Introduction

The TZIDC / TZIDC-200 is an intelligent digital positioner for communication via HART within the positioner product range.

Additional Information

Additional documentation on TZIDC / TZIDC-200 is available for download free of charge at www.abb.com/positioners. Alternatively simply scan this code:
Table of contents

1 Application area .......................................................................................... 3
2 Acronyms and abbreviations ........................................................................ 3
3 Standards and definitions of terms ............................................................. 4
   IEC 61508 Standard .................................................................................... 4
   Dangerous failure ....................................................................................... 4
   Safety-related system .................................................................................. 4
   Safety function ........................................................................................... 4
4 Determining the Safety Integrity Level (SIL) ............................................... 4
5 Safety-related system .................................................................................. 5
   Functional description ................................................................................ 5
   TZIDC/TZIDC-200 safety function with shutdown module ....................... 5
   TZIDC/TZIDC-200 safety function with power supply 0 mA ...................... 5
6 Information for the safety function ............................................................ 6
7 Behavior during operation and failure ....................................................... 6
8 Other relevant documents .......................................................................... 6
9 Recurring tests ............................................................................................ 6
   Safety inspections .................................................................................... 6
   Function test ............................................................................................. 6
   Test requirements ..................................................................................... 6
   Service life of electrical components ....................................................... 7
   Repair ........................................................................................................ 7
10 Safety parameters ....................................................................................... 7
   Assumptions ............................................................................................. 7
   Specific safety parameters ........................................................................ 7
11 SIL-Declaration of Conformity ................................................................. 8
12 Management summary .............................................................................. 9
# 1 Application area

This manual is valid only in relation to the use of the single-acting depressurizing version of the ABB TZIDC / TZIDC-200 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 in accordance with IEC 61508
- 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>PFDav</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

IEC 61508 Standard


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., alarm signalling unit) 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

4 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 (PFDav)
- Hardware Fault Tolerance (HFT)
- Safe Failure Fraction (SFF)

The specific safety parameters for the TZIDC / TZIDC-200 and the shutdown module, as part of a safety function, are listed in the Safety parameters on page 7 section.

The following table shows the dependence of the Safety Integrity Level (SIL) on the average Probability of Failure on Demand of the entire safety-related system (PFDav). The table assumes 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>PFDav (low demand mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-5} ) to (&lt; 10^{-4} )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-4} ) to (&lt; 10^{-3} )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-3} ) to (&lt; 10^{-2} )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-2} ) to (&lt; 10^{-1} )</td>
</tr>
</tbody>
</table>
5 Safety-related system

Sensor, logic 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 of the entire safety-related system’ (PFD_{av}) is usually divided between the sensor, logic unit and actuator sub-systems in accordance with the following table.

Typical division of the average Probability of Failure on Demand (PFD_{av}) across subsystems

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

Note
This documentation applies to the TZIDC / TZIDC-200 digital positioners and the optional shutdown module as part of a safety function.

Functional description

TZIDC/TZIDC-200 safety function with shutdown module

The controller for the shutdown module is usually electrically isolated from the other 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 converter in the positioner is interrupted and depressurizes the pneumatic actuator. The actuator 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.

TZIDC/TZIDC-200 safety function with power supply 0 mA

The safety functions in the application are activated if the electrical input signal fails.

When this occurs, the positioner depressurizes 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 the output 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.
6 Information for the safety function

**CAUTION**
Without the input signal, the pneumatic module in the positioner vents the drive and the installed spring in it moves the valve in a predetermined end position (OPEN or CLOSED).

**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

**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>Product designation</th>
<th>Document name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TZIDC/110/120</td>
<td>CI/TZIDC/110/120</td>
</tr>
<tr>
<td>TZIDC-200/210/220</td>
<td>CI/TZIDC-200/210/220</td>
</tr>
<tr>
<td><strong>Commissioning Instruction</strong></td>
<td></td>
</tr>
<tr>
<td>TZIDC, TZIDC-110, TZIDC-120</td>
<td>42/18-84</td>
</tr>
<tr>
<td>TZIDC-200, TZIDC-210, TZIDC-220</td>
<td>42/18-85</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

**Safety inspections**
The safety function for the entire safety loop must be checked regularly in accordance with IEC 61508 / IEC 61511. 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.

**Function test**

**Test requirements**
The device must not be in the safety position.

Perform the following steps (without the shutdown module):
- Interrupt the electric input signal.
- Check whether the positioner depressurizes the pneumatic actuator.
- Check whether the spring moves the valve to a safe end position (OPEN or CLOSED).

Perform the following steps (with the shutdown module):
- Interrupt the separate 24 V DC supply for the shutdown module.
- Check whether the positioner depressurizes the pneumatic actuator.
- Check whether the 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 is successful, a test coverage of 99 % can be assumed.
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.

