RXplore

RXplore

Cyber Security Deployment Guideline

Document ID: 2NGA000487
Issued: 2023-04-24
Revision: E
Product version: 1.9

Copyright

Trademarks

ABB and Relion are registered trademarks of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders. SSC600 is an approved Intel® IoT Market Ready Solution.

Warranty

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

www.abb.com/mediumvoltage

Disclaimer

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

This product has been designed to be connected and communicate data and information via a network interface which should be connected to a secure network. It is the sole responsibility of the person or entity responsible for network administration to ensure a secure connection to the network and to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, encryption of data, installation of 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.

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

Contents

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 environment on which RXplore is deployed. 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 environment on which RXplore is deployed. 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 quick start guide provides basic instructions on how to use RXplore. The manual provides instructions for typical use cases in operation and field.

1.3.2 Document revision history

Document revision/date	Product version	History
A/2020-10-14	RXplore 1.0	First release
B/2021-01-19	RXplore 1.1	Content updated
C/2021-10-18	RXplore 1.3	FP3 added
D/2022-06-29	RXplore 1.6	Content updated
E/2023-04-24	RXplore 1.9	Content updated

1.3.3 Related documentation

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

1.4 Symbols and conventions

1.4.1 Symbols

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

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

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

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

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

1.4.2 Document conventions

A particular convention may not be used in this manual.

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

  Select **Main menu/Settings**.
- 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**.
- 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.

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 RXplore network setup

Below picture shows the RXplore network setup:

- Mobile network is used for reading product information and fetching IED firmware packages from ABB Data Care.
- RXplore mobile application is connected to IEDs over wireless access point.

It is recommended to use the latest wireless technologies for the communication between RXplore and the IEDs.

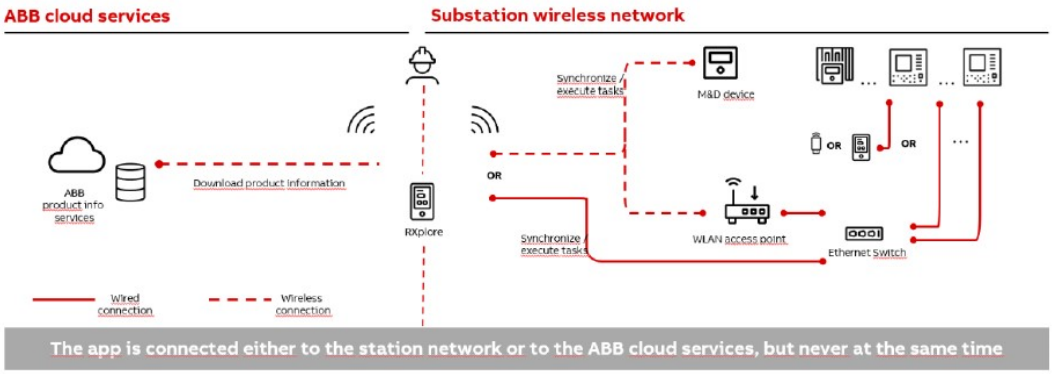

Figure 1: RXplore network setup

2.3 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.

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
- Physical access control

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

To set up an IP firewall, see the IED-specific cyber security deployment guidelines for the ports that are used to communicate and to configure the IEDs. All closed ports can be opened in the configuration. Ports that are open by default are used for configuring or monitoring the protection IED.

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. RXplore supports FTPS and is able to download and upload configuration files in encrypted format from IED.

4 User management

4.1 RXplore user authentication

RXplore mobile application does not have own user management, but it supports working with IEDs where user authorization is enabled.

In case IED user authorization has been enabled, user is indicated in RXplore user interface that communicating with the IED requires entering user credentials. If given username and password were chosen to be used as default credentials, they are persisted in mobile device storage securely so that they can be used when needed.

For IED user authentication, see the IED-specific cyber security deployment guidelines.

5 Configuration of mobile phone

5.1 General security actions

In general, the mobile phone operating system can be protected from the malicious attacks by keeping the device operating system up to date, installing latest security updates and by using with PIN code protection.

5.2 Operating systems

Table 1: Supported operating systems for RXplore

Operating system	Version
Android	9.0 or newer
iOS	13 or newer

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

5.3 OS updates and patch management

The compatibility of RXplore with the latest supported Operating System updates is tested and verified regularly by ABB.

It's recommended to install latest Operating System updates.

5.4 Virus scanner

RXplore 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.

5.5 Malware protection

It is recommended to use organization specific de facto malware protection software, which has to be configured manually.

5.6 External storage usage

RXplore supports installation on external storage, e.g. SD card. There might be operating system dependent differences on how installation on external storage needs to be done.

5.7 Firewall, ports and services

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

Table 2: IP ports used from RXplore to IED

Port number	Type	Description
20,21	TCP	File Transfer protocol (FTP/ FTPS)
102	TCP	IEC 61850
50000	TCP	SWICOM application

Table 3: IP ports used from RXplore to Cloud

Port number	Type	Description
80,443	TCP	Web Server HTTPS

6 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

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.

[1] Ongoing: major changes will affect the final solution

7 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
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
SD	Secure Digital
TCP/IP	Transmission Control Protocol/Internet Protocol
UAC	User Account Control
VPN	Virtual Private Network
WHMI	Web human-machine interface

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

2NGA000487 E