
# H250 M40 Supplementary Instructions

## Variable area flowmeter

**Safety manual acc. to IEC 61508:2010**

SIL 2
Safety Integrity Level



KROHNE

# CONTENTS

## 1.1 Field of application

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

**The measuring device meets the requirements regarding**

- Functional safety in accordance with IEC 61508-2:2010 (Edition 2)
- EMC directive 2014/30/EU and NAMUR recommandation NE 21
- ATEX directive 2014/34/EU
- PED directive 2014/68/EU

For further information please refer to the declaration of conformity in the Downloadcenter of the manufacturer website.

## 1.2 User benefits

**Use for**

- Volume flow monitoring
- Continuous flow measurement and local analogue indication
- Easy commissioning
- Excellent price-performance ratio

## 1.3 Relevant standards / Literature

[N1] IEC 61508-2:2010 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

[N2] Electrical & Mechanical Component Reliability Handbook, 2nd Edition 2008, exida L.L.C. ISBN 978-0-9727234-6-6

[N3] IEC 60654-1:1993-02 2nd edition, Industrial process measurement and control equipment - Operating conditions - Part 1: Climatic conditions

### Terms and definitions

| | |
|---|---|
| $DC_D$ | Diagnostic Coverage of dangerous failures |
| FIT | Failure In Time ($1x10^{-9}$ failures per hour) |
| FMEDA | Failure Modes, Effects and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance |
| Low demand mode | 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. |
| $PFD_{AVG}$ | Average Probability of Failure on Demand |
| SFF | 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. |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| Type A component | "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2. |
| Type B component | "Complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2. |
| T[Proof] | Proof Test Interval |

## 2.1 Description of the considered profiles

### Mechanical database

| Profile | Profile according to IEC 60654-1 | Ambient temperature [°C] | | Temperature cycle [°C / 365 days] |
|---|---|---|---|---|
| | | Average (external) | Mean (inside box) | |
| 2 | C3 | 25 | 30 | 25 |
| 4 | D1 | 25 | 30 | 35 |

Profile 2 (low stress): Mechanical field products with minimal self heating, subject to daily temperature swings.

Profile 4 (high stress): Unprotected mechanical field products with minimal self heating, subject to daily temperature swings and rain or condensation.

### Electronic database

| Profile | Profile according to IEC 60654-1 | Ambient temperature [°C] | | Temperature cycle [°C / 365 days] |
|---|---|---|---|---|
| | | Average (external) | Mean (inside box) | |
| 2 | C3 | 25 | 30 | 25 |

Profile 2 Low power electrical (2-wire) field products have minimal self heating and are subjected to daily temperature swings.

## 3.1 Functional principle

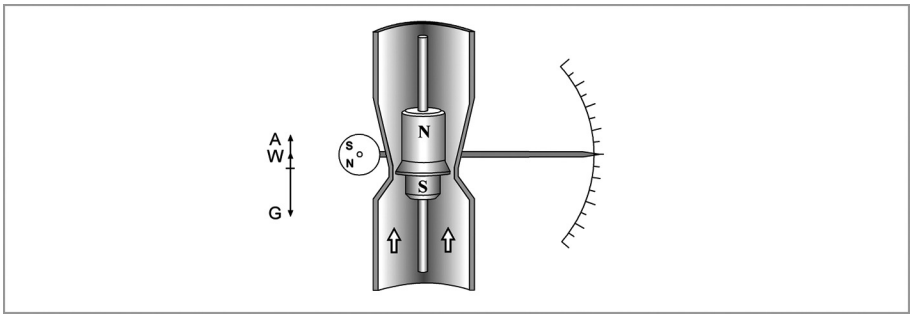



Figure 3-1: Functional principle

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 and weight G are in equilibrium (G = 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.

