Relion® Protection and Control

RER620 1.3
Cyber Security Deployment Guideline

Power and productivity
for a better world™

Document ID: 1MAC303953-RG
Issued: 07/20/2017
Revision: A
Product version: First release

Copyright

Trademarks

Warranty

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

ABB Inc.
Distribution Automation
4300 Coral Ridge Drive
Coral Springs, FL 33065, USA
Toll-free: 1 (800) 523-2620
Phone: +1 954-752-6700
Fax: +1 954 345-5329
http://www.abb.com/substationautomation

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 anti virus 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.

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 2004/108/EC) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2006/95/EC). This conformity is the result of tests conducted by ABB 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.

Table of Contents

Section 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 cyber security during the engineering, installation and commissioning phases, and during normal service.

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

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

1.3Product documentation

1.3.1 Product documentation set

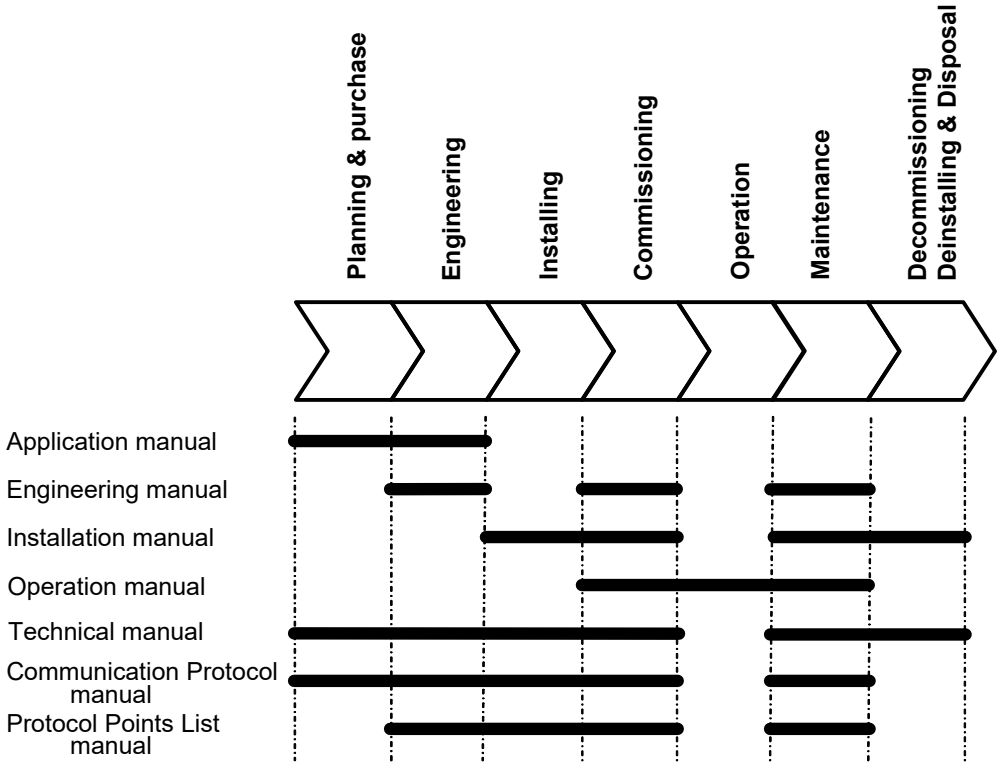

Figure 1: The intended use of manuals in different lifecycles

Product series- and product-specific manuals can be downloaded from the ABB Web site http://www.abb.com/relion.

1.3.2 Document revision history

Document revision/date	Product series version	History
A/07/20/2017	1.3	First release

Download the latest documents from the ABB web site http://www.abb.com/substationautomation.

1.3.3 Related documentation

Product series- and product-specific manuals can be downloaded from the ABB web site http://www.abb.com/substationautomation.

1.4 Symbols and conventions

1.4.1 Safety indication 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 to 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 should be understood that operation of damaged equipment could, under certain operational conditions, 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 in this manual 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, for example:

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

  Select **Main menu > Settings**.
- LHMI messages are shown in Courier font, for example:

  To save the changes in non-volatile memory, select `Yes` and press  .
- Parameter names are shown in italics, for example:

  The function can be enabled and disabled with the *Operation* setting.
- Parameter values are indicated with quotation marks, for example:

  The corresponding parameter values are "On" and "Off".
- Input/output messages and monitored data names are shown in Courier font, for example:

  When the function starts, the `START` output is set to TRUE.
- This document assumes that the parameter setting visibility is "Advanced".

