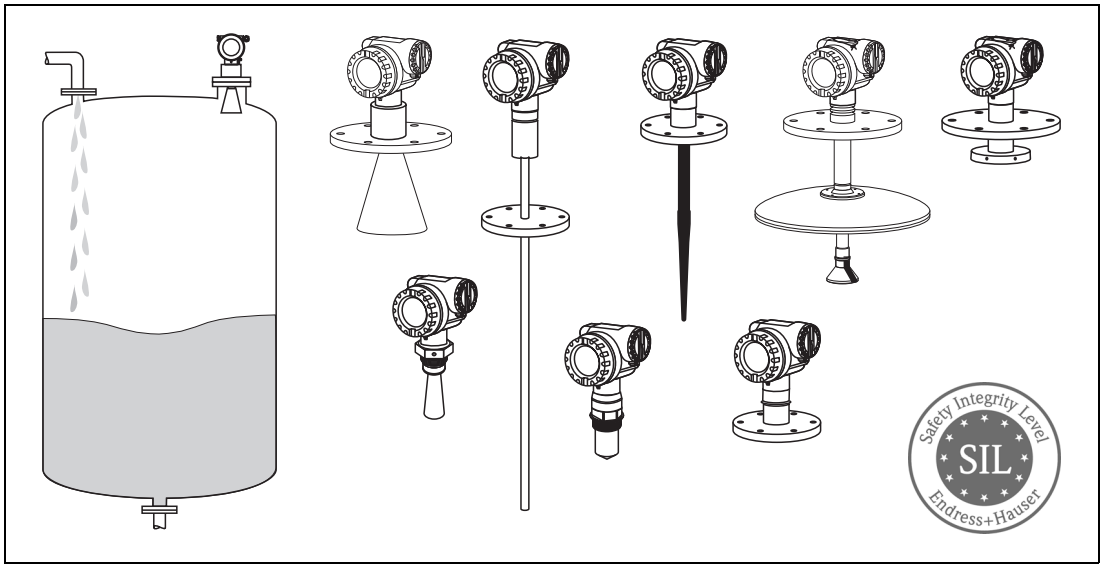
Level | Pressure | Flow | Temperature | Liquid Analysis | Registration | Systems Components | Services | Solutions

Functional Safety Manual

Micropilot M FMR230/231/232/233/240/244/245

Level-Radar
With 4...20 mA output signal



Application

Overspill protection or operating maximum detection of all types of liquids in tanks to satisfy particular safety systems requirements as per IEC 61508/IEC 61511-1.

The measuring device fulfils the requirements concerning

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

Your benefits

- For overspill protection up to SIL 2
  - Independently assessed (Functional Assessment) by *exida.com* as per IEC 61508/IEC 61511-1
- Permanent self-monitoring
- Continuous measurement
- Non-contact measurement: measurement is virtually independent of product properties
- Easy commissioning

SD150F/00/en/03.04
52016606

Endress+Hauser

People for Process Automation

Table of contents

SIL Declaration of Conformity

KD 02 001

ENDRESS + HAUSER

SIL Declaration of Conformity

Functional safety of a level measuring device according to IEC 61508/IEC 61511

Endress+Hauser GmbH+Co. KG, Hauptstrasse 1, 79689 Maulburg
declares as manufacturer, that the level measuring device

Micropilot M (4 ...20mA)

is suitable for the use in a safety instrumented system up to SIL 2 (for overspill protection) according to the standard IEC 61511-1, if the corresponding safety instructions are observed.

