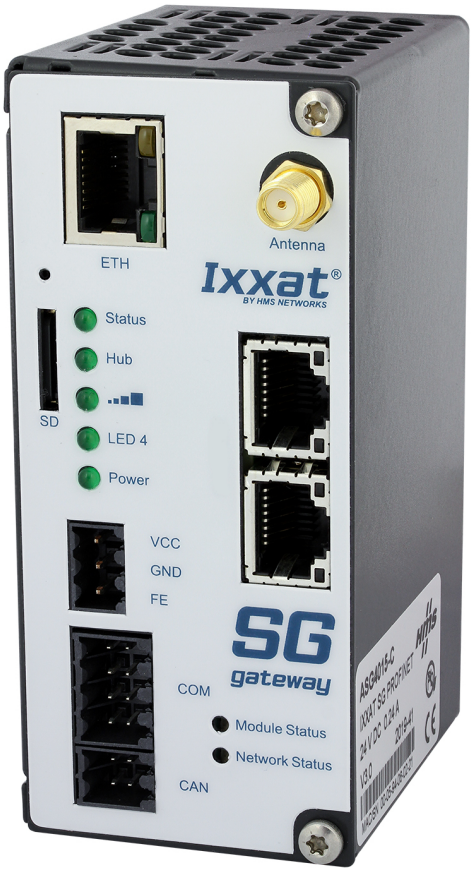
Ixxat®
BY HMS NETWORKS

# SG-gateway

## Extended Version

## USER MANUAL

**4.01.0402.20000 1.7 en-US ENGLISH**




HMS Connecting Devices™

# Important User Information

## Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

# Table of Contents

Page

# 1 User Guide

Please read the manual carefully. Make sure you fully understand the manual before using the product.

## 1.1 Target Audience

This documentation is intended for use by skilled staff who is familiar with the applicable national standards of the application field. Exclusively trained staff authorized by the operator is allowed to install, commission and maintain the device. The contents of the user manual must be made available to any person authorized to use or operate the product.

This guide provides information on hardware installation and the setup of the SG-gateway as well as the basic steps how to access the integrated web-based user interface, the so-called WEB-PLC. All configuration done via the WEB-PLC are described in detail in the integrated WEB-PLC online help, available via the web-interface.

## 1.2 Related Documents

| Document | Author |
|---|---|
| OpenVPN documentation http://openvpn.net | OpenVPN |
| WEB-PLC — Online Help | HMS |

For additional related documentation like Startup Guides for various protocols, How-to videos, and file downloads see support website at www.ixxat.com/sg-gw-download.

## 1.3 Document History

| Version | Date | Description |
|---|---|---|
| 1.0 | May 2017 | First release IXXAT product |
| 1.1 | September 2017 | Combined installation guide and extended user manual |
| 1.2 | October 2017 | Added information about Open Source Software |
| 1.3 | October 2017 | Corrected information about PROFINET |
| 1.4 | September 2019 | Layout changes, corrected number of possible slave devices with M-Bus, divided into installation guide and extended user manual |
| 1.5 | January 2020 | Corrected operating temperature |
| 1.6 | February 2020 | Additional information about Open Source Software |
| 1.7 | May 2021 | Added new variants, corrections in Compliance, added data security information |

## 1.4 Trademark Information

## 1.5 Conventions

Instructions and results are structured as follows:

- ► instruction 1
- ► instruction 2
  - → result 1
  - → result 2

Lists are structured as follows:

- item 1
- item 2

**Bold typeface** indicates interactive parts such as connectors and switches on the hardware, or menus and buttons in a graphical user interface.

```
This font is used to indicate program code and other
kinds of data input/output such as configuration scripts.
```

This is a cross-reference within this document: *Conventions, p. 4*

This is an external link (URL): www.hms-networks.com

Safety advice is structured as follows:

> **!** Cause of the hazard!
>
> Consequences of not taking remediate action.
>
> How to avoid the hazard.

Safety signs and signalwords are used dependent on the level of the hazard.

*This is additional information which may facilitate installation and/or operation.*

> **!** This instruction must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

> **Caution**
> This instruction must be followed to avoid a risk of personal injury.

> **WARNING**
> This instruction must be followed to avoid a risk of death or serious injury.

# 2 Safety Instructions

**Caution**
The device may only be put into service and operated by qualified personnel. To ensure the safe operation of the device, prevent access to the device by unauthorized persons.

**Caution**
This equipment emits RF energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this equipment meet appropriate susceptibility specifications for this type of RF energy.

**Caution**
Risk of injury when mounting and unmounting the device with the DIN lock mechanism.

**Caution**
The device is intended for use only in a restricted access area.

Risk of interference if used with antenna (wireless)!

In case of interference install device or antenna in other location.

## 2.1 General Safety Instructions

- Protect product from moisture and humidity.
- Protect product from too high or too low temperature (see *Technical Data, p. 38*).
- Protect product from fire.
- Do not paint the product.
- Do not modify or disassemble the product. Service must be carried out by HMS Industrial Networks.
- Store products in dry and dust-free place.

## 2.2 Data Security Features

The SG-gateway supports various security features. HMS recommends to activate and use this security features as described in the following chapters.

### 2.2.1 OpenVPN

HMS recommends using encoding via OpenVPN, if supported by all participants, to increase the internet safety.

The firmware includes an OpenVPN client, that can be used to integrate the SG-gateway into a virtual private network. For more information about OpenVPN and possible settings see the WEB-PLC Online Help — Settings — Network — OpenVPN. Additionally a How-to video and a Startup Guide for OpenVPN are available on www.ixxat.com/sg-gw-download.

### 2.2.2 WEB-PLC Security

**HTTPS**

> To increase the internet security, HMS recommends activating HTTPS to access the WEB-PLC.

If the WEB-PLC is accessed with activated HTTPS the integrity and confidentiality of the session and the login data are ensured. For information about activating HTTPS see *Activating HTTPS, p. 19*.

**Terminating a Session**

On a static web page the session is terminated (log out) after 10 minutes of inactivity or when the browser is closed. On a dynamic web page there is no automatic log out as long as the browser is active. Make sure to log out manually or to close the browser to log out if WEB-PLC programming page or event log is opened.

### 2.2.3 Password Protected Configuration

> HMS recommends exporting configuration files password protected. For security reasons exclude user credentials and access rights from the export.

The configuration file can optionally be secured with a password. If a configuration file is secured with a password, the configuration can only be imported after entering the password. For more information about the export and import of configurations see *Exporting and Importing a Configuration, p. 24*.

### 2.2.4 Restrictive Access Rights

> HMS recommends configuring access rights for each user as restrictive as possible.

It is possible to configure for each user different access rights for the different device functions. Make sure, that each user only has the access rights that are required to perform the tasks of their role to minimize security risks (principle of least privilege). For more information about the configuration of user accounts and access rights see *Changing Password and Access Rights, p. 22*.

### 2.2.5 Password Policy

> HMS recommends configuring the password policy according to the international password guideline NIST Special Publication 800-63.

> The password must be changed after the first login.

It is possible to define requirements for passwords that apply for all created users. To ensure that adequately strong passwords are used, the configuration of the password guideline should be based on the international password guideline NIST Special Publication 800-63. For more information about configuring user accounts and access rights see *Changing Password and Access Rights, p. 22*.

### 2.2.6 Firewall

> If device is connected directly to the internet (without router), the firewall must be enabled.

> HMS recommends using the device only in the local network and behind a firewall.

> For security reasons block communications ports that are not used.

The firewall improves the security of the device by analyzing network traffic and blocking unallowed traffic. The firewall has a blocking policy: outgoing connections are allowed while incoming connections are blocked except if a rule allows this specific connection.

Dynamic rules are created by the firewall for outgoing connections. Static rules allow access to a specific service on the device from the network. For more information about configuring the firewall see **WEB PLC Online Help – Settings – Network - Firewall**.

### 2.2.7 Firmware Updates

> HMS recommends to install always the latest firmware version to maintain device security.

The firmware is constantly improved and expanded. Firmware updates are encrypted and digitally signed by HMS to ensure the authenticity of the firmware version. For more information about updating the firmware see *Updating the Firmware, p. 19*.

### 2.2.8 Event Log

> The event log is cleared when the device is restarted and new events may overwrite older events once the ring buffer is completely filled. The events that are stored in the event log can be downloaded as csv file.

The event log is available in the WEB-PLC and includes security events like failed login attempts with timestamp, message and event type. For more information see *Diagnostics and Logging, p. 31*.

### 2.2.9 Disposal

> Make sure, that all sensitive data is removed from the device before decommissioning.

Follow the guidelines for secure, safe, and sustainable disposal of devices after use (see *Decommissioning and Disposal, p. 39*).

## 2.3 Intended Use

The components are used to connect MODBUS devices, energy communication systems and industrial equipment with each other and to SCADA or cloud systems. They are intended for installation on standard DIN rail and for use only in a restricted access area.

# 3 Scope of Delivery

Included in scope of delivery:

- SG-gateway
- Installation Guide *SG-gateway*
- Micro SD card
- 1 x power connector 3-pin
- 1 x CAN connector (CAN not supported by SG-gateway software)
- 1 x COM connector
- Multi I/O and Digital I/O variant: 1 x I/O connector
- Variants with WLAN: WLAN antenna

Dependent on variant and protocol further connectors may be included.

For variants with 3G or with 4G modem the antenna is not included. HMS offers a 3G/4G antenna with SMA connector.

# 4 Product Description

The SG-gateway family provides communication solutions for the energy infrastructure and the energy production for energy suppliers, system integrators, energy consumers and in transportation. The SG-gateway that is available in different variants provides safe and reliable communication between energy systems, control rooms and industrial automation systems.

> **!** Information in this document is about the hardware versions ASGxxx-C. Check the hardware version of the device in use on the product label. For information about another hardware, contact HMS Industrial Networks.

