Masterpact MTZ

Cybersecurity Guide

06/2017

DOCA0122EN-01

www.schneider-electric.com

Schneider Electric™

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

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 to help prevent unauthorized access to device settings 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 industrial control 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.

Related Documents

Title of documentation	Reference number
Micrologic X Control Unit - User Guide	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note

You can download these technical publications and other technical information from our website at *http://www.schneider-electric.com/en/download*.

Trademark Notice

All trademarks are owned by Schneider Electric Industries SAS or its affiliated companies.

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:

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 following 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 cybersecurity on a dedicated page on the *Schneider Electric* global website.

Why Cybersecurity Is Relevant for Masterpact MTZ Circuit Breakers

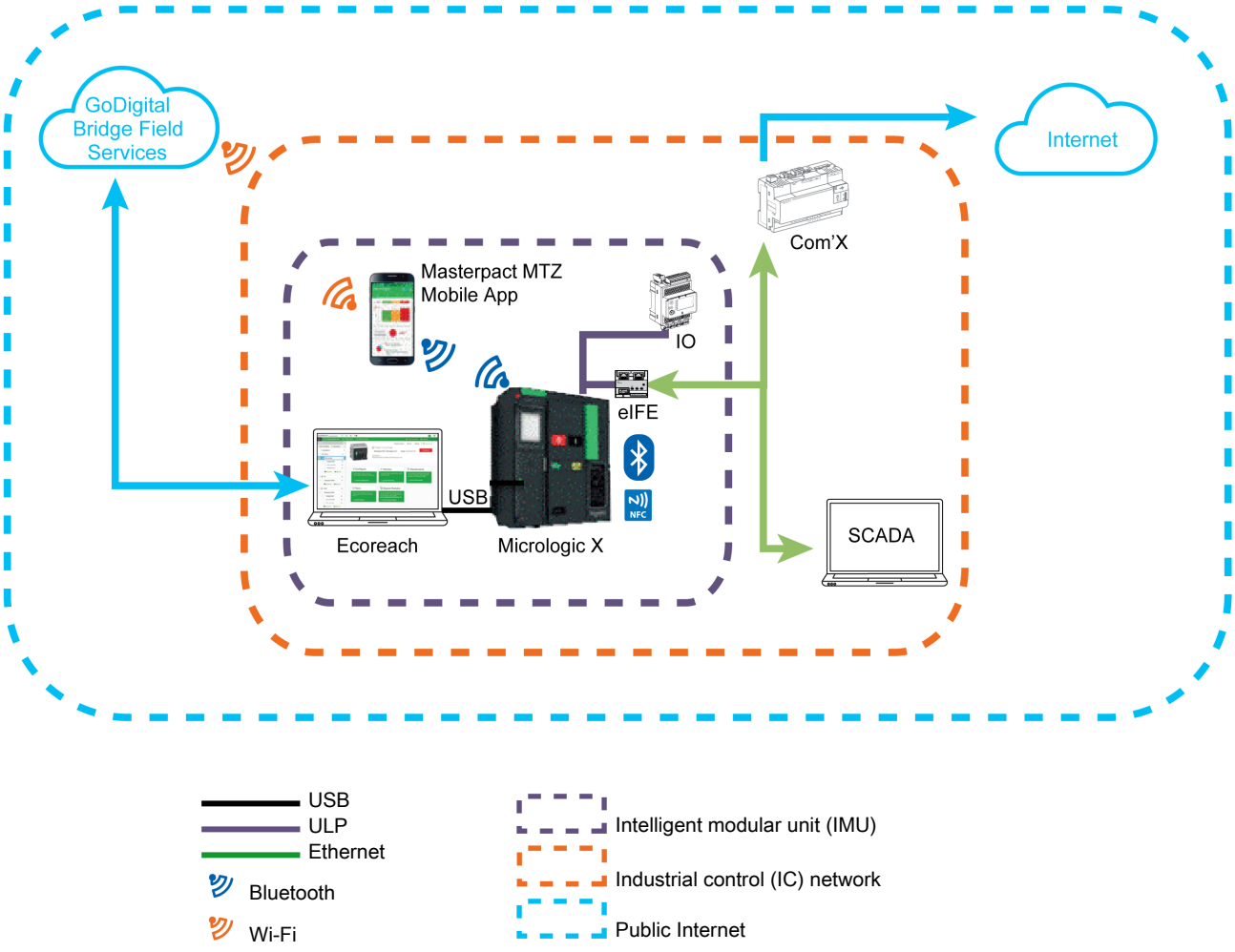
Overview

The Masterpact MTZ circuit breaker is a key component of any plant or equipment because it controls the power supply to the system, provides electrical protection, and delivers sensitive 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 system. However, they also make it potentially vulnerable 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 that interfaces with 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 module.

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 Ecoreach software
  - A smartphone running the Masterpact MTZ Mobile App
- Ethernet connection through the Industrial Control (IC) network when the communication interface is present
- Modbus-SL connection through the Industrial Control (IC) 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. 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 industrial control (IC) network that includes the Masterpact MTZ intelligent modular unit (IMU). The recommendations and guidelines in this chapter help to promote a secure operating environment.

What Is in This Chapter?

This chapter contains the following topics:

Identifying and Protecting Sensitive Information and Operations

Overview

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

As a general principle, sensitive information includes:

- Any information that can be used to access your installation and your industrial control network
- Information about operations accessible through the Masterpact MTZ IMU

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 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 certain tasks on the Micrologic X control unit, whatever the access mode (through Ethernet / Modbus-SL, USB connection, or Bluetooth)
- Logging into the PC that runs Ecoreach software
- Logging onto IFE and EIFE webpages

