

Safety Manual

VEGAMET 391

Unité de commande 4 ... 20 mA

Avec qualification SIL



Document ID: 40888



VEGA

Table des matières

1	Langue du document	3
2	Domaine de validité	4
2.1	Version d'appareil.....	4
2.2	Domaine d'application.....	4
2.3	Conformité SIL	4
3	Conception	5
3.1	Fonction de sécurité.....	5
3.2	État de sécurité.....	5
3.3	Conditions requises pour le fonctionnement	6
4	Caractéristiques techniques relatives à la sécurité	7
4.1	Caractéristiques spécifiques générales pour toutes les applications.....	7
4.2	Caractéristiques spécifiques pour application 1	7
4.3	Caractéristiques spécifiques pour application 2	8
4.4	Caractéristiques spécifiques pour application 3	8
4.5	Caractéristiques selon ISO 13849-1.....	9
4.6	Informations complémentaires	9
5	Mise en service	11
5.1	Paramétrage des appareils	11
5.2	Montage et installation	12
6	Comportement au cours du fonctionnement et en cas de pannes	13
6.1	Généralités.....	13
6.2	Comportement en cas d'erreur.....	13
7	Test de fonctionnement périodique	15
7.1	Généralités.....	15
7.2	Test application 1 - Une sortie relais	15
7.3	Test application 2 - Deux sorties relais pour surveillance de plage.....	16
7.4	Test application 3 - Sortie courant	16
8	Annexe A : Compte-rendu test de fonctionnement périodique	17
9	Annexe B: Définition des termes	19
10	Annexe C: Conformité SIL	20

1 Langue du document

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

2 Domaine de validité

2.1 Version d'appareil

Ce manuel de sécurité est valable pour le unité de commande **VEGA-MET 391 avec qualification SIL**

Version valable :

- à partir de la version du matériel 1.0.0
- à partir de la version logicielle 1.0.0

2.2 Domaine d'application

Le unité de commande peut, en combinaison avec un capteur de pression 4 ... 20 mA, être utilisé pour la mesure de niveau, le seuil de niveau et d'autres grandeurs de process comme système de mesure dans une fonction de protection relevant de la sécurité selon IEC 61508 dans les modes de fonctionnement *low demand mode* et *high demand mode* :

En raison de l'appropriation systématique SC2, cela reste possible jusqu'à :

- SIL2 dans une architecture à un canal
- SIL3 dans une architecture à plusieurs canaux seulement avec redondance diversitaire

Les interfaces suivantes sont ici utilisables :

- Entrée capteur : 4 ... 20 mA avec alimentation du capteur (Ex)
- Sortie de relais : Relais 3 et 4, contact NO ¹⁾
- Sortie courant : 4 ... 20 mA



Non autorisé pour des applications relevant de la sécurité :

- Entrées numériques 1 et 2
- Sorties relais 1 et 2
- Interfaces de communication existantes (par ex. HART, USB)

2.3 Conformité SIL

La conformité SIL a été évaluée et certifiée indépendamment par *exida* Certification LLC selon CEI 61508. ²⁾

¹⁾ NO = Normal Open

²⁾ Voir l'annexe pour les documents de preuve

3 Conception

3.1 Fonction de sécurité

Le capteur de pression alimenté par le unité de commande crée un signal proportionnel à la grandeur de process entre 3,8 et 20,5 mA.

Fonction de sécurité sortie relais

En fonction de ce signal analogue et des points de commutation réglés, un ou deux relais sont commutés pour la surveillance de la valeur limite.

Fonction de sécurité sortie courant

De plus, ce signal analogue peut être transmis à une unité d'exploitation connectée en aval (par ex. APS). Les points de commutation qui y sont réglés peuvent être utilisés pour la surveillance de la valeur limite.

Tolérance de sécurité

Si le système de diagnostic interne reconnaît une falsification de la valeur de mesure supérieure à 2 % causée par des erreurs de matériel, les signaux de sortie seront mis à l'état Défaut.

Cela doit être pris en compte lors de la configuration de la fonction de sécurité.

