SIEMENS

SIPART

Electropneumatic positioner
Functional safety for SIPART PS2

Product Information

Supplement to the manuals 6DR501*, 6DR511*, 6DR521*, 6DR531*

09/2006
A5E00442122-03

Safety Guidelines

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

Danger

indicates that death or severe personal injury **will** result if proper precautions are not taken.

Warning

indicates that death or severe personal injury **may** result if proper precautions are not taken.

Caution

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

Caution

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

Notice

indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

Warning

This device may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Automation and Drives
Postfach 48 48
90437 NÜRNBERG
GERMANY

Order No.: A5E00442122-03
Edition 10/2006

Table of contents

Introduction 1

1.1 Purpose of this document

This document contains information and safety instructions that you will require when using the electropneumatic positioner in safety-instrumented systems.

It is aimed at system planners, constructors, service and maintenance engineers and personnel who will commission the device.

1.2 Scope of this document

Documentation

This document deals with the SIPART PS2 positioner exclusively as part of a safety function.

The documentation at hand applies only in combination with the following documentation and is valid for positioners with firmware versions C4, C5, or 4.00.00 and higher:

No.	Name	Order no.
/1/	SIPART PS2 Manual	A5E00074631
/2/	SIPART PS2 Operating Instructions	A5E00074600

1.3 Document history

The following table shows the most important changes in the documentation compared to each previous edition:

Edition	Comment
06/2005	First edition
07/2005	What has changed? Safety parameters
09/2006	Provision for the latest FW version 4.00.00 Chapters 3.2 and 3.6: notes on the partial stroke test supplemented Appendix A2: declaration of conformity updated.

1.4 Further information

Information

The contents of these instructions shall not become part of or modify any prior or existing agreement, commitment or legal relationship. All obligations on the part of Siemens AG are contained in the respective sales contract, which also contains the complete and solely applicable warranty conditions. Any statements contained herein do not create new warranties or modify the existing warranty.

The content reflects the technical status at the time of printing. We reserve the right to make technical changes in the course of further development.

Siemens Regional Offices

If you need more information or have particular problems which are not covered sufficiently by the operating instructions, contact your local Siemens Regional Office. You will find the address of your local Siemens Regional Office on the Internet.

Product information on the Internet

The Programming Manual forms a part of the supplied CD and is also available on the Siemens homepage on the Internet. On the enclosed CD, you will find an extract of the catalog FI 01 "Field devices for process automation" with the current ordering data. The complete catalog FI 01 is available on the Internet.

See also

Siemens regional offices (https://www.siemens.com/processinstrumentation/contacts)

Product information on the Internet (http://www.siemens.com/sipartps2)

Instructions and manuals (http://www.siemens.com/processinstrumentation/documentation)

Catalog FI 01 (https://www.siemens.com/fi01)

General safety instructions 2

2.1 Safety-instrumented system

Definition: Safety-instrumented system

A safety-instrumented system executes the safety functions that are required to achieve or maintain a safe status in a system. It consists of a sensor, logic unit/control system and final controlling element.

Example:

A safety-instrumented system is made up of a pressure transmitter, a limit signal sensor and a control valve.

Definition: Safety function

Defined function executed by a safety-instrumented system with the objective of achieving or maintaining a safe system status taking into account a defined dangerous occurrence.

Example:

Limit pressure monitoring

Definition: Dangerous failure

Failure with the potential to bring the safety-instrumented system into a dangerous or non-functional status.

Description

The sensor, logic unit/control system and final controlling element combine to form a safety-instrumented system, which executes a safety function.

Note

This document deals with the SIPART PS2 positioner exclusively as part of a safety function.

