

RELION® PROTECTION AND CONTROL

REX640

Operation Manual





Document ID: 1MRS759118

Issued: 2023-02-10

Revision: D

© Copyright 2023 ABB. All rights reserved

Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB and Relion are registered trademarks of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Open Source Software

This product contains open source software. For license information refer to product documentation at www.abb.com.

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

www.abb.com/mediumvoltage

Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product has been designed to be connected and communicate data and information via a network interface which should be connected to a secure network. It is the sole responsibility of the person or entity responsible for network administration to ensure a secure connection to the network and to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the product and the network, its system and interface included, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2014/30/EU) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2014/35/EU). This conformity is the result of tests conducted by the third party testing laboratory Intertek in accordance with the product standard EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.

Contents

1	Introduction.....	11
1.1	This manual.....	11
1.2	Intended audience.....	11
1.3	Product documentation.....	12
1.3.1	Product documentation set.....	12
1.3.2	Document revision history.....	12
1.3.3	Related documentation.....	12
1.4	Symbols and conventions.....	13
1.4.1	Symbols.....	13
1.4.2	Document conventions.....	13
2	Environmental aspects.....	14
2.1	Sustainable development.....	14
2.2	Disposal of a device.....	14
3	REX640 overview.....	15
3.1	Overview.....	15
3.2	Relay hardware.....	15
3.3	Local HMI.....	16
3.4	Switchgear HMI.....	20
3.4.1	Bay overview area.....	22
3.4.2	Physical and virtual Home buttons.....	23
3.4.3	Navigation.....	23
3.5	HMI communication ports.....	24
3.6	Web HMI.....	24
3.6.1	Command buttons.....	26
3.7	User authorization.....	27
	Local user account management.....	28
3.8	Station communication.....	29
3.9	PCM600.....	29
3.9.1	Connectivity packages.....	29
3.9.2	PCM600 and relay connectivity package version.....	30
3.10	Modification Sales.....	30
4	Using HMI.....	31
4.1	Logging in.....	31
4.1.1	Managing forgotten password.....	33
4.2	Logging out.....	33

4.3	Selecting local or remote use.....	34
4.4	Identifying device.....	35
4.5	Changing backlight brightness and timeout.....	36
4.6	Changing setting visibility.....	37
4.7	Monitoring relay status.....	38
4.7.1	Switchgear HMI status indications.....	39
4.8	Changing language.....	41
4.9	Alarms.....	41
4.9.1	Viewing alarm list.....	41
4.9.2	Acknowledging alarms.....	41
4.10	Measurements and phasor diagrams.....	43
4.10.1	Viewing measurements.....	43
4.10.2	Viewing phasor diagrams.....	43
4.11	Showing parameters.....	44
4.11.1	Viewing Protection Characteristics.....	45
4.12	Editing values.....	46
4.13	Committing settings.....	47
4.14	Clearing and acknowledging.....	48
4.15	Accessing disturbance records.....	49
4.16	Viewing fault records.....	50
4.17	Selecting USB actions.....	51
4.18	Using local HMI help.....	52
4.19	Changing setting group.....	53
4.20	Controlling.....	54
4.21	Bookmarking pages.....	57

5 Using Web HMI..... 59

5.1	Connecting to Web HMI.....	59
5.1.1	Logging in.....	59
5.1.2	Logging out.....	62
5.2	Navigating in menus.....	62
5.3	Identifying device.....	62
5.4	Viewing dashboard.....	63
5.5	Viewing self-supervision.....	63
5.6	Changing language.....	64
5.7	Alarms.....	64
5.7.1	Viewing alarm list.....	64
5.7.2	Acknowledging alarms.....	65
5.8	Measurements and phasor diagrams.....	67
5.8.1	Viewing measurements.....	67
5.8.2	Viewing phasor diagrams.....	67
5.9	Viewing monitoring.....	69
5.10	Viewing single-line diagram.....	70
5.11	Showing parameters.....	71

5.12	Editing values.....	72
5.13	Committing settings.....	74
5.14	Clearing and acknowledging.....	76
5.15	Accessing event view.....	77
5.16	Accessing disturbance record view.....	78
5.16.1	Saving disturbance records.....	79
5.16.2	Triggering disturbance recorder manually.....	79
5.16.3	Deleting disturbance records.....	80
5.17	Viewing fault records.....	81
5.18	Exporting load profile records.....	81
5.19	Importing and exporting of settings.....	82
5.19.1	Exporting settings.....	82
5.19.2	Importing settings.....	82
5.20	Exporting report summary.....	84
5.21	Using Web HMI help.....	85

6 Troubleshooting.....86

6.1	Fault tracing.....	86
6.1.1	Identifying hardware errors.....	86
6.1.2	Identifying runtime errors.....	86
6.1.3	Identifying communication errors.....	86
6.1.4	Reading of internal log files.....	87
6.1.5	Checking local HMI connectivity.....	88
6.2	Self-supervision.....	88
6.2.1	Internal faults.....	90
6.2.2	Warnings.....	99
6.2.3	Power supply module Ready LED and HMI Home button LED.....	101
6.3	Correction procedures.....	103
6.3.1	Creating relay backup in HMI.....	103
6.3.2	Rebooting the software.....	104
6.3.3	Restoring factory settings.....	104
6.3.4	Restoring relay backup from local HMI.....	104
6.3.5	Restoring relay backup from switchgear HMI.....	108
6.3.6	Setting passwords.....	108
6.3.7	Identifying relay application problems	109

7 Commissioning.....111

7.1	Commissioning checklist.....	111
7.2	Checking installation.....	111
7.2.1	Checking power supply.....	111
7.2.2	Checking CT circuits.....	112
7.2.3	Checking VT circuits.....	112
7.2.4	Checking binary input and output circuits.....	113

7.3	Authorizations.....	113
7.3.1	User authorization	113
7.4	Setting protection relay and communication.....	114
7.4.1	Setting the communication between protection relays and PCM600.....	115
7.4.2	Communication settings.....	116
7.4.3	Connecting and setting HMI.....	125
7.5	Testing of protection relay operation.....	138
7.5.1	Selecting IED test mode	138
7.5.2	Testing and commissioning support on local HMI.....	138
7.5.3	Using HMI Client.....	149
7.5.4	Selecting the internal fault test.....	150
7.5.5	Selecting IED blocked or IED test and blocked mode.....	150
7.6	ABB Product Data Registration.....	151
8	Maintenance and Periodical Testing.....	153
8.1	Maintenance and Periodical Testing.....	153
8.1.1	Maintenance.....	153
8.1.2	Periodical Testing.....	153
9	Glossary.....	158

1 Introduction

1.1 This manual

The operation manual contains instructions on how to operate the protection relay once it has been commissioned. The manual provides instructions for monitoring, controlling and setting the relay. The manual also describes how to identify disturbances and how to view calculated and measured power grid data to determine the cause of a fault.

1.2 Intended audience

This manual addresses the operator who operates the protection relay frequently.

The operator must be trained in and have a basic knowledge of how to operate protection equipment. The manual contains terms and expressions commonly used to describe this kind of equipment.

1.3 Product documentation

1.3.1 Product documentation set

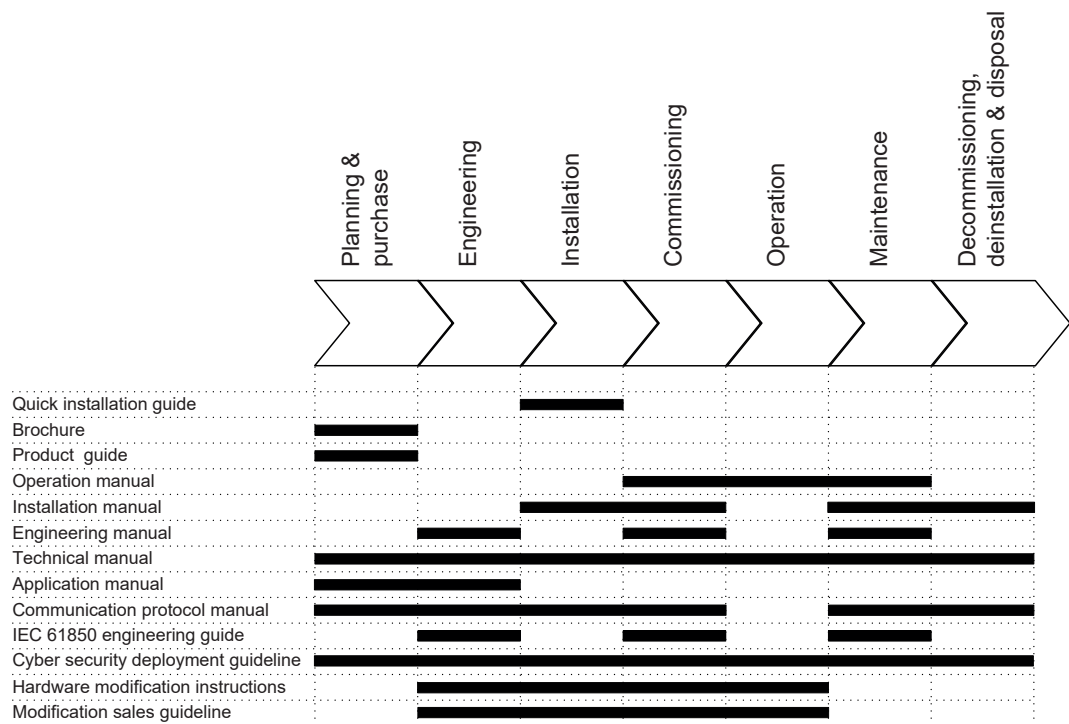


Figure 1: The intended use of documents during the product life cycle

1.3.2 Document revision history

Document revision/date	Product connectivity level	History
A/2019-05-24	PCL1	First release
B/2020-02-13	PCL2	Content updated to correspond to the product connectivity level
C/2020-12-10	PCL3	Content updated to correspond to the product connectivity level
D/2023-02-10	PCL4	Content updated to correspond to the product connectivity level

1.3.3 Related documentation

Download the latest documents from the ABB Web site www.abb.com/mediumvoltage.

1.4 Symbols and conventions

1.4.1 Symbols



The electrical warning icon indicates the presence of a hazard which could result in electrical shock.



The warning icon indicates the presence of a hazard which could result in personal injury.



The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.



The information icon alerts the reader of important facts and conditions.



The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

1.4.2 Document conventions

A particular convention may not be used in this manual.

- Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.
- Menu paths are presented in bold.

Select **Main menu > Settings**.

- WHMI menu names are presented in bold.

Click **Information** in the WHMI menu structure.

- Parameter names are shown in italics.

The function can be enabled and disabled with the *Operation* setting

- Parameter values are indicated with quotation marks.

The corresponding parameter values are "On" and "Off".

- Input/output messages and monitored data names are shown in Courier font.

When the function starts, the `START` output is set to TRUE.

- Values of quantities are expressed with a number and an SI unit. The corresponding imperial units may be given in parentheses.
- This document assumes that the parameter setting visibility is "Advanced".

2 Environmental aspects

2.1 Sustainable development

Sustainability has been taken into account from the beginning of the product design including the pro-environmental manufacturing process, long life time, operation reliability and disposing of the device.

The choice of materials and suppliers has been made according to the EU RoHS directive (2011/65/EU). This directive limits the use of hazardous substances.

Operational reliability and long life time have been ensured with extensive testing during the design and manufacturing processes. Moreover, long life time is supported by maintenance and repair services as well as by the availability of spare parts.

Design and manufacturing have been done under a certified environmental system. The effectiveness of the environmental system is constantly evaluated by an external auditing body. We follow environmental rules and regulations systematically to evaluate their effect on our products and processes.

2.2 Disposal of a device

Definitions and regulations of hazardous materials are country-specific and change when the knowledge of materials increases. The materials used in this product are typical for electric and electronic devices.

All parts used in this product are recyclable. When disposing of a device or its parts, contact a local waste handler who is authorized and specialized in disposing of electronic waste. These handlers can sort the material by using dedicated sorting processes and dispose of the product according to the local requirements.

Table 1: Materials of the protection relay parts

Device	Parts	Material
Case	Casted enclosure	Aluminium
	Metallic plates	Aluminium
	Screws, bushes	Steel
	Plastic parts	PC ¹ , LCP ²
	LHMI	Various
Package	Box	Cardboard
Attached material	Manuals	Paper

¹ Polycarbonate

² Liquid crystal polymer

3 REX640 overview

3.1 Overview

REX640 is a powerful all-in-one protection and control relay for use in advanced power distribution and generation applications with unmatched flexibility available during the complete life cycle of the device – from ordering of the device, through testing and commissioning to upgrading the functionality of the modular software and hardware as application requirements change.

The modular design of both hardware and software elements facilitates the coverage of any comprehensive protection application requirement that may arise during the complete life cycle of the relay and substation.

REX640 makes modification and upgrading easy and pushes the limits of what can be achieved with a single device.

3.2 Relay hardware

The relay includes a Ready LED on the power supply module that indicates the relay's status. In normal situations, the Ready LED has a steady green light. Any other situation that requires the operator's attention is indicated with a flashing light.

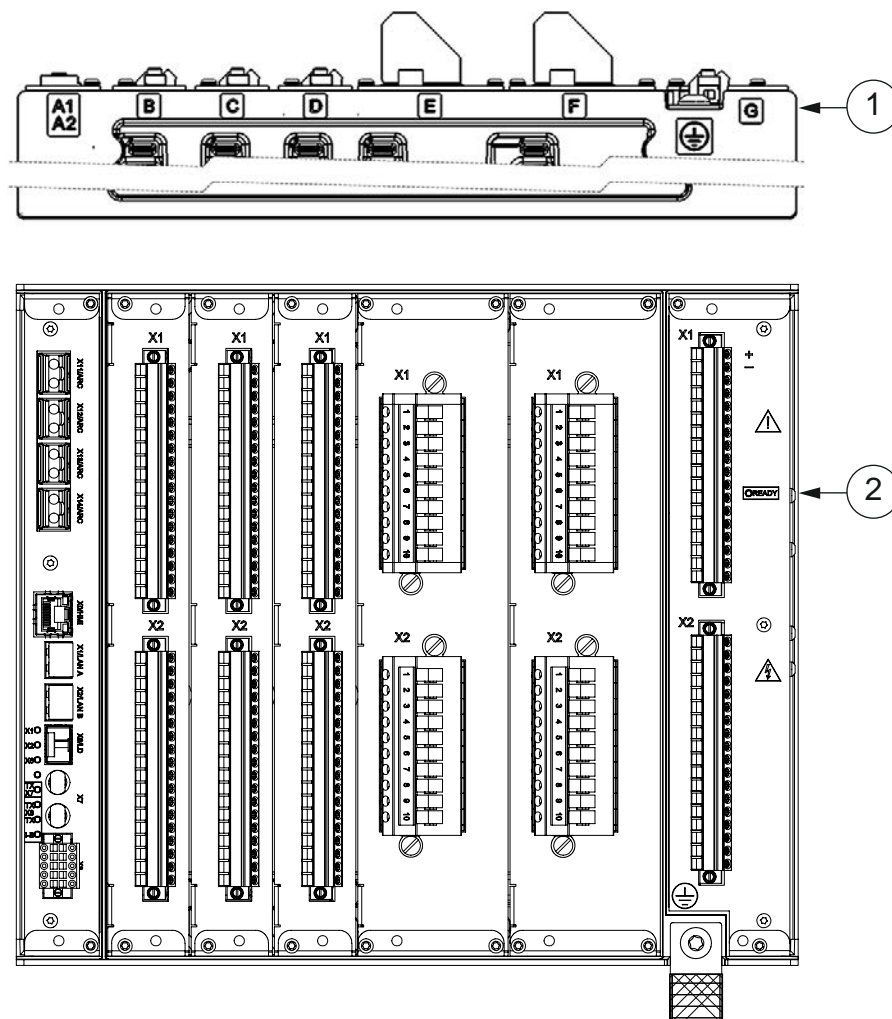


Figure 2: Hardware module slot overview of the REX640 relay

- 1 Slot markings in enclosure (top and bottom)
- 2 Ready LED

The relay has a nonvolatile memory which does not need any periodical maintenance. The nonvolatile memory stores all events, recordings and logs to a memory which retains data if the relay loses its auxiliary supply.

3.3 Local HMI

The LHMI is used for setting, monitoring and controlling the protection relay and the related process. It comprises a 7-inch color screen with capacitive touch sensing and a Home button at the bottom of the LHMI.



The LHMI is an accessory for the relay which is fully operational even without the LHMI.

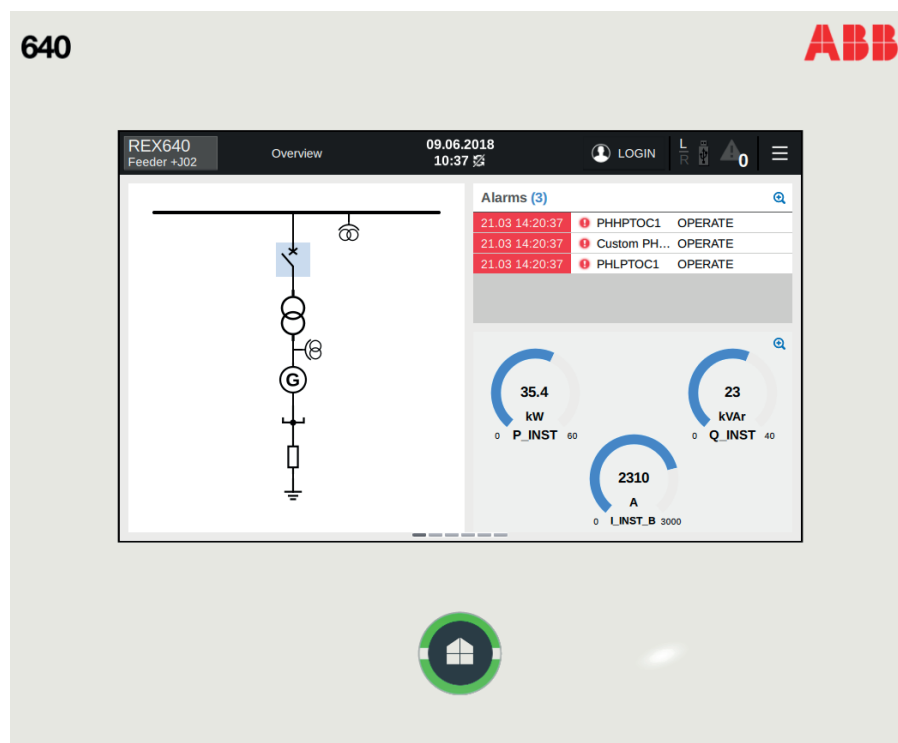


Figure 3: Example of a local HMI page

The LHMI presents pages in two categories.

- Operator pages are typically required as a part of an operator's normal activities, such as a single-line diagram, controls, measurements, events or alarms
- Engineer pages are specifically designed pages supporting relay parametrization, troubleshooting, testing and commissioning activities

The Operator pages can be scrolled either by pressing the Home button or by swiping the actual pages. The Engineer pages are accessible by tapping the menu button in the menu bar on the top of the LHMI display.

The Home button indicates the relay's status at a glance. In normal situations, the Home button shows a steady green light. Any other situation that requires the operator's attention is indicated with a flashing light, a red light or a combination of these.

Table 2: Power supply module Ready LED and local HMI Home button LED

State	Power supply module Ready LED	LHMI Home button	Alarm acknowledged
Relay under normal operation and LHMI connected	Steady green	Steady green	N/A
Relay's IRF activated, but communicates with LHMI	High frequency blinking green ¹	High frequency blinking red ¹	N/A
Communication lost between Relay and LHMI, but no IRF	Steady green	High frequency blinking green ¹	N/A

Table continues on the next page

¹ High frequency = 3 Hz

State	Power supply module Ready LED	LHMI Home button	Alarm acknowledged
LHMI not running normally or in start-up initialization phase	Steady green	High frequency blinking green ¹	N/A
Process related alarm active	Steady green	Low frequency blinking red ²	No
Process related alarm active	Steady green	Steady red	Yes
Process related alarm has been active earlier, but is not any more active.	Steady green	Low frequency blinking red ²	No
Process related alarm has been active earlier, but is not any more active.	Steady green	Steady green	Yes
Relay set to Test Mode	Low frequency blinking green ²	Low frequency blinking green ²	No

The Operator pages can be used as such or customized according to the project's requirements using Graphical Display Editor in PCM600. The Engineer pages are fixed and cannot be customized.

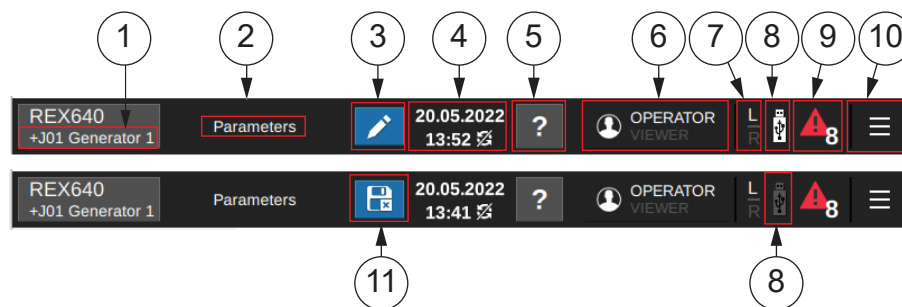


Figure 4: Menu bar elements

- 1 Bay name for the relay
- 2 Page name
- 3 Edit mode active (parameter editing)
- 4 Date, time and time synchronization status
- 5 Page help (visible if help is available for the page)
- 6 Login button/logged in user and role indication
- 7 Local/remote indication
- 8 USB memory not connected/connected (visible only if USB port is enabled)
- 9 Number of active alarms
- 10 Menu button for Engineer pages
- 11 Store or reject changed parameters indication

² Low frequency = 1 Hz

Table 3: Local HMI default pages

Page category	Pages	Subpages
Operator pages	Overview	Alarms
	Events	
	Fault Records	
	Timeline	
	Measurements	Phasors Load Profile Records
Engineer pages	Parameters	
	Testing and Commissioning	Force Functions Force Outputs Simulate Inputs View I/O Send Events Secondary Injection Monitoring Protection Measurement Direction Coil Controller Commissioning ³ View GOOSE sending View GOOSE receiving View SMV sending View SMV receiving
	Relay Status	Monitoring
	Clear	
	Disturbance Records	
	Alarms	
	Device Information	
	USB Actions	
	Network Settings	

³ Available with the Petersen coil control application package

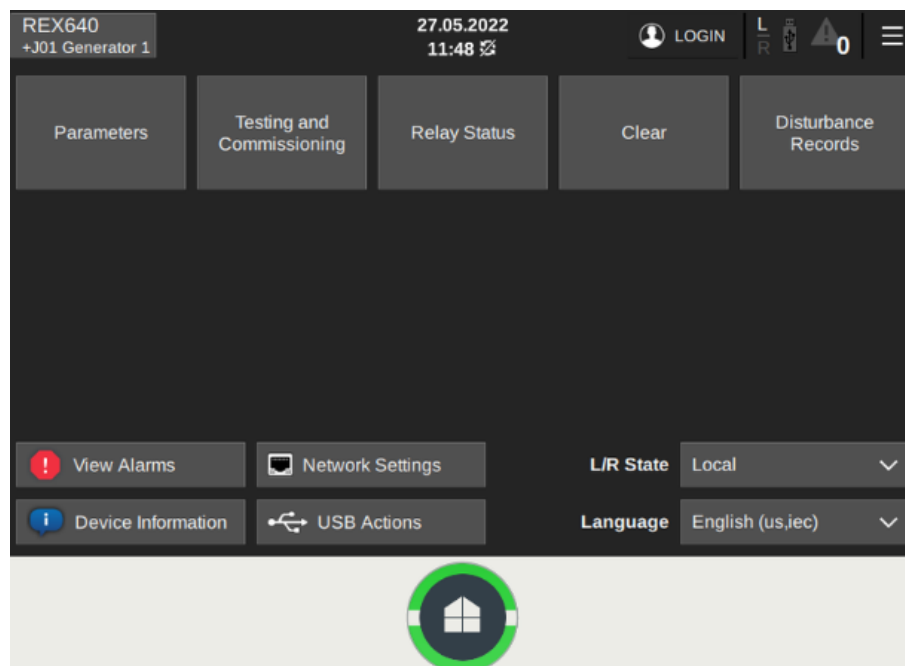


Figure 5: Engineer pages menu

3.4 Switchgear HMI

The SHMI is used for setting, monitoring and controlling up to 20 REX640 protection relays and the related processes. It comprises a 7-inch color screen with capacitive touch sensing and a Home button at the bottom of the SHMI. All features of standard HMI are also available in the SHMI.



The SHMI is an accessory for the relay which is fully operational even without the SHMI.

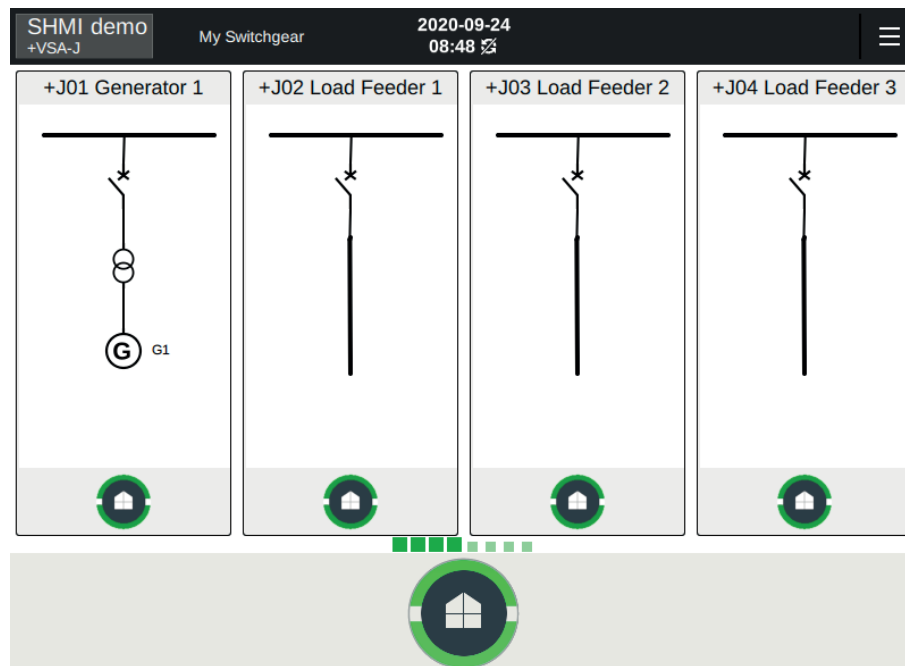


Figure 6: Example of a switchgear HMI navigation page

The SHMI has a navigation page which presents the physical switchgear lineup installation and indicates the status of each REX640 within the system. The area presenting a single switchgear bay has a small user-configurable bay overview section and a virtual Home button showing the status of the connected relay. By tapping the selected bay overview area, the SHMI connects with the related REX640 and works as normal LHMI for that relay.

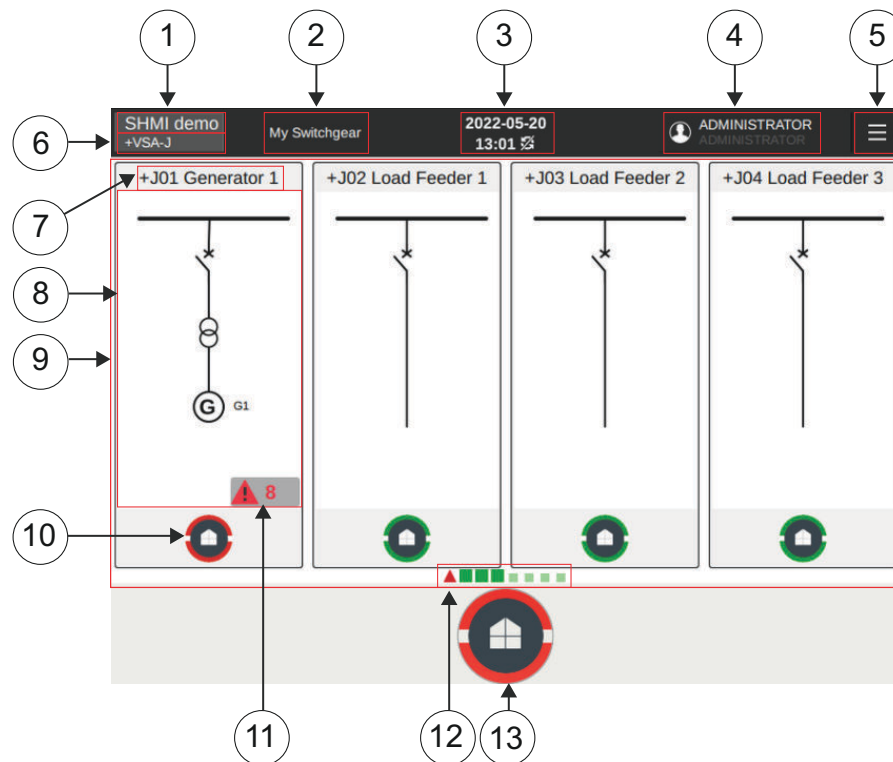


Figure 7: Navigation page elements

- 1 User-defined substation name
- 2 User-defined name for the switchgear or sub-part of switchgear lineup controlled by the SHMI
- 3 Date, time and time synchronization status
- 4 Logout button and authentication status
- 5 Menu button
- 6 User-defined voltage level name
- 7 User defined bay name and voltage level extension
- 8 Bay overview area showing static or dynamic information for a bay and functioning as a navigation point to launch the HMI view for the respective relay, user-defined content
- 9 SHMI navigation page
- 10 Virtual Home button representing the status of the respective relay's physical Home button
- 11 Number of active alarms
- 12 Panel lineup overview showing the current status of all connected relays and the current position of navigation page
- 13 SHMI's physical Home button

3.4.1 Bay overview area

Bay overview area consists either of a static picture or a dynamic SLD. They are configured with Graphical Display Editor in PCM600. One relay can have two overview pages.

Static picture may be, for example, a drawing or a photo of switchgear lineup. Maximum size of the picture is 186 × 320 px.

SLD does not support control operations. The following features are available.

- Static symbols such as connections, measurement devices, transformers and reactors
- Dynamic status for switching devices, but no control operations
- Dynamic and static text objects
 - Boolean state text
 - Integer state text
 - Label (translation not supported)
 - Numeric value
 - String value
- Custom symbols
- Busbar coloring

3.4.2 Physical and virtual Home buttons

On the SHMI navigation page, the virtual Home button shows the status of each relay as it would be shown with the physical Home button on a normal LHMI panel. In normal situations, the virtual Home button shows a steady green light. All other situations in which the relay requires operator's attention are indicated with a flashing light, a red light or a combination of these.

SHMI's physical Home button has two operation modes.

- On the SHMI navigation page, the Home button indicates the combined status of all connected relays. If multiple relays have different statuses, the Home button shows the indication with the highest priority.
- On the HMI view, the Home button indicates the status of the respective relay as described in [Table 2](#).

3.4.3 Navigation

Navigation page is the default view for the SHMI. The navigation page shows bay overviews areas which are lined up to represent the actual panel installations. The navigation page can be scrolled by swiping the screen horizontally or by pressing the physical Home button to move the page from left to right one bay overview at a time.

Bay overview area is the configured view for one relay. It may show static or dynamic information but all control operations are disabled. The whole bay overview area works as a navigation point to the relay's HMI view. Tapping this area opens the HMI view of the respective relay.

Panel lineup overview shows the position of the navigation page by highlighting the visible bay overviews. It also shows the status of all connected relays and helps in

identifying which relay requires operator's attention when the bay overview is not visible on the navigation page.

When the HMI view is opened for a relay, the SHMI works exactly like a normal HMI. All the same features are available, and the Home button switches between the configured home pages and indicates the alarm status for the respective relay.

Navigation area on the top left corner of the HMI view is used to navigate back to the SHMI's navigation page. The navigation area shows the bay name on the button to identify which relay's HMI is open.

3.5 HMI communication ports

The relay communication module has a dedicated port where the LHMI is connected using an RJ-45 connector and a CAT 6 S/FTP galvanic cable. The HMI can be connected to the relay also via station communication network if a longer distance is required between the relay and the HMI.

Additionally, the HMI contains one Ethernet service port with an RJ-45 connector and one USB port. The service port can be used for the PCM600 connection or for WHMI connection. Data transfer to a USB stick is enabled via the USB port. By default the USB port is disabled and has to be taken into use with a specific parameter.

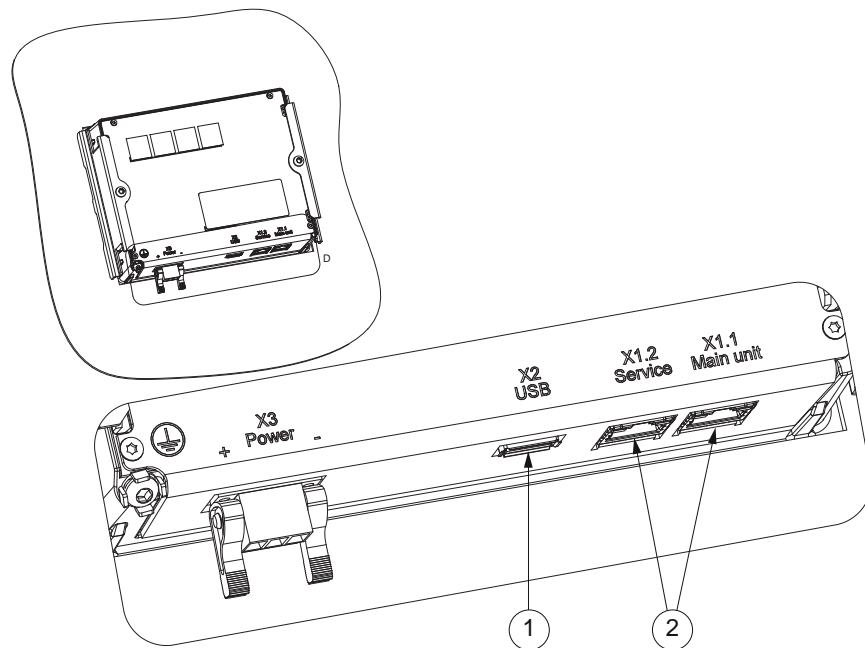


Figure 8: Local HMI connectors

- 1 USB port
- 2 RJ-45 ports

3.6 Web HMI

The WHMI allows secure access to the protection relay via a Web browser. The WHMI is verified with Google Chrome, Mozilla Firefox and Microsoft Edge.

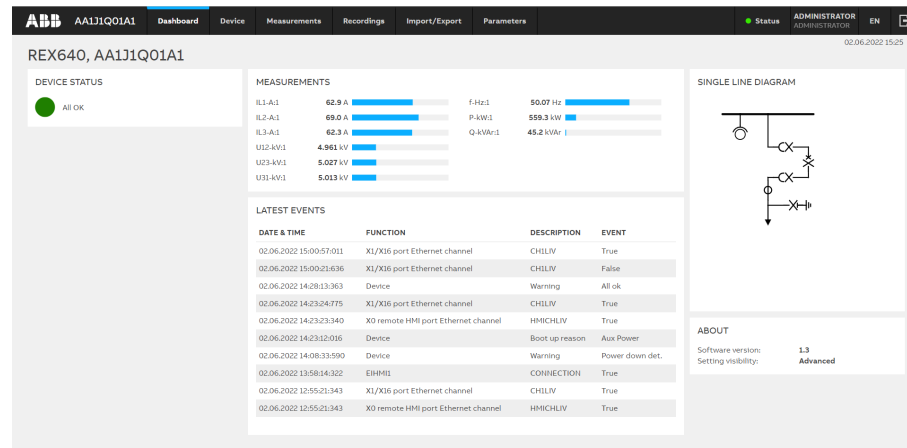


Figure 9: Example view of the Web HMI

WHMI offers several functions. The menu tree structure on the WHMI is almost identical to the one on the LHMI.

Table 4: Web HMI main groups and submenus

Main groups	Submenus	Description
Dashboard		Used to see an overview of the protection relay including status, measurements, single-line diagram and latest events
Device	Monitoring Information Self-supervision Single Line Diagram Clear Change Password About	Used to navigate to monitoring, information, self-supervision, single-line diagram or clear pages
Measurements	Measurements Phasor Diagrams	Used to navigate to the measurements or phasor diagrams
Recordings	Events Disturbance records Fault records Load Profile Record Alarm List	Used to view the events, disturbance records, fault records, load profile records and alarms
Import/Export	Report Summary Import/Export Settings Parameter List	Used to export a parameter list or a report summary, and to import and export settings

Table continues on the next page

Main groups	Submenus	Description
Parameters		Used to view the menu tree structure for the protection relay's setting parameters
Language selection		Used to change the language
Logout		Used to end the session

The WHMI can be accessed locally and remotely.

- Locally by connecting the laptop to the protection relay
- Remotely over LAN/WAN

3.6.1 Command buttons

Command buttons can be used to edit parameters and control information via the WHMI.

Table 5: Command buttons



















Name	Description
 Enable Edit	Enabling parameter editing
Disable Edit	Disabling parameter editing
	Filtering the parameter list view
Write to Relay	Writing parameters to the protection relay
 Refresh Values	Refreshing parameter values
 Print	Printing out parameters
Store Changes	Storing changes to protection relay's nonvolatile flash memory
Reject Changes	Rejecting changes
	Showing context sensitive help messages
	Going to the previous event page
	Going to the next event page
	Going to the last event page
	Going to the first event page
Clear from Relay	Clearing events
 Trigger Recording	Triggering the disturbance recorder manually

Table continues on the next page

Name	Description
 Export ▾	Saving values to TXT or CSV file format
 Freeze	Freezing the values so that updates are not displayed
 Continue	Receiving continuous updates to the monitoring view
 Delete	Deleting the disturbance record(s)
 Export	Saving the disturbance record files
View All	Viewing all fault records
 Clear All	Clearing all fault records
Import Settings	Importing settings
Export Settings	Exporting settings
Select All	Selecting all
 Refresh	Refreshing the parameter list view
Setting Group 1* ▾	Changing the visible setting group
Persisting Alarms	Viewing persisting alarms
Fleeting Alarms	Viewing fleeting alarms
Available Alarms	Viewing all available alarms
Acknowledge	Acknowledging the selected alarm
Select reference	Selecting reference phasor
20 per page ▾	Selecting events per page
Change	Changing the password
Cancel	Canceling the password change
	Logging out

3.7 User authorization

The user management for the protection relay can be handled in two possible ways. Only one user management way can be enabled in the protection relay at a time. For more information, see the cyber security deployment guideline.

Local user account management

Four factory default user accounts (VIEWER, OPERATOR, ENGINEER and ADMINISTRATOR) have been predefined for the LHMI and the WHMI, each with different rights and default passwords. The roles for these user accounts are the same as the username. Additional user accounts can be added for the protection relay.

IED Users in PCM600 is used to manage the user accounts. Each protection relay supports eight fixed roles and 50 user accounts belonging to any one of these roles. Each user account can be mapped to a maximum of eight roles.

The factory default passwords can be changed with Administrator user rights or by the users themselves. Relay user passwords can be changed using the LHMI, IED Users in PCM600 or the WHMI. Only Administrator can create user accounts and update the roles-to-rights mapping. Administrator can also reset the passwords of the users.

User authorization is disabled by default for the LHMI and can be enabled with the *Local override* parameter via the menu path **Configuration > Authorization > Passwords**. WHMI always requires authentication. Changes in user management settings do not cause the protection relay to reboot. The changes are taken into use immediately after committing the changed settings.

Central account management

The user accounts and roles can be created and authenticated centrally in a CAM server. CAM needs to be activated in the protection relay from Account Management in PCM600.

A CAM server can be an Active Directory (AD) server such as Windows AD. There can also be a secondary or redundant CAM server configured which can act as a backup CAM server if the primary CAM server is not accessible.

The protection relay is the CAM client and can maintain its own replica database of the user accounts and roles configured in the CAM server. This CAM replica database acts as a backup authentication mechanism if primary and secondary CAM servers are not accessible from the protection relay.

