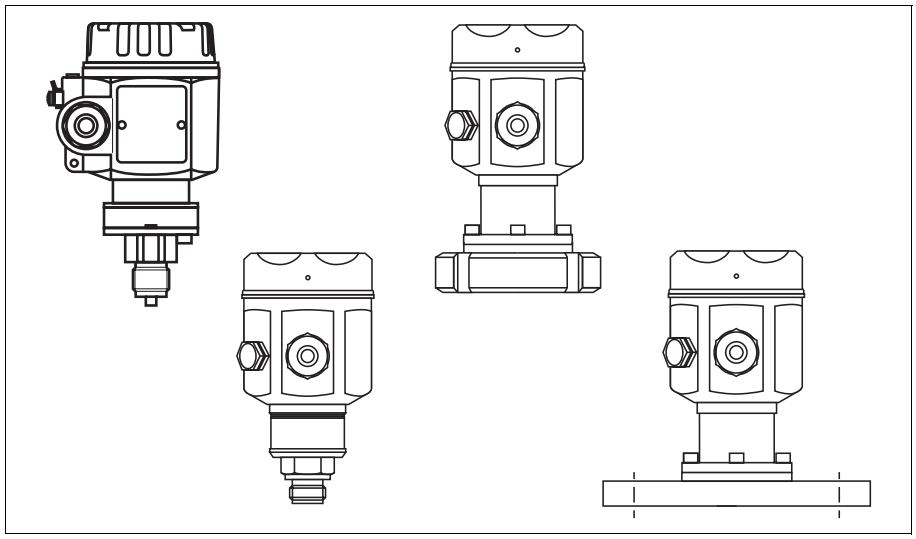
Safety Manual
SD 172P/00/en
71036063

Pressure Transmitter
cerabar M PMC 41/45
cerabar M PMP 41/45/46/48
with Output Signal 4...20 mA/HART

Functional Safety Manual



Application
Pressure measurement (e.g. limit pressure monitoring) to satisfy particular safety systems requirements as per IEC 61508/ IEC 61511-1.

The measuring device fulfils the requirements concerning:
- Functional safety in accordance with IEC 61508/IEC 61511-1
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per EN 61326 and NAMUR recommendation NE 21.

Your benefits
- Used for pressure monitoring (MIN, MAX, range) up to SIL 2, independently evaluated by exida.com as per IEC 61508/ IEC 61511-1
- Continuous measurement
- Easy commissioning

Endress+Hauser
The Power of Know How

Table of contents

SIL declaration of conformity

The binding document is included in the scope of delivery when the Cerabar M is ordered with the "SIL 2/IEC 61508 Declaration of conformity" option.

SIL-03011c/00/a2

SIL-Konformitätserklärung

Funktionale Sicherheit nach IEC 61508 / IEC 61511

SIL Declaration of Conformity

Functional safety according to IEC 61508 / IEC 61511

Endress+Hauser GmbH+Co. KG, Hauptstraße 1, 79689 Maulburg

Level
Pressure
Flow
Temperature
Liquid Analysis
Registration
Systems Components
Services
Solutions

erklärt als Hersteller, dass der Drucktransmitter (Seriennummer
declares as manufacturer, that the pressure transmitter (Serial number

für den Einsatz in Schutzeinrichtungen entsprechend der IEC 61508/IEC 61511-1 geeignet ist, wenn die Sicherheitshinweise und nachfolgende Parameter beachtet werden:
is suitable for the use in safety-instrumented systems according to IEC 61508/IEC 61511-1, if the safety instructions and following parameters are observed:

Gerät/Product	Cerabar M PMC41/45			Cerabar M PMP41/45/46/48 [5]		
SIL	2					
Prüfintervall/Proof test interval	≤ 5 Jahre/years					
Gerätetyp/Device type	B					
HFT [1]	0 (einkanalige Verwendung / single channel use)					
SFF	74 %			71 %		
PFD_{AVG} [2] T_1 = 1 Jahr/year	$6,96 \times 10^{-4}$			$6,78 \times 10^{-4}$		
PFD_{AVG} [2] T_1 = 5 Jahre/years	$3,5 \times 10^{-3}$			$3,4 \times 10^{-3}$		
Sicherheitsfunktion [4] Überwachung / Safety function monitoring	min	max	Bereich/ Range	min	max	Bereich/ Range
λ_{sd}	146 FIT	21 FIT	167 FIT	132 FIT	46 FIT	178 FIT
λ_{su}	290 FIT	290FIT	290 FIT	210 FIT	210 FIT	210 FIT
λ_{dd}	21 FIT	146 FIT	0 FIT	46 FIT	132 FIT	0 FIT
λ_{du}	159 FIT	159 FIT	159 FIT	155 FIT	155 FIT	155 FIT
$MTBF_{tot}$ [3]	182 Jahre/years			205 Jahre/years		

