ABB MEASUREMENT & ANALYTICS | SIL-SAFETY INSTRUCTION

ProcessMaster FEP300, FEP500
HygienicMaster FEH300, FEH500
Electromagnetic flowmeter

Information about functional safety

Measurement made easy

ProcessMaster
FEP300, FEP500
HygienicMaster
FEH300, FEH500

Electromagnetic Flowmeter for flow measurement of liquid, pulpy or pasty measurement media with electrical conductivity

Further information

Additional documentation on ProcessMaster FEP300, FEP500/HygienicMaster FEH300, FEH500 is available for download free of charge at www.abb.com/flow.

FEP300 FEP500 FEH300 FEH500

Manufacturer

ABB Limited
Measurement & Analytics
Oldends Lane, Stonehouse
Gloucestershire, GL10 3TA
Tel: +44 (0)1453 826 661
Fax: +44 (0)1453 829 671
Email: instrumentation@gb.abb.com

Customer Service
Tel: +49 0180 5 222 580
Email: automation.service@de.abb.com

ABB Inc.
Measurement & Analytics
125 E. County Line Road
Warminster
PA 18974
USA
Tel: +1 215 674 6000
Fax: +1 215 674 7183

ABB Engineering (Shanghai) Ltd.
Measurement & Analytics
No. 4528, Kangxin Highway,
Pudong New District
Shanghai, 201319,
P.R. China
Tel: +86(0) 21 6105 6666
Fax: +86(0) 21 6105 6677
Email: china.instrumentation@cn.abb.com

ABB Automation Products GmbH
Measurement & Analytics
Dransfelder Str. 2
37079 Göttingen
Deutschland
Tel: 0800 1114411
Fax: 0800 1114422
Email: vertrieb.messtechnikprodukte@de.abb.com

Contents

1 Acronyms and abbreviations

Abbreviation	Designation	Description
HFT	Hardware Fault Tolerance	Hardware fault tolerance of the unit. Ability of a functional unit (hardware) to continue to perform a required function when faults or errors are prevailing.
MTBF	Mean Time Between Failures	Mean time between failures.
MTTR	Mean Time To Restoration	Mean time between the occurrence of an error in a unit or in a system and its repair.
PFD	Probability of Dangerous Failure on Demand	Probability of hazardous failures for a safety function on demand.
PFD_{AVG}	Average Probability of Dangerous Failure on Demand	Average probability of hazardous failures for a safety function on demand.
SIL	Safety Integrity Level	The international standard IEC 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for the failure of a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will not perform the required safety function.
Low Demand Mode	Low Demand Mode of operation	Measurement type with low request rate. Measurement type for which the request rate for the safety-related system is not more than once a year and not greater than twice the frequency of the retest.
DCS	Distributed Control System	Control system used in industrial applications to monitor and control decentralized units.
HMI	Human Machine Interface	In this case, the HMI is a combined module consisting of an LCD display with or without a local keyboard.
DTM	Device Type Manager	A DTM is a software module that supports specific functions for accessing device parameters, the setup and the operation of devices, and diagnostics. The DTM is not executable software. It requires an FDT container program in order to be activated.
LRV	Device Configuration	Lower Range Value of the measurement range.
URV	Device Configuration	Upper Range Value of the measurement range.
DC	Diagnostic Coverage	Fraction of dangerous failures covered by cyclical diagnosis functions on runtime.
Multidrop	Multidrop Mode	In Multidrop Mode, up to 15 field devices are connected in parallel to a single wire pair. The analog current signal simply serves to supply power to the devices in two-wire technology with a fixed current of ≤ 4 mA.

2 Standards and definitions of terms

2.1 Standard IEC 61508 (2010), Part 1 and 2

— English
  Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices).
— German
  Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme (Zielgruppe: Hersteller und Lieferanten von Geräten).

2.2 Dangerous failure

A failure that has the potential to place the safety-related system in a dangerous state or render the system inoperative.

2.3 Safety-related system

A safety-related system performs the safety functions that are required to achieve or maintain a safe condition, e.g., in a plant.
Example: pressure meter, logics unit (e.g., alarm signalling unit) and valve form a safety-related system.

