# Masterpact MTZ

## 网络安全指南

06/2017

DOCA0122ZH-01

www.schneider-electric.com

本文档中提供的信息包含有关此处所涉及产品之性能的一般说明和/或技术特性。本文档并非用于 (也不代替) 确定这些产品对于特定用户应用场合的适用性或可靠性。任何此类用户或设备集成商都有责任就相关特定应用场合或使用方面对产品执行适当且完整的风险分析、评估和测试。Schneider Electric 或其任何附属机构或子公司对于误用此处包含的信息而产生的后果概不负责。如果您有关于改进或更正此出版物的任何建议、或者从中发现错误、请通知我们。

本手册可用于法律所界定的个人以及非商业用途。 在未获得施耐德电气书面授权的情况下，不得翻印传播本手册全部或部分相关内容、亦不可建立任何有关本手册或其内容的超文本链接。施耐德电气不对个人和非商业机构进行非独占许可以外的授权或许可。 请遵照本手册或其内容原义并自负风险。与此有关的所有其他权利均由施耐德电气保留。

在安装和使用本产品时，必须遵守国家、地区和当地的所有相关的安全法规。出于安全方面的考虑和为了帮助确保符合归档的系统数据，只允许制造商对各个组件进行维修。

当设备用于具有技术安全要求的应用场合时，必须遵守有关的使用说明。

未能使用施耐德电气软件或认可的软件配合我们的硬件，则可能导致人身伤害、设备损坏或不正确的运行结果。

不遵守此信息可能导致人身伤害或设备损坏。

# 目录

# 安全信息

## 重要信息

### 声明

在尝试安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。下述特别信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。

在“危险”或“警告”标签上添加此符号表示存在触电危险，如果不遵守使用说明，会导致人身伤害。

这是提醒注意安全的符号。提醒用户可能存在人身伤害的危险。请遵守所有带此符号的安全注意事项，以避免可能的人身伤害甚至死亡。

**⚠ 危险**

危险表示若不加以避免，将会导致严重人身伤害甚至死亡的危险情况。

**⚠ 警告**

警告表示若不加以避免，可能会导致严重人身伤害甚至死亡的危险情况。

**⚠ 小心**

小心表示若不加以避免，可能会导致轻微或中度人身伤害的危险情况。

**注意**

注意用于表示与人身伤害无关的危害。

### 请注意

电气设备的安装、操作、维修和维护工作仅限于合格人员执行。Schneider Electric 不承担由于使用本资料所引起的任何后果。

专业人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

### 网络安全注意事项

**⚠ 警告**

**系统可用性、完整性和保密性的潜在危害**

- 更改默认密码将有助于防止擅自访问设备设置和信息。
- 禁用未使用的端口/服务和默认账户将有助于尽量减少恶意攻击的途径。
- 将联网设备布置在多层网络防御（例如防火墙、网络分段、网络入侵检测和保护）之后。
- 采用网络安全最佳实践（例如，最低权限、责任分离）来帮助阻止非法曝露、丢失、数据和日志修改、或服务中断。

**不遵循上述说明可能导致人员伤亡或设备损坏。**

# 关于本书

## 概览

### 文档范围

本指南中的信息涉及带 Micrologic™ X 控制单元的 Masterpact™ MTZ 断路器的网络安全，旨在帮助系统设计人员和操作人员为产品打造一个安全的运行环境。

本指南并不涉及较常见的主题，比如，如何保护您的工业控制网络或企业以太网网络。有关网络安全威胁及其应对方法的概述，请参阅 *我如何减少网络攻击漏洞？*。

**注意：** 在本指南中，术语**安全**是指网络安全。

### 有效性说明

本指南中的信息涉及带 Micrologic X 控制单元的 Masterpact MTZ 断路器。

### 相关文档

| 文档标题 | 参考号 |
| --- | --- |
| *Micrologic X 控制单元 - 用户指南* | DOCA0102EN<br>DOCA0102ES<br>DOCA0102FR<br>DOCA0102ZH |
| *我如何减少网络攻击漏洞？* | Cybersecurity System Technical Note |

您可以在我们的网站 *http://www.schneider-electric.com/en/download*下载这些技术出版物和其他技术信息。

### 商标声明

所有商标由 Schneider Electric Industries SAS 或其附属公司所有。

# 第1章
# 网络安全简介

## 综述

本章概述了 Schneider Electric 网络安全策略，以及带 Micrologic X 控制单元的 Masterpact MTZ 断路器为什么会涉及到网络安全。

## 本章包含了哪些内容？

本章包含了以下主题：

# 网络安全简介

## 简介

网络安全旨在保护您的通讯网络及其所连接的所有设备免受可能中断操作（可用性）、修改信息（完整性）或泄露机密信息（保密性）的攻击。网络安全的目的在于，提升信息和物理资产的保护级别，以免遭受盗窃、破坏、滥用或发生事故，同时保证其预期用户的访问和使用。网络安全包含许多方面，包括设计安全系统、利用物理和数字方法限制访问、识别用户、以及实施安全程序和最佳实践策略。

## Schneider Electric 指南

除了本指南中针对 Masterpact MTZ 断路器所给的具体建议之外，您还应遵循网络安全的 Schneider Electric 深度防御方法。以下的系统技术说明中介绍了这种方法：

