Electropneumatic positioner

SIPART PS2 PA and
SIPART PS2 FF
SIL Safety Manual (PA/FF)

Supplement to manual

6DR551x
6DR561x
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.
Table of contents

1 Introduction ........................................................................................................................................ 1-1
  1.1 Purpose of this document ............................................................................................................ 1-1
  1.2 Scope of this document ............................................................................................................... 1-1
  1.3 Document history ...................................................................................................................... 1-1
  1.4 Further information .................................................................................................................... 1-2

2 General safety instructions ............................................................................................................. 2-1
  2.1 Safety-instrumented system ........................................................................................................ 2-1
  2.2 Safety Integrity Level (SIL) ......................................................................................................... 2-2

3 Device-specific safety instructions ............................................................................................... 3-1
  3.1 Applications ................................................................................................................................ 3-1
  3.2 Safety function .......................................................................................................................... 3-2
  3.3 Settings ...................................................................................................................................... 3-2
  3.4 Behavior in case of faults ............................................................................................................ 3-3
  3.5 Maintenance/Checking ............................................................................................................... 3-4
  3.6 Safety characteristics ................................................................................................................. 3-5

A Appendix ........................................................................................................................................ A-1
  A.1 SIL Declaration of Conformity ..................................................................................................... A-2
  A.2 Test report (extract) .................................................................................................................... A-3
  A.3 Literature and standards ............................................................................................................ A-7

B List of Abbreviations/Acronyms ..................................................................................................... B-1
  B.1 Abbreviations ............................................................................................................................ B-1

Glossary ............................................................................................................................................ Glossary-1

Index .................................................................................................................................................. Index-1

Tables

Table 2-1 Safety Integrity Level ........................................................................................................ 2-3
Introduction

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

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

This document only applies in conjunction with the following documentation.

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Order no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>/1/</td>
<td>SIPART PS2 PA Manual 6DR55xx</td>
<td>A5E00127926</td>
</tr>
<tr>
<td>/2/</td>
<td>SIPART PS2 FF Manual 6DR56xx</td>
<td>A5E00214569</td>
</tr>
</tbody>
</table>

1.3 Document history

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

<table>
<thead>
<tr>
<th>Edition</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 09/2005</td>
<td>First edition</td>
</tr>
</tbody>
</table>
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.

The document's location in the information landscape

These instructions are on the supplied CD "sipart ps2 POSITIONERS" (order number A5E00214567). You will find more detailed information on the supplied CD and in the Internet at:

www.siemens.com/sipartps2

Click on "More Info" and "-> Operating Instructions and manuals".

On the enclosed CD, you will find an extract of the catalog FI 01 "Field devices for process automation" with the current order data. The entire FI 01 catalog is also available at the above Web address.

References

If there are references to further information on an aspect described here, these will always be found at the end of a chapter under "See also"
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
A 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.
2.2 Safety Integrity Level (SIL)

Function

The transmitter generates a process-specific measured value. The programmable controls (SPS) monitors this value in case it exceeds a preset limit value. If a fault occurs, the SPS generates a shut-off signal for the connected positioner. The positioner switches the corresponding valve to the specified safety position. The communication with the positioner via PROFIBUS PA or FOUNDATION field bus remains unrestricted, i.e. position and status signals are still possible.

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\textsubscript{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\textsubscript{AVG})
The table deals with "Low demand mode", i.e. the safety function is required a maximum of once per year on average.

<table>
<thead>
<tr>
<th>SIL</th>
<th>PFD\textsubscript{AVG}</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥ 10^{-5}...&lt; 10^{-4}</td>
</tr>
<tr>
<td>3</td>
<td>≥ 10^{-4}...&lt; 10^{-3}</td>
</tr>
<tr>
<td>2</td>
<td>≥ 10^{-3}...&lt; 10^{-2}</td>
</tr>
<tr>
<td>1</td>
<td>≥ 10^{-2}...&lt; 10^{-1}</td>
</tr>
</tbody>
</table>

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

![Figure 2-2 PFD distribution](image)

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

<table>
<thead>
<tr>
<th>SFF</th>
<th>HFT (for type A sub-systems)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt; 60%</td>
<td>SIL 1</td>
</tr>
<tr>
<td>60 to 90%</td>
<td>SIL 2</td>
</tr>
<tr>
<td>90 to 99%</td>
<td>SIL 3</td>
</tr>
<tr>
<td>&gt; 99%</td>
<td>SIL 3</td>
</tr>
</tbody>
</table>
General safety instructions

2.2 Safety Integrity Level (SIL)

See also

Safety characteristics (Page 3-5)
Device-specific safety instructions

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 device versions SIPART PS2 PA (6DR551*) and SIPART PS2 FF (6DR561*) are available for applications with PROFIBUS PA and for the FOUNDATION field bus respectively.