2.4 Safety function

A specified function that is performed by a safety-related system with the goal, under consideration of a defined hazardous incident, of achieving or maintaining a safe condition for the plant.
Example: limit pressure monitoring

3 Other applicable documents and papers

The following documentation must be available for the flowmeter. These documents include details about functional specifications of the analog output and how to operate and configure the device.

Document name	Document type
CI/FEX300/FEX500	Commissioning Instruction
OI/FEX300/FEX500	Operating Instruction

For devices in explosion-proof design, the Safetey Instructions must also be observed.

Document name	Document type
SM/FEX300/FEX500	Safety Instructions

4 Determine the Safety Integrity Level (SIL)

The achievable Safety Integrity Level for a device certificated according EN 61508-2 route 2S and 2H is determined by the following safety-related parameters:

— Average probability of hazardous failures for a safety function on demand (PFD_{AVG})
— Hardware Fault Tolerance (HFT)

Table below shows the achievable Safety Integrity Level (SIL) based on the Average Probability of Failure on Demand (PFD_{AVG}) for the complete safety function system consisting of the Flowmeter, the Logics Unit and the Actuator.

Safety Integrity Level (SIL)	**PFD_{AVG} (low demand mode)**
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Table below shows the achievable Safety Integrity Level (SIL) for the complete safety-related system for type B systems depending on the Hardware Fault Tolerance (HFT).
Type B systems are, for example, sensors with complex components such as microprocessors (see IEC 61508, Part 2).

Hardware Fault Tolerance (HFT)		
0	**1**	**2**
SIL 1	SIL 3	SIL 4
SIL 2 (low demand mode)	SIL 2 (high demand mode / continuous mode)	

NOTICE

ProcessMaster and HygienicMaster flowmeter fulfill HFT = 0 and are applicable for safety-related systems as per table above.
In low demand mode the demand rate for the safety-related system is not more than once a year and not greater than double the frequency of the periodic test.

5 The Flowmeter as part of the safety function system

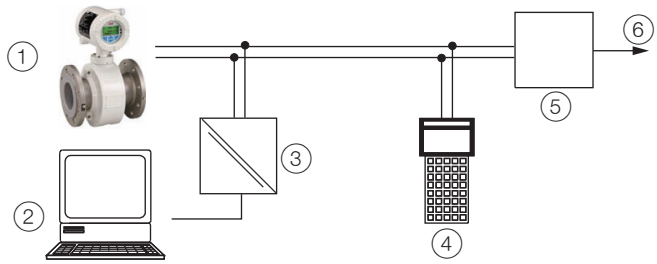

Fig. 1: Safety function (e.g. min / max flowrate monitoring) with flowmeter as a sub-system

(1) ProcessMaster or HygienicMaster
(2) Notebook with configuration Tool such as SMART VISION
(3) FSK-Modem (4) Handheld terminal
(5) Automation System, Logic-Unit, PLC, alarm signalling unit, etc.
(6) Actuator

The Flowmeter transmitter generates an analog signal (4 ... 20 mA) proportional to the flowrate. The analog signal is fed to a downstream logics unit such as a PLC or an alarm signalling unit, and is monitored for exceeding a specified maximum or minimum value.

NOTICE

The safety-related signal is the 4 ... 20 mA analog output signal of the flowmeter transmitter.
All safety functions refer exclusively to this analog output (terminals 31 / 32).

