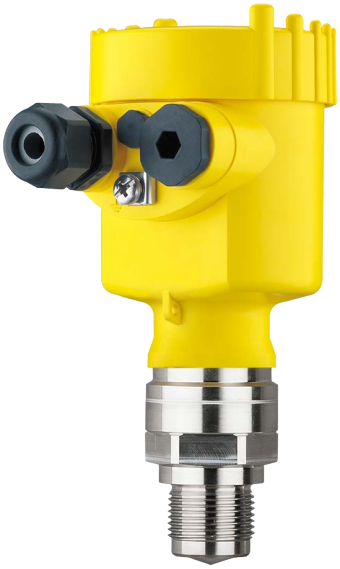
IT-Sicherheitsrichtlinien

VEGAPULS 6X



Document ID: 1007792

Inhaltsverzeichnis

Redaktionsstand: 2023-01-17

1007792-DE-230117

1 Geltungsbereich

1.1 Geräteausführung

Dieses Sicherheitshandbuch gilt für die Sensoren

VEGAPULS 6X

- Zweileiter 4 … 20 mA/HART mit IT-Sicherheit
- Zweileiter 4 … 20 mA/HART - SIL mit IT-Sicherheit

Gültige Versionen

- ab HW Ver 1.0.0
- ab SW Ver 1.0.0

1.2 Anwendungsbereich

Das Gerät ist nach den Anforderungen an eine sichere Produktentwicklung nach IEC 62443-4-1 entwickelt worden und ist zertifiziert nach IEC 62443-4-2.

Damit die gestaffelte Sicherheitsstrategie des Geräts wie vorgesehen greift, sind die Anforderungen aus diesem Dokument und der zugehörigen Betriebsanleitung zu beachten.

1007792-DE-230117

2 Defense-in-Depth

2.1 Defense-in-Depth-Strategie

Die Defense-in-Depth-Strategie ist ein gestaffeltes Sicherheitskonzept, das mehrere IT-Sicherheitsschichten umfasst. Es beinhaltet die Anlagensicherheit, die Netzwerksicherheit und die Sicherheitsstrategie der Systemkomponente.

Abb. 1: Defense-in-Depth-Strategie

1 Verwaltung der IT-Sicherheit
2 Anlagensicherheit
3 Gerätesicherheit
4 Cyber-Bedrohungen

2.2 Maßnahmen der Umgebung

Für einen sicheren Betrieb des Geräts sind folgende Maßnahmen zwingend notwendig.

Anlagensicherheit

- Überwachen Sie sensible Bereiche Ihrer Anlage
- Gewähren Sie den Zugang zu Komponenten, Netzwerken und Systemen nur Personen, bei welchen dies unbedingt erforderlich ist
- Deaktivieren Sie unbenutzte Kommunikationskanäle

HART-Kommunikation

Das standardisierte HART-Protokoll bietet, bezogen auf die IEC 62443, keinen ausreichenden Schutz vor Datenmanipulation und Spionage. Lassen Sie dieses Protokoll nur aktiv:

- wenn das Gerät in einer Zone mit einem Schutzniveau entsprechend SL-1 integriert ist
- wenn Sie sicherstellen können, dass keine unbefugten Personen Zugang zu den Signalleitungen erlangen

Betrieb mit anderen VEGA-Geräten

Die folgenden VEGA-Geräte verhalten sich rückwirkungsfrei auf die IT-Sicherheit:

- VEGADIS 82

10077792-DE-230117

- Schnittstellenadapter VEGACONNECT

Die folgenden VEGA-Geräte verhalten sich bei entsprechender Konfiguration rückwirkungsfrei auf die IT-Sicherheit:

- Anzeige- und Bedienmodul PLICSCOM, auch in Verbindung mit dem VEGADIS 81

Hinweis:
Die Bluetooth-Funktion wird nicht automatisch terminiert. Deaktivieren Sie diese daher nach der Parametrierung.

Hinweis:
Das PLICSCOM mit Bluetooth-Funktionalität unterstützt die Bedienung mit Magnetstift. Der Schutz durch Verplombung/Versiegelung des Gehäusedeckels kann dadurch beeinträchtig werden.

Serielle Schnittstelle

Die serielle Schnittstelle bietet, bezogen auf die IEC 62443, keinen ausreichenden Schutz vor Datenmanipulation und Spionage.

Stellen Sie deshalb sicher, dass

- der Gehäusedeckel bei Nichtbenutzung verplombt ist, oder
- keine unbefugten Personen Zugang zu den Signalleitungen erlangen

2.3 Defense-in-Depth-Strategie für das Gerät

Unter Einhaltung der Anwendungsrichtlinien bietet das Gerät Schutz gegen die folgenden Bedrohungen:

- Datenmanipulation (Verletzung der Integrität)
- Denial of Service DoS (Verletzung der Verfügbarkeit)
- Spionage (Verletzung der Vertraulichkeit)

Das Gerät verfügt über bewährte Sicherheitsfunktionen:

- Benutzer-Authentifizierung
- Ereignisspeicher (Logging)
- Integritätschecks der Firmware
- Ressourcenmanangement
- Datensicherung zur Wiederherstellung

1007792-DE-230117

3 Richtlinien für die Härtung der IT-Sicherheit

Dieser Abschnitt gibt Anweisungen, wie eine Härtung der IT-Sicherheit des Geräts erreicht und aufrecht erhalten wird. Die genauen Angaben für Installation, Erstinbetriebnahme, Betrieb, Wartung und Entsorgung entnehmen Sie der Betriebsanleitung. Zusätzliche Anforderungen im Hinblick auf die IT-Sicherheit werden nachfolgend beschrieben.

