RELION® PROTECTION AND CONTROL

# REX610

## Cyber Security Deployment Guideline


Document ID: 2NGA000818
Issued: 2023-05-02
Revision: B
Product version: 1.1

## Copyright



### Trademarks



### Warranty

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

*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 KEMA 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

## 1.1 This manual

The cyber security deployment guideline describes the process for handling cyber security when communicating with the protection relay. The cyber security deployment guideline provides information on how to secure the system on which the protection relay is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service.

## 1.2 Intended audience

This guideline is intended for the system engineering, commissioning, operation and maintenance personnel handling cybersecurity during the product lifecycle.

The personnel is expected to have general knowledge about topics related to cybersecurity.

- Protection and control devices, gateways and workstations
- Networking, including Ethernet and TCP/IP with its concept of ports and services
- Security policies
- Firewalls
- Antivirus protection
- Application whitelisting
- Secure remote communication

# 1.3 Product documentation

## 1.3.1 Product documentation set

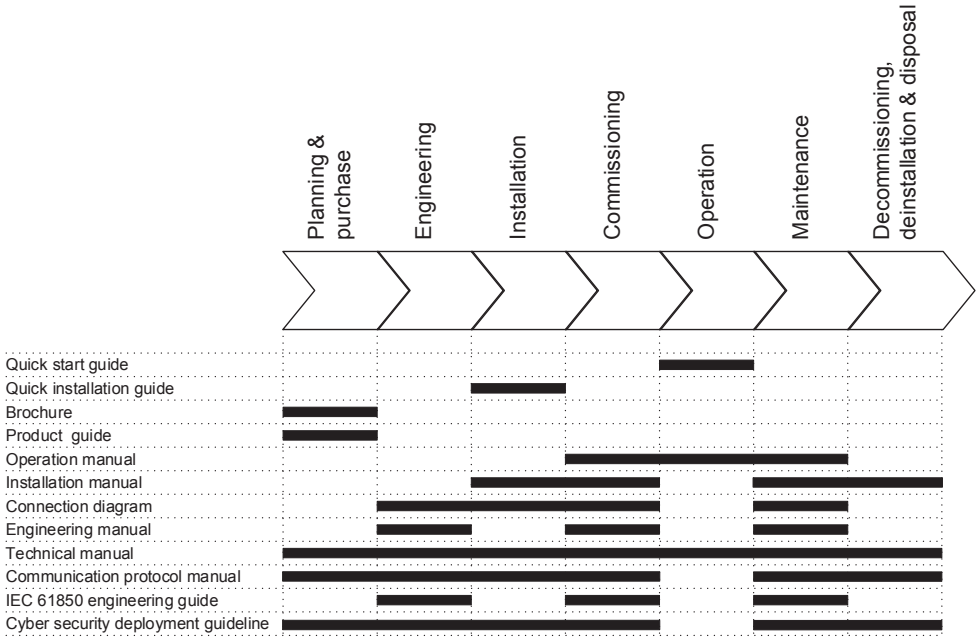


*Figure 1: The intended use of documents during the product life cycle*

## 1.3.2 Document revision history

| Document revision/date | Product version | History |
|---|---|---|
| A/2022-04-21 | 1.0 | First release |
| B/2023-05-02 | 1.1 | Content updated to correspond to the product version |

## 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 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.
- Push button navigation in the LHMI menu structure is presented by using the push button icons.

  To navigate between the options, use  and  .
- Menu paths are presented in bold.

  Select **Main menu** > **Settings**.
- LHMI messages are shown in Courier font.

  To save the changes in nonvolatile memory, select Yes and press  .
- 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".
- A functional earth terminal is indicated in figures with the symbol  .

- Equipment protected throughout by double insulation or reinforced insulation (equivalent to class II of IEC 61140) is indicated in figures with the symbol ⧈.

