Safety Manual

VEGAWAVE série 60

- sortie électronique statique

Document ID:
32363

Vibration

Sommaire

1 Sécurité fonctionnelle

1.1 Généralités 3
1.2 Conception 4
1.3 Consignes de réglage. 6
1.4 Mise en service 7
1.5 Comportement au cours du fonctionnement et en cas de pannes 7
1.6 Test de fonctionnement périodique 7
1.7 Caractéristiques techniques relatives à la sécurité . . . 8

2 Annexe

32363-FR-110510

1 Sécurité fonctionnelle

1.1 Généralités

Matériel concerné

Ce manuel de sécurité est valable pour les systèmes de mesure comprenant le détecteur vibrant VEGAWAVE de la série 60 avec préamplificateur intégré WE60C :

VEGAWAVE 61, 62, 63

Versions hardware et software valables :

- Numéro de série de l'électronique > 14215928
- Logiciel du capteur à partir de rév. 1.03

Domaine d'application

Le système de mesure peut être utilisé pour la détection de niveau de pulvérulents ou granulés, satisfaisant aux exigences particulières de la technique de sécurité.

Dans une architecture à un canal (1oo1D), il est possible de l'utiliser jusqu'à SIL2 et dans une architecture redondante à multi-canaux, jusqu'à SIL3.

Remarque:
Par un réglage spécial en usine, le système de mesure sera également approprié à la détection sous l'eau de solides décantés (voir notice de "*Mise en service*").

Conformité SIL

Les documents de preuve en annexe témoignent de la conformité SIL.

Abréviations, termes

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
λ_{sd}	Rate for safe detected failure
λ_{su}	Rate for safe undetected failure
λ_{dd}	Rate for dangerous detected failure
λ_{du}	Rate for dangerous undetected failure
DC_S	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd}+\lambda_{su})$
DC_D	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd}+\lambda_{du})$
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure

MTTR	Mean Time To Repair

D'autres abréviations et termes sont indiqués dans la norme IEC 61508-4.

Normes concernées

- IEC 61508 (disponible également comme DIN EN)
  - Functional safety of electrical/electronic/programmable electronic safety-related systems

Exigences de sécurité

Valeurs limites de défaillance pour une fonction de sécurité, selon la classe SIL (IEC 61508-1, 7.6.2)

Niveau d'intégrité de sécurité	**Mode demande faible**	**Mode demande élevée**
SIL	**PFD_{avg}**	**PFH**
4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Intégrité de sécurité du matériel (hardware) pour les systèmes partiels relatifs à la sécurité de type B (IEC 61508-2, 7.4.3)

Proportion de défaillances en sécurité	**Tolérance aux anomalies matérielles (hardware)**		
SFF	**HFT = 0**	**HFT = 1**	**HFT = 2**
< 60 %	non autorisé	SIL1	SIL2
60 % … < 90 %	SIL1	SIL2	SIL3
90 % … < 99 %	SIL2	SIL3	(SIL4)
≥ 99 %	SIL3	(SIL4)	(SIL4)

1.2 Conception

Fonction de sécurité

La fonction de sécurité de ce système de mesure est la reconnaissance et la signalisation de l'état de l'élément vibrant.

On différenciera entre les deux états "*immergé*" et "*émergé*".

Etat de sécurité

L'état de sécurité dépend du mode de fonctionnement :

	Protection antidébordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
Elément vibrant à l'état de sécurité positive	immergé	émergé
Circuit de sortie à l'état de sécurité positive	désexcité/hors tension	désexcité/hors tension

L'état de sécurité du système de mesure est l'état hors circuit (principe du courant repos) :

- Electronique C : sortie électronique statique ouverte
- Electronique R : sortie relais désexcitée
- Electronique T : sortie transistor ne commute pas

Description d'une anomalie

Il y a défaillance en sécurité (safe failure) si le système de mesure passe à l'état de sécurité défini ou au mode défaut sans une requête du process.

Si le système de diagnostic interne reconnaît une anomalie, le système de mesure passera alors au mode défaut.

Il y a défaillance dangereuse non détectée (dangerous undetected failure), si le système de mesure ne passe ni à l'état de sécurité défini, ni au mode défaut à une requête du process.

Configuration de l'unité d'exploitation

L'unité de traitement doit exploiter le circuit de sortie du système de mesure en respectant le principe du courant repos.

L'unité d'exploitation doit correspondre au niveau SIL de la chaîne de mesure.

Mode demande faible

Si la fréquence du mode de sollicitation ne dépasse pas une fois par an, le système de mesure pourra être utilisé comme système partiel de sécurité en mode "*low demand mode*" (IEC 61508-4, 3.5.12).

