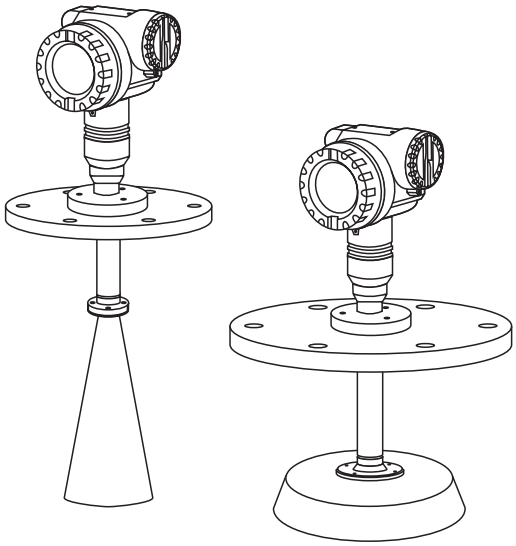
Level | Pressure | Flow | Temperature | Liquid Analysis | Registration | Systems Components | Services | Solutions

Functional Safety Manual

Micropilot M FMR250

Level-Radar with 4 to 20 mA Output Signal



Application

Overfill protection or operating maximum detection of powdery to granular bulk solids and all types of liquids in systems to satisfy particular safety systems requirements as per IEC 61508/IEC 61511.

The measuring device fulfils the requirements concerning

- Functional safety as per IEC 61508/IEC 61511
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per EN 61326 and NAMUR recommendation NE 21
- Electrical safety as per IEC/EN 61010-1

Your benefits

- For overfill protection up to SIL 2
  - Independently assessed (Functional Assessment) by *exida.com* as per IEC 61508/IEC 61511
- Permanent self-monitoring
- Continuous measurement
- Non-contact measurement: measurement is virtually independent of product properties
- Easy commissioning

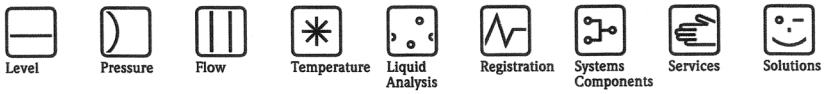
SD305F/00/EN/12.09
71107888

Endress+Hauser

People for Process Automation

Table of contents

SIL Declaration of Conformity



SIL-09016a/00/A2

SIL-Konformitätserklärung

Funktionale Sicherheit nach IEC 61508

SIL Declaration of Conformity

Functional safety according to IEC 61508

Endress+Hauser GmbH+Co. KG, Hauptstraße 1, 79689 Maulburg
erklärt als Hersteller, dass das Gerät
declares as manufacturer, that the device

Micropilot M FMR250

für den Einsatz in Schutzeinrichtungen entsprechend der IEC 61508 / IEC 61511 geeignet ist, wenn das Handbuch zur Funktionalen Sicherheit und die Kenngrößen in der folgenden Tabelle beachtet werden:
is suitable for the use in safety-instrumented systems according to IEC 61508 / IEC 61511, if the functional safety manual and the characteristics specified in the following table are observed:

Gerät/Device	Micropilot M FMR250 2-Draht/2-wire
Handbuch zur Funktionalen Sicherheit/ Functional safety manual	SD305F/00
Schutzfunktion/Safety function	Maximum-Grenzstandüberwachung/Maximum detection
SIL*4	2
HFT	0
Gerätetyp/Device type	B
Betriebsart/Mode of operation	Low demand mode
SFF	76,6 %
PFD_{avg} *1 T_1 = 1 Jahr/year	3.14×10^{-3}
λ_{sd} *2	99 FIT
λ_{su} *2	1340 FIT
λ_{dd} *2	917 FIT
λ_{du} *2	718 FIT
MTBF *3	35 Jahre/years

*1 Die Werte entsprechen SIL 2 nach ISA S84.01. PFD_{avg}-Werte für andere T_1-Werte siehe Handbuch zur Funktionalen Sicherheit.
The values comply with SIL 2 according to ISA S84.01. PFD_{avg} values for other T_1-values see Functional Safety Manual.

