PacT Series

Master**PacT,** Com**PacT,** Power**PacT**

网络安全指南

PacT Series 提供出众的断路器和开关

DOCA0122ZH-11
09/2025

www.se.com

法律声明

本文档中提供的信息包含与产品/解决方案相关的一般说明、技术特性和/或建议。

本文档不应替代详细调研、或运营及场所特定的开发或平面示意图。它不用于判定产品/解决方案对于特定用户应用的适用性或可靠性。任何此类用户都有责任就相关特定应用场合或使用方面，对产品/解决方案执行或者由所选择的任何业内专家（集成师、规格指定者等）对产品/解决方案执行适当且全面的风险分析、评估和测试。

施耐德电气品牌以及本文档中涉及的施耐德电气及其附属公司的任何商标均是施耐德电气或其附属公司的财产。所有其他品牌均为其各自所有者的商标。

对于将本文档 或其内容用作商业用途的行为，施耐德电气未授予任何权利或许可，但以“原样”为基础进行咨询的非独占个人许可除外。

对于本文档或其内容或其格式，施耐德电气有权随时修改或更新，恕不另行通知。

在适用法律允许的范围内，对于本文档信息内容中的任何错误或遗漏，以及对本文档内容的任何非预期使用或误用，施耐德电气及其附属公司不会承担任何责任或义务。

目录

安全信息

重要信息

在试图安装、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。下述特定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”安全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。它用于提醒您注意潜在人身伤害风险。
遵守此符号后面的安全说明，以免发生伤害或死亡事故。

⚠ 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

注意用于指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有资质的人员执行。施耐德电气不承担由于使用本资料所引起的任何后果。

有资质的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。

关于本文档

文档范围

本指南中的信息涉及带 MicroLogic 脱扣单元和控制单元的 MasterPacT、ComPacT 和 PowerPacT 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并实现一个安全的运行环境。

注:

- 本文档中与新一代 ComPacT NS 和 PowerPacT P和 R 型 断路器相关的信息也适用于现有的 ComPact NS 和 PowerPact P和 R 型 系列断路器。如有例外，将专门说明。
- 本文档中与新一代 ComPacT NSX 和 PowerPacT H-, J-, and L-Frame 断路器相关的信息也适用于现有的 ComPact NSX 和 PowerPacT H 型、J 型和 L 型 系列断路器。如有例外，将专门说明。
- 这些新系列所依托的技术和尺寸架构与现有断路器系列相同。

本指南并不涉及较常见的主题，比如，如何保护您的运营技术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 *How Can I Reduce Vulnerability to Cyber Attacks?*。

注: 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以下断路器：

- 配备有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic 脱扣单元的 MasterPacT NT/NW 断路器
- 配备有 MicroLogic 脱扣单元的 ComPacT NS 断路器
- 配备有 MicroLogic 脱扣单元的 PowerPacT P 型和 R 型断路器
- 配备有 MicroLogic 脱扣单元的 ComPacT NSX 断路器
- 配备有 MicroLogic 脱扣单元的 PowerPacT H、J 和 L 型断路器

注: 本指南中的信息还与旧式 ComPact 和 PowerPact 系列相关。

在线信息

本文档中描述的产品特性旨在与上提供的特性相匹配 www.se.com。作为我们持续改进的企业战略的一部分，我们可能随着时间的推移修改内容以提高清晰度和准确性。如果您发现本文档中的特性与 www.se.com 上的特性存在差异，可考虑 www.se.com 以包含最新信息。

一般网络安全说明

近年来，随着联网机器和生产设备的数量日益增多，发生非法访问、数据泄露和运营中断等网络威胁的几率也相应增加。因此，您必须考虑众多可能的网络安全措施，以帮助保护资产和系统免于此类威胁。

为了有助于保持和保护 Schneider Electric 产品的安全，强烈建议您采取 Cybersecurity Best Practices 文档中所述的网络安全最佳做法。

Schneider Electric 还提供其他信息和帮助：

- 订阅 Schneider Electric 安全资讯。
- 访问 Cybersecurity Support Portal 网页，以：
  - 查看安全通知。
  - 报告漏洞和事件。
- 访问 Schneider Electric Cybersecurity and Data Protection Posture 网页，以：
  - 了解网络安全态势。
  - 在网络安全学院中了更详细地了解网络安全。
  - 深入了解 Schneider Electric 的网络安全服务。

产品相关的网络安全信息

⚠警告

系统可用性、完整性和保密性的潜在危害

- 首次使用时，更改缺省密码和 PIN 码，以有助于防止擅自访问设备设置、控件和信息。
- 禁用未使用的端口/服务和缺省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。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

环境数据

有关产品合规性和环境信息，请参阅 Schneider Electric Environmental Data Program。

文档的可用语言

文档提供以下语言版本:

- 英语 (DOCA0122EN)，原始语言
- 西班牙语 (DOCA0122ES)
- 法语 (DOCA0122FR)
- 中文 (DOCA0122ZH)

IEC 设备的相关文档

文档名称	参考编号
MasterPacT MTZ - MicroLogic X 控制单元 - 用户指南	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
MasterPacT MTZ - MicroLogic Active 控制单元 - 用户指南	DOCA0265EN DOCA0265ES DOCA0265ZH
*ComPacT NSX – Micrologic 5/6/7*电子脱扣单元 - 用户指南	DOCA0188EN DOCA0188ES DOCA0188FR DOCA0188ZH
*ComPact NSX – Micrologic 5/6/7*电子脱扣单元 - 用户指南	DOCA0141EN DOCA0141ES DOCA0141FR DOCA0141ZH
MasterPacT NT/NW - MicroLogic A 和 *E* 脱扣单元 - 用户指南	04443724AA (EN) EAV16735 (ES) 04443723AA (FR)
MasterPacT NT/NW - MicroLogic P 脱扣单元 - 用户指南	04443726AA (EN) EAV16736 (ES) 04443725AA (FR)
MasterPacT NT/NW - MicroLogic H 脱扣单元 - 用户指南	04443728AA (EN) EAV16737 (ES) 04443727AA (FR)
ComPacT NS - MicroLogic A/E 脱扣单元 - 用户指南	DOCA0218EN DOCA0218ES DOCA0218FR DOCA0218ZH
ComPacT NS - MicroLogic P 脱扣单元 - 用户指南	DOCA0219EN DOCA0219ES DOCA0219FR DOCA0219ZH
Enerlin'X EIFE - 用于单个 *MasterPacT MTZ* 抽出式断路器的嵌入式以太网接口 - 用户指南	DOCA0106EN DOCA0106ES DOCA0106FR DOCA0106ZH
Enerlin'X IFE - 以太网交换机服务器 - 用户指南	DOCA0084EN DOCA0084ES DOCA0084FR DOCA0084ZH
Enerlin'X IFE - 用于单个断路器的以太网接口 - 用户指南	DOCA0142EN DOCA0142ES DOCA0142FR DOCA0142ZH
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note
MicroLogic 脱扣单元和控制单元 - 固件历史	DOCA0155EN
MasterPacT MTZ - MicroLogic X Control Unit - Firmware Release Notes	DOCA0144EN
MasterPacT MTZ - MicroLogic Active Control Unit - Firmware Release Notes	DOCA0267EN
Enerlin'X IFM - 用于单个断路器的 *Modbus-SL* 接口 *(TRV00210/ STRV00210)* - 固件发行说明	DOCA0145EN
Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker (LV434000) - Firmware Release Notes	DOCA0146EN
Enerlin'X IFE/EIFE Ethernet Interface - 固件发行说明	DOCA0147EN
Enerlin'X IFE 交换机服务器 - 固件发行说明	DOCA0148EN
Enerlin'X IO Input/Output Application Module for One Circuit Breaker - 固件发行说明	DOCA0149EN

文档名称	参考编号
Enerlin'X FDM121 - 固件发行说明	DOCA0150EN
Enerlin'X FDM128 - Ethernet Display for Eight Devices - Firmware Release Notes	DOCA0151EN
BCM ULP - 固件发行说明	DOCA0152EN
ComPacT NSX / PowerPacT H 型、*J* 型和 *L* 型 *MicroLogic 5/6* - 固件发行说明	DOCA0153EN
ComPacT NSX - MicroLogic 7 Trip Unit - Firmware Release Notes	DOCA0154EN
*ComPacT NSX BSCM Modbus SL/ULP*模块 - 固件发行说明	DOCA0329ZH
用于 *MicroLogic Active* 控制单元的断路器通讯和隔离模块 *(BCIM)* - 固件发行说明	DOCA0395EN
EcoStruxure Cybersecurity Admin Expert User Guide	CAE_EN_UM_B4.1
EcoStruxure Panel Server - 用户指南	DOCA0172EN DOCA0172ES DOCA0172FR DOCA0172DE DOCA0172IT DOCA0172PT

您可以在我们的网站下载这些技术出版物和其他技术信息：www.se.com/ww/en/download/。

UL/ANSI 设备的相关文档

文档名称	参考编号
MasterPacT MTZ - MicroLogic X 控制单元 - 用户指南	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
PowerPacT H 型、*J* 型和 *L* 型 - *MicroLogic 5* 和 *6* 脱扣单元 - 用户指南	48940-312-01 (EN, ES, FR)
MasterPacT NT/NW - MicroLogic A 脱扣单元 - 用户指南	48049-136-05 (EN, ES, FR)
MasterPacT NT/NW - MicroLogic P 脱扣单元 - 用户指南	48049-137-05 (EN)
MasterPacT NT/NW - MicroLogic H 脱扣单元 - 用户指南	48049-330-03 (EN, ES, FR)
Enerlin'X EIFE - 用于单个 *MasterPacT MTZ* 抽出式断路器的嵌入式以太网接口 - 用户指南	DOCA0106EN DOCA0106ES DOCA0106FR DOCA0106ZH
Enerlin'X IFE - 以太网交换机服务器 - 用户指南	DOCA0084EN DOCA0084ES DOCA0084FR DOCA0084ZH
Enerlin'X IFE - 用于单个断路器的以太网接口 - 用户指南	DOCA0142EN DOCA0142ES DOCA0142FR DOCA0142ZH
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note
MicroLogic 脱扣单元和控制单元 - 固件历史	DOCA0155EN
MasterPacT MTZ - MicroLogic X Control Unit - Firmware Release Notes	DOCA0144EN
Enerlin'X IFM - 用于单个断路器的 *Modbus-SL* 接口 *(TRV00210/STRV00210)* - 固件发行说明	DOCA0145EN
Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker (LV434000) - Firmware Release Notes	DOCA0146EN