**Common Features**

- 1 x Ethernet 100/100 Mbit/s
- 1 x RS232/RS485 (switchable via software)
- Modbus-TCP Client/Server
- Modbus-RTU Master/Slave
- IEC 61850 Client/Server including GOOSE Subscriber and Publisher (optional)
- IEC 60870-5-104 Client/Server including support for Redundancy clients according to Norwegian user convention (optional)
- DNP3 outstation (optional)
- web based configuration via browser
- OPC-UA server
- MQTT publisher/subscriber
- Kolibri for connection to the optional HMS Hub IoT cloud
- Simple Network Management Protocol (SNMP)
- CODESYS network variables
- remanent variables
- timer functionality
- DHCP server
- Simple Network Time Protocol (SNTP)
- Network Address Translation (NAT)
- OpenVPN client
- Transport Layer Security (TLS)
- password protection, user and access rights management
- firewall supporting dynamic and static rules
- event log
- encrypted and signed firmware
- diagnostics (Pcap, Ping, DNS lookup etc.)
- export of configuration files with optional password protection
- Diagnosis (Pcap, Ping, DNS lookup etc.)

**Variant Dependent Features**

Different hardware device variants of the SG-gateway are available. Depending on the device variant the following features are available as option:

- 4-port Ethernet 100/100 Mbit/s switch as additional Ethernet interface
- Digital I/O: 4 x input, 4 x output
- Multi I/O: 8 x digital in/out, 8 x analog input
- EtherNet/IP adaptor
- PROFINET device
- PROFIBUS slave
- 3G/UMTS modem
- 4G/LTE modem (depending if version for Europe or for North America)
- WLAN modem

For protocol specific features see protocol specific Startup Guides on www.ixxat.com/sg-gw-download.

# 5 Installation

## 5.1 System Requirements

The WEB-PLC software runs on any up-to-date web browser on any PC operating system. The Ixxat Energy IP configurator, used to determine or configure the IP address of the device, runs on Windows.

The following features are needed on the local computer for the IP configuration:

- Ixxat Energy IP configurator, available on www.ixxat.com/sg-gw-download
- Ethernet network interface
- Microsoft Windows 7/10

*The IP address can also be determined with other IP/Mac scanners. If the IP address of the device is already known, the configuration can also be done in the WEB-PLC.*

The following features are needed on the local computer for the device configuration:

- Ethernet network interface and Ethernet connection to the device (local or internet)
- Java-script capable web browser
- recommended OS:
  - Windows 7/10
  - Linux Kernel 4.x or 5.x
  - MacOS X
- recommended web browser:
  - Mozilla Firefox 87 or higher
  - Google Chrome 89 or higher
  - Chromium browser 88 or higher
  - Apple Safari 14 or higher
  - Opera 75 or higher

### Firmware

The firmware is constantly improved and expanded. To configure the device the latest firmware must be downloaded on the device. For more information about updating the firmware see *Updating the Firmware, p. 19*.

### WEB PLC Help

After connecting the SG-gateway and accessing the Embedded Web server, the WEB PLC Online Help is available via the button in the WEB PLC.

## 5.2 Wireless via 3G or 4G Cellular Modem (Optional)

To use the wireless function a SIM card and an antenna must be installed and the cellular modem must be enabled. See WEB PLC Online Help **Settings — Network — Cellular Modem** for more information how to enable and configure the cellular modem.

### 5.2.1 Inserting the SIM Card

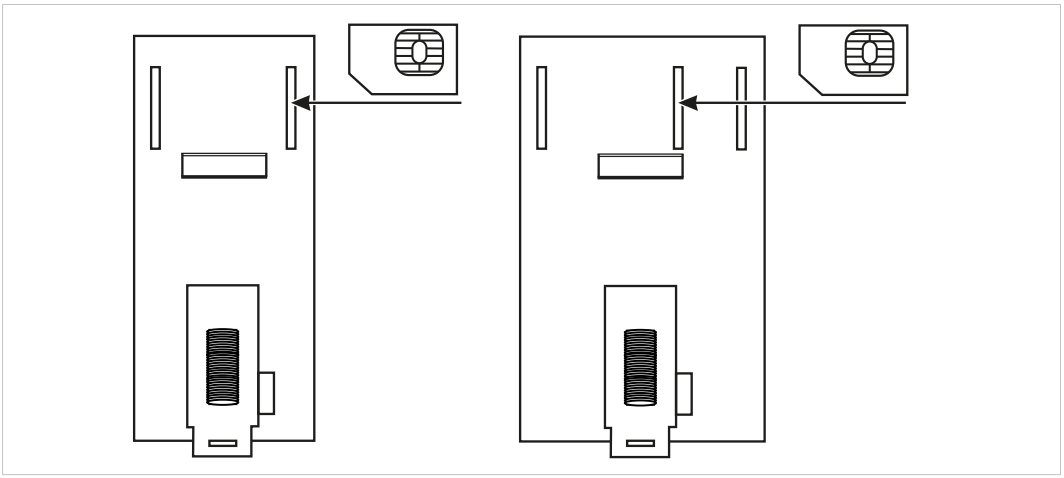


**Fig. 1 Inserting the SIM card in devices without 4-port switch and in devices with 4-port switch**

Only insert SIM card with format 2FF/UICC (mini SIM) into the device.

- ► Make sure, that the device is switched off.
- ► Insert the SIM card at the rear of the device.

> **!** Note that the slot is located differently depending on the device variant. On device variant without 4-port switch the SIM slot is located on the left, on device variants with 4-port switch the SIM slot is located in the middle.

- ► Push the SIM card until it locks.

### 5.2.2 Installing the Antenna

> Use antenna exclusively in areas where operation of wireless equipment is allowed.

> If antenna is installed outdoors, make sure to be in compliance of lightning protection standard VDE V0185.

> Modifications of antenna or connection such as extension cords may void the certification for the cellular modem for certain regions.

*For variants with 3G or with 4G modem the antenna is not included. HMS offers a 3G/4G antenna with SMA connector. Further accessories like extensions cables or outdoor antennas are also available from HMS.*

- Observe the EMC lightning protection zone concept.
- Make sure, that the antenna has at least 20 cm distance to persons or other antennas (recommended radiological limits).
- Make sure, that the device is switched off.
- Screw the antenna hand-tight on connector **Antenna**.

## 5.3 Connecting the Device to the Computer

- Connect Ethernet port (**ETH** or **ETH0**) of the device directly to the Ethernet port of the computer or via hub or switch.

## 5.4 Connecting the Power Connector

> Damaged device caused by reverse polarity or wrong power supply!
>
> Make sure that power is connected with correct polarity and that power supply is of recommended type.

> The device must be electrically grounded using a grounded safety low voltage circuit (PELV) for EMC compliance.

> Device goes in into safe mode if insufficient power is supplied! Make sure to connect sufficient power supply and current consumption (see *Technical Data, p. 38*).

The power supply must be a grounded circuit (PELV) and a 24 V DC ±15% regulated limited power source according to EN 62368-1, annex Q, or IEC/EN 60950-1, clause 2.5. The digital I/Os are provided with a detached anti-surge fuse of 4 A.

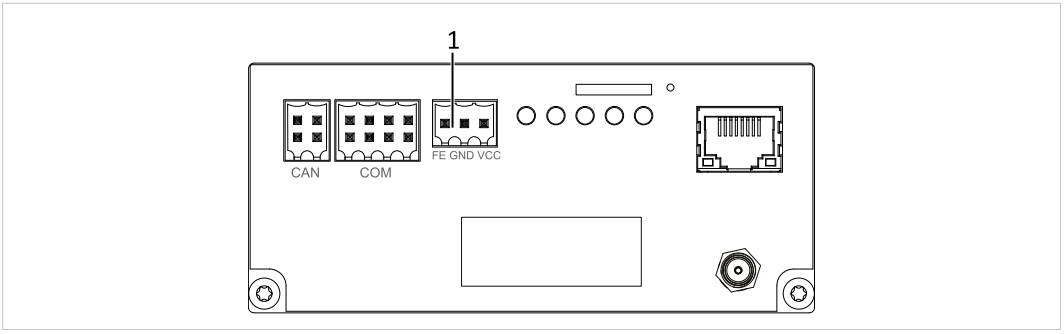



**Fig. 2 Power connector**

*For detailed description of connectors of the 4-port switch device variants see Fig. 17 Device overview 4-port witch variant, p. 34.*

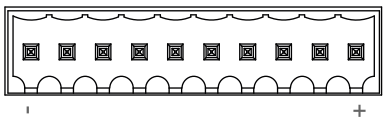
| Pin Allocation of Power Connector | |
|---|---|
| **Pin** | **Description** |
| FE | Functional earth |
| GND | Ground |
| VCC | 24 V DC |

*FE and GND are directly connected.*

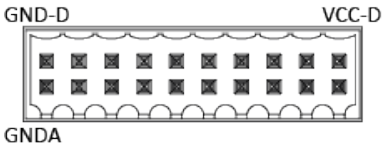
- Unplug the connector.
- Connect cables to the power connector.
- Plug the power connector to the power supply jack of the device (**1**).

## 5.5 Connecting I/O and Multi I/O Interfaces

When using the I/O interface or Multi I/O interface the interface must be connected to supply voltage.




**Pin allocation I/O interface**




**Pin allocation Multi I/O interface**

The power supply must be a 24 V DC ±15% regulated limited power source according to EN 62368-, annex Q, or IEC/EN 60950-1, clause 2.5.

### I/O Interface

- Apply voltage of 24 V (VCC) to the pin **+** of the interface.
- Apply ground to pin **–** of the interface.

### Multi I/O Interface

- Apply voltage of 24 V (VCC) to the pin **VCC-D** of the interface.
- Apply ground to pins **GND-D** and **GNDA** of the interface.