*2 Gemäß Siemens SN29500.
According to Siemens SN29500.

*3 Gemäß Siemens SN29500, einschließlich Fehlern, die außerhalb der Sicherheitsfunktionen liegen.
According to Siemens SN29500, including faults outside the safety fuction.

*4 Betrachtung gemäß IEC 61511-1 Abschnitt 11.4.4
consideration according to IEC 61511-1 clause 11.4.4

Das Gerät einschließlich Software, wurde auf Basis der Betriebsbewährung bewertet. Bei Geräteänderungen wird ein Modifikationsprozess nach IEC 61508 angewendet.
The device including software was assessed on the basis of proven-in-use. In case of device modifications, a modification process according to IEC 61508 is applied.

Maulburg, 14.12.2009

i.V.

(Dr. Arno Götz)
Leitung Zertifizierung /
Manager Certification

i.V.

(Peter Kloefer)
Abteilungsleiter Kontinuierliche Füllstandsmessung , F&E /
Head of Department Continuous Level Measurement ,R&D

Endress+Hauser
People for Process Automation

SIL_08006a_de

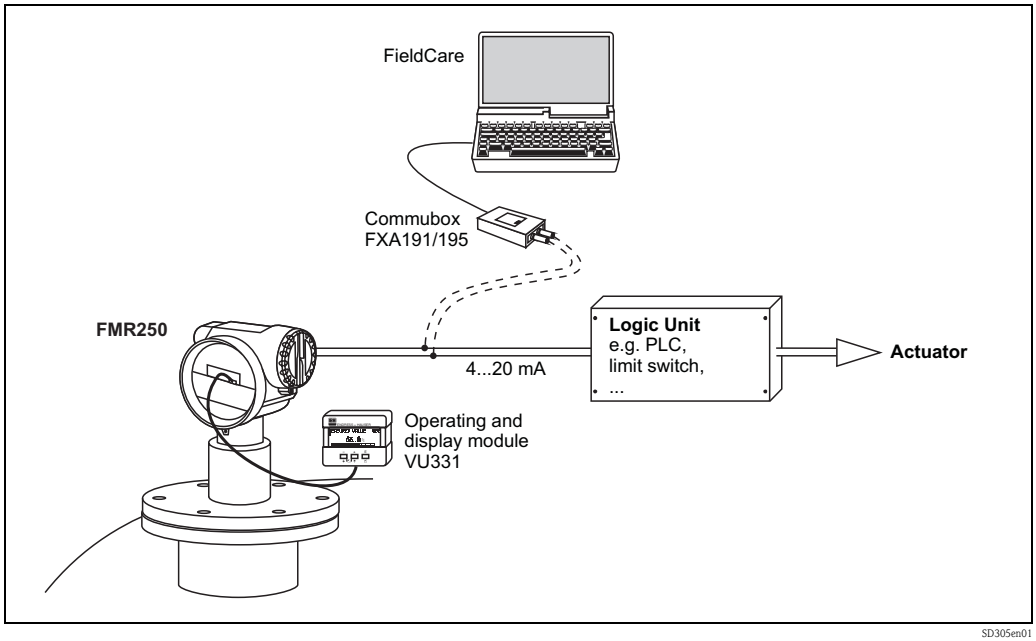
Introduction

Note!
General information on functional safety (SIL) is available at:
www.de.endress.com/SIL (German) or www.endress.com/SIL (English) and in Competence Brochure CP002Z "Functional Safety in the Process Industry – Risk Reduction with Safety Instrumented Systems".

Structure of the measuring system

System components

The measuring system's devices are displayed in the following diagram (example).