Repair
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 for the return:

ABB Automation GmbH
- Service Instruments -
Schillerstraße 72
D-32425 Minden
Germany
Fax: +49 571 830-1744
Email: parts-repair-minden@de.abb.com

10 Safety parameters

Assumptions
- 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 to 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 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 observed 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).

Specific safety parameters

<table>
<thead>
<tr>
<th>Positioner type</th>
<th>Category</th>
<th>SFF</th>
<th>PFD\text{avg}</th>
<th>(\lambda_{\text{dd}} \times \lambda_{s})</th>
<th>(\lambda_{du})</th>
</tr>
</thead>
<tbody>
<tr>
<td>TZIDC / TZIDC-200 as SIL2</td>
<td></td>
<td></td>
<td>94%</td>
<td>1.76 x 10^{-4}</td>
<td>718 FIT</td>
</tr>
<tr>
<td>a shutdown module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>40 FIT</td>
</tr>
<tr>
<td>TZIDC / TZIDC-200 with power supply 0 mA</td>
<td></td>
<td></td>
<td>94%</td>
<td>1.76 x 10^{-4}</td>
<td>651 FIT</td>
</tr>
</tbody>
</table>

The systematic safety integrity is suited for SIL2.

\(\lambda_{\text{dd}} \times \lambda_{s}\) Failure rate for detected dangerous failures and safe failures
\(\lambda_{du}\) Failure rate for dangerous, undetected failures

Note
The PFD\text{avg} values shown in the table above only refer to the TZIDC / TZIDC-200 positioner or to the shutdown module.
For additional information, see the ‘Management Summary’.
11 SIL-Declaration of Conformity

SIL-DECLARATION OF CONFORMITY

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

Functional Safety according to IEC 61508/61511

We as the manufacturer declare that the a.m. products are suitable for the use in safety related application up to SIL 2.
A proven-in-use assessment according to IEC61511 is to be conducted. The attached safety instructions must be observed.
The assessment of the safety critical and dangerous random error results according to IEC61508:2000 provide in case of an annual function test the following parameters:

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

<table>
<thead>
<tr>
<th>Product</th>
<th>SFF</th>
<th>PFDAv</th>
<th>$\lambda_{ud} + \lambda_{s}$</th>
<th>$\lambda_{du}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>TZIDC / TZIDC-200 as shutdown module</td>
<td>94%</td>
<td>$1.76 \times 10^{-4}$</td>
<td>718 FIT</td>
<td>40 FIT</td>
</tr>
<tr>
<td>TZIDC / TZIDC-200 with supply current of 0 mA</td>
<td>94%</td>
<td>$1.76 \times 10^{-4}$</td>
<td>651 FIT</td>
<td>40 FIT</td>
</tr>
</tbody>
</table>

2014-03-24

Date

i. V. Tilo Merlin
Head of Research & Development

i. V. Manfred Küppel
Head of Quality Assurance
12 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
Management summary

This report summarizes the results of the hardware assessment carried out on the intelligent positioner TIDC / TIDC-200. Table 1 gives an overview of the two possible safety applications of the considered intelligent positioner TIDC / TIDC-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

<table>
<thead>
<tr>
<th>[SA1]</th>
<th>Shutdown module</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SA2]</td>
<td>Fail-safe position with supply current of 0 mA</td>
</tr>
</tbody>
</table>

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 TIDC / TIDC-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 TIDC / TIDC-200 are used for safety applications the device is considered to be a Type A\(^1\) 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 TIDC / TIDC-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

<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>695</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>0</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>40</td>
</tr>
<tr>
<td>Residual</td>
<td>23</td>
</tr>
<tr>
<td>MTBF = MTTF + MTTR</td>
<td>150 years</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>λsd</th>
<th>λsu</th>
<th>λsd</th>
<th>λsu</th>
<th>SFF</th>
<th>DCs</th>
<th>DC0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 FIT</td>
<td>718 FIT</td>
<td>0 FIT</td>
<td>40 FIT</td>
<td>94%</td>
<td>0%</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Summary for TZIDC / TZIDC-200 with supply current of 0 mA – 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>695</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>0</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>40</td>
</tr>
<tr>
<td>Residual</td>
<td>0</td>
</tr>
<tr>
<td>MTBF = MTTF + MTTR</td>
<td>165 years</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>λsd</th>
<th>λsu</th>
<th>λsd</th>
<th>λsu</th>
<th>SFF</th>
<th>DCs</th>
<th>DC0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 FIT</td>
<td>651 FIT</td>
<td>0 FIT</td>
<td>40 FIT</td>
<td>94%</td>
<td>0%</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

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).
Introduction

The TZIDC / TZIDC-200 is an intelligent digital positioner for communication via HART within the positioner product range.

Additional Information

Additional documentation on TZIDC / TZIDC-200 is available for download free of charge at www.abb.com/positioners. Alternatively simply scan this code:

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail.

ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB.

© ABB 2019