

# Safety Manual

## OPTISWITCH series 3000

### - two-wire



---

Variable area flowmeters

---

Vortex flowmeters

---

Flow controllers

---

Electromagnetic flowmeters

---

Ultrasonic flowmeters

---

Mass flowmeters

---

**Level measuring instruments**

---

Communications engineering

---

Engineering systems & solutions

---

Switches, counters, displays and recorders

---

Heat metering

---

Pressure and temperature

## Content

### 1 Functional safety

1.1	General . . . . .	3
1.2	Planning . . . . .	4
1.3	Adjustment instructions . . . . .	7
1.4	Setup . . . . .	7
1.5	Reaction during operation and in case of failure	7
1.6	Recurring function test . . . . .	8
1.7	Safety-related characteristics . . . . .	9

# 1 Functional safety

## 1.1 General

**Scope** This safety manual applies to measuring systems consisting of the vibrating level switch OPTISWITCH series 3000 with integrated oscillator VB60Z:

### OPTISWITCH 3100 C, 3200 C, 3300 C

Valid hardware and software versions:

- Serial number of the electronics >14215176
- Sensor software from Rev. 1.03

**Area of application** The measuring system can be implemented for level detection of bulk solids (powders and granulates) which meets the special requirements of safety technology.

This is possible up to SIL2 in a single channel architecture (1oo1D), and up to SIL3 in a multiple channel, redundant architecture.



#### Note:

With a special factory setting, the measuring system is also suitable for detection of solids in water (see "Operating instructions manual").

**SIL conformity** The SIL declaration of conformity can be downloaded from our homepage in the Internet.

**Abbreviations, terms** Further abbreviations and terms are stated in IEC 61508-4.

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD <sub>avg</sub>	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
$\lambda_{sd}$	Rate for safe detected failure
$\lambda_{su}$	Rate for safe undetected failure
$\lambda_{dd}$	Rate for dangerous detected failure
$\lambda_{du}$	Rate for dangerous undetected failure
DC <sub>S</sub>	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd} + \lambda_{su})$
DC <sub>D</sub>	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd} + \lambda_{du})$

FIT	Failure In Time (1 FIT = 1 failure/10 <sup>9</sup> h)
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTRR	Mean Time To Repair

**Relevant standards**

- IEC 61508 (also available as DIN EN)
  - Functional safety of electrical/electronic/programmable electronic safety-related systems

**Safety requirements**

Failure limit values for a safety function, depending on the SIL class (of IEC 61508-1, 7.6.2)

Safety integrity level	Low demand mode	High demand mode
SIL	PFD <sub>avg</sub>	PFH
4	$\geq 10^{-5} \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-4} \dots < 10^{-3}$	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-3} \dots < 10^{-2}$	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$

Safety integrity of hardware for safety-related subsystems of type B (IEC 61508-2, 7.4.3)

Safe failure fraction	Hardware fault tolerance		
	HFT = 0	HFT = 1	HFT = 2
SFF	HFT = 0	HFT = 1	HFT = 2
< 60 %	not permitted	SIL1	SIL2
60 % ... < 90 %	SIL1	SIL2	SIL3
90 % ... < 99 %	SIL2	SIL3	(SIL4)
$\geq 99$ %	SIL3	(SIL4)	(SIL4)

**1.2 Planning****Safety function**

The safety function of this measuring system is the identification and signalling of the condition of the vibrating element.

A difference is made between the two conditions "covered" and "uncovered".

**Safe state**

The safe state depends on the mode:

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
Vibrating element in safe state	covered	uncovered
Output current in safe condition if mode switch on the sensor is set to "max."	12.5 ... 23.5 mA	2.3 ... 11.5 mA
Output current in safe condition if mode switch on the sensor is set to "min."	2.3 ... 11.5 mA	12.5 ... 23.5 mA
Failure current "fail low"	< 2.3 mA	< 2.3 mA
Failure current "fail high"	> 23.5 mA	> 23.5 mA

**Fault description**

A safe failure is present when the measuring system switches to the defined safe state or the fault mode without the process demanding it.

If the internal diagnosis system detects a failure, the measuring system goes into fault mode.