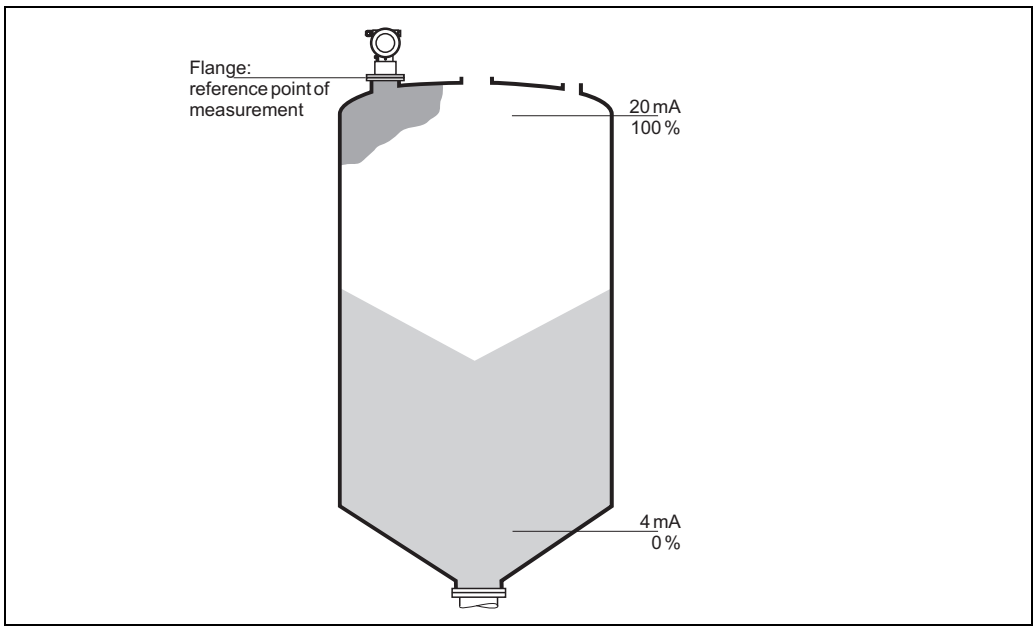
SD305en01

An analog signal (4 to 20 mA) in proportion to the level is generated in the transmitter. This is sent to a downstream logic unit (e.g. PLC, limit signal transmitter, etc.) where it is monitored to determine whether it is above a specified limit value.
For fault monitoring, the logic unit must recognize both HI-alarms (≥ 21.0 mA) and LO-alarms (≤ 3.6 mA).

Description of use as a protective system

The Micropilot M is a "downward-looking" measuring system that functions according to the ToF method (ToF = Time of Flight). The distance from the reference point (process connection of the measuring device) to the product surface is measured. Radar impulses are emitted by an antenna, reflected off the product surface and received again by the radar system.

Typical measuring arrangement:



Note!
Correct installation is a prerequisite for safe operation of the device.

Permitted device types

The details pertaining to functional safety in this manual relate to the device versions listed below and are valid as of the specified software and hardware version. Unless otherwise specified, all subsequent versions can also be used for safety instrumented systems.
A modification process according to IEC 61508 is applied for device changes.

Valid device versions for safety-related use:

Micropilot M FMR250		
Feature	**Designation**	**Version**
010	Approval	all
020	Antenna	all
030	Antenna Seal; Temperature	all
040	Antenna Extension	all
050	Process Connection	all
060	Output; Operating	A, B, K
070	Housing	all
080	Cable Entry	all
090	Additional Option	all

Valid software version: as of 01.05.00
Valid hardware version (electronics): as of delivery date January 2010

Supplementary device documentation

Documentation	Contents	Comment
Technical Information TI390F/00	– Technical data – Instructions on accessories	– The documentation is available on the Internet. → www.de.endress.com.
Operating Instructions BA284F/00	– Identification – Installation – Wiring – Operation – Commissioning – Maintenance – Accessories – Troubleshooting – Technical data – Appendix	– The documentation is supplied with the device. – The documentation is also available on the Internet. → www.de.endress.com.
Operating Instructions (Device Functions) BA291F/00	– Instructions on use – Micropilot M function menu – Function groups ... – ... – Envelope curve – Troubleshooting – Function menu index	– The documentation is available on the Internet. → www.de.endress.com.
Safety instructions depending on the selected version "Approval"	– Safety, installation and operating instructions for devices, which are suitable for use in potentially explosive atmospheres or as overfill protection (WHG, German Water Resources Act).	Additional safety instructions (XA, XB, XC, ZE, ZD) are supplied with certified device versions. Please refer to the nameplate for the relevant safety instructions.