- *我如何减少网络攻击漏洞？*

此外，*Schneider Electric* 全球网站的专门页面中也提供了许多有关网络安全的有用资源和最新信息。

# Masterpact MTZ 断路器为什么会涉及到网络安全

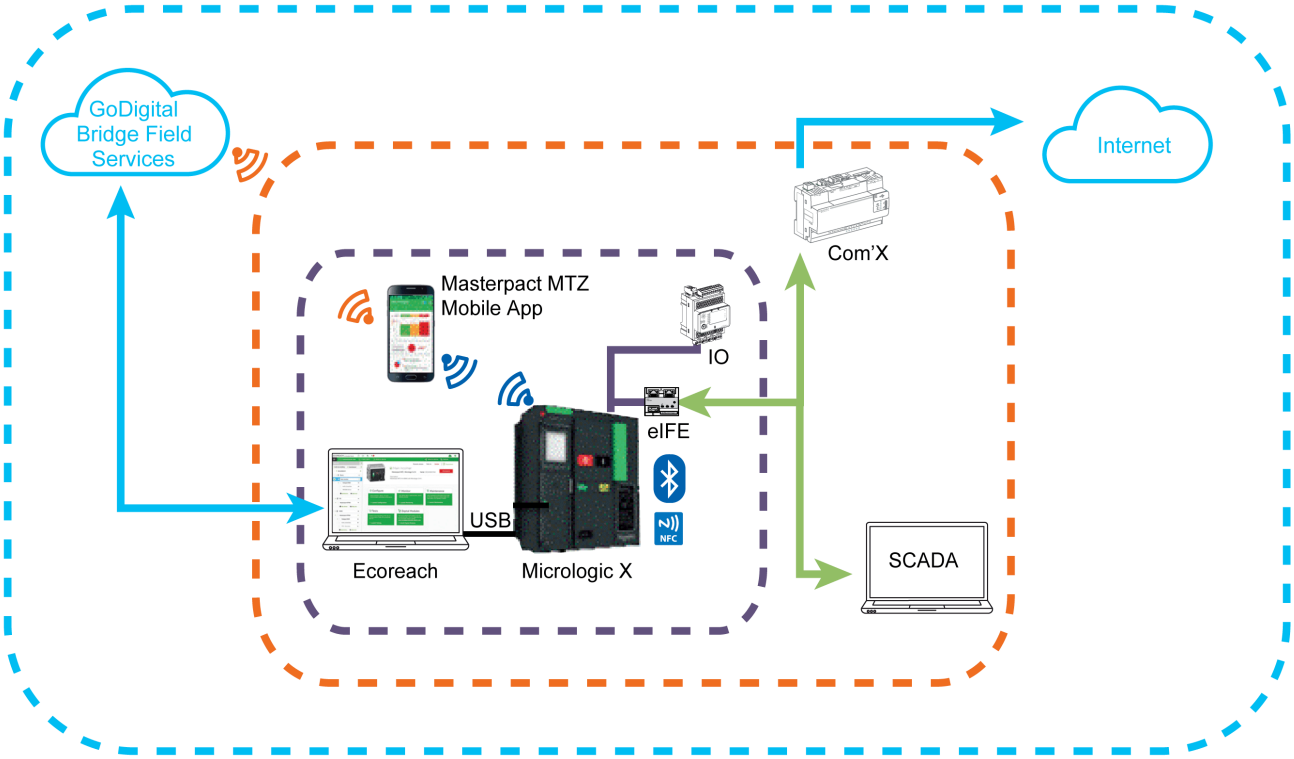
## 综述

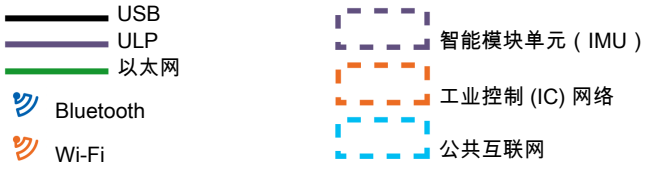
Masterpact MTZ 断路器是一切工厂或设备的关键部件，它负责控制系统供电、提供电气保护和传输敏感信息。

具有通讯功能的 Masterpact MTZ 断路器能够每天不间断访问实时控制功能并进行数据监视。这些功能提高了系统管理的效率和灵活性。但它们也易于受到潜在的网络攻击。

## Masterpact MTZ 断路器和运行环境

下图显示了与 Masterpact MTZ 断路器所连接的 Micrologic X 控制单元通讯的各种方式。




Masterpact MTZ 智能模块单元（IMU）包含断路器、Micrologic X 控制单元以及相关的 ULP 模块、通讯接口和 IO 模块。

如要通过 Micrologic X 控制单元与 Masterpact MTZ 断路器通讯，可使用以下通讯途径：

- Micrologic X 人机界面 (HMI)
- 通过智能手机的无线 NFC 连接
- 通过智能手机的无线 Bluetooth Low Energy (BLE) 连接
- 通过以下设备连接到 Micrologic X 控制单元的 Mini Type B USB 端口：
  - 运行 Ecoreach 软件的 PC
  - 运行 Masterpact MTZ Mobile App 的智能手机
- 在有通讯接口的情况下，通过工业控制 (IC) 网络实现的 Ethernet 连接
- 在有 IFM 接口的情况下，通过工业控制 (IC) 网络实现的 Modbus-SL 连接

## 遭受网络攻击的系统隐患

上述每种通讯途径都是系统中的潜在隐患。本指南旨在帮助保护这些通讯途径免受蓄意攻击或意外误用。

# 第2章
# 系统设计、规划和安装的网络安全建议

## 章节概述

本章提供了在设计、规划和安装包含 Masterpact MTZ 智能模块单元（IMU）的工业控制 (IC) 网络期间应考虑的重要信息。本章中的建议和指导有助于打造安全的运行环境。

## 本章包含了哪些内容？

本章包含了以下主题：

# 识别和保护敏感信息和操作

## 综述

规划和设计工业控制网络时，必须识别对操作有着重要影响的信息。一旦识别，就必须保护这些敏感信息。

一般来讲，敏感信息包括：

- 任何可用于访问您的系统和工业控制网络的信息
- 与操作有关且可通过 Masterpact MTZ IMU 访问的信息

您应负责判断如何在确保您组织的最佳利益的前提下分析和使用这些信息。

## 有关企业通讯网络的信息

可用于访问您的系统和工业控制网络的敏感信息包括：

- 系统架构
- 联网通讯设备的 IP 地址或 MAC 地址
- Ethernet 通讯端口数
- 用户 ID 和用户密码

以上并未穷尽所有，必须考虑您组织特有的并且可有助于访问关键系统的所有信息。

## 访问控制

网络安全的一个重要部分是设计有效的访问控制策略。访问控制包括识别组织内的用户组或个体员工，并确定他们有效开展工作所需的访问类型。

## 可通过每个访问途径访问的信息和操作汇总

根据用于访问 Masterpact MTZ 智能模块单元（IMU）的通讯接口或通讯途径，可用的信息和控制操作各有不同。下表总结了对信息和控制操作的访问：

| 信息和控制操作 | 本地访问 | | | | 远程访问 |
|---|---|---|---|---|---|
| | Micrologic X HMI | NFC | Bluetooth low energy | USB | Ethernet / Modbus-SL |
| 数据监视 | 读取 | 读取 | 读取 | 读取 | 读取 |
| 保护设置 | 读/写 | 读取 | 读/写 | 读/写 | 读/写 |
| 其他设置 | 读/写 | 读取 | 读/写 | 读/写 | 读/写 |
| 分闸/合闸/复位 | 否 | 否 | 是 | 是 | 是 |

