MasterPact MTZ

Cybersecurity Guide

06/2020

DOCA0122EN-03

www.schneider-electric.com

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information 5
About the Book 7
Chapter 1 An Introduction to Cybersecurity 9
An Introduction to Cybersecurity 10
Why Cybersecurity Is Relevant for MasterPact MTZ Circuit Breakers 11
Chapter 2 Cybersecurity Recommendations for System Design, Planning and Installation 13
Identifying and Protecting Sensitive and Critical Information and Operations 14
Designing a Password Policy 15
Training 18
Chapter 3 Cybersecurity Recommendations for Local Access 19
Restricting Local Access to the MasterPact MTZ Circuit Breaker 20
Recommendations for Protecting Local Access to the MicroLogic X HMI 21
Recommendations for Protecting Access Through NFC 22
Recommendations for Protecting Access Through Bluetooth 23
Recommendations for Protecting Access to the MicroLogic X Control Unit Through Mini USB Port 25
Chapter 4 Cybersecurity Recommendations for Remote Access 27
Restricting Remote Access to the MasterPact MTZ Circuit Breaker 28
Separating OT Network from Corporate Network 29
Recommendations for Protecting Remote Access to the MicroLogic X Control Unit Through Ethernet 30
Recommendations for Protecting Remote Access to the MicroLogic X Control Unit Through Modbus-SL 31
Chapter 5 Cybersecurity Recommendations for Firmware Updates and Digital Modules 33
Installing Firmware Updates 34
Purchasing and Installing Digital Modules 36
Schneider Electric Cybersecurity Support Portal 37
Glossary 39

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

CYBERSECURITY SAFETY NOTICE

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About the Book

At a Glance

Document Scope

This guide provides information on cybersecurity aspects for MasterPact™ MTZ circuit breakers with MicroLogic™ X control units to help system designers and operators promote a secure operating environment for the product.

This guide does not address the more general topic of how to secure your operational technology network, or your enterprise Ethernet network. For a general introduction to cybersecurity threats and how to address them, refer to *How Can I Reduce Vulnerability to Cyber Attacks?*.

NOTE: In this guide, the term **security** is used to refer to cybersecurity.

Validity Note

The information in this guide is relevant for MasterPact MTZ circuit breakers with MicroLogic X control units.

The information contained in this guide is likely to be updated at any time. Schneider Electric strongly recommends that you have the most recent and up-to-date version available on *www.se.com/ww/en/download*.

The technical characteristics of the devices described in this guide also appear online. To access the information online, go to the Schneider Electric home page at *www.se.com*.

Related Documents

Title of Documentation	Reference Number
MasterPact MTZ - MicroLogic X Control Unit - User Guide	*DOCA0102EN*
How Can I Reduce Vulnerability to Cyber Attacks?	*Cybersecurity System Technical Note*
MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note	*DOCA0144EN*
Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker - Release Note	*DOCA0146EN*
Enerlin'X IFE Switchboard Server IFE/EIFE Ethernet Interface - Release Note	*DOCA0147EN*
Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Release Note	*DOCA0149EN*
Enerlin'X FDM128 - Ethernet Display for Eight Devices - Release Note	*DOCA0151EN*
EcoStruxure Cybersecurity Admin Expert User Guide	*NRJUSG18807EN*

You can download these technical publications and other technical information from our website at https://www.se.com/ww/en/download/ .

Trademark Notice

Chapter 1
An Introduction to Cybersecurity

Overview

This chapter provides general information on the Schneider Electric cybersecurity policy, and why cybersecurity is relevant for MasterPact MTZ circuit breakers with MicroLogic X control units.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
An Introduction to Cybersecurity	10
Why Cybersecurity Is Relevant for MasterPact MTZ Circuit Breakers	11

An Introduction to Cybersecurity

Introduction

Cybersecurity is intended to protect your communication network and all equipment connected to it from attacks that could disrupt operations (availability), modify information (integrity), or give away confidential information (confidentiality). The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. There are many aspects to cybersecurity including designing secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security procedures and best practice policies.

Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to MasterPact MTZ circuit breakers, you should follow the Schneider Electric defense-in-depth approach to cybersecurity.

This approach is described in the system technical note *How Can I Reduce Vulnerability to Cyber Attacks?*.

In addition, you will find many useful resources and up-to-date information on the Cybersecurity Support Portal on the Schneider Electric global website *(see page 37)*.

