settings are irrelevant for a safe shutdown.

### 1.1.1 Shutdown mode with shutdown threshold below 0,6mA

The positioner in this case is operated in a way that at least the input current (power supply) is less than the shutdown threshold of 0,6mA. For this case the failure rates as listed in chapter 5.2 are applicable.

## 1.2 Requirements

For safety related applications according to the IEC 61508 / IEC 61511-1 the following requirements have to be observed:

- For applications of the positioner the technical data as specified in [Ref. 4], in specific regarding the application- and ambient-conditions, need to be observed.
- Only single-acting positioners are considered for these safety applications
- The actuator has to be designed that the valve is closed in the event of a depressurization, supported by the force of springs.
- The supplied instrument air has to be free of water, oil and dust according to ISO 8573-1, particle-size and –density based on class 2 and the oil-content based on class 3.
- Average ambient operating temperature over a longer period of time shall not exceed +40°C (+104°F)
- The SRI990 is only operated in applications where the demand rate is low.
- After mounting, connection and start-up the positioner has to undergo a functional test as described in [Ref. 5]:
  - Apply a setpoint of 4 mA and check if the actuator/valve drives into the designated position.
  - Apply a setpoint of 20 mA and check if the actuator/valve drives into the designated position.
  - Apply a setpoint of 12 mA and check if the actuator/valve drives into the designated position of 50% (if a linear valve characteristic is applied).
  - Check the voltage across the connection terminals at 20 mA. The measured voltage should not exceed 6V DC for the model SRI990-BIxxx.
- A functional test should be carried out periodically (see chapter 4.2).

# 2 GENERAL

## 2.1 Relevant Regulatory

- DIN EN 61508 part 1 to 7: Functional safety for safety related electric/electronical/programmable systems.
- DIN IEC 61511 part 1 to 3: Functional safety – Safety systems for the process industry

## 2.2 Definitions

The listed definitions are based on [Ref. 1], part 4 and [Ref. 2], part 1.

| Name | Description |
|---|---|
| Actuator | Part of the safety system that performs interactions with the process to achieve a safe condition. |
| Failure | Completion of the ability of a functional unit to perform a demanded function. |
| Diagnostic coverage factor | Relationship of the failure rate of the errors recognized by diagnostic tests to the failure rate of the component or subsystem. The degree of diagnostic does not contain errors determined at repeated inspections. |
| Fault | Abnormal condition, which can cause a reduction or a loss of the ability of a functional unit to perform a demanded function. |
| Functional safety | Part of the total safety, which refers to the process and the BPCS and the intended function of the SIS and other safety levels. |
| Functional unit | Unit from hardware or software or both, which are suitable for the execution of a fixed task. |
| Dangerous Failure | Loss with the potential to shift the safety-relevant system into a dangerous condition or a non functioning state. |
| Safety | Liberty of untenable risks |
| Safety function | Function, which is executed by a SIS, safety-related systems based on other technologies or from external installations and mechanisms for risk-reduction, with the goal of achieving or keeping up, under consideration of a fixed dangerous incident, a safe condition for the process. |
| Safety Integrity | Average probability that a safety-relevant system executes the demanded safety-relevant functions, in accordance with the required conditions within a fixed period of time. |
| Safety Integrity Level (SIL) | One out of four discrete levels to specify the requirements for the safety integrity of the safety functions, which are assigned to the safety-related system, whereby the safety integrity level 4 represents the highest degree of the safety integrity, the safety integrity level 1 the lowest. |
| Safety Instrumented System (SIS) | Safety-related system for the execution of one or several safety-ralated functions. A SIS consists of sensor(s), logic system and actuator(s). |
| Safe failure | failure without the potential to set the safety-related system into a dangerous or a nonfunctioning condition. |

## 2.3 Abbreviation

| Abbreviation | Description (English) | Description (German) |
|---|---|---|
| $\lambda$ | Failure rate per hour | Ausfallrate pro Stunde |
| $\lambda_D$ | Dangerous failure rate per hour | Rate gefahrbringender Ausfälle je Stunde |
| $\lambda_{DD}$ | Detected Dangerous failure rate per hour | Rate erkannter gefahrbringender Ausfälle je Stunde |
| $\lambda_{DU}$ | Undetected Dangerous failure rate per hour | Rate unerkannter gefahrbringender 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 Interpretation Tables

The following tables serve for the determination of the safety integrity level (SIL).

