Functional Safety Manual for Ultrasonic Flowmeters

FLUXUS

FSFLUXUS_V2-3-7EN

Relevant Safety Aspects:

Constant monitoring of min. and max. of volumetric flow rate and mass flow rate

Continuous self-diagnostic

Output via current output 4...20 mA

FLEXIM GmbH
Boxberger Straße 4
12681 Berlin
Germany

Tel.: +49 (30) 936 67 660
Fax: +49 (30) 936 67 680
E-mail: info@flexim.com
www.flexim.com

User Manual on Functional Safety
FLUXUS
FSFLUXUS_V2-3-7EN, 2023-01-01

Table of contents

1 Introduction

1.1 Regarding this manual on functional safety

This FLUXUS flowmeter user manual on functional safety has been written to facilitate the operator:

- to interpret the safety functions for SIL 1 or SIL 2
- to integrate the transmitter in the installation
- to operate the PCS safety function.

1.2 Applicable standards

This manual on functional safety contains information according to IEC 61508 ("Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems") and IEC 61511 ("Functional Safety - Safety Instrumented Systems for the Process Industry Sector"). It does not include information about explosion protection.

1.3 Applicable documents

In addition to the manual on functional safety the information of the following documents are important:

- UMFLUXUS: User's Manual FLUXUS flowmeter
- SIFLUXUS: Safety instructions for the use of the FLUXUS flowmeter in explosive atmospheres
- TSFLUXUS: Technical specification of the FLUXUS flowmeter

1.4 Terms and abbreviations

In this manual on functional safety the following terms and abbreviations are used:

Tab. 1.1: Terms and Abbreviations

term/abbreviation	english term	description
SIL	safety integrity level	Safety Integrity Level: one of four stages which corresponds to a value range of the safety integrity. Within safety integrity SIL 4 corresponds to the highest and SIL 1 to the lowest stage.
EUC	equipment under control	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.
Safety-Related System	safety-related system	A system that • executes the necessary safety functions, which are essential to achieve and maintain a safe sate for the EUC • is intended to achieve, on its own or with other safety-related E/E/PE-systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety function
mode of operation	mode of operation • low demand mode • high demand mode • continuous mode	Type of use of a safety function • Operating mode with low demand rate: the safety function is performed on request only to transfer the EUC to a determined safe state. The frequency of the demand rate is less than or equal to once a year. • Operating mode with high demand rate: the safety function is performed on request only to transfer the EUC to a determined safe state. The frequency of the demand rate is greater than once a year. • Operating mode with continuous demand rate: the safety function retains the EUC within its normal safe state.
MTBF	mean time between failures	Mean Time between Failures
MTTF	mean time to failure	Mean Time to Failure

Tab. 1.1: Terms and Abbreviations

term/abbreviation	english term	description
MTTR	mean time to restoration	Mean Time to Restoration consisting of: • time of detecting an incident • time to start repairing • the actual time of the repair • time of restoring the service of the repaired component

2 Description of the measuring system

The FLUXUS flowmeter satisfies the systematic capability and required characteristics according to SIL 2 and is therefore suitable to interpret Safety Instrumented Systems.

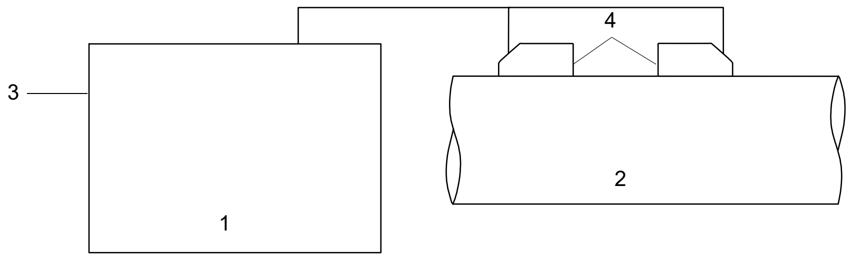
For the ultrasonic measurement of the flow rate, the flow velocity of the fluid in a pipe is determined. Further physical quantities (e.g., volumetric flow rate, mass flow rate) are derived from the flow velocity.

