OPTISWIRL 4200  Supplementary Instructions

Vortex flowmeter

Safety manual
1 Introduction

1.1 Scope of the document
1.2 Revision history
1.3 Device description
1.4 Related documentation
1.5 Terms and definitions

2 Specification of the safety function

2.1 Preconditions
2.2 Safety application conditions (SAC)
  2.2.1 General
  2.2.2 Installation
  2.2.3 Functional safe configuration
  2.2.4 Maintenance
  2.2.5 Operation
  2.2.6 Homogeneous redundancy
2.3 Operation modes
2.4 Definition
2.5 Safety reaction and safe state

3 Operation

3.1 Preparation for SIL mode operation
  3.1.1 Entering the SIL mode key
  3.1.2 Parametrisation for SIL mode operation
  3.1.3 Verification of configuration
3.2 Reconfiguration of a device operated in SIL mode
3.3 Switch to non-SIL mode
3.4 Error conditions
3.5 Parameter types

4 Service

4.1 Maintenance
4.2 Availability of services
4.3 Operation modes and proof test
4.4 Resetting the fail-safe flags
4.5 Troubleshooting
CONTENTS

5 Technical data

5.1 General notes ................................................................................................................. 24
5.2 SIL certificate .................................................................................................................. 25
5.3 Declaration ..................................................................................................................... 26
5.4 Safety relevant key indicators ........................................................................................ 27
5.5 Measuring accuracy ....................................................................................................... 28
5.6 Useful lifetime ................................................................................................................ 29
5.7 Support for SIL-approved devices .................................................................................. 29

6 Appendix

6.1 Explanations to safety application conditions (SAC) ...................................................... 30
1.1 Scope of the document

This document is the safety manual for the OPTISWIRL 4200. Its content applies if the measurement device is operated in SIL mode or prepared for SIL mode, respectively.

General hint
This vortex flowmeter is a functionally safe flowmeter. It may be deployed within safety critical systems requiring the safety function (for details refer to Specification of the safety function on page 8) at a safety integrity level 2, in homogeneous redundant configuration at safety integrity level 3 (for more information about homogeneous redundancy refer to Operation modes on page 10).

In case of a detected potentially hazardous failure, the system performs a safety reaction to bring the device to a safe state, which is indicated by a failure current on the current output.

Depending on the failure, the device will resume the measuring mode as soon as the root cause of the failure disappears (transient application dependent failure) or remains in failure mode (persistent system integrity failure). In the latter case, operator’s interaction is required to restart measuring mode.

For safe operation, the operator / integrator must fulfil some conditions. These conditions are defined as Safety Application Conditions (SAC). For further information refer to Safety application conditions (SAC) on page 8.

INFORMATION!
The data in this supplement only contains the data applicable to the SIL approval. The technical data for the standard version in the handbook (document [N1]) shall be valid, provided that it is not rendered invalid or replaced by this supplement. If necessary, parts of [N1] are referenced herein.

INFORMATION!
Installation, commissioning and maintenance may only be carried out by properly trained and authorised personnel.

INFORMATION!
Configuration for SIL mode operation needs a login as role “Expert” (for details refer to [N1], chapter “Security and permissions”). Nevertheless the operator shall protect the flowmeter against unauthorised access.
1.2 Revision history

This safety manual is valid for all versions which are operated in SIL mode, identified by the V numbers according to the following tables, until its incompatibility with a new version is stated.

<table>
<thead>
<tr>
<th>Code</th>
<th>VG16/ SG16</th>
<th>a</th>
<th>b</th>
<th>cde</th>
<th>f</th>
<th>gh</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
<th>m</th>
<th>n</th>
<th>o</th>
<th>p</th>
<th>q</th>
<th>rst</th>
<th>vwx</th>
<th>z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional safety relevant</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Valid flow sensor codes for SIL device variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>VG16/SG16</td>
<td>Prefix to code</td>
<td>-</td>
</tr>
<tr>
<td>a</td>
<td>Manufacturer specific</td>
<td>-</td>
</tr>
<tr>
<td>b</td>
<td>General information</td>
<td>1, 3, L, M, N</td>
</tr>
<tr>
<td>cde</td>
<td>Flange connection, rating and sealing surface</td>
<td>-</td>
</tr>
<tr>
<td>f</td>
<td>Measuring section</td>
<td>-</td>
</tr>
<tr>
<td>gh</td>
<td>Pressure sensor options and gaskets</td>
<td>-</td>
</tr>
<tr>
<td>i</td>
<td>Approvals for hazardous and ordinary locations</td>
<td>-</td>
</tr>
<tr>
<td>j</td>
<td>Signal converter housings</td>
<td>1, 2, 4, 5, 7, A, B, D, E</td>
</tr>
<tr>
<td>k</td>
<td>System design</td>
<td>0 only</td>
</tr>
<tr>
<td>l</td>
<td>Display</td>
<td>1 only</td>
</tr>
<tr>
<td>m</td>
<td>Cable glands</td>
<td>-</td>
</tr>
<tr>
<td>n</td>
<td>Firmware feature</td>
<td>-</td>
</tr>
<tr>
<td>o</td>
<td>Programming language</td>
<td>-</td>
</tr>
<tr>
<td>p</td>
<td>Communication options</td>
<td>0 only</td>
</tr>
<tr>
<td>q</td>
<td>Marking</td>
<td>-</td>
</tr>
<tr>
<td>rstuvwx</td>
<td>Diverse certificates (CoC, calibration, pressure testing, material, hardness testing, cleaning, X-ray/dye penetration)</td>
<td>-</td>
</tr>
<tr>
<td>y</td>
<td>Manual</td>
<td>-</td>
</tr>
<tr>
<td>z</td>
<td>Spare</td>
<td>-</td>
</tr>
</tbody>
</table>

**INFORMATION!**

Check in case a firmware is updated or any part of the device is replaced, whether a new safety manual is available on the manufacturer’s internet site.