Si le rapport entre le taux de tests de diagnostic du système de mesure et le mode de demande dépasse la valeur 100, le système de mesure pourra être traité comme effectuant une fonction de sécurité en mode de demande faible (IEC 61508-2, 7.4.3.2.5).

Le paramètre associé est la valeur PFD_{avg} (average Probability of dangerous Failure on Demand). La valeur dépend de l'intervalle de vérification T_{Proof} entre les tests de fonctionnement de la fonction de sécurité.

Vous trouverez la valeur au chapitre "*Caractéristiques techniques relatives à la sécurité*".

Mode demande élevée

Si le "*mode demande faible*" ne convient pas, il faudra utiliser le système de mesure comme système partiel de sécurité en mode "*high demand mode*" (IEC 61508-4, 3.5.12).

Le temps de tolérance aux anomalies de tout le système doit être ici supérieur à la somme des temps de réaction et/ou des durées de test de diagnostic de tous les composants de la chaîne de mesure de sécurité.

Le paramètre associé est la valeur PFH (taux de défaillance).

Vous trouverez la valeur au chapitre "*Caractéristiques techniques relatives à la sécurité*".

Suppositions

La réalisation de la FMEDA repose sur les suppositions suivantes :

- les taux de défaillance sont constants, l'usure des composants mécaniques n'a pas été prise en considération
- les taux de défaillance des alimentations courant externes n'ont pas été pris en compte dans le calcul
- les erreurs multiples n'ont pas été considérées
- La température ambiante moyenne pendant la durée de fonctionnement 40 °C (104 °F)
- les conditions environnementales correspondent à un environnement industriel moyen
- la durée d'utilisation des composants est comprise entre 8 et 12 ans (IEC 61508-2, 7.4.7.4, Note 3)
- la durée de réparation (remplacement du système de mesure) après une défaillance en sécurité est de huit heures (MTTR = 8 h)
- l'unité d'exploitation évalue le circuit de sortie du système de mesure selon le principe du courant repos
- l'intervalle de scrutation d'une unité de commande et d'exploitation raccordée s'élève à 1 heure maximum pour réagir à des défaillances dangereuses reconnaissables
- Les interfaces de communication existantes (p. ex. HART, bus I^2C) ne seront pas utilisées pour la transmission des informations relatives à la sécurité.

Remarques générales et restrictions

Il faudra veiller à une utilisation du système de mesure conforme à l'application en tenant compte de la pression, de la température, de la densité et des propriétés chimiques du produit.

Les limites spécifiques à l'application sont à respecter. Il ne faut pas aller au-delà des spécifications de la notice de mise en service.

A tenir compte lors de l'utilisation en tant que protection conte la marche à vide :

- Eviter tout colmatage de produit au système vibrant (il se peut que de plus petits intervalles de test Proof soient nécessaires)
- Version lames vibrantes : éviter une granulométrie du produit > 15 mm (0.6 in)

1.3 Consignes de réglage

Éléments de réglage

Les conditions dans l'installation ayant une influence sur la sécurité du système de mesure, il faudra régler les éléments de réglage en fonction de l'application :

- Potentiomètre d'adaptation du point de commutation
- Commutateur DIL pour inversion du mode de fonctionnement

La fonction des éléments de réglage vous sera décrite dans la notice de mise en service.

1.4 Mise en service

Montage et installation

Respectez les consignes de montage et d'installation de la notice de mise en service.

Dans le cadre de la mise en oeuvre de l'appareil, nous vous recommandons de vérifier la fonction de sécurité en procédant à un premier remplissage.

1.5 Comportement au cours du fonctionnement et en cas de pannes

Fonctionnement et panne

Les éléments de réglage et/ou les paramètres des appareils ne doivent pas être modifiés durant le fonctionnement.

En cas de changements apparaissant pendant le fonctionnement, respectez les fonctions de sécurité.

Les signalisations de défaut se manifestant durant le fonctionnement sont décrites dans la notice technique de mise en service de l'appareil.

En présence d'anomalies détectées ou de signalisations de défaut, il faudra mettre tout le système de mesure hors service et maintenir le process dans un état de sécurité par d'autres dispositions.

Le changement de l'électronique est simple. Il vous sera décrit dans la notice de mise en service. Respectez pour cela les indications concernant le paramétrage et la mise en oeuvre.

Si vous remplacez l'électronique ou le capteur complet en raison d'une anomalie constatée, vous aurez à le signaler au fabricant de l'appareil (y compris une description de l'anomalie).