5.1 Device specific data related to functional safety

Term	Value
DeviceType	ProcessMaster FEP300, FEP500, HygienicMaster FEH300, FEH500
Firmware Level	from 01.02.01 to 01.03.02
Hardware Level	Electronics compartment Part number D674A903U01 Rev. 05 to 13 Par tnumber D674A904U01 Rev. 05 to 13 Part number D674A905U01 Rev. 05 to 13 Part number D674A906U01 Rev. 05 to 13
Type of Assessment	Proven in Use Assessment according IEC 61508-2 route 2S
Hardware Fault Tolerance	Architecture Route 2H according to IEC 61508-2
SIL capability	SIL2 (Low demand mode)
HFT	0
Component Type	B

Failure Rates	SIL Detector	
	OFF	ON
DC	71.1 %	82.6 %
PFD_{AVG} after 10 years with Proof Test Interval of 1 year and Proof Test Coverage of 90 % (valid for FEX311, FEX511, FEX315, FEX515, FEX325, FEX525)	2,65E-03	1,51E-03
PFD_{AVG} after 6 years with Proof Test Interval of 1 year and Proof Test Coverage of 90 % (valid for FEX321, FEX521)	2,09E-03	1,20E-03
λ_{SD}	0 FIT	0 FIT
λ_{SU}	943 FIT	943 FIT
λ_{DD}	937 FIT	1070 FIT
λ_{DU}	317 FIT	181 FIT

NOTICE

The configuration menu of the device includes a parameter called “SIL Detector”. To assure PFD value as per table above, the Detector has to be set accordingly.

NOTICE

The listed failure rates λ_{SD}, λ_{SU}, λ_{DD} and λ_{DU} depend on the meter design (standard or high temperature design).
The listed failure rates λ_{SD}, λ_{SU}, λ_{DD} and λ_{DU} are valid for ambient temperatures up to 45 °C. For higher ambient temperatures up to 60 °C, the failure rates and the PFD_{AVG} must be multiplied with a factor of 2.5. See diagram below.

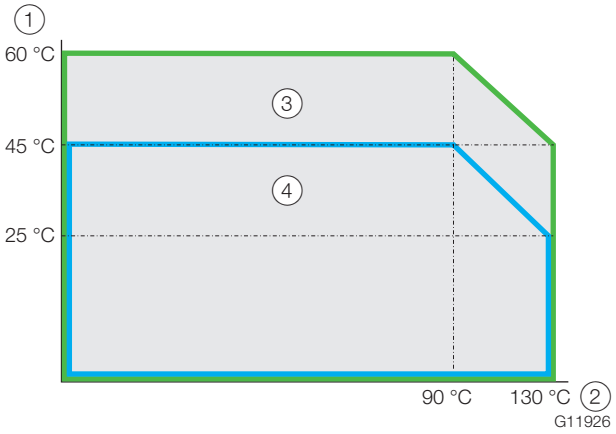

Fig. 2: Standard temperature design
(1) Ambient temperature (2) Fluid temperature
(3) Failure rates and PFD_{AVG} to be multiplied with a factor of 2.5
(4) Failure rates and PFD_{AVG} as per table

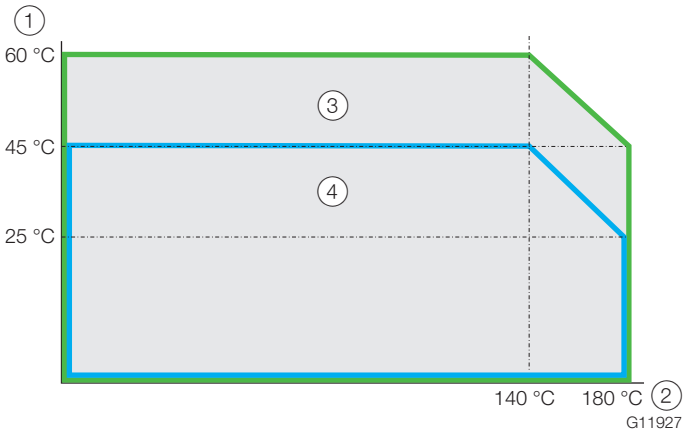

Fig. 3: High temperature design
(1) Ambient temperature (2) Fluid temperature
(3) Failure rates and PFD_{AVG} to be multiplied with a factor of 2.5
(4) Failure rates and PFD_{AVG} as per table

5.2 Prerequisites operating the device functional safety compliant

- The analog signal of the transmitter can be considered to be safe after 30 minutes (warm up time).
- A dangerous error is an error during which the output analog output of the transmitter no longer responds to the input signal or deviates by more than 2 % from the maximum flowrange $Q_{max}DN$.
- For $Q_{max}DN$ see device nameplate or refer to instruction manual.
- The maximum reaction time of the device on error is less than 3 hours.
- The response time of the current output depends on the parameterization (Noise Filter settings and Damping) and is less than 5 Minutes.

