

and Shutdown Module for TZIDC / TZIDC-200
Information regarding functional safety



Electro-Pneumatic Positioner

TZIDC / TZIDC-200

SIL-Safety Instructions

37/18-79-EN

02.2010

Rev. D

Manufacturer:

ABB Automation Products GmbH

Schillerstraße 72

32425 Minden

Germany

Tel.: +49 551 905-534

Fax: +49 551 905-555

Customer service center

Phone: +49 180 5 222 580

Fax: +49 621 381 931-29031

automation.service@de.abb.com

© Copyright 2010 by ABB Automation Products GmbH

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.

1	Field of Application	4
2	Acronyms and abbreviations	5
3	Relevant standards	6
4	Terms and definitions	6
5	Determining the Safety Integrity Level (SIL)	7
6	Safety-related system	8
7	Information for the safety function	9
8	Applicable device documentation	9
9	Behavior during operation and failure	9
10	Periodic checks	10
11	Safety engineering parameters	11
11.1	Prerequisites	11
11.2	Specific safety-related parameters.....	11
12	SIL declaration of conformity	12
13	Management summary	13

1 Field of Application

Provide positioning control for valves with pneumatic actuators up to SIL 2 in accordance with the safety engineering requirements of IEC 61508.

The devices are single-acting, depressurizing ABB positioners of type TZIDC / TZIDC-200 and 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 in accordance with IEC 61508
- Explosion protection (depending on version)
- Electromagnetic compatibility in accordance with EN 61000

2 Acronyms and abbreviations

Acronym	Designation	Description
HFT	Hardware Fault Tolerance	Hardware Fault Tolerance Ability of a functional unit (hardware) to continue to perform a required function in the presence of faults or errors.
MTBF	Mean Time Between Failures	Mean Time Between Failures
MTTR	Mean Time To Repair	Mean time between occurrence of an error in a unit or system and its repair.
PFD	Probability of Failure on Demand	Probability of hazardous failures for a safety function on demand
PFD _{av}	Average Probability of Failure on Demand	Average probability of hazardous failures for a safety function on demand
SIL	Safety Integrity Level	Safety Integrity Level The international standard IED 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 perform the requested safety function.
SFF	Safe Failure Fraction	Amount of safe failures.
FIT	Failure in Time	1×10^{-9} Failures per hour.
TI	Test Interval between live testing of the safety function	Test interval between live testing of the safety function.
λ_{sd}	Failure rate for all safe detected failures	Overall rate for all safe detected failures.
λ_{su}	Failure rate for all safe undetected failures	Overall rate for all safe undetected failures.
λ_{dd}	Failure rate for all dangerous detected failures	Overall rate for all dangerous detected failures.
λ_{du}	Failure rate for all dangerous undetected failures	Overall rate for all dangerous undetected failures.

3 Relevant standards

Standard	English	German
IEC 61508, Part 1 to 7	Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices).	Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices).

4 Terms and definitions

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

5 Determining the Safety Integrity Level (SIL)

The achievable Safety Integrity Level is determined by the following safety-related parameters:

- Average probability of hazardous failures for a safety function on demand (PFD_{av})
- Hardware Fault Tolerance (HFT)
- Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF)

The specific safety-related parameters for TZIDC / TZIDC-200 positioners and the shutdown module, as part of a safety function, are listed in the section "Safety-related parameters".

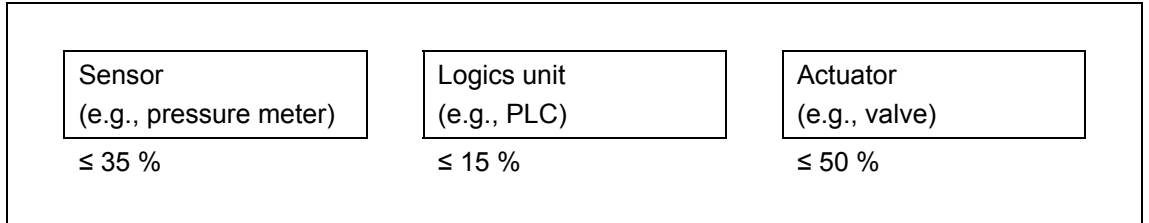
The following table shows the dependence of the Safety Integrity Level (SIL) on the Average Probability of Failure on Demand (PFD_{av}). The table applies the "low demand mode", i.e. the safety-related system is checked at most once a year.

Safety Integrity Level (SIL)		(low demand mode)
4	PFD_{av}	$\geq 10^{-5} \dots < 10^{-4}$
3		$\geq 10^{-4} \dots < 10^{-3}$
2		$\geq 10^{-3} \dots < 10^{-2}$
1		$\geq 10^{-2} \dots < 10^{-1}$

6 Safety-related system

Sensor, 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 sensor, logics unit and actuator sub-systems.