Why Cybersecurity Is Relevant for MasterPact MTZ Circuit Breakers

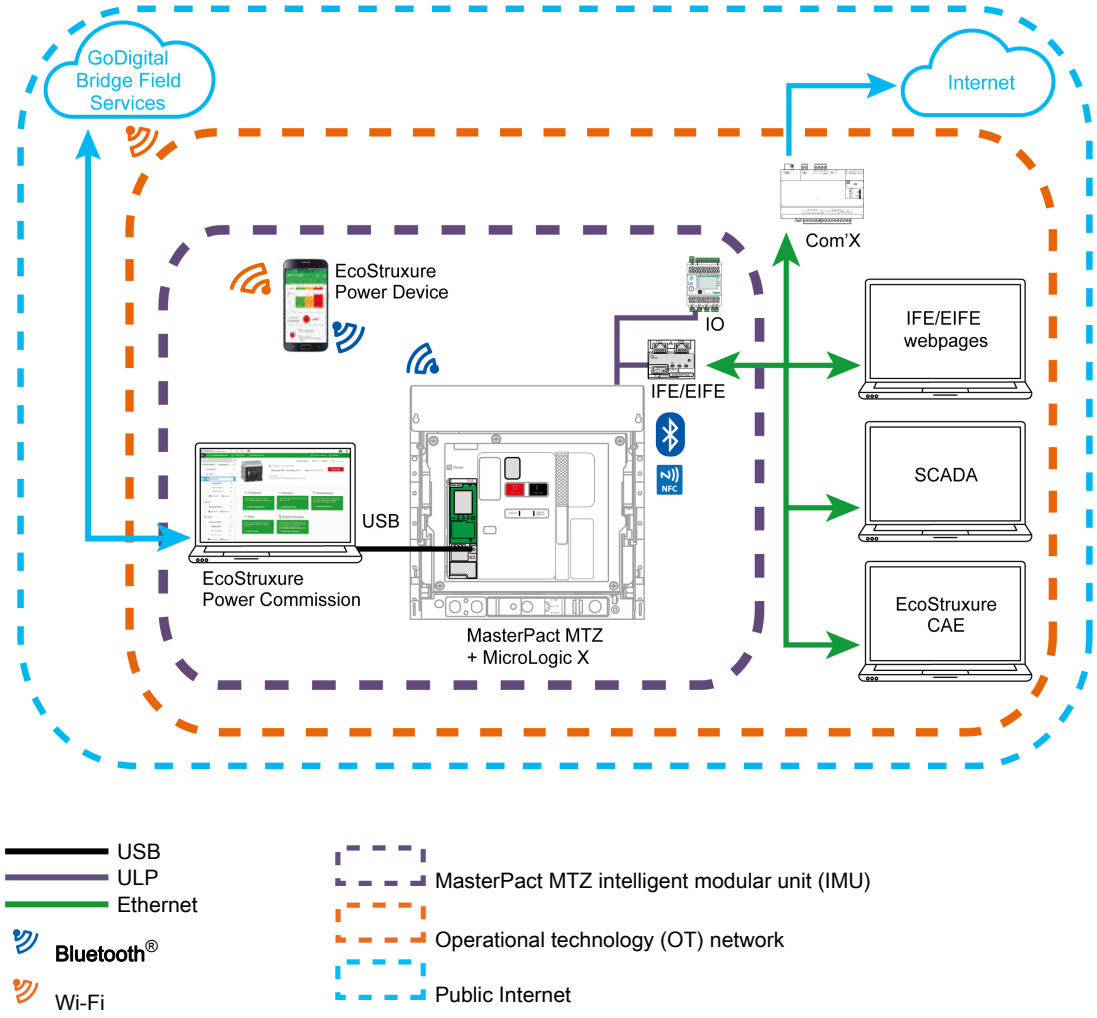
Overview

The MasterPact MTZ circuit breaker is a key component of any plant or equipment because it controls the power supply to the process, provides electrical protection, and delivers critical information.

MasterPact MTZ circuit breakers with communication features also provide 24/7 access to real-time control functions and to monitoring data. These features bring greater efficiency and flexibility in managing your electrical distribution system. However, they may be subject to cyber attacks.

MasterPact MTZ Circuit Breaker and Operating Environment

The following figure shows the various ways of communicating with the MicroLogic X control unit of the MasterPact MTZ circuit breaker.



The MasterPact MTZ intelligent modular unit (IMU) represents the circuit breaker, the MicroLogic X control unit, and the associated ULP modules, communication interface, and IO modules.

To communicate with the MasterPact MTZ circuit breaker through its MicroLogic X control unit, the following communication paths are available:

- MicroLogic X human-machine interface (HMI)
- Wireless NFC connection from a smartphone
- Wireless Bluetooth Low Energy (BLE) connection from a smartphone
- Connection to the mini type B USB port of the MicroLogic X control unit from:
  - A PC running EcoStruxure™ Power Commission software.
  - A smartphone running the EcoStruxure Power Device app
- Ethernet (Modbus TCP/IP or IEC 61850 protocols) connection through the operational technology (OT) network when the communication interface is present
- Modbus-SL connection through the operational technology (OT) network when the IFM interface is present.

System Vulnerability to Cyber Attacks

Each of the communication paths listed above represents a potential vulnerable point in your system if security measures are not put in place. This guide provides guidelines to help secure these communication paths to avoid intentional attacks or accidental misuse.

Chapter 2
Cybersecurity Recommendations for System Design, Planning and Installation

Chapter Overview

This chapter provides important information to consider during the design, planning, and installation phases of an operational technology (OT) network that includes the MasterPact MTZ intelligent modular unit (IMU). The recommendations and guidelines in this chapter help to build a secure operating environment.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Identifying and Protecting Sensitive and Critical Information and Operations	14
Designing a Password Policy	15
Training	18

Identifying and Protecting Sensitive and Critical Information and Operations

Overview

When planning and designing an operational technology network, it is important to identify information that is critical or sensitive for your operations. Once identified, this information must be protected.

As a general principle:

- Critical information includes data and operations accessible through the MasterPact MTZ IMU (for example, status of the circuit breaker, trip, or open/close command).
- Sensitive information includes any information that can be used to access your installation and your operational technology network (for example, passwords or access codes for equipment or for locked rooms).

It is your responsibility to determine how this information could be analyzed and used against your organization best interest.

Information About the Enterprise Communication Network

Sensitive information that can be used to access your installation and control network includes:

- Your system architecture
- IP addresses or MAC addresses of networked communicating devices
- Port numbers used for Ethernet communication
- User IDs and user passwords

This list is not exhaustive, and it is important to consider all information specific to your organization that can facilitate access to critical systems.

Access Control

An important part of cybersecurity consists in designing an effective access control policy. Access control consists in identifying groups of users or individual employees within your organization, and determining the type and the level of access they need to carry out their jobs effectively.

Summary of Information and Operations Accessible Through Each Access Path

Depending on the communication interface or the communication path used to access the MasterPact MTZ intelligent modular unit (IMU), the information and control operations available are different. The following table summarizes access to information and control operations:

Information and control operations	Local access				Remote access
	MicroLogic X HMI	NFC	Bluetooth low energy	USB	Ethernet / Modbus-SL
Data monitoring	Read	Read	Read	Read	Read
Protection settings	Read/Write	Read	Read/Write	Read/Write	Read/Write
Other settings	Read/Write	Read	Read/Write	Read/Write	Read/Write
Open/Close/Reset	No	No	Yes	Yes	Yes

For information on protecting each communication interface and access path, see the recommendations for local access *(see page 19)* or for remote access *(see page 27)*, as appropriate.

Designing a Password Policy

Overview

A carefully designed password policy is the first line of defense against cyber attacks.

