

Safety Manual

VEGACAP série 60

Deux fils



Document ID: 31813



VEGA

Table des matières

1	Sécurité fonctionnelle	3
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	10

1 Sécurité fonctionnelle

1.1 Généralités

Domaine de validité

Ce manuel de sécurité est valable pour les systèmes de mesure comprenant le détecteur capacitif de la série VEGACAP 60 avec électronique intégrée CP60Z :

VEGACAP 62, 63, 64, 65, 66, 69

Versions hardware et software valables :

- Numéro de série de l'électronique > 14678431
- Software du capteur à partir de rév. 1.01

Domaine d'application

Le système de mesure peut être utilisé pour la détection de niveau de liquides et solides en vrac/pulvérulents, satisfaisant aux exigences particulières de la technique de sécurité.

En raison de l'appropriation systématique SC3, cela reste possible jusqu'à :

- SIL2 dans une architecture à un canal
- SIL3 dans une architecture à plusieurs canaux



L'utilisation du système de mesure équipé d'un flotteur

Conformité SIL

La conformité SIL est attestée par les documents de contrôle en annexe.

Abréviations, termes

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PF _{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 faible demande	Mode demande élevée
SIL	PFD _{avg}	PFH
4	$\geq 10^5 \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-4} \dots < 10^{-3}$	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-3} \dots < 10^{-2}$	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$

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)		
	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

Le système de mesure génère sur sa sortie courant un signal correspondant au niveau compris entre 3,8 mA et 20,5 mA.

Ce signal analogique est transmis à une unité d'exploitation connectée en aval pour surveiller les états suivants :

- Dépassement vers le haut d'un niveau prédéterminé.
- Dépassement vers le bas d'un niveau prédéterminé

L'atteinte du point de commutation réglé génère un signal.

État de sécurité

L'état de sécurité dépend du mode de fonctionnement :

	Protection antidébordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
État de sécurité	Dépassement du point de commutation vers le haut	Dépassement du point de commutation vers le bas
Courant de sortie à l'état de sécurité positive	> point de commutation (-3 %)	< point de commutation (+3 %)
Courant défaut " fail low "	< 2,3 mA	< 2,3 mA

	Protection anti-débordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
Courant défaut " fail high "	> 23,5 mA	> 23,5 mA

La tolérance du courant $\pm 3\%$ se rapporte à la plage de mesure complète de 16 mA.

Description de l'erreur

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

Si le système de diagnostic interne détecte une anomalie, le système de mesure passera alors en 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 en mode défaut suite à une requête du process.

Configuration de l'unité d'exploitation

Si le système de mesure délivre des courants de sortie de " fail low " ou de " fail high ", il faut alors considérer qu'il y a présence d'une défaillance.

C'est pourquoi l'unité d'exploitation doit interpréter de tels courants comme défaut et délivrer une signalisation de défauts adéquate.

Si ce n'est pas le cas, il faudra attribuer les parts correspondantes des taux de défaillance aux anomalies dangereuses. Ce qui peut conduire à une dégradation des valeurs indiquées au chapitre " *Caractéristiques techniques relatives à la sécurité* ".

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

Mode faible demande

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 faible demande (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 faible demande " 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 de défaillance 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* ".

Postulats

La réalisation de la FMEDA repose sur les postulats suivants :

- 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 de sécurité est de huit heures (MTTR = 8 h)
- L'unité d'exploitation peut interpréter les défaillances " *fail low* " et " *fail high* " comme panne et délivrer une signalisation de défaut adéquate
- l'intervalle de scrutation d'une unité de commande et d'exploitation raccourdie s'élève à 1 heure maximum pour réagir à des défaillances dangereuses reconnaissables
- Les interfaces de communication existantes (p. ex. HART, bus I²C) 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, de la constante diélectrique 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 contre la marche à vide :

- Eviter une rupture de câble ou de tige (il se peut que des intervalles de test Proof plus courts soient nécessaires)

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 :

- Commutateur DIL pour la sélection de la plage de mesure

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

Montage et installation	1.4 Mise en service <p>Respecter les consignes de montage et d'installation de la notice de mise en service.</p> <p>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.</p>
Fonctionnement et panne	1.5 Comportement au cours du fonctionnement et en cas de pannes <p>Les éléments de réglage et/ou les paramètres des appareils ne doivent pas être modifiés durant le fonctionnement.</p> <p>En cas de changements apparaissant pendant le fonctionnement, respectez les fonctions de sécurité.</p> <p>Les signalisations de défaut se manifestant durant le fonctionnement sont décrites dans la notice technique de mise en service de l'appareil.</p> <p>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.</p> <p>Le changement de l'électronique est simple. Il vous est décrit dans la notice de mise en service. Respectez pour cela les indications concernant le paramétrage et la mise en oeuvre.</p> <p>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).</p>
Raison	1.6 Test de fonctionnement périodique <p>Le test de fonctionnement périodique sert à vérifier la fonction de sécurité et à déceler les anomalies ou défaillances dangereuses potentielles non détectables. 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 " <i>Caractéristiques techniques relatives à la sécurité</i> ".</p> <p>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.</p>
Exécution	<p>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 par moyen physique.</p>

Les méthodes et procédés utilisés au cours des tests doivent être spécifiés tout comme leur degré d'efficacité. 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.