[1] gemäß Kapitel/according to subclause 11.4.4/der/of IEC 61511-1

[2] Die Werte entsprechen SIL 2 nach IEC 61508 und ISA S84.01. PFD_{AV}-Berechnungen für andere T_1 siehe Handbuch zur Funktionalen Sicherheit. / The values comply with SIL 2 according to IEC 61508 and ISA S84.01. PFD_{AV} calculations for other T_1 values refer to the Functional Safety Manual.

[3] gemäss/according to Siemens SN29500

[4] unter Annahme der Einstellung /assuming the setting 4…20 mA

[5] Zur Bewertung der Druckmittlersysteme von PMP45 und PMP48 sind die Hinweise in Handbuch zur Funktionalen Sicherheit (SD172) zu berücksichtigen. / For the evaluation of the diaphragm seal systems of PMP45 and PMP48 the instructions, written the functional safety manual (SD172) have to be taken into account.

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

The assessment according to the proven-in-use properties of the device has been performed including the modifications process.

Maulburg, 12.10.2006

Endress+Hauser GmbH+Co. KG

i.V.
Leitung Zertifizierungsstelle
Management Certification Department

i.A.
Leitung Entwicklungsprojekt
Management R&D Project

Endress+Hauser
People for Process Automation

Validity of the Safety Manual

Valid device versions and software versions

The evaluation described in this Safety Manual regarding functional safety is valid for the device versions and software versions specified below. Unless otherwise stated, all of the following versions can also be used for safety functions because they are subject to the internal modification process, within which the effects of modifications regarding functional safety are also evaluated.

The valid device versions are as follows:

- Cerabar M PMC 41/45-xxxxHxxx
- Cerabar M PMC 41/45-xxxxJxxx
- Cerabar M PMP 41/45/46/48-xxxxHxxx
- Cerabar M PMP 41/45/46/48-xxxxJxxx

Valid software version:

- as of SW 1.1

Warning!
The evaluation of the devices with regard to functional safety includes the basic device with main electronics, sensor electronics and sensor through to the sensor membrane and directly fitted process connection.

- The following applies for diaphragm seals (PMP46 and PMP48):
  The additional use of diaphragm seal systems has an impact on the overall accuracy of the measuring transmission and the settling time. In these cases, the planning instructions for diaphragm seal systems in Technical Information TI 399P must be observed. Assessing the suitability of the overall system, consisting of the basic device and the diaphragm seal, for safety-relevant operation is the responsibility of the operator.

Introduction

Abbreviations, standards and terms

Abbreviations

Information on abbreviations in connection with functional safety and their explanations can be found in the E+H brochure "Functional Safety in the Process Industry – reducing risks with SIL" (SD 002Z).

Relevant standards

Standard	English	Deutsch
IEC 61508, Part 1 – 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, Part 1 – 3	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)

Terms

Term	Explanation
Dangerous failure	Failure with the potential to put the safety-related system in a dangerous or non-functional condition.
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 measuring device – logic unit (e.g. limit signal generator) – valve form a safety-related system.
Safety function	Defined function, which is performed by a safety-related system with the aim of achieving or maintaining a safe condition for the plant, considering a specified dangerous incident. Example: limit pressure monitoring

Determining the Safety Integrity Level (SIL)

The achievable Safety Integrity Level is determined by the following technical safety characteristic quantities:
- Average Probability of Failure on Demand (PFD_{av})
- Hardware Fault Tolerance (HFT) and
- Safe Failure Fraction (SFF).

The specific technical safety characteristic quantities for the Cerabar M, as a part of the safety function, are listed in the "Technical safety characteristic quantities" chapter.

The following table displays the dependence of the "Safety Integrity Level" (SIL) on the "Average Probability of Failure on Demand" (PFDav). Here, the "Low demand mode" has been observed, i.e. the requirement rate for the safety-related system is maximum once a year.