Password for Micrologic X Critical Settings and Controls

When accessing the Micrologic X control unit, any 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, each one corresponding to a level.

A level is assigned to a role:

- Levels 1, 2, and 3 are used for general-purpose roles, like an operator role.
- Level 4 is the administrator level. The administrator level is required to write the settings to the Micrologic X control units using Ecoreach software.

When connecting through the Masterpact MTZ Mobile App or Ecoreach 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

These passwords must be changed periodically after the first installation of the Masterpact MTZ circuit breaker, using Ecoreach software. They must only be shared with a limited number of trusted users. Follow the password policy recommendations below where applicable.

Passwords and User IDs for Networked PCs

PCs that run Ecoreach 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.

See the recommendations below concerning the password policy.

Passwords for IFE and EIFE Webpages

Users of the IFE and EIFE webpages have a personal user ID and password to log into the webpages. They must change their password after logging into the IFE and EIFE webpages for the first time.

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

Cybersecurity Recommendations Concerning Password Policy

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
- Forbidding reuse of old passwords
- Regularly reminding users about best practices concerning passwords

To protect your PC and all software that runs on it, at a minimum you should:

- Enforce the use of strong passwords
- Set the minimum password length to 10 characters
- Set the minimum validity period to three days and the maximum to 180 days
- Keep the history of the eight latest passwords and forbid reusing them

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

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 confidential or 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 cannot be hacked 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:

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 Masterpact MTZ Mobile 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 Ecoreach software or smartphone with Masterpact MTZ Mobile 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. Refer to the *Micrologic X Control Unit - User Guide* for instructions.

Recommendations for Protecting Access Through NFC

Functions Accessible Through NFC

Through wireless near field communication (NFC), 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.
- You must have Masterpact MTZ Mobile 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 the *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 no unauthorized 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.
- Disable Bluetooth communication on the smartphone.
- Do not enter a pairing code if prompted for it, because it is not required for an NFC connection.

