OPTIBAR 5060 SERIE

Supplementary instructions

Safety Handbook according to IEC 61508:2010

Up to SIL2 in a single-channel architecture

Up to SIL3 in a multiple-channel architecture

SIL2

KROHNE

1.1 Device version

This Safety Handbook applies to OPTIBAR PC 5060 and PM 5060 pressure transmitters.

Electronics types:

- 2 wire 4...20 mA / HART® with SIL qualification
- 2 wire 4...20 mA / HART® with SIL qualification and supplementary electronics "Additional current output 4...20 mA"
- Slave electronics for electronic differential pressure with SIL qualification

Valid versions:

- From HW Version 1.0.0
- From SW Version 1.0.0
- Slave electronics from HW Version 1.0.0

The following versions are excluded from safety-relevant applications

- Climate compensated versions
- Diaphragm seals with coated diaphragm

1.2 Field of application

The pressure transmitters can be used for process pressure measurement or hydrostatic level measurement of gases, vapours and liquids in a safety-related system according to IEC 61508 in modes low demand mode or high demand mode:

- Up to SIL2 in a single-channel architecture
- Up to SIL3 in a multiple-channel architecture

The following interface should be used to output the measured value:

- Current output = 4...20 mA.

The following interfaces are only permitted for parameter adjustment and for informative use:

- HART®
- Display and Adjustment module
- Additional current output 4...20 mA

1.3 SIL conformity

The SIL conformity was independently judged and certified by the TÜV Rheinland according to IEC 61508:2010 (Ed.2).

The certificate is valid for the entire service life of all devices that were sold before the certificate expired!

2.1 Safety function

On its current output, the signal converter generates a signal between 3.8 mA and 20.5 mA corresponding to the process pressure or level. This analogue signal is fed to a connected processing system to monitor the following conditions:

- Exceeding a process pressure or level limit
- Falling below a process pressure or level limit
- Monitoring of a process pressure or level range

Safety tolerance

For the interpretation of the safety function, the following aspects must be taken into account in respect to the tolerances:

- Due to a dangerous undetected failure in the range between 3.8 mA and 20.5 mA, an incorrect output signal can be generated which deviates from the real measured value by up to 2%
- Due to the special application conditions, increased measurement deviations can be caused (see Technical data in the operating instructions)

2.2 Safe state

The safe state of the current output depends on the safety function and the characteristics set on the sensor.

Characteristics	Monitoring upper limit value	Monitoring lower limit value
4...20 mA	Output current ≥ Switching point	Output current ≤ Switching point
20...4 mA	Output current ≤ Switching point	Output current ≥ Switching point

Output signals in case of malfunction

Possible fault currents:

- ≤ 3.6 mA ("fail low")
- ≥ 21 mA ("fail high")

2.3 Prerequisites for operation

- The measuring system should be used appropriately taking pressure, temperature, density and chemical properties of the medium into account. The application-specific limits must be observed.
- The specifications according to the operating instructions manual, particularly the current load on the output circuits, must be kept within the specified limits.
- Existing communication interfaces (e.g. HART®, USB) are not used for transmission of the safety-relevant measured value.
- The instructions in chapter "Safety-related characteristics" must be noted.
- All parts of the measuring chain must correspond to the planned "Safety Integrity Level (SIL)".

3.1 Characteristics acc. to IEC 61508 for process pressure measurement or hydrostatic level measurement

OPTIBAR 5060 series

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture
	SIL3 in multiple-channel architecture ①
Hardware error tolerance	HFT = 0
Device type	TYP B
Mode	Low demand mode, High demand mode
SFF	> 90%
MTBF ②	0.50 x 10^6hours (57 years)
Diagnosis test interval ③	< 30 minutes

① Homogeneous redundancy possible
② Including errors outside the safety function
③ Time during which all internal diagnoses are carried out at least once

Failure rates

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	1121 FIT	44 FIT	9 FIT	59 FIT	34 FIT	19 FIT

