PositionMaster EDP300
Electro-Pneumatic Positioner
and Shutdown-Modul

Hardware Version 1.0
Manufacturer
ABB Automation Products GmbH
Process Automation
Schillerstr. 72
32425 Minden
Germany
Tel: +49 551 905-534
Fax: +49 551 905-555

Customer service center
Phone: +49 (0) 180 5 222 580
Fax: +49 (0) 621 381 931-29031
automation.service@de.abb.com

© Copyright 2011 by ABB
Subject to changes without notice
This document is protected by copyright. It assists the user in safe and efficient operation of the device. The contents of this
document, whether whole or in part, may not be copied or reproduced without prior approval by the copyright holder.
Contents

1 Application area .............................................................. 4
2 Acronyms and abbreviations ............................................. 4
3 Standards and definitions of terms ................................. 5
   3.1 Standard IEC 61508 2000 (Edition 1), Part 1 to 7. 5
   3.2 Dangerous failure.................................................. 5
   3.3 Safety-related system ........................................... 5
   3.4 Safety function................................................... 5
4 Determining the Safety Integrity Level (SIL)................. 5
5 Safety-related system .................................................... 6
   5.1 Functional description without shutdown module . 6
   5.2 Functional description with shutdown module ...... 6
6 Information for the safety function ............................... 7
7 Behavior during operation and failure ............................ 7
8 Other relevant documents .............................................. 7
9 Recurring tests ................................................................ 8
   9.1 Safety inspections................................................ 8
   9.2 Functional checks ............................................... 8
   9.2.1 Requirement for checks................................. 8
   9.3 Service life of electrical components..................... 8
   9.4 Repairs............................................................... 8
10 Safety engineering parameters ..................................... 9
  10.1 Prerequisites......................................................... 9
  10.2 Specific safety-related parameters ....................... 9
11 Management Summary.................................................. 10
1 Application area

This manual is valid only in relation to the use of the single-acting depressurizing version of the ABB PositionMaster EDP300 positioner in conjunction with pneumatic actuators with spring-return mechanism.

In the event of a power failure (electrical or pneumatic), the positioner depressurizes the actuator and the return spring moves the valve to a predefined, safe end position (either OPEN or CLOSED).

The positioners meet the following requirements:
— Functional safety according to IEC 61508 2000 (Edition 1)
— Explosion protection (depending on version)
— Electromagnetic compatibility in accordance with EN 61000

2 Acronyms and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>English</th>
<th>German</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td></td>
<td>Ability of a functional unit (hardware) to continue to perform a required function when faults or errors are prevailing.</td>
<td></td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Restoration</td>
<td>Mean time between the occurrence of an error in a unit or in a system and its repair.</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of Failure on Demand</td>
<td>Probability of hazardous failures for a safety function on demand</td>
</tr>
<tr>
<td>PFD_{av}</td>
<td>Average Probability of Failure on Demand</td>
<td>Average probability of hazardous failures for a safety function on demand</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td></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 the failure of a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will not perform the required safety function.</td>
<td></td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
<td>Amount of safe failures.</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure in Time</td>
<td>(1 \times 10^{-9}) Failures per hour.</td>
</tr>
<tr>
<td>TI</td>
<td>Test Interval between live testing of the safety function</td>
<td>Test interval between live testing of the safety function.</td>
</tr>
<tr>
<td>(\lambda_{sd})</td>
<td>Failure rate for all safe detected failures</td>
<td>Overall rate for all safe detected failures.</td>
</tr>
<tr>
<td>(\lambda_{su})</td>
<td>Failure rate for all safe undetected failures</td>
<td>Overall rate for all safe undetected failures.</td>
</tr>
<tr>
<td>(\lambda_{dd})</td>
<td>Failure rate for all dangerous detected failures</td>
<td>Overall rate for all dangerous detected failures.</td>
</tr>
<tr>
<td>(\lambda_{du})</td>
<td>Failure rate for all dangerous undetected failures</td>
<td>Overall rate for all dangerous undetected failures.</td>
</tr>
</tbody>
</table>
3 Standards and definitions of terms

3.1 Standard IEC 61508 2000 (Edition 1), Part 1 to 7

— English
  Functional safety of electrical / electronic / programmable
electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices).
— German
  Funktionale Sicherheit sicherheitsbezogener
elektrischer / elektronischer / programmierbarer
elektronischer Systeme (Zielgruppe: Hersteller und Lieferanten von Geräten).

