Protection and Control IED Manager PCM600
Cyber Security Deployment Guideline

Power and productivity
for a better world™

Document ID: 1MRS758440
Issued: 2016-09-29
Revision: B
Product version: 2.8

Copyright

Trademarks

Warranty

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

www.abb.com/substationautomation

Disclaimer

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.

Table of contents

Table of contents

Section 1 Introduction

1.1 This manual

The cyber security deployment guideline describes the process for handling cyber security when engineering and monitoring protection and control IEDs. The cyber security deployment guideline provides information on how to secure the engineering environment on which the IED is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service. See also all IED-related cyber security deployment guidelines.

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 IEDs, 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

1.3 Product documentation

1.3.1 Product documentation set

The cyber security deployment guideline describes the process for handling cyber security when engineering and monitoring protection and control IEDs. The cyber security deployment guideline provides information on how to secure the engineering environment on which the IED is installed. The guideline can be used as a technical reference during the engineering phase, installation and commissioning phase, and during normal service. See also all IED-related cyber security deployment guidelines.

The getting started guide provides basic instructions on how to use PCM600. The manual provides instructions for typical use cases in operation and field, as well as for use cases in engineering and commissioning. The purpose of the manual is to describe the PCM600 tool functionality, and it can be seen as a complementary manual to the application-related instructions, such as the relay-specific operation or engineering manuals.

The online help contains instructions on how to use the software.

1.3.2 Document revision history

Document revision/date	Product version	History
A/2015-11-20	2.7	First release
B/2016-09-29	2.8	Content updated

1.3.3 Related documentation

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

1.3.4 Symbols and conventions

1.3.4.1 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.

Operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to information or property loss. Therefore, comply fully with all notices.

1.3.4.2 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**.
- Menu, tab, button, list and box names as well as window or dialog box titles are presented in bold.
  On the **File** menu, click **New Project**.
  Right-click the **MainApp** tab and select **Copy** from the shortcut menu.
  Click **OK** to start the comparing.
- Shortcut keys are presented in uppercase letters.
  A page can also be added pressing the shortcut keys CTRL+SHIFT+P.
- Command prompt commands are shown in Courier font.
  Type `ping <devices_IP_address>/t` and wait for at least one minute to see if there are any communication breaks.
- Parameter names are shown in italics.
  The function can be enabled and disabled with the *Operation* setting.

Section 2 Security in substation and distribution automation systems

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.

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.

See also all IED-related cyber security deployment guidelines.

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 IEDs 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 IEDs 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
- 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
- Using principle of least privilege

It is important to utilize the defence-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.

3.2 TCP/IP based protocols and used IP ports

The following table summarizes the IP ports used by the device to set up an IP firewall. All closed ports can be opened in the configuration. Ports which are open by default are used for configuring or monitoring the protection IED. Ports defined in Table 1 are needed only for local connection.

Table 1: IP ports used by PCM600

Port number	Type	Default state	Description
5555	TCP, UDP	Open	PCMMessengerService, which allows multiple PCM600s to interact on same computer
5556	TCP, UDP	Open	PCMSchedulerService, which allows scheduled services being run with PCM600 (for example, automatic disturbance report retrieve)

Additionally, see the IED-specific cyber security deployment guidelines for ports that are required to communicate and to configure the IEDs.

In case Scheduler is not required on the setup, it is recommended to close ports 5555 and 5556. It is also recommended to first stop and then disable PCMSchedulerService and PCMMessengerService from Services.

When PCMMessengerService is stopped but not disabled, an output message is displayed:

```
PCM600 could not start PCMMessengerService on local
computer: Cannot start service PCMMessengerService on
computer. The service did not respond to the start or
control request in a timely fashion.

Please restart PCM600 on 'Run as administrator' option.
You can also try to fix the problem by rebooting your
computer.
```

If PCMSchedulerService and the related ports are disabled, none of the configured tasks are run. If the PCMMessengerService and related ports are disabled, the configured PCMScheduler tasks will not be executed.

3.3 Secure communication

Some of the protection IEDs support encrypted communication according to the principles of IEC 62351 in secured communication for WHMI and file transfer protocol. If the *Secure Communication* parameter is activated in the IED, protocols

require TLS protocol based encryption method support from the clients. In case of file transfer, the client must use FTPS. PCM600 supports FTPS and is able to download and upload configuration files in encrypted format from IED.