PFD_{AVG}	0.037 x 10^{-2}	(T1 = 1 Year)
PFD_{AVG}	0.054 x 10^{-2}	(T1 = 2 Years)
PFD_{AVG}	0.106 x 10^{-2}	(T1 = 5 Years)
PFH	0.044 x 10^{-6} 1/hour	

Coverage with the proof test (PTC)

Test type ①	Remaining dangerous undetected failures	PTC
Test 1	21 FIT	52%
Test 2	2 FIT	95%

① See section Proof test

OPTIBAR 5060 series with diaphragm seal

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture
	SIL3 in multiple-channel architecture ①
Hardware error tolerance	HFT = 0
Device type	Type B
Mode	Low demand mode, High demand mode
SFF	> 90%
MTBF ②	0.56 x 10^6hours (64 Years)
Diagnosis test interval ③	< 30 minutes

① Homogeneous redundancy possible
② Including errors outside the safety function
③ Time during which all internal diagnoses are carried out at least once

Failure rates

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	986 FIT	75 FIT	9 FIT	59 FIT	34 FIT	19 FIT

PFD_{AVG}	0.063 x 10^{-2}	(T1 = 1 Year)
PFD_{AVG}	0.093 x 10^{-2}	(T1 = 2 Years)
PFD_{AVG}	0.181 x 10^{-2}	(T1 = 5 Years)
PFH	0.075 x 10^{-6} 1/hour	

Coverage with the proof test (PTC)

Test type ①	Remaining dangerous undetected failures	PTC
Test 1	53 FIT	29%
Test 2	2 FIT	95%

① See section Proof test

3.2 Characteristics according to IEC 61508 for electronic differential pressure measurement

Electronic differential pressure consisting of two OPTIBAR 5060

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture
	SIL3 in multiple-channel architecture ①
Hardware error tolerance	HFT = 0
Device type	Type B
Mode	Low demand mode, High demand mode
SFF	> 90%
MTBF ②	0.39 x 10^6hours (44 Years)
Diagnosis test interval ③	< 30 minutes

① Homogeneous redundancy possible
② Including errors outside the safety function
③ Time during which all internal diagnoses are carried out at least once

Failure rates

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	1406 FIT	63 FIT	9 FIT	59 FIT	34 FIT	19 FIT

PFD_{AVG}	0.054 x 10^{-2}	(T1 = 1 Year)
PFD_{AVG}	0.079 x 10^{-2}	(T1 = 2 Years)
PFD_{AVG}	0.154 x 10^{-2}	(T1 = 5 Years)
PFH	0.063 x 10^{-6} 1/hour	

Coverage with the proof test (PTC)

Test type ①	Remaining dangerous undetected failures	PTC
Test 1	40 FIT	36%
Test 2	3 FIT	95%

① See section Proof test

Electronic differential pressure consisting of two OPTIBAR 5060 with an OPTIBAR DS diaphragm seal

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture
	SIL3 in multiple-channel architecture ①
Hardware error tolerance	HFT = 0
Device type	Type B
Mode	Low demand mode, High demand mode
SFF	> 90%
MTBF ②	0.43 x 10^6hours (49 Years)
Diagnosis test interval ③	< 30 minutes

① Homogeneous redundancy possible
② Including errors outside the safety function
③ Time during which all internal diagnoses are carried out at least once

Failure rates

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	1270 FIT	96 FIT	9 FIT	59 FIT	34 FIT	19 FIT

PFD_{AVG}	0.081 x 10^{-2}	(T1 = 1 Year)
PFD_{AVG}	0.118 x 10^{-2}	(T1 = 2 Years)
PFD_{AVG}	0.231 x 10^{-2}	(T1 = 5 Years)
PFH	0.096 x 10^{-6} 1/hour	

Coverage with the proof test (PTC)

