



User manual
netPi
NOIT-E-NPI3-51-EN-RE



Hilscher Gesellschaft für Systemautomation mbH
www.hilscher.com

DOC170801UM01EN | Revision 1 | English | 2017-09 | Released | Public

Table of contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 4 |
| 1.1 | About the user manual | 4 |
| 1.2 | List of revisions | 4 |
| 1.3 | Further sources of information | 4 |
| 2 | Brief description | 5 |
| 3 | Device drawings | 6 |
| 3.1 | Positions of the interfaces | 6 |
| 3.2 | Dimensions | 8 |
| 4 | Connectors and mounting | 9 |
| 4.1 | Mounting | 9 |
| 4.2 | Power supply..... | 9 |
| 4.3 | LAN connectors..... | 9 |
| 4.4 | Real-Time Ethernet connectors | 9 |
| 4.5 | USB connectors | 9 |
| 4.6 | Wi-Fi..... | 10 |
| 4.7 | HDMI connector | 10 |
| 4.8 | Slot for expansion modules..... | 10 |
| 5 | LEDs | 11 |
| 5.1 | Positions of the LEDs on the gateway | 11 |
| 5.2 | Gateway status LEDs..... | 12 |
| 5.3 | LEDs of the LAN interface..... | 13 |
| 5.4 | LEDs of the PROFINET IO Device interface..... | 14 |
| 5.5 | LEDs der EtherCAT Slave interface..... | 15 |
| 5.6 | LEDs of the EtherNet/IP Adapter interface | 16 |
| 6 | Commissioning the Edge Gateway | 17 |
| 6.1 | Establishing the IP address communication | 17 |
| 6.2 | Using the web browser to establish a connection with the Edge Gateway | 18 |
| 6.2.1 | Using the host name | 18 |
| 6.2.2 | Access to the Edge Gateway in the Windows network environment | 19 |
| 7 | Edge Gateway manager | 20 |
| 7.1 | Calling the Edge Gateway Manager | 20 |
| 7.2 | Edge Gateway manager web page..... | 21 |
| 8 | Control Panel | 22 |
| 8.1 | Opening the control panel | 22 |
| 8.1.1 | First login | 23 |
| 8.1.2 | Secure connection | 24 |
| 8.2 | Control Panel commands..... | 28 |
| 8.2.1 | Overview and main menu | 28 |
| 8.2.2 | System information and system time | 29 |
| 8.2.3 | Packet management | 34 |

| | | |
|-----------|---|-----------|
| 8.2.4 | Network..... | 35 |
| 8.2.5 | Services | 37 |
| 8.2.6 | User management | 38 |
| 8.2.7 | Security certificates..... | 41 |
| 8.2.8 | Help..... | 44 |
| 8.2.9 | Session | 44 |
| 9 | Isolated application execution with Docker | 46 |
| 9.1 | Docker, image, and container | 46 |
| 9.2 | Container for netPI: Examples | 48 |
| 9.3 | Working with Docker via the web GUI..... | 49 |
| 9.3.1 | The portainer.io interface | 49 |
| 9.3.2 | Example: Executing the web server NGINX as a container..... | 52 |
| 10 | Technical data | 54 |
| 10.1 | Technical data NIOT-E-NPI3-51-EN-RE..... | 54 |
| 11 | FCC authorization | 56 |
| 12 | Decommissioning, dismantling and disposal | 57 |
| 12.1 | Putting the device out of operation..... | 57 |
| 12.2 | Removing device from top hat rail..... | 57 |
| 12.3 | Disposal of waste electronic equipment..... | 57 |
| 13 | Appendix..... | 58 |
| 13.1 | Legal notes..... | 58 |
| | List of figures | 62 |
| | List of tables..... | 63 |
| | Contacts..... | 64 |

1 Introduction

1.1 About the user manual

This user manual describes the installation, configuration and functionality of the device NIOT-E-NPI3-51-RE-EN.

In this description, the device NIOT-E-NPI3-51-RE-EN is named **netPI** and **Edge Gateway** likewise. The name **netPI** is in reference to the Raspberry Pi function and **Edge Gateway** is in reference to the use on the "Edge" between the IT network and the OT network.

1.2 List of revisions

| Revision | Date | Author | Change |
|----------|------------|--------|-----------------------|
| 1 | 2017-09-18 | HH, RG | All sections created. |

Table 1: List of revisions

1.3 Further sources of information

The following table lists web addresses where you can get further information for netPI.

| Web address | This site offers you |
|---|---|
| https://www.netiot.com/netPI | Product presentation, documentation, tutorials, informationen on expansion modules, blog, FAQ, and forum on netPI and IIoT. |
| https://hub.docker.com/r/hilschernetpi/ | Docker hub with example images for netPI. |
| https://www.raspberrypi.org/ | Information, blog, downloads, community, forum, and education on Raspberry Pi. |

Table 2: Further information

2 Brief description

netPI is a Raspberry Pi 3 architecture based platform for implementing Cloud, Internet of Things and Industry 4.0 customized Edge Automation projects safely. The device contains the original Raspberry Pi 3 circuitry along with Hilscher's multiprotocol chip netX and thus supports popular Real-Time Ethernet networks.

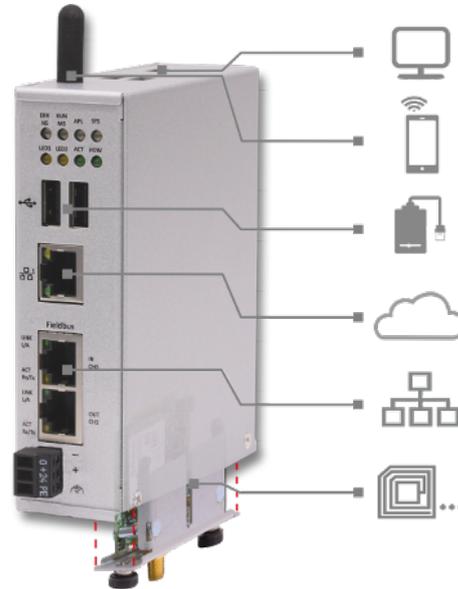


Figure 1: netPI

netPI was specifically designed for applications on the "Edge" between the IT network and the OT network and therefore is a programmable **Edge Gateway**. The LAN interface connects to the IT network and is the interface for the device configuration via a web browser. The two additional Ethernet interfaces connect the device to the Real-Time Ethernet network (OT network). With the WiFi antenna, the device supports also wireless network communication.

To expand the functional range of the device a slot for expansion modules is provided, e.g. a module for digital I/Os.

The system of netPI is based on an AppArmor-secured Yocto Linux build. The device boots secure, and only allows system changes with integrity-checked Hilscher software. User access is granted via a web browser over https-secured connections only.

The open source software „Docker“ by Docker, Inc. allows the user to execute own applications on the secured Linux operating system of the Edge Gateways while all protection mechanisms are fully preserved. The applications are executed in protected, isolated runtime environments. To accomplish this, Docker uses special techniques from virtualization of operating systems.

3 Device drawings

3.1 Positions of the interfaces

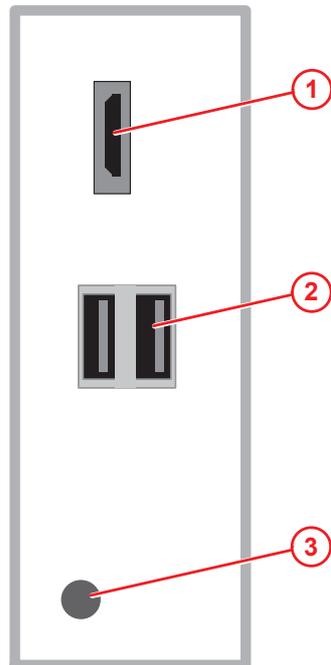


Figure 2: NIOT-E-NPI3-51-EN-RE (Top view)

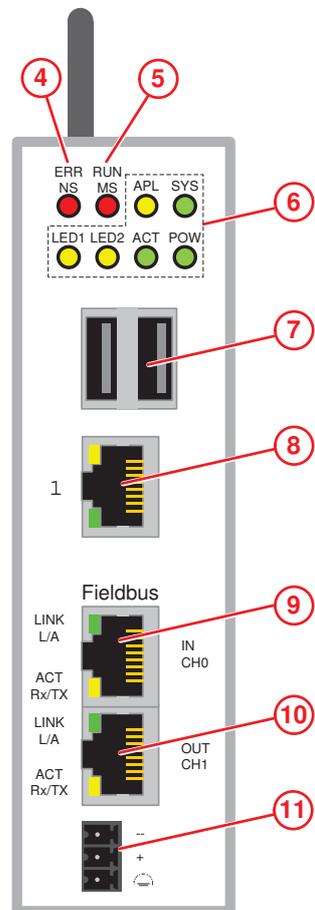


Figure 3: NIOT-E-NPI3-51-EN-RE (Front view)

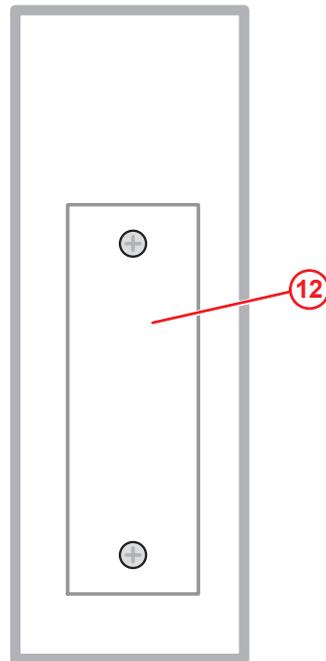


Figure 4: NIOT-E-NPI3-51-EN-RE (Bottom view)

| Pos. | Interface | For details see |
|------|--|--|
| (1) | Connector for digital LCD display (HDMI) | HDMI connector [▶ page 10] |
| (2) | USB connectors (2x USB 2.0 on top of device) | USB connectors [▶ page 9] |
| (3) | Antenna (1 x Wi-Fi) | Wi-Fi [▶ page 10] |
| (4) | ERR/NS LED (communication status) | Names of the LEDs [▶ page 11] |
| (5) | RUN/MS LED (communication status) | |
| (6) | Gateway status LEDs (6 x) | Gateway status LEDs [▶ page 12] |
| (7) | USB connectors (2x USB 2.0 on front of device) | USB connectors [▶ page 9] |
| (8) | LAN connector (RJ45 jacket) port 1 / Eth0 | LAN connectors [▶ page 9] |
| (9) | Real-Time Ethernet connector (RJ45 jacket) channel 0 | Real-Time Ethernet connectors [▶ page 9] |
| (10) | Real-Time Ethernet connector (RJ45 jacket) channel 1 | Real-Time Ethernet connectors [▶ page 9] |
| (11) | +24 V DC supply voltage connector (Mini Combicon) | Power supply [▶ page 9] |
| (12) | Slot for expansion module (Cover bolted) | Slot for expansion modules [▶ page 10] |

Table 3: Positions of the interfaces

3.2 Dimensions

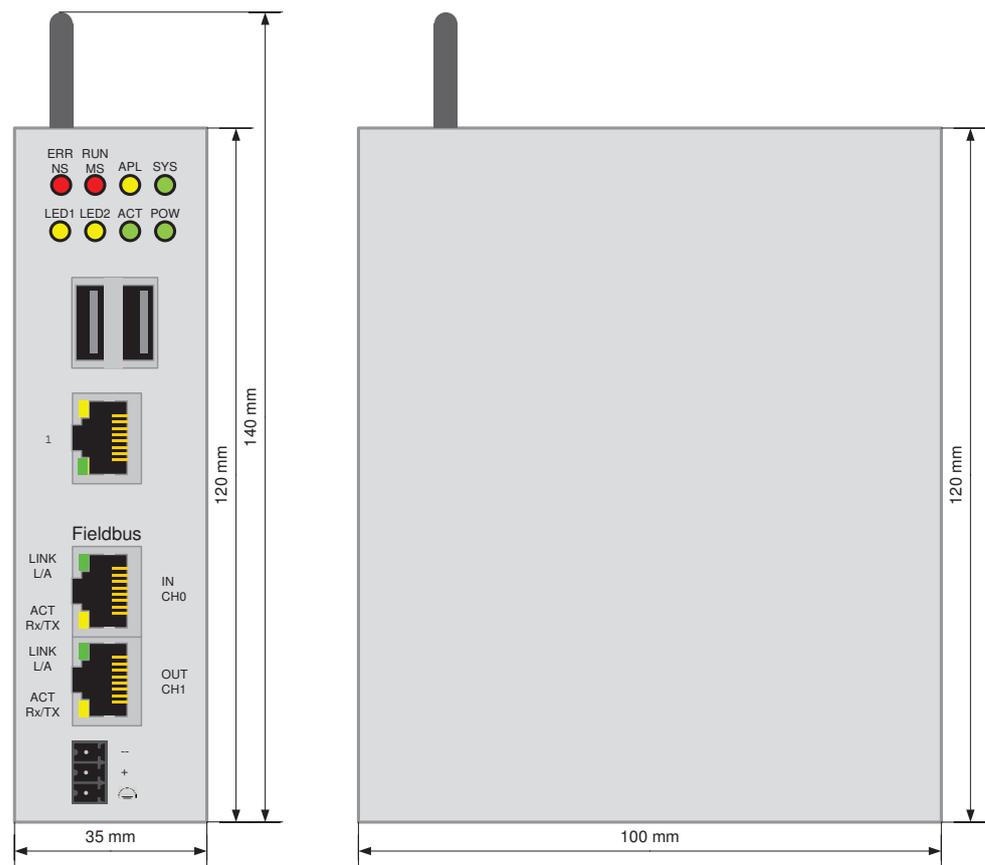


Figure 5: Dimensions

4 Connectors and mounting

4.1 Mounting

Mount the Edge Gateway on a DIN rail onto the wall of the cabinet.