In the context of installations that include the MasterPact MTZ circuit breaker with the MicroLogic X control unit, passwords are required for:

- Performing intrusive commands on the MicroLogic X control unit, whatever the access mode (through Modbus-TCP / Modbus-SL, USB connection, or Bluetooth)
- Logging in to the PC that runs EcoStruxure Power Commission software
- Logging in to IFE and EIFE interface webpages
- Logging in to IFE server webpages
- Logging in to FTP server for IEC 61850 configuration of the IFE and EIFE interfaces

Cybersecurity Recommendations Concerning Password Policy

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The password policy is one of the main elements of the cybersecurity policy. A good password policy consists of:

- Using strong passwords
- Changing passwords regularly
- Using a password vault to manage access passwords
- Forbidding reuse of old passwords
- Regularly reminding users about best practices concerning passwords

To help protect your system, at a minimum you should:

- Enforce the use of strong passwords
- Set the minimum password length to 10 characters
- Change the password periodically

All users must be aware of best practices concerning passwords. These include:

- Not sharing personal passwords
- Not displaying passwords during password entry
- Not transmitting passwords in email or by any other means
- Not saving the passwords on PCs or other devices

Password for MicroLogic X Critical Settings and Controls

When accessing the MicroLogic X control unit via a communication interface, any intrusive commands that modify the behavior of the MasterPact MTZ circuit breaker require a password. For example, making changes to the protection settings, or operating the circuit breaker requires the password for the MicroLogic X control unit.

Four passwords are defined for a MicroLogic X control unit, one for each of the following four user profiles:

- Administrator
- Services
- Engineer
- Operator

For more information on user profiles, refer to *DOCA0102EN MasterPact MTZ - MicroLogic X Control Unit - User Guide*.

When connecting through the EcoStruxure Power Device app or EcoStruxure Power Commission software, the user is prompted to provide one of these passwords.

When connecting from a remote monitoring and control interface, the password must be part of the communication request.

The password is composed of four ASCII characters. The password is case-sensitive and the allowed characters are:

- Digits from 0 to 9
- Lower case letters from a to z
- Upper case letters from A to Z

Default passwords must be changed at first installation of the MasterPact MTZ circuit breaker and periodically after the first installation, using EcoStruxure Power Commission software. Store passwords using a password vault. Only share passwords with a limited number of trusted users. Follow the password policy recommendations where applicable.

Passwords and User IDs for Networked PCs

PCs that run EcoStruxure Power Commission software, or that access the MicroLogic X control unit using any other means (for example, IFE or EIFE webpages, or SCADA), must prompt users for a login and password. You must ensure that users define strong passwords and change them periodically. In addition, you must set a timer to lock the PC screen automatically after a period of idle time.

A strong password includes uppercase and lowercase letters, numbers, and special characters, where these are available. It should have a minimum length of 10 characters.

Follow the password policy recommendations where applicable.

Passwords for IFE Interface Webpages and EIFE Interface Webpages, and IFE and EIFE FTP Server

Access to the IFE interface webpages, EIFE interface webpages, and IFE and EIFE FTP server is checked by Role-Based Access Control (RBAC) mechanism.

With RBAC, users are assigned a role that defines the assets they can access.

The security administrator of your system lists the system users and assigns a role to each of them.

The security administrator can manage the users of the IFE or EIFE interface:

- On the IFE or EIFE interface webpages
- With the EcoStruxure Cybersecurity Admin Expert (CAE) software

The security administrator can use CAE software to define the security policy of the system.

The security policy applies to all elements of the system that are compatible with CAE software. For low voltage systems, it applies to the IFE and EIFE interfaces in the system.

The security administrator can set the following parameters of the security policy with CAE software:

- Minimum inactivity period. After the duration without any action from the user, IFE or EIFE interface webpages are locked. The user must re-enter their password to unlock it.
- Maximum number of login attempts
- Locking period duration

For more information, refer to *NRJUSG18807EN EcoStruxure Cybersecurity Admin Expert User Guide*.

Passwords for IFE Server Webpages

Each user of the IFE server webpages has a personal user ID and password to log in to the webpages. A user must change the password after logging in to the webpages for the first time.

You must define which users in your organization require a login on the IFE server webpages, and follow the password policy recommendations where applicable.

Training

Overview

Employee awareness and training is an extremely important foundational part of any cybersecurity strategy. You must ensure that all users who are granted access to the control network for your installation are aware of the corporate security information policy. You must also ensure that they have received adequate training in performing their tasks in compliance with that policy.

In particular, users must be aware, and regularly reminded of best practices concerning:

- Not sharing sensitive information such as passwords or access codes for equipment or for locked rooms
- Keeping PCs safely locked away when not in use
- Ensuring smartphones that can be used to access the system are kept with them at all times and are protected against hacking over Bluetooth or over the Internet
- Not circumventing any security polices for reasons of convenience

For further information on designing and implementing a good training policy, refer to *How Can I Reduce Vulnerability to Cyber Attacks?*.

Chapter 3
Cybersecurity Recommendations for Local Access

Chapter Overview

This chapter lists the local access paths to the MasterPact MTZ circuit breaker. It also provides recommendations for securing these access paths. These are important considerations for operation.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Restricting Local Access to the MasterPact MTZ Circuit Breaker	20
Recommendations for Protecting Local Access to the MicroLogic X HMI	21
Recommendations for Protecting Access Through NFC	22
Recommendations for Protecting Access Through Bluetooth	23
Recommendations for Protecting Access to the MicroLogic X Control Unit Through Mini USB Port	25

Restricting Local Access to the MasterPact MTZ Circuit Breaker

Overview

The MasterPact MTZ intelligent modular unit (IMU) offers both local and remote access possibilities. You must ensure that only authorized users are granted access.

Local Access to MasterPact MTZ Circuit Breaker

Local access to the MasterPact MTZ intelligent modular unit provides various possibilities for accessing information about the system and controlling it.