These are single-acting, depressurizing positioners for installation on pneumatic actuators with spring return.

The positioner depressurizes the valve actuator when faults occur or on demand by means of the separate input for the safety shutdown. The valve actuator thus switches the valve to the specified safety position. Except for the valve control, all other device functions including position and status signals and the communication via PROFIBUS PA or FOUNDATION field bus remain unrestricted.

These positioners meet the following requirements:

- Functional safety to SIL 2 in accordance with IEC 61508 and IEC 61511-1 regarding the safety shutdown
- 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 depressurizing of the connected valve actuator is the safety function on the SIPART PS2 PA and SIPART PS2 FF positioner. The built-in spring brings the valve into the required safety position - this is known as tight closing. Depending on the direction of action of this spring, the valve is completely opened or closed.

The safety function is triggered if the following occurs:

- The signal at the input for the safety shutdown (terminals 81 and 82) is less than 4.5 V. This function is likewise referred to as "safety shutdown" in the device documentation.
- The auxiliary electrical power from the PROFIBUS PA or the FOUNDATION field bus connection fails.
- Failure of auxiliary pneumatic power
Device-specific safety instructions

3.3 Settings

The safety function is not effected by other device functions, particularly the microcontroller, software and communication interface. Therefore, with regard to this safety function, both SIPART PS2 PA and SIPART PS2 FF positioners are considered to be a type A sub-system as specified in EN 61508-2.

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 PA and SIPART PS2 FF positioners is 73 years. The MTBF for the basic electronics module is 187 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 recalled in the local display or by means of the PROFIBUS PA or FOUNDATION field bus communication.

Reference
Device manual /1/, /2/ Section 4.5 "Diagnostics", diagnostic values 31=VENT1 and 32=VENT2

See also
Settings (Page 3-2)
Safety characteristics (Page 3-5)

3.3 Settings

The coding bridge on the basic electronic system must be plugged without fail on to the left position facing the terminals ("safe pos.") or removed completely for the safety function to work properly.

Special parameter settings are not necessary.

Reference
Device manual /1/, /2/, Section 3.4 "Electrical connection"
Protection against configuration changes
You should attach the housing cover so that the device is protected against unwanted and unauthorized changes/operation.

Checking the safety function
To check the safety function, proceed as follows:
- Set the nominal value to 50% either by using the local operation (manual operation), the PROFIBUS PA or the FOUNDATION field bus communication
- Apply a LOW signal, i.e. a voltage less than 4.5 V, at the input for the safety shutdown
- Check whether the valve moves to the specified safety position

3.4 Behavior in case of faults

Fault
The procedure in case of faults is described in the device manual.

Reference
Manual /1/, Section 4.8 "Fault correction" and Manual /2/, Section 4.8 "Troubleshooting"

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 name 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.

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}).

The following tests are particularly relevant for the SIPART PS2 PA and SIPART PS2 FF positioners and are to be carried out:

1. Inspection of the safety shutdown
   - Apply a LOW signal, i.e. a voltage less than 4.5 V, at the input for the safety shutdown
   - Check whether the valve moves to the safety position.

2. Inspection of the actuator behavior
   - Apply a HIGH signal, i.e. a voltage more than 13 V, at the input for the safety shutdown
   - Set the nominal value to 50% either by using the local operation (manual operation), the PROFIBUS PA or the FOUNDATION field bus communication
   - 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 using the system are listed in the SIL declaration of conformity (see "Appendix A"). 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).
- The coding bridge on the basic electronic system was plugged on to the left position facing the terminals ("safe pos.") or removed completely.
- The positioner is blocked against unwanted and unauthorized changes/operation.
- The shut-off signal for the SIPART PS2 PA and SIPART PS2 FF positioners is generated at the input for the safety shutdown (terminals 81 and 82) by a safe system which meets at least SIL2. The LOW level has a maximum of 4.5 V at the input terminals.
- 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 drive must move the valve to the pre-defined, safe end position.
- A dangerous failure of the positioner is when the pressure outlet is not depressurized, or the safety position is not reached, when the LOW signal is less than 4.5 V at the input for the safety shutdown.

