Safety Manual

VEGACAL série 60

Deux fils 4 … 20 mA/HART

Document ID: 35593

Table des matières

Date de rédaction : 2018-11-29

35593-FR-181129

1 Sécurité fonctionnelle

1.1 Généralités

Domaine de validité

Ce manuel de sécurité est valable pour les systèmes de mesure se composant d'un capteur de niveau capacitif VEGACAL de la série 60 en version deux fils 4 … 20 mA/HART :

VEGACAL 62, 63, 64, 65, 66, 69

Versions hardware et software valables :

- Numéro de série de l'électronique > 14557661
- Software du capteur à partir de rév. 1.01

Domaine d'application

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

De part le retour d'expérience, ils pourront être utilisés en architecture à un canal jusqu'à SIL2 et en architecture multi-canaux en version diversitaire redondante jusqu'à SIL3.

L'utilisation du système de mesure dans une architecture à plusieurs canaux, homogène et redondante est exclue.

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
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

- Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511-1
  - Functional safety - safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

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	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
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 (0)**	**HFT = 2**
< 60 %	non autorisé	SIL1	SIL2
60 % … < 90 %	SIL1	SIL2	SIL3
90 % … < 99 %	SIL2	SIL3	(SIL4)
≥ 99 %	SIL3	(SIL4)	(SIL4)

Retour d'expérience

Selon IEC 61511-1, paragraphe 11.4.4, la tolérance aux anomalies HFT pour les systèmes partiels validés en utilisation peut être réduite de un si les conditions suivantes sont satisfaites:

- L'appareil est validé en utilisation
- Seuls les paramètres importants pour le process sont modifiables (p. ex. plage de mesure, sortie courant en cas de défaut …)
- La modification de ces paramètres importants au process est protégée (p. ex. par un mot de passe, …)
- La fonction de sécurité requiert un niveau inférieur à SIL4

L'expertise des modifications est prise en compte dans L'évaluation du retour d'expérience.

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 :

	Surveillance du niveau haut	**Surveillance du niveau bas**
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 (-2 %)	< point de commutation (+2 %)
Courant défaut " fail low "	< 3,6 mA	< 3,6 mA
Courant défaut " fail high "	> 21,5 mA	> 21,5 mA

La tolérance du courant ±2 % se rapporte au réglage de 0 … 120 pF (voir notice de mise en service).

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 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, 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 conte 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 Paramétrage des appareils

Outils de réglage

Si les conditions d'implantation ont une influence sur la sécurité du système de mesure, il faudra régler les paramètres des appareils en fonction de l'application.

Ceci se fait avec les outils suivants :

- Le DTM approprié au VEGACAL en liaison avec le logiciel de configuration selon le standard FDT/DTM, p.ex. PACTware
- Module de réglage et d'affichage

Remarque:
Veillez à utiliser le catalogue DTM 10/2005 ou une version plus récente.

Créer une voie de mesure

Si le système de mesure n'a pas été commandé spécialement pour une application dans des systèmes instrumentés de sécurité (SIS), il faudra activer le paramètre "*Capteur selon SIL*" dans le menu "*Réglage de base*" de logiciel de configuration. Dans le cas d'utilisation du module de réglage et d'affichage est utilisé, il faudra activer dans la zone de menus "*Service*" le paramètre "*SIL*".

Comportement en cas de panne

Le paramétrage du courant de défaut influence les caractéristiques techniques relatives à la sécurité. C'est pourquoi seuls les courants de défauts suivants sont tolérés pour les applications de sécurité :

- fail low = <3,6 mA (valeur Default)
- fail high = 22 mA

Atténuation du signal de sortie

L'atténuation du signal de sortie doit être adaptée à la durée de sécurité du process.

Modes de fonctionnement non autorisés

La transmission des valeurs de mesure au moyen de signaux HART ainsi que le mode de fonctionnement HART multidrop ne sont pas autorisés.

Possibilités de vérification

L'efficacité des paramètres réglés doit être vérifiée d'une manière appropriée.

- Après le raccordement de l'appareil, le signal de sortie bascule sur le courant de défaut réglé à la fin de la phase de mise en route.
- En mode "*Simulation*", le signal courant peut être simulé indépendamment du niveau actuel

Blocage d'accès

Pour protéger l'appareil contre des modifications involontaires ou non autorisées, les paramètres réglés doivent être sauvegardés contre un accès intempestif :

- Activer la protection par mot de passe via le logiciel de configuration
- Activer le code PIN via le module de réglage et d'affichage

L'accès à l'aide d'une console HART ou similaire n'est pas admis.