4.2 Power supply

| DC 24V | Pin | Signal | Description |
|---|---|----------|------------------------------|
|  | - | GND | Ground (Reference potential) |
| | + | +24 V DC | +24 V DC |
| |  | FE | Functional earth |

Table 4: Power supply connector

4.3 LAN connectors

The Edge Gateway has one LAN connector for connecting it to the cloud network (IT network), position (8) (see section *Positions of the interfaces* [▶ page 6]).

The MAC addresses of the LAN interfaces are printed on the device label.

Section *Configuring Ethernet communication (LAN)* [▶ page 35] describes, how you can set the IP address parameters of the LAN interfaces.

4.4 Real-Time Ethernet connectors

The Edge Gateway has 2 RJ45-connectors to connect the fieldbus to a Real-Time Ethernet network (OT network), positions (9) and (10) (see section *Positions of the interfaces* [▶ page 6]).

4.5 USB connectors

The Edge Gateway has 4 USB connectors (4 x USB 2.0), positions (2) and (7) (see section *Positions of the interfaces* [▶ page 6]).

You can connect for example a USB stick, an external hard drive or a keyboard and use it together with a Docker image.

4.6 Wi-Fi

You can use the Edge Gateway for wireless network communication. The Edge Gateway supports 2 Wi-Fi operating modes: **Access Point** and **Client**. Operating mode Access Point allows the Edge Gateway to connect to other Wi-Fi devices in order to configure the Edge Gateway from a mobile device for example. Operating mode Client allows the Edge Gateway to be connected to any Wi-Fi Access Point.

Section WiFi describes how you activate the antennas and how to set the Wi-Fi operating mode.

4.7 HDMI connector

The Edge Gateway has an HDMI-connection for a monitor (position (1)) which is not required for the operation of the Edge Gateway.

The HDMI interface is inactive by default and just outputs boot information during the boot process of the device. If you want to use it, find an example docker image with activated HDMI interface and desktop at <https://hub.docker.com/r/hilschernetpi/>.

4.8 Slot for expansion modules

To expand the functional range of the device a slot for expansion modules is provided, e.g. a module for digital I/Os.

5 LEDs

5.1 Positions of the LEDs on the gateway

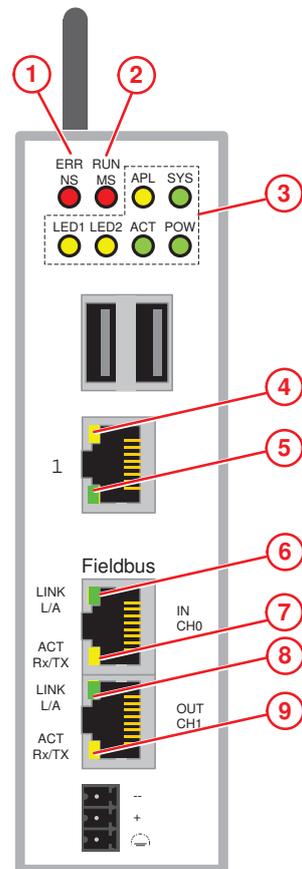


Figure 6: LED positions

| Pos. | LED | For details see |
|------|---|---|
| (1) | ERR/NS communication status Real-Time Ethernet Name and function depends on used RTE protocol: PROFINET IO Device: ERR (Bus error) EtherCAT Slave: ERR (Error) EtherNet/IP Adapter = NS (Network status) | <i>LEDs of the PROFINET IO Device interface</i> [▶ page 14] <i>LEDs der EtherCAT Slave interface</i> [▶ page 15] <i>LEDs of the EtherNet/IP Adapter interface</i> [▶ page 16] |
| (2) | RUN/MS communication status Real-Time Ethernet Name and function depends on used RTE protocol: PROFINET IO Device: RUN (System error) EtherCAT Slave: RUN EtherNet/IP Adapter = MS (Module status) | |
| (3) | Gateway status LEDs (6 x) | <i>Gateway status LEDs</i> [▶ page 12] |
| (4) | LINK LAN | <i>LEDs of the LAN interface</i> [▶ page 13] |
| (5) | ACT / RxTx LAN | |
| (6) | LINK / L/A Real-Time Ethernet channel 0 Name and function depends on used RTE protocol. | <i>LEDs of the PROFINET IO Device interface</i> [▶ page 14] |
| (7) | ACT / Rx/Tx Real-Time Ethernet channel 0 Name and function depends on used RTE protocol. | <i>LEDs der EtherCAT Slave interface</i> [▶ page 15] <i>LEDs of the EtherNet/IP Adapter interface</i> [▶ page 16] |
| (8) | LINK / L/A Real-Time Ethernet channel 1 Name and function depends on used RTE protocol. | |
| (9) | ACT / Rx/Tx Real-Time Ethernet channel 1 Name and function depends on used RTE protocol. | |

Table 5: Names of the LEDs

5.2 Gateway status LEDs

LEDs indicating communication status, system status, application status and voltage supply. The position of the LEDs is indicated by position (3) in section *Positions of the LEDs on the gateway* [▶ page 11].

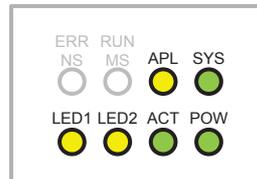


Figure 7: Gateway status LEDs

| LED | Color | Status | Meaning |
|------|----------------------|----------|--|
| APL | ● (yellow) | - | Application status Without function. |
| SYS | Duo LED yellow/green | | System status (Real-Time Ethernet) |
| | ● (green) | On | Operating system Real-Time Ethernet processor is running. |
| | ☀ (green/ yellow) | Blinking | Real-Time Ethernet processor waits for firmware. |
| | ● (yellow)/ | On | Real-Time Ethernet processor (= Romloader) waits for Second Stage Boot Loader. |
| | ● (off) | Off | Supply voltage missing. |
| LED1 | ● (yellow) | - | GPIO12, programmable |
| LED2 | ● (yellow) | - | GPIO13, programmable |
| ACT | ☀ (green) | Blinking | Activity Linux operating system is active. |
| POW | ● (green) | On | Supply voltage OK |
| | ● (off) | Off | No supply voltage or supply voltage below 4.65 V. |

Table 6: Description of gateway status LEDs

5.3 LEDs of the LAN interface

LEDs indicating state of the LAN communication. For the positions of the LAN LEDs, see section *Positions of the LEDs on the gateway* [▶ page 11].

| LED | Color | State | Meaning |
|--|--|-----------------------------|--|
| LINK Position in the device drawing (3) | LED green | | |
| |  (green) | On | 100 MBit MBit network connection |
| |  (off) | off | 10 MBit or no network connection |
| RX/TX Position in the device drawing (2) | LED yellow | | |
| |  (yellow) | Flickering (load dependent) | The device sends/receives frames |
| |  (off) | off | The device does not send/receive frames. |

Table 7: LEDs LAN interface

5.4 LEDs of the PROFINET IO Device interface

| LED | Color | State | Meaning |
|--|--|-----------------------------|--|
| RUN (System Failure) Position in the device drawing: (2) | Duo-LED red/green | | |
| |  (off) | Off | No error |
| |  (red) | Flashing (1 Hz, 3 s) | DCP signal service is initiated via the bus. |
| |  (red) | On | Watchdog timeout; channel, generic or extended diagnosis present; system error |
| ERR (Bus Failure) Position in the device drawing: (1) | Duo-LED red/green | | |
| |  (off) | Off | No error |
| |  (red) | Flashing (2 Hz) | No data exchange |
| |  (red) | On | No configuration; or low speed physical link; or no physical link |
| LINK CH0 (6) , CH1 (7) | LED green | | |
| |  (green) | On | The device is linked to the Ethernet. |
| |  (off) | Off | The device has no link to the Ethernet. |
| RX/TX CH0 (8) , CH1 (9) | LED yellow | | |
| |  (yellow) | Flickering (load dependent) | The device sends/receives Ethernet frames. |
| |  (off) | Off | The device does not send/receive Ethernet frames. |

Table 8: LED states for the PROFINET IO-Device protocol

| LED state | Definition |
|-----------------------------|--|
| Flashing (1 Hz, 3 s) | The indicator turns on and off for 3 seconds with a frequency of 1 Hz: "on" for 500 ms, followed by "off" for 500 ms. |
| Flashing (2 Hz) | The indicator turns on and off with a frequency of 2 Hz: "on" for 250 ms, followed by "off" for 250 ms. |
| Flickering (load dependent) | The indicator turns on and off with a frequency of approximately 10 Hz to indicate high Ethernet activity: "on" for approximately 50 ms, followed by "off" for 50 ms. The indicator turns on and off in irregular intervals to indicate low Ethernet activity. |

Table 9: LED state definitions for the PROFINET IO-Device protocol

5.5 LEDs der EtherCAT Slave interface

| LED | Color | State | Meaning |
|---|---|-----------------------------|--|
| RUN Position in the device drawing: (2) | Duo LED red/green | | |
| |  (off) | Off | INIT: The device is in INIT state. |
| |  (green) | Blinking (2.5 Hz) | PRE-OPERATIONAL: The device is in PRE-OPERATIONAL state. |
| |  (green) | Single flash | SAFE-OPERATIONAL: The device is in SAFE-OPERATIONAL state. |
| |  (green) | On | OPERATIONAL: The device is in the OPERATIONAL state. |
| ERR Position in the device drawing: (1) | Duo LED red/green | | |
| |  (off) | Off | No error: The EtherCAT communication of the device is in working condition. |
| |  (red) | Blinking (2.5 Hz) | Invalid configuration: General Configuration Error Possible reason: State change commanded by master is impossible due to register or object settings. |
| |  (red) | Single flash | Local error: Slave device application has changed the EtherCAT state autonomously. Possible reason 1: A host watchdog timeout has occurred. Possible reason 2: Synchronization Error, device enters Safe-Operational automatically. |
| |  (red) | Double flash | Application watchdog timeout: An application watchdog timeout has occurred. Possible reason: Sync Manager Watchdog timeout. |
| L/A IN, L/A OUT Ch0 (6) , Ch1 (8) | LED green | | |
| |  (green) | On | Link: The device is linked to the Ethernet, but does not send/receive Ethernet frames. |
| |  (green) | Flickering (load dependent) | Activity: The device is linked to the Ethernet and sends/receives Ethernet frames. |
| |  (off) | Off | The device has no link to the Ethernet. |
| Ch0 (7) , Ch1 (9) | LED yellow | | |
| |  (off) | Off | This LED is not used. |

Table 10: LED states for the EtherCAT Slave protocol

| LED state | Definition |
|-----------------------------|--|
| Blinking (2.5 Hz) | The indicator turns on and off with a frequency of 2.5 Hz: "on" for 200 ms, followed by "off" for 200 ms. |
| Single flash | The indicator shows one short flash (200 ms) followed by a long "off" phase (1,000 ms). |
| Double flash | The indicator shows a sequence of two short flashes (each 200 ms), separated by a short off phase (200 ms). The sequence is finished by a long off phase (1,000 ms). |
| Flickering (load dependent) | The indicator turns on and off with a frequency of approximately 10 Hz to indicate high Ethernet activity: on for approximately 50 ms, followed by off for 50 ms. The indicator turns on and off in irregular intervals to indicate low Ethernet activity. |

Table 11: LED state definitions for the EtherCAT Slave protocol

5.6 LEDs of the EtherNet/IP Adapter interface

| LED | Color | State | Meaning |
|--|---|-----------------------------|--|
| MS (module status) Position in the device drawing: (2) | Duo LED red/green | | |
| |  (green) | On | Device operational: The device is operating correctly. |
| |  (green) | Flashing (1 Hz) | Standby: The device has not been configured. |
| |  (red/green) | Flashing (1 Hz) | Self-test: The device is performing its power up testing. |
| |  (red) | Flashing (1 Hz) | Minor fault: The device has detected a recoverable minor fault. E. g. an incorrect or inconsistent configuration can be considered as a minor fault. |
| |  (red) | On | Major fault: The device has detected a non-recoverable major fault. |
| |  (off) | Off | No power: The power supply to the device is missing. |
| NS (Network status) Position in the device drawing: (1) | Duo LED red/green | | |
| |  (green) | On | Connected: The device has at least one established connection (even to the Message Router). |
| |  (green) | Flashing (1 Hz) | No connections: The device has no established connections, but has obtained an IP address. |
| |  (red/green) | Flashing (1 Hz) | Self-test: The device is performing its power up testing. |
| |  (red) | Flashing (1 Hz) | Connection timeout: One or more of the connections in which this device is the target have timed out. This status will be finished only if all timed out connections are reestablished or if the device is reset. |
| |  (red) | On | Duplicate IP: The device has detected that its IP address is already in use. |
| |  (off) | (Off) | Not powered, no IP address: The device does not have an IP address (or is powered off). |
| LINK CH0 (6) , CH1 (7) | LED green | | |
| |  (green) | On | The device is linked to the Ethernet. |
| |  (off) | Off | The device has no link to the Ethernet. |
| ACT CH0 (8) , CH1 (9) | LED yellow | | |
| |  (yellow) | Flickering (load dependent) | The device sends/receives Ethernet frames. |
| |  (off) | Off | The device does not send/receive Ethernet frames. |

Table 12: LED states for the EtherNet/IP Adapter protocol

| LED state | Definition |
|-----------------------------|---|
| Flashing (1 Hz) | The indicator turns on and off with a frequency of 1 Hz: "on" for 500 ms, followed by "off" for 500 ms. |
| Flickering (load dependent) | The indicator turns on and off with a frequency of approximately 10 Hz to indicate high Ethernet activity: on for approximately 50 ms, followed by off for 50 ms. The indicator turns on and off in irregular intervals to indicate low Ethernet activity |

Table 13: LED state definitions for the EtherNet/IP Adapter protocol

6 Commissioning the Edge Gateway

6.1 Establishing the IP address communication

An IP address is required to address the Edge Gateway in the LAN network.

