

Elektropneumatische Stellungsregler Electro-Pneumatic Positioner TZIDC / TZIDC-200 und Shutdown Modul für TZIDC / TZIDC-200 and Shutdown Module for TZIDC / TZIDC-200

D Elektropneumatische Stellungsregler TZID / TZIDC-200
und Shutdown Modul für TZIDC / TZIDC-200
Hinweise zur funktionalen Sicherheit
SIL – Sicherheitshinweise

GB Electro-Pneumatic Positioner TZID / TZIDC-200
and Shutdown Module for TZIDC / TZIDC-200
Instructions for Functional Safety
SIL – Safety Instructions



Inhalt / Content

Seite / Page

D Deutsch	3
GB English	11
Anhang/Appendix 1: Management Summary	19

Inhalt	Seite
1 Anwendungsbereich	4
2 Abkürzungen	4
3 Relevante Normen	4
4 Begriffe	5
5 Bestimmung des Safety Integrity Level (SIL)	5
6 Sicherheitsbezogenes System	5
7 Angaben für die Sicherheitsfunktion	7
8 Mitgeltende Gerätedokumentationen	8
9 Verhalten im Betrieb und bei Störung	8
10 Wiederkehrende Prüfungen	8
11 Einstellungen	9
11.1 Verriegeln/Entriegeln	9
12 Sicherheitstechnische Kenngrößen	9
12.1 Annahmen	9
12.2 Spezifische sicherheitstechnische Kenngrößen	9
13 SIL-Konformitätserklärung	10

1 Anwendungsbereich

Zur Stellungsregelung an Armaturen mit pneumatischen Antrieben, welche den besonderen Anforderungen der Sicherheitstechnik bis SIL 2 nach IEC 61508 / IEC 61511-1 genügen sollen.

Es handelt sich dabei um einfachwirkende, entlüftende ABB Stellungsregler Typ TZIDC / TZIDC-200 und pneumatische Antriebe mit Federrückstellung. Bei Ausfall der Hilfsenergie (elektrisch bzw. pneumatisch) oder bei einem Fehler im Stellungsregler entlüftet der Stellungsregler den Antrieb und die Feder im Antrieb fährt die Armatur in eine vorbestimmte, sichere Endlage (AUF oder ZU).

Die Stellungsregler erfüllen folgende Anforderungen:

- Funktionale Sicherheit gemäß IEC 61508/IEC 61511-1
- Explosionsschutz (je nach Version)
- Elektromagnetische Verträglichkeit nach EN 61000

2 Abkürzungen

Abkürzung	Englisch	Deutsch
HFT	Hardware Fault Tolerance	Hardware Fehlertoleranz Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen.
MTBF	Mean Time Between Failures	mittlere Zeitdauer zwischen zwei Ausfällen
MTTR	Mean Time To Repair	mittlere Zeitdauer zwischen dem Auftreten eines Fehlers in einem Gerät oder System und der Reparatur
PFD	Probability of Failure on Demand	Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall
PFD _{av}	Average Probability of Failure on Demand	mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall
SIL	Safety Integrity Level	Die internationale Norm IEC 61508 definiert vier diskrete Safety Integrity Level (SIL 1 bis SIL 4). Jeder Level entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion. Je höher der Safety Integrity Level der sicherheitsbezogenen Systeme ist, um so geringer ist die Wahrscheinlichkeit, dass sie die geforderten Sicherheitsfunktionen nicht ausführen.
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle. Anteil von Ausfällen ohne Potential, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.
FIT	Failure In Time	1*10 ⁹ Fehler pro Stunde
TI	Test Interval between life testing of the safety function	Prüfintervall zwischen Funktionstests der Schutzfunktion
XooY	"X out of Y" Voting (e.g. 2oo3)	Klassifizierung und Beschreibung des sicherheitsbezogenen Systems hinsichtlich Redundanz und angewandtem Auswahlverfahren. „Y“ gibt an, wie oft die Sicherheitsfunktion ausgeführt wird (Redundanz). „X“ bestimmt, wieviele Kanäle korrekt arbeiten müssen. Beispiel Druckmessung: 1oo2-Architektur. Ein sicherheitsbezogenes System entscheidet, dass eine vorgegebene Druckgrenze überschritten ist, wenn einer von zwei Drucksensoren diese Grenze erreicht. Bei einer 1oo1-Architektur ist nur ein Drucksensor vorhanden.

3 Relevante Normen

Norm	Englisch	Deutsch
IEC 61508, Teil 1 bis 7	Functional safety of electrical/electronic/programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (Zielgruppe: Hersteller und Lieferanten von Geräten)
IEC 61511, Teil 1	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)	Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie (Zielgruppe: Planer, Errichter und Nutzer)

4 Begriffe

Begriff	Erklärung
gefahrbringender Ausfall	Ausfall mit dem Potenzial, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu versetzen.
sicherheitsbezogenes System	Ein sicherheitsbezogenes System führt die Sicherheitsfunktionen aus, die erforderlich sind, um einen sicheren Zustand z.B. in einer Anlage zu erreichen oder aufrechtzuerhalten. Beispiel: Druckmessgerät - Logikeinheit (z.B. Grenzsinalgeber) - Ventil bilden ein sicherheitsbezogenes System..
Sicherheitsfunktion	Definierte Funktion, die von einem sicherheitsbezogenen System ausgeführt wird, mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalles, einen sicheren Zustand für die Anlage zu erreichen oder aufrechtzuerhalten. Beispiel: Grenzdrucküberwachung

5 Bestimmung des Safety Integrity Level (SIL)

Der erreichbare Safety Integrity Level wird durch folgende sicherheitstechnischen Kenngrößen bestimmt:

- mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall (PFD_{av})
- Hardware Fehlertoleranz (HFT) und
- Anteil ungefährlicher Ausfälle (SFF).