Recommendations for Using Masterpact MTZ Mobile App

To restrict access to the Micrologic X control unit from a smartphone running Masterpact MTZ Mobile App, it is recommended to use only the official Schneider Electric Masterpact MTZ Mobile 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 Masterpact MTZ Mobile App are password protected and used for work only.
- Harden the smartphones that have the Masterpact MTZ Mobile 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 confidential or 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 Masterpact MTZ Mobile 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 Masterpact MTZ Mobile 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 the Bluetooth 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 the *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 no unauthorized 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

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 *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 so that intruders cannot see the pairing code entered.
- 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 Masterpact MTZ Mobile App

To restrict access to the Micrologic X control unit from a smartphone running Masterpact MTZ Mobile App, it is recommended to use only the official Schneider Electric Masterpact MTZ Mobile 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 Masterpact MTZ Mobile App are password protected and used for work only.
- Harden the smartphones that have the Masterpact MTZ Mobile 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 confidential or 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 Ecoreach software to the mini USB port of the control unit.
- Connecting a smartphone running Masterpact MTZ Mobile 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 Ecoreach 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 Masterpact MTZ Mobile 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 no unauthorized 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 Ecoreach 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 Ecoreach software require 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 PCs following the most recent vendor guidelines for the operating system running on your PC.
- Limit the number of users allowed to use Ecoreach software.
- Keep antivirus applications for PCs up to date.

Recommendations for Smartphones Running Masterpact MTZ Mobile 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 Masterpact MTZ Mobile App are password protected and used for work only.
- Harden the smartphones running Masterpact MTZ Mobile 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 confidential or 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:

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. In particular, remote access through Ethernet or Modbus-SL can give full control over your installation. Therefore, it is extremely important to control remote access to your system.

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, EIFE or IFM interface. By default, remote control is enabled.

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

On the EIFE interface, connect a PC running Ecoreach 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. Refer to the *Micrologic X Control Unit - User Guide* for instructions.

Separating IC Network from Corporate Network

Overview

In the design and implementation of your industrial control 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) devices
- Implementing security policies and training programs
- Defining incident response mechanisms

Guidelines for designing an industrial control 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 Ecoreach software is connected to the Ethernet 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.
- 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 interface.
  - An EIFE interface.
  - An IFM interface stacked to an IFE server.
- You must have a PC or other device (for example, FDM128, or PLC) running monitoring and control software (SCADA, Ecoreach) connected to the Ethernet network giving remote access.
- You must have a user ID and password with the appropriate access permissions to log in to Ecoreach 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 web pages, or SCADA) requires 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 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 Ecoreach software 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, Ecoreach) 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 Ecoreach 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 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 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 Upgrades and Digital Modules

What Is in This Chapter?

This chapter contains the following topics:

Installing Firmware Upgrades

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 authencity of all components of the Masterpact MTZ IMU, namely the Micrologic X control unit, the IFE, EIFE, or IFM interface, and the IO module, all Schneider Electric original firmware upgrades are digitally signed.

Upgrade all firmware using Ecoreach software. You must have the latest version of Ecoreach software. Use Ecoreach software to upgrade all firmware through the firmware menu. Ecoreach documentation can be downloaded from the Schneider Electric download site (*https://www.schneider-electric.com/en/download/*).

Cybersecurity Recommendations Concerning Firmware Upgrades

It is essential to install the latest firmware.

When installing firmware upgrades for components of the Masterpact MTZ IMU, it is recommended to:

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

Signed Firmware

All firmware designed for the Masterpact MTZ IMU is signed using the Schneider Electric public key infrastructure. The digital signatures are authenticated using the public certificate that is present in Ecoreach software.

When firmware is uploaded to the Masterpact MTZ IMU through Ecoreach software, the Micrologic X control unit also automatically verifies the digital signature of the upgrade package. This verification is done using the public certificate present in the control unit.

For security reasons, public certificates are subject to change. Therefore, it is a major security requirement (and it is your responsibility) to check that the version of Ecoreach software that you use to download and install firmware upgrades is the latest version. Having the latest version of Ecoreach 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). This list is available on the Schneider Electric official website.

Benefits of Using Ecoreach Software for Firmware Upgrades

Ecoreach software plays an important part in helping ensure the integrity of your industrial control network during firmware upgrades. Use only the latest version of Ecoreach 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 Ecoreach software, the digital signature of the packages is automatically verified.
- When you upload firmware to the Micrologic X control unit (using Ecoreach software over a USB connection), the digital signature of the upgrade package is automatically verified.

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

Refer to Ecoreach online help for detailed procedures explaining how to download and install firmware upgrades.