Test type ①	Remaining dangerous undetected failures	PTC
Test 1	73 FIT	24%
Test 2	3 FIT	97%

① See section Proof test

Electronic differential pressure consisting of two OPTIBAR 5060 each with an OPTIBAR DS diaphragm seal

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture
	SIL3 in multiple-channel architecture ①
Hardware error tolerance	HFT = 0
Device type	Type B
Mode	Low demand mode, High demand mode
SFF	> 90%
MTBF ②	0.48 x 10^6hours (55 Years)

Diagnosis test interval ③	< 30 minutes

① Homogeneous redundancy possible
② Including errors outside the safety function
③ Time during which all internal diagnoses are carried out at least once

Failure rates

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	1135 FIT	127 FIT	9 FIT	59 FIT	34 FIT	19 FIT

PFD_{AVG}	0.107×10^{-2}	(T1 = 1 Year)
PFD_{AVG}	0.157×10^{-2}	(T1 = 2 Years)
PFD_{AVG}	0.307×10^{-2}	(T1 = 5 Years)
PFH	0.127×10^{-6} 1/hour	

Coverage with the proof test (PTC)

Test type ①	Remaining dangerous undetected failures	PTC
Test 1	105 FIT	17%
Test 2	4 FIT	97%

① See section Proof test

3.3 Characteristics acc. to ISO 13849-1 for process pressure measurement or hydrostatic level measurement

OPTIBAR 5060 series

Derived from the safety-related characteristics, the following figures result according to ISO 13849-1 (machine safety): (ISO 13849-1 was not part of the certification of the device.)

Parameter	Value
MTTFd	90 Years
DC	97%
Preformance Level	4.35×10^{-8} 1/hour (corresponds "e")

OPTIBAR 5060 series with OPTIBAR DS diaphragm seal

Parameter	Value
MTTFd	98 Years
DC	94%
Preformance Level	7.48×10^{-8} 1/hour (corresponds "e")

3.4 Characteristics according to ISO 13849-1 for electronic differential pressure measurement

Electronic differential pressure consisting of two OPTIBAR 5060

Derived from the safety-related characteristics, the following figures result according to ISO 13849-1 (machine safety): (ISO 13849-1 was not part of the certification of the device.)

Parameter	Value
MTTFd	73 Years
DC	96%
Preformance Level	6.33 x 10^{-8} 1/hour (corresponds "e")

Electronic differential pressure consisting of two OPTIBAR 5060 with an OPTIBAR DS diaphragm seal

Parameter	Value
MTTFd	78 Years
DC	93%
Preformance Level	9.56 x 10^{-8} 1/hour (corresponds "e")

Electronic differential pressure consisting of two OPTIBAR 5060 each with an OPTIBAR DS diaphragm seal

Parameter	Value
MTTFd	84 Years
DC	91%
Preformance Level	1.27 x 10^{-7} 1/hour (corresponds "e")

3.5 Supplementary information

Determination of the failure rates

The failure rates of the device were determined by an FMEDA according to IEC 61508. Basis for the calculations are the component failure rates according to SN 29500.

All figures refer to an average ambient temperature of 40°C (104°F) during the operating time. For higher temperatures, the values should be corrected:

- Continuous application temperature > 50°C (122°F) by factor 1.3
- Continuous application temperature > 60°C (140°F) by factor 2.5

Similar factors apply if frequent temperature fluctuations are expected.

Assumptions of the FMEDA

- The failure rates are constant. Take note of the useful service life of the components according to IEC 61508-2.
- Multiple errors are not taken into account
- Wear on mechanical parts is not taken into account
- Failure rates of external power supplies are not taken into account
- The environmental conditions correspond to an average industrial environment

Calculation of PFD_{AVG}

The values for PFD_{AVG} specified above were calculated as follows for a 1oo1 architecture:

$PFD_{AVG} = (PTC \times \lambda_{DU} \times T1 / 2) + \lambda_{DD} \times MTTR + ((1-PTC) \times \lambda_{DU} \times LT / 2)$

- T1 (Proof Test Interval)
- MTTR = 8 hours
- PTC = 90%
- LT = 10 Years

Boundary conditions relating to the configuration of the processing unit

A connected control and processing unit must have the following properties:

- The output circuit of the signal converter is judged according to the idle current principle
- "fail low" and "fail high" signals are interpreted as a failure, which triggers a fault message

If this is not the case, the respective percentages of the failure rates must be assigned to the dangerous failures and the values stated in chapter "Safety-related characteristics" redetermined!

