Safety Manual
OPTISWITCH series 5000
- two-wire
Contents

1 Functional safety
  1.1 General information ................................................................. 3
  1.2 Planning .................................................................................. 4
  1.3 Adjustment instructions .......................................................... 6
  1.4 Setup ...................................................................................... 6
  1.5 Reaction during operation and in case of failure ................. 6
  1.6 Recurring function test ............................................................. 7
  1.7 Safety-related characteristics .................................................. 8
1 Functional safety

1.1 General information

Scope
This safety manual applies to measuring systems consisting of the vibrating level switch OPTISWITCH series 5000 with electronics module SWE60Z:

OPTISWITCH 5100 C, 5150 C, 5200 C, 5250 C

Note:
For instruments with enamelled fork, electronics module SWE60Z.E or SWE60Z.E1 is required.

Area of application
The measuring system can be implemented for level detection (of liquids) 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.

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

Abbreviations, terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
</tr>
<tr>
<td>PFD&lt;sub&gt;avg&lt;/sub&gt;</td>
<td>Average Probability of dangerous Failure on Demand</td>
</tr>
<tr>
<td>PFH</td>
<td>Probability of a dangerous Failure per Hour</td>
</tr>
<tr>
<td>FMEDA</td>
<td>Failure Mode, Effects and Diagnostics Analysis</td>
</tr>
<tr>
<td>λ&lt;sub&gt;sd&lt;/sub&gt;</td>
<td>Rate for safe detected failure</td>
</tr>
<tr>
<td>λ&lt;sub&gt;su&lt;/sub&gt;</td>
<td>Rate for safe undetected failure</td>
</tr>
<tr>
<td>λ&lt;sub&gt;dd&lt;/sub&gt;</td>
<td>Rate for dangerous detected failure</td>
</tr>
<tr>
<td>λ&lt;sub&gt;du&lt;/sub&gt;</td>
<td>Rate for dangerous undetected failure</td>
</tr>
<tr>
<td>DC&lt;sub&gt;s&lt;/sub&gt;</td>
<td>Diagnostic Coverage of safe failures; DC&lt;sub&gt;s&lt;/sub&gt; = λ&lt;sub&gt;sd&lt;/sub&gt;/(λ&lt;sub&gt;sd&lt;/sub&gt;+λ&lt;sub&gt;su&lt;/sub&gt;)</td>
</tr>
<tr>
<td>DC&lt;sub&gt;d&lt;/sub&gt;</td>
<td>Diagnostic Coverage of dangerous failures; DC&lt;sub&gt;d&lt;/sub&gt; = λ&lt;sub&gt;dd&lt;/sub&gt;/(λ&lt;sub&gt;dd&lt;/sub&gt;+λ&lt;sub&gt;du&lt;/sub&gt;)</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure In Time (1 FIT = 1 failure/10&lt;sup&gt;9&lt;/sup&gt; h)</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failure</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Repair</td>
</tr>
</tbody>
</table>

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

Relevant standards
- IEC 61508
  - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511-1
  - Functional safety - safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements
Safety requirements

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

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Low demand mode</th>
<th>High demand mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>$\geq 10^{-5} \ldots &lt; 10^{-4}$</td>
<td>$\geq 10^{-8} \ldots &lt; 10^{-6}$</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^{-4} \ldots &lt; 10^{-3}$</td>
<td>$\geq 10^{-7} \ldots &lt; 10^{-5}$</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^{-3} \ldots &lt; 10^{-2}$</td>
<td>$\geq 10^{-6} \ldots &lt; 10^{-4}$</td>
</tr>
<tr>
<td>SIL 1</td>
<td>$\geq 10^{-2} \ldots &lt; 10^{-1}$</td>
<td>$\geq 10^{-5} \ldots &lt; 10^{-3}$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFF</td>
<td>HFT = 0</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>60 % ... &lt; 90 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>90 % ... &lt; 99 %</td>
<td>SIL3</td>
</tr>
<tr>
<td>$\geq$ 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

Service proven

According to IEC 61511-1, paragraph 11.4.4, the failure tolerance HFT can be reduced by one for service-proven subsystems if the following conditions are met:

- The instrument is service proven
- Only process-relevant parameters can be modified on the instrument (e.g. measuring range, current output in case of failure …)
- These process-relevant parameters are protected (e.g. password, …)
- The safety function requires less than SIL4

The assessment by change management staff was a part of the "service proven" verification.