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

Sensor, logic unit and actuator together form a safety-related system, which performs a safety function. The "Average Probability of Failure on Demand" (PFDav) is usually divided up into the sensor, logic unit and actuator sub-systems as per Figure 1.

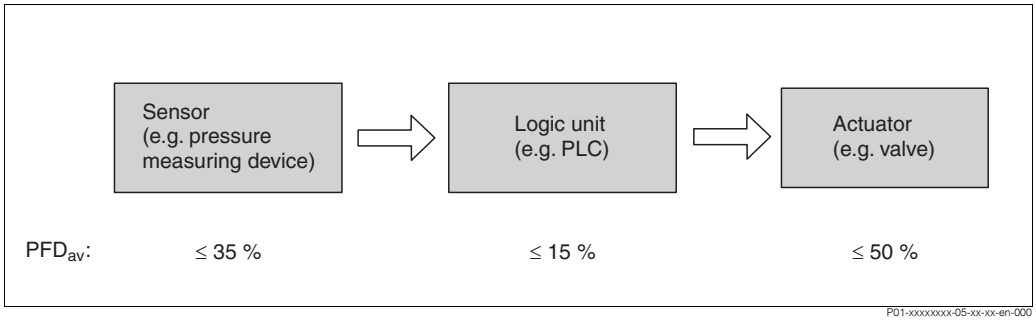


Fig. 1: usual division of the "Average Probability of Failure on Demand" (PFD_{av}) into the sub-systems

Note!
This documentation considers the Cerabar M as a component of a safety function.

The following table displays the achievable "Safety Integrity Level" (SIL) of the entire safety-related system for type B systems depending on the "Safe Failure Fraction" (SFF) and the "Hardware Fault Tolerance" (HFT). Type B systems are, for example, sensors with complex components such as microprocessors (→ see also IEC 61508, Part 2).

Safe Failure Fraction (SFF)	**Hardware Fault Tolerance (HFT)**		
	0	**1 (0) [1]**	**2 (1) [1]**
< 60%	not permitted	SIL 1	SIL 2
60 ...< 90%	SIL 1	**SIL 2**	SIL 3
90 ...< 99%	SIL 2	SIL 3	–
≥ 99 %	SIL 3	–	–

1) In accordance with IEC 61511-1, Section 11.4.3, the "Hardware Fault Tolerance" (HFT) can be reduced by one (values in brackets), if the following conditions are true for devices using sensors and actuators with complex components:
– The device is "proven in use".
– The device allows adjustment of process-related parameters, e.g. measuring range, upscale or downscale failure direction, etc.
– The adjustment the process-related parameters of the device is protected, e.g. jumper, password (here: numeric code or key combination).
– The function has a SIL requirement of less than 4.

All conditions are true for the Cerabar M.