### 2.4.1 Average probability of failure on demand ($PFD_{avg}$)

This table shows the attainable safety integrity level (SIL) as a function of the average probability of a failure on demand. The here indicated failure-limit values are valid for a safety function that are operated in the mode with low requirement (see [Ref. 1] part 1, chapter 7.6.2.9).

| Safety Integrity Level (SIL) | $PFD_{avg}$ with low demand rate |
|---|---|
| 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 Safety Integrity of the hardware

Based on [Ref. 1] part 2, chapter 7.4.3.1.2 and 7.4.3.1.3. it has to be differentiated between systems of type A and systems of type B.

To Type A – systems applies:

- The failure behavior of all assigned components is sufficiently defined and
- the behavior of the subsystem under fault conditions can be completely determined and
- sufficient and reliable data for the failure reasons based on field-experience for the subsystem exist to show that the accepted failure rates for dangerous identified and dangerous unidentified failures are achieved.

To Type B – systems applies:

- The failure behavior of at least one assigned component is not sufficiently defined or
- the behavior of the subsystem under fault conditions cannot be completely determined or
- no sufficiently reliable data for the failure reasons based on field-experience for the subsystem are available, in order to support the failure rates for dangerous identified and dangerous unidentified failures.

These following tables indicate the attainable safety integrity level (SIL) as a function of the fraction of the safe failures (SFF) and the fault tolerance of the hardware (HFT) for safety-related subsystems of type A and type B (see [Ref. 1] part 2, chapter 7.4.3.1.4).

| **Fraction of safe failures (SFF)** | **Fault tolerance of hardware (HFT) for Type 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 |

| **Fraction of safe failures (SFF)** | **Fault tolerance of hardware (HFT) for Type B** | | |
|---|---|---|---|
| | **0** | **1 (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 |

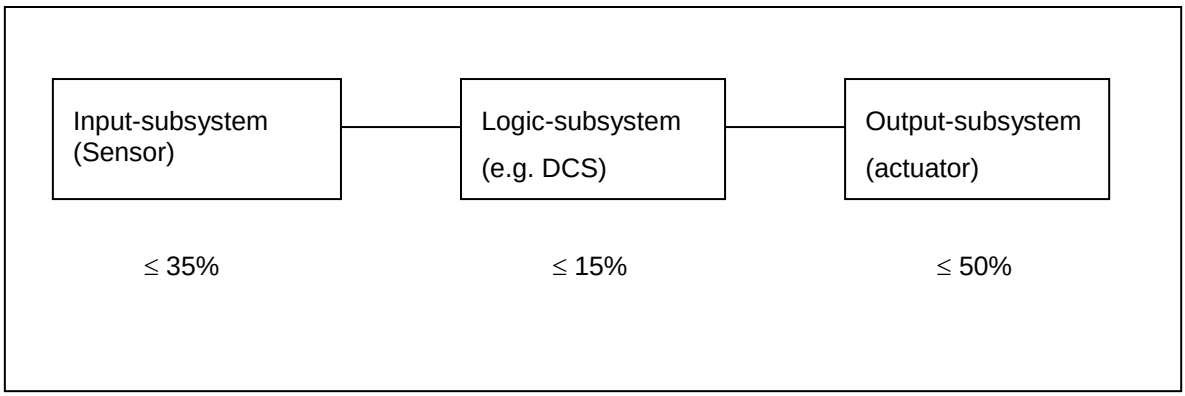
1) Based on [Ref. 2] part 1, chapters 11.4.4 it is possible for subsystems e.g. sensors and actuators to reduce the value for the hardware failure tolerance (HFT) by one (values in parentheses), if the used equipment fulfills all following conditions:

- The device is proven in operation
- The device only allows to change process-relevant parameters
- Changes of the process-relevant parameters is protected (e.g. password, Jumper, etc..)
- The function/application has a demanded safety integrity level of less than SIL 4.