6 Setup

6.1 Analog output

The status of this analog output (4 … 20 mA output) during alarm conditions, can be configured either to go to a “high alarm” level or to a “low alarm” level. (See instruction manual).
For “high alarm” level, a range from 21 … 23 mA can be assigned to the analog output.
For “low alarm” level, a range from 3.5 … 3.6 mA can be assigned to the analog output.

i NOTICE

The safety function of the automation system must be able to detect errors that result in “high alarm” level as well as those that result in “low alarm” level.
The analog output signal of the transmitter can be configured as “active mode” or as “passive mode”. With the analog output configured “passive mode”, the external supply power of the 20mA loop must be capable to provide the required voltage level even in case of a “high alarm” level.

i NOTICE

After completion of the parameter configuration, the safety function has to be checked.
The transmitter software menu allows for simulation of the analog output. See Instruction manual.
Behavior during operation and failure is described in the operating instructions.

6.2 Locking / Unlocking the configuration level

⚠ WARNING

Unauthorized changes of the parameter settings may affect the safety function.
This device can be configured through the local Keypad or using HART communication.
During configuration and in case of simulation and driving the device in HART Multidrop Mode, the device is not safety compliant.
Once configuration is completed, the device must be protected against unauthorized access.
Refer to Instruction manual – set hardware write switch to ensure the keypad is locked and write protection through HART is enabled too.
With the hardware write protection switched to ON, try to alter a parameter to make sure the write protection mechanism is enabled properly.

To lock the device access menu „Device Setup / Access Control” and set the password of the corresponding log in level.

Menu / parameter	Value range	Description
Device Setup / ....Access Control		
Standard Password	Alphanumeric	Enter the password for the "Standard" access level.
Advanced Password	Alphanumeric	Enter the password for the "Advanced" access level.
Read Only Switch	Display only (ON / OFF)	Display the setting of the configuration of the Read Only switch (BR902 - hardware write protection)

6.2.1 Hardware write protection

In addition to the software password protection, it is possible to enable a hardware write protection.