Multiple channel architecture

In multiple channel systems for SIL3 applications, this measuring system can also be used in a homogeneously redundant configuration.
The safety-related characteristics must be calculated especially for the selected structure of the measuring chain using the stated failure rates. In doing this, a suitable Common Cause Factor must be considered (see IEC 61508-6, appendix D).

4.1 General

Take note of the mounting and installation instructions in the operating instructions manual.

Functional check

When locking the adjustment, the device checks the data of the measurement loop and decides on the basis of the evaluation results if it is necessary to check the level. Hence the following actions must be carried out at the time of every startup:

- Unlock adjustment
- if necessary, change parameters
- Lock adjustment and verify modified parameters, if necessary

4.2 Device parameter adjustment

The following adjustment units are permitted for parameterization of the safety function:

- Display and Adjustment module
- The DTM suitable for OPTIBAR 5060 in conjunction with an adjustment software according to the FDT/DTM standard, e.g. PACTware
- The device description EDD suitable for OPTIBAR 5060

The parameter adjustment is described in the operating instructions manual.

Safety-relevant parameters

For protection against unwanted or unauthorised adjustment, the set parameters must be protected against unauthorised access. For this reason, the device is shipped in locked condition. The PIN in delivery status is "0000".
The default values of the parameters are listed in the operating instructions. When shipped with customer-specific parameter settings, the device is accompanied by a list of the values differing from the default values.

Safe parameterisation

To avoid or detect possible errors during parameter adjustment for unsafe operating environments, a verification procedure is used that allows the safety-relevant parameters to be checked.
Parameter adjustment proceeds according to the following steps:

- Unlock adjustment
- Change parameters
- Lock adjustment and verify modified parameters

The exact process is described in the operating instructions.

For verification, all modified, safety-relevant and non safety-relevant parameters are shown. The verification texts are displayed either in German or, when any other menu language is used, in English.

Unsafe device status

WARNING!
When adjustment is unlocked, the safety function must be considered as unreliable. This applies until the parameters are verified and the adjustment is locked again. If the parameter adjustment process is not carried out completely, the device statuses described in the operating instructions must be taken into consideration. If necessary, you must take other measures to maintain the safety function.

Device reset

WARNING!
In case a reset to "Delivery status" or "Basic adjustment" is carried out, all safety-relevant parameters must be checked or set anew.

5.1 Behaviour in case of failure

The device is permanently monitored by an internal diagnostic system. If a malfunction is detected, the respective output signals change to the status configured especially for this condition (see section "Safe status").
The diagnosis interval is specified in chapter "Safety-related characteristics".

A fault message coded according to the type of fault is outputted. The fault messages are listed in the operating instructions.

5.2 Repair

Behaviour in case of failure

If faults are detected, the entire measuring system must be shut down and the process held in a safe state by other measures.
The manufacturer must be informed of the occurrence of a dangerous, undetected error (incl. fault description).

Electronics exchange

The procedure is described in the operating instructions manual. Note the instructions for parameter adjustment and setup.

Software update

The procedure is described in the operating instructions manual. Note the instructions for parameter adjustment and setup.

6.1 General

WARNING!
During the function test, the safety function must be treated as unreliable. Take into account that the function test influences downstream connected devices. If necessary, you must take other measures to maintain the safety function. After the function test, the status specified for the safety function must be restored.

