Safety Manual

VEGAMET 391

4 … 20 mA controller

With SIL qualification

Document ID: 40888

Contents

Editing status: 2022-07-05

40888-EN-220705

1 Document language

DE	Das vorliegende *Safety Manual* für Funktionale Sicherheit ist verfügbar in den Sprachen Deutsch, Englisch, Französisch und Russisch.
EN	The current *Safety Manual* for Functional Safety is available in German, English, French and Russian language.
FR	Le présent *Safety Manual* de sécurité fonctionnelle est disponible dans les langues suivantes: allemand, anglais, français et russe.
RU	Данное руководство по функциональной безопасности *Safety Manual* имеется на немецком, английском, французском и русском языках.

2 Scope

2.1 Instrument version

This safety manual applies to the controller **VEGAMET 391 with SIL qualification**

Valid version:

- from hardware version 1.0.0
- from software version 1.0.0

2.2 Application area

The controller can be used in combination with a 4 … 20 mA transmitter for measurement of level, limit level and other process variables as measuring system in a safety-relevant protective function according to IEC 61508 in the modes *low demand mode* and *high demand mode*:

Due to the systematic capability SC2 this is possible up to:

- SIL2 in single-channel architecture
- SIL3 in a multiple-channel architecture only with diversitary redundancy

The following interfaces can be used:

- Sensor input: 4 … 20 mA with transmitter power supply
- Relay output: Relay 3 and 4, NO contact [1]
- Current output: 4 … 20 mA

SIL

Not permissible for safety-relevant applications:

- Digital inputs 1 and 2
- Relay outputs 1 and 2
- Existing communication interfaces (e.g. HART, USB)

2.3 SIL conformity

The SIL conformity was independently judged and certified by *exida* Certification LLC according to IEC 61508. [2]

[1] NO = Normal Open
[2] Verification documents see "appendix"

40888-EN-220705

3 Planning

3.1 Safety function

The transmitter powered by the controller generates a signal between 3.8 and 20.5 mA which is proportional to the process variable.

Safety function relay output
Dependent on this analogue signal and the adjusted switching points, one or two relays for limit value monitoring will be switched.

Safety function current output
This analogue signal can be also fed to a connected processing unit (e.g. safety-oriented PLC). The set switching points can be used for limit value monitoring.

Safety tolerance

If the internal diagnostics system detects a measured value falsification of more than 2% caused by a hardware error, the output signals are set to "Failure".

This must be taken into account for the interpretation of the safety function.

3.2 Safe state

Safe state relay output
The safe state on the relay output is when the closing contact is open. That's why only the closing contact (NO contact) may be used for the safety function (idle current principle).

Safe state, current output
The safe state of the current output depends on the mode and the characteristics set in the sensor.

	Monitoring upper limit value	**Monitoring lower limit value**
Rising characteristics: 4 mA = 0 %; 20 mA = 100 %	Output current > Switching point -334 µA	Output current < Switching point +334 µA
Falling characteristics: 20 mA = 0 % 4 mA = 100 %	Output current < Switching point +334 µA	Output current > Switching point -334 µA

Output signals in failure mode

Relay output
- Closing contact is open

Current output
- "fail low" ≤ 3.6 mA
- "fail high" > 21 mA

3.3 Prerequisites for operation

Instructions and restrictions

- The measuring system should suit the application. The application-specific limits must be maintained
- The specifications according to the operating instructions manual, particularly the current load on the output circuits, must be kept within the specified limits
- To avoid a fusing of the relay contacts, these must be protected by an external fuse that triggers at 60 % of the max. contact current load.
- Existing communication interfaces (e. g. HART, USB) are not used for transmission of the safety-relevant measured value
- The instructions in chapter " *Safety-related characteristics*", paragraph " *Supplementary information*" must be noted
- All parts of the measuring chain must correspond to the planned " *Safety Integrity Level (SIL)*"

4 Safety-related characteristics

4.1 General figures for all applications

Parameter according to IEC 61508	**Value**
Safety Integrity Level	SIL2
Hardware fault tolerance	HFT = 0
Instrument type	Type B
Mode	Low demand mode/High demand mode
MTTR	8 h
MTBF = MTTF + MTTR [3]	0.38 x 10^6 h (44 years)
Diagnostic test interval [4]	< 4 min
Demand mode	> 50 h