Each protection relay supports eight roles and 50 user accounts in the CAM replica database. Each user account can be mapped to a maximum of eight roles.



For more information on user management and security logging, see the cyber security deployment guideline.



For user authorization for PCM600, see the PCM600 documentation.

3.8 Station communication

Operational information and controls are available through a wide range of communication protocols including IEC 61850 Edition 2, IEC 61850-9-2 LE, IEC 60870-5-103, IEC 60870-5-104, Modbus® and DNP3. Full communication capabilities, for example, horizontal communication between the relays, are only enabled by IEC 61850.

The relay provides the possibility for a second IP address and a second subnetwork when the communication modules with three Ethernet ports (COM1001...1003) are used. However, only one IP network can be used as the default route. Using two IP addresses, communication networks can be separated based on the dominant user's needs. For example, one IP address can serve the dispatchers and the other one can serve the service engineers' needs.

The IEC 61850 protocol is a core part of the relay as the protection and control application is fully based on standard modelling. The relay supports Edition 2 and Edition 1 versions of the standard. With Edition 2 support, the relay has the latest functionality modelling for substation applications and the best interoperability for modern substations. The relay supports flexible product naming (FPN) facilitating the mapping of relay's IEC 61850 data model to a customer defined IEC 61850 data model.

3.9 PCM600

Protection and Control IED Manager PCM600 offers all the necessary functionality to work throughout all stages of the protection relay's life cycle.

- Planning
- Engineering
- Commissioning
- Operation and disturbance handling
- Functional analysis

The whole substation configuration can be controlled and different tasks and functions can be performed with the individual tool components. PCM600 can operate with many different topologies, depending on the project needs.



For more information, see the PCM600 documentation.

3.9.1 Connectivity packages

A connectivity package is a software component that consists of executable code and data which enable system tools to communicate with a protection relay. Connectivity packages are used to create configuration structures in PCM600. The latest PCM600 and connectivity packages are backward compatible with older protection relay versions.

A connectivity package includes all the data which is used to describe the protection relay. For example, it contains a list of the existing parameters, data format used, units, setting range, access rights and visibility of the parameters. In addition, it contains code which allows the software packages that use the connectivity package to properly communicate with the protection relay.

3.9.2 PCM600 and relay connectivity package version

- Protection and Control IED Manager PCM600 Ver. 2.12 or later
- REX640 Connectivity Package Ver. 1.3.0 or later



Download connectivity packages from the ABB Web site www.abb.com/mediumvoltage or directly with Update Manager in PCM600.

3.10 Modification Sales

Modification Sales is a concept that provides modification support for already delivered relays. Under Modification Sales it is possible to modify both the hardware and software capabilities of the existing relay. The same options are available as when a new relay variant is configured and ordered from the factory: it is possible to add new hardware modules into empty slots, change the type of the existing modules within the slots or add software functions by adding application and, if necessary, add-on packages. If it is needed to use the possibilities provided by the Modification Sales concept, please contact your local ABB unit.

4 Using HMI

4.1 Logging in

1. Once the HMI is connected to the relay, tap the **LOGIN** icon on the menu bar.



Figure 10: Logging in to local HMI

2. Acknowledge the login banner notification if displayed.

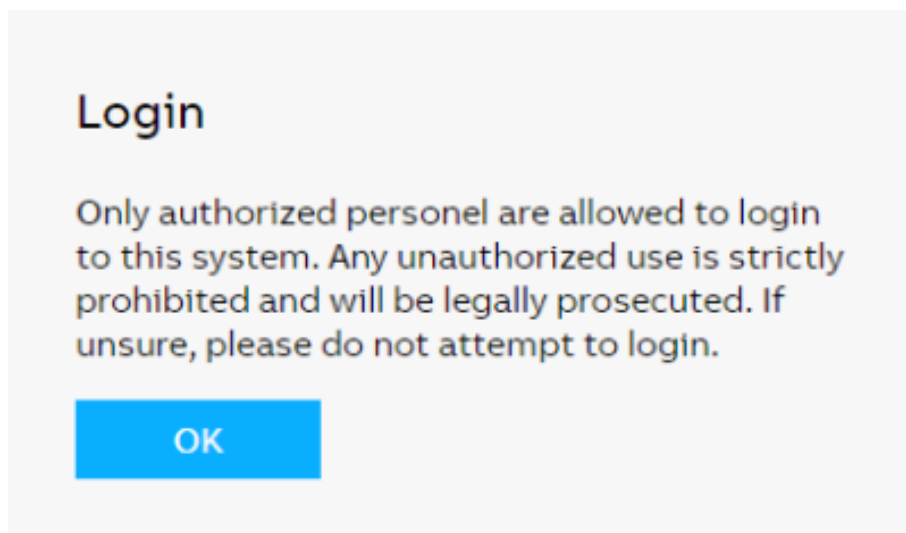


Figure 11: Login banner in local HMI



User Editable login banner provides a way to display a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s) as is required by IEC 62443-4-2 Component Requirement 1.12 System use notification.

3. Provide the username and password in the dialog box.



Keep the SHIFT key pressed for two seconds to switch from typing in lowercase to typing in uppercase, and vice versa.

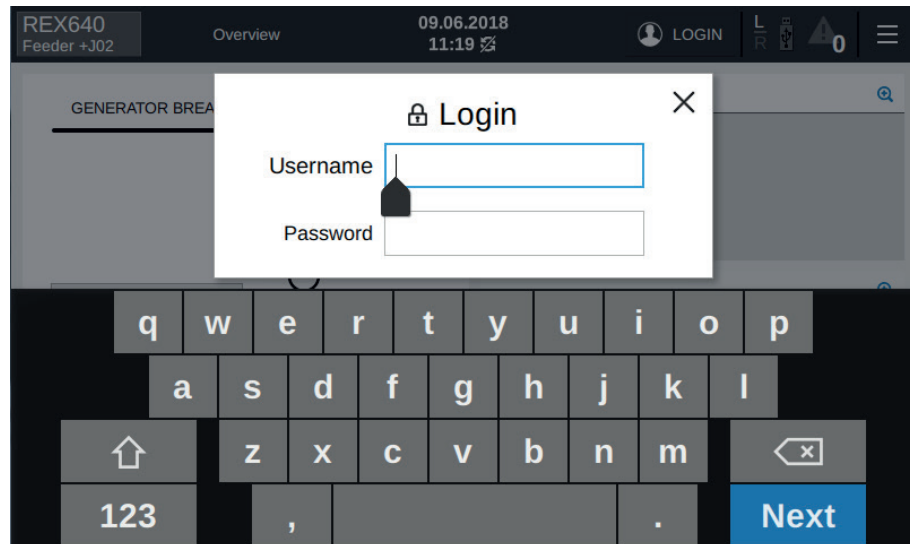


Figure 12: Providing the user credentials

The user is logged in to the protection relay and the username is displayed on the menu bar of the HMI.

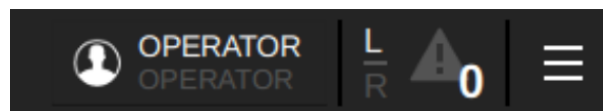


Figure 13: Logged in user



After a successful authentication to one relay, the SHMI tries to automatically log in to the other relays using the same username, password and role. If the login fails, username and password are asked again.

If the login fails because all sessions are in use, an error message is shown on the login page.

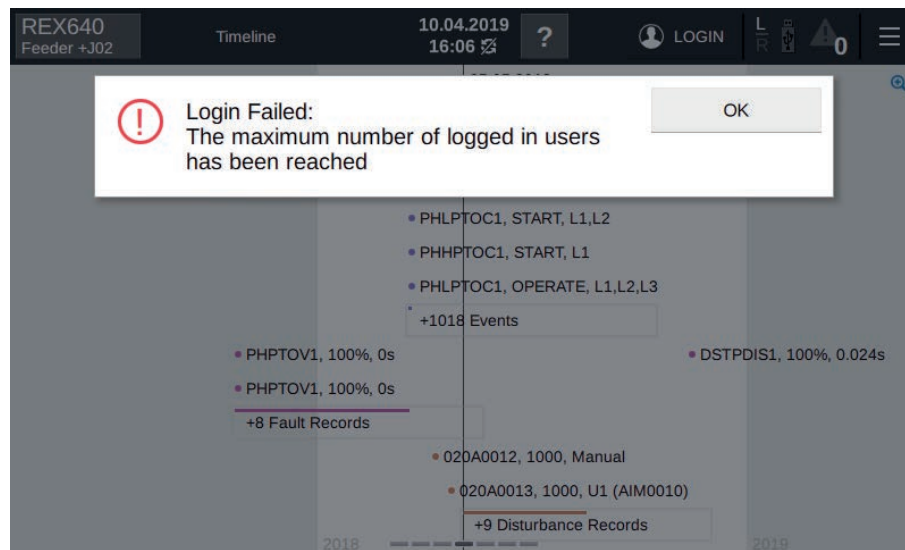


Figure 14: Local HMI error message

4.1.1 Managing forgotten password

If the ADMINISTRATOR password is lost and there is no user account available to be used for logging in to the protection relay, a one-time password can be generated.

1. Connect a computer to the HMI port of the protection relay.
2. Open a Web browser and go to <https://192.168.0.254/OTP.html>. (Note that default HMI port's IP address is used in this instruction, check e.g. from PCM600 project if it has been changed.)
3. Forward the displayed OTP related information to ABB's technical customer support to receive a one-time password.
4. Reset the ADMINISTRATOR password.
 - a) Open <https://192.168.0.254/OTP.html>. (Note that default HMI port's IP address is used in this instruction, check e.g. from PCM600 project if it has been changed.)
 - b) Type the ADMINISTRATOR username with capital letters.
 - c) Type the one-time password.
 - d) Click **Reset**.



Once the OTP is used to reset the protections relays' user accounts (that is, the user accounts are reverted to factory defaults), the previous Local User Account Management/CAM configuration is lost and needs to be reconfigured from the Account Management Tool in PCM600.

4.2 Logging out

1. Tap the username on the menu bar.

2. Tap **Log out**.

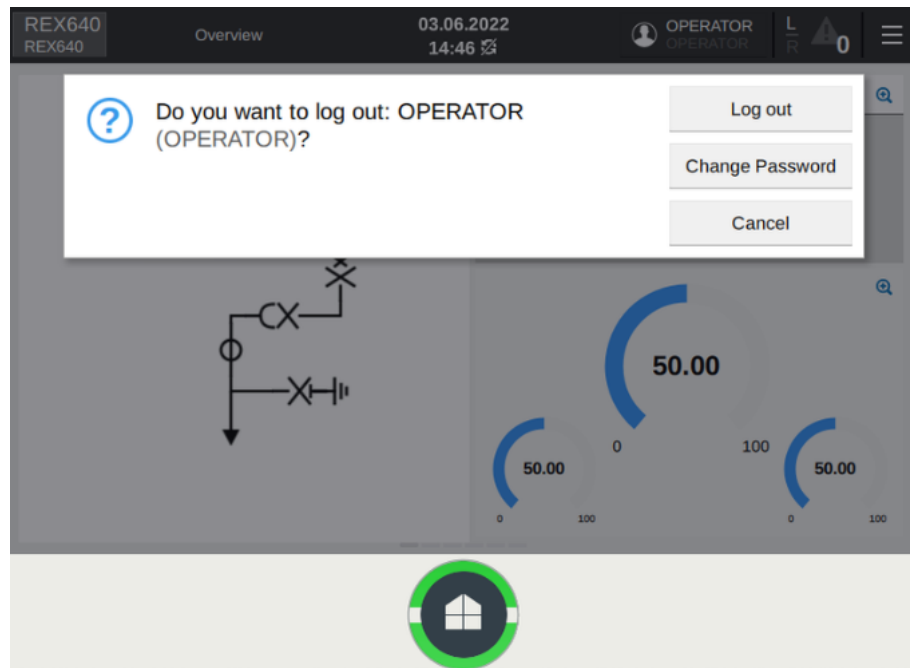


Figure 15: Logging out



Logging out from the SHMI automatically results in a logout from all of the connected relays.



Changing the password causes an immediate logout. Changing password is not available in the logout menu when the navigation page is open. Navigate to a relay and use the logout menu in the relay's HMI to change the password.



If the HMI and the protection relay have not been paired and there is no user activity for the duration set in **Configuration > Web HMI timeout**, the HMI session is logged out. By default, the timeout duration is three minutes.

4.3 Selecting local or remote use

In local position, the primary equipment, such as circuit breakers or disconnectors, can be controlled via the LHMI or SHMI when connected to a selected relay. In remote position, control operations are possible only from a higher level, that is from a control center.

The control position of the protection relay can be changed via the **Local > Remoted** dialog box.

1. Tap the menu button.
2. Tap the selection button alongside the **L/R State** text.

3. Select **Off**, **Local** or **Remote**.

By setting **Station authority** parameter, more choices such as **L+R** and **L+S+R** will become available.

In local position, the primary equipment, such as circuit breakers or disconnectors, can be controlled via the LHMI or SHMI when connected to a selected relay. In remote position, control operations are possible only from a higher level, that is from a control center.

Local/Remote control supports multilevel access for control operations in substations according to the IEC 61850 standard. Available options in Local/Remote dialog box depends on **Configuration > Control > General > Station authority**.

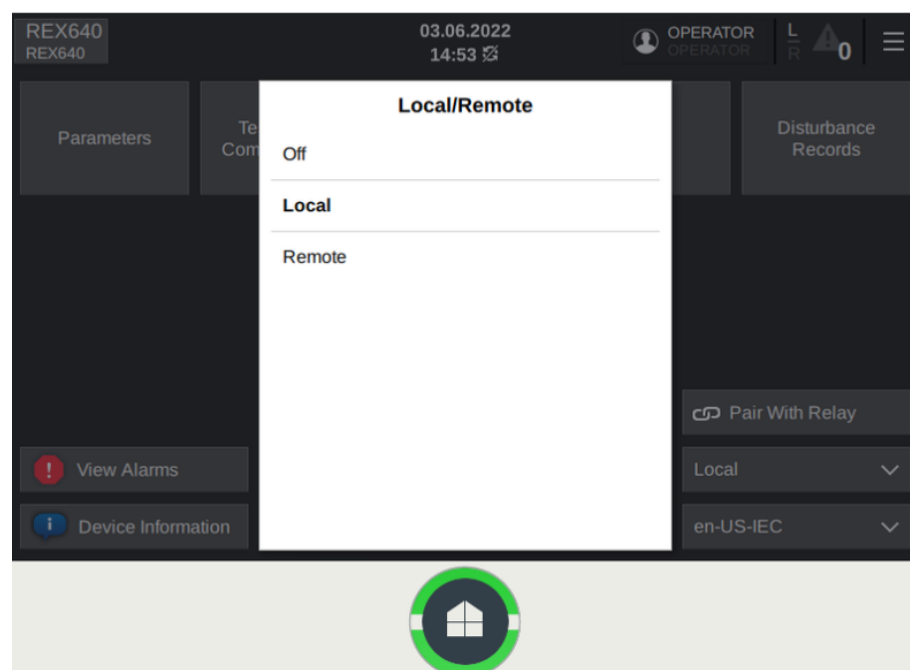


Figure 16: Selecting local or remote use



To control the protection relay, log in with the appropriate user rights.

4.4 Identifying device

1. Tap the menu button.
2. Tap **Device Information**. **Product Identifiers** are shown by default on the page.

3. Tap **HW modules** and select **Detached LHMI** to check the information of the LHMI.

<div> <div>REX640</div> <div>REX640</div> </div> <div>Device Information</div> <div> <div>03.06.2022</div> <div>14:57</div> </div> <div> <div>L R</div> <div>0</div> <div>≡</div> </div>	
Product identifiers	Type
Site identifiers	Product version
	Serial number
System identifiers	Production date
	SW version
HW modules	SW date
	SW number
Legal information	Interface level
	Order code
Composition code	
<div>HMI version:</div> <div>22-04-29-14:49D</div>	

Figure 17: Identifying device

4.5 Changing backlight brightness and timeout

1. Tap the menu button.
2. Tap **Parameters**.
3. Tap **Configuration** and then **HMI**.
4. Tap **Edit**.
5. Tap **Backlight brightness** value field.
6. Give the new value and tap **OK**.
7. Tap **Backlight timeout** value field to change the backlight timeout.

8. Give the new value and tap **OK**.

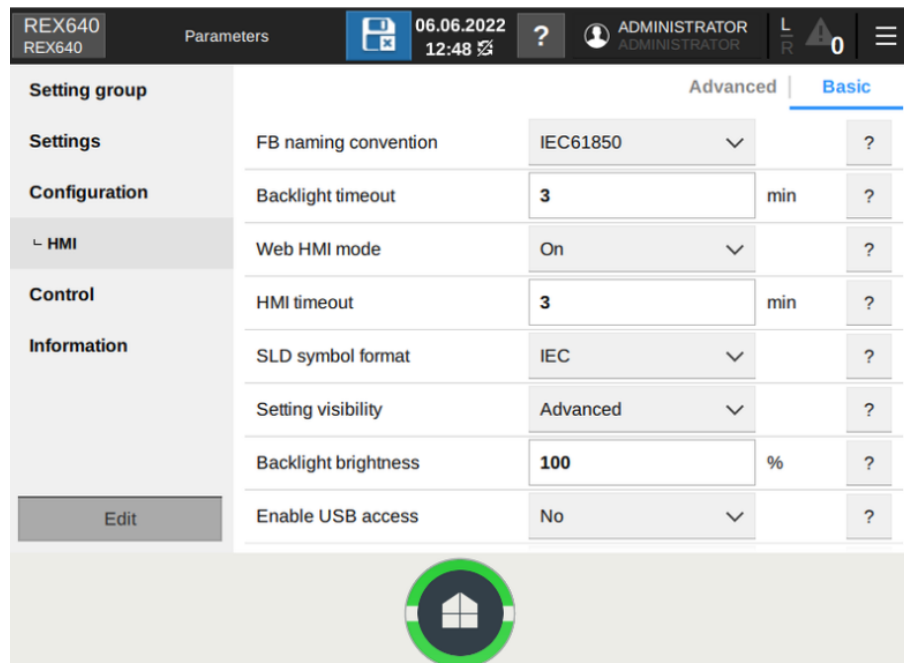


Figure 18: Changing backlight brightness

4.6 Changing setting visibility

1. Tap the menu button.
2. Tap **Parameters**.
3. Tap **Settings** from the left and select a function.

4. Tap **Advanced** or **Basic** on the upper right corner of the page.

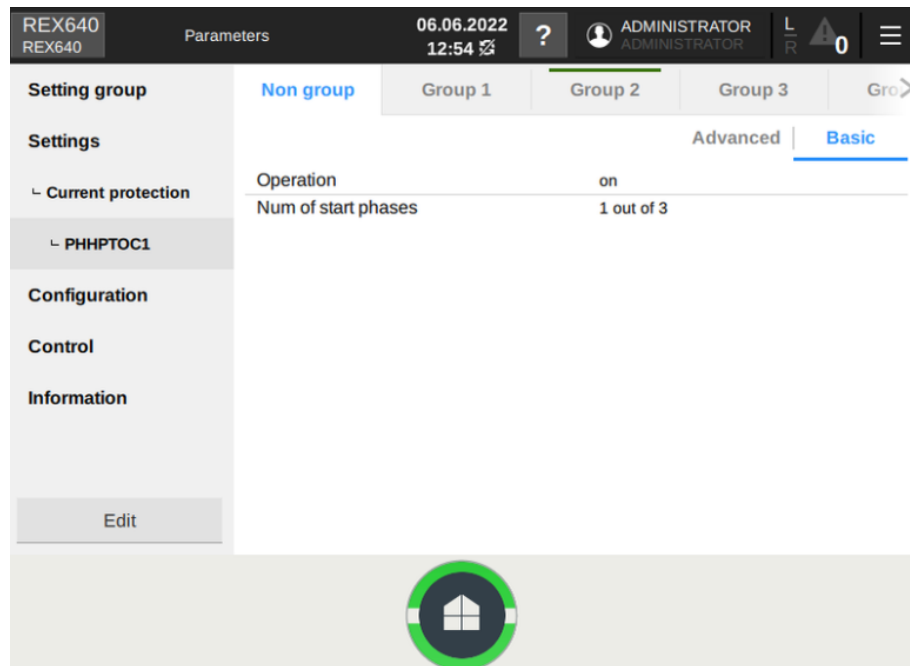


Figure 19: Changing setting visibility

4.7 Monitoring relay status

1. Tap the menu button.
2. Tap **Relay Status**.
3. In case of active internal fault or warning, tap **More Information**.

4. Tap **Monitoring** to open the monitoring menu.

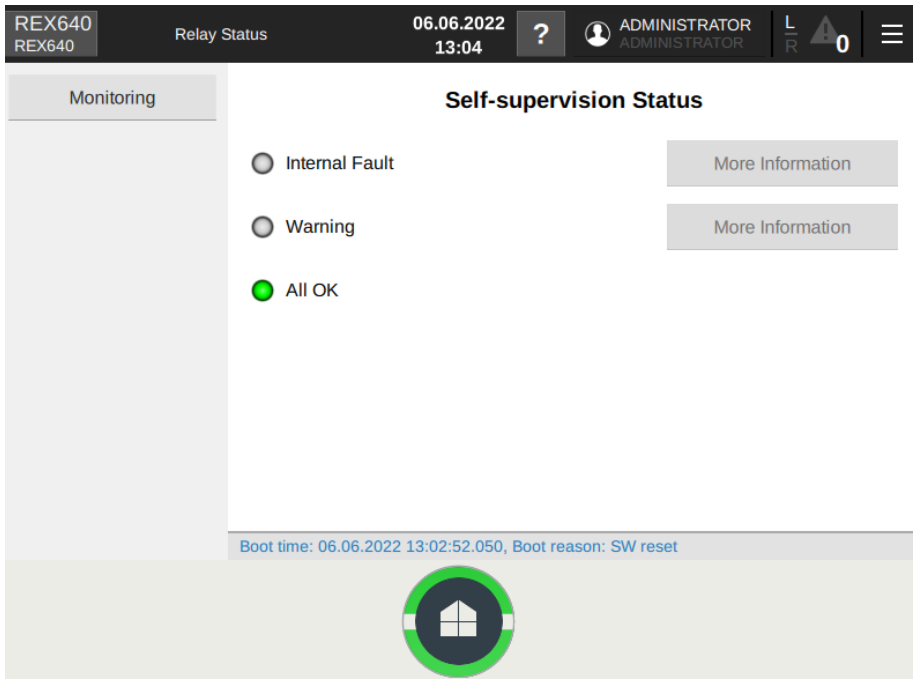





Figure 20: Selecting self-supervision

4.7.1 Switchgear HMI status indications

In the panel lineup overview, a green square indicates a healthy state and a red triangle the states that require operator's attention.

Table 6: Status icons

Status icon	Description
	Normal relay status
	The relay has alarms or some other state that requires operator's attention.
	Connection to relay is lost or the relay is not trusted.

Physical Home and virtual Home button indications behave identically although the physical Home button shows a combination of home buttons for each connected relay. When relays have different statuses, the physical Home button shows the status with the highest priority.

Table 7:









Status	Priority	Home button	Overview	Acknowledged
Relay's IRF activated	5	High frequency flashing red ¹		N/A
Relay set to test mode	4	Low frequency flashing green ²		N/A
Process related alarm active	3	Low frequency flashing red		No
Process related alarm active	2	Steady red ²		Yes
Process related alarm that has been active earlier but is currently inactive.	3	Low frequency flashing red ²		No
Communication lost between a relay and the SHMI	1	High frequency flashing green ¹		N/A
Process related alarm that has been active earlier but is currently inactive.	0	Steady green		Yes

Table continues on the next page

¹ High frequency = 3 Hz

² Low frequency = 1 Hz

Status	Priority	Home button	Overview	Acknowledged
Relay under normal operation and connected to the SHMI	0	Steady green		N/A

4.8 Changing language

1. Tap the menu button.
2. Tap **Language** on the lower right corner of the page.
3. Select a language from the list.

4.9 Alarms

4.9.1 Viewing alarm list

The Home button flashing a red light indicates at least one alarm is active or unacknowledged.

- Open the alarm list in one of the alternative ways.
- If the LHMI is in sleep mode, tap the Home button to open the alarm list page.
- If the LHMI is active, tap the **Alarms** section on the **Overview** page or tap the menu button and select **View Alarms**.



The SHMI always opens to a navigation page. An alarm page is opened if the user navigates to a relay with an alarming status.

4.9.2 Acknowledging alarms

On the **Alarms** page there are three list groups.

- Persisting alarms: Alarms that are still active
- Fleeting alarms: Alarms that are not active anymore, but have not been acknowledged
- Available alarms: Overview of all events predefined as alarms with status and latest time stamp

More information about an alarm can be seen by tapping the alarm row.

1. Select the alarms in one of the alternative ways.
 - Select one or multiple alarms by tapping the check boxes.
 - Select all alarms by tapping **Select All**.
2. Tap **Acknowledge**.



Lockout or latched trip can also be reset on this page by tapping **Reset Trip**.



When a persisting alarm is acknowledged, it does not disappear from the list until the cause of the alarm is resolved.

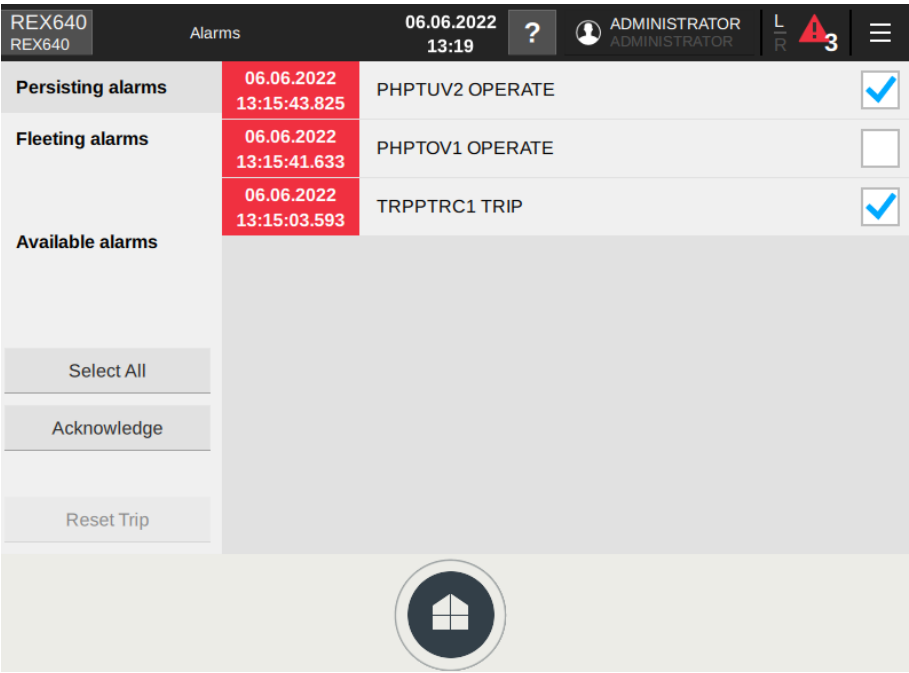


Figure 21: Acknowledging alarms

4.10 Measurements and phasor diagrams

4.10.1 Viewing measurements

The **Measurements** page is usually one of the Operator pages.

1. Swipe the LHMI screen until the **Measurement** page is shown. The number of measurements on the **Measurement** page depends on the LHMI configuration made with GDE. If there are more measurements configured than fitting on the screen at a time, a vertical scroll bar is shown on the right of the measurement list window.
2. Swipe the list vertically to see the remaining measurements. If configured with GDE, warning or alarm limits are indicated in the individual measurement bars with dash or solid lines. Measurement with bad quality is shown by grey value in parentheses.

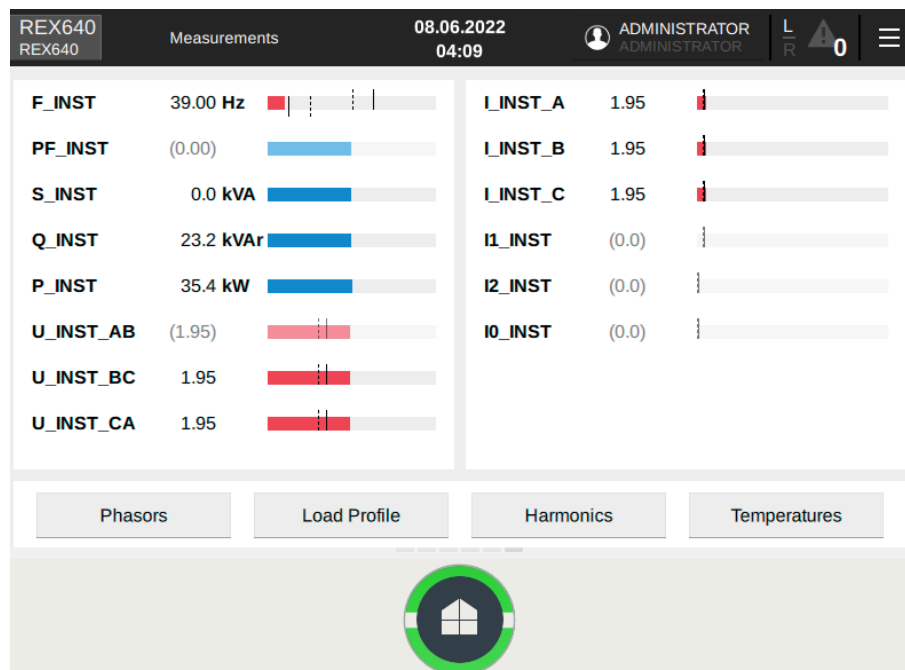


Figure 22: Measurements page

4.10.2 Viewing phasor diagrams

Phasor diagrams can be found through the **Measurements** page.

1. Tap **Phasors** at the bottom of the page.

- If more than one phasor diagram page are available, select one from the list opened.

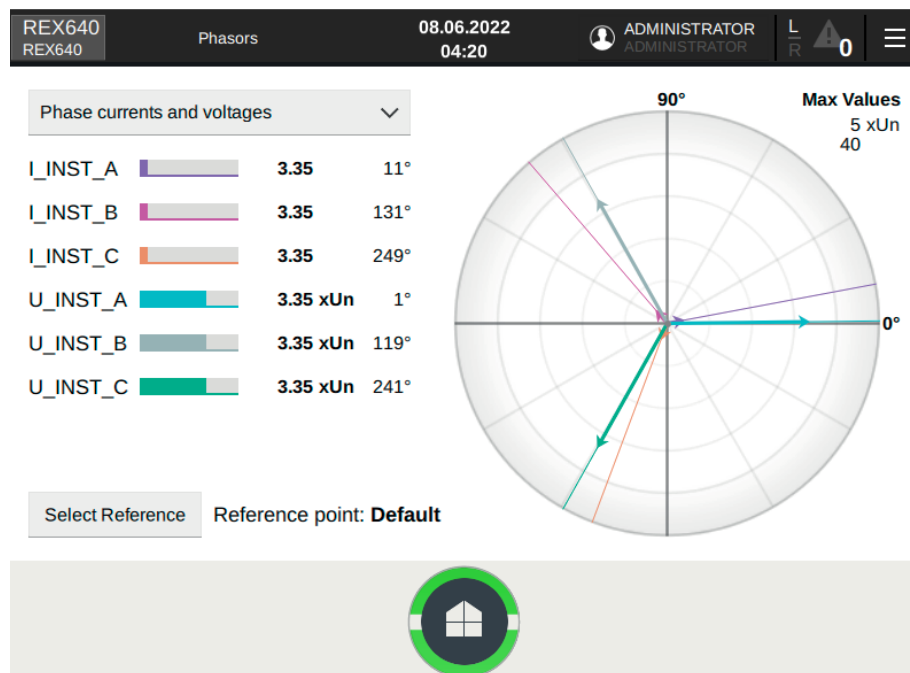


Figure 23: Phasors page

4.11 Showing parameters

- Tap the menu button.
- Tap **Parameters**.

- 3. Tap Settings from the left and select a function.

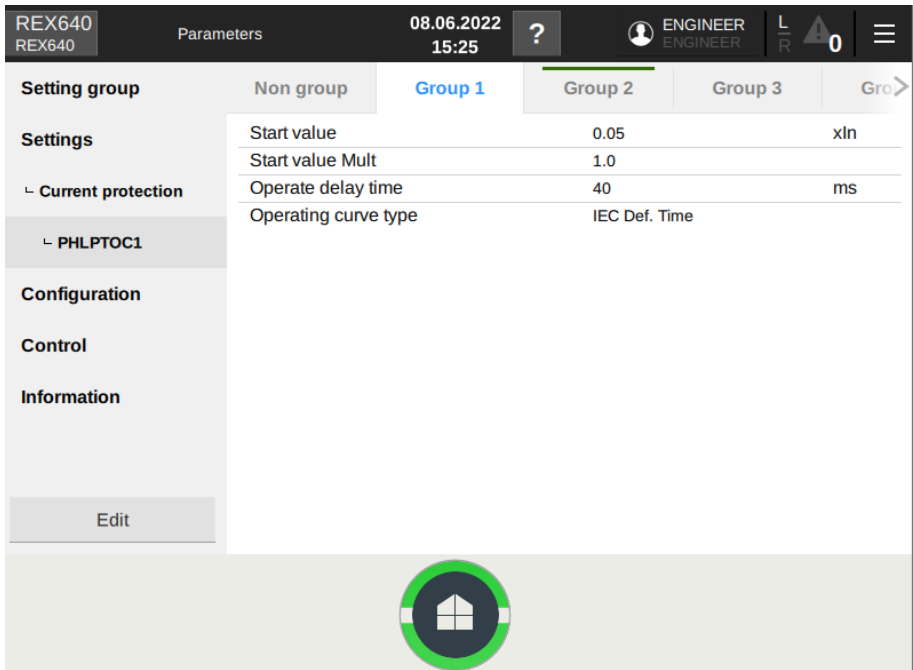


Figure 24: Showing parameters

4.11.1 Viewing Protection Characteristics

- 1. Navigate to **Parameters** > **Settings**.
- 2. Select protection function to enter to parameter page.
- 3. Tap **Characteristics** button to show function characteristics.
- 4. Tap **Characteristics** button to return to parameter page.

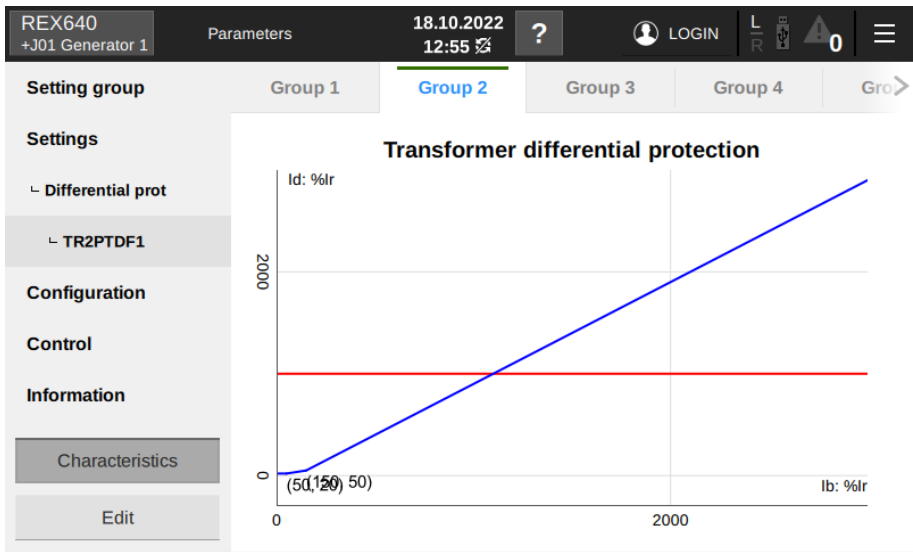



Figure 25: Setting Characteristics

4.12 Editing values

1. Tap **Edit** on the lower left corner of the page to activate the edit mode. A blinking  icon on the menu bar indicates that the edit mode is active.
2. Enter a value and tap **OK**.

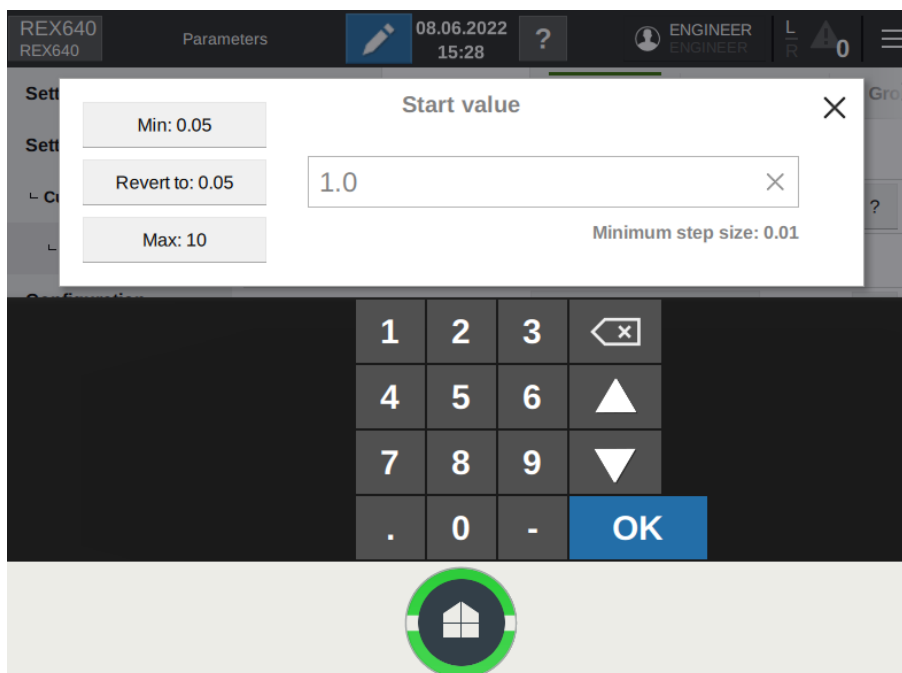


Figure 26: Entering a numeric value

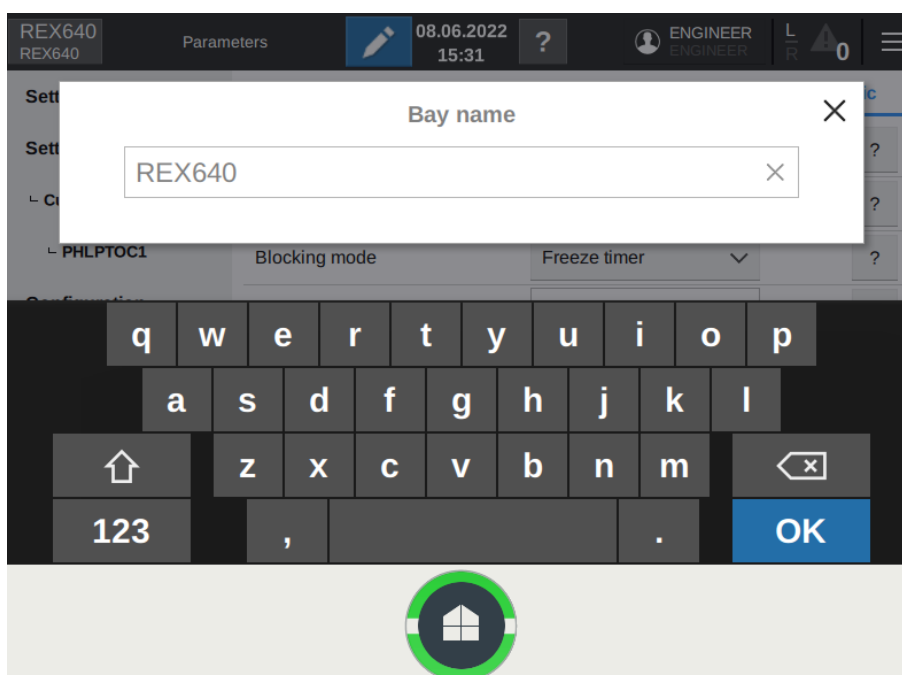



Figure 27: Entering an alphanumeric value

4.13 Committing settings

The blinking  icon on the menu bar indicates that at least one parameter value has been changed and storing to the nonvolatile memory is required.