Section 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 60870-5-104, DNP3 and 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 continual improvement of cyber security solutions also 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.

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

Operational reliability and long life time have been assured 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 Reference documents

Information security in critical infrastructure like electrical distribution and transmission networks has been in high focus for both vendors and utilities. This together with developing technology, for example, appliance of Ethernet and IP based communication networks in substations, power plants and network control centers creates a need of specifying systems with cyber security.

ABB is involved in the standardization and definition of several cyber standards, the most applicable and referred ones are ISO 2700x, IEC 62443, IEEE P1686 and IEC 62351. Besides standardization efforts there are also several governments initiated requirements and practices like NERC CIP and BDEW. ABB fully understands the importance of cyber security for substation automation systems and is committed to support users in efforts to achieve or maintain compliance to these.

Section 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 upto-date
- Removing all unnecessary user accounts
- Changing default passwords and using strong enough passwords
- Checking that the link from substation to upper level system uses strong enough encryption and authentication
- Separating public network from automation network
- Segmenting traffic and networks
- Using firewalls and demilitarized zones
- Assessing the system periodically
- Using antivirus software in workstations and keeping those up-to-date

It is important to utilize the defense-in-depth concept when designing system security. 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.

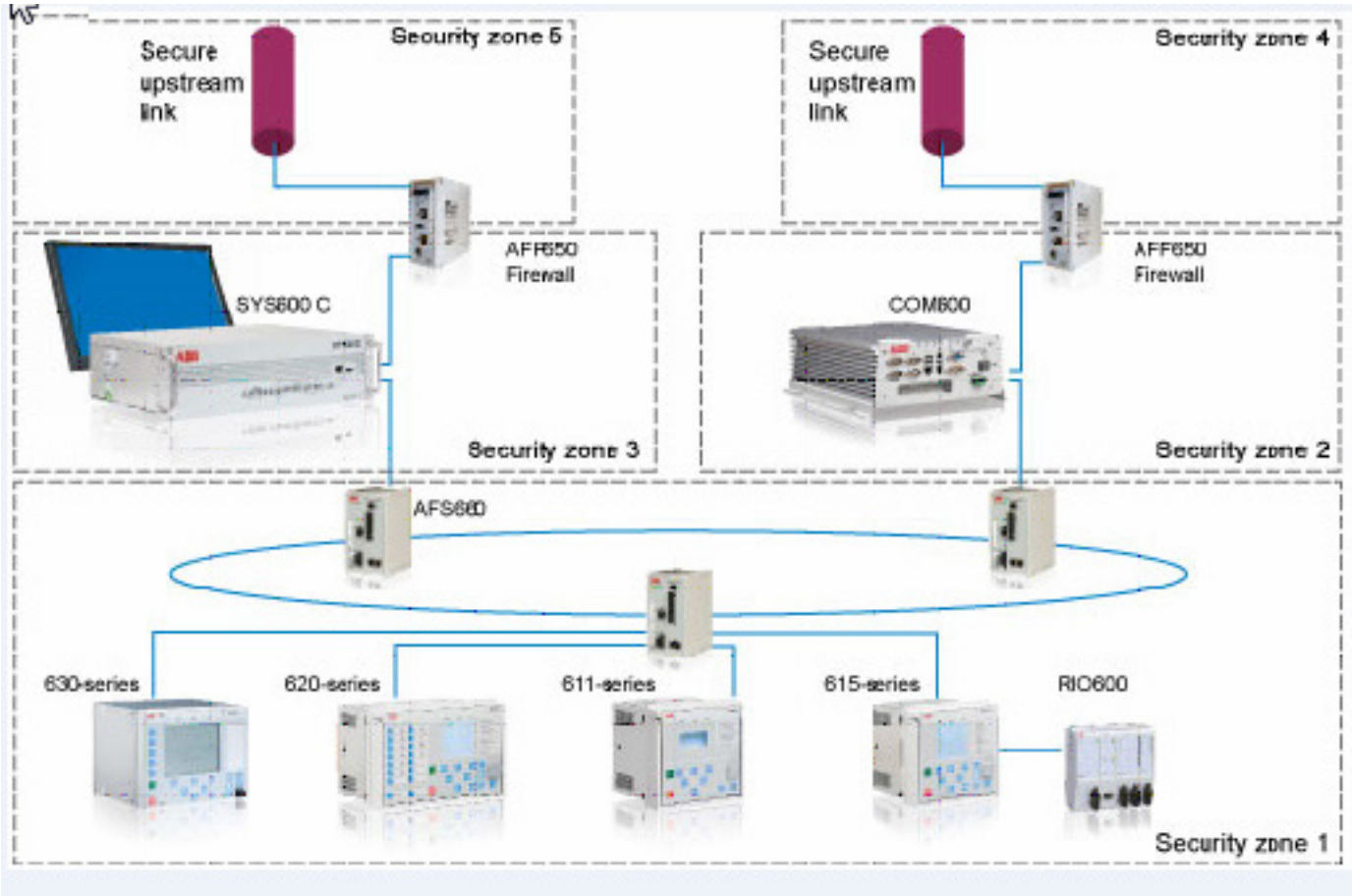

Figure 2: *Distribution substation example*

3.2 Relay communication interfaces

All physical ports dedicated for station bus communication can be opened and closed in relay configuration. Front port is used for engineering and it can be used only for point-to-point configuration access with PCM600 or WHMI. Front port should not be connected to any Ethernet network.

Table 1: Physical ports on relay's communication cards

Port ID	Type	Default state	Description
X1...X3	RJ-45 or fiber optic	Open	Ethernet station bus
X5	RS485	Closed	Serial station bus
X6	RS232/RS485	Closed	Serial station bus
X9	ST serial	Closed	Serial station bus
X12	ST serial	Closed	Serial station bus
X16	Fiber optic Ethernet	Open	Line Differential
Front port	RJ-45	Open	LHMI service access