4.2 Specific figures for application 1

One relay output

One relay for control of an actor for monitoring a limit value (e.g. overfill or dry run protection)

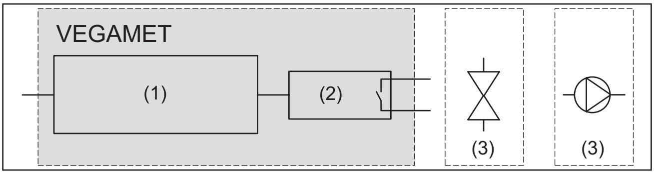

Fig. 1: Structure of application

1 Current input and processing electronics
2 Relay 3 or relay 4
3 Actor

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0 FIT	716 FIT	0 FIT	24 FIT	96 %	94 %

PFD_{AVG}	0.0254 x 10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.0342 x 10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.0604 x 10^{-2}	(T1 = 5 years)
PFH	0.0238 x 10^{-6} 1/h	

4.3 Specific figures for application 2

Two relay outputs

Two relays for control of two actors for monitoring two limit values (e.g. range monitoring).

[3] MTBF: Including errors outside the safety function
[4] Time during which all internal diagnoses are carried out at least once.

40888-EN-220705

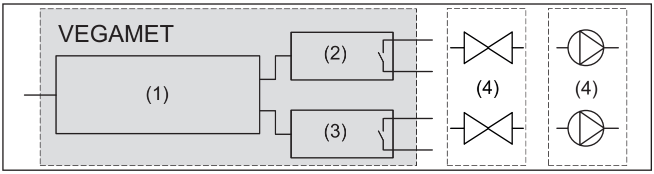

Fig. 2: Structure of application

1. *Current input and processing electronics*
2. *Relay 3*
3. *Relay 4*
4. *Actors*

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0 FIT	758 FIT	0 FIT	25 FIT	96 %	94 %

PFD_{AVG}	0.0271×10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.0364×10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.0643×10^{-2}	(T1 = 5 years)
PFH	0.0253×10^{-6} 1/h	

4.4 Specific figures for application 3

Current output

One current output for control of a connected processing unit (e.g. a SPLC).

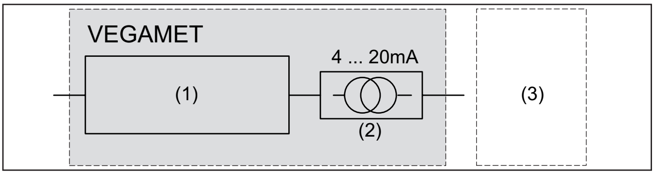

Fig. 3: Structure of application

1. *Current input and processing electronics*
2. *Current output*
3. *Connected processing unit*

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0 FIT	0 FIT	860 FIT	23 FIT	97 %	97 %

PFD_{AVG}	0.0276×10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.0357×10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.0599×10^{-2}	(T1 = 5 years)
PFH	0.0227×10^{-6} 1/h	

40888-EN-220705

4.5 Characteristics acc. to ISO 13849-1

Derived from the safety-related characteristics, the following figures result according to ISO 13849-1 machine safety): [5)]

Parameter according to ISO 13849-1	Value for application 1	Value for application 2	Value for application 3
$MTTF_d$	243 years	236 years	129 years
DC	94 %	94 %	97 %
Performance Level	4.68×10^{-7} 1/h	4.83×10^{-7} 1/h	8.83×10^{-7} 1/h

4.6 Supplementary information

Determination of the failure rates

The failure rates of the instruments were determined by an FMEDA according to IEC 61508. The calculations are based on failure rates of the components according to **exida Profile 1** with the following data:

Profile according to IEC 60654-1	B2
Ambient Temperature (Average, external)	30 °C
Ambient Temperature (Mean, in Box)	60 °C
Temperature Cycle	5 °C/365 days

Assumptions of the FMEDA

- The failure rates are constant. Take note of the useful service life of the components according to IEC 61508-2.
- Multiple failures are not taken into account
- Wear on mechanical parts is not taken into account
- Failure rates of external power supplies are not taken into account
- The environmental conditions correspond to an average industrial environment
- To avoid a fusing of the relay contacts, these must be protected by an external fuse