Die spezifischen sicherheitstechnischen Kenngrößen für den TZIDC / TZIDC-200 und das Shutdown Modul, als Teil der Sicherheitsfunktion, sind im Kapitel "Sicherheitstechnische Kenngrößen" aufgeführt.

Die folgende Tabelle zeigt die Abhängigkeit des "Safety Integrity Level" (SIL) von der mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion des gesamten sicherheitsbezogenen Systems" (PFD_{av}). Dabei wird der "Low demand mode" betrachtet, d.h. die Sicherheitsfunktion wird maximal einmal im Jahr geprüft.

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 Sicherheitsbezogenes System

Sensor, Logikeinheit und Aktor (Stellungsregler, pneumatischer Antrieb und Armatur) bilden zusammen ein sicherheitsbezogenes System, das eine Sicherheitsfunktion ausführt. Die "mittlere Wahrscheinlichkeit gefahrbringender Ausfälle des gesamten sicherheitsbezogenen Systems" (PFD_{av}) teilt sich üblicherweise auf die Teilsysteme Sensor, Logikeinheit und Aktor gemäß Bild 6-1 auf.

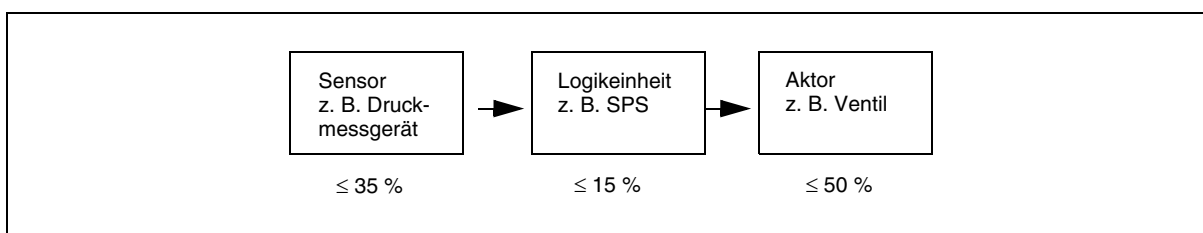


Bild 6-1 Übliche Aufteilung der „mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall“ (PFD_{av}) auf die Teilsysteme



Hinweis!

Diese Dokumentation behandelt die elektropneumatischen Stellungsregler TZIDC, TZIDC-200 und das Shutdown Modul für die Stellungsregler als Teil einer Sicherheitsfunktion.

Die folgende Tabelle zeigt den erreichbaren „Safety Integrity Level“ (SIL) des gesamten sicherheitsbezogenen Systems für Systeme vom Typ B abhängig vom „Anteil ungefährlicher Ausfälle“ (SFF) und der „Hardware Fehlertoleranz“ (HFT). Systeme vom Typ B sind z. B. Sensoren und Stellungsregler mit komplexen Komponenten wie z. B. Mikroprozessoren (siehe auch IEC 61508, Teil 2).

Anteil ungefährlicher Ausfälle	Hardware Fehlertoleranz (HFT)		
	0	1 (0) ¹⁾	2 (1) ¹⁾
< 60 %	nicht erlaubt	SIL 1	SIL 2
60...< 90 %	SIL 1	SIL 2	SIL 3
90...< 99 %	SIL 2	SIL 3	–
≥ 99 %	SIL 3	–	–

1) Nach IEC 61511-1, Abschnitt 11.4.3, kann bei Sensoren und Aktoren mit komplexen Komponenten die „Hardware Fehlertoleranz“ (HFT) um eins reduziert werden (Werte in Klammern), wenn für das Gerät folgende Bedingungen zutreffen:

- Das Gerät ist betriebsbewährt.
- Der Anwender kann nur prozessbezogene Parameter konfigurieren, z. B. Messbereich, Signalrichtung im Fehlerfall usw.
- Die Konfigurationsebene der Firmware ist geschützt.
- Die Funktion hat einen geforderten „Safety Integrity Level“ (SIL) von weniger als 4.

Alle Bedingungen treffen für den Stellungsregler TZIDC / TZIDC-200 und das Shutdown Modul zu.

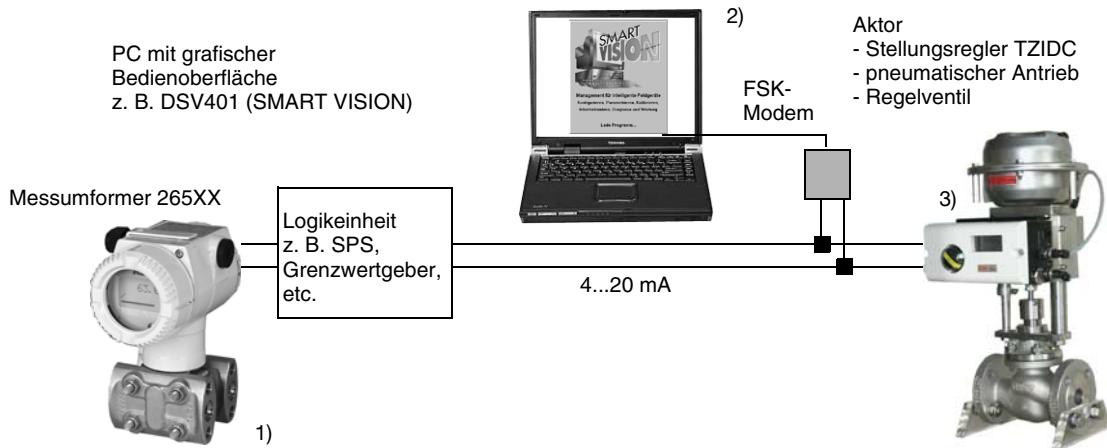


Bild 6-2 Beispiel: Sicherheitsfunktion "Grenzdrucküberwachung" mit Stellungsregler TZIDC als Teilsystem

- 1 265xx mit Vor-Ort-Bedienung, Möglichkeit zur Einstellung von Messanfang und -ende sowie Dämpfung
- 2 Computer mit Bedienoberfläche z.B. Smart Vision zur Inbetriebnahme, Konfiguration, Parametrierung und Auslesen / Speichern / Schreiben der Gerätedaten.
- 3 Pneumatischer Stellungsregler TZIDC mit Vor-Ort-Bedienmöglichkeit zur Inbetriebnahme, Konfiguration und Parametrierung

Funktionsbeschreibung

Der Messumformer erzeugt ein dem Prozess proportionales analoges Signal (4...20 mA). Es wird einer nachgeschalteten Logikeinheit z.B. einer SPS oder Grenzsignalgeber zugeführt und dort auf das Überschreiten eines eingestellten Grenzwertes überwacht.