# 2 Security in distribution automation

## 2.1 General security in distribution automation

Technological advancements and breakthroughs have caused a significant evolution in the electric power grid. As a result, the emerging “smart grid” and “Internet of Things” are quickly becoming a reality. At the heart of these intelligent advancements are specialized IT systems – various control and automation solutions such as distribution automation systems. To provide end users with comprehensive real-time information, enabling higher reliability and greater control, automation systems have become ever more interconnected. To combat the increased risks associated with these interconnections, ABB offers a wide range of cyber security products and solutions for automation systems and critical infrastructure.

The new generation of automation systems uses open standards such as IEC 61850 and commercial technologies, in particular Ethernet and TCP/IP based communication protocols. They also enable connectivity to external networks, such as office intranet systems and the Internet. These changes in technology, including the adoption of open IT standards, have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only to office or enterprise IT systems.

To counter cyber security risks, open IT standards are equipped with cyber security mechanisms. These mechanisms, developed in a large number of enterprise environments, are proven technologies. They enable the design, development and continuous improvement of cyber security solutions for control systems, including distribution automation applications.

ABB understands the importance of cyber security and its role in advancing the security of distribution networks. A customer investing in new ABB technologies can rely on system solutions where reliability and security have the highest priority.

At ABB, we are addressing cyber security requirements on a system level as well as on a product level to support cyber security standards or recommendations from organizations such as NERC CIP, IEC 62351, IEC 62443, IEEE 1686, ENISA and BDEW Whitepaper.

Reporting of vulnerability or cyber security issues related to any ABB product can be done via cybersecurity@ch.abb.com.

# 3 Secure system setup

## 3.1 Basic system hardening rules

Today's distribution automation systems are basically specialized IT systems. Therefore, several rules of hardening an automation system apply to these systems, too. Protection and control relays are from the automation system perspective on the lowest level and closest to the actual primary process. It is important to apply defense-in-depth information assurance concept where each layer in the system is capable of protecting the automation system and therefore protection and control relays are also part of this concept. The following should be taken into consideration when planning the system protection.

- Recognizing and familiarizing all parts of the system and the system's communication links
- Removing all unnecessary communication links in the system
- Rating the security level of remaining connections and improving with applicable methods
- Hardening the system by removing or deactivating all unused processes, communication ports and services
- Checking that the whole system has backups available from all applicable parts
- Collecting and storing backups of the system components and keeping those up-to-date
- Removing all unnecessary user accounts
- Defining password policies
- Changing default passwords and using strong passwords
- Checking that the link from substation to upper level system uses strong encryption and authentication
- Segregating public network (untrusted) from automation networks (trusted)
- Segmenting traffic and networks
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using malware protection in workstations and keeping those up-to-date

It is important to utilize the defence-in-depth concept when designing automation system security. It is not recommended to connect a device directly to the Internet without adequate additional security components. The different layers and interfaces in the system should use security controls. Robust security means, besides product features, enabling and using the available features and also enforcing their use by company policies. Adequate training is also needed for the personnel accessing and using the system.