Calculation of PFD_{AVG}

The values for PFD_{AVG} specified above were calculated as follows for a 1oo1 architecture:

$$PFD_{AVG} = \frac{PTC \times \lambda_{DU} \times T1}{2} + \lambda_{DD} \times MTTR + \frac{(1 - PTC) \times \lambda_{DU} \times LT}{2}$$

Parameters used:

- T1 = Proof Test Interval
- PTC (Applikation 1 & 2) = 84 %
- PTC (Applikation 3) = 81 %
- LT = 10 years
- MTTR = 8 h

Boundary conditions relating to transmitters

The transmitter used, must output an error current if it is powered by a voltage outside its voltage range.

5) ISO 13849-1 was not part of the certification of the instrument.

Boundary conditions relating to the configuration of the processing unit

A connected control and processing unit must have the following properties:

- The failure signals of the measuring system are judged according to the idle current principle
- " *fail low*" and " *fail high*" signals are interpreted as a failure, whereupon the safe state must be taken on

If this is not the case, the respective percentages of the failure rates must be assigned to the dangerous failures and the values stated in chapter *Safety-related characteristics*“ redetermined!

Multiple channel architecture

In multiple channel systems for SIL3 applications, this measuring system must only be used with diversitary redundancy.

The safety-related characteristics must be calculated especially for the selected structure of the measuring chain using the stated failure rates. In doing this, a suitable Common Cause Factor (CCF) must be considered (see IEC 61508-6, appendix D).

5 Setup

5.1 Instrument parameter adjustment

Tools

The following adjustment units are permitted for parameterization of the safety function:

- The integrated display and adjustment unit for on-site adjustment
- The DTM suitable for VEGAMET 391 in conjunction with an adjustment software according to the FDT/DTM standard, e. g. PACTware
- Keep in mind that DTM Collection 06/2011 or a newer version is required.

The parameter adjustment is described in the operating instructions manual.

SIL The change of safety-relevant parameters is only possible with active connection to the instrument (online mode)

Safety-relevant parameters

To prevent unintentional or unauthorized adjustment, the set parameters must be protected from unauthorized access. For this reason the instrument is shipped in locked condition. The PIN in delivery status is "0000".

The instrument is shipped with an overview listing all safety-relevant parameters and their value in delivery status. By means of the serial number, this list is also available as a download via " www.vega.com", " *Search*".

Safe parameterization

To avoid or detect possible errors during parameter adjustment for unsafe operating environments, a verification procedure is used that allows the safety-relevant parameters to be checked.

Parameter adjustment proceeds according to the following steps:

- Unlock adjustment
- Change parameters
- Lock adjustment and verify modified parameters

The exact process is described in the operating instructions.

With the adjustment software, the current safety-relevant parameters can be printed or stored. This function, however, is only possible with active connection of the instrument to the adjustment software (online mode).

SIL The instrument is shipped in locked condition!

SIL For verification, only the modified, safety-relevant parameters are shown. The verification texts are displayed either in German or, when any other menu language is used, in English.

Unsafe device status

Warning:
When the instrument is unlocked, the safety function must be considered as unreliable. This applies until the parameter adjustment is finished.

If necessary, you must take other measures to maintain the safety function.

Incomplete process of the parameter adjustment

Warning:
If the described process was not carried out completely or correctly (e.g. interruption or voltage loss), the instrument remains in unsafe and unlocked instrument status.

Instrument reset

Warning:
In case of a reset to basic settings, all safety-relevant parameters will be reset to default values. Then all safety-relevant parameters must be checked or set anew.

5.2 Mounting and installation

Take note of the mounting and installation instructions in the operating instructions manual.

During setup, it is recommended to check the safety function, e.g. by means of a first filling or simulation of the input signal. The procedure described in chapter " *Recurring function test*" can be used.

6 Reaction during operation and in case of failure

6.1 General information

Device behaviour during operation or in case of malfunction as well as the respective fault signal are described in the operating instructions manual.

The manufacturer must be informed of the occurrence of a dangerous undetected failure (incl. fault description).