These listed conditions apply to positioner SRI990.

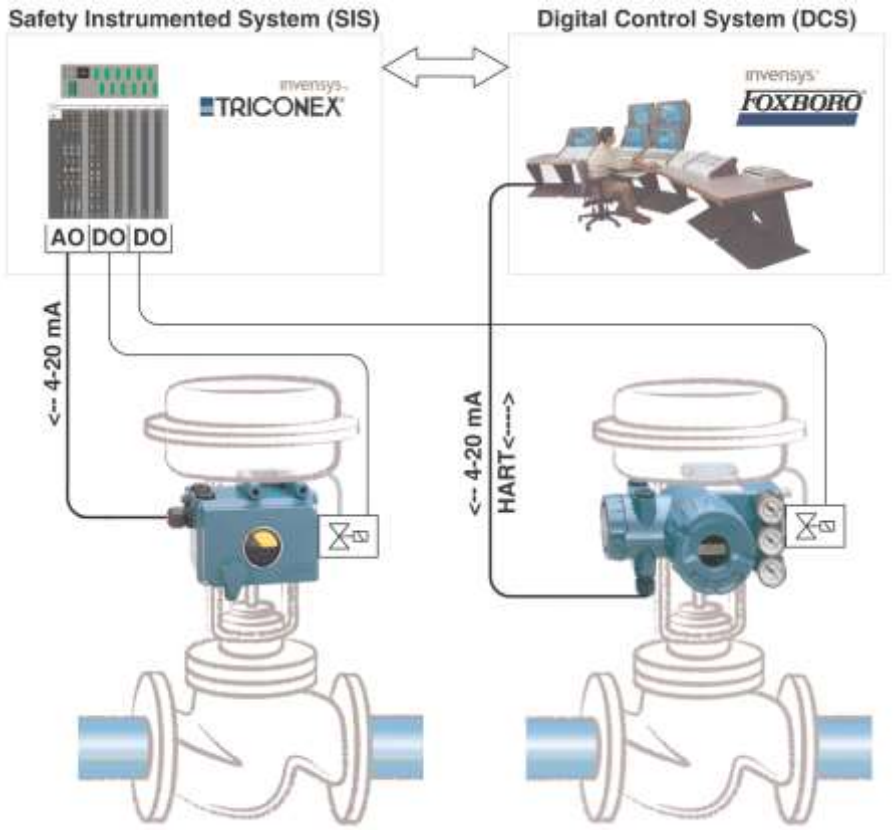
### 2.4.3 Safety-related System

Safety-related systems usually consist of three subsystems, the input subsystem (sensor), logic subsystem (SPS or control system) and output system (control valve consisting of positioner, actuator and valve). The average probability of a failure on demand is usually divided as follows:




Example of a connection of the positioner SRI990 with HFT=1

- into a safety-related system by means of AO-modules and additional control of a solenoid valve by means of a DO module
- into a control system by means of an analog control signal and additional control of a solenoid valve by means of a DO module



# 3 BEHAVIOR IN OPERATION AND FAULT STATE

The behavior during operation and fault state is described in the Master Instruction MI EVE0107 A [Ref. 5] for SRI990.

# 4 RECURRING EXAMINATIONS OF THE POSITIONER

## 4.1 Security Examination

In accordance with IEC 61508/61511 the safety function of the entire safety circuit is to be examined regularly. The therefore necessary test intervals are determined for the respective safety circuit.