文档名称	参考编号
Enerlin'X IFE/EIFE Ethernet Interface - 固件发行说明	DOCA0147EN
Enerlin'X IFE 交换机服务器 - 固件发行说明	DOCA0148EN
Enerlin'X IO Input/Output Application Module for One Circuit Breaker - 固件发行说明	DOCA0149EN
Enerlin'X FDM121 - 固件发行说明	DOCA0150EN
Enerlin'X FDM128 - Ethernet Display for Eight Devices - Firmware Release Notes	DOCA0151EN
BCM ULP - 固件发行说明	DOCA0152EN
ComPacT NSX / PowerPacT H 型、*J* 型和 *L* 型 *MicroLogic 5/6* - 固件发行说明	DOCA0153EN
*ComPacT NSX BSCM Modbus SL/ULP*模块 - 固件发行说明	DOCA0329ZH
EcoStruxure Cybersecurity Admin Expert User Guide	CAE_EN_UM_B4.1
EcoStruxure Panel Server - 用户指南	DOCA0172EN DOCA0172ES DOCA0172FR DOCA0172DE DOCA0172IT DOCA0172PT

您可以在我们的网站下载这些技术出版物和其他技术信息：www.se.com/us/en/download/。

有关非包容性或非敏感术语的信息

作为一家负责任、具有包容性的公司，Schneider Electric 不断更新其包含非包容性或非敏感术语的沟通方式和产品。但是，尽管我们做了这些努力，我们的内容仍可能包含某些客户认为不合适的条款。

商标

QR Code 是 DENSO WAVE INCORPORATED 在日本和其他国家或地区的注册商标。

网络安全简介

此部分内容

概述

本部分概述了 Schneider Electric 网络安全策略，以及带 MicroLogic 脱扣单元或控制单元的 MasterPacT、ComPacT 和 PowerPacT 断路器为什么会涉及到网络安全。

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、ComPacT 和 PowerPacT 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。

此方法在系统技术说明中介绍*How Can I Reduce Vulnerability to Cyber Attacks?*。

此外，Schneider Electric 全球网站的 Cybersecurity Support Portal, 57 页 中也提供了许多有用的资源和最新信息。

PacT Series 主系列

Schneider Electric 的低压和中压 PacT Series 让您的装置不会过时。PacT Series 以传奇的 Schneider Electric 创新为基础，包括出众的断路器、开关、漏电保护装置和熔断器，适用于任何标准和特定应用。在支持 EcoStruxure 的开关柜中，通过 PacT Series 在 16 到 6300 A 的低压和最高 40.5 kV 的中压开关柜中体验强大的性能。

MasterPacT、ComPacT 和 PowerPacT 断路器为什么会涉及到网络安全

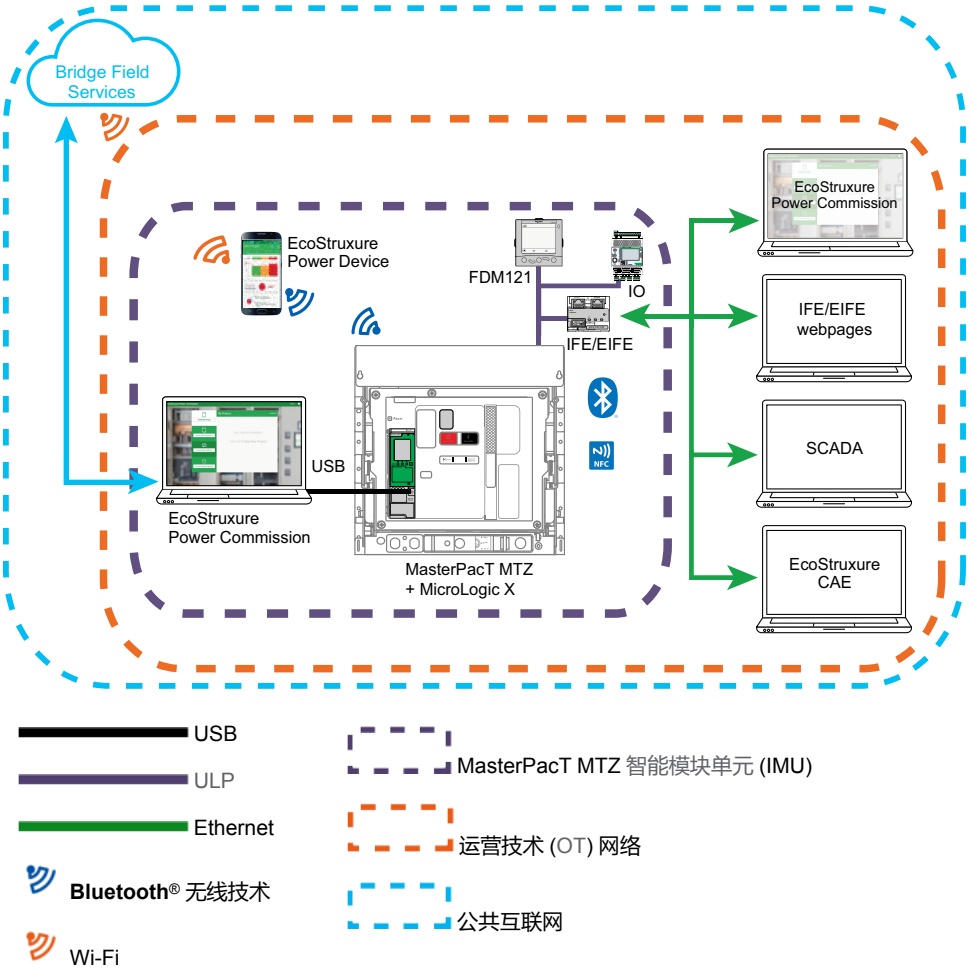
概述

MasterPacT、ComPacT 和 PowerPacT 断路器是一切工厂或设备的关键部件，它负责控制过程供电、提供电气保护和传输关键信息。

具有通讯功能的 MasterPacT、ComPacT 和 PowerPacT 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。这些功能提高了配电系统管理的效率和灵活性。但它们易受网络攻击。

配有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器工作环境

下图显示了与 MasterPacT MTZ 断路器的 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。

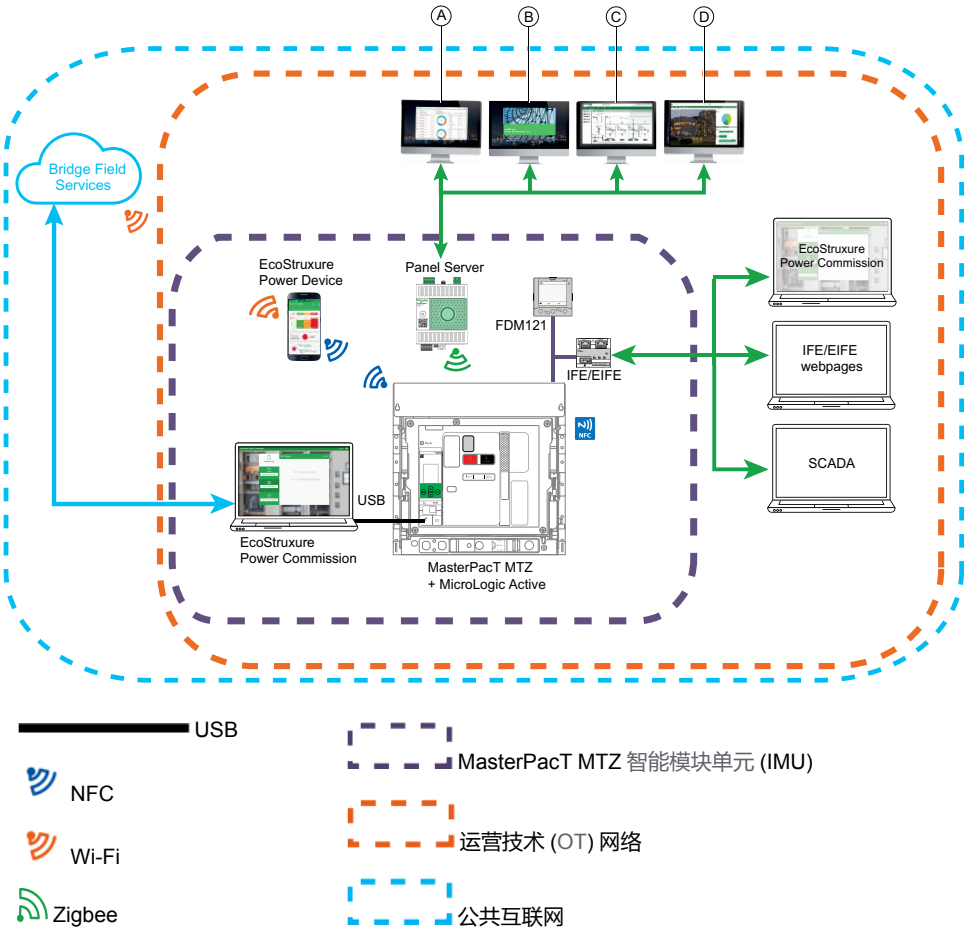
如要通过 MicroLogic X 控制单元与 MasterPacT MTZ 断路器通讯，可使用以下通讯途径：