The following figure shows the factory setting of the LAN interfaces and the assignment of the connections.

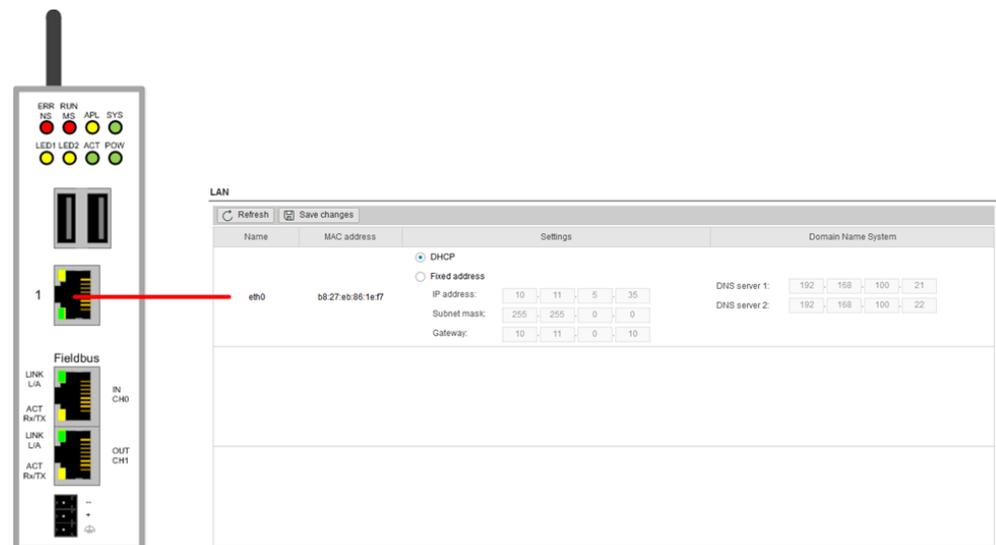


Figure 8: Default settings of the Ethernet network connectors

Network connection - DHCP server available

If a DHCP server is available in the network:

- Use an Ethernet cable to connect the LAN connection port 1 (`eth0`) (see (7) in *Positions of the interfaces* [▶ page 6]) with a network in which a DHCP server is available.
- ⇒ The Edge Gateway obtains an IP address from the DHCP server. Access to the Edge Gateway is possible now.



Note:

The Edge Gateway sends a request to a DHCP server once after switching on the device or after each connection of the Ethernet cable, i.e. when the Edge Gateway detects a link signal. If you want to activate a request of the Edge Gateway to the DHCP server manually, pull off the Ethernet cable from the Edge Gateway and reconnect it to the Edge Gateway.

Read section *Using the web browser to establish a connection with the Edge Gateway* [▶ page 18] to find out how to access the Edge Gateway.

6.2 Using the web browser to establish a connection with the Edge Gateway

You have three possibilities to access the Edge Gateway:

1. by means of the host name (see section *Using the host name* [▶ page 18])
2. by access via the Windows network (see section *Access to the Edge Gateway in the Windows network environment* [▶ page 19]),
3. by using the IP address (see section *Using the IP address*).

6.2.1 Using the host name

The Edge Gateway has a host name you can use to access the device.

Where do you find the host name on the device?

The device is delivered (factory setting) with a label printed at its bottom. In the figure below the host name has a red frame.

Establishing a connection with the host name

- Enter the following address in the address line of your browser:

`https://<hostname>`

Example: For the device with the host name `NT0002A233E559` enter

`https://NT0002A233E559`

- ⇒ The Edge Gateway Manager opens.

You can now use the Edge Gateway manager to configure the device. For this purpose, read section *Edge Gateway manager web page* [▶ page 21].

6.2.2 Access to the Edge Gateway in the Windows network environment

To be located easily in the network, the Edge Gateway uses the UPnP technology (Universal Plug and Play). This technology will display the Edge Gateway in the Windows network environment.

- To display all devices in the network, click on **Network** in the Windows Explorer.
- ⇒ You will find the Edge Gateway under **Other Devices**:

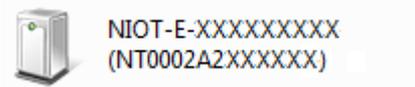
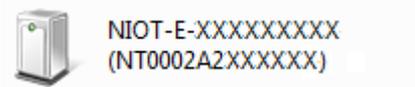


Figure 9: netIOT Edge Gateway in the Windows network

- Open the context menu of this entry and select **Properties**.
- ⇒ The menu provides information on the Edge Gateway, e.g. serial number, MAC address, host name or die IP address.
- Click on the link under Device web page.
- ⇒ The Edge Gateway manager opens.
- To open the Edge Gateway manager, you can also double-click on the device icon.



- ⇒ The Edge Gateway manager opens.

You can now use the Edge Gateway manager to configure the device. For this purpose, read section *Edge Gateway manager web page* [▶ page 21].

7 Edge Gateway manager

7.1 Calling the Edge Gateway Manager

The Edge Gateway manager is a web page with tiles that allow rapid access to the applications integrated in the device or to external web pages.

The Edge Gateway uses the secured HTTPS protocol to access web pages stored in the Edge Gateway.

- To open the Edge Gateway manager, enter the following information in the address line of your browser:

`https://<Host name of the Edge Gateway>`

or

`https://<IP address of the Edge Gateway>`

- ⇒ Your browser displays the Edge Gateway manager.

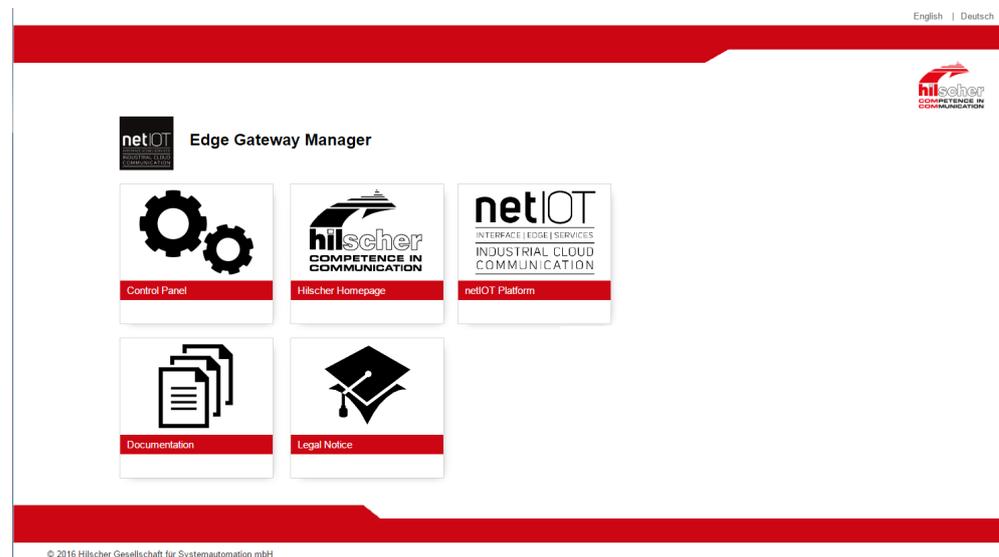


Figure 10: Edge Gateway Manager



Note:

Remember that the secured **HTTPS** protocol is used here, not the widely spread **HTTP** protocol.

7.2 Edge Gateway manager web page

The Edge Gateway manager displays tiles that allow rapid access to the applications integrated in the device or external web pages.

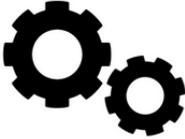
| Icon | Function |
|--|--|
|  Control Panel | <p>Opens the control panel of the Edge Gateway.</p> <p>The control panel configures the Edge Gateway and displays information on the system. Section <i>Control Panel</i> [▶ page 22] describes the possibilities of configuration as well as the displayed information on the system.</p> |
|  docker Docker Management | <p>Opens the Docker management.</p> <p>See section <i>Isolated application execution with Docker</i> [▶ page 46].</p> |
|  Documentation | <p>Opens the Edge Gateway documentation stored in the device.</p> |
|  netIOT Platform | <p>Opens the homepage of the netIOT platform in the Internet.</p> <p>Requires a connection to the Internet.</p> |
|  Hilscher Homepage | <p>Opens the Hilscher homepage in the Internet.</p> <p>Requires a connection to the Internet.</p> |
|  Legal Notice | <p>Opens legal information concerning the Edge Gateway.</p> <p>Requires a connection to the Internet.</p> |

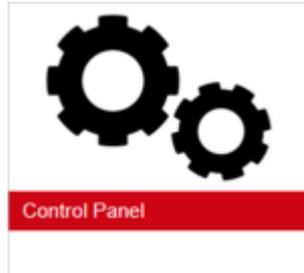
Table 14: Starting applications with the Edge Gateway manager

8 Control Panel

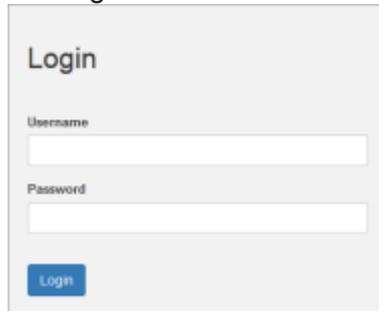
8.1 Opening the control panel

With the control panel you can configure the Edge Gateway and display device-specific information.

- Click the tile **Control Panel**.



- The login screen for the **Control Panel** is displayed.

A login screen with a light gray background. At the top, the word "Login" is displayed in a bold, dark font. Below it, there are two input fields: "Username" and "Password". Each field has a white border and a white background. Below the "Password" field is a blue button with the word "Login" in white text.

- Enter your user name and your password.
- Click at **Login**.
- ⇒ The **Control Panel** will be displayed.

8.1.1 First login

Setting the administrator password when the control panel is called for the first time

The dialog box **Set Administrator Password** is displayed when the control panel is called for the first time.

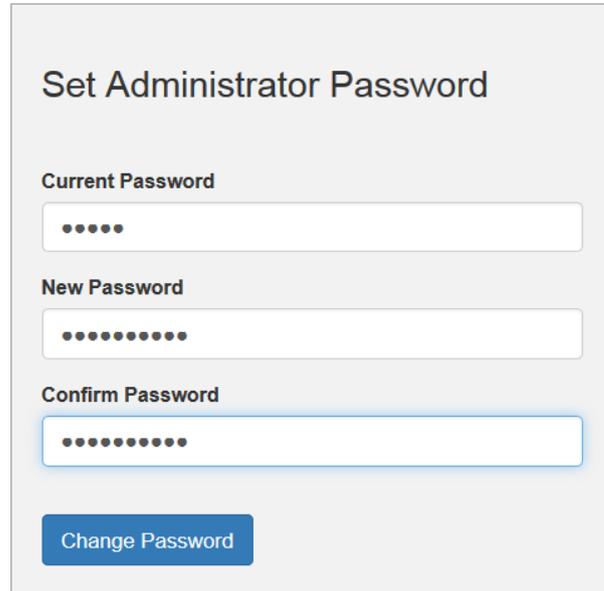
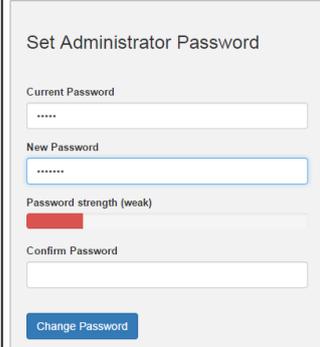
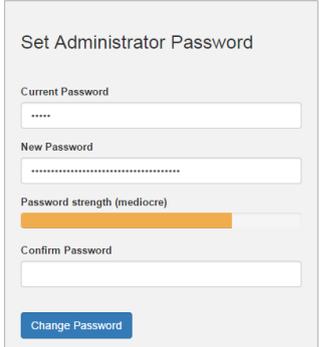
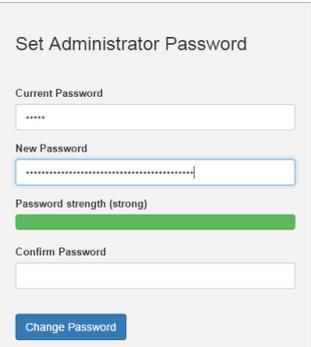


Figure 11: Edge Gateway Manager - Setting the administrator password

To set a new administrator password, proceed as follows:

- Enter the preset password under **Current Password**. With the first commissioning, the password is:
`admin`
- Enter the new administrator password. It must have at least 7 characters. For reasons of safety, Hilscher recommends using significantly more characters. A strong password consists of upper and lower case letters, digits and special characters. A quality indicator in the dialog box evaluates the password.

| Weak password | Mediocre password | Strong password |
|---|--|---|
|  |  |  |

- Click **Change Password** only after the entered password has been evaluated as strong.
- ⇒ The administrator password for the user account **Admin** has thus been changed.