6.2 Behaviour in case of failure

Internal diagnosis

The instrument is permanently monitored by an internal diagnostic system. If a malfunction is detected, the respective output signals change to the safe status (see section " *Safe status*").

This conditions is kept for at least 5 seconds. If no error is detection, then the safety function is again carried out correctly.

The diagnosis interval is specified in chapter " *Safety-related characteristics*".

Fault reaction time safety-relevant fault signals

Dependent on the fault, a respective fault signal is triggered with the following reaction time:

Fault signal during operation	**Reaction time**
E012 Hardware error, sensor input	< 1 min
E014 Short circuit sensor input	< 5 s
E015 Line break sensor input	< 5 s
E034 EEPROM-CRC error	< 2 s
E035 Program memory CRC error	< 1 min
E037 RAM defective	< 4 min
E040 Hardware defective	< 4 min
E080 Microcontroller defective	< 4 min
E113 Hardware error, current output	< 1 min
E117 Pump signals failure	Parametrizable
E125 Instrument electronics temperature	1 h

Fault signal during parameter adjustment	**Reaction time**
E017 Adjustment span too low	< 5 s
E021 Scaling span too small	< 5 s
E062 Pulse priority too small	< 5 s
E110 Relay switching points: Span too small	< 5 s
E111 Relay switching points interchanged	< 5 s
E115 Behaviour in case of failure wrong	< 5 s
E116 Output mode faulty	< 5 s

7 Recurring function test

7.1 General information

The recurring function test (*Proof Test*) serves to test the safety function and to identify possible undetected, dangerous failures. The functional capability of the measuring system has to be tested in adequate time intervals. It is the user's responsibility to choose the type of testing. The time intervals are subject to the PFD_{AVG} in chapter " *Safety-relevant characteristics*".

With high demand rate, a recurring function test is not requested in IEC 61508. The functional efficiency of the measuring system is demonstrated by the frequent use of the system. In double channel architectures it is a good idea to verify the effect of the redundancy through recurring function tests at appropriate intervals.

For documentation of these function tests, the test protocol in the appendix can be used.

If the function test proves negative, the entire measuring system must be switched out of service and the process held in a safe state by means of other measures.

In a multiple channel architecture this applies separately to each channel.

Tools

- Suitable calibrated ammeter (accuracy better than ±0.1 mA)
- Suitable calibrated resistance measuring instrument
- If necessary, simulator for sensor current (passive current source)

Preparation

- Determine safety function (mode, switching points)
- If necessary, remove the instruments from the safety chain and maintain the safety function by other means

Unsafe device status

⚠ **Warning:**
During the function test, the safety function must be treated as unreliable. Take into account that the function test influences downstream connected devices.

If necessary, you must take other measures to maintain the safety function.

After the function test, the status specified for the safety function must be restored.

7.2 Test application 1 - One relay output

Procedure for mode overfill protection

1. Adjust the sensor current below the lower relay switching point "Lo"
2. Adjust the sensor current directly above the upper relay switching point "Hi"

Procedure for mode dry run protection

1. Adjust the sensor current above the upper relay switching point "Hi"
2. Set the sensor current directly below the lower relay switching point "Lo"

40888-EN-220705

Expected result

The implemented SIL relay contact must be closed at point 1 and open at point 2 within the safety tolerance (+334 µA).

Proof Test Coverage

PTC = 84 %

7.3 Test application 2 - Two relay outputs for range monitoring

Procedure

1. Adjust at least three values of the sensor current within the range limits
2. Adjust the sensor current directly above the upper relay switching point "Hi" for the upper range limit
3. Set the sensor current directly below the lower relay switching point "Lo" for the lower range limit

Expected result

Point 1: Both SIL relay contacts must be closed.

Point 2: The SIL relay contact for monitoring the upper range limit must be opened within the safety tolerance (+334 µA).

Point 3: The SIL relay contact for monitoring the lower range limit must be opened within the safety tolerance (+334 µA).

Proof Test Coverage

PTC = 84 %

7.4 Test application 3 - Current output

Procedure

Set at least five values of the sensor current within the measuring range.

Expected result

All measured current output values deviate by less than 2 % (+334 µA) from the expected output current.

