Modicon 控制器系统

网络安全

用户指南

原始指令翻译

11/2024

EIO0000002004.10

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。

本文档及其内容受适用版权法保护，并且仅供参考使用。未经施耐德电气事先书面许可，不得出于任何目的，以任何形式或方式（电子、机械、影印、录制或其他方式）复制或传播本文档的任何部分。

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 5
开始之前 6
启动与测试 7
操作和调整 7
关于本书 9
简介 16
Schneider Electric 指南 16
如何帮助保护架构 18
系统视图 18
在 Control Expert 中设置密码 19
加强 PC 22
禁用未使用的嵌入式通讯服务 29
限制来自控制网络的数据流（访问控制） 30
设置加密通讯 33
CSPN 安全目标 39
设置网络安全审计（事件记录） 48
Event Log Message Descriptions for Control Expert 55
M580 控制器（固件版本不低于 V4.10）和 BMENOR2200H（固件版本不低于 3.01）的事件日志消息描述 60
M580 控制器（固件版本低于 4.10）、BMENUA0100 和 BMENOR2200H（固件版本低于 3.01）的事件日志消息描述 74
控制识别和身份验证 87
控制授权 91
管理数据完整性检查 94
配置 Control Expert 与 M580 以太网控制器之间的安全工程链路 97
安全连接的相关功能 97
配置安全连接程序 99
运行模式注意事项 101
强制安全性编程兼容性和限制 102
通讯适配器兼容性 103
M580 以太网服务和端口 107

每个系统的网络安全服务 109
网络安全服务 109
Modicon M340 安全服务 115
Modicon M580 安全服务 116
Modicon Quantum 安全服务 116
Modicon X80 安全服务 118
Modicon Premium/Atrium 安全服务 120
Modicon Momentum MDI 安全服务 121
Modicon MC80 安全服务 121
如何使用 EAGLE40 藉由 VPN 保护 M580、M340、Momentum MDI 和 MC80 架构 122
EAGLE40 防火墙 122
前提条件 123
典型架构 124
配置防火墙 124
术语 133
索引 153

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”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。

开始之前

不得将本产品在缺少有效作业点防护的机器上使用。如果机器上缺少有效的作业点防护，则有可能导致机器的操作人员严重受伤。

⚠警告

未加以防护的设备

- 不得将此软件及相关自动化设备用在不具有作业点防护的设备上。
- 在操作期间，不得将手放入机器。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

此自动化设备及相关软件用于控制多种工业过程。根据所需控制功能、所需防护级别、生产方法、异常情况、政府法规等因素的不同，适用于各种应用的自动化设备的类型或型号会有所差异。在某些应用情况下，如果需要后备冗余，则可能需要一个以上的处理器。

只有用户、机器制造商或系统集成商才能清楚知道机器在安装、运行及维护过程中可能出现的各种情况和因素，因此，也只有他们才能确定可以正确使用的自动化设备和相关安全装置及互锁设备。在为特定应用选择自动化和控制设备以及相关软件时，您应参考适用的当地和国家标准及法规。National Safety Council's Accident Prevention Manual（美国全国公认）同样提供有非常有用的信息。

对于包装机等一些应用而言，必须提供作业点防护等额外的操作人员防护。如果操作人员的手部及其他身体部位能够自由进入夹点或其他危险区域内，并且可导致人员严重受伤，则必须提供这种防护。仅凭软件产品自身无法防止操作人员受伤。因此，软件无法被取代，也无法取代作业点防护。

在使用设备之前，确保与作业点防护相关的适当安全设备与机械/电气联锁装置已经安装并且运行。与作业点防护相关的所有联锁装置与安全设备必须与相关自动化设备及软件程序配合使用。

注: 关于协调用于作业点防护的安全设备与机械/电气联锁装置的内容不在本文档中功能块库、系统用户指南或者其他实施的范围之内。

启动与测试

安装之后，在使用电气控制与自动化设备进行常规操作之前，应当由合格的工作人员对系统进行一次启动测试，以验证设备正确运行。安排这种检测非常重要，而且应该提供足够长的时间来执行彻底并且令人满意的测试。

⚠警告

设备操作危险

- 验证已经完成所有安装与设置步骤。
- 在执行运行测试之前，将所有元器件上用于运送的挡块或其他临时性支撑物拆下。
- 从设备上拆下工具、仪表以及去除碎片。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

执行设备文档中所建议的所有启动测试。保存所有设备文档以供日后参考使用。

必须同时在仿真与真实的网络境中进行软件测试。

按照地方法规（例如：依照美国 National Electrical Code ）验证所完成的系统无任何短路且未安装任何临时接地线。如果必须进行高电位电压测试，请遵循设备文档中的建议，防止设备意外损坏。

在对设备通电之前：

- 从设备上拆下工具、仪表以及去除碎片。
- 关闭设备柜门。
- 从输入电源线中拆除所有的临时接地线。
- 执行制造商建议的所有启动测试。

操作和调整

以下预防措施摘自 NEMA Standards Publication ICS 7.1-1995：

（如果任何译文与英文原文存在分歧或矛盾，以英文原文为准。）

- 无论在设计与制造设备或者在选择与评估部件时有多谨慎，如果对此类设备造作不当，将会导致危险出现。
- 有时会因为对设备调节不当而导致设备运行不令人满意或不安全。在进行功能调节时，始终以制造商的说明书为向导。进行此类调节的工作人员应当熟悉设备制造商的说明书以及与电气设备一同使用的机器。

- 操作人员应当只能进行操作人员所需的运行调整。应当限制访问其他控件，以免对运行特性进行擅自更改。

关于本书

文档范围

本章明确了有助于对较不易遭受网络攻击的系统进行配置的那些网络安全元素。

注: 本文档通篇使用了关于网络安全主题的术语“安全性”、“安全”、“受保护”、“保护”。

V有效性说明

本文档已针对 EcoStruxure™ Control Expert V16.0 进行了更新。

有关产品合规性和环境信息（RoHS、REACH、PEP、EOLI 等），请转 www.se.com/ww/en/work/support/green-premium/。

文档的可用语言

文档提供以下语言版本:

- 简体中文 (EIO0000002004)
- 英语 (EIO0000001999)
- 法语 (EIO0000002001)
- 德语 (EIO0000002000)
- 意大利语 (EIO0000002002)
- 西班牙语 (EIO0000002003)

网络安全相关说明

在 Schneider Electric 网站上提供了网络安全的相关说明：https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

在网络安全支持部分中提供了可供下载的文档：

文档名称	网页地址
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations	www.se.com/ww/en/download/document/STN v2

相关文档

文档名称	商业型号
Modicon M580 系统规划指南	HRB65322（简体中文） HRB62666（英语） HRB65318（法语） HRB65319（德语） RB65320（意大利语） HRB65321（西班牙语）
Modicon M580 硬件参考指南	EIO0000001583（简体中文） EIO0000001578（英语） EIO0000001579（法语） EIO0000001580（德语） EIO0000001582（意大利语） EIO0000001581（西班牙语）
Modicon M580 BMENOC0301 / BMENOC0311 Ethernet 通讯模块安装和配置指南	HRB65316（简体中文） HRB62665（英语） HRB65311（法语） HRB65313（德语） HRB65314（意大利语） HRB65315（西班牙语）
用于 *Ethernet* 的 *Modicon M340* 通讯模块和处理器用户手册	31007493（简体中文） 31007131（英语） 31007132（法语） 31007133（德语） 31007494（意大利语） 31007134（西班牙语）
Quantum TCP/IP 配置用户手册	31007110（简体中文） 33002467（英语） 33002468（法语） 33002469（德语） 31008078（意大利语） 33002470（西班牙语）
Premium 和 Atrium 以太网网络模块用户手册	31007102（简体中文） 35006192（英语） 35006193（法语） 35006194（德语） 31007214（意大利语） 35006195（西班牙语）

文档名称	商业型号
EcoStruxure™ Control Expert 操作模式	33003697（简体中文） 33003101（英语） 33003102（法语） 33003103（德语） 33003696（意大利语） 33003104（西班牙语）
Quantum 使用 EcoStruxure™ Control Expert 硬件参考手册	35012184（简体中文） 35010529（英语） 35010530（法语） 35010531（德语） 35013975（意大利语） 35010532（西班牙语）
使用 EcoStruxure™ Control Expert 的 Quantum 140NOC77101 Ethernet 通讯模块用户手册	S1A33993（简体中文） S1A33985（英语） S1A33986（法语） S1A33987（德语） S1A33989（意大利语） S1A33988（西班牙语）
使用 EcoStruxure™ Control Expert 的 Premium TSXETC101 Ethernet 以太网通讯模块用户手册	S1A34008（简体中文） S1A34003（英语） S1A34004（法语） S1A34005（德语） S1A34007（意大利语） S1A34006（西班牙语）
Modicon M340 BMXNOC0401 Ethernet 通讯模块用户手册	S1A34014（简体中文） S1A34009（英语） S1A34010（法语） S1A34011（德语） S1A34013（意大利语） S1A34012（西班牙语）
Quantum EIO 控制网络安装和配置指南	S1A48999（简体中文） S1A48993（英语） S1A48994（法语） S1A48995（德语） S1A48997（意大利语） S1A48998（西班牙语）
EcoStruxure™ Control Expert 通讯功能块库	33003683（简体中文） 33002527（英语） 33002528（法语） 33002529（德语） 33003682（意大利语） 33002530（西班牙语）
Quantum Ethernet 网络模块用户手册	31007112（简体中文） 33002479（英语） 33002480（法语） 33002481（德语）