A dangerous undetected failure exists if the measuring system switches neither to the defined safe condition nor to the failure mode when the process requires it.

**Configuration of the processing unit**

If the measuring system delivers output currents of "fail low" or "fail high", it can be assumed that there is a malfunction.

The processing unit must therefore interpret such currents as a malfunction and output a suitable fault signal.

If this is not the case, the corresponding portions of the failure rates must be assigned to the dangerous failures. The stated values in chapter "Safety-relevant characteristics" can thus worsen.

The processing unit must correspond to the SIL level of the measurement chain.

If an SU 501 Ex is used for processing, the mode switch on the sensor must be set to "max."

**Low demand mode**

If the demand rate is only once a year, then the measuring system can be used as safety-relevant subsystem in "low demand mode" (IEC 61508-4, 3.5.12).

If the ratio of the internal diagnostics test rate of the measuring system to the demand rate exceeds the value 100, the measuring system can be treated as if it is executing a safety function in the mode with low demand rate (IEC 61508-2, 7.4.3.2.5).

An associated characteristic is the value  $PFD_{avg}$  (average Probability of dangerous Failure on Demand). It is dependent on the test interval  $T_{Proof}$  between the function tests of the protective function.

Number values see chapter "*Safety-related characteristics*".

### High demand mode

If the "*low demand rate*" does not apply, the measuring system as safety-relevant subsystem in "*high demand mode*" should be used (IEC 61508-4, 3.5.12).

The fault tolerance time of the complete system must be higher than the sum of the reaction times or the diagnostics test periods of all components in the safety-related measurement chain.

An associated characteristic is the value PFH (failure rate).

Number values see chapter "*Safety-related characteristics*".

### Assumptions

The following assumptions form the basis for the implementation of FMEDA:

- Failure rates are constant, wear of the mechanical parts is not taken into account
- Failure rates of external power supplies are not taken into account
- Multiple errors are not taken into account
- The average ambient temperature during the operating time is 40 °C (104 °F)
- The environmental conditions correspond to an average industrial environment
- The lifetime of the components is around 8 to 12 years (IEC 61508-2, 7.4.7.4, remark 3)
- The repair time (exchange of the measuring system) after a nondangerous malfunction is eight hours (MTTR = 8 h)
- The processing unit can interpret "*fail low*" and "*fail high*" failures as errors and trigger a suitable error message
- The scanning interval of a connected control and processing unit is max. 1 hour, in order to react to dangerous, detectable errors
- Existing communication interfaces (e. g. HART, I<sup>2</sup>C-Bus) are not used for transmission of safety-relevant information

**General instructions and restrictions**

The measuring system should be used appropriately taking pressure, temperature, density and chemical properties of the medium into account.

The user-specific limits must be kept. The specifications of the operating instructions manual must not be exceeded.

Keep in mind when using as dry run protection:

- Avoid buildup on the vibrating system (probably shorter proof test intervals will be necessary)
- Fork version: avoid granulate size of the medium > 15 mm (0.6 in)

### 1.3 Adjustment instructions

**Adjustment elements**

Since the plant conditions influence the safety of the measuring system, the adjustment elements must be set according to the application:

- DIL switch for switching point adaptation
- DIL switch for mode adjustment

The function of the adjustment elements is described in the operating instructions manual.

### 1.4 Setup

**Mounting and installation**

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

In the setup procedure, a check of the safety function by means of an initial filling is recommended.

### 1.5 Reaction during operation and in case of failure

The adjustment elements or device parameters must not be modified during operation.

If modifications have to be made during operation, carefully observe the safety functions.

Fault signals that may appear are described in the appropriate operating instructions manual.

If faults or error messages are detected, the entire measuring system must be shut down and the process held in a safe state by other measures.

An exchange of the electronics is easily possible and is described in the operating instructions manual.

If due to a detected failure the electronics or the complete sensor is exchanged, the manufacturer must be informed (incl. a fault description).

## 1.6 Recurring function test

### General

The recurring function test is used to check the safety function, to detect possible non-recognisable, dangerous faults. The function of the measuring system must be checked in adequate intervals.