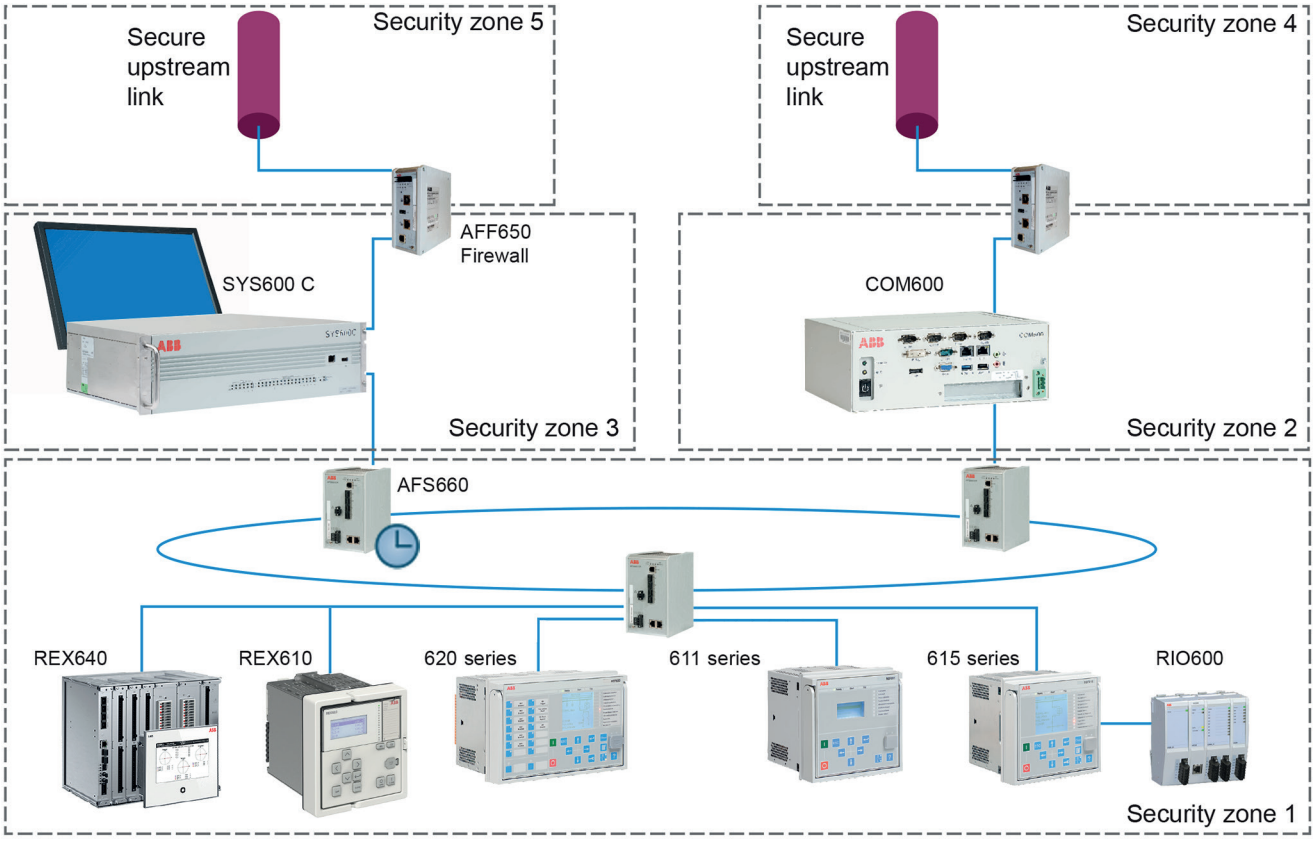


*Figure 2: Distribution substation example*

## 3.2 Relay communication interfaces

Some physical ports dedicated for station bus communication can be opened and closed in relay configuration. Few ports are always open as they are needed in communication for monitoring, control and configuration. The front port is used for engineering and it can be used only for point-to-point configuration access with PCM600.

**Table 1: Physical ports on relay's communication cards**

| Port ID | Type | Default state | Description |
|---|---|---|---|
| A2 | RJ-45 | Open | Ethernet station bus |
| A2 | RS-485 | Closed | Serial station bus |
| Front port | USB | Closed | Service access |

Serial ports are closed by default and Ethernet ports are open. All protocol instances, except for IEC 61850 and FTP, are by default off and do not respond to protocol requests in serial or Ethernet ports. The IEC 61850 protocol and rear Ethernet ports are by default activated as those are used for protection relay engineering. The front port is segregated from rear ports' station bus communication.

## 3.3 TCP/IP based protocols and used IP ports

IP port security depends on specific installation, requirements and existing infrastructure. The required external equipment can be separate devices or devices that combine firewall, router and secure VPN functionality. When the network is divided into security zones, it is done with substation devices having firewall functionality or with dedicated firewall products. Security zone boundaries are inside the substation or between the substation and the outside world.

