SIEMENS

Reyrolle 7SR5 Operating

V2.31

Manual

C53000-B7040-C013-1

NOTE

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Document version: C53000-B7040-C013-1.01

Edition: 05.2022

Version of the product described: V2.31

Preface

Purpose of the Manual

This manual describes the operation of the device and gives information about safety, commissioning, and operation as well as checks and tests.

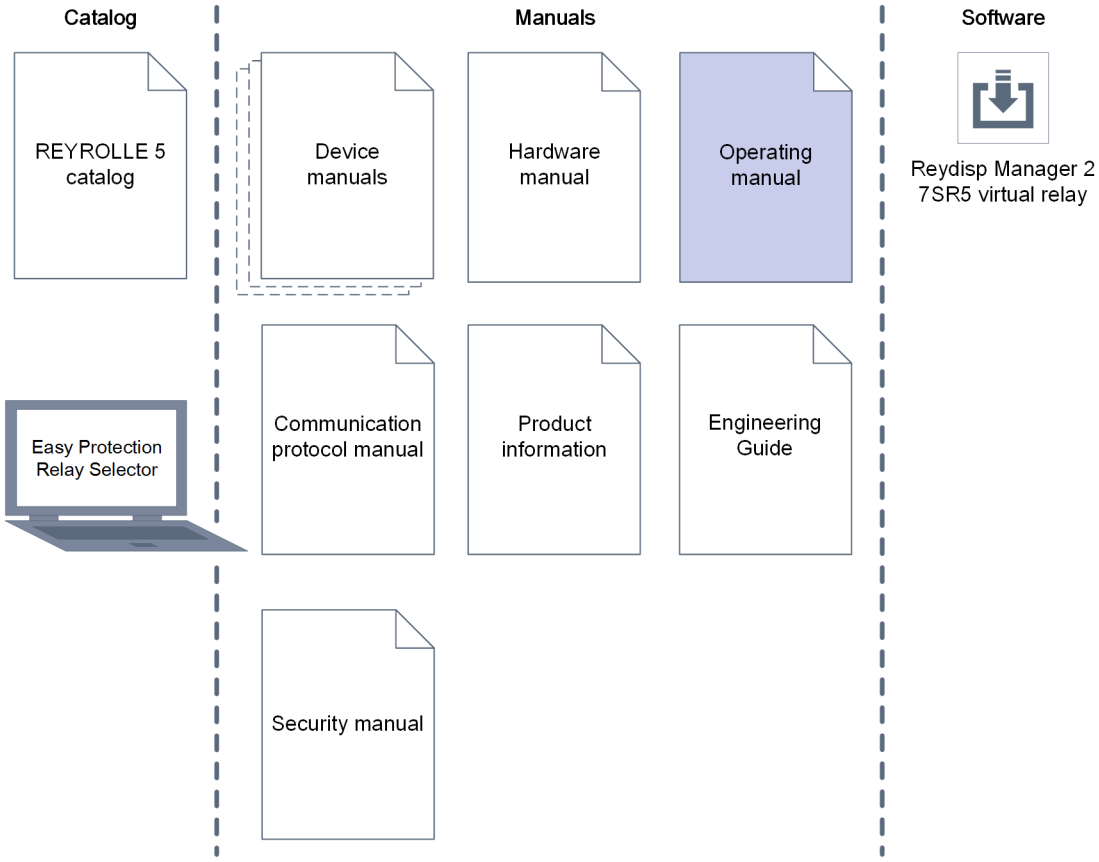
Target Audience

This manual is mainly intended for protection system engineers, commissioning engineers, persons entrusted with the setting, testing and maintenance of automation, selective protection and control equipment, and operational crew in electrical installations and power plants.

Scope

This manual applies to the Reyrolle 7SR5 device family.

Further Documentation



[dw_7SR5_furtherdocumentation_operatingmanual, 4, en_US]

- Device manuals
  Each device manual describes the functions and applications of a specific Reyrolle 7SR5 device. The printed manual for the device has the same informational structure.
- Hardware manual
  The hardware manual describes the hardware building blocks and device combinations of the Reyrolle 7SR5 device family.
- Operating manual
  The operating manual describes the basic principles and procedures for operating and installing the devices of the Reyrolle 7SR5 range.
- Communication protocol manual
  The communication protocol manual contains a description of the protocols for communication within the Reyrolle 7SR5 device family and to higher-level network control centers.
- Security manual
  The security manual describes the security features of the Reyrolle 7SR5 devices and Reydisp Manager 2.
- Product information
  The product information includes general information about device installation, technical data, limiting values for input and output modules, and conditions when preparing for operation. This document is provided with each Reyrolle 7SR5 device.
- Engineering Guide
  The engineering guide describes the essential steps when engineering with Reydisp Manager 2. In addition, the engineering guide shows you how to load a planned configuration to a Reyrolle 7SR5 device and update the functionality of the Reyrolle 7SR5 device.
- Virtual Relay
  The virtual relay allows a user to view, control and manipulate a virtual Reyrolle 7SR5 device. The virtual relay is a tool that can facilitate training and understanding of the controls and functions on a Reyrolle 7SR5 device.
- Reyrolle 7SR5 catalog
  The Reyrolle 7SR5 catalog describes the system features and the devices of Reyrolle 7SR5.
- Easy Protection Relay Selector for Reyrolle and SIPROTEC
  This tool gives a quick guidance to find a protection relay of SIPROTEC 5, SIPROTEC 4, SIPROTEC Compact, Reyrolle which would fit your needs.

Additional Support

For questions about the system, contact your Siemens sales partner.

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens AG
Smart Infrastructure – Protection Automation
Customer Support Center

Tel.: +49 911 2155 4466
E-Mail: *energy.automation@siemens.com*

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG
Siemens Power Academy TD
Humboldtstraße 59
90459 Nuremberg
Germany

Phone: +49 911 9582 7100
E-mail: *poweracademy@siemens.com*
Internet: *www.siemens.com/poweracademy*

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid property damage.

NOTE

Important information about the product, product handling or a certain section of the documentation which must be given attention.

OpenSSL

This product includes software developed by the OpenSSL Project for use in OpenSSL Toolkit (*http://www.openssl.org/*).

This product includes software written by Tim Hudson (*tjh@cryptsoft.com*).

This product includes cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Table of Contents

1 First Steps

1.1 Unpacking, Repacking, Returning, and Storing

Unpacking a Device

NOTE

Devices are tested prior to delivery. The test certificate is a component of the devices.

- Check the packaging for external transport damage. Damaged packaging may indicate that the devices inside have also sustained damage.
- Unpack devices carefully; do not use force.
- Check the devices via a reception control to ensure they are in perfect mechanical condition.
- Check the enclosed accessories against the delivery note to make sure everything is complete.
- Keep the packaging in case the devices must be stored or transported elsewhere.
- Return damaged devices to the manufacturer, stating the defect. Use the original packaging or transport packaging where possible.
- Check the wiring terminal connectors are all included.
- Check the mounting fixings are included.
- Check the screws are included – one packet per terminal block.

Repacking a Device

- If you store devices after reception control, they must be packed in appropriate storage packaging.
- If the device is to be transported, pack it in transport packaging.
- Enclose the accessories supplied and the test certificate in the package with the device.

Returning a Device

- Return devices to the manufacturer, stating the defect. Use the original packaging or transport packaging where possible. Send damaged devices to the following address:

  Siemens AG
  EM DG PRO MF Rückwaren
  Rohrdamm 7
  13629 Berlin
  Germany
- Protect the optical interfaces on the communication modules and AFD when fitted against the ingress of dust. Use, for example, the protective caps provided in the delivery condition.

Storing a Device

- Only store devices on which you have carried out an incoming inspection, This action ensures that the warranty remains valid. The incoming inspection is described in *1.3 Incoming Inspection*.
- Reyrolle devices must be stored in rooms, which are clean and dry. Devices must be stored at a temperature of -25 °C to +70 °C.
- The relative humidity must be at a level where condensed water and ice are prevented from forming.
- Siemens recommends that you observe a restricted storage temperature range of +10 °C to +35 °C, in order to prevent the electrolytic capacitors used in the power supply from ageing prematurely.

- If the device has been in storage for more than 2 years, connect it to an auxiliary voltage for 1 to 2 days. This action will cause the electrolytic capacitors to form on the printed circuit board assemblies again.
- If devices are to be shipped elsewhere, you can reuse the transport packaging. Storage packing of the individual devices is not adequate for transport purposes.

1.2 Environmental Protection Hints

Disposal of Old Equipment and Batteries (Applicable only for European Union and Countries with a Recycling System)

The disposal of our products and possible recycling of their components after decommissioning has to be carried out by an accredited recycling company, or the products/components must be taken to applicable collection points. Such disposal activities must comply with all local laws, guidelines and environmental specifications of the country in which the disposal is done. For the European Union the sustainable disposal of electronic scrap is defined in the respective regulation for "waste electrical and electronic equipment" (WEEE).

The crossed-out wheelie bin on the products, packaging and/or accompanying documents means that used electrical and electronic products and batteries must not be mixed with normal household waste.

According to national legislation, penalties may be charged for incorrect disposal of such waste.

By disposing of these products correctly you will help to save valuable resources and prevent any potential negative effects on human health and the environment.

NOTE

Our products and batteries must not be disposed of as household waste. For disposing batteries it is necessary to observe the local national/international directives.

Disposal of Mobile Storage Devices (e.g. USB Sticks and Memory Cards)

When disposing of/transferring mobile storage devices, using the **format** or **delete** functions only changes the file management information and does not completely delete the data from your mobile storage device. When disposing of or transferring a mobile storage device, Siemens strongly recommends physically destroying it or completely deleting data from the mobile storage device by using a commercially available computer data erasing software.

REACH/RoHS Declaration

You can find our current **REACH/RoHS** declarations at:
https://www.siemens.com/global/en/home/products/energy/ecotransparency/ecotransparency-downloads.html

NOTE

You can find more information about activities and programs to protect the climate at the EcoTransparency website:
https://www.siemens.com/global/en/home/products/energy/ecotransparency.html

1.3 Incoming Inspection

Safety Notes

DANGER

Danger during incoming inspection

Noncompliance with the safety notes, can result in death, severe injury or considerable material damage.

✧ Comply with all given safety notes when carrying out the incoming inspection.

✧ Please note that hazardous voltages are present when you perform the incoming inspection.

- If you identify a defect during the incoming inspection, do not rectify it yourself. Repack the device and return it to the manufacturer, stating the defect. Use the original packaging or transport packaging where possible.

Performing a Follow-Up Inspection on a Device

- Visually check for external damage as soon as you have unpacked the devices; they must not show any signs of dents or cracks.

Checking the Rated Data and Functions

- Check the rated data and functions using the complete order designation/the product code. The device manual contains all technical data and a description of the functions.
- Check the information provided on the rating plate too. The device features a product adhesive label, which contains the Technical data.
- Make sure that the rated data of the device properly matches the power-system data. You can find the necessary information in the device manual.

1.4 Electrical Inspection

Device Protection

DANGER

Danger when connecting the 7SR5 device

Noncompliance with the safety notes will result in death, severe injury or considerable material damage.

✧ The device must be situated in the operating area for at least 2 hours before you connect it to the power supply for the first time. This prevents condensate from forming in the device.

✧ If the device has been in storage for more than 2 years, connect it to an auxiliary voltage for 1 to 2 days. This will cause the electrolytic capacitors on the printed circuit-board assemblies to form again.

- Perform the electrical inspection.

Earthing a Device

The 7SR5 devices are protection class I equipment and must be connected to the system earth prior to commissioning.

- Terminal B28 (power supply unit) should be connected to the case earth stud. A minimum wire size of 2.5 mm^2 is recommended.
  The case earth stud should be solidly earthed to the panel earth. Located at the top rear of the case is a case earth stud, this must be connected to the main panel earth.

Connecting a Device

- Connect all cables and lines. Use the connection diagrams in the Hardware and Device manuals. Use the screws provided.
- Tighten the terminal screws. The rear terminal blocks comprise M4 female terminals for wire connections. Each terminal can accept 2 x M4 diameter crimps.

Safety Notes

DANGER

Danger during electrical inspection

Noncompliance with the safety notes will result in death, severe injury or considerable material damage.

✧ Comply with all given safety notes when carrying out the electrical inspection.

✧ Please note that hazardous voltages are present when you perform the electrical inspection.

- During the electrical inspection, check that the device becomes ready for operation once it has been connected to the power supply.

Performing the Electrical Inspection

- Connect the power supply via an external HRC fuse rated at 6 A (BS88/IEC 60259).
- Ensure that the correct auxiliary supply voltage and polarity is applied to B22 and B24 terminals, by using diagrams for the relay connections. Terminal B28 should be connected to the case earth stud.

- Activate the power supply.

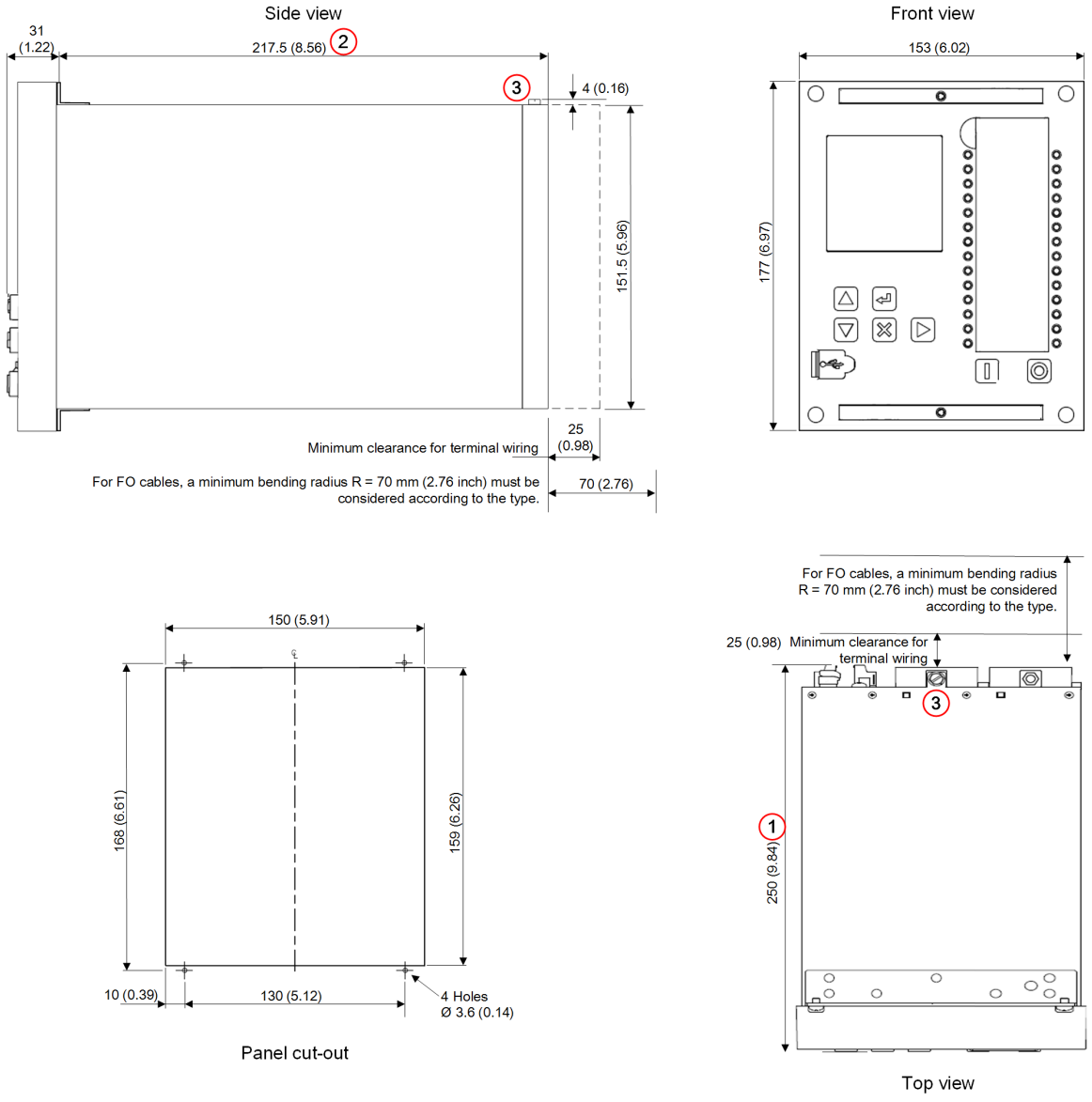
  After (initial) activation, the **`Device Not Configured`** message will be displayed on the LCD screen after a short duration if the user has not changed any parameter in the device.

  The display of the message cannot be disabled, the act of changing any parameter or loading a user configuration will automatically turn it off.

- If the device fails to power on, pack this device and return it to the manufacturer, stating the defect.
- COM-1 port RS485 (Block A and X1 Terminals) connection to this communication facility is by screened, twisted pair cable. On site when wiring other facilities ensure that these terminals are not obscured by other wiring runs. Cable should be RS485 compliant.
- Laser class 1 is maintained in compliance with EN 60825-1 and EN 60825-2 when using 1 mm polymer optical fibres.

2 Installing the Devices

2.1 Device Dimensions and Drilling Drawings



Dimensions in mm. Values in brackets in inches.

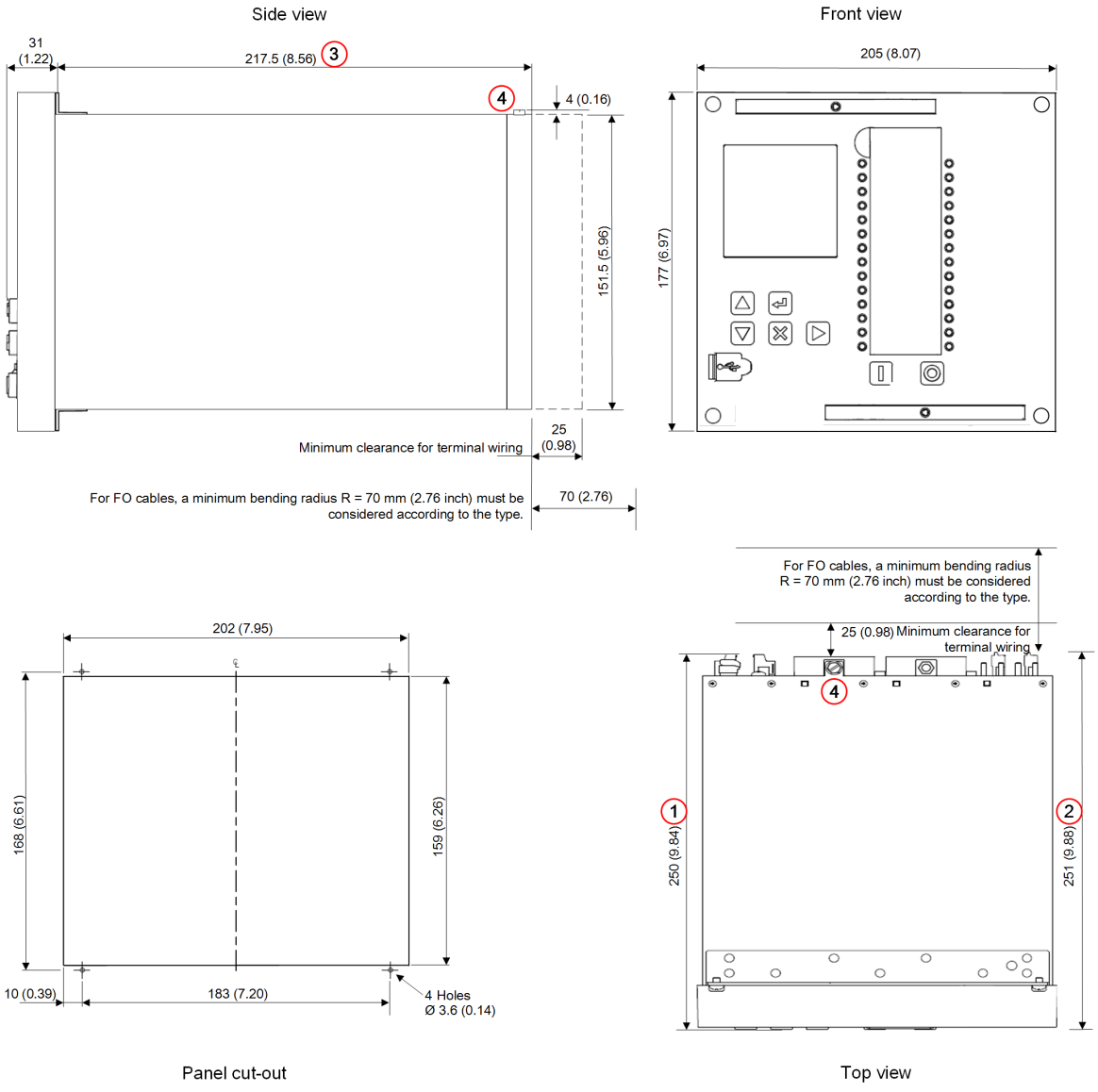
[dw_7SR5_E6_dimensions, 5, en_US]

Figure 2-1 Size 6 Case

(1) Overall length with AFD/RS485 plugs
(2) Overall length to standard terminal blocks
(3) Earth screw

NOTE

3.6 mm holes are suitable for M4 thread-forming screws supplied with the device for typical panel thickness.



Dimensions in mm. Values in brackets in inches.

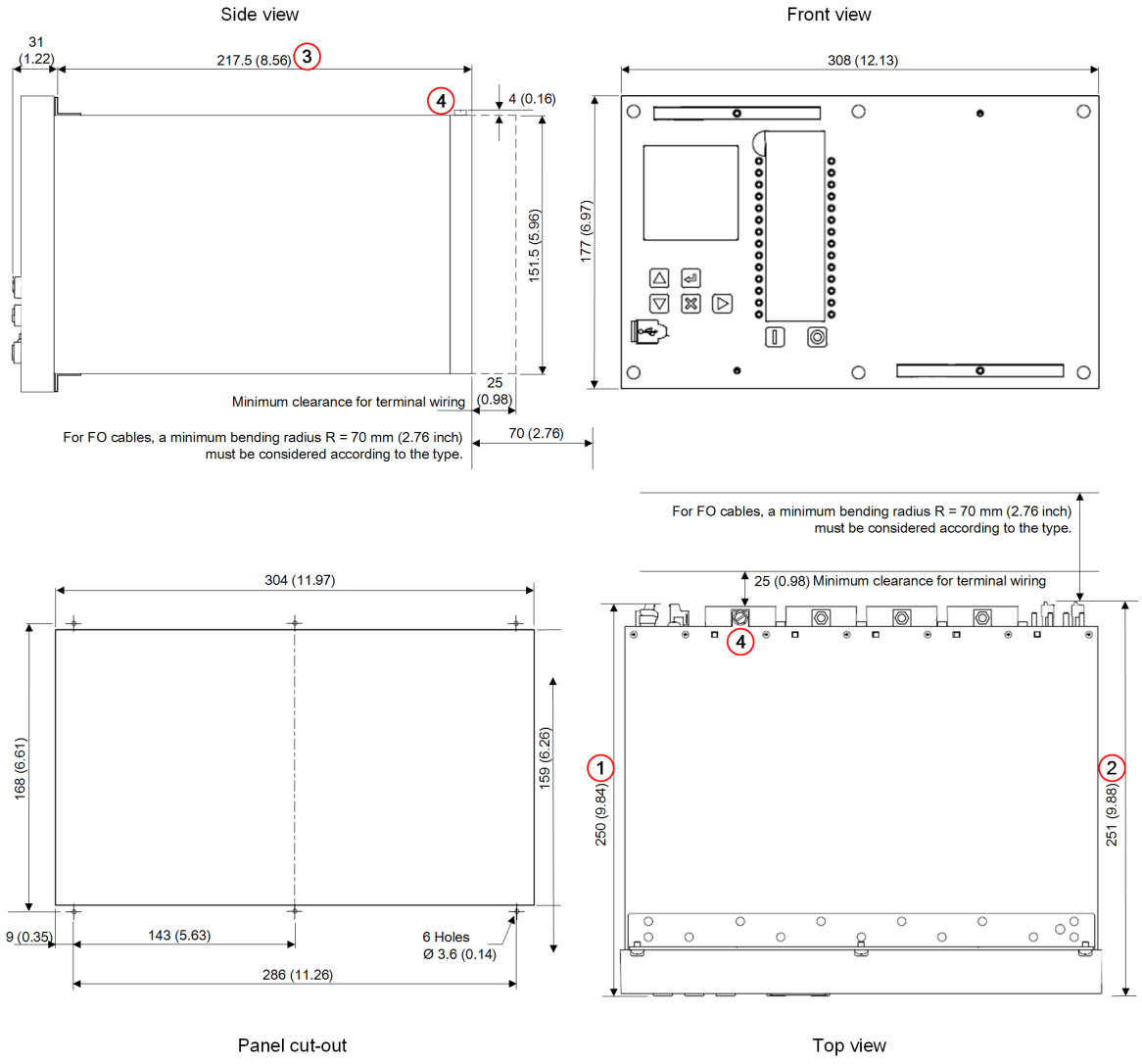
[dw_7SR5_E8_dimensions, 2, en_US]

Figure 2-2 Size 8 Case

(1) Overall length with AFD/RS485 plugs
(2) Overall length with TSI plugs
(3) Overall length to standard terminal blocks
(4) Earth screw

NOTE

3.6 mm holes are suitable for M4 thread-forming screws supplied with the device for typical panel thickness.



[dw_7SR5_E12_dimensions, 5, en_US]

Figure 2-3 Size 12 Case

(1) Overall length with AFD/RS485 plugs
(2) Overall length with TSI plugs
(3) Overall length to standard terminal blocks
(4) Earth screw

NOTE

3.6 mm holes are suitable for M4 thread-forming screws supplied with the device for typical panel thickness.

2.2 Installing Devices

Preparations

NOTE

The installation depth for 1 device is at least 275 mm (11.83 in). This dimension may need to be enhanced to accomodate the necessary bending radius for the various connectors.

The ∅ 3.6 mm holes are for M4 thread forming trilobular screws. These are supplied as standard and suitable for use in Ferrous/Aluminium panels 1.6 mm thick and above. For other panels, holes to be M4 clearance (typically ∅ 4.5 mm) and relays mounted using M4 screws, nuts and lockwashers (Supplied in panel fixing kit).

WARNING

Danger due to device being improperly screw-fastened

Incomplete and careless screw-fastening can lead to death, severe injury, and considerable material damage.

✧ Ensure that screw fastening is installed and secure at all intended bolting points.

- If no assembly opening is prepared, then cut out the required assembly opening.
- Produce the holes as shown in the drilling plan.

Fitting Devices

- Insert the device in the installation opening. Make sure that the fastening screws of the on-site operation panels also protrude exactly into the openings.
- Secure the device to the panel at the top and bottom using the M4 machine screws, lock washers, and nuts provided. All fixing points should by used, the size 6 and 8 case has 4 fixing points and the size 12 has 6 fixing points, and checked and tightened to ensure the device is secure.
- Check for secure attachment.

Fixings

Crimps

Ring tongued crimps with 90° bend are recommended.

Panel Fixings

Typical mounting screw kit per device consists of:

- Case 6
  - 4 off M4 x 10 mm screws
  - 4 off M4 nuts
  - 4 off M4 lock washers
- Case 8
  - 4 off M4 x 10 mm screws
  - 4 off M4 nuts
  - 4 off M4 lock washers

- Case 12
  - 6 off M4 x 10 mm screws
  - 6 off M4 nuts
  - 6 off M4 lock washers

A typical rear terminal block fixing kit (1 kit per used terminal block fitted to relay) consists of:

- 28 x M4, 8 mm screws
- 28 x M4 lock washers

NOTE

Fixing kits are not supplied for unused terminal blocks, refer to the wiring diagram for the number of blocks used.

2.3 Connections and Earthing

Earthing the Devices

The 7SR5 devices are protection class I equipment and must be connected to the system earth before commissioning.

DANGER

Danger due to device being improperly earthed

Incomplete and careless earthing leads to death, severe injury, and considerable material damage!

- ✧ The device must be situated in the operating area for at least 2 hours before you connect it to the power supply for the first time. This method prevents condensation of water in the device.
- ✧ If the device has been in storage for more than 2 years, connect it to an auxiliary voltage for 1 to 2 days. This will cause the electrolytic capacitors to form on the printed circuit board assemblies again.

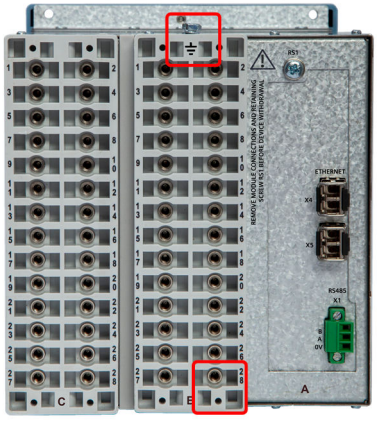
The case earth stud should be solidly earthed to the panel earth. Terminal B28 (power supply unit) should be connected to the case earth stud. A minimum wire size of 2.5 mm^2 is recommended.

Connecting Devices

- Connect all cables and leads. Use the connection diagrams in the Hardware and Device manuals.

Earthing the Device

- Join several on-site operation panels to one another with firm contact.
  The case earth stud should be solidly earthed to the panel earth. Terminal B28 (power supply unit) should be connected to the case earth stud. A minimum wire size of 2.5 mm^2 is recommended.



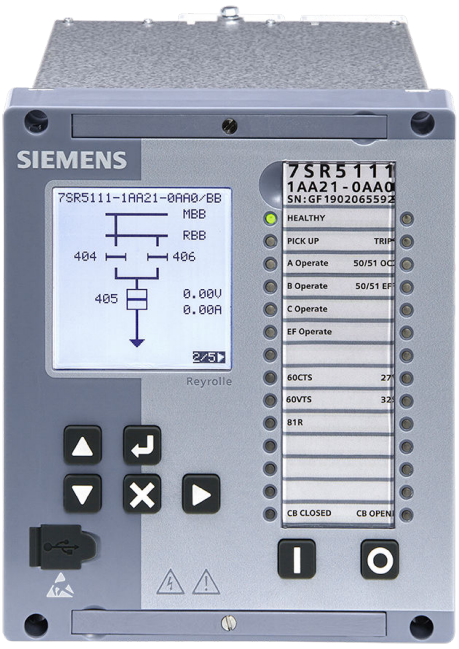
[sc_7SR5_size6_Earthing, 1, en_US]

Figure 2-4 Earthing Points (S6 with 2 x Optical LC Ports)

3 Handling of the Device

3.1 Case and Element

Size 6 Case and Device



[sc_7SR5_size6_FrontPhoto, 2, --_--]

Figure 3-1 Front View (S6)

[sc_7SR5_size6_FrontPhotoRightView, 2, --_--]

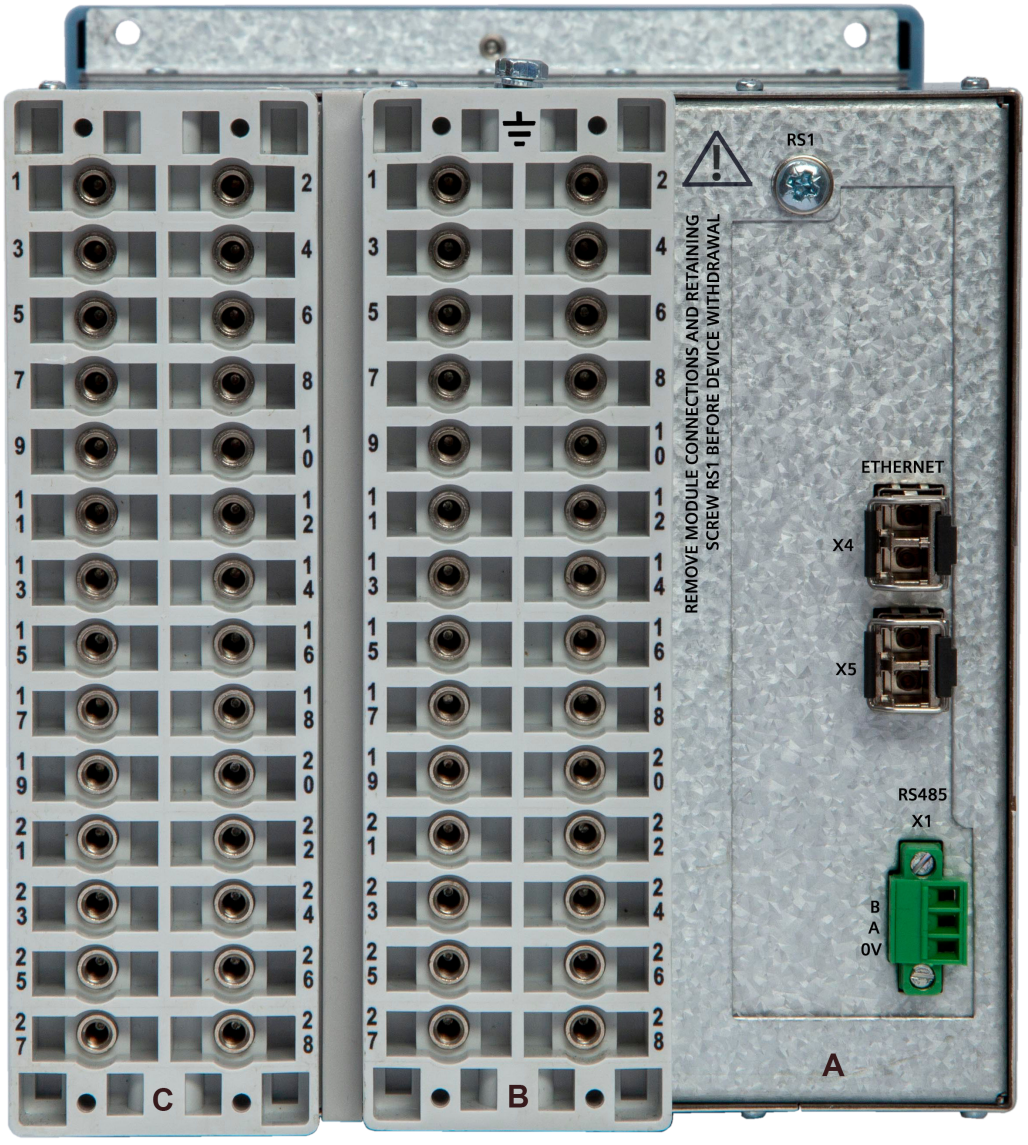
Figure 3-2 Front/Side View

[sc_7SR5_size6_front angle, 2, --_--]

Figure 3-3 Front/Side/Label View

[sc_7SR5_size6_labelView, 2, --_--]

Figure 3-4 Label View

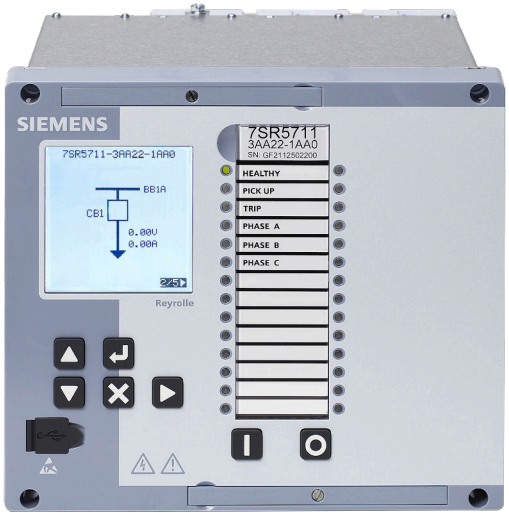


[sc_7SR5_Size6_rear, 1, --_--]

Figure 3-5 Rear View

Device fitted with optical LC ports
RS485 2-part connector shown fitted

Size 8 Case and Device



[sc_7SR5_size8_FrontPhoto, 1, --_--]

Figure 3-6 Front View (S8)

[sc_7SR5_size8_FrontPhotoRightView, 1, --_--]

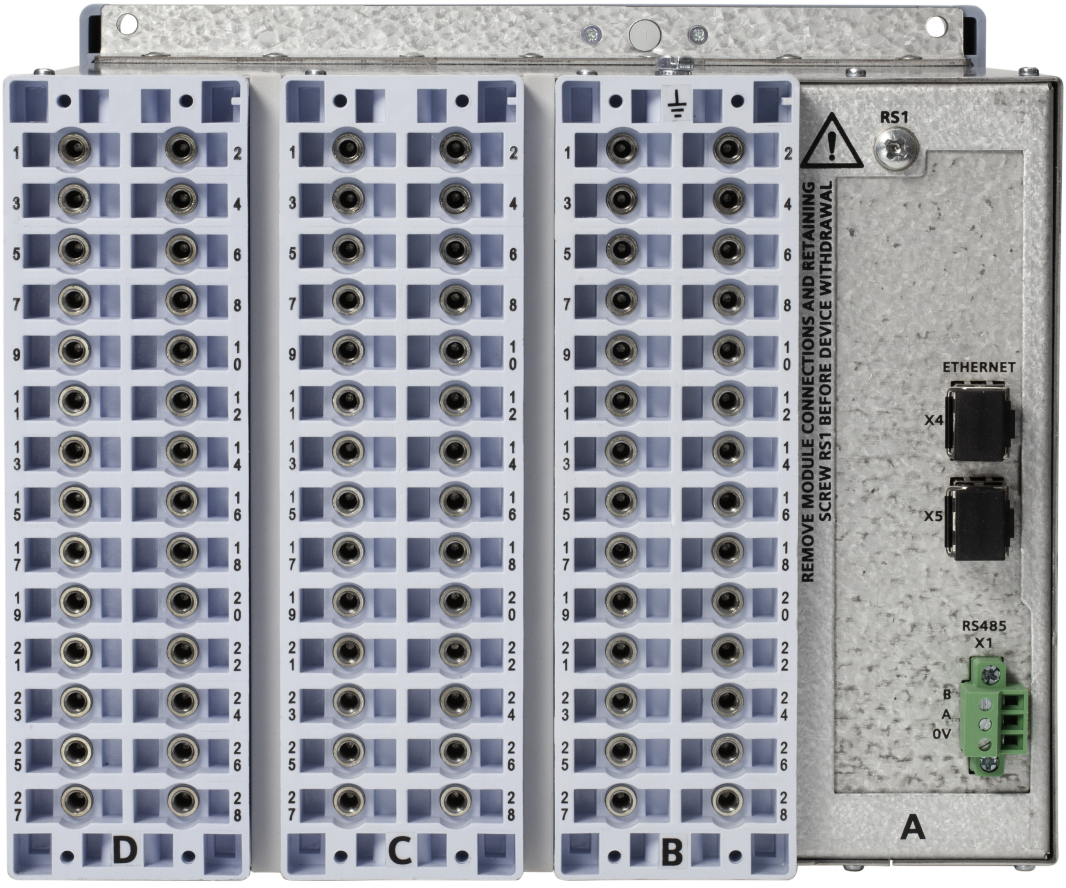
Figure 3-7 Front/Side View

[sc_7SR5_size8_FrontLablePhotoLeftView, 1, --_--]

Figure 3-8 Front/Side/Label View

[sc_7SR5_size8_labelView, 1, --_--]

Figure 3-9 Label View



[sc_7SR5_Size8_rear, 1, --_--]

Figure 3-10 Rear View

Size 12 Case and Device

[sc_7SR5_size12_FrontPhoto, 2, --_--]

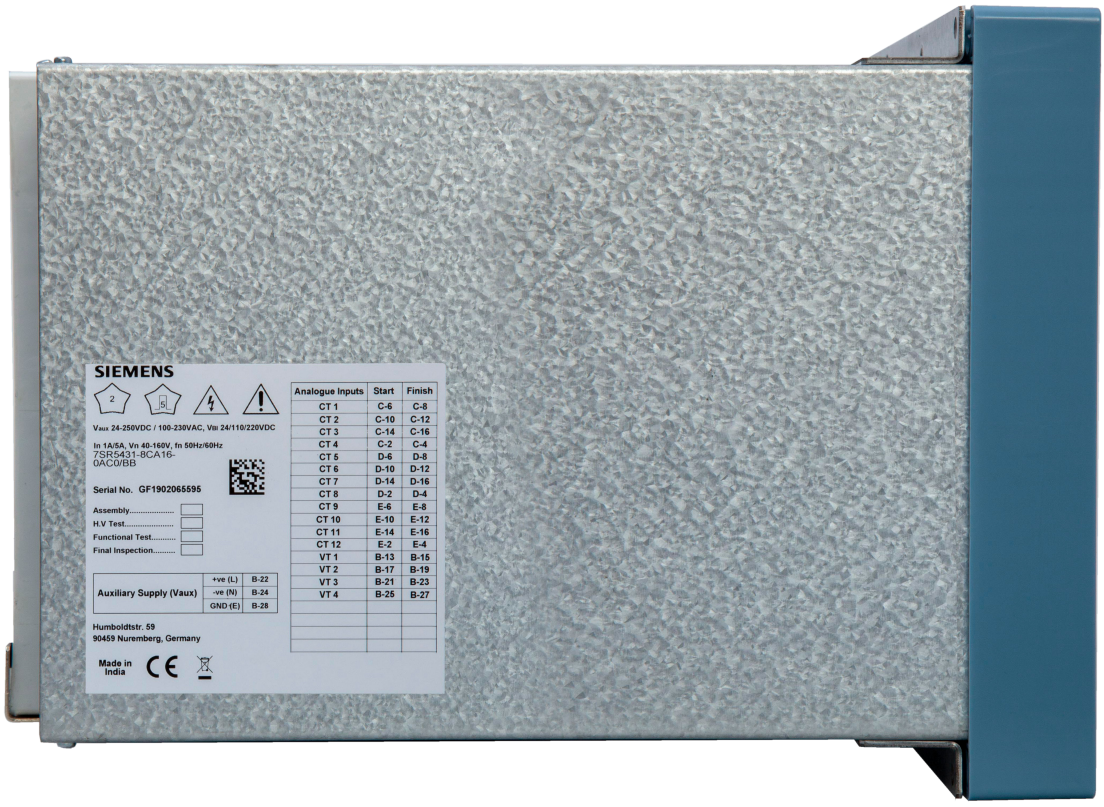
Figure 3-11 Front View (S12)

[sc_7SR5_size12_TopRightFrontView, 2, --_--]

Figure 3-12 Front/Side View

[sc_7SR5_size12_TopLeftFrontView, 2, --_--]

Figure 3-13 Front/Side/Label View



[sc_7SR5_size12_LeftSideView, 2, --_--]

Figure 3-14 Label View

[sc_7SR5_size12_RearView, 1, --_--]

Figure 3-15 Rear View

Device fitted with RJ45 ports
RS485 2-part connector shown not fitted

3.2 Withdrawing the Device Element

Size 6 Withdrawn

NOTE

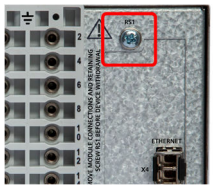
The rear retaining screw must be removed to allow withdrawal of the device from its case.