To identify possible undetected, dangerous failures, the safety function must be checked in adequate intervals by a proof test. It is the user's responsibility to choose the type of testing. The time intervals are subject to the PFD_{AVG} (see chapter "Safety-related characteristics"). If one of the tests proves negative, the entire measuring system must be switched out of service and the process held in a safe state by means of other measures.

In a multiple channel architecture this applies separately to each channel.

- Determine safety function (mode, switching points)
- If necessary, remove the device from the safety chain and maintain the safety function by other means
- Provide an approved adjustment unit

6.2 Test 1 - without checking the pressure value

Conditions

- Device in installed condition
- Output signal corresponds to the process pressure or the level
- Device status in the menu Diagnosis is "OK"

Procedure

1. Carry out a restart (switch the device off and then on again)
2. Simulate High alarm and check current output (test line resistor)
3. Simulate Low alarm and check current output (test line resistance)

Expected result

- To 1: Output signal corresponds to the process pressure or level and the device status in the menu Diagnosis is "OK"
- To 2: Output signal corresponds to the High alarm
- To 3: Output signal corresponds to the Low alarm

Coverage of the test

See Safety-related characteristics

6.3 Test 2 - with check of the pressure value

Conditions

- Device in installed condition
- Output signal corresponds to the process pressure or the level
- Device status in the menu Diagnosis is "OK"

Procedure

1. Carry out a restart (switch the device off and then on again)
2. Simulate High alarm and check current output (test line resistor)
3. Simulate Low alarm and check current output (test line resistance)
4. Reference pressure measurement at 0% - 50% - 100% of the measuring range (4 mA - 12 mA - 20 mA)
5. If necessary, sensor calibration through service log-in and subsequent reference pressure measurement

Expected result

- To 1: Output signal corresponds to the process pressure or level and the device status in the menu Diagnosis is "OK"
- To 2: Output signal corresponds to the High alarm
- To 3: Output signal corresponds to the Low alarm
- To 4 and 5: Output signal corresponds to the reference pressure measurement

Coverage of the test

See Safety-related characteristics

7.1 Appendix 1 - Test report

Identification

Company/Tester	
Plant/Device TAG	
Meas. loop TAG	
Device type/Order code	
Device serial number	
Date, setup	
Date, last function test	

Test reason/Test scope

	Setup without function test
	Setup with function test
	Proof test without function test
	Proof test with function test

Mode

	Overfill protection
	Dry run protection
	Range monitoring

Adjusted parameters of the safety function are documented

	Yes
	No

Test result

Test point	Process pressure/Level	Expected measured value	Actual value	Test result
Process pressure/Level 1				
Process pressure/Level 2				
Process pressure/Level 3				
Process pressure/Level 4				
Process pressure/Level 5				

Confirmation

Date:	Signature:

7.2 Appendix B - Term definitions

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{AVG}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of a dangerous failure per hour (Ed.2)
FMEDA	Failure Mode, Effects and Diagnostics Analysis
FIT	Failure In Time (1 FIT = 1 failure/109 hours)
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
λ_S	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_H	Rate for failure, who causes a high output current (> 21 mA)
λ_L	Rate for failure, who causes a low output current (≤ 3.6 mA)
λ_{AD}	Rate for diagnostic failure (detected)
λ_{AU}	Rate for diagnostic failure (undetected)
DC	Diagnostic Coverage
PTC	Proof Test Coverage
T1	Proof Test Interval
LT	Life Time
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration (Ed.2)
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

KROHNE – Process instrumentation and measurement solutions

- Flow
- Level
- Temperature
- Pressure
- Process Analysis
- Services

Head Office KROHNE Messtechnik GmbH
Ludwig-Krohne-Str. 5
47058 Duisburg (Germany)
Tel.: +49 203 301 0
Fax: +49 203 301 10389
info@krohne.com

The current list of all KROHNE contacts and addresses can be found at:
www.krohne.com

KROHNE