Dans une architecture à plusieurs canaux, ceci est valable séparément pour chaque canal.

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 anti-débordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
λ_{sd}	38 FIT	69 FIT
λ_{su}	245 FIT	241 FIT
λ_{dd}	130 FIT	98 FIT
λ_{du}	35 FIT	40 FIT
DC _S	13 %	22 %
DC _D	78 %	71 %
MTBF = MTTF + MTTR	1,97 x 10 ⁶ h	1,97 x 10 ⁶ h

Temps de réaction en cas de défaillance

Durée d'un test de diagnostic	< 360 sek.
-------------------------------	------------

Architecture à un canal

Caractéristiques spécifiques

SIL	SIL2
HFT	0

Type d'appareil	type B	
	Protection anti-débordement (fonctionnement maxi.)	Protection contre la marche à vide (fonctionnement mini.)
SFF	92 %	91 %
PF_{avg}		
$T_{Proof} = 1 \text{ an}$	$< 0,016 \times 10^{-2}$	$< 0,018 \times 10^{-2}$
$T_{Proof} = 5 \text{ ans}$	$< 0,078 \times 10^{-2}$	$< 0,088 \times 10^{-2}$
$T_{Proof} = 10 \text{ ans}$	$< 0,155 \times 10^{-2}$	$< 0,177 \times 10^{-2}$
PFH	$< 0,035 \times 10^{-6}/\text{h}$	$< 0,04 \times 10^{-6}/\text{h}$

L'évolution de PF_{avg} dans le temps

L'évolution de PF_{avg} dans le temps 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 effectué.

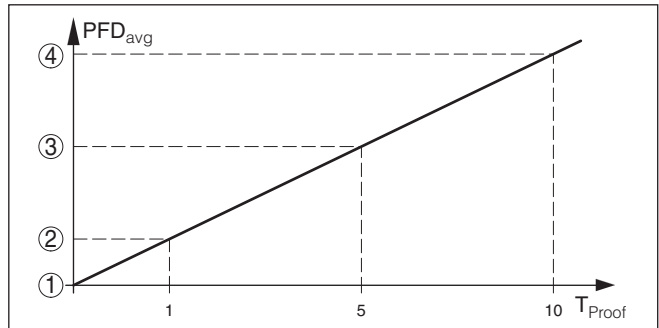


Fig. 1: Evolution PF_{avg} dans le temps (valeurs numériques voir tableaux représentés ci-dessus)

- 1 PF_{avg} = 0
- 2 PF_{avg} après 1 an
- 3 PF_{avg} après 5 ans
- 4 PF_{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 calculer les valeurs des caractéristiques de sécurité de la chaîne de mesure spécialement pour l'application sélectionnée, en fonction des taux indiqués précédemment.

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

2 Annexe



The manufacturer may use the mark:



Revision 2.0 February 24, 2015



ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証

VEGA 100981C P0011 C002

exida hereby confirms that the:

**VEGACAP 60 Level Switch
Output R,T, Z**

**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 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; SIL 3 @ HFT = 1; Route 1_H

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

Safety Function:

The VEGACAP 60 will de-energize its output (R & T) or set current (Z) to fail-safe output when the level goes above (or below) the trip point 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

**VEGACAP 60
Level Switch**



64 N Main St
Sellersville, PA 18960

T-002, V3R8

Certificate / Certificat / Zertifikat / 合格証

VEGA 100981C P0011 C002

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; SIL 3 @ HFT = 1; Route 1_H

**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) 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 stated.

Random Capability:

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

Versions:

	Type	Application	Electronics
V1.1	VEGACAP 60 R	MIN detection	SB1221 SB1226 SB1236 SB1237
V1.2	VEGACAP 60 R	MAX detection	SB1223 SB1226 SB1236 SB1237
V2.1	VEGACAP 60 T	MIN detection	SB1235 SB1226 SB1236 SB1237
V2.2	VEGACAP 60 T	MAX detection	SB1235 SB1226 SB1236 SB1237
V3.1	VEGACAP 60 Z	MIN detection	SB1235 SB1226 SB1236 SB1237
V3.2	VEGACAP 60 Z	MAX detection	SB1235 SB1226 SB1236 SB1237

Model	Fail-Safe state	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
R Max / High trip	Out De-energized	0	438	116	54
R Min / Low trip	Out De-energized	0	440	116	52
T Max / High trip	Out De-energized	0	395	115	35
T Min / Low trip	Out De-energized	0	397	115	33
Z Max / High trip	Out > 13 mA	38	245	130	35
Z Min / Low trip	Out < 11 mA	69	241	98	40

All failure rates are given in FIT (failures / 10⁹ 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 05/05-36 R013 V1R3

Safety Manuals: VEGACAP 60:

R: 31814 T: 31815 Z: 31813

Page 2 of 2



Date d'impression:

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.

Sous réserve de modifications

© VEGA Grieshaber KG, Schiltach/Germany 2018



31813-FR-181129

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