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



i

Important

This documentation applies to TZIDC and TZIDC-200 electro-pneumatic positioners and their shutdown modules as part of a safety function. The following table displays the achievable Safety Integrity Level (SIL) for the entire safety-related system for type A systems depending on the Safe Failure Fraction (SFF) and the Hardware Fault Tolerance (HFT).

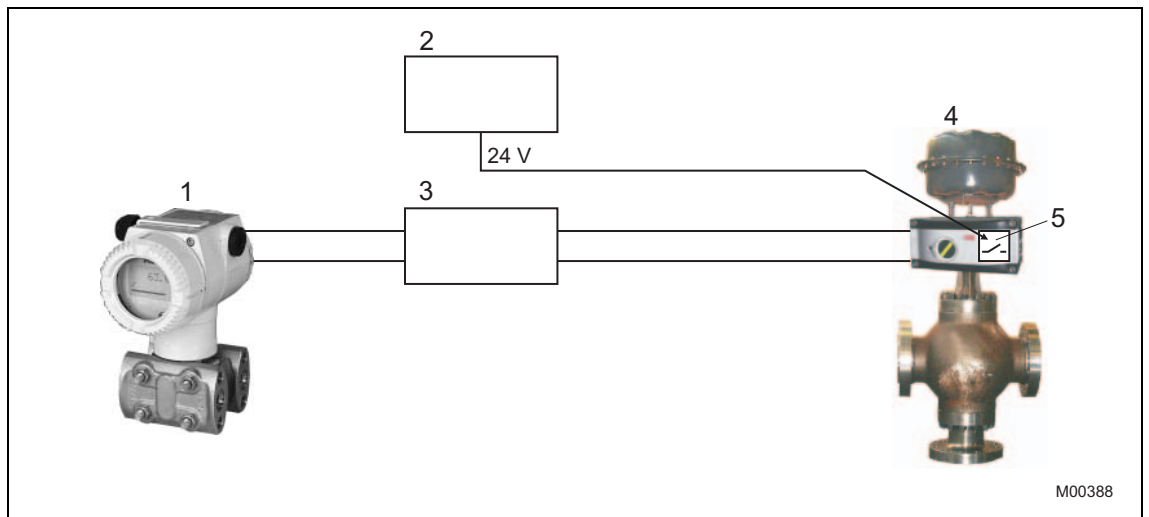


Fig. 1 Safety function "System-independent plant monitoring" with TZIDC-200 positioner and shutdown module as subsystems

- | | |
|---|--|
| <ul style="list-style-type: none"> 1 265xx transmitter with local operation, option for setting upper and lower range limits as well as damping value. 2 Monitoring 3 Control 4 Pneumatic positioner TZIDC with control valve and local operation for commissioning, setup and configuration. | <ul style="list-style-type: none"> 5 Shutdown module integrated in the positioner, for depressurizing the pneumatic actuator. The module is controlled independently of the process control system. |
|---|--|

Functional description

Control for the shutdown module is galvanically 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.

7 Information for the safety function



Attention!

If the input signal fails, the pneumatic module depressurizes the actuator and the integrated return spring moves the valve to a predefined end position (OPEN or CLOSED).



Important

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.

8 Applicable device documentation

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

Type	Operating instructions
TZIDC and shutdown module	41/18-84 xx
TZIDC-200 and shutdown module	42/18-85 xx

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

9 Behavior during operation and failure



Important

Behavior during operation and failure is described in the operating instructions.

10 Periodic checks

Safety checks

The safety function for the entire safety loop must be checked regularly in accordance with IEC 61508. The test intervals are determined when calculating the individual safety loops of a plant (PFD_{av} 's).

Functional checks

The safety function during operation (0 mA signal, shutdown module (if installed)) must be checked on annual basis.

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.

Repairs

When you send a defective device to the repair department, include information describing the error and, if possible, the cause.



Important

When ordering replacement devices always provide the serial number of the original device (on the name plate).

Address

ABB Automation GmbH
Parts & Repair
Schillerstrasse 72
32425 Minden
GERMANY

11 Safety engineering parameters

11.1 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.
- If the power supply fails (4 ... 20 mA), the pneumatic output of the TZIDC / TZIDC-200 positioner is depressurized and a spring in the pneumatic actuator moves the valve to a predefined end position.
- The compressed air 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.
- The positioner is used only in applications with low request rates (low demand mode).

11.2 Specific safety-related parameters

Positioner type	Category	SFF	PFD _{av}	$\lambda_{dd} + \lambda_s$	λ_{du}
TZIDC / TZIDC-200 as shutdown module	SIL2	94 %	1.76×10^{-4}	718 FIT	140 FIT
TZIDC / TZIDC-200 with supply current 0 mA		94 %	$1,76 \times 10^{-4}$	651 FIT	40 FIT

$\lambda_{dd} + \lambda_s$: Failure rate for detected dangerous failures and safe failures

λ_{du} : Failure rate for dangerous, undetected failures



Important

The PFD_{av} values provided in the table are valid for TZIDC/TZIDC-200 positioners and the shutdown module.

