Variable area flowmeter
Safety manual acc. to IEC 61508:2010
CONTENTS

1 Introduction 3
   1.1 Fields of application ................................................................. 3
   1.2 User benefits ........................................................................... 3
   1.3 Relevant standards / literature .................................................. 3

2 Terms and definitions 4

3 Description 5
   3.1 Functional principle................................................................. 5

4 Specification of the safety function 6
   4.1 Description of the failure categories ......................................... 6

5 Project planning 7
   5.1 Applicable device documentations............................................. 7
   5.2 Project planning, behaviour during operation and malfunction........ 7

6 Life time / Proof tests 8
   6.1 Life time.................................................................................. 8
   6.2 Proof tests ............................................................................. 9

7 Safety-related characteristics 10
   7.1 Assumptions .......................................................................... 10
   7.2 Specific safety-related characteristics ...................................... 10

8 Annex 11
   8.1 Annex 1 ................................................................................ 11
   8.2 Annex 2 .............................................................................. 12

9 Notes 13
Introduction

1.1 Fields of application

Measurements of volume flow rate of liquids, gases and vapor that shall meet the special safety requirements according to IEC 61508.

The measuring unit meets the requirements regarding

- Functional safety in accordance with IEC 61508-2:2010 (Edition 2)
- EMC directive 2004/108/EC
- ATEX directive 94/9/EC
- PED directive 97/23/EC

For further information please refer to the CE declaration of conformity which is available at the Download Center at www.krohne.com.

1.2 User benefits

Use for

- Volume flow monitoring
- Continuous measurement and local analog indication
- Easy commissioning

1.3 Relevant standards / literature


[N3] FMD-91, RAC 1991 Failure Mode / Mechanism Distributions

[N4] FMD-97, RAC 1997 Failure Mode / Mechanism Distributions


[N6] SN 29500 Failure rates of components


## Terms and definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCD</td>
<td>Diagnostic Coverage of dangerous failures</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure In Time ((1 \times 10^{-9} \text{ failures per hour}))</td>
</tr>
<tr>
<td>FMEDA</td>
<td>Failure Modes, Effects and Diagnostic Analysis</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>Low demand mode</td>
<td>Mode, where the frequency of demand for operation made on a safety-related system is not greater than one per year and not greater than twice in the proof test frequency.</td>
</tr>
<tr>
<td>PFDAVG</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction summarizes the fraction of failure, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>Type A component</td>
<td>&quot;Non-complex&quot; subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.</td>
</tr>
<tr>
<td>Type B component</td>
<td>&quot;Complex&quot; subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.</td>
</tr>
<tr>
<td>T[Proof]</td>
<td>Proof Test Interval</td>
</tr>
</tbody>
</table>
3.1 Functional principle

The flowmeter operates in accordance with the float measuring principle.

A metal cone is installed in the measuring unit H250, in which a suitably shaped float can move freely up and down.

The flowmeter is inserted into a vertical pipeline and the medium flows through it from bottom to top.

The guided float adjusts itself so that the buoyancy force $A$ acting on it, the form drag $W$, the weight $G$ and the spring load $S$ are in equilibrium $[G + S = A + W]$.

An annular gap results which width depends on the current flow rate.

The height of the float in the measuring unit, which depends on the float, is transmitted by a magnetic coupling and displayed on a scale.

Strong deflecting magnetic fields can lead to deviations in the measured value.
4.1 Description of the failure categories

In order to judge the failure behavior of the variable-area flowmeter H250/M9 with limit switch output, the following definitions for the failure of the product were considered.

<table>
<thead>
<tr>
<th>Failure Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail-Safe State</td>
<td>The fail-safe state is defined as the output being de-energized or one of</td>
</tr>
<tr>
<td></td>
<td>the 2 limit switches is triggered. Fail Safe Failure that causes the module</td>
</tr>
<tr>
<td></td>
<td>/ (sub) system to go to the defined fail-safe state without a demand from</td>
</tr>
<tr>
<td></td>
<td>the process.</td>
</tr>
<tr>
<td>Fail Dangerous</td>
<td>Failure that does not respond to a demand from the process (i.e. being</td>
</tr>
<tr>
<td></td>
<td>unable to go to the defined fail-safe state).</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>Failure that is dangerous and that is not being diagnosed by internal</td>
</tr>
<tr>
<td></td>
<td>diagnostics.</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>Failure that is dangerous but is detected by internal diagnostics. (These</td>
</tr>
<tr>
<td></td>
<td>failures may be converted to the selected fail-safe state.)</td>
</tr>
<tr>
<td>Not Effect</td>
<td>Failure of a component that is part of the safety function but that has no</td>
</tr>
<tr>
<td></td>
<td>effect on the safety function.</td>
</tr>
<tr>
<td>Not part</td>
<td>Failures of a component which is not part of the safety function but part of</td>
</tr>
<tr>
<td></td>
<td>the circuit diagram and is listed for completeness. When calculating the</td>
</tr>
<tr>
<td></td>
<td>SFF this failure mode is not taken into account. It is also not part of the</td>
</tr>
<tr>
<td></td>
<td>total failure rate.</td>
</tr>
</tbody>
</table>

In IEC 61508 edition 1 the “No Effect” failures were defined as safe undetected failures, even though they would not cause the safety function to go to a safe state.

