ABB MEASUREMENT & ANALYTICS | SIL-SAFETY MANUAL | SM/TZIDC/TZIDC-200/SIL-EN REV. G

TZIDC / TZIDC-200

Digital Positioner

Additional instructions for IEC 61508 compliant devices from HW Rev. 05.xx

TZIDC
TZIDC-200

Introduction

Safety Manual for TZIDC / TZIDC-200 digital Positioner.

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

This document must be considered in conjunction with the related operating instructions.

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

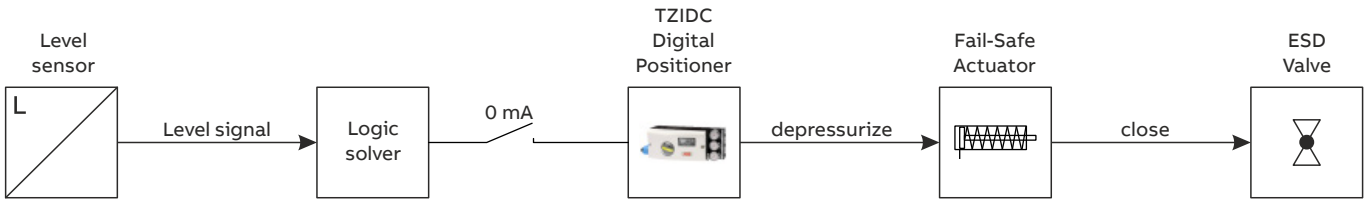

Figure 1: Tank overfill protection (example)

The TZIDC is an electronically configurable 2-wire 4 to 20 mA valve positioner with HART® communication capabilities designed for mounting on pneumatic linear or rotary actuators.

The TZIDC-200 is a variant designed with a flameproof enclosure as explosion protection concept.

The integrated I/P module with subsequent pneumatic amplifier is used to control the attached pneumatic actuator.

The SIL Safety Function is intended to open or close actuator/valves assemblies as emergency application.

By providing 0 mA as control/setpoint signal the positioner depressurizes the fail-safe actuator which return spring moves the valve to a predefined, safe end position (either OPEN or CLOSED).

Figure 1 is demonstrating the safety instrumented function as example on a Tank Overfill Protection.

The TZIDC pneumatic system can be supplied in four versions: for single acting or double acting actuators and each with the 'fail-safe' or 'fail-freeze' safety behavior.

The SIL Safety Function is limited to the version: 'single-acting, fail safe' in conjunction with pneumatic fail-safe actuators with spring-return mechanism.

The table below is demonstrating the safety instrumented functions provided by ABBs Positioner TZIDC & EDP300 as informational comparison:

Safety Function	Supported by	SIL related parts	Pro+/Con–
Control Signal forced to 0 mA	ABB TZIDC ABB EDP300	• Pneumatic I/P module	+ No influence of electronics, software and device setup + no additional field installation lines
Shut Down Module forced to 0 VDC	ABB EDP300	• Shut Down Module • Pneumatic I/P module	+ No influence of electronics, software and device setup + Position feedback signal available even on fail safe operation – additional 24 V DC binary out field installation line demanded

The order variant 'CS2 – SIL 2 Declaration of Conformity' is capable to meet the SIL safety requirements for the integration in Safety Instrumented Systems in compliance to IEC 61508-2 within the process industry sector according to IEC 61511.

The area of safety applications is limited to:

- up to SIL 2
- as Low Demand Mode of operation

with further constraints as stated within this safety manual.

In case of questions and detected safety critical device failures please contact the ABB Customer Service Center by stating the ´Product Type Designator´ and ´Functional Safety SIL´ as request headlines.

Customer service center:

Tel: +49 180 5 222 580

Email: automation.service@de.abb.com

2 Purpose

The purpose of the safety manual is to document the important information required to enable the integration of this product into a safety-related system in compliance with the requirements of the IEC 61508 and IEC 61511 standard.