3.2 État de sécurité

État de sécurité sortie relais

L'état de sécurité sur la sortie relais est le contact de travail est ouvert. C'est pourquoi, seul le contact de travail (NO-Contact) doit être utilisé pour la fonction de sécurité (principe du courant repos)

État de sécurité sortie courant

L'état de sécurité de la sortie courant dépend du mode de fonctionnement et de la courbe caractéristique réglée sur le capteur.

	Surveillance de la valeur limite haut	Surveillance de la valeur limite minimale
Courbe caractéristique croissante : 4 mA = 0 %; 20 mA = 100 %	Courant de sortie > Point de commutation -334 µA	Courant de sortie < Point de commutation +334 µA
Courbe caractéristique décroissante : 20 mA = 0 % 4 mA = 100 %	Courant de sortie < Point de commutation +334 µA	Courant de sortie > Point de commutation -334 µA

Signaux de sortie en mode défaut

Sortie relais

- Le contact de travail est ouvert

Sortie courant

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

3.3 Conditions requises pour le fonctionnement

- Remarques et restrictions**
- Il faut veiller à ce que le système soit utilisé conformément à l'application pour laquelle il est conçu. Les limites spécifiques à son application doivent être respectées
 - Les spécifications selon les indications de la notice de mise en service, en particulier la charge de courant des circuits de sortie, doivent rester dans les limites indiquées
 - Pour éviter la fusion des contacts, ceux-ci doivent être protégés par un fusible externe qui se déclenche à 60 % de la charge maximale de courant des contacts
 - Les interfaces de communication existantes (p. ex. HART, USB) ne seront pas utilisées pour la transmission de la valeur de mesure relative à la sécurité.
 - Respecter les indications contenues dans le chapitre "*Caractéristiques techniques relatives à la sécurité*", paragraphe "*Informations complémentaires*"
 - Toutes les parties intégrantes de la chaîne de mesure doivent correspondre au "*Safety Integrity Level (SIL)*" prévu

4 Caractéristiques techniques relatives à la sécurité

4.1 Caractéristiques spécifiques générales pour toutes les applications

Grandeur caractéristique selon la norme IEC 61508	Valeur
Safety Integrity Level	SIL2
Tolérance aux anomalies matérielles	HFT = 0
Type d'appareil	Type B
Mode de fonctionnement	Low demand mode/High demand mode
MTTR	8 h
MTBF = MTTF + MTTR ³⁾	0,38 x 10 ⁶ h (44 ans)
Intervalle des tests de diagnostic ⁴⁾	< 4 min
Mode de demande	> 50 h

4.2 Caractéristiques spécifiques pour application 1

Une sortie relais

Un relais servant à la commande d'un acteur pour la surveillance d'une valeur limite (par ex. protection antidébordement ou protection contre la marche à vide).

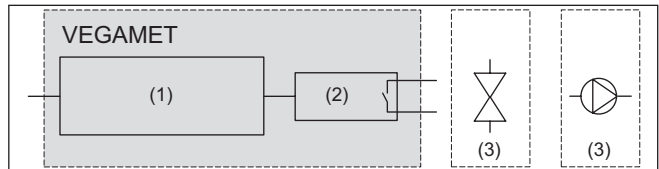


Fig. 1: Structure de l'application

- 1 Entrée du courant et électronique d'exploitation
- 2 Relais 3 ou Relais 4
- 3 Acteur

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 an)
PFD _{AVG}	0,0342 x 10 ⁻²	(T1 = 2 ans)
PFD _{AVG}	0,0604 x 10 ⁻²	(T1 = 5 ans)
PFH	0,0238 x 10 ⁻⁶ 1/h	

³⁾ MTBF : erreurs situées en dehors de la fonction de sécurité incluses

⁴⁾ Intervalle de temps pendant lequel tous les diagnostics internes sont effectués au moins une fois.

4.3 Caractéristiques spécifiques pour application 2

Deux sorties relais

Deux relais servant à la commande de deux acteurs pour la surveillance de deux valeurs limites (par ex. surveillance de plage).