If the protection relay is ordered with station bus option, serial ports are closed by default and Ethernet ports are open. IEC 61850, Modbus and DNP3 protocols are ON by default on Ethernet ports. The protocols are OFF by default on serial ports. IEC 61850 protocol and rear Ethernet ports are by default activated as those are used for engineering of the protection relay. 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.

The relay supports an option with multiple station communication Ethernet ports. In this case, all ports use the same IP and MAC address regardless of what redundancy option is activated in the relay configuration.

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)
102	TCP	Open	IEC 61850
80	TCP	Closed	Web Server HTTP
123	UDP	Client service not active by default in relay	Simple Network Time Protocol
502	TCP	Closed	Modbus TCP
20000	TCP	Closed	DNP TCP
20000	UDP	Closed	DNP UDP

FTP 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 HTTP and FTP protocols, the relay supports three Ethernet-based substation automation communication protocols, IEC 61850, Modbus and DNP3.

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/UDP port is closed and unavailable. RER620 can be ordered with more than one protocol. If the protocol service is configured, the corresponding port is open all the time.

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

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

3.4 Encryption algorithms

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

3.5 Web HMI

The WHMI is one of the available user access services in the protection relay and by default the service is disabled in which case the HTTP TCP ports are closed. WHMI can be enabled with the Web HMI mode parameter via LHMI menu path **Main menu/Configuration/HMI**.

The access to the relay's WHMI is protected by the HTTP Digest Access

Authentication (DAA) that requires a user name and password. DAA ensures that the user credentials are encrypted secure before sending over the network. See RFC2617 "HTTP Authentication: Basic and Digest Access Authentication" for detailed information about DAA.

User authentication is always required in WHMI.

If the Internet Explorer is used as Web client the advanced option "Show friendly HTTP error messages" might be enabled by default. It is recommended to disable this option. If this option is enabled, detailed error information of the WHMI is shown. The option can be found in the "Advanced" tab of the "Internet Options".

Section 4 User management

4.1 User roles

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

The default passwords in the protection relay delivered from the factory can be changed with Administrator user rights. Relay user passwords can be changed using LHMI, WHMI or the IED User Management tool in PCM600 and the user information is stored to the protection relay's internal memory.