2.1 Measuring setup

The measuring setup consists of a transmitter with a current output (4…20 mA), the ultrasonic transducers (shear wave or Lamb wave) as well as the transducer cables and the pipe on which the measurement is conducted.

The ultrasonic transducers are mounted on the outside of the pipe. Ultrasonic signals are sent through the fluid and received by the transducers. The transmitter controls the measuring cycle, eliminates the disturbance signals and analyzes the useful signals. The measured values can be displayed, used for calculations and transmitted by the current output.

Fig. 2.1: Measuring setup



1 – transmitter
2 – pipe
3 – current output
4 – transducers

2.2 Measurement principle

The flow velocity of the fluid is measured using the ultrasonic-transit time difference correlation principle (see section 2.2.1).

The volumetric flow rate is calculated by multiplying the flow velocity by the cross-sectional pipe area:

$$\dot{V} = v \cdot A$$

The mass flow rate is calculated by multiplying the volumetric flow rate and the density of the fluid:

$$\dot{m} = \dot{V} \cdot \rho$$

2.2.1 Measurement of the flow velocity

The signals are emitted and received by two transducers alternatively in and against the flow direction. If the fluid moves, the signals propagating in the fluid are displaced with the flow. This displacement causes a reduction in distance for the signal in the flow direction and an increase in distance for the signal against the flow direction in the section of the receiving transducer (see Fig. 2.2 and Fig. 2.3). This causes a change in the transit times. The transit time of the signal in the flow direction is shorter than the transit time against the flow direction. This transit time difference is proportional to the average flow velocity.

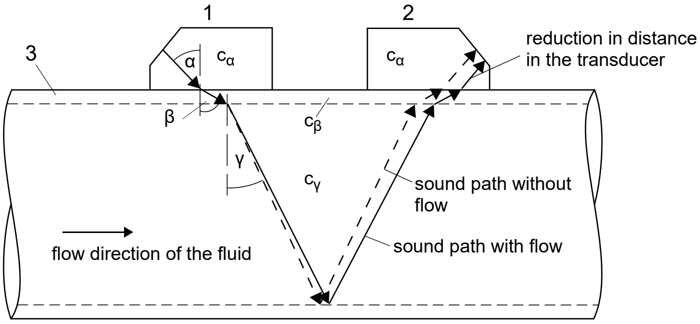
The average flow velocity of the fluid is calculated as follows:

$$v = k_{Re} \cdot k_a \cdot \frac{\Delta t}{2 \cdot t_\gamma}$$

with

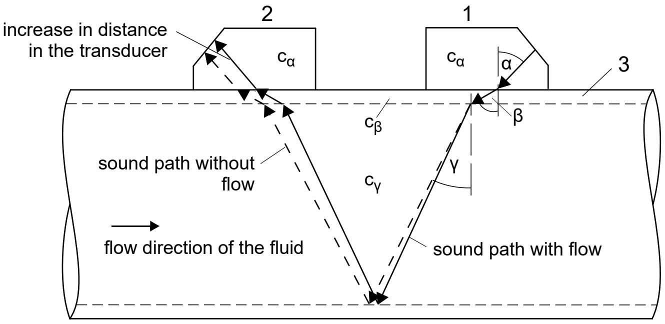
v – flow velocity of the fluid
k_{Re} – fluid mechanics correction factor
k_a – acoustic calibration factor
Δt – transit time difference
t_γ – transit time in the fluid