See also

Settings (Page 3-2)
SIL Declaration of Conformity (Page A-2)
Appendix
A.1 SIL Declaration of Conformity

A.1 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 PA / FF
single acting, with PROFIBUS PA / FOUNDATION Fieldbus
Ordering Nr.: 6DR551* / 6DR361*

We as manufacturer declare that the above Positioners SIPART PS2 PA / FF are suitable for use in safety instrumented systems according to IEC 61508 / 61511.
Safety function: Safety shutdown (depressurizing the output) via separate digital input.
The appropriate SIL Safety Manual must be observed.
The failure rates were calculated via FMECDA (Failure Modes, Effects and Diagnostic Analysis) according to IEC 61508. The calculation was carried out by exida.com.
The proven-in-use was verified according to IEC 61508 / 61511 and evaluated by exida.com.

Safety Related Characteristics:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>SIL</th>
<th>HFT</th>
<th>PFD_{AVG}</th>
<th>λ_{sd}</th>
<th>λ_{su}</th>
<th>λ_{dd}</th>
<th>λ_{du}</th>
<th>SFF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Average Probability of Failure on Demand</td>
<td>Safe detected Failure Rate</td>
<td>Safe undetected Failure Rate</td>
<td>Dangerous detected Failure Rate</td>
<td>Dangerous undetected Failure Rate</td>
<td>Safe Failure Fraction</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6,7 * 10^{-4}</td>
<td>0 FIT</td>
<td>1010 FIT</td>
<td>13 FIT</td>
<td>152 FIT</td>
<td>87%</td>
</tr>
</tbody>
</table>

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, 19.08.2005
Siemens AG

Dr. Schmidt, General Manager Instrumentation

Schmidt, Segment Manager Positioner

No. A5E00481296D - 01
A.2 Test report (extract)

FMEDA and Proven-in-use Assessment

Project:
Electro-pneumatic Positioner SIPART PS2 PA / FF
single acting shut-down module using shut-down input (terminal 81/82)

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

Contract No.: SIEMENS 05/01-04
Report No.: SIEMENS 05/01-04 R014
Version V1, Revision R1.0, August 2005
Stephan Aschenbrenner

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 with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Electro-pneumatic Positioner SIPART PS2 PA / FF. Table 1 gives an overview of the different configurations that belong to the considered Electro-pneumatic Positioner SIPART PS2 PA / FF.

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

<table>
<thead>
<tr>
<th>Conf</th>
<th>Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6DR551*-<em>E</em>**_**** PROFIBUS PA EX; single-acting</td>
</tr>
<tr>
<td>2</td>
<td>6DR551*-<em>N</em>**_**** PROFIBUS PA Standard; single-acting</td>
</tr>
<tr>
<td>3</td>
<td>6DR561*-<em>E</em>**_**** FF EE; single-acting</td>
</tr>
<tr>
<td>4</td>
<td>6DR561*-<em>N</em>**_**** FF Standard; single-acting</td>
</tr>
</tbody>
</table>

For safety applications only the shut-down input (terminal 81/82) with the corresponding pressure output was considered to work as a single-acting shut-down module (“tight closing”). 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 [D17] and [R3]). The results of the quantitative analysis are included in the calculations described in sections 5.2 and 5.3.