- ⇒ As an administrator you can now use the control panel, create further users in the user management, and assign access rights.

Also see about this

 User management [[▶ 38](#)]

8.1.2 Secure connection

Edge Gateways support web connections secured by SSH/TSL via `https://` accesses only.

By definition, a secure connection can provide an efficient protection only if a certificate proves that the server is secure. Only then can running transactions of the initiating browser and the server be considered as protected against interception and data theft.

This is why the browser at first inquires a certificate of verification from the server (Gateway). This certificate proves that the issuer has verified the security of the server. Each browser provides a preinstalled list of known authorized issuers of certificates.

Each time the certificate of the server arrives at the browser, the browser compares the issuer of the certificate with the issuers stored in the list of known authorized issuers of certificates.

If the issuer of the certificate is not listed, the browser will signal a certificate error and request the user's confirmation to continue because it assumes that the connection is insecure.

As standard, Edge Gateways contain a certificate issued by Hilscher that is not on the list of the known authorized issuers of certificates. Due to that, the browser signals an insecure connection and requests the confirmation to continue. When this confirmation has been given once, any future connections will be established without further requests.



Note:

In the control panel you can replace this certificate any time by the certificate of a known authorized issuer of certificates, see section *Uploading and installing own security certificates* [[▶ page 42](#)]).

8.1.2.1 Connection without certificate with Microsoft Internet Explorer

Microsoft Internet Explorer: Edge Gateway Manager will not be displayed

If you use the Microsoft Internet Explorer and the following page is displayed, click the option **Continue to this web site (not recommended)**.

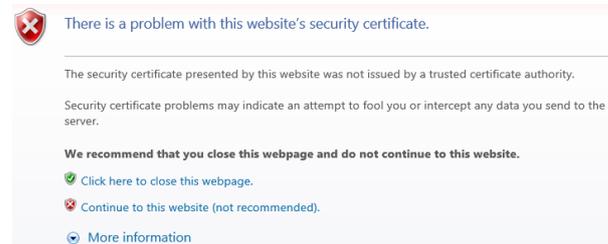


Figure 12: Security error message of the Internet Explorer

8.1.2.2 Connection without certificate with Firefox

If you use Firefox as a browser, a self-signed certificate will cause the following error message:



Figure 13: Security error message of the Firefox browser (1)

To avoid this message caused by a self-signed certificate, proceed as follows:

- To display the complete message, click **Advanced**.

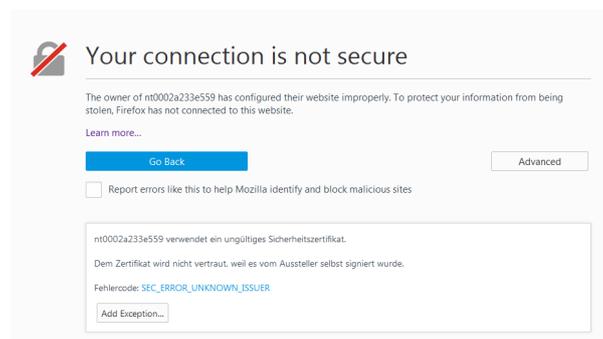


Figure 14: Security error message of the Firefox browser (2)

- To define an exceptional rule that enables the display of the user interface without repeated error messages, click **Add Exception**.



Figure 15: Firefox dialog box: Adding exceptional safety rule

- To save the setting permanently, check the box **Permanently store this exception**.
- To save the rule, click **Confirm Security Exception**.
- ⇒ When you open the control panel in future, security messages will no longer be displayed.

8.1.2.3 Connection without certificate with Google Chrome

If you use Google Chrome as web browser, you will get the following error message due to a self-signed certificate.

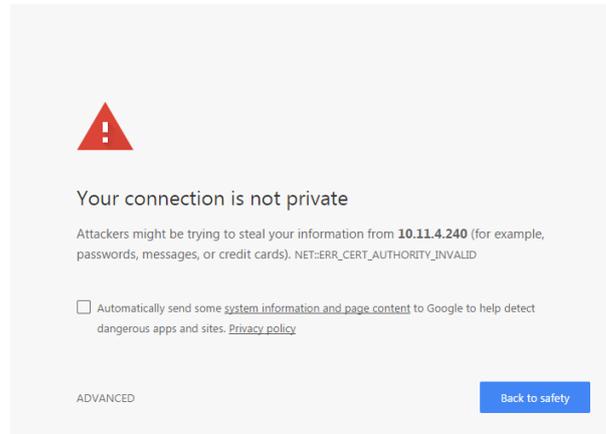


Figure 16: Security error message of Google Chrome (1)

Proceed as follows in order to avoid the following message, which is caused by a self-signed certificate,

- Click at **ADVANCED** to display the complete message.

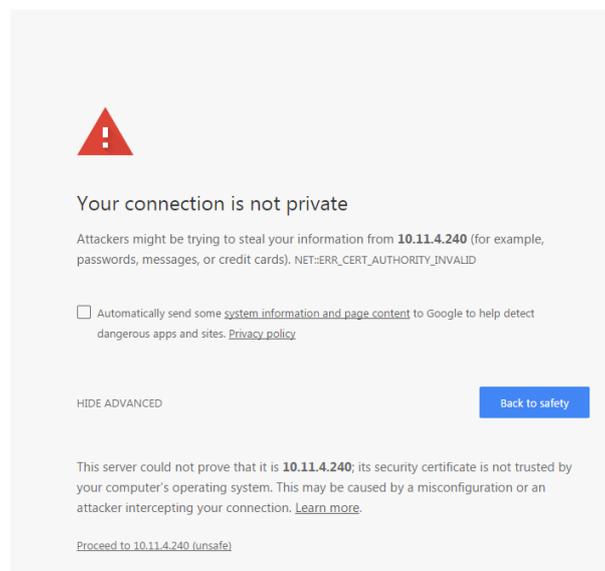


Figure 17: Security error message of Google Chrome (2)

- In order to continue, click at **Proceed to ... (unsafe)**.
- ⇒ The Control Panel is displayed.

8.2 Control Panel commands

8.2.1 Overview and main menu

The following figure displays the main menu of the Control Panel.

System ▾ Package Manager ▾ Network ▾ Services ▾ User Management ▾ Security ▾ Help ▾ Session ▾

Figure 18: Main menu of the Control Panel

| Menu | Submenu | Description | Details in section |
|-----------------|-----------------|--|---|
| System | Info Center | Displaying the system information, monitoring of the processor core temperature, and a system monitor for the usage of CPU, main memory, and SSD | <i>Displaying system information</i> [▶ page 29] |
| | Time | Settings of system time and time synchronization. | <i>Setting the system time</i> [▶ page 30] |
| | Reboot | Rebooting the Linux operating system of the Edge Gateway | <i>Rebooting the system</i> [▶ page 32] |
| | Shutdown | Shutting down the Linux operating system of the Edge Gateway | <i>System shutdown</i> [▶ page 33] |
| Package Manager | Packages | Managing the packages of the Linux-based operating system of the Edge Gateway. | <i>Packet management</i> [▶ page 34] |
| Network | LAN | Configuring the Ethernet interfaces to the field or cloud. | <i>Configuring Ethernet communication (LAN)</i> [▶ page 35] |
| | WiFi | Configuring the WiFi communication | WiFi |
| | Hostname | Displaying and configuring the host name identifying the Edge Gateway in the network. | <i>Hostname</i> [▶ page 36] |
| Services | Service List | Displaying, starting, and stopping the services of the Edge Gateway. | <i>Services</i> [▶ page 37] |
| User Management | Roles | Displaying and configuring the permissions for user roles. | <i>Managing user roles</i> [▶ page 38] |
| | Accounts | Displaying user accounts und assigning user roles. | <i>Managing user accounts</i> [▶ page 40] |
| Security | SSL Certificate | Installing the SSL safety certificate. | <i>Security certificates</i> [▶ page 41] |
| Help | Info | Displaying current software version. | <i>Help</i> [▶ page 44] |
| Session | User Profile | Displaying the permissions of the user. | <i>User profile</i> [▶ page 44] |
| | Logout | Logout | <i>Logout</i> [▶ page 45] |

Table 15: Functional overview of the Control Panel

For the pages which can be invoked via the Control Panel, the following applies:

If for the selected page, no access right for reading is present, this has the following implications:

- No data are displayed. All important controls and displays of the page are grayed out respectively inactive.
- The error message **Permission denied** is displayed when accessing the page.

If there is read but no write access right present, this has the following implications:

- The error message **Permission denied** is displayed when trying to make a change.

8.2.2 System information and system time

8.2.2.1 Displaying system information

Open this page with **System > Info Center**. No access rights are required in order to open this page. This page shows e.g. the firmware version and the serial number of the Edge Gateway.

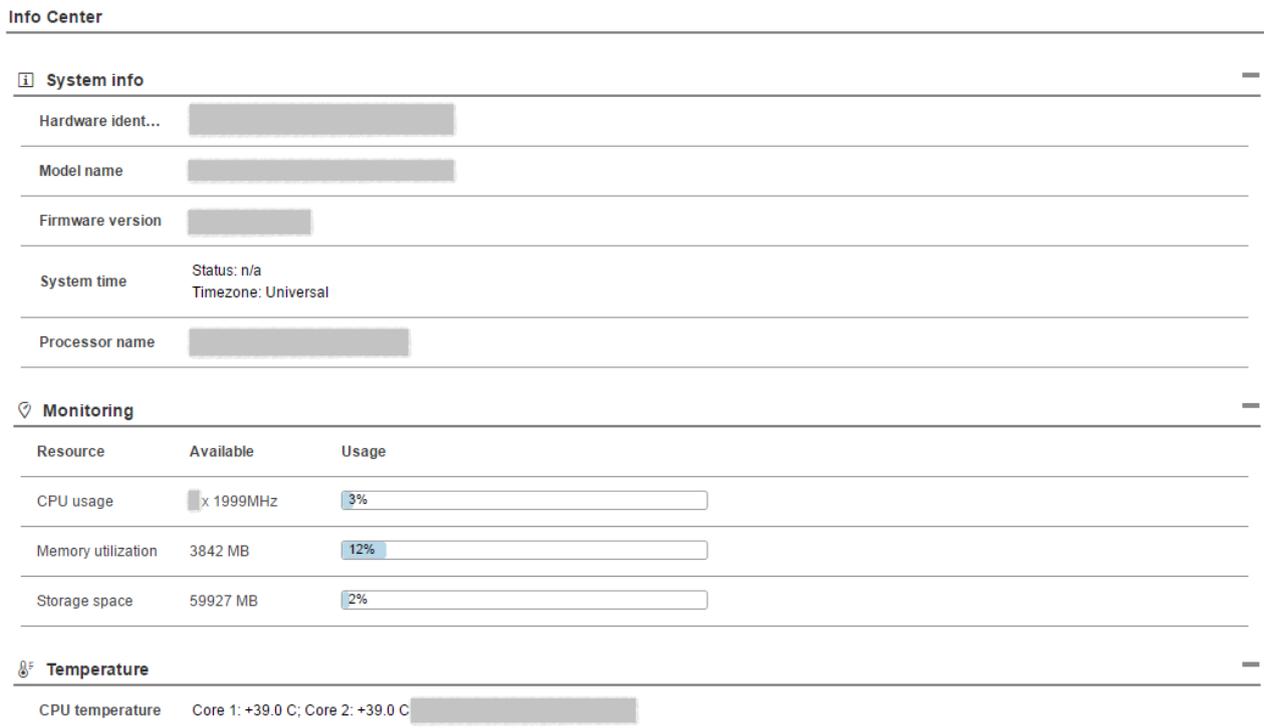


Figure 19: Page Info Center

The Info Center displays the following information:

| System info | Description |
|------------------|--|
| Hardware ident. | Serial number of the Edge Gateway |
| Model name | Model designation of the Edge Gateway (NIOT-E-NPI3-51-RE-EN) |
| Firmware version | Complete version designation of the firmware stored in the Edge Gateway |
| System time | Synchronization status of the internal clock of the Edge Gateway. When the clock is synchronized via the network, the IP address and the name of the time server used for synchronization will be displayed. The user has to configure the time zone. |
| Processor name | Name of the microprocessor (CPU) installed in the Edge Gateway. |

Table 16: Info Center: Area System info

| Monitoring | Description |
|--------------------|--|
| CPU usage | Number of microprocessor cores plus clock frequency and average utilization of each core in the Edge Gateway |
| Memory utilization | Size and average utilization of the main memory in the Edge Gateway |
| Storage space | Display of available memory and the memory that is currently utilized on the integrated Solid-State-Disk of the Edge Gateway |

Table 17: Info Center: Area Monitoring

| Temperature | Description |
|-----------------|---|
| CPU temperature | Display of the temperature of each processor core in the Edge Gateway |

Table 18: Info Center: Area Temperature

If the data of the area **Monitoring** cannot be read, this is grayed out.