1. Tap the  icon or **Edit** button.

2. Tap **Store**, **Reject** or **Cancel** in the dialog box that opens. Tapping **Reject** exits the edit mode without storing the values to the nonvolatile memory. Tapping **Cancel** closes the dialog box and returns to parameter editing.

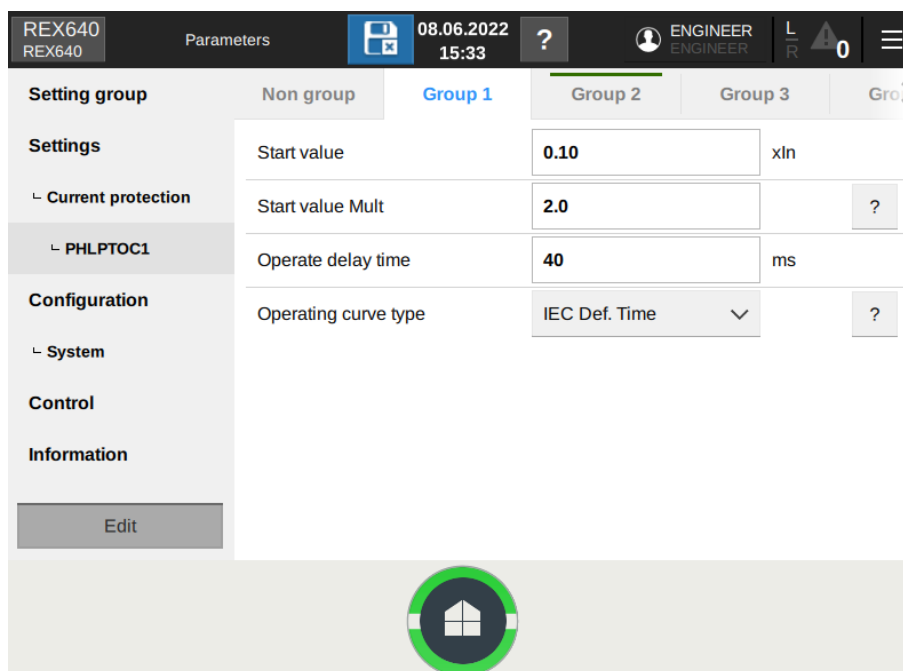


Figure 28: Storing required indication on the menu bar

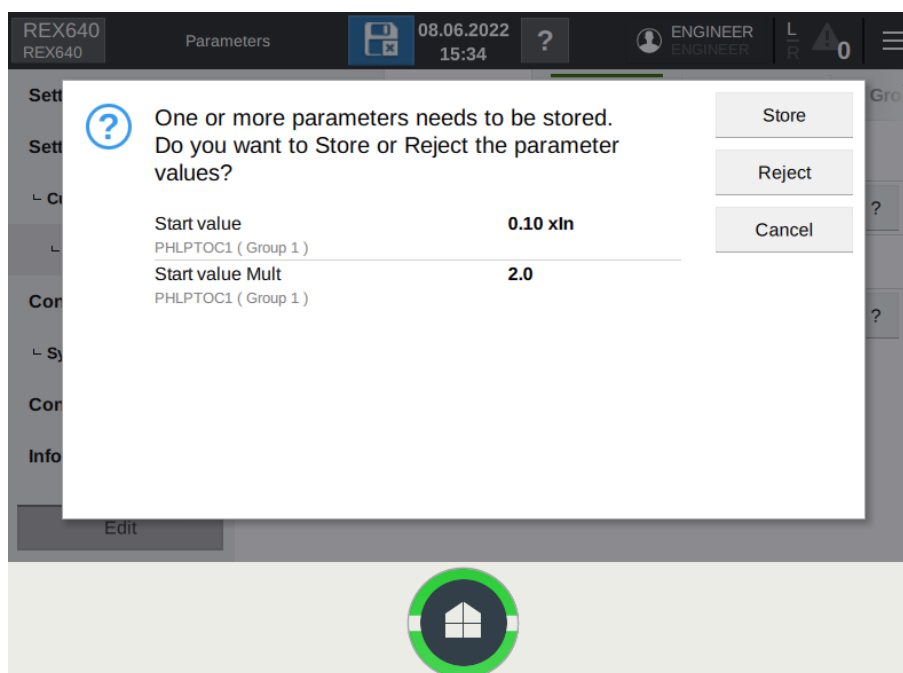


Figure 29: Storing or rejecting parameter changes

4.14 Clearing and acknowledging

1. Tap the menu button.
2. Tap **Clear**.
3. Select the items to be cleared or acknowledged by tapping the corresponding rows. Swipe the list vertically to scroll up and down.
4. Tap **Clear from Relay** to clear or acknowledge the selected items.

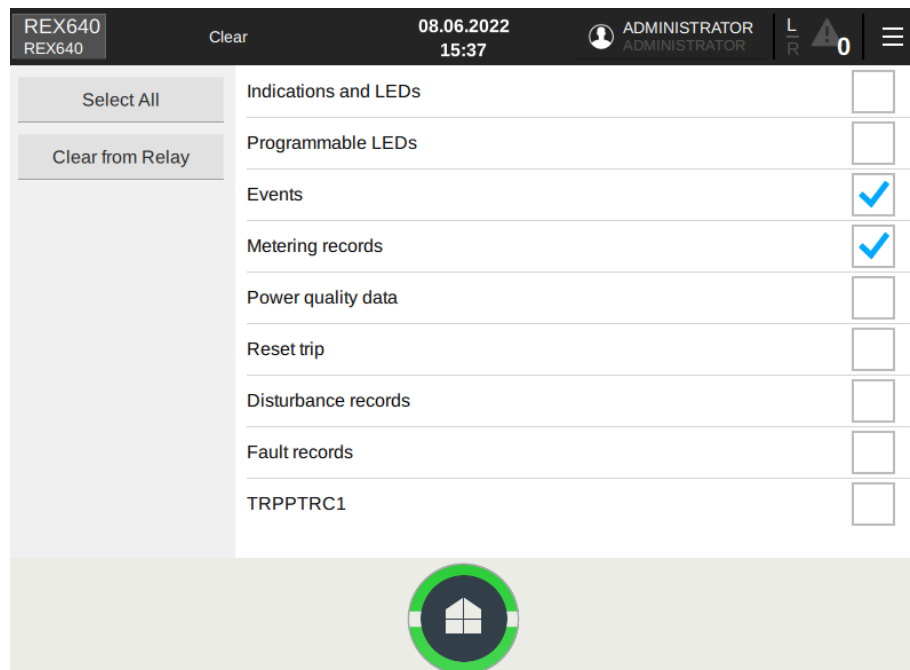


Figure 30: Clearing and acknowledging

4.15 Accessing disturbance records

1. Tap the menu button.
2. Tap **Disturbance Records**.
3. Select the records to be saved to USB or deleted by tapping the corresponding rows. Swipe the list vertically to scroll up and down.

4. Tap **Save to USB** to save the selected records to the USB memory.



Save to USB is not activated until a USB memory is connected to the USB port of the HMI.

REX640 REX640	Disturbance Records	08.06.2022 15:47	ENGINEER ENGINEER	L R	0	≡
Select All	Date & Time	Name	Length	Reason		
Delete Selected	08.06.2022 15:46:55.815	020A0011	1000	Manual	<input checked="" type="checkbox"/>	
Save to USB	08.06.2022 15:46:54.320	020A0010	1000	Manual	<input checked="" type="checkbox"/>	
Safely Remove USB	08.06.2022 15:46:52.925	020A0009	1000	Manual	<input type="checkbox"/>	
	08.06.2022 15:46:51.455	020A0008	1000	Manual	<input type="checkbox"/>	
	08.06.2022 15:46:49.850	020A0007	1000	Manual	<input type="checkbox"/>	
	08.06.2022 15:46:40.145	020A0006	1000	Manual	<input type="checkbox"/>	
	08.06.2022 15:46:38.423	020A0005	1000	Manual	<input type="checkbox"/>	
Trigger Recording	08.06.2022 15:46:36.938	020A0004	1000	Manual	<input type="checkbox"/>	
Recordings: 11, remaining: 89/100, memory used: 2%						

Figure 31: Selecting disturbance records



Tap **Trigger Recording** to manually trigger a recording.

4.16 Viewing fault records

The **Fault Records** page is usually one of the Operator pages.

1. Swipe the LHMI screen until the **Fault Records** page is shown. The fault records stored in the relay are listed by time stamps on the left of the page.

2. Tap the time stamp in the list to see the data of the record. Both the fault records list and the data window can be scrolled up and down by swiping vertically the corresponding section of the page.

REX640

REX640

FaultRecords

08.06.2022

15:52

ENGINEER

ENGINEER

L

R

0

≡

21.03.2018 14:20:37	Fault number	4	
	Time and date	21.03.2018 14:20:37.175	
21.03.2018 14:18:43	Protection (rec. set 1)	PHLPTOC1	
	Protection (rec. set 2)	None	
01.02.2018 05:03:24	Start duration	100.00	%
	Operate time	0.000	s
06.12.2017 00:17:45	Breaker clear time	(3.000)	s
	Fault distance	(0.00)	pu
08.11.2017 00:17:32	Fault resistance	(0.00)	ohm
	Fault reactance	0.0	ohm
24.10.2017 16:50:11	Active group	1	
	Shot pointer	1	
24.10.2017 16:40:30	Max diff current IL1:1	0.000	pu
	Max diff current IL2:1	0.000	pu
24.10.2017 16:30:22	Max diff current IL3:1	0.000	pu
	Diff current IL1:1	0.000	pu
	Diff current IL2:1	0.000	pu
	Diff current IL3:1	0.000	pu

Clear All

Figure 32: Fault records page

4.17 Selecting USB actions

The **USB Actions** page enables exporting various data from the relay.

Device information, events, fault records, parameters and the alarm list are saved in TXT format.

Disturbance records and load profile record files are saved in CFG and DAT formats.

1. Tap the menu button.
2. Tap **USB Actions**.
3. Select the data to be saved to USB by tapping the corresponding rows.

4. Tap **Save to USB**.



The USB port of the LHMI is disabled by default. To be able to access the USB actions page, the USB port needs to be enabled by the parameter *Enable USB access* via **Parameters** > **Configuration** > **HMI**.



Save to USB is not activated until a USB memory is connected to the USB port of the HMI.



The supported file systems for the USB memory are FAT, FAT32, NTFS, EXT2, EXT3 and EXT4.

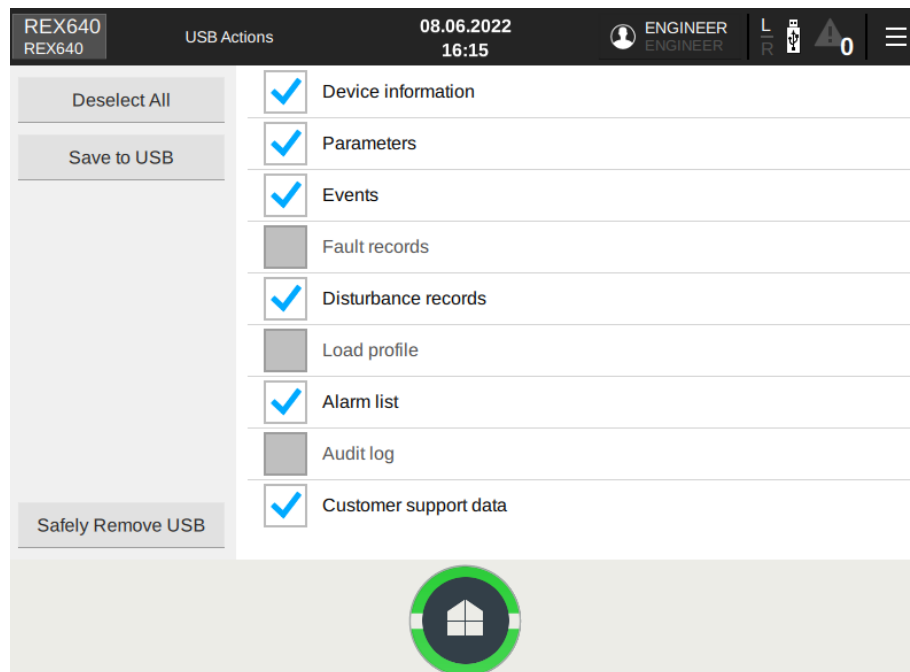



Figure 33: USB Actions page

4.18 Using local HMI help

There are two levels of help on the LHMI.

- Help for a specific page
- Help for a specific parameter on the **Parameters** page and for some specific monitored data on the **Monitoring** page
- Access the LHMI help in one of the alternative ways.
 - Tap the button on the menu bar to access the page-specific help. This help button is visible only when there is help available for a page.
 - Tap the button at the end of a parameter or monitored data row to access parameter or monitored data specific help.



The edit mode needs to be activated to see the  buttons on the **Parameters** and **Monitoring** pages.

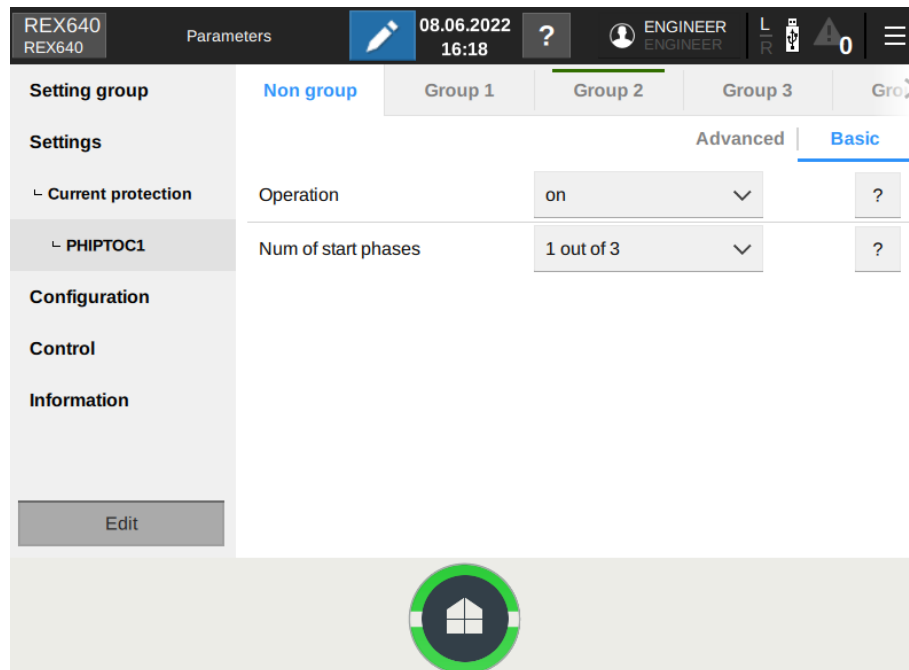



Figure 34: Page help and parameter help buttons

4.19 Changing setting group

1. Tap the menu button.
2. Tap **Parameters**. Setting group list is opened by default.
3. Tap **Edit**.
4. Select the group by tapping the corresponding row and tap **Set Active**.
5. Tap the  icon or **Edit**.

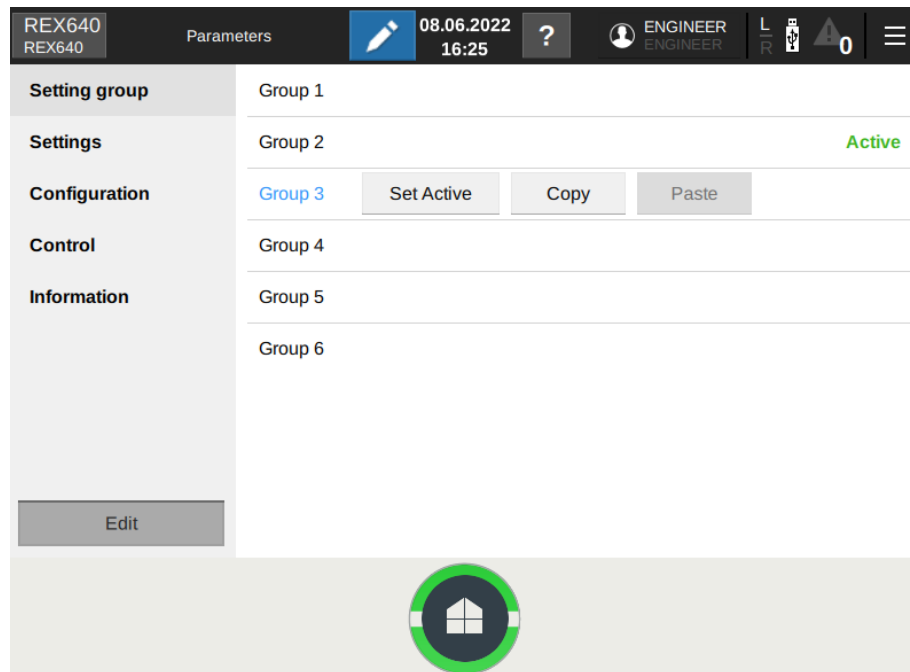
6. Tap **Store**.

Figure 35: Selecting active setting group

4.20 Controlling

Controllable objects, such as circuit breakers, disconnectors and earthing switches, can be opened and closed via the single-line diagram.

1. Tap the object in the single-line diagram to select it.

2.

Tap  to open or  to close the selected object.

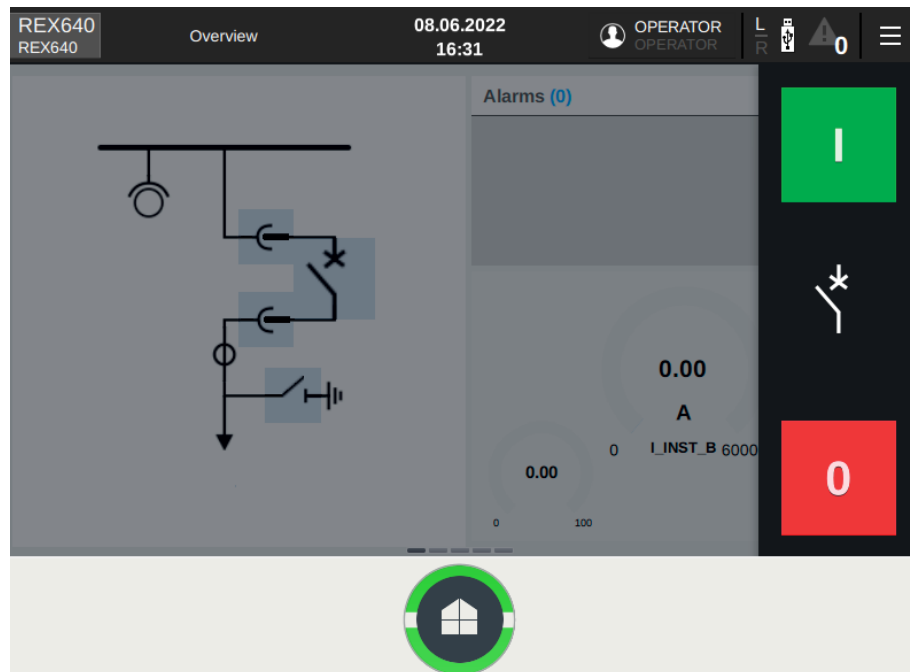



Figure 36: Selecting object (circuit breaker) and control buttons



An interlocked object is indicated by the padlock symbol  in the single-line diagram.

If the parameter *Breaker operation* in **Configuration > Control > HMI** is set to "After confirmation", a confirmation dialog box opens after tapping the control button. The confirmation dialog box has a progress bar indicating the *Select timeout* set for the controllable object. If the *Control mode* setting of a control function is set to "sbo-with-enhanced-security", the confirmation dialog box always opens regardless of the *Breaker operation* setting value.

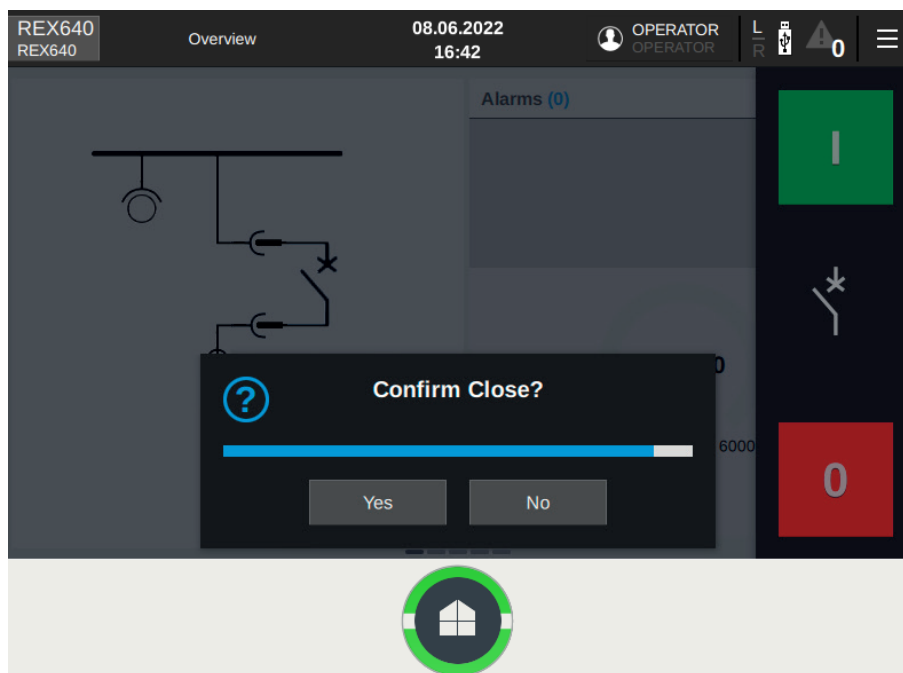


Figure 37: Confirming object closing



Control operations cannot be executed from the SHMI navigation page. Navigate to the HMI view to perform control operations.

If the parameter *Close delay mode* in **Configuration > Control > LHMI** is set to "In use", a timer is started after tapping the close button and accepting the possible confirmation dialog. Close operation is performed only after the timer reaches zero. Remaining time is displayed on top of close button, user can cancel the operation during countdown by tapping the Cancel button. The delay time can be configured by setting *Close delay* parameter in **Configuration > Control > LHMI**.

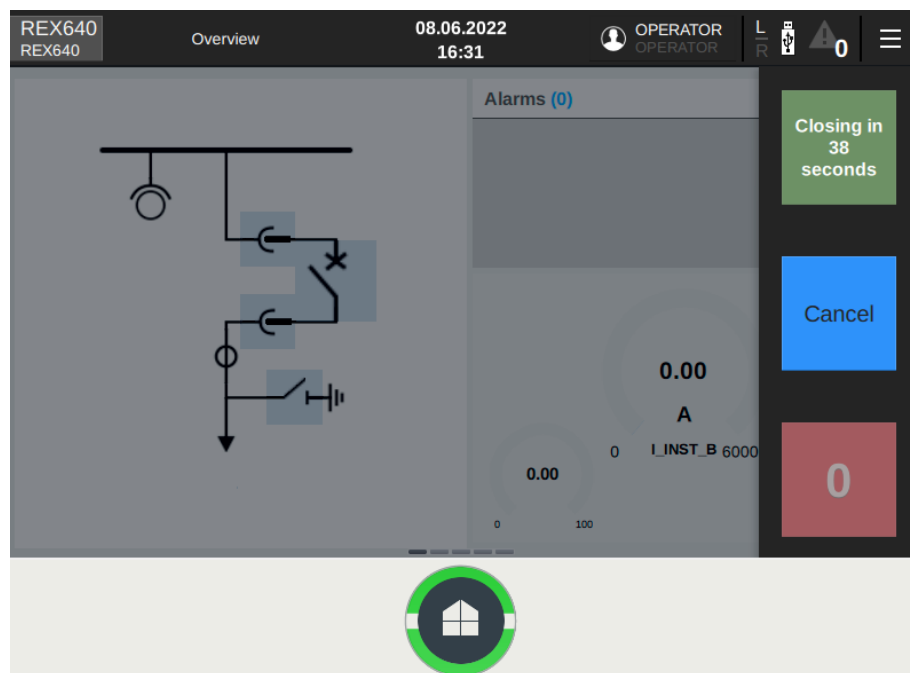


Figure 38: Closing circuit breaker with a delay

4.21 Bookmarking pages

A bookmark can be created to any page on the LHMI. Maximum six bookmarks can be created.

1. Navigate to the page to be bookmarked.
2. Touch the Home button for one second to open the **Bookmarks** page.
3. Tap any **Bookmark the active page** icon to store the bookmark for the selected page.
4. On any page, touch the Home button for one second to open the Bookmarks page.
5. Use the bookmarks in one of the alternative ways.
 - a) Tap the bookmark icon for the page to be opened.
 - b) Drag the bookmark icon onto the trash can symbol to remove the bookmark.



To go to the Home page from any page, touch the Home button for one second and tap the **Go to Home** symbol of the Bookmarks page.

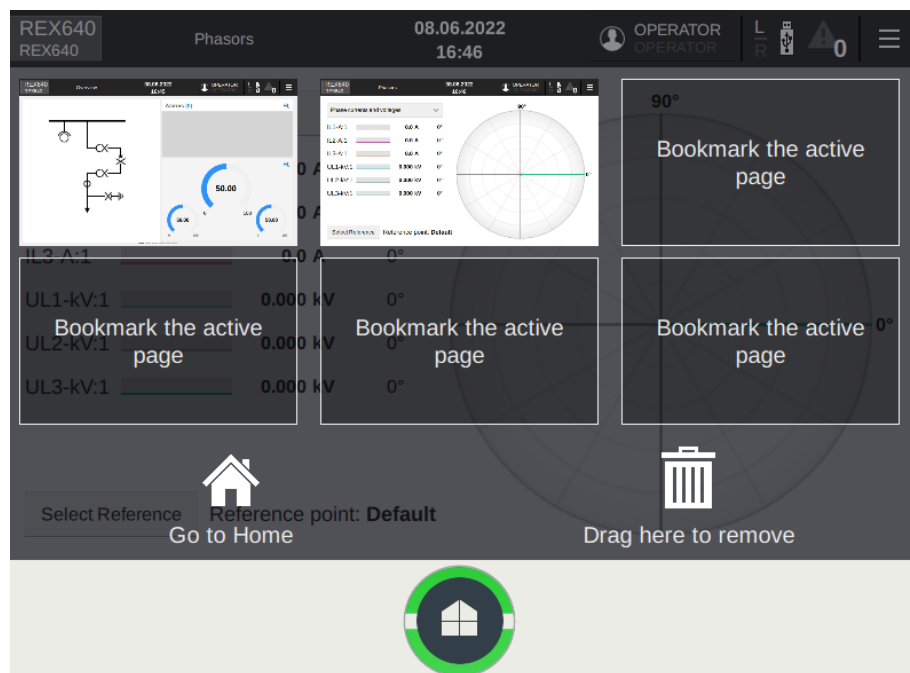


Figure 39: Bookmarking pages

5 Using Web HMI

5.1 Connecting to Web HMI

Connection to WHMI can be established using different communication card ports or the LHMI service port. WHMI is disabled by default and can be enabled with a setting parameter. As only secure communication is supported for the WHMI, it must be accessed from a Web browser using the HTTPS protocol. Three simultaneous LHMI and WHMI sessions are supported.

1. To enable the WHMI, select **Configuration > HMI > Web HMI mode** and set the parameter to "On".
2. Reboot the relay for the change to take effect.
3. Log in with the proper user rights to use the WHMI.

If the WHMI is accessed through the LHMI service port, use the corresponding IP address of the relay communication port. The IP address can be obtained via the Engineer pages. Tap the relay's name on the LHMI menu bar to open the Relay address dialog box.



To establish a remote WHMI connection to the protection relay, contact the network administrator to check the company rules for IP and remote connections.



HTTPS is enabled for all ports by default. To disable the HTTPS for station ports, select **Communication > Protocols > Network1 > HTTPS** or **Communication > Protocols > Network2 > HTTPS** and set the parameter to "Off". HTTPS is always enabled for the X0/HMI port.



The WHMI write access can be limited with the parameter *HTTPS write access* in **Configuration > Authorization > Network1** or **Configuration > Authorization > Network2**.



Disable the Web browser proxy settings or make an exception to the proxy rules to allow the protection relay's WHMI connection, for example, by including the relay's IP address in **Internet Options > Connections > LAN Settings > Advanced > Exceptions**.

5.1.1 Logging in

1. Open a Web browser.
2. Type the protection relay's IP address in the address bar and press ENTER.

3. Acknowledge the login banner notification if displayed.

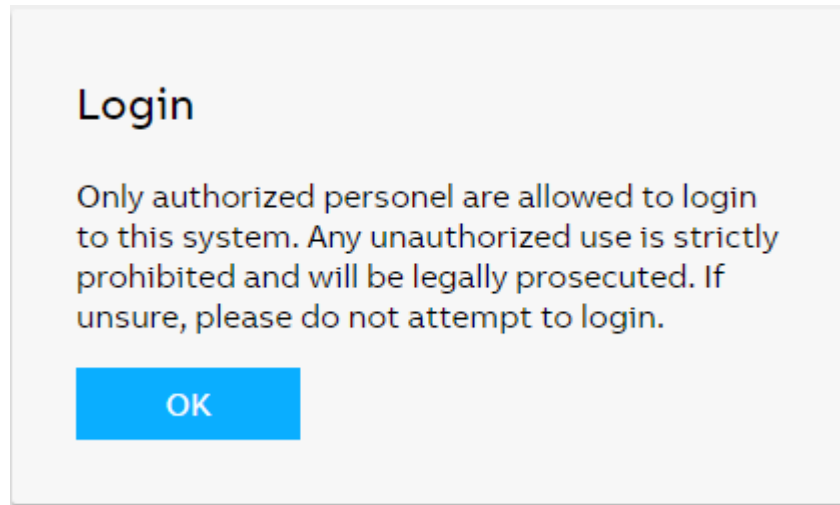


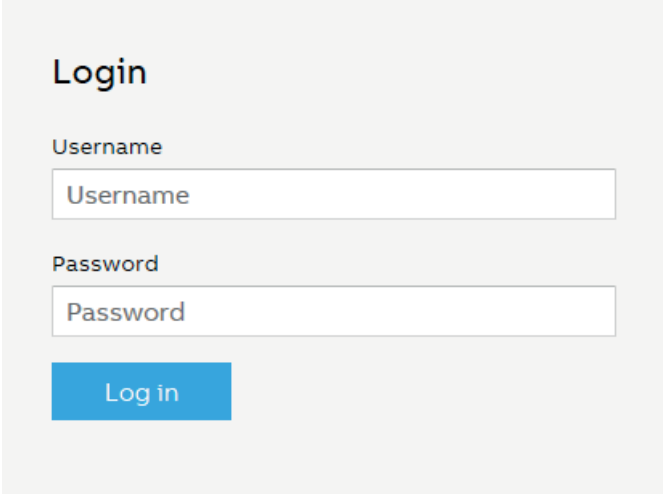
Figure 40: Login banner in WebHMI



User Editable login banner provides a way to display a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s) as is required by IEC 62443-4-2 Component Requirement 1.12 System use notification.

4. Type the username.

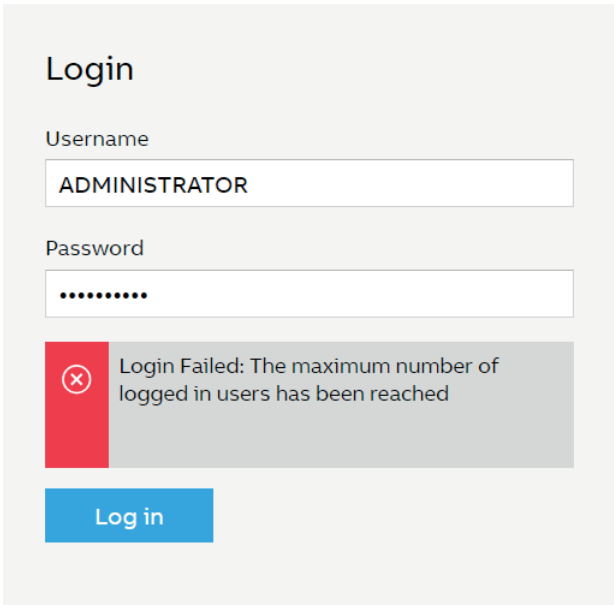
5. Type the password.



The image shows a login form titled "Login". It contains two input fields: "Username" and "Password". The "Username" field has the placeholder text "Username" inside it. The "Password" field has the placeholder text "Password" inside it. Below the fields is a blue button labeled "Log in".

Figure 41: Entering username and password to use the Web HMI

If logging in fails because all sessions are used, an error message is shown on the login page.



The image shows the same login form as Figure 41, but with an error message displayed. The "Username" field now contains the text "ADMINISTRATOR". The "Password" field is filled with dots. Below the fields, a red box with a white "X" icon is shown, followed by the text "Login Failed: The maximum number of logged in users has been reached". The "Log in" button is still present at the bottom.

Figure 42: Web HMI error message

6. Select the role if an additional view opens.

This view opens if there are several user roles configured.

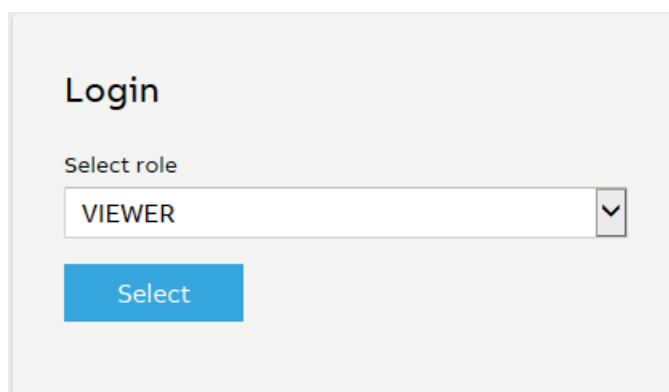
A screenshot of a 'Login' dialog box. At the top, the word 'Login' is displayed in a large, bold font. Below it, there is a label 'Select role' followed by a dropdown menu. The dropdown menu is open, showing the word 'VIEWER' in all caps. To the right of the dropdown is a small downward-pointing arrow icon. Below the dropdown is a blue rectangular button with the word 'Select' in white text.

Figure 43: Selecting user role

The progress indicator is displayed until the WHMI opens and the dashboard view is shown.



It is recommended to disable the auto-complete feature, which is usually enabled by default, in the Web browser to prevent the usernames and passwords from being stored in the browser's cache.

5.1.2

Logging out

The user is logged out after session timeout. The timeout can be set in **Configuration > HMI > HMI timeout**.

-

To log out manually, click  on the menu bar.



If password authorization is enabled (*Local override* is set to "False") and there is no user activity for the duration set in **Configuration > HMI > HMI timeout**, the LHMI session is logged out. By default, the timeout duration is three minutes.

5.2

Navigating in menus

The menu bar contains main groups which are divided further into more detailed submenus.

- Use the menu bar to access different views.

5.3 Identifying device

The Information menu includes detailed information about the device, for example, revision and serial number.

- 1. Select **Device** on the menu bar.
- 2. Select **Information**.
- 3. Click a submenu to see the data.

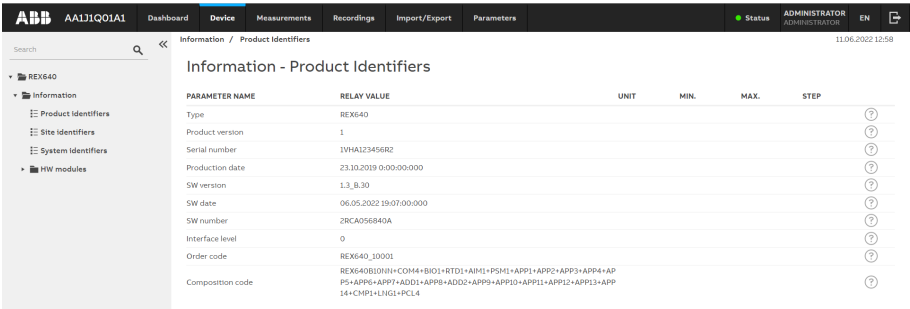


Figure 44: Viewing device information

5.4 Viewing dashboard

The Dashboard view is active automatically after logging in to WHMI and provides an overview of the protection relay including, for example, the device status, measurements, single-line diagram and latest events.

- Select **Dashboard** on the menu bar to view the dashboard.

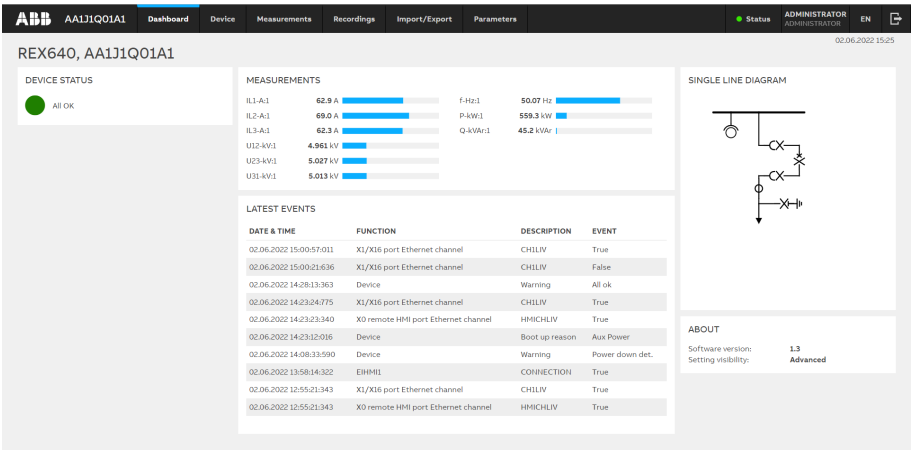


Figure 45: Viewing dashboard

5.5 Viewing self-supervision

- 1. Select **Device** on the menu bar.

2. Select **Self-Supervision**. The Self-Supervision view shows currently active internal faults and warnings.

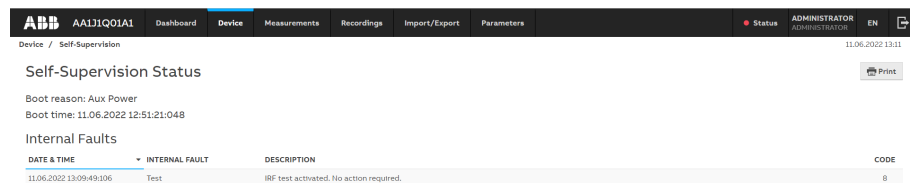


Figure 46: Self-supervision: one internal fault is currently active

5.6 Changing language

The active language of the Web server session is indicated in the caption of the menu bar button.

1. Click the active language button to view all available languages.
2. Select the language from the drop-down list.

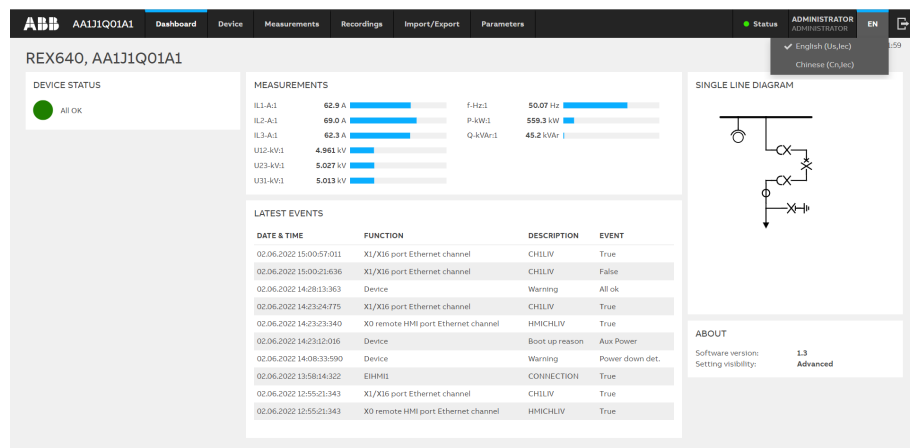


Figure 47: Changing language

5.7 Alarms

5.7.1 Viewing alarm list

1. Select **Recordings** on the menu bar.
2. Select **Alarm List** to access the alarm list.
3. Click one of the three buttons to select an alarm view.