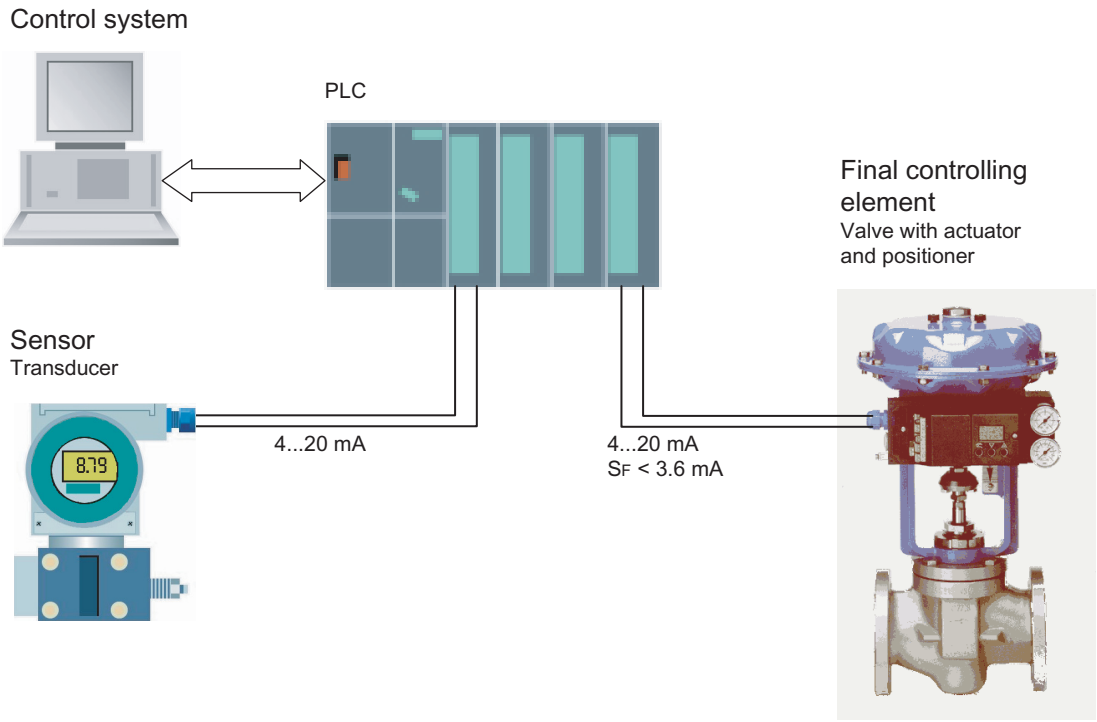

Figure 2-1 Example of a safety-instrumented system

S_F Failure signal

Function

The transmitter generates a process-specific analog signal. The downstream control system monitors this signal to ensure it does not exceed a set limit value. In case of a fault, the control system generates a fault signal of < 3.6 mA for the connected positioner, which switches the associated valve to the specified safety position - this is known as tight closing.

2.2 Safety Integrity Level (SIL)

Definition: SIL

The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL) from SIL 1 to SIL 4. Each level corresponds to the probability range for the failure of a safety function. The higher the SIL of the safety-instrumented system, the higher probability that the required safety function will work.

The achievable SIL is determined by the following safety characteristics:

- Average probability of dangerous failure of a safety function in case of demand (PFD_{AVG})
- Hardware fault tolerance (HFT)
- Safe failure fractions (SFF)

Description

The following table shows the dependency of the SIL on the "average probability of dangerous failures of a safety function of the entire safety-instrumented system" (PFD_{AVG}) The table deals with "Low demand mode", i.e. the safety function is required a maximum of once per year on average.

Table 2-1 Safety Integrity Level

SIL	**PFD_{AVG}**
4	≥ 10^{-5}...< 10^{-4}
3	≥ 10^{-4}...< 10^{-3}
2	≥ 10^{-3}...< 10^{-2}
1	≥ 10^{-2}...< 10^{-1}

The "average probability of dangerous failures of the entire safety-instrumented system" (PFD_{AVG}) is normally split between the three sub-systems in the following figure.