1.6 Test de fonctionnement périodique

Raison

Le test de fonctionnement périodique sert à vérifier la fonction de sécurité et à déceler les anomalies ou défaillances dangereuses potentielles non reconnaissables. C'est pourquoi le bon fonctionnement du système de mesure doit être vérifié à des intervalles périodiques adéquats. C'est à l'exploitant de l'installation qu'il incombe de définir le type de vérification. Les intervalles de temps sont fonction de la valeur PFD_{avg} utilisée aux tableau et diagramme indiqués au chapitre "*Caractéristiques techniques relatives à la sécurité*".

En mode de demande élevée, un test de fonctionnement périodique n'est pas prévu dans la norme IEC 61508. On considère ici comme preuve de bon fonctionnement l'utilisation fréquente du système de mesure. Cependant, dans les architectures à deux canaux, il est judicieux de prouver l'effet de la redondance par des tests de fonctionnement périodiques dans des intervalles de temps appropriés.

Exécution

Le test doit prouver le parfait fonctionnement de la fonction de sécurité en corrélation avec tous les composants asservis. Ceci est garanti en faisant monter le niveau jusqu'au seuil de commutation dans le cadre d'un remplissage de cuve. Si un remplissage jusqu'au seuil de commutation n'est pas praticable, le système de mesure doit alors être déclenché par une simulation adéquate du niveau ou d'un effet de mesure physique.

Les méthodes et procédés utilisés au cours des tests doivent être spécifiés tout comme leur degré d'aptitude. Les contrôles sont à documenter.

Si le test de fonctionnement décèle des défauts, mettez tout le système de mesure hors service et maintenez le process dans un état de sécurité avec d'autres mesures de protection.

Ceci est valable séparément pour chacun des deux canaux en architecture à deux canaux (1oo2D).

1.7 Caractéristiques techniques relatives à la sécurité

Bases

Les taux de défaillance de l'électronique, des parties mécaniques de l'élément de mesure ainsi que du raccord process ont été calculés par une FMEDA selon IEC 61508. La base de ces calculs repose sur les taux de défaillance des composants selon SN 29500. Toutes ces valeurs numériques se rapportent à une température ambiante moyenne de 40 °C (104 °F) pendant la durée de fonctionnement.

L'expérience nous a montré que pour une température moyenne plus élevée de 60 °C, les taux de défaillance doivent être multipliés par un facteur de 2,5. En cas de variations de température fréquentes, il faut calculer avec un facteur similaire.

Les calculs s'appuient toujours sur les remarques indiquées au chapitre "*Conception*".

Durée d'utilisation

Après 8 à 12 ans, les taux de défaillance des composants électroniques vont augmenter, conduisant à une dégradation des valeurs PFD et PFH qui en découlent (IEC 61508-2, 7.4.7.4, note 3).

Taux de défaillance

	Protection antidébordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
λ_{sd}	0 FIT	0 FIT
λ_{su}	506 FIT	481 FIT
λ_{dd}	124 FIT	135 FIT
λ_{du}	41 FIT	56 FIT
DC_S	0 %	0 %
DC_D	75 %	71 %
MTBF = MTTF + MTTR	$1{,}45 \times 10^6$ h	$1{,}45 \times 10^6$ h

Temps de réaction en cas d'anomalie

Durée d'un test de diagnostic	< 100 sec.

Caractéristiques spécifiques

Architecture monocanale (1oo1D)

SIL	SIL2
HFT	0
Type de capteur	type B

	Protection antidébordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
SFF	94 %	92 %
PFD_{avg} T_{Proof} = 1 an T_{Proof} = 5 ans T_{Proof} = 10 ans	 $< 0{,}018 \times 10^{-2}$ $< 0{,}089 \times 10^{-2}$ $< 0{,}178 \times 10^{-2}$	 $< 0{,}024 \times 10^{-2}$ $< 0{,}122 \times 10^{-2}$ $< 0{,}243 \times 10^{-2}$
PFH	$< 0{,}041 \times 10^{-6}$/h	$< 0{,}056 \times 10^{-6}$/h

Déroulement en fonction du temps de PFD_{avg}

Le déroulement temporel de PFD_{avg} est presque linéaire à la durée de fonctionnement pendant une période maximale de 10 ans. Les valeurs indiquées précédemment sont valables uniquement pour l'intervalle T_{Proof} après lequel un test de fonctionnement périodique doit être effectuer.