Zusätzlich werden zur Störüberwachung in der Logikeinheit die HI / LO-Alarme des Messumformers (> 20 mA / < 4 mA) ausgewertet.

Entsprechend den Erfordernissen der Anlagesicherheit wird im Störfall von der Logikeinheit ein Stellsignal (4...20 mA) an den Stellungsregler ausgegeben, um das Ventil in die sichere Position zu verstellen.

Bei Ausfall der Hilfsenergie (Druckluft oder 20 mA) oder Gerätefehler entlüftet das Pneumatikmodul im Stellungsregler den Antrieb und die darin eingebaute Feder fährt die Armatur in eine vorbestimmte Endlage (AUF oder ZU).

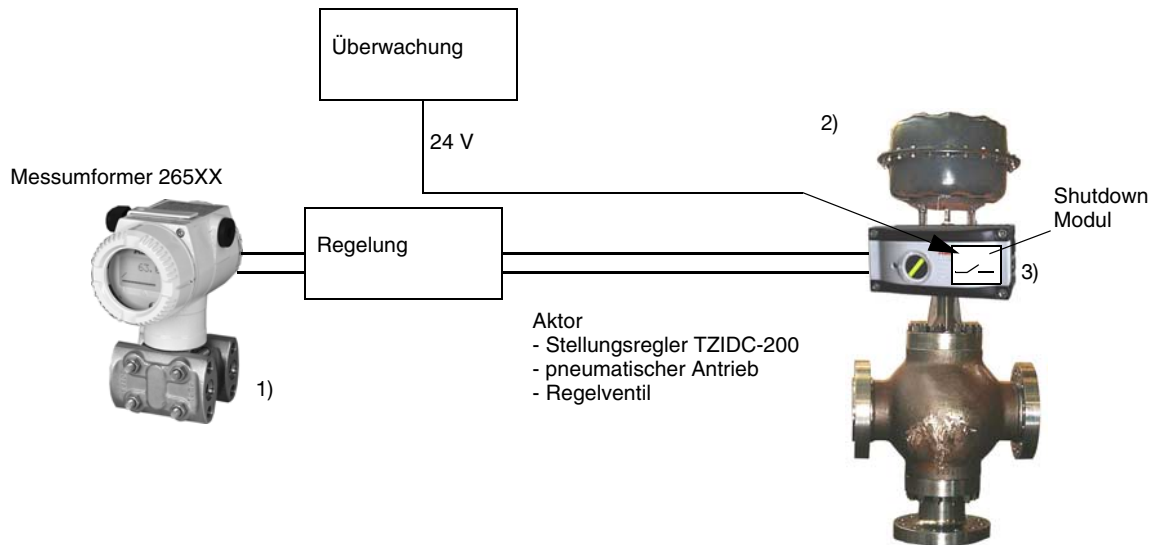


Bild 6-3 Sicherheitsfunktion "Systemunabhängige Anlagenüberwachung" mit Stellungsregler TZIDC-200 und Shutdown Modul als Teilsysteme

- 1) 265xx mit Vor-Ort-Bedienung, Möglichkeit zur Einstellung von Messanfang und -ende sowie Dämpfung
- 2) Pneumatischer Stellungsregler TZIDC mit Vor-Ort-Bedienmöglichkeit zur Inbetriebnahme, Konfiguration und Parametrierung.
- 3) Im Stellungsregler eingebautes Shutdown Modul zum Entlüften des pneumatischen Antriebes. Die Ansteuerung des Moduls erfolgt unabhängig vom Regelsystem.

Funktionsbeschreibung

Die Ansteuerung des Shutdown Modul ist vom übrigen Stellungsregler galvanisch getrennt. Daher ist es einem Überwachungssystem möglich, unabhängig vom Regelsystem, auf das Stellgerät einzuwirken.

Bei Wegfall der separat eingespeisten 24 V DC für das Shutdown Modul wird die Versorgung des I/P-Wandlers im Stellungsregler unterbrochen und entlüftet daraufhin den pneumatischen Antrieb, der dann federgetrieben die Armatur in eine sichere Endlage (AUF oder ZU) fährt.

Die Hauptplatine im Stellungsregler einschließlich Kommunikation und Rückmeldungen ist weiterhin aktiv, da sie über das analoge Sollwertsignal gespeist wird.

7 Angaben für die Sicherheitsfunktion

Achtung!

Die verbindlichen Einstellungen und Angaben für die Sicherheitsfunktionen sind in den Kapiteln „Einstellungen“ und „Sicherheitstechnische Kenngrößen“ aufgeführt.



Für die Reaktionszeit des Messumformers siehe Datenblatt.

Hinweis!

Sicherheitsbezogene Systeme ohne selbstverriegelnde Funktion müssen nach Ausführung der Sicherheitsfunktion innerhalb MTTR (8 Stunden) in einen überwachten oder anderweitig sicheren Zustand gebracht werden.



Die Lebensdauer der Geräte ist entsprechend den angegebenen Werten für die MTBF zu beurteilen.

8 Mitgeltende Gerätedokumentationen

Für den Stellungsregler TZIDC und das Shutdown Modul ist die Betriebsanleitung 41/18-79 DE und die Konfigurations- und Parametrieranleitung 45/18-79 DE zu beachten.