DANGER

Element Withdrawn

✧ Do not insert anything into the case after withdrawing the element.

Contacts in the case ensure that the CT circuits and normally closed contacts are short-circuited when the device is removed. It is recommended to apply external CT shorting and isolate external connections if the case is wired in service e.g. using appropriate external isolation links. The removed device should not be carried using the fascia levers, it should be held by the top and bottom plates and exposed PCB's should not be touched. The device should be protected from damage, handled with care and not exposed to contamination. The device should be re-inserted into the case without the use of excessive force.



[sc_7SR5_size6_RetainingScrew, 1, en_US]

Figure 3-16 Retaining Screw

NOTE

Remove RS485 connector and ethernet cables if connected.

To withdraw the device from the case loosen both captive screws, then pull the levers as shown in the following figures.

[sc_7SR5_size6_LooseningScrews, 2, --_--]

Figure 3-17 Screws Loosened and Levers Opened

[sc_7SR5_size6_TopViewPartWithdrawn, 1, --_--]

Figure 3-18 Top View – Device Partially Withdrawn from the Case

Size 8 Withdrawn

NOTE

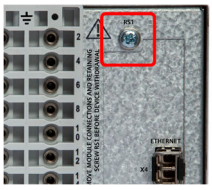
The rear retaining screw must be removed to allow withdrawal of the device from its case.

DANGER

Element Withdrawn

✧ Do not insert anything into the case after withdrawing the element.

Contacts in the case ensure that the CT circuits and normally closed contacts are short-circuited when the device is removed. It is recommended to apply external CT shorting and isolate external connections if the case is wired in service e.g. using appropriate external isolation links. The removed device should not be carried using the fascia levers, it should be held by the top and bottom plates and exposed PCB's should not be touched. The device should be protected from damage, handled with care and not exposed to contamination. The device should be re-inserted into the case without the use of excessive force.



[sc_7SR5_size6_RetainingScrew, 1, en_US]

Figure 3-19 Retaining Screw

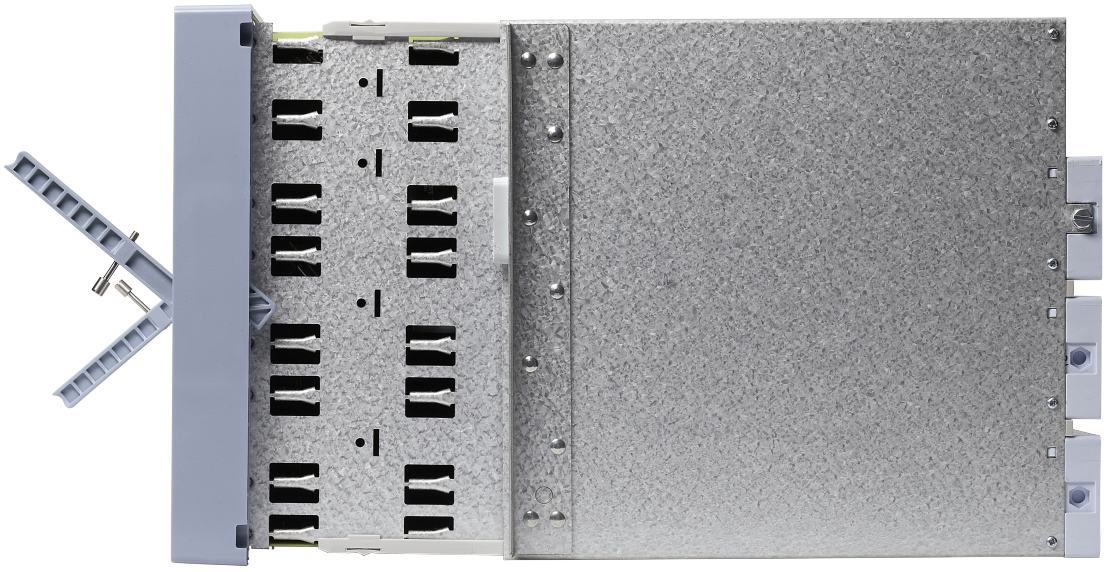
NOTE

Remove RS485 connector and ethernet cables if connected.

To withdraw the device from the case loosen both captive screws, then pull the levers as shown in the following figures.

[sc_7SR5_size8_LooseningScrews, 1, --_--]

Figure 3-20 Screws Loosened and Levers Opened



[sc_7SR5_size8_TopViewPartWithdrawn, 1, --_--]

Figure 3-21 Top View – Device Partially Withdrawn from the Case

[sc_7SR5_size8_FrontViewPartWithdrawn, 1, --_--]

Figure 3-22 Front View – Device Partially Withdrawn from the Case

[sc_7SR5_size8_RearViewFullyWithdrawn, 1, --_--]

Figure 3-23 Rear View – Device Fully Withdrawn from the Case

Size 12 Withdrawn

NOTE

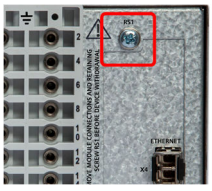
The rear retaining screw must be removed to allow withdrawal of the device from its case.

DANGER

Element Withdrawn

✧ Do not insert anything into the case after withdrawing the element.

Contacts in the case ensure that the CT circuits and normally closed contacts are short-circuited when the device is removed. It is recommended to apply external CT shorting and isolate external connections if the case is wired in service e.g. using appropriate external isolation links. The removed device should not be carried using the fascia levers, it should be held by the top and bottom plates and exposed PCB's should not be touched. The device should be protected from damage, handled with care and not exposed to contamination. The device should be re-inserted into the case without the use of excessive force.



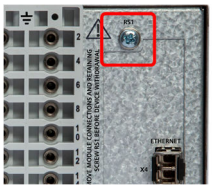
[sc_7SR5_size6_RetainingScrew, 1, en_US]

Figure 3-24 Retaining Screw

NOTE

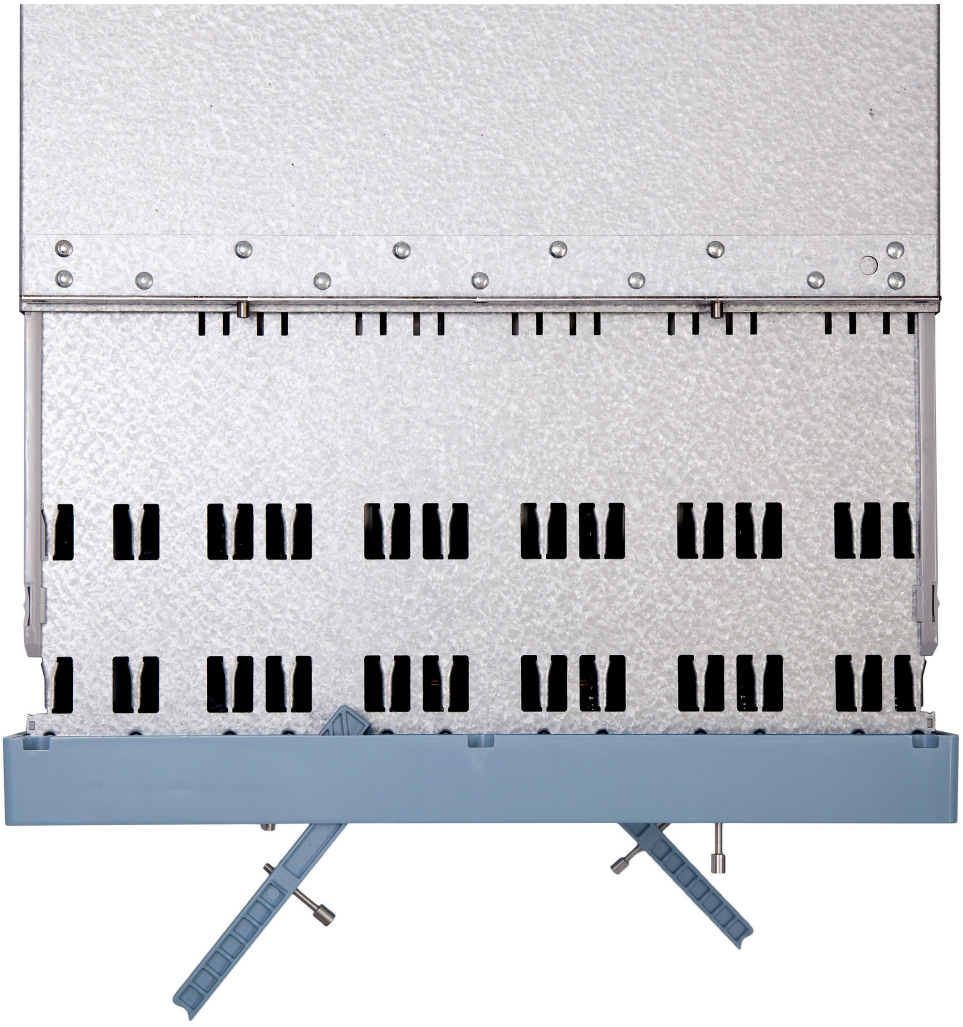
Remove RS485 connector and ethernet cables if connected.

To withdraw the device from the case loosen both captive screws, then pull the levers as shown in the following figures.



[sc_7SR5_size6_RetainingScrew, 1, en_US]

Figure 3-25 Retaining Screw



[sc_7SR5_size12_TopViewPartWithdrawn, 1, –_–]

Figure 3-26 Top View – Device Partially Withdrawn from the Case

4 Using the Device Fascia

4.1 General

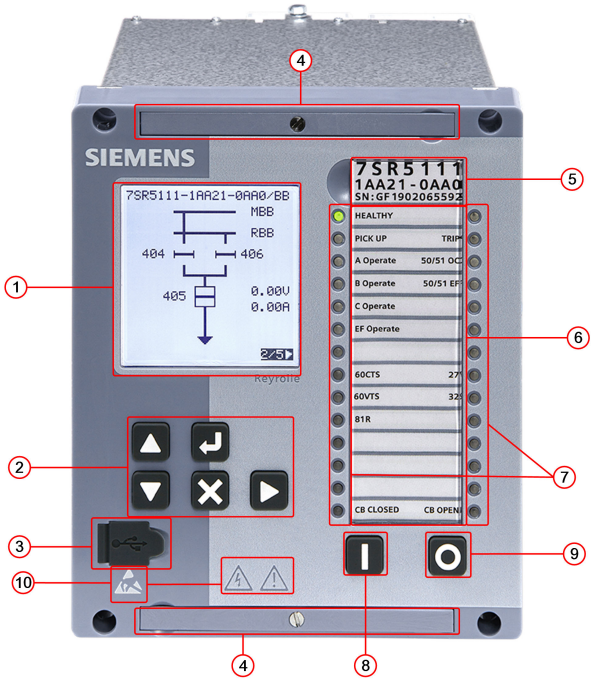
All 7SR5 devices can be operated via the Reydisp Manager 2 interface of your PC and via the on-site operation fascia front panel.
Operation is via the push buttons on the relay. LEDs and large HMI screen provide information to the operator.

Operating Concept

The operating concept allows you to do the following on-site operator actions:

- Navigation in the menu tree
- Modification of settings
- Resetting saved information
- Showing default and control displays, measured values and logs
- Executing switching operations with large graphical HMI screen
- Initiating configured actions via function keys
- Binary output test from **Maintenance** menu
- Status display with LED
- Function configuration
- Configuring inputs, outputs and LEDs
- CT/VT configuration
- Setting serial communication parameters
- Display device information such as firmware version, and IP address

4.2 Overview of Operator Elements and Display Elements

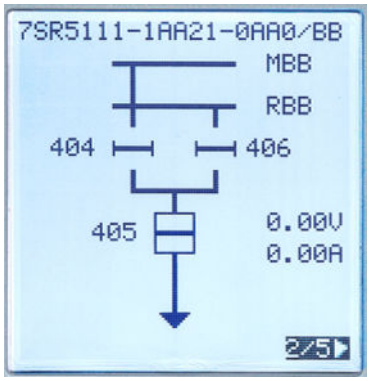


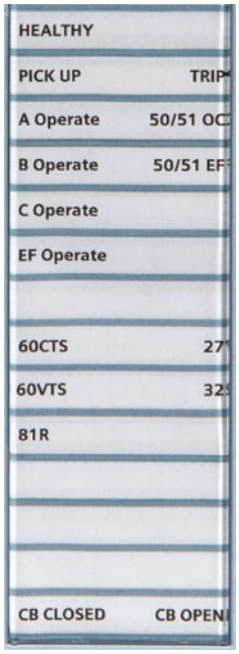
[dw_7SR5_fascia, 2, en_US]

Figure 4-1 Device Fascia

(1) LCD
(2) Push buttons
(3) USB port cover
(4) Withdrawal lever
(5) Device identification number
(6) Transparent LED label door
(7) 28 3-colored LEDs
(8) Function key 1
(9) Function key 0
(10) Warning symbols

The following table gives you a detailed explanation of the function of the operator and display elements.

Operator Element/Display Element	Function
 Figure 4-2 LCD Display	LCD display showing menus and settings
 Figure 4-3 Fascia Up Button	Menu navigation and settings increase
 Figure 4-4 Fascia Down Button	Menu navigation and settings decrease
 Figure 4-5 Fascia Navigation Button	Menu navigation. Binary output reset from home screen (3 second delay). LED test/reset.
 Figure 4-6 Fascia Enter Button	**Enter** key, used to initiate and accept settings changes
 Figure 4-7 Fascia Cancel Button	**Cancel** key, used to cancel settings changes and/or move up the menu structure by one level per press
 Figure 4-8 USB Port Cover	USB port to connect to other devices e.g. laptop.
 Figure 4-9 Withdrawal Lever	2 levers are located on the front of the relay. They are used to withdraw the relay from it's case.
 Figure 4-10 Device Label	Label displaying the relay MLFB code and serial number.

Operator Element/Display Element	Function
 Figure 4-11 Labelling Strip	Customizable label for LEDs with transparent door
 Figure 4-12 28 3-colored LEDs	28 tri-colored LEDs to show the status of the functions etc on the label. The 28 LEDs are in 2 lines of 14. The left hand line of LEDs are numbered 1 to 14 from top to bottom. The right hand line of LEDs are numbered 15 to 28 from top to bottom.
 Figure 4-13 Fascia Function 1 Button	**Binary input > Function button 1**
 Figure 4-14 Fascia Function 0 Button	**Binary input > Function button 0**

Operator Element/Display Element	Function
 Figure 4-15 Electrical Hazard	Danger: Electrical hazard
 Figure 4-16 Refer to Device Documentation	Refer to device documentation (Product information, Device manual, Hardware manual, Operating manual, and Communication protocol manuals)
 Figure 4-17 ESD Warning	Electrostatic Sensitive Devices warning

4.3 Displays for Indication and Control

Displays

Displays for indication and control offer you the possibility of quickly obtaining an overview of important operating modes. You can configure a total of up to 5 different display screens in Reydisp Manager 2 using the display editor. The following contents are available here:

- Dynamically updated measured values
- Status of indications
- Switch positions of switching objects
- Static or dynamic texts
- Graphical and controllable elements
- Add access control via Setting and User IDs
- Resetting of password is a fascia operation

NOTE

The displays and controls on the HMI screen are created in Reydisp Manager 2.

The LCD contrast can be adjusted by pressing the **Enter** and **Cancel** pushbuttons together and then using the ▲ or ▼ keys to increase or decrease the contrast.

The backlight brightness adjusted by pressing the **Enter** and **Cancel** pushbuttons together, then pressing the right arrow ► pushbutton to select brightness and then using the ▲ or ▼ keys to increase or decrease the level.

To conserve power the display backlighting is extinguished when no buttons are pressed for a user defined period. The **Backlight Timer** setting within the **Configuration > Device** menu allows the timeout to be adjusted from 1 to 60 minutes and **Off** (backlight permanently on).

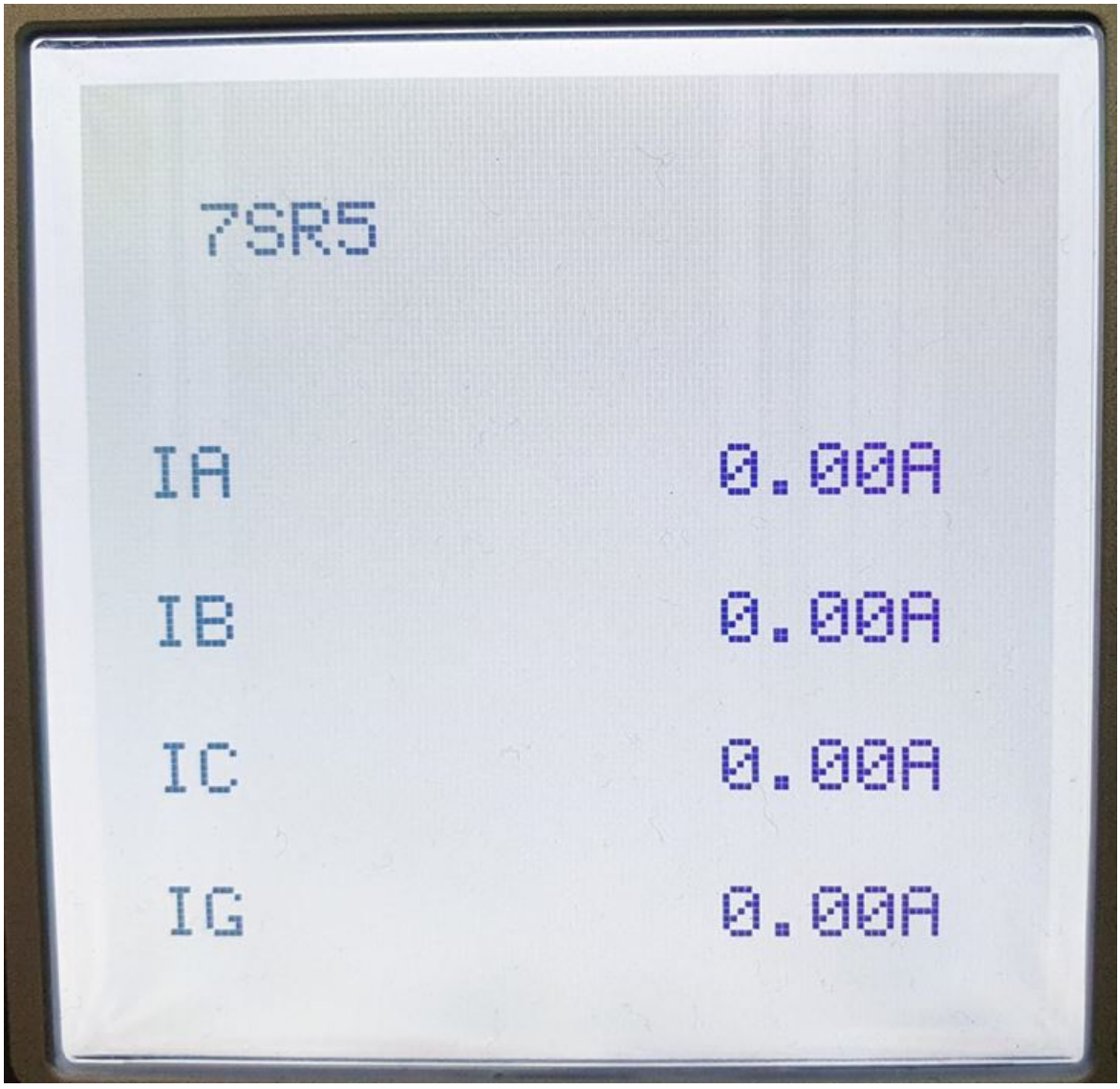
Default Displays

The **Device Not Configured** message will flash up on the LCD after a short duration if the user has not changed any parameter in the device (see *Figure 4-18*). The display of the message cannot be disabled. The action of changing any parameter or user configuration will automatically disable this alert message.

[sc_7SR5_DeviceNotConfigured, 3, --_--]

Figure 4-18 Device Not Configured

A device ready for operation will display the primary current default screen display image (see *Figure 4-19*) after sending configuration to the device if no user HMI screens have been configured.



[sc_7SR5_PrimaryCurrentScreen, 1, --_--]

Figure 4-19 Primary Current Default Screen

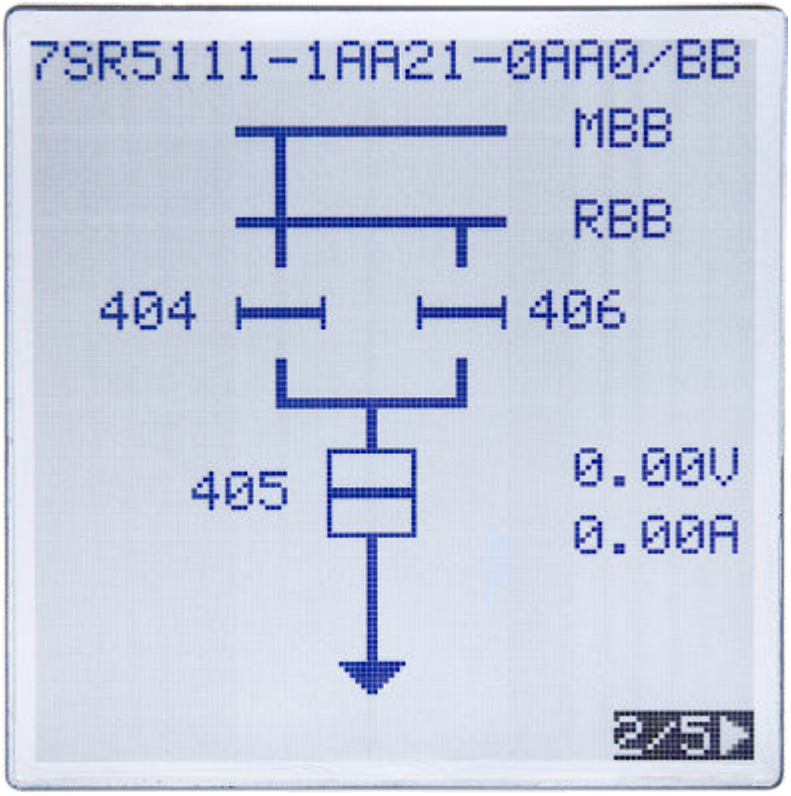
This default screen can be changed by using the Reydisp Manager 2 tool.

During normal in service operation (not after operation caused by a system fault) the user can return to the default **Home** screen by pressing the Cancel button several times from anywhere within the menu structure.

If several display images are available, you can select them in order of parameterized sequence by pressing the fascia navigation button (right arrow).

Control Displays

The 7SR5 device graphic display can be configured to show a mimic of the associated plant by using the Reymimic editor in Reydisp Manager 2. The control displays can graphically and dynamically update the switch position of switching objects. In addition, control displays offer you the possibility of selecting individual switching objects and activating them according to switching authority and switching mode.



[sc_7SR5 Fascia - Example Mimic Displays, 3, --_--]

Figure 4-20 Control Display

A ready-to-run device can display a user defined plant control mimic after booting. By pressing the Enter button, function key 1, or function key 0 buttons, you get to the control display defined as standard. By pressing the Enter button and using the up or down buttons, you get to the control mode of the currently displayed control display.

If there are multiple displays, the Navigation (right arrow) buttons is used to display the different screens. If several controllable objects exist on a single screen, pressing Enter and using the up or down keys allows the user to toggle between different objects. After pressing function key 1 or function key 0, a confirmation screen appears to activate the control function. Control mode is reset after a switching procedure or after a period of 30 seconds time duration without a switching operation or confirmation.

4.4 Structure of the Menu

Device Menu

The **User** menu can be reached after pressing the down fascia key or up fascia key whilst the main screen is displayed. The fascia Navigation button is used for proceeding to the menu.

Setting Mode

This mode allows you to view and change settings, configuration, inputs/outputs, CT/VT ratios, and protection parameters in the device.

See section 3.1.2 in the device manual for further information.

Instrument Mode

This mode allows you to view the following conditions of the device:

- Operational measured values
- Input/output (I/O) status
- Miscellaneous status

Instrument Mode

The instrument mode submenu displays the current values, status of binary inputs, and binary outputs. The following meters are available and can be navigated by using the ▲, ▼, and ► keys.

See section 8.1 in the device manual for further information.

Fault Data Mode

The 7SR5 stores a maximum of 100 relay trip fault records. Each stored fault data can be viewed by pressing the ► key. Each record contains data of the operated elements, analogue values, and LED status at the time of the fault. The data is viewed by scrolling down using the ▼ key.

NOTE

Phase LEDs are not illuminated when the trip is caused by the 49 function.

NOTE

LCD does not display phase information when the trip is caused by the 49 function.

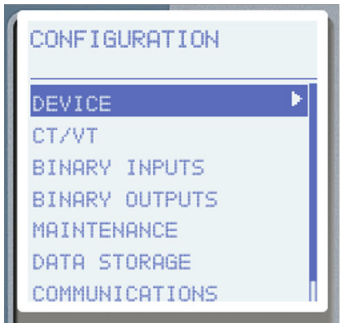
4.5 Menu Tree

Main Menu

The main menu structure is firmly set and is not changeable. The submenus depend on the hardware variants and the configuration of functions.

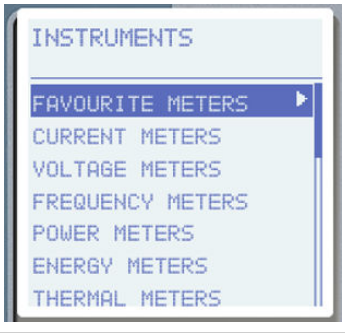
Pressing the right arrow button ► is to enter submenus and the X cancel button is to return to the main menu. The arrow keys navigate between the menus.

Settings Menu



In the **Settings** menu, relay settings, CT/VT configuration, inputs/outputs are available, and function configuration can be selected. Binary outputs can be tested from the **Maintenance** menu and the serial RS-485 port communication settings are available in the **Communications** submenu.

Instruments Menu



In the **Instruments** menu, you can display various real time measured values from analogue inputs and the status of some elements.

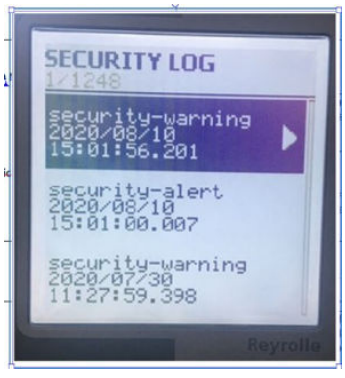
Fault Data Menu

Fault data records can be viewed on the HMI LCD with the time and date of the trip. These include the LED status at the time of recording and the fault currents. Fault number 1 is the most recent fault.

Event Log Menu

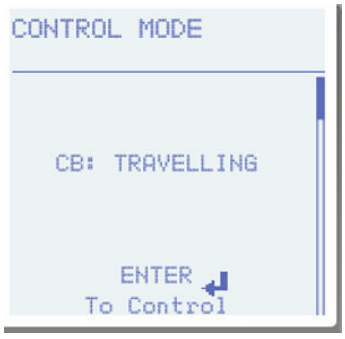
The **Event Log** menu shows the time tagging of any change of state (Event) in the device as a record, along with a time and date stamp to a resolution of 1 ms. **`Raised`** means the event is in the on state and **`Cleared`** means the event is in the off state.

Security Log Menu



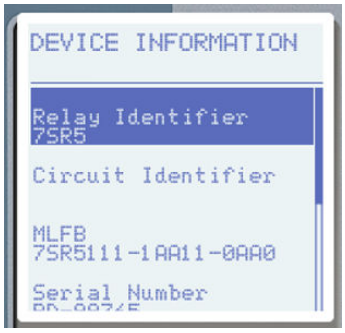
The **Security Log** menu lists the events associated with the security access to the device and are categorized as Events or Alarms. These can be viewed by entering the Security ID, if it has been configured in the device configuration using Reydisp Manager.

Control Mode Menu



The **Control Mode** menu shows controllable plant items that have been included by the user in the configurable fascia LCD. For the chosen item the **`Enable Output Signals`** can be selected to allow the item to be a **`Controllable Item`** by using the Enter button and function keys.

Device Information Menu

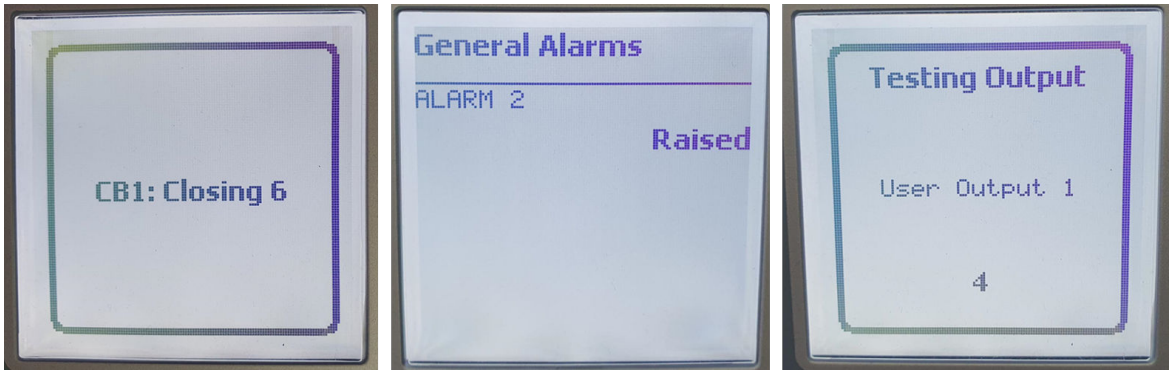


The **`Device Information`** menu offers you detailed information about the device such as the firmware version, serial number, etc.

4.6 Notification and Dialog Windows

Notification Windows

The notification windows appear briefly to give the user important information during on-site operation and close automatically. For example, they contain the following information:



[sc_7SR5_DeviceNotificationWindows, 1, --_--]

Figure 4-21 Examples of Notification Windows

Dialogs

Dialogs are interactive notification windows in the base bar. In the dialogs, you are prompted to actively carry out actions.

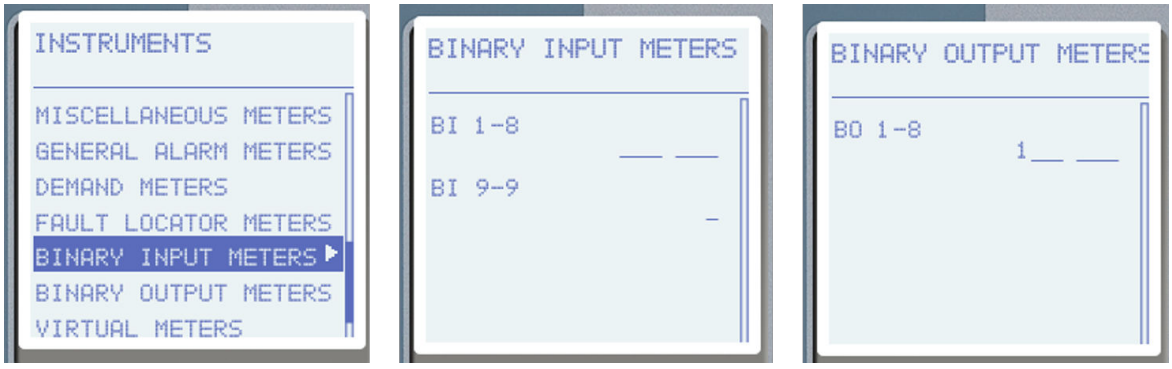
You confirm the context-dependent command prompts offered here by pressing the softkeys below the prompts.

4.7 Display of Routings and Status

You can route signals from the 7SR5 device matrix to binary inputs and binary outputs. With the menu item **Main Menu > Instruments > Binary Input Meters** on the device you can display the status of the logical signals and their status.

In order to display the status in the 7SR5 device, proceed as follows:

- In order to access the **Binary IO** from the main menu, use the fascia navigation keys:
  Main Menu > Instruments > Binary Input Meters
- Use the navigation keys of the front fascia to navigate within the displayed list and select one of the 2 following menu entries:
  - Binary inputs
  - Binary outputs



[sc_7SR5_DeviceBinaryInputOutputMenu, 1, --_--]

Figure 4-22 Binary Inputs and Output Menu

All available binary inputs of the 7SR5 device will be displayed.

The following table shows the meaning of the status of the individual menu entries **Binary inputs** and **Binary outputs**.

Menu Item	Status	Description
Binary input	1	Input is active
	–	Input is not active
Binary output	1	Output is active (contact is closed)
	–	Output is not active (contact is open)

The status of the respective binary inputs, binary outputs or the LEDs is updated automatically by the actual state in the device.

- Use the navigation keys to navigate around the Meter pages.

Configuring Binary Outputs

Any function element in the Output Matrix can be selected to operate any output relay, LED or virtual input/output.

Functions and signals that initiate operation of each binary output are defined in the **Settings > Configuration > Binary Outputs > Output Matrix** menu. All outputs are fully user configurable from the front fascia and can be programmed to operate from any or all of the available functions and signals in the output matrix menu.

Figure 4-23 shows an assignment to a binary output following the menu steps. The 50-1 overcurrent protection stage is assigned to BO-1 and LED11.

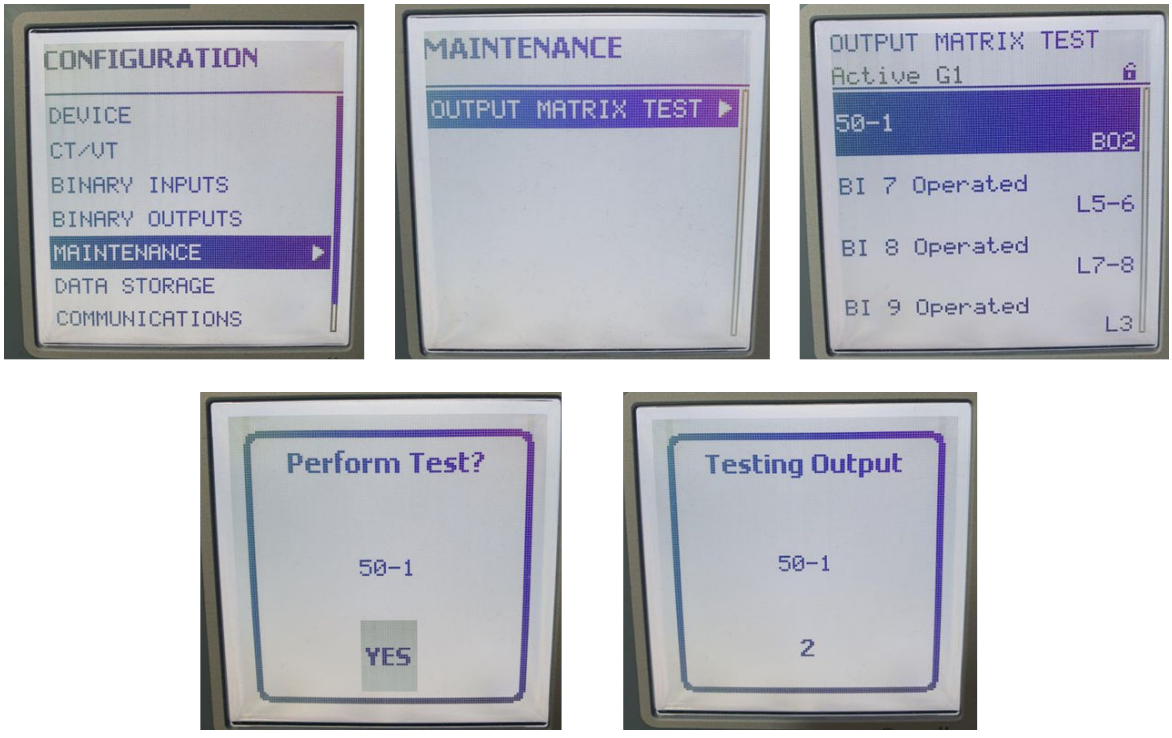
In the Output Matrix, use the up or down keys to see the required function, then press the Enter button to configure a binary output, LED or virtual to this signal. Use the right arrow key to proceed to further BOs.

Use the up arrow key by making 1 to map an output, then press the Enter button to confirm your assignment.