Description of the safety requirements and boundary conditions

Safety function

The mandatory settings and safety function data emanate from the descriptions from Page 7.
The measuring system's reaction time is ≤ 5 s.

Note!
MTTR is set at eight hours.

Safety-related signal:

The Micropilot M's safety-related signal is the 4 to 20 mA analog output signal.
All safety measures refer to this signal exclusively.

The Micropilot M additionally communicates effectively via HART and contains all HART features with additional device information.

The safety-related output signal is fed to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter where it is monitored for the following:

- Overshooting a specified level limit.
- The occurrence of a fault, e.g. error current (≤ 3.6 mA, ≥ 21.0 mA, interruption or short-circuit of the signal line).

Restrictions for use in safety-related applications

The measuring system must be used correctly for the specific application, taking into account the medium properties and ambient conditions. Carefully follow instructions pertaining to critical process situations and installation conditions from the Operating Instructions.
The specifications from the Operating Instructions (→ 🖹 6, "Supplementary device documentation") must not be exceeded.

The following restriction also applies to safety-related use:

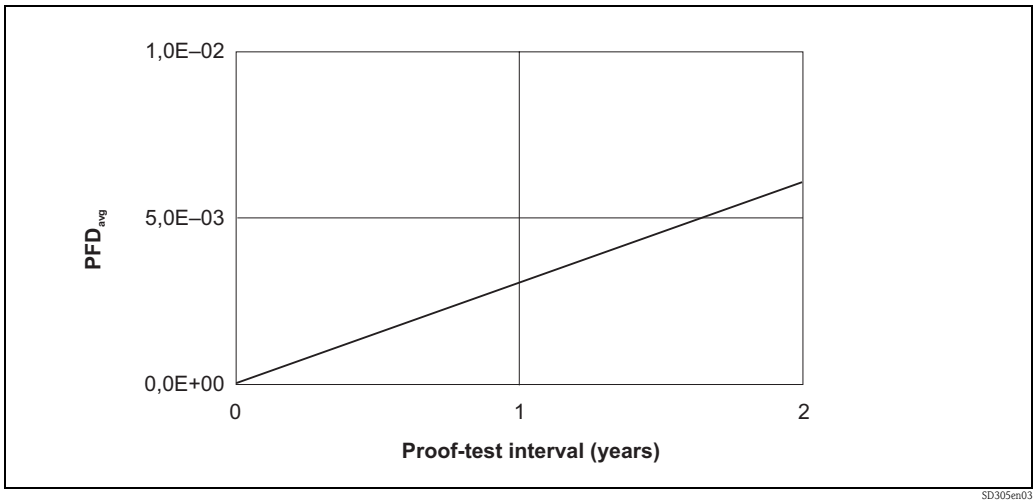
- The accuracy of the 4 to 20 mA safety-related output signal is ± 2%.

Functional safety indicators

The following tables show specific indicators for functional safety.

Characteristic as per IEC 61508	**Micropilot M with 4 to 20 mA output**
Safety functions	MAX
SIL	2
HFT	0
Device type	B
Mode of operation	Low demand mode
SFF	76.6 %
MTTR	8 h
Recommended time interval for proof-testing T_1	1 year
λ_{sd} *2	99 FIT
λ_{su} *2	1340 FIT
λ_{dd} *2	917 FIT
λ_{du} *2	718 FIT
λ_{tot} *3	3256 FIT
PFD_{avg} for T_1 = 1 year *1	3.14×10^{-3}
MTBF *3	35 years
System reaction time *4	≤ 5 s

*1 PFD_{avg} values for other T_1-values see "Proof-test interval".
*2 According to Siemens SN29500.
*3 According to Siemens SN29500, including faults outside the safety function.
*4 Step response time as per DIN EN 61298-2.



Proof-test interval

Dangerous undetected failures in this scenario:

An incorrect output signal that deviates from the real measured value by more than 2%, but is still in the range of 4 to 20 mA, is considered a dangerous, undetected failure.