The FMEDA with analysis of the safety critical and dangerous faults provides under the assumption of an annual functional test cycle following parameters:

SIL	:	2			
HFT	:	0[1] (single use)			
Device type	:	Type B			
		FMR23x		FMR24x	
		with display	without display	with display	without display
SFF	:	>75%	>75%	> 76%	> 77%
PFD_{avg} [2]	:	$0{,}335 \times 10^{-2}$	$0{,}301 \times 10^{-2}$	$0{,}297 \times 10^{-2}$	$0{,}263 \times 10^{-2}$
$MTBF_{total}$	:	37 years	40,6 years	38,6 years	42,4 years
λ_{du}	:	766 FIT	689 FIT	680 FIT	603 FIT
λ_{dd}	:	882 FIT	882 FIT	850 FIT	850 FIT
λ_{su}	:	1340 FIT	1150 FIT	1340 FIT	1150 FIT
λ_{sd}	:	87 FIT	87 FIT	87 FIT	87 FIT

[1] according to clause 11.4 of IEC 61511-1
[2] The PFD_{avg} values are also within the range for SIL2 according to ISA S84.01.

The assessment of the proven-in-use demonstration covers the device and its software including the modification process.

Maulburg, 12.2.2004

Endress+Hauser GmbH+Co. KG

i.V. Manager Certification

i.V. Projectmanager

L00-FMR2xxxx-02-00-01-en-009

Introduction

General depiction of a safety system (protection function)

Rating tables for determining Safety Integrity Level (SIL)

The following tables define the achievable SIL or the requirements regarding the "Average Probability of a Dangerous Failure on Demand" (PFDav), the "Hardware Fault Tolerance" (HFT) and the "Safe Failure Fraction" (SFF) of the safety system. The specific values for the Micropilot M measuring system can be found in the tables in the appendix. Permitted failure probability of the complete safety function dependent on the SIL for systems which must react on demand (e.g. exceeding a defined max. level/switch point) (Source: IEC 61508, Part 1).

SIL	PFD_{av}
4	10^{-5} ...< 10^{-4}
3	10^{-4} ...< 10^{-3}
2	10^{-3} ...< 10^{-2}
1	10^{-2} ...< 10^{-1}

The following table shows the achievable Safety Integrity Level (SIL) as a function of the probability of safety-oriented errors and the hardware fault tolerance of the complete safety system for type B systems (complex components, for definition see IEC 61508, Part 2):

SFF		HFT		
		0	**1 (0)[1]**	**2 (1)[1]**
none:	<60%	not allowed	SIL 1	SIL 2
low:	60 % ...< 90 %	SIL 1	**SIL 2**	SIL 3
medium:	90% ...<99%	SIL 2	SIL 3	
high:	99 %	SIL 3		

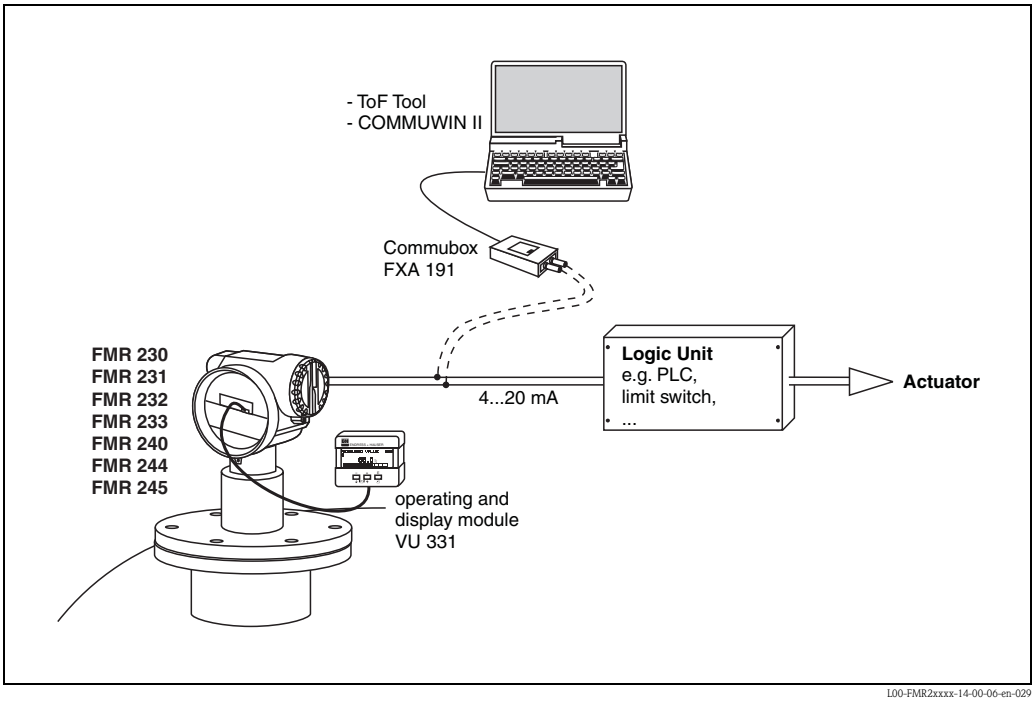
1) In accordance with IEC 615111-1 (chapter 11.4.4), the HFT can be reduced by one (values in brackets) if the devices used fulfil the following conditions:
- the device is proven in use,
- only process-relevant parameters can be changed at the device (e.g. measuring range, ...),
- changing the process-relevant parameters is protected (e.g. password, jumper, ...),
- the function requires less than SIL 4.