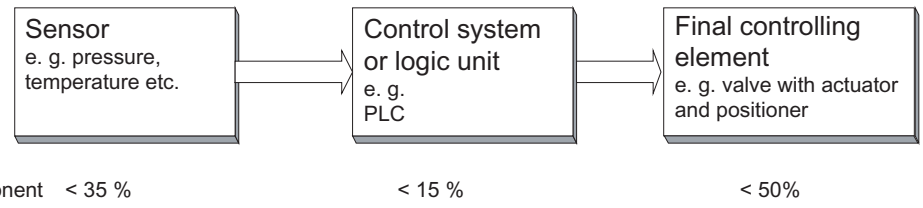

Figure 2-2 PFD distribution

The following table shows the achievable Safety Integrity Level (SIL) for the entire safety-instrumented system for type B subsystems depending on the safe failure fraction (SFF) and the hardware fault tolerance (HFT). Type B subsystems include analog transmitters and shut-off valves without complex components, e.g. microprocessors (also see IEC 61508, Section 2).

SFF	**HFT**		
	0	**1 (0) [1)]**	**2 (1) [1)]**
< 60%	Not permitted	SIL 1	SIL 2
60 to 90%	SIL 1	SIL 2	SIL 3
90 to 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

[1)] As per IEC 61511-1, Section 11.4.4

According to IEC 61511-1, Section 11.4.4, the hardware fault tolerance (HFT) can be reduced by one (values in brackets) for sensors and final controlling elements with complex components if the following conditions are applicable for the device:

- The device is proven-in-use.
- The user can configure only the process-related parameters, e.g. control range, signal direction in case of a fault, limiting values, etc.
- The configuration level of the firmware is blocked against unauthorized operation.
- The function requires SIL of less than 4.

The SIPART PS2 positioner fulfills these conditions.

See also

Safety characteristics (Page 3-5)

Device-specific safety instructions

3

3.1 Applications

The SIPART PS2 positioner is also suitable for control valves that satisfy the special requirements in terms of function safety to SIL 2 in accordance with IEC 61508 or IEC 61511-1. The 6DR501*, 6DR511*, 6DR521* and 6DR531* variations are available for this purpose.

These are single-acting, depressurizing positioners with an input from 4 to 20 mA for installation on pneumatic actuators with spring return.

The positioner automatically depressurizes the valve actuator on demand or in case of faults, which thus switches the valve to the specified safety position.

These positioners meet the following requirements:

- Functional safety to SIL 2 under IEC 61508 or IEC 61511-1, from firmware version C4
- Explosion protection on 6DR5***-*E*** variations
- Electromagnetic compatibility in accordance with EN 61326/A1, Appendix A.1

3.2 Safety function

Safety function on positioner

The safety function on the SIPART PS2 positioner is the depressurizing of the connected valve actuator. The built-in spring brings the valve to the required safety position. Depending on the direction of action of this spring, the valve is completely opened or closed.

This function is referred to as "tight closing" in the device documentation.

This safety function can be triggered by:

- Failure of auxiliary electrical power
- Failure of auxiliary pneumatic power

- Falling below failure signal 3.6 mA at set current input (I_w)

Note

Partial stroke test

If a partial stroke test is running, the safety function is only triggered if the electrical and pneumatic power supply is switched off. The safety function is not triggered by an input current less than 3.6 mA.

If the valve actuator cannot be depressurized on demand or in case of a fault, this represents a dangerous failure.

Warning

The binding settings and conditions are listed in the "Settings" and "Safety characteristics" sections.

These conditions must be met in order to fulfil the safety function.

When the safety function has been executed, safety-instrumented systems with no self-locking function should be brought to a monitored or otherwise safe status within the Mean Time To Repair (MTTR). The MTTR is 8 hours.

The calculated Mean Time Between Failures (MTBF) for the SIPART PS2 positioner is 90 years. The MTBF for the basic electronics module is 181 years in line with SN29500.

The characteristic service life of the valve block depends on the load. On average it is approx. 200 million switching operations for each of the two pilot valves with symmetrical load. The actual number of switching operations performed can be called in the local display or via HART communication.