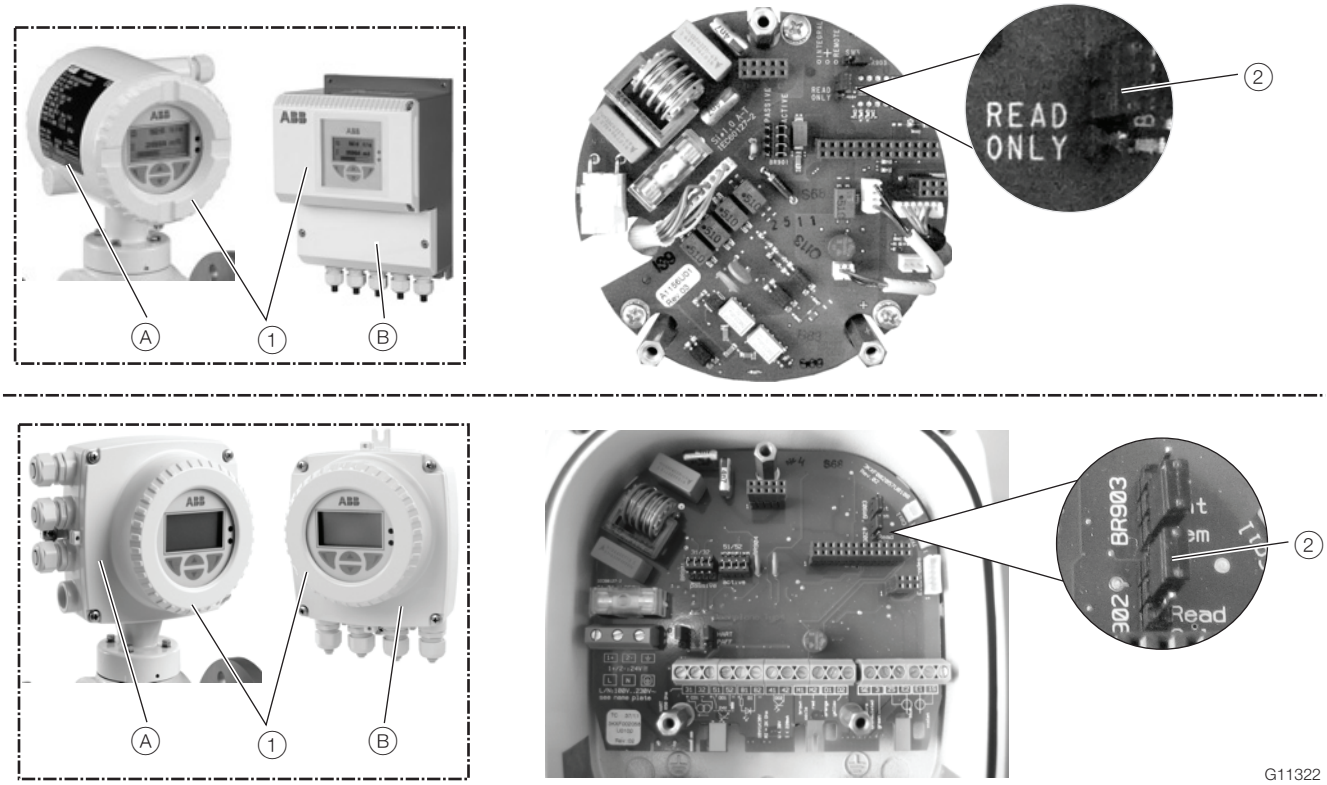

Fig. 4: Jumper for hardware write protection
(A) Integral mount design (B) Remote mount design
(1) Housing cover (2) Jumper (BR902) for hardware write protection

1. Switch off power supply.
2. Open the housing cover.
3. Remove the mounting screws for the transmitter electronics unit.
4. Pull out the transmitter electronics unit.
5. Set jumpers on backplane in accordance with the following table.

Jumper	Number	Function
BR902	Read only	Hardware write protection active

6. Reinstall the transmitter electronic unit in reverse order.

6.3 Configuration of the flowmeter transmitter

Note

Some parameter settings may affect the safety function.
Changing these parameters, the safety function has to be checked again.
Refer to Commissioning Instruction (CI/FEX300/FEX500) and Operating Instruction (OI/FEX300/FEX500) for Settings and Installation Instructions.

Menu / parameter	Description	Action
Diagnostics / ....Diagnosis Control / Sil Detection		
Sil Detection	To assure PFD value as per table in chapter 2.1, the Detector has to be set accordingly.	Check Safety Function.

Easy Setup		
Q [units]	Select the engineering unit for flowrate indication in the display.	Check Safety Function once parameter setting is completed.
Qmax	Select the flow range for forward and reverse flow. Default setting: 1 x QmaxDN.	Check Safety Function once parameter setting is completed.
Damping	Select the damping. The setting relates to 1 T (Tau). The damping affects the analog output response time. Default setting: 1 second.	Check Safety Function once parameter setting is completed.
Iout at Alarm	Status of the analog output during error conditions can be configured either to go to a “high alarm” level or to a “low alarm” level. (See instruction manual). Default setting: “High”.	Check Safety Function once parameter setting is completed.
Low Alarm Value	Analog output “Low alarm” level. A range from 3,5 to 3,6mA can be assigned to the analog output. Default setting: 3.5 mA.	Check Safety Function once parameter setting is completed.
High Alarm Value	Analog output “High alarm” level. A range from 21 to 23mA can be assigned to the analog output. Default setting: 21.8 mA.	Check Safety Function once parameter setting is completed.
System Zero	Manual adjustment of the system zero.	Check Safety Function once parameter setting is completed.
Cable length	Enter the signal cable length between the transmitter and the flowmeter sensor. For devices with a compact design (FEP311, FEH311, FEP315, FEH315) 0.01 m must be entered.	Check Safety Function once parameter setting is completed.