La protection contre un déréglage involontaire ou non autorisé peut se faire par exemple en scellant le couvercle du boîtier.

Avertissement !
Après avoir restauré les paramètres d'origine par un reset, il est nécessaire de les contrôler et/ou de les régler à nouveau.

1.4 Mise en service

Montage et installation

Respecter 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 est 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 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 " *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 par moyen physique.

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

Est valable pour la protection antidébordement et la contre la marche à vide :

λ_{sd}	0 FIT
λ_{su}	212 FIT
λ_{dd}	458 FIT
λ_{du}	208 FIT
DC_S	0 %
DC_D	68 %
MTBF = MTTF + MTTR	0,93 x 10^6 h

Temps de réaction en cas de défaillance

E013 (aucune valeur de mesure existante)	< 10 sek.
E036/E037 (le logiciel du capteur ne fonctionne pas)	< 1 h

Architecture à un canal

Caractéristiques spécifiques

SIL	SIL2
HFT	0
Type d'appareil	type B

Est valable pour la protection antidébordement et la contre la marche à vide :

SFF	76 %
PFD_{avg} T_{Proof} = 1 an T_{Proof} = 5 ans	 < 0,091 x 10^{-2} < 0,182 x 10^{-2}
PFH	< 0,208 x 10^{-6}/h

L'évolution de PFD_{avg} dans le temps

L'évolution de PFD_{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.

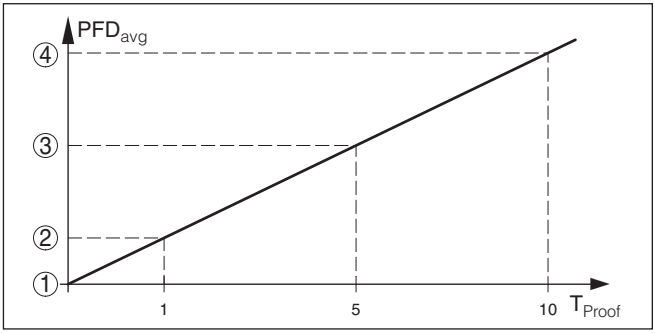

Fig. 1: Evolution PFD_{avg} dans le temps (valeurs numériques voir tableaux représentés ci-dessus)

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 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.

Le système de mesure ne doit être utilisé que dans une architecture diversitaire et redondante!

2 Annexe

Konformitätserklärung
Declaration of conformity
Déclaration de conformité

IEC 61508 / IEC 61511

VEGA Grieshaber KG,
Am Hohenstein 113,
77761 Schiltach / Germany

erklärt als Hersteller, dass die kapazitiven Füllstandsensoren der Produktfamilie

declares as manufacturer, that the capacitive level sensors of the product family

déclare en tant que fabricant que les capteurs de niveau capacitifs de la famille

VEGACAL 62, 63, 64, 65, 66, 69

4 ... 20 mA/HART

entsprechend der IEC 61511-1, Abschnitt 11.4.4 („Betriebsbewährtheit") für den Einsatz in sicherheitsinstrumentierten Systemen (SIS) als Untersystem bis **SIL2** geeignet sind.
Die Sicherheitstechnischen Kennzahlen sowie die Sicherheitshinweise im „Safety Manual" sind zu beachten.
Die Beurteilung des Änderungswesens war Bestandteil des Nachweises der Betriebsbewährtheit.

according to IEC 61511-1, section 11.4.4 ("proven in use")
are suitable as a subsystem until **SIL2** in safety instrumented systems (SIS).
The safety related characteristics as well as the safety instructions in the "Safety Manual" must be considered.
The assessment of the modification management was part of the proof for "proven in use".

conviennent à une utilisation dans les systèmes instrumentés de sécurité (SIS) comme sous-système jusqu'à **SIL2** suivant la norme IEC 61511-1, paragraphe 11.4.4 ("validé en utilisation").
Les caractéristiques techniques relatives à la sécurité ainsi que les consignes de sécurité stipulées dans le „Safety Manual" sont à respecter.
L'évaluation du service de modifications a fait partie de la preuve de la validité en utilisation.

Schiltach, 18 Februar 2009

J. Fehrenbach

Josef Fehrenbach
R&D Director

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

35593-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