<table>
<thead>
<tr>
<th>Release date</th>
<th>Electronic revision</th>
<th>Changes and compatibility</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-07-10</td>
<td>ER 2.0.0_</td>
<td>Initial version</td>
<td>AD OPTISWIRL 4200 SIL R01</td>
</tr>
<tr>
<td>2017-10-01</td>
<td>ER 2.0.1_</td>
<td>Sensor diagnostics update</td>
<td>AD OPTISWIRL 4200 SIL R02</td>
</tr>
</tbody>
</table>
1.3 Device description

The OPTISWIRL 4200 is a 2-wire vortex flowmeter measuring volume flow rate, temperature and optionally pressure of liquids, steam and gases. From these data the device calculates normalised flow rate, mass flow rate, power flowrate, etc.

In SIL mode the OPTISWIRL 4200 measures the volume flow rate and outputs the measurement via the safe 4...20 mA current output.

For measurement in SIL mode the following conditions apply:

- The 4...20 mA current output provides a safe output exclusively.
- Local display, HART® Interface and the binary output do not provide a safe output.
- The local display and HART® Interface are read-only during SIL mode.
- Parameters can only be changed in non-SIL mode.
- The binary output can also be used in order to provide non-safety related measurement values.
- The current input can be used for non-safety related functionalities.

1.4 Related documentation

[N1] OPTISWIRL 4200 Handbook
## 1.5 Terms and definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC</td>
<td>Diagnostic Coverage of dangerous failures</td>
</tr>
<tr>
<td>EUC</td>
<td>Equipment Under Control</td>
</tr>
<tr>
<td>Firmware</td>
<td>Software embedded in the device</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure In Time (1x10^-9 failures per hour)</td>
</tr>
<tr>
<td>FMEDA</td>
<td>Failure Modes, Effects and Diagnostics Analysis</td>
</tr>
<tr>
<td>FRT</td>
<td>Fault Response Time (diagnostic test interval + Fault Reaction Time)</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>I/O</td>
<td>Input / output</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>$\lambda_{SD}$</td>
<td>Rate for safe detected failure</td>
</tr>
<tr>
<td>$\lambda_{SU}$</td>
<td>Rate for safe undetected failure</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Repair</td>
</tr>
<tr>
<td>MTR</td>
<td>Mean Time To Restoration</td>
</tr>
<tr>
<td>PFDAVG</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>PFH</td>
<td>Probability of a dangerous Failure per Hour</td>
</tr>
<tr>
<td>PTC</td>
<td>Proof Test Coverage</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented Systems</td>
</tr>
<tr>
<td>Systematic Capability</td>
<td>Measure [expressed on a scale of SC 1 to SC 4] of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions.</td>
</tr>
<tr>
<td>Type A system</td>
<td>“Non-complex” system [all failure modes are well defined]. For more data, refer to subsection 7.4.3.1.2 of IEC 61508-2.</td>
</tr>
<tr>
<td>Type B system</td>
<td>“Complex” system [all failure modes are not well defined]. For more data, refer to subsection 7.4.3.1.2 of IEC 61508-2.</td>
</tr>
<tr>
<td>$T_{Proof}$</td>
<td>Proof Test Interval</td>
</tr>
<tr>
<td>$T_{Repair}$</td>
<td>Time to Repair</td>
</tr>
<tr>
<td>$T_{Test}$</td>
<td>Internal Diagnostics Test Interval</td>
</tr>
<tr>
<td>1oo1</td>
<td>1 out of 1 channel architecture [single architecture performs the safety function]</td>
</tr>
<tr>
<td>1oo1D</td>
<td>1 out of 1 channel architecture with diagnostics</td>
</tr>
</tbody>
</table>
2.1 Preconditions

The device must be operated within the process and ambient conditions specified in the handbook ([N1]) of the device.

The following chapter defines additional conditions, which have to be obeyed for safety applications.

2.2 Safety application conditions (SAC)

**INFORMATION!**
This chapter defines the conditions which must be met by the operator to ensure safe operation. Further explanations can be found in appendix I. The safety application condition is valid, while the related explanation might be incomplete.

2.2.1 General

**SAC1: System changes**
The flowmeter can be deployed as device with safety responsibility. Non specified changes are not allowed. Especially after maintenance measures, carrier and operator must ensure that no hazardous states came up, and that all safety application conditions are still met.

2.2.2 Installation

**SAC2: Mounting and connecting**
[N1] defines requirements regarding installation and electrical connections of the device. These requirements are safety critical and must be strictly observed.

2.2.3 Functional safe configuration

**SAC3: SIL mode**
The flowmeter is functionally safe only if configured for operation in SIL mode.

**SAC4: Parameter input**
Parameters are changed under responsibility of the operator.

2.2.4 Maintenance

**SAC5: Maintenance mode**
If maintenance mode (for definition refer to Operation modes on page 10) is entered, the device is operated under responsibility of the operator.

**SAC6: Resetting the fail-safe flag**
Resetting the fail-safe flag is done under responsibility of the operator. He is responsible for the correct execution of appropriate tests and the evaluation of test results.

**SAC7: Firmware update**
Firmware may be updated by authorised personnel only.
SAC8: Inspection intervals

The definition of the maximum proof test intervals [for details refer to Operation modes and proof test on page 19] are calculated for operation under reference conditions. The operator is responsible for adjusting the proof test intervals if the deployment conditions deviate from the reference conditions.

SAC9: Modification

The flowmeter must not be manipulated.

SAC10: Repair

Repair of the flowmeter must only be done by manufacturer’s personnel or personnel authorised by the manufacturer. Exceptions regarding replacement with spare parts are shown in chapter “Service” in [N1]. In all other cases, send the flowmeter to the manufacturer for repair [for instructions refer to chapter “Returning the device to the manufacturer” in [N1]].

2.2.5  Operation

SAC11: Operational limits

The operational limits as shown in [N1] in the chapter “Technical data” must be observed. To prevent unintentional trigger of the safety reaction, a permanent operation near the operational limits should be avoided.

SAC12: Supervision of failure current

If a safety critical failure has been detected, the device outputs a failure current on the current output (4...20 mA). The operator must supervise both failure currents (< 3.6 mA and > 21 mA).

In case of the occurrence of any failure current the operator has to ensure that the safety loop reacts according to relevant application specific norms [e.g. the safety loop must be prevented from automatically resuming operation after failure notification disappears].

2.2.6 Homogeneous redundancy

SAC13:

The logic subsystem must compare the current values transmitted by the two flowmeters (or one dual version respectively) permanently. In case of a difference greater than 4% of the measurement range over a time interval greater than 30 seconds, the devices must be regarded as non-safe, or defect respectively.

