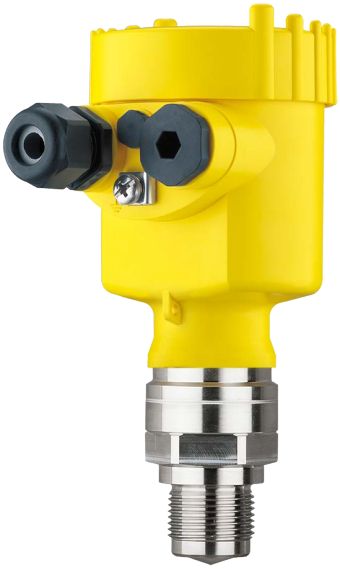
IT security guidelines

VEGAPULS 6X



Document ID: 1007792

Contents

Editing status: 2023-01-23

10077792-EN-230301

1 Scope

1.1 Instrument version

This safety manual applies to sensors

VEGAPULS 6X

- Two-wire 4 … 20 mA/HART with IT security
- Two-wire 4 … 20 mA/HART - SIL with IT security

Valid versions:

- from HW Ver 1.1.0
- from SW Ver 1.1.0

1.2 Application area

The device has been developed in accordance with the requirements for secure product development according to IEC 62443-4-1 and is certified according to IEC 62443-4-2.

In order for the staggered security strategy of the device to take effect as intended, the requirements from this document and the associated operating instructions must be observed.

1007792-EN-230301

2 Defense-in-Depth

2.1 Defense-in-Depth strategy

The defence-in-depth strategy is a staggered security concept that encompasses several IT security layers. It includes plant security, network security and the system component security strategy.

Fig. 1: Defense-in-Depth strategy

1 IT security management
2 System security
3 Device safety
4 Cyber threats

2.2 Measures of the environment

The following measures are mandatory for safe operation of the device.

System security

- Monitor sensitive areas of your facility
- Only grant access to components, networks and systems to persons for whom this is absolutely necessary
- Deactivate unused communication channels

HART communication

The standardised HART protocol does not offer sufficient protection against data manipulation and espionage, with reference to IEC 62443. Only leave this protocol active:

- if the device is integrated in a zone with a protection level corresponding to SL1
- if you can ensure that no unauthorised persons have access to the signal cables

Operation with other VEGA devices

The following VEGA devices behave without reaction to IT security:

- VEGADIS 82
- Interface adapter VEGACONNECT

The following VEGA devices, if configured accordingly, behave without reaction to the IT security:

1007792-EN-230301

- Display and adjustment module PLICSCOM, also in conjunction with VEGADIS 81

Note:
The Bluetooth function is not automatically terminated. Therefore, deactivate it after parameterisation.

Note:
The PLICSCOM with Bluetooth functionality supports operation with a magnetic pen. The protection provided by the sealing of the housing cover may be impaired.

Standard interface

The serial interface does not offer sufficient protection against data manipulation and espionage in relation to IEC 62443.

Therefore, make sure that

- the housing cover is sealed when not in use, or
- no unauthorised persons get access to the signal cables

2.3 Defense-in-Depth strategy for the device

In compliance with the application guidelines, the device provides protection against the following threats:

- Data manipulation (violation of integrity)
- Denial of Service DoS (violation of availability)
- Spying (breach of confidentiality)

The device has proven safety functions:

- User authentication
- Event memory (logging)
- Integrity check of the firmware
- Resource management
- Data backup for recovery

3 Guidelines for strengthening IT security

This section provides instructions on how to achieve and maintain strengthening of the IT security of the device. Refer to the operating instructions for detailed information on installation, initial setup, operation, maintenance and disposal. Additional requirements with regard to IT security are described below.

Planning

Plan your security needs carefully by conducting an application-specific risk assessment. Pay attention to possible legal and normative specifications.

Use application-specific solutions that provide a level of protection that meets your safety objectives. You can get proof of this with the device via the certification in the appendix of this document.

Note:
In order to carry out a complete assessment of a cyber security-relevant system, all relevant requirements of the IEC 62443 series of standards must be applied to the overall system in which the assessed VEGAPULS 6X component is to be integrated, for the required security levels.

Installation

Install the device only in the intended IT security environment within a protected environment, e.g. in a facility not accessible to the public.

Note for setup the device via the app and Bluetooth:

- An access code is required to establish Bluetooth communication
- Bluetooth communication is encrypted
- After configuring the device, deactivate Bluetooth communication

Avoid standard or easily identifiable access codes. Use a different access code for each device, depending on the danger situation.

Access protection is active by default, but can be deactivated. Please note that the cyber security requirements can only be fulfilled with active access protection.

To protect against manipulation of the parameters and device software, seal the housing cover with the housing body. For the plastic housing, seal the lid with a security label.

Operation

Regularly check the integrity of the seal or label. If damage to these elements is visible, device data may have been manipulated. In this case, check the device settings.

The parameter change counter serves as a support. Make a note of the counter reading after each change.

Note:
All parameter changes and login attempts to the device are logged with date and time, but not with information about the user.

You should be informed as quickly as possible about IT security-relevant events. Therefore, create a myVEGA account. We will inform you about security incidents and the end of support for your devices via the stored e-mail address.

10077792-EN-230301

Maintenance

Make sure that the device code is only accessible to authorised persons in order to make changes to the device. For further information, see the requirements for installation.

The functionality of the security functions can be tested by attempting to release the device with an incorrect device code. This faulty authentication must then be recorded in the IT security event memory. In addition, check the event memory regularly to detect attacks or manipulation. The IT security event memory is available in the DTM under " *Diagnosis -> Device memory -> Event memory*".

Synchronise the system time using HART Common Practice Commands 89 and 90 (summer and winter time).

The HART Command 0 can be used to query information on the manufacturer, serial number, device ID and device revision. In addition, the serial number and firmware version can be queried via PACTware/DTM.

Disposal

For safe disposal of the device, we recommend deleting the application-specific settings. To do this, reset the device to default settings.

4 IT security incidents

You will be informed of IT security-relevant events via the e-mail address stored in myVEGA. If you notice any weaknesses in our IT security functions, please let us know.

On our website www.vega.com/PSIRT, you can find out more about how you can reliably report back vulnerabilities and receive information about VEGA Grieshaber KG's vulnerability handling process.

VEGA works closely with CERT@VDE, an IT security platform for industrial companies, to report (reports are made via psirt@vega.com) and disclose vulnerabilities. Via the CERT@VDE website, you have the possibility to view and report vulnerabilities for other industrial products as well.

1007792-EN-230301

1007792-EN-230301

Printing date:

All statements concerning scope of delivery, application, practical use and operating conditions of the sensors and processing systems correspond to the information available at the time of printing.
Subject to change without prior notice

1007792-EN-230301

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany

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