User authorization is disabled by default for the LHMI and can be enabled with the Local override parameter via the LHMI path Main Menu/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 on menu root level.

Table 3: Predefined user categories

Username	User rights
VIEWER	Read only access
OPERATOR	• Selecting remote or local state with  (only locally) • Changing setting groups • Controlling • Clearing alarm and indication LEDs and textual indications
ENGINEER	• Changing settings • Clearing event list • Clearing DFRs • Changing system settings such as IP address, serial baud rate or DFR settings • Setting the relay to test mode • Selecting language
ADMINISTRATOR	• All listed above • Changing password • Factory default activation

If the Remote override parameter from the Main menu/Configuration/ Authorization/Passwords menu has been disabled, changes have to be made in the IED's object properties in PCM600. When the protection relay uses remote authentication, the activated user level and its password are required when the protection relay is configured using PCM600

Table 4: Object properties to change

Object Properties field	Value
Is Authentication Disabled	False
Is Password used	True
Password	Write the correct password

When communicating with the protection relay with PCM600 tools and with the relay authentication enabled, the relay username and password must be given when prompted. When setting the technical key, the username and password must be given twice.

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.

When Remote override is disabled, also MMS clients need authentication using correct password.

FTP always requires authentication.

4.2 Password policies

Passwords are settable for all predefined user categories. The LHMI password must be at least four and WHMI password at least nine characters. The maximum number of characters is 8 for the LHMI password and 20 for the WHMI password. Only the following characters are accepted.

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

User authorization is disabled by default and can be enabled via the LHMI or WHMI **Main Menu/Configuration/Authorization/ Passwords.**

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

Table 5: Predefined user categories and default passwords

Username	LHMI password	WHMI password	User rights
VIEWER	0001	remote0001	Only allowed to view
OPERATOR	0002	remote0002	Authorized to make operations
ENGINEER	0003	remote0003	Allowed to change protection relay parameters but no operation rights.
ADMINISTRATOR	0004	remote0004	Full access

For user authorization for PCM600, see PCM600 documentation.

4.2.1 Setting passwords

For user authorization for PCM600, see PCM600 documentation. can be set via the LHMI or WHMI or with PCM600.

Local passwords can be changed only via the LHMI. Remote passwords can be changed via the LHMI or WHMI or with PCM600.

1. Select **Main menu /Configuration/Authorization/Passwords.**
2. Select the password to be reset with  or  .
3. Press  , change ehpassword with  or  and press  again.
4. Repeat steps 2 and 3 to set the rest of the passwords.

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

Section 5 Using the HMI

5.1 Using the local HMI

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 parameter to *Local override* to "False".

5.1.1 Logging in

1. Press  to activate the login procedure.
2. Press  or  to select the user level.

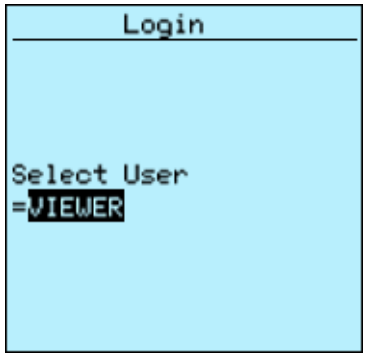

Figure 3: Selecting access level

3. Confirm the selection with  .

4. Enter the password when prompted digit by digit.
   - Activate the digit to be entered with ← and →.
   - Enter the character with ↑ and ↓.

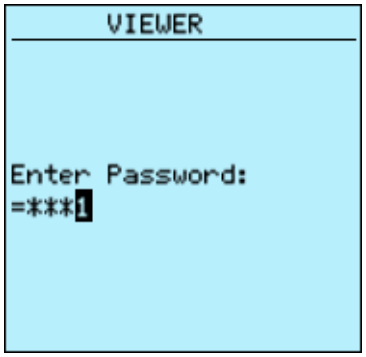

Figure 4: Entering password

5. Press ↵ to confirm the login.
   - To cancel the procedure, press ESC.

Figure 5: Error message indicating wrong password

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

5.1.2 Logging out

An automatic logout occurs 30 seconds after the backlight timeout.