3 Other relevant documents

The following corresponding product documents must be taken into consideration in addition to this SIL -safety manual:

Product designation	Document name
Data sheet	
TZIDC	DS/TZIDC
TZIDC-200	DS/TZIDC-200
Operating Instruction	
TZIDC	OI/TZIDC
TZIDC-200	OI/TZIDC-200

The documents can be downloaded in the available languages from the ABB website at www.abb.com/positioners.

In addition, the user of this device is responsible for ensuring compliance with applicable legal regulations and standards.

4 Safety Data Overview

This chapter provides information's on the safety function and safety integrity data based on NE 130:2011 Form B.1.

General			
Device designation and permissible types	TZIDC / TZIDC-200 with SIL Declaration of Conformity: Order-Code CS2		
Safety-related output signal	Y1 / OUT1		
Safe State	The safe state is defined as the pressure differential between the output pressure of the TZIDC I/P module to the attached actuator versus the atmospheric pressure being 0 bar		
Safety function(s)	Setpoint 0 mA will depressurized Y1 / OUT1 to reach the safe-state and move the attached actuator/valve assembly to the safe position OPEN or CLOSED		
Device type acc. to IEC 61508-2	☒ Type A (HFT=0)	☐ Type B (HFT=0)	
Operating Mode	☒ Low Demand Mode	☐ High Demand/Continuous Mode	
Valid Hardware-Version	5.x		
Valid Software-Version	NA (because No Part of the Safety Function)		
Type of evaluation	☐ Complete HW/SW development process evaluation incl. FMEDA and change management acc. to IEC 61508-2,3 ☐ Evaluation of „Prior use´ performance for HW/SW incl. FMEDA and change management acc. to IEC 61508-2,3 ☐ Evaluation of HW/SW field data to verify ´prior use´ acc. to IEC 61511 ☒ Evaluation by FMEDA acc. to IEC 61508-2:2000		
Evaluation through - report no.	Exida.com GmbH: FMEDA Report ABB 07/07-40 R016 Version V1, Revision R0		

Safety Integrity			
Safety integrity	Single-channel use (HFT = 0)	☒ SIL 2 capable	☐ SIL 3 capable

Failure Rates and Diagnostic Data		
λDU	40 FIT*	Further details listed within chapter **FMEDA failure data** on page 11.
λDD	0 FIT*	
λSU	651 FIT*	
λSD	0 FIT*	
SFF – Safe Failure Fraction	94 %	
Proof-Test Coverage PTC	Proof Test 1: 70 % Proof Test 2: 95 % in using the procedure described with **Periodic Proof-Test and Maintenance** on page 9	