All conditions are met by the Micropilot M.

Measuring system layout with Micropilot M (FMR 230, FMR 231, FMR 232, FMR 233, FMR 240, FMR 244, FMR 245)

Limit level measuring system

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



An anologue signal (4...20 mA) proportional to the level is generated in the transmitter (Micropilot M) and is fed to a downstream Logic Unit (e.g. PLC, level limit sensor, ...) where it is monitored to ensure that it does not exceed the max. value.
For fault monitoring, the Logic Unit must detect both HI-alarms (21.5 mA) and LO-alarms (≤ 3.8 mA).

The characteristic values determined (see appendix) apply only to the following models:

FMR 230:
FMR 230######A###
FMR 230######B###
FMR 230######K###

FMR 231:
FMR 231#####A####
FMR 231#####B####
FMR 231#####K####

FMR 232:
FMR 232#####A###
FMR 232#####B###
FMR 232#####K###

FMR 233:
FMR 233#####A###
FMR 233#####B###
FMR 233#####K###

FMR 240:
FMR 240#######A###
FMR 240#######B###
FMR 240#######K###

FMR 244:
FMR 244######A###
FMR 244######B###
FMR 244######K###

FMR 245:
FMR 245#####A###
FMR 245#####B###
FMR 245#####K###

Safety function data

The **mandatory settings** and safety function data emanate from the description on **Page 7 ff.** and the **appendix** .
The measuring system's reaction time is ≤ 5 s.

Note!
MTTR is set at eight hours.

Supplementary device documentation

The following documentation must be available for the measuring system:

Device type	Operating Instructions	Description of device functions	Brief instructions (in the device)
FMR 230	BA 218F/00/en	BA 221F/00/en	KA 159F/00/a2
FMR 231	BA 219F/00/en	BA 221F/00/en	KA 159F/00/a2
FMR 232	SD 514F/00/en	BA 221F/00/en	KA 159F/00/a2
FMR 233	SD 515F/00/en	BA 221F/00/en	KA 159F/00/a2
FMR 240	BA 220F/00/en	BA 221F/00/en	KA 159F/00/a2
FMR 244	BA 248F/00/en	BA 221F/00/en	KA 159F/00/a2
FMR 245	BA 251F/00/en	BA 221F/00/en	KA 159F/00/a2

For devices with an explosion protection approval, the corresponding Safety Instructions (XA) or Control Drawings (ZD) must also be observed.

Settings and installation instructions

Installation instructions

The instructions for correct installation of the Micropilot M can be found in the corresponding Operating Instructions (BA) (see table on Page 6).
Since the application conditions have an influence on the reliability of the measurement, the corresponding instructions in the Technical Information (TI) and Operating Instructions (BA) must be observed.