Safety function with Cerabar M

Safety function for limit pressure monitoring

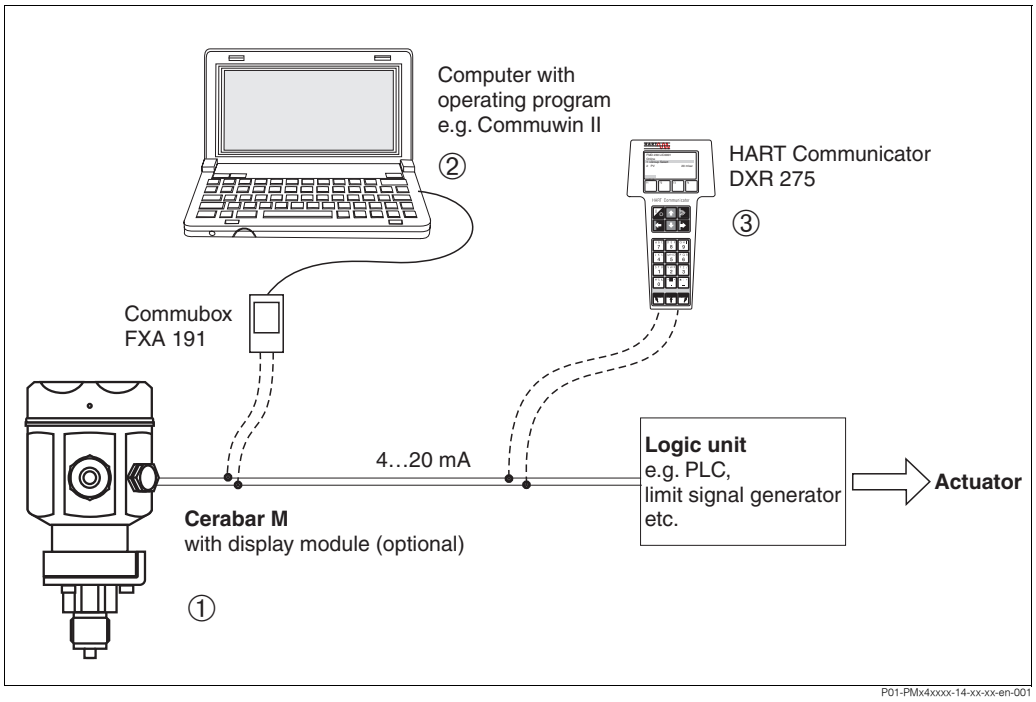


Fig. 2: Safety function (e.g. for limit pressure monitoring) with Cerabar M as sub-system

1 Cerabar M with local operation, option for setting the lower range-value and upper-range value and the attenuation
2 Computer with operating program e.g. Commuwin II for setting all parameters such as alarm behaviour, max. alarm, operating mode, etc.
3 Handheld terminal HART Communicator DXR 275 for setting all parameters such as alarm behaviour, max. alarm, operating mode, etc.

Safety-relevant signal

The Cerabar M transmitter with electronic insert 4…20 mA/HART generates an analog signal (4…20 mA) proportional to the pressure. The analog signal is fed to a downstream logic unit, such as a PLC, or a limit signal generator and monitored there for:

- exceeding a maximum pressure value or
- undershooting a minimum pressure value or
- leaving a pressure range that is to be monitored

For fault monitoring, the logic unit must be able to detect both HI-alarms (22 mA) and LO-alarms (3.6 mA).

Safety function data

Caution!
The compulsory settings and data for the safety functions are listed in the "Settings" and "Technical safety characteristic quantities" chapters.

For the reaction time of the transmitter, see Technical Information TI 399P.

Note!
MTTR is set at eight hours.

Safety-related systems without a self-locking function must be monitored or set to an otherwise safe state after carrying out the safety function within MTTR.

Supplementary device documentation

Depending on the version, the following documentation must be available for the transmitter:

Explosion protection certificate	Devices	Operating Instructions (BA)	Other documentation (XA, ZE or ZD)
Standard	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	none
ATEX II 1/2 G EEx ia IIC T4/T6	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Safety Instructions XA 039P
ATEX II 2 G EEx ia IIC T4/T6	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Safety Instructions XA 039P
ATEX II 3 G EEx nA II T5	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Safety Instructions XA 052P
ATEX II 1/2 D EEx ia IIC T4/T6 IP66 T50°C/T82°C	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Safety Instructions XA 038P
ATEX II 1/3 D IP66 T110°C	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Safety Instructions XA 040P
CSA General Purpose	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	none
CSA IS (suitable Div. 2) Class I, II, III; Div. 1, Groups A – G	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Control Drawing ZD 040P
CSA Class II, III; Div. 1; Groups E – G	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	none
FM IS (non-incendive) Class I, II, III; Div. 1, Groups A – G	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	Control Drawing ZD 039P
FM DIP Class II, III, Div. 1; Groups E– G	PMC 41/45, PMP 41/45, PMP 46/48	BA 201P	none

Caution!
- The installation and setting instructions, and the technical limit values must be observed in accordance with the Operating Instructions (BA 201P).
- For devices used in explosion-hazardous areas, the supplementary documentation (XA, ZD) in accordance with the table must also be observed.

Supplementary documentation Cerabar M
For more information, see Technical Information TI 399P.

Behaviour in operation and failure

Note!

The behaviour in operation and failure is described in the Operating Instructions BA 201P.

Commissioning and iterative tests

Using the Cerabar M for continuous measurements

The functional ability of the safety device must be checked at appropriate intervals. It is the responsibility of the user to select the type of check and the intervals in the specified time frame. The check must be carried out such that perfect functioning of the safety equipment in conjunction with all components is proven.

Settings

Alarm behaviour and current output

In the event of a fault, the current output is set to the value you have selected. The settings can be made either using the Endress+Hauser Commuwin II operating program or with the HART Communicator DXR 275 handheld terminal. The alarm behaviour can be set using the "Set output safety" parameter.