Reference

Device manual /1/ Section 4.5 "Diagnostics", Diagnostic values 31=VENT1 and 32=VENT2

See also

Settings (Page 3-3)

Safety characteristics (Page 3-5)

3.3 Settings

After assembly and commissioning in line with the device manual, the following parameter settings should be made for the safety function:

Safety parameters

Parameter name	Function	Set parameter value	Meaning
2.YAGL	Rated angle of rotation of the feedback shaft	33° or 90° to match the setting for the transmission ratio selector	Adaptation to the mechanically set range of stroke / rotation angle
6.SCUR	Current range of setpoint	4 MA	4...20 mA
7.SDIR	Setpoint direction	riSE	Rising - for actuators with safety position down/closed (valve closed)
		FALL	Falling - for actuators with safety position up/open (valve open)
12.SFCT	Setpoint function	Everything except "FrEE"	• linear • constant percentage • inverse constant percentage
39.YCLS	Tight closing with manipulated variable	do	Depressurizing - for actuators with safety position down/closed (valve closed)
		uP	Depressurizing - for actuators with safety position up/open (valve open)

Reference

Device manual /1/ chapter 2 "Design and method of operation"
chapter 2.2 "Transmission ratio selector", figure 2-1
chapter 2.2.3 "Allocation of the actuator directions", figure 2-5

Device manual /1/ chapter 3 "Preparing for operation"

Device manual /1/ chapter 4 "Operation"

Protection against configuration changes

After configuration, the SIPART PS2 positioner must be switched to automatic operation. You should then fit the housing cover so that the device is protected against unwanted and unauthorized changes/operation.

The SIPART PS2 positioner is fitted with an additional protective function to prevent configuration changes:

1. Configure the parameter 43.BIN1 = bLoc2.
2. Bridge terminals 9 and 10 of the binary input BE1.

   In this condition, the "configuration" operating level using the keys and HART communication and manual operation are blocked.

Checking the safety function

To check that the safety configuration is correct, apply a set current of 3.6 mA.

In this condition, the valve actuator must bring the valve to the intended safety position.

3.4 Behavior in case of faults

Fault

The procedure in case of faults is described in the device Operating Instructions.

Reference

Operating Instructions /2/ Section 7.4 "Fault elimination"

Repairs

Defective devices should be sent in to the repair department with details of the fault and the cause. When ordering replacement devices, please specify the serial number of the original device. The serial number can be found on the rating plate.

The address of the responsible repair center, contacts, spare parts lists etc. can be found on the Internet at:

Reference

www.siemens.com/automation/services&support

www.automation.siemens.com/partner

3.5 Maintenance/Checking

Checking the function

We recommend that the functioning of the positioner is checked at regular intervals of one year.

Check at least the following:

1. Connect the set value of 4 mA.
   - Check whether the valve moves to the appropriate end position.
   - Check the locally displayed internal, digitized values for the setpoint and position.
2. Connect the set value of 20 mA.
   - Check whether the valve moves to the appropriate end position.
   - Check the locally displayed internal, digitized values for the setpoint and position.

Checking safety

You should regularly check the safety function of the entire safety circuit in line with IEC 61508/61511. The testing intervals are determined during the calculation for each individual safety circuit in a system (PFD_{AVG}).

On the SIPART PS2 positioner the following specific checks should be carried out:

1. Connect the set value of 3.6 mA.
   - Check whether the valve moves to the safety position.
2. Connect the set value of 20 mA.
   - Reduce the inlet pressure (P_z) to a third of the maximum supply pressure
   - Check whether the valve moves to the safety position.
3. Check the filters in the pneumatic connections for contamination and clean them if necessary.

3.6 Safety characteristics

The safety characteristics necessary for use of the system are listed in the SIL declaration of conformity (see "Appendix"). These values apply under the following conditions:

- The positioner is only used in applications with a low demand rate for the safety function (low demand mode).
- Communication with the HART protocol is only used for
  - Device configuration
  - Reading diagnostic values
  - However, it is not used for operations critical to safety. In particular, the trace function must not be activated in safety related operation.