* FIT = failures per 10^9 operating hours

5 Acronyms and abbreviations

IEC 61508	International Standard ´Functional safety of electrical/electronic/programmable electronic safety-related systems´
IEC 61511	International Standard ´Functional safety – safety instrumented systems for the process industry sector´
Safety Integrity	Probability of a safety system satisfactorily performing the specified safety functions under the stated conditions.
SIL Safety Integrity Level	Discrete safety integrity level corresponding to a range of safety integrity values, where level 4 has the highest and level 1 has the lowest.
Functional safety	Part of the overall safety relating to the controlled system that depends on the correct functioning of the safety system and other risk reduction measures.
Safety function	Function to be implemented by a safety system or other risk reduction measures, that is intended to achieve or maintain a safe state for the controlled system, in respect of a specific hazardous event.
Hardware fault tolerance HFT n	Ability to continue to perform a required function in the presence of n hardware faults or errors.
Architectural constraints	The highest safety integrity level that can be claimed limited by the hardware constraints (SFF, HFT)
Low demand mode	The safety function is only performed on demand with a demand interval no greater than one per year and greater than twice the proof-test interval.
Dangerous failure	Failure that prevents the safety function from operating as expected
Dangerous detected failure	Dangerous failure but detected and forced to alarm state
Dangerous undetected failure	Dangerous failure not being diagnosed
Safe failure	Failure that results in a fail-safe state
No effect, no part failure	Failure without effect above the safety deviation or which are not part on the specified safety function
Annunciation failure	Failure within automatic diagnostics
FIT	Failure in Time (1x10-9 failures per hour) named λ Lambda
Failure rate	Number of failures per unit time assuming to be a constant value declared as FIT λ_{DD} – detected dangerous failures λ_{DU} – undetected dangerous failures λ_{SD} – detected safe failures λ_{SU} – safe failures
PFD_{AVG}	Average probability of dangerous failure on demand
Safe failure fraction SFF	Fraction of the overall failure rate that results to a safe failure SFF = $(\lambda_{SD}+\lambda_{SU}+\lambda_{DD}) / (\lambda_{SD}+\lambda_{SU}+\lambda_{DD}+\lambda_{DU})$
Proof-test	Periodic test performed to detect dangerous hidden failures and weaknesses in the mechanical integrity within the final application environment
Proof-test interval	Execution interval of the period proof-test
Proof-test coverage PTC	Fraction of detected dangerous failures by the periodic proof-test
Diagnostic coverage DC	Fraction of dangerous failures detected by on-line diagnostic tests. DC = $\lambda_{DD} / (\lambda_{DU}+\lambda_{DD})$
Type A element Type B element	An element can be regarded as type A if, the failure modes of all constituent components are well defined; and the behavior of the element under fault conditions can be completely determined; and there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met. Otherwise, the element shall be regarded as type B.
Useful lifetime	Beyond the useful lifetime the probability of failure increases with time and the probabilistic failure rate estimation is invalid.
Mission Time	Final plant operation time for the safety system. Used for the PFD_{AVG} and Proof-Test Interval calculation.
FMEDA	Failure Modes, Effects and Diagnostics Analysis
MTBF	Mean Time Between Failure MTBF = $(1 / (\lambda_{total} + \lambda_{AU} + \lambda_{no\ effect} + \lambda_{no\ part})) + MTTR$
MTTR	Mean Time to Repair
MTTF	Mean Time to Failure
NAMUR NE43	Standardization of the signal level for the breakdown information of digital 4..20 mA transmitters
SIS	Safety Instrumented System, e.g., consisting out of Sensors & Transmitter, Logic Solver and ESD Actuator

6 Safety function

The safety function is activated if the electrical 4 to 20 mA setpoint signal is set to 0 mA. This 0 mA signal might be forced as direct logic solver/DCS output or by an additional electrical open/close switch within the 4 to 20 mA setpoint line.

As reaction on the 0 mA signal the electronics, firmware & position measurement is deactivated and bypassed, and the mechanical pneumatic system of the positioner will be depressurized into the fail-safe position.

The return spring of the attached pneumatic actuator will move the valve to a safe end position (OPEN or CLOSED) subsequently.

The final safe state is achieved if the valve is located in the safe end position.

The time taken to reach the expected safe end position at the process valve is only partly determined by the positioner; it is also dependent on the attached actuator and valve assembly and further external conditions, therefore the correct safety function as expected within the final application must be checked during installation & commissioning and the end user is responsible to validate whether the safe state is achieved in the expected direction and within the expected time frame.

The positioner safety function is declared as Type A element with HFT=0 according to IEC 61508 capable to be used for SIL Functional Safety Functions up to SIL 2.

According to IEC 61508-2, 7.4.7.4 a useful lifetime, based on experience should be assumed.

The components of the positioner do not contain any specific components with a reduced useful lifetime that are contributing to the dangerous undetected failure rates.

Because the positioner is a moving masses system supplied by instrumented air the final device usage and environmental operating conditions (e.g., no/many open-close cycles, good/bad supply air quality) will have an impact on the useful lifetime.

Therefore, the useful lifetime should be evaluated by the end user according to the final plant experience data.

The Periodic Proof-Test methods within chapter **Periodic Proof-Test and Maintenance** on page 9 are suggested to validate the correct safety function.

When final plant experience, proof testing and related field monitoring data indicates a limiting useful lifetime by related operating conditions, then the plant experience-based lifetime must be used and considered on the failure rates, proof-test intervals, and replacement intervals.