## 5.6 Mounting the Device

> Damage caused by overheating!
>
> Ensure adequate air circulation. Observe the recommended mounting distance.

> Use in dry rooms exclusively.

> The device must be electrically grounded through the DIN rail for EMC compliance. Make sure that the device is correctly mounted on the rail and the rail is properly grounded.

The device is designed for installation on a grounded 35 mm DIN rail. HMS recommends to mount the device vertically, i.e on a horizontal DIN rail.

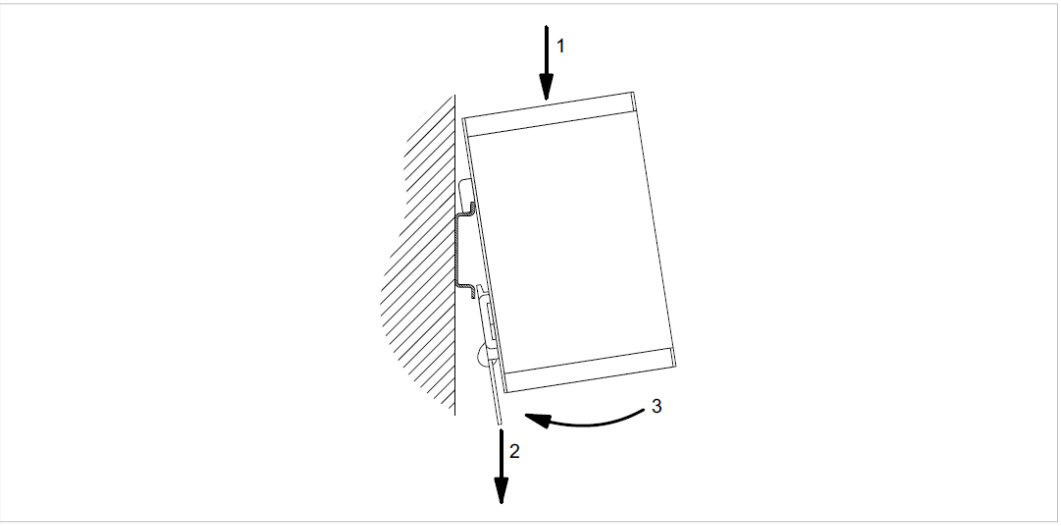



**Fig. 3 Mounting the device**

- Ensure adequate air circulation and observe the recommended mounting distance:
  - If venting slots are covered: 2 cm distance on top and bottom
  - If venting slots are covered about 50 %: 1 cm distance on top and bottom.
- Make sure, that the device is connected to power supply (see *Connecting the Power Connector, p. 13*).
- Make sure, that the device is connected to the computer (see *Connecting the Device to the Computer, p. 13*).
- Mount the device on the rail (**1**).
- Pull the tab downwards (**2**) and push the device towards the rail (**3**).
- Release the tab.
  - → After the installation the housing of the device is connected to functional earth.
- To remove the device, pull the tab downwards (**2**) to release the device from the rail.

## 5.7 Factory Reset

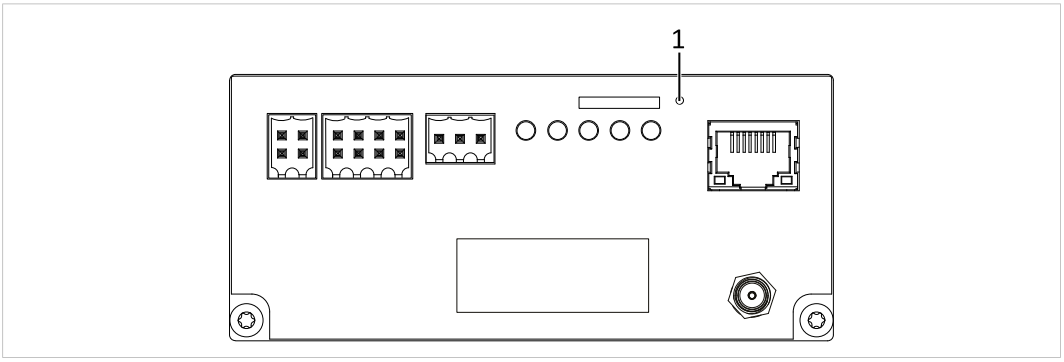



**Fig. 4 Reset the device**

*For detailed description of connectors of the 4-port switch device variants see Fig. 17 Device overview 4-port witch variant, p. 34.*

All settings are lost when device is reset.

- Disconnect the device from power supply.
- To restore the factory settings, press and hold the **Reset** button (**1**) with a pointed object.
- While holding the **Reset** button (**1**) connect the device to power supply.
- Hold the **Reset** button until all LEDs are flashing twice. This can take up to 15 seconds.
- Release the **Reset** button (**1**).
- Wait until the device is started up. Do not disconnect the power supply before the device is started up.

# 6 Configuration

## 6.1 Accessing the Device

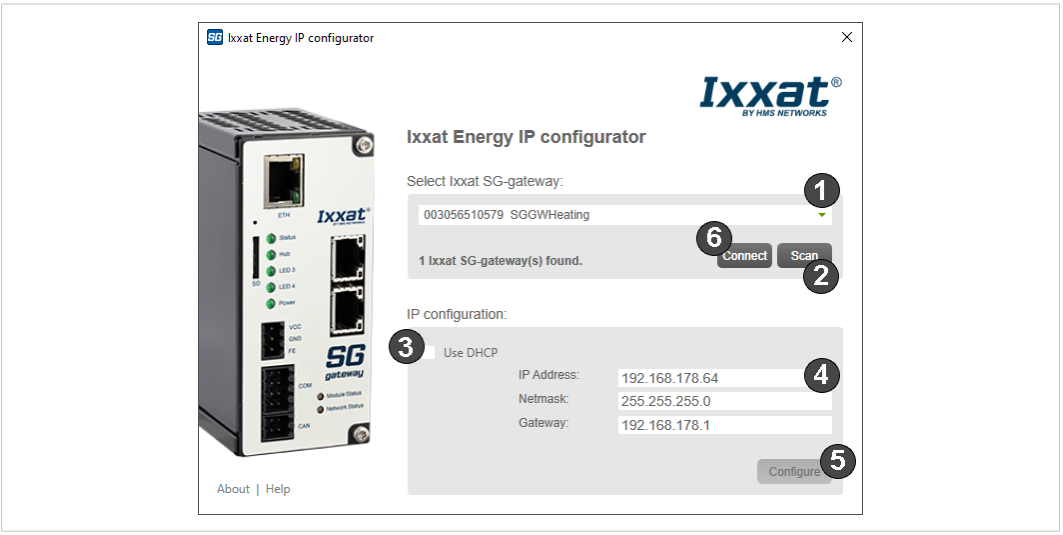



**Fig. 5 Ixxat Energy IP configurator**

*The IP address can also be determined with other IP/Mac scanners. If the IP address of the device is already known, the configuration can also be done in the WEB-PLC.*

- Connect the device to the computer (see *Connecting the Device to the Computer, p. 13*).
- Download the latest Ixxat Energy IP configurator from www.ixxat.com/sg-gw-download.
- Start Ixxat Energy IP configurator.
  - → Ixxat Energy IP configurator scans for SG devices on the local network.
  - → Found devices are shown in drop-down list (**1**).
- To identify the device, compare the number in the list (**1**) with the MAC on the label of the device.
- To rescan the network click button **Scan** (**2**).
- Select desired device in drop-down list (**1**).
  - → Current IP configuration of the device is displayed (**4**).
  - → By default the device tries to get an IP address from a DHCP server.
- Check if settings match the needs of the network.
- If necessary, use a static IP address:
  - Uncheck **Use DHCP** (**6**) and set the IP address manually (**4**).
  - Click button **Configure** (**5**).
  - In the opened popup enter username (default: ixxat) and password (default: ixxat) and click **OK**.
    - → If the configuration is successful, *Configuration completed* is shown.
- If desired device is selected and configured, click button **Connect** (**3**).
  - → Standard browser to access the WEB-PLC and to configure the device is opened (see *Accessing the Embedded WEB-PLC, p. 18*).

## 6.2 Accessing the Embedded WEB-PLC

- ► Enter IP address of the device in use into a web browser.
  - → Log in window is opened.
- ► Enter user name (default: ixxat) and password (default: ixxat).
  - → Home page of the WEB-PLC is opened.


**Fig. 6 Accessing the embedded WEB-PLC**

*Password has to be changed after first login (see Changing Password and Access Rights, p. 22).*

The home page shows the following information:

- overview of the device status
- current values of the I/Os
- information about device hardware and software
- information about special components such as the cellular modem or OpenVPN

- ► To configure the settings, click icon **Settings**.
  - → **Event Log** is opened, which displays all events (information messages, warnings and errors) generated by the device.
- ► For information about the protocol specific configuration see protocol specific Startup Guides on www.ixxat.com/sg-gw-download.
- ► For detailed information about the settings possibilities and event log messages open the **WEB-PLC Online Help** via button.
- ► To open the WEB-PLC editor, click button **Editor** (for more information see *WEB-PLC Editor, p. 26*).

## 6.3 Activating HTTPS

To increase the internet security, HMS recommends to activate HTTPS to access the WEB-PLC.

If the WEB-PLC is accessed with activated HTTPS the integrity and confidentiality of the session and the login data are ensured.

- Open the WEB-PLC (see*Accessing the Embedded WEB-PLC, p. 18*).
- Click icon **Settings** and open tab **Settings**.
- In the configuration tree select **Network**.