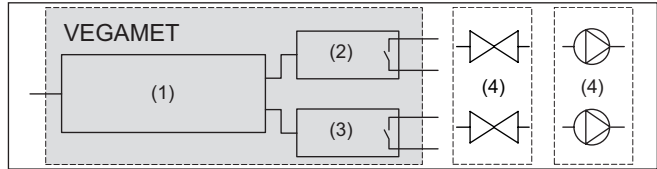


Fig. 2: Structure de l'application

- 1 Entrée du courant et électronique d'exploitation
- 2 Relais 3
- 3 Relais 4
- 4 Acteurs

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 x 10 ⁻²	(T1 = 1 an)
PFD _{AVG}	0,0364 x 10 ⁻²	(T1 = 2 ans)
PFD _{AVG}	0,0643 x 10 ⁻²	(T1 = 5 ans)
PFH	0,0253 x 10 ⁻⁶ 1/h	

4.4 Caractéristiques spécifiques pour application 3

Sortie courant

Une sortie courant servant à la commande d'une unité d'exploitation connectée en aval (par APS).

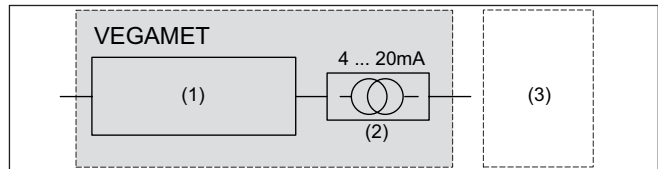


Fig. 3: Structure de l'application

- 1 Entrée du courant et électronique d'exploitation
- 2 Sortie courant
- 3 Unité d'exploitation connectée en aval

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 x 10 ⁻²	(T1 = 1 an)
PFD _{AVG}	0,0357 x 10 ⁻²	(T1 = 2 ans)
PFD _{AVG}	0,0599 x 10 ⁻²	(T1 = 5 ans)

PFH	0,0227 x 10 ⁻⁶ 1/h	
-----	-------------------------------	--

4.5 Caractéristiques selon ISO 13849-1

Les caractéristiques suivantes découlent des caractéristiques relevant de la sécurité selon ISO 13849-1 (sécurité des machines) :⁵⁾

Grandeur caractéristique selon ISO 13849-1	Valeur pour application 1	Valeur pour application 2	Valeur pour application 3
MTTF _d	243 ans	236 ans	129 ans
DC	94 %	94 %	97 %
Performance Level	4,68 x 10 ⁻⁷ 1/h	4,83 x 10 ⁻⁷ 1/h	8,83 x 10 ⁻⁷ 1/h

4.6 Informations complémentaires

Détermination des taux de défaillance

Les taux de défaillance de l'appareil ont été déterminés par une analyse FMEDA selon IEC 61508. Ces calculs reposent sur les taux de défaillance des éléments de construction selon **exida Profile 1** :

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 Jours

Suppositions de la FMEDA

- Les taux de défaillance sont constants. Respecter la durée d'utilisation des composants selon CEI 61508-2.
- Les défaillances multiples n'ont pas été considérées
- 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 conditions environnementales correspondent à un environnement industriel moyen
- Pour éviter la fusion des contacts, ceux-ci sont protégés par un fusible externe

Calcul de PFD_{AVG}

Les valeurs susmentionnées pour PFD_{AVG} ont été calculées de manière suivante pour une architecture 1oo1 :

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

Paramètres utilisés :

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

⁵⁾ La norme ISO 13849-1 ne faisait pas partie de la certification de l'appareil.

Conditions marginales en fonction du capteur de pression

Le capteur de pression utilisé doit émettre un courant parasite lorsqu'il est alimenté avec une tension hors de sa plage de tension spécifiée.

Conditions marginales en fonction de la configuration de l'unité d'exploitation

Une unité d'exploitation et de commande connectée en aval doit offrir les caractéristiques suivantes :

- Les signaux de sortie du système de mesure sont évalués selon le principe du courant repos
- Les signaux " *fail low*" et " *fail high*" sont interprétés comme des défauts, ensuite l'état sûr doit être pris !