文档名称	商业型号
	31007213（意大利语） 33002482（西班牙语）
Modicon M580 BMECXM CANopen 模块用户手册	EIO0000002134（简体中文） EIO0000002129（英语） EIO0000002130（法语） EIO0000002131（德语） EIO0000002132（意大利语） EIO0000002133（西班牙语）
EcoStruxure Automation Device Maintenance 固件升级工具	EIO0000004050（简体中文） EIO0000004033（英语） EIO0000004046（法语） EIO0000004048（德语） EIO0000004049（意大利语） EIO0000004047（西班牙语）
Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide	HRB44124（英语）
Modicon MC80 Program Logic Controller (PLC) User Manual	EIO0000002071（英语）

产品相关信息

⚠⚠危险

触电、爆炸或弧闪危险

- 去掉护盖或门，以及在安装或拆除任何附件、硬件、电缆或导线之前，断开所有设备（包括所连接的设备）的所有电源，但本设备相应硬件指南中所指定的特定情形除外。
- 根据相应指示，始终使用规格适当的电压传感设备来确认电源已关闭。
- 更换并紧固所有护盖、附件、硬件、电缆与电线，并确认接地连接正确后再对设备通电。
- 在操作设备及任何相关产品时，必须使用指定电压。

未按说明操作将导致人身伤亡等严重后果。

⚠警告

失去控制

- 请对您的应用进行“失效模式和效果分析”(FMEA) 或与之相当的风险分析，并在实施前部署预防性和检测性控制措施。
- 针对不期望的控制事件或过程提供反馈状态。
- 在需要时，提供单独的或冗余的控制路径。
- 提供适当参数，尤其是限制参数。
- 评估传输延迟的影响，并采取相应的应对措施。
- 评估通讯链路中断的影响，并采取相应的应对措施。
- 根据风险分析以及适用的法规和规定为控制功能（比如，急停、超限状态和故障状态）提供独立路径。
- 遵循当地的事故预防和安全规范指南。[1]
- 在投入使用前，对系统的每个实现进行测试，以确保其工作正常。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

[1] 有关详细信息，请参阅 NEMA ICS 1.1（最新版）中的“安全指导原则 - 固态控制器的应用、安装和维护”以及 NEMA ICS 7.1（最新版）中的“结构安全标准及可调速驱动系统的选择、安装与操作指南”或您特定地区的类似规定。

⚠警告

意外的设备操作

- 本设备只能搭配经 Schneider Electric 认可的软件。
- 每次更改物理硬件配置后，请更新应用程序。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

⚠警告

意外的设备运行、丧失控制、数据丢失

您以及拥有、设计、操作本产品和/或使用 Ecostruxure Control Expert 维护本产品的任何人必须阅读、理解并遵守本文档中的说明。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

商标

摘自标准的术语

此处包含的或者出现在产品自身中/上的技术术语、术语、符号和相应描述基本上均源自国际标准的条款或定义。

在功能安全系统、变频器和一般自动化领域，举例来说，这可能包括但不限于以下术语：安全、安全功能、安全状态、故障、故障复位、失灵、失败、错误、错误消息、危险等。

其中，相关标准包括：

标准	说明
IEC 61131-2:2007	可编程控制器，第 2 部分：设备要求和测试。
ISO 13849-1:2023	机械安全：安全相关的控制系统部件。 设计通则。
EN 61496-1:2020	机械安全：电敏保护装置 第 1 部分：一般要求和测试。
ISO 12100:2010	机械安全 - 设计的一般原则 - 风险评估和风险抑制
EN 60204-1:2006	机械安全 - 机器电气设备 - 第 1 部分：总要求
ISO 14119:2013	机械安全 - 与防护设备关联的联锁设备 - 设计和选择原则
ISO 13850:2015	机械安全 - 紧急停止 - 设计原则
IEC 62061:2021	机械安全 - 安全相关的电气、电子和可编程电子控制系统的功能性安全
IEC 61508-1:2010	电气/电子/可编程电子安全相关系统的功能安全：一般要求。
IEC 61508-2:2010	电气/电子/可编程电子安全相关系统的功能安全：电气/电子/可编程电子安全相关系统的要求。
IEC 61508-3:2010	电气/电子/可编程电子安全相关系统的功能安全：软件要求。
IEC 61784-3:2021	工业通信网络 - 配置 - 第 3 部分：功能安全现场总线 - 一般规则和配置定义。
2006/42/EC	机械指令
2014/30/EU	电磁兼容性规程
2014/35/EU	低电压规程

此外，本文中所用的名词可能是被无意中使用，因为它们是从其他标准中衍生出来的，如：

标准	说明
IEC 60034 系列	旋转电机
IEC 61800 系列	可调速电力驱动系统
IEC 61158 系列	用于测量和控制的数字数据通讯：用于工业控制系统的现场总线

最后，操作区一词可结合特定危险的描述一起使用，其定义相当于以下位置中的风险区或危险区：机器指令 (*2006/42/EC*) 和 *ISO 12100:2010*.

注: 对于当前文档中引用的特定产品，上述标准可能适用，也可能不适用。若要了解与适用于此处所述产品的各项标准有关的更多信息，请参阅这些产品参考的特性表。

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。

简介

简介

这本书旨在介绍在 Modicon 控制器和关联软件应用程序中实现的网络安全解决方案。除本手册中所述的解决方案外，请遵循 Schneider Electric 网络安全技术说明（在 Schneider Electric website 上）中提供的准则。

Schneider Electric 指南

简介

PC 系统可以运行各种应用程序，以帮助增强控制环境中的安全。系统具有出厂缺省设置，这些要求重新配置以符合深度防御方法的 Schneider Electric 设备加强准则。

在 Schneider Electric website 的支持区域中，提供了专用于网络安全的主题。

深度防御方法

除本文档中所述的解决方案外，请遵循以下文档中所述的 Schneider Electric 深度防御方法：

- **手册标题**： How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations
- **网站链接说明**（**手册说明**）： How Can I Reduce Vulnerability to Cyber Attacks in PlantStruxure Architectures?

管理漏洞

报告的 Schneider Electric 设备漏洞记录在**网络安全支持**网页（位置 http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page）中。

单击**安全通知**，它会将您带到 https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp，由此可访问安全通知列表。

如果您面临的网络安全事件或漏洞未在 Schneider Electric 提供的列表中提及，则可以单击**网络安全支持**网页上的**报告漏洞**，以打开：https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp

如何帮助保护架构

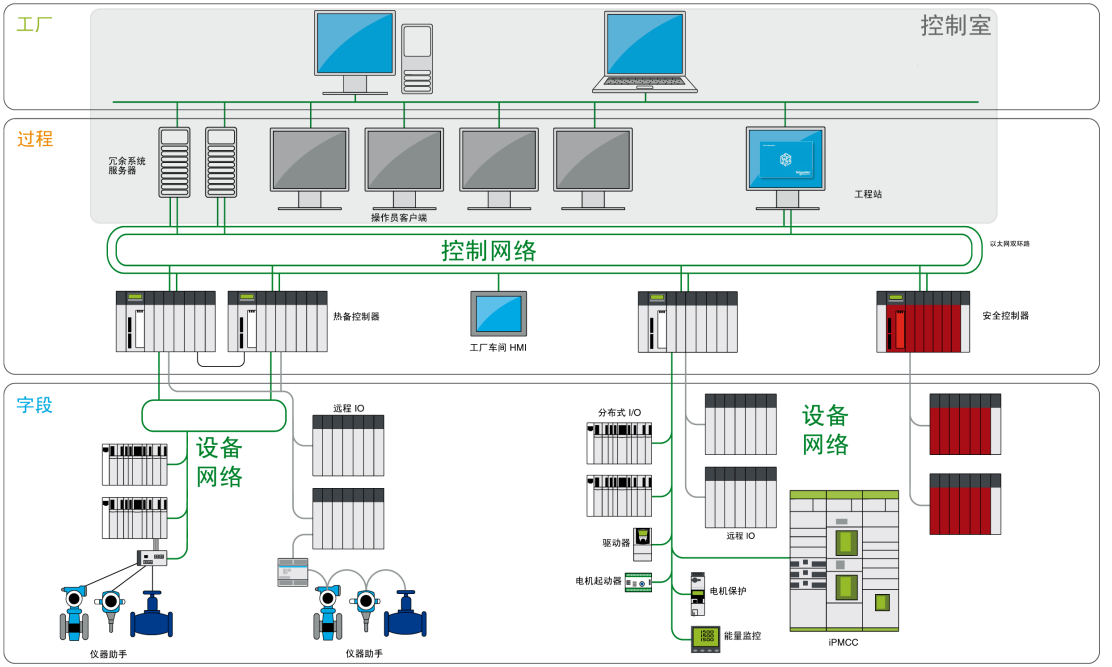
简介

本章介绍如何帮助提升 Modicon 控制器的安全性。

系统视图

系统架构

以下架构突出显示具备更安全的多层架构（含控制网络和设备网络）的必要性。扁平化架构（所有设备连接到同一网络）无法进行适当保护。



更安全的通讯

控制室内的设备相比连接到设备网络的设备会更多地暴露于攻击。因此，需在控制室与 controller 和设备之间实现更安全的通讯。将设备网络与其他网络层相隔离（如控制网络与远程网络）。