Section 4 PCM600 user management

4.1 PCM600 user authentication

This section describes the user authentication for PCM600. For IED user authentication, see the IED-specific cyber security deployment guidelines.

PCM600 supports working with authenticated and anonymous users. No authentication method is enabled by default.

It is not recommended to use PCM600 without authentication.

When PCM600 is started for the first time, a PCM600 administrator account has to be created and named. The password is not set by default. It is recommended to change the password immediately for the created administrator account.

It is not recommended to use the administrator accounts by default. It is recommended to create limited user accounts that have privileges only for performing the necessary tasks related to the user role.

4.2 Activating user authentication

The system engineer can enable or disable the user authentication. When the user authentication is disabled, all the users get full rights to operate. The login function also works according to this function. For more information on the login functions, see the getting started guide.

1. On the main menu, point to **Tools** and select **Options** to start the user management.
2. Select the **System Settings** folder.
3. Select or clear the **Use Authentication** check box to enable or disable the user authentication.
4. Select **PCM Authentication** or **Windows Authentication** under the **Authentication Method** field.
   The Windows authentication uses current user's Windows account to determine if the user is allowed to log in to PCM600. If this authentication is selected, it is checked that all the user accounts contain the Windows account name, which is used to log in the user.

The PCM authentication uses user name and password specified in the user management of PCM600. This information must then be provided in the **Log in** dialog.

Recommended authentication method is the Windows authentication.

4.3 User categories

4.3.1 Creating user categories

The user management is based on the users and the user categories. The users have a user account for PCM600. Each user account is mapped to one user category, which defines the permission to access certain functions. There are three default user categories.

- System Engineer acts as an administrator for the system and has full rights to perform any function and can define the user accounts.
- Operator can perform certain simple tasks and has read-only access to certain functionality of PCM600.
- Application Engineer can access most of the functions and has read and write access to the IED engineering functionality.

Check the actual settings of the user categories from **Tools/Options/Category Manager** in PCM600.

The members of the System Engineer user category can create new user categories. The name of the user category must be unique.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select the **Category Manager** folder.
3. Click **Add New Category** to open the **Add New Category** dialog.
4. Type the name for the new user category.
5. Specify the rights to perform different functions under the **Functions And Rights** field.
6. Select **OK** to save the definition.

4.3.2 Deleting user categories

A user with the System Engineer rights can delete the user categories. The System Engineer category cannot be deleted. If there are members in the deleted category, a confirmation for removing the category appears. If the category is removed, the user

accounts remain, but they are no longer mapped to any user category. The category changes are saved to the system configuration data.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select the **Category Manager** folder.
3. Select the right user category from the drop-down list.
4. Click **Delete Category** to remove the user category.
5. Click **Yes** to confirm the delete operation.

4.3.3 Modifying existing user categories

System Engineer can change the access rights of an existing user category. The access rights of the System Engineer user category cannot be changed. The System Engineer user category has always full privileges.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select **Category Manager** folder.
3. Select the right user category from the **User Categor**y drop-down list to activate the **Functions And Rights** field.
4. Change the user rights by selecting one of the user levels in the drop-down menu of the function.

The Functions And Rights field is divided into different sections for you to specify the user rights by a specific tool component or function.

4.4 User management

This chapter describes the user management for PCM600. For IED user management, see the IED-specific cyber security deployment guidelines.

4.4.1 Creating users

Create a new user to PCM600 and define the user information.

- User name (mandatory)
- Real name of the user
- User category

The Windows account can be used to log in automatically. Multiple Windows account names can be used for a single PCM600 account.

The Windows account names are separated by a semicolon (;). These Windows account names are only used for login, if the administrator has enabled the Windows authentication.

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select the **User Manager** folder.
   The default **Real Name** is System Administrator and makes it easier to find the user.
3. Click **Add New User** in the **User Profile** field.
   The **Add New User** dialog is displayed.
4. Type **User Name** and select **User Category** from the drop-down list.
   The user name must be at least three characters long.
5. Click **OK** to confirm.
   The new user is created.

The new user name has to be a member of a user category to have permission to PCM600 functions.

4.4.2 Deleting users

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select **User Manager** folder.
3. Select the right user name from the **User Name** drop-down list.
4. Click **Delete User** under the User Profile field.

