Safety Manual

VEGATRENN 14*

With SIL qualification

Document ID: 52434

Contents

52434-EN-160414

Editing status: 2016-03-15

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.

52434-EN-160414

2 Scope

2.1 Instrument version

This safety manual applies to the separators

VEGATRENN 141, 142

Valid versions:

- from HW Ver 1.0.0

2.2 Area of application

The instruments VEGATRENN 14* are used for voltage supply of 4 … 20 mA/HART sensors in two-wire version where the measured value is outputted in a galvanically separated current loop.

With suitable transmitters, the VEGATRENN 14* can be used for level detection or range monitoring in a safety-related system according to IEC 61508 in the modes *low demand mode* or *high demand mode*:

- Up to SIL2 in single-channel architecture
- Up to SIL3 in a multiple-channel architecture (systematic suitability SC3)

SIL The HART interface must not be used to output the measured value.

2.3 SIL conformity

The SIL conformity was independently judged and certified by the *TÜV Rheinland* according to IEC 61508:2010 (Ed.2).[1)]

SIL The certificate is valid for the entire service life of all instruments that were sold before the certificate expired!

[1)] Verification documents see appendix.

3 Planning

3.1 Safety function

Safety function

The intrinsically safe current of the transducers in Ex areas is detected and provided on the non-intrinsically safe output for further processing.

Safety tolerance

For the design of the safety function, the following aspect must be taken into account with regard to the tolerances:

Due to undetected failures in the range between 3.8 mA and 20.5 mA, an incorrect output signal can be generated which deviates from the real measured value by up to 2 %

3.2 Safe state

Safe state

The safe state of the current output depends on the safety function perceived by the connected transducer.

Fault signal in case of malfunction

Possible fault currents:

- ≤ 3,6 mA ("fail low")
- > 21 mA ("fail high")

3.3 SIL2 application for 1oo1 architecture

SIL2 qualification

SIL2 can be reached through a single-channel architecture consisting of:

- a VEGATRENN 141 or
- a VEGATRENN 142, where one of the channels is used for the safety function

3.4 SIL3 application for 1oo2 architecture

SIL3 application

SIL3 can be reached through a double-channel architecture consisting of:

- two VEGATRENN 141 or
- a VEGATRENN 142, where two channels is used redundantly for the safety function acc. to the following procedure:

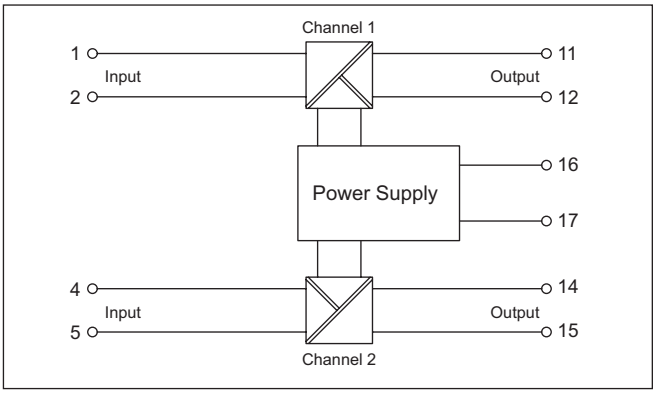

Fig. 1: SIL3 application for 1oo2 architecture

SIL If VEGATRENN 142 is used, then the failure rates *"Power Supply"* are influencing the PFD calculation as 1oo1 share and the failure rates *"OneChannel"* as 1oo2 share.

In any case, "failures caused by hardware due to common cause" must be taken into account.

For respective number values see chapter "*Safety-related characteristics*".

3.5 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
- The installation site must comply with IP 54 protection
- 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)*"

SIL For instruments with UL or CSA approval, an overvoltage arrester must be connected with networks of overvoltage category III and supply voltages of more than 150 V.

4 Safety-related characteristics

4.1 Key figures acc. to IEC 61508

VEGATRENN 141 or one channel of VEGATRENN 142

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture SIL3 in multiple channel architecture[2)]
Hardware error tolerance	HFT = 0
Instrument type	Type A
Mode	Low demand mode, High demand mode
SFF	> 60 %
MTBF[3)]	1.98 x 10^6 h (227 years)

Failure rates

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L		
30 FIT	50 FIT	42 FIT	6 FIT	160 FIT		

SIL

For calculation of PFD_{AVG}, the failure rates λ_H and λ_L are assigned to category λ_{DD}.