8.2.2.2 Setting the system time

Open this page with **System > Time**.

In order to access this page you require the following access right:

Setting the system time

On this page, you can set the system time and the time zone this time relates to. You can set the system time in two ways:

| Type | Selection | Method | Standard presetting |
|---------------|------------------|---------------------------|---------------------|
| manually | Manual selection | by entering date and time | yes |
| automatically | NTP synchronized | by means of a time server | no. |

Table 19: Setting the system time

Time

Timezone: Universal

Manual

Time:

Date:

NTP synchronized

Status n/a

| | Server |
|--------------------------|-----------------|
| <input type="checkbox"/> | ptbtime1.ptb.de |
| <input type="checkbox"/> | |

Figure 20: Time configuration page

Setting the system time manually

- Click the option **Manual**.
- Enter the time in the input field **Time** in the format `hh:mm:ss`.
- Set the date using the calendar input field **Date**.
- Click at  **Save changes**.
- ⇒ The system time is set.

Setting the system time automatically using a time server

You can synchronize the time using a time server that uses the Network Time Protocol (NTP). Under **NTP synchronized** there is a list where you can enter such time servers. The list of NTP servers will be worked off from top to bottom until a server gives a valid answer and synchronization occurs.

- Click the option **NTP Synchronized**.
- Click **Add NTP server**.
- ⇒ The dialog box for entering the NTP server is displayed.



- In the input field **NTP server** enter the address of a server which uses the NTP to synchronize the time:
E.g.: To add the server for time synchronization of the Physikalisch-Technische Bundesanstalt (the National Metrology Institute of Germany) to the list, enter the address `ptbtime1.ptb.de` in the input field **NTP server**.
- Click **Add**.
- ⇒ The system time is set via the NTP. As soon as the system time is set successfully, the following information will be displayed under **Status**:
`Synchronized to time server <IP address of the time server>:<Port number of the time server > (<NTP address of the time server>)`

Setting the time zone

With the selection list *Timezone* you can adjust the time zone to your local time in which the Edge Gateway is so that the set time can be interpreted correctly (e.g. summer time conversion). For this purpose, the selection list *Timezone* offers many setting options. The default value is *Universal*. For Central European Time set *CET*.

Take care of the following notes:



NOTICE

Effects of setting the system time

Once the system has been set, system services and Node-RED flows, which use the system time for synchronization, lose their reference time, i.e. they refer to the new time set.



Note:

For information on the NTP, see Wikipedia under https://en.wikipedia.org/wiki/Network_Time_Protocol (English) or https://de.wikipedia.org/wiki/Network_Time_Protocol (German). There you will also find links to lists of NTP servers for various countries.

8.2.2.3 Rebooting the system

You have to login as Administrator to use this function.

In order to reboot the system:

- Within the Control Panel select menu entry **System>Reboot**
- ⇒ The following safety query is displayed:



Figure 21: Reboot safety query

- If you really intend to reboot the system, answer to the safety query with **Yes**.
- ⇒ The Linux operating system of your Edge Gateway is shut down and then immediately restarted.



Note:

Take care of the consequences of shutting down and restarting for your network, if you reboot the Edge Gateway.

8.2.2.4 System shutdown

You have to login as Administrator to use this function.

In order to shut down the system:

- Within the Control Panel select menu entry **System>Shutdown**.
- ⇒ The following safety query is displayed:

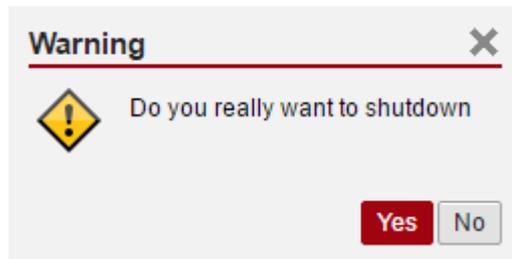


Figure 22: Warning for consequences of shutdown

- If you really intend to shut down the system, answer to the safety query with **Yes**.
- ⇒ The Linux operating system of your Edge Gateway is shut down.



Note:

Take care of the consequences for your network, if you shut down the Edge Gateway.

8.2.3 Packet management

8.2.3.1 Managing packets

Open this page with **Package Manager > Packages**.

In order to access this page you require the following access right:

Managing packets

This page contains the package management of the Linux-based operating system of the Edge Gateway. This page

- lists the installed packages including version,
- adds new signed packages or
- updates already installed signed packages.

**Note:**

You can only install packages signed by Hilscher!

Use the package management only when Hilscher requests you to use the package management.

8.2.4 Network

8.2.4.1 Configuring Ethernet communication (LAN)

Open this page with **Network > LAN**.

In order to access this page you require the following access right:

Access to LAN (Ethernet network)

On this page you configure the Ethernet interfaces `eth0`, `eth1` (both on the side of the cloud) and `cifx0` (on the side of the fieldbus). For each Ethernet interface you can configure how to set the IP address:

- The Edge Gateway is to obtain the IP address parameters automatically from a DHCP server: Option *DHCP*.
- The IP address parameters are manually entered by the user: Option *Fixed address*.

The IP address parameters include the IP address, the subnet mask, the Gateway address, and the IP addresses of the 1st and 2nd domain name server.

The default IP address of the LAN connection port 2 is `192.168.253.1` with the subnet mask `255.255.255.0`.

| Column | Meaning |
|--------------------|---|
| Name | displays the name of the LAN interface. |
| MAC address | displays the MAC address of the LAN interface. |
| Settings | Selecting the configuration method: Here you can select between <ul style="list-style-type: none"> • <i>DHCP</i> (IP address parameters automatically obtained from a DHCP server) or • <i>Fixed address</i> (IP address parameters entered by the user) If you enter the IP address manually, also always enter the subnet mask and the Gateway address. |
| Domain Name System | If you enter the IP address parameters manually, enter the IP address of the 1st and 2nd domain name server. |

Table 20: Table LAN: Meaning of the columns

If you want to permanently save the changes you made, click at

 afterwards.

8.2.4.2 Hostname

Open this page with **Network > Hostname**.

In order to access this page you require the following access right:

Access to hostname of Edge Gateway

On this page you configure the host name.

The host name identifies the device via the WiFi or LAN network.

The default host name starts with the two letters "NT" followed by the LAN MAC address of the LAN connection port 1 of the Edge Gateway. Example NT0002A233E559. The default host name is printed on the label at the bottom of the Edge Gateway. With the host name you can access the Edge Gateway from your PC even without knowing the IP address of the Edge Gateway (also see *Using the web browser to establish a connection with the Edge Gateway* [▶ page 18]).

If the Edge Gateway does not obtain an IP address from a DHCP server, the system cannot translate the host name and you cannot access the device.

Hostname

Hostname

Figure 23: Hostname

Input field Hostname

In order to specify the hostname, enter a string with arbitrary length consisting of ASCII characters into the input field **Hostname**.

Saving the host name

The hostname is saved by clicking at .

If storing the hostname has succeeded, the following message box is displayed:

Hostname settings are successfully saved

8.2.5 Services

8.2.5.1 Starting, stopping and configuring services

Open this page with **Services > Service List**.

On this page you can

- display the list of the running services,
- den Betriebszustand jedes Dienstes anzeigen,
- display the operating status of each service,
- activate/deactivate Autostart, and

A service can allow you individual settings.

The list of services is displayed at the left edge:



Figure 24: List of default services

For a quick overview, the operating status of each service is displayed in color.

| Color | Operating status |
|--------|---|
| green | The service is being executed. |
| yellow | The service is configured, but not executed. |
| red | The service is neither configured nor executed. |
| grey | Right for accessing this service is missing |

Table 21: Operating statuses of the services

8.2.6 User management

The administrator manages users by means of two configuration pages:

- User roles (determining new roles and assigning access rights) and
- User accounts (adding, processing, and deleting).

Defining a user account is accomplished by assigning a predefined role to the user.

8.2.6.1 Managing user roles

Open this page with **User Management > Roles**.

On this page, you can determine roles and assign access rights onto resources to these roles.

The roles *Administrator* and *View* are standard and cannot be deleted.

Roles

| + Create new role | | Delete role | |
|-------------------|--|---------------|--|
| Role | | | |
| Administrator | | | |
| View | | | |
| | | | |
| Save changes | | | |
| Resource | | Access rights | |
| | | | |

Figure 25: Page for configuring roles

An access right is set per resource. Each configuration page of the control panel which contains settable device parameters is a resource. Access via REST-API (see Functions of the Edge Server) is also a resource.

An access right can be assigned to the following single resources:

| Access right / Resource | Access to resource accomplished via menu entry | Usage |
|---|--|---|
| System | | |
| Setting the system time | System > Time | <i>Setting the system time</i> [▶ page 30] |
| Packet management | | |
| Managing packets | Package Manager > Packages | <i>Managing packets</i> [▶ page 34] |
| Network access | | |
| Access to LAN (Ethernet network) | Network > LAN | <i>Configuring Ethernet communication (LAN)</i> [▶ page 35] |
| Access onto WiFi (wireless network) | Network > WiFi | Configuring wireless communication (WiFi) |
| Access onto hostname of Edge Gateway | Network > Hostname | <i>Hostname</i> [▶ page 36] |
| Access onto Field network (Ethernet network) | Network > Field | |
| Services | | |
| Configure service "S" (The displayed names depend on the installed services.) | Services > Service "S" | <i>Starting, stopping and configuring services</i> [▶ page 37] |
| Security | | |
| Install security certificates | Security > SSL/TLS Certificate | <i>Uploading and installing own security certificates</i> [▶ page 42] |
| Edge Server | | |
| Access via REST-API | Edge Server (REST API) | Functions of the Edge Server |

Table 22: Access rights onto resources

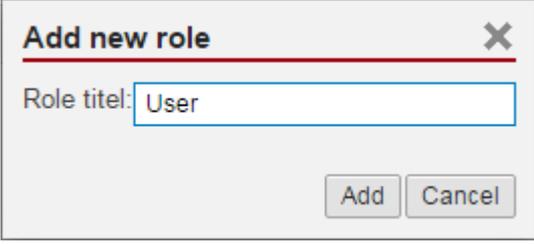
Each resource may obtain one of the following access rights:

| Access rights onto resource | Checkbox |
|-----------------------------|--------------------|
| No access | <i>None</i> |
| Read access only | <i>Read</i> |
| Read and write access | <i>Read, Write</i> |

Table 23: Access rights to resources

Adding a new role

- Click at 
- ⇒ The dialog box for entering the role name is displayed.



The dialog box titled "Add new role" has a close button (X) in the top right corner. It contains a text input field labeled "Role title:" with the word "User" entered. Below the input field are two buttons: "Add" and "Cancel".

- Enter a name for the role, e.g. **User**.
- Click **Add**.
- ⇒ The role is added.

Setting the access rights of a role

- Click a role.
- ⇒ The resources and access rights for this role will be displayed.
- Assign the access right per resource.
- Click at 

8.2.6.2 Managing user accounts

Open this page with **User Management > Accounts**.

On this page you can

- add
- process
- delete user accounts.

User Accounts

| User name | Role | E-mail |
|-----------|---------------|--------|
| admin | Administrator | |

Figure 26: User account page

Each user account has a user name, a password, and an assigned role.

8.2.7 Security certificates

The menu *Security* offers you the possibility to display the contents of security certificates and to upload and install these.

It looks like:



Figure 27: Security submenu

On selection of menu entry *SSL Certificate* the page *SSL certificate* is opened.

In order to access this page you require the following access right:

Install security certificates

This page *SSL certificate* information about the currently used security certificate. You also can upload and install a new security certificate here (File type * .pem, File size <=0.5 MB).