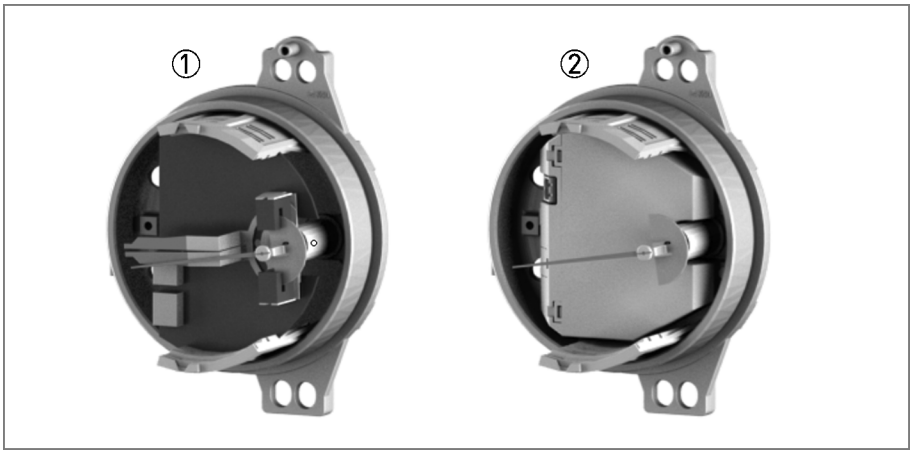
Strong deflecting magnetic fields can lead to deviations in the measured value.

## 3.2 Description of the subsystem

### H250 M40 - versions


① Standard version
② HT version

### H250 M40 with electrical built ins




① Version with K1/K2
② Version with ESK4

## 4.1 Description of the failure categories

In order to judge the failure behaviour of the variable area flowmeters H250 M40, the following definitions for the failure of the flowmeter were considered:

| | |
|---|---|
| Fail - Safe | Failure that causes the subsystem to go to the defined fail-safe state without a demand from process. |
| Fail Dangerous Undetected | Failure that is dangerous and that is not being diagnosed by internal diagnostics. |
| Fail Dangerous Detected | Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state) |
| Fail No Effect | Failure of a component that is part of the safety function but is neither a safe failure nor a dangerous failure and has no effect on the safety function. |
| Not part | Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate. |

### H250 M40 with inductive limit switch output

| | |
|---|---|
| Fail-Safe State | The fail-safe state is defined as the output beeing de-energized |
| Fail Dangerous | Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) |

### H250 M40 with 4…20mA output

| | |
|---|---|
| Fail-Safe State | The fail-safe state is defined as the output exceeding the user defined threshold |
| Fail Dangerous | Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or that deviates the output current by more than 2.5% of full span. |
| Fail High | Failure that causes the output signal to go to the maximum output current (>21mA) according NAMUR NE43. |
| Fail Low | Failure that causes the output signal to go to the minimum output current (< 3.6 mA) according NAMUR NE43. |

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 M40 is < 2s.

## 5.1 Applicable device documentation

[D1] TD H250/M40-Rxx-en
Technical datasheet H250/M40 – Variable area flowmeter

[D2] MA H250/M40-Rxx-en
Handbook including installation and operating instructions

[D3] exida FMEDA report: KROHNE 10/10020361 R010 Version 2

## 5.2 Project planning, behaviour during operation and malfunction

- The stress levels shall be average for an industrial outdoor environment and shall be similar to exida Profile 2 or Profile 4 with temperature limits within the manufacture's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.
- Under normal conditions the maximum operating time will be 10 years.
- Requirements made in the operating manual have to be kept.
- Repair and inspection intervals have to be based on the safety calculations.
- Follow the repair instructions of the manufacturer in the printed manual.
- Modifications made without specific authorisation of the manufacturer are strictly prohibited.
- Follow the installation and operating instructions.
- The application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures. The failure rates of the safety logic solver are not included in the listed failures rates.
- The parameters given by the FMEDA are considered as planning support. The end user is responsible for the overall functional safety of the application.
- For help to find the correct order text see annex 1.

## 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 $PFD_{AVG}$ 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.

KROHNE recommends 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 life time demonstrating the required results (e.g. constant failure rate), this can allow safety capability exceeding this period on the user' s own responsibility.

For the required cyclic proof test refer to *Proof tests* on page 10.

## 6.2 Proof tests

**Possible proof tests to detect dangerous undetected faults**

### Proof test for H250/M40/K* with inductive limit switches

1. Take appropriate action to avoid a false trip.
2. Inspect the device for any visible damage, corrosion or contamination.
3. Force the variable area flowmeter H250 M40 to reach a defined “MAX” threshold value and verify that the inductive limit switch goes into the safe state.
4. Force the variable area flowmeter H250 M40 to reach a defined “MIN” threshold value and verify that the inductive limit switch goes into the safe state.
5. Restore the loop to full operation.
6. Restore normal operation

It is assumed that the test will detect approximately 99% of possible dangerous undetected failures.