1. Press 🔑.
2. To confirm logout, select `Yes` and press ↵.

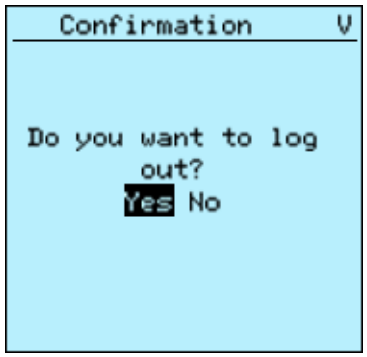

Figure 6: Logging out

- To cancel logout, press ESC.

5.2 Using the Web HMI

WHMI is disabled by default, and has to be activated in the protection relay configuration.

1. To enable the WHMI, select **Main menu / Configuration / HMI/ Web HMI mode** via the LHMI.
2. Reboot the relay for the change to take effect.
3. Log in with the proper user rights to use the WHMI.

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

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.**

5.2.1 Logging in

1. Open Internet Explorer
2. Type the protection relay's IP address in the Address bar and press ENTER.
3. Type the username with capital letters.
4. Type the password.

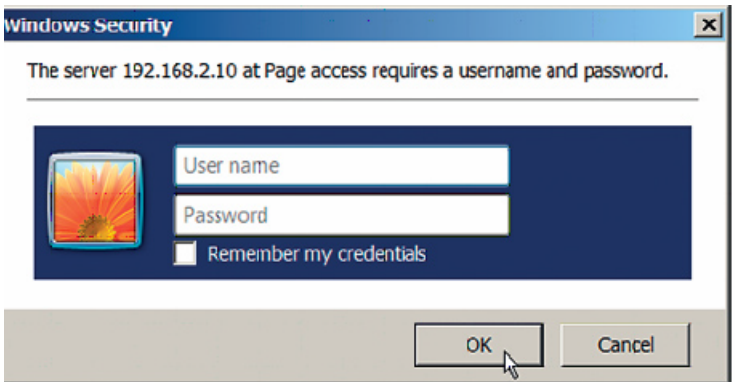

Figure 7: Entering username and password to use the WHMI

5. Click **OK**.
   The language file starts loading and the progress bar is displayed.

5.2.2 Logging out

The user is logged out after session timeout. The timeout can be set in **Main menu /Configuration/HMI/Web HMI timeout**.

To log out manually, click **Logout** on the menu bar.

Section 6 Protection of relay and system configuration

6.1 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.

6.1.1 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.

6.1.2 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.

6.2 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 and configuration files stored in the factory are restored. Only the administrator can restore the factory settings

1. Select **Main menu /Configuration/General/Factory setting** and press 
2. Select 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.

6.3 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.

Section 7 Glossary

BDEW	Bundesverband der Energie- und Wasserwirtschaft
CA	Certification authority
DAA	HTTP Digest Access Authentication
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.
DOM	Binary output module, four channels
DPC	Double-point control
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
HMI	Human-machine interface
HSR	High-availability seamless redundancy
HTML	Hypertext markup language
HTTP	Hypertext Transfer Protocol
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 61850-8-1	A communication protocol based on the IEC 61850 standard series
IED	Intelligent electronic device (protection and control relay)
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEEE 1588 v2	Standard for a Precision Clock Synchronization Protocol for networked measurement and control systems
IEEE 1686	Standard for Substation Intelligent Electronic Devices' (IEDs') Cyber Security Capabilities
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.
IRIG-B	Inter-Range Instrumentation Group's time code format B
ISO	International Standard Organization
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.
NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection
PCM600	Protection and Control IED Manager
PRP	Parallel redundancy protocol
PTP	Precision Time Protocol
RJ-45	Galvanic connector type
RS-232	Serial interface standard
RS-485	Serial link according to EIA standard RS485
SMV	Sampled measured values
SNTP	Simple Network Time Protocol
ST	Connector type for glass fiber cable
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User datagram protocol
VPN	Virtual Private Network
WHMI	Web human-machine interfacel

Contact us

ABB Inc.
Distribution Automation
4300 Coral Ridge Drive
Coral Springs, FL 33065, USA
Phone:+1 (800) 523-2620
Phone:+1 954-752-6700
Fax:+1 954 345-5329
www.abb.com/substationautomation

Power and productivity
for a better world™