Therefore, it is important to restrict local access to the MasterPact MTZ circuit breaker by installing it in a locked area to avoid:

- Unauthorized access to the MicroLogic X HMI with the risk of changes to settings from the HMI
- Unauthorized access to wireless Bluetooth communication with the risk of changes to settings from EcoStruxure Power Device app
- Unauthorized access to wireless NFC communication with the risk of data disclosure
- Unauthorized connection through the mini USB port on the MicroLogic X control unit with the risk of changes to settings from EcoStruxure Power Commission software or smartphone with EcoStruxure Power Device app
- Unauthorized access to the IO module with the risk of changes to the switch setting for the predefined application in use

It is also important to implement rules for managing access to the locked area. In particular, you must ensure that:

- The area is kept locked at all times.
- The area is equipped with an authentication and authorization system.
- Only authorized personnel have a key or access code.
- The communication network cables entering the room and the connection ports on communicating devices outside the room are protected.
- All devices such as PCs, smartphones, and tablets that access the MicroLogic X control unit are hardened following the latest vendor guidelines.

When the MasterPact MTZ circuit breaker is installed in a locked area, you must implement an emergency opening process. For example:

- Equip that area with at least one emergency stop button accessible from outside
- Equip the circuit breaker with an MN undervoltage release (failsafe system)

Recommendations for Protecting Local Access to the MicroLogic X HMI

Functions Accessible from HMI

Any person having access the enclosure where the MasterPact MTZ circuit breaker is located has access to the HMI on the MicroLogic X control unit.

Some critical functions such as the protection settings for the equipment can be configured from the MicroLogic X HMI.

Recommendations for Protecting Access Through the MicroLogic X HMI

The MicroLogic X HMI is neither password protected nor capable of being physically locked to prevent access to the display screen. Therefore, to protect access to the HMI, you must:

- Install the MasterPact MTZ circuit breaker in a locked area.
- Keep that area locked at all times.
- Give the key or access code to authorized personnel only.

For further information on protecting access to the MasterPact MTZ circuit breaker, refer to Implementing a Restricted Access Policy *(see page 20)*.

Locking Protection Settings

You can lock the protection settings of the MasterPact MTZ circuit breaker to prevent them from being changed locally on the HMI. By default, changing the protection settings from the HMI is allowed.

It is recommended to disable local modification of protection settings on the HMI if you do not use this function. For more information, refer to *DOCA0102EN MasterPact MTZ - MicroLogic X Control Unit - User Guide*.

Recommendations for Protecting Access Through NFC

Functions Accessible Through NFC

Through wireless near field communication (NFC), diagnostic data can be downloaded from the MicroLogic X control unit to a smartphone, even when the control unit is not powered. It is not possible to change any settings on the control unit, nor to open, close, or reset the MasterPact MTZ circuit breaker.

Prerequisites for Establishing an NFC Connection

To establish a wireless NFC connection with the MicroLogic X control unit, the prerequisites are:

- You must have physical access to the room where the MasterPact MTZ circuit breaker is located, and to the equipment enclosure.
- You must have EcoStruxure Power Device app installed on your smartphone,
- The smartphone must support NFC.

Any person who meets these conditions can download data that may be confidential for your operation. In the MicroLogic X control unit, there is no record of connections established through NFC.

For the detailed procedure on how to establish an NFC connection, refer to *DOCA0102EN MasterPact MTZ - MicroLogic X Control Unit - User Guide*.

General Recommendations for Protecting Access Through NFC

To protect access to data accessible through wireless NFC, it is recommended to:

- Install the MasterPact MTZ circuit breaker in a locked area so that only authorized person can access the MicroLogic X control unit.
- Keep that area locked at all times.
- Give the key or access code to authorized personnel only.

For further information, see the recommendations for restricting local access to the MasterPact MTZ circuit breaker *(see page 20)*.

Recommendations for NFC Communication

To protect access to functions accessible through wireless NFC, it is recommended to:

- Disconnect the smartphone from the Internet (for example, by setting it to flight mode) during an NFC connection with the MicroLogic X control unit.
- Do not enter a pairing code if prompted for it, because it is not required for an NFC connection.

Recommendations for Using EcoStruxure Power Device app

To restrict access to the MicroLogic X control unit from a smartphone running EcoStruxure Power Device app, it is recommended to use only the official Schneider Electric EcoStruxure Power Device app to connect to the MasterPact MTZ circuit breaker.

Recommendations for Using Smartphones

To restrict access to the MicroLogic X control unit from a smartphone, it is recommended to:

- Make sure that the smartphones that have the EcoStruxure Power Device app are password protected and used for work only.
- Harden the smartphones that have the EcoStruxure Power Device app by implementing all of the security features recommended by the smartphone vendor or manufacturer.
- Keep antivirus applications for smartphones up to date.
- Do not disclose information about the smartphone (telephone number, MAC address) if it is not necessary.
- Disconnect the smartphone from the Internet (for example, by setting it to flight mode) during an NFC connection with the MicroLogic X control unit.
- Do not store sensitive information on smartphones.

Recommendations for Protecting Access Through Bluetooth

Functions Accessible Through Bluetooth

NOTICE
RISK OF UNINTENDED OPERATION ● The device must only be configured and set by qualified personnel, using the results of the installation protection system study. ● During commissioning of the installation and following any modification, check that the MicroLogic X configuration and protection function settings are consistent with the results of this study. ● MicroLogic X protection functions are set by default to the minimum value, except for the long time protection function which is set to the maximum value, by default. **Failure to follow these instructions can result in equipment damage.**

Using wireless Bluetooth low energy (BLE) communications, you can access the MicroLogic X control unit from a smartphone running EcoStruxure Power Device app. This application offers a task-oriented interface with the control unit. Data transferred over Bluetooth is encrypted using AES 128-bit encryption.

Prerequisites for Establishing a Bluetooth Connection

To establish a wireless Bluetooth connection with the MicroLogic X control unit, the prerequisites are:
- The MicroLogic X control unit must be powered on.
- The Bluetooth function must be enabled on the MicroLogic X control unit.
- Only one smartphone at a time can connect to a control unit.
- You must have a smartphone with EcoStruxure Power Device app installed.
- The smartphone must support Bluetooth low energy (4.0 or above).
- You must have access to the MicroLogic X control unit to activate Bluetooth by pressing the activation pushbutton, and be physically within range (usually within 20 to 30 meters or yards) for the duration of the connection.