### Proof test for H250/M40/ESK with 4…20mA output

1. Bypass the safety PLC or take other appropiate action to avoid a false trip.
2. Perform 5-point calibration verification of the variable area flowmeter H250 M40.
3. Force the variable area flowmeter H250 M40 to go to the high alarm current output and verify that the analog current reaches that value.
4. Force the variable area flowmeter H250 M40 to go to the low alarm current output and verify that the analog current reaches that value.
5. Restore the loop to full operation.
6. Remove the bypass from the safety PLC or otherwise restore normal operation.

It is assumed that the test will detect approximately 99% of possible dangerous undetected 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*

## 7.1 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the variable area flowmeter H250 M40.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures resulting from incorrect use of the flowmeters H250 M40, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets, are not considered.
- Failures during parameterisation are not considered
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analysed.
- The mean time to restoration (MTTR) after safe failure is 24 hours.
- All modules are operated in the low demand mode of operation.
- External power failure rates are not included.
- The HART® protocol at H250 M40 is only used for setup, calibration and diagnostics purpose, not during safety operation mode.
- Practical fault insertion test can demonstrate the correctness of the failure effects assumed during FMEDAs.
- The stress levels are average for an industrial outdoor environment and can be compared to exida Profile 2 or Profile 4 with temperature limits within the manufacture's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.
- The switching contact outputs are connected to a NAMUR amplifier. The failure rates of the amplifier are not included in the listed failure rates.
- Only the current output 4...20 mA or the limit switch outputs are used for safety applications.
- Lead breakage and short circuit detection is activated.
- The application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures. The failure rates of the safety logic solver are not included in the listed failures rates.

The variable area flowmeter **H250/M40/K*** with inductive limit switches are classified as **Type A subsystems** (non-complex subsystem according 7.4.3.1.2. of IEC 61508-2) with hardware fault tolerance HFT=0. For Type A subsystems the SFF has to be > 60% for SIL2 subsystems with a hardware fault tolerance of 0 (table 2 of IEC 61508-2).

The variable area flowmeter **H250/M40/ESK** with 4…20mA output is classified as **Type B subsystem** (complex subsystem according 7.4.3.1.3. of IEC 61508-2) with hardware fault tolerance HFT=0. For Type B subsystems the SFF has to be > 60% for SIL1 subsystems with a hardware fault tolerance of 0 (table 3 of IEC 61508-2).

## 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:

**H250/M40/K*-SK** with 1 or 2 **fail-safe limit switches** (MIN/MAX) ① and **welded** process connections

| | $\lambda_{SD}$ | $\lambda_{SU}$ | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF ② | $DC_D$ | MTBF | SIL AC ③ |
|---|---|---|---|---|---|---|---|---|
| Stress profile 2 (low stress) | 0 FIT | 50 FIT | 10 FIT | 38 FIT | 61% | 20% | 487 years | SIL2 |
| Stress profile 4 (high stress) | 0 FIT | 50 FIT | 10 FIT | 73 FIT | 45% | 12% | 356 years | SIL1 |

| T[Proof] ④ | 1 year | 2 years | 5 years |
|---|---|---|---|
| $PFD_{AVG}$ ⑤ | 1.82*E-04 | 3.46*E-04 | 8.41*E-04 |

**H250/M40/K*-SK** with 1 or 2 **standard limit switches** (MIN/MAX) ⑥ and **welded** process connections

| | $\lambda_{SD}$ | $\lambda_{SU}$ | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF ② | $DC_D$ | MTBF | SIL AC ③ |
|---|---|---|---|---|---|---|---|---|
| Stress profile 2 (low stress) | 0 FIT | 81 FIT | 10 FIT | 77 FIT | 54% | 11% | 376 years | SIL1 |
| Stress profile 4 (high stress) | 0 FIT | 81 FIT | 10 FIT | 112 FIT | 44% | 8% | 293 years | SIL1 |

| T[Proof] ④ | 1 year | 2 years | 5 years |
|---|---|---|---|
| $PFD_{AVG}$ ⑤ | 3.68*E-04 | 7.02*E-04 | 1.70*E-03 |

① The switching contact output is connected to a fail-safe NAMUR amplifier (e.g. Pepperl+Fuchs KF**-SH-Ex1). The failure rates of the amplifier are not included in the listed failure rates.