SSL Certificate

Certificate

Private Key

Certificate information

Subject:

| | | |
|---------------------|------|-----------------------------|
| Identity | (CN) | = 'NT0002A233E559' |
| country | (C) | = '' |
| state | (ST) | = '' |
| locality | (L) | = '' |
| organization | (O) | = 'self-signed certificate' |
| organizational unit | (OU) | = '' |
| mail | (CN) | = '' |

Issuer:

| | | |
|---------------------|------|-----------------------------|
| verified by | (CN) | = 'NT0002A233E559' |
| country | (C) | = '' |
| state | (ST) | = '' |
| locality | (L) | = '' |
| organization | (O) | = 'self-signed certificate' |
| organizational unit | (OU) | = '' |
| mail | (CN) | = '' |

validity starts = 'May 29 07:16:51 2017 GMT'

validity ends = 'May 29 07:16:51 2018 GMT'

Figure 28: Page SSL Certificate

8.2.7.1 Uploading and installing own security certificates

In the upper area of page *SSL Certificate* you can select an own security certificate including the private key that is associated with the certificate.

SSL Certificate

| | | |
|-------------|----------------------|--|
| Certificate | <input type="text"/> | <input type="button" value="Browse..."/> |
| Private Key | <input type="text"/> | <input type="button" value="Browse..."/> |

Figure 29: SSL Certificate – Upload area

Uploading and installing the certificate

1. In order to upload and install the certificate, proceed as follows:
 - Select your certificate to be uploaded and installed with the *Browse* button right of the field *Certificate*.
 - Select the private key associated with your certificate with the *Browse* button right of the field *Private Key*.



Note:

The expected file type for security certificates and private keys is *.pem (Privacy enhanced electronic mail format). You can find more information about this file format in Wikipedia at [https://en.wikipedia.org/wiki/Privacy-enhanced Electronic Mail](https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail).

- Click at *Upload and install certificates*.
- ⇒ The security certificate is uploaded and installed.

8.2.7.2 Information about the currently loaded security certificate

In the lower area of page *SSL Certificate* information concerning the currently loaded security certificate is displayed.

Certificate information

```

Subject:
Identity          (CN)   = 'NT0002A233E559'
country          (C)   = ''
state            (ST)  = ''
locality         (L)   = ''
organization     (O)   = 'self-signed certificate'
organizational unit (OU)  = ''
mail             (CN)  = ''

Issuer:
verified by     (CN)   = 'NT0002A233E559'
country         (C)   = ''
state           (ST)  = ''
locality        (L)   = ''
organization    (O)   = 'self-signed certificate'
organizational unit (OU)  = ''
mail            (CN)  = ''

validity starts = 'May 29 07:16:51 2017 GMT'
validity ends   = 'May 29 07:16:51 2018 GMT'
    
```

 Refresh

Figure 30: SSL Certificate – Info area

The single lines have the following meanings:

| Line | Abbreviation | Meaning |
|----------------------|--------------|---|
| Identity/verified by | CN | Identity/verified by |
| country | C | Country |
| state | ST | State |
| locality | L | Locality |
| organization | O | Organization |
| organizational unit | OU | Organization unit |
| mail | CN | E-mail address |
| validity starts | - | Start of validity duration of certificate |
| validity ends | - | End of validity duration of certificate |

Table 24: Information about the security certificate

In factory-new state the Edge Gateway contains a self-signed certificate. You should replace this by an own certificate that you can upload and install in the way described above.

Also see about this

 [Uploading and installing own security certificates \[▶ 42\]](#)

8.2.8 Help

Open this page with **Help> Info**. No access rights are required in order to open this page.

This page displays the firmware version of the Edge Gateway.

Info

Version

Figure 31: Info page

8.2.9 Session

8.2.9.1 User profile

Open this page with **Session> User Profile**. No access rights are required in order to open this page.

User Profile

[Edit user account](#)

User name

E-mail

Role

Permissions

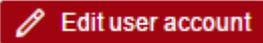
| Resource | Access |
|-----------------------|---|
| System | |
| • Time | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| Package Manager | |
| • Packages | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| Network | |
| • LAN | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| • WiFi | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| • Host Name | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| Services | |
| • Node-RED | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| • Secure shell (SSH) | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| • MQTT Broker | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| Security | |
| • SSL/TLS Certificate | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |
| Edge Server | |
| • REST API | <input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write |

Figure 32: User profile page

On this page you can

- display the access rights of your user account,
- change your E-mail address, and
- change your password.

Changing the e-mail address

- Click at .
- ⇒ The dialog **Edit user account** is displayed.

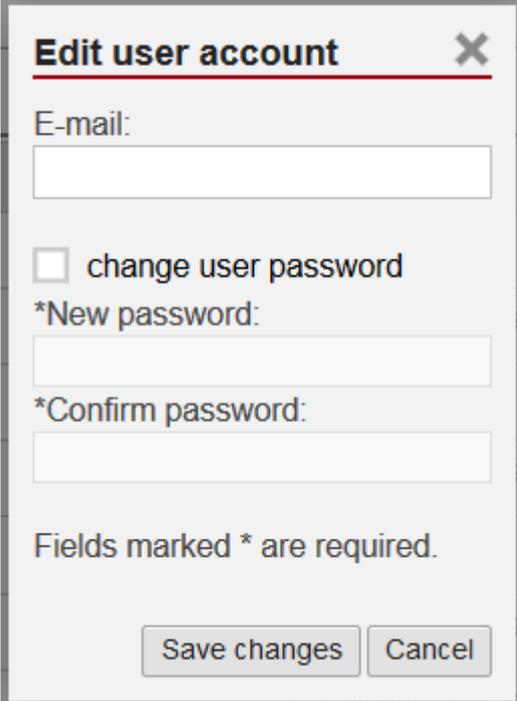
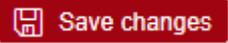
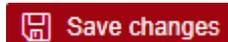


Figure 33: Dialog "Edit user account"

- Specify your e-mail address at the input field **E-mail**.
- Click at .
- ⇒ The specified e-mail address is stored.

Changing the password

- Click on .
- ⇒ The dialog **Edit user account** is displayed.
- Check **change user password**.
- Specify your password at the input field **New Password**.
- In order to confirm your input, specify your password again at the input field **Confirm Password**.
- Click on .
- ⇒ The changed password is saved.

8.2.9.2 Logout

To log out from the Edge Gateway, use **Session**> **Logout**. No access rights are required to select this menu entry. Prior to accessing the Edge Gateway again, a new login (Specifying user name and password) is necessary.

9 Isolated application execution with Docker

The Edge Gateway enables the user to execute his own applications within the protected Linux operating system. A software platform becomes necessary to allow the execution of said applications without simultaneously opening the possibility of evading the safety mechanisms of the Linux operating system. For that purpose, the Edge Gateway uses the open-source software "Docker" from Docker Inc. (<https://www.docker.com/>).

In order to work with Docker, read and write access rights at Docker UI are required. You can check whether you have the required access rights via the menu entry *User profile* [▶ page 44]. Granting read and right access rights requires administrator rights and is described in section *Managing user roles* [▶ page 38].

**Note:**

For more information on Docker, see the documentation of the Docker organization under <https://docs.docker.com/>.

9.1 Docker, image, and container

Docker

Docker offers a platform for the isolated execution of applications within protected environments and, moreover, a standard for the distribution of software. This platform allows Edge Gateway users to run their own applications within the protected Linux operating system without being able to weaken or evade its safety mechanisms.

For realizing containers, Docker internally uses techniques from operating system virtualization. On the Edge Gateway, Docker is running as a service (Docker daemon `dockerd`).

As standard with Linux, Docker is controlled by entering commands via the command line. For reasons of safety, a command line service is not installed on the Edge Gateway.

Thus, Docker cannot be operated via a CLI (Command Line Interface) as described in the official Docker documentation (<https://docs.docker.com/>). An easy-to-use GUI (Graphical User Interface) `portainer.io` is installed instead. This GUI provides the essential functions for managing the Docker services.

**Note:**

For more information on `portainer.io`, see <http://portainer.io>.

Image

An image is the basis for a container and includes only its program code and basic settings.

It does not include information the program code generates on a storage medium or RAM while it is running.

Moreover, it does not include any information on the environment the image is to be executed in, i.e. it is platform-neutral.

An image always relates to the defined processor architecture it is compiled for, e.g. x86, x64 or ARM. If a container is generated from an image, make sure that the image is suitable for the hardware platform used.

For distributing images via the Internet, the Docker organization provides a so-called repository under <https://hub.docker.com/>. Images stored there are freely accessible. Users can also manage their own repositories.



Note:

For more information on images, see the Docker documentation <https://docs.docker.com/engine/docker-overview/%23docker-objects> and, in particular, its glossary <https://docs.docker.com/glossary/?term=image>.

Container

A container is a runtime instance of an image.

A container represents an image that is being executed in its individual runtime environment and can be compared with a running process. Running an image in a container is commonly denominated as "starting" the container. The term "starting" implies that Docker transfers the image to an individual runtime environment to execute it there. This runtime environment is isolated against host machine and other containers, i.e. neither host machine nor other containers can influence it. Access to resources of the host system as e.g. host files and ports occurs only if explicitly configured.

A container consists of:

- a Docker image,
- a runtime environment, and
- a standard command architecture.

The runtime environment contains e.g. current information on configuration and status. For storing this information, Docker generates a virtual drive in the container, a so-called "volume"

Docker can start several containers, even containers originating from the same image.

**Note:**

For more information on containers, see the Docker documentation (<https://docs.docker.com/get-started/#prerequisites>) and, in particular, its glossary (<https://docs.docker.com/glossary/?term=container>).

9.2 Container for netPI: Examples

The device contains a Docker host enabling the deploy of own Edge automation applications to execute them in safe containers. Since netPI is a Docker host only, you cannot build images on-board. netPI's security concept prohibits SSH servicing and hence you cannot get access to "Docker build commands". Since containers run the same on any compatible hardware use a Raspberry Pi 3 instead for image development. Buying the consumer Pi for a low price is a riskless invest for getting familiar with Docker, making usability and performance tests of applications before moving them onto the professional netPI.

Docker hub is an Internet platform to share container images with co-workers, customers and the Docker community. For netPI there is a registry as well providing you examples for immediate use, such as the Thing Editor Node-RED or a HDMI desktop environment and many more. Use them also as templates for your own ideas when starting creating own images.

Address: <https://hub.docker.com/r/hilschernetpi/>

| Name | Container contains |
|-----------------------------------|---|
| netpi-desktop-hdmi | HDMI desktop environment Activates the HDMI interface to connect a monitor and has a desktop. |
| netpi-raspbian | Raspbian-Betriebssystem Raspbian (jessy) |
| netpi-nodered-fieldbus | Node-RED and fieldbus node Processes I/O data of the Real-Time Ethernet using the Thing Editor Node-RED. netPI can be used for example as PROFINET IO Device, EtherCAT Slave or EtherNet/IP Adapter. |
| netpi-netx-programming-examples | Programming example Processes I/O data of the Real-Time Ethernet using access over the API. netPI can be used for example as PROFINET IO Device, EtherCAT Slave or EtherNet/IP Adapter. |
| netpi-nodered-fram | FRAM and Node-RED Using the FRAM with the Thing Editor Node-RED. |
| netpi-container-build-environment | Container environment Environment to develop container for netPI. |

Table 25: Container for netPI: Examples

The following figure shows a possible usage of containers.

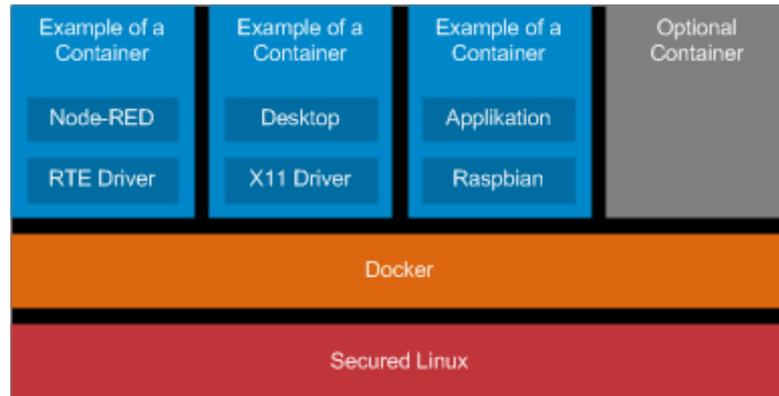


Figure 34: netPI block diagram

9.3 Working with Docker via the web GUI

This section describes

- how to operate Docker via the portainer.io interface of the browser
- how to run additional software on the Edge Gateway with Docker (using the web server NGINX as an example).

9.3.1 The portainer.io interface

Tasks of the portainer.io interface

The portainer.io interface serves:

- to add new containers
- to provide functions for controlling the code execution such as *Start*, *Stop*, *Kill*, *Restart*, *Pause*, *Resume*, and *Remove*
- to configure the containers.

Starting the portainer.io interface for working with the containers

To start the portainer.io interface, proceed as follows:

- Open the Edge Gateway Manager, if it is not already open.
For this purpose see *Calling the Edge Gateway Manager* [▶ page 20]
- Click the tile *Docker Management* in the *Edge Gateway Manager*..