Any person who meets these conditions, and establishes a connection, has access to functions which can impact your installation.

For detailed procedures on how to establish a Bluetooth connection, refer to *DOCA0102EN MasterPact MTZ - MicroLogic X Control Unit - User Guide*.

General Recommendations for Protecting Access Through Bluetooth

To protect access to functions accessible through wireless Bluetooth, it is recommended to:
- Install the MasterPact MTZ circuit breaker in a locked area so that only authorized person can access the MicroLogic X control unit.
- Keep that area locked at all times.
- Give the key or access code to authorized personnel only.

For further information on protecting access to the MasterPact MTZ circuit breaker, refer to Implementing a Restricted Access Policy *(see page 20)*.

Recommendations for Using Bluetooth

The implementation of the Bluetooth function complies with the NIST Special Publication 800-121 Revision 1. Nevertheless, to protect access to functions accessible through wireless Bluetooth, it is recommended to:
- Disable the Bluetooth function on the MicroLogic X control unit, as explained in *MasterPact MTZ - MicroLogic X Control Unit - User Guide*, and enable it only when you are ready to establish a connection.
- Set the Bluetooth disconnection timer to 5 minutes.
- Except when you are starting a Bluetooth connection, Bluetooth must not be activated from the activation pushbutton on the front face of the MicroLogic X control unit. Bluetooth must remain off when not in use.
- Press the Bluetooth pushbutton to end the communication when you have finished.
- Pairing must be done as infrequently as possible, and in a secure area.
- Do not enter a pairing code if unexpectedly prompted for it.
- During Bluetooth pairing, keep the smartphone as close as possible to the MicroLogic X control unit.

Recommendations for Using EcoStruxure Power Device app

To restrict access to the MicroLogic X control unit from a smartphone running EcoStruxure Power Device app, it is recommended to use only the official Schneider Electric EcoStruxure Power Device app to connect to the MasterPact MTZ circuit breaker.

Recommendations for Using Smartphones

To restrict access to the MicroLogic X control unit from a smartphone, it is recommended to:

- Make sure that the smartphones that have the EcoStruxure Power Device app are password protected and used for work only.
- Harden the smartphones that have the EcoStruxure Power Device app by implementing all of the security features recommended by the smartphone vendor or manufacturer.
- Keep antivirus applications for smartphones up to date.
- Do not disclose information about the smartphone (telephone number, MAC address) if it is not necessary.
- Disconnect the smartphone from the Internet during a Bluetooth connection with the MicroLogic X control unit.
- Do not store sensitive information on smartphones.

Recommendations for Protecting Access to the MicroLogic X Control Unit Through Mini USB Port

Functions Accessible Through Mini USB Port

It is possible to access all the functions of the MicroLogic X control unit by:

- Connecting a PC running EcoStruxure Power Commission software to the mini USB port of the control unit.
- Connecting a smartphone running EcoStruxure Power Device app to the mini USB port of the control unit through a USB OTG adapter.

Note that the mass storage function is not implemented in the control unit. Therefore, it is not possible to attack the system by downloading malware from a USB key or other mass storage device.

Prerequisites for Establishing a USB or USB OTG Connection

To establish a USB connection with the MicroLogic X control unit, the prerequisites are:

- You must have physical access to the room where the MasterPact MTZ circuit breaker is located.
- For a connection from a PC:
  - You must have a USB cable with a mini USB connector to connect your PC to the mini USB port on the MicroLogic X control unit.
  - You must have a PC running EcoStruxure Power Commission software.
- For a connection from a smartphone:
  - You must have an OTG adapter and a USB cable with a mini USB connector to connect your smartphone to the mini USB port on the MicroLogic X control unit.
  - You must have a smartphone running EcoStruxure Power Device app.

General Recommendations for Protecting Access Through Mini USB Port

To protect access to functions accessible through the mini USB port on the MicroLogic X control unit, it is recommended to:

- Install the MasterPact MTZ circuit breaker in a locked area so that only authorized person can access the MicroLogic X control unit.
- Keep that area locked at all times.
- Give the key or access code to authorized personnel only.

For further information, see the recommendations for restricting local access to the MasterPact MTZ circuit breaker *(see page 20)*.

Recommendations for PCs Running EcoStruxure Power Commission Software

To protect access to the MicroLogic X control unit from PC connected locally to the mini USB port on the front of the control unit, it is recommended to:

- Keep PCs safely locked away when not in use.
- Make sure that PCs that run the EcoStruxure Power Commission software require a user login and password.
- Enforce the use of strong passwords *(see page 15)*.
- Make sure that user passwords are changed regularly.
- Forbid reuse of old passwords.
- Set a timer to lock the PC screen after a period of idle time.
- Harden PCs following the most recent vendor guidelines for the operating system running on your PC.
- Limit the number of users allowed to use EcoStruxure Power Commission software.
- Keep antivirus applications for PCs up to date.

Recommendations for Smartphones Running EcoStruxure Power Device app

To protect access to the MicroLogic X control unit from a smartphone connected locally to the mini USB port on the front of the control unit, it is recommended to:

- Make sure that the smartphones running EcoStruxure Power Device app are password protected and used for work only.
- Harden the smartphones running EcoStruxure Power Device app by implementing all of the security features recommended by the smartphone vendor or manufacturer.
- Keep antivirus applications for smartphones up to date.
- Do not disclose information about the smartphone (telephone number, MAC address) if it is not necessary.
- Disconnect the smartphone from the internet during a USB OTG connection with the MicroLogic X control unit.
- Do not store sensitive information on smartphones.