SAC14:

The two flowmeters (or one dual version respectively) must be operated independently. Any hazardous re-activeness from the logic subsystem [for details refer to Operation modes on page 10] on the two measurement devices must be excluded. This means at least:

- Current loops are independently driven.
- Current loops are installed in a way that failures affecting both lines at a time [common cause] can be avoided.
- The logic subsystem must provide an appropriate low failure rate.
2.3 Operation modes

SIL mode
In SIL mode, the device executes the safety function and will react safely if an error is detected which prevents the correct execution of the safety function. In this mode, the device is functionally safe and the safety relevant key figures like hazard rate, FRT etc. can be guaranteed.

Non-SIL mode
In non-SIL mode, the device operates as a standard device. Its behaviour is state-of-the-art, its specific functionality depends on the individual, customised parameter settings.

Maintenance mode
Maintenance mode is intended to boot a potentially defect device in order to test it in its normal operational environment. During this time, operation is done under responsibility of the operator. To avoid improvident and unintentional entering of the maintenance mode the operator is requested to enter the password for "Expert" level access.

By entering the (correct) password, the operator acknowledges the above regulation regarding responsibility, also regarding safety responsibility if the device is operated in SIL mode.

As the maintenance mode is intended for testing, the operator shall provide additional measures to secure the safety of the overall system. Therefore, the operator shall install additional measures to provide safety of the overall system.
Homogeneous redundancy
The degree of a functional safe device is determined by the accomplished qualitative safety integrity level and the quantitative hazard rate determined by the failure rate of the deployed hardware.

If two or more identically constructed devices are used in parallel (device A is of the same type as device A' like the "Dual Version"), the hazard rate for the combination (here: sensor subsystem) can be reduced.

A precondition for this is a logic subsystem comparing the output of devices A and A': The complete sensor subsystem fails if at least one of the two devices fails (availability is reduced to 50% of the value of a single device A!).

![Figure 2-1: Homogeneous redundancy](image)

2.4 Definition
The flowmeter provides a safety function according to the international standard IEC 61508 [N2]. It is defined as follows:

**Output of the volume flow rate at the 4...20 mA current output with a maximum delay of 30 seconds and a measurement accuracy better than 4%.**

Remarks
- The function is always and only executed in SIL mode.
- The measurement uncertainty of the flowmeter in safe operation equals to those in non-SIL operation as described in [N1]. It consists of the uncertainty of measurement function and current output.
- Concerning random errors in the device, the safety tolerance must be considered. The safety tolerance is the tolerable error before setting the safe state of the device. A random fault can cause an error of up to 2% of the present measurement value or output current before it is signaled. For further information refer to Measuring accuracy on page 28.
2.5 Safety reaction and safe state

As soon as a failure is detected, the vortex flowmeter reacts safely, by setting the current output to the low or high failure current (safety reaction). As an additional feature, temporary and persistent failures can be distinguished:

- A failure current of approximately 3.5 mA is output in case of a transient failure.
- A failure current of approximately 3.35 mA or below, is output in case that a persistent failure is assumed. A device with a persistent failure will not boot into SIL mode without operator’s interaction (for details refer to Troubleshooting on page 23).

Remarks

- The decision whether a failure is transient or persistent will be made within 30 seconds after its detection.
- A too low volume flow (below the lower sensor limit) is classified as a typical transient application dependent failure.
- Some failures will prevent the output of the lower failure current. In such cases, the device tries to output the high failure current (> 21 mA).
- The fault response time is 30 seconds. Any output older than 30 seconds is correct if the safety reaction is not triggered due to a safety critical device failure.
3.1 Preparation for SIL mode operation

For execution of the safety function, the device must be unlocked for SIL mode operation and configured for SIL mode.

Devices, which have been ordered as SIL devices, have been unlocked for SIL mode by factory setting. Devices, which have not been ordered as SIL devices, must be unlocked with a key code. Please contact the manufacturer for registration and individual 4-digit key code.

The preparation for SIL mode is done in three steps:

1. Unlocking of the SIL mode by entering the SIL mode key code (Not applicable for devices ordered as SIL devices [for details refer to Entering the SIL mode key on page 13].
2. Setup the device for SIL mode operation (for details refer to Parametrisation for SIL mode operation on page 14).
3. Verification of the actual configuration and subsequent confirmation of successful verification by setting the SIL jumper (for details refer to Verification of configuration on page 14).

3.1.1 Entering the SIL mode key

This step has only to be performed once before the first configuration for SIL mode operation. It is only applicable for devices, which have not been ordered as SIL devices. For basic principles of local display operation and menu structure overview refer to [N1].

INFORMATION!
For entering the SIL mode key code it is required to gain “Expert” access level before (for details refer to [N1], chapter “Security and permissions”).

<table>
<thead>
<tr>
<th>Menu</th>
<th>To do</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter menu</td>
<td>Enter menu</td>
<td>1 x →</td>
</tr>
<tr>
<td>A Quick Setup</td>
<td>Go to “C Setup”</td>
<td>2 x ↓</td>
</tr>
<tr>
<td>C Process</td>
<td>Go to “C6 Device”</td>
<td>1 x →, 5 x ↓</td>
</tr>
<tr>
<td>C6 Device</td>
<td>Go to “C6.2 Security”</td>
<td>1 x →, 1 x ↓</td>
</tr>
<tr>
<td>C6.2 Security</td>
<td>Go to “C6.2.4 Unlock SIL”</td>
<td>1 x →, 3 x ↓</td>
</tr>
<tr>
<td>C6.2.4 Unlock SIL</td>
<td>Enter menu and unlock SIL by entering the four digits of the password, confirm with enter key</td>
<td>1 x →, ****, 1 x ←↓</td>
</tr>
</tbody>
</table>

After entering the SIL mode key code and confirming with enter key, return to measuring mode.