② The number listed is for reference only. The SFF must be determined for the complete subsystem.

③ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural contraints for the corresponding SIL level.

④ It is assumed that proof testing is performed with a proof test coverage of 99%.

⑤ The $PFD_{AVG}$ was calculated for profile 2 using the Markov modelling. The results must be considered in combination with $PFD_{AVG}$ values of other devices of the Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL)
For SIL1 applications, the $PFD_{AVG}$ value needs to be < $10^{-1}$.
For SIL2 applications, the $PFD_{AVG}$ value needs to be < $10^{-2}$.

⑥ The switching contact output is connected to a standard NAMUR switching amplifier (e.g. Pepperl+Fuchs KF**-SR2-Ex*.W). The failure rates of the amplifier are not included in the listed failure rates.

**H250/M40/HT/K*-SK** with 1 or 2 **fail-safe limit switches** (MIN/MAX) ① and **welded** process connections

| | $\lambda_{SD}$ | $\lambda_{SU}$ | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF ② | $DC_D$ | MTBF | SIL AC ③ |
|---|---|---|---|---|---|---|---|---|
| Stress profile 2 (low stress) | 0 FIT | 50 FIT | 10 FIT | 58 FIT | 50% | 14% | 432 years | SIL1 |
| Stress profile 4 (high stress) | 0 FIT | 50 FIT | 10 FIT | 114 FIT | 34% | 8% | 308 years | SIL1 |

| T[Proof] ④ | 1 year | 2 years | 5 years |
|---|---|---|---|
| $PFD_{AVG}$ ⑤ | 2.77*E-04 | 5.29*E-04 | 1.28*E-03 |

**H250/M40/HT/K*-SK** with 1 or 2 **standard limit switches** (MIN/MAX) ⑥ and **welded** process connections

| | $\lambda_{SD}$ | $\lambda_{SU}$ | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF ② | $DC_D$ | MTBF | SIL AC ③ |
|---|---|---|---|---|---|---|---|---|
| Stress profile 2 (low stress) | 0 FIT | 81 FIT | 10 FIT | 97 FIT | 48% | 9% | 342 years | SIL1 |
| Stress profile 4 (high stress) | 0 FIT | 81 FIT | 10 FIT | 152 FIT | 37% | 6% | 260 years | SIL1 |

| T[Proof] ④ | 1 year | 2 years | 5 years |
|---|---|---|---|
| $PFD_{AVG}$ ⑤ | 4.63*E-04 | 8.84*E-04 | 2.15*E-03 |

① The switching contact output is connected to a fail-safe NAMUR amplifier (e.g. Pepperl+Fuchs KF**-SH-Ex1). The failure rates of the amplifier are not included in the listed failure rates.

② The number listed is for reference only. The SFF must be determined for the complete subsystem.

③ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural contraints for the corresponding SIL level.

④ It is assumed that proof testing is performed with a proof test coverage of 99%.

⑤ The $PFD_{AVG}$ was calculated for profile 2 using the Markov modelling. The results must be considered in combination with $PFD_{AVG}$ values of other devices of the Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL)
For SIL1 applications, the $PFD_{AVG}$ value needs to be < $10^{-1}$.
For SIL2 applications, the $PFD_{AVG}$ value needs to be < $10^{-2}$.

⑥ The switching contact output is connected to a standard NAMUR switching amplifier (e.g. Pepperl+Fuchs KF**-SR2-Ex*.W). The failure rates of the amplifier are not included in the listed failure rates.

**H250/M40/ESK-SE** with 4..20 mA current output and **welded** process connections

| | $\lambda_{SD}$ | $\lambda_{SU}$ | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF ② | $DC_D$ | MTBF | SIL AC ③ |
|---|---|---|---|---|---|---|---|---|
| Stress profile 2 (low stress) | 0 FIT | 0 FIT | 293 FIT | 110 FIT | 72% | 72% | 170 years | SIL1 |
| Stress profile 4 (high stress) | 0 FIT | 0 FIT | 307 FIT | 146 FIT | 67% | 67% | 151 years | SIL1 |

| T[Proof] ④ | 1 year | 2 years | 5 years |
|---|---|---|---|
| $PFD_{AVG}$ ⑤ | 5.37*E-04 | 1.02*E-03 | 2.46*E-03 |