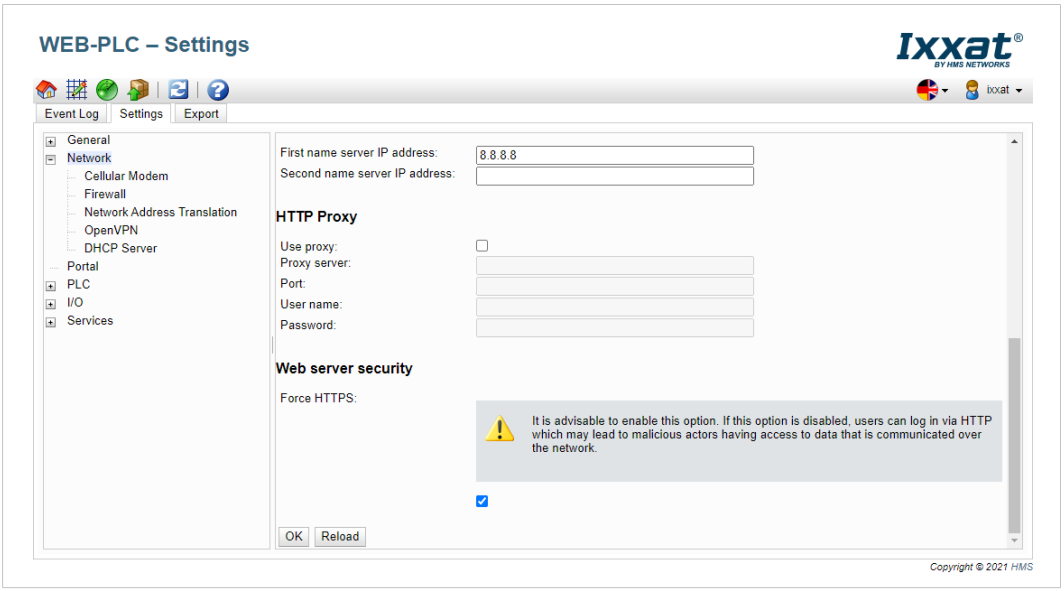



**Fig. 7 WEB-PLC network settings**

- In **Web server security** activate checkbox **Force HTTPS**.
- Click button **OK** and button **Reboot** to apply the changes.

## 6.4 Updating the Firmware

The firmware is constantly improved and expanded. To configure the device, the latest firmware must be downloaded on the device. For more information about updating the firmware see **WEB PLC Online Help — Update.**

> **!** Damaged device if ongoing firmware update is stopped or cancelled!
>
> Do not disconnect the power supply, reset the device or perform any other operations while the update is in progress. Firmware update can take up to 10 minutes.

> **!** The device restarts several times during the update and error messages may occur.

> **!** Risk of resetting the configuration!
>
> Identify the device and the device IP settings using the latest Ixxat IP configurator.
>
> Use an up to date browser version.

### 6.4.1 Saving Existing Configurations

HMS recommends to export and save existing configurations before updating the firmware as backup in case the configuration is reset during the update.

- Identify the device and the device IP settings using the latest Ixxat IP configurator (downloadable from www.ixxat.com).
- Use an up to date browser version (Firefox, Chrome, Chromium, MS Edge, or Apple Safari).
- Enter IP address of the device in use into a web browser.

  → Log in window is opened.
- Enter user name and password.

  → Home page of the WEB-PLC is opened.
- Click icon **Settings** and open tab **Export**.
- Export the existing device configuration.
- Check if the saved configuration is complete.
- Update the firmware online or offline.

### 6.4.2 Online Update

- Save existing configurations (see *Saving Existing Configurations, p. 20*).
- Identify the device and the device IP settings using the latest Ixxat IP configurator (downloadable from www.ixxat.com).
- Use an up to date browser version (Firefox, Chrome, Chromium, MS Edge, or Apple Safari).
- Enter IP address of the device in use into a web browser.

  → Log in window is opened.
- Enter user name and password.

  → Home page of the WEB-PLC is opened.
- To check the current firmware version, expand the list entry **Device Information**.

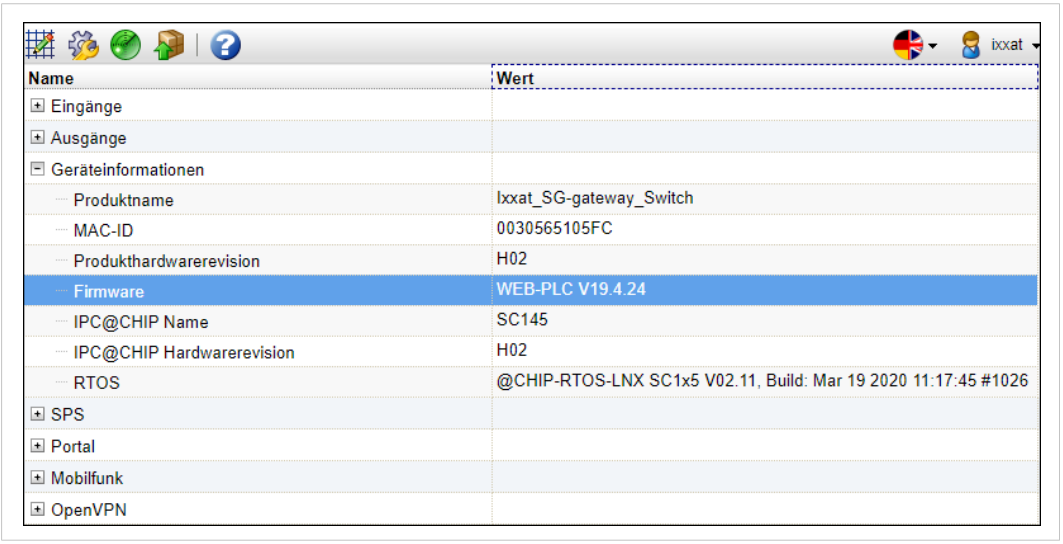



**Fig. 8 Home page**

- Check if newer version is available on www.ixxat.com/sg-gw-download.

- If newer version is available, download the firmware update zip file and extract for the firmware update cup file.
- If the firmware on the device is older than 19.3.32, update first to firmware version 19.3.32, and then to newer versions. Update to version 19.4.5 and newer is only possible from version 19.3.32 and newer.
- Make sure, that the SD card (minimum 500 MB free memory) is inserted before starting the device.

> **!** Upload may fail if SD card is inserted **after** the start-up of the device!
>
> If the SD card is inserted after the start-up of the device, reboot the device before updating.

- Click button **Update**  .
- Browse for the update package with button **Choose File**, select the desired file and click button **Start update**.
  - → Start-up directory is created on SD card.
  - → Device is programmed with the new software.
  - → When firmware is updated, a message is shown that includes a link to the index page.
- Do not disconnect the power supply, reset the device or perform any other operations while the update is in progress. Firmware update can take up to 10 minutes.
- To make sure, that the new version of the website is shown, clear the browser cache with **Ctrl + F5**.

### 6.4.3 Offline Update

Whether updating offline is allowed or not, can be configured in **Settings — Services — Update**.

> **!** If the firmware on the device is older than 19.3.32, update first to firmware version 19.3.32, and then to newer versions. Update to version 19.4.5 and newer is only possible from version 19.3.32 and newer.

If the update package is stored on the SD card and the cup file is extracted, updating is possible without access to the WEB PLC.

- Save existing configurations (see *Saving Existing Configurations, p. 20*).
- Make sure that the update package is named *update.cup* and stored in the *com.tom* directory on the SD card.
- Disconnect the device from power supply.
- Insert the SD card (minimum 500 MB free memory).
- Connect the device to power supply and start up the device.
- Press and hold the **Reset** button with a pointed object until all LEDs are flashing twice.
  - → This can take up to 15 seconds.
- Wait until the update is finished. Do not disconnect the power supply, reset the device or perform any other operations while the update is in progress. Firmware update can take up to 10 minutes.

## 6.5 Changing Password and Access Rights

It is possible to configure 8 different users with individual passwords and access rights, and to change the password policy. The password policy applies to all created users. For more information see **WEB PLC Online Help — Settings — Settings — General — User Management**.

As default user the user **ixxat** is configured (password: ixxat).

- Click icon **Settings** and select tab **Settings**.
- In configuration tree select **General — User Management**.

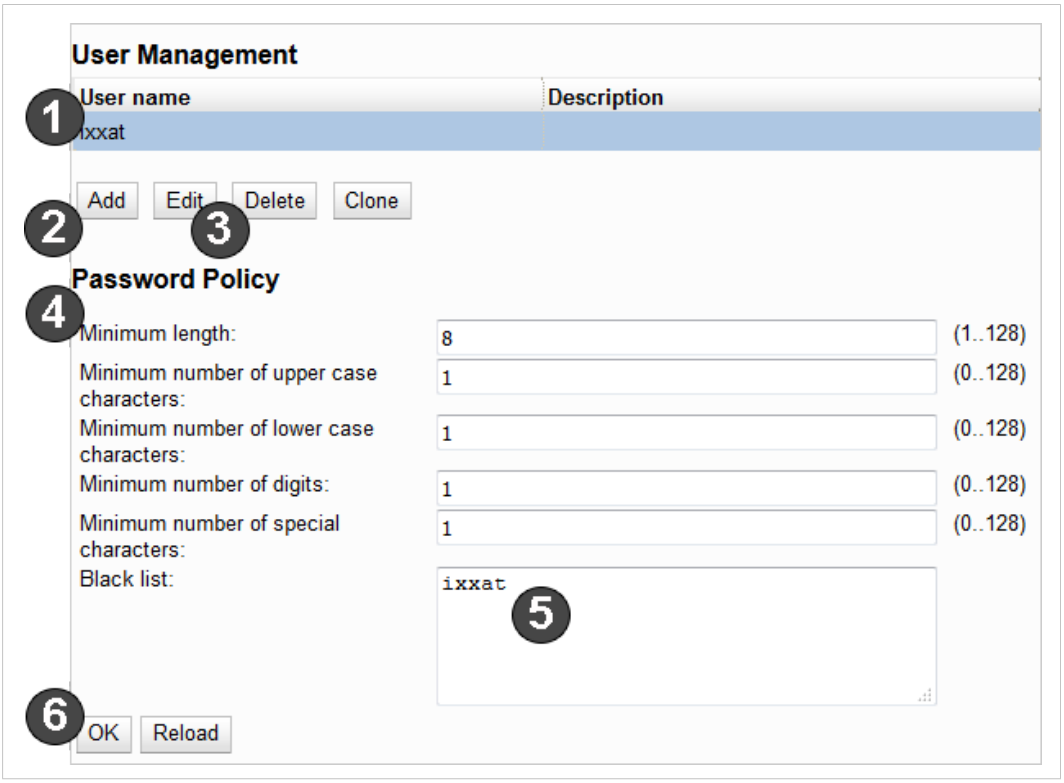



**Fig. 9 User management**

**To change the password of user *ixxat*:**

- Select **ixxat** in the user list (**1**), click button **Edit** (**3**).