[sc_7SR5_DeviceBinaryOutputMenuSteps, 1, --_--]

Figure 4-23 Binary Output Menu Steps

Output Matrix Test



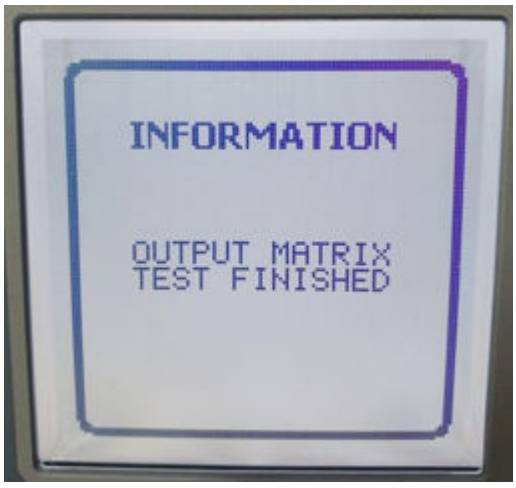
[sc_7SR5_DeviceOutputMatrixTestSteps, 1, --_--]

Figure 4-24 Output Matrix Test Steps

The **Output Matrix Test** allows the user to test Binary Outputs. Before performing this test, signals must be mapped in the **Binary Outputs > Output Matrix** from the **Settings > Configuration** menu

The **Settings > Configuration > Maintenance > Output Matrix Test** menu displays the functions that are assigned to any binary output.

In the **Output Matrix Test** menu, view the signals with the down arrow key. Press the Enter button to perform a test in this signal then, after a confirmation page, choose Yes with the up or down key and the press Enter. The configured binary output(s) will close.



[sc_7SR5_DeviceOutputMatrixTestCompleted, 1, --_--]

Figure 4-25 Output Matrix Test Completed

5 Using Reydisp Manager 2

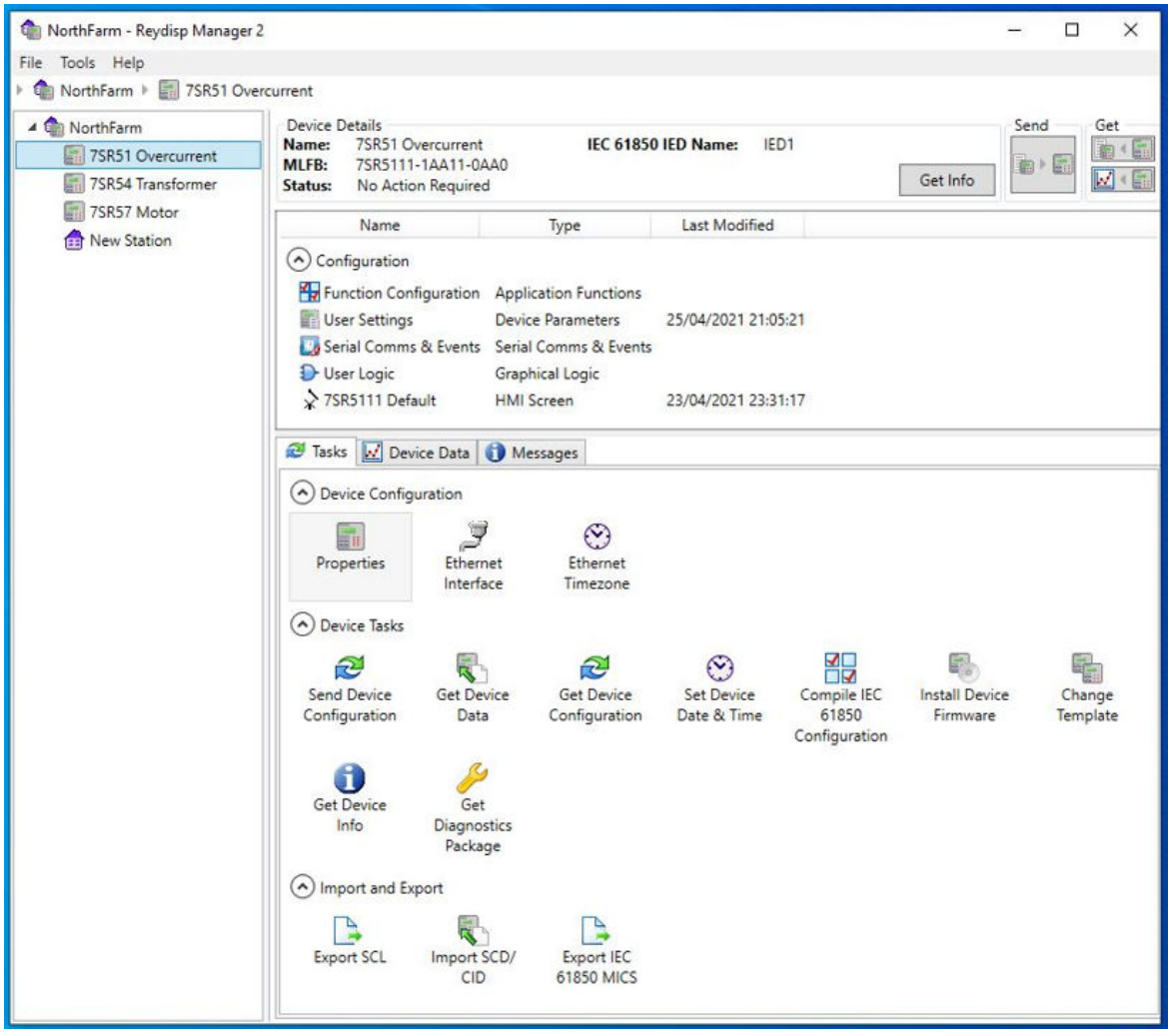
5.1 General

Reydisp Manager 2 is a PC operating program. It is the engineering and operating tool for all 7SR5 protection devices. The user can perform all configuration tasks offline from the PC without needing a 7SR5 device. All data can be transferred to the device online at a later date – for example, via a direct USB connection or a communication network. More information is available in the Engineering Guide.

Reydisp Manager 2 is available to download free of charge from *https://www.siemens.com/reyrolle* directly.

Download package Reydisp Manager V02.XX should be used for the installation of Reydisp Manager 2.

Reydisp Manager 2 uses templates to update and configure 7SR5 devices. The templates need to be installed in Reydisp Manager for any required device type and version. All device templates must be installed separately for the required PC software and device type. Template installers are also available to download from the Siemens web page e.g. **`7SR5_DeviceFW-V2.10CFG-V2.10_RDT-V2.10.exe`**



[sc_7SR5_ReydispManager2ProjectStructure, 2, --_--]

Figure 5-1 Project View of Reydisp Manager 2 (Main Screen)

It provides the following features:

- Configure device functionality
- Configure device settings
- Create and edit logic diagrams
- Create user defined single lines and mimic diagrams for HMI screens

- Configure device IEC 61850 interface/time zone
- Create user-definable current/voltage/thermal curves
- Configure serial communication data points and fascia event log
- Edit IEC 61850 Stations using the optional System Configurator with seamless integration with Digsi

5.2 Operator Actions in the Offline and Online Area

Offline Configuration

The offline configurations indicated offline in a project include all data to be edited of a protection device on the engineering PC. There is no need for a connection to a physically existing device.

You can execute the following actions in the offline area:

- Adding 7SR5 devices to the project tree
- Selecting a template of the device
- Defining functional scope of a 7SR5 device
- Entering individual function settings and parameters
- Routing binary inputs, outputs and LEDs
- Editing HMI screen display diagrams
- Designing logic functions such as interlocking mechanisms
- Configuring the communication network and setting communication parameters
- Displaying saved fault records and evaluating them from waveform records
- Exporting and printing data

Online Configuration

All data can be transferred to the device using an online connection and perform the following tasks when there is a physical connection between Reydisp Manger 2 and a 7SR5 device:

- Sending device configuration
- Retrieve device data such as event logs, fault logs and waveform fault records
- Retrieve device configuration
- Set device date and time
- Displaying selected analogue measured values
- Protection setting parameterization

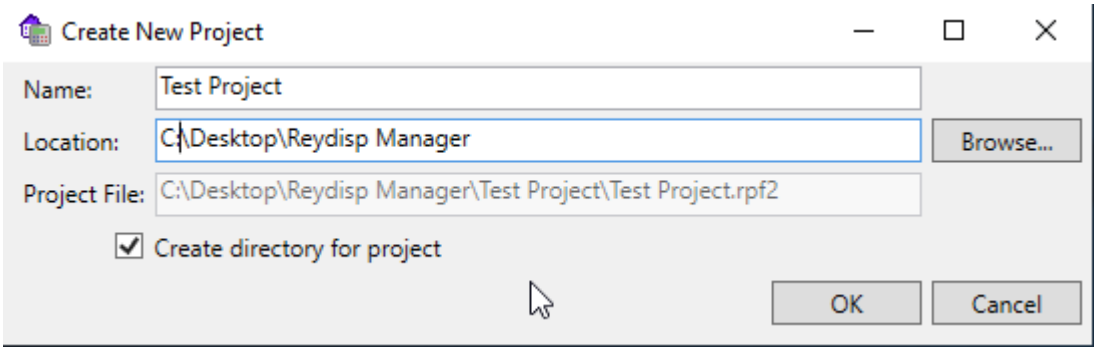
Creating a Project

In the Start menu under Reydisp Manager 2, select the program entry for the current Reydisp Manager 2 version or double click the shortcut icon on the desktop to open the engineering tool of the 7SR5 device.

A small start-up screen opens.

Click on the **New Project** icon and enter a project name in the **Name** box as shown in *Figure 5-2*.

Then click **OK** to proceed to the main screen.



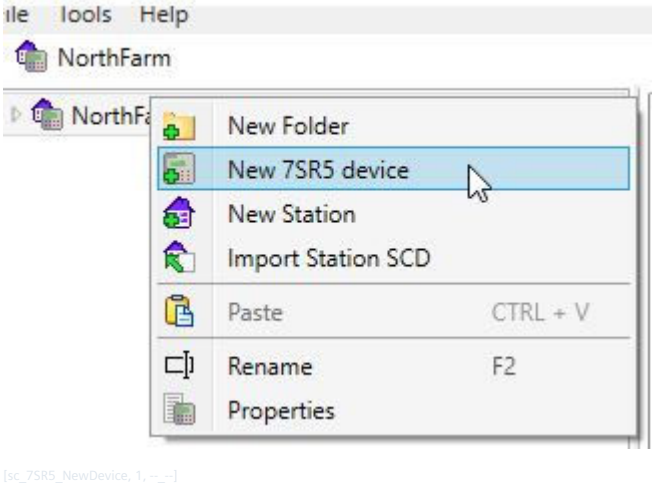
[sc_7SR5_ReydispManager2NewProjectDialog, 1, --_--]

Figure 5-2 Creating a New Project

After starting Reydisp Manager 2, you are shown a main screen. Right click on the project name in the project tree which is located on the left side and select **New 7SR5 device**.

This lets you open a **Create Device** dialog box enabling you to add a new 7SR5 device.

Make sure to install the device templates before this operation.



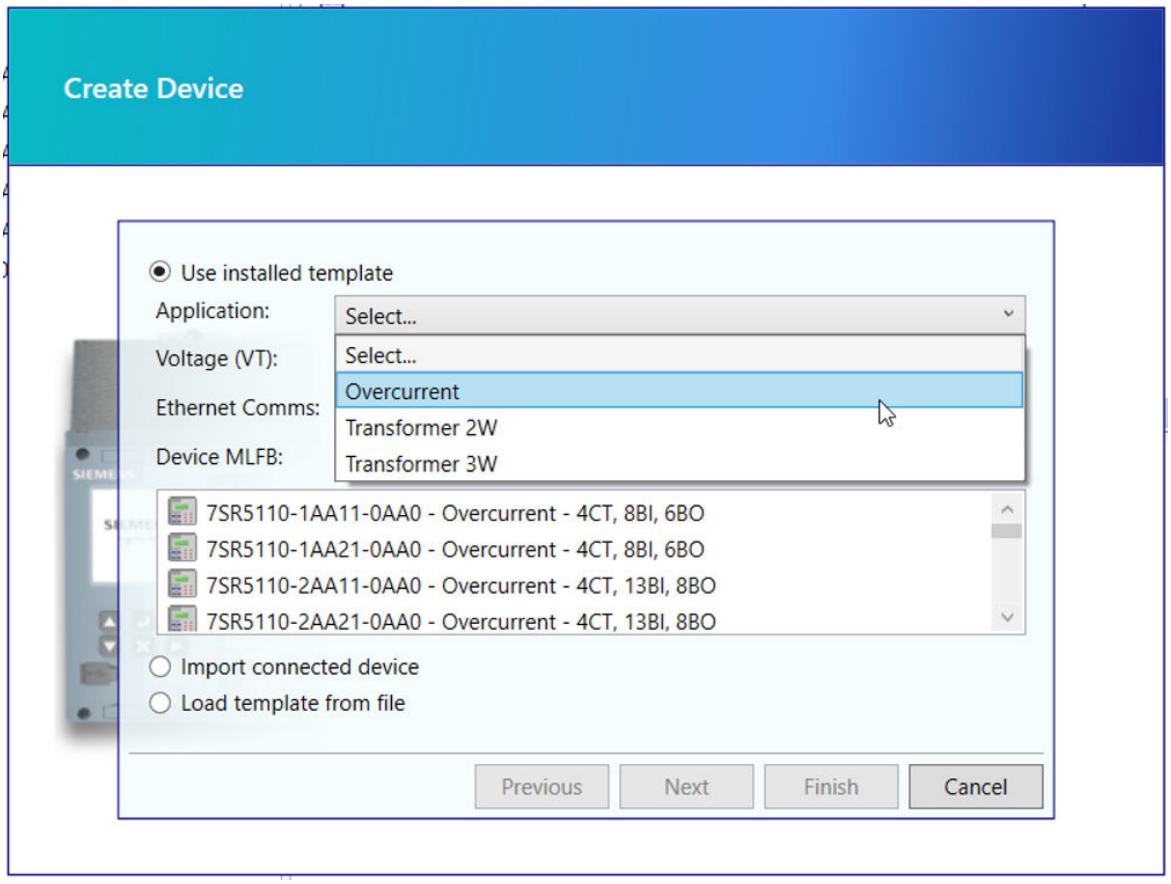
[sc_7SR5_NewDevice, 1, --_--]

Figure 5-3 New 7SR5 Device Menu Item

Several options are available for inserting a 7SR5 device into a project:

- A device can directly be inserted in the project tree with the aid of a valid product MLFB code starting 7SR5XXX-XXX on the label on the fascia. Everything specified by this product code is created afterwards in Reydisp Manager 2.
- All installed device templates are in the template list. The device could be selected directly from the template list.
- The product code can be entered directly into the **Device MLFB user entry** box as a partial code or complete code and the selection will be filtered automatically to assist the selection.
- If the device is connected to the PC by a USB cable the product code can be provided from the device using the **From Connected Device** option. This can be used to get the product code from a connected device and proceed to create a new configuration.
- You can also select **Import the connected device** for copying the USB cable connected device configuration and parameters into the project. This method is recommended when working with a device that has an associated Reydisp Manager 2 project (already configured before). This way the user can obtain a copy of the preconfigured device in the project.

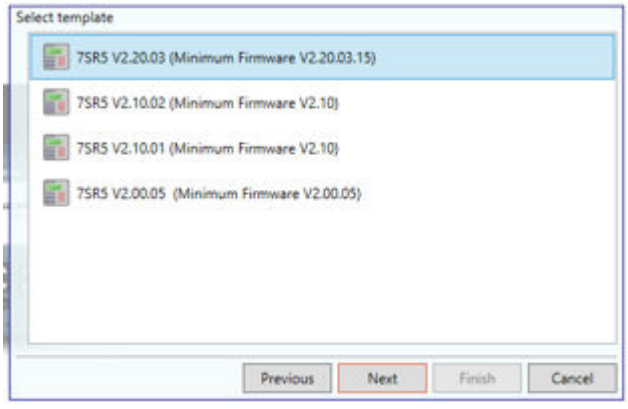
Choose one adding device option and click the **Next** button to create the device.



[sc_7SR5_ReydispManager2NewDevice, 2, --_--]

Figure 5-4 Inserting a New 7SR5 Device

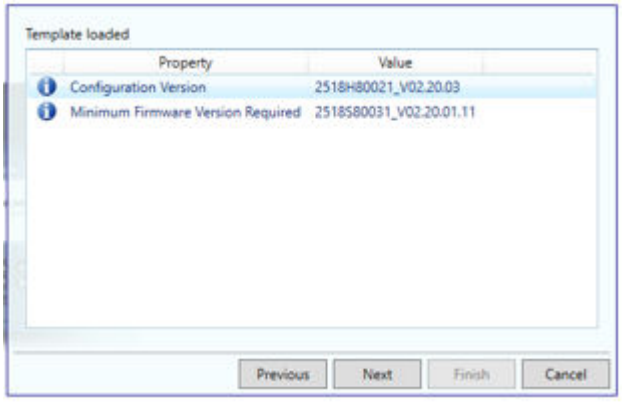
The following images show the creation of a device step-by-step.



[sc_7SR5_ReydispManager2SelectTemplate, 2, --_--]

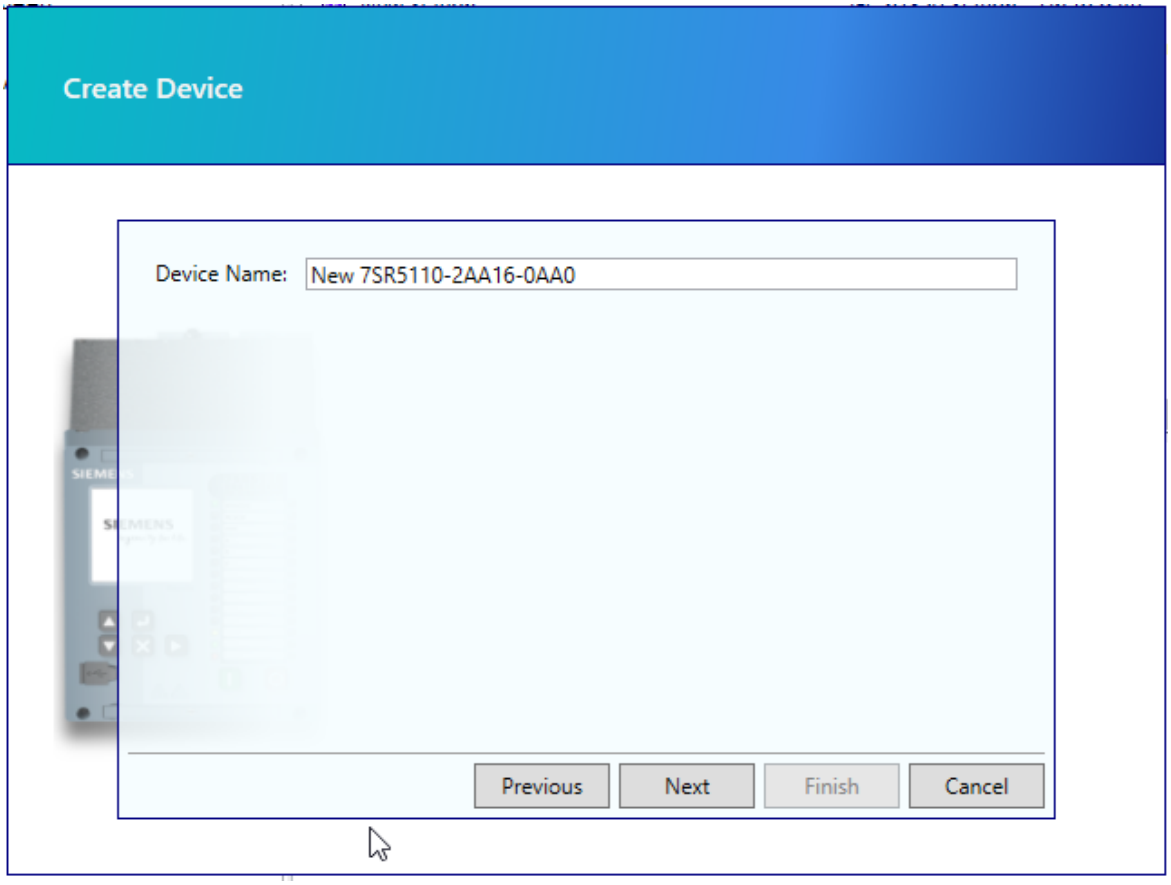
Figure 5-5 Selecting a Template

Select the relay firmware version and give a name to the device as a device name in the project.



[sc_7SR5_ReydispManager2MinimumFirmware, 2, --_--]

Figure 5-6 Showing the Minimum Firmware



[sc_7SR5_ReydispManager2DeviceName, 1, --_--]

Figure 5-7 Entering the Device Name

Enter an IED name for using in the IEC 61850 project and select the IEC 61850 edition.

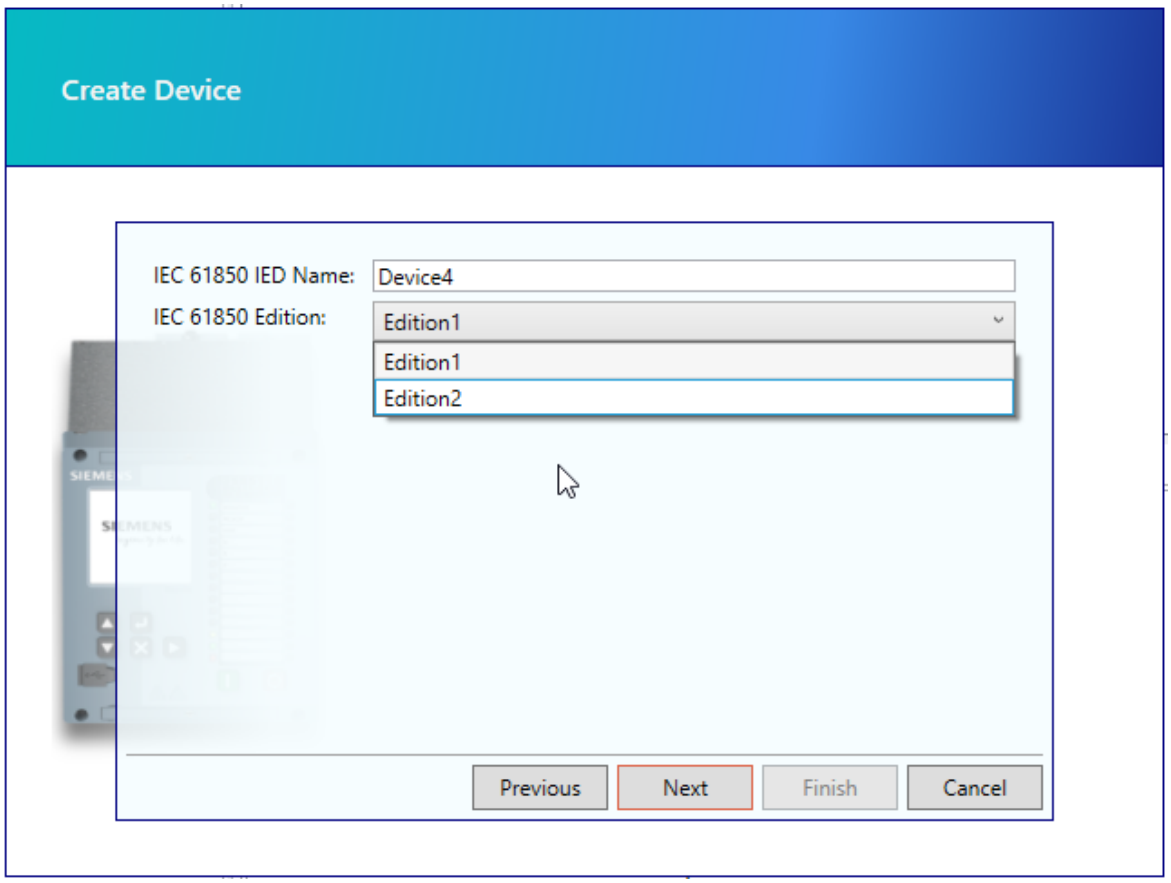


Figure 5-8 Entering IED Name and Selecting IEC 61850 Edition

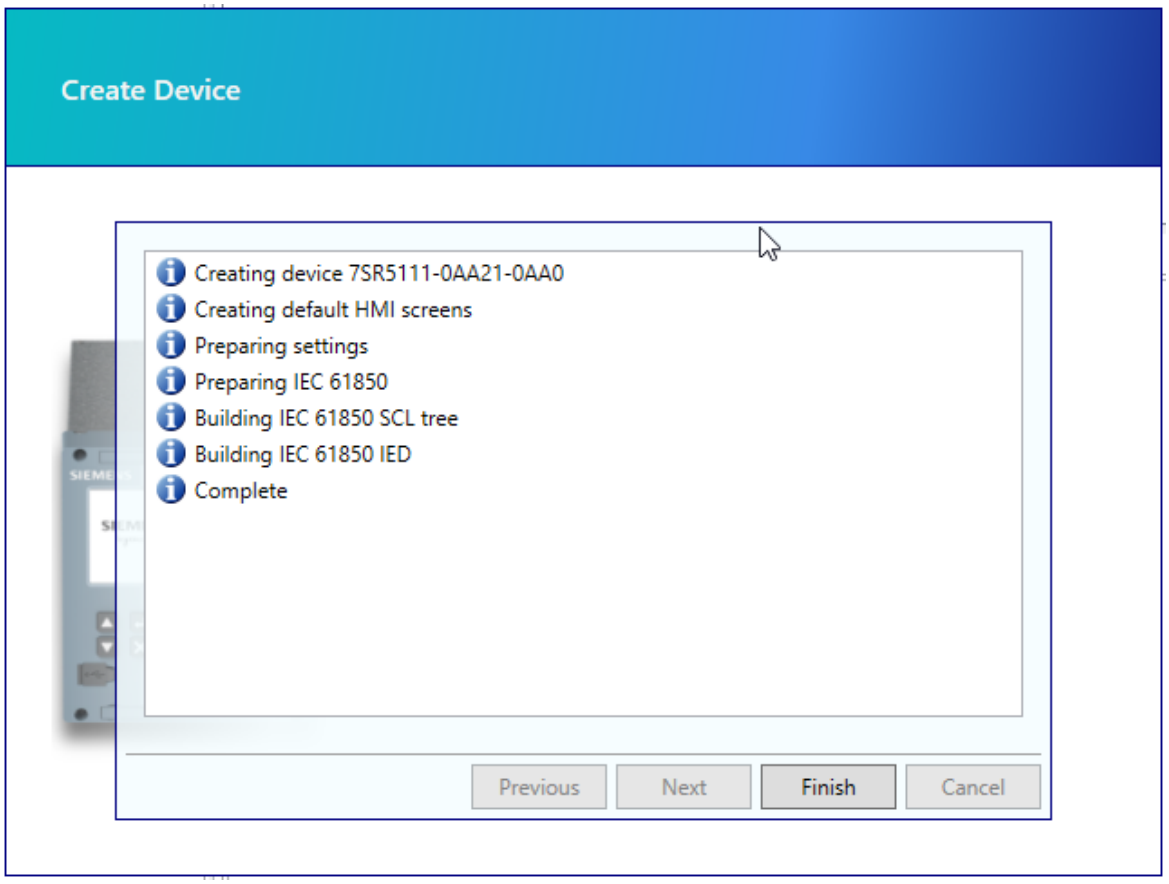


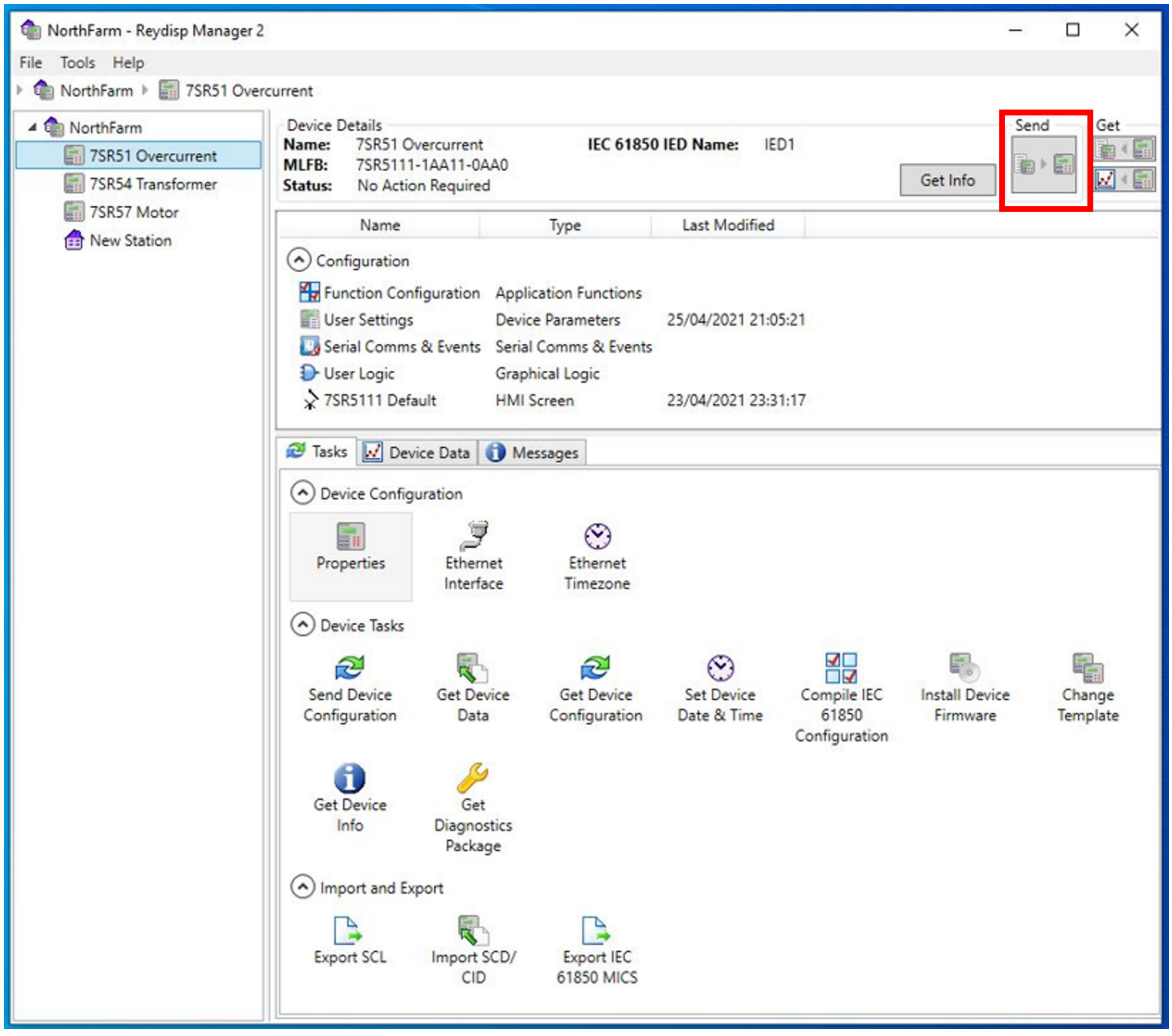
Figure 5-9 Device Construction

Click the **Finish** button after the device creation is complete.

5.3 Transmitting the Configuration to a 7SR5 Device for the First Time

When the device is delivered from the factory it will display a message intermittently on the fascia advising the device is not configured. Changing any parameter setting from the fascia or sending a device configuration file will remove this message. The similar message advising that the IEC 61850 is not configured, will be removed if a configuration is sent to the device. This message can be disabled by setting of the user setting **`IEC 61850 Configuration Alert`** if this protocol is not to be used. Before commissioning a device, as a minimum, the device must be paramerterized from the fascia. It is recommended that the device is fully configured from the Reydisp Manager 2 PC software.

In Reydisp Manager 2, initialization with a configuration associates the offline configuration with the 7SR5 device. For this, the 7SR5 device transmits its serial number, which is then entered in the corresponding offline configuration.



[sc_7SR5_SendDeviceConfiguration, 2, --_--]

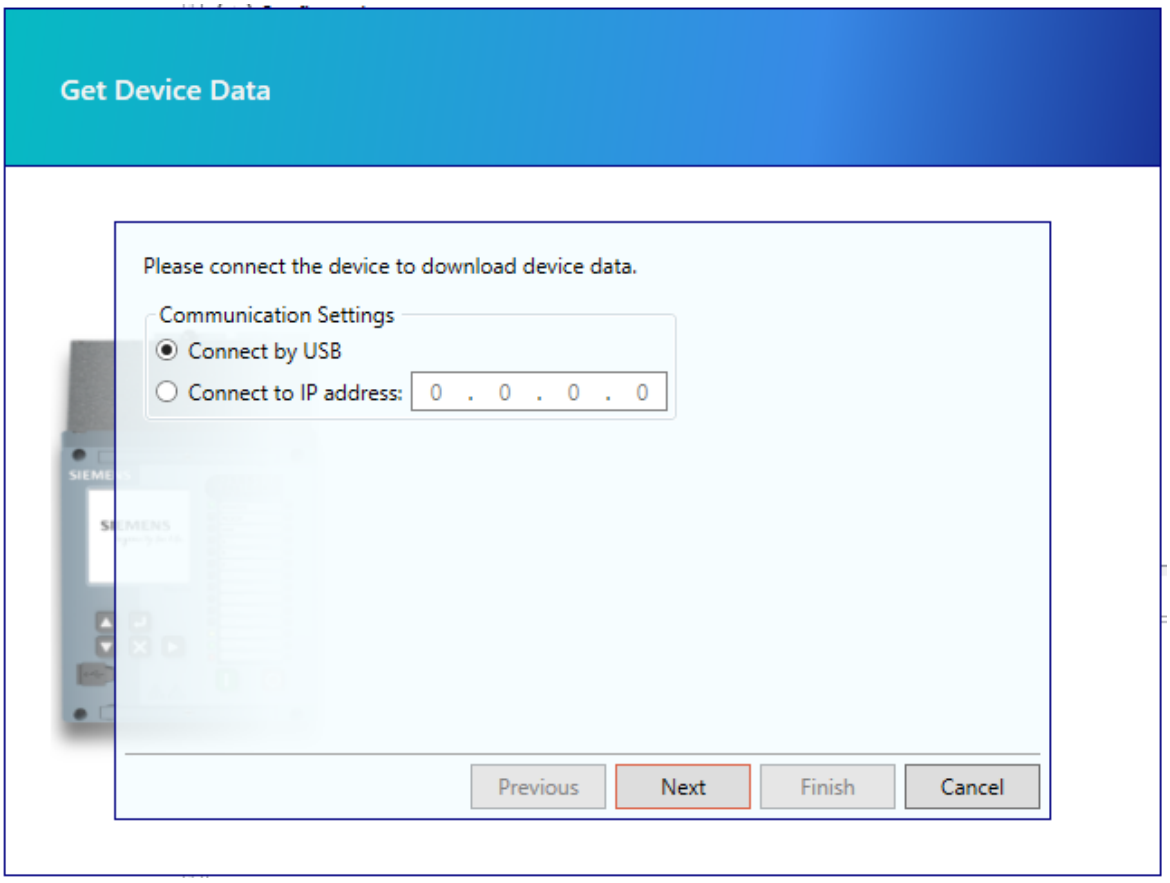
Figure 5-10 Send Device Configuration

In the project tree, select the device of the offline configuration and in the device tasks menu click **Send Device Configuration**.

Alternatively click the **Send** button in the **`Device Details`** screen on the right hand side.

The **Send Device Configuration** window opens and the user can then select the connection method. Select **Connect by USB** for first time connection to the relay.

Reydisp Manager 2 recognizes automatically that the device is connected via USB cable.

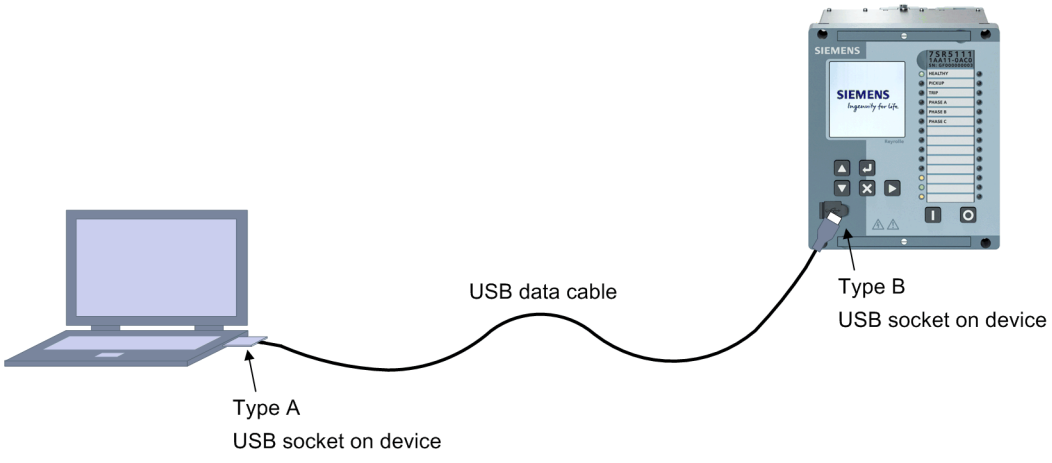


[sc_7SR5_ReydispManager2ConnectByUSB, 1, _, _]

Figure 5-11 Send Device Configuration Window

Connect by USB

The 7SR5 device provides one front USB communication interface (Com2) on the fascia to connect to every modern PC. Sending configuration for the first time must be done via a USB port. Once a conventional USB cable is connected to the relay, proceed with **Connect by USB** in communication settings.



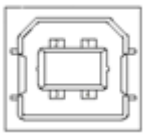
[dw_7SR5_communication_to_front_USB_port, 1, en_US]

Figure 5-12 Front USB Connection

The front USB port for local connection (Standard) with a cover provides environmental protection.

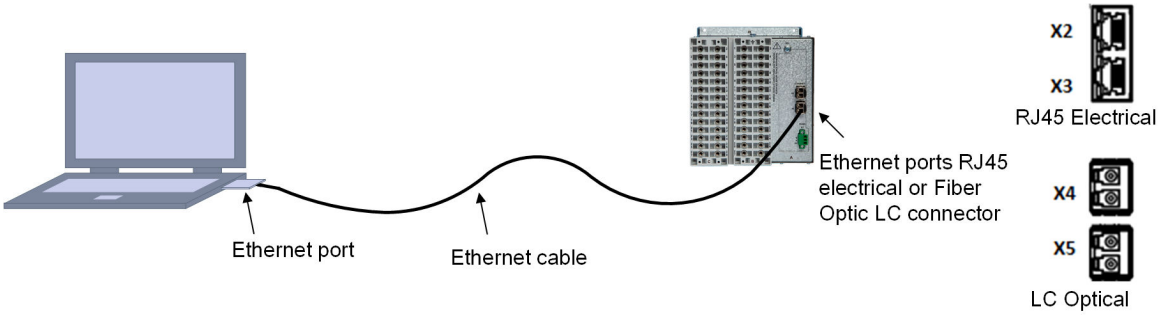
The device functions can be set on a PC using Reydisp Manager 2 software via the relay USB port by a standard USB cable.

The COM-2 USB port has the IP address 192.168.2.1.

A Type-B  connection is required for a 7SR5 device and a Type-A  plug for a PC connection.

Connect to IP Address

Ethernet ports installed on the rear of the device can be used for IEC 61850, DNP3 TCP, and Modbus TCP communications to a substation SCADA, integrated control system, or engineer remote access using Reydisp Manager 2 configuration software.