Setting instructions

Note!
The allocation of the Operating Instructions (BA) to the relevant device can be found in the table on Page 6.

The Micropilot M can be set in various ways:
- On-site operation using LCD display VU 331
- Operation with handheld terminal DXR 275
- Remote operation using a PC:
  - with ToF tool (graphic operating program for measuring devices from E+H that work according to the Time of Flight principle)
  - Commuwin II (graphics-supported operating program for intelligent measuring devices)

  Caution!
  The reaction time of the device can slow down significantly during the transfer of envelope curves, mapping or FAC. Suitable measures should be taken against overfilling during this time.

Further instructions on settings can be found in the corresponding Operating Instructions (BA).

Setting the Micropilot M for operation as overspill protection

After the Micropilot M has been successfully calibrated in accordance with the Operating Instructions (BA), the parameter "*overspill prot.* " (Position 018) is set to "*german WHG* ".
Now no parameters can be changed, except for position 018, neither via the LCD display nor via communication; at the same time, several parameters are set according to the table on Page 9.
We recommend subsequent activation of the hardware lock on site via the keys on the LCD display VU 331 (all 3 keys together).
The device can now be neither configured nor unlocked via communication.
The device is unlocked by first deactivating the hardware lock on site via the keys on the LCD display VU 331 (all 3 keys together) and then setting the parameter "*overspill prot.* " (Position 018) to "*Standard* ".

A measuring condition (echo) that leads to an ALARM in the "Safety distance SD" range can be reset or deleted by
- confirming the ALARM in position 017 on site via the LCD display VU 331;
- confirming the alarm via the communication protocol (HART) (Commuwin II: Position V1 H7, ToF tool: under safety settings "*ackn. alarm*").

Note!
Changed settings (display/ToF Tool) in the "*extended calibr.*" function group (position 05 or Commuwin II V4) such as "*offset*" or "*output*" function group e.g. "*curr.output mode*" (position 063 or Commuwin II V5 H3) influence the output signal. This must be taken into consideration when calculating the response height (see the corresponding Operating Instructions for this).
We recommend to check that the course of the current signal matches the expected response (correctness of the configuration) using a level simulation (see BA).

Setting plan / Basic setup

ToF tool / plain text display	Display VU 331 Position	Commuwin II Position
Tank shape[1]	002	V0 H2
↓		
Medium property	003	V0 H3
↓		
Process conditions	004	V0 H4
↓		
Empty calibration E	005	V0 H5
↓		
Full calibration F	006	V0 H6
↓		
Pipe diameter (for bypass / stilling well)	007	V0 H7
Mapping	see BA[2]	see BA[2]
↓		
Further settings Function group	see BA[2] 05	see BA[2] V4
↓		
Overspill protection WHG	018	V1 H8
↓		
On site: 3 keys pressed on the display VU 331	yes	yes

1) For the FMR 240 with wave guide antenna, stilling well must always be selected as "Tank shape" (002).

2) BA = Operating Instructions

Locking

Type of security locking	Code / Action	Position / Display VU 331	Commuwin II
Software mandatory	german WHG	018	V1 H8
↓			
Hardware recommended	3 keys together "lock"	On site via display VU 331 (Keys ⊞ and ⊟ and Ⓔ)	

Unlocking

Hardware[1]	3 keys together "unlock"	On site via display VU 331 (Keys ⊞ and ⊟ and Ⓔ)	
↓			
Software	Standard	018	V1 H8

1) if locked

The "*german WHG*" setting is used to set the following parameters, independent of previously set values, as follows:

ToF tool / plain text display	Value / Parameter	Display VU 331	Commuwin II
Safety settings			
output on ALARM	Max. 110 %, 22 mA	010	V1 H0
outp. echo loss	ALARM	012	V1 H2
delay time	1	014	V1 H4
in safety distance	Self-retaining	016	V1 H6
Filtering / Averaging / Delaying			
Envelope statistics	2	**0D21**	**V72 H1**
MAM filt. length	5	**0D11**	**V71 H1**
MAM filt. border	1	**0D12**	**V71 H2**
output damping	0	058	V4 H8
Echo detection			
FAC adder	6 dB	**0D35**	**V73 H5**
Tank bottom detection	OFF	**0D61**	**V76 H1**
First echo factor	unchanged, but if previously smaller than 30, then: 0D53	**0D51**	**V75 H1**
FEF threshold	0	**0D52**	**V75 H2**
FEF at near distance	30 dB	**0D53**	**V75 H3**
FEF distance near	500 mm	**0D54**	**V75 H4**
FEF distance far	3000 mm	**0D55**	**V75 H5**
Max. filling speed	0	**0D15**	**V71 H5**
Max. drain speed	0	**0D16**	**V71 H6**
Miscellaneous			
Hysterese width	0 mm	**0D14**	**V71 H4**
Communication address	0	060	V5 H0
Current output mode	"Standard" if previously "fixed current"	063	V5 H3
Simulation	Sim. / OFF	065	V5 H5

Note!
The parameters in **bold** (for Display VU 331 and Commuwin II) are located in the service level which can only be opened by a certain code.

Setting instructions for evaluation unit

Setting instructions for using the level sensor as a continuous measuring device

When using the level sensor as a continuous measuring device, the determined limit value must be entered at the subsequent limit contactor (Logic Unit).
For all calibration and setting procedures, refer to the relevant Operating Instructions.

Response in operation and failure

Note!
The response in operation and failures is described in the device documentation (see table on Page 6).

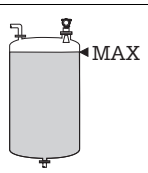
Commisioning and recurrent functional test of the measuring system

The operativeness of the overspill protection must be checked at appropriate time intervals (see appendix). It is the responsibility of the user to select the type of check and the intervals in the specified time frame.
The check must be carried out in such a way that it is proven that the overspill protection functions perfectly in interaction with all components.
This is guaranteed when the response height is approached in a filling process. If it is not practical to fill to the response height, a suitable simulation of the level or of the physical measuring effect must be used to make the level sensor respond. If the operativeness of the level sensor/transmitter can be determined otherwise (exclusion of errors that impair function), the check can also be completed by simulating the corresponding output signal.