Chapter 4
Cybersecurity Recommendations for Remote Access

Chapter Overview

This chapter lists the remote access paths to the MasterPact MTZ circuit breaker. It also provides recommendations for securing these access paths. These are important considerations for operation.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Restricting Remote Access to the MasterPact MTZ Circuit Breaker	28
Separating OT Network from Corporate Network	29
Recommendations for Protecting Remote Access to the MicroLogic X Control Unit Through Ethernet	30
Recommendations for Protecting Remote Access to the MicroLogic X Control Unit Through Modbus-SL	31

Restricting Remote Access to the MasterPact MTZ Circuit Breaker

Overview

The MasterPact MTZ intelligent modular unit (IMU) offers both local and remote access possibilities. You must ensure that only authorized users are granted access.

Remote Access to MasterPact MTZ Circuit Breaker

Depending on your system architecture, there are probably several ways of gaining remote access to the MasterPact MTZ circuit breaker.

It is extremely important to control remote access to your system, as remote access through the following communication pathways can give full control over your installation:

- EcoStruxure Power Commission software through an Ethernet connection via an IFE, EIFE, or IFM interface
- EcoStruxure Power Commission software through Modbus-SL via an IFM interface
- IFE or EIFE webpages through an Ethernet connection via an IFE or EIFE interface

In particular, you must consider:

- How the system can be accessed using the various communication paths available *(see page 11)*
- The information and controls available through each access path *(see page 14)*

Enabling and Disabling Remote Control of the MasterPact MTZ Circuit Breaker

Remote control of the MasterPact MTZ circuit breaker refers to the following operations:

- Opening, closing and resetting the circuit breaker
- Modifying the circuit breaker settings

If remote control of the MasterPact MTZ circuit breaker is not a requirement, it is highly recommended to disable remote control using the IFE or EIFE interface, IFE server, or IFM interface. By default, remote control is enabled.

On the IFE interface or IFE server, use the locking pad on the front panel to enable or disable remote control commands sent over the Ethernet network.

On the EIFE interface, connect a PC running EcoStruxure Power Commission software to the mini USB port on the front of the MicroLogic X control unit to enable or disable remote control of the MasterPact MTZ circuit breaker through the Ethernet network.

On the IFM interface, use the locking pad on the front panel to enable or disable remote controls sent over the Modbus-SL network.

Locking Protection Settings

You can lock the protection settings of the MasterPact MTZ circuit breaker to prevent them from being changed remotely. By default, changing the protection settings remotely is allowed.

It is recommended to disable remote modification of protection settings if you do not use this function. For more information, refer to *DOCA0102EN MasterPact MTZ - MicroLogic X Control Unit - User Guide*.

Disable the Unused IP Network Services

The communication ports on the IFE or EIFE interface can be disabled from the IFE or EIFE interface webpages.

It is recommended to:

- Disable the unused communication ports of the IFE or EIFE interface.
- Access the IFE or EIFE interface webpages using HTTPS service instead of HTTP.

Separating OT Network from Corporate Network

Overview

In the design and implementation of your operational technology network, you must use segregation mechanisms to keep it separate from your corporate network. This helps restrict access to the MasterPact MTZ intelligent modular unit.

In particular, you must consider:

- Using firewalls
- Creating demilitarized zones
- Using intrusion detection system (IDS) and/or intrusion prevention system (IPS) solutions
- Implementing security policies and training programs
- Defining incident response procedures

Guidelines for designing an operational technology network, and keeping it separate from the corporate intranet are issued and updated by specialized organizations (for example, NIST) and standardization bodies (for example, ISO, IEC/IEEE). Refer to these publications to address the points listed above.

Recommendations for Protecting Remote Access to the MicroLogic X Control Unit Through Ethernet

Functions Accessible Through Ethernet

When a PC running monitoring and control software (SCADA, EcoStruxure Power Commission software) is connected to the Ethernet (Modbus/TCP) network, all the functions of the MicroLogic X control unit are accessible in the following cases:

- The MasterPact MTZ circuit breaker is connected to an IFE interface or an IFE server.
- The MasterPact MTZ circuit breaker includes the EIFE interface.
- The MasterPact MTZ circuit breaker is connected to an IFM interface stacked to an IFE server.

Prerequisites for Establishing an Ethernet Connection

To establish an Ethernet connection with the MicroLogic X control unit, the prerequisites are:

- The MicroLogic X control unit must be powered on
- The MicroLogic X control unit must be connected to an Ethernet network through one of the following:
  - An IFE or an EIFE interface
  - An IFE server
  - An IFM interface stacked to an IFE server
- You must have a PC or other device (for example, FDM128 display, or PLC) running monitoring and control software (SCADA, EcoStruxure Power Commission) connected to the Ethernet network, giving remote access
- You must have a PC running a web browser connected to the Ethernet network, giving access to the IFE or EIFE webpages
- You must have a user ID and password with the appropriate access permissions to log in to:
  - IFE and EIFE interface webpages
  - IFE server webpages
  - IFE and EIFE FTP server
- You must have a user ID and password with the appropriate access permissions to log in to EcoStruxure Power Commission software

Recommendations for PCs Connected to Ethernet

To protect access to the MicroLogic X control unit from a networked PC, it is recommended to:

- Keep PCs safely locked away when not in use.
- Make sure that the PC that provides access to the MicroLogic X control unit using Ethernet (for example, through IFE or EIFE interface webpages, IFE server webpages, or SCADA) requires a user login and password.
- Enforce the use of strong passwords *(see page 16)*.
- Use IP filtering capability of IFE and EIFE interfaces and IFE server to allow communication only with selected remote IP addresses.
- Make sure that user passwords are changed regularly.
- Forbid reuse of old passwords.
- Set a timer to lock the PC screen after a period of idle time.
- Harden the PC by following the most recent vendor guidelines for the operating system running on your PC.
- Limit the number of users allowed to access the MicroLogic X control unit from a networked PC.
- Keep antivirus applications for PCs up to date.

In addition to the above precautions, you must also follow the general guidelines and recommendations for protecting your installation given in *How Can I Reduce Vulnerability to Cyber Attacks?*.

Recommendations for Protecting Remote Access to the MicroLogic X Control Unit Through Modbus-SL

Functions Accessible Through Modbus-SL

When a PC running monitoring and control software (SCADA) is connected to the Modbus-SL network, all the functions of the MicroLogic X control unit are accessible when the MasterPact MTZ circuit breaker is connected to an IFM interface.