[dw_7SR5_communication_to_rear_ethernet_port, 1, en_US]

Figure 5-13 Rear Ethernet Port Communication by IP Address

2 rear Ethernet ports (Standard) could be RJ45 electrical or LC optical duplex connector types (Fibre optic) optionally with Channel 1 and Channel 2.

2 electrical (RJ45) ports (Channel 1/Terminal Reference X2 and Channel 2/Terminal Reference X3) or 2 optical (LC) ethernet ports (Channel 1/Terminal Reference X4 and Channel 2/Terminal Reference X5).

The Ethernet port is unconfigured by default. IP addresses can be entered manually via the **Configure Interface** menu in **Tasks** by the user.

- IEC 61850, HSR , PRP and RSTP operation
- Remote access to Reydisp Manager

If a device does not have a configured IP address on the rear Ethernet port, then the device configuration must be sent from Reydisp Manager 2 using the front USB port.

Once a device has the rear Ethernet port configured with an IP address then the Ethernet port can be used for device configuration.

[sc_7SR5_DeviceConfigWindowSuccessUnsuccess, 1, --]

Figure 5-14 Sending Device Configuration Window With and Without Success

Loading of the configuration from the Reydisp Manager 2 project to the device is then initiated showing *Figure 5-14*. The offline configuration is thereby transferred to the device once **Complete** is shown at the end. After a successful transfer, the device will restart.

When uploading settings to the device, Reydisp Manager 2 checks that the settings are compatible with the designated device. If they are incompatible the settings are not uploaded to the device. There will be warning messages displayed in red on the information window without the word **Complete**. The user should check these incompatible settings.

5.4 Transferring Device Data from the Device to the PC

The device stores data that can be viewed and analyzed on the PC.
The following data files can be retrieved from the device using Reydisp Manager 2:

- Waveform records storage
- Fault records storage
- Event log

When retrieved from the device the files will be associated with the device in the project and stored on the PC using the time and date of the file as the default name.

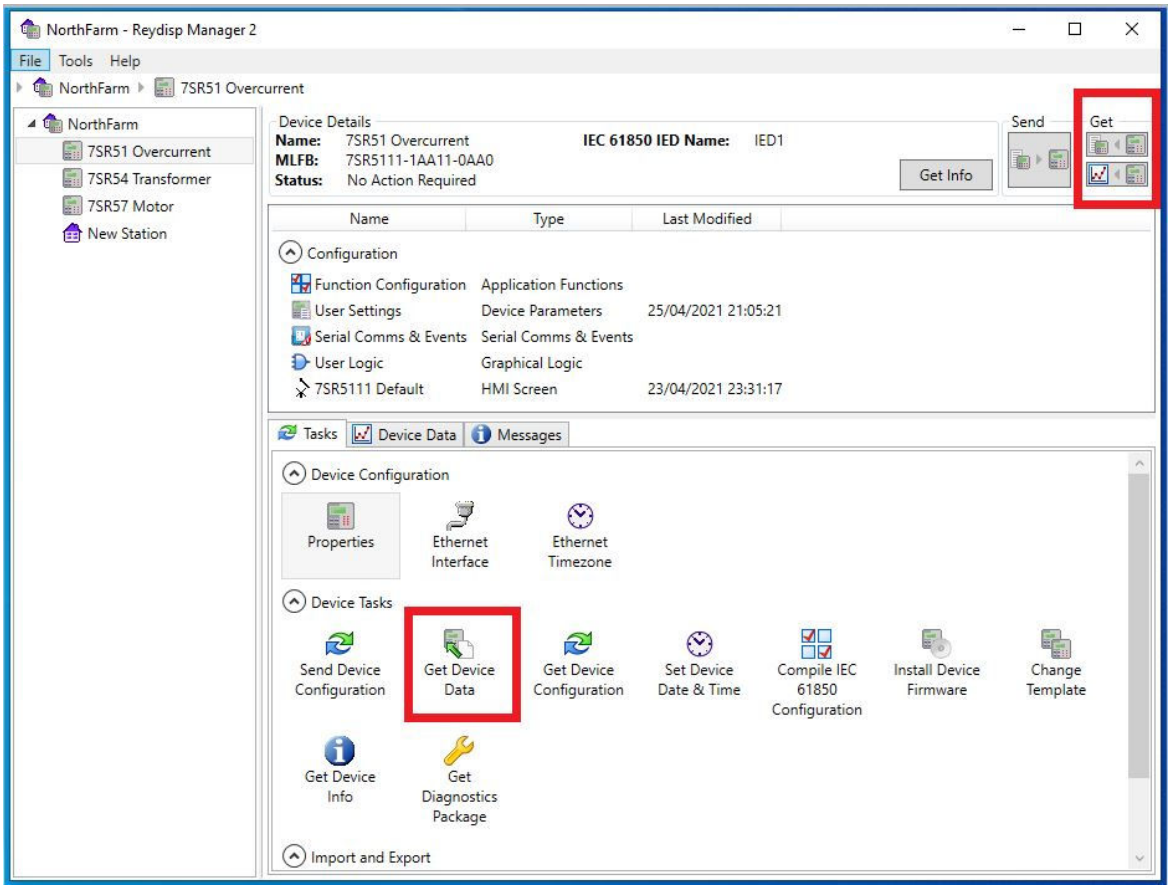
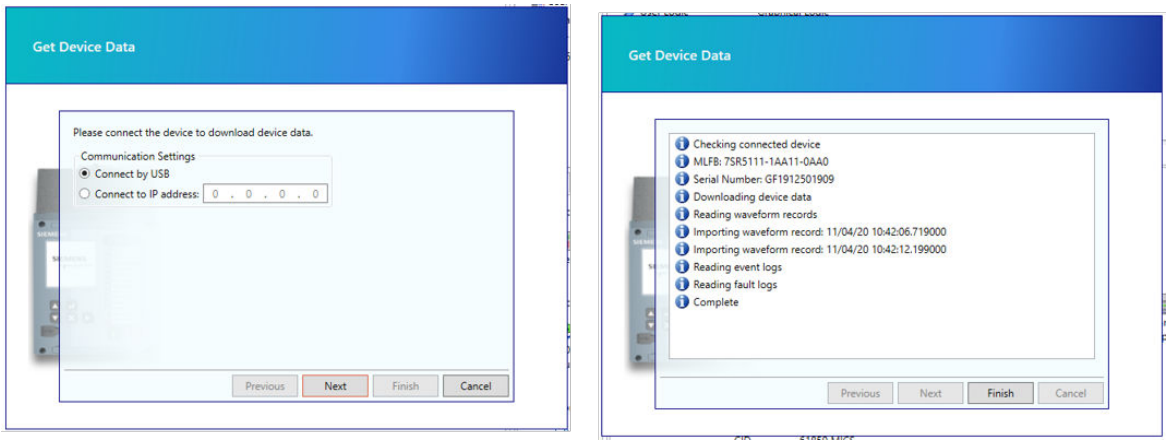


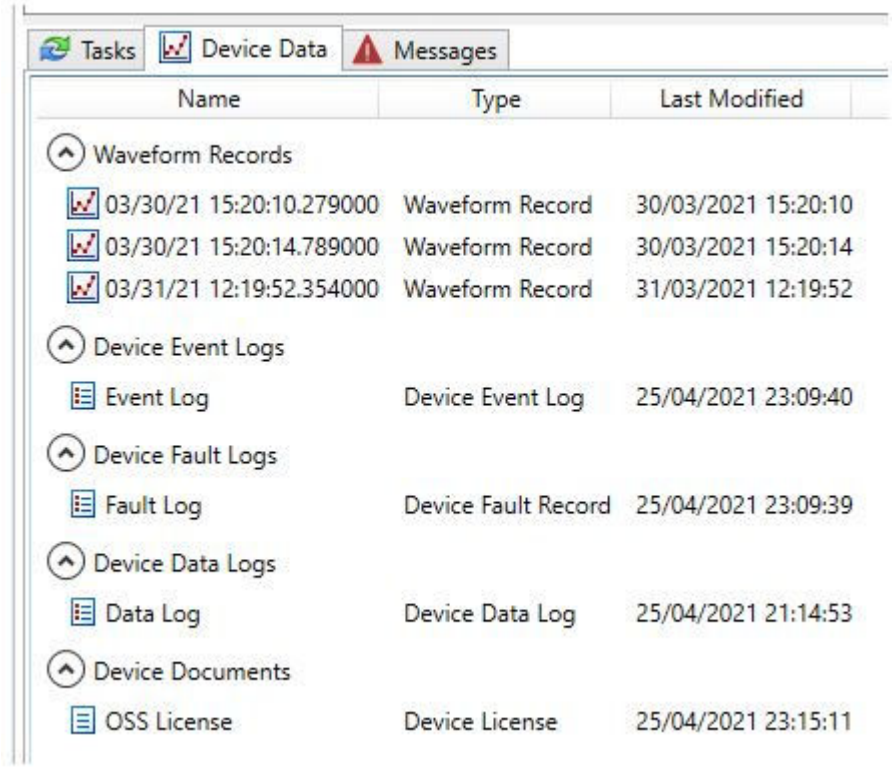
Figure 5-15 Get Device Data

Once **Get Device Data** has been selected, the device data can be retrieved from the device.
A connection window is provided to select between the default USB connection method or connecting via the rear Ethernet port using the IP address of the device. The connection type to the device can be selected and the **Next** button clicked to start getting device data read from the device.



[sc_7SR5_GetDeviceDataWindow, 1, --_--]

Figure 5-16 Get Device Data Window



[sc_7SR5_DeviceDataTab, 1, --_--]

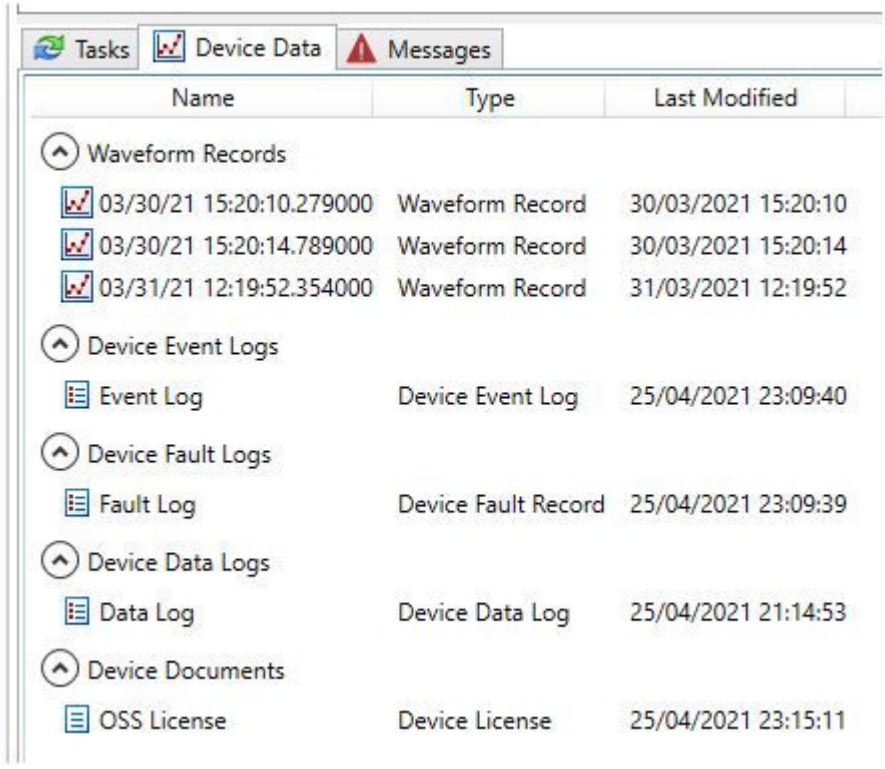
Figure 5-17 Device Data Tab

Once complete, available data files will be stored under the **Device Data** tab that are read from the device. All entries can be archived as files which can be used in further applications.

The file name can be changed by the user by a right-click of the mouse on the waveform record and entering the preferred name followed by **Apply**.

5.5 Retrieving Fault Records and Log Contents

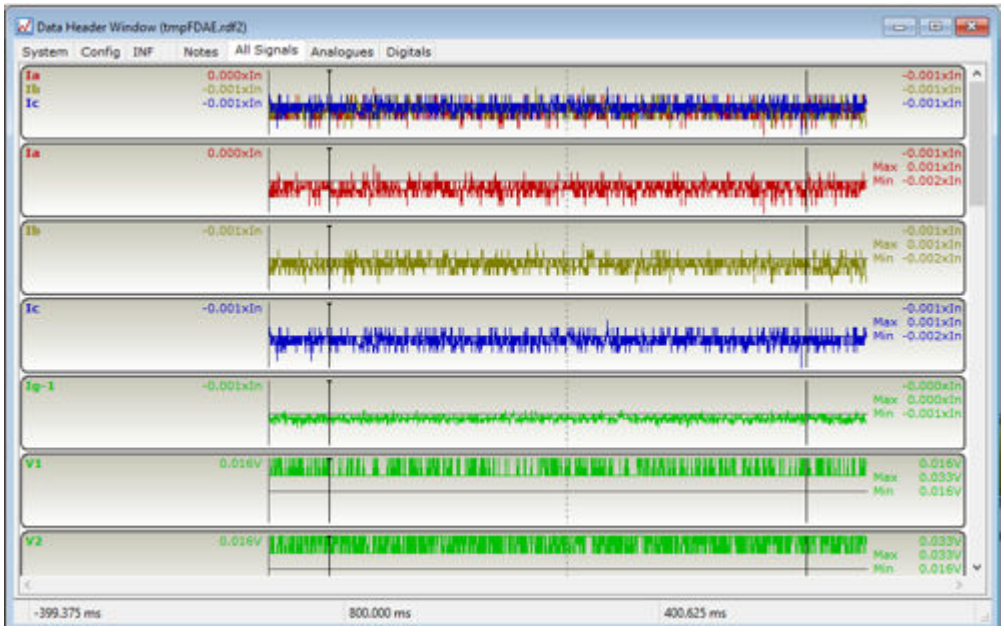
To retrieve fault records the user must select and double click on the available Waveform record from the **Device Data** window to open the data content.



[sc_7SR5_DeviceDataTab, 1, --_--]

Figure 5-18 Device Data Window

The waveform display window will open as illustrated in *Figure 5-19*.



[sc_7SR5_WaveformDisplay, 1, --_--]

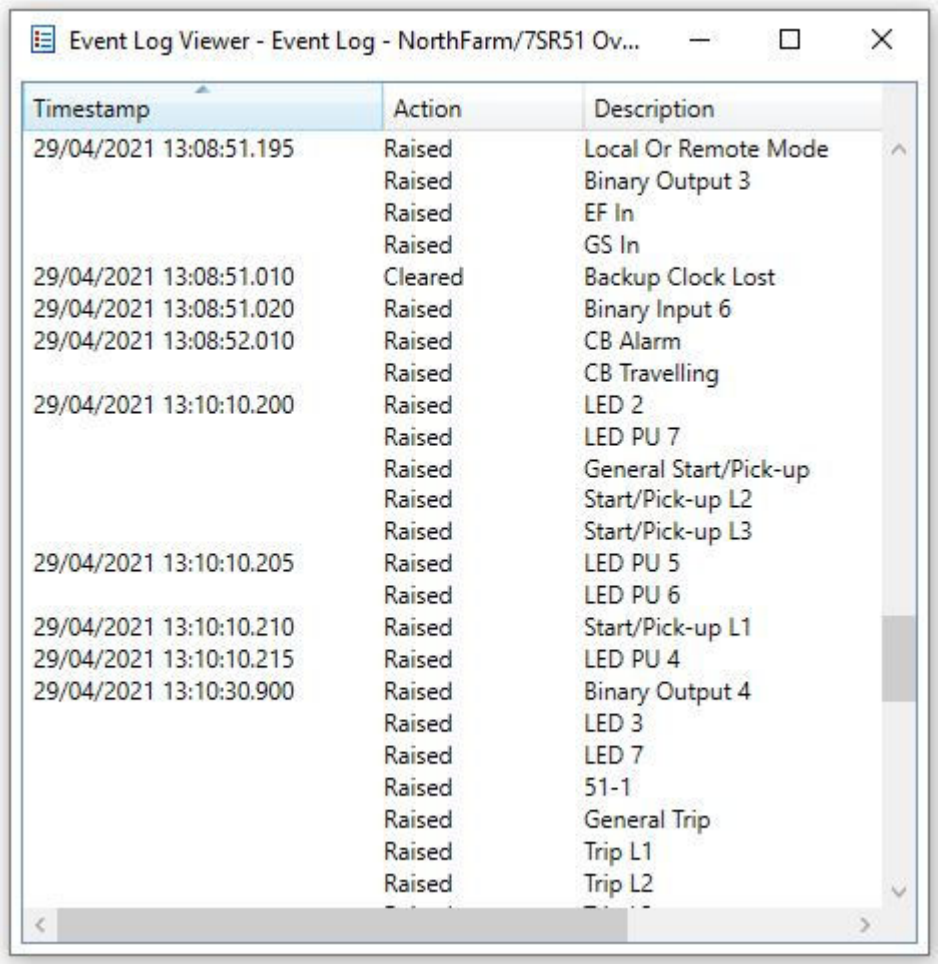
Figure 5-19 Waveform Display

Initially for each type of device there are default views defined containing the Analogue Channels, Digital Channels and All Channels. Users can create new views or modify existing views, edit the analogue channel information, and format the display using the View/Properties command.

To retrieve log records the user must select and double click on the available Event record from the **Device Data** window.

The **Event Log Viewer** window will open and any time tagging of any change of state (Event) in the relay can be seen. As an event occurs, the actual event condition is logged as a record along with a time and date stamp to a resolution of 1 millisecond.

When a starter picks-up (raised) and sometime later drops-off (cleared). In summary, a one stage event is Raised only, a two stage event maybe Raised or Cleared.



[sc_7SR5_EventLogViewer, 1, --_--]

Figure 5-20 Event Log Viewer

6 Commissioning

6.1 Overview

This chapter contains information about the commissioning of the 7SR5 device. You will get an overview of the numerous possibilities of initial startup in chapter *6.2 Initial Startup*.

The commissioning and maintenance of this equipment should only be carried out by skilled personnel trained in protective relay maintenance and capable of observing all the safety precautions and regulations appropriate to this type of equipment and also the associated primary plant.

Various tests have to be performed for commissioning to warrant the correct function of the device.

Secondary tests can never replace primary tests because they cannot include connection faults. They provide a theoretical check of the setting values only. Primary tests may be done only by qualified personnel who are familiar with the commissioning of protection systems, with the operation of the system, and with safety regulations and provisions (switching, grounding, etc.). Switching operations also have to be performed for the commissioning. The described tests require that these be capable of being performed safely. They were not conceived for operational checks.

Inspection

Check that the device is not physically damaged.

The equipment ratings, operating instructions, installing instructions, and terminals must be checked before commissioning or maintenance actions.

The integrity of any protective earth conductor connection shall be checked before carrying out any other actions.

Ensure that all connections are tight and correct to the wiring diagram and the scheme diagram in the device manuals. Check that the relay is the correct model and version and is correctly configured. Check that it is fully inserted into the case.

Ensure that the device is grounded from the earthing points correctly.

Hardware Tests

Operation of all inputs and outputs are tested in the factory. Tests can be repeated to check the device operation in its intended application or by simple direct operation tests as described in this section.

The status indications of the respective binary inputs and binary outputs can be read from **Instruments > Binary I/O meters** that are described in *4.7 Display of Routings and Status*.

The user must apply the required supply voltage onto each binary input in turn and check for correct operation.

Each individual binary output can be tested with the **Output Matrix Test** menu from **Settings > Configuration > Maintenance** by performing a close command.

AC measuring accuracy is calibrated and tested in the factory but can be easily tested by checking values displayed by the instruments during secondary injection as described.

The LEDs may be tested in 3 ways:

- Pressing the ► key for ≥ 3 seconds when the home screen is displayed
- Energizing a suitably programmed binary input
- Sending an appropriate command over the data communications channel(s)

Putting into Service

After tests have been performed satisfactorily the relay should be put back into service as follows:

- Remove all test connections
- Firmly tighten all screws. Tighten all terminal screws, including those that are not used.
- Replace all secondary circuit fuses and links, or close miniature circuit-breakers.
- Ensure the Protection Healthy LED is on and steady if configured, and that all LED indications are correct. If necessary press the X key until the **Relay Identifier** screen is displayed, then press ► to reset the indication LEDs for ≥ 3 seconds.

- The meters should be checked in Instruments Mode with the relay on load.
- The complete configuration should be downloaded to a computer and a copy stored for record of the settings produced. The installed settings should then be compared against the required settings supplied before testing began. Check if protection, control and auxiliary functions to be found with the configuration parameters are set correctly. Automated setting comparison can be carried out by Reydisp using the check operation of Reydisp Manager. Settings can be downloaded from the device, and compared, using Reydisp Manager. The described tests are for guidance for experienced personnel that can ensure that these are performed safely.

Routine Maintenance

The device does not require scheduled preventative maintenance although some users apply periodic checking schedules to all protection devices. Operational checking can be limited to periodic visual checks of measured analogue values at the device instruments or the data provided over the communications channels to supplement the continuous self-checking features of the device.

Repair

The device is designed with no user serviceable parts and if a device reports a failure it can be returned to Siemens for investigation and repair. Contact and return details will be provided by the local Siemens office. Necessary precautions such as isolating the equipment, power supply and connections should be applied before investigating further, particularly with respect to safety earthing.

6.2 Initial Startup

It is assumed that the steps in chapters 1 to 4 have been followed. Check the connection of the auxiliary power supply. 7SR5 devices have universal power-supply unit designs (Between DC 24 V and DC 250 V, AC 100 V and AC 230 V auxiliary voltage range).

Ensure that the correct auxiliary supply voltage and polarity is applied. Before making any connections, the device must be grounded.

See the relevant scheme diagrams in the device manual for the following relay connection terminals:

- B22 terminal for + or L polarity
- B24 terminal for – or N polarity
- B28 terminal for Ground (Earthed)

After successful testing of the voltage source, the device can be switched on.

The device is now energized with the **`Device Not Configured`** message on it's LCD display if it has not been configured. The display of the message cannot be disabled as the act of changing any parameter or loading a user configuration will automatically turn it off.

Afterwards, configuration can be sent to the device with Reydisp Manager 2 by reading the information in *5.4 Transferring Device Data from the Device to the PC*.

Settings and Configuration

Select the required relay configuration and settings for the application. If more than 1 settings group is to be used for the application, it may be necessary to test both groups and also to test operation of the change mechanism.

When using settings groups it is important to remember that the relay need not necessarily be operating according to the settings that are currently being displayed on the device screen. There is an Active Settings Group on which the relay operates and an Edit/View Settings Group which is visible on the display and which can be changed from the fascia keys. This allows the settings in 1 group to be altered from the relay fascia while the protection continues to operate on a different unaffected group. The Active Settings Group and the Edit Settings Group are selected in the **Configuration Device** menu.

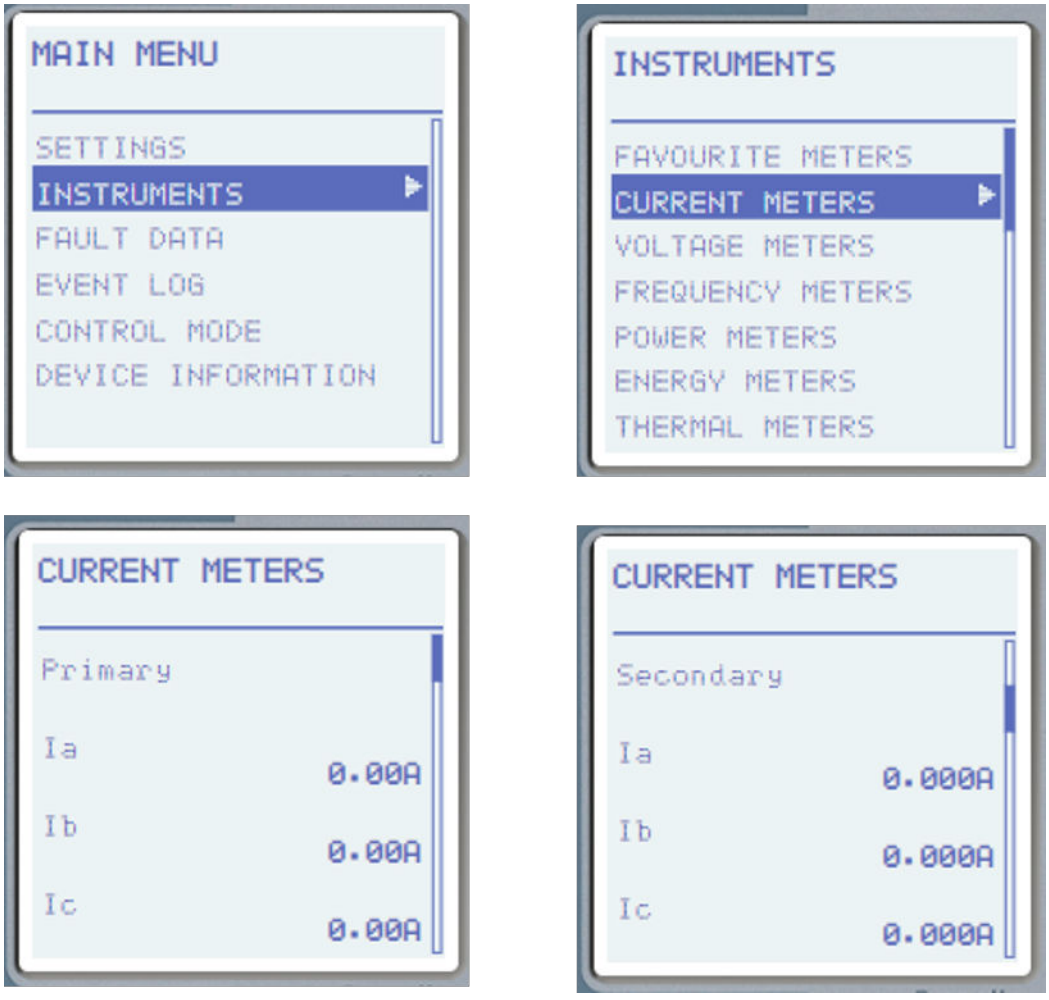
The currently Active Group and the group currently Viewed are shown at the top of the display in the **Settings** display screen. If the View Group is not shown at the top of the display, this indicates that the setting is common to all groups.

CT/VT ratio, I/O mapping and other settings which are directly related to hardware are common to all groups. If the relay is allowed to trip during testing then the instruments display will be interrupted and replaced by the **Trip Alert** screen which displays fault data information. If this normal operation interferes with testing then this function can be temporarily disabled for the duration of testing by use of the Trip Alert enabled/disabled setting in the **Configuration Device** menu.

Instruments from Fascia HMI

The **Instruments** menu shows measured or calculated values and some indications read from the 7SR5 device. Measurement sub-menus display key quantities and information to aid with commissioning. The following meters are available and are navigated around by using the ▲ and ▼ buttons dependent on the analogue input configuration of the device.

The device instrumentation and metering provides real-time measured quantities and data. This is displayed on the relay fascia LCD (when in the **Instruments** menu) or via the data communications interface.



[sc_7SR5_CurrentMetersDisplay, 1, --_--]

Figure 6-1 Current Meters Display

The **Main Menu > Instruments > Current Meters** menu displays the real-time measured current from analogue current inputs with primary and secondary values (by pressing the ▼ button to see the secondary values).

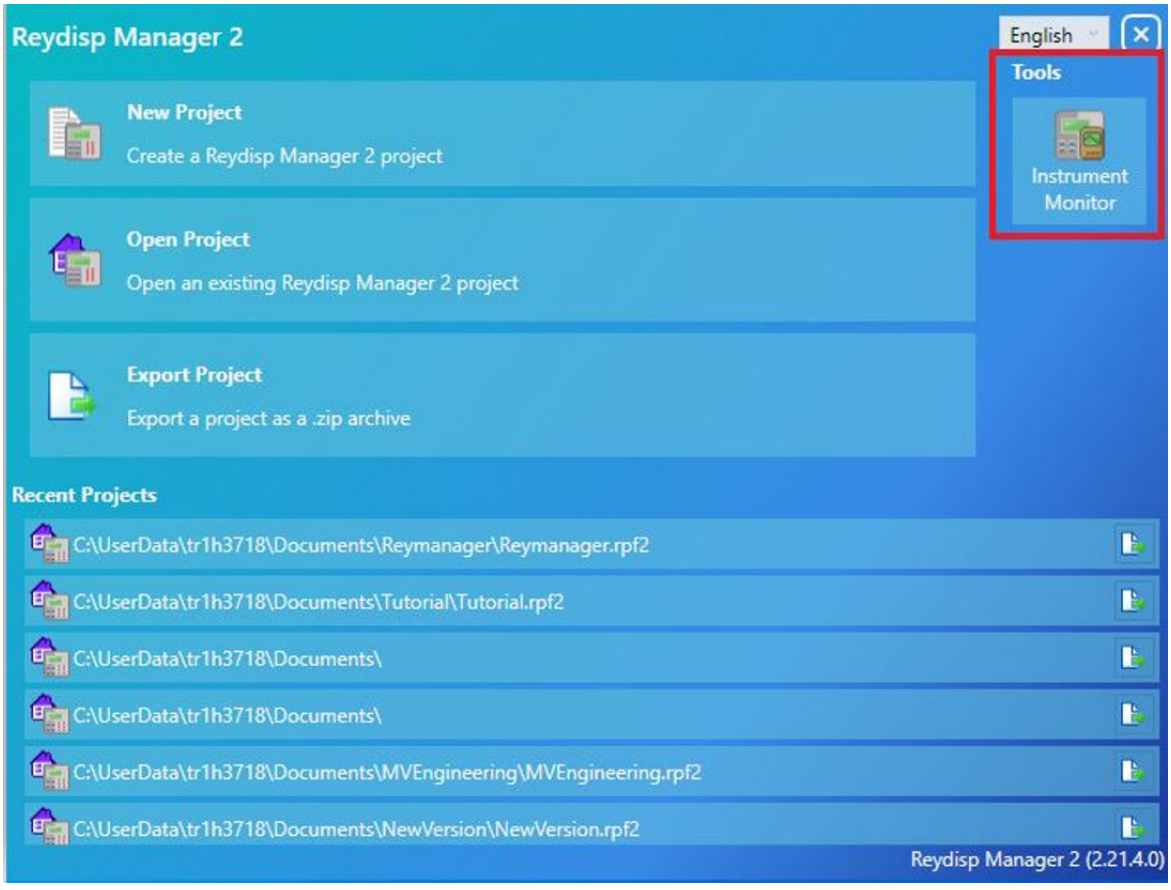
Instruments from Reydisp Manager 2 (Relay Monitor Tool)

The **`Relay Monitor Tool`** displays a real time list of instruments from a device. Real time analogue values measurement requires a device to be connected to a PC using a USB or rear ethernet port for data to be transferred to the PC online.

If there is a communication connection to systems control, measured values that the operational crew can verify are also transmitted here by rear ethernet communication.

The device is able to indicate the measurand values from Reydisp Manager 2 software with connection by COM-2 using the front USB port which has the IP address 192.168.2.1. or user configured IP address from the rear ethernet ports (Electrical or LC optical).

In order to access the online monitor tool, click the **Instrument Monitor** box on the **Reydisp Manager 2 Startup** screen.



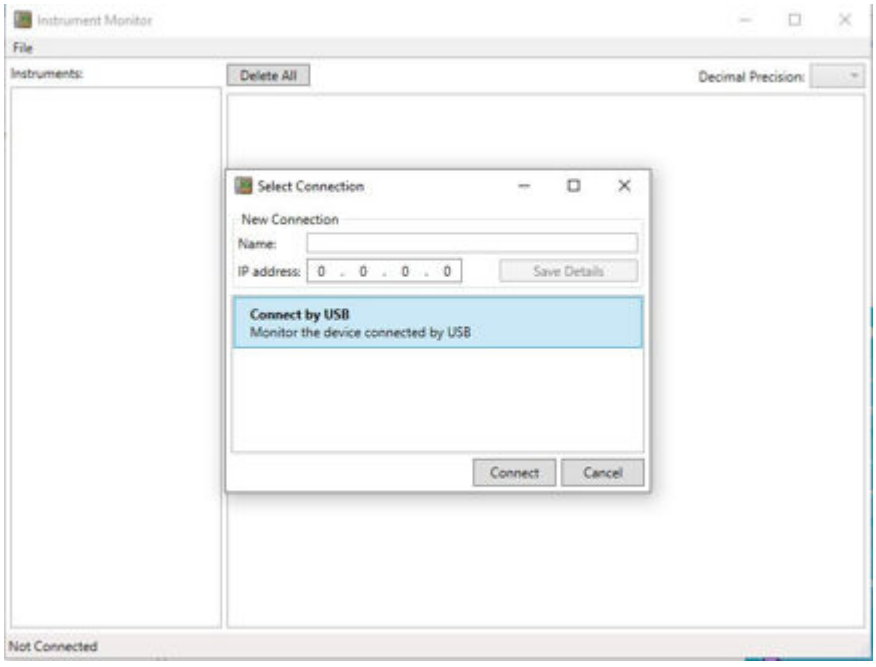
[sc_7SR5_InstrumentMonitor, 1, --_--]

Figure 6-2 Opening the Relay Monitor Tool

The user should click on the **Create New Connection** button at the top of window.

The IP address 192.168.2.1 should be typed for the USB front port connection or user defined IP address for the rear ethernet port connection to the IP Address box.

The user can then click the **Create** button and select connection, then click the **Connect** button to open the **`Relay Monitor Tool`**.



[sc_7SR5_ConnectionWindow, 1, --_--]

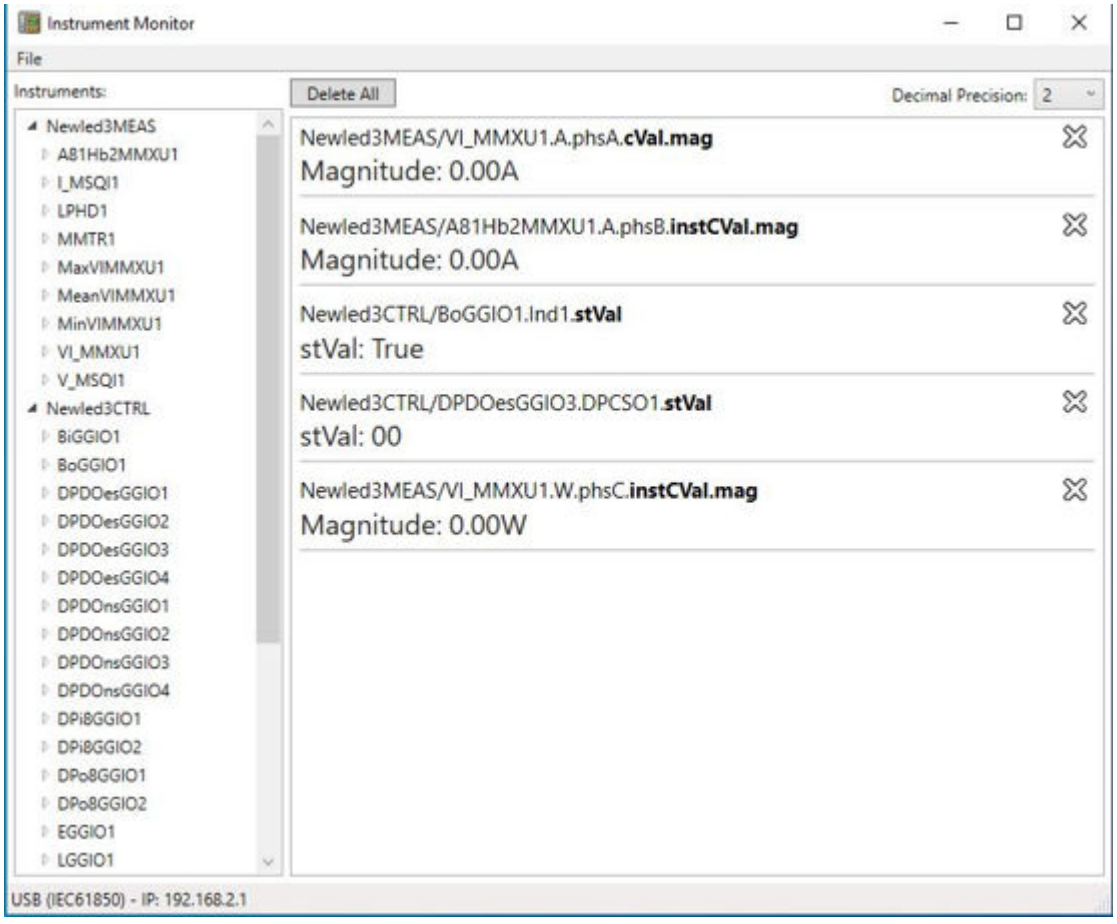
Figure 6-3 Connection Window

There is an instrument list on the left pane containing measurand groups depending on the device type. Groups can be expanded and collapsed by clicking on an item.

Available measurands can be selected by clicking on the left **instruments** tree and dragging this signal to the right side main window, then releasing the mouse button.

Several signals can be dragged to the main window on the right and provide continuous monitoring of the measurands. Alternatively, the measurands could be deleted and removed from the main window by clicking the X symbol on the right side of the window.

Several measured-value windows are preadjustable by adding relevant measurands.



[sc_7SR5_RelayMonitorTool, 1, --_--]

Figure 6-4 Relay Monitor Tool

6.3 Secondary Tests

Secondary tests can never replace primary tests because they cannot detect connection faults. They provide a theoretical check of the setting values only. Please see section 9 of the device manual for further information.

For tests using secondary test equipment, make sure that all necessary input signals are simulated and output circuits are interrupted, particularly trip and close commands to the circuit-breakers and other plant unless that functionality is included in the test.

When testing the device with secondary test equipment, make sure that no other measurement quantities are connected and that the trip and close circuits to the circuit-breakers and other primary switches are disconnected from the device.

Isolate the auxiliary DC supplies for alarm and tripping from the relay and remove the trip and intertrip links.

Ensure that any essential services that share supplies are not interrupted.

Disconnect communications ports or configure control systems to prepare for the tests.

In **`Out of service`** mode the output relays will not operate and the serial communications signals will not be sent over the rear Remote port. In **`Test`** mode the IEC 61850 signals will be marked as test.

Carry out injection tests for each relay function as required as described in this document.

NOTE

For all high current tests it must be ensured that the test equipment has the required rating and stability and that the relay is not stressed beyond its thermal limit. The maximum duration of the current injection should be limited in case an error is present such that the expected relay operation does not stop the test.

Secondary tests must only be carried out by personnel who are qualified electricians and are familiar with the commissioning of protection systems, the operation of the system, and with safety regulations and provisions (switching, grounding, etc.).

Make sure that there are no connections to the primary system during the secondary test. In the secondary test it is assumed that there are still no connections to the primary system, but if you do this in the primary system, special safety conditions must be followed. Connection examples for current and voltage transformer circuits are provided in the device manuals.