INFORMATION!
Before switching to SIL mode the customer has to ensure the proper condition of the device. In case of any doubt, a Proof Test may be performed. Previous hours of operation have to be taken into account for failure rate calculation.
### 3.1.2 Parametrisation for SIL mode operation

<table>
<thead>
<tr>
<th>Display indication</th>
<th>To do</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press &gt; button to enter SIL setup</td>
<td>Enter SIL configuration menu</td>
<td>1 x (\rightarrow)</td>
</tr>
<tr>
<td>A Quick Setup</td>
<td>Change parameters in “Quick Setup” or “Setup” as described in [N1]</td>
<td>-</td>
</tr>
<tr>
<td>Leave Quick Setup” or “Setup”</td>
<td>“Save Configuration?” [only displayed, if any parameter has been changed]</td>
<td>Confirm settings with “YES” or cancel all changes with “NO”</td>
</tr>
<tr>
<td>Switch to SIL mode?</td>
<td>Confirm switching to SIL mode with “YES” or cancel with “NO”</td>
<td>YES / NO (\leftarrow)</td>
</tr>
<tr>
<td>If last question was confirmed with “YES”: “Password?”</td>
<td>Enter password for “Expert” [refer to [N1], chapter “Security and permissions”]</td>
<td>**** (\leftarrow)</td>
</tr>
<tr>
<td>Wait for reboot</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If question “Switch to SIL mode?” has been confirmed with “YES”, the operator will be requested to enter the password for the access level “Expert” [refer to [N1], chapter “Security and permissions”] and the system will reboot automatically. If question “Switch to SIL mode?” has been refused with “NO”, the device will stay in non-SIL mode. Nevertheless, the changed parameters are stored persistently.

By displaying “Press key for verification” the device shows preparedness for verification of the SIL configuration.

### 3.1.3 Verification of configuration

During configuration verification, the device will output the complete range between 4 and 20 mA in 2 mA steps and the failure currents <3.6 and >21 mA. Each value will be held for approx. 2 seconds (after the output of >21 mA, the next output will be <3.6 mA again).

The test is performed in an endless loop which can be terminated by setting the SIL jumper or by refusing the SIL mode request [for details refer to Reconfiguration of a device operated in SIL mode on page 15].

**Required equipment**
- Calibrated current meter

**Execution of the verification**

**The parameter verification is performed as follows:**
- Integrate a calibrated current meter into the current loop.
- The device will perform an automatic restart.
- Confirm request “Press key for verification” by pressing any key.
- Check carefully, whether the device shows <3.6, 4 mA, 6 mA…20, >21 mA in a loop.
- Confirm request “Set SIL jumper or press key to cancel” by setting the SIL jumper or refuse switch to SIL mode by pressing any key.
Setting of the SIL jumper

- Remove the display while device is powered (for details refer to [N1], chapter “Turning the display”).
- Set the jumper to SIL position as shown in the figures below.
- Reattach the display.

After setting the jumper to the SIL position, the flowmeter will perform an automatic reboot and start operation in SIL mode. The operation in SIL mode is indicated by a small SIL logo.

3.2 Reconfiguration of a device operated in SIL mode

The device must be set to non-SIL mode first, before any parameter can be changed, as changing of parameters is prohibited in SIL mode.

Follow the steps shown in the next chapter and then reconfigure the device.
3.3 Switch to non-SIL mode

In order to switch the device from SIL mode to non-SIL mode the following steps have to be performed.

- Remove the display (for details refer to [N1], chapter “Turning the display”).
- Set the jumper to non-SIL position (for details refer to Preparation for SIL mode operation on page 13).
- Reattach the display.
- The flowmeter will perform an automatic reset.
- Confirm request “Press key for verification” by pressing any key.
- Refuse request “Set SIL jumper or press key to cancel” by pressing any key.
- Enter password for access level “Expert”.

The device will now perform an automatic reboot and start operation in non-SIL mode.

3.4 Error conditions

In principle, the error conditions for non-SIL mode and SIL mode are the same [refer to chapter “Status messages and diagnostic information” in N1].

In SIL mode, the following special conditions apply additionally:

- Safety critical failures will always result in an output of a failure current.
- The failure current is the only safety relevant signal. Regarding the safe state of the device, all other interfaces must be ignored (Example: a failure current indicates a safety critical defect, even if the HART® interface is still online).
- Due to power considerations, the lower failure current is the pre-defined failure current. The related user’s configuration in non-SIL mode is ignored in SIL mode. High failure current will only be set if the lower failure current cannot be output for any reasons.
- The events shown in the following table are SIL specific, i.e. they will occur only if the device is operated in SIL mode.

<table>
<thead>
<tr>
<th>Status type</th>
<th>Event group</th>
<th>Description</th>
<th>Actions to eliminate the event</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Electronics</td>
<td>Emergency off triggered</td>
<td>Restart the device according to given procedure (for details refer to Resetting the fail-safe flags on page 23).</td>
</tr>
</tbody>
</table>
### 3.5 Parameter types

In SIL mode the device parameters are distinguished in three parameter types. Two types affect safety:

- **Safety critical data**: These parameters have a fixed setting and cannot be changed but read only. They are marked with a padlock symbol.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Fixed setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Out. Meas.</td>
<td>Volume Flow</td>
<td>Index of the device variable which is mapped to the current output.</td>
</tr>
<tr>
<td>4mA Trimming</td>
<td>0.004 [A]</td>
<td>The externally measured analogue level during trimming (user calibration) of the “Analog Lower Endpoint Value”.</td>
</tr>
<tr>
<td>20mA Trimming</td>
<td>0.020 [A]</td>
<td>The externally measured analogue level during trimming (user calibration) of the “Analog Upper Endpoint Value”.</td>
</tr>
<tr>
<td>High Error Current</td>
<td>0.0215 [A]</td>
<td>High failure current.</td>
</tr>
<tr>
<td>Low Error Current</td>
<td>0.0035 [A]</td>
<td>Low failure current.</td>
</tr>
<tr>
<td>Analog Lower Endpoint Value</td>
<td>0.004 [A]</td>
<td>Corresponds to 0% range and therefore to the “Lower Range Value” of the range conversion.</td>
</tr>
<tr>
<td>Lower Ext. Range</td>
<td>0.004 [A]</td>
<td>The minimum value that the analogue channel is capable of or is limited to.</td>
</tr>
<tr>
<td>Analog Upper Endpoint Value</td>
<td>0.02 [A]</td>
<td>Corresponds to 100% range and therefore to the “Upper Range Value” of the range conversion.</td>
</tr>
<tr>
<td>Upper Ext. Range</td>
<td>0.02 [A]</td>
<td>The maximum value that the analogue channel is capable of or is limited to.</td>
</tr>
<tr>
<td>Error Function</td>
<td>ALARMSELECTION LOW</td>
<td>States whether the alarm is indicated with high or low signal level or not at all.</td>
</tr>
<tr>
<td>Current Loop Mode</td>
<td>ON</td>
<td>A switch for enabling/disabling loop current signalling. ON: HART® multidrop mode is disabled.</td>
</tr>
<tr>
<td>k-Factor / Offset</td>
<td>0.0</td>
<td>Offset value to adapt k-factor.</td>
</tr>
<tr>
<td>k-Factor Linear. / Function</td>
<td>OFF</td>
<td>Switches the k-factor linearisation on/off.</td>
</tr>
<tr>
<td>Temp. Comp. / Function</td>
<td>ON</td>
<td>Setup of k-factor temperature compensation.</td>
</tr>
<tr>
<td>Lin. Thermal Exp. 1/K</td>
<td>0.0000175 [per Kelvin]</td>
<td>Coefficient of linear thermal expansion (bluff body).</td>
</tr>
<tr>
<td>Min/Max Oper. Dens. / Function</td>
<td>OFF</td>
<td>Switch for use of upper and lower densities for calculation of sensor limits.</td>
</tr>
<tr>
<td>Sensor Overrange</td>
<td>0</td>
<td>Is used to determine the high flow cutoff factor.</td>
</tr>
<tr>
<td>Vortex Algorithm / Filter Mode</td>
<td>FULL AUTO SETTINGS</td>
<td>Filter configuration: “FULL_AUTO_SETTINGS” means that all settings are derived from Pickup configuration.</td>
</tr>
<tr>
<td>Vortex Algorithm / Min. Amplitude</td>
<td>0.01 [V]</td>
<td>Indicator for valid measurement of vortex frequency.</td>
</tr>
<tr>
<td>Gain CA</td>
<td>0</td>
<td>Piezo configuration.</td>
</tr>
<tr>
<td>VA Piezo Test Mode (no menu entry available)</td>
<td>PIEZO TESTMODE OFF</td>
<td>Piezo configuration.</td>
</tr>
<tr>
<td>Distortion Reduction / Function</td>
<td>ON</td>
<td>Amplitude correction.</td>
</tr>
</tbody>
</table>
**Safety relevant data:** These parameters can be changed under responsibility of the operator. Misconfiguration via erroneous setting is detected by the parameter verification procedure which is executed automatically if the device is setup for SIL mode and parameters have been changed (for details refer to Preparation for SIL mode operation on page 13).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Fixed setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distortion Reduction / $K_P$</td>
<td>204011</td>
<td>Amplitude correction P-factor.</td>
</tr>
<tr>
<td>Distortion Reduction / $K_I$</td>
<td>140737</td>
<td>Amplitude correction I-factor</td>
</tr>
<tr>
<td>Distortion Reduction / Smoothing Factor</td>
<td>2141041197</td>
<td>Amplitude correction filter factor.</td>
</tr>
<tr>
<td>Vortex Filter / Filter Length</td>
<td>25</td>
<td>Output filter length.</td>
</tr>
<tr>
<td>Vortex Filter / Smoothing Factor</td>
<td>0.05</td>
<td>Output filter smoothing factor.</td>
</tr>
<tr>
<td>Vortex Algorithm / Min. SNR</td>
<td>50.0</td>
<td>Indicator for valid measurement of vortex frequency.</td>
</tr>
<tr>
<td>Time Constant</td>
<td>2.0 [s]</td>
<td>Time constant (for filter).</td>
</tr>
<tr>
<td>Low Flow Cutoff</td>
<td>0.0 [cubic meters per second]</td>
<td>Low flow cutoff (When the flow rate drops below low flow cutoff, the current output is 4 mA)</td>
</tr>
<tr>
<td>Minimum hold time transient error (no menu entry available)</td>
<td>5000 [ms]</td>
<td>Minimum hold time of the failure current in case of transient errors.</td>
</tr>
<tr>
<td>Vortex Algorithm / Extended Sensor Limits</td>
<td>OFF</td>
<td>Extended sensor limits</td>
</tr>
</tbody>
</table>

**Non-SIL data:** These parameters do not have any influence on the safety function and may be changed as in non-SIL mode.

The parametrisation in SIL mode works as described in chapter "Operation" in [N1] for the most parameters. However, there are some parameters which have an influence on functional safety if set incorrectly.

For every safety affecting parameter, two values, potentially equal ones, exist in the device: one is used for non-SIL, the other for SIL operation. Depending on the device's state, either the one parameter set or the other is shown or can be edited. As soon as the SIL mode is requested, the SIL mode parameters become active.
4.1 Maintenance

You must follow the maintenance instructions given in the handbook [N1].

4.2 Availability of services

The manufacturer offers a range of services to support the customer after expiration of the warranty. These include repair, maintenance, technical support and training.

INFORMATION!
For more precise information, please contact your local sales office.

4.3 Operation modes and proof test

Continuous and high demand mode
If the flowmeter is operated in continuous or high demand mode within the specified environmental limits, the device needs no proof test during its useful lifetime (for details refer to Useful lifetime on page 29). Observe SAC 11 regarding useful lifetime and constant failure rates, respectively.

Low demand mode
The flowmeter includes a comprehensive set of online diagnostic tests which are executed fast and frequently, resulting in a very low mean down time. Assuming reasonable low repair and restoration times as well, the device fulfils SIL2 compatible PFD values as well during the whole useful life time without additional proof tests.

Proof test
Proof tests are required in case of:

• Deployment under extreme conditions beyond the device’s specification. In this case, environmental conditions might increase the failure rate. To keep undetected failures small such deployment requires more frequent proof tests. For details refer to Useful lifetime on page 29, operational limits as set forth in SAC 11 must not be exceeded.
• Achieving the required PFD_{AVG} over time.

WARNING!
SIS engineers must calculate the interval of proof tests based on the required PFD_{AVG}.

