Directives de sécurité informatique

VEGAPULS 6X

Document ID: 1007792

Table des matières

Date de rédaction : 2023-01-23

1007792-FR-230306

1 Domaine de validité

1.1 Version d'appareil

Ce manuel de sécurité est valable pour les capteurs

VEGAPULS 6X

- Deux fils 4 … 20 mA/HART avec sécurité informatique
- Deux fils 4 … 20 mA/HART - SIL avec sécurité informatique

Versions valables :

- à partir de la vers. mat. 1.1.0
- à partir de la vers. logicielle 1.1.0

1.2 Domaine d'application

L'appareil a été développé selon les exigences envers un développement de produit sûr selon CEI 62443-4-1 et est certifié selon CEI 62443-4-2

Il est impératif de respecter les exigences du présent document et de la mise en service correspondante afin que la stratégie de sécurité échelonnée de l'appareil entre en jeu comme prévu.

1007792-FR-230306

2 Defense-in-Depth

2.1 Stratégie de défense en profondeur

La stratégie Defense-in-Depth est un concept échelonné de sécurité qui inclut plusieurs couches de sécurité informatique. elle inclut la sécurité de l'installation, la sécurité du réseau et la stratégie de sécurité des composants système.

Fig. 1: Stratégie de défense en profondeur

1 *Administration de la sécurité informatique*
2 *Sécurité de l'installation*
3 *Sécurité de l'appareil*
4 *Cybermenace*

2.2 Mesures environnementales

Les mesures suivantes sont absolument nécessaires pour une exploitation sûre de l'appareil.

Sécurité de l'installation

- Surveillez les zones sensibles de votre installation
- Octroyez l'accès aux composants, aux réseaux et aux systèmes uniquement aux personnes pour lesquelles cela est absolument nécessaire.
- Désactivez les canaux de communication inutilisés

Communication HART

Le protocole HART standardisé, fondé sur la CEI 62443, n'offre pas une protection suffisante contre la manipulation des données et l'espionnage. Maintenez ce protocole actif uniquement :

- si l'appareil est intégré dans une zone avec un niveau de protection correspondant à SIL-1
- s'il vous est possible de garantir qu'une personne non autorisée n'obtient accès aux lignes de signaux

Exploitation avec d'autres appareils VEGA

Les appareils VEGA suivants n'ont aucune influence sur la sécurité informatique :

- VEGADIS 82

1007792-FR-230306

- Adaptateur d'interfaces VEGACONNECT

Les appareils VEGA suivants n'ont aucune influence sur la sécurité informatique avec la configuration correspondants :

- Module de réglage et d'affichage PLICSCOM, y compris en liaison avec le VEGADIS 81

Remarque:
La fonction Bluetooth n'est pas terminée automatiquement. Il vous faut donc désactiver celle-ci après le paramétrage.

Remarque:
Le PLICSCOM avec fonctionnalité Bluetooth prend en charge le paramétrage avec stylet magnétique. La protection par plombage/scellage du couvercle du boîtier peut en être affectée.

Interface sérielle

L'interface sérielle fondée sur la CEI 62443 n'offre pas une protection suffisante contre la manipulation des données et l'espionnage.

Assurez donc de ce fait que

- le couvercle du boîtier est plombé en cas d'inutilisation, ou
- qu'aucune personne non autorisée obtient l'accès aux lignes de signaux

2.3 Defense-in-Depth-Strategie pour l'appareil

L'appareil offre une protection contre les menaces suivantes dans le respect des directives d'application :

- Manipulation des données (atteinte à l'intégrité)
- Denial of Service DoS (atteinte à la disponibilité)
- Espionnage (atteinte à la confidentialité)

L'appareil est doté de fonctions de sécurité ayant fait leurs preuves :

- Authentification de l'utilisateur
- Mémoire des événements (logging)
- Contrôles d'intégralité du micrologiciel
- Gestion des ressources
- Sauvegarde des données pour la restauration

3 Directives pour le renforcement de la sécurité informatique

La présente section fournit des instructions sur la manière d'obtenir et de maintenir un renforcement de la sécurité informatique de l'appareil. Les indications précises pour l'installation, la première mise en service, l'exploitation, la maintenance et l'élimination figurent dans la notice de mise en service. Les exigences supplémentaires en matière de sécurité informatique sont décrites ci-dessous.

Planification

Planifiez soigneusement vos besoin en sécurité informatique en réalisant une évaluation des risques spécifiques de votre application. Tenez compte des éventuelles obligations légales et normatives.