Before checking, the user should familiarize themselves with the measuring principle of the protection function in the Device manual and consider the test recommendations given in the Device manual:

- Perform the tests using multi-phase test equipment since numerous protection functions require a 3-phase system.
- Most protection functions can be tested using stationary signals. Some protection functions require transient signals. Typical examples are the testing of protection reaction on power swings (power-swing blocking in distance protection and out-of-step protection) and the transient effect on transformers. They generate transient test files with a dynamic network calculation program or these test files are provided by special test programs.
- If setting values are offered only in percent or per unit, the setting values refer only to rated quantities of the protected object. Secondary test quantities must be converted using the transformer ratio.
- Perform the tests successively. Activate only the function that you wish to test. Make use of Reydisp Manager 2 support.
- Since protection functions can be assigned to different protection function groups, check the interaction between function groups as well. If the user has created their own application template or modified the delivered template, Siemens recommends that they check the interaction. The application templates provided with the device have been tested.
- Check the reaction of the protection functions via the indications in the corresponding logs. The indications in the spontaneous indication log (available in online mode), which are shown at the moment of occurrence, are a good tool. Testing using the fault record (binary signal traces in relation to the input variables) is also advisable for transient processes.

- Check the correct routing of signals of the protection function.
- Check individual protection functions in the test editor using signals from test equipment or the internal signal generator (sequences). Examine the test sequence in the characteristic curve of the protection function and its spontaneous indications.

6.4 Primary Tests

A requirement for the primary test is that prior tests (see *6.2 Initial Startup* and *6.3 Secondary Tests*) have been completed successfully.

Primary tests may be done only by qualified personnel who are familiar with the commissioning of protection systems, with the operation of the system, and with safety regulations and provisions (switching, earthing, etc.).

Primary injection tests are essential to check the CT ratio and polarity of the CT transformer connections as well as the secondary wiring to the device terminals.

Switching operations also have to be performed for complete commissioning of the protection system.

NOTE

For all high current if the current transformers associated with the protection are located in power transformer bushings it may not be possible to apply test connections between the current transformer and the power transformer windings. Primary injection is needed, however, to verify the polarity of the CTs. In these circumstances primary current must be injected through the associated power transformer winding. It may be necessary to short circuit another winding in order to allow current to flow. During these primary injection tests the injected current is likely to be small due to the impedance of the transformer and limitations of test equipment.

DANGER

Danger due to hazardous voltages during the operation of electric devices

Noncompliance with the safety notes will result in death or severe injuries.

✧ Only electrically qualified personnel may work on these devices. The electrically qualified personnel must be thoroughly familiar with pertinent safety regulations and precautionary measures as well as the warnings in this manual.

6.5 Device Configuration

6.5.1 Date and Time Synchronization

The integrated date and time synchronization of a 7SR5 device allows the user to assign the precise time of events to an internally maintained device time. Events in the logs are stamped with the device time. These time stamps are also transmitted during transmission to substation automation technology or via a protection interface. The user can synchronize the device time using external time sources. The user can also take local time zones and daylight-saving time arrangements into consideration.

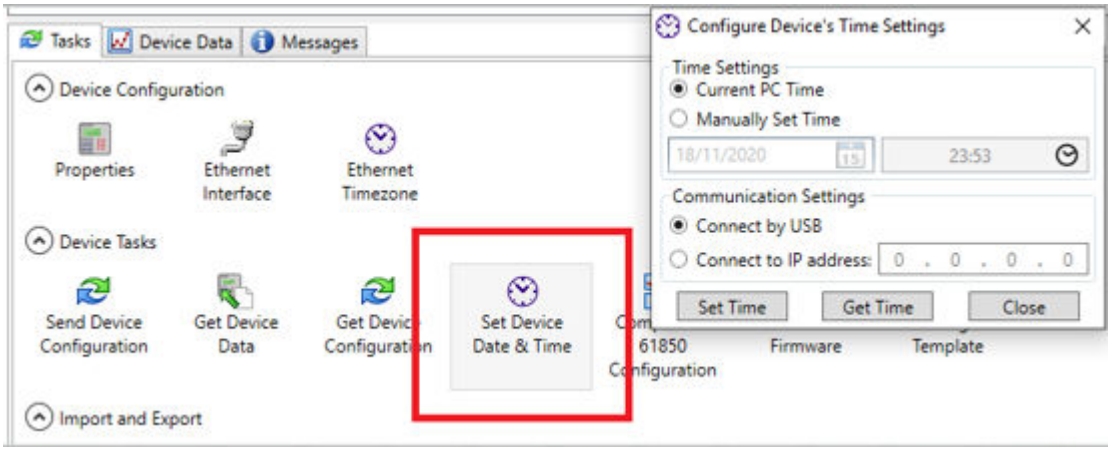
6.5.2 Setting Time and Date

Date and time are internal device quantities that can be set from a 7SR5 device on the device fascia using the menu keys as well as Reydisp Manager 2.

6.5.3 Setting via Reydisp Manager 2

The device task operations for each device include the option to **Set Device Date & Time**.

Double clicking the icon in the Tasks menu opens a time setting window to select the preferred source of the time to be sent to the device. The default option is to use the time from the PC as the source but an option is also available to manually enter a preferred time and date.



[sc_7SR5_SetDateTime, 1, --, --]

Figure 6-5 Set Device Date & Time

The window also includes the connection options available, with the default connection selected as a direct connection from the PC to the front USB port and an option to select an IP address for ethernet connection.

The **Set Time** button is clicked to send the time and date to the device.

The **Get Time** button will retrieve the time and date from the device to confirm the time is correct. The time retrieved from the device will be shown in the Time Settings area of the window.

6.5.4 Setting Date and Time via Front Fascia Keys

To reach the date and time settings from the main menu, use the navigation keys on the front fascia **Main Menu > Settings > Configuration > Device**.

Select the **Date** and **Time** menus.

Press the Enter button to change the date and time, then by using ▲,▼, buttons increase and decrease the values. Once complete confirm the new value using the Enter button.

[sc_7SR5_SetDateTimeFascia, 1, --_--]

Figure 6-6 Set the Date & Time from the Front Fascia

6.5.5 Device Configuration of the Ethernet Timezone

The device operational time is set in local time. The Ethernet Timezone feature allows the timezone to be set for the device Ethernet port and allows the daylight saving times to be set. This is only applicable for Ethernet communication.

By default, the relay is set to GMT, with no daylight saving offset specified.

To set the Ethernet timezone in the device configuration the user must select the following icon.

The Edit Timezone dialogue window will appear for editing as required by the system application.

Clicking **Apply** will apply the new timezone to the device in the project.

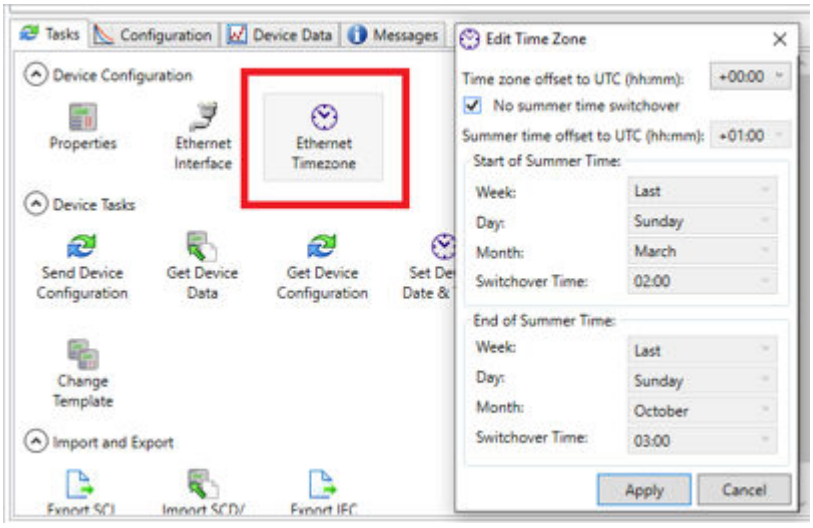


Figure 6-7 Ethernet Timezone

Table 6-1 Timezone Settings

Setting	Description
Time zone offset to UTC	This should be set to the offset to UTC
No summer time switchover	Selecting this results in the time remaining the same throughout the year. If this is ticked, the options below it relating to summer time are disabled.
Summer time offset to GMT	This should be set to the offset to GMT for summer time.
Start of Summer Time	The time daylight savings start
End of Summer Time	The time daylight savings ends

6.5.6 Changing the Language on the Device Display

The language of the text displayed on the device LCD can be selected and supports multi language capability.

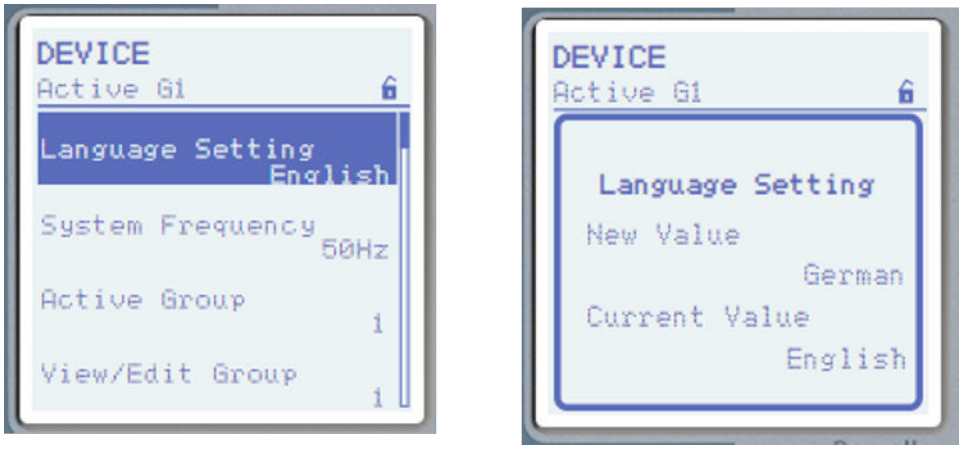
To reach the language selection menu, go to **Main Menu > Settings > Configuration > Device**, and select **Language Setting**.

Press the Enter button to change language, then by using ▲,▼ buttons select the desired language from the list.

The languages available are:

- English
- French
- German
- Portuguese
- Spanish
- Turkish

After confirming setting changes, the device will restart with the new language on the LCD display.

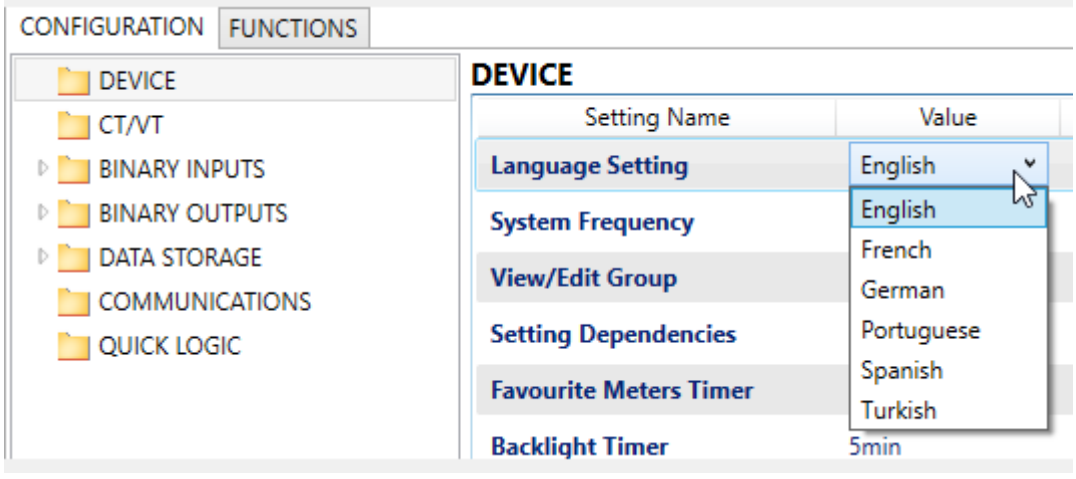


[sc_7SR5_LanguageSettings, 1, --_--]

Figure 6-8 Language Settings via the Front Fascia

The language of the text displayed on the device LCD can also be changed using Reydisp Manager 2 from the **Configuration > Device** menu.

The setting is accepted in the device through sending the device configuration into the device.



[sc_7SR5_LanguageSettingsReydisp, 1, --_--]

Figure 6-9 Language Settings via Reydisp Manager 2

6.5.7 Changing Confirmation IDs

Confirmation IDs are used for protection against unintentional and unauthorized operation. If a confirmation ID is activated, you must enter it before the relevant action is enabled by the 7SR5 device. For this purpose, the confirmation ID is transmitted in an encrypted way to the 7SR5 device, where it is checked.

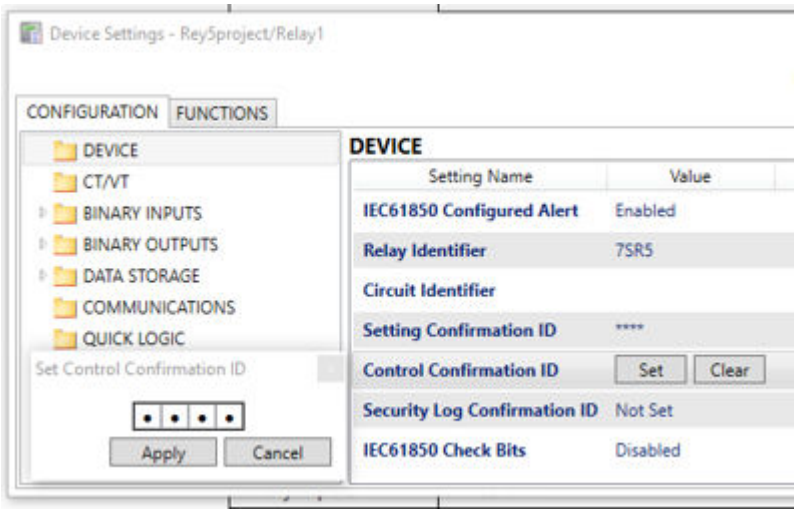
Authorization for security-relevant operations on the device directly via the fascia or Reydisp Manager 2 is assured by the assignment of confirmation IDs. These confirmation IDs are assigned exclusively using Reydisp Manager 2. You can find more information in the Security Manual.

To reach the menu for the confirmation IDs of your 7SR5 device, open **Configuration > User Settings > Device settings** in Reydisp Manager 2.

The confirmation IDs for 3 different access types will appear in this window.

`Not Set` means no confirmation IDs are parametrized for this function.

`****` means a confirmation ID is already parametrized for this function.



[sc_7SR5_ConfirmationID, 1, --_--]

Figure 6-10 Confirmation ID

Activate or deactivate a confirmation ID by clicking on it and selecting **Set** to open the change window.

To change a confirmation ID, enter a new 4 character alpha-numeric code into the boxes and click the apply button.

A user identifier code is required for settings changes at the device fascia. The Setting ID is set in Reydisp Manager (**Configuration > Device > Settings Confirmation ID > Set**).

Settings changes can only be made at the device fascia after the Setting ID code is entered.

The Setting ID will timeout 60 minutes after the last key press, or if the Control ID is entered.

A user identifier code is required to carry out control operations from the device fascia. The Control ID is set in Reydisp Manager (**Configuration > Device > Control Confirmation ID > Set**).

Settings changes can only be made at the device fascia after the Setting ID code is entered.

The Control ID will timeout 60 minutes after the last key press, or if the Control ID is entered.

A user identifier code is required for settings changes at the device security log. The Security Log Confirmation ID is set in Reydisp Manager (**Configuration > Device > Security Log Confirmation ID > Set**).

The security log can only be viewed at the device fascia after the Security Log Confirmation ID has been entered.

After activating a confirmation ID, when using the front fascia menu, the user can access settings by entering the ID using ▲or ▼ buttons.

[sc_7SR5_ConfirmationIDWindow, 1, --_--]

Figure 6-11 Confirmation ID Display

6.5.8 Settings Group Switching

For different applications and operation, cases require different function settings. In a settings group, the user can set the settings specifically for an operating case.

All 7SR5 devices support up to 4 independent settings groups.

Group number (Gn) 1 to 4.

At any 1 time only 1 group of settings can be active.

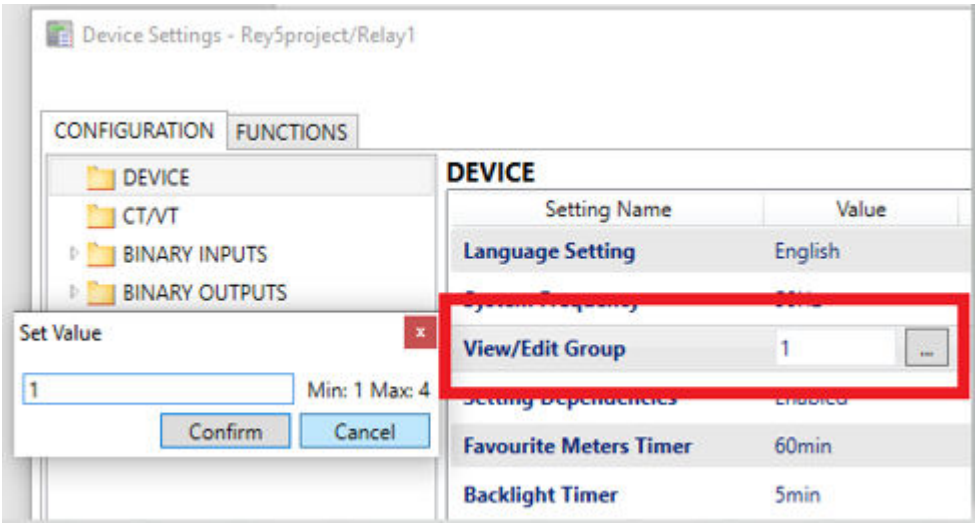
The user can save the respective function settings in so-called Settings groups and, if necessary, activate them quickly. In the process, only one settings group is active at any given time. During operation, the user can switch between settings groups. The source of the switchover can be selected via a parameter.

Switchover of the settings groups can be done via the following alternatives:

- Via the front fascia LCD display menu directly on the device
- Via an online PC connection to the device via Reydisp Manager 2
- Via binary inputs
- Via communication connection to a substation automation technology

The communication protocols IEC 60870-5-103, IEC 61850, DNP3 TCP, Modbus RTU, and Modbus TCP can be used for switching the settings groups.

A settings group includes all switchable settings of the device. Except for a few exceptions (for example, general device settings such as rated frequency), all device settings can be switched.



[sc_7SR5_SettingsGroupsReydisp, 1, --_--]

Figure 6-12 Settings Group via Reydisp Manager 2

6.5.9 Changing Setting Group via Device Display

To reach the Setting Group menu, proceed via **Main Menu > Settings > Configuration > Device**.

Select **Active Group** to activate one of the setting groups (1 to 4).

Select **View/Edit Group** to edit 1 group while the relay operates in accordance with settings from another active group using.

Press the Enter button to change group number, then by using ▲,▼ buttons select the group.

The device is informed about a settings group change process from the display.

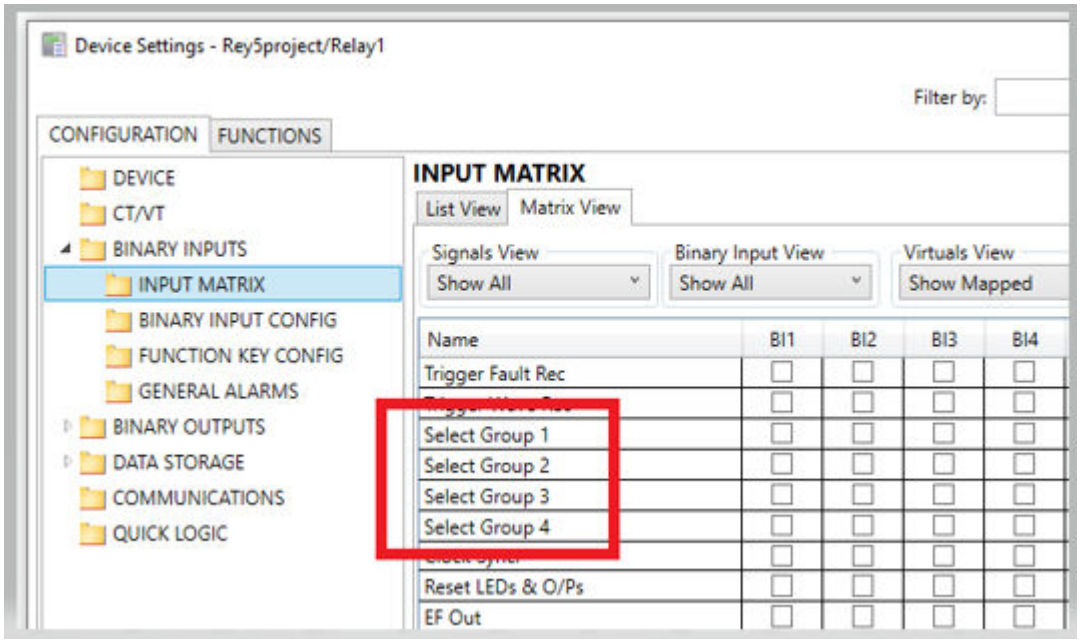
[sc_7SR5_SettingsGroupFascia, 1, --_--]

Figure 6-13 Settings Group via Front Fascia

6.5.10 Changing Setting Group via Binary Inputs

For settings group switching via binary inputs on your 7SR5 device, the user must have configured the binary input signals that are necessary for switching the settings group to the contacts of the device.

These can be found in Reydisp Manager 2 from **Configuration > User Settings > Configuration > Binary Inputs > Input Matrix**.



[sc_7SR5_SettingsGroupChange, 1, --_--]

Figure 6-14 Settings Group Change via Binary Inputs

6.5.11 Changing Setting Groups via Communication Protocols

The communication protocols IEC 60870-5-103, IEC 61850, DNP3 TCP, Modbus RTU, and Modbus TCP can be used for switching the settings groups via a communication connection. See relevant Communication and Device manuals for detailed information.

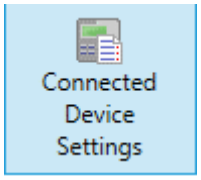
6.5.12 Updating a Parameter Setting on a Connected Device

A device parameter value can be changed on a connected device without an entire configuration update. This enables protection parameters to be changed quickly during testing and commissioning. On completion of any required changes the project parameter setting file can be resent to the devices to disreguard any changes, or the new parameter settings can be imported into the device in the project.

Selecting the **Connected Device Settings** icon in the tasks will allow connection to the device and extract the device protection parameters.

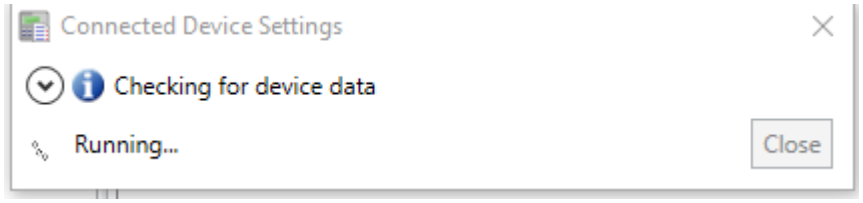
NOTE

The device must have previously been configured.



[sc_7SR5_ConnectedDeviceSettingsIcon, 1, --_--]

Figure 6-15 Connected Device Settings Icon



[sc_7SR5_ConnectedDeviceSettingsRunning, 1, --_--]

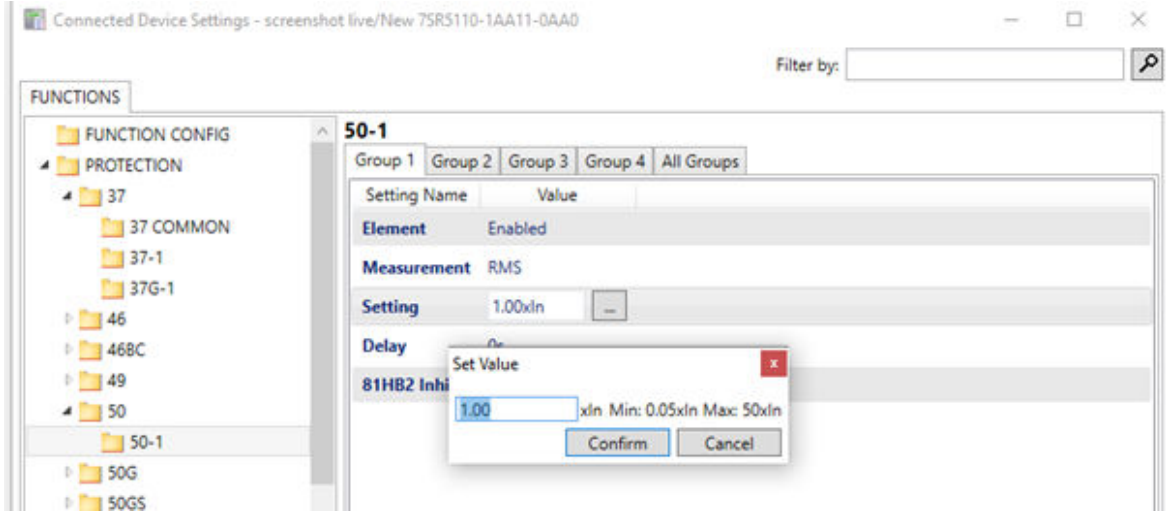
Figure 6-16 Connected Device Settings Running

The settings window will display the device settings as they are in the device.

[sc_7SR5_ConnectedDeviceSettingsWindow, 1, --_--]

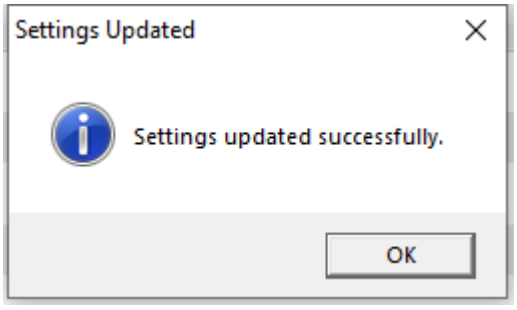
Figure 6-17 Connected Device Settings Window

Parameter settings can be changed as a single setting, or multiple settings can be changed and then the **Send to Device** option selected.



[sc_7SR5_ConnectedDeviceSettingsChanged, 1, --_--]

Figure 6-18 Connected Device Settings Changed



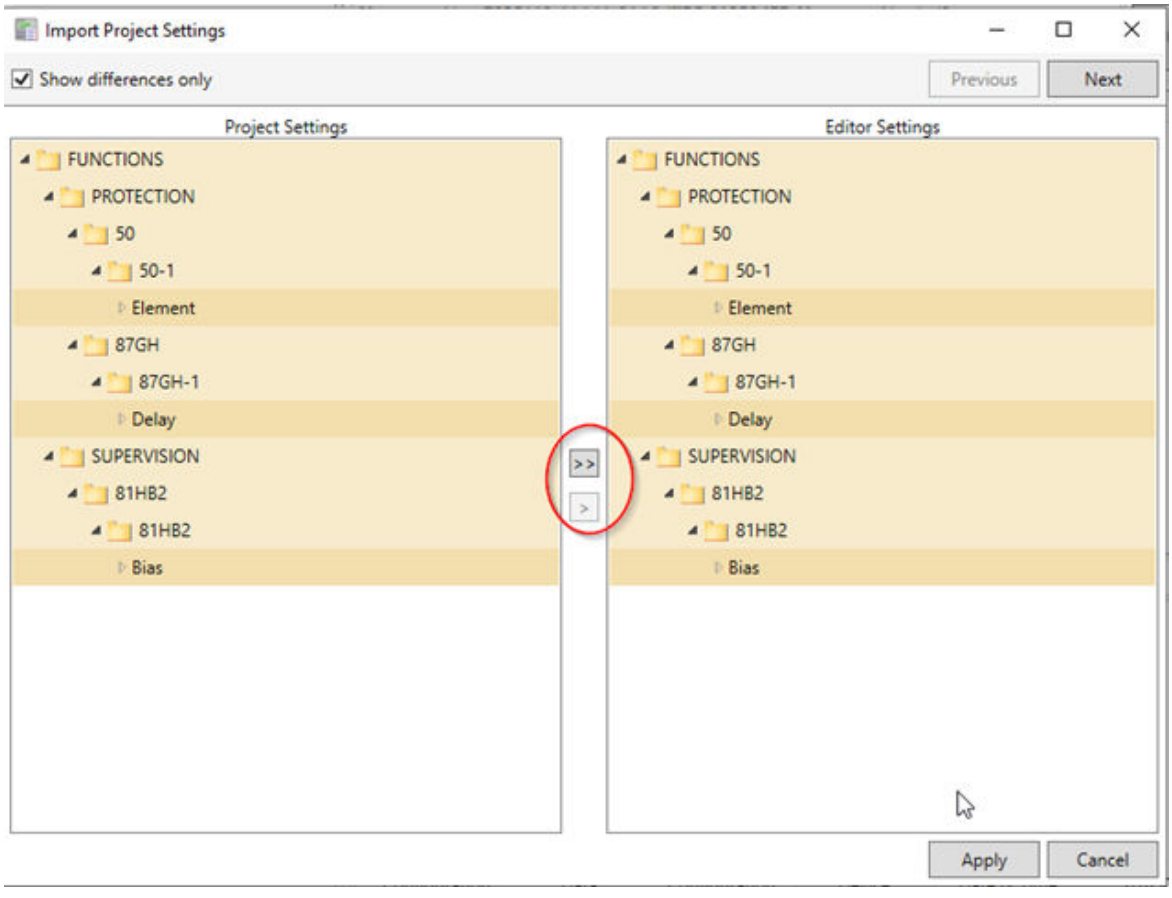
[sc_7SR5_ConnectedDeviceSettingsDialog, 1, --_--]

Figure 6-19 Connected Device Settings Changed Dialog

When the online session is complete the user has the option to close the window using the **X** in the top right hand corner, or import the device settings saved in the project device by selecting the **Import Project Settings**.

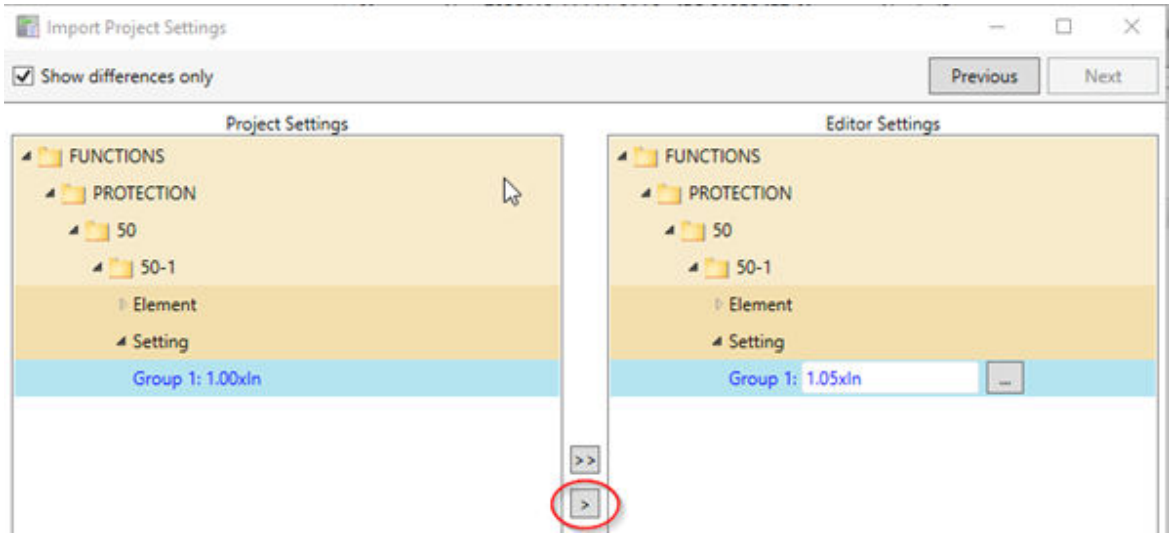
Importing the project settings allows the device to be returned to a known state after testing.

Any differences between the settings in the setting window and the device project setting will be highlighted. The option is available to transfer all of the project setting differences using the double arrow, see *Figure 6-20*, or selecting the individual setting and using the single arrow, see *Figure 6-21*.



[sc_7SR5_ImportProjectSettingsDoubleArrow, 1, --_--]

Figure 6-20 Import All Project Settings

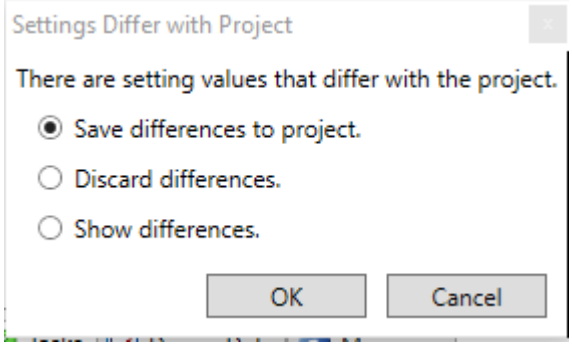


[sc_7SR5_ImportProjectSettingsSingleArrow, 1, --_--]

Figure 6-21 Import Selected Protect Settings

Selecting the **Apply** option will return to the connected device task to allow the revised settings to be sent to the device.

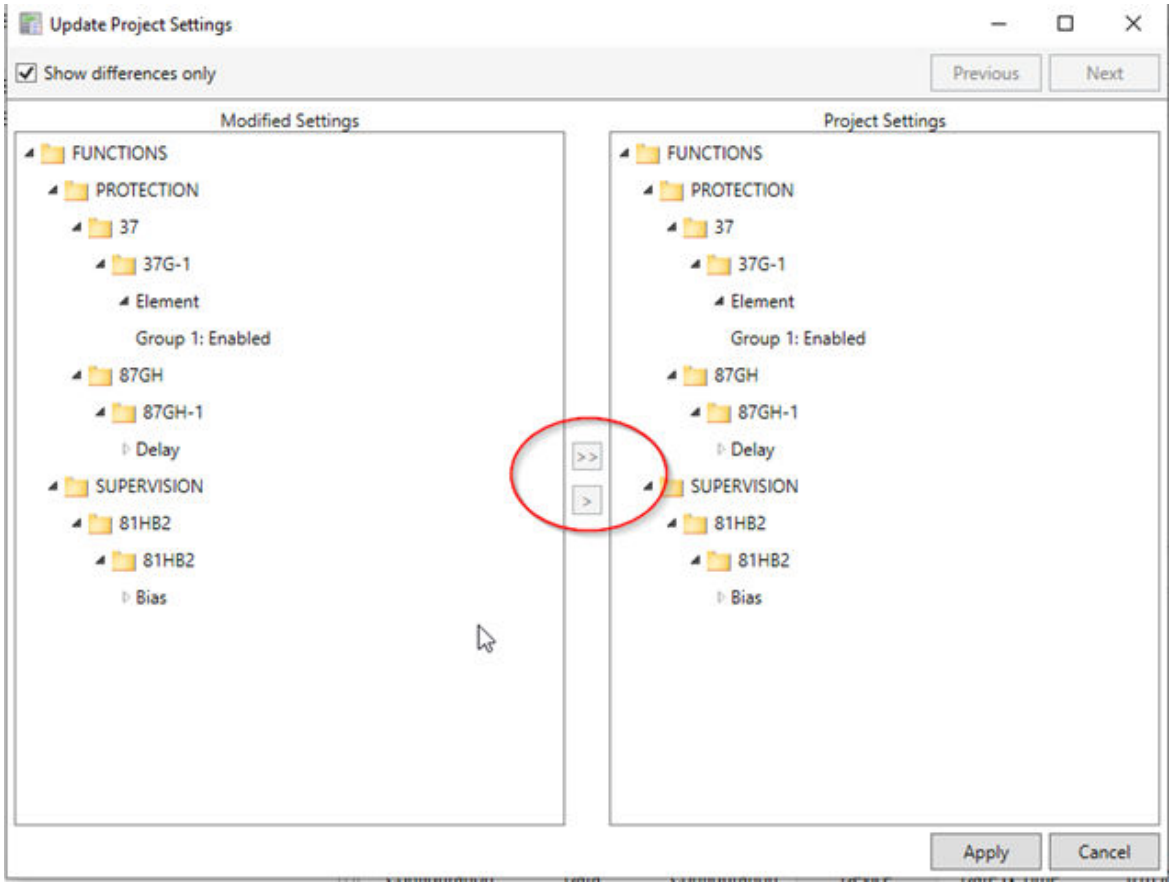
On closing the session a number of user options are provided as shown in *Figure 6-22*.



[sc_7SR5_ImportProjectSettingsUserOptions, 1, --_--]

Figure 6-22 User Options

Save differences to the project	The settings shown in the connected device settings are saved into the project without further confirmation.
Discard differences	Any setting changes in the editor window are lost if they are not sent to the device and stored in the project. We recommend any changes made to the device are also saved to the project.
Show differences	Any differences between the connected device settings editor and the device project settings are highlighted and the user can compare.



[sc_7SR5_ImportProjectSettingsUpdated, 1, --_--]

Figure 6-23 Updated Project Settings

7 In Service Operation

7.1 Overview

This chapter describes the handling of a 7SR5 device in the operating state. It contains the following information:

- Reading information from the device
- Functions of the device in the operating state
- Controlling your system via the device

More detailed information about the function of the device is not needed. The user must be familiar with the principles of operation according to chapter *5 Using Reydisp Manager 2* and chapter *4 Using the Device Fascia*.

Take note that the examples shown are general examples and in terms of wording and detail can vary on the given device depending on variant and configured functional scope. Please refer to the respective device manual for the process data that your device can process.

7.2 Safety Notes

Authorized Operational Staff

DANGER

Danger due to inadmissible or improper operator control actions

Noncompliance with the safety notes will result in death or severe injuries.

- ✧ Only personnel who are skilled electricians with precise knowledge of the system may operate devices during operation.
- ✧ Please carry out all operator control actions in the indicated sequence.

NOTE

Operator control actions are Confirmation ID protected. This ensures that only operational staff members with access rights can use the device during operation.

7.3 Operation Options

7.3.1 General

The device is operated via a Reydisp Manager 2 PC or directly using the fascia keys. You have the following operating options during operation:

- Readout of indications
- Readout, backup, and deletion of logs and records
- Resetting event counters
- Changing device settings such as date, time, and interface language
- Changing passwords/Confirmation ID
- Changing function parameters and switching of settings groups
- Controlling equipment

NOTE

Reydisp Manager 2 Communication

Operation using a Reydisp Manager 2 PC requires a functioning communication connection from the Reydisp Manager 2 PC to the device. For this purpose, you can use the USB interface on the fascia, the integrated or other Ethernet interfaces.

NOTE

Protection from Operating Errors and Unauthorized Access

Operator

- Changes to device settings and the deletion of process data can be prevented by enabling the setting confirmation IDs. After entering the setting ID, if no action takes place within certain times (60 minutes after the last key press, or if the Control ID is entered), an open confirmation query is automatically terminated. Every action carried out within these times restarts the time. After a confirmation query has ended you must confirm changes in device settings again by entering confirmation IDs.
- Before modified settings or the activation of control commands is accepted, there will be additional requests to enter the confirmation ID. You acknowledge these requests directly on the on-site operation panel by pressing the front fascia buttons. You confirm the interactive dialog in Reydisp Manager 2 by mouse click.