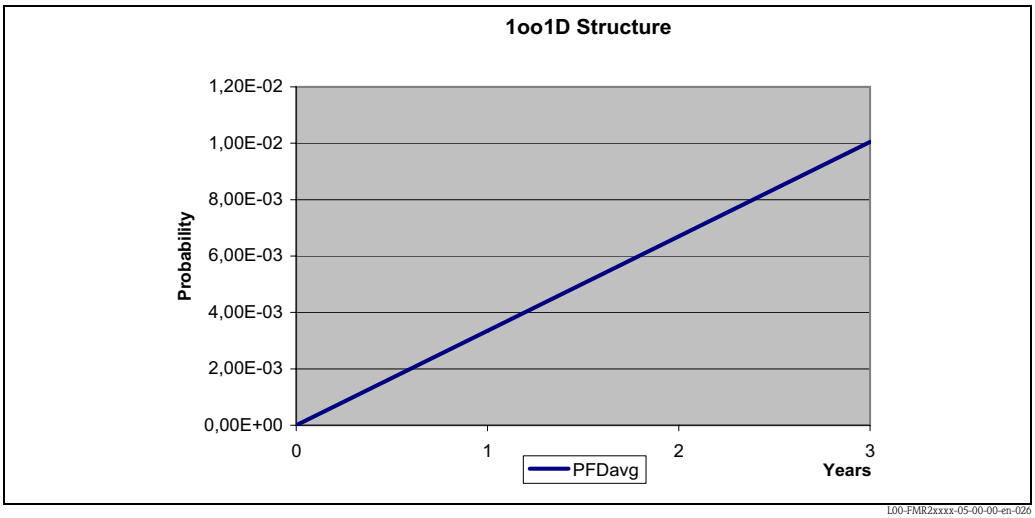
Appendix

Specific values for the Micropilot M measuring system

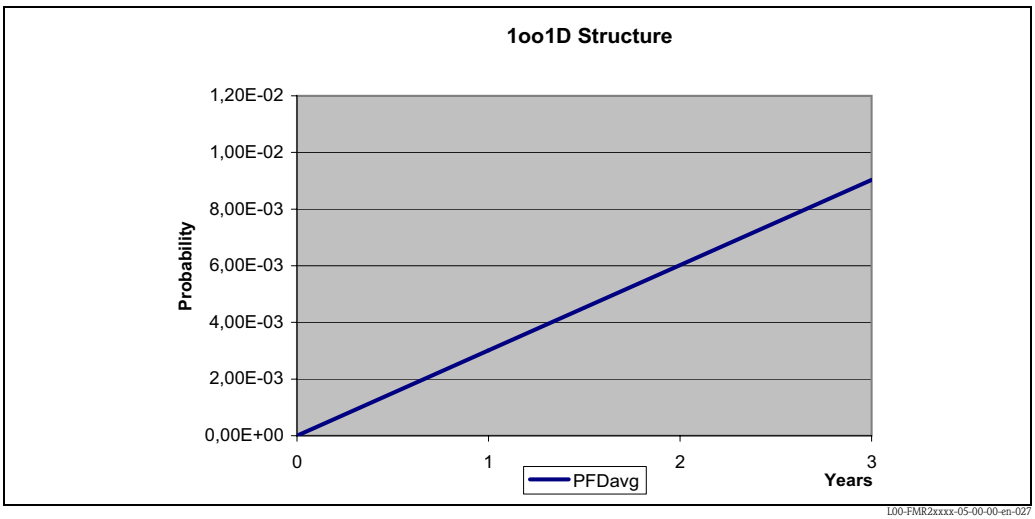
The tables show the specific safety characteristic values for the Micropilot M measuring system.

Specific values		
Micropilot M FMR 230, FMR 231, FMR 232, FMR 233	with display 	without display 
SIL	SIL 2	SIL 2
HFT	0	0
SFF	> 75 %	> 75 %
PFD_{av}	≤ 0.335 x 10^{-2}	≤ 0.301 x 10^{-2}
Complete function test, e.g. by approaching level	annual[1]	annual[1]

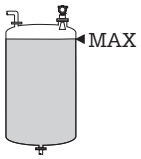
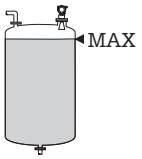
1) for further values see the following diagram