For additional information, see the Management Summary.

12 SIL declaration of conformity

49/18-79EN
Rev. C



SIL DECLARATION OF CONFORMITY

Manufacturer: ABB Automation Products GmbH
Address: Schillerstraße 72 - D-32425 Minden
Product name: Positioner TZIDC – TZIDC-200 (4...20 mA) and Shutdown Modul
Valid from: Software-Revision 3.00

Functional safety according to IEC 61508


We as the manufacturer declare that the a.m. products are suitable for the use in a safety related application up to SIL 2 according to IEC 61508, provided that the attached safety instructions are observed. The assessment of the safety critical and dangerous random errors results, in case of an annual function test, in the following parameters:

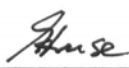
SIL (Safety integrity level): 2 **Type: A**
HFT (Hardware failure tolerance): 0 (one-channel application)

Product	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TZIDC / TZIDC-200 as shutdown module	94%	$1,76 * 10^{-4}$	718 FIT	40 FIT
TZIDC / TZIDC-200 with supply current of 0 mA	94%	$1,76 * 10^{-4}$	651 FIT	40 FIT

2008-01-21

Date


 Dr. Wolfgang Scholz
 Head of Research & Development


 Bernhard Kruse
 Head of Quality Management

13 Management summary



Failure Modes, Effects and Diagnostic Analysis

Project:

Intelligent Positioner TZIDC / TZIDC-200

Customer:

ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 07/07-40

Report No.: ABB 07/07-40 R016

Version V1, Revision R0, January 2008

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 carried out on the intelligent positioner TZIDC / TZIDC-200. Table 1 gives an overview of the two possible safety applications of the considered intelligent positioner TZIDC / TZIDC-200.

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: Overview of possible safety applications

[SA1]	Shutdown module
[SA2]	Fail-safe position with supply current of 0 mA

All other possible input and output variants or electronics are not covered by this report.

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

For [SA2] only the mechanical components of the intelligent positioner TZIDC / TZIDC-200 have been considered as all electronic components will only lead to safe or residual failures. Considering the mechanical components only represents the worst-case.

As only the mechanical components and the shutdown module of the intelligent positioner TZIDC / TZIDC-200 are used for safety applications the device is considered to be a Type A¹ subsystem. It consists of certain redundant parts but overall it is considered to be a device with a hardware fault tolerance of 0.

For Type A subsystems 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.

Failure rates that are assigned to the various failure modes of the (electro-)mechanical and pneumatic components of the intelligent positioner TZIDC / TZIDC-200 were obtained from field failure data collected and analyzed by ABB Automation Products GmbH using only operational hours from the warranty period of operation. Confidence Interval calculations were done using a chi-square distribution and an upper limit failure rate based on a 70% confidence factor per IEC 61508. The failure rate results were compared with industry databases and found to be within a reasonable range.

¹ Type A subsystem: "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.



Table 2: Summary for TZIDC / TZIDC-200 as shutdown module – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected	0
Fail Safe Undetected	695
Fail Dangerous Detected	0
Fail Dangerous Undetected	40
Residual	23
MTBF = MTTF + MTTR	150 years

Table 3: Summary for TZIDC / TZIDC-200 as shutdown module – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	718 FIT	0 FIT	40 FIT	94%	0%	0%

Table 4: Summary for TZIDC / TZIDC-200 with supply current of 0 mA – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected	0
Fail Safe Undetected	651
Fail Dangerous Detected	0
Fail Dangerous Undetected	40
Residual	0
MTBF = MTTF + MTTR	165 years

Table 5: Summary for TZIDC / TZIDC-200 with supply current of 0 mA – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	651 FIT	0 FIT	40 FIT	94%	0%	0%

A user of the intelligent positioner TZIDC / TZIDC-200 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 sections 5.2 and 5.3 along with all assumptions.

It is important to realize that the “residual” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their 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 intelligent positioner TZIDC / TZIDC-200 (see Appendix 2).

ABB has Sales & Customer Support expertise in over 100 countries worldwide.

www.abb.com/instrumentation

The Company's policy is one of continuous product improvement and the right is reserved to modify the information contained herein without notice.

Printed in the Fed. Rep. of Germany (02.2010)

© ABB 2010

3KXE341001R4801



ABB Limited

Salterbeck Trading Estate
Workington, Cumbria
CA14 5DS
UK
Tel: +44 (0)1946 830 611
Fax: +44 (0)1946 832 661

ABB Inc.

125 E. County Line Road
Warminster, PA 18974
USA
Tel: +1 215 674 6000
Fax: +1 215 674 7183

ABB Automation Products GmbH

Schillerstr. 72
32425 Minden
Germany
Tel: +49 551 905-534
Fax: +49 551 905-555