OPTISOUND 30*0 C Safety Manual

Ultrasonic Level Transmitter

4 … 20 mA/HART - two-wire
4 … 20 mA/HART - four-wire
# Contents

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

1.1 General information

Scope
This safety manual applies to measuring systems consisting of ultrasonic sensor OPTISOUND 3010 C, 3020 C, 3030 C in two-wire and four-wire 4…20 mA/HART versions:

OPTISOUND 3010 C
OPTISOUND 3020 C
OPTISOUND 3030 C

Valid hardware and software versions:
- Serial number of the electronics > 14455153
- Sensor software from Rev. 3.26

Application area
The measuring system can be used for level measurement of liquids and solids that meets the special requirements of safety engineering.

Due to the service-proven reliability, implementation is possible in a single channel architecture (1oo1D) up to SIL2 and in a multi-channel, diversitary redundant architecture up to SIL3.

The use of the measuring system in a multiple channel, homogeneous redundant architecture is excluded.

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

Abbreviations, terms

<table>
<thead>
<tr>
<th>SIL</th>
<th>Safety Integrity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
</tr>
<tr>
<td>PFD(_{avg})</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>(\lambda_{sd})</td>
<td>Rate for safe detected failure</td>
</tr>
<tr>
<td>(\lambda_{su})</td>
<td>Rate for safe undetected failure</td>
</tr>
<tr>
<td>(\lambda_{dd})</td>
<td>Rate for dangerous detected failure</td>
</tr>
<tr>
<td>(\lambda_{du})</td>
<td>Rate for dangerous undetected failure</td>
</tr>
<tr>
<td>DC(_S)</td>
<td>Diagnostic Coverage of safe failures; (DC_S = \lambda_{sd}/(\lambda_{sd}+\lambda_{su}))</td>
</tr>
<tr>
<td>DC(_D)</td>
<td>Diagnostic Coverage of dangerous failures; (DC_D = \lambda_{dd}/(\lambda_{dd}+\lambda_{du}))</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure In Time (1 FIT = 1 failure/10(^9) 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
1 Functional safety

- 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></td>
<td>$PFD_{av}$</td>
<td>$PFH$</td>
</tr>
<tr>
<td>4</td>
<td>$\geq 10^{-6} \ldots &lt; 10^{-4}$</td>
<td>$\geq 10^{-8} \ldots &lt; 10^{-6}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4} \ldots &lt; 10^{-3}$</td>
<td>$\geq 10^{-7} \ldots &lt; 10^{-5}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3} \ldots &lt; 10^{-2}$</td>
<td>$\geq 10^{-6} \ldots &lt; 10^{-4}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2} \ldots &lt; 10^{-1}$</td>
<td>$\geq 10^{-6} \ldots &lt; 10^{-5}$</td>
</tr>
</tbody>
</table>

Safety integrity of hardware for safety-related subsystems of type B (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>not permitted</td>
</tr>
<tr>
<td>60 % ... &lt; 90 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>90 % ... &lt; 99 %</td>
<td>SIL2</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 measuring system generates on the current output a signal between 3.8 mA and 20.5 mA corresponding to the level.

This analogue signal is transmitted to a connected processing unit to monitor the following conditions:

- Exceeding a preset level
- Falling below a preset level
When the switching point set on the processing unit is reached, a signal is outputted.

Safe state

The safe state depends on the mode:

<table>
<thead>
<tr>
<th>Monitoring upper level</th>
<th>Monitoring lower level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe state</td>
<td>Exceeding the switching point</td>
</tr>
<tr>
<td></td>
<td>Falling below the switching point</td>
</tr>
<tr>
<td>Output current in safe state</td>
<td>&gt; Switching point (-1 %)</td>
</tr>
<tr>
<td></td>
<td>&lt; Switching point (+1 %)</td>
</tr>
<tr>
<td>Failure current “fail low”</td>
<td>&lt; 3.6 mA</td>
</tr>
<tr>
<td>Failure current “fail high”</td>
<td>&gt; 21.5 mA</td>
</tr>
</tbody>
</table>

The current tolerance ±1 % refers to the full measuring range of 16 mA.

Fault description

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

If the internal diagnostic 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 state 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.

Configuration of the processing unit

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.

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 $P_{FD_{avg}}$ (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 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".

**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 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
- Existing communication interfaces (e.g. HART, I²C-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 complied with. The specifications of the operating instructions manual must not be exceeded.