The operator is responsible for choosing the type of check. The time intervals depend on the selected  $PFD_{avg}$  value according to chart and diagram in paragraph "*Safety-related characteristics*".

With high demand rate, a recurring function test is not requested in IEC 61508. The function of the measuring system is demonstrated by the frequent use of the system. In double channel architectures it is a good idea to verify the redundancy through recurring function tests at appropriate intervals.

The test must be carried out in a way that verifies the flawless operation of the safety functions in conjunction with all system components.

This is ensured by a controlled reaching of the response height during filling. If filling up to the response height is not possible, then a response of the measuring system must be triggered by a suitable simulation of the level or the physical measuring effect.

The methods and procedures used during the tests must be stated and their suitability must be specified. The tests must be documented.

If the function test 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 the double channel architecture 1oo2D this applies separately to both channels.

### Function test in mode overfill protection

If the measuring system is used as overfill protection, the proof of the function is ensured by a simple function test which can be triggered and monitored manually or by a connected control system.

This function test is triggered by an interruption of the supply cable for at least two seconds. Then a special warm-up reaction of the current output is carried out which must be recorded.

The test procedure is described in detail in the operating instructions manual.

**Test key on the signal conditioning instrument:**

If a connected signal conditioning instrument with test key is used for processing, the stated function test can be easily carried out by pushing the test key. Suitable signal conditioning instruments are listed in chapter "*Technical data*" of the operating instructions manual.



**Note:**

This test can be carried out only if the vibrating element is uncovered.

**1.7 Safety-related characteristics**

**Basics**

The failure rates of the electronics, the mechanical parts of the transmitter as well as the process fitting are determined by an FMEDA according to IEC 61508. The calculations are based on component failure rates according to SN 29500. All values refer to an average ambient temperature during the operating time of 40 °C (104 °F).

For a higher average temperature of 60 °C (140 °F), the failure rates should be multiplied by a factor of 2.5. A similar factor applies if frequent temperature fluctuations are expected.

The calculations are also based on the specifications stated in chapter "*Planning*".

**Service life**

After 8 to 12 years, the failure rates of the electronic components will increase, whereby the derived PFD and PFH values will deteriorate (IEC 61508-2, 7.4.7.4, note 3).

**Failure rates**

Mode switch on the sensor to "**max.**"

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
$\lambda_{sd}$	49 FIT	39 FIT
$\lambda_{su}$	387 FIT	352 FIT
$\lambda_{dd}$	163 FIT	182 FIT

	Overflow protection (max. operation)	Dry run protection (min. operation)
$\lambda_{du}$	18 FIT	43 FIT
DC <sub>S</sub>	11 %	10 %
DC <sub>D</sub>	90 %	81 %
MTBF = MTTF + MTTR	$1.59 \times 10^6$ h	$1.59 \times 10^6$ h

Mode switch on the sensor to "min."

	Overflow protection (max. operation)	Dry run protection (min. operation)
$\lambda_{sd}$	39 FIT	45 FIT
$\lambda_{su}$	373 FIT	361 FIT
$\lambda_{dd}$	168 FIT	173 FIT
$\lambda_{du}$	36 FIT	37 FIT
DC <sub>S</sub>	9 %	11 %
DC <sub>D</sub>	82 %	82 %
MTBF = MTTF + MTTR	$1.59 \times 10^6$ h	$1.59 \times 10^6$ h

Diagnosis test period	< 100 sek.
-----------------------	------------

### Single channel architecture (1oo1D)

SIL	SIL2
HFT	0
Sensor type	Type B

Mode switch on the sensor to "max."

	Overflow protection (max. operation)	Dry run protection (min. operation)
<b>SFF</b>	97 %	93 %
<b>PFD<sub>avg</sub></b> T <sub>Proof</sub> = 1 year T <sub>Proof</sub> = 5 years T <sub>Proof</sub> = 10 years	< $0.008 \times 10^{-2}$ < $0.039 \times 10^{-2}$ < $0.077 \times 10^{-2}$	< $0.019 \times 10^{-2}$ < $0.093 \times 10^{-2}$ < $0.186 \times 10^{-2}$
<b>PFH</b>	< $0.018 \times 10^{-6}/h$	< $0.043 \times 10^{-6}/h$

Mode switch on the sensor to "min."