7.3.2 Online Operation Using Reydisp Manager 2

During online operation, you must establish a direct connection to the device to be operated. Use this method for:

- Commissioning
- Test and diagnostics
- Changing settings in the operating state

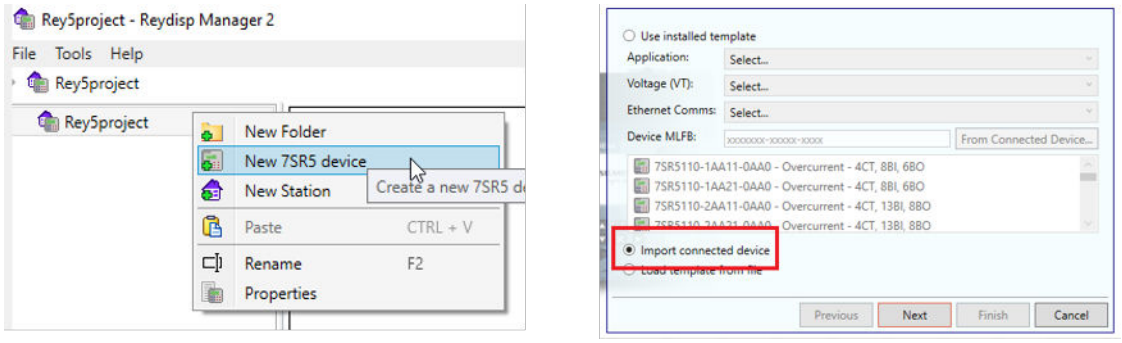
Online operation with Reydisp Manager 2 is beneficial in these operating modes. A device must be added to the project and the configuration transferred from the connected device. As soon as you have created the corresponding device in a project, however, only operate the device from there. Your settings are then saved on your PC and are available for offline configuration and parameterization tasks.

Procedure

✧ Establish a PC connection to a 7SR5 device via a communication interface.

✧ Create a device by right-clicking on the existing project name and selecting **New 7SR5 device**.

Select **Import connected device** to import a copy of the connected device.

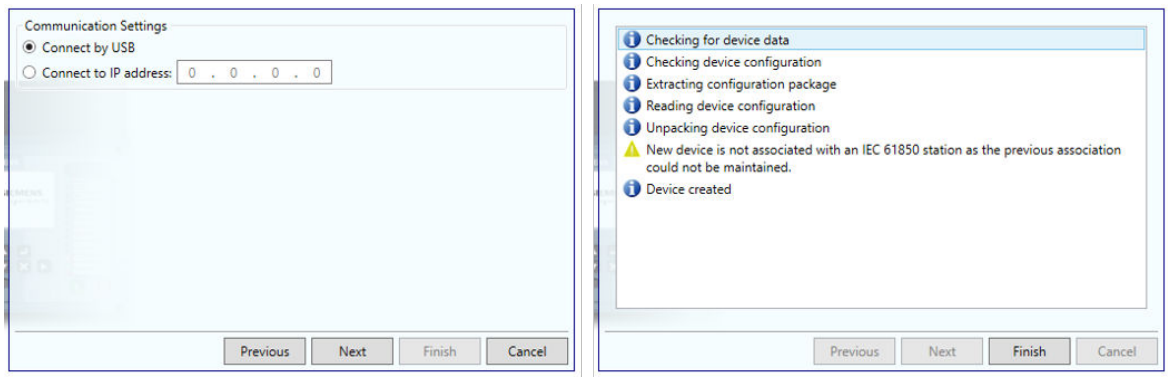


[sc_7SR5_AddingADevice, 1, --_--]

Figure 7-1 Adding a Connected Device in Reydisp Manager 2

✧ Select connection type USB or IP address from the rear port in the **Communication Settings** window and click the **Next** button.

Click the **Finish** button after device is created.

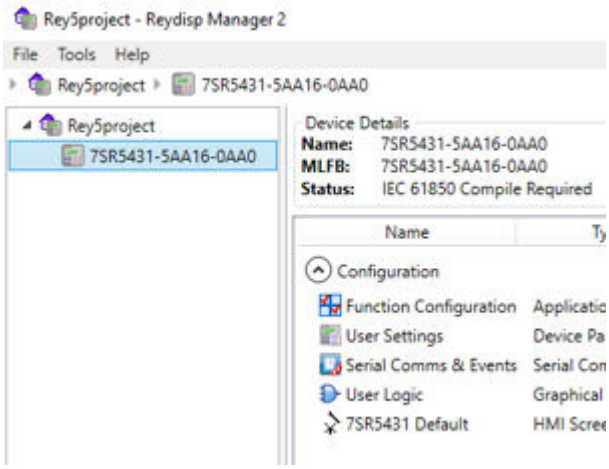


[sc_7SR5_CreatingADeviceWindow, 1, --_--]

Figure 7-2 Creating Device Windows

✧ Select the device from the project tree on the left.
The basic information is displayed below the device.

You can find the following tabs in the menu item **Device Information**:
Device information
User Settings
Function Configuration



[sc_7SR5_DeviceWindow, 1, --_--]

Figure 7-3 Device Window

7.3.3 Offline Operation Using Reydisp Manager 2

Offline operation offers you the ability to carry out complete configurations and extensive parameterization of a device. Once you have finished all settings, you can load the configuration from the Reydisp Manager 2 PC to the device. If the loading operation was successful, the device restarts automatically.

Typical Applications of Offline Configuration

- ✧ Creating a configuration by selecting a suitable application template and subsequently adjusting the settings to the individual conditions

NOTE

It is not recommended to update a device when in service/operation.

- ✧ Reusing a standardized configuration in multiple devices
- ✧ Extensive changes in configurations and setting parameters

NOTE

For a device to be editable offline, you must first have created it in a project. After successful loading of the configuration, the device restarts automatically.

Procedure

- ✧ From the project tree, select the project containing the device to be operated.
- ✧ Select the respective device within the project.
- ✧ Open the related menu on the right side of the working area, **Configuration and Tasks**.
- ✧ You can now carry out configurations and settings in offline mode.

7.3.4 Using the On-Site Operation Panel

You can operate the device directly on the on-site operation panel even without a Reydisp Manager 2 PC. A standard large LDC display, push buttons, and function keys are available to you for this purpose.

LEDs allow the display of binary output signals.

You will find detailed descriptions of components of the on-site operation panel and of navigation in the device menu tree in chapter *4 Using the Device Fascia*.

7.4 Indications

7.4.1 General

During operation, indications deliver information about operational states. These include:

- Measured data
- Power-system data
- Device supervisions
- Device functions
- Function procedures during testing and commissioning of the device

In addition, indications give an overview of important fault events after a failure in the system. All indications include the date, time, and it's state.

Indications are saved in logs inside the device and are available for later analyses. The following number of indications are saved at least in the respective buffer (depending on the scope of the indications):

- Event log 5000 indications
- Fault log 100 indications
- Waveform log 20 indications
- Data log average values of current, voltage, and power (where applicable)

If the maximum capacity of the user-defined log or of the operational log is exhausted, the oldest entries disappear before the newest entries. During a supply-voltage failure, recorded data are securely held by means of storage in the memory. You can read and analyze the log from the device with Reydisp Manager 2. The device display and navigation using keys allow you to read and analyze the logs on site.

Indications can be output spontaneously via the communication interfaces of the device and through external request via general interrogation.

Reading Indications

To read the indications of your 7SR5 device you can use the LCD display of the device or a PC on which you have installed Reydisp Manager 2. The subsequent section describes the general procedure.

7.4.2 Reading Indications on the LCD Display from the Front Fascia

The device fascia LCD displays an event log of filtered events with a time and date stamp.

Procedure

✧ Event logs for indication can be reached selecting the menu options **Main Menu > Event Log**.

The latest event is stamped with the number 1 and shows up to 5000 events by pressing ▼ button on the front fascia.

[sc_7SR5_EventLogDisplay, 1, --_--]

Figure 7-4 Event Log Display

7.4.3 Filtered Events from Front Fascia

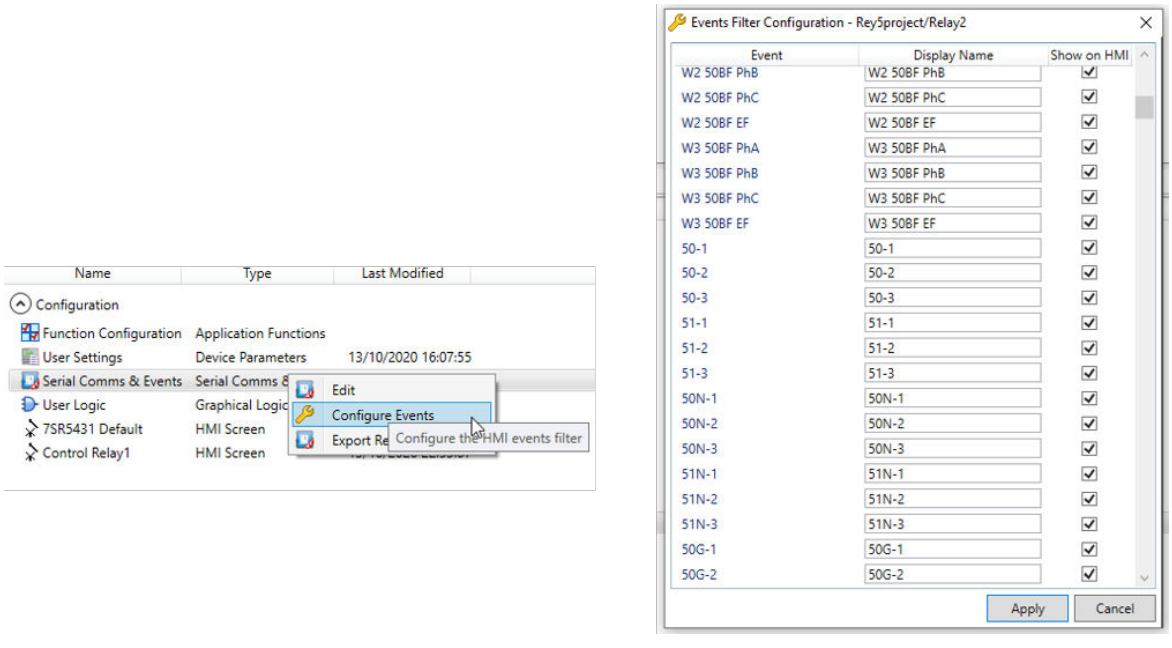
Filtered events are available from the relay fascia display.

The filtered events can be configured in Reydisp Manager 2. To access the user should right click on **Configuration > Serial Comms & Events** and select **Configure Events** to open the configuration events window.

Indications can then be selected. To show the desired events in the event log the user can click on the right side boxes (Show on HMI).

The event text displayed in the event log can be edited in the Display Name window of the event filter configuration.

After completing any filtering and editing required the file is saved as part of the device configuration and will be sent when the configuration is sent to the device. After sending the configuration to the device, selected events are shown in the front fascia HMI display event log list. This enables the user to determine associated events displayed from the front fascia events (for example only faults).



[sc_7SR5_EventsConfiguration, 1, --_--]

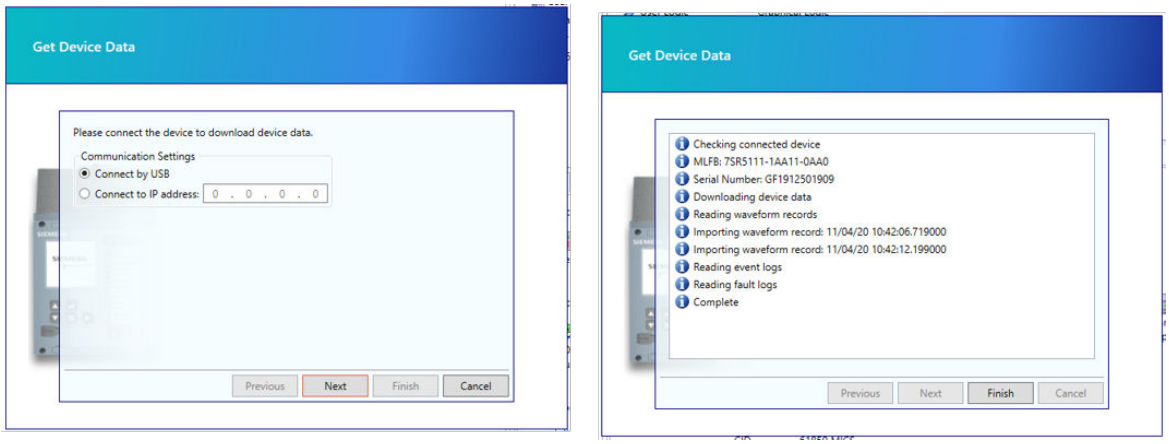
Figure 7-5 Configuration of Event Logs

7.4.4 Reading Indications from the PC with Reydisp Manager 2

To read the indications with Reydisp Manager 2 your PC must be connected via the USB user interface of the on-site operation panel or via an Ethernet interface of the device. You can establish a direct connection to your PC via the Ethernet interfaces. It is also possible to access all connected 7SR5 devices via a data network from your Reydisp Manager 2 PC.

After clicking **Get Device Data** on the Tasks screen or alternatively **Get** buttons on the right hand side, the device data can be retrieved from the device.

A connection window is provided to select between the default USB connection method or connecting via the rear Ethernet port using the IP address of the device. Select the connection type to the device and click the **Next** button to start getting device data read from the device.



[sc_7SR5_GetDeviceDataWindow, 1, --_--]

Figure 7-6 Get Device Data

Once complete, available data files will be stored under the **Device Data** tab that are read from the device. All entries are archived and can be used with further applications.

To open data content the user can select and double click on the available Event log from the Device Data window.

The Event Log Viewer window opens and any time tagging of any change of state (Event) in the relay can be seen. As an event occurs, the actual event condition is logged as a record along with a time and date stamp to a resolution of 1 millisecond.

When a starter picks-up (raised) and sometime later drops-off (cleared). In summary, a one stage event is Raised only, a two stage event may be Raised or Cleared.

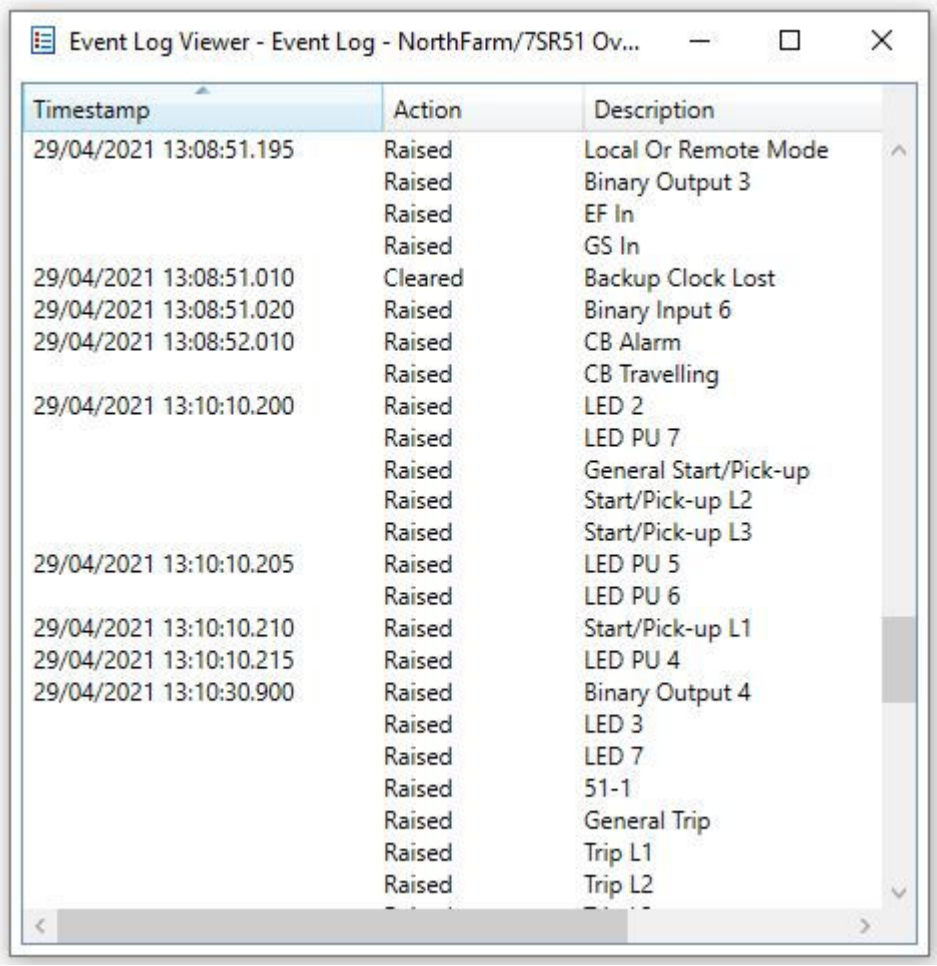


Figure 7-7 Event Logs

7.4.5 Reading Fault Data from the HMI Screen

Fault indications are events which arise during a fault. Fault indications are triggered from the **`Trip Config`** parameter setting which must be set to the trip contact. A fault is started by the incoming pickup of a protection function and ends after the trip command with the pickup cleared.

Fault data records can be viewed on the HMI LCD with the time and date of the trip. These include the LED status at the time of recording and the fault currents.

Available fault data is displayed in **Main Menu > Fault Data** in date and time format.

The number of faults stored is shown on the top of the LCD. If no faults have been stored the display will indicate **`No Faults to display`**.

Previous fault data records are stored with actual LEDs status.

The fault data is displayed in date/time order with the most recent first.

NOTE

`Trip Binary Output` must be configured as a trip contact from **Binary Outputs > Trip Config > Trip Contacts** to initiate a fault record and trip screen.

[sc_7SR5_DeviceFaultDataMenu, 1, --_--]

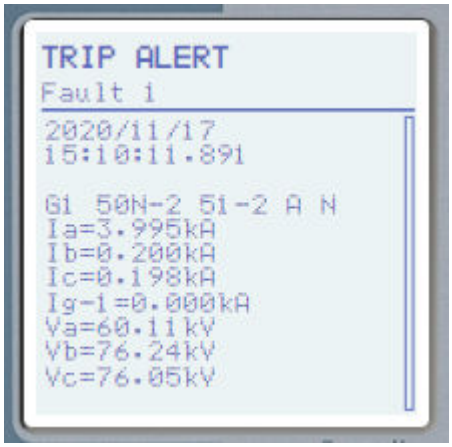
Figure 7-8 Fault Data

After a fault, the most important data of the last fault can be displayed automatically on the device display with operational fault measures (Trip Alert must be enabled from Device settings in the Configuration menu).

NOTE

LEDs will remain illuminated when viewing other screens if the fault screen has not been acknowledged.

These displays remain stored in the device until manual acknowledgment or release by LED reset.



[sc_7SR5_TripAlert, 1, --_--]

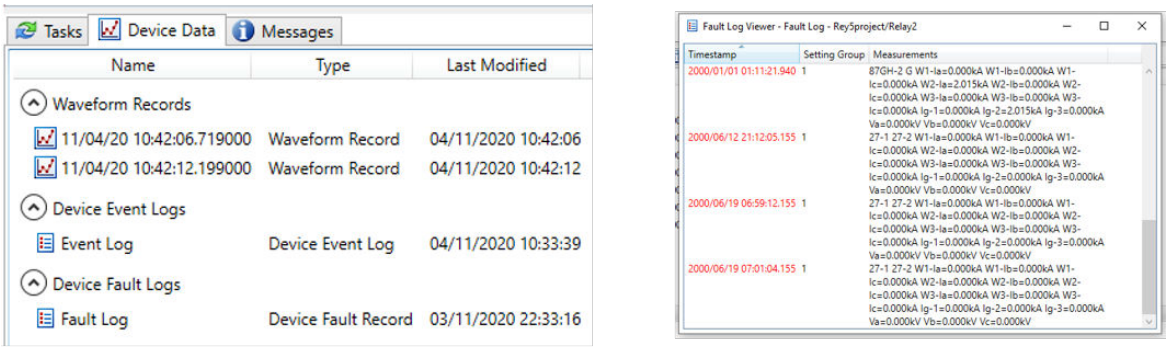
Figure 7-9 Trip Alert Display Screen

7.4.6 Reading Fault Data from the PC with Reydisp Manager 2

To read fault data from the PC, connect and get device data into the **Device Data** tab.

Select and double click on the available log from the **Device Data** tab.

Click **Fault Log** from **Device Fault Logs** or click **Waveform records** from the **Waveform Records** menu to open data content. The available logs display window will open as illustrated in *Figure 7-10*.



[sc_7SR5_FaultData, 1, --_--]

Figure 7-10 Fault Data

Initially for each type of device there are default views defined containing the Analogue Channels, Digital Channels and All Channels. Users can create new views or modify existing views, edit the analogue channel information, and format the display using the **View > Properties** command.

7.4.7 Reading Waveform Records from Webpage

The waveform records can also be retrieved from the device webpage via the front USB port or rear Ethernet port. This can be done by browsing to the homepage. The pages are accessed by browsing to https:// 192.168.2.1/home from the front USB port.

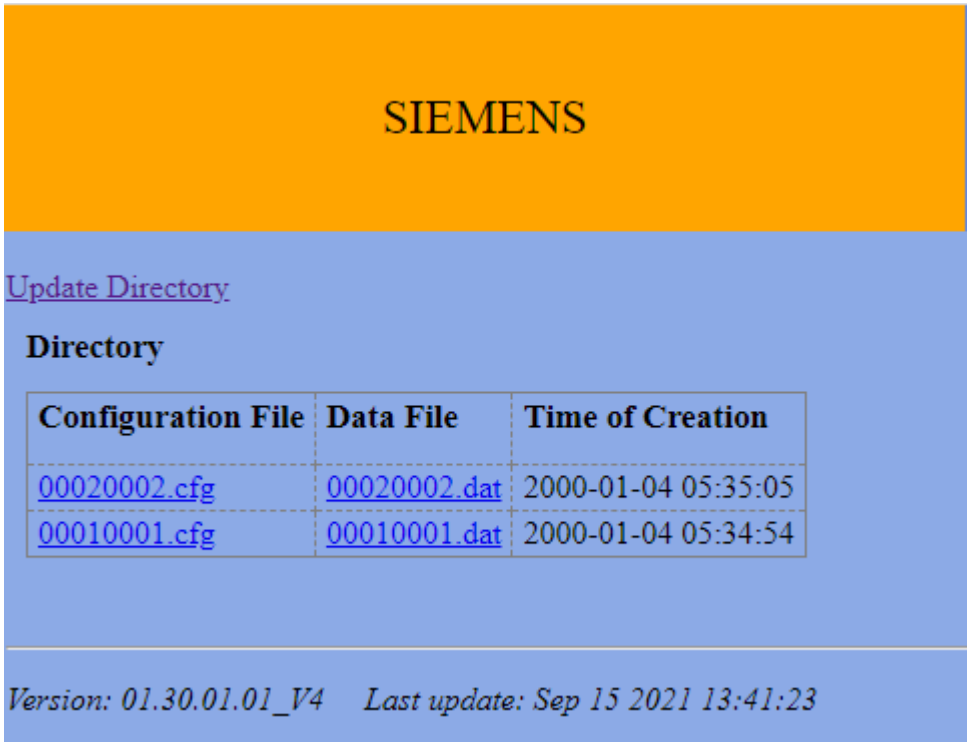
[sc_7SR5_EthernetEN100Homepage, 2, --_--]

Figure 7-11 EN100 Homepage

NOTE

This functionality is only available from > V1.30 communications firmware.

Select the **Fault recording** option from the left hand side menu.
To access the page, the maintenance password must be active and entered.



[sc_7SR5_EthernetEN100WaveformRecords, 1, --_--]

Figure 7-12 Waveform Records

The waveform records are listed with the latest first.
The files are stored in Comtrade format. The ***.CFG** file contains configuration data on what is in the ***.DAT file** including information such as signal names, start time of the samples, number of samples, min/max values, and more.

The files can now be downloaded and viewed in a suitable Comtrade viewer tool. Reydisp Evolution also supports the viewing of these files.

An update directory link allows the table to be refreshed.

7.4.8 Reading Waveform Records from Webpage

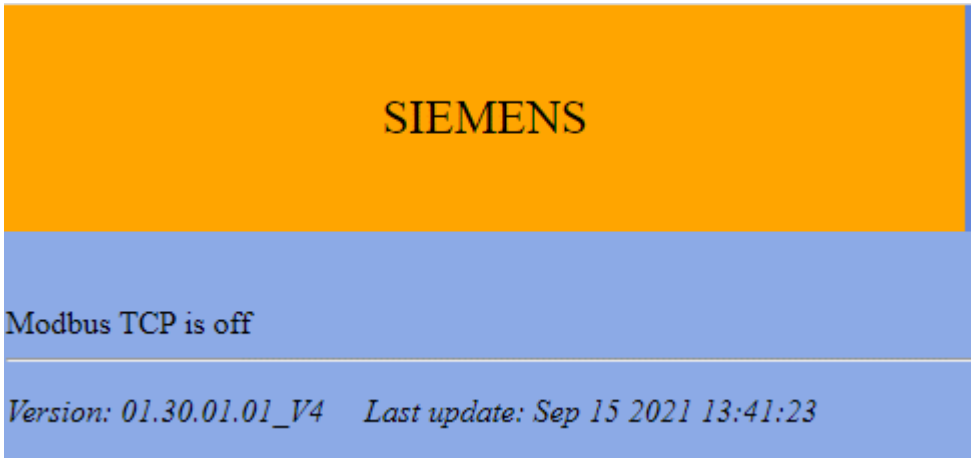
Both the Modbus TCP and DNP3 TCP are listed when available even though only one protocol can be active in the device.

The homepage also provides the configuration and statistics from the DNP3 TCP or Modbus TCP protocols when active in the device.

[sc_7SR5_EthernetEN100ModbusDnp3, 1, --_--]

Figure 7-13 Modbus TCP and DNP3 TCP Menu Options

When selected, if the protocol is disabled in the device, a screen will show the feature is **`off`**, as shown in *Figure 7-14*.



[sc_7SR5_EthernetEN100ModbusOff, 1, --_--]

Figure 7-14 Modbus Off

Clear statistics Update statistics

Statistics

	DNP Server 1	DNP Server 2
Connected	no	no
DNP Client IP address:Port	0.0.0.0:0	0.0.0.0:0
Received DNP messages	0	0
Sent DNP messages	0	0
Errors	0	0
Last error	none	none

Parameters

	DNP Server 1	DNP Server 2
DNP Server port	20000	20001
Master address	100	101

DNP settings		DNP unsolicited events		TCP communication	
Outstation address	1	Enable unsolicited events	no	DNP Client address 1	*.*.*.*
Validate Master address	no	Retry delay	5.0 s	DNP Client address 2	*.*.*.*
Application confirm timeout	5.0 s	Max. number of retries	3	DNP Client address 3	*.*.*.*
Select timeout	3.0 s	Class 1 events limit	5	DNP Client address 4	*.*.*.*
Enable DNP time synchronization	no	Class 2 events limit	5	DNP Client address 5	*.*.*.*
Preferred DNP time synch. master	at DNP Server 1	Class 3 events limit	5	Application keep-alive timeout	20.0 s
DNP time synchronization as UTC	yes	Class 1 events hold time	5.0 s		
		Class 2 events hold time	5.0 s		
		Class 3 events hold time	5.0 s		

Version: 01.30.01.01_V4 Last update: Sep 15 2021 13:41:23

[sc_7SR5_EthernetEN100DNP31, 1, --_--]

Clear statistics Update statistics

Statistics

	Modbus Server 1	Modbus Server 2
Connected	no	no
Modbus Client IP address:Port	0.0.0.0:0	0.0.0.0:0
Received Modbus messages	0	0
Sent Modbus messages	0	0
Errors	0	0

Parameters

Parameters	Settings
Slave Address	1
Master1 Tcp Port	502
Master2 Tcp Port	504
Accept Broadcast Message for Coil Status Register	Yes
Accept Broadcast Message for Hoilding Register	Yes
Modbus Time Synchronization	Disable
Acceptance of Clock Synch. Data	Current written
Control of Double Command	Multiple Coils
Exception Message Use 'Slave Device Busy'	No

[sc_7SR5_EthernetEN100Modbus1, 1, --_--]

7.5 Instruments and Meters

7.5.1 Overview of Measured and Metered Values

7SR5 devices have numerous measured and metered values. The measurands are recorded from the analogue inputs.

Further measurands are calculated from these measured values where the instrument or meter requires measurands from more than 1 input. For example, the electric power is calculated from the voltage and current measurands.

Instruments and meters can be viewed without entering a password or user ID.

The device functionality is dependent on the analogue input configuration (current and voltage inputs).

Please refer to the Device manual of the 7SR5 device for detailed information and setting instructions.

The user can read measured and metered values on the device display or with Reydisp Manager 2.

7.5.2 Reading Instrument Values from the Device Fascia, HMI screen

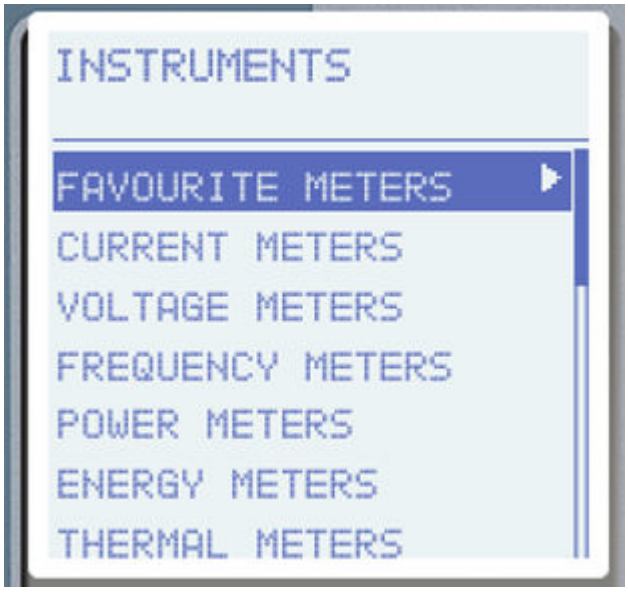
You can read measured and metered values on the device display.

For the display, the measured values of a device are summed up in the following groups:

- Operational measured values
- Fundamental and symmetrical components
- Function-specific measured values
- Minimum values, maximum values, average values
- Energy metered values

The device instrumentation and metering provides real-time measured quantities and data. This is displayed on the relay fascia LCD from **Main Menu > Instruments**.

The instruments are grouped to topic and can be viewed using the arrow buttons, Right arrow → to enter a group and Up ↑ and Down ↓ arrows to scroll through the instruments.



[sc_7SR5_DeviceInstrumentsMenu, 1, --_--]

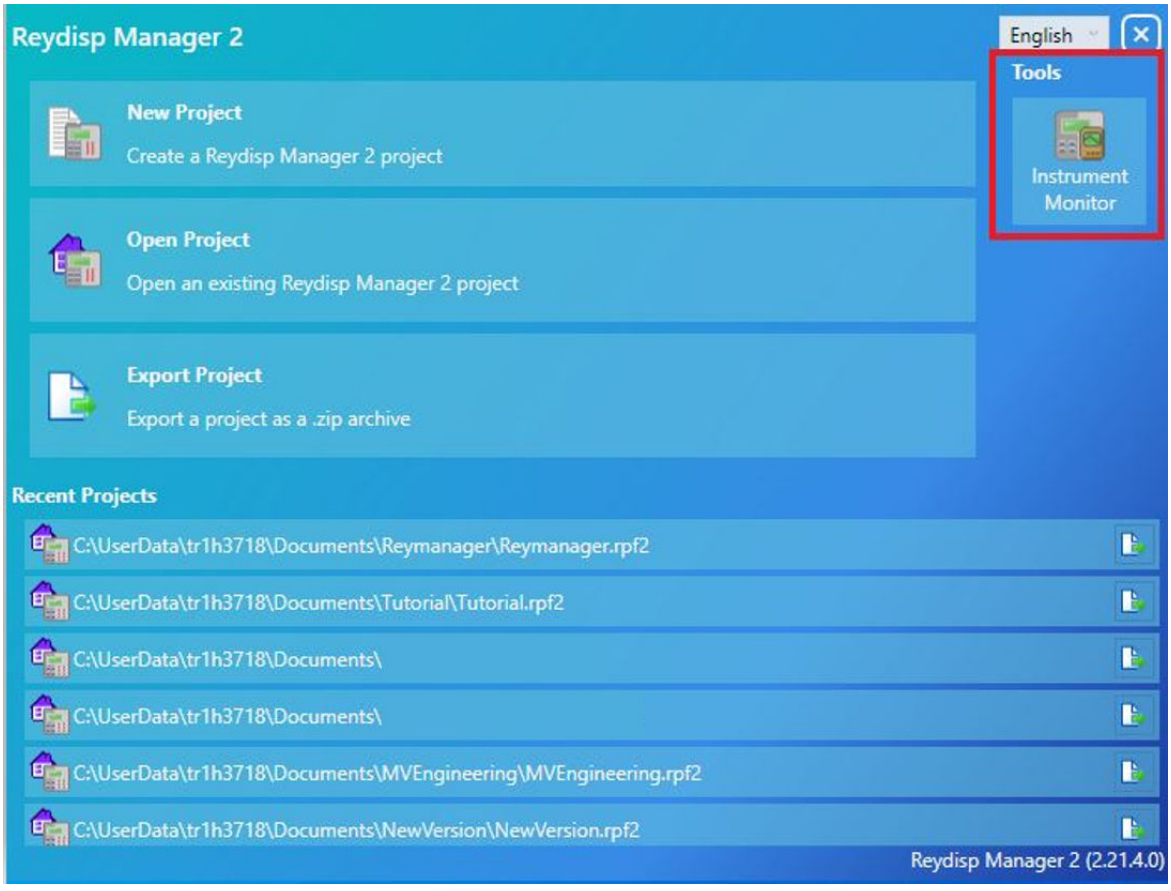
Figure 7-15 Instruments Menu

7.5.3 Reading Instrument Values from Reydisp Manager 2

The Relay Instrument Monitor tool displays a real time list of instruments from the device. Real time analogue values measurement requires the device to be connected to a PC from a USB or rear ethernet port to be data transferred to a PC online.

If there is a communication connection to systems control, measured values that the operational crew can verify are also transmitted here by rear ethernet communication.

The device is able to indicate the measurand values from Reydisp Manager 2 with connection by a COM-2 front USB port with the IP address 192.168.2.1, or user configured IP address from rear ethernet ports (Electrical or LC optical).

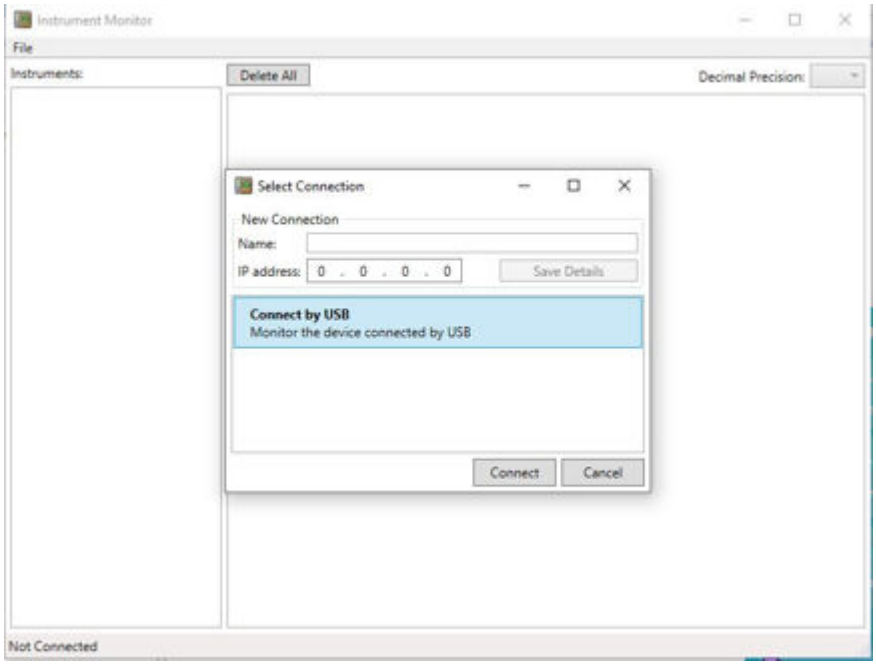


[sc_7SR5_InstrumentMonitor, 1, --_--]

Figure 7-16 Opening the Relay Monitor Tool

Click on the **Connect by USB** button to connect through a USB front port or type a user defined IP address to connect via a rear ethernet port.

Click the **Connect** button to open the Instruments window.



[sc_7SR5_ConnectionWindow, 1, --_--]

Figure 7-17 Connection Window

There is an instrument list on the left pane containing measurand and digital signal groups depending on the device type. The user can collapse and expand the groups by clicking an item.

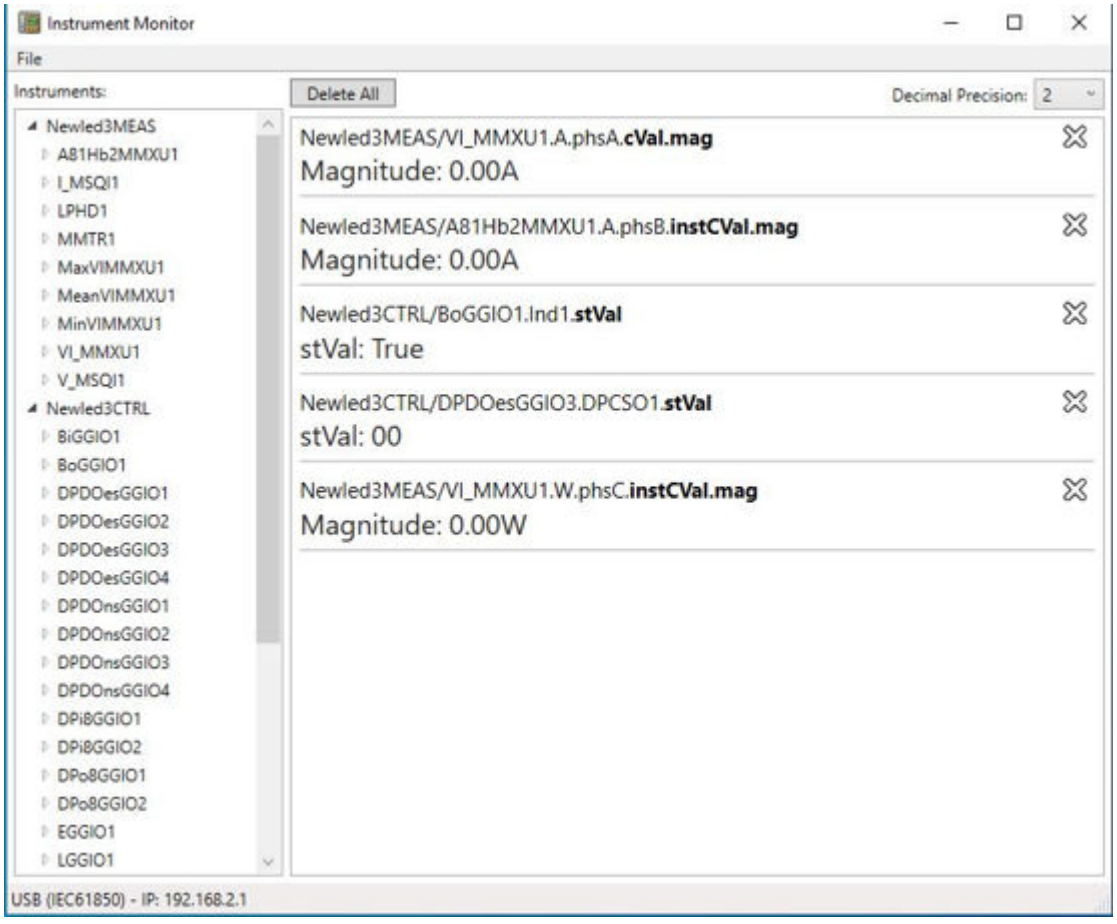
Available measurands can be selected by clicking on the left **instruments** tree and dragging this signal to the right side main window, then releasing the mouse button.