Für den Stellungsregler TZIDC-200 und das Shutdown Modul ist die Betriebsanleitung 42/18-80 DE und die Konfigurations- und Parametrieranleitung 45/18-80 DE zu beachten.

9 Verhalten im Betrieb und bei Störung

Hinweis!

Das Verhalten im Betrieb und bei Störung wird in der Betriebsanleitung beschrieben.



10 Wiederkehrende Prüfungen

Überprüfung der Sicherheit

Die Sicherheitsfunktion des gesamten Sicherheitskreises ist gemäß IEC 61508/61511 regelmäßig zu prüfen. Die Testintervalle werden u.a. bei der Berechnung jedes einzelnen Sicherheitskreises einer Anlage (PFDav's) bestimmt.

Überprüfung der Funktion

Jährlich ist die Funktionsfähigkeit des Stellungsreglers in der Anwendung zu prüfen. Dabei ist wie folgt zu verfahren:

- Sollwert 4 mA vorgeben, überprüfen ob die Armatur in die entsprechende Endlage fährt. Gleichzeitig über HART-Kommunikation die internen, digitalisierten Werte für Sollwert und Position auslesen.
- Sollwert 20 mA vorgeben, überprüfen ob die Armatur in die entsprechende Endlage fährt. Gleichzeitig über HART-Kommunikation die internen, digitalisierten Werte für Sollwert und Position auslesen.
- Manuell einen Selbstabgleich des Stellungsreglers starten. (Genaue Beschreibung in entsprechender Konfigurations- und Parametrieranweisung)
 - Aus der Arbeitsebene in die Konfigurationsebene wechseln. Dort den Parameter 1.1 wählen und manuell den Selbstabgleich starten.
 - Wenn erfolgreich, ist es nicht erforderlich zu Speichern, da mit dem Selbstabgleich nur die Regelfunktion und das dynamische Verhalten getestet wird.

Der Stellungsregler selbst ist wartungsfrei. Art und Umfang von weiteren empfohlenen Prüfungen sind in den entsprechenden Betriebsanleitungen im Kapitel "Funktionstest / Wartung" beschrieben

Reparatur

Defekte Geräte sind, möglichst mit Angabe der Störung und Ursache, an die Reparaturabteilung einzusenden. Bei Bestellung von Ersatzgeräten bitte die Seriennummer (auf dem Typenschild) des Originalgeräts angeben

Anschrift:

ABB Process Industries

Abteilung SPM

Schillerstraße 72

32425 Minden

DEUTSCHLAND

11 Einstellungen

Mit den Tasten am Gerät oder über eine Bedienoberfläche z.B. DSV401 (Smart Vision) kann ein Standard-Selbstabgleich gestartet werden, bei dem der Stellungsregler an den Arbeitsbereich der Armatur abgeglichen wird und die Regelparameter, Wirkrichtung der Feder und Nullpunkt ermittelt werden.

Weiter können Funktionen ausgewählt und Parameter der Anwendung entsprechend verändert werden.

11.1 Verriegeln/Entriegeln

Hinweis!

Die Stellungsregler TZIDC / TZIDC-200 sind standardmäßig mit einer Funktion ausgestattet, um gegen ungewollte und unbefugte Veränderungen/Bedienung zu schützen.



- Hierzu sind am Binäreingang DI (Klemmen + 81 / - 82) 24 V DC anzulegen, das Gerät über die Tastatur in den Konfigurations-Mode zu schalten, die Parametergruppe 10 zu wählen und unter - P10.0, FUNCTION - "LOCK_ALL" zu wählen und zu speichern. (Genaue Beschreibung in entsprechender Konfigurations- und Parametrieranweisung)
- Nach Entfernen der 24V Versorgung ist die Bedienung und jegliche Konfiguration über Tasten oder Bedienoberfläche gesperrt.
- Die Verriegelung kann nur durch Anlegen einer 24V-Versorgung wieder aufgehoben oder geändert werden.

Teilweise Sperrung von Funktionen ist auch möglich. Genaue Beschreibung in entsprechender Konfigurations- und Parametrieranweisung.

12 Sicherheitstechnische Kenngrößen

12.1 Annahmen

- Kommunikation mit HART Protokoll wird nur verwendet um das Gerät zu konfigurieren, zu kalibrieren oder für Diagnosefunktionen aber nicht für sicherheitstechnisch kritische Operationen.
- Im Störfall wird der pneumatische Ausgang des Stellungsreglers TZIDC / TZIDC-200 entlüftet und eine Feder im pneumatischen Antrieb fährt die Armatur in eine vordefinierte Endlage.
- Das Stellsignal 4 ... 20 mA für den Stellungsregler TZIDC / TZIDC-200 kommt von einem SIL2 sicheren System.
- Die pneumatische Hilfsenergie ist frei von Öl, Wasser und Staub nach DIN/ISO 8573-1.
- Die zyklische Abarbeitung der Eigendiagnose ist innerhalb einer Stunde abgeschlossen und wird dann automatisch wieder neu gestartet.
- Die Reparaturzeit (MTTR) nach einem Gerätefehler beträgt 8 Stunden
- Die mittlere Temperatur über einen langen Zeitraum betrachtet beträgt 40°C
- Der Stellungsregler wird nur in Anwendungen mit niedriger Anforderungsrate eingesetzt (low demand mode)
- Ein gefahrbringender Ausfall des Stellungsreglers ist ein Ausfall, bei dem der Druckausgang auf das Eingangssignal nicht mehr reagiert bzw. die Position um mehr als 2% vom eingestellten Toleranzband abweicht.