Fig. 2.2: Sound path of the signal in the flow direction



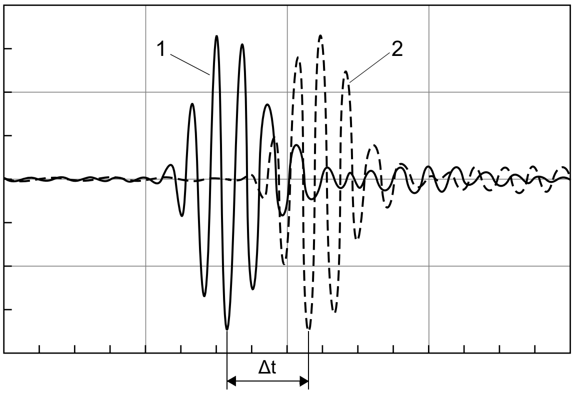
c – sound speed
1 – transducer (emitter)
2 – transducer (receiver)
3 – pipe wall

Fig. 2.3: Sound path of the signal against the flow direction



c – sound speed
1 – transducer (emitter)
2 – transducer (receiver)
3 – pipe wall

Fig. 2.4: Transit time difference Δt



1 – signal in the flow direction
2 – signal against the flow direction

2.3 Accuracy

The measurement error at flow measurement in standard calibration and known flow profile is ±1.6 % of the measured value ±0.01 m/s. In addition to the application specific measurement error a further safety-oriented accuracy of ±2 % of the max. measurement range has to be added.

For information about necessary conditions to achieve measurement accuracy see Technical Specification TSFLUXUS. An appropriate measuring point has to be selected according to the instruction of the user manual UMFLUXUS, chapter "Selection of the Measuring Point".

2.4 Instructions of installation

The FLUXUS flowmeter can only be installed and handled by qualified personnel considering the documentation of the respective task, especially the safety and warning notes. Due to the training and experience, qualified personnel is able to identify risks and avoid potential dangers using the FLUXUS flowmeter (see user manual UMFLUXUS).

If any problem appears which cannot be solved with the help of this user manual, contact our sales office and give a precise description of the problem. Specify the type, the serial number and the firmware version of the transmitter.

Any kind of device repairs are to be carried out by the manufacture exclusively.

2.5 Software version

The FLUXUS flowmeter is equipped with the software version: 6.14.

2.6 Hardware version

The FLUXUS flowmeter is equipped with the following hardware components:

704SR-** & *705SR-*

components	revision of the circuit diagram	revision of the parts list
FBM8	3.13	4.00
AP42	1.40	1.63
DSA3 (Doppelstromschleife)	1.0	1.10

800SR-**, *801SR-** & *808SR-*

components	revision of the circuit diagram	revision of the parts list
Apx2	1.3	1.41
Ufp2	1.2	1.2
Yxm3	2.10	2.10
Pwx3	1.0	1.03
KSX1	1.0	1.0
KOX1	1.0	1.0
Bfx1	1.0	1.1
Blo2	1.10	1.10
PWX5	1.3	1.3

2.7 Device overview

The FLUXUS flowmeter is available in the following hardware versions:

*704SR-**
*705SR-**
*800SR-**
*801SR-**
*808SR-**

[SR] Special Safety Requirements

[*] Fluid

[F] Fluid

[G] Gas

[**] Explosion protection designation

[NN] without explosion proof protection

[A] Atex

[F] FM

[E] EAC TRTS, formerly GOST

Model codes

F70x	G70x	F80x	G80x
F704SR-NN	G704SR-NN	F800SR-A1	G800SR-A1
F704SR-A2	G704SR-A2	F800SR-E1	G800SR-E1
F704SR-F2	G704SR-F2	F801SR-A1	G801SR-A1
F704SR-E2	G704SR-E2	F801SR-E1	G801SR-E1
F705SR-NN	G705SR-NN	F808SR-A1	
F705SR-A2	G705SR-A2	F808SR-F1	
F705SR-F2	G705SR-F2	F808SR-E1	
F705SR-E2	G705SR-E2		

2.8 Environmental conditions

Concerning allowed environmental conditions of the FLUXUS flowmeter see Technical Specification TSFLUXUS.

2.9 Set-up the safety function

The FLUXUS flowmeter is a device of type B with Hardware Fault Tolerance (HFT) 0.

The FLUXUS flowmeter measures the volumetric flow rate or mass flow rate and generates a proportional signal (4…20 mA) which is transmitted by the current output of the flowmeter. The safety function refers to the output signal.