Si cela n'est pas le cas, il faudra attribuer les parts correspondantes des taux de défaillance aux anomalies dangereuses et les valeurs citées contenues dans le chapitre " *Caractéristiques techniques* " doivent être de nouveau déterminées !

Architecture à plusieurs canaux

Dans des systèmes à plusieurs canaux pour application SIL3, ce système de mesure ne doit être utilisé qu'avec une redondance diversitaire.

Les valeurs des caractéristiques relatives à la sécurité doivent être spécialement calculées pour la structure de la chaîne de mesure sélectionnée à l'aide des taux de défaillance indiqués précédemment. Dans ce cas, il faudra tenir compte d'un facteur Common Cause (CCF) (voir CEI 61508-6, Annexe D).

5 Mise en service

5.1 Paramétrage des appareils

Outil

Les unités de réglage suivantes sont autorisées pour le paramétrage de la fonction de sécurité :

- L'unité de réglage et d'affichage intégrée pour le paramétrage sur site
- Le DTM approprié au VEGAMET 391 en liaison avec le logiciel de configuration selon le standard FDT/DTM, p.ex. PACTware
- La collection DTM 06/2011 ou une version plus récente est nécessaire.

La procédure de paramétrage est décrite dans la notice de mise en service.



La modification de paramètres relevant de la sécurité n'est possible que lorsqu'une liaison à l'appareil est active (mode en ligne).

Paramètre relevant de la sécurité

Pour protéger l'appareil contre un paramétrage involontaire ou non autorisé, les paramètres réglés doivent être protégés contre tout accès intempestif. Pour cette raison, l'appareil est livré à l'état verrouillé. Le code PIN à la livraison est "0000".

Un aperçu qui liste tous les paramètres relevant de la sécurité et leur valeur à l'état de livraison est livré avec l'appareil. Vous pouvez également télécharger cette liste au moyen du numéro de série via "www.vega.com", "Recherche".

Paramétrage sécurisé

Afin d'éviter d'éventuelles défaillances lors du paramétrage en mode non bloqué, une procédure de vérification est appliquée aux paramètres relevant de la sécurité.

Les étapes suivantes sont exécutées lors du paramétrage :

- Autoriser paramétrage
- Modifier paramètre
- Bloquer le paramétrage et vérifier les paramètres modifiés

Le déroulement exact est décrit dans la notice de mise en service.

Les paramètres actuels relevant de la sécurité peuvent être imprimés ou enregistrés avec le logiciel de configuration. Cette fonction n'est cependant accessible que lorsqu'une liaison entre l'appareil et le logiciel de configuration est active (Mode en ligne).



L'appareil est livré à l'état verrouillé !



Seuls les paramètres relevant de la sécurité sont représentés pour la vérification. Les textes de vérification sont disponibles soit en allemand, soit en anglais pour toutes les autres langues du menu.

État de l'appareil non fiable



Attention !

Si l'appareil est déverrouillé, la fonction de sécurité doit être considérée comme non fiable. Cela est valable jusqu'à ce que le paramétrage soit dûment terminé.

Le cas échéant, des mesures doivent être prises afin de maintenir la fonction de sécurité.

Déroulement incomplet du paramétrage de l'appareil**Attention !**

Lorsque le déroulement du paramétrage décrit n'est pas complet (par ex. à cause d'une interruption ou d'une panne de courant), l'appareil reste alors dans un état de sécurité non garanti et déverrouillé.

Reset appareil**Attention !**

Lors d'un reset vers le réglage de base, tous les paramètres relevant de la sécurité sont réinitialisés sur le réglage d'usine. Tous les paramètres relevant de la sécurité doivent ensuite être vérifiés ou de nouveau réglés.

5.2 Montage et installation

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

Nous vous recommandons, dans le cadre de la mise en service, de vérifier la fonction de sécurité, par ex., au moyen d'un premier remplissage ou d'une simulation d'un signal d'entrée. Pour cela, la procédure décrite dans le chapitre "*Test de fonctionnement périodique*" peut être utilisée.