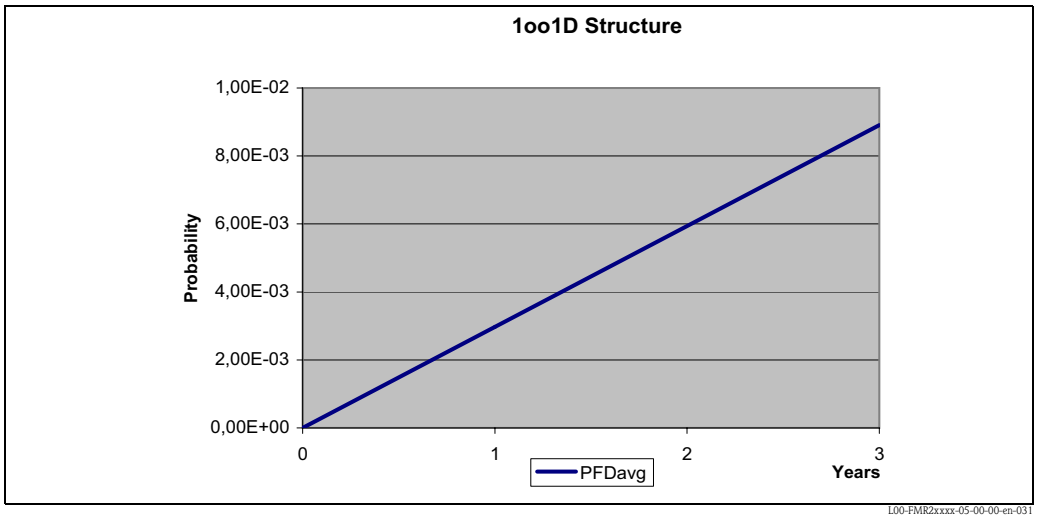
$PFD_{AVG}(t)$ FMR23x with display



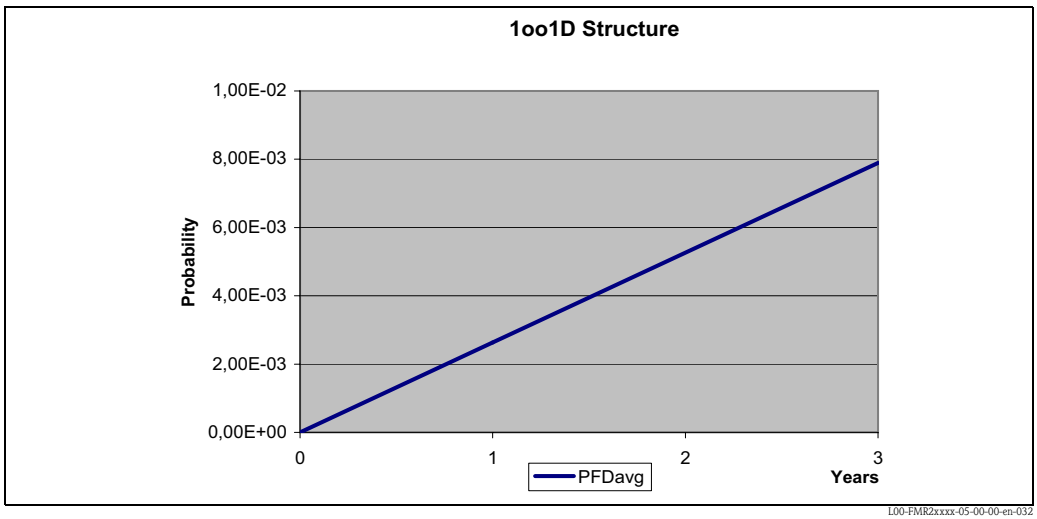
$PFD_{AVG}(t)$ FMR23x without display

Specific values		
Micropilot M **FMR 240, FMR 244, FMR 245**	with display 	without display 
SIL	SIL 2	SIL 2
HFT	0	0
SFF	> 76 %	> 77 %
PFD_{av}	≤ 0.297 x 10^{-2}	≤ 0.263 x 10^{-2}
Complete function test, e.g. by approaching level	annual[1]	annual[1]

1) for further values see the following diagram



$PFD_{AVG}(t)$ FMR24x with display



$PFD_{AVG}(t)$ FMR24x without display

exida.com®
excellence in dependable automation

FMEDA and Prior-use Assessment

Project:
Micropilot M - FMR 23x and FMR 24x
Applications with overspill protection

Customer:
Endress+Hauser GmbH+Co.
Maulburg
Germany

Contract No.: E+H 02/07-15
Report No.: E+H 02/07-15 R002
Version V2, Revision R1.1, November 2003
Stephan Aschenbrenner

exida.com®
excellence in dependable automation

Management summary

This report summarizes the results of the hardware assessment with prior-use consideration according to IEC 61508 / IEC 61511 carried out on the Micropilot M family FMR 23x and FMR 24x with software version V2.02 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. Table 1 gives an overview of the different types that belong to the considered family.