3.2 Dangerous failure
A failure that has the potential to place the safety-related system in a dangerous state or render the system inoperative.

3.3 Safety-related system
A safety-related system performs the safety functions that are required to achieve or maintain a safe condition, e.g., in a plant.
Example: pressure meter, logics unit (e.g., limit signal generator) and valve form a safety-related system.

3.4 Safety function
A specified function that is performed by a safety-related system with the goal, under consideration of a defined hazardous incident, of achieving or maintaining a safe condition for the plant.
Example: limit pressure monitoring

4 Determining the Safety Integrity Level (SIL)

The achievable Safety Integrity Level is determined by the following safety-related parameters:
— Average Probability of Failure on Demand (PFD\textsubscript{av})
— Hardware Fault Tolerance (HFT)
— Safe Failure Fraction (SFF)
— Systematic safety integrity

The specific safety-related parameters for the PositionMaster EDP300 and the shutdown module, as part of a safety function, are listed in the section "Safety-related parameters".

The following table shows the dependence of the Safety Integrity Level (SIL) on the Average Probability of Failure on Demand (PFD\textsubscript{av}). The table applies the "low demand mode"; i.e., the safety function is requested at most once a year.

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>(low demand mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>PFD\textsubscript{av} ≥ 10^{-5} … &lt; 10^{-4}</td>
</tr>
<tr>
<td>3</td>
<td>PFD\textsubscript{av} ≥ 10^{-4} … &lt; 10^{-3}</td>
</tr>
<tr>
<td>2</td>
<td>PFD\textsubscript{av} ≥ 10^{-3} … &lt; 10^{-2}</td>
</tr>
<tr>
<td>1</td>
<td>PFD\textsubscript{av} ≥ 10^{-2} … &lt; 10^{-1}</td>
</tr>
</tbody>
</table>
5 Safety-related system

The positioner includes multiple electrical interfaces. The list below shows which interface is included in the safety evaluation.

<table>
<thead>
<tr>
<th>Interface</th>
<th>SIL</th>
<th>Not SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 … 20 mA signal input</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Digital input</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Alarm output</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Analog position feedback</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Digital position feedback</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Shutdown module</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Universal input module</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Mechanical limit switches</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Hart communication</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Monitoring unit, logics unit and actuator (positioner, pneumatic actuator and valve) form a safety-related system that performs a safety function. The Average Probability of Failure on Demand (PFD_{av}) is usually divided between the monitoring unit, logics unit and actuator sub-systems as per the figure below.

Typical division of the Average Probability of Failure on Demand (PFD_{av}) across sub-systems

<table>
<thead>
<tr>
<th>Monitoring Unit</th>
<th>Logics unit (e.g., PLC)</th>
<th>Actuator (e.g., valve)</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 35 %</td>
<td>≤ 15 %</td>
<td>≤ 50 %</td>
</tr>
</tbody>
</table>

The figures below depict the safety function "System-independent plant monitoring" in conjunction with the PositionMaster EDP300 positioner and a shutdown module.

5.1 Functional description without shutdown module

If the input current fails, the power supply to the I/P module in the positioner is disconnected and this depressurizes the pneumatic actuator. The actuator return spring then moves the valve to a safe end position (OPEN or CLOSED).

5.2 Functional description with shutdown module

Control for the shutdown module is electrically isolated from the other parts of the positioner. As a result, a monitoring system can act on the final control element independently of the process control system.

If the separate 24 V DC power supply to the shutdown module fails, the I/P module in the positioner is deactivated and depressurizes the pneumatic actuator. The actuator return spring then moves the valve to a safe end position (OPEN or CLOSED).

The positioner motherboard as well as communication and position feedback are still active, since they are powered by the analog setpoint signal.

When the shutdown module is used, the switch shown in the figure must be in the "I" position.