  → Window **Edit user** is opened.
- Define a new password.
- If desired, change the user name and the access rights.
- Click button **OK**.

  → Window **Edit user** is closed.
- Click button **OK** (**6**) and button **Reboot** to apply the changes.

**To change the password policy:**

- Define the requirements for a password in the respective fields (**4**).
- To block a word as password, enter the word in the field **Black list** (**5**) (one password per line).
- Click button **OK** (**6**) and button **Reboot** to apply the changes.

**To add additional users:**

- Click button **Add** (**2**).
  → Window **Add user** is opened.
- Define a user name and a password.
- Define the access rights for the different device functions.
- Observe the distinction between the right to modify data or to only view data.
- Click button **OK**.
  → Window **Add user** is closed.
  → New user is entered in the list.
- Click button **OK** (**6**) and button **Reboot**  to apply the changes.

## 6.6 Exporting and Importing a Configuration

A configuration can be exported and packed into an update package. The update package can be imported to other SG-gateway devices.

- Make sure, that the SD card (minimum 200 MB free memory) is inserted.
- Click icon **Settings** and select tab **Export** (**1**).

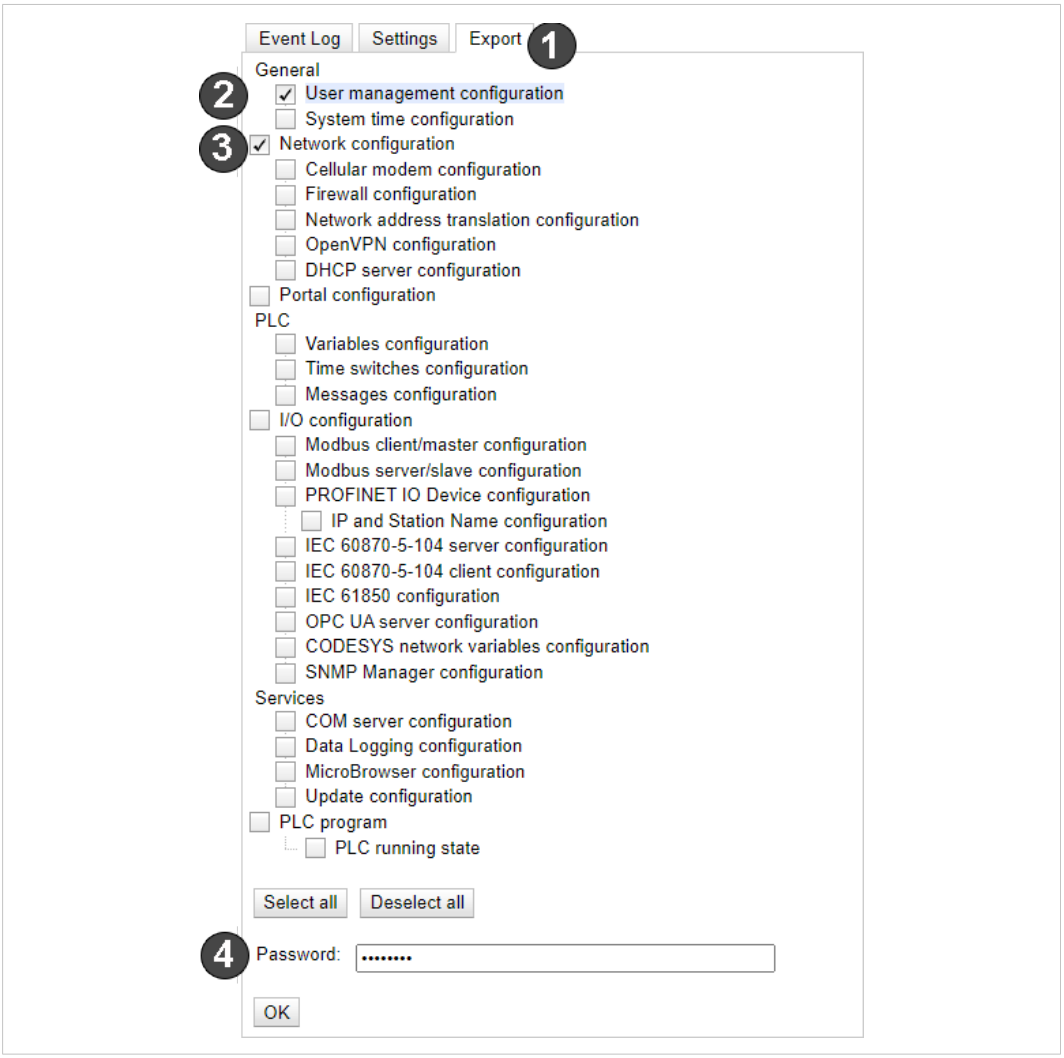



**Fig. 10 Export possibilities**

- Select the settings to be exported.
- Note, that if the user management settings (**2**) are contained in the export, the login settings of a device are changed when importing this package.
- Note, that if the IP settings are contained in the export (**3**), the IP address of a device may be changed when importing this package.
- To secure the configuration file with a password, define a password in field Password (**4**).
  - → If a password is defined, the configuration file can only be imported after entering this password.
  - → If field Password is empty, the configuration file is exported without password protection.

- ► Click button **OK**.

  → Update package is created.

- ► Download the update package.
- ► To import the configuration in the update package to another SG-gateway, update the device with the downloaded file (see *Online Update, p. 20*).
- ► If new protocol settings are imported, check if the PLC diagram is still valid in the WEB PLC editor.

> **!** All settings that are contained in the imported configuration overwrite the respective existing settings on the device. Existing configurations of other protocols and settings, that are not contained in the imported configuration are not deleted but remain.

# 7 WEB-PLC Editor

The WEB-PLC firmware provides an editor to edit the PLC program. The editor consists of two components: a diagram to connect, view and modify the inputs and outputs of the device via function blocks and I/O mapping to map inputs and outputs directly.

## 7.1 Creating an Application

The following example application of a timer shows how to create an application in the WEB-PLC editor. For descriptions of all available units see **WEB-PLC Online Help — WEB-PLC Editor — Diagram — Units**.

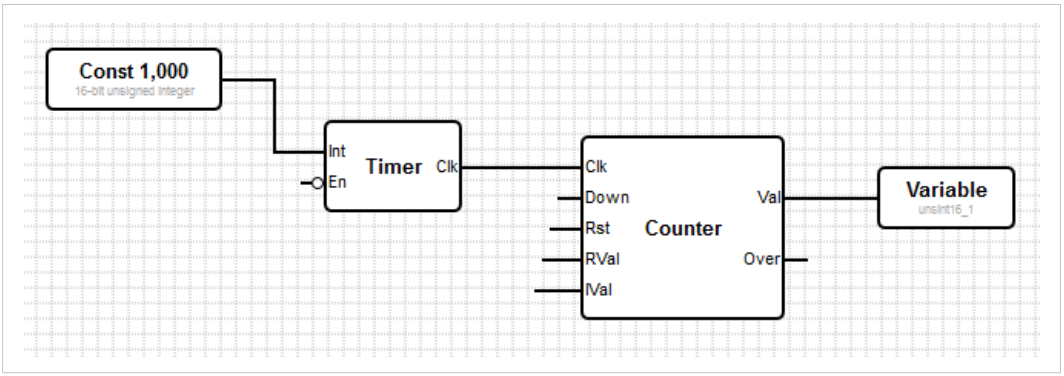



**Fig. 11 Example application**

- Click button **Editor**.
  → Tab **Diagram** is opened.
- To add a timer, click **Add unit** and select **Timing — Timer**.
  → Timer unit is added to the diagram.
- To add a counter, click **Add unit** and select **Numerical — Counter**.
  → Counter unit is added to the diagram.
- To add a constant, click **Add constant**.
  → Window **Define constant** is opened.
- Enter the desired value, select a data type and click button **OK**.
  → Constant unit is added to the diagram.
- To add a variable, click **Add variable**.
- Select **As output — portalvar0**.
  → Variable unit is added to the diagram.
- Rearrange units via drag and drop. The units should not overlap.
- To connect the units, click and hold the left mouse button when the cursor is over the port and drag the line that appears to the desired port.

► When the cursor is over the second port release the mouse button.

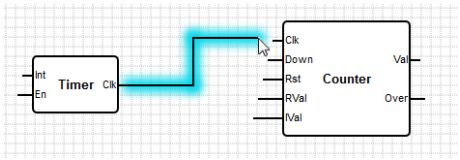



**Fig. 12 Connecting units**

► Connect the ports according to *Fig. 11 Example application*.

→ If ports with different data types are connected, the data type of the output is automatically converted to the data type of the input.

→ Port **En** of the unit timer is 0. Open input ports have value 0 by default.

► To activate the timer, double click on port **En**.

→ Port **En** is set to 1 (enabled) and timer is activated.

→ In the example the timer generates a clock signal with an interval of 1000 ms and the rising edge of the clock signal triggers the counter unit to increment its value.