7 Safety operation constraints

The following constraints need to be considered when using the positioner for SIL safety applications:

- Only the 4 to 20 mA setpoint signal is used for the safety function, all other inputs or not part of the safety function.
- The proof-test specified within this safety manual (or an equivalent test as specified for the final SIS safety function) shall be performed before activating the safety operation and in periodical cycles as demanded by the final PFDAVG demands.
- The device is installed per manufacturer's instructions
- The safety-related system (safety logic solver) must be able to force the 0 mA signal direct or by using a safety capable switch on the 4 to 20 mA signal.
- Materials are compatible with the final process conditions.
- The environmental, measurement and application limits stated within the referenced documentations must be considered accordingly for the SIL safety application.

The positioner does not meet safety requirements under the following conditions:

- during installation, configuration, repair and simulation
- during an inspection or proof-test

Before commissioning the positioner in a safety loop application, the end user must check whether the installation setup confirms to the system's safety function.

The end user must verify also that the correct positioner has been installed at the correct positioning point.

Whenever the positioners operating conditions are changed (for instance, if the mounting position is changed or the setup is modified), the safety function must be checked again.

8 Periodic Proof-Test and Maintenance

According to IEC 61508 and IEC 61511 proof-testing shall be performed to reveal dangerous faults.
The end user is responsible for selecting the type and the intervals according to the overall safety system demands.
The inspections must be conducted in a manner that enables users to verify the proper function of the safety equipment in combination with all related components.

The below described proof-test procedures are recommended variants which could be performed after installation, configuration changes and within the required periodical proof-test interval derived from the safety instrument system engineering demands (e.g., 1oo1, 1oo2 or 2oo3 architecture) and related PFD_{AVG} calculations.

Proof Test 1

Which will detect approximately 70 % of possible dangerous failures.

Step	Test Action (consecutive steps)
1.	Bypass the safety function or take other appropriate action to avoid a false trip.
2.	Provide a 0 mA setpoint control signal to the positioner to open/close the valve and verify that the valve is open/closed as expected.
3.	Provide a 4 mA setpoint control signal to the positioner to open/close the valve and verify that the valve is open/closed as expected and that the internal digitalized control signal via HART corresponds to the provided setpoint control signal.
4.	Provide a 20 mA setpoint control signal to the positioner to open/close the valve and verify that the valve is open/closed as expected and that the internal digitalized control signal via HART corresponds to the provided setpoint control signal.
5.	Restore the loop to full operation.
6.	Restore normal operation.

Proof Test 2

Which will detect approximately 95% of possible dangerous failures

Step	Test Action (consecutive steps)
1.	Bypass the safety function or take other appropriate action to avoid a false trip.
2.	Perform Proof Test 1.
3.	Start the ´automatic adjustment´ procedure of the positioner and verify the correct result messages
4.	Restore the loop to full operation.
5.	Restore normal operation.

Notes on partial valve stroke testing
The described test procedures 1 and 2 are both performing full stroke testing.

- Partial stroke testing in moving only a partial valve range can provide a diagnostic coverage on failures resulting from blocking, coupling & broken springs but cannot completely proof, that the demanded process valve open/close position can be reached.

Repair & Replacement

In case of detected failures, corrective actions may be demanded.
Possible safety critical failures shall be reported to the ABB Customer service center.
Defective positioners send to ABB for repair or failure analysis should include information's about the operation context, the failure effect, the safety application and the environmental conditions.

Address for the return:

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

9 Installation, Commissioning and Configuration

The positioner shall be installed, configured, commissioned and maintained by personnel with trained knowledge of positioner applications in general, the specific knowledge on the related functional safety application and the specific knowledge of this safety manual and applicable documentation content referenced within chapter **Other relevant documents** on page 4 of this safety manual.

Any configuration, installation or repair change may affect the safety function of the positioner.

Therefore, the safety function shall be checked again after configuration, installation, or repair change in using the described ´Proof-Test´ or equivalent procedures.

The constraints and limitations as provided within the operating instruction and data sheet as referenced within chapter **Other relevant documents** on page 4 must be considered by the end user.

10 Product identification

Device

Type	Description	HW Version
TZIDC	Digital Positioner	05.xx
TZIDC-200	Digital Positioner with flameproof enclosure	05.xx

Output / Safe Position: Single acting, fail safe

For safety applications, the software is a “Not Part” element.