For this purpose, the following tests can be performed. The diagnostic coverage of all tests together is nearly as good as the tests and procedures in the factory which were executed during or at the end of the production cycle. Only flow sensor calibration is missed here which requires a reference meter.
Proof test coverage

<table>
<thead>
<tr>
<th>Step</th>
<th>Measure</th>
<th>Proof Test Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>Current output verification via OPTICHECK [N4]</td>
<td>12%</td>
</tr>
<tr>
<td>1b</td>
<td>Current output check according to routine in chapter “Verification of configuration”.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Test with simulated vortex frequencies.</td>
<td>96%</td>
</tr>
</tbody>
</table>

Calibration verification (optional)

A proof test coverage of > 97% can be reached with a calibration verification. If appropriate facilities are not available, please contact the manufacturer for calibration verification.

Test with simulated vortex frequencies (step 2)

Required equipment

- Power supply 14…30 VDC
- Calibrated frequency generator, accuracy << 1%, two channels 180° phase shifted, 100 mVpp amplitude (step 2)
- Calibrated current meter (steps 1b and 2)
- OPTICHECK (optionally; step 1a)

Execution of frequency simulation for the proof test

To setup the device for proof testing, the following steps have to be performed:

- Set the device to non-SIL mode (for details refer to Switch to non-SIL mode on page 16).
- Unfix the electronics housing by loosening the 4 cylinder screws ① and take off the electronics housing carefully.

Figure 4-1: Unfixing of the electronics housing

① Cylinder screws
② Washers
③ Gasket
• Integrate a current meter into the current loop.
• Disconnect the 3-pole plug and connect a frequency generator as illustrated below.
  The 2-pole and 5-pole plugs must remain connected!

![Diagram of frequency generator connection](image)

**Figure 4-2: Connection of frequency generator**
1. Frequency f1
2. Grounding
3. Frequency f2, phase-shifted by 180° compared to f1

• Set start frequencies f1 and f2 to almost 0 Hz.
• Connect the flowmeter with the power supply.
• Boot the device.
• Confirm request "Press key for verification" by pressing any key.
• Login as "Expert".
• After reboot of the device activate proof test as follows:

<table>
<thead>
<tr>
<th>Menu/display</th>
<th>To do</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter menu</td>
<td></td>
<td>1 x →</td>
</tr>
<tr>
<td>A Quick Setup</td>
<td>Go to “C Setup”</td>
<td>2 x ↓</td>
</tr>
<tr>
<td>C Setup</td>
<td>Go to “C6 Device”</td>
<td>1 x →, 5 x ↓</td>
</tr>
<tr>
<td>C6 Device</td>
<td>Go to “C6.8 Proof Test”</td>
<td>1 x →, 6 x ↓</td>
</tr>
<tr>
<td>C6.8 Proof Test</td>
<td>Enter “Proof Test”</td>
<td>1 x →</td>
</tr>
<tr>
<td>“Unsaved parameters will be lost!”</td>
<td>Confirm warning with enter</td>
<td>1 x ←↓</td>
</tr>
<tr>
<td>“Run Proof Test?”</td>
<td>Confirm start of proof test with “YES” or cancel with “NO”</td>
<td>YES / NO ←↓</td>
</tr>
</tbody>
</table>

If question "Confirm start of proof test?" has been confirmed with "YES", the device is prepared for proof test and displays "Proof Test is running...".
• Increase frequencies stepwise. The loop current must follow according to the following table:

<table>
<thead>
<tr>
<th>Frequency [Hz]</th>
<th>Nominal current [mA]</th>
<th>Acceptable current range [mA]</th>
</tr>
</thead>
<tbody>
<tr>
<td>355</td>
<td>4.0</td>
<td>3.96...4.04</td>
</tr>
<tr>
<td>817</td>
<td>8.5</td>
<td>8.41...8.58</td>
</tr>
<tr>
<td>1229</td>
<td>12.5</td>
<td>12.38...12.63</td>
</tr>
<tr>
<td>1636</td>
<td>16.5</td>
<td>16.30...16.63</td>
</tr>
<tr>
<td>2000</td>
<td>20.0</td>
<td>19.81...20.21</td>
</tr>
</tbody>
</table>

• Continue only if test is successful. Stop if any current is out of the accepted limits!
• To finish or cancel the proof test press "Enter". The device will display "Device will be reset now!" and perform an automatic reboot after pressing the "Enter" key once again.
• Re-attach the electronics housing: Carefully place the electronics housing with the gasket on the device as shown in the figure "Unfixing of the electronics housing". Pay attention not to pinch the cable! Fasten the cylinder screws including the washers with a bolting torque of 8 Nm.

**INFORMATION!**
A current value below or above the acceptable limits is an indicator for wear out of the electronics. Please refer to chapters "Maintenance" and "Availability of service".

**INFORMATION!**
The frequency test does not consider the sensor element, configuration and drift errors.
4.4 Resetting the fail-safe flags

Rebooting of a device operated in SIL mode with a detected safety critical failure is inhibited. In this case, the following message is shown on the display:

SIL locked!
Press key to start test

The test is performed under full responsibility of the operator! The device will operate in SIL mode to allow extensive testing, but the SIL tag is not shown in the header bar on the display (because the device is actually non-safe!). Consequently, additional measures should be installed to prevent the overall system from safety critical failures. The flowmeter might be defect persistently!

**INFORMATION!**
In case of any doubt, call the service department of the manufacturer and leave the device in the current safe state!

<table>
<thead>
<tr>
<th>Menu/display</th>
<th>To do</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL locked!</td>
<td>Start maintenance mode under full responsibility of the operator for testing purposes.</td>
<td>Any key.</td>
</tr>
<tr>
<td>Password?</td>
<td>Enter the 4 digit “Expert” password.</td>
<td>**** ←</td>
</tr>
<tr>
<td>Clear fail safe flag?</td>
<td>Clear if the device is intact without doubt; do not clear otherwise!</td>
<td>YES / NO ←</td>
</tr>
<tr>
<td>Password?</td>
<td>Enter the 4 digit “Expert” password.</td>
<td>**** ←</td>
</tr>
<tr>
<td>Wait for reboot</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

4.5 Troubleshooting

**INFORMATION!**
- Modifications to SIL capable devices by the user are not permitted.
- Only authorised personnel from the manufacturer shall repair the device.