在上述系统架构中，控制室区域被灰显，以将其与控制器和其他设备相区分。

更安全地访问 USB 端口

需要对 USB 端口的物理访问进行控制。

注: 只能通过物理方式（例如，机柜或物理钥匙）来保护 USB 端口安全。

热备链路和设备网络的更安全访问

控制对热备链路和设备网络的访问。

测试

Control Expert 提供了一个仿真器，用于在将应用程序作为工业自动化系统的一部分进行调试之前，测试您的应用程序。此仿真器符合以下网络安全要求：

- 只有在 Control Expert 中打开了应用程序时，才能操作仿真器。
- 无法将仿真器中打开的应用程序从仿真器上传到控制器。

有关如何操作仿真器的信息，请参阅 *EcoStruxure™ Control Expert Controller Simulator* (https://youtu.be/RrkorSe0G8s) 的帮助文件。

在 Control Expert 中设置密码

使用 Control Expert 软件设置有助于保护项目安全的密码。可以设置以下密码：

- 应用程序密码，含或不含文件加密
- 安全相关区密码
- 固件升级密码
- 程序单元、段和子程序密码

- 数据存储/Web 密码

应用程序密码

Control Expert 提供密码机制来防止对应用程序的未授权访问。在您执行以下操作的情况下，Control Expert 使用密码：

- 在 Control Expert 中打开应用程序。
- 在 Control Expert 中连接到控制器。

通过密码进行应用程序保护能够防止意外的应用程序修改、下载或防止意外打开应用程序文件。密码加密存储在应用程序中。

除密码保护外，您还可以对 .STU、.STA 和 .ZEF 文件加密。Control Expert 中的文件加密功能有助于防止遭到无权限人员的非法更改，并加强了知识产权的防盗保护以及对其他恶意意图的防护。文件加密选项受密码机制保护。

注: 当将控制器作为系统项目的一部分进行管理时，应用程序密码和文件加密在 Control Expert 编辑器中处于禁用状态，并且需要使用拓扑管理器来管理。

有关如何设置和使用应用程序密码的说明，请参阅 *EcoStruxure™ Control Expert* 操作模式手册中的应用程序保护主题。

安全相关区密码

安全控制器包含安全相关区密码保护功能，可通过项目的**属性**屏幕来访问。此功能用于帮助保护位于功能安全项目的安全相关区中的项目元素。

当安全相关区密码保护功能已激活时，无法修改应用程序的安全相关部分。

有关如何设置和使用安全相关区密码的说明，请参阅 *EcoStruxure™ Control Expert* 操作模式手册中的安全相关区密码保护主题。

固件更新密码

利用密码保护固件有助于防止模块遭到非预期访问。

对于 M580 控制器，固件更新的管理取决于用于创建应用程序的控制器固件版本。

- 对于早于 4.01 的控制器固件版本：
  - 使用 FTP 管理固件更新。
  - 固件更新访问能够受到密码保护。

- 对于控制器固件版本 4.01 及更高版本：
  - 使用 HTTPS（比 FTP 更安全）管理固件更新访问。
  - 固件更新访问必须受到密码保护。
  - 使用相同的密码保护数据存储和网页访问。

有关如何设置和使用固件密码的说明，请参阅 *EcoStruxure™ Control Expert* 操作模式 手册中的固件保护主题。

程序单元、段和子程序密码

程序单元、段和子程序保护功能（在已启用时）使用密码来帮助保护这些程序元素。此功能可在离线模式下从项目的“属性”屏幕进行设置和访问。

有关如何设置和使用程序单元、段和子程序密码的说明，请参阅 *EcoStruxure™ Control Expert* 操作模式 手册中的程序单元、段和子程序保护主题。

数据存储/Web 密码

通过密码进行的保护有助于防止对 SD 存储卡数据存储区域的非预期访问（如果控制器中已插入有效的存储卡）。

对于使用以下 Control Expert 版本创建的项目中的 M580 控制器：

- 低于 15.1 的版本，可以为数据存储访问提供密码保护。
- 不低于 15.1 的版本，可以为 Web 诊断和数据存储访问提供密码保护。

对于 M580 控制器，数据存储和 Web 接口的管理取决于用于创建应用程序的控制器固件版本：

- 对于早于 4.01 的控制器固件版本：
  - 使用 FTP 管理数据存储。
  - 数据存储访问能够受到密码保护。
  - 网页访问不能受密码保护。
- 对于控制器固件版本 4.01 及更高版本：
  - 使用 HTTPS（比 FTP 更安全）管理数据存储。
  - 数据存储和网页访问必须受到密码保护。
  - 使用相同的密码保护数据存储和网页访问。

有关如何设置和使用数据存储/Web 密码的说明，请参阅 *EcoStruxure™ Control Expert* 操作模式 手册中的数据存储*/Web* 保护主题。

加强 PC

位于控制室内的工作站 PC 遭受攻击的风险较高。需要加强这些支持 EcoStruxure™ Control Expert 或 EcoStruxure™ Server Expert 的 PC。

由于这些应用程序都在 Windows 操作系统上运行，因此本章介绍了如何通过关注 Windows 10 的安全性来加强 PC。

加强工程工作站

以下关键功能旨在帮助保护工作站。单击相应项，可了解有关该功能的更多信息：

- 减少攻击面, 22 页
- 安全策略配置和检查, 23 页
- 用户帐户管理, 23 页
- 访问控制管理, 24 页
- 保护网络服务, 24 页，包括：
  - 禁用远程桌面协议, 25 页
  - 禁用 LANMAN 和 NTLM, 25 页
  - 禁用未使用的网络接口卡, 26 页
  - 配置局域连接, 26 页
- 启用或安装防病毒保护工具, 26 页
- 系统补丁管理, 27 页
- 备份管理, 27 页
- 保密管理, 28 页
- 审计管理, 28 页

本主题还引用了若干 Windows 10 网络安全配置指南, 28 页。

减少攻击面

网络系统的攻击面是入侵者可能试图添加或提取数据的区域集合。

为了帮助减少潜在攻击面，应：

- 禁用所有未使用的软件应用程序、服务和通讯端口。
- 禁用或限制对可移除存储设备（例如，USB）的访问。

- 仅将工作站用于单个功能（例如，在不同 PC 上安装 OPC UA Server Expert 和 Control Expert）。

安全策略配置和检查

Windows 安全策略可以通过组策略对象进行设置。

组策略对象 (GPO) 是一组可应用于 PC 工作站的配置更改。有关本地组策略编辑器的详细信息，请参阅下文所述, 28 页的来自互联网安全中心 (CIS) 的安全配置指南。

域 GPO 也可在 Windows Active Directory 中定义。

需要定期自动检查安全配置。

用户帐户管理

- **更改缺省密码**：

  在部署任何新资产之前，应将所有缺省密码更改为与管理级帐户一致的值。

  禁用 Windows 自动登录。

  有关 Windows 帐户密码设置的说明，请参阅下文所述, 28 页的来自互联网安全中心 (CIS) 的安全配置指南。
- **设置用户帐户**：

  用户帐户可以在独立计算机上本地定义（工作组），也可以通过 Windows Active Directory 域控制器定义，该域控制器允许集中管理系统中的所有用户。

  设置用户帐户时，请遵循以下准则：
  - 使用标准的单个用户帐户（无管理员权限）来运行被配置成作为独立应用程序运行的软件应用程序（例如，Control Expert）。
  - 为被配置成作为服务运行的软件应用程序（例如，OFS UA）使用本地系统帐户。
  - 使用专门的管理帐户来安装软件应用程序和配置 IPSec。
  - 设置密码管理器以管理密码（例如 KeyPass）。
  - 禁用与业务无关的所有帐户（例如，调试帐户）。请参阅“CIS 控制”16.8, 28 页。
  - 在设置的不活动时长结束后，自动禁用休眠帐户。请参阅“CIS 控制”16.9, 28 页。
  - 在标准不活动时长结束后，自动锁定工作站会话。请参阅“CIS 控制”16.11, 28 页。

访问控制管理

需要控制对存储在具有文件系统、网络共享、声明、应用程序或数据库的系统上的所有信息的访问。这些控制实施了**最低权限原则**，这意味着，只有经授权的人员才能访问信息，而他们能够访问的信息是他们在自身职责下需获得的基本信息。

权限与对象相关。根据具体的对象，可以基于以下方面实现权限：

- Windows Active Directory 对象。
- 通过任意访问控制列表 (DACL) 进行的 NTFS 文件访问。
- 共享文件夹权限。
- 远程注册表服务（启用/禁用）。