## 4.2 Functional Examination

The functional examination / inspection has to be performed regularly once per year to ensure a normal operability of the positioner. Therefore the following functions need to be checked:

- Examine the supply air filter and if necessary exchange in accordance with MI EVE0107 A for SRI990 chapters 10.2 ([Ref. 5]).
- Apply an input signal value of 4 mA and examine whether the valve-/actuator-combination drives into the correct end position.
- Apply an input signal value of 20 mA and examine whether the valve-/actuator-combination drives into the correct end position.
- Apply an input signal value of 12 mA and examine whether the valve-/actuator-combination drives into the correct position (e.g. 50% with linear characteristic).
- Examine the voltage across the two connection terminals. The voltage at 20 mA input signal value should not exceed the value of 6 VDC for the device type SRI990-BIxxx.

The positioner does not require a regular maintenance. For maintenance or repairs refer to chapter 11 of the Master Instruction MI EVE0107 A ([Ref. 5]).

## 4.3 Repairs

Defective devices should be returned to the service & repair department of Foxboro Eckardt, under indication and description of the possible failure reason.

# 5 SAFETY RELEVANT CHARACTERISTICS

With respect to the safety-relevant characteristics as described in chapter 1.1 the application is based on the shutdown mode. Further information, beyond this summary, is contained in chapter 8.

## 5.1 Assumptions

The characteristics indicated in the following sub-chapters apply to the following assumption:

- The requirements from chapter 1.2 are fulfilled.
- The repair time (MTTR) after a device failure amounts to 8 hours.
- Testing-interval: ≤ 1 year.
- The diagnostic time of the internal tests amounts to testing-interval: ≤ 20 minutes.
- A dangerous failure for both ways of a shutdown is defined as a failure, in the case of which the device does not react to the requirement of a shutdown below the respective threshold.

## 5.2 Shutdown below threshold of 0,6mA

| Device-Type | Category | HFT | SFF | $PFD_{avg}$ | $\lambda_{du}$ | $\lambda_{dd}$ | $\lambda_{su}$ | $\lambda_{sd}$ |
|---|---|---|---|---|---|---|---|---|
| A | SIL 3 | 0 | 94% | $8{,}8x10^{-5}$ | 20 FIT | 0 FIT | 327 FIT | 0 FIT |

# 6 BIBLIOGRAPHY

[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 Analog Positioner
Product Specification Sheet
Foxboro Eckardt GmbH, PSS EVE0107 A

[Ref. 5] SRI990 Analog Positioner
Master Instruction
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 DECLARATION OF CONFORMITY

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

| Einsatzart<br>Usage | Stromabschaltung unter Schwelle 0,6mA<br>Shutdown device,<br>threshold 0,6mA |
|---|---|
| SIL | 3 |
| Prüfintervall / Proof test interval | ≤ 1 Jahr / year |
| Gerätetyp / Device Type | A |
| HFT | 0 [1] (einkanalige Verwendung / single channel usage) |
| SFF | 94% |
| $PFG_{avg}$ | $8,8x10^{-5}$ |
| $\lambda_{du}$ | 20 FIT |
| $\lambda_{dd}$ | 0 FIT |
| $\lambda_{su}$ | 327 FIT |
| $\lambda_{sd}$ | 0 FIT |
| $DC_S$ | 0% |
| $DC_D$ | 0% |

[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:
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

exida.com®
excellence in dependable automation

## 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[1] 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.

exida.com
excellence in dependable automation

**Table 2: Summary for SRI 990 as shutdown device, threshold 0,6mA – $PFD_{AVG}$ 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.



FOXBORO ECKARDT GmbH
Pragstrasse 82
D-70376 Stuttgart
Germany
Tel. + 49(0)711 502-0
Fax + 49(0)711 502-597
http://www.foxboro-eckardt.de

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