Failures that are critical to functional safety must be reported to technical support of the manufacturer. If you find a problem, please contact your local representative. If the device must be returned to the manufacturer, refer to “Returning the device to the manufacturer” in [N1].
5.1 General notes

- The safety relevant key indicators (for details refer to Safety relevant key indicators on page 27) are related to the safety function (for details refer to Operation modes on page 10).
- Commissioning and use of the device presupposes agreement with its design and performance characteristics. This includes ambient and process conditions (refer to handbook [N1]).
- The values shown in the table for the safety relevant key indicators have been determined for an environmental temperature of +40°C / +104°F and below. For higher temperatures refer to Useful lifetime on page 29.
- Failure rates are assumed to be constant during the useful lifetime (for details refer to Useful lifetime on page 29).
- Failure rates do not include mechanical wear of the sensor and bluff body. The operator is responsible for observing the specification for intended use (refer to chapter "Intended use" in [N1], respectively for adequate inspections if the device is deployed out of specification and damages caused by the process need to be assumed.
- Installation of the device must be in accordance with the instructions and the requirements of the application.
- All components that are not necessary to execute the safety function and cannot influence the safety function are not included in the calculation of the failure rates.
- External power failure rates are not included in the calculation of the failure rates.
- The FMEDA of the device was calculated with the exida tool FMEDA v7.1.17. The tool uses the latest values from the database SN 29500 [N3].
5.2 SIL certificate

CERTIFICATE
No. Z10 17 02 90730 003

Holder of Certificate: KROHNE Messtechnik GmbH
Ludwig-Krohne-Str. 5
47058 Duisburg
GERMANY

Factory(ies): 90730

Certification Mark:

Product: Safety Related Programmable Electronic System

Model(s): OPTISWIRL 4200

Parameters:
Safety Parameters:
HPT=0 / SIL.2
HPT=1 / SIL.3

The report and the user documentation in the current valid revision are mandatory part of this certificate. The product complies with the following safety requirements only if the specifications documented in the currently valid revision of this report are met.

Tested according to:
IEC 61508-1(ed.2) (SIL 2)
IEC 61508-2(ed.2) (SIL 2)
IEC 61508-3(ed.2) (up to SIL 3)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: KD900520C
Valid until: 2017-01-31

Date, 2017-02-09
Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Rüdierstraße 65 · 80339 München · Germany
5.3 Declaration

Declarations of Conformity
Functional Safety according to IEC 61508:2010

Type: OPTISWIRL 4200
Electronic Revision: ≥ ER 2.0_x_
Device Variants: as specified in the safety manual

We, as manufacturer, declare that the device listed above is developed, produced and tested according to a SIL2/3 compliant process, as defined in IEC 61508:2010. The instructions of the Safety Manual have to be followed. Furthermore, the device is assessed, independently from the manufacturer, by TÜV Süd.

KROHNE has an established, own Functional Safety Management. The related certification can be examined under number Q4B 14/12 907 30 001 at TÜV Süd.

Duisburg, 2017-02-09

Michael Klausing
Safety Manager

Abba Brigio
Managing Director
### 5.4 Safety relevant key indicators

All values shown in the following table are related to reference conditions according to [N3]:

- Temperature: +15...+25°C / +59...+77°F
- Pressure: 1013 mbar ±50 mbar / 14.69 psi ±0.73 psi
- Relative air humidity: 60% ±15%

<table>
<thead>
<tr>
<th>Key indicator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Type B system</td>
</tr>
<tr>
<td>Systematic Capability</td>
<td>3</td>
</tr>
<tr>
<td>Safety Integrity Level</td>
<td>Single channel (HFT = 0) SIL 2</td>
</tr>
<tr>
<td></td>
<td>Homogeneous redundant (HFT = 1)(1) SIL 3</td>
</tr>
<tr>
<td>Architecture</td>
<td>1oo1 D</td>
</tr>
<tr>
<td>HFT</td>
<td>0</td>
</tr>
<tr>
<td>Failure current (failure notification)</td>
<td>For persistent failures: &lt; 3.4 mA</td>
</tr>
<tr>
<td></td>
<td>For transient failures: 3.5...3.6 mA</td>
</tr>
<tr>
<td></td>
<td>Alternatively for failures: &gt; 21.5 mA</td>
</tr>
<tr>
<td>Operation mode</td>
<td>Low and high demand, continuous mode</td>
</tr>
<tr>
<td></td>
<td>Non-Ex/Ex i</td>
</tr>
<tr>
<td></td>
<td>C</td>
</tr>
<tr>
<td>SFF</td>
<td>94.3%</td>
</tr>
<tr>
<td>( \lambda_S )</td>
<td>721 FIT</td>
</tr>
<tr>
<td>( \lambda_{DD} )</td>
<td>371 FIT</td>
</tr>
<tr>
<td>( \lambda_{DU} (= PFH) )</td>
<td>46.4 FIT</td>
</tr>
<tr>
<td>( \lambda_{DU} (= PFH) ) for homogeneous redundant configuration (1)</td>
<td>&lt;1 FIT</td>
</tr>
<tr>
<td>PFD(<em>{AVG}) ( (T</em>{proof} = 1 \text{ year}) ) (2, 6)</td>
<td>&lt;2 ( \times 10^{-4} )</td>
</tr>
<tr>
<td>PFD(<em>{AVG}) ( (T</em>{proof} = 12 \text{ years}) ) (3, 6)</td>
<td>&lt;3 ( \times 10^{-3} )</td>
</tr>
<tr>
<td>PTC (4)</td>
<td>12%...97%</td>
</tr>
<tr>
<td>FRT (5)</td>
<td>30 seconds</td>
</tr>
<tr>
<td>MTBF (7)</td>
<td>68 years</td>
</tr>
</tbody>
</table>

(1) The PFH values for the dual version, or other device configurations deployed in homogeneous redundant configuration (for details refer to Operation modes on page 10) is applicable only, if SACs 13 and 14 are fulfilled.
(2) If deployed within specified environment conditions (for details refer to Useful lifetime on page 29).
(3) For reference conditions, but with an extended temperature range up to +40°C / +104°F.
(4) Value depends on the depth of the proof test (for details refer to Operation modes and proof test on page 19).
(5) This is the part of the process safety time which must be reserved for the safety reaction of the flowmeter or for the delay of its safety function respectively.
(6) Assuming MTTR = MTR = 8 hours.
(7) Related to hardware components relevant for safe operation.
5.5 Measuring accuracy

The flowmeter measures with the same accuracy in both operation modes, in the non-SIL mode as well as in the SIL mode, as long as the device is intact.