有关每个通讯接口和通讯途径的保护说明，请参阅本地访问 (参见第 *17* 页)或远程访问 (参见第 *25* 页)的相关建议。

# 设计密码策略

## 综述

精心设计的密码策略是抵御网络攻击的第一道防线。

如果系统中包含带 Micrologic X 控制单元的 Masterpact MTZ 断路器，则在以下情形下需要使用密码：
- 对 Micrologic X 控制单元执行某些任务，无论在哪种访问模式（通过 Ethernet/Modbus-SL、USB 连接或 Bluetooth）下
- 登录到运行 Ecoreach 软件的 PC
- 登录到 IFE 和 EIFE 网页

## 用于 Micrologic X 关键设置和控制的密码

访问 Micrologic X 控制单元时，任何改变 Masterpact MTZ 断路器行为的命令都需要使用密码。比如，修改保护设置或者操作断路器，都要求使用 Micrologic X 控制单元密码。

已定义的密码共有 4 个，且每个密码对应一个等级。

给每个等级分配一个角色：
- 1、2 和 3 级用于普通角色，比如操作员。
- 4 级属于管理员级别。管理员级别需要使用 Ecoreach 软件给 Micrologic X 控制单元写入设置。

当通过 Masterpact MTZ Mobile App 或 Ecoreach 软件连接时，会提示用户提供上述其中一种密码。

当通过远程监控接口连接时，密码必须为通讯请求的一部分。

密码仅包含四个 ASCII 字符。密码区分大小写，允许使用以下字符：
- 0 到 9 的数字
- a 到 z 的小写字母
- A 到 Z 的大写字母

Masterpact MTZ 断路器首次安装完成之后，必须使用 Ecoreach 软件定期修改这些密码。这些密码只能被数量有限的可信用户共享。视情况采纳以下的密码策略建议。

## 联网 PC 的密码和用户 ID

运行 Ecoreach 软件或者通过任何其他方式（比如，IFE 或 EIFE 网页，或 SCADA）访问 Micrologic X 控制单元的 PC 必须提示用户登陆并输入密码。必须确保用户定义的是强密码，并定期修改这些密码。此外，必须设置定时器，以便在达到某个闲置时间之后自动锁定 PC 屏幕。

如果可以，强密码应包含大小写字母、数字和特殊字符，其长度应至少为 10 个字符。

请参阅以下有关密码策略的建议。

## IFE 和 EIFE 网页的密码

IFE 和 EIFE 网页用户拥有个人用户 ID 和密码，以便登录到这些网页中。在首次登陆到 IFE 和 EIFE 网页中后，用户必须修改密码。

您必须明确组织中的哪些用户需要登录到 IFE 和 EIFE 网页，且必须遵循以下密码策略建议。

## 有关密码策略的网络安全建议

密码策略是网络安全策略的主要元素之一。良好的密码策略包含以下几方面：
- 使用强密码
- 定期修改密码
- 禁止重新使用旧密码
- 定期就密码的相关最佳做法对用户给与提醒

为了保护您的 PC 以及其上运行的所有软件，至少应执行以下措施：
- 强制使用强密码
- 设置长度至少为 10 个字符的密码
- 将密码有效期设置为至少 3 天，至多 180 天
- 保留八个最近密码的记录，禁止重新使用这些密码

所有用户必须知悉密码的相关最佳做法。其中包括：
- 不外泄个人秘密
- 密码输入时不显示密码
- 不通过电子邮件或任何其他方式传送密码
- 不将密码保存在 PC 或其他设备上

# 培训

## 综述

员工认知和培训是任何网络安全策略的极重要基础。您必须确保有权访问您系统控制网络的用户都了解公司的安全信息策略。您还必须确保他们在根据该策略执行任务方面接受过相应的培训。

具体地讲，用户必须了解并且必须定期向用户提醒有关以下方面的最佳做法：

- 不透露机密或敏感性信息，如设备或锁闭室的密码或进入密码。
- PC 未使用时，保持安全锁闭隔离
- 确保可用于访问系统的智能手机始终由用户保管，并且不会遭受通过 Bluetooth 或互联网发起的黑客攻击。
- 不为了一时之便规避任何安全策略

有关设计和实施良好培训策略的更多信息，请参阅 *我如何减少网络攻击漏洞？*。

# 第3章
# 本地访问的网络安全建议

## 章节概述

本章列出了 Masterpact MTZ 断路器的本地访问途径。它还就保护这些访问途径的安全提供了相应建议。这些都是设备运行要考虑的重要因素。

## 本章包含了哪些内容？

本章包含了以下主题：

# Masterpact MTZ 断路器本地访问限制

## 综述

Masterpact MTZ 智能模块单元（IMU）提供本地访问和远程访问功能。您必须确保仅为授权用户授予访问权限。

## Masterpact MTZ 断路器本地访问

对 Masterpact MTZ 智能模块单元的本地访问为系统相关信息访问以及系统控制提供了各种可能。

因此，必须将 Masterpact MTZ 断路器安装在锁闭的区域中，由此来限制其本地访问，以避免：

- 未授权访问 Micrologic X HMI，从而发生通过 HMI 修改设置的风险
- 未授权访问无线 Bluetooth 通讯，从而发生通过 Masterpact MTZ Mobile App 修改设置的风险
- 未授权访问无线 NFC 通讯，从而发生数据泄露的风险
- 在未经授权的情况下通过 Micrologic X 控制单元上的 Mini USB 端口进行连接，从而发生通过 Ecoreach 软件或带 Masterpact MTZ Mobile App 的智能手机修改设置的风险
- 未授权访问 IO 模块，从而发生修改正使用的预定义应用程序的开关设置的风险