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 PA / FF 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 PA / FF when using the shut-down input (terminal 81/82) for the safety function is considered to be a Type A component with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

---

1 Type A component: “Non-complex” component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
As the Electro-pneumatic Positioner SIPART PS2 PA / FF 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 A Electro-pneumatic Positioner SIPART PS2 PA / FF when using the shut-down input (terminal 81/82) for the safety function, with a hardware fault tolerance of 0 and a SFF of 60% to < 90% is 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 – Failure rates

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Failure rates (in FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Safe Detected</td>
<td>0</td>
</tr>
<tr>
<td>Fail Safe Undetected</td>
<td>940</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>13</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>152</td>
</tr>
<tr>
<td>No Effect</td>
<td>70</td>
</tr>
<tr>
<td>Not part</td>
<td>397</td>
</tr>
<tr>
<td>MTBF = MTTF + MTTR</td>
<td>73 years</td>
</tr>
</tbody>
</table>

Table 3: Summary – IEC 61508 failure rates

<table>
<thead>
<tr>
<th>λsd</th>
<th>λsu</th>
<th>λdd</th>
<th>λdu</th>
<th>SFF</th>
<th>DC_s</th>
<th>DC_D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 FIT</td>
<td>10 FIT</td>
<td>13 FIT</td>
<td>152 FIT</td>
<td>87%</td>
<td>0%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Table 4: Summary – PFD AVG values

<table>
<thead>
<tr>
<th>T[Proof] = 1 year</th>
<th>T[Proof] = 5 years</th>
<th>T[Proof] = 10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFD AVG = 6,65E-04</td>
<td>PFD AVG = 3,32E-03</td>
<td>PFD AVG = 6,63E-03</td>
</tr>
</tbody>
</table>

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 PA / FF when used as a single-acting shut-down module ("tight closing") has a PFD_{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 86% when using the shut-down input (terminal 81/82) for the safety function.

The Electro-pneumatic Positioner SIPART PS2 PA / FF has been developed without considering IEC 61508, however, and so IEC 61511-1 First Edition 2003-01 section 11.4.4 is used as a basis for arguing that proven-in-use shows the unlikelihood of systematic failures for the mechanical / pneumatic components.

The failure rates listed above do not include failures resulting from incorrect use of the Electro-pneumatic Positioner SIPART PS2 PA / FF, 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 40°C. 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 PA / FF 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 is presented in sections 5.2 and 5.3 along with all assumptions.

It is important to realize that the "no effect" 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.

The failure rates are valid for the useful life of the Electro-pneumatic Positioner SIPART PS2 PA / FF, which is estimated to be 10 years (see Appendix 3).
### A.3 Literature and standards

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

A.3 Literature and standards
### List of Abbreviations/Acronyms

#### B.1 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full term in English</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
<td>Capability of a function unit to continue executing a required function in the presence of faults or deviations.</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
<td>Average period between two failures</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Repair</td>
<td>Average period between the occurrence of a fault in a device or system and the repair</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of Failure on Demand</td>
<td>Probability of dangerous failures of a safety function on demand</td>
</tr>
<tr>
<td>PFD&lt;sub&gt;Avg&lt;/sub&gt;</td>
<td>Average Probability of Failure on Demand</td>
<td>Average probability of dangerous failures of a safety function on demand</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
<td>Proportion of safe failures: Proportion of failures without the potential to bring the safety-instrumented system into a dangerous or non-permissible functional status.</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
<td>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.</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented System</td>
<td>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.</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure in Time</td>
<td>Frequency of failure Number of faults within 10&lt;sup&gt;9&lt;/sup&gt; hours</td>
</tr>
<tr>
<td>TI</td>
<td>Test Interval</td>
<td>Testing interval of the protective function</td>
</tr>
<tr>
<td>XooY&lt;sub&gt;X&lt;/sub&gt;</td>
<td>&quot;X out of Y&quot; voting</td>
<td>Classification and description of the safety-instrumented system in terms of redundancy and the selection procedures used.</td>
</tr>
<tr>
<td></td>
<td>&quot;Y&quot;</td>
<td>Specifies how often the safety function is executed (redundancy).</td>
</tr>
<tr>
<td></td>
<td>&quot;X&quot;</td>
<td>Determines how many channels have to work correctly.</td>
</tr>
</tbody>
</table>

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.
List of Abbreviations/Acronyms

B.1 Abbreviations
Index

C
characteristics
   Safety, 3-4
   Checking, 3-3

D
documentation.
   required, 1-1

F
Fault, 3-3

M
Maintenance, 3-3

P
Pz, 3-4

S
Safety function, 3-3
   Checking, 3-3
   Safety function, 3-1
   Safety shutdown, 3-1
   system
      Safety-instrumented, 2-1

T
Tight closing, 3-1

Y
Y1, 3-4