In order to configure the safety function properly, the error values for the analog output need to be configured according to NAMUR NE 43. This means setting the output's Error-value via the "other value" setting as described in the "User's Manual UMFLUXUS" (either < 3.6 mA, or > 21 mA). This allows the PLC to monitor and detect any detected faults in the flowmeter.

The output signal is emitted to a connected logic unit which monitors that the signal does not exceed the max. or goes below the min. limit of the volumetric flow rate or mass flow rate.

If the threshold value defined by the user is reached, the state is considered safe.

If a valid safe current output deviates more than the determined safety-oriented range of precision of the correct process value, the state is considered dangerous.

A fail high failure (H) is defined as a failure that causes the output signal to go to the max. alarm output current (> 21 mA). A fail low failure (L) is defined as a failure that causes the output signal to go to the min. alarm output current (< 3.6 mA).

2.10 Safe parameterization

The FLUXUS flowmeter offers the possibility to enter application specific parameters to optimize measurement results or for experimental purposes. These settings are enabled in the SuperUser mode. (see user manual UMFLUXUS)

Parameterization via HART is not possible.

Configuration steps for a safety-related configuration:

• Configuration of different process relevant parameters via the display

• Visual control of the entered parameters

• Start measurement

• Restart FLUXUS

• After the restart further visual parameter check on the display

• Read out configuration via serial interface and check parameter on the computer

The FLUXUS flowmeter is equipped with a program code which enables password protected measurements to prevent accidental operation.

If a program code has been defined, it will be requested when there is an intervention in the measurement (a command or key BRK).
If a program code is active, the message Program code active will be displayed for a few seconds when a key is pressed.
To execute a command, it is sufficient to enter the first three digits of the program code (= access code).
To stop an ongoing measurement, the complete program code has to be entered (= break code).
The input of a program code is interrupted by pressing key C.

• A program code will remain valid as long as:

• no other valid program code is entered or

• the program code is not deactivated.

2.11 Useful lifetime

The determined failure rates are valid within the useful lifetime of the FLUXUS flowmeter. The probability of a failure increases significantly after expiration the useful lifetime.

According to IEC 61508-2, section 7.4.9.5, the useful life is based on field experience, though experience has shown the useful life often lies within a range of 8 to 12 years. FLEXIm recommends not to exceed the useful lifetime of safety-related applications of 10 years. If the FLUXUS flowmeter is supervised throughout its entire lifetime and mantains the same behavior (e.g. constant failure rates), the operatinf lifetime can be extended on one's own responsibility.

For recommendation regarding Proof tests see chapter 3.

3 Proof test

3.1 Required actions

According to IEC 61508 the safety function has to be checked in appropriate intervals within the scope of proof tests. Proof tests can detect hidden and dangerous failures in a safety-related system, so that the system, if necessary, can be brought into a "like-new" state or as close as possible to this state by repair.

The operator is responsible to define type and interval of the proof tests appropriately. In Tab. 3.1 a proposal to test the safety function is described. Realizing the test a coverage rate of 85 % can be reached.

Tab. 3.1: Suggestion to test the safety function

step	description
1	Override the safety function to avoid an accidental activation of the alarm.
2	If necessary, execute a two-point calibration of the flowmeter. Compare the measured values of the FLUXUS flowmeter with the measured values of the reference measuring device.
3	Perform a functional test of the current output with high alarm value. Check if the output signal reaches this value (see user manual UMFLUXUS, chapter, "Outputs").
4	Perform a functional test of the current output with low alarm value. Check if the output signal reaches this value (see user manual UMFLUXUS, chapter, "Outputs").
5	Perform a functional test of the current output with the error value. Check if the output signal reaches this value (see user manual UMFLUXUS, chapter, "Outputs").
6	Restore the complete functionality of the current output.
7	Remove the override of the safety functions to restore the normal operation.

3.2 Additional actions during the proof test

The following additional actions serve to ensure a safe and exact flow measurement.