- The safety-related parameters/settings (see "Settings" section) have been entered by local operation or HART communication and checked on the local display before commencing safety-instrumented operation.
- The positioner is blocked against unwanted and unauthorized changes/operation.
- The 4 to 20 mA input signal for the SIPART PS2 positioner is generated by a safe system that fulfills a minimum of SIL 2.
- The connected valve actuator must be single acting and switch the valve to its safe end position by spring force in the following cases:
  - Pressure failure
  - At a chamber pressure (Y1 connection) up to a third of the maximum available inlet pressure (Pz connection)
- The air outlet does not contain any additional cross-sectional contractions leading to an increased dynamic pressure. In particular, a silencer is only allowed if icing or other contamination is ruled out.
- The restrictor in the Y1 circuit may not be completely closed during operation.
- The auxiliary pneumatic power is free of oil, water and dirt in line with:

  DIN/ISO 8573-1, maximum class 2
- The average temperature viewed over a long period is 40°C.
- The MTTR after a device fault is 8 hours.
- In case of a fault, the pneumatic outlet of the positioner is depressurized. A spring in the pneumatic actuator must move the valve to the pre-defined, safe end position.
- A dangerous failure of the positioner is a failure where the pressure outlet is not depressurized, or the safety position is not reached, when the input current < 3.6 mA.
- If a partial stroke test is running, the safety function is only triggered when the electrical and pneumatic power supply is switched off. The safety function is not triggered by an input current less than 3.6 mA. The partial stroke test is available as of firmware version 4.00.00.

See also

Settings (Page 3-3)

SIL Declaration of Conformity (Page A-2)

Test report (extract) (Page A-3)

Appendix

A

A.1 Literature and standards

No.	Standard	Description
/1/	IEC 61508 Section 1-7	Functional safety of following systems: • Safety-instrumented • Electrical • Electronic • Programmable Target group: Manufacturers and suppliers of equipment
/2/	IEC 61511 Section 1-3	Functional safety - Safety systems for the process industry Target group: Planners, constructors and users

A.2 SIL Declaration of Conformity

SIEMENS **SIL Declaration of Conformity**

Functional Safety According to IEC 61508 und IEC 61511

Siemens AG
Automation & Drives
Process Instrumentation and Analytics
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Product:	**Electropneumatic Positioner SIPART PS2** 4-20mA, single acting
Ordering Nr.:	6DR501*, 6DR511*, 6DR521*, 6DR531*
Firmware:	Versions C4, C5, 4.00.00 and higher

We as manufacturer declare that the above Positioner SIPART PS2 is suitable for use in a safety instrumented system according to IEC61508 / 61511. Depressurizing the output ("shut-down") is the usable safety function. The appropriate SIL Safety Manual must be observed.

The proven-in-use was verified according to IEC61508 / 61511 and evaluated by exida.com.
Revisions will be carried out according to IEC61508.
The failure rates were calculated via an FMEDA (Failure Modes, Effects and Diagnostic Analysis) according to IEC 61508. The calculation was carried out by exida.com.

Safety Related Characteristics:

Device Type		**B**
SIL	Safety Integrity Level (single mode)	**2**
HFT[1]	Hardware Failure Tolerance	**0**
PFD_{AVG}	Average Probability of Failure on Demand	**$7{,}94*10^{-4}$**
λ_{sd}	Safe detected Failure Rate	**0 FIT**
λ_{su}	Safe undetected Failure Rate	**1013 FIT**
λ_{dd}	Dangerous detected Failure Rate	**4 FIT**
λ_{du}	Dangerous undetected Failure Rate	**182 FIT**
SFF	Safe Failure Fraction	**84,8%**

These characteristics are valid for low demand operation mode within an 1oo1 architecture.
(Guidance to calculation according to IEC 61508-6, annex B).
The PFD_{AVG} value is valid under the assumption of mean time to repair MTTR = 8h and proof test interval T1 = 8760h

Karlsruhe, 30.06.2006

Siemens AG

i.V. _____ i.V. _____

Dr. Schmidt, General Manager Instrumentation — Schradi, Segment Manager Positioner

1) HFT is reduced by one in accordance with IEC 61511-1, Paragraph 11.4.4.