还必须实施锁定区域进入管理规则。具体地讲，您必须确保：

- 该区域始终保持锁闭。
- 该区域配备有身份验证和授权系统。
- 仅授权人员才拥有钥匙或进入密码。
- 接入室内的通讯网络电缆以及室外通讯设备上的连接端口受到保护。
- 访问 Micrologic X 控制单元的 PC、智能手机、平板电脑等所有设备已根据最新供应商指南加以强化。

在 Masterpact MTZ 断路器安装在锁闭区域中的情况下，您必须实施应急打开程序。例如：

- 为该区域配备至少一个可在外部使用的急停按钮
- 为断路器配备 MN 欠压线圈（失效保护系统）

## Micrologic X HMI 本地访问的保护建议

### 可通过 HMI 访问的功能

任何能够触及安装有 Masterpact MTZ 断路器的机箱的人员都能够访问 Micrologic X 控制单元上的 HMI。

一些关键的功能，比如设备的保护设置，可以通过 Micrologic X HMI 来配置。

### 通过 Micrologic X HMI 访问的保护建议

Micrologic X HMI 既没有密码保护，又不能够物理地锁闭以隔离显示屏。因此，如要保护对 HMI 的访问，您必须：

- 将 Masterpact MTZ 断路器安装在锁闭区域中。
- 始终保持该区域锁闭。
- 仅将钥匙或进入密码交给授权人员。

有关 Masterpact MTZ 断路器访问保护的更多信息，请参阅实施限制访问策略 (参见第 *18* 页)。

### 锁定保护设置

您可以锁定 Masterpact MTZ 断路器的保护设置，以免它们遭到通过 HMI 进行的本地修改。缺省情况下，是允许通过 HMI 修改保护设置的。

如果不需要在 HMI 上本地修改保护设置，则建议禁用此功能。相关说明，请参阅 *Micrologic X 控制单元 - 用户指南*。

## 通过 NFC 访问的保护建议

### 可通过 NFC 访问的功能

通过无线近场通讯 (NFC)，即使 Micrologic X 控制单元未通电，也可以将数据从控制单元下载到智能手机。无法修改控制单元上的任何设置，也无法使 Masterpact MTZ 断路器分闸、合闸或复位。

### 建立 NFC 连接的前提条件

与 Micrologic X 控制单元建立 NFC 连接的前提条件是：

- 必须能够物理上进入 Masterpact MTZ 断路器所在的房间。
- 智能手机上必须安装有 Masterpact MTZ Mobile App，
- 智能手机必须支持 NFC。

任何满足这些条件的人员都可以下载对于您的操作而言可能具有机密性的数据。在 Micrologic X 控制单元中，不会记录通过 NFC 建立的连接。

有关建立 NFC 连接的详细程序，请参阅 *Micrologic X 控制单元 - 用户指南*

### 通过 NFC 访问的一般保护建议

如要保护可通过无线 NFC 进行的数据访问，建议：

- 将 Masterpact MTZ 断路器安装在锁闭的区域，使得未授权人员无法触及 Micrologic X 控制单元。
- 始终保持该区域锁闭。
- 仅将钥匙或进入密码交给授权人员。

有关更多信息，请参阅 断路器 (参见第 *18* 页)本地访问Masterpact MTZ限制建议。

### NFC 通讯建议

如要保护可通过无线 NFC 进行的功能访问，建议：

- 在与 Micrologic X 控制单元进行 NFC 连接期间，断开智能手机的网络连接（例如，将智能手机设置成飞行模式）。
- 禁用智能手机上的 Bluetooth 通讯。
- 即便提示输入配对代码，也不要输入，因为 NFC 连接是不需要输入配对代码的。

### Masterpact MTZ Mobile App 使用建议

如要限制运行 Masterpact MTZ Mobile App 的智能手机对 Micrologic X 控制单元的访问，建议仅使用官方 Schneider Electric Masterpact MTZ Mobile App 来连接到 Masterpact MTZ 断路器。

### 智能手机使用建议

如要限制智能手机对 Micrologic X 控制单元的访问，建议：

- 确保安装有 Masterpact MTZ Mobile App 的智能手机受到密码保护并且仅供工作之用。
- 实施智能手机供应商或制造商推荐的所有安全功能，由此强化安装有 Masterpact MTZ Mobile App 的智能手机。
- 保持智能手机的防病毒应用程序为最新版本。
- 在非必要情况下，不得透露与智能手机有关的信息（电话号码、MAC 地址）。
- 在与 Micrologic X 控制单元进行 NFC 连接期间，断开智能手机的网络连接（例如，将智能手机设置成飞行模式）。
- 不得在智能手机上存储机密或敏感性信息。

# 通过 Bluetooth 访问的保护建议

## 可通过 Bluetooth 访问的功能

**注意**

**运行失控危险**

- 设备只能由有资格的人员，利用安装保护系统研究的结果进行配置和设定。
- 在安装调试期间及进行任何更改之后，检查 Micrologic X 配置和保护功能设置是否与此研究的结果一致。
- Micrologic X 保护功能缺省设置为最小值，但若为长期保护功能，则缺省设置为最大值。

**不遵循上述说明可能导致设备损坏。**

利用无线 Bluetooth low energy (BLE) 通讯，您可以通过运行 Masterpact MTZ Mobile App 的智能手机访问 Micrologic X 控制单元。此应用提供了与控制单元的面向任务的对接。通过 Bluetooth 传输的数据利用 AES 128 位加密法加密。