1.2 Planning

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:

<table>
<thead>
<tr>
<th></th>
<th>Overflow protection (max. operation)</th>
<th>Dry run protection (min. operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vibrating element in safe state</td>
<td>covered</td>
<td>uncovered</td>
</tr>
<tr>
<td>Output current in safe state</td>
<td>12.5 ... 23.5 mA</td>
<td>2.3 ... 11.5 mA</td>
</tr>
<tr>
<td>Failure current &quot;fail low&quot;</td>
<td>&lt; 2.3 mA</td>
<td>&lt; 2.3 mA</td>
</tr>
<tr>
<td>Failure current &quot;fail high&quot;</td>
<td>&gt; 23.5 mA</td>
<td>&gt; 23.5 mA</td>
</tr>
</tbody>
</table>
A safe failure exists when the measuring system switches to the defined safe state or the fault mode without the process demanding it. 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.

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 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".

If the "low demand rate" does not apply, the measuring system should be used as a safety-relevant subsystem in the mode "high demand mode" (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".

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 an non-dangerous malfunction is eight hours (MTTR = 8 h)

The processing unit can interpret "fail low" and "fail high" failures as a disruption 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

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 complied with. 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)
- Avoid solids > 5 mm (0.2 in) stored in the medium
- Avoid foam generation with a density of > 0.5 g/cm³ (0.018 lbs/in³)

1.3 Adjustment instructions

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

- DIL switch for sensitivity adjustment

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

1.4 Setup

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.

The exchange of the electronics is simple and described in the operating instructions manual. Note the instructions for parameter adjustment and setup.
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

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 functional efficiency 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 effect of 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 a multiple channel architecture this applies separately to each channel.

#### Simple function test

If the conditions of the following instructions are applicable, a simple function test can be triggered by interrupting the voltage supply for at least two seconds.

This can be the case through:

- Manual interruption of the supply cable
- Interruption of the supply cable through a connected control (SPLC)
- Pushing the Test key on a connected signal conditioning instrument (you can find suitable signal conditioning instruments in chapter "Technical data" of the operating instructions)

**Note:**

Conditions for the simple function test:

- A mechanical damage of the vibrating element as well as corrosion are excluded
- Buildup on the vibrating element which can cause a considerable damping of the vibrating frequency is excluded
- There should be no solid components in the medium which can jam in the tuning fork
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

<table>
<thead>
<tr>
<th></th>
<th>Overflow protection (max./A-operation)</th>
<th>Dry run protection (min./B-operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \lambda_{sd} )</td>
<td>35 FIT</td>
<td>141 FIT</td>
</tr>
<tr>
<td>( \lambda_{su} )</td>
<td>101 FIT</td>
<td>91 FIT</td>
</tr>
<tr>
<td>( \lambda_{gd} )</td>
<td>141 FIT</td>
<td>35 FIT</td>
</tr>
<tr>
<td>( \lambda_{gu} )</td>
<td>25 FIT</td>
<td>35 FIT</td>
</tr>
<tr>
<td>MTBF = MTTF + MTTR</td>
<td>3.31 x 10^6 h</td>
<td>3.31 x 10^6 h</td>
</tr>
</tbody>
</table>

Fault reaction time

Fault reaction time < 1.5 sec.

Specific characteristics

Single channel architecture (1oo1D)

<table>
<thead>
<tr>
<th>SIL</th>
<th>SIL2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFT</td>
<td>0</td>
</tr>
</tbody>
</table>

Instrument type Type A

<table>
<thead>
<tr>
<th>SFF</th>
<th>91 %</th>
<th>88 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFD_{avg}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( T_{proof} = 1 \text{ year} )</td>
<td>( &lt; 0.011 \times 10^{-2} )</td>
<td>( &lt; 0.016 \times 10^{-2} )</td>
</tr>
<tr>
<td>( T_{proof} = 5 \text{ years} )</td>
<td>( &lt; 0.055 \times 10^{-2} )</td>
<td>( &lt; 0.078 \times 10^{-2} )</td>
</tr>
<tr>
<td>( T_{proof} = 10 \text{ years} )</td>
<td>( &lt; 0.11 \times 10^{-2} )</td>
<td>( &lt; 0.155 \times 10^{-2} )</td>
</tr>
</tbody>
</table>

PFH < 0.025 x 10^{-6}/h < 0.035 x 10^{-6}/h

Time-dependent process of PFD_{avg}

The chronological sequence of PFD_{avg} is nearly linear to the operating time over a period up to 10 years. The above values apply only to the \( T_{proof} \) interval after which a recurring function test must be carried out.
Functional safety

OPTISWITCH series 5000 • two-wire

Fig. 1: Chronological sequence of $PFD_{avg}$ (figures see above charts)
1 $PFD_{avg} = 0$
2 $PFD_{avg}$ after 1 year
3 $PFD_{avg}$ after 5 years
4 $PFD_{avg}$ 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 measuring 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.