- MicroLogic X 人机界面 (HMI)
- 用于单个电路断路器的 FDM121 前显示模块

- 通过智能手机的无线 NFC 连接
- 通过智能手机的无线 Bluetooth Low Energy 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 EcoStruxure™ Power Commission 软件的 PC
  - 运行 EcoStruxure Power Device 应用 的智能手机
- 在有 IFE 或 EIFE 接口或者 IFE 服务器的情况下，通过运营技术 (OT) 网络进行 Ethernet（Modbus TCP/IP 或 IEC 61850 协议）连接
- 在有 IFM 接口的情况下，通过运营技术 (OT) 网络进行 Modbus-SL 连接

配有 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器工作环境

下图显示了与 MasterPacT MTZ 断路器的 MicroLogic Active 控制单元通讯的各种方式。



A Panel Server 网页

B EcoStruxure Power Monitoring Expert (PME) 软件

C EcoStruxure Power Operation (PO) 软件

D POI Plus，配有能源管理软件的工业工作站

MasterPacT MTZ 智能模块单元（IMU）包含断路器、MicroLogic Active 控制单元以及相关的 ULP 模块和通讯接口。

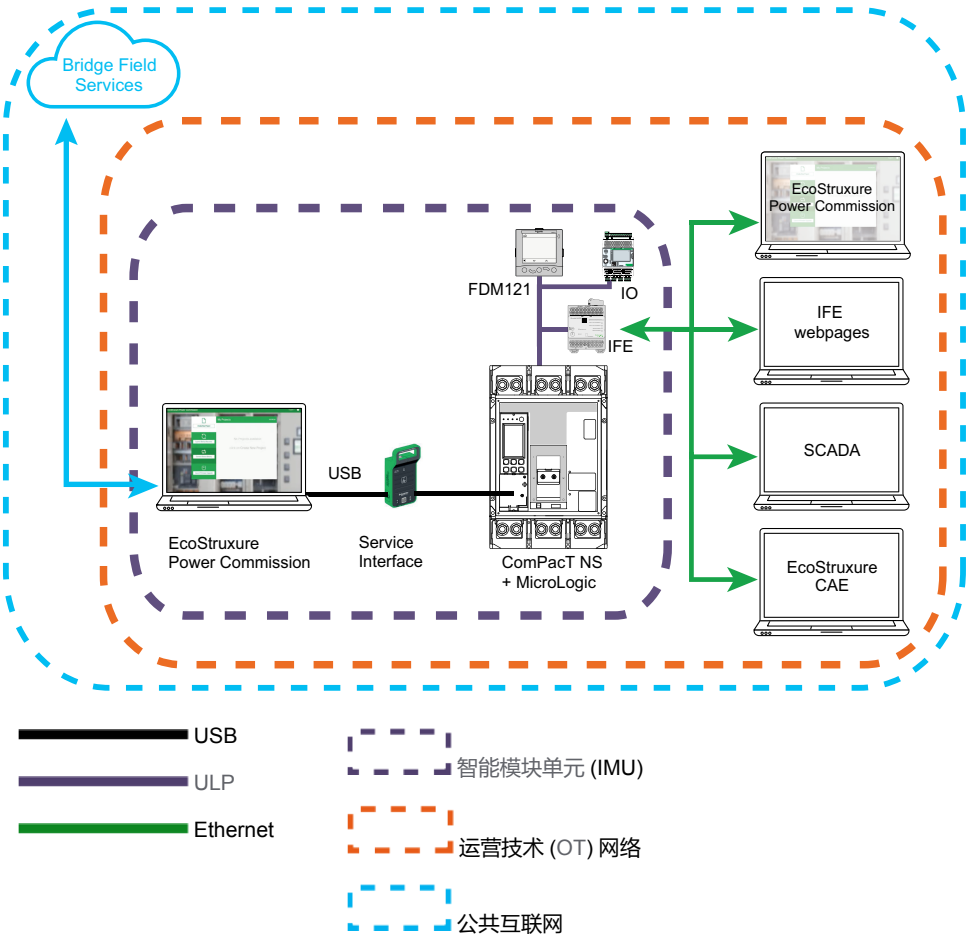
如要通过 MicroLogic Active 控制单元与 MasterPacT MTZ 断路器通讯，可使用以下通讯途径：

- MicroLogic Active 人机界面 (HMI)

- 用于单个电路断路器的 FDM121 前显示模块
- 通过智能手机的无线 NFC 连接
- 通过以下设备连接到 MicroLogic Active 控制单元的 USB-C 端口：
  - 运行 EcoStruxure™ Power Commission 软件的 PC
  - 运行 EcoStruxure Power Device 应用 的智能手机
- 无线 Zigbee 连接，连接到 MicroLogic Active AP/EP 控制单元的 Panel Server。
- 在有 IFE 或 EIFE 接口或 IFE 服务器的情况下，通过运营技术 (OT) 网络进行 Ethernet（Modbus TCP/IP 协议）连接
- 在有 IFM 接口的情况下，通过运营技术 (OT) 网络进行 Modbus-SL 连接

MasterPacT NT/NW、ComPacT NS 及 PowerPacT P 型和 R 型断路器运行环境

下图显示了与 MicroLogic 断路器的脱扣单元通讯的各种方式。



智能模块单元 (IMU) 包含 MasterPacT NT/NW、ComPacT NS 或 PowerPacT P 或 R 型断路器、MicroLogic 脱扣单元以及相关的 ULP 模块、通讯接口和 IO 模块。

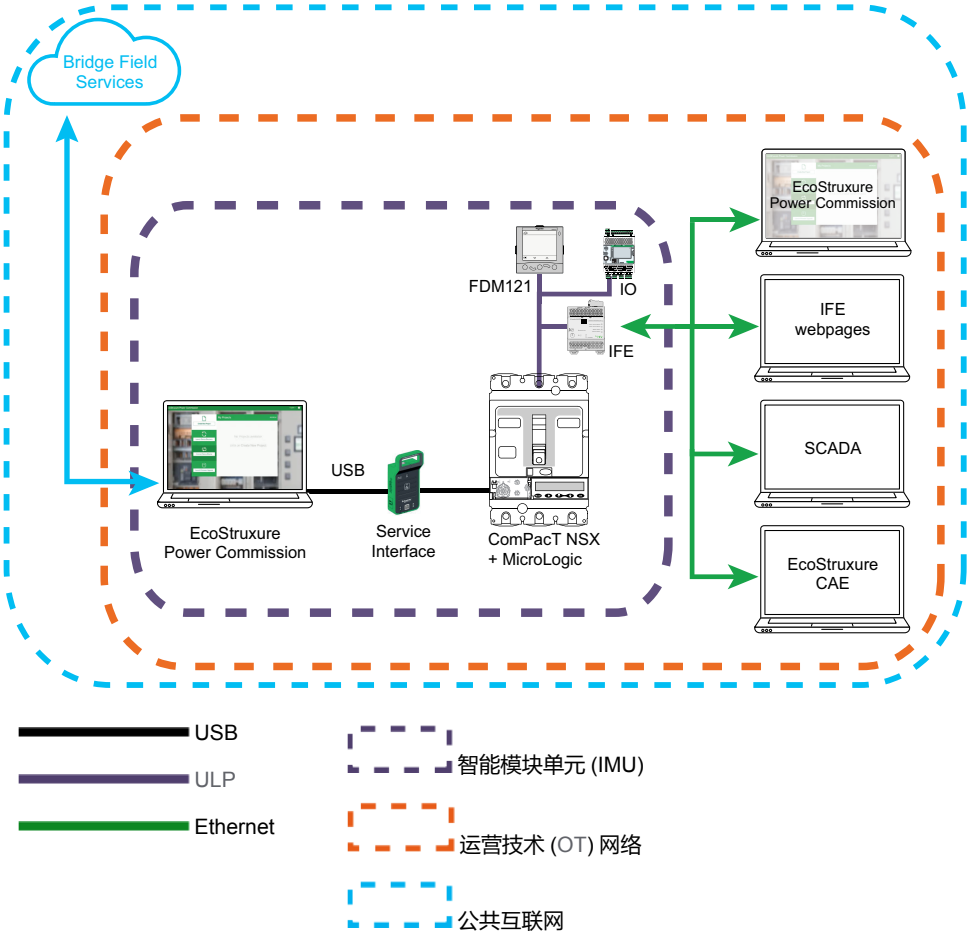
如要通过 MicroLogic 脱扣单元与断路器通讯，可使用以下通讯途径：

- MicroLogic 人机界面 (HMI)
- 用于单个电路断路器的 FDM121 前显示模块
- 通过服务接口从运行 EcoStruxure Power Commission 软件的 PC 连接到 MicroLogic 脱扣单元
- 在有 IFE 接口或 IFE 服务器的情况下，通过运营技术 (OT) 网络进行 Ethernet（Modbus TCP/IP 协议）连接

- 在有 IFM 接口的情况下，通过运营技术 (OT) 网络进行 Modbus-SL 连接

ComPacT NSX 及 PowerPacT H、J 和 L 型断路器运行环境

下图显示了与 MicroLogic 断路器的脱扣单元通讯的各种方式。



智能模块单元 (IMU) 包含 ComPacT NSX 或 PowerPacT H、J 或 L 型断路器、MicroLogic 脱扣单元以及相关的 ULP 模块、通讯接口和 IO 模块。

如要通过 MicroLogic 脱扣单元与断路器通讯，可使用以下通讯途径：

- MicroLogic 人机界面 (HMI)
- 用于单个电路断路器的 FDM121 前显示模块
- 通过服务接口或 USB 维护接口从运行 EcoStruxure Power Commission 软件的 PC 连接到 MicroLogic 脱扣单元
- 在有 IFE 接口或 IFE 服务器的情况下，通过运营技术 (OT) 网络进行 Ethernet（Modbus TCP/IP 协议）连接
- 在有 IFM 接口或 BSCM Modbus SL/ULP 模块的情况下，通过运营技术 (OT) 网络进行 Modbus-SL 连接

遭受网络攻击的系统隐患

如果安全措施不到位，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。

以下安全特性用于降低与在运营技术 (OT) 环境中使用 IFE 和 EIFE 接口、IFE 服务器及 MasterPacT、ComPacT 和 PowerPacT 设备有关的内在威胁。