⚠ WARNING

RISK OF UNINTENDED OPERATION

- Update your version of Ecoreach software as soon as you receive a notification that an update is available.
- Use this latest version of Ecoreach software to upgrade 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.

Checking the Certificate Revocation List

At regular intervals, and at a minimum of every three months, you must look up the certificate revocation list (CRL) published by Schneider Electric to make sure that it does not list any certificates used by your equipment.

Do as follows to check the CRL:

Step	Action
1	Display the CRL published on the Schneider Electric website *(see page 38)*.
2	If the list is empty, it means that your current certificates are valid; no further action is required. If the list is not empty, continue to Step 3.
3	Check that you are using the latest version of Ecoreach software. If it is not the case, update your Ecoreach software.
4	Upgrade your 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 Ecoreach 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 system for validation before installing and deploying them in your production environment.
- Only use the latest version of Ecoreach 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

You must use only Ecoreach software to install Digital Modules for the Micrologic X control unit.

Ecoreach software plays an important part in helping ensure the integrity of your industrial control network. Use only the latest version of Ecoreach software to install Digital Modules because it is the only software that can provide the following benefits:

- When you upgrade the firmware of a device of the IMU using Ecoreach software over a USB connection, the digital signature of the firmware upgrade is automatically verified.
- When you upload a Digital Module to the Micrologic X control unit using Ecoreach software over a USB connection, the digital signature of the Digital Module is automatically verified.

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

Refer to Ecoreach online help for detailed procedures explaining how to download and install Digital Modules.

⚠ WARNING

RISK OF UNINTENDED OPERATION

- Update your version of Ecoreach software as soon as you receive a notification that an update is available.
- Use this latest version of Ecoreach software to upgrade 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.

Checking the Certificate Revocation List

At regular intervals, and at a minimum of every three months, you must look up the certificate revocation list (CRL) published by Schneider Electric to make sure that it does not list any certificates used by your equipment.

Do as follows to check the CRL:

Step	Action
1	Display the CRL published on the Schneider Electric website *(see page 38)*.
2	If the list is empty, it means that your current certificates are valid; no further action is required. If the list is not empty, continue to Step 3.
3	Check that you are using the latest version of Ecoreach software. If it is not the case, update your Ecoreach software.
4	Upgrade your digital module.

Schneider Electric Cybersecurity Portal

Overview

The Schneider Electric cybersecurity 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.

The Schneider Electric cybersecurity portal can be accessed at *http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp*.

Information Available on the Schneider Electric Cybersecurity Portal

The 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
- Access to resources that provide information about securing your system environment.
  These environments include:
  - Industrial processes.
  - Building management and access control systems.
  - Data centers.
  - Electrical infrastructure control systems.
- Certificates and certificate revocation lists through the tab **Firmware PKI**.

Certificate Revocation Lists (CRL) Available on the Schneider Electric Cybersecurity Portal

The following table provides the list of CRLs:

Product	CRL
MTZ control unit	LV breaker Micrologic master
IO module	LV breaker Micrologic master
IFE	Adv communication master
EIFE	Adv communication master
IFM	LV breaker Micrologic master

Glossary

B

BLE

Bluetooth low energy.

E

EIFE

Embedded Ethernet interface that is an optional module of the Masterpact MTZ drawout circuit breaker. With this module, the circuit breaker is accessible through the company intranet.

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.

I

IC

Industrial control. Refers to the hardware and software systems used to monitor and control a company production processes and equipment.

IFE

Ethernet interface that can be connected to the Masterpact MTZ circuit breaker. With this module, the circuit breaker is accessible through the company intranet.

IFM

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 industrial control (IC) network, or OT (operational technology) network.

L

LAN

Local area network. Refers to the company intranet, or IT network.

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

PIN

Personal identification number.

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

RAS

Remote access server.

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.

T

TCP/IP

Transmission control protocol/Internet protocol. Refers to the suite of protocols used for communications over the Internet.

V

VPN

Virtual private network. You use a VPN to establish a secured / private "tunnel" between an authenticated external access point and the trusted enterprise network.

DOCA0122EN-01

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

http://www.schneider-electric.com

06/2017