To set up an IP firewall the following table summarizes the IP ports used by the device. All closed ports can be opened in the configuration. Ports which are by default open are used for configuring the protection relay.

**Table 2: IP ports used by the relay**

| Port number | Type | Default state | Description |
|---|---|---|---|
| 20, 21 | TCP | Open | File transfer protocol (FTP/FTPS) |
| 102 | TCP | Open | IEC 61850 |
| 502 | TCP | Closed | Modbus TCP |

FTP/FTPS and IEC 61850 are primary services needed for relay configuration and those cannot be disabled. Additionally, the protection relay uses layer 2 communications in GOOSE, which needs to be taken into account when designing the network.

In addition to the FTP/FTPS protocol, the relay supports two Ethernet-based substation automation communication protocols, IEC 61850 and Modbus. IEC 61850 is always enabled, and the relay can be ordered with one additional station bus protocol. Additional protocols must be enabled in the configuration, otherwise the communication protocol TCP port is closed and unavailable. If the protocol service is configured, the corresponding port is open all the time.

See the technical manual and the corresponding protocol documentation for configuring a certain communication protocol.

In Modbus it is possible to assign the TCP port number if required and it is also possible to allow connection requests only from a configured client IP address.

## 3.4 Secure communication

The protection relay supports secure communication for file transfer protocol using Transport Layer Security protocol. File transfer client must use explicit FTPS to communicate to the relay.

FTPS is always enabled by default but the relay also supports FTP communication. PCM600 always uses FTPS to communicate with the relay.

It is recommended to always use FTPS communication.

### 3.4.1 Certificate handling

For encryption and secure identification, FTPS protocols in the protection relay use public key certificates that bind together a public key with an identity, that is, information such as the name of an organization, their address and so on. The server certificate used by the protection relay is generated by the relay itself as a self-signed certificate and not issued by any certification authority (CA).

Certificates use encryption to provide secure communication over the network. A self-signed X.509 certificate and an RSA key-pair with key-length of 1024 bits is generated by the protection relay. The RSA key stored in the certificate is used to establish secure communication.

The certificate is used to verify that a public key belongs to an identity. The public key is one part of an asymmetric key algorithm in which one key is used to encrypt a message and another key is used to decrypt it. The public private key pair (asymmetric key) is used to exchange the symmetric key, which is used to encrypt and decrypt the data that is exchanged between server and client.

Messages encrypted with the public key can only be decrypted with the other part of the algorithm, the private key. Public and private key are related mathematically and represent a cryptographic key pair. The private key is kept secret and stored safely in the protection relay, while the public key may be widely distributed.

Once the protection relay certificate has been manually trusted in a separate dialog box, the certificate is trusted in communication between the relay and PCM600.

### 3.4.2 Encryption algorithms

TLS connections are encrypted with either AES 256 or AES 128. At start-up a negotiation decides between these two options.

A hashed representation of the passwords with SHA 256 is stored in the protection relay. These are not accessible from outside via any ports. No passwords are stored in clear text within the protection relay.

# 4 User management

## 4.1 Local user account management

Four factory default user accounts have been predefined, each with different rights and default passwords. The roles for these four user accounts are the same as the username.

- VIEWER
- OPERATOR
- ENGINEER
- ADMINISTRATOR

The default passwords in the protection relay delivered from the factory can be changed with Administrator user rights or by the users themselves. Relay user passwords can be changed using the LHMI or IED Users in PCM600.

Each protection relay supports four roles and eight user accounts. Each user can be mapped to only one role.

IED Users in PCM600 is used to manage the local user accounts.

- User accounts can be created under any role.
- 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.
- The user accounts' password can be changed by the users from IED Users or from the LHMI.
- Administrator can reset the user passwords.

The user account information is written to the protection relay from IED Users in PCM600. The user account information is securely maintained in a local database in the protection relay.

Any user logging into the protection relay from LHMI or PCM600 (FTPS/USB) is authenticated based on the user account information and this user's rights are defined by the user's role.