所提供的安全特性

MasterPacT、ComPacT 和 PowerPacT IMU 支持以下网络安全功能：

- 用户帐户管理：
  - 在 IFE 和 EIFE 接口上
  - 在 IFE 服务器上
  - 在 MicroLogic Active 控制单元上
- 访问码保护
- 可配置的安全服务和设置
- 固件更新机制
- 通过 Modbus TCP/TLS 实现的安全机器到机器通讯（在 IFE 和 EIFE 接口以及 IFE 服务器上）
- Syslog 格式或 CSV 格式的安全日志（在 IFE 和 EIFE 接口以及 IFE 服务器上）

这些特性所提供的安全功能有助于保护产品免遭可能造成以下影响的安全威胁：

- 干扰产品运行（可用性）
- 修改信息（完整性）
- 公开机密信息（保密性）

IFE/EIFE 接口与 IFE 服务器之间的安全功能比较

下表提供了以下固件版本的可用安全功能之间的比较：

- 固件版本为 004.•••.••• 和 005.•••.••• 的 IFE/EIFE 接口
- 固件版本为 003.•••.••• 的 IFE 服务器
- 固件版本为 005.•••.••• 的 IFE 服务器

Schneider Electric 建议您更新 IFE/EIFE 接口和 IFE 服务器 的固件版本，以便获得最新功能。

功能	可用性			可用功能的缺省状态
	EIFE 接口 (LV851001) IFE 接口 (LV434001)	IFE 服务器 (LV434002)（固件版本 003.•••.•••）	IFE 服务器 (LV434002)（固件版本 005.•••.•••）	
HTTP	是	是	是	已启用
HTTPS	是	否	是	已启用
FTP 服务器	是	是	是	已禁用
FTP 客户端	是	是	是	已禁用
FTPS	是	否	是	已启用
NTP	是	否	是	已禁用
SNTP	否	是	否	已禁用
RSTP	是	否	是	已禁用
Modbus TCP	是	是	是	已启用
Modbus Secure	是	否	是	已禁用
RBAC	是	否	是	已启用
IEC 61850	是	否	是	已禁用
Syslog	是	否	是	已启用
SMTP	是	是	是	已禁用

功能	可用性			可用功能的缺省状态
	EIFE 接口 (LV851001) **IFE 接口 (LV434001)**	**IFE 服务器 (LV434002)** （**固件版本 003.•••.•••**）	**IFE 服务器 (LV434002)** （**固件版本 005.•••.•••**）	
IPv6 支持和 DPWS 发现	是	否	是	已启用
SNMP	是	是	是	已禁用
升级固件的时间	大约 4 分钟	大约 16 分钟	大约 4 分钟	–

系统设计、规划和安装的网络安全建议

此部分内容

概述

本部分提供了在设计、规划和安装包含 MasterPacT、ComPacT 和 PowerPacT 智能模块单元 (IMU) 的运营技术 (OT) 网络期间应考虑的重要信息。本部分中的建议和指导有助于打造安全的运行环境。

识别和保护敏感且关键的信息和操作

概述

规划和设计运营技术网络时，必须识别对操作有着重要影响或者敏感的信息。一旦识别，就必须保护这些信息。

一般原则：

- 关键信息包括可通过 MasterPacT、ComPacT 和 PowerPacT IMU 访问的数据和操作（比如，断路器状态、脱扣或分闸/合闸命令）。
- 敏感信息包括任何可用于访问您的系统和运营技术网络的信息（比如，设备或锁闭室的密码或访问码）。

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和等级。

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、ComPacT 和 PowerPacT 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。

下表总结了通过配有 MicroLogic X 控制单元的 MasterPacT MTZ IMU 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	FDM121 显示屏	NFC	Bluetooth Low Energy technology	USB	Ethernet / Modbus-SL
数据监视	读取	读取	读取	读取	读取	读取
保护设置	读/写	读取	读取	读/写	读/写	读/写
其他设置	读/写	读取	读取	读/写	读/写	读/写
分闸/合闸/复位	否	是	否	是	是	是

下表总结了通过配有 MicroLogic Active 控制单元的 MasterPacT MTZ IMU 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 Active HMI	FDM121 显示屏	NFC	USB	Zigbee	Ethernet / Modbus-SL
数据监视	读取	读取	读取	读取	读取	读取
保护设置	读/写	读取	读取	读/写	否	读取
其他设置	读/写	读取	读取	读/写	读取	读取
分闸/合闸/复位	否	是，仅在 Auto Local control mode 下	否	是	否	是，仅在 Auto Remote control mode 下

下表总结了通过 MasterPacT NT/NW、ComPacT NS 及 PowerPacT P 型和 R 型 IMU 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 HMI	FDM121 显示屏	测试端口	Ethernet / Modbus-SL
数据监视	读取	读取	读取	读取
保护设置	读/写	读取	读/写	读/写
其他设置	读/写	读取	读/写	读/写
分闸/合闸/复位	否	是	是	是

下表总结了通过 ComPacT NSX 及 PowerPacT H、J 和 L型 IMU 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 HMI	FDM121 显示屏	测试端口	Ethernet / Modbus-SL
数据监视	读取	读取	读取	读取
保护设置	读/写	读取	读/写	读/写
其他设置	读/写	读取	读/写	读/写
分闸/合闸/复位	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, 30 页或远程访问, 43 页的相关建议。

设计密码策略

概述

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 脱扣单元或控制单元的 MasterPacT、ComPacT 和 PowerPacT 断路器，则在以下情形下需要使用密码：

- 对 MicroLogic 控制单元执行入侵性命令，无论在哪种访问模式（通过 Modbus-TCP / Modbus-SL、USB 连接或 Bluetooth 无线技术）下
- 对 MicroLogic 脱扣单元执行入侵性命令，无论在哪种访问模式（通过 Modbus-TCP / Modbus-SL、FDM121 显示屏 或测试端口）下
- 登录到运行 EcoStruxure Power Commission软件的 PC
- 登录到 IFE 和 EIFE 接口网页
- 登录到 IFE 服务器网页
- 通过EcoStruxure Power Commission 软件从 MasterPacT MTZ IMU 登录 IFE 和 EIFE 界面以及 IFE 服务器网页
- 登录到 FTPS 服务器，对 IFE 和 EIFE 接口执行 IEC 61850 配置，并从 MasterPacT MTZ 登录到 IFE 服务器

有关密码策略的网络安全建议

⚠警告

系统可用性、完整性和保密性的潜在危害

首次使用时，更改默认密码，以有助于防止擅自访问设备设置、控件和信息。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

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
- 使用密码保险箱管理访问密码
- 禁止重新使用旧密码
- 定期就密码的相关最佳实践对用户给与提醒

如要保护系统，至少应该：

- 强制使用强密码
- 设置长度至少为 10 个字符的密码
- 定期修改密码

所有用户必须知悉密码的相关最佳实践。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

用于 MicroLogic Active 关键设置和控制的密码

通过 EcoStruxure Power Device 应用 或 EcoStruxure Power Commission 软件访问 MicroLogic Active 控制单元时，任何改变带 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器行为的入侵性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 Active 密码。

为 MicroLogic Active 控制单元定义了单一用户帐户和密码。

当通过 EcoStruxure Power Device 应用 或 EcoStruxure Power Commission 软件连接时，会提示用户提供此密码。

密码由 8 到 32 个 ASCII 字符组成，并有以下限制：

- 仅允许 ASCII [32-126] 字符
- 至少一个大写字母
- 至少一个小写字母
- 不得包含用户名
- 必须与先前密码不同

首次安装配有 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器时必须使用 EcoStruxure Power Commission 软件更改缺省密码，且在首次安装后必须定期更改。使用密码保险箱存储密码。这些密码只能被数量有限的可信用户共享。视情况遵循密码策略建议。

重要:

- 从 FDM121 显示器连接时，只允许在 Auto Local control mode 中执行入侵性命令。
- 从远程监控界面连接时，只允许在 Auto Remote control mode 中执行入侵性命令。
- 不允许在 Manual control mode 中执行入侵性命令。

用于其他 MicroLogic 关键设置和控制的密码

通过通讯接口访问 MicroLogic 脱扣单元或控制单元时，任何改变 MasterPacT、ComPacT 和 PowerPacT 断路器行为的入侵性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 密码。

为 MicroLogic 脱扣单元或控制单元定义了四个密码，以下四种用户类型各一个：

- Administrator
- Services
- Engineer
- Operator

有关用户类型的更多信息，请参阅 MicroLogic 用户指南, 8 页。

当通过 EcoStruxure Power Device 应用 或 EcoStruxure Power Commission 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

首次安装 MasterPacT、ComPacT 和 PowerPacT 断路器时必须使用 EcoStruxure Power Commission 软件更改缺省密码，且在首次安装后，必须定期更改密码。使

用密码保险箱存储密码。这些密码只能被数量有限的可信用户共享。视情况遵循密码策略建议。

在通过 IFE 或 EIFE 接口或 IFE 服务器远程访问 MicroLogic 控制单元时所用的密码

在 MasterPacT MTZ IMU 内，当通过以下方式建立连接时，通过基于角色的访问控制 (RBAC) 机制来检查对 MicroLogic X 或 MicroLogic Active 控制单元的访问：

- EcoStruxure Power Commission 软件（藉由以太网）
- IFE 接口或 IFE 服务器 网页
- EIFE 接口网页
- 用于 IFE 和 EIFE 接口的 FTPS 服务器，以及 IFE 服务器。

有关 RBAC 机制的更多信息，请参阅 用于 *IFE* 或 *EIFE* 接口网页以及 *IFE* 或 *EIFE FTPS* 服务器的密码, 25 页。

在通过 IFE 接口或 IFE 服务器远程访问 ComPacT NSX 脱扣单元时所用的密码

在配备有 MicroLogic 5、6 或 7 脱扣单元的 ComPacT NSX IMU 内，当通过以下方式建立连接时，通过基于角色的访问控制 (RBAC) 机制来检查对 MicroLogic 脱扣单元的访问：