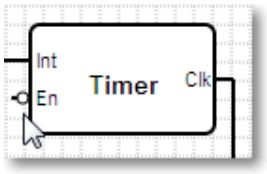



**Fig. 13 Enabled timer**

*Enabling the port by double clicking on the port is called negation. Negation is performed logically (value 0 is negated to 1, value unequal 0 is negated to 0, string results in an empty string). For more information see negation in **WEB PLC Online Help**.*

► To store the diagram on the device, click **Save program** .

→ Traffic light in toolbar changes from red to yellow.

→ PLC LED of the device, that indicates diagram execution is blinking

► To run the application, click **Start** .

→ Traffic light in toolbar changes to green.

→ PLC LED of the device, that indicates diagram execution is switched on.

→ Diagram is processed and the counter value increments.

## 7.2 Debugging

The current state of the variables and constants in the PLC can be checked directly in the diagram view via the Live View function.

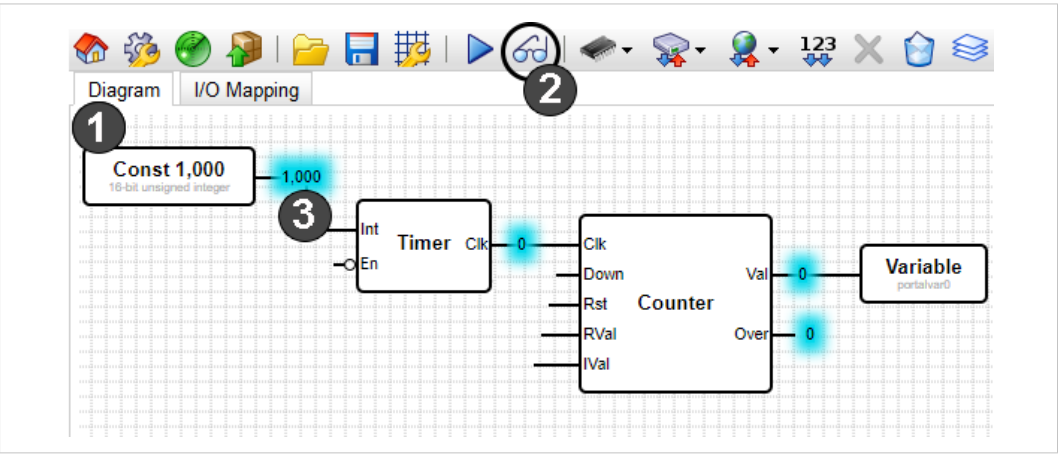



**Fig. 14 Live view**

- Click button **Editor** to open the WEB-PLC editor and open tab **Diagram** (**1**).
- To check the state of a configured PLC, click button **Start Live View** (**2**).
  - → Current value of each output port is shown next to the port in blue (**3**).
  - → Values are updated constantly.

> **!** Stop Live View before changing the diagram! If the PLC does not match the diagram, an error occurs and the Live View is stopped.

## 7.3 Mapping I/Os Directly

In the WEB-PLC editor inputs and outputs can be mapped directly via a mapping table. If inputs and outputs with different data types are mapped, the type is automatically converted.

- Click button **Editor** to open the WEB-PLC editor and open tab **I/O Mapping**.
- To add a mapping to the list, click button **Add** in the toolbar.
  - → Window **Add mapping** is opened.
- To select or enter an input, open combo box **Input**.
  - → Names of the I/Os are composed of the interface name, the device name and the value name.
  - → Variables contain the prefix *Variables*.
- In combo box **Output** select or enter an output.
- Click button **OK**.
  - → Mapping is entered in the list.
- To edit a mapping, click button **Edit** in the toolbar.
- To delete a mapping, click button **Delete** in the toolbar.
- For more information, open **WEB-PLC Online Help — WEB—PLC Editor — I/O Mapping**.

## 7.4 Configuring SMS Messaging

The SG-gateway with 3G/4G cellular modem is capable of sending and receiving short messages via the mobile network (SMS).

- Make sure, that the cellular modem is enabled.
- For information how to add messages, open **WEB-PLC Online Help — Settings — Settings — PLC — Messages**.

If messages are added in the settings:

- In the WEB-PLC editor add the unit **Send Msg 0** to the current application for each configured send message.
  - → **Send Msg 0** transmits the first configured message when its transmitting trigger input port (**Snd**) receives a high signal (1).
- In the WEB-PLC editor add the unit **Recv Msg 0** to the current application for each added receive message.
  - → **Recv Msg 0** puts out a high signal (1) on its output port when the first configured message is received.
- To send a message every time the receive message is processed, connect **Send Msg 0** and **Recv Msg 0**.

## 7.5 Configuring MQTT Messages

The SG-gateway supports MQTT v3.1.1 and can act as publisher and as subscriber. To be able to exchange messages via MQTT a broker must be configured.

> **!** MQTT is an open and unprotected protocol and third parties can read the transmitted messages if a public broker is used. HMS recommends to use TLS to prevent transmitting data in clear type.
>
> Note that the default host port depends on the TLS settings and that some brokers need TLS with a specific port to establish a communication.

> **!** Note that the SG-gateway only receives messages that have the same topic and the same data as defined in the WEB-PLC in the SG-gateway MQTT receive message list.

- Enable MQTT in the WEB-PLC in **Settings — PLC — Messages**.
- For information how to add messages, open **WEB-PLC Online Help — Settings — Settings — PLC — Messages**.

TheSG-gateway only receives messages if the receive message is added to the **Receive message list** (with same topic and content) and if the respective unit is added to the WEB-PLC diagram.

If messages are added in the settings:

- In the WEB-PLC editor add the unit **Send Msg 0** to the current application for each configured send message.
  - → **Send Msg 0** transmits the first configured message when its transmitting trigger input port (**Snd**) receives a high signal (1).
- In the WEB-PLC editor add the unit **Recv Msg 0** to the current application for each added receive message.
  - → **Recv Msg 0** puts out a high signal (1) on its output port when the first configured message is received.

For more information about the MQTT configuration and security options when publishing to the cloud see Startup Guide *SG-gateway How to Use MQTT and SMS Messages* on www.ixxat.com.

# 8 Diagnostics and Logging

## 8.1 Event Log

System events are logged to a ring buffer in RAM with timestamp, message and event type. When the ring buffer is full old events are overwritten and the event log is emptied when the device is restarted. For detailed information about the event log see **WEB-PLC Online Help — Settings — Event Log** via button .

- Click icon **Settings** .
  - → Event Log is opened.
  - → Event messages consisting of message text, timestamp and event type are shown.
  - → Timestamps are displayed in the time zone of the SG-gateway.

> **!** If the system clock of the SG-gateway is not synchronized, the timestamps are not displayed correctly.

- For more information about a message click on the message text.
  - → WEB-PLC online help with detailed information about the respective message is opened.

## 8.2 Diagnostics Console

The WEB-PLC provides a diagnostics console to check via various commands if the device is working correctly and to get additional information in case of issues. For detailed information about the command options see **WEB-PLC Online Help — Diagnostics — Diagnostics Console** via button .

> Commands cannot be executed simultaneously. Execute the commands one by one.
>
> Exception: Sniff commands run in the background and other commands can be started simultaneously.

► To open the diagnostics console, click button **Diagnostics** .

→ Diagnostics console with a tab for each possible command is opened.

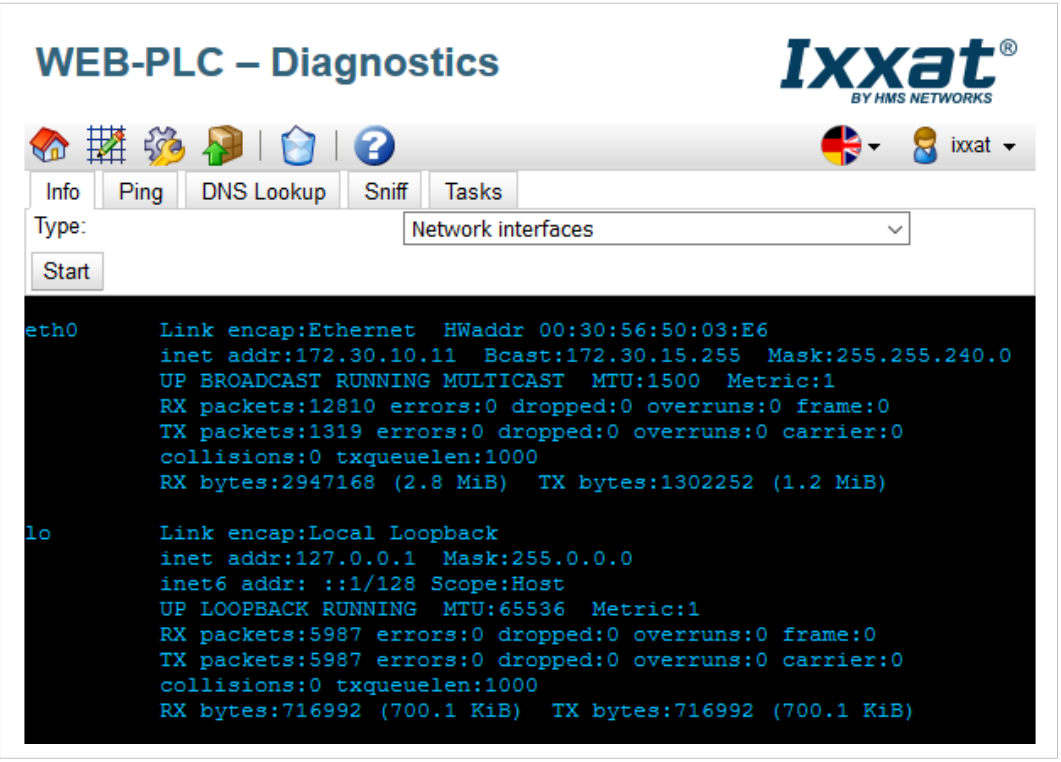



**Fig. 15 Diagnostics console**

► Select the tab of the desired command.

| | |
|---|---|
| **Info** | Shows information about the available network, the routing table, or the DNS configuration. |
| **Ping** | Transmits ping packages to another host in the network and evaluates the answer. |
| **DNS Lookup** | Tries to resolve a host name into an IP address. |
| **Sniff** | Captures network packages and stores the packages temporarily on the SD card. When finished the created *.cap* file is automatically downloaded and can be opened with the program *Wireshark* for example. A separate file is created for each network interface. |
| **Task** | Shows information about the RTOS and Linux tasks that are running inside the system. |
| **Database** | Shows information about the database that is running in the system. |

- For sniffing command make sure, that the SD card (minimum 200 MB free memory) is inserted.