Only users with System Engineer rights can delete a user.

The System Engineer account cannot be deleted.

4.4.3 Changing password

1. On the menu bar, click **Tools** and select **Options** to start the user management.
2. Select **User Manager** folder.
3. Click **Set Password** under User Preferences to open **Set Password** dialog.
4. Type the old password.
5. Type the new password.
   The password must meet certain requirements.

- Cannot be empty
- Starts and ends with an alphabetic character
- Contains at least one special character ~!@#$%^*_-+=`|\(){}[]:<>,.?/
- Is at least eight characters long
- Contains at least one number 0-9
- Contains at least one uppercase character
- Contains at least one lowercase character

6. Retype the new password for confirmation and click **OK**.

When changing the authentication password, the validity of password is checked and a new password is saved to the database.

Section 5 Configuration of computer settings for PCM600

5.1 General security actions

In general, the Windows operating system can be protected from the malicious attacks with the latest service packs and security updates, firewalls, security policies, application whitelisting, and virus scanners. In computers where PCM600 is installed, programs and services that are not used can be uninstalled or disabled to reduce the attack surface.

This section gives an overview of different ways to secure the operating systems on which PCM600 is installed.

If PCM600 is run on virtual computer, these recommendations still apply.

5.2 Operating systems

Table 2: Supported operating systems for PCM600 installation

Edition	Operating system
Desktop	Windows Vista Windows 7.0 Windows 8.0 Windows 8.1 Windows 10.0
Server	Windows Server 2008 R2 Windows Server 2012 R2

See the operating system related documentation and best practices to further reduce the attack surface in the operating system.

5.3 BIOS settings

Passwords must be enabled and remote wake up/wake on LAN disabled manually.

5.4 Windows updates and patch management

There are nine update classifications defined by Microsoft. These include, for example, critical updates, drivers, security updates and service packs. The compatibility of PCM600 with the latest Microsoft security updates and service packs is tested and verified monthly by ABB. The report does not cover computers from which PCM600 is accessed remotely. In general, it is recommended to install all the Windows updates.

Windows Update vs. Microsoft Update

Windows Update receives updates only for the Windows operating system. Microsoft Update must be used for other installed Microsoft products. The updates must be configured manually.

After PCM600 installation, it is recommended to update the system to the latest ABB verified patch level of all installed ABB software products. For other vendors' software products, see the respective documentation.

5.5 Virus scanner

PCM600 does not create specific requirements for anti-virus software. It is recommended to use organization specific de facto anti-virus software, which has to be configured manually.

5.6 Firewall, ports and services

PCM600 does not have specific firewall requirements. PCM600 is a client system from the communication point of view. The firewall has to be configured manually.

5.7 Disabling of devices

It is recommended to disable any unused devices in the system, such as USB ports, CD/DVD drives, communication ports, or floppy disc controllers. Devices are disabled manually in devmgmt.msc (Device Manager).

Disabling of autorun functionality

If it is not possible to disable a device, disable the autorun functionality of the device. The autorun functionality is disabled to prevent the automatic start of the malicious

code contained in a removable device. For more information, see support.microsoft.com/kb/967715/en-us, How to disable the Autorun functionality in Windows.

5.8 User Account Control

User Account Control (UAC) is a security feature in Windows 7, Windows Server 2008 R2 and the later versions. UAC is recommended to be enabled in PCM600 and in computers that are used to access PCM600.

Table 3: Actions if the program requires privilege elevation

User role	Action
Administrators	A dialog is shown for selecting **Continue** or **Cancel**. In Windows Server edition, **Prompt for consent** is used for non-Windows binaries.
Standard users	A message box is shown stating that a program has been blocked. This setting was introduced in Windows 7, Server 2008 R2 and the later versions.

A shield in the program icon indicates that it requires administrative privileges to run. This is automatically detected by the operating system, if for example, Run as administrator flag is set in the file properties, or if the program has previously asked for administrative privileges.

It is not recommended to use administrator accounts by default. It is recommended to create limited user accounts that have privileges only to perform the necessary tasks related to the user role.

5.9 Intrusion detection system

An intrusion detection system (IDS) is a device or software application that monitors the network or system activities for malicious activities or policy violations and produces reports to the management station. It is recommended that organization specific IDS; to be configured manually, is deployed on the computer running PCM600.