权限是未与对象绑定但特定于机器的用户权限。它们可通过组策略设置进行管理，例如，本地组策略编辑器中的“可移动存储访问”设置可以限制对 USB 设备存储的访问（读或写）。

帮助保护网络服务

卸载或禁用不必要的或未使用的网络服务。

禁用服务的方法有多种（服务工具、安全模板、组策略对象、PowerShell、SC.exe）。

使用 Windows 防火墙和缺省拒绝规则，该规则将丢弃除显式允许的服务和端口外的所有通讯流。

- **防火墙使用**：

  在 Windows 10 上配置 IPSEC 时，需要用到 Windows 防火墙。在包括 Windows 10 在内的 Windows 操作系统的最新版本中，缺省启用了防火墙。有关 Windows 防火墙设置的更多详细信息，请参阅下文所述的来自互联网安全中心 (CIS) 的安全配置指南。
- **Server Manager 工具**：

  Server Manager 让您能够查看功能的所有从属项，以便您能够确定是否可以将其从 Windows Server 中删除。

  可以选择服务器角色（例如，Web 服务器 (IIS)、DNS 服务器等）。

  可以选择服务器特性（例如，BitLocker、.NET Framework 等）。
- **互联网信息服务器 (IIS) - Web 服务器安全**：

  使用最新版本的最低安装。

  配置 IIS 访问控制（TLS 和用户身份验证）。

  启用记录并查看非法入侵签名日志。

  CIS 基准文档中提供了有关 IIS 设置的更多详细信息（请参阅下面的链接）。，28 页

- **禁用 SMBv1**：

  服务器消息块版本 1 (SMBv1) 是用于通过网络在 PC 之间共享服务（如打印、文件和通讯）的协议。SMBv1 的已被证实的漏洞是，允许在主机 PC 上执行远程代码。

  您可以禁用 SMBv1 以帮助最大程度地减少漏洞。

禁用远程桌面协议

Schneider Electric 的深度防御方法准则包括禁用远程桌面协议 (RDP)，除非您的应用程序需要 RDP。以下步骤介绍了如何禁用该协议：

步骤	操作
1	在 Windows 10 中，使用**计算机 > 系统属性 > 高级系统设置**来禁用 RDP。
2	在**远程**选项卡中，取消选中**允许远程协助连接这台计算机**复选框。
3	选择**不允许连接这台计算机**复选框。

禁用 LANMAN 和 NTLM

禁用 Microsoft LAN Manager 协议 (LANMAN) 或及其后续 NT LAN Manager (NTLM)以最大程度减少漏洞。

以下步骤介绍了如何在 Windows 10 系统中禁用 LANMAN 和 NTLM：

步骤	操作
1	在命令窗口中，执行 `secpol.msc`，以打开**本地安全策略**窗口。
2	打开**安全设置 > 本地策略 > 安全选项**。
3	选择**仅发送 NTLMv2 响应。在以下位置拒绝 LM & NTLM**：**网络安全**：**LAN Manger 验证级别**字段。
4	选择**网络安全**：**不要在下次更改密码时存储 LAN Manager 的哈希值**复选框。
5	在命令窗口中，输入 `gpupdate`，以确认更改的安全策略。

禁用未使用的网络接口卡

禁用应用程序不需要的网络接口卡。例如，如果您的系统有 2 张卡，且应用程序只使用一张，则验证是否禁用另一张网络卡（本地连接 2）。

在 Windows 10 中禁用网络卡：

步骤	操作
1	打开**控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置**。
2	右键单击未使用的连接。选择**禁用**。

配置局域连接

各种 Windows 网络设置增强了与深度防御方法相一致的安全性。

在 Windows 10 系统中，通过打开**控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置 > 局域连接 (x)** 来访问这些设置。

以下列表是您可能在**本地连接属性**屏幕上对系统进行的配置更改的示例：

- 禁用各个网络卡上的所有 IPv6 堆栈。
- 取消选择所有**局域连接属性**项，**QoS 数据包计划程序**和 **Internet 协议版本 4** 除外。
- 在**高级 TCP/IP 设置**上的 **Wins** 选项卡下方，取消选择**启用 LMHOSTS** 和 **禁用 TCP/IP 上的 NetBIOS** 复选框。
- 启用 **Microsoft 网络的文件和打印机共享**。

Schneider Electric 的深度防御准则还包括以下内容：

- 仅定义静态 IPv4 地址、子网掩码和网关。
- 不使用控制室内的 DHCP 或 DNS。

启用或安装防病毒保护工具

可以使用 Windows 10 中的内置工具来改善系统对病毒和恶意代码的响应能力。如有必要，还可以安装其他杀毒软件。

Windows 10 的企业版包括 *Windows Defender Advanced Threat Protection*，它是一个监控端点（比如，使用行为传感器的 Windows 10 PC）的安全平台。微软的 *SmartScreen* 技术是另一项内置功能，可扫描、下载并阻止访问已知存在恶意的网站和下载。

有关 *Windows Defender* 设置的更多详细信息，请参阅下文所述的互联网安全中心 (CIS) 文档，其中包括：

- 确保组织的反恶意软件定期更新其扫描引擎和签名数据库（“CIS 控制”8.2）。
- 配置可移动介质的防恶意软件扫描：USB（请参阅“CIS 控制”8.4）。, 28 页
- 将设备配置为不自动从可移动介质运行内容：USB（请参阅“CIS 控制”8.5）。, 28 页

系统补丁管理

始终安装操作系统、应用程序（包括 Web 浏览器和电子邮件客户端）、驱动程序的任何安全相关更新的最新稳定版本。

在 Windows 10 中启用自动更新。

有关更多详细信息，请参阅下文所述, 28 页的互联网安全中心 (CIS) 文档。

备份管理

确保：

- 定期自动备份所有系统数据（请参阅“CIS 控制”10.1）。, 28 页
- 通过映像等过程将组织的关键系统作为完整系统进行备份，以实现整个系统的快速恢复。（请参阅“CIS 控制”10.2）。, 28 页
- 在存储备份时，以及在跨网络转移备份时，通过物理安全或加密正确保护备份。这包括远程备份和云服务。（请参阅“CIS 控制”10.4。）, 28 页
- 所有备份都有至少一个离线（无法通过网络连接访问）备份目标（请参阅“CIS 控制”10.5）, 28 页。

用户可以：

- 使用 Windows 10 中的 *File History* 和其他免费工具创建文件备份。
- 创建恢复盘，从映像备份恢复系统。
- 使用存储同步和共享服务，将备份放在云（如 *OneDrive*、*Dropbox* 或 *Google Drive*）中。

有关 Windows File History、备份/恢复设置的更多详细信息，请参阅下文所述的 CIS 文档。

保密管理

从网络中删除组织未定期访问的敏感数据或系统。这些系统可以用作需要偶尔使用它们的业务部门的独立系统（与网络断开连接），也可以在需要之前被完全虚拟化并关机。请参阅下文所述的 CIS 文档。（请参阅“CIS 控制”13.2）。, 28 页

使用 *Bitlocker* 启用磁盘加密。有关 *Bitlocker* 设置的更多详细信息，请参阅下文所述的 CIS 文档。

审计管理

确保已在 Windows 主机上配置本地安全日志。有关审计策略配置的详细信息，请参阅下文所述的 CIS 文档。, 28 页

Windows 10 网络安全配置指南

确认使用的是具有网络安全设置的完整 Windows 10，以使用 Windows 配置指南，包括：

- 来自互联网安全中心 (CIS) 的安全配置指南

  https://www.cisecurity.org/press-release/cis-controls-microsoft-windows-10-cyber-hygiene-guide/

  - IG1 级：

    https://www.cisecurity.org/cis-benchmarks/

    https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

    https://www.cisecurity.org/benchmark/microsoft_iis/

- 美国国防部 (DISA STIG) 制定的安全配置指南

  https://www.stigviewer.com/stig/windows_10/2020-06-15/

“CIS 基准”文档和“STIG Windows 10 安全技术实施指南”都提供了可选方案。您对方案的选择取决于您在 Windows 上运行的应用程序的关键性。

禁用未使用的嵌入式通讯服务

嵌入式通讯服务

嵌入式通讯服务是基于 IP 的通讯服务，以服务器模式用于嵌入式产品（例如 HTTP 或 FTP）。

禁用未使用的服务

为了有助于减少攻击风险，请禁用任何未使用的嵌入式服务（例如 HTTP 和 FTP），以关闭潜在的通讯门。

在 Control Expert 中禁用 Ethernet 服务

您可以使用 control Expert 中的 Ethernet 选项卡来启用/禁用 Ethernet 服务。为以下每种系统提供了选项卡描述：

- Modicon M340, 115 页
- Modicon M580, 116 页
- Modicon Quantum, 116 页
- Modicon X80 modules, 118 页
- Modicon Premium/Atrium, 120 页
- Modicon Momentum MDI, 121 页
- Modicon MC80, 121 页

在将应用程序下载到 controller 之前，先设置 Ethernet 选项卡。

默认设置（最大的安全性级别）会降低通讯功能。如果需要服务，则必须启用这些服务。

注: 在某些产品上，`ETH_PORT_CTRL (see EcoStruxure™ Control Expert, Communication, Block Library)` 功能块让您能够禁用在 Control Expert 应用程序中完成了配置后所启用的服务。服务可以使用同样的功能块再次启用。