But diagnostic measures need a reasonable gap between the states intact and defect for availability reasons. Therefore, a safety engineer integrating the flowmeter into the overall system must take the higher measurement inaccuracy into consideration.

The following figure illustrates the logical coherences.

![Figure 5-1: Measuring accuracy vs. flow](image_url)

- **x**: Flow
- **y**: Measuring accuracy

1. Bounds for non-SIL, device intact (designed, tested)
2. SIL bounds (supervised)
3. Actual inaccuracy, noise etc.
5.6 Useful lifetime

The established failure rates of electronic components apply within the useful lifetime according to IEC 61508-2, section 7.4.9.5 note 3.

The useful lifetime can only be extended under responsibility of the plant operator regarding special operation conditions and the employment of suitable intervals for testing and maintenance.

As a consequence for the safety function, the total failure rate, and consequently $\lambda_{DU}$ must not be assumed as constant at the end of the life time. The following table provides an overview about the downgrade of lifetime, depending on electronic temperature which is the most lifetime reducing factor.

### Non-Ex/Ex i [IS]

<table>
<thead>
<tr>
<th>Profile</th>
<th>Temperature [°C / °F]</th>
<th>$\lambda_{DU}$ [/h]</th>
<th>Reduction of Reliability to [%]</th>
<th>Exp. Lifetime [years]</th>
<th>Recommended Proof Test Interval [years]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40 / 104</td>
<td>$4.64 \times 10^{-8}$</td>
<td></td>
<td>11.5</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>60 / 140</td>
<td>$9.79 \times 10^{-8}$</td>
<td>47</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>80 / 176</td>
<td>$2.13 \times 10^{-7}$</td>
<td>22</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

### Ex d/Ex t/Ex nA [XP/DIP/NI]

<table>
<thead>
<tr>
<th>Profile</th>
<th>Temperature [°C / °F]</th>
<th>$\lambda_{DU}$ [/h]</th>
<th>Reduction of Reliability to [%]</th>
<th>Exp. Lifetime [years]</th>
<th>Recommended Proof Test Interval [years]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40 / 104</td>
<td>$4.72 \times 10^{-8}$</td>
<td></td>
<td>11.5</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>60 / 140</td>
<td>$9.98 \times 10^{-8}$</td>
<td>47</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>80 / 176</td>
<td>$2.17 \times 10^{-7}$</td>
<td>22</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

1. The expected lifetime is defined here as time interval wherein less than 15% of all devices failed.
2. For low demand applications for a tolerated residual failure probability of 0.0003 per demand.

5.7 Support for SIL-approved devices

All instruments which are unlocked for the use in a SIL mode are registered by the manufacturer.

In case that modifications at the supplied fl owmeter will be necessary which are relevant to the safety function of the device, the manufacturer will inform the customer immediately.
6.1 Explanations to safety application conditions (SAC)

For some SACs (for details refer to Safety application conditions (SAC) on page 8) additional explanations are given below:

SAC1: System changes
Every state of the system which does not meet its specification might be hazardous, because those states were not completely analyzed. Hazardous states can be reached by
- the use of failed, but not as “failed” marked parts, or not tested parts,
- changing the wiring, especially the use of the serial interfaces in combination with a service computer ("notebook") during operation with safety responsibility.

Most measures within the communication network are harmless, but not all. In any case, the related safety application conditions must be observed.

SAC2: Mounting and connecting
Incorrect installation will have an effect on measurement and on the measuring accuracy in general. Therefore, the correct execution of the safety function cannot be guaranteed if the installation conditions are not met.

SAC3: SIL mode
The device can be operated in SIL mode, providing the safety function or in non-SIL mode. In non-SIL mode, the key figures given in this manual (for details refer to Safety relevant key indicators on page 27) are not valid. During operation in non-SIL mode, some diagnostic measures are disabled for performance reasons and the safety reaction is switched off.

SAC4: Parameter input
The internal check functions can only detect range failures or incompatibilities in the whole data set. They cannot decide whether the data is configured as intended.

The actual parameter setting must be executed carefully.

SAC5: Maintenance mode
The maintenance mode is intended to test a device which has already potentially failed. To provide full test capability, the safe output (4…20 mA current output) is not blocked. Consequently, the operator must implement other measures temporarily to keep the overall system in a safe state.

SAC6: Resetting the fail-safe flag
When the safety reaction is triggered because a hazardous failure has been detected, a flag is saved in persistent memory to prevent the device from starting safe operation after a reset.

The device must be completely tested (for details refer to Operation modes and proof test on page 19). The fail-safe flag shall be reset only, if the operator is sure that the device is still intact (for details refer to Resetting the fail-safe flags on page 23). Note that the device will (re-)start safe operation as soon as the fail-safe flag is reset.

The NAMUR diagnostic information must not be used to decide whether the device is intact or not. Reason is that this information is not safe, as the “latest” diagnostic message(s) may get lost due to a device failure.
SAC7: Firmware update
Firmware update requires special tooling and can be provided by the authorised personnel of the manufacturer only.

SAC8: Inspection intervals
Many external events, e.g. environment temperature, may cause the device to age faster than expected. This has an effect on the failure rate which is assumed as constant over the lifetime at reference conditions.

For recommendations regarding the calculation of the proof test intervals refer to Operation modes and proof test on page 19 and refer to Useful lifetime on page 29.

SAC9: Modification
A modification may have unexpected influence on the safety function. Such effects must be analysed. This can only be done by deep knowledge of the internal construction of the device.

SAC10: Repair
Repair of the device exceeding the defined exceptions need more tooling, test and calibration facilities than available in the field.

SAC12: Supervision of failure current
The preferred failure current is low as it is a state with the lowest energy consumption. Nevertheless, a failure might prohibit the output of the lower failure current. In that case the output will be switched to the high failure current.

The failure current (low/high) is configurable but the configuration is only effective in non-SIL mode. Consequently, a device evaluating the current output must react on both failure currents, not only on the configured one.
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