- EcoStruxure Power Commission 软件（藉由以太网）
- IFE 接口或 IFE 服务器 网页
- 用于 IFE 接口 的 FTPS 服务器，或者 IFE 服务器。

有关 RBAC 机制的更多信息，请参阅 用于 *IFE* 或 *EIFE* 接口网页以及 *IFE* 或 *EIFE FTPS* 服务器的密码, 25 页。

联网 PC 的密码和用户 ID

运行 EcoStruxure Power Commission 软件或者通过任何其他方式（比如，IFE 网页或 SCADA）访问 MicroLogic 脱扣单元或控制单元的 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。

视情况遵循密码策略建议。

用于 IFE/EIFE 接口或 IFE 服务器（带固件版本 005.•••.•••）网页和 FTPS 服务器的密码

对 IFE 接口网页、EIFE 接口网页、IFE 服务器 网页、用于 IFE 和 EIFE 接口的 FTPS 服务器、以及 IFE 服务器的访问由基于角色的访问控制 (RBAC) 机制来检查。

利用 RBAC，可为用户指定定义功能访问权限的角色。

系统的安全管理员列出系统用户，并为每个用户指定角色。

安全管理员可以通过以下方式管理 IFE 或 EIFE 接口的用户或 IFE 服务器的用户：

- 在 IFE 或 EIFE 接口或 IFE 服务器网页上
- 利用 EcoStruxure Cybersecurity Admin Expert (CAE) 软件

安全管理员可以使用 CAE 软件定义系统的安全策略。

此安全策略适用于兼容 CAE 软件的所有系统元素。如果是低压系统，它适用于系统中的 IFE 和 EIFE 接口以及 IFE 服务器。

安全管理员可以使用 CAE 软件设置安全策略的以下参数：

- 最短不活动时长。在用户不执行任何操作的时长达到该时长后，IFE 或 EIFE 接口网页锁定。用户必须重新输入密码，才可将其解锁。
- 最大登录尝试次数
- 锁定时长

有关更多信息，请参阅 CAE_EN_UM_B4.1 *EcoStruxure Cybersecurity Admin Expert User Guide*。

用于 IFE 服务器（带固件版本 003.•••.•••）网页的密码

对于固件版本为 003.•••.••• 的 IFE 服务器 服务器，IFE 服务器网页的每个用户都拥有个人用户 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 服务器网页，且必须视情况遵循密码策略建议。

设计 PIN 码策略

概述

在配有 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器环境中，可通过 PIN 码保护对 MicroLogic Active HMI 上的数据的本地访问。

有关 PIN 码策略的网络安全建议

⚠警告

系统可用性、完整性和保密性面临的潜在威胁

首次使用时，更改缺省 PIN 码，有助于防止擅自访问设备设置、控件和信息。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

PIN 码策略是网络安全策略的主要元素之一。良好的 PIN 码策略包括：

- 避免使用容易猜测的 PIN 码，例如生日、重复数字或数字序列
- 定期更改 PIN 码
- 使用密码保险箱管理访问 PIN 码
- 禁止重复使用旧 PIN 码
- 定期就 PIN 码的相关最佳实践对用户给与提醒

如要保护系统，至少应该：

- 强制使用强 PIN 码
- 定期更改 PIN 码

所有用户必须知悉关于 PIN 码的最佳实践。其中包括：

- 不共享个人 PIN 码
- 在输入 PIN 代码期间不显示 PIN 码
- 不通过电子邮件或任何其他方式传送 PIN 码
- 不将 PIN 码保存在 PC 或其他设备上

用于 MicroLogic Active 关键设置和控制的 PIN 码

访问 MicroLogic Active HMI 上的受保护参数时，系统会提示您创建帐户并设置 PIN 码。然后，每次访问受保护参数时，都会提示您输入该 PIN 码。

缺省情况下，PIN 码与 SecurityAdmin 帐户关联。您可以通过 EcoStruxure Power Commission 软件更改此帐户名。

下列操作可受 PIN 码保护：

- HMI PIN 码修改
- 保护功能设置
- 保护功能测试
- 日期和时间修改
- 控制模式修改
- 替换 MicroLogic Active 设置

PIN 码必须由 6 位数字组成，从 0 到 9。

有关创建 PIN 码的详细信息，请参阅 *MasterPacT MTZ - MicroLogic Active* 控制单元 - 用户指南, 8 页。

培训

概述

员工认知和培训是任何网络安全策略的极重要基础。您必须确保有权对您系统中的 OT 通讯网络进行访问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：

- 不透露敏感性信息，如设备或锁闭室的密码或访问码
- 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 无线技术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 *How Can I Reduce Vulnerability to Cyber Attacks?*。

本地访问的网络安全建议

此部分内容

概述

本部分列出了 MasterPacT、ComPacT 和 PowerPacT 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。

MasterPacT、ComPacT 和 PowerPacT 断路器本地访问限制

概述

MasterPacT、ComPacT 和 PowerPacT 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、ComPacT 和 PowerPacT 断路器本地访问

对 MasterPacT、ComPacT 和 PowerPacT 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、ComPacT 和 PowerPacT 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 HMI，从而发生通过 HMI 更改设置的风险
- 未授权访问无线 Bluetooth 通讯，从而发生通过 EcoStruxure Power Device 应用 更改设置的风险
- 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 控制单元上的 USB 端口进行连接，从而发生通过 EcoStruxure Power Commission 软件或带 EcoStruxure Power Device 应用 的智能手机更改设置的风险
- 在未经授权的情况下通过 MicroLogic 脱扣单元上的测试端口进行连接，从而发生通过 EcoStruxure Power Commission 软件或利用服务接口或 USB 维护接口修改设置的风险
- 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 脱扣单元或控制单元的 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、ComPacT 和 PowerPacT 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 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断路器的机箱的人员都能够访问 MicroLogic HMI 。

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

通过 MicroLogic Active HMI 访问的保护建议

MicroLogic Active HMI 可以启用 PIN 码保护。建议在 MicroLogic Active 控制单元上使用 PIN 码保护。有关 PIN 码保护的更多信息，请参阅设计 PIN 码策略, 27 页。

为了提高安全性，您必须：

- 对 MicroLogic Active HMI 的保护盖进行铅封。
- 盖上MicroLogic Active USB 端口的保护盖。
- 将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。

有关断路器访问保护的更多信息，请参阅实施限制访问策略, 31 页。

通过其他 MicroLogic HMI 访问的保护建议

下列断路器中的 MicroLogic HMI 未使用 PIN 码或密码保护：

- 配备有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic 脱扣单元的 MasterPacT NT/NW 断路器
- ComPacT 断路器
- PowerPacT 断路器

此外，并非所有 MicroLogic HMI 都能被物理地锁定以防止有人访问显示屏幕。因此，如要保护对 HMI 的访问，您必须：

- 对 MicroLogic HMI 的保护盖进行铅封（如果此盖能够铅封）。
- 将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。

有关断路器访问保护的更多信息，请参阅实施限制访问策略, 31 页。

锁定保护设置

下列断路器的保护设置可以进行物理锁定，以免它们遭到通过 HMI 进行的本地更改：

- 配备有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic 脱扣单元的 MasterPacT NT/NW 断路器
- ComPacT 断路器
- PowerPacT 断路器

缺省情况下，在这些断路器中允许从 HMI 更改保护设置。如果不希望使用此功能，建议您锁定保护设置。有关更多信息，请参阅 MicroLogic 用户指南, 8 页

通过 NFC (MasterPacT MTZ) 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 或 MicroLogic Active 控制单元未通电，也可以将诊断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 或 MicroLogic Active 控制单元建立 NFC 无线连接的前提条件是：

- 必须能够物理上进入 MasterPacT MTZ 断路器所在的房间以及设备柜。
- 智能手机上必须安装有 EcoStruxure Power Device 应用。
- 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 或 MicroLogic Active 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 或 MicroLogic Active 用户指南, 8 页。

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，使得只有授权人员才能够触及 MicroLogic X 或 MicroLogic Active 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, 31 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 或 MicroLogic Active 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）。
- 即便提示输入配对代码，也不要输入，因为 NFC 连接不需要输入配对代码。

EcoStruxure Power Device 应用 使用建议

如要限制通过运行 EcoStruxure Power Device 应用 的智能手机对 MicroLogic X 或 MicroLogic Active 控制单元的访问，建议仅使用官方 Schneider Electric EcoStruxure Power Device 应用 来连接 MasterPacT MTZ 断路器。

智能手机使用建议

如要限制智能手机对 MicroLogic X 或 MicroLogic Active 控制单元的访问，建议：

- 确保安装有 EcoStruxure Power Device 应用 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 EcoStruxure Power Device 应用 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 或 MicroLogic Active 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）。
- 切勿在智能手机上存储敏感信息。

通过 Bluetooth® 无线技术 (MasterPacT MTZ) 访问的保护建议

通过 Bluetooth 无线技术访问功能

注意

意外操作风险

- 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 Bluetooth Low Energy 无线技术，您可以通过运行 EcoStruxure Power Device 应用 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 无线技术传输的数据利用 AES 128 位加密算法加密。

注: Bluetooth 无线技术不可用于 MicroLogic Active 控制单元。

建立 Bluetooth 连接的前提条件

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

- MicroLogic X 控制单元必须通电。
- 必须在 MicroLogic X 控制单元上启用 Bluetooth 功能。
- 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 EcoStruxure Power Device 应用。
- 智能手机必须支持 Bluetooth Low Energy 无线技术（4.0 或以上）。
- 必须能够触及 MicroLogic X 控制单元，以便通过按下激活按钮来激活 Bluetooth 功能，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）。
- 必须输入由 MicroLogic X 控制单元随机生成且在 MicroLogic X HMI 上显示的 6 位配对码。

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 *MasterPacT MTZ - MicroLogic X 控制单元 - 用户指南*, 8 页。