No. A5E00481296A - 02

A.3 Test report (extract)

FMEDA and Proven-in-use Assessment

Project:
Electro-pneumatic Positioner SIPART PS2 –
single acting shut-down module

Customer:
SIEMENS AG, A&D PI TQ2
Karlsruhe
Germany

Contract No.: SIEMENS 04/12-06
Report No.: SIEMENS 04/12-06 R004
Version V1, Revision R1.0, April 2005
Stephan Aschenbrenner

exida.com®
excellence in dependable automation

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Electro-pneumatic Positioner SIPART PS2 with software version C4 and C5. Table 1 gives an overview of the different configurations that belong to the considered Electro-pneumatic Positioner SIPART PS2.

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.

Table 1: Configuration overview

[Conf 1]	6DR501*_*E***_****	2-wire Ex (L250) without HART; single-acting
[Conf 2]	6DR501*_*N***_****	2-wire standard (L350) without HART; single-acting
	6DR511*_*****_****	2-wire standard (L300) with HART; single-acting
[Conf 3]	6DR521*_*****_****	2-, 3-, 4-wire Ex (L200) with HART; single-acting
[Conf 4]	6DR531*_*****_****	2-, 3-, 4-wire standard (L220) without HART; single-acting

For safety applications only the 4..20 mA control input with the corresponding pressure output was considered to work as a single-acting shut-down module ("tight closing bottom"). All other possible input and output variants or electronics are not covered by this report.

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500.

SIEMENS AG, A&D PI TQ2 and exida.com together did a quantitative analysis of the mechanical parts of the Electro-pneumatic Positioner SIPART PS2 to calculate the mechanical failure rates using different failure rate databases ([N6], [N7], [N8] and exida's experienced-based data compilation) for the different mechanical components (see [D32] and [R6]). The results of the quantitative analysis are included in the calculations described in sections 5.2 to 5.5.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 50% of the total SIF PFD_{AVG} value is caused by the final element. However, as the Electro-pneumatic Positioner SIPART PS2 is only one part of the final element it should not claim more than 20% of the range. For a SIL 2 application the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the positioner would then be 2,00E-03.

The Electro-pneumatic Positioner SIPART PS2 is considered to be a Type B[1] component with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

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

As the Electro-pneumatic Positioner SIPART PS2 is supposed to be a proven-in-use device, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. The proven-in-use investigation was based on field return data collected and analyzed by SIEMENS AG, A&D PI TQ2. This data cannot cover the process connection. The proven-in-use justification for the process connection still needs to be done by the end-user.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.1 the Type B Electro-pneumatic Positioner SIPART PS2 with a hardware fault tolerance of 0 and a SFF of 60% to < 90% are considered to be suitable for use in SIL 2 safety functions The decision on the usage of proven-in-use devices, however, is always with the end-user.

The following tables show how the above stated requirements are fulfilled for the worst case configuration listed in Table 1.

Table 2: Summary for SIPART PS2 as single-acting shutdow n module – Failure rates

Failure categor y	Failure rates (in FIT)
Fail Safe Detected	0
Fail Safe Undetected	919
Fail Dangerous Detected	4
Fail Dangerous Undetected	182
No Effect	93
Annunciation Undetected	1
Not part	76
MTBF = MTTF + MTTR	90 years

Table 3: Summary for SIPART PS2 as single-acting shutdow n module – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0 FIT	1013 FIT	4 FIT	182 FIT	84%	0%	2%

Table 4: Summary for SIPART PS2 as single-acting shutdow n module – PF D_{AVG} values

T[Proof] = 1 y ear	T[Proof] = 5 y ears	T[Proof] = 10 y ears
PF D_{AVG} = 7,94E-0 4	PF D_{AVG} = 3,96E-0 3	PF D_{AVG} = 7,91E-0 3

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 2,00E-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 2,00E-03.