> ! If the SD card memory is full, no logging data is written to the SD card.

- Configure the command options and click button **Start**.
  → Results are shown in the diagnostics console.

## 8.3 Data Logging

With Data Logging values can be stored in the WEB-PLC database and exported as *.csv* file. For detailed information see **WEB-PLC Online Help — Settings — Settings — Services — Data Logging** via button .

> ! If the SD card memory is full, no logging data is written to the SD card.

- Make sure, that the SD card (minimum 200 MB free memory) is inserted.
- Click icon **Settings** and select tab **Settings**.
- In configuration tree select **Services — Data Logging**.
- To define a value to be stored in the database, add an element to the data logging list.
- To add an element, click button **Add**.
  → Window **Edit Element** is opened.
- Configure the element settings.

| **Element Settings** | |
|---|---|
| **Name** | Description of the corresponding database entry |
| **Element** | Value to be stored in the database |
| **TriggerMode** | Mode how the storage of values is triggered (cyclic or deadband). |
| **Cycle** | Used if trigger mode is cyclic: cycle time in seconds |
| **Deadband** | Used if trigger mode is deadband: new value is only stored if the difference to the last stored value is equal or lager than the deadband. |

- Click button **OK**.
  → Window **Edit Element** is closed.
  → Element is entered in the list.
- To edit an element, select the element in the list and click button **Edit**.
- Click button **OK** and button **Reboot** to apply the changes.
- To export the stored values to a comma separated .csv file, click button **Start Export**.

> *If the checkbox **Erase all entries in next startup** is deactivated, all configurations and values are retained and can be exported.*

# 9 Operation

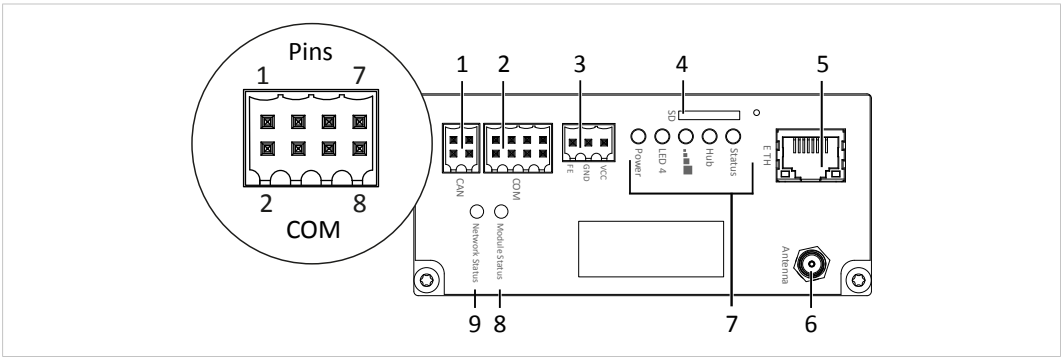



**Fig. 16 Device overview**

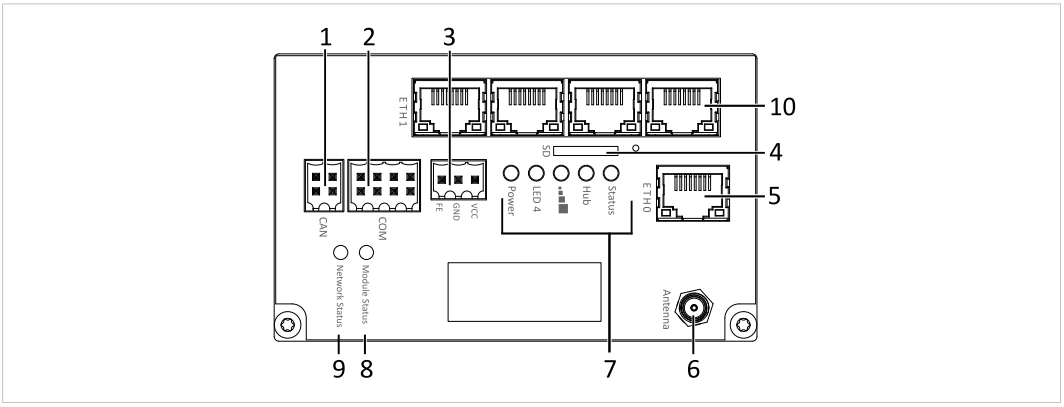



**Fig. 17 Device overview 4-port witch variant**

| | |
|---|---|
| 1 | CAN interface (not supported) |
| 2 | Serial interface RS232/RS485 |
| 3 | Power connector |
| 4 | Micro SD slot |
| 5 | Ethernet interface |
| 6 | Antenna connector (only in version with modem) |
| 7 | LED array |
| 8 | Module Status LED (only with variants PROFINET, PROFIBUS and EtherNet/IP) |
| 9 | Network Status LED (only with variants PROFINET, PROFIBUS and EtherNet/IP) |
| 10 | 4-port switch (only witch 4-port switch variants) |

## 9.1 Serial Interface (COM)

The serial interface is only used for Modbus RTU.

There are no resistors for line polarization in the device. The device itself does not need line polarization.

If a device in RS485 mode is last in line in the bus topology a termination is required. To activate the internal termination resistor of the device, connect pin 5 and pin 7.

**Pin Allocation RS232/RS485**

| Pin | Signal |
|---|---|
| 1 | GND |
| 2 | CTS |
| 3 | B |
| 4 | TXD |
| 5 | A |
| 6 | RTS |
| 7 | TERM_B |
| 8 | RXD |

## 9.2 Ethernet Interface

| | |
|---|---|
| Green LED | Activity indication |
| Yellow LED | Connection indication |

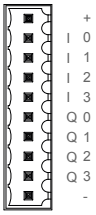
## 9.3 Digital I/O Interface

Only available with the I/O device variant.

**Digital I/Os**

| | |
|---|---|
| + | 24 VDC IN |
| I0-I3 | Digital pulse input, sink |
| Q0-Q3 | Digital output, source |
| - | Ground |

**I/O interface**




The power supply must be a 24 V DC ±15% regulated limited power source according to EN 62368-, annex Q, or IEC/EN 60950-1, clause 2.5.

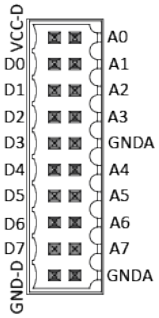
> **!** Make sure, that voltage (24 V) is applied to pin **+** and ground to pin **-** (see *Connecting I/O and Multi I/O Interfaces, p. 14*).

## 9.4 Multi I/O Interface

Only available with the Multi I/O device variant.

| Multi I/Os | |
|---|---|
| GNDA | Ground |
| A0 - A7 | Analog input |
| D0 - D7 | Digital I/O (usable as input and output) |
| VCC-D | 24 VDC IN |
| GND-D | Ground |

**Multi I/O interface**




The power supply must be a 24 V DC ±15% regulated limited power source according to EN 62368-, annex Q, or IEC/EN 60950-1, clause 2.5.

> **!** Make sure, that voltage (24 V) is applied to pin **VCC-D** and ground to pins **GND-D** and **GNDA** (see *Connecting I/O and Multi I/O Interfaces, p. 14*).

## 9.5 LEDs

### 9.5.1 Status LED

The Status LED indicates the status of the PLC.

| LED | Description |
|---|---|
| Off | No program loaded, PLC not running |
| Slowly blinking (0.5 Hz) | Program loaded, PLC not running |
| On | Program loaded, PLC running |
| Fast blinking (4 Hz) | Task cycle of PLC violated (e.g. cycle time too short in relation to complexity of program, check duty cycle of PLC in status bar of editor), see **WEB-PLC-Help — Status LEDs** for more information |

### 9.5.2 Hub LED

The Ixxat SG-gateway supports the use of the HMS Hub. The Hub LED indicates the status of the HMS Hub connection. For further information see **WEB-PLC-Help — Status LEDs**.

### 9.5.3 Radio LED/LED3

The LED is named differently depending on the device variant.

In device variants with radio modems (WLAN, 3G and 4G) the Radio LED indicates the status of the radio modem connection.

In device variants without modem the LED 3 has no function.

*On legacy product labels the Radio LED may be labelled as GSM LED.*

| LED | Description |
|---|---|
| Off | Connection is not enabled. |
| Slowly blinking (0.5 Hz) | Connection is being established. |
| On | Connection is established. |

### 9.5.4 Power LED

| LED | Description |
|---|---|
| Off | Device not supplied with power |
| On | Device is supplied with power |

### 9.5.5 Module Status LED

The Module Status LED is only available with device variants PROFINET, PROFIBUS and EtherNet/IP. See protocol specific Startup Guides on www.ixxat.com/sg-gw-download for more information.

### 9.5.6 Network Status LED

The Network Status LED is only available with device variants PROFINET, PROFIBUS and EtherNet/IP. See protocol specific Startup Guides on www.ixxat.com/sg-gw-download for more information.