SIL marking

The order variant ´SIL - Declaration of Conformity´ is marked with a SIL logo on the name plate as specified within the Chapter ´Product Identification´ of the referenced operating instruction.

11 FMEDA failure data

This chapter provides the summary of the probabilistic estimation on failure data according **'FMEDA Report ABB 07/07-40 R016 Version V1, Revision R0'** (Exida.com GmbH).

The failure rates were chosen to match operating stress conditions of an industrial field environment similar to IEC 60654-1 class C. It is expected that the final number of field failures will be less than the number by these failure rates.

Some industrial plant sites have high levels of operational & environmental stress conditions.
Under those conditions the failure rate data might be higher and shall be adjusted to higher values to account for the specific conditions of the plant.
The end user of these numbers is responsible for determining their applicability to the final plant environment.
Accurate plant specific data may be used for this purpose.
If the data collected from the operational use within the specific plant environment or from a suitable proof testing reporting system indicates higher failure rates, the higher numbers shall be used.

Failure category	Failure Rates (in FIT*)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	651
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Undetected (λ_{DU})	**40**
SFF (Safe Failure Fraction)	94%
Total failure rate (safety function)	691
MTBF = MTTF + MTTR (safety function)	165 years

* FIT = Failures per 10^9 operation hours

Assumptions & Constraints

- Failure rates are constant, wear out mechanism are not included
- The positioner is operated with instrumented air that is free of oil, water and dust according to DIN/ISO 8573-1 (purity and oil content should meet the requirements according to Class 3, pressure dew point 10 K below the operating temperature).
- The electronics, firmware, position measurement, optional digital input, digital and analog outputs are not considered to be part of the safety function.
- The failure rates are valid for 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.
- The ambient temperature and humidity levels are within the data sheet ratings.
- The positioner is operated in the low demand mode of safety operation.
- The MTTR (Mean Time to Restoration) is assumed to 8 hours.

12 PFD_{AVG} calculation

The PFD_{AVG} calculation must be done based on certain important variables including:

① Failure Rates and Failure Modes
② Redundancy Architecture incl. Common Cause Failures
③ Proof-Test Coverage, Proof-Test Interval, Proof-Test Duration
④ Mission Time (planned total operating time before replacement)
⑤ Operational/Maintenance Capability
⑥ Mean Time to Repair

As only ① is under control of the device manufacturer, it is the responsibility of the SIS designer to perform the PFD_{AVG} calculations for the final assembled SIS in order to determine suitability for the demanded Safety Integrity Level (SIL).

Accordingly, the PFD_{AVG} and the Architectural constraints (in terms of HFT & SFF) must be verified for each application by the end user and the positioner must be properly designed into the target safety instrumented function.

For SIL 2 applications, the PFD_{AVG} of the complete safety function needs to be < $1.00E^{-02}$.

A generally accepted distribution of the PFD_{AVG} values over sensor part, logic solver part and final elements assumes that 50 % of the total PFD_{AVG} values is caused be the final element. However, as the positioner is only one part of the final element it should not claim more that 20 % of the PFD_{AVG} range.

Therefore, for a SIL 2 application the positioners maximum PFD_{AVG} value would be $2.00E^{-03}$.

In assuming a mission time of 10 years, a Mean Time to Restoration of 8 hours and a proof-test coverage of 95 % (see **Periodic Proof-Test and Maintenance** on page 9) the resulting PFD_{AVG} values are shown in the table below.

PFD_{AVG} values for variety of proof-test intervals (T_{Proof})		
T_{Proof} = 1 year	T_{Proof} = 5 years	T_{Proof} = 10 years
$PFD_{AVG} = 2.59E^{-04}$	$PFD_{AVG} = 9.25E^{-04}$	$PFD_{AVG} = 1.76E^{-03}$

This means, the PFD_{AVG} for all selected Proof-Test Intervals are within the allowed range of SIL 2.

Notes

Notes

Notes

ABB Measurement & Analytics

For your local ABB contact, visit:
www.abb.com/contacts

For more product information, visit:
www.abb.com/positioners

3KXE341001R4801

SM/TZIDC/TZIDC-200/SIL-EN Rev. G 04.2023