**Table 3: Default user roles**

| Role | Description |
|---|---|
| VIEWER | Viewing what objects are present in the logical device |
| OPERATOR | Viewing what objects are present in the logical device Performing control operations such as opening or closing the circuit breaker |
| ENGINEER | Viewing what objects are present in the logical device Making parameter setting and configuration changes in addition to having full access to the data sets and files |
| ADMINISTRATOR | Superset of all the roles |

*Table 4* describes the default mapping of all the user rights associated with all the roles in the protection relay. This mapping can be modified according to the user requirements.

**Table 4: Default roles-to-rights mapping**

| Rights/Roles | ADMINISTRATOR | ENGINEER | OPERATOR | VIEWER |
|---|---|---|---|---|
| Settings & Configuration | Read/Write | Read/Write | Read | Read |
| Settings Group Handling | Read/Write | Read | Read/Write | Read |
| Control Operations | Read/Write | Read | Read/Write | Read |
| Record Handling | Read/Write | Read/Write | Read | Read |
| Test Mode | Read/Write | Read/Write | Read | Read |
| System Update | Read/Write | Read | Read | Read |
| User Management | Read/Write | Read | Read | Read |

User account information can be exported from IED Users in PCM600 to an encrypted file which can be imported into another protection relay.

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**. 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 on the menu root level. When the *Local override* parameter is set to "False", Local User Account Management comes into use.

If the *Remote override* parameter under **Configuration** > **Authorization** > **Passwords** menu has been disabled, all MMS communication (such as communication with SCADA) requires authentication using the correct password. Remote override is enabled by default. Remote override does not impact FTP/FTPS/USB clients such as PCM600. Username and password are always required for communication with the relay over FTP/FTPS. Authentication on the LHMI is required to use USB communication with PCM600.

If the PCM600 authentication has been enabled in PCM600 System Settings, a relay user can be linked to the current PCM600 user by selecting the **Remember me** check box in the **Login** dialog. After that, the user credentials are no longer asked at tool communication as logging in PCM600 also provides the authentication credentials to the protection relay.

The Administrator user shall not be allowed to delete the last ADMINISTRATOR user and itself. FTP/FTPS logins are done by entering the username and password; there is no role selection required. The highest role for the username is automatically selected by the protection relay. Performing the Restore Factory settings operation in IED Users in PCM600 restores user accounts to the factory user accounts.

## 4.2 Password policies

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

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

There are default password policies in the protection relay.

- Minimum password length: 4
- Maximum password length: 8
- 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 5: Predefined users, their passwords and roles**

| Username | Password | Predefined role |
|---|---|---|
| VIEWER | 0001 | VIEWER |
| OPERATOR | 0002 | OPERATOR |
| ENGINEER | 0003 | ENGINEER |
| ADMINISTRATOR | 0004 | ADMINISTRATOR |

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

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

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

User configuration change 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.

For user authorization for PCM600, see the PCM600 documentation.

# 5 Security logging

## 5.1 Audit trail

The protection relay offers a large set of event-logging functions. Critical system and protection relay security-related events are logged to a separate nonvolatile audit trail for the administrator.

Audit trail is a chronological record of system activities that allows the reconstruction and examination of the sequence of system and security-related events and changes in the protection relay. Both audit trail events and process related events can be examined and analyzed in a consistent method with the help of Event List in LHMI and Event Viewer in PCM600.

The protection relay stores 2048 audit trail events to the nonvolatile audit trail. Additionally, 1024 process events are stored in a nonvolatile event list. Both the audit trail and event list work according to the FIFO principle. Nonvolatile memory is based on a memory type which does not need battery backup nor regular component change to maintain the memory storage.

Audit trail events related to user authorization (login, logout) are defined according to the selected set of requirements from IEEE 1686. The logging is based on predefined user names or user categories. The user audit trail events are accessible from Event Viewer in PCM600.