通过 Bluetooth 无线技术访问的一般保护建议

如要保护可通过 Bluetooth 无线技术进行的功能访问，建议：

- 将 MasterPacT MTZ 断路器安装在锁闭的区域，使得只有授权人员才能够触及 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, 31 页。

有关 Bluetooth 无线技术的使用建议

Bluetooth 功能的实现符合 NIST Special Publication 800-121（修订版 1）。然而，如要保护可通过 Bluetooth 无线技术进行的功能访问，建议：

- 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。

  有关禁用 Bluetooth 功能的详细程序，请参阅 *MasterPacT MTZ - MicroLogic X 控制单元 - 用户指南*，8 页。
- 将 Bluetooth 功能断开定时器设置为 5 分钟。
- 除非正在启动 Bluetooth 连接，否则不得通过 MicroLogic X 控制单元正面的激活按钮激活 Bluetooth 功能。Bluetooth 功能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。
- 只有在必要时以及在安全的区域中，才能执行配对。
- 即使意外地发现提示输入配对码，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。

EcoStruxure Power Device 应用 使用建议

如要限制通过运行 EcoStruxure Power Device 应用 的智能手机对 MicroLogic X 控制单元的访问，建议仅使用官方 Schneider Electric EcoStruxure Power Device 应用 来连接 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 EcoStruxure Power Device 应用 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 EcoStruxure Power Device 应用 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。
- 切勿在智能手机上存储敏感信息。

通过 USB 端口 (MasterPacT MTZ) 访问 MicroLogic 控制单元的保护建议

可通过 USB 端口访问的功能

MicroLogic X 或 MicroLogic Active 控制单元的功能可以通过以下方式来访问：

- 将运行 EcoStruxure Power Commission 软件的 PC 连接到控制单元的 USB 端口。
- 通过 USB OTG 适配器将运行 EcoStruxure Power Device 应用 的智能手机连接到控制单元的 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。

与 MicroLogic X 控制单元建立 USB 或 USB OTG 连接的先决条件

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带 MicroLogic X 控制单元的 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 EcoStruxure Power Commission 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 EcoStruxure Power Device 应用。

与 MicroLogic Active 控制单元建立 USB 或 USB OTG 连接的先决条件

与 MicroLogic Active 控制单元建立 USB 连接的前提条件是：

- 必须能够物理上进入带 MicroLogic Active 的 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 USB-C 连接器的 USB 电缆来将 PC 连接到 MicroLogic Active 控制单元上的 USB-C 端口。
  - 您的 PC 上必须运行有 EcoStruxure Power Commission 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 USB-C 连接器的 USB 电缆来将智能手机连接到 MicroLogic Active 控制单元上的 USB-C 端口。

    注: 您可以使用 USB-C 至 USB-C 电缆（而不是 OTG 适配器）将智能手机连接到 MicroLogic Active 控制单元。
  - 您的智能手机上必须运行有 EcoStruxure Power Device 应用。

通过 USB 端口访问的一般保护建议

如要保护可通过 MicroLogic X 或 MicroLogic Active 控制单元上的 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，使得只有授权人员才能够触及 MicroLogic X 或 MicroLogic Active 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, 31 页限制建议。

运行 EcoStruxure Power Commission 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 USB 端口的 PC 进行的 MicroLogic X 或 MicroLogic Active 脱扣单元访问，建议：

- PC 未使用时，保持安全锁闭隔离。
- 确保运行 EcoStruxure Power Commission 软件的 PC 需要用户登陆和密码。
- 强制使用强密码, 23 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 EcoStruxure Power Commission 软件的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

运行 EcoStruxure Power Device 应用 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 USB 端口的智能手机进行的 MicroLogic X 或 MicroLogic Active 脱扣单元访问，建议：

- 确保运行 EcoStruxure Power Device 应用 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 EcoStruxure Power Device 应用 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 或 MicroLogic Active 控制单元进行 USB OTG 连接期间，断开智能手机的网络连接。
- 切勿在智能手机上存储敏感信息。

IEC 61850 配置建议

对于 MicroLogic X 控制单元，使用 FTPS 协议将 IEC 61850 配置文件上传到 IFE 或 EIFE 接口或 IFE 服务器。

通过测试端口访问 MicroLogic 脱扣单元的保护建议

经由 USB 维护接口通过测试端口访问功能

可以将运行 EcoStruxure Power Commission 软件的 PC 通过 USB 维护接口连接到脱扣单元的测试端口，由此访问 MicroLogic 脱扣单元的功能。

USB 维护接口让您能够将运行 EcoStruxure Power Commission 软件的 PC 连接到脱扣单元的测试端口，从而对 MicroLogic 脱扣单元执行一系列的检查、测试和调整。

USB 维护接口与下列设备兼容：

- ComPacT NSX 断路器
- PowerPacT H 、J 和 L 型断路器

经由服务维护接口通过测试端口访问功能

可以将运行 EcoStruxure Power Commission 软件的 PC 通过服务接口连接到脱扣单元的测试端口，由此访问 MicroLogic 脱扣单元的功能。

服务接口让您能够将运行 EcoStruxure Power Commission 软件的 PC 连接到脱扣单元的测试端口，从而对 MicroLogic 脱扣单元执行一系列的检查、测试和调整。

服务接口与下列设备兼容：

- MasterPacT NT/NW™ 断路器
- EasyPact™ MVS 断路器
- ComPacT NS 断路器
- PowerPacT P 型和 R 型断路器
- ComPacT NSX 断路器
- PowerPacT H 型、J 型和 L 型断路器

通过测试端口访问的一般保护建议

如要保护可通过 MicroLogic 脱扣单元上的测试端口进行的功能访问，建议：

- 将 MasterPacT NT/NW、ComPacT 或 PowerPacT 断路器安装在锁闭的区域，使得只有授权人员才能够触及 MicroLogic 脱扣单元。
- 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、ComPacT 和 PowerPacT 断路器本地访问, 31 页限制建议。

运行 EcoStruxure Power Commission 软件的 PC 的相关建议

如要保护通过本地连接到脱扣单元正面测试端口的 PC 进行的 MicroLogic 脱扣单元访问，建议：

- PC 未使用时，保持安全锁闭隔离。
- 确保运行 EcoStruxure Power Commission 软件的 PC 需要用户登陆和密码。

- 强制使用强密码, 23 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 EcoStruxure Power Commission 软件的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

通过 FDM121 显示屏 访问 MicroLogic 控制或脱扣单元的保护建议

可通过 FDM121 显示屏 访问的功能

可以通过连接到 IMU 的 FDM121 显示屏 访问 MicroLogic 控制或脱扣单元的功能。

FDM121 显示屏 显示来自 IMU 的测量结果、报警和操作支持数据。FDM121 显示屏 可用于控制：

- 配有电动机构的断路器
- 由 IO 模块执行的预定义应用程序。

FDM121 显示屏 与下列设备兼容：

- 配备有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器
- MasterPacT NT/NW 断路器
- ComPacT NS 断路器
- PowerPacT P 型和 R 型断路器
- ComPacT NSX 断路器
- PowerPacT H 、J 和 L 型断路器

通过 FDM121 显示屏 访问的一般保护建议

为了保护可通过 FDM121 显示屏 进行的功能访问，建议：

- 将 MasterPacT MTZ、ComPacT 或 PowerPacT 断路器及相关的 FDM121 显示屏 安装在锁闭的区域，使得只有授权人员才能够触及 FDM121 显示屏
- 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、ComPacT 或 PowerPacT 断路器本地访问限制, 31 页建议。

通过 FDM121 显示屏 访问 MicroLogic Active 控制单元的保护建议

只有在 Auto Local control mode 中才允许通过 FDM121 显示屏 访问 MicroLogic Active 控制单元。建议将控制模式设置为 Manual，以避免入侵性命令。

远程访问的网络安全建议

此部分内容

概述

远程访问可通过以下断路器进行：

- 配备有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器
- 配备有 MicroLogic 脱扣单元的 MasterPacT NT/NW 断路器
- ComPacT 断路器
- PowerPacT 断路器

本部分列出了这些断路器的远程访问路径，另外还提供了保护这些访问路径的建议。这些都是设备运行要考虑的重要因素。

MasterPacT、ComPacT 和 PowerPacT 断路器远程访问限制

概述

MasterPacT、ComPacT 和 PowerPacT 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、ComPacT 和 PowerPacT 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、ComPacT 和 PowerPacT 断路器的远程访问。

必须控制系统的远程访问，因为通过以下通讯途径的远程访问能够提供对您系统的全面控制：

- EcoStruxure Power Commission 软件（通过 Ethernet 连接，使用 IFE、EIFE 或 IFM 接口，或 IFE 服务器，或 BSCM Modbus SL/ULP 模块）
- EcoStruxure Power Commission 软件（通过 Modbus-SL，使用 IFM 接口或 BSCM Modbus SL/ULP 模块）
- IFE 或 EIFE 网页（通过 Ethernet 连接，使用 IFE 或 EIFE 接口，或 IFE 服务器）

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, 14 页访问系统
- 通过每个访问途径可获得的信息和控制, 22 页

支持的协议

IFE 和 EIFE 接口以及 IFE 服务器支持以下通讯协议：

- HTTPS，用于通过嵌入式网页执行配置
- Modbus TCP/IP，用于与其他 OT 设备通讯
- Modbus TCP over TLS
- DHCP，用于网络 IP 寻址
- DNS，用于网络名称解析
- SNTP，用于时间同步
- DPWS，用于网络传输
- SMTPS，用于发送电子邮件
- FTPS，用于 IEC 61850 配置和事件通知
- IEC 61850，用于与子站中的设备和系统通讯