## 建立 Bluetooth 连接的前提条件

与 Micrologic X 控制单元建立 Bluetooth 连接的前提条件是：

- Micrologic X 控制单元必须通电。
- Micrologic X 控制单元上的 Bluetooth 功能必须已启用。
- 一次只能有一台智能手机连接到控制单元。
- 您的智能手机上必须安装有 Masterpact MTZ Mobile App。
- 智能手机必须支持 Bluetooth low energy（4.0 或以上）。
- 必须能够触及 Micrologic X 控制单元，以便激活 Bluetooth 按钮，并且在连接持续时间内，工作人员必须在相应距离范围内（通常在与控制单元相距 20 至 30 米或码的范围内）。

任何满足这些条件并且建立了连接的人员都可以访问能够影响您设备系统的功能。

有关建立 Bluetooth 连接的详细程序，请参阅 *Micrologic X 控制单元 - 用户指南*。

## 通过 Bluetooth 访问的一般保护建议

如要保护可通过无线 Bluetooth 进行的功能访问，建议：

- 将 Masterpact MTZ 断路器安装在锁闭的区域，使得未授权人员无法触及 Micrologic X 控制单元。
- 始终保持该区域锁闭。
- 仅将钥匙或进入密码交给授权人员。

有关 Masterpact MTZ 断路器访问保护的更多信息，请参阅实施限制访问策略 (参见第 *18* 页)。

## Bluetooth 使用建议

如要保护可通过无线 Bluetooth 进行的功能访问，建议：

- 按照 *Micrologic X 控制单元 - 用户指南* 中所述，禁用 Micrologic X 控制单元上的 Bluetooth 功能，只有在准备好建立连接的情况下才启用此功能。
- 将 Bluetooth 断开连接定时器设置为 5 分钟。
- 除非正在启动 Bluetooth 连接，否则不得通过 Micrologic X 控制单元正面上的激活按钮来激活 Bluetooth。Bluetooth 在不使用时必须保持关闭。
- 完成后，按下 Bluetooth 按钮，即可终止通讯。
- 尽量减少配对次数，并且只能在安全区域内执行配对，以防入侵者看到所输入的配对代码。
- 即使意外地发现提示输入配对代码，也不要输入。
- 在 Bluetooth 配对期间，使智能手机尽可能靠近 Micrologic X 控制单元。

## Masterpact MTZ Mobile App 使用建议

如要限制运行 Masterpact MTZ Mobile App 的智能手机对 Micrologic X 控制单元的访问，建议仅使用官方 Schneider Electric Masterpact MTZ Mobile App 来连接到 Masterpact MTZ 断路器。

## 智能手机使用建议

如要限制智能手机对 Micrologic X 控制单元的访问，建议：

- 确保安装有 Masterpact MTZ Mobile App 的智能手机受到密码保护并且仅供工作之用。
- 实施智能手机供应商或制造商推荐的所有安全功能，由此强化安装有 Masterpact MTZ Mobile App 的智能手机。
- 保持智能手机的防病毒应用程序为最新版本。
- 在非必要情况下，不得透露与智能手机有关的信息（电话号码、MAC 地址）。
- 在与 Micrologic X 控制单元进行 Bluetooth 连接期间，断开智能手机的网络连接。
- 不得在智能手机上存储机密或敏感性信息。

# 通过 Mini USB 端口访问 Micrologic X 控制单元的保护建议

## 可通过 Mini USB 端口访问的功能

Micrologic X 控制单元的所有功能都可以通过以下方式来访问：
- 将运行 Ecoreach 软件的 PC 连接到控制单元的 Mini USB 端口。
- 将运行 Masterpact MTZ Mobile App 的智能手机通过 USB OTG 适配器连接到控制单元的 Mini USB 端口。

请注意，控制单元中没有大容量存储功能。因此，无法通过从 USB 存储盘或其他大容量存储设备下载恶意软件的方式攻击系统。

## 建立 USB 或 USB OTG 连接的前提条件

与 Micrologic X 控制单元建立 USB 连接的前提条件是：
- 必须能够物理上进入 Masterpact MTZ 断路器所在的房间。
- 对于 PC 与控制单元的连接：
  - 必须使用带 Mini USB 连接器的 USB 电缆来将 PC 连接到 Micrologic X 控制单元上的 Mini USB 端口。
  - 您的 PC 上必须运行有 Ecoreach 软件。
- 对于智能手机与控制单元的连接：
  - 必须使用 OTG 适配器以及带 Mini USB 连接器的 USB 电缆来将智能手机连接到 Micrologic X 控制单元上的 Mini USB 端口。
  - 您的智能手机上必须运行有 Masterpact MTZ Mobile App。

## 通过 Mini USB 端口访问的一般保护建议

如要保护可通过 Micrologic X 控制单元上的 Mini USB 端口进行的功能访问，建议：
- 将 Masterpact MTZ 断路器安装在锁闭的区域，使得未授权人员无法触及 Micrologic X 控制单元。
- 始终保持该区域锁闭。
- 仅将钥匙或进入密码交给授权人员。

有关更多信息，请参阅 Masterpact MTZ 断路器本地访问 (参见第 *18* 页)限制建议。

## 运行 Ecoreach 软件的 PC 的相关建议

如要保护通过本地连接到控制单元正面 Mini USB 端口的 PC 进行的 Micrologic X 控制单元访问，建议：
- PC 未使用时，保持安全锁闭隔离。
- 确保运行 Ecoreach 软件的 PC 需要用户登陆和密码。
- 强制使用强密码 (参见第 *15* 页)。
- 确保定期修改用户密码。
- 禁止重新使用旧密码。
- 设置定时器，以便在达到某个闲置时间之后锁定 PC 屏幕。
- 根据 PC 上运行的操作系统的最新供应商指南，强化 PC。
- 限制可使用 Ecoreach 软件的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

## 运行 Masterpact MTZ Mobile App 的智能手机的相关建议

如要保护通过本地连接到控制单元正面 Mini USB 端口的智能手机进行的 Micrologic X 控制单元访问，建议：
- 确保运行 Masterpact MTZ Mobile App 的智能手机受到密码保护并且仅供工作之用。
- 实施智能手机供应商或制造商推荐的所有安全功能，由此强化运行 Masterpact MTZ Mobile App 的智能手机。
- 保持智能手机的防病毒应用程序为最新版本。
- 在非必要情况下，不得透露与智能手机有关的信息（电话号码、MAC 地址）。
- 在与 USB OTG 控制单元进行 Micrologic X 连接期间，断开智能手机的网络连接。
- 不得在智能手机上存储机密或敏感性信息。