12.2 Spezifische sicherheitstechnische Kenngrößen

Gerät	Kategorie	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TZIDC TZIDC-200	SIL2	85 %	$6,89 \times 10^{-4}$	925 FIT	157 FIT
Shutdown Modul für TZIDC / TZIDC-200	SIL2	94 %	$1,76 \times 10^{-4}$	718 FIT	40 FIT
		Anteile ungefährlicher Ausfälle	Mittlere Wahrscheinlichkeit gefahrbringender Ausfälle	Fehlerrate gefährliche entdeckte und sichere Fehler	Fehlerrate gefährliche unentdeckte Fehler

Wichtig:

Die in der oben dargestellten Tabelle genannten PFDav-Werte beziehen sich nur auf die Stellungsregler TZIDC/ TZIDC-200 bzw. das Shutdown Modul.

Weitere Detailinformationen siehe Management Summary im Anhang.

13 SIL-Konformitätserklärung

49/18-79DE
Rev. B



SIL-KONFORMITÄTSERKLÄRUNG

Hersteller: ABB Automation Products GmbH
Adresse: Schillerstraße 72 - D-32425 Minden
Produkt: Stellungsregler TZIDC – TZIDC-200 (4...20 mA) und Shutdown Modul

Funktionale Sicherheit nach IEC 61508 / IEC 61511

Wir erklären als Hersteller, dass die o.g. Geräte für den Einsatz in einer sicherheitsrelevanten Anwendung bis einschließlich SIL 2 entsprechend der IEC 61511-1 geeignet sind, wenn beiliegende Sicherheitshinweise beachtet werden.

Die Analyse der sicherheitskritischen und gefährlichen Zufallsfehler liefert unter der Annahme einer jährlichen Funktionsprüfung folgende Parameter:

SIL (Sicherheitsintegritätslevel): 2 **Typ:** B
HFT (Hardwarefehlertoleranz): 0¹⁾ (einkanalige Verwendung)

Produkt	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TZIDC / TZIDC-200	85%	$6,89 * 10^{-4}$	925 FIT	157 FIT
TZIDC / TZIDC-200 mit Shutdown Modul	94%	$1,76 * 10^{-4}$	718 FIT	40 FIT

1) gemäß Kapitel 11.4 der IEC 61511

Im Rahmen des Nachweises der Betriebsbewährtheit wurde das Gerät einschließlich des Änderungs wesens beurteilt.

14.09.2007
Datum


Dr. Wolfgang Scholz
Leiter Entwicklung


Manfred Klüppel
Leiter Qualitätssicherung

Content	Page
1 Field of application	12
2 Acronyms and abbreviations	12
3 Relevant standards	12
4 Terms and definitions	13
5 Determination of the Safety Integrity Level (SIL)	13
6 Safety-related system	13
7 Specifications for the safety function	15
8 Applicable device documentation	16
9 Behavior during operation and in case of malfunction	16
10 Periodic checks	16
11 Settings	17
11.1 Locking/Unlocking	17
12 Safety-related characteristics	17
12.1 Assumptions	17
12.2 Specific safety-related characteristics	17
13 SIL conformity declaration	18

1 Field of application

Positioning of valves with pneumatic actuators that shall meet the special safety requirements of SIL 2 in accordance with IEC 61508 / IEC 61511-1.

The devices are single-acting, depressurizing ABB positioners of type TZIDC / TZIDC-200 and pneumatic actuators with spring-return mechanism. In case of a failure of electrical power or compressed air supply or when a positioner malfunction occurs, the positioner depressurizes the actuator, and the return spring in the actuator moves the valve to a pre-defined, safe end position (either OPEN or CLOSED).

The positioners meet the requirements regarding

- functional safety in accordance with IEC 61508/IEC 61511-1
- explosion protection (depending on the version)
- electromagnetic compatibility in accordance with EN 61000

2 Acronyms and abbreviations

Acronym / Abbreviation	Designation	Description
HFT	Hardware Fault Tolerance	The hardware fault tolerance of the device. This is the capability of a functional unit to continue the execution of the demanded function in case of faults or deviations.
MTBF	Mean Time Between Failures	This is the mean time period between two failures.
MTRR	Mean Time To Repair	This is the mean time period between the occurrence of a failure in a device or system and its repair.
PFD	Probability of Failure on Demand	This is the likelihood of dangerous safety function failures occurring on demand.
PFD _{av}	Average Probability of Failure on Demand	This is the average likelihood of dangerous safety function failures occurring on demand.
SIL	Safety Integrity Level	The international standard IEC 61508 specifies four discrete safety integrity levels (SIL 1 to SIL 4). Each level corresponds to a specific probability range regarding the failure of a safety function. The higher the safety integrity level of the safety-related systems, the lower the likelihood of non-execution of the demanded safety functions.
SFF	Safe Failure Fraction	The fraction of non-hazardous failures, i.e. the fraction of failures without the potential to set the safety-related system to a dangerous or impermissible state.
FIT	Failure In Time	1*10 ⁹ failures per hour
TI	Test interval between life testing of the safety function	Time interval between the functional tests of the safety function.
XooY	"X out of Y" Voting (e.g. 2oo3)	Classification and description of the safety-related system regarding redundancy and the selection procedure used. "Y" indicates how often the safety function is carried out (redundancy). "X" determines how many channels must work properly. Example (pressure measurement): 1oo2 architecture. When one out of two pressure sensors reaches a defined limit value, a safety-related system decides, that the pressure limit has to be considered as exceeded. In a system with a 1oo1 architecture only one pressure sensor exists.

3 Relevant standards

Standard	Designation
IEC 61508, Part 1 to 7	Functional safety of electrical/electronic/programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)
IEC 61511, Part 1	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)

4 Terms and definitions

Terms	Definitions
Dangerous failure	Failure with the potential to set the safety-related system to a dangerous or inoperative state.
Safety-related system	A safety-related system carries out the safety functions needed to establish or maintain a safe state e.g. in a plant. Example: A pressure gauge, a logic unit (e.g. limit signal transmitter) and a valve form a safety-related system.
Safety function	A defined function carried out by a safety-related system in order to establish or maintain a safe state of the plant under consideration of a specified dangerous incident. Example: Pressure limit monitoring

5 Determination of the Safety Integrity Level (SIL)

The reachable safety integrity level depends on the following safety-related characteristics:

- Average probability of failure on demand (PFD_{av})
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF).