3.2.1 Visual inspection of the measurement system

Carry out a visual inspection of the measuring instrument. Look for the following signs of wearout or damage which can negatively influence the measurement:

- obvious external damage
- corrosion
- loose parts
- skewed arrangement of the transducer mounting fixtures (in relation to the pipe axis)
- open housings

3.2.2 Inspection of the wiring

In order to ensure correct wiring of the measuring instrument, check the following:

- all cables and terminals (transducers, outputs, power supply)
- shielding and cathodic corrosion protection, if present
- earth/ground
- cable glands

3.2.3 Inspection of the transducers

In order to ensure correct mounting of the transducers, check the following:

- coupling between the contact surface of the transducers and the pipe surface
- contact pressure of the transducers on the pipe
- secure fastening of the transducer mounting fixtures to the pipe
- correct orientation of the transducers
- sufficient length of the inlet and outlet pipe section

3.2.4 Verification of the diagnostic values

Notice!

For the verification of diagnostic values, it is necessary to interrupt the measurement and exit the normal operation mode. Inform the responsible person.

Notice!

It is recommended to activate the storing of diagnostic values. The stored diagnostic values can be read out using the serial data kit and the FLEXIM software FluxData. During the read out the stored diagnostic values, the measurement is interrupted and the last measured value is displayed via the current output.

For the storing of diagnostic values see user manual UMFLUXUS, chapter "Data Logger".

Activate the SuperUser-Mode. To activate the SuperUser-Mode see user manual UMFLUXUS, chapter "SuperUser-Mode".

Displaying diagnostic values see user manual UMFLUXUS. chapter "Basic Measurement".

The following table shows diagnostic values enabling conclusions about quality and accuracy of a measurement. Some of these diagnostic values can have global limits. These limits indicate in which range the respective diagnostic value for an exact measurement should be located.

display	diagnostic value	description	limits
`c`	speed of Sound	The speed of sound is calculated from the transit time of sound and the path length in the fluid. The transit time in the fluid is calculated by subtracting the transit time in the transducer and the pipe wall from the total transit time. The path length is calculated from the outer pipe diameter, wall thickness, transducer distance and transducer constant. If the theoretic speed of sound of the fluid is known, the measured sound speed can be compared with the theoretic value. Due to the high temperature dependence of speed of sound the temperature must be known as well.	depending on the fluid
`S`	signal amplitude	The signal amplitude particularly depends on the signal attenuation, the transducer frequency, the sound path length, the pipe wall material as well as the pipe lining (inside and outside) and last but not least the quality of the transducer coupling. It can vary in a great range. The accuracy of the measurement does not depend on the signal amplitude as long as the signal is strong enough to be detected. The signal amplitude, however, should remain constant throughout the measurement if the measurement conditions do not change.	
`Gain`	gain	The actual gain is calculated from the max. gain and the actual signal amplitude.	max. 107 dB (shear wave transducers) or max. 113 dB (Lamb wave transducers)
`SNR`	SNR	The SNR (signal-to-noise ratio) is the ratio of the power of useful signal to the power of random noise. Such noise can be provoked by electronic and acoustic disturbance sources. The influence of electronic disturbance sources is minimized by careful shielding and grounding. A low SNR can refer to those errors.	min. 15 dB
`SCNR`	SCNR	The SCNR (signal-to-correlated-noise ratio) is defined to SNR. Here, however, the random noise is not captured but noises which are correlated with the measuring signal. The signal fractions created by the sensor reach the receiving transducer through the fluid by other means, e.g. via pipe wall along the pipe circumference or in axial direction as well as after reflecting at the next flange.	min. 20 dB

Compare the actual diagnostic values with the diagnostic values from the start-up and the last proof test of the FLUXUS flowmeter. If the diagnostic values deviate significantly from the recommended or previously obtained values, please contact FLEXIM.

3.2.5 Verification of the outputs

Verify the measured values displayed in the control room. It is also possible to verify the signal of the analog outputs manually using a multimeter (see user manual UMFLUXUS, chapter "Outputs").