Planung

Planen Sie Ihre Security-Bedürfnisse sorgfältig indem Sie eine applikationsspezifische Risikobeurteilung durchführen. Achten Sie auf mögliche rechtliche und normative Vorgaben.

Setzen Sie anwendungsspezifische Lösungen ein, die ein Schutzniveau, entsprechend Ihren Sicherheitszielen bieten. Den Nachweis erhalten Sie bei dem Gerät über die Zertifizierung im Anhang in diesem Dokument.

Hinweis:
Um eine vollständige Beurteilung eines Cybersecurity-relevanten-Systems durchzuführen, müssen alle relevanten Anforderungen der Normenserie IEC 62443 auf das Gesamtsystem, in welchem die bewertete VEGAPULS 6X-Komponente integriert werden soll, für die erforderlichen Security-Level angewendet werden.

Installation

Installieren Sie das Gerät nur in dem vorgesehenen IT-Sicherheitsumfeld innerhalb einer geschützten Umgebung, z. B. in einer nicht öffentlich zugänglichen Anlage.

Beachten Sie bei der Inbetriebnahme über App und Bluetooth:

- Zum Aufbau der Bluetooth-Kommunikation ist ein Zugangscode erforderlich
- Die Bluetooth-Kommunikation ist verschlüsselt
- Nach der Konfiguration des Geräts die Bluetooth-Kommunikation deaktivieren

Vermeiden Sie Standard- oder leicht zu erratene Zugangscodes. Verwenden Sie, der Gefahrensituation angepasst, auch für jedes Gerät einen unterschiedlicher Zugangscode.

Der Zugriffsschutz ist standardmäßig aktiv, kann jedoch deaktiviert werden. Beachten Sie, dass nur mit aktivem Zugriffschutz die Anforderungen zur Cybersecurity erfüllt werden können.

Zum Schutz vor Manipulation der Parameter und Gerätesoftware verplomben Sie den Gehäusedeckel mit dem Gehäusekörper. Beim Kunststoffgehäuse versiegeln Sie den Deckel mit einem Sicherheitsetikett.

Betrieb

Prüfen Sie regelmäßig die Unversehrtheit der Verplombung oder des Etiketts. Wenn Beschädigungen an diesen Elementen erkennbar sind, können Gerätedaten manipuliert worden sein. Kontrollieren Sie in diesem Fall die Geräteeinstellungen.

Zur Unterstützung dient der Parameteränderungszähler. Notieren Sie sich nach jeder Änderung den Zählerstand.

1007792-DE-230117

Hinweis:
Alle Parameteränderungen und Anmeldeversuche am Gerät werden mit Datum und Uhrzeit, jedoch nicht mit Informationen zum Benutzer geloggt.

Zu IT-sicherheitsrelevanten Ereignissen sollen Sie schnellstmöglich informiert werden. Legen Sie sich deshalb einen myVEGA Account an. Über die hinterlegte Email-Adresse informieren wir Sie über Sicherheitsvorfälle und über das Ende des Supports Ihrer Geräte.

Wartung

Achten Sie darauf, dass der Gerätecode nur berechtigten Personen zugänglich ist, um Änderungen am Gerät durchzuführen. Weitere Hinweise entnehmen Sie den Anforderungen bei Installation.

Die Funktionalität der Security Funktionen kann getestet werden, indem eine Freigabe des Gerätes mit einem fehlerhaften Gerätecodes versucht wird. Diese fehlerhafte Authentifizierung muss anschließend im Ereignisspeicher IT-Sicherheit vermerkt sein. Prüfen Sie zusätzlich regelmäßig den Ereignisspeicher, um Angriffe oder Manipulation festzustellen. Der Ereignisspeicher IT-Sicherheit steht im DTM unter "*Diagnose -> Gerätespeicher -> Ereignisspeicher*" zur Verfügung.

Synchronisieren Sie die Systemzeit mittels den HART Common Practice Commands 89 und 90, (Sommer und Winterzeit).

Durch das HART Command 0 können Infos zum Hersteller, Seriennummer, Device ID und Device Revision abgefragt werden. Zudem können Seriennummer und Firmware Version über PACTware/DTM abgefragt werden.

Entsorgung

Zur sicheren Entsorgung des Geräts empfehlen wir, die applikationsspezifischen Einstellungen zu löschen. Setzen Sie das Gerät dazu auf Werkseinstellungen zurück.

1007792-DE-230117

4 IT-Sicherheitsvorfälle

Über die in myVEGA hinterlegte Email-Adresse werden Sie bei IT-sicherheitsrelevanten Ereignissen informiert. Sollten Sie Schwachstellen an unseren IT-Sicherheitsfunktionen feststellen, bitten wir Sie, uns diese mitzuteilen.

Auf unserer Webseite www.vega.com/PSIRT erfahren Sie mehr darüber, wie Sie Schwachstellen sicher zurückmelden können und erhalten Infos über den Schwachstellenbehandlungsprozess der VEGA Grieshaber KG.

Bei der Meldung (Meldungen erfolgen über psirt@vega.com) und Offenlegung von Schwachstellen arbeitet VEGA eng mit dem CERT@VDE, einer IT-Sicherheitsplattform für Industrieunternehmen, zusammen. Über die Webseite des CERT@VDE haben Sie die Möglichkeit, Schwachstellen auch für weitere Industrieprodukte einzusehen und zu melden.

1007792-DE-230117

1007792-DE-230117

Druckdatum:

Die Angaben über Lieferumfang, Anwendung, Einsatz und Betriebsbedingungen der Sensoren und Auswertsysteme entsprechen den zum Zeitpunkt der Drucklegung vorhandenen Kenntnissen.
Änderungen vorbehalten

1007792-DE-230117

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Deutschland

Telefon +49 7836 50-0
E-Mail: info.de@vega.com
www.vega.com