6 Comportement au cours du fonctionnement et en cas de pannes

6.1 Généralités

Le comportement pendant le fonctionnement et en cas d'anomalie ainsi que les signalisations de défaut correspondantes sont décrits dans la notice de mise en service.

L'apparition d'une défaillance synonyme de danger non détectée doit être signalée au fabricant (description de l'erreur incluse).

6.2 Comportement en cas d'erreur

L'appareil est surveillé en permanence par un système de diagnostic interne. Si un défaut de fonctionnement est détecté, les signaux de sortie correspondants passent à l'état sûr (voir paragraphe " *État de sécurité* ").

Cet état est maintenu au moins 5 secondes. Si aucune erreur n'est reconnue, la fonction de sécurité est réexécutée correctement.

L'intervalle des tests de diagnostic est indiqué dans le chapitre " *Caractéristiques techniques relatives à la sécurité* ".

Diagnostic interne

Temps de réaction en cas d'anomalie relatives à la sécurité

Selon le type d'anomalies, une signalisation de défaut correspondante est délivrée avec le temps de réaction suivant :

Signalisations de défaut pendant le fonctionnement	Temps de réaction
E012 Erreur de matériel entrée capteur	< 1 min
E014 Court-circuit de ligne entrée capteur	< 5 s
E015 Rupture de ligne entrée capteur	< 5 s
E034 Erreur EEPROM-CRC	< 2 s
E035 Erreur CRC mémoire du programme	< 1 min
E037 RAM défectueuse	< 4 min
E040 Matériel défectueux	< 4 min
E080 Microcontrôleur défectueux	< 4 min
E113 Erreur matériel sortie courant	< 1 min
E117 Pompe signale un dérangement	Paramétrable
E125 Température de l'électronique de l'appareil	1 h

Signalisations de défaut pendant le paramétrage	Temps de réaction
E017 Écart de réglage trop faible	< 5 s
E021 Échelle d'étalonnage trop faible	< 5 s
E062 Valence d'impulsion trop petite	< 5 s
E110 Points de commutation relais : échelle trop petite	< 5 s
E111 Les points de commutation relais ont été intervertis	< 5 s

Signalisations de défaut pendant le paramétrage	Temps de réaction
E115 Comportement incorrect en cas de défaut	< 5 s
E116 Mode de fonctionnement sortie incorrect	< 5 s

7 Test de fonctionnement périodique

7.1 Généralités

Le test de fonctionnement périodique (*Proof Test*) sert à vérifier la fonction de sécurité et à déceler les défaillances dangereuses potentielles non détectées. 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} (voir 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.

Le compte-rendu contenu dans l'annexe peut être utilisé pour la documentation de ces tests fonctionnel.

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.

Outils

- Ampèremètre approprié calibré (précision meilleure que $\pm 0,1$ mA)
- Appareil de mesure de la résistance approprié et calibré
- Le cas échéant, simulateur pour courant capteur (source courant passive)

Préparation

- Déterminer la fonction de sécurité (mode de fonctionnement, points de commutation)
- Si besoin est, ôter l'appareil de la chaîne de sécurité et maintenir la fonction de sécurité d'une autre manière.

État de l'appareil non fiable



Attention !

Pendant le test de fonctionnement, la fonction de sécurité doit être considérée comme non fiable. Tenez compte du fait que le test de fonctionnement a des effets sur les appareils connectés en aval.

Le cas échéant, des mesures doivent être prises afin de maintenir la fonction de sécurité.

Lorsque le test de fonctionnement est achevé, l'état spécifique pour la fonction de sécurité doit de nouveau être créé.

7.2 Test application 1 - Une sortie relais

1. Régler courant capteur en-dessous du point de commutation relais inférieur "Lo"
2. Régler courant capteur juste au-dessus du point de commutation relais supérieur "Hi"

Déroutement pour mode de fonctionnement sécurité antidébordement

Déroulement pour mode de fonctionnement protection contre la marche à vide

1. Régler courant capteur au-dessus du point de commutation relais supérieur "Hi"
2. Régler courant capteur juste en-dessous du point de commutation relais inférieur "Lo"

Résultat escompté

Le contact relais SIL utilisé doit être fermé au point 1 et ouvert au point 2 dans la tolérance de sécurité (+334 μ A).