The specific safety-related characteristics for the TZIDC / TZIDC-200 positioner and its shutdown module as a part of the safety function are detailed in chapter "Safety-related characteristics".

The following table shows the dependence of the safety integrity level (SIL) on the average probability of failure on demand (PFD_{av}). The "Low demand mode" is considered here. In this mode, the safety function is checked 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

The sensor, the logic unit and the final control element (positioner, pneumatic actuator and valve) form together a safety-related system which carries out a safety function. The average propability of failure on demand (PFD_{av}) is usually distributed over the subsystems (sensor, logic unit and final control element) as seen in Fig. 6-1.

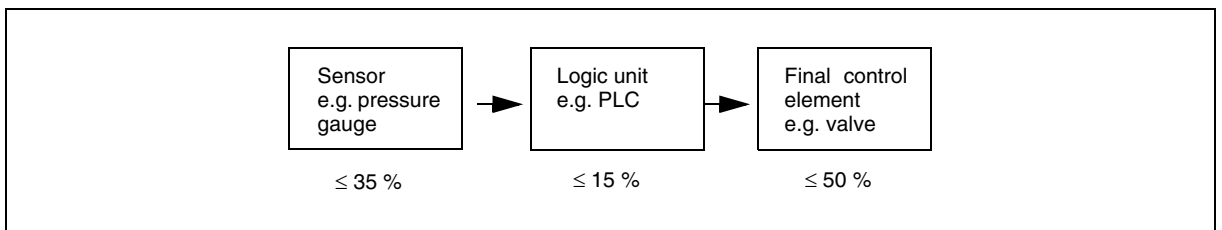


Fig. 6-1 Normal distribution of the average probability of failure on demand (PFD_{av}) over the subsystems



Note!

This documentation applies to the electro-pneumatic positioners TZIDC, TZIDC-200 and their shutdown module as part of a safety function.

The following table shows the reachable safety integrity level (SIL) of the entire safety-related system for systems of type B, depending on the safe failure fraction (SFF) and the hardware fault tolerance (HFT). Systems of type B are e.g. sensors and positioners with complex components like microprocessors (see also IEC 61508, Part 2).

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1 (0) ¹⁾	2 (1) ¹⁾
< 60 %	impermissible	SIL 1	SIL 2
60...< 90 %	SIL 1	SIL 2	SIL 3
90...< 99 %	SIL 2	SIL 3	–
≥ 99 %	SIL 3	–	–

¹⁾ Acc. to IEC 61511-1, Part 11.4.3, the hardware fault tolerance (HFT) of sensors and final control elements with complex components can be decreased by one (value in brackets), if the following requirements are met:

- The device is proven-in-field.
- The user can only configure process-related parameters like the measuring range, signal direction in case of fault, etc.
- The firmware configuration level is access-protected.
- The function has a required safety integrity level (SIL) of less than 4.

TZIDC / TZIDC-200 positioners and their shutdown module meet all requirements.

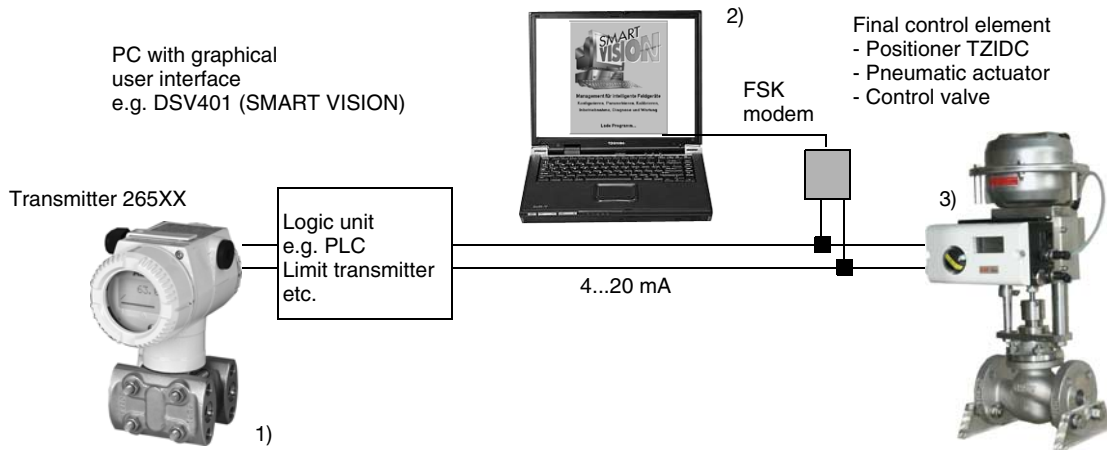


Fig. 6-2 Example: Safety function “Pressure limit monitoring” with the positioner TZIDC as a subsystem

- 1 265xx with local operation option and adjustable lower and upper range value and damping
- 2 Computer with user interface like Smart Vision, for commissioning, configuring and parameter setting and for reading/saving/writing device data.
- 3 Electro-pneumatic positioner TZIDC, with local operation option for commissioning, configuring and parameter setting

Functional description

The transmitter produces an analog signal (4...20 mA) proportional to the process. This signal is fed to a subsequent logic unit, e.g. a PLC or limit transmitter, and monitored for violation of a defined limit value.

Additionally, the HI / LO alarms from the transmitter (> 20 mA / < 4 mA) are evaluated in the logic unit, in order to allow for malfunction detection.

According to the plant safety requirements, the logic unit outputs a corrective signal (4...20 mA) to the positioner in case of a malfunction, in order to move the valve to its safe position.

In case of an energy supply failure (compressed air or 20 mA) or device malfunction, the pneumatic module in the positioner depressurizes the actuator, and the return spring in the actuator moves the valve to its predefined end position (OPEN or CLOSED).