限制来自控制网络的数据流（访问控制）

控制网络的数据流

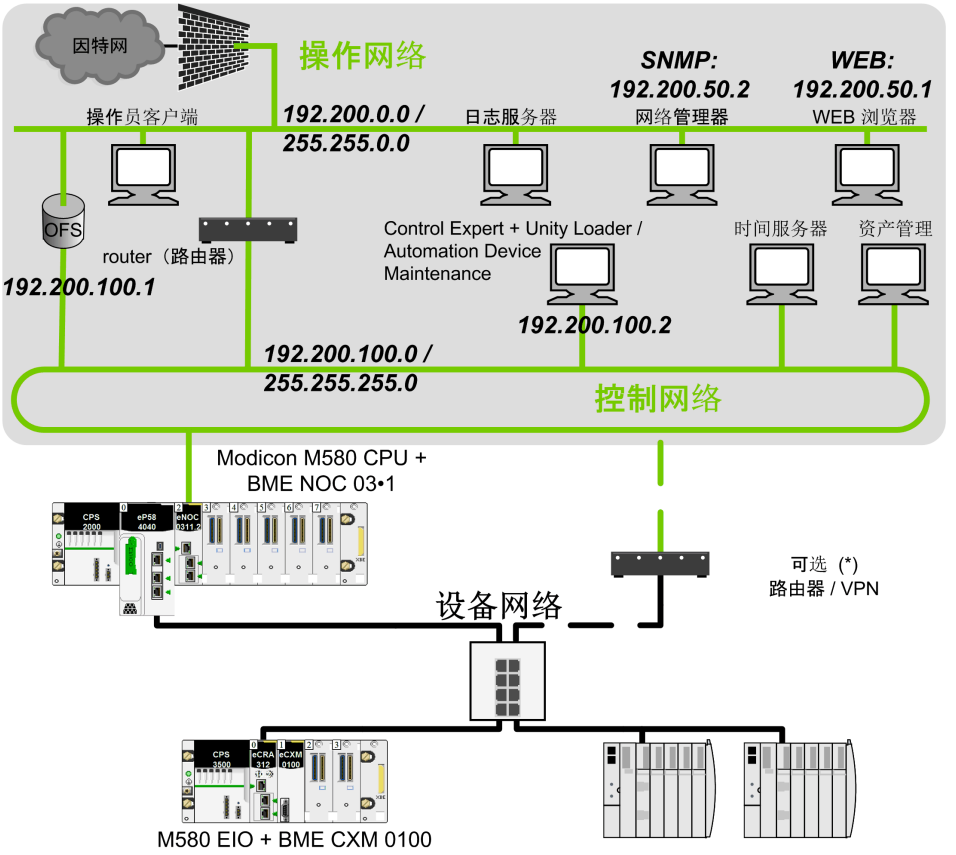
控制网络的数据流是通过控制网络发起的基于 IP 的数据流。

说明

为了控制对嵌入式产品中通讯服务器的访问，访问控制管理限制从控制网络流向授权来源或子网 IP 地址的基于 IP 的数据流。

架构示例

下图的目的是展示访问控制设置的角色和影响。访问控制管理来自通过操作和控制网络通讯的设备（位于灰显区域中）的 Ethernet 数据流。



(*) 某些服务要求访问设备网络（例如：在源时标期间进行固件更新）。在这种情况下，可选的路由器/VPN 有助于保护访问控制。

在架构示例中设置授权地址

访问控制目的：

- 连接到操作网络的任何设备（IP 地址 = 192.200.x.x）都能够访问控制器 Web 服务器。
- 连接到控制网络的任何设备（IP 地址 = 192.200.100.x）都能够使用 Modbus TCP 与控制器通讯，并能够访问 Web 服务器。

如要在上一个架构示例中限制数据流，请按照以下方式在 EcoStruxure Control Expert 访问控制表中设置授权的地址和服务：

来源	IP 地址	子网	子网掩码	FTP	TFTP	HTTP / HTTPS	Port502	EIP	SNMP
网络管理器	192.200.50.2	否	–	–	–	–	–	–	+
操作网络	192.200.0.0	是	255.255.0.0	–	–	+	–	–	–
Automation Device Maintenance	192.200.100-.2	否	–	+ [1]	–	– [2]	+	–	–
控制网络	192.200.100-.0	是	255.255.255-.0	–	–	–	+	–	–

+ 已选中

– 未选中或无内容

[1] 对于不低于 v4.10 的 M580 固件版本，未选择 FTP。

[2] 对于不低于 v4.10 的 M580 固件版本，选择了 HTTP/HTTPS。

设置描述

为有权使用 Modbus TCP 或 EtherNet/IP 与控制器通讯的设备设置授权的地址。

前一示例中每个 IP 地址的服务设置说明：

192.200.50.2 (SNMP)	设置此选项，可授权使用 SNMP 从网络管理器访问。
192.200.0.0 (HTTP/HTTPS)	操作网络子网被设置为授权连接到操作网络的所有 Web 浏览器访问控制器 Web 浏览器。
192.200.100.2 (FTP) [1)]	设置此选项，可授权使用 FTP 从 Automation Device Maintenance 访问。
192.200.100.0 (Port502)	控制网络子网被设置为授权连接到控制网络（OFS, Control Expert、Automation Device Maintenance）的所有设备使用 Port502 Modbus 访问控制器。
[1)] 对于不低于 v4.10 的 M580 固件版本，未使用 FTP。而应使用 HTTP/HTTPS。	

注: 访问列表分析经过访问控制列表的每个条目执行。如果发现成功匹配（IP 地址 + 允许的服务），则其他条目将忽略。

在 EcoStruxure Control Expert **安全**屏幕中，对于专用子网，请在子网规则前输入特定规则。例如：若要为 SNMP 设备授予特定 192.200.50.2 权限，请在全局子网规则 192.200.0.0/255.255.0.0 之前输入允许对子网的所有设备执行 HTTP 访问的规则。

设置加密通讯

简介

加密通讯的目标是帮助保护通讯通道，该通道允许远程访问系统的关键资源（例如 Modicon M580 PAC 嵌入式应用程序、固件）。IPsec（因特网协议安全）是 IETF 提供的一种开放标准，用于藉由加密和协议安全机制的结合，通过 IP 网络提供受保护且隐私的通讯，我们的 IPsec 保护实现包括防重放、消息完整性检查和消息来源验证。

Microsoft Windows V7 和 V10 上支持 IPsec。它通过 PC 操作系统启动。

描述

IPsec 功能有助于保护以下操作的安全：

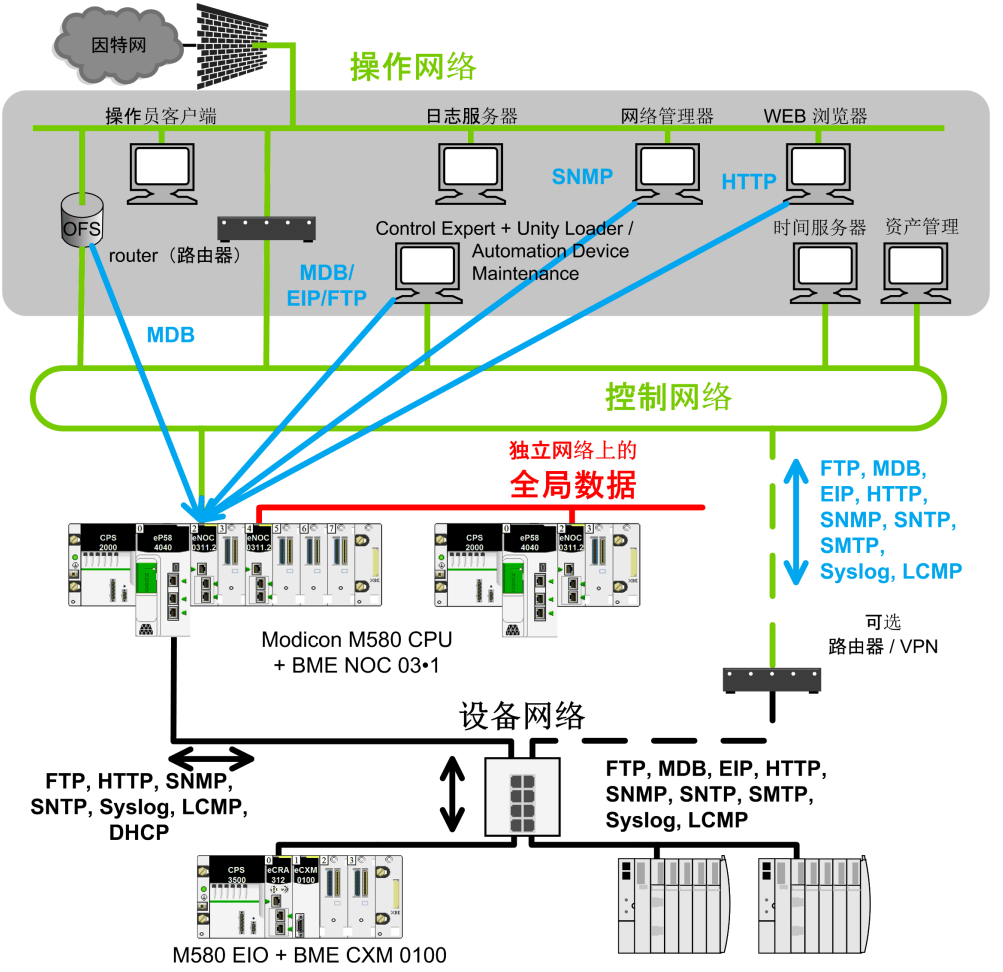
- 控制室通过 BMENOC0301 and BMENOC0311 模块对控制器进行的 Modbus 访问。
- 控制室在服务器模式下对在 BMENOC0301 and BMENOC0311 模块内部运行的通讯服务进行的访问（Modbus、EtherNet/IP、HTTP、FTP、SNMP）。