PFD_{AVG}	0.020 x 10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.038 x 10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.093 x 10^{-2}	(T1 = 5 years)
PFH	0.042 x 10^{-6} 1/h	

Proof Test Coverag (PTC)

Test type[4)]	Remaining failure rate of dangerous undetected failures	PTC
Test 1	0 FIT	99 %

4.2 Figures according to ISO 13849-1

VEGATRENN 141 or one channel of VEGATRENN 142

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

Parameter	Value
MTTFd	443 years
DC	84 %
Performance Level	4.19 x 10^{-8} 1/h (corresponds to "e")

[2)] Homogeneous redundancy possible, because systematical suitability SC3.
[3)] Including errors outside the safety function.
[4)] See section "Proof test".
[5)] ISO 13849-1 was not part of the certification of the instrument.

4.3 Characteristics acc. to IEC 61508 for 1oo2 architecture

VEGATRENN 142

Parameter	Power supply	OneChannel	1oo2 architecture
SIL	SIL2 / SIL3	SIL2	SIL3
HFT	HFT = 0	HFT = 1	HFT = 0
Instrument type	Type A	Type A	Type A
Mode	Low demand mode, High demand mode		
SFF	98 %	79 %	
MTBF[6]	1.17 x 10^6 h (133 years)		
λ_S	0 FIT	30 FIT	
λ_{DD}	21 FIT	29 FIT	
λ_{DU}	1 FIT	42 FIT	
λ_H	0 FIT	6 FIT	
λ_L	68 FIT	92 FIT	
PFD_{AVG} (T1 = 1 year)	0.66 x 10^{-5}	1.01 x 10^{-5}	1.67 x 10^{-5}
PFD_{AVG} (T1 = 2 years)	1.20 x 10^{-5}	1.92 x 10^{-5}	3.13 x 10^{-5}
PFD_{AVG} (T1 = 5 years)	2.82 x 10^{-5}	4.72 x 10^{-5}	7.54 x 10^{-5}
PFH	1.2 x 10^{-9} 1/h	2.1 x 10^{-9} 1/h	3.3 x 10^{-9} 1/h
PTC			99 %

SIL

The specified characteristics apply to the SIL application described in section 3.4 if the two channels of VEGATRENN 142 are used. Requirement is that the connected control and processing unit compares the measured values of the two channels to max. 2 % difference.

For calculation of SFF, PFD_{AVG} and PFH, the failure rates λ_H and λ_L are assigned to category λ_{DD}.

The characteristics PFD_{AVG} and PFH for the 1oo2 architecture are the result of the addition of the values of "Power Supply" and "OneChannel".

4.4 Supplementary information

Determination of the failure rates

The failure rates of the instrument were determined by an FMEDA according to IEC 61508. Basis for the calculations are the component failure rates according to **SN 29500**.

All figures refer to an average ambient temperature of 40 °C (104 °F) during the operating time. For higher temperatures, the values should be corrected:

- Continuous application temperature > 50 °C (122 °F) by factor 1.3
- Continuous application temperature > 60 °C (140 °F) by factor 2.5

Similar factors apply if frequent temperature fluctations are expected.

[6] Including errors outside the safety function.

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

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 = 99 %
- LT = 10 years
- MTTR = 8 h

Calculation of PFD_{AVG} and PFH for the 1oo2 architecture

The characteristics for the share "OneChannel" are calculated as follows:

- PFD_{AVG} acc. to IEC 61508-6, B.3.2.5

- PFH acc. to IEC 61508-6, B.3.3.2.2

Parameters used:

- T1 = Proof Test Interval
- PTC = 99 %
- T2 = LT = 10 years
- MTTR = MRT = 8 h
- ß = $ß_D$ = 5 %

Boundary conditions relating to transmitters

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

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!

Configuration of the processing unit for the 1oo2 architecture

A connected control and processing unit must compare the measured values of the two channels up to max. 2 % difference. The safe state must be taken on in case of a higher difference.

Multiple channel architecture

Due to the systematic suitability SC3, this instrument can also be used in multiple channel systems up to SIL3, also with a homogeneously redundant configuration.

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).

52434-EN-160414

5 Setup

5.1 General information

Mounting and installation

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

Setup must be carried out under process conditions.

5.2 Adjustment instructions

Adjustment elements

There are no adjustment elements available.