**Table 6: Audit trail events**

| Event ID | Audit trail event | Description |
|---|---|---|
| 1110 | Login | Successful login from LHMI and PCM600 |
| 1210 | Logout | Successful logout from LHMI, PCM600 or IEC 61850 |
| 1130 | Login failure | Login failed for using the wrong user credentials |
| 13200 | Configuration transfer | Configuration transferred successfully to the device |
| 1380 | Parameter change | Parameter changed successfully |
| 1422 | IED configuration update failed | IED configuration or setting change update is failed |
| 1460 | Parameter change fail | Parameter change failed |

*Table continues on the next page*

| Event ID | Audit trail event | Description |
|---|---|---|
| 1510 | Software update initiated successfully | Software update initiation is successful |
| 2210 | Password change | User password changed successfully |
| 2220 | Password change fail | User password change failed |
| 5120 | Reset trips | Latched trips reset |
| 5270 | System startup | Software reset |
| 6110 | Test on | Test mode started |
| 6120 | Test off | Test mode ended |
| 6130 | Control operation | Control operation performed successfully |

PCM600 Event Viewer can be used to view the audit trail events and process related events. Audit trail events are visible through dedicated Security events view. Since only the administrator has the right to read audit trail, authorization must be used in PCM600. The audit trail cannot be reset, but PCM600 Event Viewer can filter data.

# 6 Using local HMI

## 6.1 Logging in

To use the LHMI, logging in and authorization are required. Password authorization is disabled by default and can be enabled via the LHMI.

To enable password authorization, select **Main menu** > **Configuration** > **Authorization** > **Passwords**. Set the *Local override* parameter to “False”.

1. Press ↵ to activate the login procedure.
2. Press ^ or v to enter the username character by character.

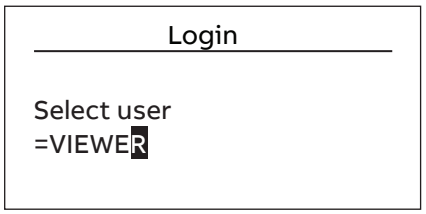


*Figure 3: Selecting access level*

3. Confirm the selection with ↵.
4. Enter the password when prompted character by character.

Special characters are not allowed.

- Activate the digit to be entered with < and >.
- Enter the character with ^ and v.

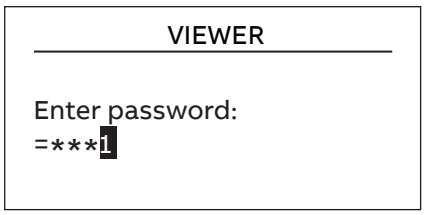


*Figure 4: Entering password*

5. Press ↵ to confirm the login.

- To cancel the procedure, press ESC.

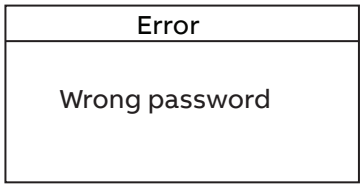


*Figure 5: Error message indicating wrong password*

When entering the username or password, pressing the ESC key will go back to previous screen.

The current user level is shown on the display's upper right corner in the icon area.

When local override is disabled, the Login page is shown in case of any LHMI activity.

### 6.1.1 Logging in via USB port

The relay can be configured via the USB port.

1. Select **Main menu** > **Configuration** > **System** > **Enable USB** and press ↵.
2. Select **True** and press ↵ to enable the relay to detect the USB connection.
3. Connect a computer with PCM600 to the relay's USB port.
4. Enter the credentials, if prompted.
   - If the *Remote override* parameter is "False", the LHMI prompts for username and password credentials before the relay is mounted as a USB device in the connected computer. The rights granted to engineer the relay via the USB port depend on the role of the user account used to log in. See *Chapter 4.1 Local user account management* for details.
   - If the *Remote override* parameter is "True", username and password credentials are not prompted in the LHMI. In this case, the rights provided to the client connected via the USB port are equivalent to ADMINISTRATOR.