- a) The **Persisting Alarms** view lists the active alarms.
- b) The **Fleeting Alarms** view shows the alarms that are not active anymore but are not acknowledged.
- c) The **Available Alarms** view contains all configured alarms.



Acknowledged alarms are indicated using icon  Priority alarms are indicated with icon 


ABB AA1J1Q01A1 Dashboard Device Measurements Recordings Import/Export Parameters Status ADMINISTRATOR ADMINISTRATOR EN							
Recordings / Alarm List 11.06.2022 14:06							
Alarm List Persisting Alarms Fleeting Alarms Available Alarms Acknowledge							
<input type="checkbox"/>	ACTIVATED	FUNCTION	DESCRIPTION	EVENT	ALARM TEXT	DURATION	
<input type="checkbox"/>	 11.06.2022 13:56:56.549	PHPTUV2	OPERATE	True		Still Active	
<input type="checkbox"/>	11.06.2022 13:56:51.839	PHPTUV1	OPERATE	True		Still Active	
<input type="checkbox"/>	11.06.2022 13:55:59.534	PHIPTOC1	OPERATE	True		Still Active	
<input type="checkbox"/>	11.06.2022 13:55:41.257	EFHPTOC1	OPERATE	True		Still Active	
<input type="checkbox"/>	11.06.2022 13:55:34.422	TRPPTRC1	TRIP	True		Still Active	
<input type="checkbox"/>	11.06.2022 13:55:20.822	Device	Internal Fault	Test		Still Active	

Figure 48: Viewing persisting alarms


ABB AA1J1Q01A1 Dashboard Device Measurements Recordings Import/Export Parameters Status ADMINISTRATOR ADMINISTRATOR EN							
Recordings / Alarm List 11.06.2022 14:26							
Alarm List Persisting Alarms Fleeting Alarms Available Alarms Acknowledge							
<input type="checkbox"/>	ACTIVATED	FUNCTION	DESCRIPTION	EVENT	ALARM TEXT	DURATION	
<input type="checkbox"/>	 11.06.2022 13:56:56.549	PHPTUV2	OPERATE	True		18 min 52 s	
<input type="checkbox"/>	11.06.2022 13:55:34.422	TRPPTRC1	TRIP	True		17 min 30 s	
<input type="checkbox"/>	11.06.2022 13:55:59.534	PHIPTOC1	OPERATE	True		16 min 55 s	
<input type="checkbox"/>	11.06.2022 13:55:41.257	EFHPTOC1	OPERATE	True		17 min 7 s	
<input type="checkbox"/>	11.06.2022 13:56:51.839	PHPTUV1	OPERATE	True		15 min 44 s	
<input type="checkbox"/>	11.06.2022 13:55:34.422	PHHPTOC1	OPERATE	True		16 s	

Figure 49: Viewing fleeting alarms




ABB AA1J1Q01A1 Dashboard Device Measurements Recordings Import/Export Parameters Status ADMINISTRATOR ADMINISTRATOR EN							
Recordings / Alarm List 11.06.2022 14:28							
Alarm List Persisting Alarms Fleeting Alarms Available Alarms Acknowledge							
<input type="checkbox"/>	ACTIVATED	FUNCTION	DESCRIPTION	EVENT	ALARM TEXT	DURATION	
<input type="checkbox"/>	 11.06.2022 13:56:56.549	PHPTUV2	OPERATE	True		17 min 30 s	
<input type="checkbox"/>	11.06.2022 13:55:59.534	PHIPTOC1	OPERATE	True		16 min 55 s	
<input type="checkbox"/>	11.06.2022 13:55:41.257	EFHPTOC1	OPERATE	True		17 min 7 s	
<input type="checkbox"/>	11.06.2022 13:56:51.839	PHPTUV1	OPERATE	True		15 min 44 s	
<input type="checkbox"/>	11.06.2022 13:55:34.422	PHHPTOC1	OPERATE	True		16 s	
	11.06.2022 13:55:34.422	TRPPTRC1	TRIP	True		18 min 52 s	
	11.06.2022 13:55:20.822	Device	Internal Fault	Test		31 min 33 s	
		TRPPTRC1	CL_LKOUT			0 s	
		PHPTOV2	OPERATE			0 s	
		PHPTOV1	OPERATE			0 s	
		PHLPTOC1	OPERATE			0 s	
		PCSITPC1	ALARM			0 s	
		EFLPTOC1	OPERATE			0 s	
		EFIPTOC1	OPERATE			0 s	
		Device	Warning			0 s	

Figure 50: Viewing all available alarms

5.7.2 Acknowledging alarms

- 1. Select **Recordings** on the menu bar.
- 2. Select **Alarm List**.
- 3. Select the alarm view.
- 4. Select the alarms using check boxes.
- 5. Click **Acknowledge**.

ABB AAI1IQ01A1

DashboardDeviceMeasurementsRecordingsImport/ExportParameters

StatusADMINISTRATORADMINISTRATOREN

Recordings / Alarm List11.06.2022 14:33

Alarm List

Persisting AlarmsFleeting AlarmsAvailable AlarmsAcknowledge

	ACTIVATED	FUNCTION	DESCRIPTION	EVENT	ALARM TEXT	DURATION
<input type="checkbox"/>	11.06.2022 13:55:59.534	PHIPTOC1	OPERATE	True		16 min 55 s
<input checked="" type="checkbox"/>	11.06.2022 13:55:41.257	EFHPTOC1	OPERATE	True		17 min 7 s
<input checked="" type="checkbox"/>	11.06.2022 13:56:51.839	PHPTUV1	OPERATE	True		15 min 44 s
<input type="checkbox"/>	11.06.2022 13:55:34.422	PHIPTOC1	OPERATE	True		16 s

Figure 51: Acknowledging alarms



Alarm list items can be configured in HMI Event Filtering in PCM600.

5.8 Measurements and phasor diagrams

5.8.1 Viewing measurements

1. Select **Measurements** on the menu bar.
2. Select **Measurements** from the drop-down list.

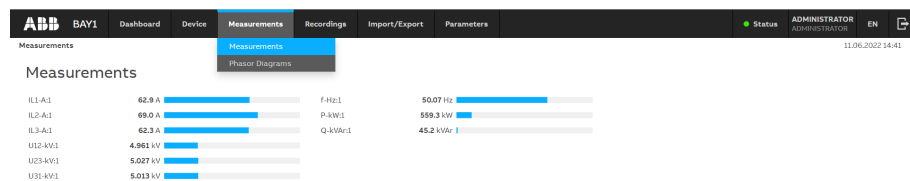


Figure 52: Viewing measurements



Measurements are also displayed in the Dashboard view.

5.8.2 Viewing phasor diagrams

1. Select **Measurements** on the menu bar.
2. Select **Phasor Diagrams** from the drop-down list.

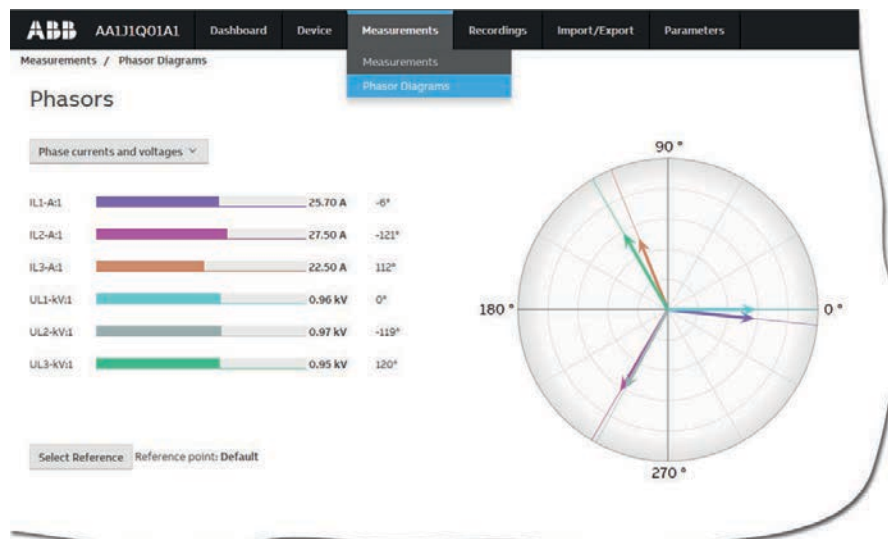


Figure 53: Monitoring phasors

3. Select the phasor from the drop-down list on the **Phasor Diagrams** page to view it.

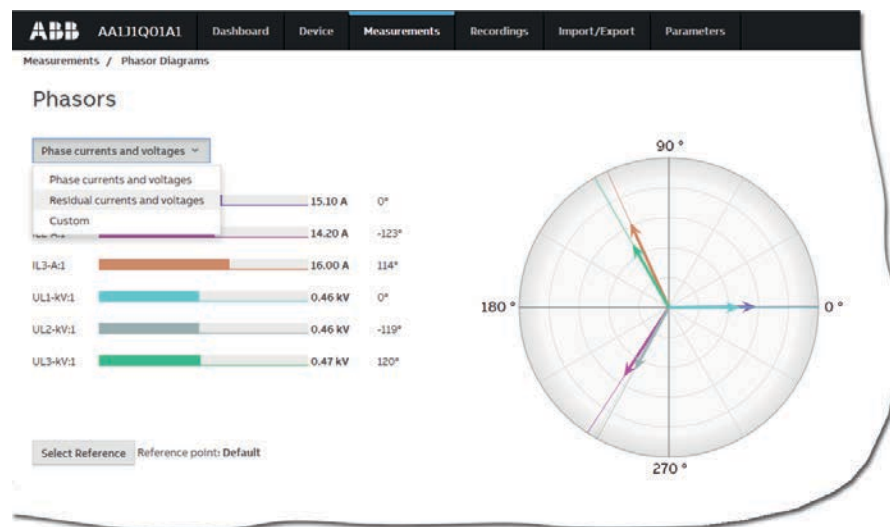


Figure 54: Selecting the phasor

4. Select **Custom** from the drop-down list on the **Phasor Diagrams** page to open the dialog with the phasor list.

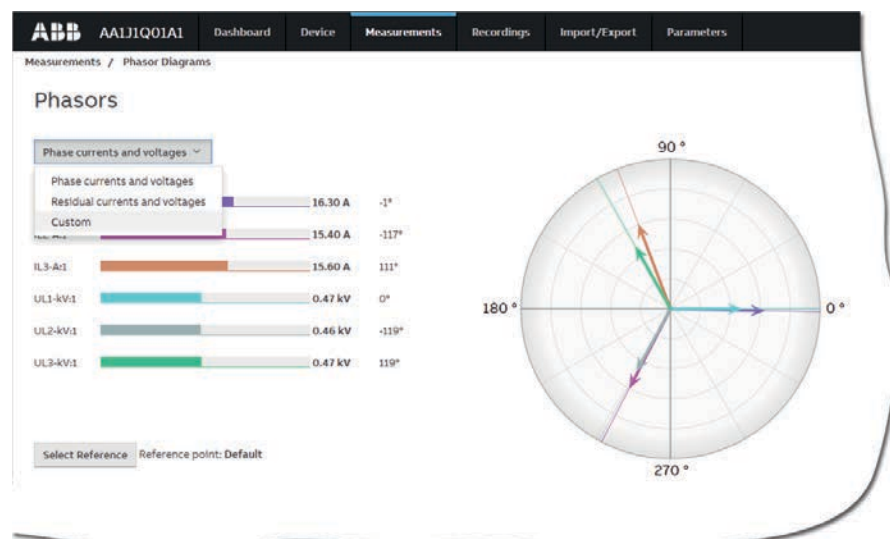


Figure 55: Selecting the custom phasors

5. In the **Custom** dialog, select the phasors to be monitored and click **Close**.

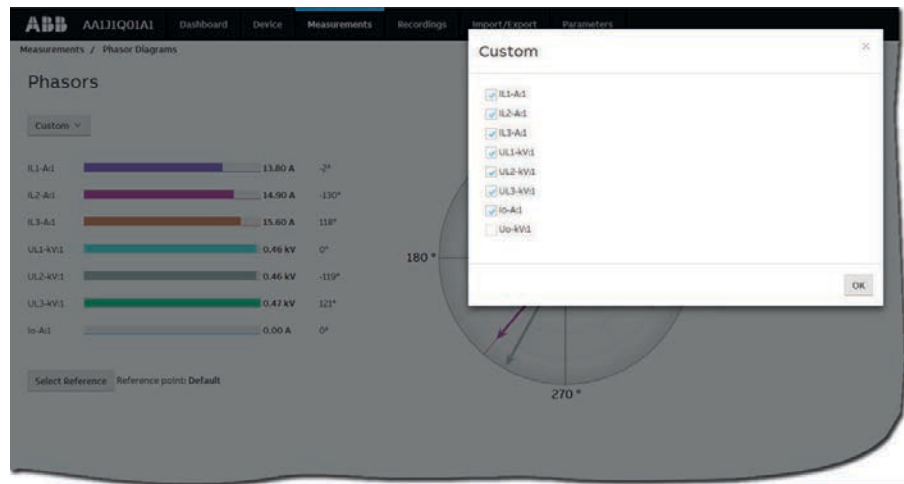


Figure 56: Editing custom phasor list

6. Click the **Select reference** button to select a reference phasor and then click **Close**.

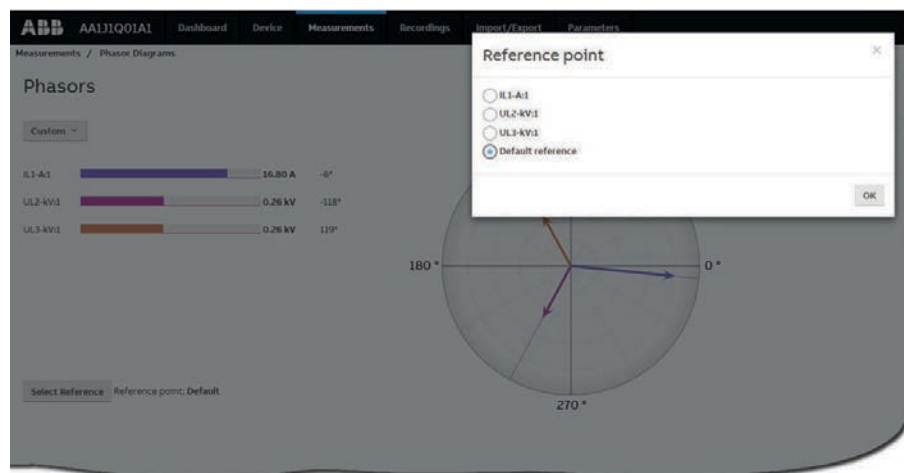


Figure 57: Selecting the reference phasor



WHMI measurements and phasor diagrams follow LHMI definitions and can be edited with Graphical Display Editor in PCM600.

5.9 Viewing monitoring

1. Select **Device** on the menu bar.
2. Select **Monitoring** from the drop-down list.

3. Select the monitored view from the left navigation bar.

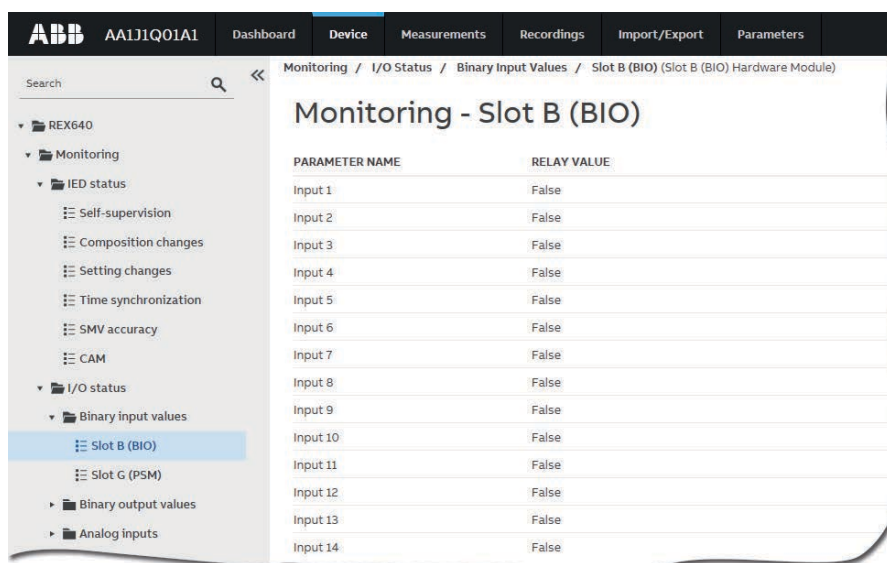


Figure 58: Monitoring data

5.10 Viewing single-line diagram

The single-line diagram is displayed on the dashboard and the Single Line Diagram page. If there are more than one page, the first page is displayed and the others are included in the drop-down list.

1. Select **Device** on the menu bar.
2. Select **Single Line Diagram** to view the single-line diagram page.

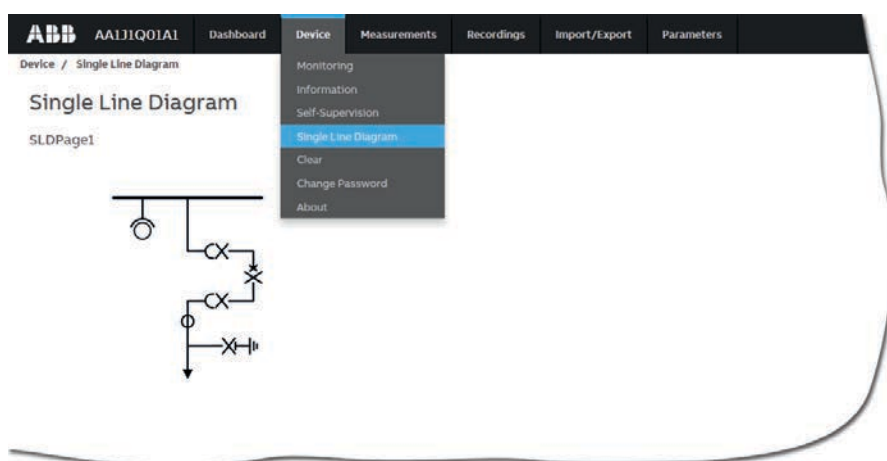


Figure 59: Viewing the single-line diagram with IEC symbols

5.11 Showing parameters

Some function blocks have a function-specific ON/OFF setting. When the function setting is "off", all settings are hidden and when the function setting is "on", all settings are visible based on the other visibility and hiding rules.



Switch a function block on or off via the *Operation* parameter under the function block.



The values "Basic" or "Advanced" of the *Setting visibility* parameter in **Configuration > HMI** have no effect on the Parameter List page. This page has its own Basic settings option which can be used to hide or show the advanced settings on the Parameter List page.

1. Select **Import/Export** on the menu bar.
2. Select **Parameter List** from the drop-down list.

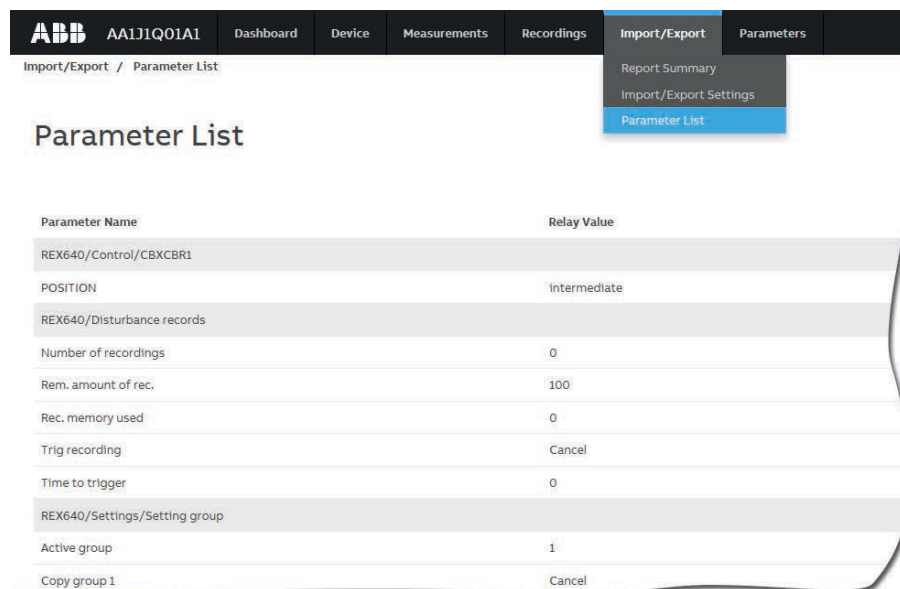



Figure 60: Displaying parameters

3. Click the filter icon .
4. In the **Apply filter** dialog, select the settings that should be shown and click **Apply**. If nothing is selected, all settings are shown.

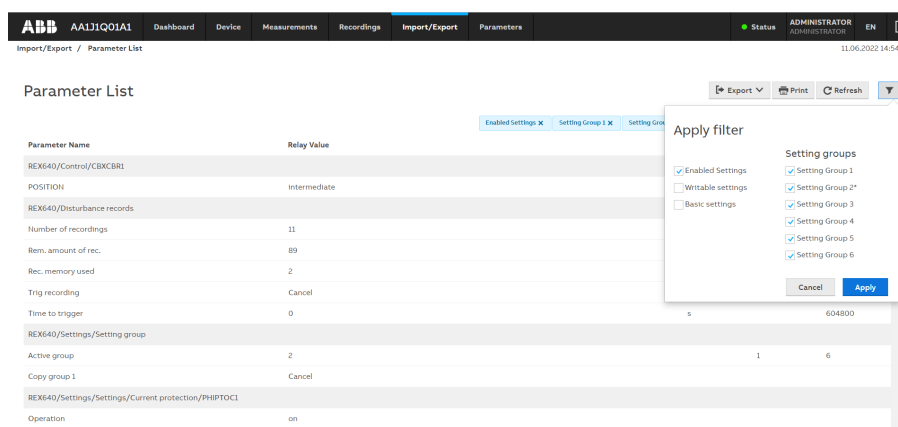


Figure 61: Enabling settings

The Parameter List page offers filtering functionality where only chosen parameters are displayed, saved or printed. There are various options for filtering.

- **Enabled Settings** hides settings of disabled function blocks. This option is checked by default.
 - **Writable settings** displays only writable settings.
 - **Basic settings** displays only basic settings.
 - **Setting group** displays only the settings of the selected setting group. Options can be combined. For example, with the **Enabled Settings** and **Writable settings** selected, only enabled and writable settings are displayed.
5. Click **Export** and select text (.txt) or comma separated values (.csv) file format to save the settings.
 6. Click **Print** to print all the selected parameters.

5.12 Editing values

1. Select **Parameters** on the menu bar.
2. Click a submenu in the left navigation bar to see the function blocks.
3. Click a function block to see the setting values.

4. Click **Enable Edit**.



If the edit mode is enabled accidentally, click **Disable Edit**. Editing cannot be disabled when a value has already been written to the protection relay. After clicking **Write to Relay**, click either **Reject Changes** or **Store Changes**.

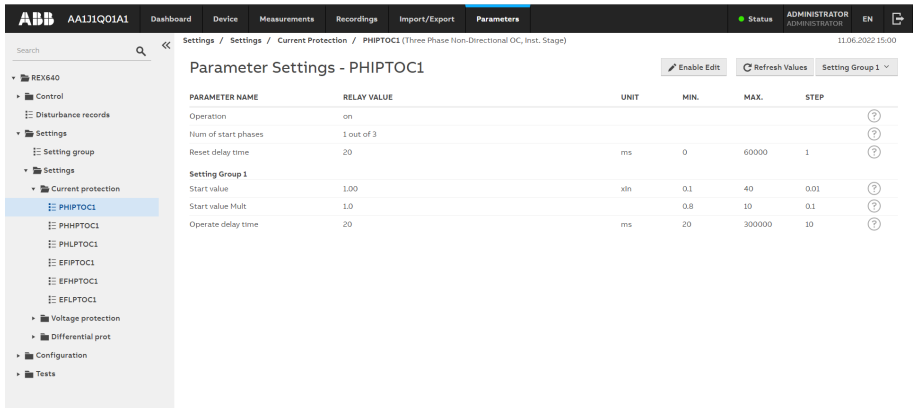


Figure 62: Enable writing to edit a value

The selected setting group is shown in the Setting Group drop-down list and the setting group parameters are listed on page. The active setting group is indicated with an asterisk *.

5. Edit the value. The minimum, maximum and step values for a parameter are shown in the MIN., MAX. and STEP columns.

Settings / Settings / Current Protection / PHIPTOC1 (Three Phase Non-Directional OC, Inst. Stage) 25.04.2019 12:51

Parameter Settings - PHIPTOC1

Disable Edit Write to Relay Refresh Values Setting Group 1*

PARAMETER NAME	RELAY VALUE	UNIT	MIN.	MAX.	STEP
Operation	on				
Num of start phases	1 out of 3				
Reset delay time	20	ms	0	60000	1
Setting Group 1					
Start value	2	sin	0.1	40	0.01
Start value Mult	1		0.8	10	0.1
Operate delay time	20	ms	20	300000	10

Figure 63: Editing a value

If the entered value is within the accepted value range, the selection is highlighted in blue. If the value is out of range, the row is highlighted in red and error text is displayed. **Write to Relay** is unavailable.

Settings / Settings / Current Protection / PHIPTOC1 (Three Phase Non-Directional OC, Inst. Stage) 25.04.2019 12:54

Parameter Settings - PHIPTOC1

Disable Edit Write to Relay Refresh Values Setting Group 1*

PARAMETER NAME	RELAY VALUE	UNIT	MIN.	MAX.	STEP
Operation	on				
Num of start phases	1 out of 3				
Reset delay time	20	ms	0	60000	1
Setting Group 1					
Start value	40	sin	0.1	40	0.01
Start value Mult	1		0.8	10	0.1
Operate delay time	20	ms	20	300000	10

The new value is out of range.

Figure 64: Error indicating that the entered value is incorrect

If writing values fails, an error message is displayed.

Tests / IED Test 25.04.2019 12:56

Parameter Settings - IED Test

Disable Edit Write to Relay Refresh Values Setting Group 1*

PARAMETER NAME	RELAY VALUE	UNIT	MIN.	MAX.	STEP
Test mode	IED test				
Internal fault test	Test off				
Test mode selection	Local				

Test mode: Rejected by setting relations

Figure 65: Error indicating that the values were not written to the protection relay

6. Commit the settings.

5.13 Committing settings

Editable values are stored either in RAM or a nonvolatile flash memory. The values stored in the flash memory are in effect also after a reboot.

Some parameters have an edit-copy. If writing is cancelled, the values with an edit-copy are immediately restored to the original value. The values without an edit-copy, such as string values, are restored to the original value only after a reboot even though the edited value is not stored in the flash memory.

1. After editing parameter values, click **Write to Relay** to put the values into the protection relay's database for use. The values are not stored to the flash memory.

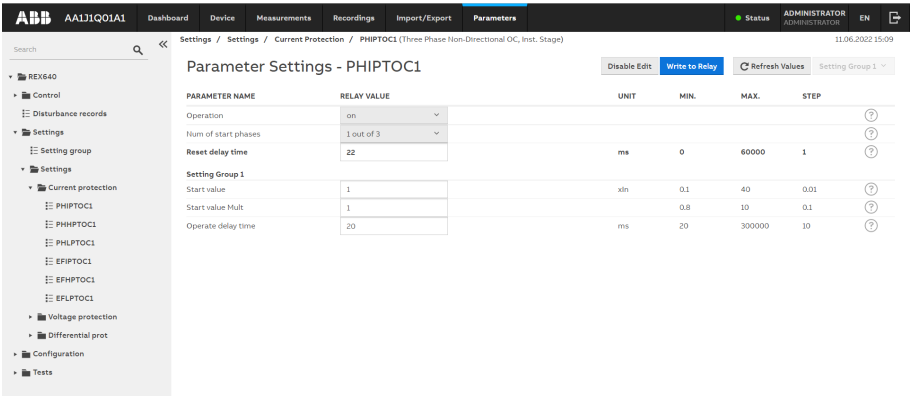


Figure 66: Writing values to the protection relay

- 2. Click **Store Changes** to store the values to the flash memory.



Click **Reject Changes** to cancel saving settings. If the parameter has an edit-copy, the original parameter value is restored. If the parameter does not have an edit-copy, the edited parameter value remains visible until the protection relay is rebooted. However, the edited value is not stored in the nonvolatile memory and thus the reboot restores the original value.

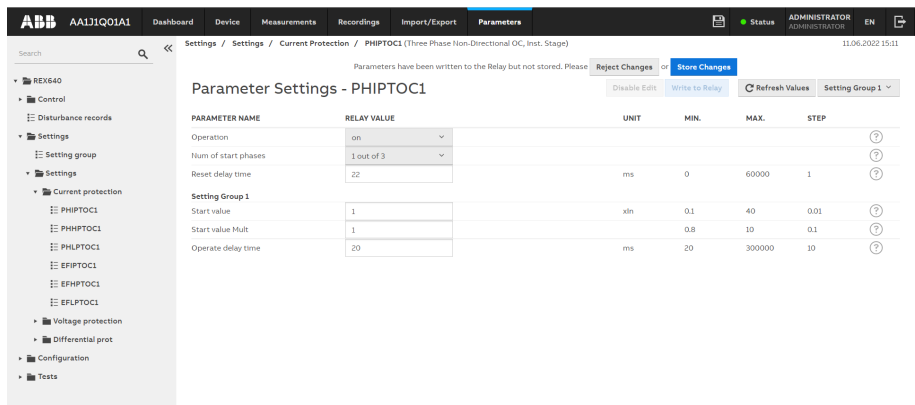


Figure 67: Storing changes



Storing values takes a few seconds.



If the values are not stored, they are not taken into use and they are lost after a reboot.

5.14 Clearing and acknowledging

Reset, acknowledge or clear all messages and indications, including LEDs and latched outputs as well as registers and recordings, in the Clear page.

- 1. Select **Device** on the menu bar.
- 2. Select **Clear** from the drop-down list.

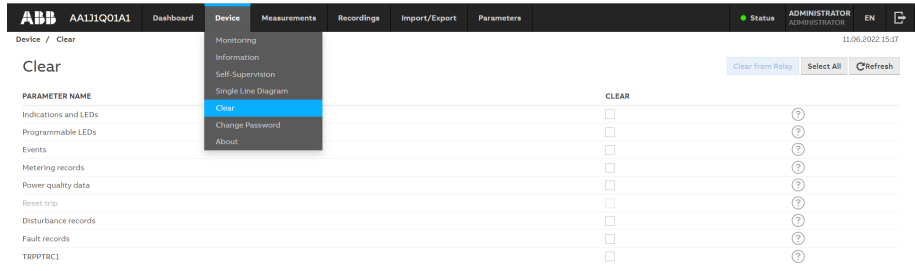


Figure 68: Opening the Clear page

3. Select the item to be cleared.
4. Click **Clear from Relay**.

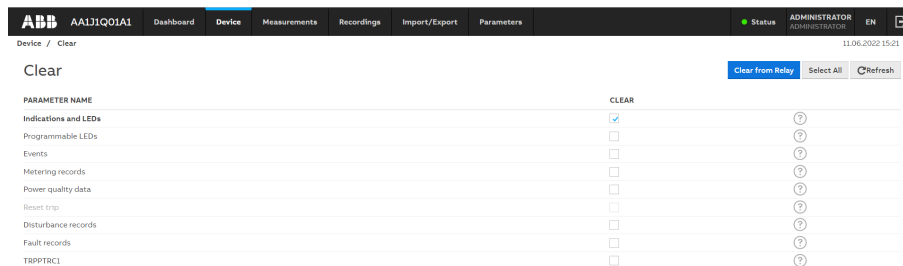


Figure 69: Clearing indications and LEDs

5.15 Accessing event view

The event view contains a list of events produced by the application configuration. When the event page is opened, it displays up to 20 latest events at one time. The event list is updated automatically.

1. Select **Recordings** on the menu bar.
2. Select **Events** from the drop-down list.

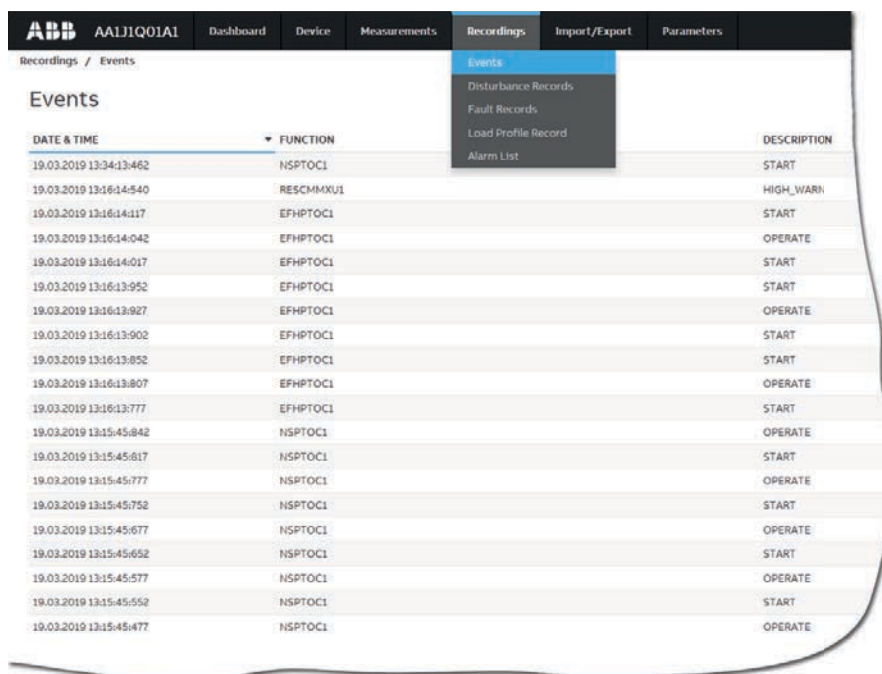


Figure 70: Monitoring events

3. Click **Freeze** to stop updating the event list.

4. Select a page to view older events.

DATE & TIME	FUNCTION	DESCRIPTION	EVENT
11.06.2022 14:41:00:881	Protection LLNO	Device state	on
11.06.2022 14:40:14:154	Device	Internal Fault	All ok
11.06.2022 14:40:11:889	Device	Internal Fault	Test
11.06.2022 14:26:54:058	Device	Internal Fault	All ok
11.06.2022 14:14:26:181	TRIPTRC1	TRIP	False
11.06.2022 13:56:56:549	PHPTUV2	OPERATE	True
11.06.2022 13:56:51:839	PHPTUV1	OPERATE	True
11.06.2022 13:56:30:344	PHPTUV1	START	True
11.06.2022 13:55:59:534	PHPTOC1	OPERATE	True
11.06.2022 13:55:41:257	EPHPTOC1	OPERATE	True
11.06.2022 13:55:34:422	PHPTOC1	OPERATE	True
11.06.2022 13:55:34:422	TRIPTRC1	TRIP	True
11.06.2022 13:55:20:802	Device	Internal Fault	Test
11.06.2022 13:54:57:837	Protection LLNO	Device state	test
11.06.2022 13:18:58:948	Protection LLNO	Device state	on
11.06.2022 13:15:13:678	Device	Internal Fault	All ok
11.06.2022 13:09:49:106	Device	Internal Fault	Test
11.06.2022 13:09:39:223	Protection LLNO	Device state	test
11.06.2022 12:56:29:439	Protection LLNO	Device state	on
11.06.2022 12:56:22:815	EH-HMI	CONNECTION	True

Figure 71: Viewing events

5. To save the events as .txt or .csv files, click **Export** and select the file format from the drop-down list.



The CSV file can be opened with a spreadsheet program such as OpenOffice.org Calc or Microsoft Excel.

6. Click **Clear Events** to clear all events from the protection relay.
7. Click **Print** to print all the selected events.

5.16

Accessing disturbance record view

Disturbance records are listed in the disturbance records view.

1. Select **Recordings** on the menu bar.
2. Select **Disturbance Records** from the drop-down list.

DATE & TIME	NAME
10.07.2018 14:12:04:306	020A0004
10.07.2018 14:11:20:286	020A0003
10.07.2018 14:11:12:468	020A0002
10.07.2018 14:09:59:765	020A0001

Figure 72: Viewing disturbance records

5.16.1 Saving disturbance records

- 1. Select **Recordings** on the menu bar.
- 2. Select **Disturbance Records** from the drop-down list.
- 3. To save the disturbance record files, click the **Export** button in the **Export Files** column of the record. Both disturbance record files CFG and DAT are saved at once.

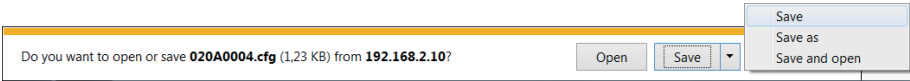


Figure 73: Saving a disturbance record



If prompted, give permission for file downloading depending on the used Web browser.

- 4. Open the disturbance record files with a suitable program.

5.16.2 Triggering disturbance recorder manually

- 1. Select **Recordings** on the menu bar.
- 2. Select **Disturbance Records** from the drop-down list.

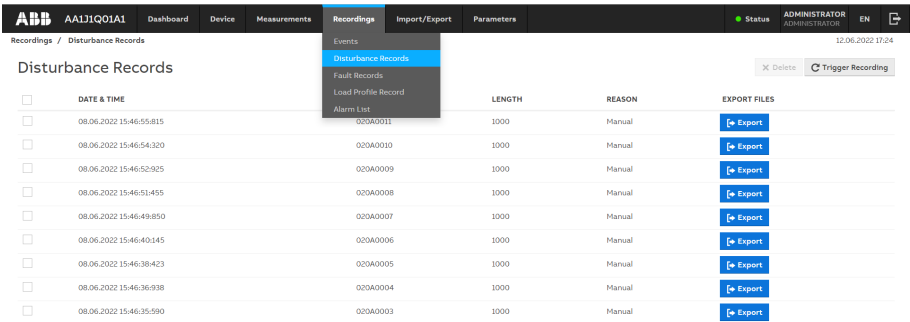
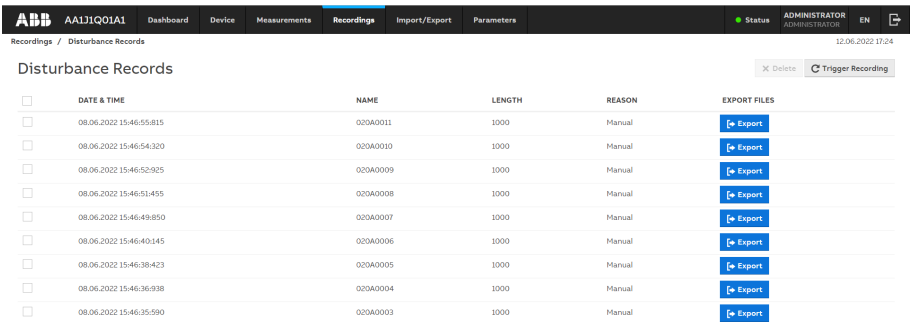


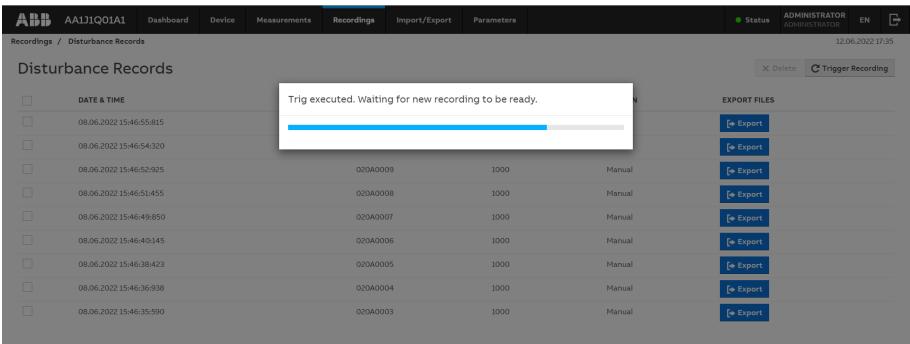
Figure 74: Selecting Disturbance Records

3. Click **Trigger Recording**Trigger Recording.



	DATE & TIME	NAME	LENGTH	REASON	EXPORT FILES
<input type="checkbox"/>	08.06.2022 15:46:55:815	020A0011	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:54:320	020A0010	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:52:925	020A0009	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:51:455	020A0008	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:49:850	020A0007	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:40:145	020A0006	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:38:423	020A0005	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:36:938	020A0004	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:35:590	020A0003	1000	Manual	Export

Figure 75: Triggering recording

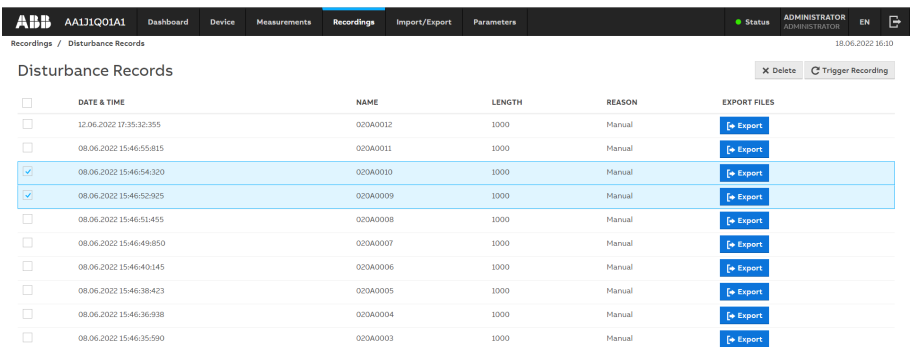


	DATE & TIME	NAME	LENGTH	REASON	EXPORT FILES
<input type="checkbox"/>	08.06.2022 15:46:55:815	020A0011	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:54:320	020A0010	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:52:925	020A0009	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:51:455	020A0008	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:49:850	020A0007	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:40:145	020A0006	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:38:423	020A0005	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:36:938	020A0004	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:35:590	020A0003	1000	Manual	Export

Figure 76: Triggering recording - progress bar

5.16.3 Deleting disturbance records

1. Select **Recordings** on the menu bar.
2. Select **Disturbance Records** from the drop-down list.
3. Delete records in one of the alternative ways.
 - Select all and click **Delete** to delete all records.
 - Select one or more recordings and click **Delete** to delete the selected records.