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.

Table 1: Version overview

FMR 23x (~ 6 GHz)	FMR 24x (~ 26 GHz)
FMR 230 (with horn antenna)	FMR 240 (with horn antenna)
FMR 231 (with rod antenna)	FMR 240 (with wave guide antenna)
FMR 232 (with planar antenna)	FMR 244 (with PTFE-enclosed horn antenna)
FMR 233 (with parabolic antenna)	FMR 245 (with flush mounted PTFE-clad flange)

For safety applications only the current output 4..20 mA was considered. All other possible output variants are not covered by this report. The different devices can be equipped with or without display.

The failure rates used in this analysis are based on 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 23x and FMR 24x are considered to be Type B[1] components 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 (sub-) systems.

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 5.4 a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% to < 90%.

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

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 tables show which modules fulfill the above stated requirements.

Table 2: Summary for FMR 23x with display

T[Proof] = 1 year	T[Proof] = 2 years	SFF
PFD_{AVG} = 3.35E-03	**PFD_{AVG} = 6.68E-03**	> 75 %

λ_{sd} = 8,67E-08 1/h = 87 FIT

λ_{su} = 1,34E-06 1/h = 1340 FIT

λ_{dd} = 8,82E-07 1/h = 882 FIT

λ_{du} = 7,66E-07 1/h = 766 FIT

Table 3: Summary for FMR 23x without display

T[Proof] = 1 year	T[Proof] = 2 years	SFF
PFD_{AVG} = 3.01E-03	**PFD_{AVG} = 6.00E-03**	> 75 %

λ_{sd} = 8,67E-08 1/h = 87 FIT

λ_{su} = 1,15E-06 1/h = 1150 FIT

λ_{dd} = 8,82E-07 1/h = 882 FIT

λ_{du} = 6,89E-07 1/h = 689 FIT

Table 4: Summary for FMR 24x with display

T[Proof] = 1 year	T[Proof] = 2 years	SFF
PFD_{AVG} = 2.97E-03	**PFD_{AVG} = 5.93E-03**	> 76 %

λ_{sd} = 8,67E-08 1/h = 87 FIT

λ_{su} = 1,34E-06 1/h = 1340 FIT

λ_{dd} = 8,50E-07 1/h = 850 FIT

λ_{du} = 6,80E-07 1/h = 680 FIT

Table 5: Summary for FMR 24x without display

T[Proof] = 1 year	T[Proof] = 2 years	SFF
PFD_{AVG} = 2.63E-03	**PFD_{AVG} = 5.26E-03**	> 77 %

λ_{sd} = 8,67E-08 1/h = 87 FIT

λ_{su} = 1,15E-06 1/h = 1150 FIT

λ_{dd} = 8,50E-07 1/h = 850 FIT

λ_{du} = 6,03E-07 1/h = 603 FIT

The boxes marked in yellow (▭) for T[Proof] = 2 years mean that the calculated PFD_{AVG} 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 boxes marked in green (▭) for T[Proof] = 1 year mean that the calculated PFD 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.

The functional assessment has shown that devices of the Micropilot M family FMR 23x and FMR 24x have a PFD_{AVG} within the allowed range for SIL 2 and a Safe Failure Fraction (SFF) of > 75%. Based on the verification of "prior use" they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the Micropilot M 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 to 5.4 along with all assumptions.

International Head Quarter

Endress+Hauser
GmbH+Co. KG
Instruments International
Colmarer Str. 6
79576 Weil am Rhein
Deutschland

Tel. +49 76 21 9 75 02
Fax +49 76 21 9 75 34 5
www.endress.com
info@ii.endress.com

Endress+Hauser

People for Process Automation

SD150F/00/en/03.04
52016606
FM+SGML 6.0 ProMoDo