IFM 接口支持 Modbus-SL 通讯协议。

BSCM Modbus SL/ULP 模块 支持 Modbus-SL 通讯协议。

MasterPacT MTZ 应用程序支持以下通讯协议：

- Bluetooth 无线技术，用于与 EcoStruxure Power Device 应用 通讯
- NFC，用于下载诊断数据

启用和禁用 MasterPacT、ComPacT 和 PowerPacT 断路器远程控制

MasterPacT、ComPacT 和 PowerPacT 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、ComPacT 和 PowerPacT 断路器的远程控制，则强烈建议使用 IFE 或 EIFE 接口、IFE 服务器或 IFM 接口禁用远程控制。缺省情况下，远程控制处于启用状态。

如果不需要对带 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器进行远程控制，强烈建议将控制模式设置为 Manual。缺省情况下，MicroLogic Active 控制模式为 Manual。

如果使用的是 IFE 接口或 IFE 服务器，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命令。

如果使用的是 EIFE 接口，则将运行 EcoStruxure Power Commission 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。

对于 BSCM Modbus SL/ULP 模块，将运行 EcoStruxure Power Commission 软件的 PC 连接到 Modbus SL 集线器并使用远程挂锁参数来启用或禁用通过 Modbus-SL 网络发送的远程控制命令。

锁定保护设置 (MasterPacT MTZ)

您可以锁定配有 MicroLogic X 控制单元的 MasterPacT MTZ 断路器的保护设置，以免它们遭到远程更改。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。有关更多信息，请参阅 *MasterPacT MTZ - MicroLogic X* 控制单元 - 用户指南, 8 页。

注: 带 MicroLogic Active 控制单元的 MasterPacT MTZ 断路器不支持远程修改保护设置。

禁用未使用的 IP 网络服务

可以从 IFE 或 EIFE 接口或 IFE 服务器网页禁用 IFE 或 EIFE 接口或者 IFE 服务器的通讯端口。

我们建议：

- 禁用 IFE 或 EIFE 接口的未用通讯端口。
- 使用 HTTPS 服务（而不是 HTTP）访问 IFE 或 EIFE 接口网页。
- 对于 MasterPacT MTZ MicroLogic 控制单元和 ComPacT NSX MicroLogic 5、6 或 7 脱扣单元，请使用安全调试（在 IFE 或 EIFE 接口网页中提供）访问 EPC 软件。

使用访问控制列表 (ACL)

在必须执行远程控制时，建议利用 IFE 和 EIFE 接口或者 IFE 服务器的 IP 过滤能力来列出有权与 IMU 通讯的应用程序（如 SCADA）的 IP 地址。经授权的应用程序的列表即为访问控制列表 (ACL)。

将 OT 网络与企业网络分离

概述

在设计和实施运营技术网络时，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、ComPacT 和 PowerPacT 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) 解决方案
- 实施安全策略和培训计划
- 制定事件响应程序

由专业化组织（比如，NIST）和标准制定机构（比如，ISO、IEC/IEEE）发布并更新运营技术网络设计指南，并使运营技术网络与企业内联网分离。请根据这些出版物来处理上述几点。

除了上述预防措施外，还必须遵循中提供的隔离网络的一般指南和建议 *How Can I Reduce Vulnerability to Cyber Attacks?* 。

通过 Ethernet 远程访问 MicroLogic 脱扣单元或控制单元的保护建议

可通过 Ethernet 访问的功能

当运行监控软件（SCADA、EcoStruxure Power Commission 软件）的 PC 已连接到 Ethernet (Modbus/TCP) 网络时，MicroLogic 脱扣单元或控制单元的功能在以下情况下能够被访问：

- MasterPacT、ComPacT 和 PowerPacT 断路器通过 IFE 接口或 IFE 服务器连接。
- MasterPacT MTZ 断路器通过 EIFE 接口连接。
- MasterPacT、ComPacT 和 PowerPacT 断路器通过堆叠到 IFE 服务器的 IFM 接口连接。
- ComPacT NSX 以及 PowerPacT H、J 和 L 型断路器通过 BSCM Modbus SL/ULP 模块 在 Modbus 模式下藉由 Modbus SL 集线器连接到 IFE 服务器。

建立 Ethernet 连接的前提条件

与 MicroLogic 脱扣单元或控制单元建立 Ethernet 连接的前提条件是：

- MicroLogic 脱扣单元或控制单元必须通电。
- MicroLogic 脱扣单元或控制单元必须通过以下方式之一连接到 Ethernet 网络：
  - IFE 或 EIFE 接口
  - IFE 服务器
  - 堆叠到 IFE 服务器的 IFM 接口
  - BSCM Modbus SL/ULP 模块，在 Modbus 模式下，此模块通过 Modbus SL 集线器连接到 IFE 服务器
- 您的 PC 或其他设备（比如，FDM128 显示器或 PLC）必须运行有监控软件（SCADA、EcoStruxure Power Commission）并且连接到允许远程访问的 Ethernet 网络
- 您的 PC 上运行的 Web 浏览器必须连接到允许访问 IFE 或 EIFE 网页的 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：
  - IFE 和 EIFE 接口网页
  - IFE 服务器网页
  - 用于 IFE 和 EIFE 接口的 FTPS 服务器，以及 IFE 服务器
  - EcoStruxure Power Commission 软件 通过 IFE 和 EIFE 接口以及 IFE 服务器连接
- 您必须拥有具备相应访问权限的用户 ID 和密码来登录到 EcoStruxure Power Commission 软件中

连接到 Ethernet 的 PC 的相关建议

如要保护联网 PC 对 MicroLogic 脱扣单元或控制单元的访问，建议：

- PC 未使用时，保持安全锁闭隔离。
- 确保能够使用使用 Ethernet 访问 MicroLogic 脱扣单元或控制单元的 PC（例如，通过 IFE 或 EIFE 接口网页、IFE 服务器网页或者 SCADA）需要用户登录名和密码。
- 强制使用强密码, 25 页。

- 利用 IFE 和 EIFE 接口以及 IFE 服务器的 IP 过滤能力，仅允许与所选择的远程 IP 地址通讯。
- 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 脱扣单元或控制单元的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

除了上述预防措施外，还必须遵循中提供的用于保护您安装的一般指南和建议*How Can I Reduce Vulnerability to Cyber Attacks?*。

有关机器对机器通讯的建议

对于支持 Modbus TCP over TLS 的系统，在 IFE 或 EIFE 接口或 IFE 服务器 网页上激活 TLS 连接安全模式。

机器到机器安全通讯要求使用连接到 IFE 或 EIFE 接口或 IFE 服务器的组件来支持安全 Modbus 通讯。

安全日志建议

为确保定期下载安全日志，请使用：

- 自动日志导出功能（藉由来自 IFE 或 EIFE 接口的 IFE服务器的 Syslog 服务）。
- 从 IFE 或 EIFE 接口或 IFE 服务器以 CSV 格式手动导出日志。

通过 Modbus-SL 远程访问 MicroLogic 脱扣单元或控制单元的保护建议

可通过 Modbus-SL 访问的功能

当运行监控软件 (SCADA) 的 PC 已连接到 Modbus-SL 网络时，MicroLogic 脱扣单元或控制单元的功能在以下情况下能够被访问：

- MasterPacT、ComPacT 和 PowerPacT 断路器连接到 IFM 接口。
- 在 Modbus 模式下，ComPacT NSX 和 PowerPacT H-、J- 或 L- 型断路器连接到 BSCM Modbus SL/ULP 模块。

建立 Modbus-SL 连接的前提条件

与 MicroLogic 脱扣单元或控制单元建立 Modbus-SL 连接的前提条件是：

- MicroLogic 脱扣单元或控制单元必须通电。
- 在 Modbus 模式下，MicroLogic 脱扣单元或控制单元必须连接到 IFM 接口或 BSCM Modbus SL/ULP 模块。
- 您的 PC 或其他设备（比如，PLC）必须运行有监控软件 (SCADA) 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 EcoStruxure Power Commission 软件中。

连接到 Modbus-SL 的 PC 的相关建议

如要保护联网 PC 对 MicroLogic 脱扣单元或控制单元的访问，建议：

- PC 未使用时，保持安全锁闭隔离。
- 确保能够使用使用 Modbus-SL 访问 MicroLogic 脱扣单元或控制单元的 PC（例如，通过 SCADA）需要用户登录名和密码。
- 强制使用强密码, 25 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 脱扣单元或控制单元的用户数。
- 保持 PC 的防病毒应用程序为最新版本。

除了上述预防措施外，还必须遵循中提供的用于保护您安装的一般指南和建议*How Can I Reduce Vulnerability to Cyber Attacks?*。

通过 Zigbee 无线技术 (MasterPacT MTZ) 访问的保护建议

Zigbee 版本

MicroLogic Active AP/EP 控制单元已通过 Zigbee 3.0 认证。

通过 Zigbee 无线技术访问功能

使用 Zigbee 无线通讯，您可以从 Panel Server Advanced (PAS800)、Panel Server Universal (PAS600) 或 Panel Server Entry (PAS400) 监视来自 MicroLogic Active AP/EP 控制单元的数据。

通过 Zigbee 无线技术传输的数据利用 AES 128 位加密算法加密。

注: Zigbee 无线技术不可用于 MicroLogic X 控制单元。

建立 Zigbee 连接的前提条件

建立 Zigbee 连接的前提条件为：

- Panel Server 必须打开。
- MicroLogic Active AP/EP 控制单元和 Panel Server 必须相距较近。
- 对于选择性配对，必须提供 Zigbee ID，其显示在 Go2SE 登录页或 MicroLogic Active 显示屏上。

如需详细了解如何建立 Zigbee 连接，请参见 配备 *MicroLogic Active* 控制单元的 *MasterPacT MTZ* 断路器用户指南, 8 页。

通过 Zigbee 无线技术访问的一般保护建议

如要保护可通过 Zigbee 无线技术进行的功能访问，建议：

- 将 MasterPacT MTZ 断路器安装在锁闭的区域，使得只有授权人员才能够触及 MicroLogic Active 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, 31 页。