# 第4章
# 远程访问的网络安全建议

## 章节概述

本章列出了 Masterpact MTZ 断路器的远程访问途径。它还就保护这些访问途径的安全提供了相应建议。这些都是设备运行要考虑的重要因素。

## 本章包含了哪些内容？

本章包含了以下主题：

# Masterpact MTZ 断路器远程访问限制

## 综述

Masterpact MTZ 智能模块单元（IMU）提供本地访问和远程访问功能。您必须确保仅为授权用户授予访问权限。

## Masterpact MTZ 断路器远程访问

根据您的系统架构，可能有多种方法来实现对 Masterpact MTZ 断路器的远程访问。具体地讲，通过 Ethernet 或 Modbus-SL 进行的远程访问让您能够全面控制您的系统。因此，必须控制您系统的远程访问。

具体地讲，您必须考虑以下方面：

- 可如何利用各种可用的通讯途径 (参见第 *11* 页)访问系统
- 通过每个访问途径可获得的信息和控制 (参见第 *14* 页)

## 启用和禁用 Masterpact MTZ 断路器远程控制

Masterpact MTZ 断路器的远程控制包含以下操作：

- 使断路器分闸、合闸和复位
- 修改断路器设置

如果不需要执行 Masterpact MTZ 断路器的远程控制，则强烈建议使用 IFE、EIFE 或 IFM 接口禁用远程控制。缺省情况下，远程控制处于启用状态。

如果使用的是 IFE 接口，则使用前面板上的挂锁来启用或禁用通过 Ethernet 网络发送的远程控制。

如果使用的是 EIFE 接口，则将运行 Ecoreach 软件的 PC 连接到 Micrologic X 控制单元正面的 Mini USB 端口，以启用或禁用通过 Ethernet 网络进行的 Masterpact MTZ 断路器远程控制。

如果使用的是 IFM 接口，则使用前面板上的挂锁来启用或禁用通过 Modbus-SL 网络发送的远程控制。

## 锁定保护设置

您可以锁定 Masterpact MTZ 断路器的保护设置，以免它们遭到远程修改。缺省情况下，是允许远程修改保护设置的。

如果不使用保护设置远程修改功能，则建议其禁用。相关说明，请参阅 *Micrologic X 控制单元 - 用户指南*。

## 将 IC 网络与企业网络分离

### 综述

在设计和实施工业控制网络时，必须使用分隔机制来将其与您的企业网络分离。这有助于限制对 Masterpact MTZ 智能模块单元的访问。

具体地讲，您必须考虑以下方面：

- 使用防火墙
- 构建控制区
- 使用入侵检测系统 (IDS) 和/或入侵防御系统 (IPS) 设备
- 实施安全策略和培训计划
- 制定事件响应机制

由专业化组织（比如，NIST）和标准制定机构（比如，ISO、IEC/IEEE）发布并更新工业控制网络设计指南，并使工业控制网络与企业互联网分离。请根据这些出版物来处理上述几点。

## 通过 Ethernet 远程访问 Micrologic X 控制单元的保护建议

### 可通过 Ethernet 访问的功能

当运行 Ecoreach 软件的 PC 已连接到 Ethernet 网络时，Micrologic X 控制单元的所有功能在以下情况下都能够被访问：

- Masterpact MTZ 断路器连接到 IFE 接口。
- Masterpact MTZ 断路器包含 EIFE 接口。
- Masterpact MTZ 断路器连接到堆叠至 IFE 服务器的 IFM 接口。

### 建立 Ethernet 连接的前提条件

与 Micrologic X 控制单元建立 Ethernet 连接的前提条件是：

- Micrologic X 控制单元必须通电。
- Micrologic X 控制单元必须通过以下方式连接到 Ethernet 网络：
  - IFE 接口。
  - EIFE 接口。
  - 堆叠到 IFE 服务器的 IFM 接口。
- 您的 PC 或其他设备（比如，FDM128 或 PLC）必须运行有监控软件（SCADA、Ecoreach）并且连接到允许远程访问的 Ethernet 网络。
- 您必须拥有具备相应访问权限的用户 ID 和密码来登录到 Ecoreach 软件中。

### 连接到 Ethernet 的 PC 的相关建议

如要保护联网 PC 对 Micrologic X 控制单元的访问，建议：

- PC 未使用时，保持安全锁闭隔离。
- 确保利用 Ethernet（比如，通过 IFE 或 EIFE 网页，或者 SCADA）访问 Micrologic X 控制单元的 PC 需要用户登陆和密码。
- 强制使用强密码 (参见第 *15* 页)。
- 确保定期修改用户密码。
- 禁止重新使用旧密码。
- 设置定时器，以便在达到某个闲置时间之后锁定 PC 屏幕。
- 根据 PC 上运行的操作系统的最新供应商指南，强化 PC。
- 限制可通过联网 PC 访问 Micrologic X 控制单元的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

除以上注意事项之外，还必须遵循 *我如何减少网络攻击漏洞？* 中的系统保护一般指南和建议。

# 通过 Modbus-SL 远程访问 Micrologic X 控制单元的保护建议

## 可通过 Modbus-SL 访问的功能

当运行 Ecoreach 软件的 PC 已连接到 Modbus-SL 网络时，Micrologic X 控制单元的所有功能在 Masterpact MTZ 断路器连接到 IFM 接口后都能够被访问。

## 建立 Modbus-SL 连接的前提条件

与 Micrologic X 控制单元建立 Modbus-SL 连接的前提条件是：

- Micrologic X 控制单元必须通电。
- Micrologic X 控制单元必须连接到 IFM 接口。
- 您的 PC 或其他设备（比如，PLC）必须运行有监控软件（SCADA、Ecoreach）并且连接到允许远程访问的 Modbus-SL 网络。
- 您必须拥有具备相应访问权限的用户 ID 和密码来登录到 Ecoreach 软件中。