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	<b>Overflow protection (max. operation)</b>	<b>Dry run protection (min. operation)</b>
182 FIT		

	Overflow protection (max. operation)	Dry run protection (min. operation)
Mode switch on the sensor to "min."  <div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px 0;"></div>	Overflow protection (max. operation)	Dry run protection (min. operation)
$\lambda_{sd}$	39 FIT	45 FIT
$\lambda_{su}$	373 FIT	361 FIT
$\lambda_{dd}$	168 FIT	173 FIT
$\lambda_{du}$	36 FIT	37 FIT
DC <sub>S</sub>	9 %	11 %
DC <sub>D</sub>	82 %	82 %
MTBF = MTTF + MTTR	$1.59 \times 10^6$ h	$1.59 \times 10^6$ h

**Fault reaction time**

Diagnosis test period	< 100 sek.
-----------------------	------------

**Single channel architecture (1oo1D)****Specific characteristics**

SIL	SIL2
HFT	0
Sensor type	Type B

**Mode switch on the sensor to "max."**

	Overflow protection (max. operation)	Dry run protection (min. operation)
<b>SFF</b>	97 %	93 %
<b>PFD<sub>avg</sub></b>		
$T_{Proof} = 1$ year	$< 0.008 \times 10^{-2}$	$< 0.019 \times 10^{-2}$
$T_{Proof} = 5$ years	$< 0.039 \times 10^{-2}$	$< 0.093 \times 10^{-2}$
$T_{Proof} = 10$ years	$< 0.077 \times 10^{-2}$	$< 0.186 \times 10^{-2}$
<b>PFH</b>	$< 0.018 \times 10^{-6}/h$	$< 0.043 \times 10^{-6}/h$

**Mode switch on the sensor to "min."**

	Overflow protection (max. operation)	Dry run protection (min. operation)
<b>SFF</b>	94 %	94 %

	Overflow protection (max. operation)	Dry run protection (min. operation)
<b>PFD<sub>avg</sub></b>		
T <sub>Proof</sub> = 1 year	< 0.016 x 10 <sup>-2</sup>	< 0.016 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 5 years	< 0.078 x 10 <sup>-2</sup>	< 0.081 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 10 years	< 0.156 x 10 <sup>-2</sup>	< 0.162 x 10 <sup>-2</sup>
<b>PFH</b>	< 0.036 x 10 <sup>-6</sup> /h	< 0.037 x 10 <sup>-6</sup> /h

**Time-dependent process of PFD<sub>avg</sub>**

The chronological sequence of PFD<sub>avg</sub> is nearly linear to the operating time over a period up to 10 years. The above values apply only to the T<sub>Proof</sub> interval after which a recurring function test must be carried out.

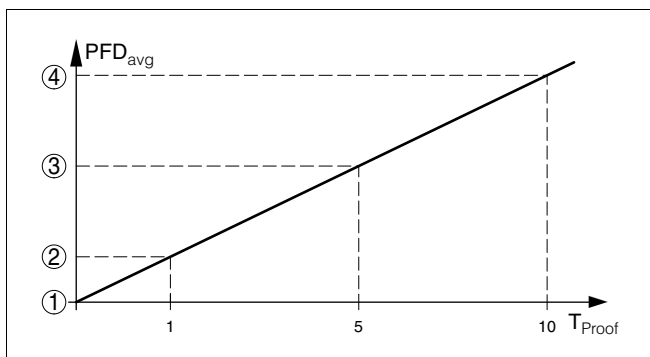


Fig. 1: Chronological sequence of PFD<sub>avg</sub> (figures see above charts)

- 1 PFD<sub>avg</sub> = 0
- 2 PFD<sub>avg</sub> after 1 year
- 3 PFD<sub>avg</sub> after 5 years
- 4 PFD<sub>avg</sub> after 10 years

**Multiple channel architecture**

**Specific characteristics**

If the measuring system is used in a multiple channel architecture, the safety-relevant characteristics of the selected structure of the meas. chain must be calculated specifically for the selected application according to the above failure rates.

A suitable Common Cause Factor must be taken into account.

Subject to change without notice