Figure 35: Tile Docker in the Edge Gateway Manager

- ⇒ The portainer.io login screen will be displayed. In the field **Username**, *admin* is already entered. This is the only predefined user name.
- Enter the password for the user name *admin*. This password is set in the user management of the Edge Gateway Manager, see *User management* [▶ page 38].
- ⇒ The start page "Dashboard" of the user interface portainer.io will be displayed.

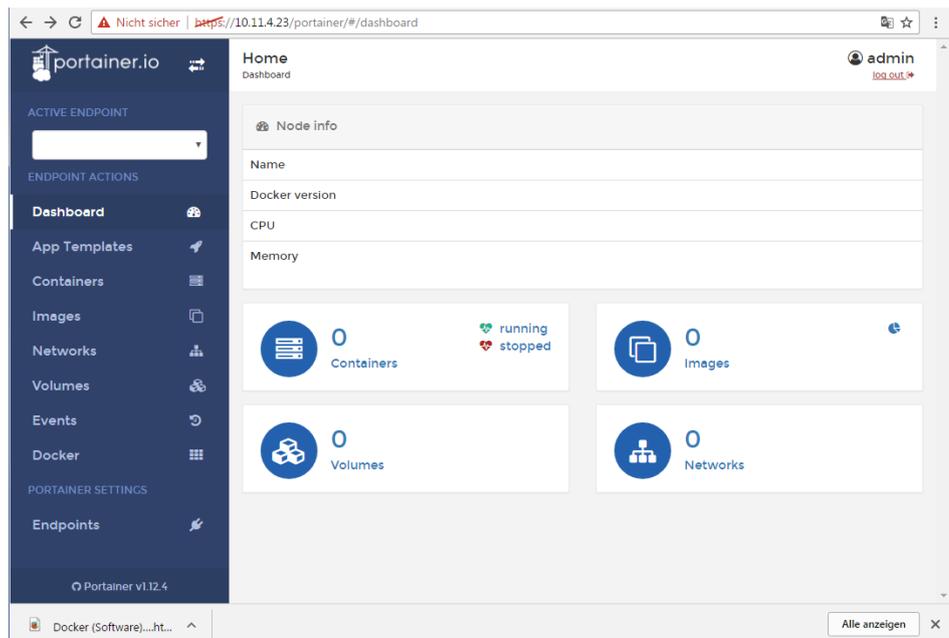


Figure 36: View of portainer.io dashboard

- Click **Containers** in the menu on the left or **Containers** on the page "Dashboard".
- ⇒ The page "Container list" will be displayed. This list contains the names and statuses of all currently known containers and provides the functions for controlling the code execution.

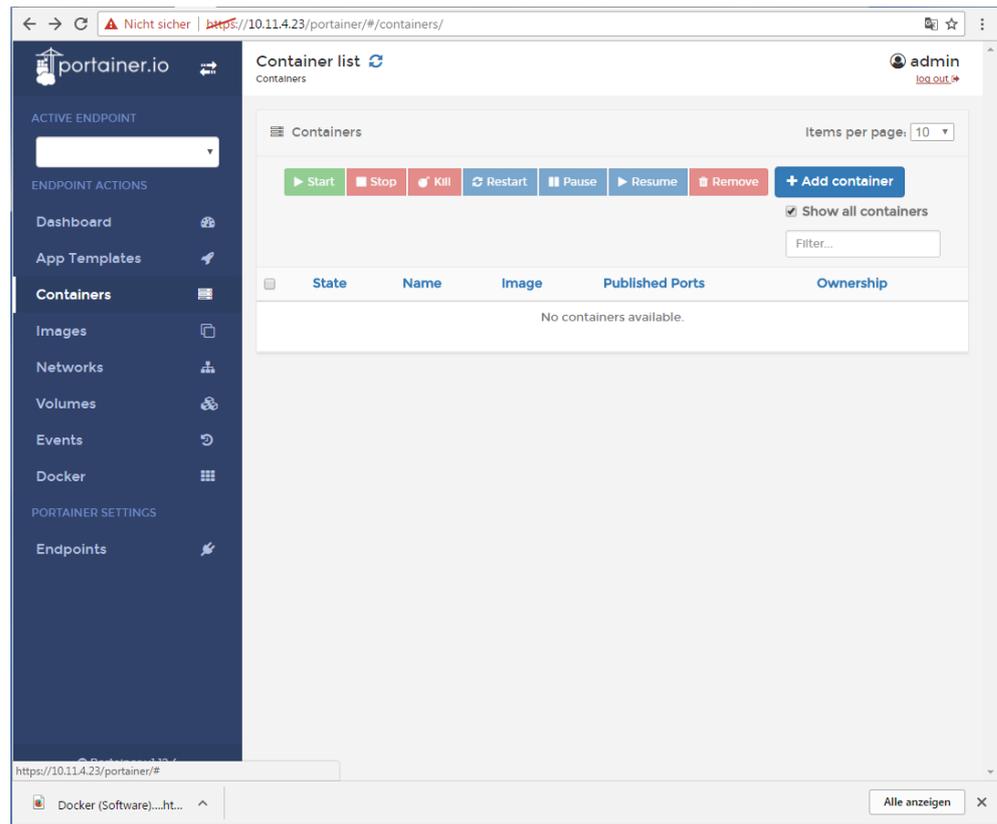


Figure 37: Container list (portainer.io)

Functions for working with containers

Docker provides the following functions for controlling the code execution:

| Icon | Function | Meaning |
|------|----------|---|
| | Start | Starting a container |
| | Stop | Stopping a container |
| | Kill | Aborting the execution of a container |
| | Restart | Repeated starting of a container |
| | Pause | Interrupting the execution of a container temporarily |
| | Resume | Continuing the execution of a container after an interruption |
| | Remove | Deleting a container |

Table 26: Functions for working with containers

9.3.2 Example: Executing the web server NGINX as a container

NGINX is an open-source web server. This section shows how to execute the web server NGINX with Docker on the Edge Gateway.



Note:

Further information on the web server NGINX can be downloaded from <https://nginx.org/>, <https://hub.docker.com/r/lalyos/rpi-nginx/> and <https://en.wikipedia.org/wiki/Nginx>.

Prerequisite

The following prerequisite must be met: The user interface portainer.io is open (see *The portainer.io interface* [▶ page 49]).

Steps

- On the page "Container list" click on **Add container**.
- ⇒ The page "Create container" will be displayed.
- In the field **Name** enter the name of your container, e.g. `MyFirstContainer`.
- In the field **Image** of the area **Image configuration** enter the name of the image to be executed in the container: `lalyos/rpi-nginx`.
- ⇒ The system will automatically search for the image in the official Docker registry, and the NGINX repository (located there) will load it. The http-address of the NGINX repository is <https://hub.docker.com/r/lalyos/rpi-nginx/>.
- Always set the switch **Always pull image** in the area **Image configuration** to **On** (i.e. the switch is in position "right"). This automatically loads the image before the start. A manual loading via the option "Images" from portainer.io is thus no longer required.
- To configure a network-port-assignment between container and Linux-host-system, click the button **map additional port**. This will deviate network port 80, used by NGINX as standard, e.g. to port 8080 and make it accessible for the web browser.
- ⇒ The fields **host** and **container** are shown on the page "Container list".
- Field **host**: Enter the port, e.g. 8080, where the NGINX can be accessed via the web browser.
- Field **container**: Enter the port, e.g. 80, that NGINX uses within the container.
- If required, set the **Advanced options** according to the documentation of the container to be started (in this case: NGINX documentation, <https://hub.docker.com/r/lalyos/rpi-nginx/>). This example does not require any further settings.
- Click on **Start container**.
- ⇒ The configuration of the container is thus ready for the execution of NGINX. Docker will first load the image from the registry (duration 2-3 minutes), deposit it in the Edge Gateway, and transform it into a container thereafter. This container will then appear in the container list and its status changes to *running*.

To check the correct installation of NGINX, proceed as follows:

- Enter the following address in the address line of your web browser:
`http://<IP address of you device>:8080`
- ⇒ The NGINX-start screen will be displayed.

10 Technical data

10.1 Technical data NIOT-E-NPI3-51-EN-RE

| NIOT-E-NPI3-51-EN-RE | Parameter | Value |
|----------------------|---|--|
| Product | Part number | 1321.500 |
| | Application | IoT and Industry 4.0 Edge automation projects |
| Processors | CPU | Broadcom BCM2837 1.2 GHz, 64 bit, 4 cores |
| | Communication controller | netX 51 |
| Integrated memory | RAM | 1 GByte |
| | FLASH | 8 GByte MLC NAND (3000 w/e) |
| | FRAM | 8 KByte |
| Power supply | Supply voltage | 18 V DC ... 30 V DC |
| | Typical/maximum current (at 24 V) | 170 mA / 400 mA |
| | Power consumption | Min. 4.2 W (no USB) Max. 9 W (USB with 1 A) |
| | Connector | 3-pin terminal block (3.5 mm) |
| LAN interface | Interface type | 10BASE-T/100BASE-TX, potential free |
| | Connector | 1 x RJ45 socket |
| Real-Time Ethernet | Interface type | 10BASE-T/100BASE-TX, potential free |
| | Connector | 2 x RJ45 socket |
| | Protocols | EtherCAT Slave EtherNet/IP Adapter PROFINET IO Device |
| Interfaces | USB | 4 x USB 2.0, max. 500 mA max. 1 A for all USB, type A |
| | Wireless | 1 x WiFi, single-band 2.4 GHz IEEE 802.11b/g/n (BCM43438) |
| | Display connector | 1 x HMDI (default: inactive) |
| | Expansion module | 1 x slot for NPIX modules, 52 pins |
| Software | Operating system | Yocto Linux, Kernel 4.9 or higher, AppArmor secured, RT patch used |
| | Docker | 17.04.0-ce or higher with Portainer.io web GUI |
| Security | Access | HTTPS |
| | Trusted platform | TPM 1.2 (inactive) |
| Display | LED display | 8 LEDs (2 programable) |
| Real-time clock | Buffering | Capacitor buffered, max. 7 days backup, maintenance free |
| Environment | Ambient temperature range for operation | -20°C ... +60°C |
| | Ambient temperature range for storage | -40°C ... +85°C |
| Device | Dimensions (H x W x L) | 140 mm x 35 mm x 105 mm |
| | Weight | 400 g |
| | Housing | Metal |
| | Mounting | DIN top hat rail |
| | Degree of protection | IP 20 |

| NIOT-E-NPI3-51-EN-RE | Parameter | Value |
|---------------------------------|--|----------------------------|
| Conformity | FCC | FCC ID: 2ANEG0001 |
| | RoHS | Yes |
| Conformance with EMC directives | CE sign | Yes |
| | Emission | EN 55011:2009 |
| | Immunity | EN 61000-6-2/3, EN 61131-2 |
| | Electrostatic discharge (ESD) (air and contact discharge method) | EN 61000-4-2 |
| | Fast transient interferences (Burst) | EN 61000-4-4 |
| | Surge voltage | EN 61000-4-5 |
| Tests | Shock | IEC 60068-2-27 Ea |
| | Vibration | IEC 60068-2-6 Fc |

Table 27: Technical data NIOT-E-NPI3-51-EN-RE

11 FCC authorization

FCC ID: 2ANEG0001

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Figure 38: FCC label

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

12 Decommissioning, dismantling and disposal

12.1 Putting the device out of operation

NOTICE**Danger of Unsafe System Operation!**

To prevent personal injury or property damage, make sure that the removal of the device from your plant during operation will not affect the safe operation of the plant.

- Disconnect all communication cables from the device.
 - Disconnect the power supply plug.
 - Remove the device from the DIN top hat rail. .
-

12.2 Removing device from top hat rail

- Before dismantling the Edge Gateway from the top hat rail, first remove the power supply cable and all data cables from the device.
- Put a screw driver into the slot of the latch at the bottom of the device.
- To disengage the lock of the hook, pull down the latch with the screw driver.
- Take the device off the top hat rail.

12.3 Disposal of waste electronic equipment

Important notes from the European Directive 2012/16/EU "Waste Electrical and Electronic Equipment (WEEE)"

**Waste electronic equipment****Art und Quelle der Gefahr**

This product must not be treated as household waste.

This product must be disposed of at a designated waste electronic equipment collecting point.

Waste electronic equipment may not be disposed of as household waste. As a consumer, you are legally obliged to dispose of all waste electronic equipment according to national and local regulations.

13 Appendix

13.1 Legal notes

Copyright

© Hilscher Gesellschaft für Systemautomation mbH

All rights reserved.

The images, photographs and texts in the accompanying materials (in the form of a user's manual, operator's manual, Statement of Work document and all other document types, support texts, documentation, etc.) are protected by German and international copyright and by international trade and protective provisions. Without the prior written consent, you do not have permission to duplicate them either in full or in part using technical or mechanical methods (print, photocopy or any other method), to edit them using electronic systems or to transfer them. You are not permitted to make changes to copyright notices, markings, trademarks or ownership declarations. Illustrations are provided without taking the patent situation into account. Any company names and product designations provided in this document may be brands or trademarks by the corresponding owner and may be protected under trademark, brand or patent law. Any form of further use shall require the express consent from the relevant owner of the rights.