## 连接到 Modbus-SL 的 PC 的相关建议

如要保护联网 PC 对 Micrologic X 控制单元的访问，建议：

- PC 未使用时，保持安全锁闭隔离。
- 确保利用 Modbus-SL（比如，通过 SCADA）访问 Micrologic X 控制单元的 PC 需要用户登陆和密码。
- 强制使用强密码 (参见第 *15* 页)。
- 确保定期修改用户密码。
- 禁止重新使用旧密码。
- 设置定时器，以便在达到某个闲置时间之后锁定 PC 屏幕。
- 根据 PC 上运行的操作系统的最新供应商指南，强化 PC。
- 限制可通过联网 PC 访问 Micrologic X 控制单元的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

除以上注意事项之外，还必须遵循 *我如何减少网络攻击漏洞？* 中的系统保护一般指南和建议。

# 第5章
# 固件升级和 Digital Modules 的网络安全建议

## 本章包含了哪些内容？

本章包含了以下主题：

# 安装固件升级

## 综述

分发经窜改或非法的软件包是越来越常见的一种网络攻击方式，这些软件包中可能包含经窜改的应用程序或附加应用程序。这些应用程序会破坏原软件的完整性及其预期使用。

为了确保 Masterpact MTZ IMU 所有组件（即，Micrologic X 控制单元、IFE、EIFE 或 IFM 接口、以及 IO 模块）的完整性和真实性，所有 Schneider Electric 原始固件升级都带有数字签名。

利用 Ecoreach 软件升级所有固件必须安装最新版的 Ecoreach 软件。利用 Ecoreach 软件，通过固件菜单升级所有固件。Ecoreach 文档可以从 Schneider Electric 下载网站 (*https://www.schneider-electric.com/en/download/*) 下载。

## 有关固件升级的网络安全建议

必须安装最新固件。

在为 Masterpact MTZ IMU 的组件安装固件升级时，建议：

- 根据认可的运营技术 (OT) 实践安装升级，比如，在生产环境中安装和部署非生产型系统之前，先对该系统进行检验测试。
- 仅使用最新版的 Ecoreach 软件来下载和安装固件升级。
- 根据操作系统的最新供应商指南，强化运行 Ecoreach 软件的 PC。

## 签名固件

为 Masterpact MTZ IMU 设计的所有固件都使用 Schneider Electric 公钥基础设施进行了签名。数字签名经由 Ecoreach 软件中的公共证书来验证。

在通过 Ecoreach 软件将固件上载到 Masterpact MTZ IMU 之后，Micrologic X 控制单元还会自动验证升级包的数字签名。这种验证通过控制单元中的公共证书来执行。

出于安全原因，公共证书会更改。因此，一个主要的安全要求（同时也是您的责任）是检查用于下载和安装固件升级的 Ecoreach 软件是否为最新版本。拥有最新版的 Ecoreach 软件就意味着用于固件签名的公共证书是最新的。

失效的证书会公布在证书撤销列表 (CRL) 中。此列表见 Schneider Electric 官方网站。

## 利用 Ecoreach 软件升级固件的好处

Ecoreach 软件能够极大地有助于确保固件升级期间工业控制网络的完整性。仅使用最新版的 Ecoreach 软件来下载和安装固件，因为它是具有以下优点的唯一软件：

- 在利用 Ecoreach 软件从 Schneider Electric 官方下载中心下载固件包时，会自动验证固件包的数字签名。
- 在（利用 Ecoreach 软件，通过 USB 连接）将固件上载到 Micrologic X 控制单元时，会自动验证升级包的数字签名。

通过 Ecoreach 软件进行的自动验证完全依赖于所使用的公共证书的有效性。

请参阅 Ecoreach 在线帮助上的相关详细程序，了解如何下载和安装固件升级。

**⚠ 警告**

**运行失控危险**

- 一旦接收到更新通知，便应更新 Ecoreach 软件的版本。
- 利用 Ecoreach 软件的最新版本来升级所有产品的固件。
- 定期核查 Schneider Electric 官方网站上公布的证书撤销列表。如果您的产品中有产品的证书被撤销，请不要安装撤销日期前的固件。

**不遵循上述说明可能导致人员伤亡或设备损坏。**

## 查看证书撤销列表

必须定期（至少每三个月）查看 Schneider Electric 公布的证书撤销列表(CRL)，确保您设备所使用的证书全都不在列。

按照以下步骤查看 CRL：

| 步骤 | 操作 |
|---|---|
| 1 | 显示 Schneider Electric 网站 (参见第 *35* 页)上公布的 CRL。 |
| 2 | 如果列表为空，则意味着您当前的证书是有效的；无需采取其他措施。<br>如果列表不为空，则转到步骤 3。 |
| 3 | 确认您正使用的 Ecoreach 软件是最新版本。<br>否则，应更新 Ecoreach 软件。 |
| 4 | 升级固件。 |

# 购买和安装 Digital Modules

## 综述

Digital Modules 是选配模块，用于扩展 Micrologic X 控制单元系列可用的功能。它们可以在初始订单中与 Masterpact MTZ 断路器一同订购，或者也可以在日后从 Schneider Electric 网上 GoDigital 商城中购买。

为 Micrologic X 控制单元设计的所有 Digital Modules 都通过 Schneider Electric 公钥基础设施 (PKI) 进行了数字签名，进一步提升了安全性。PKI 有助于确保这些下载的真实性和完整性。必须使用 Ecoreach 软件安装 Digital Modules。

## Digital Modules 购买的网络安全建议

如要为 Micrologic X 控制单元购买 Digital Modules，请仅使用官方 Schneider Electric 下载中心 GoDigital 商城。

在为 Masterpact MTZ IMU 的组件安装 Digital Modules 时，建议：

- 根据认可的运营技术 (OT) 实践安装 Digital Modules，比如，在生产环境中安装和部署非生产型系统之前，先对该系统进行检验测试。
- 仅使用最新版的 Ecoreach 软件来下载和安装 Digital Modules。
- 根据操作系统的最新供应商指南，强化用于下载和安装 Digital Modules 的 PC。