See the engineering manual for more information on how to engineer the relay using the USB port.

Once the USB connection is disconnected, the previous session is closed and a new session is initiated when reconnected.

## 6.2 Logging out

An automatic logout occurs 30 seconds after the backlight timeout.

1. Press ESC continuously for 3 seconds.
2. To confirm logout, select `Yes` and press ↵.

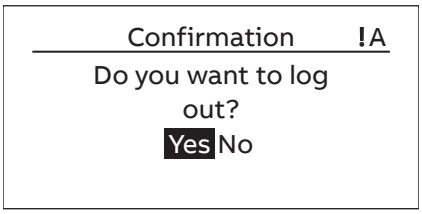


*Figure 6: Logging out*

- To cancel logout, press ESC.

# 7 Protection of relay and system configuration

## 7.1 Backup files

Backups are not directly part of the cyber security but they are important for speeding up the recovery process, for example, in case of failure of the protection relay. Backups need to be updated when there are changes in configuration.

### 7.1.1 Creating a backup from the relay configuration

1. Use the “Read from IED” function from the IED context menu in PCM600 to back up the relay configuration.

   

   User authorization is needed before using the tool.

2. Enter the user credentials if the default administrator password has been changed.

   Administrator or engineer credentials are needed for authorization.

### 7.1.2 Creating a backup from the PCM600 project

Backup from the PCM600 project is made by exporting the project.

1. On the **File** menu, click **Open** > **Manage Project** to open the project management.
2. Select the project from the **Currently available projects** dialog box.
3. Right-click the project and select **Export Project** to open the **Create target file for the project export** dialog box.
4. Browse the target location and type the name for the exported file.
   All project related data is compressed and saved to one file, which is named and located according to the definitions.

## 7.2 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 stored in the factory are restored. As the device has no configuration, the warning `Config. not available` is displayed.

Only the administrator can restore the factory settings.

1. Select **Main menu** > **Configuration** > **General** > **Factory setting** and press .
2. Set the value with or and press .
3. Confirm by selecting **Yes** with or and press .

The protection relay restores the factory settings and restarts. Restoring takes 1...3 minutes. Confirmation of restoring the factory settings is shown on the display a few seconds, after which the relay restarts.

Avoid the unnecessary restoring of factory settings, because all the parameter settings that are written earlier 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.

## 7.3 Restoring the administrator password

If authentication is enabled in the protection relay and the administrator password is lost, it is no longer possible to change passwords or operate the relay with full access rights.

- Contact ABB technical customer support to retrieve back the administrator level access to the protection relay.
- Generate a one-time password by pressing and simultaneously. The OTP can be generated only when the LHMI display prompts for the ADMINISTRATOR password.

# 8 Glossary

| | |
|---|---|
| CA | Certification authority |
| EMC | Electromagnetic compatibility |
| Ethernet | A standard for connecting a family of frame-based computer networking technologies into a LAN |
| FIFO | First in, first out |
| FTP | File transfer protocol |
| FTPS | FTP Secure |
| GOOSE | Generic Object-Oriented Substation Event |
| IEC | International Electrotechnical Commission |
| IEC 61850 | International standard for substation communication and modeling |
| IED | Intelligent electronic device |
| IEEE 1686 | Standard for Substation Intelligent Electronic Devices' (IEDs') Cyber Security Capabilities |
| IP | Internet protocol |
| LHMI | Local human-machine interface |
| Modbus | A serial communication protocol developed by the Modicon company in 1979. Originally used for communication in PLCs and RTU devices. |
| NERC CIP | North American Electric Reliability Corporation - Critical Infrastructure Protection |
| OTP | One-time password |
| PCM600 | Protection and Control IED Manager |
| RJ-45 | Galvanic connector type |
| RS-485 | Serial link according to EIA standard RS485 |
| SI | Sensor input |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| VPN | Virtual Private Network |

**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/relion**
**www.abb.com/substationautomation**



2NGA000818 B