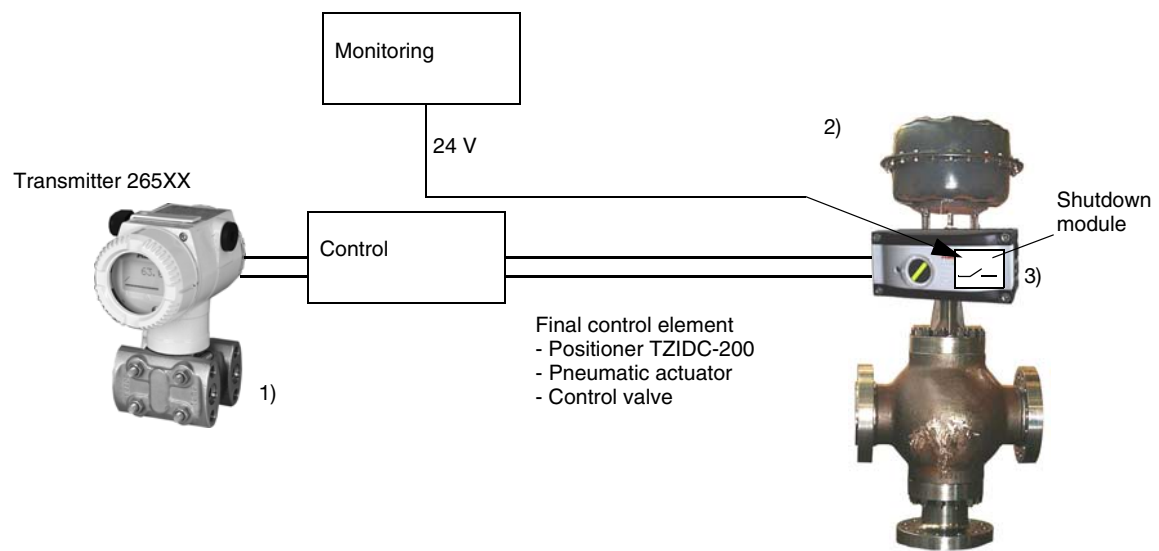


Fig. 6-3 Safety function "System-independent plant monitoring" with positioner TZIDC-200 and shutdown module as subsystems.

- 1) 265xx with local operation option and adjustable lower and upper range value and damping
- 2) Electro-pneumatic positioner TZIDC-200, with local operation option for commissioning, configuring and parameter setting
- 3) Shutdown module integrated in the positioner, for depressurizing the pneumatic actuator. The module is controlled independently of the process control system.

Functional description

Control of 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 should fail, the I/P module in the positioner is no longer powered and then depressurizes the pneumatic actuator. The actuator return spring moves the valve to a safe end position (OPEN or CLOSED).

The positioner motherboard as well as the communication and position feedback are still active, as their power is derived from the analog setpoint signal.

7 Specifications for the safety function

Caution!
Refer to chapters "Settings" and "Safety-related characteristics" of this document for the mandatory settings and specifications for the safety function.



See the relevant data sheet for the transmitter response time.



Note!
Safety-related systems without an auto-locking function must be set to a monitored or otherwise safe state within the MTTR (8 hours) after execution of the safe function.

The device lifecycle must be evaluated according to the specified MTBF.

8 Applicable device documentation

For the positioner TZIDC and the shutdown module the operating instructions 41/18-79 EN and the configuration and parameter setting instructions 45/18-79 EN must be observed.

For the positioner TZIDC and the shutdown module the operating instructions 42/18-80 EN and the configuration and parameter setting instructions 45/18-80 EN must be observed.

9 Behavior during operation and in case of malfunction

Note!

The behavior during operation and in case of malfunction is detailed in the operating instructions.



10 Periodic checks

Safety checks

The safety function of the entire safety loop must be checked on a regular basis in accordance with IEC 61508/61511. The check intervals are, among others, determined when calculating the individual safety loops of a plant (PFDavs).

Functional checks

The positioner's operativeness must be checked in the system on an annual basis. Proceed as follows:

- Apply the 4 mA setpoint signal and check that the valve moves to the respective end position. At the same time read the internal, digitized values for the setpoint and position via HART communication.
- Apply the 20 mA setpoint signal and check that the valve moves to the respective end position. At the same time read the internal, digitized values for the setpoint and position via HART communication.
- Manually start the autoadjustment function of the positioner (refer to the respective configuration and parameter setting instructions for details).
 - Change over from the operating level to the configuration level. Select parameter 1.1 and then manually start the autoadjustment function.
 - When the autoadjustment is executed successfully, it is not necessary to save the settings, as only the control function and the dynamic behavior are tested.

The positioner is virtually maintenance-free. The type and scope of other recommended tests are described in chapter "Functional test/maintenance" of the respective operating instructions.

Repair

Defective devices should be returned to the ABB service and repair department, possibly with the type of malfunction and possible reason stated. When ordering spare units please notify the serial number (on the type plate) of the original device.

Address:

ABB Process Industries

Department SPM

Schillerstrasse 72

D-32425 Minden

GERMANY

11 Settings

A standard autoadjustment can be started by using the front panel keys on the device or via the user interface, e.g. DSV401 (Smart Vision). The standard autoadjustment function automatically adapts the positioner to the valve operating range and determines the control parameters, spring action and zero point.

Additionally, it is possible to select functions and edit some parameters according to the application.

11.1 Locking/Unlocking

Note!

A special lock function protects the positioners TZIDC / TZIDC-200 against unwanted or unauthorized manipulation/control.



- To activate this lock function, apply 24 V DC to the digital input DI (terminals + 81 / - 82), set the device to the configuration mode by using the front panel keys, select parameter group 10 and under - P10.0, FUNCTION - "LOCK_ALL" and then save this setting (refer to the respective configuration and parameter setting instructions for details).
- When interrupting the 24 V DC power supply, local operation and any configuration via the local operator panel and via the user interface is disabled.
- The lock can only be undone or modified by applying a 24 V DC voltage again.