**H250/M40/HT/ESK-SE** with 4..20 mA current output and **welded** process connections

| | $\lambda_{SD}$ | $\lambda_{SU}$ | $\lambda_{DD}$ | $\lambda_{DU}$ | SFF ② | $DC_D$ | MTBF | SIL AC ③ |
|---|---|---|---|---|---|---|---|---|
| Stress profile 2 (low stress) | 0 FIT | 0 FIT | 293 FIT | 130 FIT | 69% | 69% | 163 years | SIL1 |
| Stress profile 4 (high stress) | 0 FIT | 20 FIT | 307 FIT | 186 FIT | 62% | 62% | 141 years | SIL1 |

| T[Proof] ④ | 1 year | 2 years | 5 years |
|---|---|---|---|
| $PFD_{AVG}$ ⑤ | 6.32*E-04 | 1.20*E-03 | 2.90*E-03 |

② The number listed is for reference only. The SFF must be determined for the complete subsystem.

③ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural contraints for the corresponding SIL level.

④ It is assumed that proof testing is performed with a proof test coverage of 99%.

⑤ The $PFD_{AVG}$ was calculated for profile 2 using the Markov modelling. The results must be considered in combination with $PFD_{AVG}$ values of other devices of the Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL)

For SIL1 applications, the $PFD_{AVG}$ value needs to be < $10^{-1}$.

For SIL2 applications, the $PFD_{AVG}$ value needs to be < $10^{-2}$.

## 8.1 Annex 1

**Constricted Description Code for H250/M40 Functional Safety Equipment acc. to EN 61508**

The description code for H250/M40 consists of the following elements ①


① Device type
H250 - standard version

② Materials / versions
RR - Stainless Steel
HC - Hastelloy
Ti - Titanium
F - aseptic version (food)

③ Series of indicators
M40 - Indicator M40
M40S - Indicator with added impact and corrosion protection
M40R - Indicator in Stainless Steel housing

④ High temperature version
HT - Version with HT extension

⑤ Electrical signal output
ESK - current output ESK4

⑥ Limit switch
K1 - One limit switch
K2 - Two limit switches

⑦ Explosion protection
Ex - Explosion-protected equipment

⑧ SIL compliance
SK - SIL compliant limit switches acc. to IEC 61508:2010
SE - SIL compliant current output acc. to IEC 61508:2010

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

## 8.2 Annex 2

### Fail-safe contact types, used for H250/M40:

SJ3,5-SN (Pepperl+Fuchs) 2-wire fail-safe inductive NAMUR switch

SJ3,5-S1N (Pepperl+Fuchs) 2-wire fail-safe inductive NAMUR switch (inverted)

### Recommended fail-safe switching amplifiers for the fail-safe NAMUR limit switches

| Type code | Manufacturer | Supply voltage | Channel | Output |
|---|---|---|---|---|
| KFD2-SH-Ex1 | Pepperl+Fuchs | 20…35 Vdc | 1 safe fail | Redundant relay |
| KHD2-SH-Ex1.T.OP | Pepperl+Fuchs | 20…35 Vdc | 1 safe fail | Electronic + relay |
| KHA6-SH-Ex1 | Pepperl+Fuchs | 85…253 Vac | 1 safe fail | Redundant relay |

### Standard contact types, used for H250/M40:

SC3,5-N0 (Pepperl+Fuchs) 2-wire fail-safe inductive NAMUR switch

### Recommended standard switching amplifiers for the standard NAMUR limit switches:

| Type code | Manufacturer | Supply voltage | Channel | Output |
|---|---|---|---|---|
| KFA6-SR2-Ex1.W | Pepperl+Fuchs | 230 VAC | 1 | relay |
| KFA5-SR2-Ex1.W | Pepperl+Fuchs | 115 VAC | 1 | relay |
| KFD2-SR2-Ex1.W | Pepperl+Fuchs | 24 VDC | 1 | relay |
| KFA6-SR2-Ex2.W | Pepperl+Fuchs | 230 VAC | 2 | relay |
| KFA5-SR2-Ex2.W | Pepperl+Fuchs | 115 VAC | 2 | relay |
| KFD2-SR2-Ex2.W | Pepperl+Fuchs | 24 VDC | 2 | relay |

Table 8-1: Permitted isolating switching amplifier

## 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

KROHNE