Fig. 1: Safety function with 0 mA at current input
1 PLC with 4 … 20 mA signal output
2 Monitoring unit with relay output
3 Electro-pneumatic positioner EDP300
4 Valve

Fig. 2: Safety function with shutdown module
1 PLC with 4 … 20 mA signal
2 Monitoring unit with 24 V DC output
3 Positioner
4 Valve
5 Shutdown module

Fig. 3
6 Information for the safety function

NOTICE
The safety functions in the application are activated if the electrical input signal fails. When this occurs, the positioner has to depressurize the pneumatic actuator whose return spring moves the valve to a safe end position (OPEN or CLOSED).
This function must be checked during commissioning.
The safe state is achieved if output Y1 is depressurized and the valve is located in the safe end position. The time taken for the safe state to be achieved is not exclusively determined by the positioner; it is also dependent on external conditions.
The user must therefore check whether the safe state is achieved within the necessary time frame.

NOTICE
If a shutdown module is integrated in the device, the safety function is activated if the separate 24 V DC feed for the shutdown module is interrupted. When this occurs, the positioner has to depressurize the pneumatic actuator whose return spring moves the valve to a safe end position (OPEN or CLOSED).
This function must be checked during commissioning.
The safe state is achieved if output Y1 is depressurized and the valve is located in the safe end position. The time taken for the safe state to be achieved is not exclusively determined by the positioner; it is also dependent on external conditions.
The user must therefore check whether the safe state is achieved within the necessary time frame.

IMPORTANT (NOTE)
Safety-related systems without a self-locking function must be monitored or set to an otherwise safe condition after performing the safety function within MTTR (8 hours). The device lifecycle must be evaluated according to the specified MTBF.

7 Behavior during operation and failure

IMPORTANT (NOTE)
Behavior during operation and failure is described in the operating instructions for the electro-pneumatic positioner.

8 Other relevant documents

Depending on the version, the following documentation must be available for the positioner and shutdown module:

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commissioning instructions</td>
<td>CI/EDP300</td>
</tr>
<tr>
<td>Operating instructions</td>
<td>OI/EDP300</td>
</tr>
</tbody>
</table>

For devices in explosion-proof design, the relevant EC-type examination test certificate must be present.

Outside of the EU, the relevant local operational regulations and directives apply.

The specifications for storage and operating conditions must be taken from the commissioning instruction.
9 Recurring tests

9.1 Safety inspections
The safety function for the entire safety loop must be checked regularly in accordance with IEC 61508. The inspection intervals are defined when calculating the individual safety loops for a system.
The operator is responsible for selecting the type of check and the intervals within the specified period (see the PFDAV value which depends on the selected maintenance interval).
Inspections must be conducted in a manner that enables users to verify the proper function of the safety equipment in combination with all components.
One possible procedure for recurring tests to detect hazardous and unidentified device errors is described in the following section.

9.2 Functional checks

9.2.1 Requirement for checks
The device must not be in the safety position.

The following steps must be performed (without the shutdown module):
— Interrupt the electrical input signal.
— Check whether the positioner depressurizes the pneumatic drive.
— Check whether the return spring moves the valve to a safe end position (OPEN or CLOSED).

The following steps must be performed (with the shutdown module):
— Interrupt the separate 24 V DC supply for the shutdown module.
— Check whether the positioner depressurizes the pneumatic drive.
— Check whether the return spring moves the valve to a safe end position (OPEN or CLOSED).

The user must check whether the safe state is achieved within the necessary time frame.
If this occurs, the test coverage is 99 %.

9.3 Service life of electrical components
The basic failure rates for electrical components comply with the useful service life in accordance with IEC 61508-2, section 7.4.7.4, note 3.

9.4 Repairs
Defective units need to be sent back to the ABB service and repair department. The type of error and possible reason must also be provided.
Use the original packaging or a secure transport container of an appropriate type if you need to return the device for repair or recalibration purposes. Fill out the return form (see the appendix to the positioner operating instructions) and include this with the device.
According to the EU Directive governing hazardous materials, the owner of hazardous waste is responsible for its disposal or must observe the following regulations for shipping purposes:
All devices delivered to ABB Automation Products GmbH must be free from any hazardous materials (acids, alkali, solvents, etc.).
When ordering spare parts always provide the serial number of the device. This information is located on the name plate of the original device.