	DATE & TIME	NAME	LENGTH	REASON	EXPORT FILES
<input type="checkbox"/>	12.06.2022 17:35:32:355	020A0012	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:55:815	020A0011	1000	Manual	Export
<input checked="" type="checkbox"/>	08.06.2022 15:46:54:320	020A0010	1000	Manual	Export
<input checked="" type="checkbox"/>	08.06.2022 15:46:52:925	020A0009	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:51:455	020A0008	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:49:850	020A0007	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:40:145	020A0006	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:38:423	020A0005	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:36:938	020A0004	1000	Manual	Export
<input type="checkbox"/>	08.06.2022 15:46:35:590	020A0003	1000	Manual	Export

Figure 77: Deleting disturbance records

5.17 Viewing fault records

1. Select **Recordings** on the menu bar.
2. Select **Fault Records** from the drop-down list to view a list of all available fault records.
3. Click a record from the **Fault records** list to open the fault record details view.
4. To go back to the list view, click **View All**.
5. To save the records as .txt or .csv files, select the format from the **Export** drop-down list.
 - When the fault record details view is shown, only the shown fault record is saved.
 - When fault record list view is shown, all fault records are saved.
6. To clear all fault records from the relay, click **Clear All**. This can be done only when the fault record list view is shown.
7. To print all fault records, click **Print** when the fault record list view is shown.
8. To print only one record, open it in the details view and click **Print**.

FAULT NUMBER	DATE & TIME	PROTECTION
6	18.06.2022 16:37:29912	PHLPTOC1
5	18.06.2022 16:37:01.999	PHLPTOC1
4	18.06.2022 16:34:38.780	PHLPTOC1
3	18.06.2022 16:34:14.999	PHLPTOC1
2	18.06.2022 16:33:48.916	PHLPTOC1
1	18.06.2022 16:22:06.844	EFLPTOC1

Figure 78: Fault record list view

PARAMETER NAME	RELAY VALUE	UNIT	MIN.	MAX.
Fault number	5		0	999999
Time and date	18.06.2022 16:37:01.999			
Protection (rec. set 1)	PHLPTOC1			
Protection (rec. set 2)	None			
Start duration	100.00	%	0.00	100.00
Operate time	0.000	s	0.000	1000000.000
Breaker clear time	(3.000)	s	0.000	3.000
Fault distance	(0.00)	pu	0.00	3000.00
Fault resistance	(0.00)	ohm	0.00	3000.00
Fault reactance	(0.00)	ohm	0.00	3000.00
Active group	2		1	6
Shot pointer	1		1	7
Max diff current I1,1	0.000	pu	0.000	80.000
Max diff current I2,1	0.000	pu	0.000	80.000
Max diff current I3,1	0.000	pu	0.000	80.000
Diff current I1,1	0.000	pu	0.000	80.000

Figure 79: Fault record details view

5.18 Exporting load profile records

1. Select **Recordings** on the menu bar.
2. Select **Load Profile Record** from the drop-down list.
3. To export the load profile record files, click the **Export** button in the **Export Files** column. Both load profile record files CFG and DAT are saved at once.
4. Save the CFG and DAT files in the same folder on the computer.
5. Open the load profile record COMTRADE files with a suitable program.



Open the load profile files, for example, with the Wavewin tool included in PCM600.

5.19 Importing and exporting of settings

The relay's setting parameters can be imported and exported in the XRIO file format.



When importing parameters to PCM600 via an XRIO file generated by the WHMI, some Ethernet communication and HMI-related parameters are not included in the import. Check the Output window of PCM600 for such parameters and manually update those if needed.

5.19.1 Exporting settings

The relay's setting parameters can be exported in XRIO file format.

1. Select **Import/Export** on the menu bar.
2. Select **Import/Export Settings** from the drop-down list.
3. Click **Export Settings**. The export file includes all parameters except status parameters and parameters writable only in LHMI.

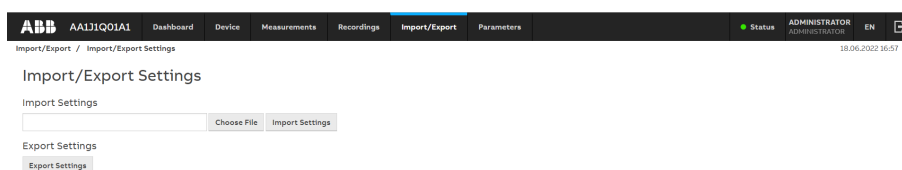


Figure 80: Exporting settings

4. Click **Save** to export the settings to the computer.

5.19.2 Importing settings

The parameter export and import function can be used, for example, when the protection relay's parameters are set using the WHMI instead of PCM600. The protection relay's settings engineered with PCM600 can be exported to XRIO files and imported to the WHMI. The WHMI can be used to write the settings to the protection relays. The WHMI can also be used to read the protection relay's setting parameters and to export those to files, which can be used by PCM600. WHMI imports all parameters from the import file except lockable and read-only parameters.



The XRIO file name supports only characters A-Z, a-z and 0-9.



The exporting and importing of settings is sensitive to the protection relay content. Settings are exported and imported for one protection relay at a time. The export files of a specific protection relay can be exchanged between PCM600, WHMI and the actual physical protection relay. To avoid errors and to efficiently manage the exporting and importing of settings, for example, in a substation with several relays, ensure that the names of the export files identify the relay to which the file should be imported.



Ensure that the correct settings are imported to the correct relay. Wrong settings may cause the relay to malfunction.

1. Select **Import/Export** on the menu bar.
2. Select **Import/Export Settings** from the drop-down list.
3. Click **Choose File** and choose the file to be imported.

Import/Export / Import/Export Settings

Import/Export Settings

Import Settings

<input type="text"/>	Choose File	Import Settings
----------------------	-------------	-----------------

Export Settings

Export Settings

Figure 81: Selecting the settings to be imported

- Click **Import Settings**. Wait until the file transfer is complete.

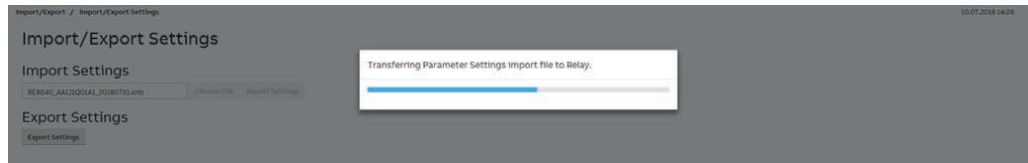


Figure 82: Importing settings

- Click **Store** to commit the imported settings to the relay. Wait until the import is complete.



Click **Cancel** to cancel the import. Both the WHMI and the relay revert to the settings in use prior to the import.



Figure 83: Writing parameter settings



Figure 84: Parameter settings written to relay



Only editable parameters are written to the relay during the import. If part of the import fails, the faulty parameters are listed separately.

5.20 Exporting report summary

The Report Summary page allows exporting protection relay recordings, logs and parameters. Events, fault records and the parameter list are saved in TXT format. The saved files contain all events, fault records and settings.

Disturbance records and load profile record files are saved in CFG and DAT formats.

- Select **Import/Export** on the menu bar.
- Select **Report Summary** from the drop-down list.
- Select the items to be exported.
 - Click **Select all** to select all items.
 - Click **Clear all** to clear all selections.

- 4. Click **Export** to export the .zip file with the selected files.

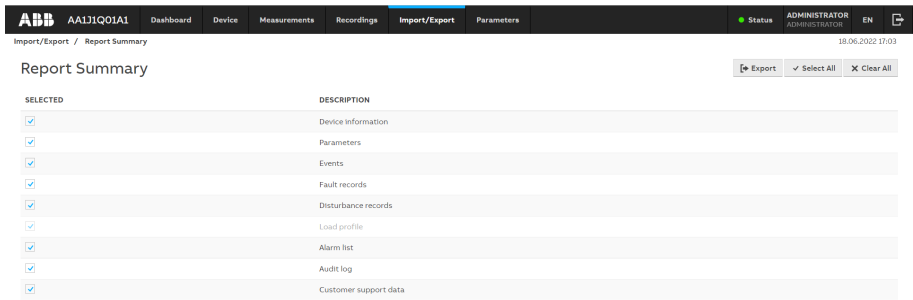


Figure 85: Report Summary page

5.21 Using Web HMI help

The context-sensitive WHMI help provides information on a single parameter, for example.

- Move the mouse over the  to display the help dialog box.

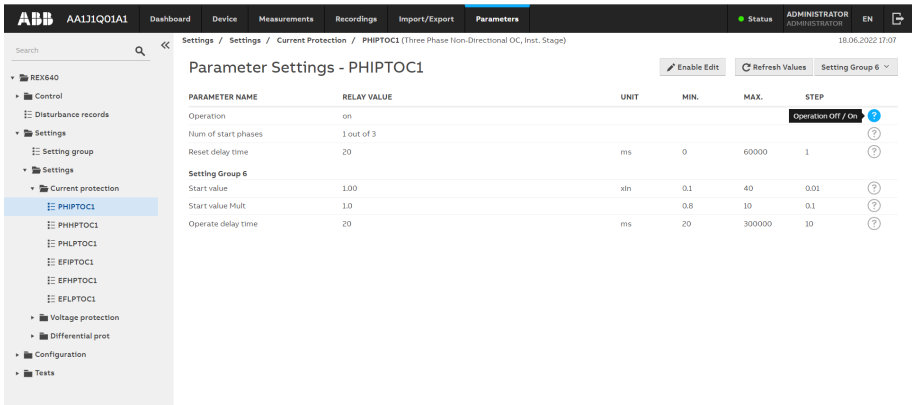


Figure 86: Opening the HMI help

6 Troubleshooting

6.1 Fault tracing

6.1.1 Identifying hardware errors

1. Check the module with an error.
Check the relay supervision events in **Relay Status** for a faulty hardware module.
2. Inspect the protection relay visually.
 - Inspect the protection relay visually to find any physical error causes.
 - If you can find some obvious physical damage, contact ABB for repair or replacement actions.
3. Check whether the error is external or internal.
 - Check that the error is not caused by external origins.
 - Remove the wiring from the protection relay and test the input and output operation with an external test device.
 - If the problem remains, contact ABB for repair or replacement actions.

6.1.2 Identifying runtime errors

1. Check the error origin from the protection relay's supervision events in **Relay Status**.
2. Reboot the protection relay and recheck the supervision events to see if the fault has cleared.
3. In case of persistent faults, contact ABB for corrective actions.

6.1.3 Identifying communication errors

Communication errors are normally communication interruptions or synchronization message errors due to communication link breakdown.

- In case of persistent faults originating from protection relay's internal faults such as component breakdown, contact ABB for repair or replacement actions.

6.1.3.1 Checking communication link operation

- Check the LEDs indicating communication link or communication activity on the communication card. They should be lit or flashing.

Table 8: Front communication LEDs

LED	Communication ok
Uplink	Steady green light
Communication	Flashing yellow light

6.1.3.2 Checking time synchronization

- Check the time synchronization via LHMI in **Relay Status > Monitoring > IED status > Time synchronization**.

6.1.4 Reading of internal log files

When contacting ABB customer service, be prepared to send the relay's internal log files for investigation. The files can be read either via the HMI's USB port or from the WHMI.

6.1.4.1 Reading internal log files from Web HMI

1. Insert a USB stick to the HMI's USB port, and navigate to the relay's HMI view if using an SHMI.
2. On the **USB Actions** page, tap **Select All** to select all items.
3. Tap **Save to USB** to save the .zip file with the selected files.
4. Wait for the confirmation that the file is saved to the USB folder, tap **OK**, and tap **Safely Remove USB**.
5. Locate the .zip file saved to the HMI folder of your USB stick and send it to ABB customer service for further analysis.



HMI's USB access is disabled by default. To enable USB, instantiate the EIHMI function block in the application configuration. After this it can be taken into use by setting the *USB access* parameter via **Configuration > HMI**.

6.1.4.2 Reading internal log files via HMI's USB port

1. Connect to the WHMI.
2. Select **Import > Export** on the menu bar.
3. Select **Report Summary** from the drop-down list.
4. Make sure that all items are selected. If not, click **Select All** to select all items..
5. Click **Export** to export a .zip file with the selected files.
6. Save the .zip file to your PC and send it to ABB customer service for further analysis.



WHMI is disabled by default. It can be enabled by the *Web HMI mode* parameter via **Configuration > HMI**. Reboot the relay for the change to take effect.

6.1.5 Checking local HMI connectivity

If the connection between the LHMI and the relay is lost, check the following.

1. Check that the RJ-45 cable is properly connected between the LHMI's main unit port X1.1. and the X0 port (HMI) of the relay's communication card. If the station communication connection (a LAN port of the communication card) is used between the LHMI and the relay, see [Chapter 7.4.3.2 Connecting local HMI to a relay through station network](#) to check the proper connection.
2. Check that the LHMI is paired with the relay. See [Chapter 7.4.3.4 Pairing local HMI with relay](#).

6.2 Self-supervision

The protection relay's extensive self-supervision system continuously supervises the relay's software, hardware and certain external circuits. It handles the run-time fault situation and informs the user about a fault via the LHMI, the relay's main unit power module Ready LED and through the communication channels. The target of the self-supervision is to safeguard the relay's reliability by increasing both dependability and security. The dependability can be described as the relay's ability to operate when required. The security can be described as the relay scheme's ability to refrain from operating when not required. The dependability is increased by letting the system operators know about the problem, giving them a chance to take the necessary actions as soon as possible. The security is increased by preventing the relay from making false decisions, such as issuing false control commands.

There are two types of fault indications.

- Internal faults
- Warnings

Warnings are indications of less severe situations which can also be caused by external reasons, for example, in case the RTD sensor measurement circuit is not complete.

On the LHMI, the self-supervision status is available as an advanced page under Relay Status page. The self-supervision status is indicated with Internal Fault, Warning and All OK LEDs. In normal operation, All OK LED is lit. The self-supervision also controls the status of IRF output relay. The IRF output relay is energized under normal conditions and de-energized under internal fault conditions.

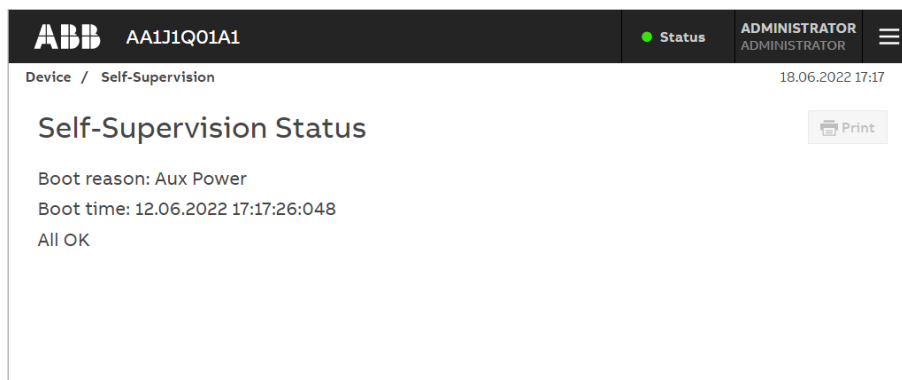


Figure 87: Relay self-supervision status on local HMI

On the WHMI, the self-supervision status is available under Device menu. The top right LED indicates the relay status.

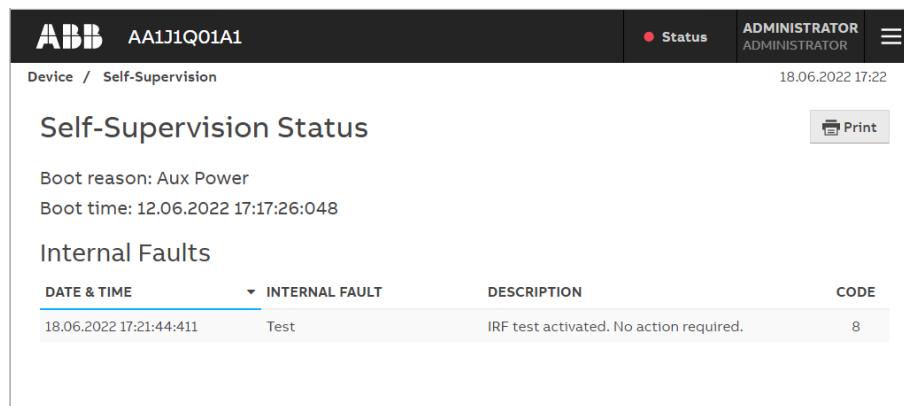


Figure 88: Relay self-supervision status on Web HMI

In addition, the last boot reason and time are shown on both LHMI and WHMI.

6.2.1 Internal faults

When an internal relay fault is detected, the relay protection operation is disabled, the self-supervision output relay is de-energized, and the change-over contact is released. In the main unit, the main indication of an internal fault is a flashing green Ready LED behind the power module, and on the HMI, a rapidly flashing red Home button.

Different actions are taken depending on the severity of the internal fault. In case of a temporary fault, the protection relay tries to recover from the situation by restarting. The restart procedure includes two stages; when the relay detects a fault, it restarts itself in a few seconds after the fault occurrence. If the relay did not recover after the first restart, or the fault reoccurs during the next 60 minutes, the second restart is delayed for 10 minutes. In case of a permanent fault, the protection relay stays in the internal fault mode. All output relays are de-energized and contacts are released for the internal fault. The protection relay continues to perform internal tests during the fault situation. If the internal fault disappears, the fault indication LEDs stop flashing and the protection relay returns to the normal service state.

One possible cause for an internal fault situation is a so-called soft error. The soft error is a probabilistic phenomenon which is rare in a single device, statistically not happening more often than once in a relay's lifetime. No hardware failures are expected and a full recovery from the soft error is possible by a self-supervision controlled restart of the relay.

The self-supervision signal output operates on the closed-circuit principle. Under normal conditions, the IRF output relay is energized and the contact gap 3-5 is closed. If the auxiliary power supply fails or an internal fault is detected, the IRF output relay is de-energized and the contact gap 3-5 opens.

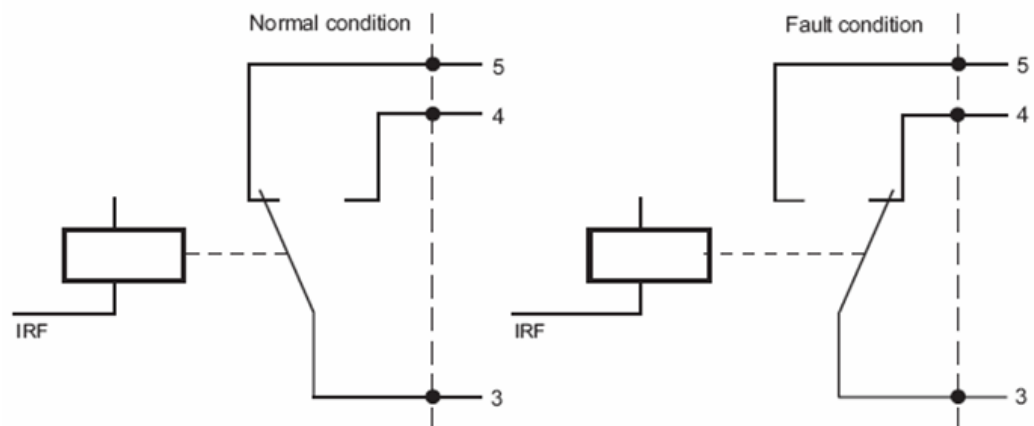


Figure 89: Output contact

The internal fault code indicates the type of internal relay fault. When a fault appears, the code must be recorded so that it can be reported to ABB customer service.

More details about the active internal fault are found on the Relay Status page. On the LHMI, the internal fault state is indicated with a red LED. More information about the fault and recovery options can be accessed by tapping More Information.

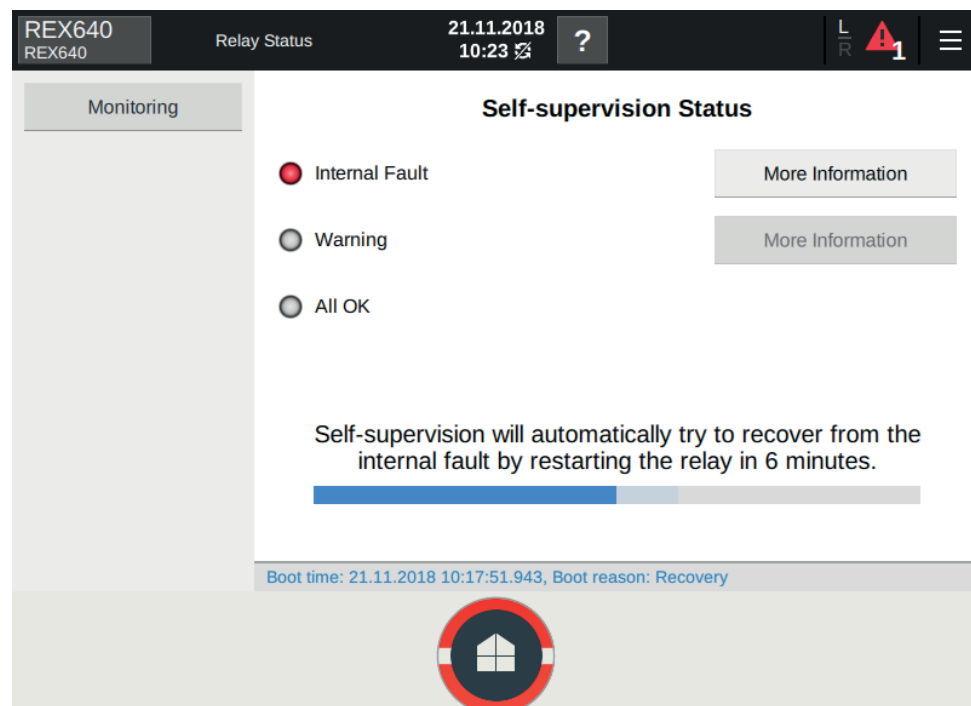


Figure 90: Internal fault state indicated with red LED

More Information shows all active faults and the corresponding fault codes. In addition, a recovery procedure is described.

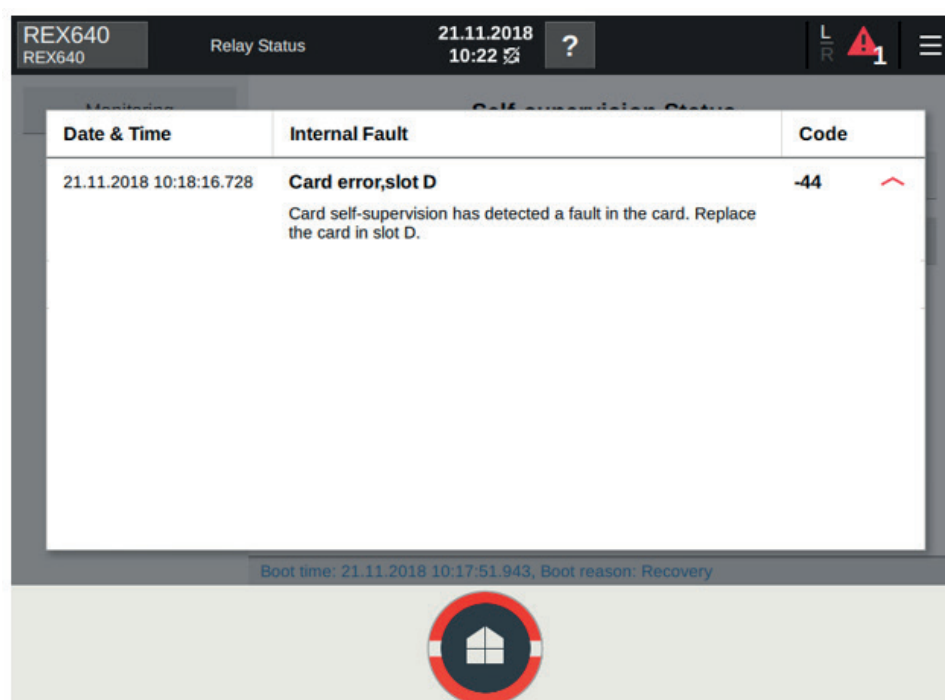


Figure 91: More information about the fault

On the WHMI, internal fault information is shown under Self-Supervision Status.

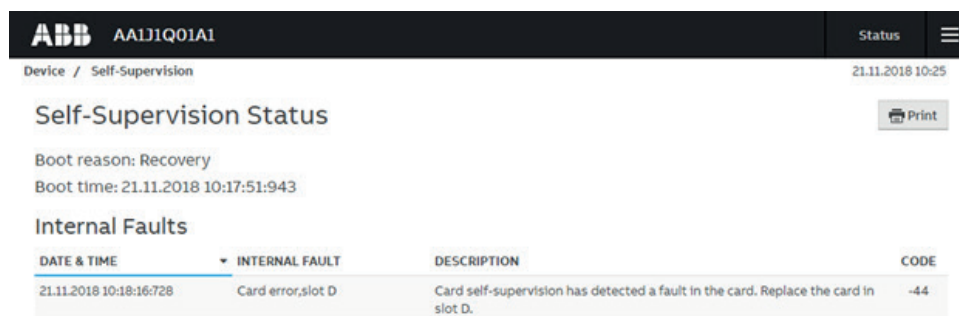


Figure 92: Internal fault information on Web HMI

Table 9: Internal fault indications and codes

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
Internal Fault System error	2	Start up error: HW/SW mismatch	No	No	Yes	If relay SW has just been updated, redo it. If not recovered, contact your nearest ABB representative to check the next possible corrective action.
Internal Fault System error	2	Start up or runtime error: Data bus error, CPU module	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation.

Table continues on the next page

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
						If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault System error	2	Start up error: SCL file missing	No	No	Yes	Do factory restore or re-write configuration using PCM600.
Internal Fault System error	2	Start up error: Missing order number	No	No	Yes	Do factory restore. If not recovered, contact your nearest ABB representative to check the next possible corrective action.
Internal Fault System error	2	Start up error: FPGA HW error, CPU module	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault System error	2	Start up error: FPGA image corrupted, CPU module	Yes	Yes (3)	No	Restart the relay or if relay SW has just been updated, redo it. If recovered by restarting, continue relay normal operation. If not recovered by restarting or redoing SW update, replace the relay, most probably hardware failure in CPU module.
Internal Fault System error	2	Runtime error: CPU internal fault	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault System error	2	Start up error: Card init fault	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recovered by restarting, check for example relay's Information menu to see which card(s) are not shown correctly and replace it (them).
Internal Fault File system error	7	Start up error or runtime error: file system error	Yes	No	Yes	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault Test	8	Internal fault test activated manually by the user.	No	No	-	Just check the "Internal fault test" -setting parameter position, if relay is in test mode
Internal Fault SW watchdog error	10	Start up error: Watchdog reset has occurred too many times within an hour. Note! This is different indication than Warning	No	No	Yes	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay.

Table continues on the next page

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
		code 10: Watchdog reset				
Internal Fault LHMI module	79	Start up error: EEPROM error in LHMI module. The fault indication may not be seen on the LHMI during the fault.	No	No	Yes	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, check LHMI connection cable and connection to be properly fixed. If then not recovered by restarting, exchange the LHMI module.
Internal Fault LHMI module	79	Runtime error: LHMI LCD error. The fault indication may not be seen on the LHMI during the fault.	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, check LHMI connection cable and connection to be properly fixed. If then not recovered by restarting, exchange the LHMI module.
Internal Fault RAM error	80	Runtime error: Error in the RAM memory on the CPU module.	No	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault ROM error	81	Runtime error: Error in the ROM memory on the CPU module.	Yes	No	Yes	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault EEPROM error	82	Start up error: Error in the EEPROM memory on the CPU module.	No	No	Yes	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault EEPROM error	82	Start up error: CRC check failure in the EEPROM memory on boot-up on the CPU module.	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault FPGA error	83	Runtime error: Error in the FPGA on the CPU module.	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.
Internal Fault RTC error	84	Start up error: Error in the RTC on the CPU module.	Yes	No	Yes	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, replace the relay, most probably hardware failure in CPU module.

Table continues on the next page

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
Internal Fault COM card error	116	Runtime error: Error in the COM card.	Yes	Yes (3)	No	Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the communication module in slot X000.
Internal Fault SO-relay(s), Slot C	-10	Runtime error: Faulty Signal Output relay(s) in card located in slot C.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot C.
Internal Fault SO-relay(s), Slot E	-11	Runtime error: Faulty Signal Output relay(s) in card located in slot E.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot E.
Internal Fault SO-relay(s), Slot A2	-12	Runtime error: Faulty Signal Output relay(s) in card located in slot A2.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot A2.
Internal Fault SO-relay(s), Slot B	-13	Runtime error: Faulty Signal Output relay(s) in card located in slot B.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot B.
Internal Fault SO-relay(s), Slot D	-14	Runtime error: Faulty Signal Output relay(s) in card located in slot D.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot D.
Internal Fault SO-relay(s), Slot F	-15	Runtime error: Faulty Signal Output relay(s) in card located in slot F.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot F.
Internal Fault SO-relay(s), Slot G	-16	Runtime error: Faulty Signal Output relay(s) in card located in slot G.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot G.
Internal Fault SO-relay(s), Slot A1	-17	Runtime error: Faulty Signal Output relay(s) in card located in slot A1.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by restarting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot A1.

Table continues on the next page

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
Internal Fault PO-relay(s), Slot C	-20	Runtime error: Faulty Power Output relay(s) in card located in slot C.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot C.
Internal Fault PO-relay(s), Slot E	-21	Runtime error: Faulty Power Output relay(s) in card located in slot E.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot E.
Internal Fault PO-relay(s), Slot A2	-22	Runtime error: Faulty Power Output relay(s) in card located in slot A2.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot A2.
Internal Fault PO-relay(s), Slot B	-23	Runtime error: Faulty Power Output relay(s) in card located in slot B	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot B.
Internal Fault PO-relay(s), Slot D	-24	Runtime error: Faulty Power Output relay(s) in card located in slot D.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot D.
Internal Fault PO-relay(s), Slot F	-25	Runtime error: Faulty Power Output relay(s) in card located in slot F.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot F.
Internal Fault PO-relay(s), Slot G	-26	Runtime error: Faulty Power Output relay(s) in card located in slot G.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot G.
Internal Fault PO-relay(s), Slot A1	-27	Runtime error: Faulty Power Output relay(s) in card located in slot A1.	Yes	Yes (3)	No	Check wirings. Restart the relay. If recovered by re-starting, continue relay normal operation. If not recover by restarting, exchange the hardware module in slot A1.
Internal Fault Conf. error, Slot C	-30	Start up error: Card in slot C is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot C is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Ex-

Table continues on the next page

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
						change the hardware module in slot C.
Internal Fault Conf. error, Slot E	-31	Start up error: Card in slot E is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot E is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the hardware module in slot E.
Internal Fault Conf. error, Slot A2	-32	Start up error: Card in slot A2 is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the communication card in slot A2 is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the communication module in slot A2.
Internal Fault Conf. error, Slot B	-33	Start up error: Card in slot B is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot B is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the hardware module in slot B.
Internal Fault Conf. error, Slot D	-34	Start up error: Card in slot D is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot D is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the hardware module in slot D.
Internal Fault Conf. error, Slot F	-35	Start up error: Card in slot F is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot F is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the hardware module in slot F.
Internal Fault Conf. error, Slot G	-36	Start up error: Card in slot G is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot G is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the hardware module in slot G.
Internal Fault Conf. error, Slot A1	-37	Start up error: Card in slot A1 is wrong type, is missing, does not belong to original configuration or card firmware is faulty.	No	No	Yes	Check that the card in slot A1 is proper type and properly installed. Then restart the relay. If does not then recover by restarting, it is hardware module failure most likely in question. Exchange the hardware module in slot A1.

Table continues on the next page

Fault indication	Fault code	Additional information	Fast self-recovery attempt	Slow 10min self-recovery (# of attempts)	Immediate IRF-mode	Action in permanent fault state
						change the hardware module in slot A1.
Internal Fault Card error, Slot C	-40	Card in slot C is faulty.	Yes	No	Yes	Exchange the hardware module in slot C.
Internal Fault Card error, Slot E	-41	Card in slot E is faulty.	Yes	No	Yes	Exchange the hardware module in slot E.
Internal Fault Card error, Slot A2	-42	Card in slot A2 is faulty.	Yes	No	Yes	Exchange the communication module in slot A2.
Internal Fault Card error, Slot B	-43	Card in slot B is faulty.	Yes	No	Yes	Exchange the hardware module in slot B.
Internal Fault Card error, Slot D	-44	Card in slot D is faulty.	Yes	No	Yes	Exchange the hardware module in slot D.
Internal Fault Card error, Slot F	-45	Card in slot F is faulty.	Yes	No	Yes	Exchange the hardware module in slot F.
Internal Fault Card error, Slot G	-46	Card in slot G is faulty.	Yes	No	Yes	Exchange the hardware module in slot G.
Internal Fault Card error, Slot A1	-47	Card in slot A1 is faulty.	Yes	No	Yes	Exchange the hardware module in slot A1.
Internal Fault 640-Prod. License error	-62	Runtime error: Product license error, license file is not found or is wrong	No	No	Yes	If SW update under Modification Sales has been carried out, redo the update. If not recovered, contact your nearest ABB representative to check the next possible corrective action.

6.2.2 Warnings

In case of a warning, the protection relay continues to operate except for those protection functions affected by the fault. The main unit status LED remains lit as during normal operation. If the device warning event is configured as alarms, the LHMI Home button flashes red.



If a warning appears, record the name and code so that it can be provided to ABB customer service. See the operation manual for more information on reading internal log files from the relay.

On the LHMI, an active warning is indicated with a yellow LED. More information about the warning and recovery options can be accessed by tapping More Information.

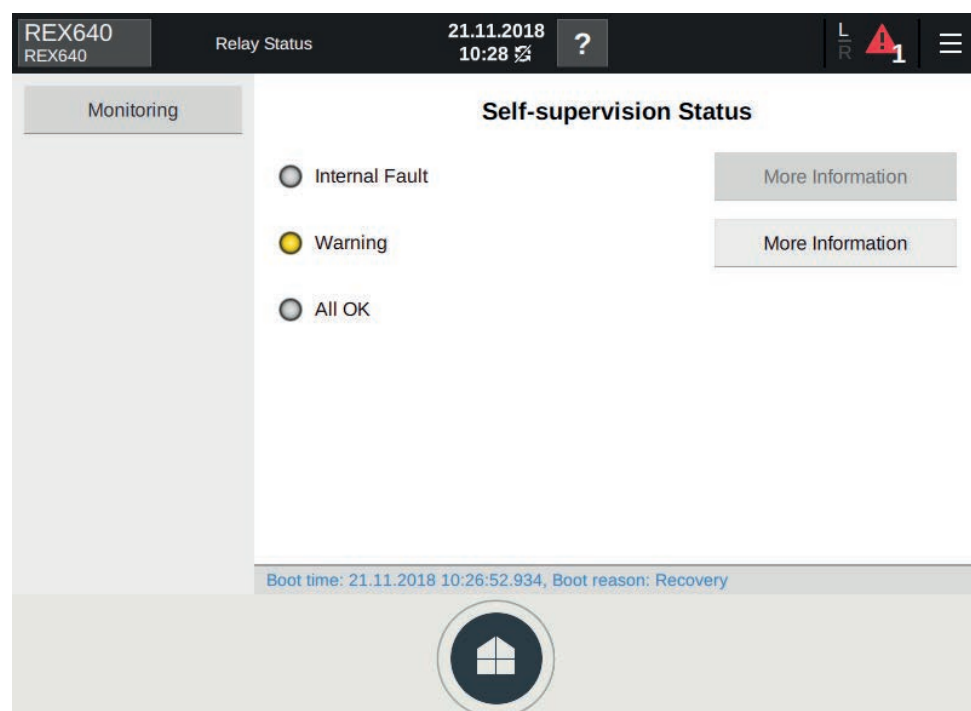


Figure 93: Active warning on local HMI

More information shows all active warnings and corresponding fault codes. In addition, a recovery procedure is described.

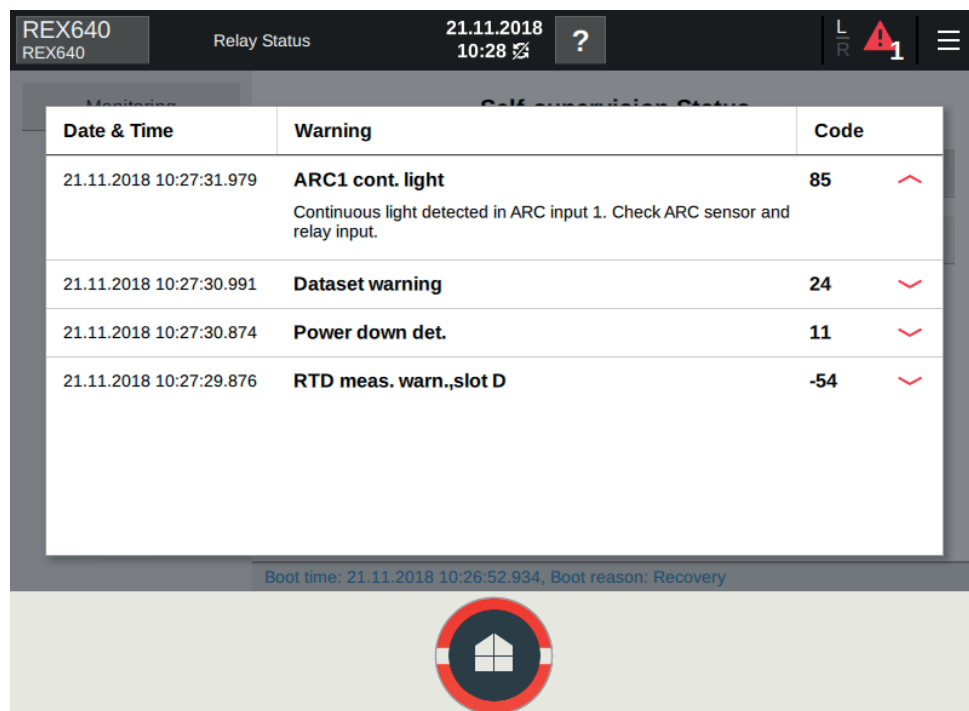


Figure 94: More information about the warning



The warning alarm is only displayed when configured in PCM600 event filtering.