Useful lifetime of electrical components:

The established failure rates of electrical components apply within the useful lifetime as per IEC 61508-2, section 7.4.7.4. note 3.

Behavior of device during operation and in case of error

Behavior of device during power-up

The safe 4 to 20 mA output signal is available after 17 s after the device is switched on or when the voltage returns.

Device response in the event of alarms or warnings

Error current

In the event of an alarm, the output current can be configured to a value of ≤ 3.6 mA or ≥ 21.0 mA.

In some cases (e.g. failure of power supply, a cable open circuit and faults in the current output itself, where the error current ≥ 21.0 mA cannot be set), output currents ≤ 3.6 mA irrespective of the configured error current can occur.

For alarm monitoring, the logic unit must therefore be able to recognize both HI-alarms (≥ 21.0 mA) and LO-alarms (≤ 3.6 mA).

Alarm and warning messages

Additional information is available in the form of fault codes on the alarm and warning messages output.

Installation

Installation, wiring and commissioning

Installation, wiring and commissioning of the device is described in the accompanying Operating Instructions (→ 🖹 6, "Supplementary device documentation").

Orientation

The permitted orientations of the device are described in the Operating Instructions.

Operation

Calibration of the measuring point

Calibration of the measuring point is described in the Operating Instructions.

The method of device configuration

Note!
Altered settings (display/FieldCare) in the "extended calibr." function group (Pos. 05) such as "offset" or "curr.turn down" (Pos. 063) in the "output" function group have an effect on the output signal.
This must be taken into account when calculating the response height (see relevant Operating Instructions).
We recommend that you check that the behavior of the current signal matches the expected behavior by means of level simulation (correctness of configuration).

Configuration schemata/basic calibration

FieldCare / Display - plain text display	**Display VU331 Position**
Media type	001
↓	
Tank shape	002
↓	
Medium property	003
↓	
Process conditions	004
↓	
Empty calibration E	005
↓	
Full calibration F	006
↓	
Pipe diameter (for bypass / stilling well)	007
↓	
Mapping	See Operating Instructions
↓	
Further settings: function group 05	See Operating Instructions
↓	
Overfill protection WHG	018
↓	
On-site locking: 3 keys on the VU331 display	Yes

With the "WHG" setting in 018, the following parameters can be set safety-oriented as follows, regardless of values already set:

FieldCare / Display - plain text display	**Value/parameter**	**Display VU331**	**Comment**
Safety settings			
output on ALARM	Max. 110 %, 22 mA	010	1
outp. echo loss	ALARM	012	1
delay time	1 s	014	2
in safety distance SD	self holding	016	4
Filtering/averaging/delay			
envelope statistics	2	**0D21**	3
MAM filt. length	5	**0D11**	3
MAM filt. border	1	**0D12**	3
output damping	0	058	3
Echo detection			
FAC adder	6 dB	**0D35**	1
Tank bottom detection	OFF	**0D61**	1
First echo factor	unchanged, but if previously smaller than 30, than: 0D53	**0D51**	4
FEF threshold	0	**0D52**	4
FEF at near distance	30 dB	**0D53**	4
FEF distance near	500 mm	**0D54**	4
FEF distance far	3000 mm	**0D55**	1
Max. filling speed	0 mm/s (factory setting)	**0D15**	1
Max. drain speed	0 mm/s (factory setting)	**0D16**	1
Other			
hysterese width	0 mm (factory setting)	**0D14**	1
Communication address	0	060	1
Current output mode	**"Standard"** if previously **"fixed current"**	063	1
Simulation	Sim. / OFF	065	1

Comment:

1. This parameter must be configured in this way.
2. This parameter determines the reaction time of the device in the event of echo loss; a setting of less than 30 s is recommended.
3. This parameter determines the reaction time of the device; deviating settings are possible.
   In case of changes in **"process cond." (004)** it is automatically adjusted. The corresponding reaction time is indicated in the documentation BA.
4. This parameter can be selected differently, depending on the application.