Mettez en oeuvre les solutions spécifiques à l'application qui offrent un niveau de protection conforme à vos objectifs de sécurité. Vous obtiendrez la preuve pour l'appareil au moyen de la certification en annexe au présent document.

Remarque:
Pour procéder à une évaluation complète d'un système touchant la cybersécurité, toutes les exigences pertinentes de la série de normes CEI 62443 doivent être appliquées à l'ensemble du système dans lequel le composant VEGAPULS 6X- évalué doit être intégré, pour les niveaux de sécurité requis.

Installation

Installez l'appareil uniquement dans l'environnement de sécurité informatique prévu au sein d'un milieu protégé, par ex. dans une installation inaccessible au public.

Prenez en compte lors de la mise en service avec appli et Blutooth :

- Un code d'accès est nécessaire pour établir la communication Bluetooth
- La communication Bluetooth est cryptée
- Désactiver la communication Bluetooth après la configuration de l'appareil

Évitez les codes d'accès standard ou faciles à deviner. Utilisez de plus pour chaque appareil un code d'accès différent adapté aux situations dangereuses.

La protection d'accès est activée par défaut, mais elle peut toutefois être désactivée. Tenez compte que les exigences envers la cybersécurité ne peuvent être remplies qu'avec la protection d'accès active.

Plombez le couvercle du boîtier avec le corps du boîtier afin de protéger contre la manipulation des paramètres et du logiciel de l'appareil. Dans le cas d'un boîtier en plastique, scellez le couvercle avec une étiquette de sécurité.

Fonctionnement

Contrôler régulièrement que le plomb ou l'étiquette sont intacts. Un endommagement de ces éléments révèle que les données d'appareil ont été manipulées. Contrôlez dans ce cas les paramètres de l'appareil.

Le compteur de modification des paramètres fait office d'assistance. Notez la lecture du compte après chaque modification.

1007792-FR-230306

Remarque:
Toutes les modifications du paramétrage et les tentatives de connexion sur l'appareil sont consignées avec la date et l'heure, toutefois pas les informations relatives à l'utilisateur.

Vous devez être informé le plus rapidement possible des événements touchant la sécurité informatique. C'est pourquoi vous devez créer un compte myVEGA. Nous vous informerons des incidents de sécurité et de la fin de l'assistance de vos appareils via l'adresse de courriel enregistrée.

Maintenance

Veillez que le code d'appareil est uniquement accessible à des personnes autorisées pour réaliser les modifications de l'appareil. Vous trouverez de plus amples instructions dans les exigences lors de l'installation.

La fonctionnalité des fonctions de sécurité peut être testée en tentant de procéder à une libération de l'appareil avec un code d'appareil erroné. Cette authentification erronée doit ensuite être consignée dans la mémoire d'événements de la sécurité informatique. Vérifiez en plus régulièrement la mémoire d'événements afin de détecter les attaques ou les manipulations. La mémoire d'événements de la sécurité informatique est disponible dans le DTM sous " *Diagnostic -> Mémoire de l'appareil -> Mémoire d'événements*".

Synchronisez l'heure système au moyen des HART Common Practice Commands 89 et 90 (heure d'hiver et heure d'été).

Des informations relatives au fabricant, au numéro de série, à l'ID de l'appareil et à la révision de l'appareil HART sont demandées par la HART Command 0. Le numéro de série et la version du progiciel peuvent en outre être interrogées via PACTware/DTM.

Élimination

Nous recommandons pour une élimination sûre de l'appareil de supprimer les réglages spécifiques à l'application. Réinitialisez à cet effet l'appareil aux réglages d'usine.

4 Incidents de sécurité informatique

L'adresse de courriel enregistrée dans myVEGA permet d'informer en cas d'événements touchant la sécurité informatique. Si vous deviez déterminer des points faibles sur nos fonctions de sécurité informatiques, nous vous prions de nous le communiquer.

Sur notre site Internet www.vega.com/PSIRT, vous en apprendrez davantage sur la façon de signaler des vulnérabilités en sécurité et vous recevrez des informations sur le processus de traitement des points faibles de VEGA Grieshaber KG.

Pour le signalement (les signalements se font via psirt@vega.com) et la divulgation des vulnérabilités, VEGA collabore étroitement avec le CERT@VDE, une plateforme de sécurité informatique pour les entreprises industrielles. Sur le site Internet du CERT@VDE, vous avez également la possibilité de consulter et de signaler des vulnérabilités pour d'autres produits industriels.

1007792-FR-230306

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

1007792-FR-230306

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Allemagne

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