With edition 2 (IEC 61508:2010) the no effect failures are no longer considered as safe undetected failures and must not contribute to the SFF calculation. Therefore the SFF values have changed.

The PFD values remain as before.

The demand response time of H250 M9 is < 2s.
5.1 Applicable device documentations

[D1]  TD H250 Rxx en
       Technical datasheet H250 – Variable area flowmeter

[D2]  MA H250 Rxx en
       Handbook including installation and operating instructions

[D3]  exida FMEDA report: KROHNE 05/06-20 R007 Version 2

5.2 Project planning, behaviour during operation and malfunction

• Average temperature for the parts in the display section M9 has to be +40°C over a long period of time. The max. allowed process temperature in relation to max. ambient temperature is shown in Figure 5-1.
• Under normal conditions the maximum operating time will be 10 years.
• Requirements made in the Handbook have to be kept.
• Repair and inspection intervals have to be based on the safety calculations.
• Follow the KROHNE repair instructions in the printed Handbook
• Modifications made without specific authorisation of the manufacturer are strictly prohibited.
• For help to find the correct Description code see ANNEX 1.

Figure 5-1: Relation between process temperature, ambient temperature and temperature of display section M9
6.1 Life time

Although a constant failure rate is assumed by the probabilistic estimation method this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive). This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behaviour for electronic components. Therefore it is obvious that the PFDavg calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. According to section 7.4.9.5 note 3 of IEC 61508-2 experience has shown that the useful lifetime often lies within a range of 8 to 12 years.

We recommend an operational life time for variable area flowmeters no longer than 10 years in SIL rated applications. However, if the user is monitoring the instruments over their lifetime demonstrating the required results (e.g. constant failure rate), this can allow safety capability exceeding this period on the user’s own responsibility.

The required cyclic proof test interval can be found in the table chapter 7.2.
6.2 Proof tests

Possible proof tests to detect dangerous undetected faults

**Proof test 1 consists of the following steps:**
1. Take appropriate action to avoid a false trip.
2. Force the variable-area flowmeter H250/M9 to reach a defined "MAX" threshold value and verify that the inductive limit switch goes into the safe state.
3. Restore the loop to full operation.
4. Restore normal operation.

**Proof test 2 consists of the following steps:**
1. Take appropriate action to avoid a false trip.
2. Force the variable-area flowmeter H250/M9 to reach a defined "MIN" threshold value and verify that the inductive limit switch goes into the safe state.
3. Restore the loop to full operation.
4. Restore normal operation.

**INFORMATION!**
Both tests together will detect approximately 90% of possible "du" failures.

**INFORMATION!**
It is necessary to open the casing of the device in order to do the electrical connection and to set the limit switch set points.
Special attention is required when the casing is open. Avoid a deformation of the precision mechanics indicator system. By deforming the pointer or the balance vane the ease-of-movement can be influenced leading to a wrong measurement.
By performing the mandatory proof-test after installation and closing the casing the ease-of-movement has to be verified.
Safety-related characteristics

7 SAFETY-RELATED CHARACTERISTICS

7.1 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the variable-area flowmeter H250/M9 with switching contact output.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- All modules are operated in low demand mode of operation.
- External power supply failure rates are not included.
- The stress levels are average for an industrial outdoor environment and can be compared to the Ground Fixed classification of MIL-HDBK-217F.

Alternatively, the assumed environment is similar to:
IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer’s rating and an average temperature over a long period of time of 40°C.

- Humidity levels are assumed within manufacturer’s rating.
- Only the switching contact output is used for safety applications.

7.2 Specific safety-related characteristics

Under the assumptions described in 7.1 and the definitions given in section 4 the following tables show the failure rates according to IEC 61508:

Based on the construction of the H250/M9 this device is specified as a type A device according to IEC 61508 with a HFT (Hardware Failure Tolerance) = 0 and a classification as SIL (Safety Integrity Level): 1.

<table>
<thead>
<tr>
<th>System</th>
<th>SFF</th>
<th>TPROOF</th>
<th>PFDAVG</th>
<th>λSD</th>
<th>λSU</th>
<th>λDD</th>
<th>λDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>H250/M9 connected to a standard switching amplifier</td>
<td>54%</td>
<td>1 year</td>
<td>5.04E-04</td>
<td>0 FIT</td>
<td>81 FIT</td>
<td>55 FIT</td>
<td>115 FIT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 years</td>
<td>2.52E-03</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 years</td>
<td>[5.03E-03]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H250/M9 connected to a fail-safe switching amplifier¹</td>
<td>57%</td>
<td>1 year</td>
<td>3.35E-04</td>
<td>0 FIT</td>
<td>50 FIT</td>
<td>55 FIT</td>
<td>77 FIT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 years</td>
<td>1.67E-03</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 years</td>
<td>3.34E-03</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ The switching contact output is connected to a fail-safe NAMUR amplifier [e.g. Pepperl + Fuchs KF**-SH-Ex1]. Failure rates of the amplifiers are not included.