  注: IPsec 旨在帮助保护在服务器模式下于控制器中运行的服务。由 Modicon M580 PAC 启动的安全客户端服务不在本手册的讨论范围内。

无线连接：当利用 PMXNOW0300 无线模块配置无线连接时，此模块的安全设置应配置到最大程度 (WPA2-PSK)。

架构示例

下图的目的是通过示例说明从控制室到 Modicon M580 controller 的加密通讯涉及的各种协议或服务。



 加密通讯 (IPsec)。

 非 Ipsec 通讯。

具有加密通讯功能的数据流

在启用了 IPsec 的情况下，使用这些服务来促进通讯：

Ethernet 服务	**数据流安全**
EIP 3 类服务器	这些服务通过加密连接得到支持。
FTP 服务器、TFTP 服务器	
HTTP	
ICMP	
Modbus 服务器（端口 502）	
ARP	这些服务通过加密和非加密连接得到支持。 **注:** 此通讯流会绕过 IPsec 中的 BMENOC 协议传输，因此不使用 IPsec。
LLDP	
回路检查协议	
Modbus 扫描器	
RSTP	
DHCP、BootP 客户端	在启用了 IPSec 的情况下，不支持这些服务。 **注:** 在对等设备 (PC) 启动 IKE/IPsec 之前，此通讯流不受 IPSec 保护。在建立了 IKE/IPSec 之后，此通讯流被 IPsec 加密。可以支持此协议，但前提是数据包接收方是配置和启用了 IPSec 的 PC。
DHCP、BootP 服务器	
EIP 1 类，TCP（正向打开）	
EIP 1 类，UDP（数据交换）	
Modbus 客户端	
NTP 客户端	
SNMP 代理	
SNMP 陷阱	
Syslog 客户端 (UDP)	

注:

- IPsec 是 OSI 第 3 层保护。OSI 第 2 层协议（ARP、RSTP、LLDP、回路检查协议）不受 IPsec 保护。
- **全局数据**通讯流（使用 BMXNGD0100 模块）无法受到 IPsec 保护。在隔离网络中使用此类配置。

限制

架构中的 IPsec 限制：BMENOC0301 and BMENOC0311 模块不支持到设备网络的 IP 转发。

如果控制网络和设备网络之间要求透明，则需要外部路由器/vpn 以在控制网络和设备网络之间提供加密通讯（如上面的架构示例图, 35 页所示）。

从控制网络执行以下操作要求透明：

- 通过 HTTPS 服务从 Automation Device Maintenance 更新 M580 控制器固件。
- 通过 SNMP 服务从网络管理工具执行 M580 控制器的网络诊断。
- 通过 EIP 服务从 DTM 诊断 M580 控制器。
- 通过 HTTP 服务从 Web 浏览器诊断 M580 控制器。
- 通过 syslog 服务将 M580 控制器网络安全事件记录到 syslog 服务器中。
- 通过 NTP 服务从全局时间服务器同步 M580 控制器时间。

设置系统架构中的 IPsec 通讯

按照以下步骤，设置 IPsec 通讯：

- 在控制室内，识别要使用 Modbus（Control Expert、Automation Device Maintenance、OFS、客户应用程序如 SGBackup...）与 Modicon M580 PAC 系统通讯的客户端授权应用程序。

  在每台支持这些授权应用程序的 PC 上配置 IPsec。
- 在控制室内，识别要与在本地机架（用于 FactoryCast BMENOC0301 and BMENOC0311 模块的 Control Expert DTM、Automation Device Maintenance、SNMP 管理器、Web 浏览器、Web 设计工具）上配置的 BMENOC0301 and BMENOC0311 模块进行通讯的客户端授权应用程序。

  在每台支持这些授权应用程序的 PC 上配置 IPsec。
- 在连接到控制网络的每个 Modicon M580 PAC 系统的背板上，添加具有 IPsec 功能的 BMENOC0301 and BMENOC0311 模块。

  如要配置 BMENOC0301 and BMENOC0311 模块上的 IPsec 功能，请按照以下 2 步操作：
  - 启用 IPsec 功能。
  - 配置预共享密钥。预共享密钥用于生成共享密钥，允许两台设备互相验证。

    注: 因为 IPsec 依赖此共享密钥，它是安全管理员管理的安全策略中的关键元素。为了有助于提高预共享密钥的安全性，建议使用外部工具（如 KeePass, 38 页）来生成适当的字符串。

使用 Control Expert 来配置 BMENOC0301 and BMENOC0311 模块。为了有助于保护此配置，最好通过点到点连接（如 USB 端口）完成首次下载。然后，假定启用了 IPsec，未来下载可以通过具有 IPsec 功能的以太网来执行。

支持 IPsec 的每台 PC 都需要满足 IPsec 配置的以下要求：

- 使用 Microsoft Windows 10 操作系统。
- 获取管理员权限以配置 IPsec。

  一旦执行了 IPsec 配置，将 Windows 帐户设置为没有管理员权限的普通用户帐户。
- **根据加强 *PC* 主题中的说明，加强 PC**, 22 页。

有关配置的更多详细信息，请参见配置 *IP* 安全通讯主题（请参阅 Modicon M580 BMENOC0301 / BMENOC0311 Ethernet 通讯模块安装和配置指南）。

生成具有最高安全性的预共享密钥

IPsec 通讯的安全性依赖于预共享密钥的复杂程度。使用专门的工具，生成具有最高安全级别的预共享密钥。

其中一种这样的工具是 KeePass，可以从互联网免费下载。下载 KeePass，将其安装到 PC，然后启动它。

配置并使用 KeePass v2.34 来生成可用作预共享密钥的密码：

步骤	操作
1	创建新的密钥数据库文件夹（**文件 > 新建**）。
2	在 **Create New Password Database** 对话框中，在 **File name** 字段输入文件夹名称，并记录您的修改。
3	在 **Create Composite Master Key** 对话框中，请输入 **Master password**。在 **Repeat** 密码字段中再次输入该密码。
4	按 **OK**，以打开 n **Step 2**，然后再次按 **OK**。
5	在新的数据库对话框中，展开 **New Database**。
6	选择 **Network**，并添加一个条目 (**Edit > Add Entry**)。
7	在 **Title** 字段中，为您的模块输入名称（例如 eNOC）。
8	在 **User name** 字段，输入一个用户名。
9	点击 **Generate a password** 图标。
10	选择 **Open password generator**。
11	按 **OK**，以填充 **Password** 和 **Repeat** 字段。

步骤	操作
12	打开 **Password Generation Options** 对话框 (**Tools** > **Generate Password**)。
13	在 **Generate using character set** 中进行以下选择： • 大写 (A、B、C、...) • 小写 (b、c、a、...) • 数字 (0、1、2、...) • 减号 (-) • 下划线 (_) • 特殊字符 (!、$、%、&、...) • 括号 ([、]、[、(、)、<、>) **注:** 在预共享密钥中不得使用这些字符。 • { • } • ; • #
14	按 **OK**。
15	在 **Database** 列表中，右键单击您的设备，然后滚动到 **Copy Password**。
16	在 Control Expert 中打开安全配置屏幕。
17	将密钥粘贴至 IPsec 配置屏幕。

诊断系统架构中的 IPsec 通讯

有关系统架构中 IPsec 诊断的相关说明，请参见配置 *IP* 加密通讯主题（请参阅 Modicon M580 BMENOC0301 / BMENOC0311 Ethernet 通讯模块安装和配置指南）。