Table 10: Warning indications and codes

Warning indication	Warning code	Additional information
Watchdog reset	10	A watchdog reset has occurred.
Power down det.	11	The auxiliary supply voltage has dropped too low.
DNP3 warning	22	Error in the DNP3 communication.
Dataset warning	24	Error in the Data set(s).
Report cont. warning	25	Error in the Report control block(s).
GOOSE contr. warning	26	Error in the GOOSE control block(s).
SCL config warning	27	Error in the SCL configuration file or the file is missing.
Logic warning	28	
SMT logic warning	29	
GOOSE input warning	30	
ACT warning	31	Analog channel configuration warning.
GOOSE rec. warning	32	
AFL warning	33	
SMV warning	34	Error in the SMV configuration.

Table continues on the next page

Warning indication	Warning code	Additional information
Comm. channel down	35	Redundant Ethernet (HSR/ PRP) communication interrupted.
Settings mismatch	36	Mismatch between parameter settings and application configuration.
Protection comm.	50	Error in protection communication.
ARC1 cont. light	85	A continuous light has been detected on the ARC light input 1.
ARC2 cont. light	86	A continuous light has been detected on the ARC light input 2.
ARC3 cont. light	87	A continuous light has been detected on the ARC light input 3.
ARC4 cont. light	88	A continuous light has been detected on the ARC light input 4.
RTD meas. warn.,slot D	-54	Abnormal signal from sensor(s) received in slot D.
RTD meas. warn.,slot C	-50	Abnormal signal from sensor(s) received in slot C.
mA output warn.,slot D	-24	Temporary error occurred in RTD module located in slot D.
mA output warn.,slot C	-20	Temporary error occurred in RTD module located in slot C.

6.2.3 Power supply module Ready LED and HMI Home button LED

Both power supply module Ready LED and LHMI Home button LED visualize the self-supervision state of the relay. [Table 11](#) shows how these states are indicated.

Table 11: Power supply module Ready LED and local HMI Home button LED

State	Power supply module Ready LED	LHMI Home button	Alarm acknowledged
Relay under normal operation and LHMI connected	Steady green	Steady green	N/A
Relay's IRF activated, but communicates with LHMI	HF blinking green	HF blinking red	N/A
Communication lost between Relay and LHMI, but no IRF	Steady green	HF blinking green	N/A
LHMI not running normally or in start-up initialization phase	Steady green	HF blinking green	N/A
Process related alarm active	Steady green	LF blinking red	No
Process related alarm active	Steady green	Steady red	Yes
Process related alarm has been active earlier, but is not any more active	Steady green	LF blinking red	No

Table continues on the next page

State	Power supply module Ready LED	LHMI Home button	Alarm acknowledged
Process related alarm has been active earlier, but is not any more active	Steady green	Steady green	Yes
Relay set to Test Mode	LF blinking green	LF blinking green	No

The physical SHMI Home button has two operation modes.

- On the SHMI's navigation page, the Home button indicates the combined status of all connected relays. If multiple relays have different statuses, the Home button shows the indication with the highest priority.
- On the HMI view, the Home button indicates the status of the respective relay as described in [Table 11](#).

6.3 Correction procedures

6.3.1 Creating relay backup in HMI

- Pair the HMI and the relay to activate the automatic backup. The relay backup is read and stored by the LHMI when any change in relay configuration files (see [Table 12](#) for details) or settings has occurred and 24 hours has elapsed from the last change. The SHMI reads a backup for all of the connected and paired relays.

Table 12: Configuration changes included in the relay backup

File or folder	Description	Part of backup and restore
.\language\	Folder containing HMI-specific language files	Yes
.\license\	640 license files	No New license files are delivered with the replacement relay.
.\pages\	640 HMI page configuration	Yes
.\SLD\	Single-line diagram related files	Yes
.\UAM\	User access management related files	Yes
ACT_graph.cact		Yes
conf.xml.gz	Relay's application configuration	Yes
conf.xml.gz.MD5	Checksum for application configuration	Yes
configsum.xml	Contains checksums of different items and change information. It is also used in the relay to verify file checksums (for example, UAM files).	Yes
done.txt	When this file is updated (date modified changes), relay knows that its configuration has changed. When the relay backup is restored, this file contains: Updated over C:/backup.zip	Yes
hmi.xml	HMI event configuration	Yes
measurements.xml	HMI-specific measurement configuration (used by phasor and measurement pages).	Yes
default_measurements.xml		No
characteristics.xml		No
udn.xml	Use-defined naming	Yes



When the relay is in IRF error (the Home button flashes red fast), the backup is not made.



The relay's device certificate and the CA root certificate are not part of the backup. If PKI has been configured, this must be reconfigured using the corresponding tools. In addition, when PKI is in use, CAM settings are not restored to avoid the condition where the relay is not able to contact the configured CAM server.

6.3.2 Rebooting the software

1. Select **Configuration > General > Software reset**.
2. Tap **Edit**, select **Activate** and tap .

6.3.3 Restoring factory settings

In case of configuration data loss or any other file system error that prevents the protection relay from working properly, the whole file system can be restored to the original factory state. All default settings and configuration files stored in the factory are restored. Only the ADMINISTRATOR can restore the factory settings.

- Select **Configuration > General > Factory setting** to restore factory settings.
- Tap **Edit**, select **Activate** and tap .

The protection relay restores the factory settings and restarts.



Avoid unnecessary restoring of factory settings, because all the parameter settings written to the relay will be overwritten with the default values. During normal use, a sudden change of the settings can cause a protection function to trip.

6.3.4 Restoring relay backup from local HMI

1. Connect the LHMI to the relay

2. In the **Pair Panel & Relay** dialog box, tap **Pair**.

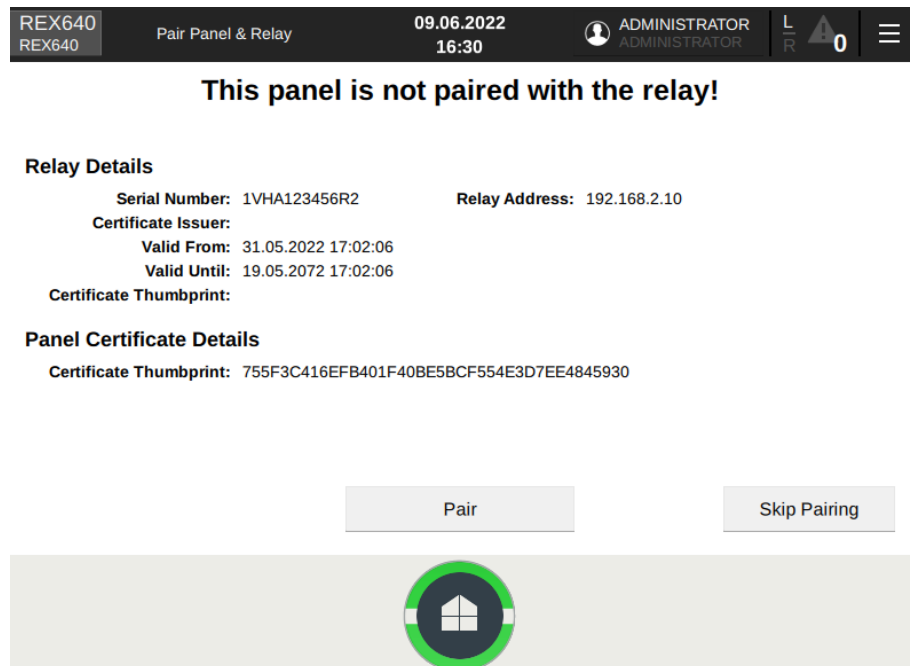


Figure 95: Panel not paired with the relay

The **Restore Configuration** dialog box automatically opens if the LHMI has a compatible backup available.

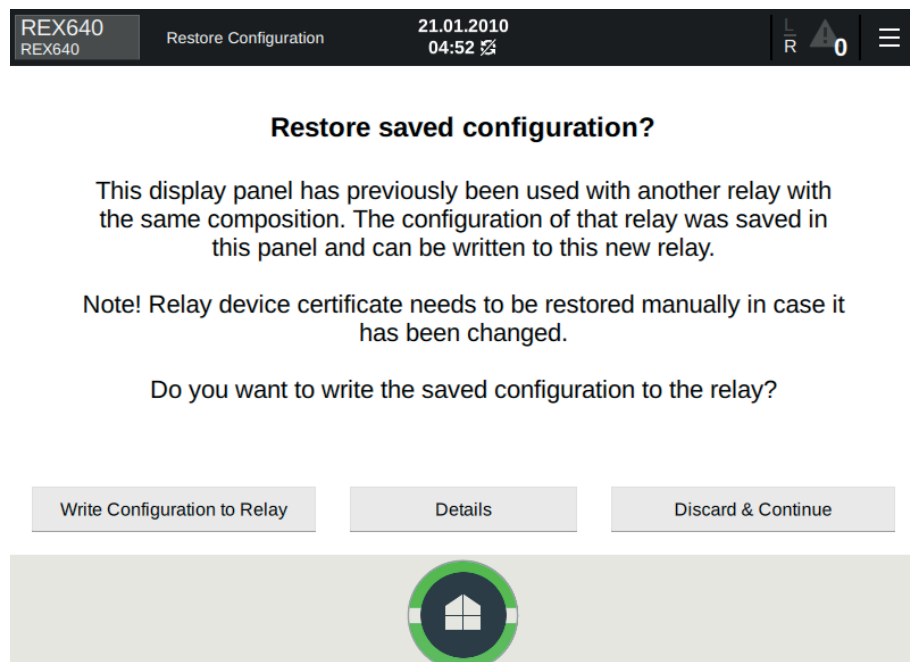


Figure 96: Restoring saved configuration

3. Tap **Details** to see the differences in product and system identifiers between the backup and the new relay.

<div> <div>REX640</div> <div>Restore Configuration</div> <div>21.01.2010 04:53</div> <div> <div>L</div> <div>R</div> <div>0</div> <div>≡</div> </div> </div>		
Relay Information	Backup Value in LHMI	Relay Value
Type	REX640	REX640
Product version	1	1
Serial number	1VHA123457R2	1VHA123456R2
Production date	14.12.2017 00:00:00.000	14.12.2017 00:00:00.000
SW version	build.2316	build.2316
SW date	25.03.2019 20:28:00.000	25.03.2019 20:28:00.000
SW number	2RAA00XXXX	2RAA00XXXX
Interface level	0	0
Order code	REX640_10001	REX640_10001
Composition code	REX640B10NN +COM2+BIO1+AIM1+PSM2+APP1+AP P2+CMP1+LNG1+SCT1+MCT1+PCL1	REX640B10NN +COM2+BIO1+AIM1+PSM2+APP1+APP2 +APP3+APP4+APP5+APP6+APP7+APP8+ APP9+APP10+APP11+APP12+APP13+AP P14+CMP1+LNG1+SCT1+MCT1+PCL1
<div> <div>Write Configuration to Relay</div> <div>Details</div> <div>Discard & Continue</div> </div>		

Figure 97: Viewing the details of the backup and the new relay

LHMI restores the relay backup if the relay's serial number is different from that in the backup and the composition code of the relay contains all the options in the backup. The relay's composition code may contain more options.

4. Tap **Write Configuration to Relay**. The relay boots so that the new configuration can be taken into use.

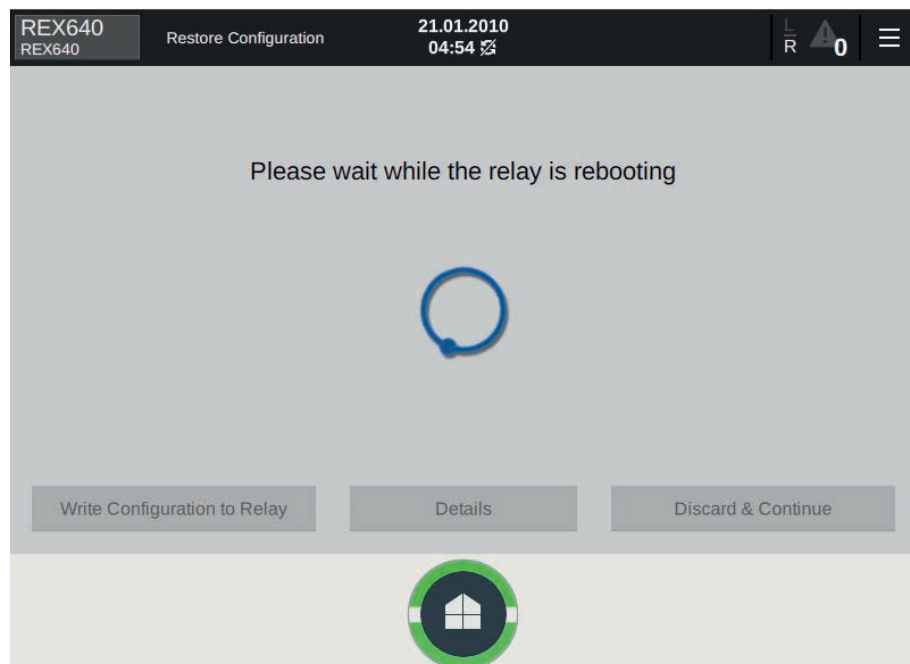


Figure 98: Relay rebooting

The following dialog box appears when the relay backup is restored.

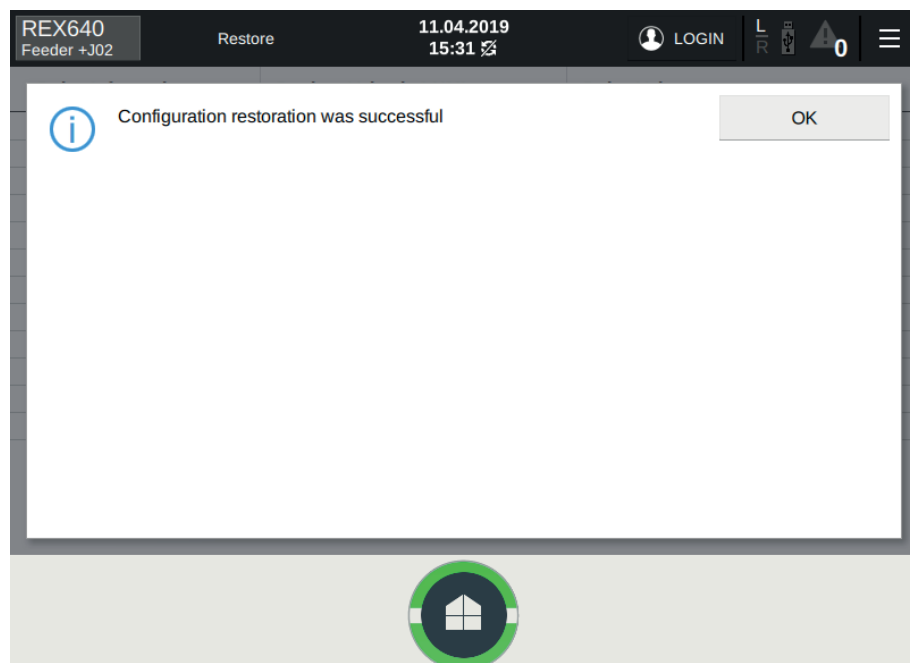


Figure 99: Backup restoring succeeds

If errors occur, the error details are shown.



Figure 100: Backup restoring fails

6.3.5 Restoring relay backup from switchgear HMI



This chapter describes how configuration backup is restored from SHMI.

As a precondition for restoring a backup from the SHMI, the replacement relay's license must include the same or wider capabilities than the faulty relay's license. The replacement relay must have the same HW modules in the same slots as the faulty relay although the other HW modules may differ.

1. Configure the faulty relay's network address to the replacement relay, and connect it to the station network so that it can be reached by the SHMI. The network address can be set by using the WHMI.
2. Go to the SHMI's navigation page and tap the menu button.
3. Tap **Connect External**.
4. Type the replacement relay's IP address and pair with the relay. The replacement relay's HMI opens on the SHMI.
5. On the HMI view, tap the menu button and select **Testing and Commissioning and Restore**.
6. Select a backup to be restored from the list of available backups and tap **Restore**.

If the Restore selection is not enabled, the relay is incompatible with the selected backup.

6.3.6 Setting passwords

IED Users in PCM600 is used to manage user accounts.

User accounts can be created under any default roles (VIEWER, OPERATOR, ENGINEER and ADMINISTRATOR) or additional roles (INSTALLER, SECADM, SECAUD and RBACMNT). Only Administrator can create user accounts and update the roles-to-rights mapping. Administrator needs to share the default password generated for the user account by the tool with the users and recommend the user to change the password.

1. In IED Users or on the LHMI, change the password of the user account.
2. Log in as administrator to reset the users' passwords. For more information on user management, see the cyber security deployment guideline.



If the administrator password is lost, contact ABB's technical customer support to retrieve the administrator level access.

6.3.7 Identifying relay application problems

- Check that the function is on.
- Check the blocking.
- Check the mode.
- Check the measurement value.
- Check the connection to trip and disturbance recorder functions.
- Check the channel settings.

6.3.7.1 Inspecting wiring

The physical inspection of wiring connections often reveals the wrong connection for phase currents or voltages. However, even though the phase current or voltage connections to protection relay terminals might be correct, wrong polarity of one or more measurement transformers can cause problems.

- Check the current or voltage measurements and their phase information from **Measurements page > Phasors**.
- Check that the phase information and phase shift between phases is correct.
- Correct the wiring if needed.
- Check the actual state of the connected binary inputs from **Testing and Commissioning > View I/O**.
- Test and change the output states manually in **Testing and Commissioning > Force Outputs**.

6.3.7.2 Sample data interruptions

Occasionally protection relays can receive corrupted or faulty measurement data during runtime. In these cases the operation system halts the corresponding application execution until correct data is received. In case of permanent faults, the measurement chain should be checked to remove the origin of the faulty measurement data.



In case of persistent faults originating from protection relay's internal faults, contact ABB for repair or replacement actions.

7 Commissioning

7.1 Commissioning checklist

Familiarize yourself with the protection relay and its functionality before you start the commissioning work.

- Ensure that you have all the needed station drawings such as single line and wiring diagrams.
- Ensure that your version of the technical manual applies to the protection relay version you test.
- Ensure that your setting software and connectivity packages work with the protection relay version you test.
- Find out if you need any additional software.
- Ensure that you have the relay settings either on paper or in electronic format. The settings and logic should be well documented.
- Inspect the settings to ensure that they are correct.
- Ensure that you have the correct cable to connect your PC to the protection relay's communication port. The RJ-45 port supports any CAT 5 Ethernet cable but the recommendation is STP.
- Test your PC's communication port before you go to the site.
- Find out who to contact if you have trouble and make sure you have a means to contact them.
- Find out who is responsible for the settings.
- Ensure that you have with you the proper test equipment and all needed connection cables.
- Ensure that the owner of the switchgear familiarizes you with the work site and any special aspects of it.
- Ensure that you know how to operate in emergency situations. Find out where the first aid and safety materials and exit routes are.



Ensure that self-supervision is not indicating active internal faults before starting commissioning work.

7.2 Checking installation

7.2.1 Checking power supply

- Check the following for both the relay and LHMI, if used.
 - The auxiliary supply voltage must remain within the permissible input voltage range under all operating conditions.

- The polarity must be correct before connecting auxiliary power supply.

7.2.2 Checking CT circuits



Check that the wiring is in strict accordance with the supplied connection diagram.

The CTs must be connected in accordance with the connection diagram of the project, both with regards to phases and polarity. The following tests are recommended for every primary CT or CT core connected to the protection relay.

- Primary injection test to verify the current ratio of the CT, the correct wiring up to the protection relay and correct phase sequence connection (that is L1, L2, L3.)
- Polarity check to prove that the predicted direction of the secondary current flow is correct for a given direction of the primary current flow. This is an essential test for the proper operation of the directional function, protection or measurement in the protection relay.
- CT secondary loop resistance measurement to confirm that the current transformer secondary loop DC resistance is within specification and that there are no high resistance joints in the CT winding or wiring.
- CT excitation test to ensure that the correct core in the CT is connected to the protection relay. Normally only a few points along the excitation curve are checked to ensure that there are no wiring errors in the system, for example, due to a mistake in connecting the CT's measurement core to the protection relay.
- CT excitation test to ensure that the CT is of the correct accuracy rating and that there are no short circuited turns in the CT windings. Manufacturer's design curves should be available for the CT to compare the actual results.
- Earthing check of the individual CT secondary circuits to verify that each three-phase set of main CTs is properly connected to the station earth and only at one electrical point.
- Insulation resistance check.



Both the primary and the secondary sides must be disconnected from the line and the protection relay when plotting the excitation characteristics.



If the CT secondary circuit is opened or its earth connection is missing or removed without the CT primary being de-energized first, dangerous voltages may be produced. This can be lethal and cause damage to the insulation. The re-energizing of the CT primary should be prohibited as long as the CT secondary is open or unearthed.

7.2.3 Checking VT circuits

Check that the wiring is in strict accordance with the supplied connection diagram.



Correct possible errors before continuing to test the circuitry.

Test the circuitry.

- Polarity check
- VT circuit voltage measurement (primary injection test)
- Earthing check
- Phase relationship
- Insulation resistance check

The polarity check verifies the integrity of circuits and the phase relationships. The polarity must be measured as close to the protection relay as possible.

The primary injection test verifies the VT ratio and the wiring all the way from the primary system to the protection relay. Injection must be performed for each phase-to-neutral circuit and each phase-to-phase pair. In each case, voltages in all phases and neutral are measured.

7.2.4 Checking binary input and output circuits

7.2.4.1 Checking binary input circuits

- Preferably, disconnect the binary input connector from the binary input cards.
- Check all the connected signals so that both the input level and the polarity are in accordance with the protection relay specifications.



Do not use AC voltage. Binary inputs are rated for DC voltage only.

7.2.4.2 Checking binary output circuits

- Preferably, disconnect the binary output connector from the binary output cards.
- Check all connected signals so that both load and voltage are in accordance with the protection relay specifications.

7.3 Authorizations

7.3.1 User authorization

The user categories have been predefined for the LHMI and WHMI, each with different rights and default passwords.

Passwords are settable for user accounts in all roles. Only the following characters are accepted.

- Numbers 0-9
- Letters a-z, A-Z
- Space
- Special characters !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

By default, the password policies in the protection relay are as follows:

- Minimum password length: 6
- Maximum password length: 20
- Minimum uppercase characters: 0
- Minimum numeric: 0
- Minimum special characters: 0

The protection relays are delivered from the factory with default passwords. It is required to change the default passwords.

Table 13: Predefined users, their passwords and roles

Username	Password	Predefined role
VIEWER	remote0001	VIEWER
OPERATOR	remote0002	OPERATOR
ENGINEER	remote0003	ENGINEER
ADMINISTRATOR	remote0004	ADMINISTRATOR

The following enforcing rules of the password policies can be customized in IED Users in PCM600.

- Option of enabling or disabling password policies (disabling sets default policies as described above)
- Minimum password length
- Use of uppercase characters
- Use of lowercase characters
- Use of numbers
- Use of special characters

It is required to login as an Administrator in PCM600 in order to change the password policies.

Each user can change their own password, but only Administrator can reset the passwords of other users.

On Factory restore, factory default usernames, passwords and password policies are restored.



User authorization is disabled by default and can be enabled via the LHMI **Configuration > Authorization > Passwords**.



For user authorization for PCM600, see the PCM600 documentation.



Policy change and configuration is not allowed when the protection relay is in offline mode in PCM600.



If the last ADMINISTRATOR password is lost, contact ABB's technical customer support to retrieve the administrator level access.

7.4 Setting protection relay and communication

7.4.1 Setting the communication between protection relays and PCM600

The communication between the protection relay and PCM600 is independent of the used communication protocol within the substation or to the NCC. It can be seen as a second channel for communication.

The media is always Ethernet and communication is based on TCP/IP.

Each protection relay has an Ethernet front connector for PCM600 access. Depending on the station concept and the used station protocol, additional Ethernet interfaces may be available on the rear side of the protection relay. All Ethernet interfaces can be used to connect PCM600.

When an Ethernet based station protocol is used, the PCM600 communication can use the same Ethernet port and IP address. The protection relay is able to separate the information belonging to the PCM600 dialog.

To configure the physical connection and the IP addresses:

1. Set up or get the IP addresses of the protection relays.
2. Set up the PC for a direct link or connect the PC or workstation to the network.
3. Configure the IP addresses in the PCM600 project for each protection relay.
The addresses are used for communication between protection relays and PCM600.

7.4.1.1 Communication between PCM600 and protection relay

The communication between the protection relay and PCM600 is independent of the used communication protocol within the substation or to the NCC.

All communication is done over Ethernet using either IEC 61850 or the FTP/FTPS protocol.

When an Ethernet-based station protocol is used, the same Ethernet port and IP address can be used for PCM600 communication.

Two basic variants have to be considered for the connection between PCM600 and the protection relay.

- Direct point-to-point link between PCM600 and service port X1.2 on the protection relay's LHMI or, if an LHMI is not used, the HMI port X0 of the communication module
 - Indirect link via station LAN or remotely via network
1. If needed, the IP address for the protection relay is set.
 2. A PC or workstation is set up for a direct link (point-to-point), or the PC or workstation is connected to the LAN/WAN network.
 3. The protection relays' IP addresses in the PCM600 project are configured to match the IP addresses of the physical IEDs.

4. Technical keys of the IEDs in the PCM600 project are configured to match the technical keys of the physical IEDs.

For successful protection relay engineering and usage, the workstation firewall TCP and UDP port configurations should be checked, especially for IEC 61850 and FTP. Other protocols are not used for engineering or they are optional.

Table 14: IP ports used by the relay

Port number	Type	Default state	Description
21	TCP	Open	Explicit FTP over TLS
22	TCP	Closed	SSH (HMI only, normally closed)
102	TCP	Open	IEC 61850
443	TCP	Open	Web server HTTPS
123	UDP	Client service not active by default in relay	SNTP
502	TCP	Closed	Modbus TCP
2404	TCP	Closed	IEC 60870-5-104 TCP
20000	TCP	Closed	DNP3 TCP
20000	UDP	Closed	DNP3 UDP
1468	TCP	Closed	CAL
514	UDP	Closed	CAL
49220...49235	TCP	Closed	Ports open on demand for data transfer when FTP PASV command is given

7.4.2 Communication settings

7.4.2.1 Ethernet ports

The protection relay allows the use of a secondary IP address for the station ports on the communication modules COM1001...COM1003. This secondary IP network is assigned to a single Ethernet port and can be used to make separate networks for different communication protocols or, for example, a separate service network for configuration purposes. Multicast station/bus communication, such as IEC 61850-9-2 LE sampled values and GOOSE, is only supported on the Network 1 interface. The parameters for setting the secondary IP network are located under **Configuration > Communication > Ethernet > Network 2 address**.

Table 15: Secondary IP address parameters

Parameter	Options	Description
Configuration/Communication/Ethernet/Network 2 address/ Enable	False (default)	Network 2 disabled
	TRUE	Network 2 enabled
Configuration/Communication/Ethernet/Network 2 address/IP address	0.0.0.0	IP address for Network 2
Configuration/Communication/Ethernet/Network 2 address/IP address	0.0.0.0	Subnet address for Network 2
Configuration/Communication/Ethernet/Network 2 address/MAC address	xx-xx-xx-xx-xx-xx	MAC address for Network 2

The IP address for Network 2 is disabled by default settings, and all Ethernet ports are assigned to the same IP address used in the Network 1 address menu **Configuration > Communication > Ethernet > Network 1**. If Network 2 is taken into use by the setting Enable="True" (requires reboot), the interlink port X3 of the COM module is assigned to this second network, using the IP address and subnet parameters in the Network 2 address menu **Configuration > Communication > Ethernet > Network 2 address**.



If the Network 2 interface is enabled, PTP time synchronization and SMV/GOOSE multicast are disabled for that port.

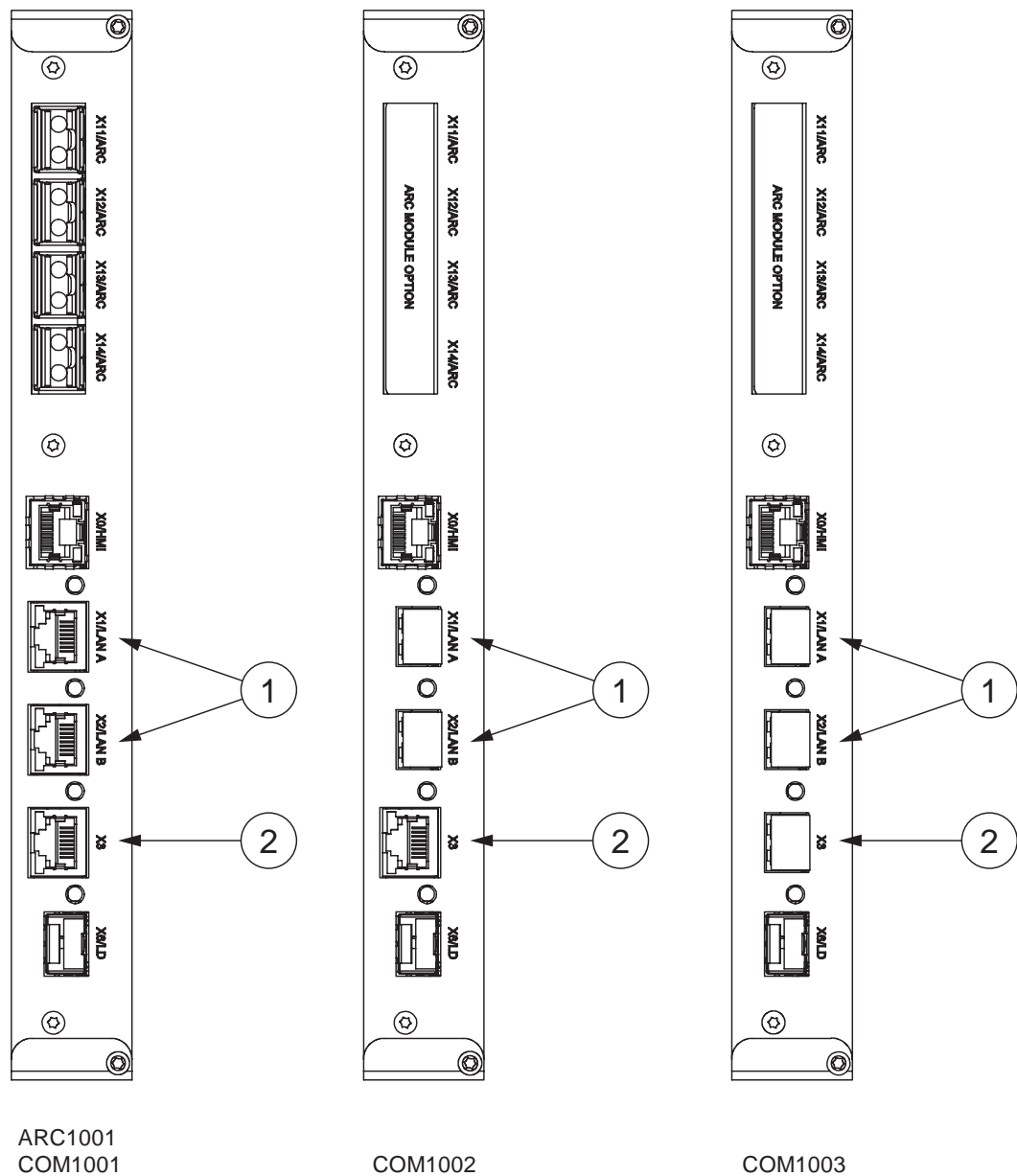


Figure 101: Ethernet modes with Network 1 and Network 2

- 1 Network 1
- 2 Network 1/Network 2

7.4.2.2

Protocol control

It is possible to allow or block different protocols for different network interfaces in the protection relay using the parameters in **Configuration > Communication > Protocols > Network1**, **Configuration > Communication > Protocols > Network2** and **Configuration > Communication > Protocols > HMI Port**.

All protocols are allowed for each network by default, and can be separately disabled.

Table 16: Protocol control in the protection relay

Parameter	Options	Description
Configuration/Communication/Protocols/Network1/FTP	Off	Denies FTP and FTPS
	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Configuration/Communication/Protocols/Network2/FTP	Off	Denies FTP and FTPS
	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Configuration/Communication/Protocols/HMI Port/FTP	Off	Denies FTP and FTPS
	On	Allows FTP and FTPS
	Secure (Default)	Allows FTPS only
Configuration/Communication/Protocols/Network1/HTTPS	Off	Denies HTTPS
	On (Default)	Allows HTTPS
Configuration/Communication/Protocols/Network2/HTTPS	Off	Denies HTTPS
	On (Default)	Allows HTTPS
Configuration/Communication/Protocols/Network1/MMS	Off	Denies IEC 61850 MMS
	On (Default)	Allows IEC 61850 MMS
Configuration/Communication/Protocols/Network2/MMS	Off	Denies IEC 61850 MMS
	On (Default)	Allows IEC 61850 MMS
Configuration/Communication/Protocols/HMI Port/MMS	Off	Denies IEC 61850 MMS
	On (Default)	Allows IEC 61850 MMS
Configuration/Communication/Protocols/Network1/DNP	Off	Denies DNP3
	On (Default)	Allows DNP3
Configuration/Communication/Protocols/Network2/DNP	Off	Denies DNP3
	On (Default)	Allows DNP3
Configuration/Communication/Protocols/Network1/Modbus	Off	Denies Modbus
	On (Default)	Allows Modbus
Configuration/Communication/Protocols/Network2/Modbus	Off	Denies Modbus
	On (Default)	Allows Modbus
Configuration/Communication/Protocols/Network1/IEC-60870-5-104	Off	Denies IEC 60870-5-104
	On (Default)	Allows IEC 60870-5-104
Configuration/Communication/Protocols/Network2/IEC-60870-5-104	Off	Denies IEC 60870-5-104
	On (Default)	Allows IEC 60870-5-104

7.4.2.3

Protocol write access rights

Write access rights are configurable for FTP, MMS, and HTTPS protocols in **Configuration > Authorization**. The write access parameters are used to narrow down services that allow setting changes on different network interfaces. Disabling

the FTP and IEC 61850 MMS write access on Network 1 and 2 prevents the user from updating the configuration to the protection relay from PCM600. Disabling the HTTPS write access prevents the user from writing setting changes from WHMI.

Table 17: Protocol write access in the protection relay

Parameter	Options	Description
Configuration/Authorization/Network1/FTP write access	Off	FTP write access denied for Network 1
	On (Default)	FTP write access allowed for Network 1
Configuration/Authorization/Network1/MMS write access	Off	IEC 61850 MMS write access denied for Network 1
	On (Default)	IEC 61850 MMS write access allowed for Network 1
Configuration/Authorization/Network1/HTTPS write access	Off	HTTPS write access denied for Network 1
	On (Default)	HTTPS write access allowed for Network 1
Configuration/Authorization/Network2/FTP write access	Off	FTP write access denied for Network 2
	On (Default)	FTP write access allowed for Network 2
Configuration/Authorization/Network2/MMS write access	Off	IEC 61850 MMS write access denied for Network 2
	On (Default)	IEC 61850 MMS write access allowed for Network 2
Configuration/Authorization/Network2/HTTPS write access	Off	HTTPS write access denied for Network 2
	On (Default)	HTTPS write access allowed for Network 2
Configuration/Authorization/HMI/FTP write access	Off	FTP write access denied for the HMI port
	On (Default)	FTP write access allowed for the HMI port
Configuration/Authorization/HMI/MMS write access	Off	IEC 61850 MMS write access denied for the HMI port
	On (Default)	IEC 61850 MMS write access allowed for the HMI port



PCM600 is using FTP or FTPS protocol to communicate with the protection relay. If the FTP write access is disabled for a network PCM600 functionality is limited to support read operations only from Disturbance handling, Event viewer and Parameter Setting.



Enabling Network 2 IP address requires additional configuration in PCM600 to define IEC 61850 subnetworks. This configuration is done via Ethernet Configuration and IEC 61850 Configuration in PCM600.

7.4.2.4 Physical locations of the serial channels

The physical location of the COM1 and COM2 drivers depends on the link mode used which, in turn, depends on the used communication hardware option. Serial channels can be found on communication boards COM1004...COM1005.

- X7 is the fiber-optic interface. Only driver COM2 can be configured into fiber-optic mode.
- X8 is the RS-485/IRIG-B interface. Both drivers COM1 and COM2 can be configured to this interface: COM1 and COM2 can act as two RS-485 2-wire links or, alternatively, COM1 can act as one single RS-485 4-wire link. Both ports are galvanically isolated serial communication ports.

Table 18: Connector X8 signals

Pin No	Pin name	Description	Alternative
1	GND	EARTH	
2	GNDC	GND connected to earth via 1nF capacitor	
3	NC		
4	IRIG-B -	ISOL2_GND	
5	IRIG-B +		
6	ISOL_GND	RS485 GND	
7	RS485 B1/-	2-wire -, COM1	4-wire TX pair, COM1
8	RS485 A1/+	2-wire +, COM1	4-wire TX pair, COM1
9	RS485 B2/-	2-wire -, COM2	4-wire RX pair, COM1
10	RS485 A2/+	2-wire +, COM2	4-wire RX pair, COM1

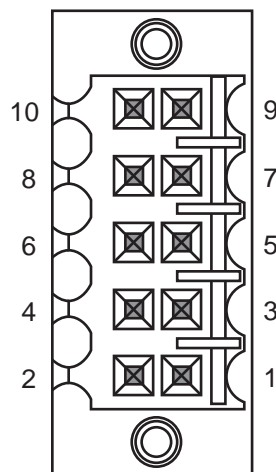


Figure 102: X8 connector pinout for socket on communication board

Table 19: LED configuration (COM1004...COM1005)

LED	Description
X1	X1 LANA
X2	X2 LANB
X6	X6 LD
X7 TX	FO-UART
X8 TX	RS-485/COM2
X8 TX	RS-485/COM1
IRIG-B	IRIG-B

7.4.2.5 Assigning of a serial communication protocol to a COM serial port

The settings of the serial communication protocol instance include a setting parameter, called either *Port* or *Serial port*, which is used to select the COM1 or COM2 setting.



Since not all serial protocol standards allow changes in link parameters, all link setting parameters are not found in the COMn settings. Additional link setting parameters are found in the setting parameter list of the used serial protocol.

7.4.2.6 Serial link diagnostics and monitoring

Serial communication diagnostics and monitoring is divided between the serial link driver and the serial communication protocol. The lower-level physical and protocol-independent aspects of the UART-based serial communication are monitored in the serial link driver. Diagnostic counters and monitoring values are located on the HMI under **Monitoring > Communication > COMn** (n= 1,2,...).

Depending on the communication protocol, the serial driver software receives single characters or complete protocol frames, based on the frame start/stop characters or on link frame timing.

Table 20: Setting parameters

Parameter	Description
Fiber mode	Defines the fiber-optic mode used. Setting "No fiber" is the same as galvanic mode.
Serial mode	Used for galvanic RS-485 modes 2- or 4-wire. This setting is relevant only if Fiber mode is set to "No fiber".
Baudrate	Communication speed used.