The following critical process and vessel situations can cause measurement errors:

- Buildup on the transducer
- Flat or sharp-edged obstacles
- False reflections when agitators are used
- Foam generation above the medium
- Different gases above the medium (particularly CO₂)
- Strong temperature gradient above the medium

Probably smaller proof test intervals required!

**1.3 Instrument parameter adjustment**

Since plant conditions influence the functional safety of the measuring system, the instrument parameters must be set in compliance with the application.

The following tools are allowed:

- The DTM suitable for OPTISOUND 3010 C, 3020 C, 3030 C in conjunction with an adjustment software according to the FDT/DTM standard, e.g. PACTware
- Display and adjustment module
1 Functional safety

Note:
Make sure that DTM Collection 10/2005 or a newer version is used.

Create a measurement loop
If the measuring system has not been ordered especially for applications in safety-instrumented systems (SIS), the parameter "Sensor according to SIL" must be selected in the adjustment software in the menu level "Basic setting". If the display and adjustment module is used, the parameter "SIL" must be activated in the menu level "Service".

Reaction when malfunctions occur
The parameter adjustment of the interference current influences the safety-related characteristics. For safety-relevant applications only the following interference currents are permitted:
- fail low = <3.6 mA (default value)
- fail high = 22 mA

Damping of the output signal
The damping of the output signal must be adapted to the process safety time.

Inadmissible modes
Measured value transmission via HART signal as well as HART multidrop mode is not permitted.

Inspection possibilities
The effectivity of the set parameters must be checked in a suitable way.
- After connecting the instrument, the output signal jumps to the set interference current (at the end of the switch-on phase)
- In mode "Simulation", the signal current can be simulated independently of the actual level

Access locking
To avoid unwanted or unauthorized modification, the set parameters must be protected against unintentional access:
- Activate the password protection in the adjustment software
- Activate the PIN on the display and adjustment module

Access by means of HART handheld or similar equipment is not permitted.
Protecting against unintentional or unauthorized adjustment can be done, e.g. by sealing the housing cover.

Caution:
After a reset of the values, all parameters must be checked or readjusted.

1.4 Setup
Mounting and installation
Take note of the mounting and installation instructions in 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 testing the safety function and to find out possible undetected, dangerous failures. The functional capability of the measuring system has to be tested in adequate time intervals. It is up to the user's responsibility to select the kind of testing. The time intervals are subject to the PFD_{avg}-value according to the chart and diagram in section "Safety-relevant 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.

Please carry out the test in such a way, that the correct safety function in combination with all components is granted. This is granted by the control of the response height during a filling process. If a filling up to the response height is not practicable, the measuring system has to be responded by an appropriate 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.

### 1.7 Safety-related characteristics

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**

Applies to overfill and dry run protection:

| λ_{sd} | 0 FIT |
| λ_{su} | 458 FIT |
| λ_{sd} | 668 FIT |
| λ_{su} | 193 FIT |
| DC_{s} | 0 % |
| DC_{d} | 77 % |

| MTBF = MTTF + MTTR | 0.6 x 10^{6} h |

**Fault reaction time**

| E013 (no measured value available) | Application liquids | < 6 min |
| Application bulk solids | < 14 min |
| E013 (hardware error) | < 2 min |
| E036/E037 (no executable sensor software) | < 25 h |

**Specific characteristics**

| SIL | SIL2 |
| HFT | 0 |
| Instrument type | Type B |

Applies to overfill and dry run protection:

| SFF | 85 % |
| PFD_{avg} | |
| T_{Proof} = 1 year | < 0.085 x 10^{2} |
| T_{Proof} = 5 years | < 0.423 x 10^{2} |
| PFH | < 0.193 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.
Specific characteristics

If the measuring system is used in a multiple channel architecture, the safety-relevant characteristics of the selected structure of the measurement 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.

The measuring system must only be used in a diversitary redundant architecture!
KROHNE product overview

- Electromagnetic flowmeters
- Variable area flowmeters
- Ultrasonic flowmeters
- Mass flowmeters
- Vortex flowmeters
- Flow controllers
- Level meters
- Temperature assemblies
- Pressure transmitters
- Analysis products
- Products and systems for the oil and gas industry

KROHNE Messtechnik GmbH & Co. KG
Ludwig-Krohne-Straße 5
D-47058 Duisburg
Tel.: +49 (0) 203 301 0
Tel.: +49 (0) 203 301 10389
info@krohne.de

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