A measuring condition (echo) which results in an ALARM in the "Safety distance SD" area can be reset or deleted by

– confirming the ALARM in Pos. 017 locally by means of the VU331 LCD display;
– confirming the alarm via the communication protocol (HART) (FieldCare: "ackn. alarm" under safety settings).

Note!
The parameters highlighted in **bold** are on the service level which can only be opened with a specific code. Instead of activating the "WHG" setting, safety-oriented configuration can also be done manually as per the "Comment" column.

Locking

The device must be locked once the Micropilot M has been calibrated as per the Operating Instructions.

Type of locking	**Code/action**	**Position/VU331 display**
Software: mandatory	WHG	018
	↓	
Hardware: recommended	3 keys together "lock"	Locally via VU331 display (keys ⊞ and ⊟ and Ⓔ)

Unlocking

The device is unlocked by firstly removing the hardware lock by locally pressing all the three keys together via the VU331 LCD display and then by setting the "Overfill protection" parameter (Position 018) to "Standard" if necessary.

Type of unlocking	**Code/action**	**Position/VU331 display**
Hardware (if locked)	3 keys together "unlock"	Locally via VU331 display (keys ⊞ and ⊟ and Ⓔ)
	↓	
Software	Standard	018

Maintenance

Please refer to the relevant Operating Instructions (→ 🖹 6, "Supplementary device documentation") for instructions on maintenance and recalibration.
Alternative monitoring measures must be taken to ensure process safety during configuration, proof-testing and maintenance work on the device.

Proof-test

Proof-test

Check the operativeness and safety of safety functions at appropriate intervals!
The operator must determine the time intervals.
You can refer to the diagram "Proof-test interval" → 🖹 8 for this purpose.

Proof-testing of the device can be performed as follows:
– Approaching the level (→ test sequence A).
– Removing the device and measuring a medium with comparable properties (→ test sequence B).

You must also check that all cover seals and cable entries are sealing correctly.

Process for proof-testing

Test sequence A

Preparation

1. Connect suitable measuring device (recommended accuracy better ±0.1 mA) to the current output.
2. Determine the safety setting (level limit monitoring).

Procedure for level limit monitoring

1. Approach the level directly below the level limit to be monitored.
2. Read the output current, record it and assess for accuracy.
3. Approach the level directly above the level limit to be monitored.
4. Read the output current, record it and assess for accuracy.
5. The test is deemed successful if the current in step 2 does not result in activation of the safety function but the current in step 4 does.

Note!
The proof-test is deemed to have failed if the expected current value deviates for a specific level by > ±2%.
For troubleshooting, → Operating Instructions (→ 🖹 6, "Supplementary device documentation"), Section 9.
98% of dangerous, undetected failures are detected using this test.

Test sequence B

Preparation

1. Prepare the test tank with the medium (dielectric constant comparable to that of the medium to be measured).
   For installation instructions, → Operating Instructions (→ 🖹 6, "Supplementary device documentation"), Section 3.
2. Remove the device and mount it in the test tank.
3. Perform interference echo mapping if the shape and size of the test tank is different.
4. Connect suitable measuring device (recommended accuracy better than ±0.1 mA) to the current output.
5. Determine the safety setting (level limit monitoring).

Procedure for level limit monitoring
→ Test sequence A

Note!
The proof-test is deemed to have failed if the expected current value deviates for a specific level by > ±2%.
For troubleshooting, → Operating Instructions (→ 🖹 6, "Supplementary device documentation"), Section 9.
98% of dangerous, undetected failures are detected using this test.

Caution!
If an interference echo mapping was performed in the test tank, a valid interference echo mapping must be performed after the device is mounted in the original tank.

Note!
If one of the test criteria from the test sequences described above is not fulfilled, the device may no longer be used as part of a safety instrumented system.
The purpose of proof-testing is to detect random device failures. The impact of systematic faults on the safety function is not covered by this test and must be assessed separately.
Systematic faults can be caused, for example, by process material properties, operating conditions, build-up or corrosion.