Partial locks for specific functions are also possible (refer to the respective configuration and parameter setting instructions for details).

12 Safety-related characteristics

12.1 Assumptions

- HART communication is only used for configuring, adjusting or diagnosing the device, but not for safety-relevant critical operations.
- In case of a malfunction, 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 4 ... 20 mA input signal for the TZIDC / TZIDC-200 positioner comes from a safe system with SIL2.
- The compressed air supplied to the positioner as the pneumatic energy is free of oil, water and dust in accordance with DIN/ISO 8573-1.
- Cyclic self-diagnosis is executed within one hour and is automatically restarted.
- The medium time to repair (MTTR) after a device failure is 8 hours.
- The long-time average temperature is 40°C.
- The positioner is only used for low demand mode applications.
- A dangerous positioner failure is a failure where the pressure output does no longer respond to the input signal or where the position deviation from the defined tolerance band is more than 2%.

12.2 Specific safety-related characteristics

Device	Category	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TZIDC TZIDC-200	SIL2	85 %	6.89×10^{-4}	925 FIT	157 FIT
Shutdown module for TZIDC / TZIDC-200	SIL2	94 %	1.76×10^{-4}	718 FIT	40 FIT
		Safe failure fraction	Average probability of dangerous failures	Failure rate of detected dangerous and of safe failures	Failure rate of undetected dangerous failures

Important:

The PFDav values stated in the table are valid for the positioner TZIDC/ TZIDC-200 and the shutdown module, only. For details refer to the management summary in the Appendix.

13 SIL conformity declaration

49/18-79EN
 Rev. B



SIL DECLARATION OF CONFORMITY

Manufacturer: ABB Automation Products GmbH
Adress: Schillerstraße 72 - D-32425 Minden
Product name: Positioner TZIDC – TZIDC-200 (4...20 mA) and Shutdown Modul

Functional safety according to IEC 61508 / IEC 61511

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 61511-1, 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: B**
HFT (Hardware failure tolerance): 0¹⁾ (one-channel application)

Product	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TZIDC / TZIDC-200	85%	$6,89 * 10^{-4}$	925 FIT	157 FIT
TZIDC / TZIDC-200 with Shutdown Modul	94%	$1,76 * 10^{-4}$	718 FIT	40 FIT

1) according to chapter 11.4 of IEC 61511

For the prior-use investigation the instrument including the modifications was analysed.

27.09.2007
 Date

Dr. Wolfgang Scholz
 Head of Research & Development

Manfred Klüppel
 Head of Quality Assurance

Anhang/Appendix 1: Management Summary



FMEDA and Proven-in-use Assessment

Project:
Intelligent Positioner TZIDC / TZIDC-200

Customer:
ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 03/09-13
Report No.: ABB 03/09-13 R003
Version V2, Revision R0, August 2007
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 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 intelligent positioner TZIDC / TZIDC-200 with software version V2.00. Table 1 gives an overview of the two possible 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 applications

Shutdown module
Smart positioner

For safety applications as a smart positioner only the 4.20 mA control input with the corresponding pressure output was considered. 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.

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 intelligent positioner TZIDC / TZIDC-200 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 intelligent positioner TZIDC / TZIDC-200 when working as a smart positioner is considered to be a Type B¹ component with a hardware fault tolerance of 0.

If only the shutdown module of the intelligent positioner TZIDC / TZIDC-200 is used then the device is considered to be a Type A² component. It consists of certain redundant parts but overall it is considered to be a device with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

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.

As the intelligent positioner TZIDC / TZIDC-200 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 ABB Automation Products GmbH. 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.

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

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



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 B intelligent positioner TZIDC / TZIDC-200 with a hardware fault tolerance of 0 and a SFF of 60% to < 90% are 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.

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.

Table 2: Summary for TZIDC / TZIDC-200 as smart positioner – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected	9
Fail Safe Undetected	831
Fail Dangerous Detected	11
Fail Dangerous Undetected	157
No Effect	70
Annunciation Undetected	4
Not part	250
MTBF = MTTF + MTTR	86 years

Table 3: Summary for TZIDC / TZIDC-200 as smart positioner – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
9 FIT	905 FIT	11 FIT	157 FIT	85%	1%	6%

Table 4: Summary for TZIDC / TZIDC-200 as smart positioner – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 6,89E-04	PFD_{AVG} = 3,44E-03	PFD_{AVG} = 6,86E-03



Table 5: 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
No Effect	23
Annunciation Undetected	0
Not part	0
MTBF = MTTF + MTTR	150 years

Table 6: 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 7: Summary for TZIDC / TZIDC-200 as shutdown module – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 1,76E-04	PFD _{AVG} = 8,78E-04	PFD _{AVG} = 1,75E-03

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 functional assessment has shown that the intelligent positioner TZIDC / TZIDC-200 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 85%. Based on the verification of "prior use" it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

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 section 5.2 and 5.3 along with all assumptions.

It is important to realize that the "don't care" failures and the "annunciation" 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.

Die Wortmarke Industrial^{IT} und alle weiteren aufgeführten
Produktnamen in der Schreibweise XXXXX^{IT} sind
registrierte oder angemeldete Warenzeichen von ABB.

ABB bietet umfassende und kompetente Beratung
in über 100 Ländern, weltweit.

www.abb.de/aktorik



ABB Automation Products GmbH

Schillerstr. 72
32425 Minden
Germany
Tel: +49 551 905-534
Fax: +49 551 905-555
CCC-support.deapr@de.abb.com

ABB optimiert kontinuierlich ihre Produkte,
deshalb sind Änderungen der technischen Daten
in diesem Dokument vorbehalten.

Printed in the Fed. Rep. of Germany (10.2007)

© ABB 2007