"Set output safety" selection	Current value in the event of a fault
"MIN"	3.6 mA
"MAX"	22 mA
"CONTINUE"	last measured value is kept

Software version	Matrix position (only for operation via Commuwin II)	Parameter	Permitted settings	⚠ Caution! Impermissible setting!
as of SW 1.1	V0H8	"Set output safety"	– "MIN" (3.6 mA) – "MAX" (22 mA)	"CONTINUE" (This setting is not permitted for the safety function!)

Warning!
When using the device as part of a safety function, the "CONTINUE" setting must not be selected!

Checks

Caution!
After entering all of the parameters, check the safety function. The Cerabar M offers the option of simulating a signal current via the "Simulation" and "Set simulation current" parameters, independently of the measured pressure. (These parameters are available when using Commuwin II and the Hart handheld terminal.) → See also the Operating Instructions BA 201P, chapter 5.2 "Current simulation".

Locking/Unlocking

Warning!
Changes to the measuring system and its settings after commissioning can have a negative effect on the safety function. For this reason, you should lock the operation of the Cerabar M after all parameters have been input and the safety function has been checked. This protects your entries against undesired and unauthorised changes.

Caution!
The locking and unlocking function is only available via the Commuwin II operating program and the Hart Communicator DXR 275. After locking, no settings via the communication tools are possible.
Operation can be unlocked via the matrix by entering a three-digit code number different to 130 in V9H9.

	Matrix	Way through menu	Input
Main group: Service			
1	Lock operation		
	V9H9	Locking	e.g. 131 Enter
2	Cancel locking		
	V9H9	Locking	130 Enter

Technical safety characteristic quantities

Specific technical safety characteristic quantities for Cerabar M

The table displays the specific technical safety characteristic quantities for the Cerabar M.

	PMC 41/45	PMP 41/45/46/48
SIL	SIL 2	SIL 2
HFT	0	0
SFF	74 %	71 %
PFD_{av}	6.96×10^{-4}	6.78×10^{-4}
TI[1]	annual	annual

1) Complete function test, e.g. by approaching the limit pressure.

PFD_{av} dependent on selected maintenance interval

The following diagram displays the dependence of the PFD_{av} on the maintenance interval. PFD_{av} increases as the maintenance interval increases.

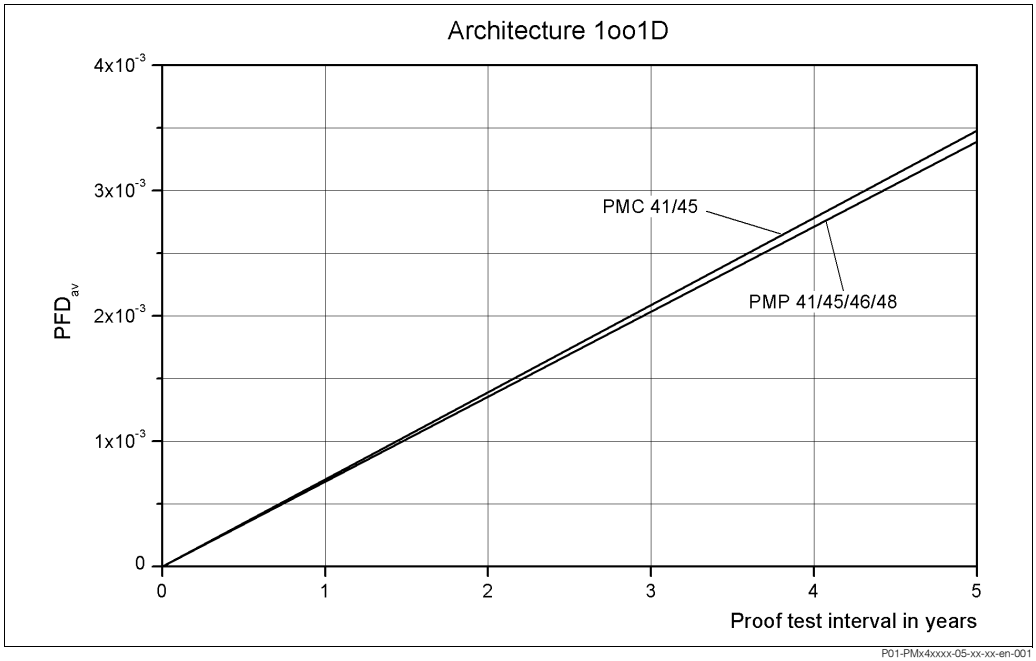


Fig. 4: "Average Probability of Failure on Demand" (PFD_{av}) dependent on the selected maintenance interval.