Device Setup / ....Sensor		
Qmax2	See Qmax.	Check Safety Function once parameter setting is completed.
Range Mode	Manual switchover between flow range Qmax and Qmax2.	Check Safety Function once parameter setting is completed.

Menu / parameter	Description	Action
Device Setup / ....Transmitter / ....Units		
Custom Vol. Type	Select whether the user-defined flow unit is displayed as a mass flow (with density) or volume flow (without density).	Check Safety Function. When a mass flow unit is selected, the corresponding density must be set.
Custom Vol. Factor	Enter the factor for a user-defined flow unit. The factor relates to the flow per liter.	Check Safety Function.

Device Setup / ....Transmitter		
Density	To show the flowrate in massflow units a fixed density must be configured to convert the volume flowrate into mass flowrate.	Check Safety Function once parameter setting is completed.

Device Setup / ....Transmitter / ....Low Flow Cut Off		
Flow Cut Off Level	Threshold for low flowrate monitoring. If the flowrate is below threshold, the flow is not measured. The current output is set to zero.	Check Safety Function.
Hysteresis	Set the hysteresis for the low flow cut off.	Check Safety Function.

Device Setup / ....Transmitter / ....Operating Mode		
Meter Mode	Measuring direction for the flowmeter. — "Forward only": The device measures only forward flow direction. — "Forward and Reverse": The device measures both directions.	Check Safety Function.

Device Setup / ....Transmitter / Noise Reduction		
Noise Reduction	Enables noise filtering. Filtering increases the response time of the SIL relevant 4 ... 20 mA output.	Check Safety Function once parameter setting is completed.

Input/Output / ....Current Output		
Iout at EP Alarm	Status of the analog output during empty pipe condition. — Off: Error is not output at the current output. — Q = 0 %: The current output assumes the value for "No flow". — High Alarm: The current output assumes the value for "High Alarm". — Low Alarm: The current output assumes the value for "Low Alarm". Default setting: Off.	Check Safety Function once parameter setting is completed.
Iout at Flow >103%	Status of the analog output when flowrate exceededs 103 % of the flow range end value set. — Off: Error is not output at the current output. — High Alarm: The current output assumes the value for "High Alarm". — Low Alarm: The current output assumes the value for "Low Alarm". Default setting: Off.	Check Safety Function once parameter setting is completed.
Iout Mode	Select the operating mode for the current output. — 4 ... 20 mA - 4 mA = No flow - 20 mA = Maximum flow — 4 ... 12 ... 20 mA - 4 mA = Maximum reverse flow - 12 mA = No flow - 20 mA = Maximum forward flow	Check Safety Function once parameter setting is completed.

Menu / parameter	Description	Action
Process Alarm / ....Group Masking		
Maintenance Required Function Check Out of Specification	Alarm messages are divided into 3 groups. Maintenance, Function Check and Out of Spec. Masking of a group results in no error message any longer for errors belonging to this group.	Masking is not allowed for parameter setting for a Functional Safety application. Parameter has to be switched to “OFF”.

Process Alarm / ....Individual Masking		
Min Flowrate Alarm Max Flowrate Alarm Flow >103% Com Controller Alarm Empty Pipe Detector	Individual alarm messages can also be masked. These alarms are not included in the masking of a group such a Maintenance. Masking of an individual alarm results in no error message any longer for this alarm.	Check Safety Function once parameter setting is completed

Process Alarm / Alarm Simulation		
Simulation Mode	Manual simulation of measured values. The output values correspond to the simulated flowrate entered. The “Configuration” information is displayed in the lower line of the display. Restore the Simulation mode to “Off” once completed. The values in the “Value range” column can be simulated.	Make sure Simulation mode is switched to “Off” once completed.