The PFDAVG value in brackets means that the calculated PFDAVG values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03.

The PFDAVG value [not in brackets] means that the calculated PFDAVG values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3.50E-03.
8.1 Annex 1

Constricted Description Code for H250 Functional Safety Equipment acc. to EN 61508

The description code for H250 consists of the following elements:

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1 | Device type H250 - standard version
| 2 | Materials / versions
|   | RR - Stainless Steel
|   | HC - Hastelloy®
|   | Ti - Titanium
| 3 | Heating jacket version
|   | B - with heating jacket
| 4 | Series of indicators
|   | M9 - Indicator M9 standard indicator
|   | M9S - Indicator with added impact and corrosion protection
|   | M9R - Indicator in Stainless Steel housing
| 5 | Position not needed for SIL 2 applications
| 6 | Position not needed for SIL 2 applications
| 7 | Position not needed for SIL 2 applications
| 8 | Limit switch
|   | K1 - One limit switch
|   | K2 - Two limit switches
| 9 | Explosion protection
|   | Ex - Explosion-protected equipment
| 10| SIL
|   | SK - SIL compliance of limit switches acc. to IEC 61508:2010

Positions which are not needed are omitted (no blank positions)

The variable-area flowmeter H250/M9 (SIL) can be equipped with a maximum of two electronic limit switches. The limit switch function with a slot-type indicator which is operated inductively through the semicircular metal vane belonging to the measuring pointer.

The correct ordering text for switches with different contact types and the fitting isolating switching amplifier are found in the right column of the two tables “option 1” and “option 2” [see next page Annex 2].
8.2 Annex 2

**Option 1:** H250/M9 connected to a standard switching amplifier

<table>
<thead>
<tr>
<th>Type code</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC3,5-N0-Y47819-ATEX-Dub.</td>
<td>2-wire technology (NAMUR)</td>
</tr>
</tbody>
</table>

**Appropriate Isolating Switching Amplifiers:**

<table>
<thead>
<tr>
<th>Type code</th>
<th>Supply voltage</th>
<th>Channel</th>
<th>Output</th>
<th>Ordering No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>KFA6-SR2-Ex1.W</td>
<td>230 VAC</td>
<td>1</td>
<td>relay</td>
<td>5015262000</td>
</tr>
<tr>
<td>KFAS-SR2-Ex1.W</td>
<td>115 VAC</td>
<td>1</td>
<td>relay</td>
<td>5015262100</td>
</tr>
<tr>
<td>KFD2-SR2-Ex1.W</td>
<td>24 VDC</td>
<td>1</td>
<td>relay</td>
<td>5015262200</td>
</tr>
<tr>
<td>KFA8-SR2-Ex2.W</td>
<td>230 VAC</td>
<td>2</td>
<td>relay</td>
<td>5015262300</td>
</tr>
<tr>
<td>KFAS-SR2-Ex2.W</td>
<td>115 VAC</td>
<td>2</td>
<td>relay</td>
<td>5015262400</td>
</tr>
<tr>
<td>KFD2-SR2-Ex2.W</td>
<td>24 VDC</td>
<td>2</td>
<td>relay</td>
<td>5015262500</td>
</tr>
</tbody>
</table>

**Option 2:** H250/M9 connected to a fail-safe switching amplifier

<table>
<thead>
<tr>
<th>Type code</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>SJ3,5-SN-ATEX</td>
<td>2-wire technology safety-oriented</td>
</tr>
<tr>
<td>SJ3,5-S1N-ATEX</td>
<td>2-wire technology safety-oriented</td>
</tr>
</tbody>
</table>

**Appropriate Isolating Switching Amplifiers:**

<table>
<thead>
<tr>
<th>Type code</th>
<th>Supply voltage</th>
<th>Channel</th>
<th>Output</th>
<th>Ordering No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>KFD2-SH-Ex1</td>
<td>20...35 VDC</td>
<td>1</td>
<td>redundant relay</td>
<td>501526800</td>
</tr>
<tr>
<td>KFD2-SH-Ex1.T.OP</td>
<td>20...35 VDC</td>
<td>1</td>
<td>Electronic and relay</td>
<td>optional</td>
</tr>
<tr>
<td>KHA6-SH-Ex1</td>
<td>85...253 VAC</td>
<td>1</td>
<td>redundant relay</td>
<td>optional</td>
</tr>
</tbody>
</table>
KROHNE product overview

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

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

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