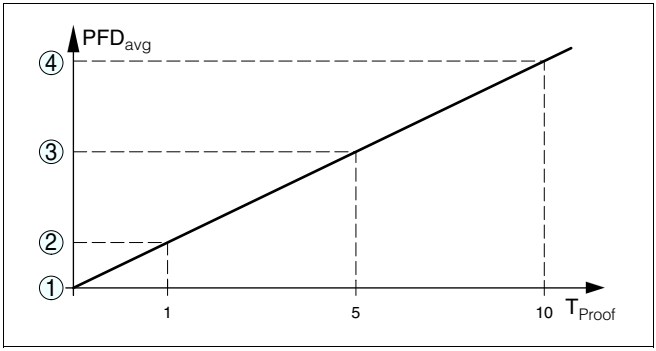

Fig. 1: Déroulement en fonction du temps de PFD_{avg} (valeurs numériques voir tableaux représentés ci-dessus)

1 PFD_{avg} = 0
2 PFD_{avg} après 1 an
3 PFD_{avg} après 5 ans
4 PFD_{avg} après 10 ans

Architecture à plusieurs canaux

Caractéristiques spécifiques

Si le système de mesure est utilisé dans une architecture à plusieurs canaux, il faudra à l'aide des taux de défaillance indiqués précédemment calculer spécialement pour l'application sélectionnée les valeurs des caractéristiques relatifs à la sécurité de la structure sélectionnée de la chaîne de mesure.

Il faudra tenir compte d'un facteur Common Cause approprié.

2 Annexe

exida CERTIFICATION

CERTIFICATE

EXIDA FS CERTIFIED

VEGA 100981C P0011 C001.1

exida Certification S.A. hereby confirms that the

VEGAVIB / VEGAWAVE 60 Level Switch
Output C, R, T, N, Z
Product Version: See listing in assessment report

VEGA Grieshaber KG
Schiltach, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000
Parts 1 - 3, and meets requirements providing a level of integrity to

Systematic Integrity : SIL 3 Capable

Random Integrity : SIL 2 @ HFT=0
SIL 3 @ HFT=1

Safety function
The VEGAVIB / VEGAWAVE 60 will de-energize its output (C,R,T,N) or set current (Z) to fail-safe output when a level goes above (or below) the trip point within the safety accuracy.

Application Restrictions
The unit must be properly designed and validated in a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor Certifying Assessor

Date: 11 Jan 2011

exida Certification SA, Nyon, Switzerland

Page 1 (2)

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

32363-FR-110510

exida® CERTIFICATION

Systematic Integrity: SIL 3 Capable

SIL 3 Capability

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. 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 the statement.

Random Integrity: SIL 2 @ HFT=0
SIL 3 @ HFT=1

Summary for the VEGAVIB / VEGAWAVE 60 Level Switch:

Type B device

IEC 61508 failure rates in FIT [:=10^{-9}/h]

Model	Fail-Safe state	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
C Max / High trip	Out De-energized	0	506	124	41
C Min / Low trip	Out De-energized	0	481	135	56
R Max / High trip	Out De-energized	0	586	124	27
R Min / Low trip	Out De-energized	0	565	135	37
T Max / High trip	Out De-energized	0	487	124	30
T Min / Low trip	Out De-energized	0	466	135	40
N Max / High trip	Out < 1.0 mA	12	160	390	47
N Min / Low trip	Out < 1.0 mA	36	155	366	52
Z Max / High trip	Out > 12.5 mA	49	387	163	18
Z Min / Low trip	Out < 11.5 mA	39	352	182	43

All failure rates are given in FIT =10^{-9}/h

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH / PFD_{AVG} considering the architecture, 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 subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory part of this certificate:

VEGA 03/05-08 R005 V3R1 Assessment Report

Safety manuals VEGAVIB / VEGAWAVE 60, all with versions:

C: 32002 / 32363 R: 32003 / 32364 T: 32004 / 32365

N: 32005 / 32366 Z: 32006 / 32367

The holder of this certificate may use this mark.

EXIDA FS CERTIFIED

exida Certification SA, Nyon, Switzerland

info@exidacert.ch

Page 2 (2)

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

32363-FR-110510

Date d'impression:

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Allemagne
Tél. +49 7836 50-0
Fax +49 7836 50-201
E-Mail: info@de.vega.com
www.vega.com

VEGA Technique S. A. S.
B. P. 20018 - ZA NORDHOUSE
67151 ERSTEIN CEDEX
France
Tél. 0388590150
Hotline techn. 0899700216 **(1,35€+ 0,34€/mn)**
Fax 0388590151
E-mail: info@fr.vega.com
www.vega.fr

Les indications de ce manuel concernant la livraison, l'application et les conditions de service des capteurs et systèmes d'exploitation répondent aux connaissances existantes au moment de l'impression.

© VEGA Grieshaber KG, Schiltach/Germany 2011