CSPN 安全目标

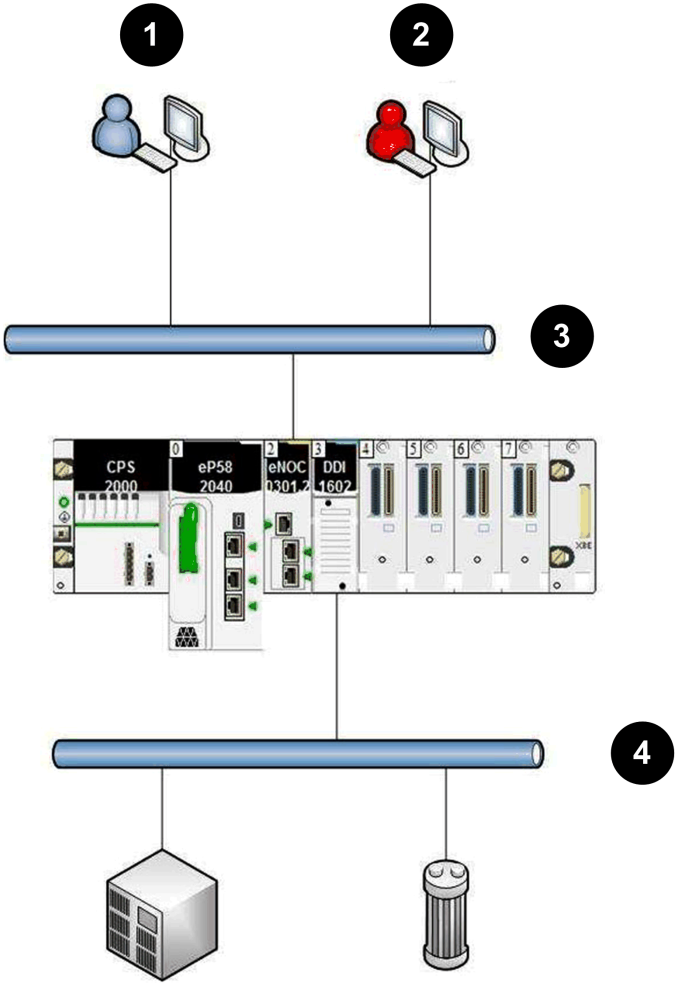
CSPN 简介

CSPN (Certification de Sécurité de Premier Niveau) 是法国当前使用的网络安全认证。经 CSPN 认证的产品能够抵御熟练黑客持续两个月的网络攻击。Modicon M580 平台就通过了 CSPN 认证。本主题介绍符合 CSPN 要求以实现最高安全等级的环境、可编程自动化控制器配置和参数。

Modicon M580 简介

Modicon M580 PAC 设计用于持续控制和命令工业过程，无需人工干预。在每个环节中，控制器处理从其输入端（传感器）接收的数据，并将命令发送至其输出端（执行器）。使用位于本地机架（带有控制器）上的 BMENOC0301 and BMENOC0311 以太网通讯模块，执行与监管设备（HMI、SCADA）的交换。

下图介绍了可能易遭受网络攻击的典型 M580 系统架构：



1 操作员使用 EcoStruxure Control Expert

2 攻击者

3 监管网络

4 没有攻击者的现场网络

M580 功能

M580 控制器具有以下功能：

功能	描述
用户程序执行	M580 控制器运行处理输入并更新输出的用户程序。
输入/输出管理	M580 控制器能够读取本地输入并写入本地输出。这些输入/输出可以是数字量形式或模拟量形式，让 M580 控制器能够控制并命令工业过程。
与监管设备通讯	M580 控制器能够与 SCADA 通讯以接收命令并使用 Modbus 协议传输过程数据。
管理功能	M580 控制器包含 EcoStruxure Control Expert 中提供的管理功能，用于执行配置和编程。
远程记录	M580 控制器支持定义远程记录策略；它能够记录安全和管理事件。

M580 配置

经 CSPN 认证的 M580 配置包含以下组件：

模块	固件	描述
BMEP58•0•0	从 V2.20 开始	控制器遵循安全文档中所述的安全规则（请参见假设条件）。
BMENOC0301 and BMENOC0311	从 V2.11 开始	此以太网模块管理与上一层（EcoStruxure Control Expert 监管与工程软件）之间的加密通讯。

注: EcoStruxure Control Expert 编程软件、PC、其他控制器模块以及背板部件不在认证范围内。

用户类型

为改善实现而与控制器交互的用户具有以下预定义的 EcoStruxure Control Expert Security Editor 用户类型：

用户类型	描述
ReadOnly	未授权任何应用程序修改。
Operate	仅启用应用程序执行和参数修改。
Program	启用所有功能。

改善实现

下列项目有助于实现改善实现的健康环境：

项目	安全注意事项
安全文档	在评估之前，应遵守文档（例如，用户指南、白皮书）中的所有说明。
管理员	系统管理员应具有相应资质、经过培训且值得信赖。
场所	控制器位置的访问仅限于值得信赖的人员。特别注意，不得让攻击者拥有控制器的物理端口访问权限。由于可以自由购买相同的产品，因此，攻击者能够获取一个产品并通过任何可能的手段研究其漏洞。
禁用未经评估的服务	应通过配置或用户方案（如安全文档中所述）禁用安全目标之外的任何服务。
用户应用程序验证	EcoStruxure Control Expert 应用程序的完整性在加载至控制器之前应由管理员进行控制。
激活记录功能	记录功能应正常且日志不得损坏。
日志检查	系统管理员应定期检查本地和远程日志。
首次配置	初始配置通过 USB 接口上传到控制器，且控制器应与网络物理断开。
固件升级	固件升级通过 USB 接口实施，且控制器应与网络物理断开。
高强度密码	系统管理员应使用组合了大写字母、小写字母、数字和特殊字符的高强度密码。

运行模式

以下运行模式符合 CSPN 要求：

- 在调试期间，可以利用与以太网端口点到点连接的**或者**与控制器的本地 USB 端口连接的 Control Expert 工程工作站来执行控制器的初始配置。
- 在正常运行条件（运行模式，SCADA 连接到以太网控制网络）下，确认 Control Expert 已断开连接。
- 利用与控制器的 USB 端口连接的 Control Expert 进一步修改配置或应用程序。

网络安全参数

下表介绍了网络安全参数：

参数	主题	用户指南
ACL 已激活。	配置安全服务	Modicon M580 BMENOC0301 / BMENOC0311 Ethernet 通讯模块安装和配置指南
以最高安全激活了 BMENOC0301/0311 上的 IPsec。	配置安全服务	
强制安全性已选择（FTP、TFTP、HTTP、DHCP/BOOTP、SNMP、EIP、NTP 协议已停用）。	配置安全服务	
日志已激活。	将 DTM 和模块事件记录至 Syslog 服务器	
仅限输入的运行/停止已激活。	管理运行/停止输入	M580 硬件参考指南
存储器保护已激活。	存储器保护	
帮助保护项目： • 使用登录名和密码锁定应用程序。 • 段保护已激活。	帮助保护 Control Expert 中的项目	
控制器内部未存储任何上传信息。	控制器内嵌数据	EcoStruxure™ Control Expert 操作模式
FTP 服务的缺省密码已修改。	固件保护	
应用程序段已设置为无读/写权限。	段和子程序保护	

关键资产

环境：下表显示了对环境至关重要的资产：

资产	正确使用说明
工业过程控制命令	控制器通过读取输入以及向执行器发送命令来控制工业过程并向其发出命令。这些操作的可用性受到保护。
工程工作站数据流	控制器与工程工作站之间的数据流的完整性、保密性和可靠性受到保护。

环境关键资产的安全性要求：

资产	可用性	保密性	完整性	可靠性
工业过程控制命令	X			
工程工作站数据流		X	X	X

控制器：下表显示了对控制器至关重要的资产：

资产	正确使用说明
固件	固件的完整性和可靠性受到保护。
控制器内存	控制器内存包含用户加载的 PAC 配置和程序。其完整性和可靠性在运行期间受到保护。
执行模式	控制器执行模式的完整性和可靠性受到保护。
用户密码	用于执行验证的所有密码均属于机密，应由适当的用户保管。

控制器关键资产的安全性要求：

资产	可用性	保密性	完整性	可靠性
固件			X	X
控制器内存			X	X
执行模式			X	X
用户密码		X	X	

安全威胁

攻击者考虑的威胁包括控制插入到监管网络中的设备：

威胁类型	工业过程控制命令	工程工作站数据流	固件	控制器内存	执行模式	用户密码
服务拒绝	Av					
固件篡改		I、Au				
执行模式篡改					Au、I	
存储器程序篡改				I、Au		
数据流篡改	Av	Au、C、I				C、I
Av：可用性 I：完整性 C：保密性 Au：可靠性						

威胁类型	描述
服务拒绝	攻击者试图通过执行非预期操作或者利用漏洞（发送不正确的请求、使用受破坏的配置文件...），来对控制器生成服务拒绝命令。这种服务拒绝会影响整个控制器或控制器的部分功能。
固件篡改	攻击者试图对控制器注入并运行受破坏的固件。这种代码注入可能是临时的，也可能是永久的，不包含任何非预期或未授权的代码执行。用户可能尝试以合法的方式将该更新安装到控制器上。最后，攻击者就试图在没有相应权限的情况下，修改控制器上安装的固件版本。
执行模式篡改	攻击者试图在未授权情况下修改控制器的执行模式（比如，实施停止命令）。
存储器篡改	攻击者试图修改（临时或永久地）控制器内存上所运行的用户程序或配置。
数据流篡改	攻击者试图规避检测进而破坏控制器与外部组件之间数据交换。攻击者可能执行诸如证书盗窃、非法访问、或控制并命令工业过程迁移等攻击。

威胁类型	服务的持续拒绝	固件篡改	执行模式篡改	存储器篡改	数据流篡改
不正确的输入管理	X				
密码存储				X	
管理接口授权					X
访问控制策略					X
固件签名		X			