Table 21: Diagnostic counters and indications

Counters	Description
Characters received	Counts all incoming non-erroneous characters. This counter operates regardless of whether the serial driver is set to detect a whole protocol link frame or just separate characters.
Frames received	Counts all protocol-specific non-erroneous frames received. Protocol-specific frames can be based on timing (for exam-

Table continues on the next page

Counters	Description
	ple, Modbus RTU) or on special start and stop characters (for example, Modbus ASCII).
Frames discarded	Counts all protocol-specific erroneous frames received. If the driver detects an error while receiving a frame, the whole frame is automatically discarded. This also means that the protocol in question never receives a faulty link frame from the driver. When this counter is incremented, one of the detailed error counters (Parity, Overrun, Framing) can also be incremented.
Frames transmitted	Counts all protocol-specific frames transmitted from the COM channel.
Collisions	Counts the number of transmission collisions that have occurred. Used in RS-485 mode by some protocols where transmissions could collide with reception. For example, DNP3 unsolicited reporting mode.
Parity errors	Counts the number of parity errors detected in characters received.
Overrun errors	Counts the number of overrun errors detected in characters received.
Framing errors	Counts the number of framing errors detected in characters received.
Link status	In write direction: By writing value 1 to this parameter, all the diagnostic counters are reset to 0.
Link status	In monitoring direction: If the driver instance is in use by any communication protocol, the monitoring value shows value 1. Otherwise, the value is 0.

7.4.2.7

Defining Ethernet port settings



Change the Ethernet port settings primarily via PCM600 to ensure that PCM600 is able to export a consistent configuration to SYS600. Ethernet port settings are recommended to be changed only when the device is stand-alone and properly configured.

1. Select **Configuration > Communication > Ethernet > Network1 address** or **Configuration > Communication > Communication > Ethernet > Network2 address**.
2. Define the settings for Network1 or Network2.
 - IP address
 - Subnet mask
 - Default gateway of the optional rear port Ethernet connector

7.4.2.8

Defining serial port settings

1. Select **Configuration > Communication > COM1** or **COM2**.
2. Define the settings for the serial port.

It is possible to change the general serial communication parameters per port. Select fiber or galvanic mode with the proper baud rate.

7.4.2.9 **Setting communication protocol parameters**

1. Select **Main menu > Configuration > Communication > <protocol>**.
2. Change the protocol specific settings.
Possible settings to be changed are, for example, the selected communication port, address and link mode.

7.4.2.10 RS-485 bias and termination settings

A 6 x DIP switch is located on the COM1004...COM1005 cards. The COM card needs to be pulled out from the relay case to access the switch. See [Figure 103](#) for the location of the switch. RS-485 biasing and termination settings are possible through this switch. If the switch is in “OFF” position, bias and termination are disabled and in “ON” position, they are enabled.

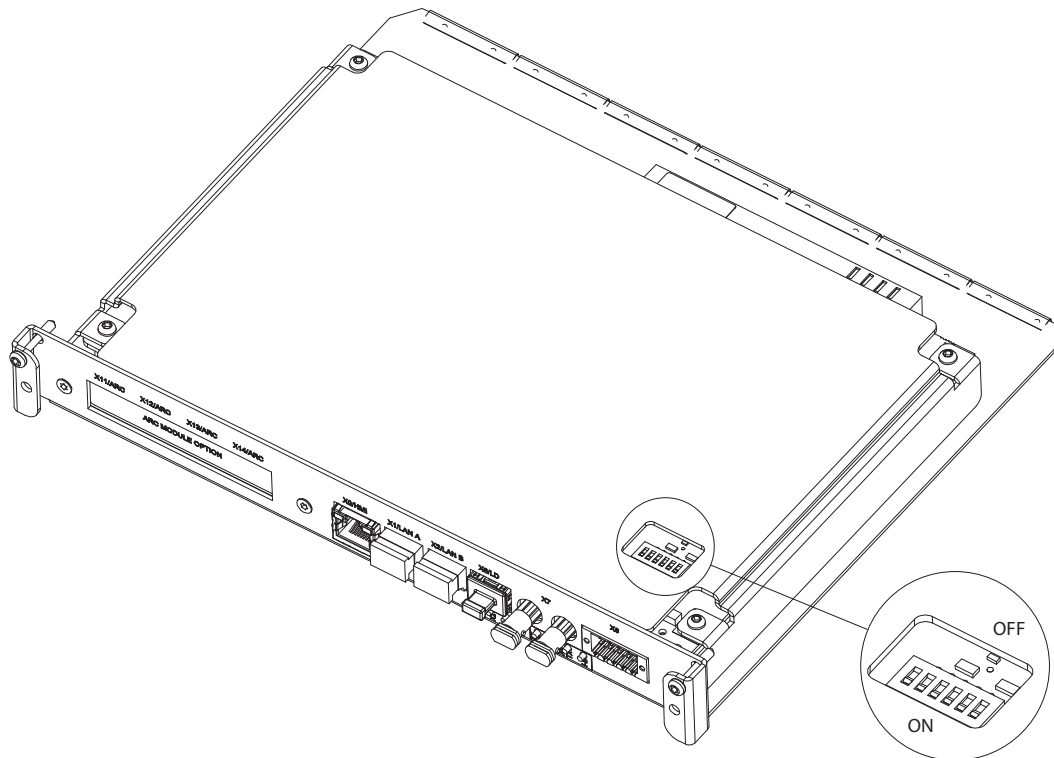


Figure 103: DIP switches on the COM1004...COM1005 cards

Table 22: Bias and termination DIP switch

Switch	Signal	X8 pin	Type
1	RS485_A1/+	8	Bias
2	RS485_A1/+ RS485_B1/-		Bus termination
3	RS485_B1/-	7	Bias
4	RS485_A2/+	10	Bias
5	RS485_A2/+ RS485_B2/-		Bus termination
6	RS485_B2/-	9	Bias

7.4.3 Connecting and setting HMI

- Connect the LHMI to the relay either directly from the main unit port X1.1 to the relay's X0/HMI port or through station network from the main unit port X1.1 to the relay's Network 1 port. The HMI's service port X1.2 is intended for local service access to the relay using PCM600 or the WHMI.
- Always connect the SHMI through the station network.
- Depending on the planned network topology communication, adapt the HMI settings to establish communication between the relay and the HMI. The service port settings must be set correctly to allow access to the relay either directly or through the station network.

Table 23: HMI settings

Communication parameter	Description
Main Unit Port/Automatic Address	Automatically obtains the address for main unit port from the relay's HMI port
Main Unit Port/Address	Static address used when the relay is connected to the station network
Main Unit Port/Netmask	Static network mask used when the relay is connected to the station network
Main Unit Port/Gateway	Gateway enabled when router is used between the relay and the HMI
Main Unit Port/Gateway Address	Router address
Service Port/Address	Static address for the service port
Service Port/Netmask	Static network mask for the service port
Service Port/Enable DHCP server	Normally enabled to route service port automatically to the main unit port and the relay



Configure the HMI service port and the main unit port to separate subnetworks.



Service port DHCP server routes the main unit network automatically to the service port.

7.4.3.1 Connecting local HMI directly to relay

- Use a CAT 6 S/FTP cable to connect the LHMI to the protection relay.
- Connect the cable to the X1.1/Main unit connector on the LHMI and to the X0/HMI connector on the protection relay's communication module.

Table 24: Example of communication settings for direct local HMI connection

Parameter		Value
HMI communication parameter	Main Unit Port/Automatic Address	Checked
	Main Unit Port/Address	-
	Main Unit Port/Netmask	-
	Main Unit Port/Gateway	Not checked
	Main Unit Port/Gateway Address	-
	Service Port/Address	192.168.1.1
	Service Port/Netmask	255.255.255.0
	Service Port/Enable DHCP server	Checked
REX640 communication parameters	Configuration/Communication/Ethernet/HMI/IP address	192.168.0.254
Computer network adapter for HMI service port	IP address	Obtain automatically

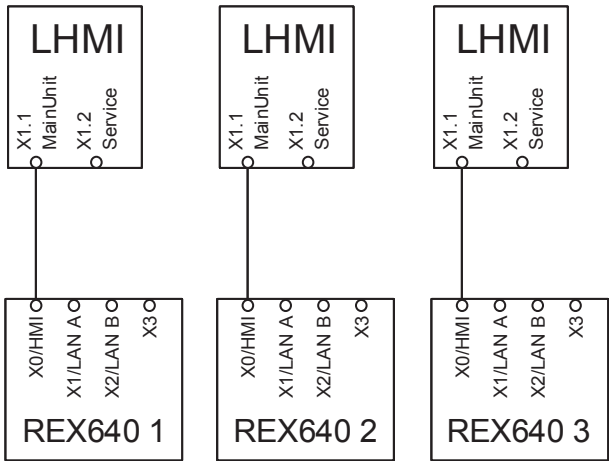


Figure 104: Example of direct local HMI connection

7.4.3.2 Connecting local HMI to a relay through station network

PCM600 or WHMI can be used to read the network settings of the relay's station port via **Configuration > Communication > Ethernet > Network1 address**.

1. On the LHMI, tap **Network Settings** to configure the network settings of the main unit port X1.1.

Network settings are also available as an Advanced page.

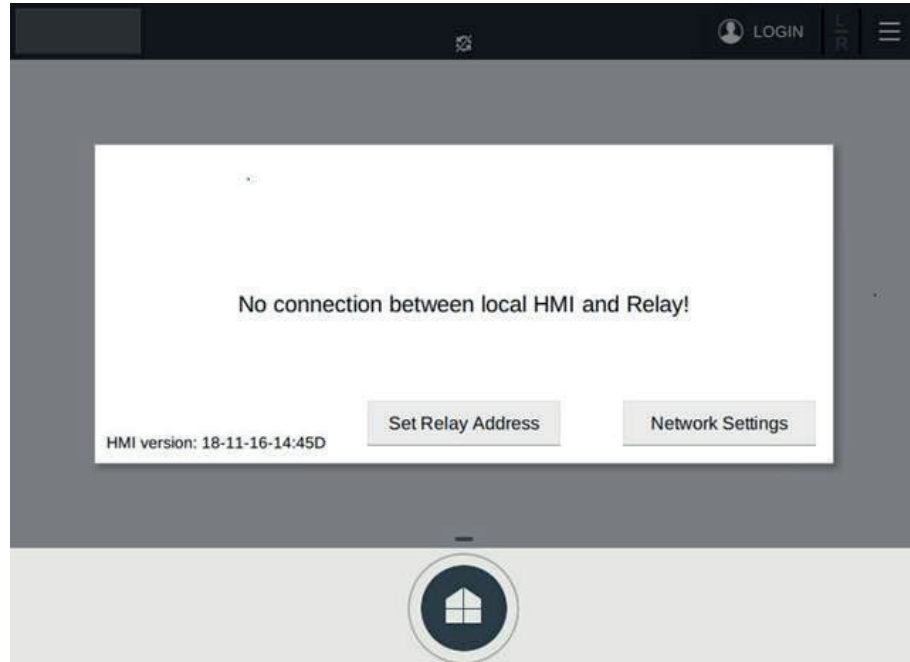


Figure 105: Opening the Network Settings page

2. On the **Network Settings** page, clear the **Automatic Address** check box and edit the network settings of the LHMI's main unit port.

Address and Netmask settings should match the relay settings found in **Configuration > Communication > Ethernet > Network1 address**.



Enter the IP address for the LHMI's main unit port, not the relay's station port. If a router is used between the relay and the LHMI, check the correct gateway IP address.

Figure 106: Configuring the network settings of the main unit port

3. Tap **Apply** and close the **Network Settings** page.
4. Connect a network cable between the LHMI and the relay station port or network switch.
5. In the **No connection between local LHMI and Relay!** dialog box, tap **Set Relay Address**.

6. In the **Relay address** dialog box, type the relay's address found in **Configuration > Communication > Ethernet > Network1 address** and tap **OK**. The LHMI connects to the relay through the station port.

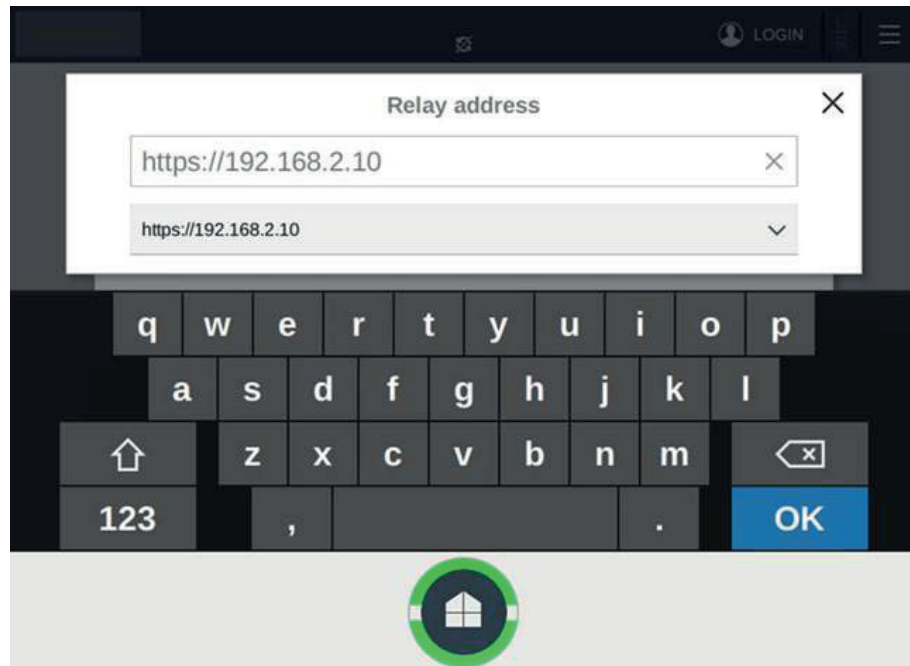


Figure 107: Typing the relay IP address

Table 25: Example of communication settings for the local HMI connection through station network

Parameter		Value
HMI communication parameter	Main Unit Port/Automatic Address	Not checked
	Main Unit Port/Address	192.168.2.123
	Main Unit Port/Netmask	255.255.255.0
	Main Unit Port/Gateway	Not checked
	Main Unit Port/Gateway Address	-
	Service Port/Address	192.168.1.1
	Service Port/Netmask	255.255.255.0
	Service Port/Enable DHCP server	Checked
REX640 communication parameters	Configuration/Communication/ Ethernet/Network1/IP address	192.168.2.10
	Configuration/Communication/ Ethernet/Network1/Subnet mask	255.255.255.0
Service PC network adapter for HMI service port	IP address	Obtain automatically

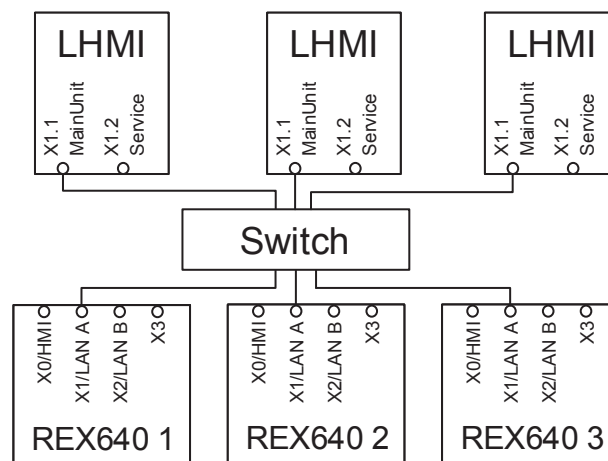


Figure 108: Example of local HMI connection through station network

7.4.3.3 Connecting switchgear HMI to a relay through station network



This chapter describes connection and next chapter pairing process.

PCM600 or WHMI can be used to read the network settings of the relay's station port via **Configuration > Communication > Ethernet > Network1 address**.

1. On the SHMI, tap **Network Settings** to configure the network settings of the main unit port X1.1.

Network settings are also available as an Advanced page.

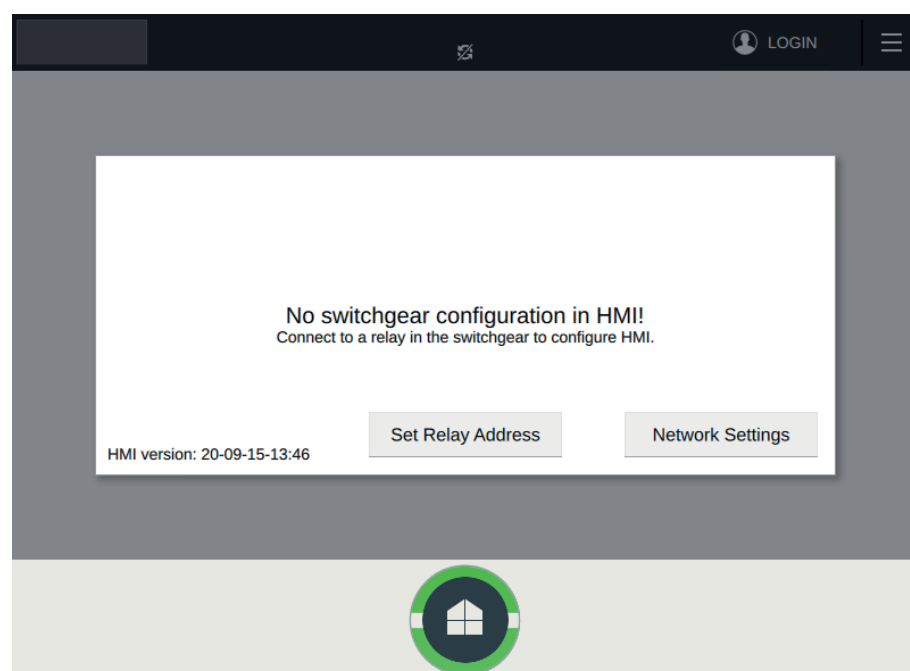


Figure 109: Opening the Network Settings page

2. On the **Network Settings** page, clear the **Automatic Address** check box and edit the network settings of the LHMI's main unit port.

Address and Netmask settings should match the relay settings found in **Configuration > Communication > Ethernet > Network1 address**.



Enter the IP address for the LHMI's main unit port, not the relay's station port. If a router is used between the relay and the LHMI, check the correct gateway IP address.

Figure 110: Configuring the network settings of the main unit port

3. Tap **Apply** and close the **Network Settings** page.
4. Connect a network cable between the SHMI and the relay station port or network switch.
5. In the **No switchgear configuration in HMI!** dialog box, tap Set **Relay Address**.

6. In the **Relay address** dialog box, type the IP address of one of the relays that belongs to the switchgear HMI configuration and tap **OK**.

The relay's address can be found in **Configuration > Communication > Ethernet > Network1 address**. The SHMI connects to the relay through the station port and automatically fetches information for the rest of the relays.

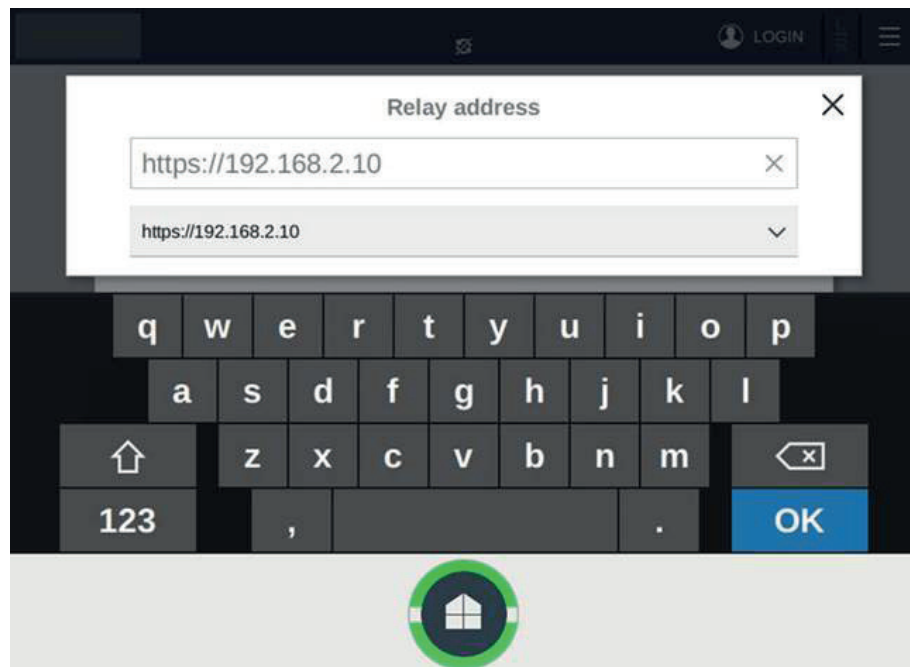


Figure 111: Typing the relay IP address



If the relays within the same switchgear have mismatching switchgear configurations, the SHMI always uploads the newest updated configuration.

Table 26: Example of communication settings for switchgear HMI connection through station network

Parameter		Value
HMI communication parameter	Main Unit Port/Automatic Address	Not checked
	Main Unit Port/Address	192.168.2.123
	Main Unit Port/Netmask	255.255.255.0
	Main Unit Port/Gateway	Not checked
	Main Unit Port/Gateway Address	-
	Service Port/Address	192.168.1.1
	Service Port/Netmask	255.255.255.0
	Service Port/Enable DHCP server	Checked

Table continues on the next page

Parameter		Value
REX640 communication parameters	Configuration/Communication/Ethernet/Network1/IP address	192.168.2.10
	Configuration/Communication/Ethernet/Network1/Subnet mask	255.255.255.0
Service PC network adapter for HMI service port	IP address	Obtain automatically

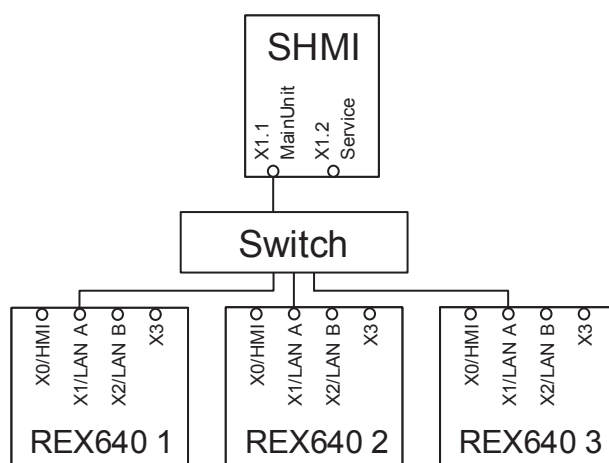


Figure 112: Example of switchgear HMI connection through station network

7.4.3.4 Pairing local HMI with relay

To enable proper connection and functionality between the LHMI and a relay they need to be paired.

1. Set up communication to establish a connection between the HMI and the relay.

2. In the confirmation window, tap **Trust this Relay**.

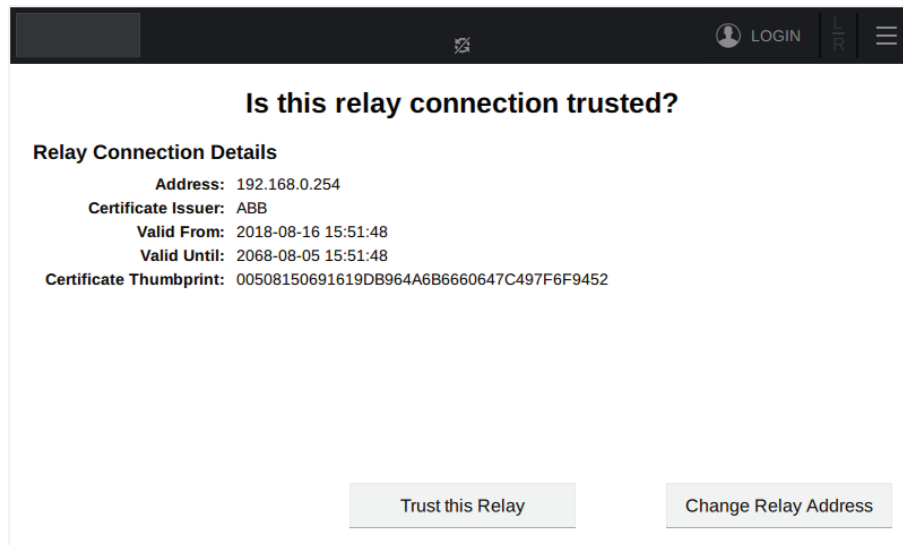


Figure 113: Confirming the relay connection

A page for initiating the pairing opens.

3. To initiate pairing, login as administrator.

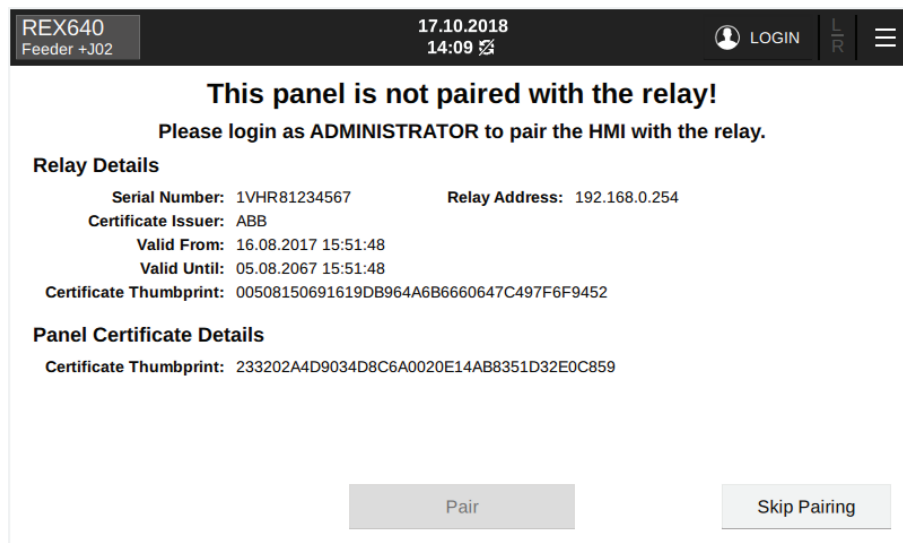


Figure 114: Administrator login required

4. Finalize the pairing process depending on the HMI used.
 - a) To pair the LHMI with one relay only, tap **Pair**.
 - b) To pair the SHMI with multiple relays, tap **Pair**. The connected relays are shown on the list of available relays. Select the trusted relays and tap Trust selected.

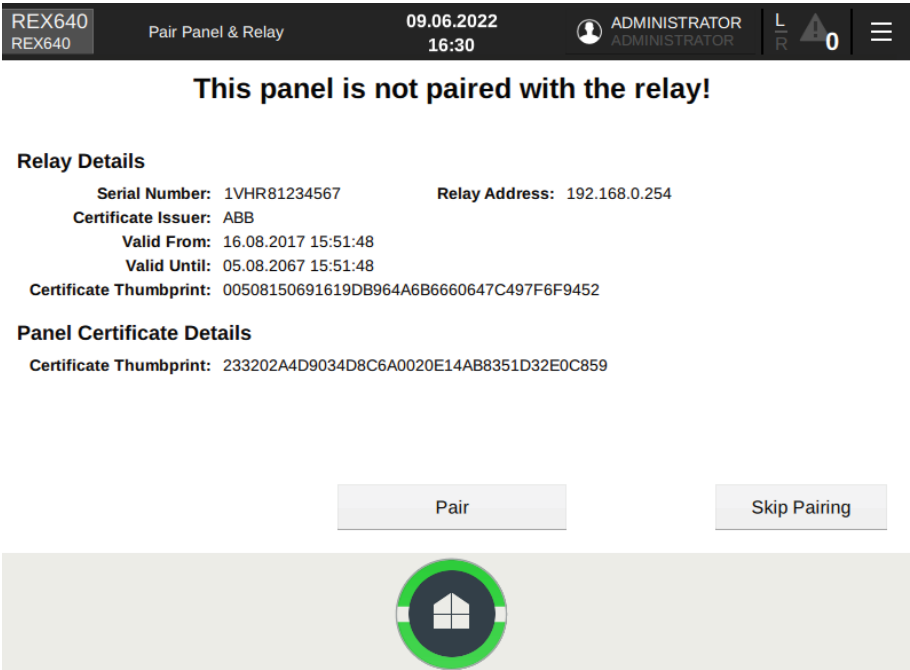


Figure 115: Pairing the local HMI with the relay

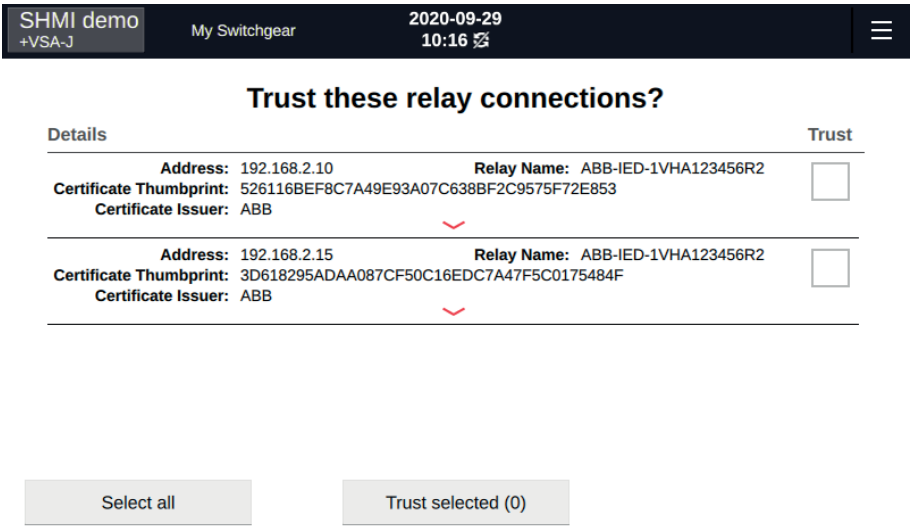


Figure 116: Pairing the switchgear HMI with the relays

After successful pairing, the LHMI Home page opens.



If Pair is selected while connecting to the first relay in a switchgear, the SHMI attempts to pair with all the relays it finds and is able to connect and login to within the switchgear. If pairing is at first skipped but needed later, initiate the connection process again by typing in the IP address of one of the relays and choose to pair. Optionally, it is possible to login and pair each relay individually.



If the pairing is skipped, the LHMI can be used for monitoring purposes only. Pairing can be initiated later via the drop-down menu.

7.4.3.5 Setting system time and time synchronization

- Select **Configuration > Time > System time** to set the system time and time zone.
- Select **Configuration > Time > Synchronization > Synch source** to set the synchronization source.

Setting daylight saving time

The protection relay can be set to determine the correct date for the DST shift every year. The local time is used to set the DST.

1. Set the *DST on day (weekday)* and *DST off day (weekday)* parameters to define on which week day the time shift occurs.
2. Set the *DST on date (day)*, *DST on date (month)* and *DST off date (month)* parameters to define on which month and week the time shift occurs.

The DST on/off date must precede the selected DST on/off day and be within the same week as the DST shift.

Table 27: Possible date values for DST change on Sunday

Day of the DST shift	DST on/off date (day)
First Sunday of the month	1
Second Sunday of the month	8
Third Sunday of the month	15
Fourth Sunday of the month	22
Last Sunday, if the month has 30 days	24
Last Sunday, if the month has 31 days	25

For example, if DST on time shift occurs on the last Sunday in March, at 03:00 local time and DST off time shift occurs on the last Sunday in October, at 04:00 local time, the settings are the following.

DST on time (hours): 3 h
 DST on time (minutes): 0 min
 DST on date (day): 25
 DST on date (month): March
 DST on day (weekday): Sunday
 DST off time (hours): 4 h
 DST off time (minutes): 0 min
 DST off date (day): 25
 DST off date (month): October
 DST off day (weekday): Sunday



Set the *DST on day (weekday)* and *DST off day (weekday)* to "reserved" to determine the exact date and time for the DST shift. Repeat the setting yearly, as the time for the DST shift is not on the same date every year.



To disable the DST, set the *DST in use* parameter to "False".

7.5 Testing of protection relay operation

The protection relay has to be in the test mode before the digital outputs and certain output signals of protection and other functions can be activated.

7.5.1 Selecting IED test mode

The test mode can be activated using the LHMI. The Home button is flashing green at low frequency to indicate that the test mode is activated. By default, the test mode can only be changed from the LHMI. Activation by remote client is possible, see the technical manual.

The test mode is useful for simulated testing of functions and outputs without providing current inputs.

- Select **Testing and Commissioning > Test mode > IED test** to activate the internal fault test.

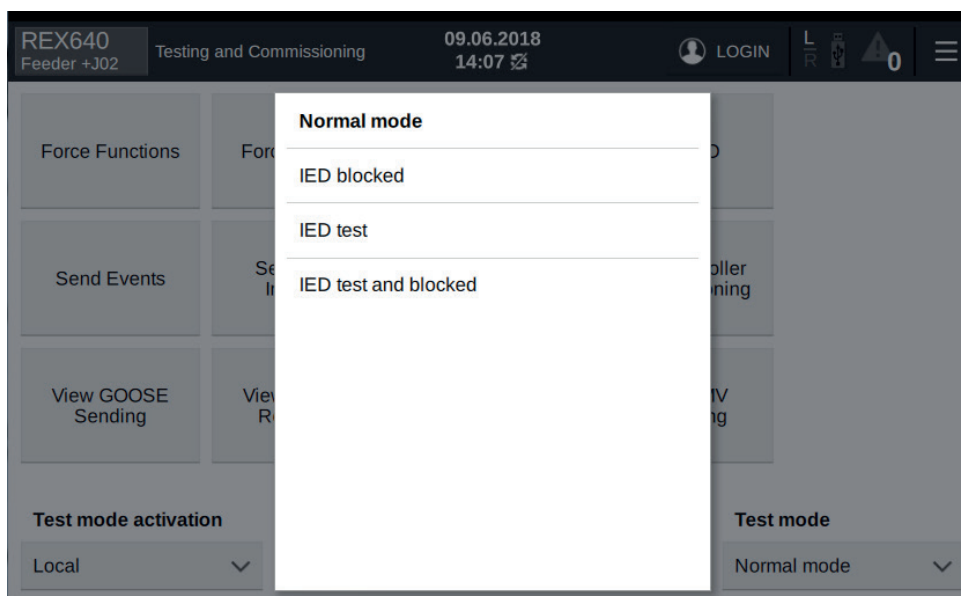


Figure 117: Selecting IED test mode



If the test mode is not cancelled, it remains on and the Home button remains flashing.

7.5.2 Testing and commissioning support on local HMI

The LHMI supports the engineer during the relay's testing, commissioning and troubleshooting activities. The information, traditionally accessible through different paths within the menu structure, is provided in a collectively grouped and

visualized format on the Testing and Commissioning pages found on the top bar menu.



HMI client can be opened from PCM600.



Some of the Testing and Commissioning pages require the relay to be set in test mode.

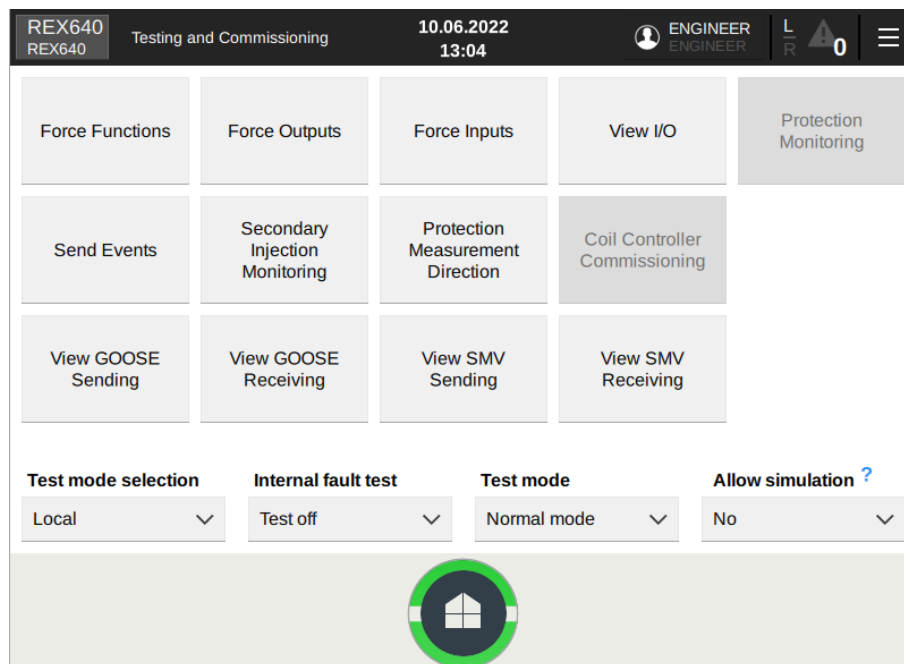


Figure 118: Home page for Testing and Commissioning pages

7.5.2.1 Testing I/O interface

1. On the **View I/O** page, monitor the status of digital inputs and outputs and analog inputs.

a) Tap the module on the page to open the module-specific page.

b) Tap  or  to scroll over the different modules.

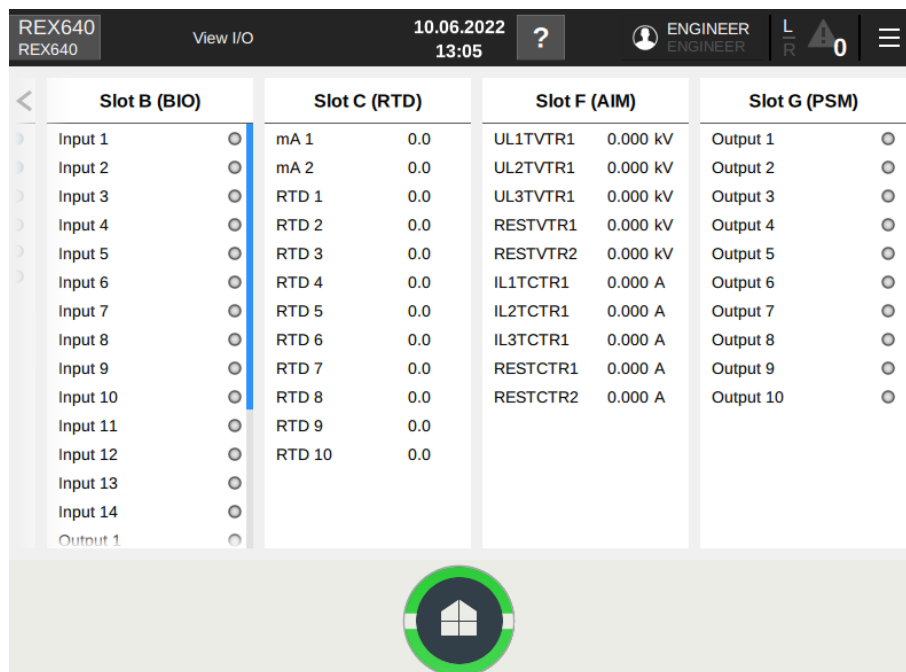


Figure 119: View I/O page

2. On the **Force Outputs** page, force the state of digital outputs.

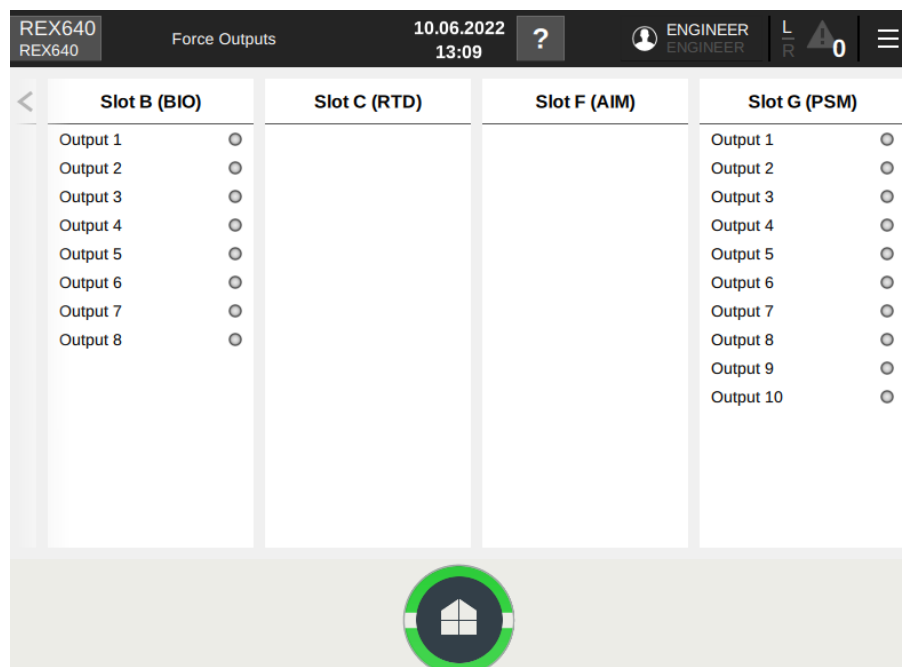




Figure 120: Force Outputs page

- a) Tap the module on the page to open the module-specific page.
- b) Tap  or  to scroll over the different modules.
- c) On the module-specific page, select state **On** or **Off** for the selected output channel and tap **Force**.