Important notes

Utmost care was/is given in the preparation of the documentation at hand consisting of a user's manual, operating manual and any other document type and accompanying texts. However, errors cannot be ruled out. Therefore, we cannot assume any guarantee or legal responsibility for erroneous information or liability of any kind. You are hereby made aware that descriptions found in the user's manual, the accompanying texts and the documentation neither represent a guarantee nor any indication on proper use as stipulated in the agreement or a promised attribute. It cannot be ruled out that the user's manual, the accompanying texts and the documentation do not completely match the described attributes, standards or any other data for the delivered product. A warranty or guarantee with respect to the correctness or accuracy of the information is not assumed.

We reserve the right to modify our products and the specifications for such as well as the corresponding documentation in the form of a user's manual, operating manual and/or any other document types and accompanying texts at any time and without notice without being required to notify of said modification. Changes shall be taken into account in future manuals and do not represent an obligation of any kind, in particular there shall be no right to have delivered documents revised. The manual delivered with the product shall apply.

Under no circumstances shall Hilscher Gesellschaft für Systemautomation mbH be liable for direct, indirect, ancillary or subsequent damage, or for any loss of income, which may arise after use of the information contained herein.

Liability disclaimer

The hardware and/or software was created and tested by Hilscher Gesellschaft für Systemautomation mbH with utmost care and is made available as is. No warranty can be assumed for the performance or flawlessness of the hardware and/or software under all application conditions and scenarios and the work results achieved by the user when using the hardware and/or software. Liability for any damage that may have occurred as a result of using the hardware and/or software or the corresponding documents shall be limited to an event involving willful intent or a grossly negligent violation of a fundamental contractual obligation. However, the right to assert damages due to a violation of a fundamental contractual obligation shall be limited to contract-typical foreseeable damage.

It is hereby expressly agreed upon in particular that any use or utilization of the hardware and/or software in connection with

- Flight control systems in aviation and aerospace;
- Nuclear fusion processes in nuclear power plants;
- Medical devices used for life support and
- Vehicle control systems used in passenger transport

shall be excluded. Use of the hardware and/or software in any of the following areas is strictly prohibited:

- For military purposes or in weaponry;
- For designing, engineering, maintaining or operating nuclear systems;
- In flight safety systems, aviation and flight telecommunications systems;
- In life-support systems;
- In systems in which any malfunction in the hardware and/or software may result in physical injuries or fatalities.

You are hereby made aware that the hardware and/or software was not created for use in hazardous environments, which require fail-safe control mechanisms. Use of the hardware and/or software in this kind of environment shall be at your own risk; any liability for damage or loss due to impermissible use shall be excluded.

Warranty

Hilscher Gesellschaft für Systemautomation mbH hereby guarantees that the software shall run without errors in accordance with the requirements listed in the specifications and that there were no defects on the date of acceptance. The warranty period shall be 12 months commencing as of the date of acceptance or purchase (with express declaration or implied, by customer's conclusive behavior, e.g. putting into operation permanently).

The warranty obligation for equipment (hardware) we produce is 36 months, calculated as of the date of delivery ex works. The aforementioned provisions shall not apply if longer warranty periods are mandatory by law pursuant to Section 438 (1.2) BGB, Section 479 (1) BGB and Section 634a (1) BGB [Bürgerliches Gesetzbuch; German Civil Code] If, despite of all due care taken, the delivered product should have a defect, which already existed at the time of the transfer of risk, it shall be at our discretion to either repair the product or to deliver a replacement product, subject to timely notification of defect.

The warranty obligation shall not apply if the notification of defect is not asserted promptly, if the purchaser or third party has tampered with the products, if the defect is the result of natural wear, was caused by unfavorable operating conditions or is due to violations against our operating regulations or against rules of good electrical engineering practice, or if our request to return the defective object is not promptly complied with.

Costs of support, maintenance, customization and product care

Please be advised that any subsequent improvement shall only be free of charge if a defect is found. Any form of technical support, maintenance and customization is not a warranty service, but instead shall be charged extra.

Additional guarantees

Although the hardware and software was developed and tested in-depth with greatest care, Hilscher Gesellschaft für Systemautomation mbH shall not assume any guarantee for the suitability thereof for any purpose that was not confirmed in writing. No guarantee can be granted whereby the hardware and software satisfies your requirements, or the use of the hardware and/or software is uninterrupted or the hardware and/or software is fault-free.

It cannot be guaranteed that patents and/or ownership privileges have not been infringed upon or violated or that the products are free from third-party influence. No additional guarantees or promises shall be made as to whether the product is market current, free from deficiency in title, or can be integrated or is usable for specific purposes, unless such guarantees or promises are required under existing law and cannot be restricted.

Confidentiality

The customer hereby expressly acknowledges that this document contains trade secrets, information protected by copyright and other patent and ownership privileges as well as any related rights of Hilscher Gesellschaft für Systemautomation mbH. The customer agrees to treat as confidential all of the information made available to customer by Hilscher Gesellschaft für Systemautomation mbH and rights, which were disclosed by Hilscher Gesellschaft für Systemautomation mbH and that were made accessible as well as the terms and conditions of this agreement itself.

The parties hereby agree to one another that the information that each party receives from the other party respectively is and shall remain the intellectual property of said other party, unless provided for otherwise in a contractual agreement.

The customer must not allow any third party to become knowledgeable of this expertise and shall only provide knowledge thereof to authorized users as appropriate and necessary. Companies associated with the customer shall not be deemed third parties. The customer must obligate authorized users to confidentiality. The customer should only use the confidential information in connection with the performances specified in this agreement.

The customer must not use this confidential information to his own advantage or for his own purposes or rather to the advantage or for the purpose of a third party, nor must it be used for commercial purposes and this confidential information must only be used to the extent provided for in this agreement or otherwise to the extent as expressly authorized by the disclosing party in written form. The customer has the right, subject to the obligation to confidentiality, to disclose the terms and conditions of this agreement directly to his legal and financial consultants as would be required for the customer's normal business operation.

Export provisions

The delivered product (including technical data) is subject to the legal export and/or import laws as well as any associated regulations of various countries, especially such laws applicable in Germany and in the United States. The products / hardware / software must not be exported into such countries for which export is prohibited under US American export control laws and its supplementary provisions. You hereby agree to strictly follow the regulations and to yourself be responsible for observing them. You are hereby made aware that you may be required to obtain governmental approval to export, reexport or import the product.

Terms and conditions

Please read the notes about additional legal aspects on our netIOT web site under <http://www.netiot.com/netiot/netiot-edge/terms-and-conditions/>.

List of figures

| | | |
|------------|---|----|
| Figure 1: | netPI | 5 |
| Figure 2: | NIOT-E-NPI3-51-EN-RE (Top view)..... | 6 |
| Figure 3: | NIOT-E-NPI3-51-EN-RE (Front view)..... | 6 |
| Figure 4: | NIOT-E-NPI3-51-EN-RE (Bottom view)..... | 7 |
| Figure 5: | Dimensions | 8 |
| Figure 6: | LED positions | 11 |
| Figure 7: | Gateway status LEDs | 12 |
| Figure 8: | Default settings of the Ethernet network connectors | 17 |
| Figure 9: | netIOT Edge Gateway in the Windows network | 19 |
| Figure 10: | Edge Gateway Manager | 20 |
| Figure 11: | Edge Gateway Manager - Setting the administrator password | 23 |
| Figure 12: | Security error message of the Internet Explorer | 25 |
| Figure 13: | Security error message of the Firefox browser (1) | 25 |
| Figure 14: | Security error message of the Firefox browser (2) | 25 |
| Figure 15: | Firefox dialog box: Adding exceptional safety rule | 26 |
| Figure 16: | Security error message of Google Chrome (1)..... | 27 |
| Figure 17: | Security error message of Google Chrome (2)..... | 27 |
| Figure 18: | Main menu of the Control Panel | 28 |
| Figure 19: | Page Info Center | 29 |
| Figure 20: | Time configuration page | 30 |
| Figure 21: | Reboot safety query | 32 |
| Figure 22: | Warning for consequences of shutdown | 33 |
| Figure 23: | Hostname | 36 |
| Figure 24: | List of default services | 37 |
| Figure 25: | Page for configuring roles..... | 38 |
| Figure 26: | User account page | 40 |
| Figure 27: | Security submenu | 41 |
| Figure 28: | Page SSL Certificate | 41 |
| Figure 29: | SSL Certificate – Upload area | 42 |
| Figure 30: | SSL Certificate – Info area | 43 |
| Figure 31: | Info page..... | 44 |
| Figure 32: | User profile page | 44 |
| Figure 33: | Dialog "Edit user account" | 45 |
| Figure 34: | netPI block diagram..... | 49 |
| Figure 35: | Tile Docker in the Edge Gateway Manager | 50 |
| Figure 36: | View of portainer.io dashboard..... | 50 |
| Figure 37: | Container list (portainer.io) | 51 |
| Figure 38: | FCC label..... | 56 |

List of tables

| | | |
|-----------|---|----|
| Table 1: | List of revisions | 4 |
| Table 2: | Further information | 4 |
| Table 3: | Positions of the interfaces..... | 7 |
| Table 4: | Power supply connector | 9 |
| Table 5: | Names of the LEDs..... | 11 |
| Table 6: | Description of gateway status LEDs | 12 |
| Table 7: | LEDs LAN interface | 13 |
| Table 8: | LED states for the PROFINET IO-Device protocol | 14 |
| Table 9: | LED state definitions for the PROFINET IO-Device protocol..... | 14 |
| Table 10: | LED states for the EtherCAT Slave protocol | 15 |
| Table 11: | LED state definitions for the EtherCAT Slave protocol | 15 |
| Table 12: | LED states for the EtherNet/IP Adapter protocol..... | 16 |
| Table 13: | LED state definitions for the EtherNet/IP Adapter protocol..... | 16 |
| Table 14: | Starting applications with the Edge Gateway manager | 21 |
| Table 15: | Functional overview of the Control Panel | 28 |
| Table 16: | Info Center: Area System info..... | 29 |
| Table 17: | Info Center: Area Monitoring..... | 30 |
| Table 18: | Info Center: Area Temperature | 30 |
| Table 19: | Setting the system time | 30 |
| Table 20: | Table LAN: Meaning of the columns..... | 35 |
| Table 21: | Operating statuses of the services | 37 |
| Table 22: | Access rights onto resources..... | 39 |
| Table 23: | Access rights to resources..... | 39 |
| Table 24: | Information about the security certificate | 43 |
| Table 25: | Container for netPI: Examples | 48 |
| Table 26: | Functions for working with containers..... | 51 |
| Table 27: | Technical data NIOT-E-NPI3-51-EN-RE | 54 |

Contacts

HEADQUARTERS

Germany

Hilscher Gesellschaft für
Systemautomation mbH
Rheinstrasse 15
65795 Hattersheim
Phone: +49 (0) 6190 9907-0
Fax: +49 (0) 6190 9907-50
E-mail: info@hilscher.com

Support

Phone: +49 (0) 6190 9907-99
E-mail: de.support@hilscher.com

SUBSIDIARIES

China

Hilscher Systemautomation (Shanghai) Co. Ltd.
200010 Shanghai
Phone: +86 (0) 21-6355-5161
E-mail: info@hilscher.cn

Support

Phone: +86 (0) 21-6355-5161
E-mail: cn.support@hilscher.com

France

Hilscher France S.a.r.l.
69500 Bron
Phone: +33 (0) 4 72 37 98 40
E-mail: info@hilscher.fr

Support

Phone: +33 (0) 4 72 37 98 40
E-mail: fr.support@hilscher.com

India

Hilscher India Pvt. Ltd.
Pune, Delhi, Mumbai
Phone: +91 8888 750 777
E-mail: info@hilscher.in

Italy

Hilscher Italia S.r.l.
20090 Vimodrone (MI)
Phone: +39 02 25007068
E-mail: info@hilscher.it

Support

Phone: +39 02 25007068
E-mail: it.support@hilscher.com

Japan

Hilscher Japan KK
Tokyo, 160-0022
Phone: +81 (0) 3-5362-0521
E-mail: info@hilscher.jp

Support

Phone: +81 (0) 3-5362-0521
E-mail: jp.support@hilscher.com

Korea

Hilscher Korea Inc.
Seongnam, Gyeonggi, 463-400
Phone: +82 (0) 31-789-3715
E-mail: info@hilscher.kr

Switzerland

Hilscher Swiss GmbH
4500 Solothurn
Phone: +41 (0) 32 623 6633
E-mail: info@hilscher.ch

Support

Phone: +49 (0) 6190 9907-99
E-mail: ch.support@hilscher.com

USA

Hilscher North America, Inc.
Lisle, IL 60532
Phone: +1 630-505-5301
E-mail: info@hilscher.us

Support

Phone: +1 630-505-5301
E-mail: us.support@hilscher.com