FMEDA and Proven-in-use Assessment

Project:
Smart Pressure Transmitter Cerabar M

Customer:
Endress+Hauser GmbH+Co. KG
Maulburg
Germany

Contract No.: E+H 03/3-04
Report No.: E+H 03/3-04 R014
Version V1, Revision R1.2, August 2003
Stephan Aschenbrenner

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 smart pressure transmitter Cerabar M with 4..20 mA output / HART® electronics and software version V1.2. Table 1 gives an overview of the different types that belong to the considered pressure transmitter Cerabar M.

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: Version overview

Cerabar M PMC 41	Ceramic sensor
Cerabar M PMC 45	Flush-mounted ceramic sensor
Cerabar M PMP 41	Metal sensor
Cerabar M PMP 45	Flush-mounted metal sensor
Cerabar M PMP 46	Metal sensor with diaphragm for hygienic applications
Cerabar M PMP 48	Metal sensor with diaphragm with threaded boss, separator, flange or flange with extension

For safety applications only the 4..20 mA output / HART® electronics was considered. All other possible output variants or electronics are not covered by this report. The different devices can be equipped with or without display.

The failure rates used in this analysis are based on 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 35% of the total SIF PFD_{AVG} value is caused by the sensor part. 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 sensor part would then be 3,50E-03.

The smart pressure transmitter Cerabar M with 4..20 mA output / HART® electronics is considered to be a Type B[1] component 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.

As the smart pressure transmitter Cerabar M with 4..20 mA output / HART® electronics 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. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.1 a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% to < 90%.
Endress+Hauser did a qualitative analysis of the sensors. This analysis was used by *exida.com* to calculate the failure rates of the sensors using different failure rate databases ([N6], [N7] and [N8]) for the different components of the sensors (see [D19], [D20] and [R5], [R6]). In addition, a failure rate determination for the sensor based on field data evaluation was done by *exida.com* to check the plausibility of the quantitative analysis. The results of the qualitative analysis based on field data evaluation of the process seal and the diaphragm (see [D28]) are used for the calculations described in section 5.3 and 5.4.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on whether the smart pressure transmitter Cerabar M with 4..20 mA output / HART® electronics is used in an application for “low level monitoring”, “high level monitoring” or “range monitoring”. For these applications the following tables show how the above stated requirements are fulfilled.

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

Table 2: Summary for Cerabar M PMC with 4..20 mA output / HART® electronics – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 6,96E-04	PFD_{AVG} = 3,47E-03	PFD_{AVG} = 6,93E-03

Table 3: Summary for Cerabar M PMC with 4..20 mA output / HART® electronics – Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	146 FIT	290 FIT	21 FIT	159 FIT	74%	33%	12%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	21 FIT	290 FIT	146 FIT	159 FIT	74%	7%	48%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	167 FIT	290 FIT	0 FIT	159 FIT	74%	37%	0%

Table 4: Summary for Cerabar M PMP with 4..20 mA output / HART® electronics – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 6,78E-04	PFD_{AVG} = 3,38E-03	PFD_{AVG} = 6,75E-03

Table 5: Summary for Cerabar M PMP with 4..20 mA output / HART® electronics – Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	132 FIT	210 FIT	46 FIT	155 FIT	71%	39%	23%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	46 FIT	210 FIT	132 FIT	155 FIT	71%	18%	46%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	178 FIT	210 FIT	0 FIT	155 FIT	71%	46%	0%

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 35% of this range, i.e. to be better than or equal to 3,50E-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 35% of this range, i.e. to be better than or equal to 3,50E-03.

The functional assessment has shown that the smart pressure transmitter Cerabar M with 4..20 mA output / HART® electronics 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 71% or 74%. 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 smart pressure transmitter Cerabar M with 4..20 mA output / HART® electronics can utilize these failure rates along with the failure rates for an impulse line, when required, 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 5.3 and 5.4 along with all assumptions.

[2] DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for Cerabar M.

Endress+Hauser GmbH+Co.
Instruments International
P.O. Box 2222
D-79574 Weil am Rhein
Germany

Tel. (07621) 975-02
Tx 773926
Fax (07621) 975 345
e-mail: info@ii.endress.com

Internet:
http://www.endress.com

Endress + Hauser
The Power of Know How

11.01

SD 172P/00/en/10.06
71036063
FM+SGML 6.0

71036063