Prerequisites for Establishing a Modbus-SL Connection

To establish a Modbus-SL connection with the MicroLogic X control unit, the prerequisites are:

- The MicroLogic X control unit must be powered on.
- The MicroLogic X control unit must be connected to an IFM interface.
- You must have a PC or other device (for example, PLC) running monitoring and control software (SCADA) connected to the Modbus-SL network giving remote access.
- You must have a user ID and password with the appropriate access permissions to log in to EcoStruxure Power Commission software.

Recommendations for PCs Connected to Modbus-SL

To protect access to the MicroLogic X control unit from a networked PC, it is recommended to:

- Keep PCs safely locked away when not in use.
- Make sure that the PC that provides access to the MicroLogic X control unit using Modbus-SL (for example, through SCADA), requires a user login and password.
- Enforce the use of strong passwords *(see page 16)*.
- Make sure that user passwords are changed regularly.
- Forbid reuse of old passwords.
- Set a timer to lock the PC screen after a period of idle time.
- Harden the PC by following the most recent vendor guidelines for the operating system running on your PC.
- Limit the number of users allowed to access the MicroLogic X control unit from a networked PC.
- Keep antivirus applications for PCs up to date.

In addition to the above precautions, you must also follow the general guidelines and recommendations for protecting your installation given in *How Can I Reduce Vulnerability to Cyber Attacks?*.

Chapter 5
Cybersecurity Recommendations for Firmware Updates and Digital Modules

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Installing Firmware Updates	34
Purchasing and Installing Digital Modules	36
Schneider Electric Cybersecurity Support Portal	37

Installing Firmware Updates

Overview

An increasingly common cyber attack is the distribution of doctored or illegitimate software packages that may contain modified applications or additional applications. These applications can compromise the integrity of the original software and its intended use.

To help ensure the integrity and authenticity of all components of the MasterPact MTZ IMU, namely the MicroLogic X control unit, IFE server, IFE or EIFE interface, IFM interface, and the IO module, all Schneider Electric original firmware is digitally signed.

Update all firmware using EcoStruxure Power Commission software. You must have the latest version of EcoStruxure Power Commission software. Use EcoStruxure Power Commission software to update all firmware through the firmware menu.

Cybersecurity Recommendations Concerning Firmware Updates

⚠ WARNING

RISK OF UNINTENDED OPERATION

- Update your version of EcoStruxure Power Commission software as soon as you receive a notification that an update is available.
- Use this latest version of EcoStruxure Power Commission software to update the firmware of all your products.
- At regular intervals, review the certificate revocation list published on the Schneider Electric official website. If there is a revoked certificate for one of your products, do not install firmware dated prior to the date of the revocation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

When installing firmware updates for components of the MasterPact MTZ IMU, it is recommended to:

- Only use the latest version of the EcoStruxure Power Commission software to download and install firmware updates.
- Harden the PC that runs EcoStruxure Power Commission software by following the most recent vendor guidelines for the operating system.
- Install updates following accepted operational technology (OT) practices such as testing on a non-production environment (if available) for validation before installing and deploying them in your production system.

Refer to the relevant release note *(see page 7)* to check if the latest update provides cybersecurity improvements. If so, updating to this version is recommended.

Signed Firmware

All firmware designed for the MasterPact MTZ IMU is signed using the Schneider Electric public key infrastructure (PKI). The digital signatures are authenticated using the public certificate that is present in EcoStruxure Power Commission software.

When firmware is uploaded to the MasterPact MTZ IMU through EcoStruxure Power Commission software, the MicroLogic X control unit also automatically verifies the digital signature of the update package. This verification is done using the public certificate present in the control unit.

For security reasons, public certificates are subject to change. Therefore, you must check that the version of EcoStruxure Power Commission software that you use to download and install firmware updates is the latest version. Having the latest version of EcoStruxure Power Commission software means that the public certificates used to sign firmware are up to date.

Certificates that are no longer valid are published on a certificate revocation list (CRL), available on the *Schneider Electric* official website.

Benefits of Using EcoStruxure Power Commission Software for Firmware Updates

EcoStruxure Power Commission software plays an important part in helping ensure the integrity of your operational technology network during firmware updates. Use only the latest version of EcoStruxure Power Commission software to download and install firmware because it is the only software that can provide the following benefits:

- When you download firmware packages from the official Schneider Electric download center using EcoStruxure Power Commission software, the digital signature of the packages is automatically verified.
- When you upload firmware to the MicroLogic X control unit (using EcoStruxure Power Commission software over a USB connection or through an Ethernet connection), the digital signature of the update package is automatically verified.

The automatic verifications done by EcoStruxure Power Commission software rely entirely on the validity of the public certificate that it uses.

Refer to *DOCA0144EN MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note* for detailed procedures explaining how to update the MicroLogic X firmware.

Purchasing and Installing Digital Modules

Overview

Digital Modules are optional modules that expand the features available across the range of MicroLogic X control units. They can be purchased along with the MasterPact MTZ circuit breaker in the initial order or at a later date from the Schneider Electric online GoDigital marketplace.

All Digital Modules designed for the MicroLogic X control unit are digitally signed for added security using the Schneider Electric public key infrastructure (PKI). The PKI helps to ensure both the authenticity and integrity of these downloads. The Digital Modules must be installed using EcoStruxure Power Commission software.

Cybersecurity Recommendations for Purchasing Digital Modules

To purchase Digital Modules for the MicroLogic X control unit, use only the official Schneider Electric download center GoDigital marketplace.

When installing Digital Modules for components of the MasterPact MTZ IMU, it is recommended to:

- Install Digital Modules following accepted operational technology (OT) practices such as testing on a non-production environment for validation before installing and deploying them in your production system.
- Only use the latest version of EcoStruxure Power Commission software to download and install Digital Modules.
- Harden the PCs used to download Digital Modules and to install them following the most recent vendor guidelines for the operating system.