Diagnostics / ....Diagnosis Control / ....Empty Pipe Detector		
Manual Adjust EP	Manual adjustment of the Empty Pipe Detector function.	Check Safety Function once parameter setting is completed.
Flow Cut Off Level	Threshold of the empty pipe detection.	Check Safety Function once parameter setting is completed.

Diagnostics / ....Diagnosis Control / ....Sensor Measurements		
Coil R. Max Alarm	Set the maximum limit value for the coil resistance. Exceeding this limit results in an alarm.	Check Safety Function once parameter setting is completed.
Coil R. Min Alarm	Set the minimum limit value for the coil resistance. Exceeding this limit results in an alarm.	Check Safety Function once parameter setting is completed.

7 Proof Test

In accordance with IEC61508, the safety function of the measuring device must be checked at appropriate time intervals. The operator must determine the checking interval and take this into account when determining the probability of failure PFDavg of the flowmeter.
The test must be carried out in such a way that it verifies correct operation of the device.
Testing the device can be performed in the following steps:

7.1 Calibration

Calibrating the device in a certified calibration rig checking the analog output safety function results in a > 98 % diagnostic coverage detecting undetected failures.

7.2 On-site test, performed by ABB service personnel

An on-site test, performed by ABB service personnel results in a > 90 % diagnostic coverage detecting undetected failures.

7.3 ScanMaster Verification

Performing a ScanMaster Verification results in a > 50 % diagnostic coverage detecting undetected failures.
If the test is not passed, the device may no longer be used as part of a protective system.
The influence of systematic faults on the safety function are not covered by the test and must be examined separately. Systematic faults can be caused, for example, by medium properties, operating conditions, build-up or corrosion.

8 Repair

To ensure the safety related function, repairs have to be performed by ABB.
Replacing modular components by original ABB spare parts is permitted if personnel was trained by ABB for this purpose.
The "Declaration of contamination and cleaning" must be enclosed when returning the defective device.
Refer to instruction manual for further details.

Adress:
ABB Automation Products GmbH
Measurement & Analytics
Dransfelder Str. 2
37079 Goettingen
Germany
Tel: +49 551 905-0
Fax: +49 551 905-777

9 SIL 2 certificate

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-11074-01-00

TÜV NORD

Certificate

No. SEBS-A.150643/15 V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies to

ABB Automation Products GmbH

Dransfelder Straße 2
37079 Göttingen, Germany

that the electromagnetic flowmeters

FEx 300/500

are capable for safety related applications up to SIL 2 and meets the requirements listed in the following standard.

- **IEC/DIN EN 61508-1/-2: 2010/2011**

The flowmeters can be used in applications according to IEC/DIN EN 61511-1: 2003/2005.

Base of certification is the report SEBS-A.150643/15TB in the valid version.
This certificate entitles the holder to use the pictured safety approved mark.

Valid until: 2020-05-27
File reference: 8112336271

Hamburg, 2015-05-28

B. Pfuff

Bianca Pfuff

Voluntary Certification
TÜV NORD
TÜV NORD Systems GmbH & Co. KG
Safety Approved
FEx 300/500
IEC/DIN EN 61508-1/-2: 2010/2011
capable up to SIL 2
SEBS-A.150643/15

Certification Body SEECERT
TÜV NORD Systems GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg, Germany

ABB Limited
Measurement & Analytics
Howard Road, St. Neots
Cambridgeshire, PE19 8EU
UK
Tel: +44 (0)870 600 6122
Fax: +44 (0)1480 213 339
Email: enquiries.mp.uk@gb.abb.com

ABB Inc.
Measurement & Analytics
125 E. County Line Road
Warminster, PA 18974
USA
Tel: +1 215 674 6000
Fax: +1 215 674 7183

ABB Engineering (Shanghai) Ltd.
Measurement & Analytics
No. 4528, Kangxin Highway, Pudong
New District
Shanghai, 201319,
P.R. China
Tel: +86(0) 21 6105 6666
Fax: +86(0) 21 6105 6677
Email: china.instrumentation@cn.abb.com

abb.com/flow

3KXF231304R4801

SM/FEX300/FEX500/SIL-EN Rev. D 05.2019