有关 Zigbee 无线技术的使用建议

Zigbee 无线通讯极易受到操作环境中未经授权的无线电发射的干扰。如要保护可通过无线 Zigbee 进行的功能访问，建议：

- MicroLogic Active AP/EP 控制单元未连接到恶意网络。
- 定期检查 Zigbee 网络，确保所有设备均有效。
- 如果任何设备无效，将修复 Zigbee 网络。
- 建议在阻隔了强大的无线电发射器的地方，如管理室，调试 Zigbee 无线设备。

- 只有在必要时以及在安全的区域中，才能执行配对。

Panel Server 使用建议

请参阅 DOCA0172•• *EcoStruxure Panel Server* - 用户指南, 8 页 的“网络安全建议”章节。

固件更新和 Digital Modules 的网络安全建议

此部分内容

安装固件更新

概述

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、ComPacT 和 PowerPacT IMU 组件（即，MicroLogic X 或 MicroLogic Active 控制单元、IFE 服务器、IFE、EIFE 或 IFM 接口、BSCM Modbus SL/ULP、BCIM 或 IO 模块和 FDM121 显示屏）的完整性和真实性，Schneider Electric 原始固件带有数字签名。

利用 EcoStruxure Power Commission 软件更新固件。必须安装最新版的 EcoStruxure Power Commission 软件。利用 EcoStruxure Power Commission 软件，通过固件菜单更新固件。

有关固件更新的网络安全建议

⚠警告

意外操作风险

- 一旦接收到更新通知，便应更新 EcoStruxure Power Commission 软件的版本。
- 利用 EcoStruxure Power Commission 软件的最新版本来更新所有产品的固件。
- 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。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

在为 MasterPacT、ComPacT 和 PowerPacT IMU 的组件安装固件更新时，建议：

- 仅使用最新版的 EcoStruxure Power Commission 软件来下载和安装固件更新。
- 根据操作系统的最新供应商指南，强化运行 EcoStruxure Power Commission 软件的 PC。
- 根据认可的运营技术 (OT) 实践安装更新，比如，在生产系统中安装和部署非生产型环境（如有）之前，先对该非生产型环境进行检验测试。

请参阅相关的固件发行说明, 8 页，查看最新更新是否包含网络安全改善。如包含，则建议更新到此版本。

签名固件

为 MicroLogic X 控制单元、MicroLogic Active 控制单元和 ULP 模块设计的固件通过 Schneider Electric 公钥基础设施 (PKI) 进行了数字签名。数字签名经由 EcoStruxure Power Commission 软件中的公共证书来验证。

通过 EcoStruxure Power Commission 软件将固件上传到设备后，还会自动验证更新包的数字签名。此验证使用各设备中的公共证书进行。

出于安全原因，公共证书会更改。因此，必须检查用于下载和安装固件更新的 EcoStruxure Power Commission 软件是否为最新版本。拥有最新版的 EcoStruxure Power Commission 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，见 Schneider Electric 官网。

利用 EcoStruxure Power Commission 软件更新固件的好处

EcoStruxure Power Commission 软件能够极大地有助于确保固件更新期间运营技术网络的完整性。仅使用最新版的 EcoStruxure Power Commission 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 EcoStruxure Power Commission 软件从 Schneider Electric 官方下载中心将固件包下载到 MicroLogic X 控制单元、MicroLogic Active 控制单元或 ULP 模块时，会自动验证固件包的数字签名。
- 在（利用 EcoStruxure Power Commission 软件，通过 USB 连接或通过 Ethernet 连接）将固件上传到 MicroLogic X 控制单元、MicroLogic Active 控制单元或 ULP 模块时，会自动验证更新包的数字签名。

通过 EcoStruxure Power Commission 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。

有关 MicroLogic 固件更新的详细程序，请参阅 *MicroLogic Trip Units and Control Units - Firmware History*, 8 页。

购买和安装 Digital Modules (MasterPacT MTZ)

概述

Digital Modules 为可选模块，可扩展整个 MicroLogic X 控制单元系列提供的功能。它们可以与断路器一起MasterPacT MTZ按初始订单购买，也可以在日后通过联系客户服务中心(CCC)购买。

为 MicroLogic X 控制单元设计的 Digital Modules 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 EcoStruxure Power Commission 软件安装 Digital Modules。

注: Digital Modules 与 MicroLogic Active 控制单元不兼容。

Digital Modules 安装的网络安全建议

⚠警告

意外操作风险

- 一旦接收到更新通知，便应更新 EcoStruxure Power Commission 软件的版本。
- 利用 EcoStruxure Power Commission 软件的最新版本来更新所有产品的固件。
- 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。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

在为 MicroLogic X 控制单元安装 Digital Modules 时，建议：

- 根据认可的运营技术 (OT) 实践安装 Digital Modules，比如，在生产系统中安装和部署非生产型环境之前，先对该非生产型环境进行检验测试。
- 仅使用最新版的 EcoStruxure Power Commission 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。

只能使用 EcoStruxure Power Commission 软件来安装 MicroLogic X 控制单元的 Digital Modules。

EcoStruxure Power Commission 软件能够极大地有助于确保运营技术网络的完整性。仅使用最新版的 EcoStruxure Power Commission 软件来安装 Digital Modules，因为它是具有以下优点的唯一软件：

- 在通过 USB 连接或 Ethernet 连接使用 EcoStruxure Power Commission 软件更新 IMU 的设备的固件时，会自动验证固件更新的数字签名。
- 在使用 EcoStruxure Power Commission 软件通过 USB 连接将 Digital Module 上传到 MicroLogic X 控制单元时，会自动验证 Digital Module 的数字签名。

通过 EcoStruxure Power Commission 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 DOCA0144EN *MasterPacT MTZ - MicroLogic X Control Unit - Firmware Release Notes* 中的相关详细程序，了解如何下载和安装 Digital Modules。

Schneider Electric Cybersecurity Support Portal

概述

Schneider Electric cybersecurity support portal 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 Cybersecurity Support Portal 上的信息

该支持门户提供以下信息：

- 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

处置或停用网络安全建议

EIFE 和 IFE 接口以及 IFE 服务器包含在调试期间配置的保密信息、当前数据值和日志。例如，此信息可包括密码或测量的功耗。

在废弃 EIFE 或 IFE 接口或者 IFE 服务器之前，必须执行出厂复位。有关更多信息，请参阅界面的相关用户指南。

术语

安全策略:

系统安全策略是在整个受保护的系统中应用的安全设置。安全策略通常涉及标准的使用。它用来定义在所有设备之间共享的任何安全相关配置。

配对代码:

由数字组成的代码，用于在建立 Bluetooth 连接时验证个体的身份。

B

BCIM:

BCIM 模块可实现 MicroLogic Active 控制单元与 ULP 系统内其他 ULP 模块之间的通讯。

Bluetooth Low Energy:

一种能耗较低的无线个域网技术。

BSCM Modbus SL/ULP 模块:

商业型号为 LV434220 的 BSCM Modbus SL/ULP 模块是一个断路器状态控制模块，可以用来通过 Modbus Serial Line 通讯网络或通过 ULP 通讯网络传输数据。

E

EIFE 接口:

可供 MasterPacT MTZ 抽出式断路器选配的嵌入式 Ethernet 接口。利用此模块，可以通过以太网网络访问断路器。EIFE 接口和 EIFE FTPS 服务器的访问授权取决于基于角色的访问控制 (RBAC) 机制。

F

FTP - 文件传输协议:

一种支持通过互联网在计算机之间传输文件的网络协议。

FTPS - 安全文件传输协议:

它是标准文件传输协议 (FTP) 的一种变体，通过安全套接层 (SSL) 或传输层安全 (TLS) 协议连接对传输数据添加安全层
。

H

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。

HTTP - 超文本传输协议:

一种通过万维网处理文件和数据的发送的网络协议。

HTTPS - 安全超文本传输协议:

它是标准 Web 传输协议 (HTTP) 的一种变体，通过安全套接层 (SSL) 或传输层安全 (TLS) 协议连接对传输数据添加安全层。

I

IEC 61850 协议:

一种用于子站中的通讯网络和系统的标准。它是一种标准化通讯方法，基于以太网协议，用于支持集成系统，由多供应商自描述智能电子设备 (IED) 组成。这些系统联网到一起，用于执行实时保护、控制、测量和监测功能。

IFE 接口:

可连接到 MasterPacT、ComPacT 或 PowerPacT 断路器且用于单个断路器的 IFE Ethernet 接口。利用此模块，可以通过以太网网络访问断路器。IFE 接口网页和 IFE FTPS 服务器的访问授权取决于基于角色的访问控制 (RBAC) 机制。

IFE 服务器:

可连接到不止一个 MasterPacT MTZ 断路器的 IFE Ethernet 交换机服务器。利用此模块，可以通过以太网网络访问断路器。

IFM 接口:

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:

内部通讯组件（MicroLogic 脱扣单元或控制单元）和外部 ULP 模块（IO 模块）连接到一个通讯接口的断路器称为智能模块单元 (IMU)。

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:

是指区别于其 OT（运营技术）网络的企业信息系统和信息网络。

L

LAN - 局域网:

是指企业内联网或 IT 网络。

M

Modbus TCP/IP:

一种协议，其在设备与通过 Ethernet 连接提供通讯的 TCP/IP 之间提供客户端/服务器通讯。

N

NFC - Near field communication:

是指一种无线通讯协议。

O

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。

P

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。

R

RBAC - 基于角色的访问控制:

一种基于用户的为实施访问而获授的定义角色来分配不同访问等级的方式。

S

SCADA - Supervisory control and data acquisition:

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。

T

TCP/IP - Transmission control protocol/Internet protocol:

是指一整套用于互联网通讯的协议。

U

ULP 连接:

ULP 是一种快速通讯链路，专用于断路器监视和控制。它将断路器连接到 Ethernet 接口或 IO 模块。ULP 以 1 Mb/s 的速度工作，即插即用。

V

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”。

Z

Zigbee:

符合 Zigbee 标准的无线通讯协议。

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

由于各种标准、规范和设计不时变更，请索取对本出版物中给出的信息的确认。

DOCA0122ZH-11