Cybersecurity Recommendations for Installing Digital Modules

⚠ WARNING

RISK OF UNINTENDED OPERATION

- Update your version of EcoStruxure Power Commission software as soon as you receive a notification that an update is available.
- Use this latest version of EcoStruxure Power Commission software to update the firmware of all your products.
- At regular intervals, review the certificate revocation list published on the Schneider Electric official website. If there is a revoked certificate for one of your products, do not install firmware dated prior to the date of the revocation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

You must use only EcoStruxure Power Commission software to install Digital Modules for the MicroLogic X control unit.

EcoStruxure Power Commission software plays an important part in helping ensure the integrity of your operational technology network. Use only the latest version of EcoStruxure Power Commission software to install Digital Modules because it is the only software that can provide the following benefits:

- When you update the firmware of a device of the IMU using EcoStruxure Power Commission software over a USB connection or Ethernet connection, the digital signature of the firmware update is automatically verified.
- When you upload a Digital Module to the MicroLogic X control unit using EcoStruxure Power Commission software over a USB connection, the digital signature of the Digital Module is automatically verified.

The automatic verifications done by EcoStruxure Power Commission software rely entirely on the validity of the public certificate used.

Refer to *DOCA0144EN MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note* for detailed procedures explaining how to download and install Digital Modules.

Schneider Electric Cybersecurity Support Portal

Overview

The Schneider Electric *cybersecurity support portal* outlines the Schneider Electric vulnerability management policy.

The aim of the Schneider Electric vulnerability management policy is to address vulnerabilities in cybersecurity affecting Schneider Electric products and systems, in order to protect installed solutions, customers, and the environment.

Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to adequately protect their installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and issuing alerts on vulnerabilities and mitigations affecting products and solutions.

The CPCERT coordinates communications between relevant CERTs, independent researchers, product managers, and all affected customers.

Information Available on the Schneider Electric Cybersecurity Support Portal

The support portal provides the following:

- Information about cybersecurity vulnerabilities of products.
- Information about cybersecurity incidents.
- An interface that enables users to declare cybersecurity incidents or vulnerabilities

Glossary

B

BLE - Bluetooth low energy
A wireless personal area network technology providing reduced power consumption.

E

EIFE interface
Embedded Ethernet interface that is an optional module of the MasterPact MTZ drawout circuit breaker. With this module, the circuit breaker is accessible over an Ethernet network. Access to the EIFE interface webpages and EIFE FTP server is authorized depending on the Role-Based Access Control (RBAC) mechanism.

F

FTP - File Transfer Protocol
A network protocol that provides the ability to transfer files over the Internet from one computer to another.

G

GoDigital
The Schneider Electric online marketplace for purchasing Digital Modules designed for the MicroLogic X control unit.

H

HMI - Human-machine interface
Refers to the display screens on the front face of a device that an operator can use to read information or configure the device.

HTTP - Hypertext Transfer Protocol
A network protocol that handles delivery of files and data on the World Wide Web.

HTTPS - Hypertext Transfer Protocol Secure
A variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol connection.

I

IEC 61850 Protocol
A standard for communication networks and systems in substations. Based on Ethernet protocol, it is a standardized method of communication developed to support integrated systems, composed of multi-vendor, self-describing Intelligent Electronic Devices (IEDs). These systems are networked together to perform real-time protection, control, measurement, and monitoring functions.

IFE interface
IFE Ethernet interface for one circuit breaker that can be connected to the MasterPact MTZ circuit breaker. With this module, the circuit breaker is accessible over an Ethernet network. Access to the IFE interface webpages and IFE FTP server is authorized depending on the Role-Based Access Control (RBAC) mechanism.

IFE server
IFE Ethernet switchboard server that can be connected to more than one MasterPact MTZ circuit breaker. With this module, the circuit breakers are accessible over an Ethernet network.

IFM interface
IFM Modbus-SL interface enables an IMU to be connected to a two-wire RS 485 serial line Modbus network. Each IMU has its own IFM interface and a corresponding Modbus address.

IMU - Intelligent modular unit

In the case of the MasterPact MTZ circuit breaker, IMU refers to the circuit breaker itself, the MicroLogic X control unit, and the associated ULP modules, IFE, EIFE, IFM interface, and IO module.

IP - Internet protocol

IP addresses are used to identify devices connected to the company intranet or to the Internet.

IT - Information technology

Refers to the company information systems and information network as opposed to its OT (operational technology) network.

L

LAN - Local area network

Refers to the company intranet, or IT network.

M

Modbus TCP/IP

A protocol, which provides master/slave communication between devices and TCP/IP that provides communications over an Ethernet connection.

N

NFC - Near field communication

Refers to a wireless communication protocol.

O

OT - Operational technology

Refers to the hardware and software systems the company uses to directly monitor and control the production processes and equipment, also called the industrial control (IC) network. OT is often used to refer to the company operational network as opposed to its IT network.

P

Pairing code

Code consisting of numbers that is used to verify the identity of the individual when establishing a Bluetooth connection.

PKI - Public key infrastructure

Defines a set of services used to generate and authenticate digital signatures. A public key infrastructure is designed to guarantee confidentiality, integrity, and authenticity of information.

R

RBAC - Role-based access control

A way to assign different levels of access based on what the user’s defined role has been granted to have access to.

S

SCADA - Supervisory control and data acquisition

Refers to systems designed to get real-time data on production processes and equipment for monitoring and controlling them remotely.

Security policy

A system security policy is the security settings that are applied throughout the entire secured system. A security policy generally refers to the use of standards. It is used to define any security-related configuration shared between all devices.

T

TCP/IP - Transmission control protocol/Internet protocol

Refers to the suite of protocols used for communications over the Internet.

U

ULP connectivity

ULP is a fast communication link dedicated to circuit breaker monitoring and control. It connects the circuit breaker to an Ethernet interface or to an IO module. ULP operates at a speed of 1 Mb/s and is plug and play.

V

VPN - Virtual private network

A VPN is used to establish a secured / private "tunnel" between an authenticated external access point and the trusted enterprise network.

DOCA0122EN-03

Schneider Electric Industries SAS
35, rue Joseph Monier
CS30323
F - 92506 Rueil Malmaison Cedex

www.schneider-electric.com

06/2020