6 Diagnostics and servicing

6.1 Behaviour in case of failure

When a malfunction was detected, a failure signal is outputted on the current output (see section "*Safe state*").

SIL If failures are detected, the entire measuring system must be shut down and the process held in a safe state by other measures.

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

6.2 Repair

Defective instruments can only be repaired by the manufacturer.

52434-EN-160414

7 Proof test

7.1 General information

Objective

To identify possible dangerous, undetected failures, the safety function must be checked by a proof test at adequate intervals. It is the user's responsibility to choose the type of testing. The time intervals are determined by the selected PFD_{AVG} (see chapter "*Safety-related characteristics*").

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

If one of the tests 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.

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 1 - with input current simulation

Conditions

- Possibility of sensor current simulation exists
- Output signals correspond to the current process variable

Procedure

1. Simulate the currents ≤ 3.6 mA, 4 mA, 12 mA, 20 mA, > 21 mA on the sensor input
2. Check output current

Expected result

The output current corresponds to the simulated input currents (tolerances see operating instructions)

Proof Test Coverage

See *Safety-related characteristics*

8 Appendix A - Test report

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

Test reason	
(…)	Setup
(…)	Proof test

Operating mode channel 1		**Operating mode channel 2**	
(…)	Max.	(…)	Max.
(…)	Min.	(…)	Min.
(…)	Range monitoring	(…)	Range monitoring

Test result				
Test point	**Real value channel 1**	**Test result**	**Real value channel 2**	**Test result**
≤ 3.6 mA				
4 mA				
12 mA				
20 mA				
> 21 mA				

Confirmation	
Date:	Signature:

52434-EN-160414

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
T1	Proof Test Interval
LT	Useful Life Time
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration (Ed.2)
MRT	Mean Repair Time
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

10 Supplement C - SIL conformity

Certificate

Nr./No.: 968/FSP 1256.00/16

Prüfgegenstand **Product tested**	Speisetrenner für 4..20mA Sensoren Separator for 4..20mA Sensors	**Zertifikats-inhaber** **Certificate holder**	VEGA Grieshaber KG Am Hohenstein 113 77761 Schiltach Germany
Typbezeichnung **Type designation**	VEGATRENN 141, VEGATRENN 142		
Prüfgrundlagen **Codes and standards**	IEC 61508 Parts 1-7:2010 IEC 61511-1:2003 + Corr. 1:2004	IEC 61010-1:2010 IEC 61326-3-2:2008	
Bestimmungsgemäße Verwendung **Intended application**	Die Speisetrenner VEGATRENN 141/142 erfüllen die Anforderungen entspr. SIL 2 / SC 3 gemäß IEC 61508 und können in einem sicherheitsbezogenen System eingesetzt werden: - bis SIL 2 (VEGATRENN 141 oder 142) (HFT=0) bzw. - bis SIL 3 bei Verwendung der 2 Kanäle des VEGATRENN 142 alternativ 2x VEGATRENN 141 oder 142 The Separators VEGATRENN 141/142 comply with the requirements of SIL 2 / SC 3 acc. to IEC 61508 and can be used in a safety-related system: - up to SIL 2 (VEGATRENN 141 or 142) (HFT=0) resp. - up to SIL 3 when using the 2 channels of VEGATRENN 142, alternatively 2x VEGATRENN 141 or 142		
Besondere Bedingungen **Specific requirements**	Die zugehörigen Betriebsanleitungen und das Safety Manual sind zu beachten. Ausgangsströme <3,6mA und >21mA müssen von dem nachgeschalteten Sicherheitsgerät als Fehler behandelt werden. In SIL 3 Anwendungen müssen die Ströme der 2 Ausgangskanäle verglichen und Unterschiede ≥2% müssen als Fehler behandelt werden. The operating instructions and the safety manual shall be considered. Output currents <3.6mA and >21mA have to be considered by the downstream safety device as a failure condition. In SIL 3 applications the currents of the two channels have to be compared and a deviation of ≥ 2% has to be considered as a failure.		

Gültig bis / Valid until 2021-03-10

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 1256.00/16 vom 10.03.2016 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. Es wird ungültig bei jeglicher Änderung der Prüfgrundlagen für den angegebenen Verwendungszweck.
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1256.00/16 dated 2016-03-10.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2016-03-10

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Printing date:

52434-EN-160414

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany

Phone +49 7836 50-0
Fax +49 7836 50-201
E-mail: info.de@vega.com
www.vega.com