5.10 Enabling of SQL Server 2014 for PCM600

PCM600 requires access to the PCMSERVER2014 instance of SQL Server. The PCM user is added to PCMSERVER2014 Users Group in Windows to provide access.

During installation, the user logged in is automatically added to PCMSERVER2014 Users Group. If additional users are required, they have to be added to

PCMSERVER2014 Users Group. This can be done by using lursmgr.msc – Local Users and Groups (Local). The local Users and Groups function provides a possibility to add both local and network user accounts to PCMSERVER2014 Users Group.

Section 6 Project backups and restoring

Backups can be created by either backing up the computer running PCM600 or by using the functionality in PCM600 that exports the project configuration to a single file.

Configuration can be backed up by storing the Backup Project from PCM600 to a location that is regularly backed up. It is important to take and manage the project backups of the engineered substations. This enables proper configuration management for the users.

6.1 Creating a backup of a project

1. On the **File** menu, click **Open** and select **Manage Project** to open the project management.
2. Click **Backup Projects** functionality.
3. Select the projects from the list of available projects.
4. Click **Backup Selected**.
5. Browse the target location and click **OK**.

Creating a project backup enables transferring project data between the based systems via different media, for instance in CD-ROM. The source and target computers do not have to be connected to the same network so the data can be transferred between two stand-alone computers.

All project related data is compressed and saved to one file, which is named and located according to the definitions.

6.2 Restoring a project

Importing a project backup enables transferring project data between the based systems via different media, for instance in CD-ROM. The source and target computers do not have to be connected to the same network so the data can be transferred between two stand-alone computers.

1. On the **File** menu, click **Open** and select **Manage Project** to open the project management.
2. Right-click **Projects on my computer**, and click **Import** to open the **Import project** dialog box.
3. Browse the location and type the name for the imported file.

A new project is created containing all the data from the imported file.

Section 7 Standard compliance statement

Cyber security issues have been the subject of standardization initiatives by ISA, IEEE, or IEC for some time. ABB plays an active role in all these organizations, helping to define and implement cyber security standards for power and industrial control systems.

Some of the cyber security standards which are most important for substation automation, such as IEC 62351 and IEC 62443 (former ISA S99), are still under active development. ABB participates in the development by delegating subject matter experts to the committee working on the respective standard. Since these standards are still under development, ABB strongly recommends to use existing common security measures available in the market, for example, VPN for secure Ethernet communication.

Table 4: Overview of cyber security standards

Standard	Main focus	Status
NERC CIP	NERC CIP cyber security regulation for North American power utilities	Released, ongoing[1)]
IEC 62351	Data and communications security	Partly released, ongoing
IEEE 1686	IEEE standard for substation intelligent electronic devices (IEDs) cyber security capabilities	Finalized

1) Ongoing: major changes will affect the final solution

ABB has identified cyber security as a key requirement and has developed a large number of product features to support the international cyber security standards such as NERC CIP, IEEE 1686, as well as local activities like the German BDEW white paper.

Section 8 Glossary

BDEW	Bundesverband der Energie- und Wasserwirtschaft
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.
Ethernet	A standard for connecting a family of frame-based computer networking technologies into a LAN
FTP	File transfer protocol
FTPS	FTP Secure
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IEC 60870-5-104	Network access for IEC 60870-5-101
IEC 61850	International standard for substation communication and modeling
IED	Intelligent electronic device (protection and control relay)
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEEE 1686	Standard for Substation Intelligent Electronic Devices' (IEDs') Cyber Security Capabilities
IP	Internet protocol
ISO	International Standard Organization
LAN	Local area network
NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection
PCM600	Protection and Control IED Manager
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UAC	User Account Control
UDP	User datagram protocol
VPN	Virtual Private Network
WHMI	Web human-machine interface

Contact us

ABB Oy
Medium Voltage Products,
Distribution Automation
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11
Fax +358 10 22 41599

www.abb.com/mediumvoltage

www.abb.com/substationautomation

ABB AB
Grid Automation Products
SE-721 59 Västerås, Sweden
Phone +46 (0) 21 32 50 00
Fax +46 (0) 21 14 69 18

www.abb.com/protection-control

Power and productivity
for a better world™