Notice!
During the verification of the outputs, the measurement will be interrupted and the outputs will have no signal. Inform the responsible person.

4 Functional safety parameters

The versions of the FLUXUS flowmeter mentioned in chapter 2.6 were submitted to a Failure Mode, Effects, and Diagnostic Analysis (FMEDA) by exida.

4.1 Failure categories

When assessing the FLUXUS flowmeter failure behavior the following failure categories were regarded:

Tab. 4.1: Failure categories

failure category	english denomination	description
(S)	safe failure	The failure of an element and/or subsystem and/or system, which takes part in the execution of the safety function and which • causes a faulty activation of the safety function, to bring the EUC (or parts thereof) in a safe state or to maintain a safe state • increases the probability of an erroneous activation of the safety function, to bring the EUC (or parts thereof) in a safe state or to maintain a safe state.
(SU)	safe undetected failure	A safe failure which, in relation to hardware, remains undetected by diagnostic tests, proof tests, operator intervention (e.g., inspection, manual tests) or during the normal operation
(SD)	safe detected failure	A safe failure which, in relation to hardware, is detected by diagnostic tests, proof tests, operator intervention (e.g., inspection, manual tests) or during the normal operation
(D)	dangerous failure	The failure of an element and/or subsystem and/or system, which takes part in the execution of the safety function and which • prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode), such that the EUC is put into a hazardous or potentially hazardous state or • decreases the probability that the safety function operates correctly when required
(DU)	dangerous undetected failure	A dangerous failure which, in relation to hardware, remains undetected by diagnostic tests, proof tests, operator intervention (e.g., inspection, manual tests) or during the normal operation
(DD)	dangerous detected failure	A dangerous failure which, in relation to hardware, is detected by diagnostic tests, proof tests, operator intervention (e.g., inspection, manual tests) or during the normal operation

4.2 Assumptions

- The FLUXUS flowmeter is a device of type B with Hardware Fault Tolerance (HFT) 0.
- The FLUXUS flowmeter is operated in low demand mode of operation.
- All failure rates are constant. Wear out mechanisms are not considered.
- The failure propagation is not relevant.
- Failures during parameterization of the measurement are not considered.
- The FLUXUS flowmeter and the transducers are installed according to the instructions of the user manual UMFLUXUS.
- The FLUXUS flowmeter is protected against unintended operation.
- In a worst-case scenario the internal fault detection time is 30 s.
- Failures rates of external power supplies are not taken into account.
- The Mean Time to Restoration (MTTR) after a safe failure is 24 h.
- The HART protocol is only used for configuration, calibration and diagnostic and not during the normal operation.
- For safety applications only the described versions of the FLUXUS flowmeter in this functional safety manual are considered.
- The output signal 4...20 mA is transferred to a PLC-system which must fulfill the requirements of at least SIL 1.
- The application of the logic unit is configured according to the standard NAMUR NE 43 and detects over-range and under-range failures, hence, it does not automatically trigger an alarm at a failure. These failures are assigned to the category of "dangerous detected".

4.3 Methods

Notice!

For the calculation of the parameters on functional safety the methods of exida were applied. These methods are state of the art and can differ from the described methods of IEC 61508.

For the calculation of the Safe Failure Fraction (SFF) the following methods were applied:

- The total failure rate λ_{total} is the sum of each failure rate:
  $\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$
- The Safe Failure Fraction results from:
  $SFF = 1 - \lambda_{DU}/\lambda_{total}$
- The diagnostic coverage of a Dangerous Failure (DCD) results from:
  $D_{CD} = \lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$
- The Mean Time Between Failure (MTBF) results from:
  MTBF = MTTF + MTTR

4.4 Results

The abstract of the results are given in the FMEDA documents.

- FLEXIM ADM 7407 13-09-094 R002 V1R3
- FLEXIM FLUXUS ADM 8x27 - F-G80x 12-06-034 R001 V1R1