The assessment has shown that the Electro-pneumatic Positioner SIPART PS2 when used as a single-acting shut-down module ("tight closing bottom") has a PF D_{AVG} 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 a Safe Failure Fraction (SFF) of more than 84%. Based on the verification of "proven-in-use" according to IEC 61508 and its direct relationship to "prior-use" of IEC 61511-1 it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

The failure rates listed above do not include failures resulting from incorrect use of the Electro-pneumatic Positioner SIPART PS2, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class Dx (outdoor location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the Electro-pneumatic Positioner SIPART PS2 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). A full table of failure rates for different operating conditions is presented in section 5.2 to 5.5 along with all assumptions.

It is important to realize that the "no effect" failures and the "annunciation" failures are included in the "safe undetected" failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

List of Abbreviations/Acronyms

B

B.1 Abbreviations

Abbreviation	Full term in English	Meaning	
HFT	Hardware Fault Tolerance	Hardware fault tolerance: Capability of a function unit to continue executing a required function in the presence of faults or deviations.	
MTBF	Mean Time Between Failures	Average period between two failures	
MTTR	Mean Time To Repair	Average period between the occurrence of a fault in a device or system and the repair	
PFD	Probability of Failure on Demand	Probability of dangerous failures of a safety function on demand	
PFD_{AVG}	Average Probability of Failure on Demand	Average probability of dangerous failures of a safety function on demand	
SFF	Safe Failure Fraction	Proportion of safe failures: Proportion of failures without the potential to bring the safety-instrumented system into a dangerous or non-permissible functional status.	
SIL	Safety Integrity Level	The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for failure of a safety function. The higher the Safety Integrity Level of the safety-instrumented system, the lower the probability that it will not execute the required safety functions.	
SIS	Safety Instrumented System	A safety-instrumented system (SIS) executes the safety functions that are required to achieve or maintain a safe status in a system. It consists of a sensor, logic unit/control system and final controlling element.	
FIT	Failure in Time	Frequency of failure Number of faults withing 10^9 hours	
TI	Test Interval	Testing interval of the protective function	
XooY	"X out of Y" voting	Classification and description of the safety-instrumented system in terms of redundancy and the selection procedures used.	
		"Y"	Specifies how often the safety function is executed (redundancy).
		"X"	Determines how many channels have to work correctly.
		Example: Pressure measurement: 1oo2 architecture. A safety-instrumented system decides that a specified pressure limit has been exceeded if one out of two pressure sensors reaches this limit. In a 1oo1 architecture, there is only one pressure sensor.	

Glossary

Dangerous failure

Failure with the potential to bring the safety-instrumented system into a dangerous or non-functional status.

Safety function

Defined function executed by a safety-instrumented system with the objective of achieving or maintaining a safe system status taking into account a defined dangerous occurrence.

Example:

Limit pressure monitoring

Safety Integrity Level

→ *SIL*

Safety-instrumented system

A safety-instrumented system executes the safety functions that are required to achieve or maintain a safe status in a system. It consists of a sensor, logic unit/control system and final controlling element.

Example:

A safety-instrumented system is made up of a pressure transmitter, a limit signal sensor and a control valve.

SIL

The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL) from SIL 1 to SIL 4. Each level corresponds to the probability range for the failure of a safety function. The higher the SIL of the safety-instrumented system, the higher probability that the required safety function will work.

The achievable SIL is determined by the following safety characteristics:

- Average probability of dangerous failure of a safety function in case of demand (PFD_{AVG})
- Hardware fault tolerance (HFT)
- Safe failure fractions (SFF)

Index