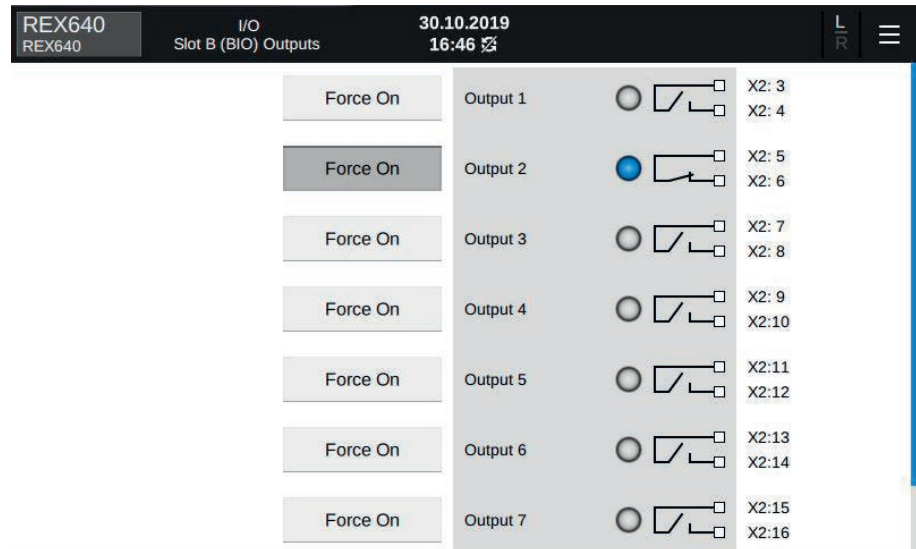




Figure 121: Forcing outputs of selected module

3. On the **Simulate Inputs** page, simulate the digital and analog inputs.
 - a) Tap the module on the page to open the module-specific page.
 - b) Tap  or  to scroll over the different modules.

- c) On the BIO module specific page, select **On** or **Off** for the selected channel and tap **Simulate**.
- d) On the AIM/SIM module specific page, select **Primary** or **Secondary** for **Simulation Unit**, set the simulation signal value for a channel and tap **Simulate**.

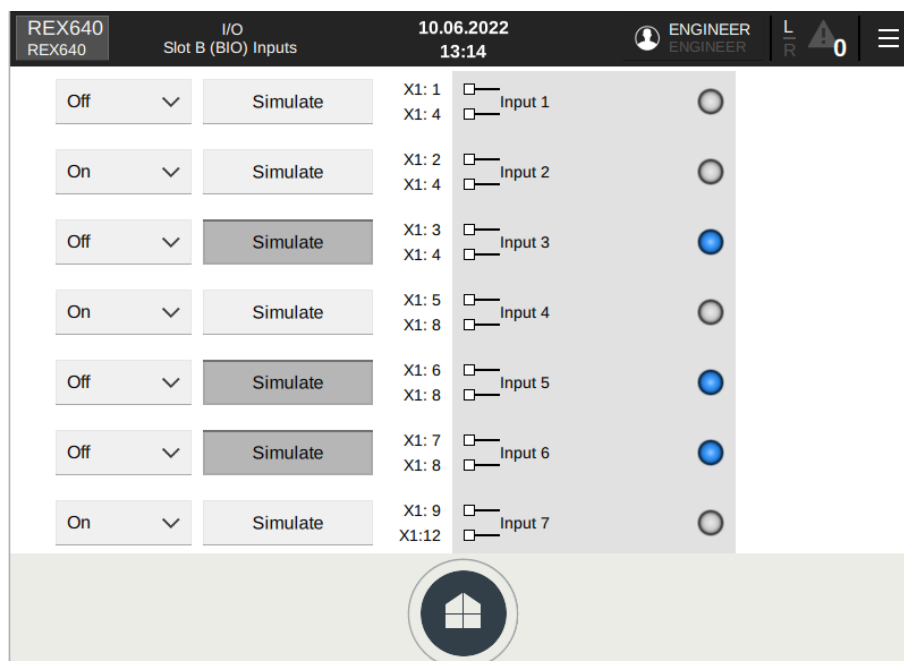


Figure 122: Simulating digital inputs of selected module

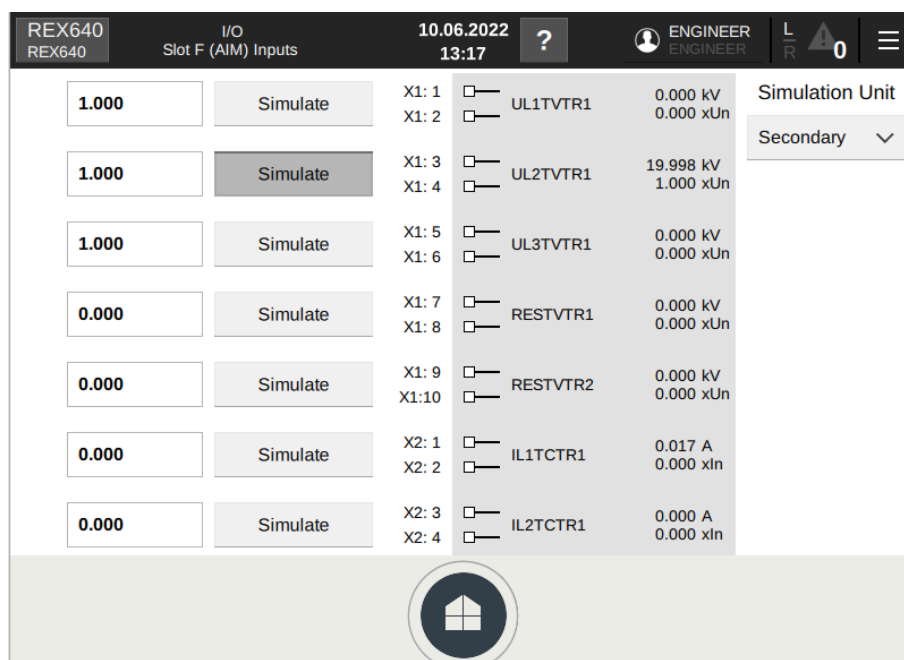


Figure 123: Simulating analog inputs of selected module



All current and voltage input signals (channels) share the same phase angle value, that is, they are in phase.

7.5.2.2

Testing functions

1. On the **Force Functions** page, activate or deactivate an output signal for protection or other function in one of the alternative ways.
 - Tap **Edit**, select the protection category from the left of the page and activate or deactivate an output signal of a function from the list.
 - Tap **Reset** to deactivate all output signals for the function.

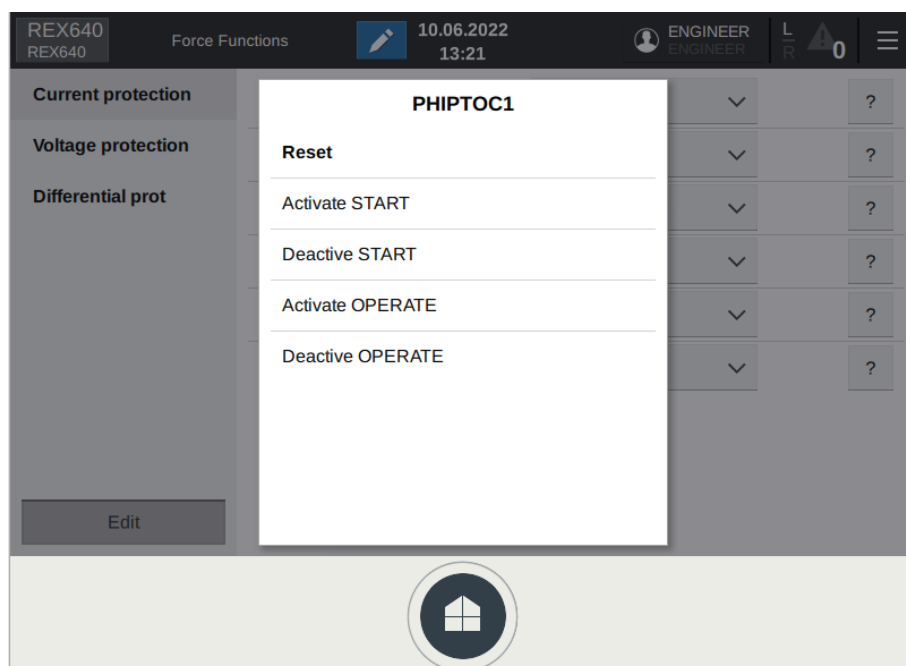


Figure 124: Force Functions page

2. On the **Send Events** page, send a selected event over the station bus to a substation client.

The sent events are defined in the IEC 61850 data sets. To send all available events in the relay, tap **Send All Events**.



When the events are sent, the related functions are not activated.

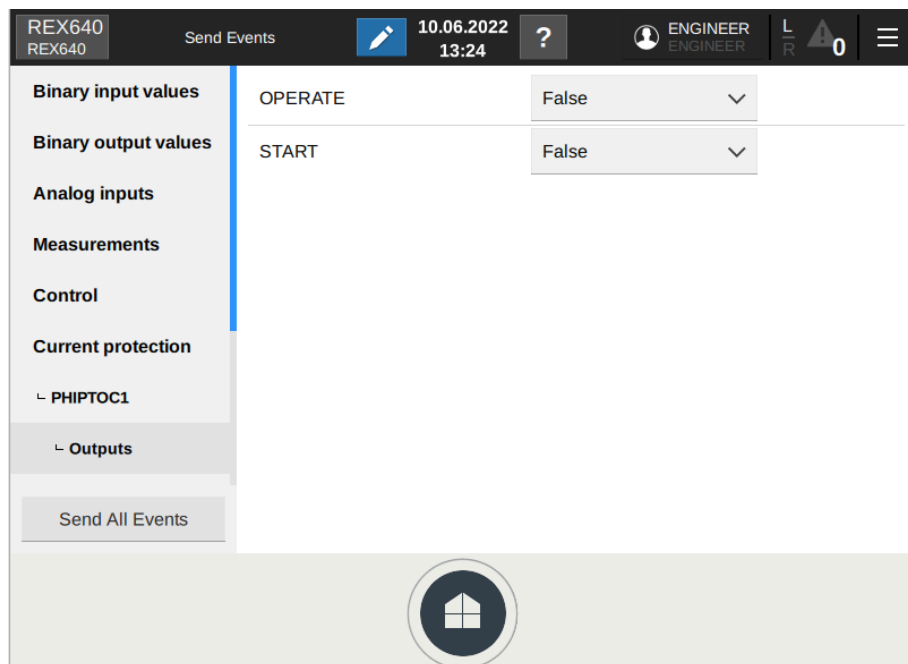


Figure 125: Send Events page

7.5.2.3 Checking GOOSE data

- 1. On the **GOOSE Receiving** page, check the GOOSE data that the relay subscribes from the Ethernet network.

The left side of this page shows a list of devices that send GOOSE messages to the relay. These devices that publish data for the relay are defined in the relay configuration. The right side of the page shows the GOOSE data the relay receives from the network. The data set consists of value and quality attributes. The received data has status indicators where green means all OK, yellow warning and red error.

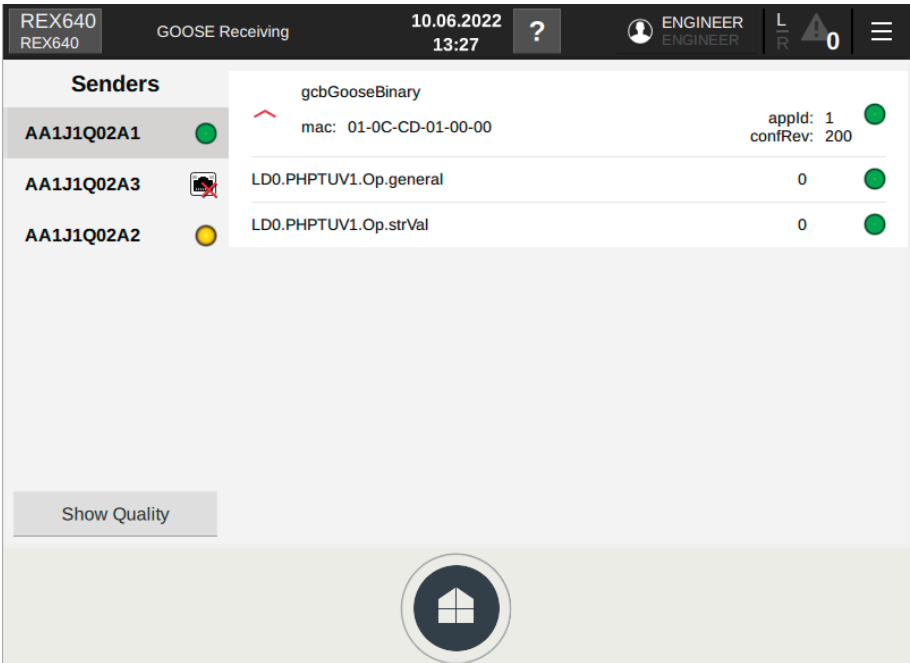


Figure 126: GOOSE Receiving page

- 2. On the **GOOSE Sending** page, check the status of the relay's configured GOOSE control blocks and the values of the sent data.

The left side of this page shows a list of the devices where the relay sends GOOSE messages. In the system there may be more devices, but these devices are according to relay configuration the ones subscribing the data from the relay. The right side of the page shows the GOOSE data that the relay sends to the network. The data set consists of value and quality attributes. The sent data has status indicators where green means all OK, yellow warning and red error.

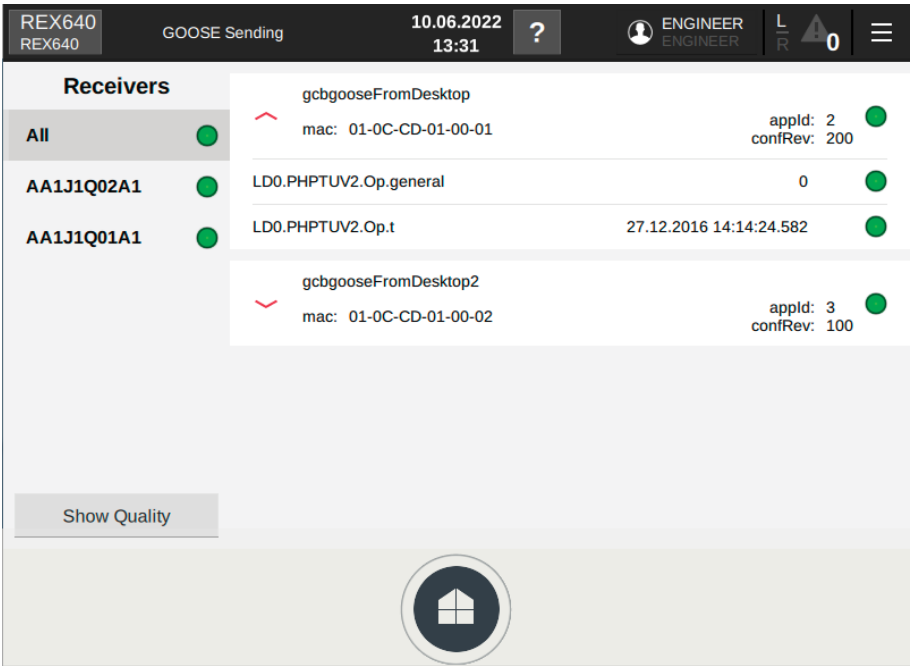


Figure 127: GOOSE Sending page

7.5.2.4 Checking SMV data

- 1. On the **SMV Receiving** page, check the sampled values data that the relay subscribes from the Ethernet network.
The left side of this page shows a list of devices that send SMV messages to the relay. These devices that publish data for the relay are defined in the relay configuration. The right side of the page shows the SMV data that the relay receives from the network. The data set consists of value and quality attributes. The received data has status indicators where green means all OK, yellow warning and red error.

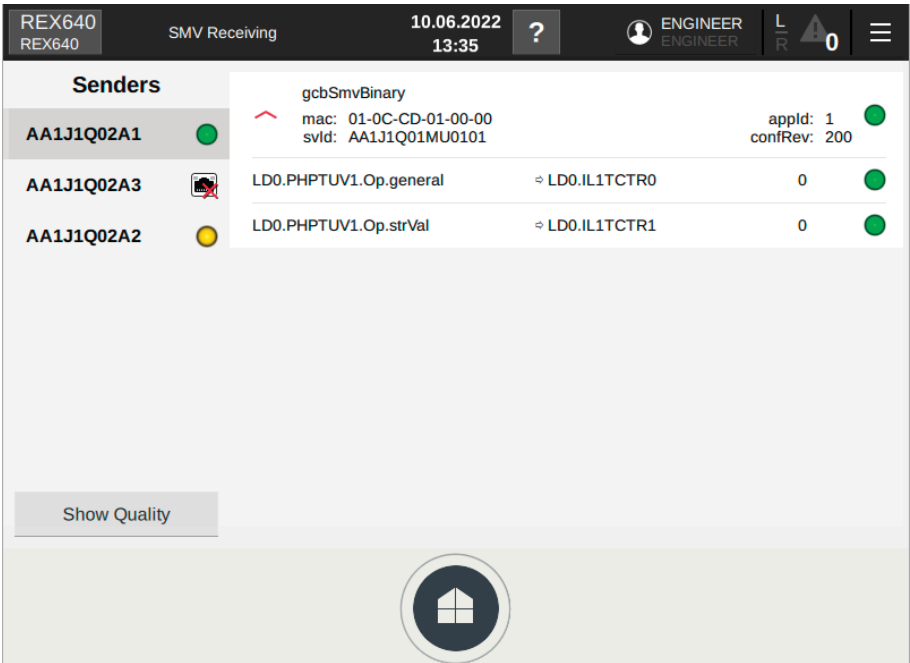


Figure 128: SMV Receiving page

- On the **SMV Sending** page, check the status of the relay's configured SMV control blocks and the values of the sent IEC 61850-9-2 sampled value data. The left side of this page shows a list of the devices where the relay sends SMV messages. In the system there may be more devices, but these devices are according to relay configuration the ones subscribing the data from the relay. The right side of the page shows the SMV data the relay sends to the network. The sent data has status indicators where green means all OK, yellow warning and red error.

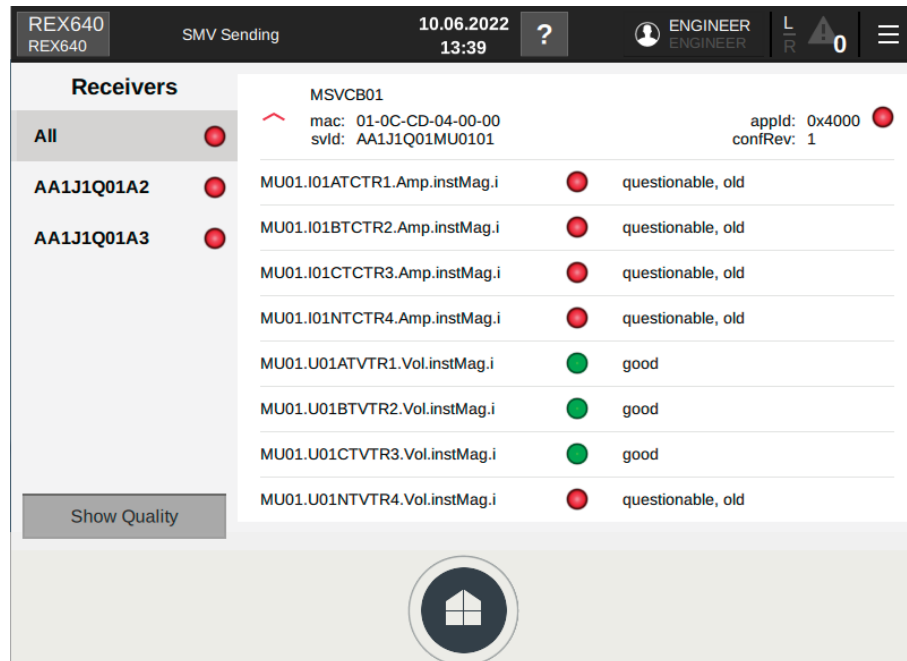


Figure 129: SMV Sending page

7.5.2.5 Using Protection Monitoring

Protection Monitoring view can be utilized during secondary injection testing. Instantaneous monitored values are shown on protection characteristics graph. Refresh rate of monitored value is 500 ms.

- Navigate to **Testing and Commissioning** page.
- Select **Protection Monitoring**.
- Select protection function

4. Tap **Home** button to return to previous page.

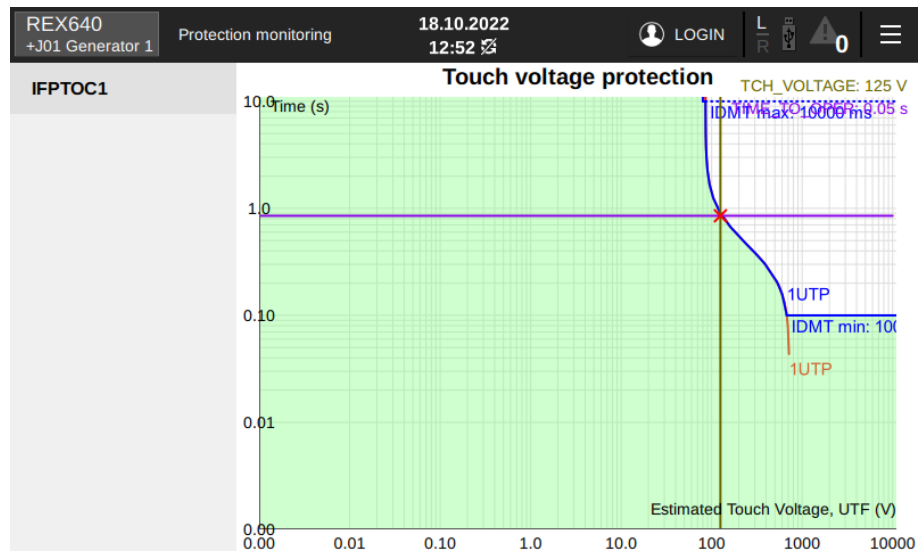


Figure 130: Protection monitoring

7.5.3 Using HMI Client

REX640 HMI Client can be launched from PCM600. It connects to REX640 via selected Communication Port and shows HMI view that is identical to actual physical HMI.

HMI client can't be paired with the REX640 and control operations are not possible.

1. Select context menu on the top of REX640 in plant structure using right click.
2. Select **Browse with HMI > HMI Client**. When connection is established "No pages configured for the current user" is shown.
3. Click **LOGIN** on and enter credentials.

4. HMI Client is showing the configured HMI pages.

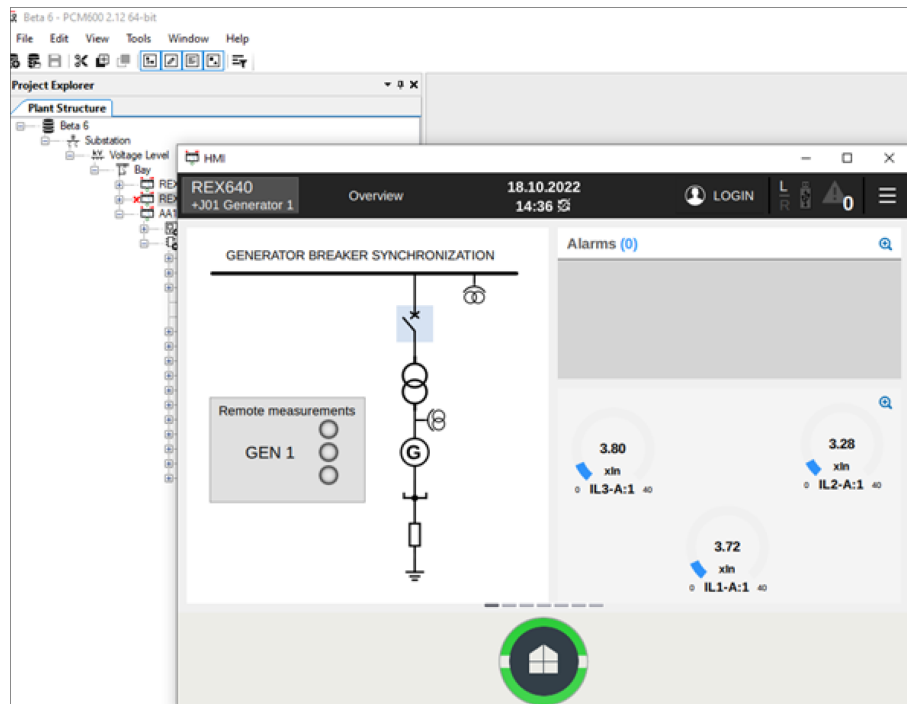


Figure 131: HMI Client

7.5.4 Selecting the internal fault test

The internal fault may be tested by using the LHMI. When enabling the test, the internal relay fault output contact, which is normally activated, will be deactivated. See the technical manual for the internal relay fault output contact location. The internal fault can only be activated by using the LHMI.



Differing from real internal fault situation, the other output contacts are not released and locked during the test. In other words, protection functions can operate and trip the outputs when the internal fault is tested.

1. Ensure that the **Test mode** is activated.
2. Select **Testing and Commissioning > Internal fault test > Test on** to activate the internal fault test.

7.5.5 Selecting IED blocked or IED test and blocked mode

The IED blocked mode and the IED test and blocked mode can be activated using the LHMI. The Home button flashes green when the device is in the IED blocked or IED test and blocked mode. By default, the test mode can only be changed from the LHMI. Activation by remote client is possible, see the technical manual.

The test mode can be used for simulated testing of functions and outputs without providing current inputs. The IED blocked mode can be used to block the physical outputs to the process.

- Select **Testing and Commissioning > Test mode > IED blocked or IED test and blocked** to activate the IED blocked mode and the IED test and blocked mode.

Table 28: Test mode

Test mode	Description	Protection BEH_BLK	Protection BEH_TST
Normal mode	Normal operation	FALSE	FALSE
IED blocked	Protection works as in “Normal mode” but the ACT configuration can be used to block physical outputs to process. Control function commands are blocked.	TRUE	FALSE
IED test	Protection works as in “Normal mode” but protection functions work in parallel with test parameters	FALSE	TRUE
IED test and blocked	Protection works as in “Normal mode” but protection functions work in parallel with the test parameter. The ACT configuration can be used to block physical outputs to process. The control function command is blocked.	TRUE	TRUE



If the IED blocked or IED test and blocked mode is not cancelled, it remains on and the Home button remain flashing.

7.6 ABB Product Data Registration

The ABB Product Data Registration feature traces composition changes in the protection relay's SW or HW. Traceability allows better support and maintenance possibilities.

Protection relay detects hardware or software change and stores this information internally. This information can be read from relay using **PCM600 Lifecycle Handling > Collect IED Composition Data**.

Composition data is automatically transferred to ABB if feature is enabled during the PCM600 installation.

The number of composition and setting changes can be seen from the *Composition changes* parameter in **Monitoring > IED status**.

LCT-generated events are reported as a bit-masked value (change flags); for example, value 9 means that hardware and site identifier changes have been done to the relay.

Table 29: LCT-generated events

Bit	Description
0	Hardware change
1	Software change
2	Configuration change
3	Site identifier change
4	Retrofit change
Other	Not in used

8 Maintenance and Periodical Testing

8.1 Maintenance and Periodical Testing

The following sections are discussing selected aspects in regards the maintenance and periodical testing of REX640 Protection and control relay. The maintenance activities are here referred as specific actions, documented by the relay manufacturer, to be performed to the relay according to predefined time intervals. There are several factors influencing the optimum frequency of periodical testing, as well as the method of testing. Local legislation, insurance policy terms, customers' own maintenance practices, level of technology used in the installation and other similar issues certainly have an impact which is not possible to comprehensively cover here.

These sections do not discuss the personnel work safety related issues, nor the expected skill level of the testing and maintenance engineers or technicians. These are obviously of paramount importance but must be instructed and supervised by the party responsible.

8.1.1 Maintenance

REX640 protection and control relays do not require any specific periodical maintenance when installed and operated according to the manufacturer's instructions and within the specified environmental conditions. The relays shall be kept clean and free of dust and yearly visual check of installation's condition is recommended. Retightening of relay's screw type terminals is recommended after the first three to six months in use.

As a part of our quality assurance process, we constantly analyze the data from the installed base. In case a systematic anomaly would be identified, we will take specific actions. The actions are highly dependent on the nature of the anomaly and could include targeted maintenance advice for a dedicated relay batch, or it could be more general advisory based on the years of relay in operation.

As a part of our products' lifecycle support activities, we publish firmware updates offering functionality enhancements for the delivered units. The REX640 users are encouraged to visit the REX640 product page to check the latest firmware updates. Each firmware update includes a release note, describing the content, and a link that can be used to download the actual firmware package. Relay specific REX640 serial number is required for downloading. Depending on the firmware patch content and the evaluated criticality of it, the relay update can be performed soonest or as mostly done, during the periodical testing of the relay. Updating the relay firmware with a patch does not itself require relay retesting.

8.1.2 Periodical Testing

Precondition for efficient and successful periodical testing is that the installation has been comprehensively tested before it has entered the commercial use, the

documentation is up to date and test records from the pre-commissioning and commissioning tests are available. Periodical testing should not be seen as a reconfirmation of commission stage testing, but as a stage where the installation's possible impaired performance is detected, documented and also corrected.

REX640 protection and control relay is a vital part of the complete protection and control scheme, but it's not the only one. The other devices within the scheme shall be considered as well. Depending on the actual installation these might include all or just a part of the following list:

- Circuit breaker primary part
- Circuit breaker trip coils, one or several
- Measurement transformers or sensors and related wiring
- Arc flash detection sensors
- Other protection relay(s) as a part of the complete scheme
- Interpanel wiring
- Interpanel communication for binary and/or analogue signals
- DC auxiliary voltage supply
- Station level Scada/monitoring system
- Process control system
- Remote level Scada system

The following is mainly concentrating on the REX640 as a part of the overall system, but other devices will be shortly discussed where seen necessary.

8.1.2.1 Method of Testing

Important aspect in periodical testing is to secure that at the end of the testing all parts of the installation are restored to the original state. For example, if some test requires disconnecting relay voltage measurements from busbar voltage transformer secondary circuits, the connections must be reestablished at the end of that testing. It's highly recommended that the test engineer keeps a record of all possible temporary modifications within the installation, to help him/her to revert to the original set-up.

In general, a good rule is to perform the tests using a method which is as close as possible to the normal operational conditions of the installation. This is one way to reduce the risk of leaving some temporary connection or setting unrestored to original position at the end of the testing.

Periodical testing is performed with the protected feeder de-energized, circuit breaker truck withdrawn to test position or in case of a fixed circuit breaker, bus- and line-disconnectors in open position. In case the other feeders within the installation remain energized and supplying loads, it's important to isolate the relay under testing from the rest of the system to avoid accidentally sending upstream trip commands during the testing.

Protection relay periodical testing is normally carried out as secondary injection testing. The currents and voltages normally measured via sensors or instrument transformers are replaced with adjustable analogue signals from the test set. In case the installation is equipped with relay test blocks, the separation of the relay from the measurement and trip circuits happens automatically when the test adaptor is inserted into the test block.

If test blocks are not present, the connection point of the test set is the LV-compartment's terminal blocks. These terminal blocks typically offer the possibility to open the terminal mid bridge connection and that way separate the relay under

testing from the measurement and trip circuits. Each protection function is then tested one by one to confirm the functionality in respect of:

- start value level
- operate value level
- reset ratio value
- operate time, typically done with an infeed of 1,5 times the operate value setting

The results are compared to the setting values and the test records from the commissioning and the latest periodical test results. In case discrepancies outside the manufacturer's stated accuracy limits are found, the corresponding test shall be repeated. If the second test results are still outside the limits, deeper considerations are needed. If the deviation is considerable, recommendation is to replace the relay with a spare relay. In case of a slight deviation the operation until the next periodical test round can be considered.

The secondary test set will also introduce certain level of inaccuracies to the tests, especially if the test set has not been calibrated as per the manufacturer's instructions. As a final task for each protection function testing, it's highly recommended to do final operate test including the circuit breaker operation. In case the circuit breaker is equipped with two trip coils, the condition of both coils shall be verified.

During the testing of protection functions, the related measurements and events shall be verified from the local HMI. The verification, if possible, is recommended to be extended all the way to the upper-level systems like Scada or process control system.

When testing individual protection functions, there will be situations where some other protection function might interfere the testing of the selected one. REX640 HMI under page "Testing and Commissioning" offers various support for testing activities. By enabling IED Test mode and entering page "Secondary Injection Monitoring" there is a possibility to disable selected protection function(s). When the relay is returned to Normal mode, the functions will regain their original status automatically.

The correct function and the related external circuitry of IRF-relay (internal relay fault) output shall be checked. This can be performed using dedicated functionality in the HMI. Under the page "Testing and Commissioning" there is a tab called "Internal fault test". By selecting position "test on", the IRF-relay will be de-energized, and the function of the related circuitry can be verified.

Arc flash sensors connected to REX640 relays include supervision functionality. This functionality will indicate if the connected sensor's, loop or lens, optical circuit is intact. It is recommended that each sensor, one by one, is disconnected from the relay to check that the correct alarm and event information is received. The supervision function is not able to detect if sensor is dirty or if the sensor is misaligned due to mechanical impact, these shall be checked visually.

8.1.2.2 Recommended Testing Intervals

The recommended periodical testing interval is between three and five years, depending on the following factors.

Installation environment

REX640 relays which are installed in harsh environments, we recommend applying the three years interval. The harsh conditions can be due to temperatures and/or

humidity near to the maximum specified for the product, or it can be due to dust, salt, chemicals, or other corrosive agents.

Infrequent operations

If the relay has performed very few operations during the observation period, which is typical for spare feeders, we recommend applying the three years periodical testing interval. The long inoperative time is not typically a problem for the relay, if the auxiliary power is turned on continuously, but it might be more problematic for the circuit breaker operation mechanism.

Frequent operations

When the relay performs several operations during the observation period, specially initiated by the protection functions, and the relay's performance during the faults are analyzed we recommend applying the five years periodical testing interval. The analyzing can be based on relay's events, fault records and disturbance records.

Utilization of relay's external and internal supervision features

REX640 contains several supervision features, both for relay's internal functionality and for relay's external circuitry. For external circuitry there are many supervision features. Whether the features are activated depends on the relay configuration and settings. It's highly recommended to take an advantage of these features, since they will cover a large part of the complete protection circuitry offering continuous supervision. The following features are included:

- Trip (and close) coil supervision
- Circuit breaker condition monitoring
- Motor operated disconnector supervision
- Current transformer secondary circuit supervision
- Fuse failure supervision
- Protection (point-to-point) communication supervision
- Station communication supervision

When in use and configured correctly, these supervision features will activate events and alarms, both on local HMI and on remote systems.

The protection relay's self-supervision function monitors the relay's performance and indicates possible problems on two levels: internal warnings and internal faults. Internal warnings effects only the concerned part of the relay's functionality, for other parts the relay will continue normal operation. The internal warnings are indicated as events and as alarms, if enabled in the configuration, on the HMI and on remote systems.

In case of internal faults, the relay operation will be disabled, IRF output relay will be de-energized and corresponding events and alarms issued. REX640 has a mechanism for recovering from internal fault situation by activating a controlled restart of the relay. Depending on the root cause, the restart can happen several times and if successfully the relay will resume full operational status.

When these supervision features are utilized and actions taken in case any of the supervision functions activates itself, we recommend applying the five years periodic testing interval.

8.1.2.3

Test Records

During pre-commissioning, commissioning, and periodical testing stages it is important to record the test cases and test results. The records shall be on such a detailed level that they can be used to detect any signs of protection performance

deterioration during the years. The history shall be available for the technician performing the testing, and for a person evaluating and approving the test result.

9 Glossary

AC	Alternating current
AD	Active directory
CAL	Central activity logging
CAM	Centralized account management
CAT 5	A twisted pair cable type designed for high signal integrity
CAT 6	Cable standard for gigabit Ethernet and other network protocols that is backward compatible with CAT 5/5e and CAT 3 cable standards
CFG	Configuration file
COMTRADE	Common format for transient data exchange for power systems. Defined by the IEEE Standard.
CT	Current transformer
DAT	1. Data attribute type 2. Data file
Data set	The content basis for reporting and logging containing references to the data and data attribute values.
DC	1. Direct current 2. Disconnecter 3. Double command
DHCP	Dynamic host configuration protocol
DIP switch	A set of on-off switches arranged in a standard dual in-line package
DNP3	A distributed network protocol originally developed by Westronic. The DNP3 Users Group has the ownership of the protocol and assumes responsibility for its evolution.
DST	Daylight-saving time
EEPROM	Electrically erasable programmable read-only memory
EMC	Electromagnetic compatibility
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN.
FPGA	Field-programmable gate array
FPN	Flexible product naming
FTP	File transfer protocol
FTPS	FTP Secure
GDE	Graphical display editor in PCM600
GND	Ground/earth
GOOSE	Generic object-oriented substation event
HF	High frequency
HMI	Human-machine interface

HSR	High-availability seamless redundancy
HTTPS	Hypertext transfer protocol secure
HW	Hardware
IEC	International electrotechnical commission
IEC 60870-5-104	Network access for IEC 60870-5-101
IEC 61850	International standard for substation communication and modeling
IEC 61850-9-2	A communication protocol based on the IEC 61850 standard series
IEC 61850-9-2 LE	Lite Edition of IEC 61850-9-2 offering process bus interface
IED	Intelligent electronic device
IP	Internet protocol
IP address	A set of four numbers between 0 and 255, separated by periods. Each server connected to the Internet is assigned a unique IP address that specifies the location for the TCP/IP protocol.
IRF	1. Internal fault 2. Internal relay fault
IRIG-B	Inter-Range Instrumentation Group's time code format B
LAN	Local area network
LCP	Liquid crystal polymer
LCT	Life cycle traceability
LED	Light-emitting diode
LF	Low frequency
LHMI	Local human-machine interface
MMS	1. Manufacturing message specification 2. Metering management system
Modbus	A serial communication protocol developed by the Modicon company in 1979. Originally used for communication in PLCs and RTU devices.
Modbus ASCII	Link mode using 7-bit ASCII characters
Modbus RTU	Link mode using 8-bit binary characters
NCC	Network control center
OTP	One-time password
PC	1. Personal computer 2. Polycarbonate
PCM600	Protection and control IED manager
PKI	Public key infrastructure
PTP	Precision time protocol
RAM	Random access memory
RJ-45	Galvanic connector type
RoHS	Restriction of hazardous substances
ROM	Read-only memory
RS-485	Serial link according to EIA standard RS485

RTC	Real-time clock
RTD	Resistance temperature detector
SCL	XML-based system configuration description language defined by IEC 61850
SHMI	Switchgear HMI
SI	Sensor input
Single-line diagram	Simplified notation for representing a three-phase power system. Instead of representing each of three phases with a separate line or terminal, only one conductor is represented.
SLD	Single-line diagram
SMV	Sampled measured values
SNTP	Simple network time protocol
SSH	Secure shell
STP	Shielded twisted-pair
SW	Software
TCP	Transmission control protocol
TCP/IP	Transmission control protocol/Internet protocol
TLS	Transport layer security
UDP	User datagram protocol
USB	Universal serial bus
VT	Voltage transformer
WAN	Wide area network
WHMI	Web human-machine interface
XRIO	eXtended relay interface by OMICRON



ABB Distribution Solutions
Digital Substation Products

P.O. Box 699

FI-65101 VAASA, Finland

Phone +358 10 22 11

www.abb.com/mediumvoltage

www.abb.com/reion

www.abb.com/substationautomation