Degré de couverture du contrôle

PTC = 84 %

7.3 Test application 2 - Deux sorties relais pour surveillance de plage**Déroulement**

1. Régler au moins trois valeurs du courant capteur dans les limites de la plage.
2. Régler capteur courant juste au-dessus du point de commutation relais supérieur "Hi" pour la limite de la plage supérieure
3. Régler capteur courant juste au-dessous du point de commutation relais inférieur "Lo" pour la limite de la plage inférieure

Résultat escompté

Points 1 : les deux contacts relais SIL doivent être fermés.

Point 2 : le contact relais SIL pour la surveillance de la limite de la plage supérieure doit être ouvert dans la tolérance de sécurité (+334 μ A).

Point 3 : le contact relais SIL pour la surveillance de la limite de la plage inférieure doit être ouvert dans la tolérance de sécurité (+334 μ A).

Degré de couverture du contrôle

PTC = 84 %

7.4 Test application 3 - Sortie courant**Déroulement**

Régler au moins cinq valeurs du courant capteur à l'intérieur de la plage de mesure.

Résultat escompté

Toutes les valeurs de sortie courant mesurées divergent de moins de 2 % (+334 μ A) du courant de sortie escompté.

Degré de couverture du contrôle

PTC = 81 %

8 Annexe A : Compte-rendu test de fonctionnement périodique

Identification	
Entreprise/Contrôleur	
TAG installation/appareils	
TAG voie de mesure	
Type d'appareil/Code de commande	
Numéro de série de l'appareil	
Date mise en service	
Date dernier test de fonctionnement	

Paramètres d'appareil réglés de la fonction de sécurité	
Sorties utilisées importantes pour la sécurité	<input type="radio"/> Relais 3 <input type="radio"/> Relais 4 <input type="radio"/> Sortie courant
Mode de fonction réglé relais 3	<input type="radio"/> Sécurité antidébordement <input type="radio"/> Protection contre la marche à vide
Point de commutation supérieur réglé relais 3 "Hi"	mA
Point de commutation inférieur réglé relais 3 "Lo"	mA
Mode de fonction réglé relais 4	<input type="radio"/> Sécurité antidébordement <input type="radio"/> Protection contre la marche à vide
Point de commutation supérieur réglé relais 4 "Hi"	mA
Point de commutation inférieur réglé relais 4 "Lo"	mA

Résultat du test 1 Sorties relais

Point de commutation	Sortie relais 3			Sortie relais 4		
	Courant capteur mesuré	État Relais 3	Résultat du test	Courant capteur mesuré	État Relais 4	Résultat du test
"Hi"	mA			mA		
"Hi"	mA			mA		
"Hi"	mA			mA		
"Lo"	mA			mA		
"Lo"	mA			mA		
"Lo"	mA			mA		

Résultat du test 2 Sortie courant

Courant capteur simulé		Escompté Courant de sortie	Mesuré Courant de sortie	Résultat du test
Courant capteur 1	mA	mA	mA	
Courant capteur 2	mA	mA	mA	
Courant capteur 3	mA	mA	mA	
Courant capteur 4	mA	mA	mA	
Courant capteur 5	mA	mA	mA	

Confirmation

Date :

Signature :

9 Annexe B: Définition des termes

Abréviations

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 Annexe C: Conformité SIL

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.



The manufacturer may use the mark:



Revision 2.0 February 26, 2015



ANSI Accredited Program
PRODUCT CERTIFICATION
#1004



Evaluating Assessor

Certifying Assessor

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**

**VEGAMET 391
Signal Conditioning
Instrument**

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 / 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 1001-83-R1-C R004 V1R2

Safety Manual: VEGAMET 391 40888



64 N Main St
Sellersville, PA 18960

T-062, V1R7







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 2022



40888-FR-220705

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Allemagne

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