## Digital Modules 安装的网络安全建议

只能使用 Ecoreach 软件来安装 Micrologic X 控制单元的 Digital Modules。

Ecoreach 软件能够极大地有助于确保工业控制网络的完整性。仅使用最新版的 Ecoreach 软件来安装 Digital Modules，因为它是具有以下优点的唯一软件：

- 在利用 Ecoreach 软件通过 USB 连接升级 IMU 的设备固件时，会自动验证固件升级的数字签名。
- 在利用 Ecoreach 软件通过 USB 连接将 Digital Module 上载到 Micrologic X 控制单元时，会自动验证 Digital Module 的数字签名。

通过 Ecoreach 软件进行的自动验证完全依赖于所使用的公共证书的有效性。

请参阅 Ecoreach 在线帮助上的相关详细程序，了解如何下载和安装 Digital Modules。

**⚠ 警告**

**运行失控危险**

- 一旦接收到更新通知，便应更新 Ecoreach 软件的版本。
- 利用 Ecoreach 软件的最新版本来升级所有产品的固件。
- 定期核查 Schneider Electric 官方网站上公布的证书撤销列表。如果您的产品中有产品的证书被撤销，请不要安装撤销日期前的固件。

**不遵循上述说明可能导致人员伤亡或设备损坏。**

## 查看证书撤销列表

必须定期（至少每三个月）查看 Schneider Electric 公布的证书撤销列表(CRL)，确保您设备所使用的证书全都不在列。

按照以下步骤查看 CRL：

| 步骤 | 操作 |
|---|---|
| 1 | 显示 Schneider Electric 网站 (参见第 *35* 页)上公布的 CRL。 |
| 2 | 如果列表为空，则意味着您当前的证书是有效的；无需采取其他措施。<br>如果列表不为空，则转到步骤 3。 |
| 3 | 确认您正使用的 Ecoreach 软件是最新版本。<br>否则，应更新 Ecoreach 软件。 |
| 4 | 升级 Digital Module。 |

# Schneider Electric 网络安全门户

## 综述

Schneider Electric 网络安全门户概述了 Schneider Electric 隐患管理策略。

Schneider Electric 隐患管理策略旨在处理影响 Schneider Electric 产品和系统的网络安全隐患，从而为现有的解决方案、客户和环境提供有效保护。

Schneider Electric 与研发人员、网络应急响应小组 (CERT) 和资产所有人密切合作，确保及时提供准确信息，适时保护系统安全。

Schneider Electric 的企业产品 CERT (CPCERT) 负责管理并发出与影响产品和解决方案的隐患和漏洞有关的警示。

CPCERT 协调相关 CERT、独立研发人员、产品经理和所有受影响客户之间的沟通。

Schneider Electric 网络安全门户可以通过 *http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp* 来访问。

## Schneider Electric 网络安全门户上的信息

该门户提供以下信息：

- 有关产品网络安全隐患的信息。
- 有关网络安全事件的信息。
- 让用户能够声明网络安全事件或隐患的界面。
- 访问提供系统环境保护相关信息的资源。
  这些环境包括：
  - 工业流程。
  - 楼宇管理和出入控制系统。
  - 数据中心。
  - 电气基础设施控制系统。
- 通过选项卡 **Firmware PKI** 访问的证书和证书撤销列表。

## Schneider Electric 网络安全门户上的证书撤销列表 (CRL)

下表列出了相关的 CRL：

| 产品 | CRL |
|---|---|
| MTZ 控制单元 | LV 断路器 Micrologic 主站 |
| IO 模块 | LV 断路器 Micrologic 主站 |
| IFE | Adv 通讯主站 |
| EIFE | Adv 通讯主站 |
| IFM | LV 断路器 Micrologic 主站 |

# 术语

**BLE**

Bluetooth low energy。

**EIFE**

可供 Masterpact MTZ 抽出式断路器选配的嵌入式 Ethernet 接口。利用此模块，可以通过企业内联网访问断路器。

**GoDigital**

Schneider Electric 网上商城，用于购买专为 Micrologic X 控制单元设计的 Digital Modules。

**HMI**

人机界面。是指位于设备正面的显示屏，操作员可使用它来读取信息或配置设备。

**IC**

工业控制。是指用于监控企业生产过程和设备的软硬件系统。

**IFE**

可连接到 Masterpact MTZ 断路器的 Ethernet 接口。利用此模块，可以通过企业内联网访问断路器。

**IFM**

IFM Modbus-SL 接口使 IMU 能够连接到两线制 RS 485 串行线路 Modbus 网络。每个 IMU 都拥有其自己的 IFM 接口和相应的 Modbus 地址。

**IMU**

智能模块单元。对于 Masterpact MTZ 断路器，IMU 是指断路器本身、Micrologic X 控制单元以及相关的 ULP 模块、IFE、EIFE、IFM 接口、以及 IO 模块。

**IP**

互联网协议。IP 地址用于识别连接到企业内联网或互联网的设备。

**IT**

信息技术。是指区别于工业控制 (IC) 网络或 OT（运营技术）网络的企业信息系统和信息网络。

**LAN**

局域网。是指企业内联网或 IT 网络。

**NFC**

近场通讯。是指一种无线通讯协议。

**OT**

运营技术。是指企业用来直接监控生产过程和设备的软硬件系统，又被称为工业控制 (IC) 网络。OT 通常用来表示区别于 IT 网络的企业运营网络。

**PIN**

个人标识号。

**PKI**

公钥基础设施。定义一组服务，以用于生成并验证数字签名。公钥基础设施旨在确保信息的保密性、完整性和真实性。

**RAS**

远程访问服务器。

**SCADA**

监控和数据采集。是指设计来获取有关生产过程和设备的实时数据以用于远程监控这些过程和设备的系统。

**TCP/IP**

传输控制协议/互联网协议。是指一整套用于互联网通讯的协议。

**VPN**

虚拟专用网络。使用 VPN 在经验证的外部访问点与信任的企业网络之间建立安全/专用“通道”。

**DOCA0122ZH-01**

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

http://www.schneider-electric.com



06/2017