Newled3MEAS are analogue signals.

Newled3CTRL are digital signals.

Several signals can be dragged on to the main window on the right and provide continuous monitoring of the measurands. Alternatively, the measurands can be deleted and removed from the main window by clicking the X symbol on the right side.

Several measured-value windows are preadjustable by adding relevant measurands.



[sc_7SR5_RelayMonitorTool, 1, --_--]

Figure 7-18 Relay Monitor Tool

Table 7-1 IEDMEAS Analogue Measurements

Current Measurements	Ia	MEAS	VI_MMXU1	A.phsA
	Ib	MEAS	VI_MMXU1	A.phsB
	Ic	MEAS	VI_MMXU1	A.phsC
	In	MEAS	VI_MMXU1	A.neut
	Ig/Isef	MEAS	VI_MMXU1	A.res
Current Sequence Components Measurements	Current	MEAS	I_MSQI1	SeqA.C1
	Current	MEAS	I_MSQI1	SeqA.C2
	Current	MEAS	I_MSQI1	SeqA.C3
Voltage Measurements	Vab	MEAS	VI_MMXU1	PPV.phsAB
	Vbc	MEAS	VI_MMXU1	PPV.phsBC
	Vca	MEAS	VI_MMXU1	PPV.phsCA
	Va	MEAS	VI_MMXU1	PhV.phsA
	Vb	MEAS	VI_MMXU1	PhV.phsB
	Vc	MEAS	VI_MMXU1	PhV.phsC
	Vn	MEAS	VI_MMXU1	PhV.neut
	Vx	MEAS	VI_MMXU1	PhV.res
Voltage Sequence Components Measurements	Voltage	MEAS	V_MSQI1	SeqV

Frequency Measurement	Frequency	MEAS	VI_MMXU1	Hz
Power Measurements	W phs A (P)	MEAS	VI_MMXU1	W
	W phs B (P)	MEAS	VI_MMXU1	W
	W phs C (P)	MEAS	VI_MMXU1	W
	Total W (P)	MEAS	VI_MMXU1	TotW
	VAr phs A (Q)	MEAS	VI_MMXU1	Var.phsA
	VAr phs B (Q)	MEAS	VI_MMXU1	Var.phsB
	VAr phs C (Q)	MEAS	VI_MMXU1	Var.phsC
	Total VAr (Q)	MEAS	VI_MMXU1	TotVAr
	VA phs A (S)	MEAS	VI_MMXU1	VA.phsA
	VA phs B (S)	MEAS	VI_MMXU1	VA.phsB
	VA phs C (S)	MEAS	VI_MMXU1	VA.phsC
	Total VA (S)	MEAS	VI_MMXU1	TotVA
	Power Factor phs A	MEAS	VI_MMXU1	PF.phsA
	Power Factor phs B	MEAS	VI_MMXU1	PF.phsB
	Power Factor phs C	MEAS	VI_MMXU1	PF.phsC
	Total Power Factor	MEAS	VI_MMXU1	TotPF

Digital signal groups in IEDCTRL:

- Binary inputs status BiGGIO
- Binary outputs status BoGGIO
- LED status LGGIO
- Virtual inputs/outputs status VGGIO

Status of signals:

- ON/TRUE: 1
- OFF/FALSE: 0

8 Device Maintenance

8.1 Execute Checks

General Information

The device does not require scheduled preventative maintenance although some users apply periodic checking schedules to all protection devices. Operational checking can be limited to periodic visual checks of measured analogue values at the device instruments or the data provided over the communications channels to supplement the continuous self-checking features of the device.

The device incorporates a number of self-monitoring features. Since the device is mainly self-monitoring, hardware and software errors are automatically forwarded. This action minimizes any downtime of the device. It also eliminates the need for frequent maintenance inspections.

Protection-Function Test

NOTE

When performing a protection-function test, make sure that it does not lead to any undesired tripping. Likewise no information must be transmitted to a higher-level systems control where the operator may incorrectly interpret it.

Trip links should be removed and the device out into **`Out of Service`** mode where possible.

- Make sure that the **`Device Healthy`** signal is routed and **`Healthy LED`** (green) on the front fascia lights up. This is how the device indicates that it is properly functioning and that no failures have been observed during self-monitoring.
- Check the **`Device Healthy`** signal is assigned to the LED from the Output Matrix by **Settings > Configuration > Binary Outputs > Output Matrix** menu. By default the Device Healthy indication is pre-routed to LED 1 and Binary Output 3.

[sc_7SR5_DeviceHealthy, 1, --_--]

Figure 8-1 Device Healthy Signal

- Make sure that the LEDs on the front cover present a plausible image of the actual state of the device. If, for example, the tripping of a protection function is saved as an LED display, the device has fault indications and a fault record for this purpose.
- Pressing the ► key for ≥ 3 seconds when the home screen is displayed is for an LED test. All LEDs light up. Stored LED displays are reset and only those states currently indicated by the device are shown.
- Read the operational measured values and compare them to the actual measurands to control the analogue inputs. To do this, enter a reference quantity into the device using secondary test equipment. This is how you check the proper operation of the analogue section of devices.

- Read the operational indications. You can do this directly on the device or following a clearly arranged procedure using Reydisp Manager 2. Make sure that they do not contain inputs about failures of the device, of measurands or other implausible information.
- If the protection equipment has picked up or disabled an error, you can verify this through the fault record and the fault log. This is how the protection equipment demonstrates its correct operation in the operating state. Additional protection-function tests can be omitted.

NOTE

The system operator is responsible for further protection-function tests within maintenance intervals. Check protection functions using secondary test equipment (see the Device manual).

Check the device information page for firmware information.

Check the Comms firmware is up to date with the latest Security Management and vulnerability updates. Refer to the Siemens Cyber Security management for further information.

8.2 Error Search and Correction

8.2.1 Troubleshooting

Procedure

If the device did not indicate Device Healthy after its self-checking procedure, then Siemens recommends that you proceed as follows:

- Check whether the auxiliary voltage on the corresponding connections has an adequate amount and correct polarity. You will find information about this in *6.2 Initial Startup*.
- If the device does not show Device Healthy and healthy LED, look for the cause of the fault in the operational log. You can do this directly on the device or with Reydisp Manager 2.
- If the **`Device Not Configured`** message display appears in the device display, then send configuration via Reydisp Manager 2 or change a parameter in device settings via the front fascia keys.
- If the confirmation ID is queried, enter it for the device initialization.

After successful initialization, the LEDs again indicate normal operation and the default display goes back into the display. If the device-specific setting values were saved in the PC during commissioning, they are again loaded into the device. The device is ready for operation.

Additional Support

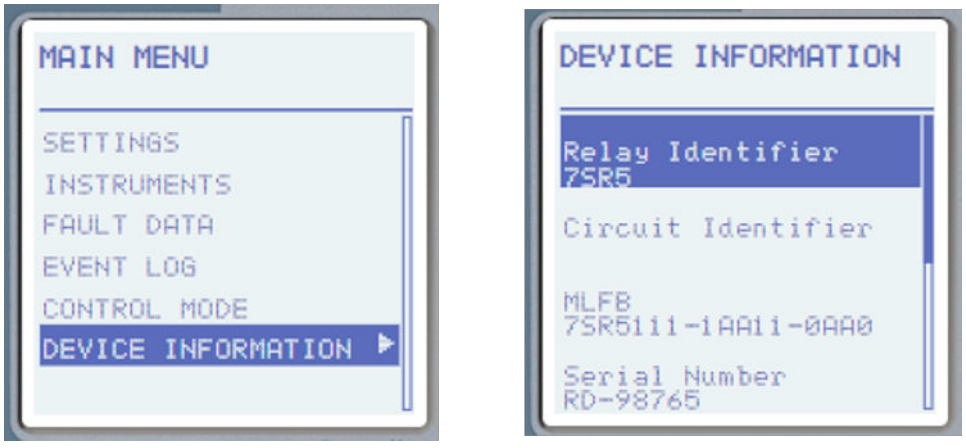
If these measures do not lead to the desired result, the Support team will help you.

When contacting a member of the support team it is advised to:

- Keep the device serial number to hand
- Read out the version of the installed firmware
- Read the event log of the 7SR5 device with the Reydisp Manager 2 tool

Read the Device Data via the Front Fascia LCD Display

With a device ready for operation, select **Main Menu > Device Information**.



[sc_7SR5_DeviceInformation, 1, --_--]

Figure 8-2 Reading Device Information

Read the Device Data with Reydisp Manager 2

Select the device in the project tree.

Double-click **Properties** in the Task tab and the Properties window will open.

The General tab displays information about the device name, hierarchy, the device model (Reyrolle devices MLFB) and serial number, and the configuration firmware version amongst other things.

The **Author** and **Comment** text boxes can have their contents changed. This text is displayed in the Author and Comment columns of the Item Pane.
Device name also can be changed by the user and the device will be renamed on the project tree.

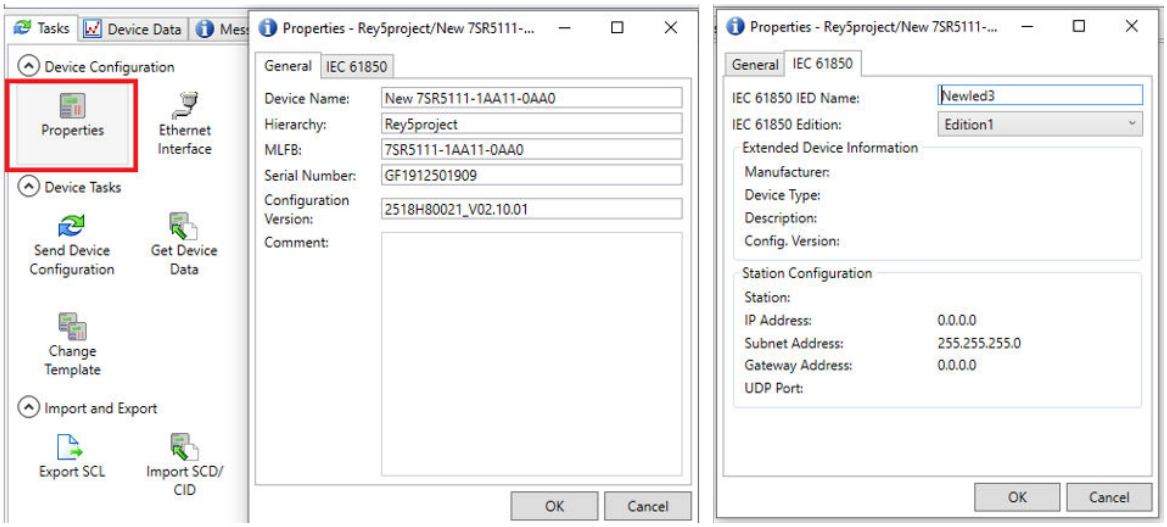


Figure 8-3 Properties Window

Each IEC 61850 device has an IED name which can be defined by the user in the IEC 61850 window.
The IEC 61850 IED name is subject to the following restrictions:

- It may be a maximum of 13 characters
- It may only contain the characters A-Z, a-z, 0-9, and _
- It must start with a letter, not a digit or underscore
- If the device is assigned to a station, an additional rule is imposed: The IED name and Edition version cannot be the same as another IED name assigned to that station.

Select from the drop down options the IEC 61850 Edition to be used on the device.

Troubleshooting

The device does not power up	Check that the correct auxiliary power supply voltage is applied and that the polarity is correct.
The Device Healthy LED does not light up	This is a general device failure. Contact a local Siemens office or representative.
The backlight is on but no text can be seen or is not readable	Adjust the relay display contrast. See *4.3 Displays for Indication and Control*.
The PC is unable to communicate with the device	Check that all of the communications settings match those used by Reydisp Manager 2. Check that the Tx and Rx fibre-optic cables are connected correctly. (Tx –> Rx and Rx –> Tx). Check that all cables, modems and fibre-optic cables work correctly. Ensure that IEC 60870-5-103 is specified for the connected port (COM1, COM2, COM3, or COM4).
The status inputs do not work	Check that the correct DC voltage is applied and that the polarity is correct. Check that the status input settings such as the pick-up and drop-off timers and the status inversion function are correctly set.

The device won't accept the confirmation ID	Check to make sure the confirmation ID being entered is correct and try again.
The **Device Not Configured** message is displayed on the LCD	Change any parameter in the device configuration or load a user configuration via Reydisp Manager 2.

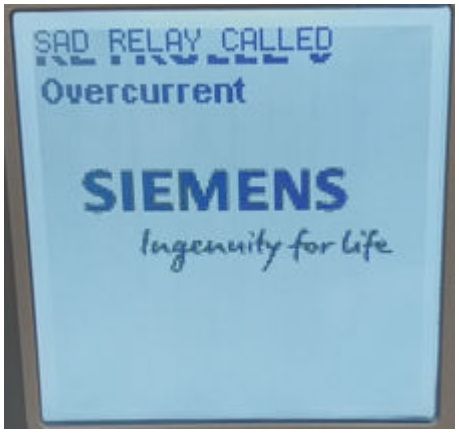
8.2.2 Error Indications

If the 7SR5 device is outside normal operating mode, this is shown by a Device Healthy indication. By default this indication is prerouted to LED 1 and Binary Output 3.

Relay failure will be indicated by the Protection Healthy LED being off.

When a device error occurs, an error message on the LCD display will read **SAD RELAY CALLED** and this means, the device is not ready for operation.

The relay will enter a locked-out mode. While in this mode it will disable operation of all LED's and Binary Outputs.

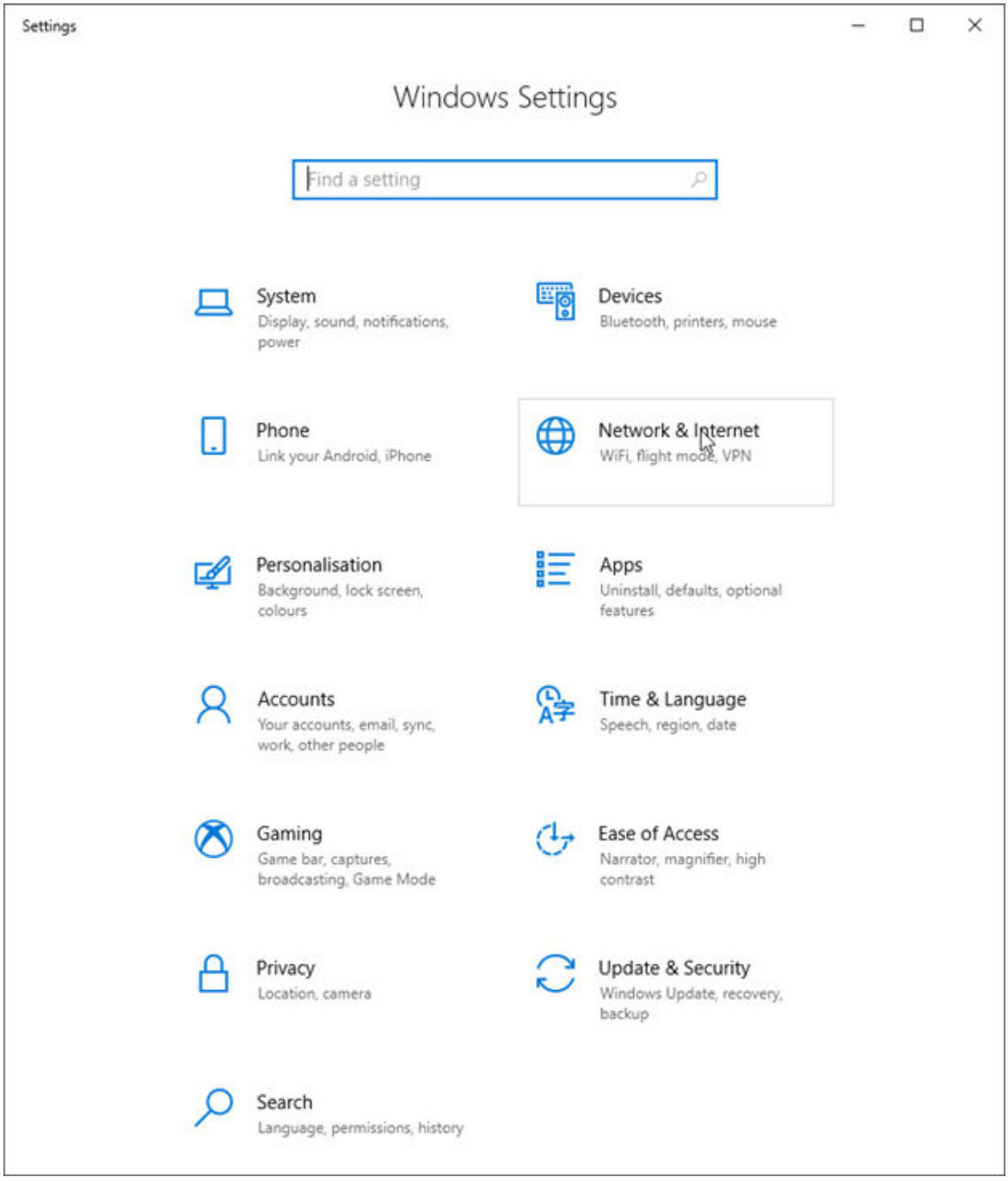


[sc_7SR5_SadRelayCalled, 1, --_--]

Figure 8-4 Sad Relay Called Display

8.2.3 Manually Changing IP Address of Reyrolle Adapter

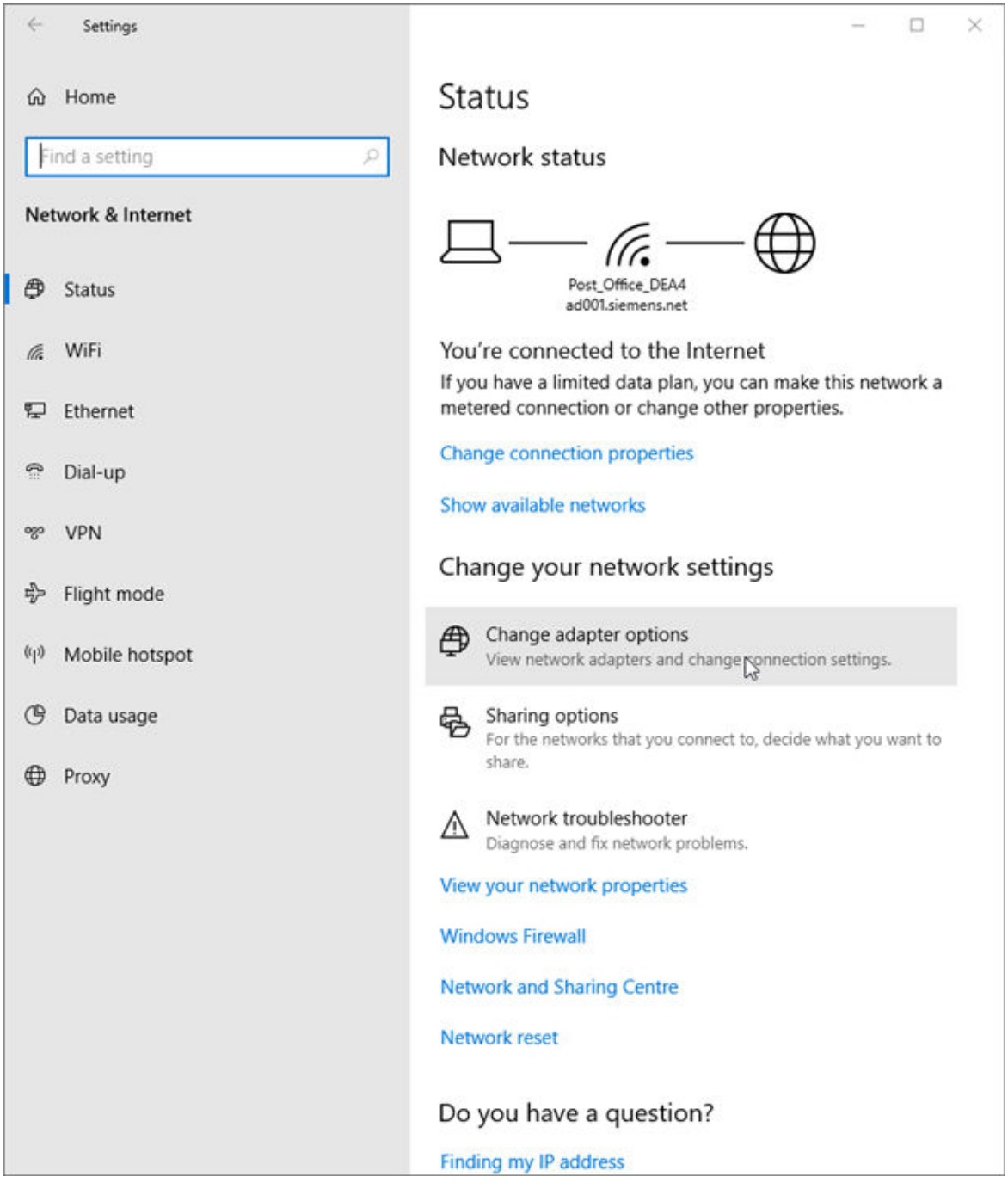
In order to manually change the IP address of the Reyrolle Adapter the user should start by opening the Windows Settings window (shortcut Windows Key + I).



[sc_7SR5_WindowsSettings, 1, --_--]

Figure 8-5 Windows Settings Window

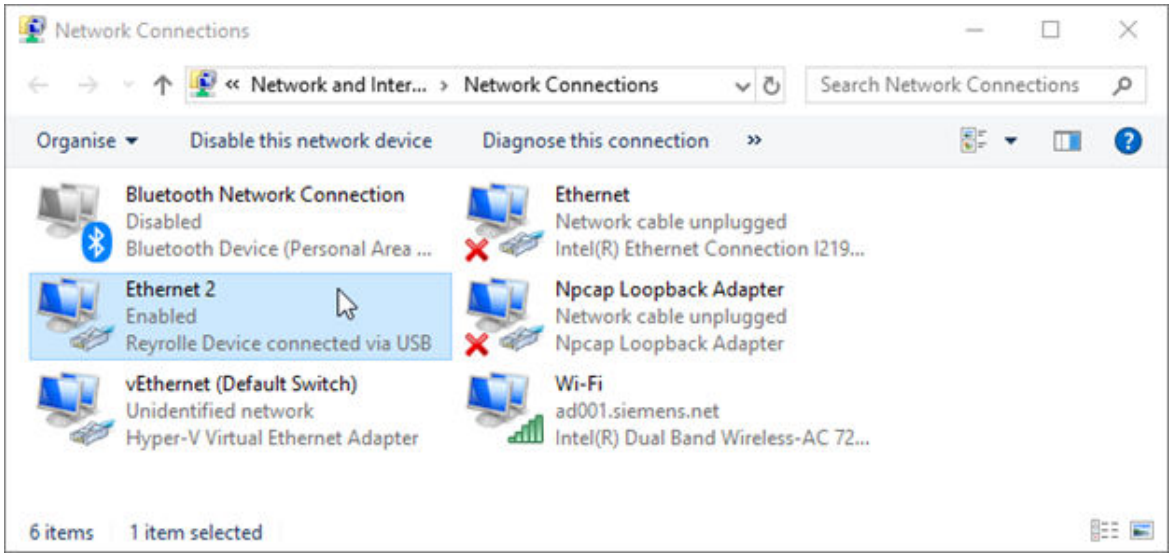
The user can then select **Network & Internet** to move to the next page.
Change adapter options should then be selected on the next screen as shown in *Figure 8-6*.



[sc_7SR5_ChangeAdapterOptions, 1, --_--]

Figure 8-6 Change Adapter Options

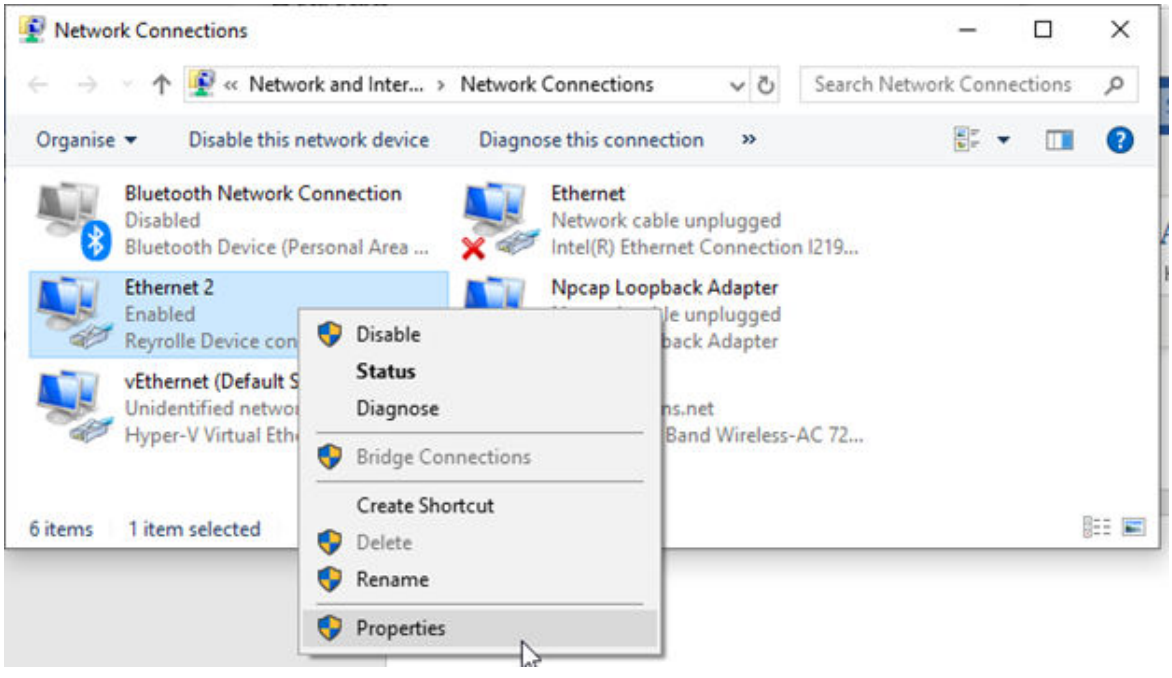
The new page should show an option **`Reyrolle Device connected via USB`** as shown in *Figure 8-7*.



[sc_7SR5_ReyrolleDeviceConnectedViaUSB, 1, --_--]

Figure 8-7 Reyrolle Device Connected Via USB

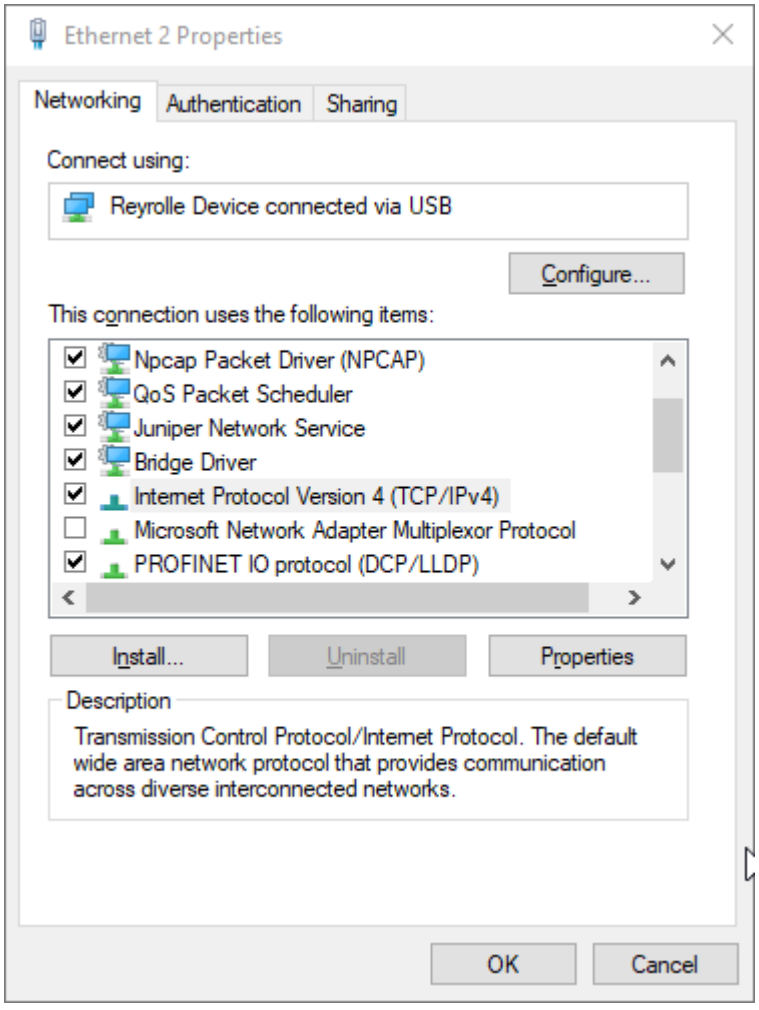
The user can right click on this option and choose **Properties** from the drop down list.



[sc_7SR5_ReyrolleDeviceConnectedViaUSBProperties, 1, --_--]

Figure 8-8 Reyrolle Device Connected Via USB Properties

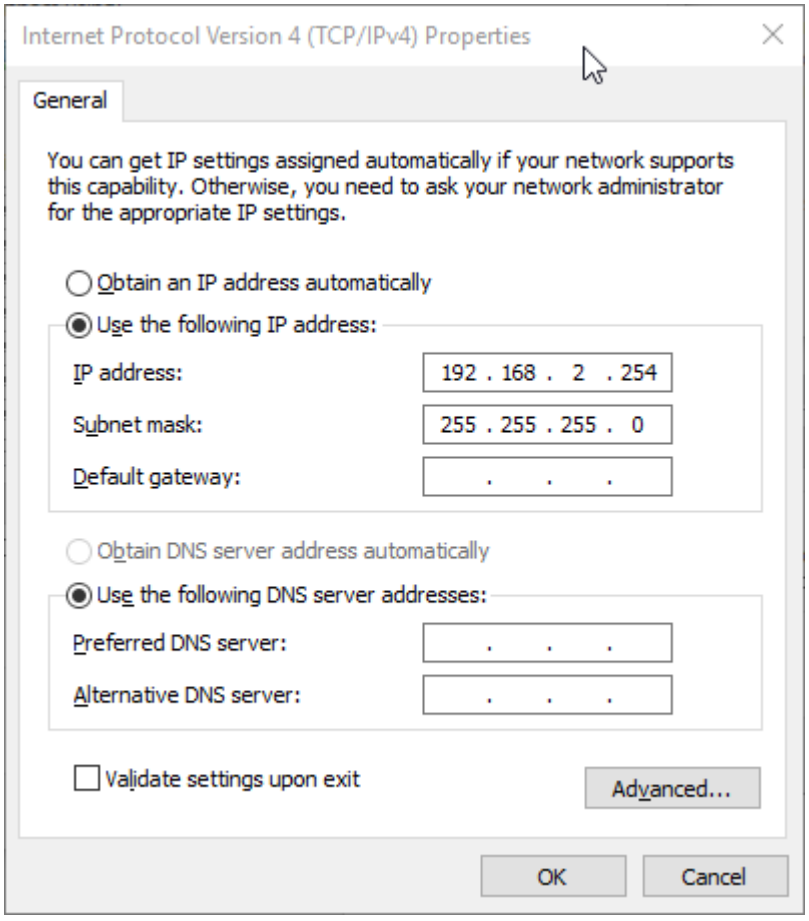
If a User Account Control Change confirmation box is displayed, click **Accept**.
The user can then find **`Internet Protocol Version 4`** in the list, select it and click **Properties**.



[sc_7SR5_Ethernet2Properties, 1, --_--]

Figure 8-9 Reyrolle Device Properties

The default address should be 192.168.2.254. In the event of an address conflict, change the last number, for example, to 253. If there is still a conflict, keep reducing the last number until it is resolved.

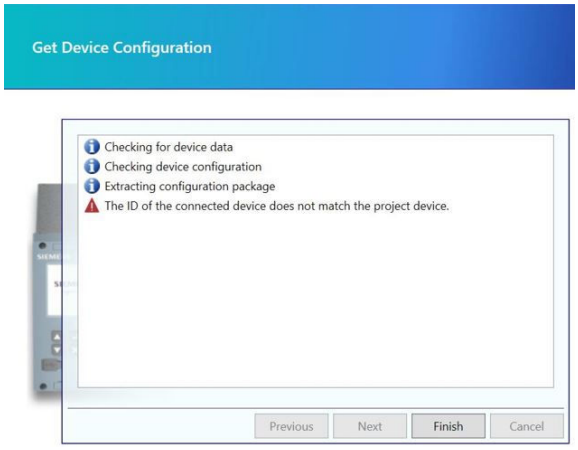
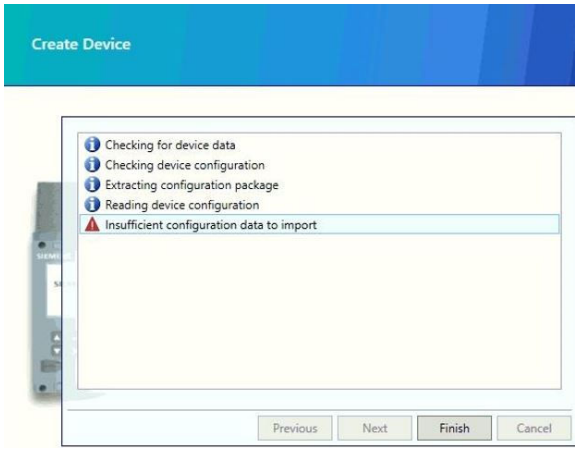


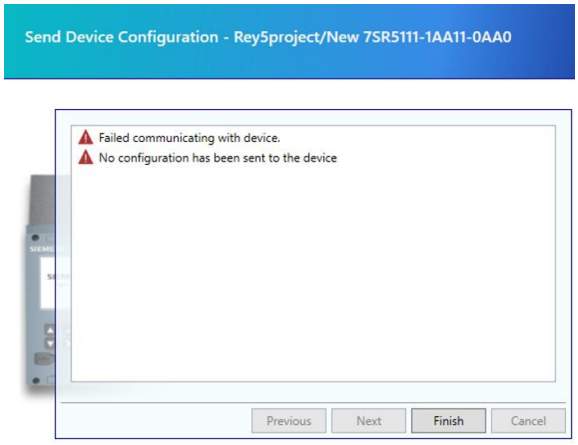
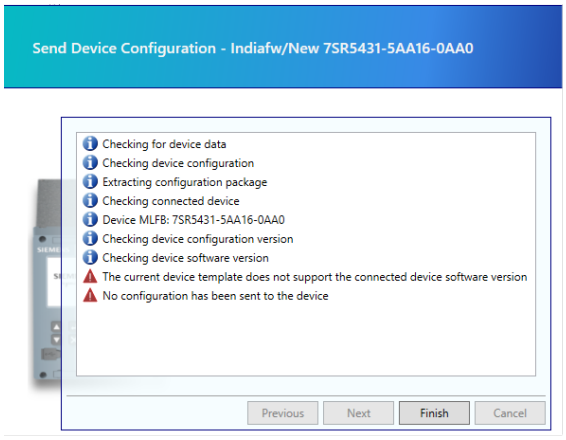
[sc_7SR5_ReyrolleDeviceIPAddress, 1, --]

Figure 8-10 Reyrolle Device IP Address

8.2.4 Error Indications in Reydisp Manager 2

Table 8-1 Error Indications in Reydisp Manager 2

Error Message	Description
 Figure 8-11 Device Code Error	The connected device and template in the project tree have a different MLFB. Check the MLFB codes on both the device front fascia and the device in the project tree in Reydisp Manager 2.
 Figure 8-12 Device Configuration Error	The device configuration file contains some errors (logic, protection setting, transformer data, etc). Check the settings and parameters.

Error Message	Description
 Figure 8-13 Device Connection Error	The device is not detected by Reydisp Manager 2. Check the device is energized with the auxiliary power supply and operational. Check wiring for the communication port.
 Figure 8-14 Device Software Error	The device firmware version does not match the selected template firmware version on Reydisp Manager 2. A Firmware upgrade should be done to the device with the correct version.

8.3 Replace and Return Defective Device

8.3.1 Error Backup Module

If you cannot correct a defect reported by the device, you can replace this device with a backup device.

The backup device is configured with available project data from Reydisp Manager 2. Once the device has failed in this manner, it is non-recoverable at site and must be returned to the manufacturer for repair.

The relay should be returned as a complete unit. No attempt should be made to disassemble the unit to isolate and return only the damaged sub-assembly. It may however be convenient to fit the withdrawable relay to the outer case from a spare relay, to avoid the disturbance of relay panel wiring, for return to local Siemens office. The withdrawable relay should never be transported without the protection of the outer case.

8.3.2 Replacing a Device

The following shows the steps that should be taken to replace a device:

- Take the device out of operation
- Remove the wired terminal blocks from the module to be exchanged or alternatively all lines from the device
- Remove the device and fitting parts
- If needed, assemble the replacement base module with the expansion modules
- Put the device back into operation (see *7 In Service Operation*).

8.3.3 Returning a Device

The following steps should be taken when returning a device:

- Ensure that the devices are either shipped with the original case – if the case is to remain in the system – or with the designated transport safety devices
- Protect the optical interfaces on the communication or arc-protection modules against the ingress of dust. Use, for example, the protective caps provided in the delivery condition.
- Pack the defective device (base module and expansion module) or the complete device (see *1.1 Unpacking, Repacking, Returning, and Storing*)
- Return the defective device to your Siemens local office or sales partner

8.4 Update Firmware and Configuration

8.4.1 General

Hardware and certain functional characteristics are selected with the latest released firmware for the chosen model.
Reydisp Manager 2 can be used for updating both the configuration and the firmware. No additional tool is necessary for updating the firmware of the device or the firmware of the communication module.

8.4.2 Downloading from the Siemens Website

Download the device drivers or protocol drivers necessary for updating the 7SR5 device from the Siemens download area *http://www.siemens.com/reyrolle*.
Click the Reyrolle5 icon and then select the device type 7SR51, 7SR54, or 7SR57 by clicking **Learn more**.
Click **Downloads** on the menu bar.
Click the link for **Manuals, Certificates, Software, Device Drivers, CAx (SIOS)**.
Click the link for **Firmware and Device drivers**
Select the desired version (for example V2.XX) and download **7SR5 Reydisp Manager Template & Device Firmware**.
Save the file to any location on your Reydisp Manager 2 installed PC.