Repairs

Repairs

Repairs on the devices must always be carried out by Endress+Hauser.
Safety functions cannot be guaranteed if repairs are carried out by anybody else.

Exception:
The following components can be replaced by the customer if the person responsible for doing so has been trained beforehand by Endress+Hauser:

- Sensor
- HF module
- Electronic insert
- Terminal module

The replaced components must be sent to Endress+Hauser for the purpose of fault analysis.
Once the components have been replaced, a proof-test must be carried out as per test sequence A (→ 🖹 13) or test sequence B (→ 🖹 13).

In the event of failure of a SIL-labeled Endress+Hauser device, which has been operated in a protection function, the "Declaration of Contamination and Cleaning" with the corresponding note "Used as SIL device in protection system" must be enclosed when the defective device is returned.
Please refer to the Section "Return" in the Operating Instructions (→ 🖹 6, "Supplementary device documentation").

Appendix

Commissioning or proof test protocol

System-specific data		
Company		
Measuring points / TAG no.		
System		
Device type / Order code		
Serial number of device		
Name		
Date		
Signature		
Device-specific commissioning parameters		
Empty calibration		
Full calibration		
Proof-test protocol		
Test stage	Set point	Actual value
1. Current value 1		
2. Current value 2		
3. If necessary current value 3		
4. If necessary current value 4		
5. If necessary current value 5		

SD305en05

FMEDA and Proven-in-use Assessment

Project:
Micropilot M – FMR 250
Applications with overspill protection

Customer:
Endress+Hauser GmbH+Co.
Maulburg
Germany

Contract No.: E+H 09/12-05
Report No.: E+H 09/12-05 R051
Version V1, Revision R0; December 2009
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Micropilot M FMR 250 with software version V5.00 / hardware version V2 for applications with overspill protection. The statements made in this report are also valid for further software versions as long as the assessed modification process is considered. Any changes are under the responsibility of the manufacturer. A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

For safety applications only the current output 4..20 mA was considered. All other possible output variants are not covered by this report.

Failure rates used in this analysis are basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part. For a SIL 2 application the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-03.

FMR 250 is considered to be a Type B[1] component device with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 subsystems.

As Micropilot M is supposed to be a proven-in-use product family, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 a hardware fault tolerance of 0 is sufficient for SIL 2 subsystems being Type B components and having a SFF of 60% to < 90%.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), a high failure can be classified as a safe detected failure and a low failure can be classified as a dangerous detected failure in case the Micropilot M is used in an application for "high level monitoring". For this application the following Table 1 shows that the FMR 250 module fulfills the above stated requirements.

Table 1: Summary for FMR 250

T[Proof] = 1 year	T[Proof] = 2 years	SFF
PFD_{AVG} = 3.14E-03	PFD_{AVG} = 6.26E-03	76.6%

λ_{sd} = 9.87E-08 1/h = 99 FIT

λ_{su} = 1.34E-06 1/h = 1340 FIT

λ_{dd} = 9.17E-07 1/h = 917 FIT

λ_{du} = 7.18E-07 1/h = 718 FIT

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

The box marked in yellow ( ) for T[Proof] = 2 years means that the calculated PFD_{AVG} value is within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but does 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 box marked in green ( ) for T[Proof] = 1 year means that the calculated PFD_{AVG} value is within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and does 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 functional assessment has shown that the Micropilot FMR 250 has a PFD_{AVG} within the allowed range for SIL 2 and a Safe Failure Fraction (SFF) of > 76%. Based on the verification of "proven-in-use" it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC (25°C ambient temperature plus internal self heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

The failure rates do not include failures resulting from incorrect use of the Micropilot M FMR 250, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

A user of the Micropilot M FMR 250 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates for different operating conditions is presented in section 5.1 along with all assumptions.

Instruments International

Endress+Hauser
Instruments International AG
Kaegenstrasse 2
4153 Reinach
Switzerland

Tel. +41 61 715 81 00
Fax +41 61 715 25 00
www.endress.com
info@ii.endress.com

Endress+Hauser

People for Process Automation

SD305F/00/EN/12.09
71107888
FM+SGML 6.0

71107888