Address:
ABB Automation GmbH
- Service Instruments -
Schillerstr. 72
D -32425 Minden
GERMANY
Spare parts:
Phone: +49 (0) 571 830-1783
Fax: +49 (0) 571 830-1744
e-mail: parts-repair-minden@de.abb.com
10 Safety engineering parameters

10.1 Prerequisites
— Communication via HART protocol is used only to configure and calibrate the device. It is also used for diagnostic functions but not for safety-related, critical operations.
— A single-acting pneumatic actuator with spring-return mechanism is used.
— If the power supply fails (4 ... 20 mA), the pneumatic output of the PositionMaster EDP300 positioner is depressurized and a spring in the pneumatic actuator moves the valve to a predefined end position.
— The pneumatic power supply is free of oil, water, and dust in accordance with DIN / ISO 8573-1.
— The repair period (MTTR) following a device fault is 8 hours.
— The mean temperature over a longer period of time is 40°C (104°F).
— The positioner is used only in applications with low request rates (low demand mode).

10.2 Specific safety-related parameters

<table>
<thead>
<tr>
<th>Positioner type</th>
<th>Category</th>
<th>SFF</th>
<th>PFD_{av}</th>
<th>(\lambda_{sd} + \lambda_{su} )</th>
<th>(\lambda_{du})</th>
</tr>
</thead>
<tbody>
<tr>
<td>PositionMaster EDP300</td>
<td>SIL2</td>
<td>88%</td>
<td>1.46E-03</td>
<td>1347 FIT</td>
<td>176 FIT</td>
</tr>
<tr>
<td>PositionMaster EDP300 as shutdown module</td>
<td>SIL2</td>
<td>88%</td>
<td>1.51E-03</td>
<td>1417 FIT</td>
<td>181 FIT</td>
</tr>
</tbody>
</table>

The systematic safety integrity is suitable for SIL2.

<table>
<thead>
<tr>
<th>Failure rate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\lambda_{sd} + \lambda_{su} + \lambda_{sd})</td>
<td>Failure rate for detected dangerous failures and safe failures</td>
</tr>
<tr>
<td>(\lambda_{du})</td>
<td>Failure rate for dangerous, undetected failures</td>
</tr>
</tbody>
</table>

IMPORTANT (NOTE)
The PFD_{av} values provided in the table above are only valid for the PositionMaster EDP300 positioner and shutdown module.
For additional information, see the "Management Summary".
11 Management Summary

TYPE CERTIFICATE

ABB 0812027C P0007 C002

exida Certification S.A. hereby confirms that the

PositionMaster EDP300
Product Version: 1.0

ABB Automation Products GmbH
Minden, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000
Parts 1 - 7, and meets requirements providing a level of integrity to

Systematic Integrity :  SIL 2 Capable
Random Integrity : Type A device, $PFD_{AVG}$ and architecture constraints must be verified for each application

Safety Function
PositionMaster EDP300 is an electro-pneumatic valve positioner for use with pneumatic linear and rotary actuators. The considered safety application is fail-safe single acting with spring return.

Application Restrictions
The unit must be properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor

Certifying Assessor

Date: 2 August 2011

exida Certification SA, Nyon, Switzerland
Systematic Integrity: SIL 2 Capable

**SIL 2 Capability**
The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without “prior use” justification by end user or diverse technology redundancy in the design.

**Summary for PositionMaster EDP300:**

Type A device  
IEC 61508 failure rates:

<table>
<thead>
<tr>
<th>Failure category</th>
<th>$\lambda_{SAFE}$</th>
<th>$\lambda_{OD}$</th>
<th>$\lambda_{DU}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDP 300 with Shutdown module</td>
<td>1407</td>
<td>10</td>
<td>181</td>
</tr>
<tr>
<td>EDP 300 with supply current of 0 mA</td>
<td>1347</td>
<td>0</td>
<td>176</td>
</tr>
</tbody>
</table>

All failure rates are given in FIT=10^-9/h

**SIL Verification:**
The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of $PFD_{avg}$ considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

**The following documents are mandatory parts this certificate:**
ABB 0812-027C R021 Assessment report EDP 300 V1RO  
Safety Manual, SM/EDP300/SIL-DE 08.2011

exida Certification SA, Nyon, Switzerland  
info@exidacert.ch  
Page 2 (2)