[sc_7SR5_FirmwareDeviceDriversLink, 1, --_--]
Figure 8-15 Firmware and Device Drivers Link

8.4.3 Installing the New Firmware Templates to Reydisp Manager

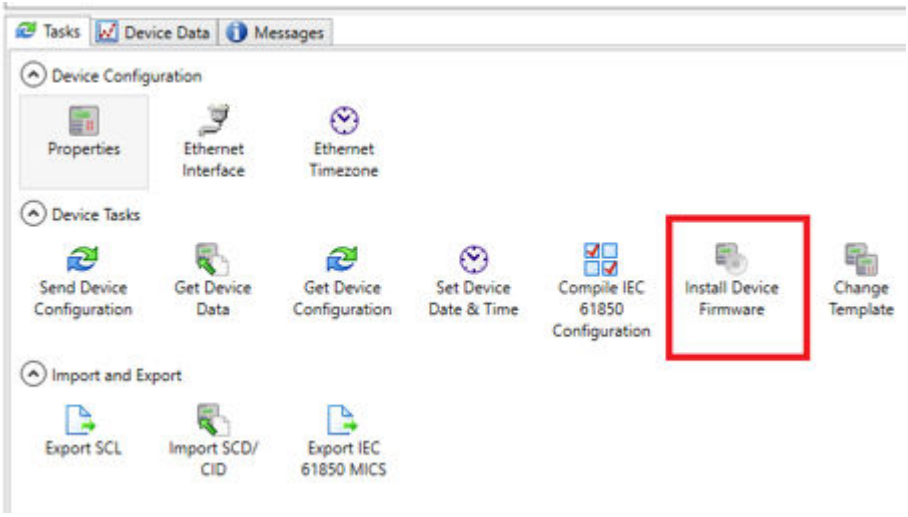
Reydisp Manager 2 must be installed on the PC to ensure the correct USB drivers are installed.
Clicking the self extracting **.exe** file will load the files into the Reydisp Manger templates location.
For a new device follow the instructions in the Engineering manual section 2.2 Starting Reydisp Manager 2 and Creating a Project and 2.4 Adding a 7SR5 Device.
When selecting the template, select the version for this upgrade.
If the device is already existing within a project, the instructions procedure in the Engineering manual section 3.2 Change Device Template must be followed to upgrade the device to the new firmware template.

8.4.4 Firmware Upgrade Procedure

The device should be out of service and disconnected from the power system.
Any configuration and data stored in the device will be lost during a firmware upload.

8.4.5 Loading Device Firmware to the 7SR5 Device

The device must be connected to the PC via the front USB port.
The PC will connect to the device and proceed to transfer the firmware package to the device.
Double-click the **Install Device Firmware** in the selected device task area.

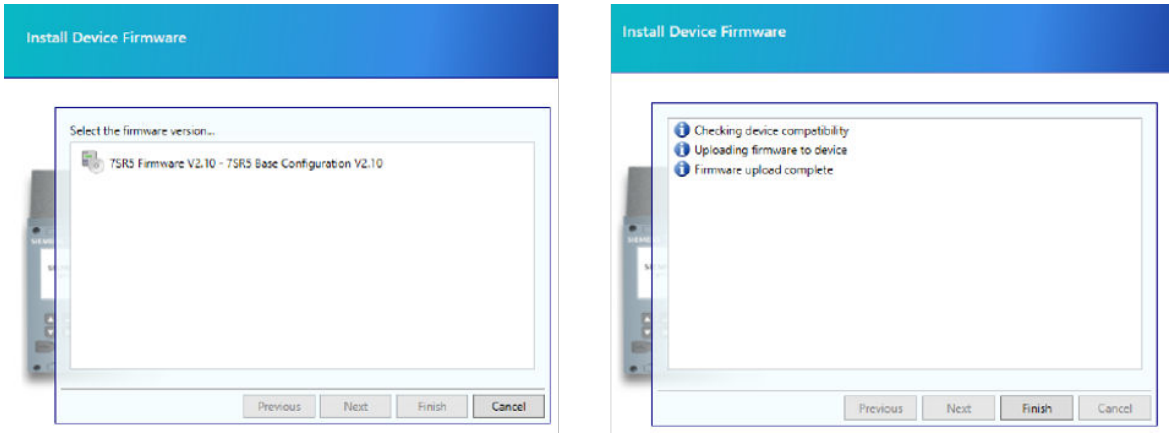


[sc_7SR5_InstallDeviceFirmwareIcon, 1, --_--]

Figure 8-16 Install Device Firmware Icon

NOTE

If the maintenance password is active a prompt window will request that it is entered before continuing.



[sc_7SR5_InstallDeviceFirmwareSteps, 1, --_--]

Figure 8-17 Install Device Firmware Steps

Confirm the firmware is the correct version by selection and click **Next** to continue.

A loader window will be visible for a short duration during the connection.

On completion of the transfer the window will notify the user the upload from the PC to the device is complete and the **Finish** option must be selected.

During the upgrade process the device fascia will display file transfer information and the device will restart on completion.

All user configuration files and data storage will be erased and the settings defaulted. Press **Enter** on the device to confirm acknowledgement. The device will display the **`Device not configured`** message on the display after a short duration.

The firmware version can be viewed in the device on the fascia in Device Information for confirmation.

8.4.6 Loading a Security Update Comms Firmware to the 7SR5 Device

Download the security patch to the PC.

The device should be out of service and disconnected from the power system.

Browse to the device homepage of the device via a direct connection to the USB port or over an ethernet connection to one of the rear ethernet ports of the device.

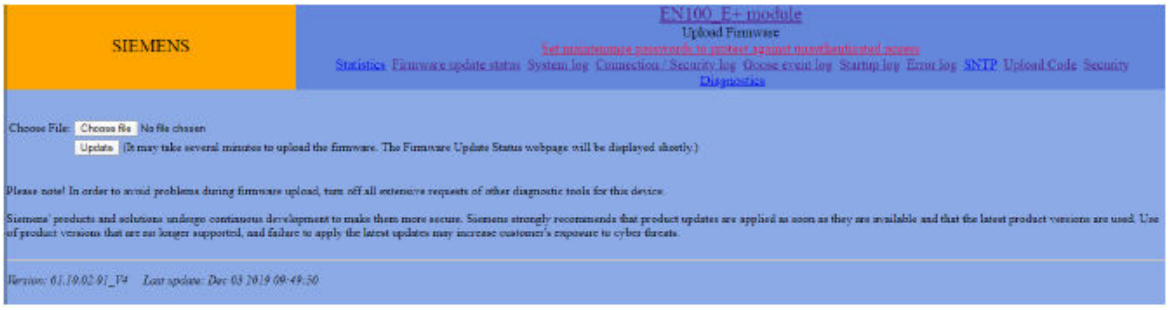
For the device front USB port use *https://192.168.2.1/upload* to navigate directly and procced to the page.

For the rear ethernet port, it must be configured and the IP address used.

Use the **Choose file** option to navigate to the security patch **.pck** file downloaded from the website and select **Update**.

NOTE

If the maintenance password is active a prompt window will request that it is entered before continuing.



[sc_7SR5_SecurityUpdate, 1, --_--]

Figure 8-18 Reydisp Manager 2 Security Update

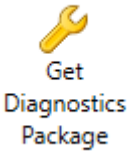
NOTE

The user configuration files and data storage files will not be erased during a security patch update.

8.5 Get Diagnostics Package

8.5.1 General

The **`Get Diagnostics Package`** feature is located in the device tasks area. This can be used to retrieve the configuration and data files from the device for investigation purposes when requesting support from the Siemens Customer Support Centre.



[sc_7SR5_GetDiagnosticsPackageIcon, 1, --_--]

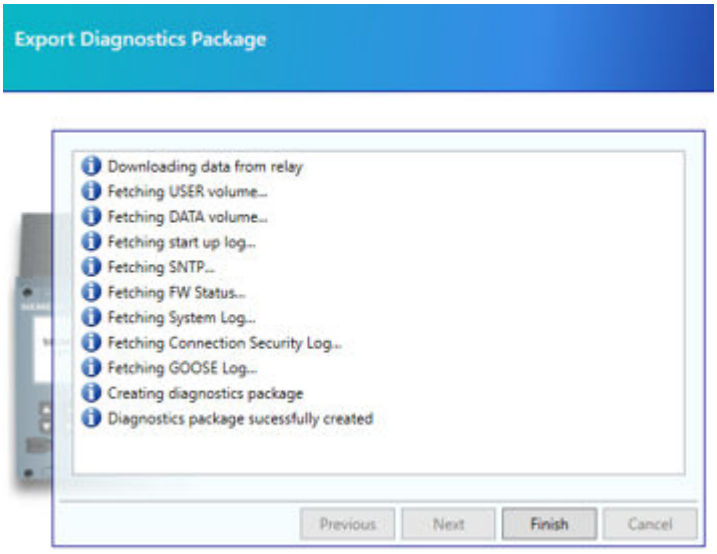
Figure 8-19 Get Diagnostics Package Icon

After clicking on the icon in the task window, a preferred communication connection must be selected.

The diagnostic information is then read from the Reyrolle 5 device.

Once completed the user can then click **Finish** and save the file into a folder.

The **`Get Diagnostics Package`** tool should only be used when seeking support from the Siemens Customer Support Centre. This will produce a single export from the device which the support team can use to investigate. The project is also useful but this retrieves all of the log files/event records as well.



[sc_7SR5_ExportDiagnosticsPackage, 1, --_--]

Figure 8-20 Export Diagnostics Package

NOTE

This process may take several minutes to extract all of the device files.

9 Security Settings

9.1 Security Design

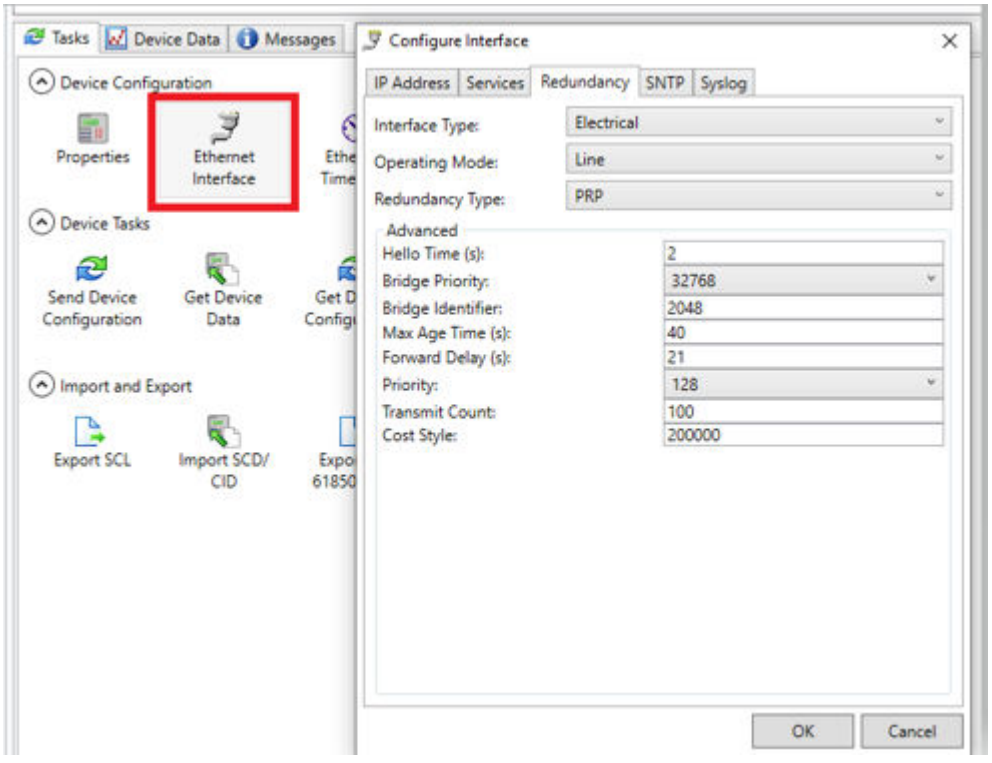
Security Design

Due to the increasing integration of bay units in Ethernet-based communication network, you must secure the communication against internal failures and attacks from outside. The specifications published by the North American Electric Reliability Council for critical infrastructure protection - NERC-CIP, for short - and the white paper published by the German Association of Energy and Water Management (BDEW) contain requirements for the safe operation of devices in critical communications infrastructure. These requirements are addressed to manufacturers and operators.

Security must be incorporated into the design of devices right from the start. This is implemented consistently in 7SR5 devices. Measures in the hardware ensure the secure use of signed files. These are provided to protect the firmware files and data records of the device. Secure storage of key material on the device makes secure communication between Reydisp Manager 2 and the device possible. The following items give you a high level of security when integrating the 7SR5 device in the network:

- Protection against attacks from the network
- Multi-stage safety concept in the operating state
- Logging of authorized and unauthorized access
- Logging of safety-critical actions

You can switch off unused Ethernet services. If, for example, the RSTP redundancy log is not being used, you can switch it off using Reydisp Manager 2. This gives a potential attacker no open interfaces and only utilized services are activated in a network.



[sc_7SR5_EthernetProtocolSettings, 1, --_--]

Figure 9-1 Ethernet Protocol Settings used in Reydisp Manager 2

9.2 Multi-Level Safety Concept

Multi-Level Security Concept

Reydisp Manager 2 offers many useful functions for the configuration and testing of your 7SR5 devices. Constant password prompts are not sensible during this phase. During operation, however, the focus is on the reading of data. Reconfiguration and switching are safety-critical operations. These operations lead to failures in operation if they are carried out inadvertently or without authorization. After completion of commissioning, you can activate a multi-level security concept in the device.

Before Reydisp Manager 2 can communicate with the 7SR5 device via its Ethernet services, the device carries out secure authentication. Only Reydisp Manager 2 has the authorization for communication with the device. In addition, a connection password that meets the strict rules of NERC-CIP can be configured. The password is securely stored in the device in the form of an equivalent salted hash. The password must contain upper-case and lower-case letters, digits, and special characters and must be at least 8 to 24 characters long. It is queried before connection is established. A connection to the 7SR5 device cannot be established until the correct password has been entered. You now have read access.

All write-access rights to the 7SR5 device such as, for example, changing setting values or switching are protected by other security prompts, the confirmation IDs. If changes are done via the integrated operation, these confirmation IDs are queried on the on-site operation panel. The confirmation ID contains only numbers that you must enter at the on-site operation panel or in Reydisp Manager 2.

NOTE

The confirmation IDs are only needed if the role-based access control (RBAC) is not activated in the 7SR5 device.

The 3-level security concept consists of secure authentication, the connection password, and other confirmation IDs. This concept provides the highest possible degree of access protection during operation. Even remote access to devices is protected. You can also use an Ethernet module exclusively for the communication with Reydisp Manager 2. Access by a substation control network with the unsecured IEC 61850 protocol and remote access with Reydisp Manager 2 are then carried out via completely separate networks. Even though the 7SR5 device communicates with Reydisp Manager 2 via an Ethernet module, communication between Reydisp Manager 2 and the device is encrypted using tap-proof technology.

Wrong password entries are identified and logged. An alarm can be triggered via a telecontrol connection. Safety-critical operations are also logged and cannot be deleted in the device. If files on the PC were manipulated by malware (for example, viruses), they cannot be loaded into the device.

NOTE

The system operator is responsible for further protection-function tests within maintenance intervals. Check protection functions using secondary test equipment (see Device manual).

9.3 Security Settings in the Device

Siemens recommends applying the provided security updates by using the corresponding tooling and documented procedures that are available with the product. If supported by the product, an automatic means to apply the security updates across multiple product instances can be used.

Siemens recommends validating any security update before being applied, and supervision by trained staff of the update process in the target environment.

The most important security requirements are the following:

- Authentication and authorization of the users
- Assurance of the integrity of the transmitted data
- Protections against virus, trojans, and other malware
- Collection and saving of log files
- Operation of the system in a protected environment (physical security)
- Every user is given the only those rights that are necessary to fulfill the corresponding work
- Assurance, that in case of a system failure, a restoration is possible without or only with marginal data loss
- Only activate required services and ports
- Network load of critical systems are limited to the extent to make the systems continue to work under maximum load. For example, limit the number of broadcasts in the power-system components.

The 7SR5 Security Manual serves as a recommendation for the secure commissioning and operations of the 7SR5 IEDs in networked environments.

During the complete product lifecycle, from commissioning to operation and maintenance, all service personnel, project personnel, customers, and operators involved should consider the recommendations in this manual.

9.4 Device Access Security

7SR5 devices support user authentication and operations for protecting access to the security-relevant operations and functions.

The 7SR5 device provides user authentication using a connection password and maintenance password. Furthermore to prevent from executing critical actions from the device fascia using the keys you can also set up confirmation ID's for local access.

The following table shows the passwords used in device EN100 for security functions.

Password	Description
Maintenance	Password for: • EN100 firmware upgrade via Ethernet or USB • Firmware upgrade via Ethernet or USB • Security log access • Resetting the connection password
Connection	Password for EN100 connection with Reydisp via Ethernet or USB

The Maintenance and Connection passwords can only be set and modified through the EN100 Web UI and selecting the Security page option.

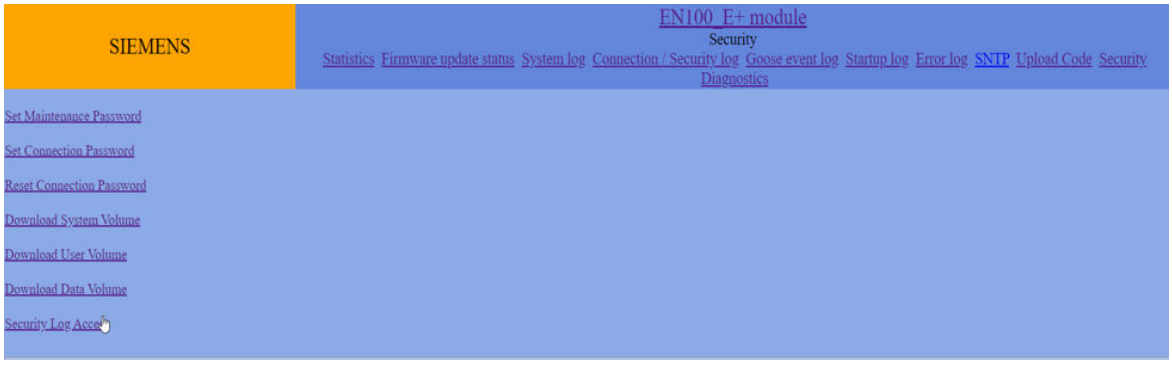


Figure 9-2 EN100 Web UI

The passwords can also be reset from the fascia using the Reset Password feature.

Confirmation IDs

Confirmation IDs are used for protection against unintentional and unauthorized operation from the fascia and will not be required for a configuration change via the USB port.

You can find more information about the confirmation ID in the 7SR5 Operation manual.

9.5 Connection Password

The connection password is not active when the device leaves the factory or is returned to the factory condition. The maintenance password must be set before the connection password can be set. If a connection password has been activated it will be required to allow a configuration to be sent to the 7SR5 device.

The connection password follows the NERC-CIP-standard (North American Electric Reliability Critical Infrastructure Protection) and consists of the following parts:

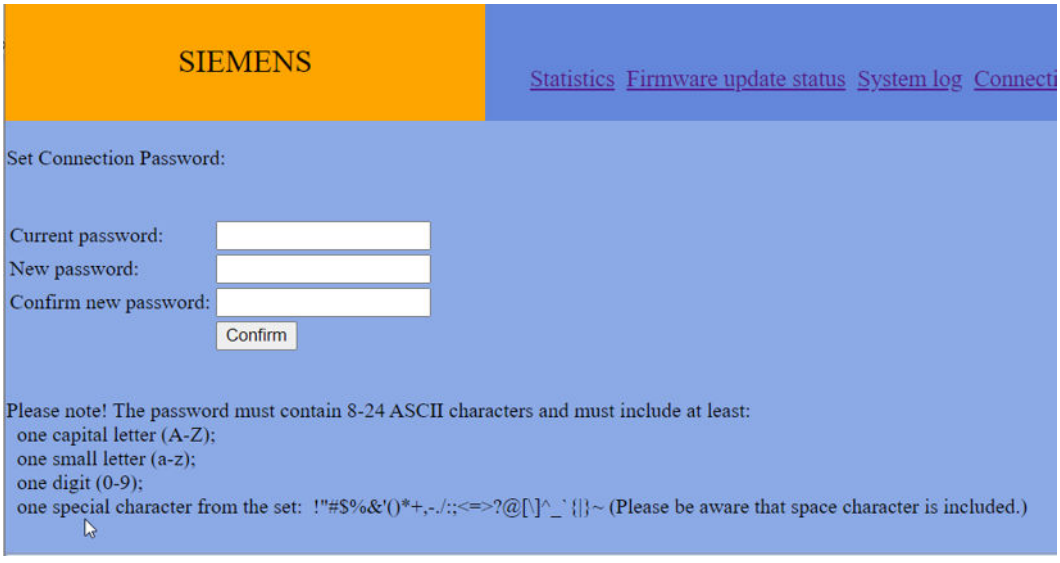
- Lower-case letters
- Upper-case letters
- Digits
- Special characters, for example, %, &, $

The length of the connection password ranges from 8 characters to 24 characters.

The connection password is empty by default. To enter a new connection password, the existing characters are concealed by asterisks. To confirm the connection password, enter it twice. This confirmation prevents erroneous entries.

NOTE

The deactivation of the connection password results in providing everyone unauthenticated and unrestricted access to the device through Reydisp Manager or through the browser-based user interface. If you wish to hinder this, set the connection password in the device.



[sc_7SR5_SetConnectionPassword, 1, --_--]

Figure 9-3 Setting Window for the Connection Password

Initialization of the connection password is possible only via the front USB interface or via an Ethernet interface of the device. In both cases, the entered connection password is securely transferred to the device via the HTTPS protocol. The connection password is not stored in the Reydisp Manager project or anywhere on the Windows PC. It is stored as a salted hash in the device.

If you have initialized the connection password, further access to the device (via Reydisp Manager or via the browser-based user interface) is possible only if you enter the correct connection password in the dialog while establishing a connection to the device. This procedure prevents unauthenticated access. Siemens recommends checking the connection password after initialization.

You can change the connection password online via an Ethernet connection or via the USB connection. After entering the current connection password and entering and repeating the new connection password, the device accepts the change.

9.6 Maintenance Password Configuration

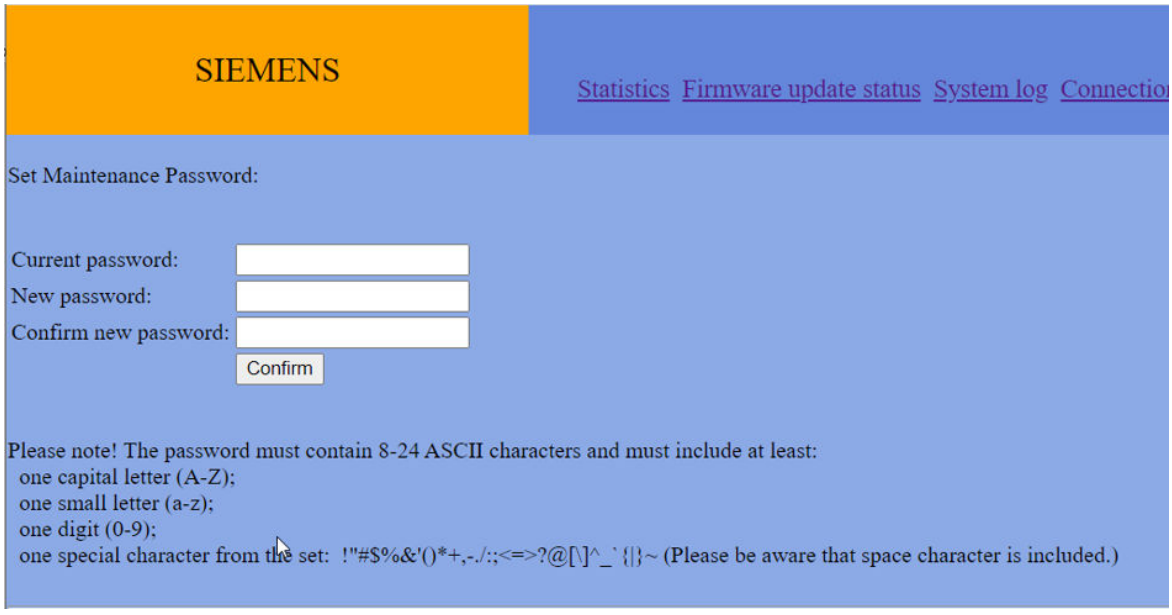
The maintenance password is not active when the device leaves the factory or is returned to the factory condition. If a maintenance password has been activated it will be required to allow new firmware to be sent to the device, the Security log or Fault record page to be accessed, or reset the **SNMP V3 Users** to default.

The maintenance password follows the NERC-CIP-standard (North American Electric Reliability Critical Infrastructure Protection) and consists of the following parts:

- Lower-case letters
- Upper-case letters
- Digits
- Special characters, for example, %, &, $

The length of the maintenance password ranges from 8 characters to 24 characters.

The maintenance password is empty by default. To enter a new maintenance password, the existing characters are concealed by asterisks. To confirm the maintenance password, enter it twice. This confirmation prevents erroneous entries.



[sc_7SR5_MaintenancePassword, 1, --_--]

Figure 9-4 Set Maintenance Password

Initialization of the maintenance password is possible only via the front USB interface or via an Ethernet interface of the device. In both cases, the entered connection password is securely transferred to the device via the HTTPS protocol. The connection password is not stored in the Reydisp Manager project or anywhere on the Windows PC. It is stored as a salted hash in the device.

If you have initialized the maintenance password, this prevents unauthenticated upload of new firmware. Siemens recommends checking the password after initialization.

You can change the connection password online via an Ethernet connection or the USB connection. After entering the current connection password and entering and repeating the new connection password, the device accepts the change.

9.7 Authentication, Connection Password, and Confirmation ID During Operation

To gain access to the device, the user is required to enter the correct connection password.

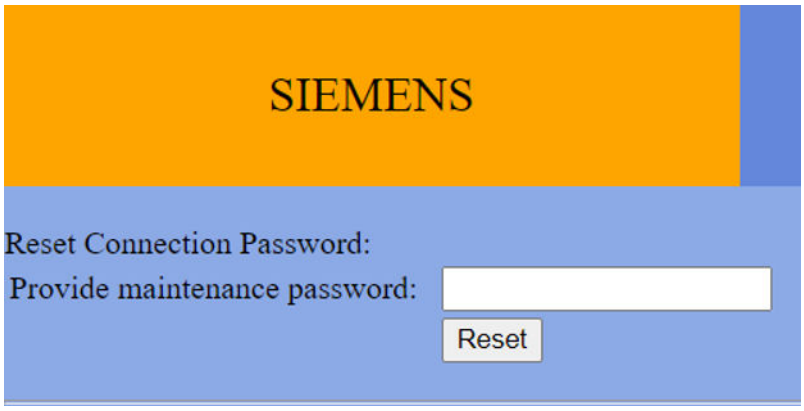
If an incorrect connection password is entered, the device records this action in the security log.

If an incorrect connection password is entered 5 times in a 5 minute period, access to the device is blocked for 30 minutes.

These operations are recorded in the security log of the device as well.

9.8 Resetting and Deactivating the Passwords

The connection password can be reset via the Ethernet or USB connection from the web page. To reset the connection password use the Reset Connection Password option in the Security page. The maintenance password must be known and entered.



[sc_7SR5_ResetConnectionPassword, 1, --_--]

Figure 9-5 Reset Connection Password

For emergency access, if the passwords are lost, the passwords can be reset from the device fascia, if the fascia access ID's are known.

In the Device Configuration a parameter is provided to allow resetting of the passwords.

Parameter: **Reset Password**

- Default Setting: **No**

  This function is accessible at the relay fascia only. The reset is applied to the connection password and the maintenance password. Completion of the reset requires the **Reset Confirmation ID**, **0000** to be entered.

9.9 Recording of Cyber-Security Events

The 7SR5 devices and Reydisp Manager provide a security audit trail which chronologically acquires and categorizes security-relevant events according to the origin and severity.

The 7SR5 devices automatically send the security-relevant events to an external syslog-server.

The transmission of the security events to the configured syslog server(s) takes place spontaneously and without a conformation via UDP (User Datagram Protocol) when the security event occurs. A later readout of the recorded security-events from the device-local security event buffer is possible. The security events are in English.

NOTE

On the syslog server(s), Siemens recommends protecting the received security-events from unauthorized read or write access with the role Auditor.

Structure of Security Events

A syslog event is built up with following elements:

Table 9-1 Security Events

Element	Description
Severity (level)	Severity levels of the event: • Warning • Alarm
Date	Date when the event is received or logged from the syslog server
Time	Time when the event is received or logged from the syslog server • T Time • hh:mm:ss.ttt Time when the event is created • +hh:mm Time deviation from GMT
IP address or port name	IP address or port name of the product or subcomponent that generates the log entry
Module name	The name of the product module that generates the log entry
BOM	Byte order mark for UTF8 encoding
Product name	The name of the product that generates the log entry
Indication text	The message part of a syslog event Depending on the event, the indication text can contain variable additional information (%A1%, %A2%, %A3%, and %A4%).

NOTE

Multiple password entry attempts in quick succession may be disregarded by the device as not genuine entry attempts.

Configuration Overview

To record cybersecurity events during the operation of 7SR5 devices, recordings are automatically created and data is collected. All security-related events and alarms recorded in the device-internal security log can also be transmitted simultaneously to a central syslog server. This action allows safety-relevant events to be recorded from various transformer stations with the requirements of standards and guidelines, such as IEEE 1686,

IEC 62443, and the BDEW White Paper. Logging is started centrally on 1 or 2 self-selected syslog servers. Combining different protocol data of the devices used gives you a general overview of the device network. You can analyze and monitor this data. This action allows safety-critical events to be logged and related changes to be tracked. You can also track attacks on the operated devices by using the log data.

You can view the collected log data in the security log locally on the device display, irrespective of the current operating mode of the device. The alarm and safety-critical indications are stored chronologically in the security log. You cannot modify or delete these entries.

You can, for example, answer to the following questions:

- How many login attempts have been made?
- When was the device configuration last updated?

Configuring the Central Syslog Server

If you have started Reydisp Manager and have the device configuration, select **Ethernet Interface** in the device Task tools. The **Syslog** menu item contains the setting options for a central syslog server. You can activate up to 2 syslog servers.

You can activate logging under **syslog server 1** and/or **2**. Enter the following data:

- IP Address
- Server UDP port

Figure 9-6 shows a setting example for the IP addresses and ports of 2 syslog servers in 7SR5 device configuration in Reydisp Manager.

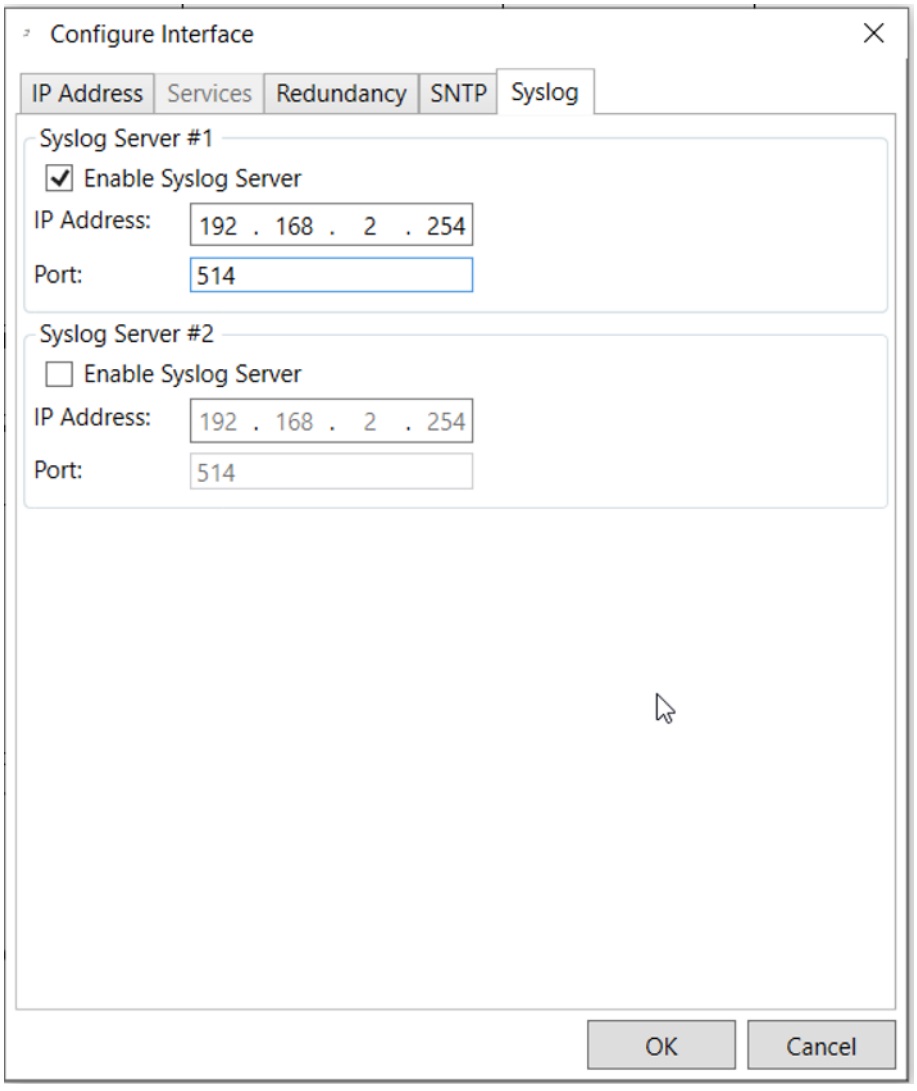


Figure 9-6 A Setting Example for the IP Addresses and Ports of the Syslog Servers

If the log organized as a ring buffer exceeds the 100 % capacity limit, the oldest entries are automatically overwritten and the capacity utilization is reset to 0 %.

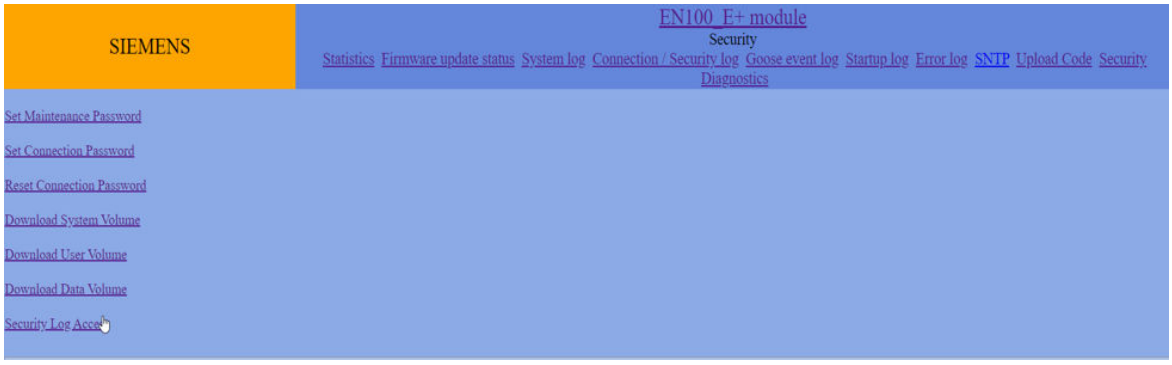
Viewing Audit Logs

Access to areas of the device with restricted access rights is recorded in the security log. Unsuccessful and unauthorized access attempts are also recorded. Up to 2048 indications can be stored in the security log.

Reading from the PC with a Browser

- To access the security log of your 7SR5 device, use the IP address to browse to the Siemens 7SR5 hompage. The device must be in Online access.

  Security -> **Security log access**

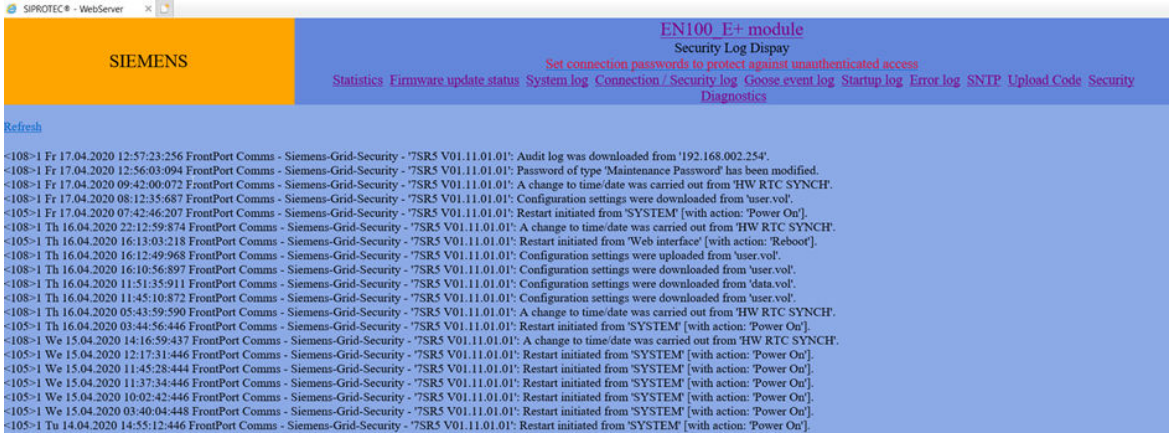


[sc_7SR5_EN100WebUI, 1, --_--]

Figure 9-7 Accessing the Security Log

The state of the security log last loaded from the device is displayed.

- The maintenance password must be entered prior to access to the security log being granted.

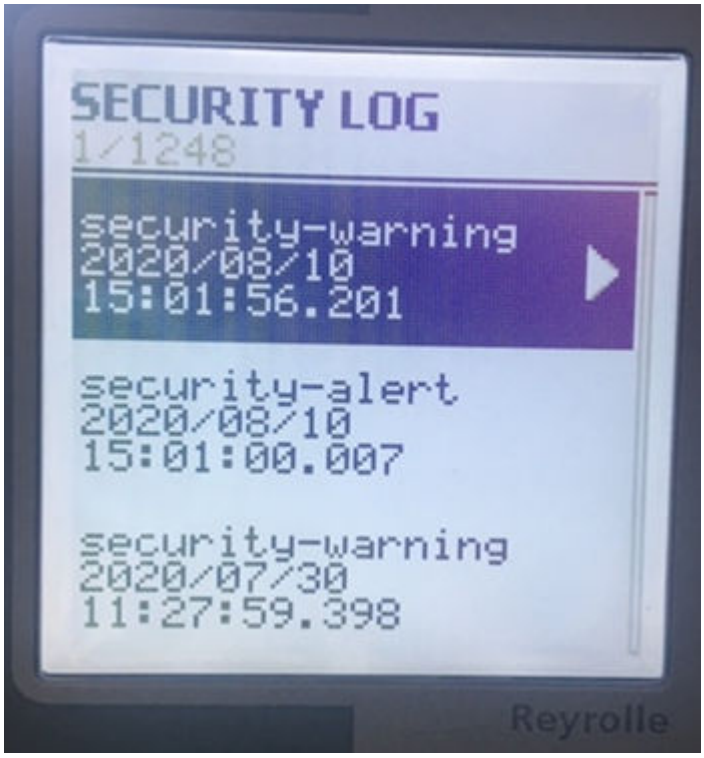


[sc_7SR5_SecurityLog, 1, --_--]

Figure 9-8 Reading the Security Indications with Internet Browser

Reading on the Device through the On-Site Operation Panel

- To access the security log from the main menu, use the navigation keys of the on-site operation panel.
  Main Menu -> **Security log**
- To access the Security log the Security log access ID must be active and entered using the fascia keys. The Security log access ID is set and activated in Reydisp Manager in the setting parameter file.
- You can navigate within the displayed indication list using the navigation keys (up/down) on the on-site operation panel.



[sc_7SR5_SecurityLogOperationPanel, 1, --_--]

Figure 9-9 Reading the Security Log on the On-Site Operation Panel of the Device

NOTE

- The logged indications are preconfigured and cannot be changed!
- You cannot delete the log which is organized as a ring buffer.
- If you want to archive security-relevant information without loss of information, you must regularly read this log.