Proof Test Coverage

PTC = 81 %

8 Supplement A: Test protocol function test

Identification	
Company/Tester	
Plant/Instrument TAG	
Meas. loop TAG	
Instrument type/Order code	
Instrument serial number	
Date, setup	
Date, last function test	

Adjusted device parameters of the safety function		
Used safety-relevant outputs	**O** Relay 3 **O** Relay 4 **O** Current output	
Adjusted mode, relay 3	**O** Overfill protection **O** Dry run protection	
Adjusted upper switching point relay 3 "Hi"	mA	
Adjusted lower switching point relay 3 "Lo"	mA	
Set mode, relay 4	**O** Overfill protection **O** Dry run protection	
Adjusted upper switching point relay 4 "Hi"	mA	
Adjusted lower switching point relay 4 "Lo"	mA	

Test result 1 **Relay outputs**

	Relay output 3			**Relay output 4**		
Switching point	**Measured sensor current**	**Condition Relay 3**	**Test result**	**Measured sensor current**	**Condition Relay 4**	**Test result**
"Hi“	mA			mA		
"Hi“	mA			mA		
"Hi“	mA			mA		
"Lo"	mA			mA		
"Lo"	mA			mA		
"Lo"	mA			mA		

Test result 2 **Current output**

Simulated sensor current		**Expected Output current**	**Measured Output current**	**Test result**
Sensor current 1	mA	mA	mA	
Sensor current 2	mA	mA	mA	
Sensor current 3	mA	mA	mA	

40888-EN-220705

Simulated sensor current		Expected Output current	Measured Output current	Test result
Sensor current 4	mA	mA	mA	
Sensor current 5	mA	mA	mA	

Confirmation

Date: Signature:

9 Appendix B: Term definitions

Abbreviations

SIL	Safety Integrity Level (SIL1, SIL2, SIL3, SIL4)
SC	Systematic Capability (SC1, SC2, SC3, SC4)
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{AVG}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of a dangerous failure per hour (Ed.2)
FMEDA	Failure Mode, Effects and Diagnostics Analysis
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
λ_S	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_H	Rate for failure, who causes a high output current (> 21 mA)
λ_L	Rate for failure, who causes a low output current (≤ 3.6 mA)
λ_{AD}	Rate for diagnostic failure (detected)
λ_{AU}	Rate for diagnostic failure (undetected)
DC	Diagnostic Coverage
PTC	Proof Test Coverage (Diagnostic coverage for manual proof tests)
T1	Proof Test Interval
LT	Useful Life Time
MTBF	Mean Time Between Failure = MTTF + MTTR
MTTF	Mean Time To Failure
MTTR	IEC 61508, Ed1: Mean Time To Repair IEC 61508, Ed2: Mean Time To Restoration
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

10 Supplement C: SIL conformity

exida

The manufacturer may use the mark:

Revision 2.0 February 26, 2015

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証

VEGA 100183C P0011 C003

exida hereby confirms that the:

VEGAMET 391
Signal Conditioning Instrument

VEGA Grieshaber KG
Schiltach - Germany

Has been assessed per the relevant requirements of:

IEC 61508 : 2000 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Device

SIL 2 @ HFT = 0

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The VEGAMET 391 will read the analog input and control its output(s) in accordance to the parameter settings within the stated safety accuracy.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

VEGAMET 391
Signal Conditioning Instrument

Certificate / Certificat / Zertifikat / 合格証

VEGA 100183C P0011 C003

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Device

SIL 2 @ HFT = 0

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability:

The Product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

Configuration	λ_S	λ_{DD}	λ_{DU}
One relay output	716	0	24
Two relay outputs	758	0	25
Two relays in series connection	758	0	24
Current output	0	860	23
Current output and one relay	291	620	24

All failure rates are given in FIT (failures / 10^9 hours)

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: VEGA 1001-83-R1-C R004 V1R2

Safety Manual: VEGAMET 391 40888

exida®

64 N Main St
Sellersville, PA 18960

T-062, V1R7

40888-EN-220705

40888-EN-220705

40888-EN-220705

Printing date:

All statements concerning scope of delivery, application, practical use and operating conditions of the sensors and processing systems correspond to the information available at the time of printing.
Subject to change without prior notice

40888-EN-220705

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany

Phone +49 7836 50-0
E-mail: info.de@vega.com
www.vega.com