# 10 Technical Data

| | |
|---|---|
| CPU | IPC@CHIP® SC145, i.Mx6, 32-bit processor with 528 MHz, 128 MB RAM (DDR3), 64 MB flash disk |
| Real-time clock | Backed by a lithium rechargeable battery |
| Supply voltage | 24 VDC (±15 %), Weidmüller BL 3.50/03 connector (regulated, limited power source) |
| Current consumption | Typ. 100 mA/24 V DC<br>Max. 250 mA/24 V DC |
| Operating temperature | 0 °C to +55 °C |
| Operational altitude | Max. 5000 m |
| Humidity range | 5-85 % RH, non-condensing (IEC 60068-2-30) |
| Dimensions (W x L x H) | 84 x 46 x 107 mm<br>4-port switch device variants: 84 x 65 x 107 mm |
| Weight | 350 g to 480 g depending on device variant |
| Housing material | Powder-coated steel sheet, RAL 7021, dull finish |
| Pollution degree | 3 |
| Ethernet interface | 10/100 BaseT, RJ45, link and traffic LED indicators |
| Serial interface | 1 x RS232/RS485 (selectable), Weidmüller BL 3.50/08 connector |
| SD card interface | microSD card SD/SDHC, push/push slot, max. 32 GB |

| **OPC-UA Server** | |
|---|---|
| Device profile | Micro Embedded Device Server Profile |
| User Token | User Name Password Server Facet |
| Security Policies | None, Basic128Rsa15, Basic256Sha256 |
| Protocol and encoding | UA-TCP, UA-SC, UA-Binary protocol and encoding |
| Data change notification | Embedded DataChange Subscription Server Facet profile |
| Protocol restrictions | Up to 128 groups, 4096 values, 8192 scalar values or array elements,<br>up to 4 concurrent client sessions |

| **MQTT** | |
|---|---|
| Protocol version | 3.1 and 3.11 |
| Encryption | TLS, Client-certificates |
| Templates | Flexible for own definition of payloads |
| Features | Last will, QoS, Keep alive interval |

| **Software** | |
|---|---|
| Operating system | IPC@CHIP® RTOS-LNX Real-time operating system |
| WEB-PLC editor and runtime | Visual programming editor running on the internal web server, quick I/O mapping editor, up to 8192 I/O values, up to 1024 HMS Hub variables |
| WEB-PLC diagram | Up to 2048 function units, I/O values, HMS Hub variables and constants, IPO cycle time: 10 to 1000 ms |

For information about the different device variants see the Ixxat SG-gateway datasheets.

| **Protocol Specific Restrictions** | |
|---|---|
| IEC 60870–5–104 | Client: up to 32 devices and 512 values (up to 1024 values including array members)<br>Server: up to 512 values (up to 1024 values including array members) |
| IEC 61850 | Client: up to 32 devices and 512 values (up to 1024 values including array members)<br>Server: up to 512 values (up to 1024 values including array members) |
| DNP3 | Outstation: up to 4 connections and 512 values (up to 1024 values including array members) |

# 11 Support/Return Hardware

## 11.1 Support

- To contact support, go to www.ixxat.com/technical-support/contact-technical-support.
- Scroll down and click button **mysupport.hms.se** to register a support case.

## 11.2 Return Hardware

- On www.ixxat.com/support/product-returns click button **Portal** to access the support portal.
- In the support portal select **Submit Product Return (RMA)**.
- Read the information and click **Create RMA Case**.
- Register a support account and sign in.
- Fill in the form for warranty claims and repair.
- Print out the Product Return Number (PRN resp. RMA).
- Pack product in a physically- and ESD-safe way, use original packaging if possible.
- Enclose PRN number.
- Observe further notes on www.ixxat.com.
- Return hardware.

# 12 Decommissioning and Disposal

> **!** Make sure, that all sensitive data is removed from the device before decommissioning.

To remove all sensitive data from the device:

- Perform a factory reset (see *Factory Reset, p. 16*).
- Remove all sensitive data from the SD card.
- Decommission the device.
- Dispose the device and the AD card separately according to national laws and regulations.
- Observe further notes about disposal of products on www.ixxat.com.

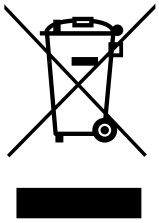
This page intentionally left blank

# A Regulatory Compliance

## A.1 EMC Compliance (CE)

The product is in compliance with the Electromagnetic Compatibility Directive. More information and the Declaration of Conformity is found at www.ixxat.com.

## A.2 Disposal and recycling



You must dispose of this product properly according to local laws and regulations. Because this product contains electronic components, it must be disposed of separately from household waste. When this product reaches its end of life, contact local authorities to learn about disposal and recycling options, or simply drop it off at your local HMS office or return it to HMS.

For more information, see www.hms-networks.com.

## A.3 ROHS and REACH

HMS standard products are RoHS compliant.

HMS products do not contain any of the banned substances defined in the REACH SVHC list in higher amounts than the specified limits.

The declaration of conformity and more information about HMS sustainability processes and goals can be found on www.hms-networks.com.

# B UL Ordinary Locations (OrdLoc)

SG-gateway devices are certified for use in ordinary locations in compliance with the following standards:

- UL 61010-1 SAFETY REQUIREMENTS FOR ELECTRICAL EQUIPMENT FOR MEASUREMENT, CONTROL, AND LABORATORY USE - PART 1: GENERAL REQUIREMENTS - Edition 3 - Revision Date 2016/04/29
- UL 61010-2-201 STANDARD FOR SAFETY REQUIREMENTS FOR ELECTRICAL EQUIPMENT FOR MEASUREMENT, CONTROL, AND LABORATORY USE - PART 2-201: PARTICULAR REQUIREMENTS FOR CONTROL EQUIPMENT - Edition 2 - Issue Date 2018/05/14
- CSA C22.2 NO. 61010-1-12 SAFETY REQUIREMENTS FOR ELECTRICAL EQUIPMENT FOR MEASUREMENT, CONTROL, AND LABORATORY USE. PT. 1, GENERAL REQUIREMENTS - Edition 3 - Revision Date 2016/04/29
- CSA C22.2 NO. 61010-2-201:14 SAFETY REQUIREMENTS FOR ELECTRICAL EQUIPMENT FOR MEASUREMENT, CONTROL, AND LABORATORY USE - PART 2-201: PARTICULAR REQUIREMENTS FOR CONTROL EQUIPMENT - Edition 2 - Issue Date 2018/02/01

The certification number of the certified devices according to OrdLoc certification is:

- E214107

According to the standards listed above, the devices are certified with the following marking:


**Intended Use**

SG-gateways are used to connect MODBUS devices, energy communication systems and industrial equipment with each other and to SCADA or cloud systems. They are intended for installation on standard DIN rail.

| | |
|---|---|
| ! | Risk of interference if used with antenna (wireless)!<br>In case of interference install device or antenna in other location. |

| | |
|---|---|
| ! | Use antenna exclusively in areas where operation of wireless equipment is allowed.<br>If antenna is installed outdoors, make sure to be in compliance of lightning protection standard VDE V0185.<br>Modifications of antenna or connection such as extension cords may void the certification for the cellular modem for certain regions. |

| | |
|---|---|
| ! | Use in dry rooms exclusively. Protect product from moisture and humidity.<br>Protect product from too high or too low temperature, and from fire. |

| | |
|---|---|
| ! | Damaged device caused by reverse polarity or wrong type of power supply!<br>Make sure that power is connected with correct polarity and that power supply is of recommended type. |

| | |
|---|---|
| ! | The equipment must be electrically grounded through the DIN rail for EMC compliance. Make sure that the equipment is correctly mounted on the rail and that the rail is properly grounded. |

**Utilisation prévue**

Les SG-gateways sont utilisées pour connecter des appareils MODBUS, des systèmes de communication appliqués à l'énergie et des équipements industriels entre eux et à des systèmes SCADA ou cloud. Ils sont destinés à être installés sur un rail DIN standard.

> **!** Risque d'interférence en cas d'utilisation avec une antenne (sans fil) !
>
> En cas d'interférence, déplacez l'appareil ou l'antenne à un autre endroit.

> **!** L'antenne ne doit être utilisée que dans les zones où l'utilisation d'équipements sans fil est autorisée.
>
> Si l'antenne est installée à l'extérieur, vérifiez la conformité à la norme VDE V0185 sur la protection contre la foudre.
>
> Toute modification de l'antenne ou connexion d'une rallonge, par exemple, peut rendre la certification pour le modem cellulaire invalide dans certaines régions.

> **!** L'utilisation doit être limitée aux pièces sèches. Protégez le produit de l'humidité.
>
> Le produit ne doit pas être soumis à des températures extrêmes et doit être protégé contre tout risque d'incendie.

> **!** Dommages sur l'appareil provoqués par une inversion de polarité ou un mauvais type d'alimentation !
>
> Lors de la connexion, vérifiez que la polarité est correcte et que l'alimentation est du type recommandé.

> **!** Les équipements doivent être mis à la masse via le rail DIN pour assurer la conformité CEM (compatibilité électromagnétique). Vérifiez que les équipements sont correctement montés sur le rail et que celui-ci est bien mis à la masse.

# C Open Source Software

The software of the Ixxat SG-gateway contains software components that are licensed as Free Software or Open Source Software by the rights holders. The corresponding licenses are available on the support area of the SG-gateway on www.ixxat.com. (Included in Firmware Download Package as well as included in Offline Help Package). You may obtain the complete corresponding source code of the software components from us on a data carrier and within three years as of the distribution of the software by us or at least for as long as we offer support and spare parts for the software, if you make a request to HMS Industrial Networks AB at the following address:

HMS Industrial Networks AB
Box 4126
SE-300 04 Halmstad
Sweden

The source code is also available at the support area of the SG-gateway on www.ixxat.com.

Box 4126
300 04 Halmstad, Sweden

info@hms.se
4.01.0402.20000 1.7 en-US / 2021-05-12 / 22403