威胁类型	服务的持续拒绝	固件篡改	执行模式篡改	存储器篡改	数据流篡改
控制器内存的完整性和可靠性				X	
控制器执行模式的完整性			X		
更安全的通讯					X

威胁类型	描述
不正确的输入管理	控制器被设计成能够正确处理不正确的输入，尤其是不正确的网络通讯。
密码强度	控制器被设计成能够正确处理不正确的输入，尤其是不正确的网络通讯。 • 使用 PSK 来安装 IPsec 隧道 • 使用应用程序密码来读取 .STU Control Expert 文件，并将文件连接到控制器 • 使用其他服务密码（如 FTP）
管理接口授权	保护会话令牌不受到拦截和回放；它们的存在时间较短。在执行任何授权的操作之前，系统性地检查用户帐户的身份和权限。在每项配置中都设置应用程序密码，这有助于防止非可信用户对控制器执行任何修改。
访问控制策略	访问控制策略有助于保证授权操作（即，可能更改所识别的关键资产的操作）的可靠性。每项配置中都激活了访问控制列表 (ACL)，只有已识别的 IP 地址才能够连接到控制器。
固件签名	每当更新固件时，在更新前都要检查新固件的完整性和可靠性。
控制器内存的完整性和可靠性	每项配置中都激活了存储器保护功能，这有助于在具体的输入或输出处没有操作的情况下防止修改正在运行的程序。如未安装输入/输出模块，编程接口会被拦截。控制器能够帮助确保用户程序的完整性和可靠性，这样就只有授权用户才能够修改程序。 存储器保护还有助于确保配置保护，其中包含若干安全参数： • 访问控制策略。 • 仅限输入的运行/停止已激活。 • 存储器保护已激活。 • 启用/禁用服务（FTP、TFTP、HTTP、DHCP、SNMP、EIP、NTP）。 • Ipsec 参数。 • Syslog 参数。
控制器执行模式的完整性	控制器能够帮助确保只能由通过验证的授权用户修改执行模式。“仅限输入的运行/停止”功能被激活，这有助于防止通过以太网接口更改运行/停止状态。
加密通讯	控制器支持在完整性、保密性和可靠性方面受到保护的加密通讯（用 ESP 执行 Ipsec 加密）。FTP 协议被禁用，IPsec 能够确保通过 BMENOC0301 and BMENOC0311 模块实现 Modbus 安全通讯。

设置网络安全审计（事件记录）

记录事件和记录分析至关重要。此分析将跟踪用户操作，以便进行维护和查找异常事件，从而指示潜在的攻击活动。

完整的系统需要在所有设备中安装强大的记录系统。与网络安全相关的事件记录在本地，并使用 Syslog 协议发送到远程服务器。

在系统架构中，事件记录涉及两个部分：

- 通过 Syslog 协议接收系统中所有网络安全事件的日志服务器。
- 日志客户端（在其中监控网络安全事件的 Ethernet 连接点：设备、Control Expert）。

事件日志服务说明

每个日志客户端的角色为：

- 检测事件并为事件添加时间戳。

  需要在系统中配置单个 NTP 设备型号，以便为网络安全事件添加时间戳。
- 将检测到的事件发送到事件记录服务器。

  事件使用 Syslog 协议（RFC 5424 规范）在客户端和服务器之间交换。

  Syslog 消息遵循 RFC 5424 规范所述的格式。

  Syslog 使用 TCP 协议来完成交换。

  在设备上，当发生瞬时网络故障时，事件不会丢失。设备复位时，事件将丢失（Modicon M580 控制器固件 ≥ 4.0 时除外）。

事件类型的类别值

符合 RFC 5424 规范且与事件类型关联的 Syslog 消息类别值：

类别值	描述
0	内核消息。
1	用户级消息。
2	邮件系统。
3	系统守护进程。
4	安全/授权消息。

类别值	描述
5	Syslog 在内部生成消息。
6	行式打印机子系统。
7	网络新闻子系统。
8	UUCP 子系统
9	时钟守护进程。
10	安全/授权消息。
11	FTP 守护进程。
12	NTP 子系统。
13	日志审计。
14	日志警报。
15	时钟守护进程。
16...23	局部使用 0...7。

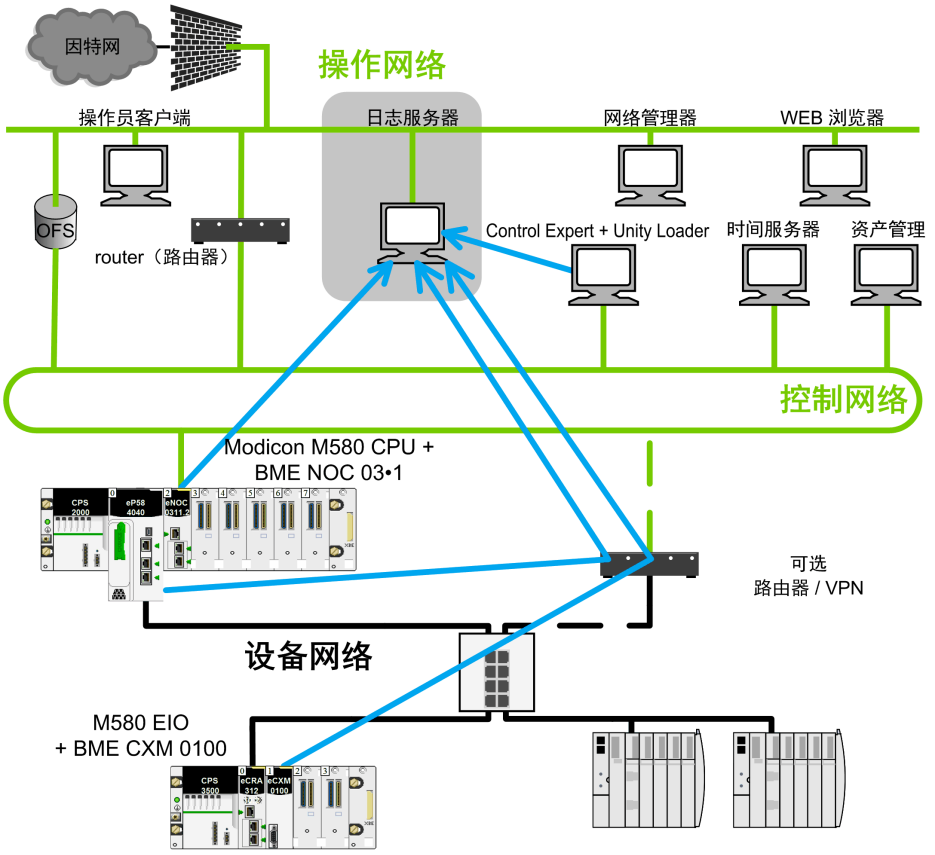
事件类型的严重性值

符合 RFC 5424 规范且与事件类型关联的 Syslog 消息严重性值：

严重性值	关键字	描述
0	Emergency	系统不可用。
1	Alert	必须立即采取操作。
2	Critical	关键状况。
3	Error	错误状况。
4	Warning	通告状况。
5	Notice	正常但重要的状况。
6	Informational	非正式消息。
7	Debug	调试级消息。

架构示例

下图突出显示系统架构中记录服务器的位置：



Modicon M580 控制器（固件版本不低于 4.10）和 BMENOR2200H（固件版本不低于 3.01）的日志事件消息结构

字段	描述
PRI	类别和严重性信息：“FACILITY”= 10，表示网络安全事件
VERSION	Syslog 协议规范的版本（版本 = 1（对于 RFC 5424））。
TIMESTAMP	时间戳格式由 RFC 3339 发布，它推荐使用以下 ISO8601 互联网日期和时间格式：YYY-MM-DD**T**hh:mm:ss.nnn**Z** **注: -**、**T**、**:**、**.**、**Z** 是必要字符，它们是时间戳字段的一部分。**T** 和 **Z** 需要以大写格式写入。**Z** 指定时间为 UTC 时间。 时间字段内容说明： • YYY：年 • MM：月 • DD：日 • hh：时 • mm：分 • ss：秒 • nnn：秒的细分单位（毫秒）（如果没有，则为 0）
HOSTNAME	识别最初发送 Syslog 消息的机器：完全限定域名 (FQDN) 或源静态 IP 地址（如果不支持 FQDN）。 源 @IP 地址 = @IP 地址 A 或 @IP 地址 B（对于 HSBY 控制器）
APP-NAME	识别发起 Syslog 消息的应用程序。它包含用于识别消息发送实体的信息（例如，商业型号的一部分）。
PROCID	发起消息的过程或协议名称（例如，Modbus、HTTPS、LocalHMI）
MSGID	事件类型的标识符（例如，CONNECTION_FAILURE_AND_BLOCK）。
事件信息	<ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="30296255-e8b7-4cf1-982e-2c45b17b1f06"><ac:plain-text-body><![CDATA[**[authn@3833], [authz@3833], [config@3833], [cred@3833], [backup@3833], [plc@3833] [system@3833]** 请参见下面的结构化数据说明。
MSG	包含事件特有结果的消息（请参见 Event Log Message Descriptions for Control Expert, 55 页）

- **STRUCTURED-DATA** 描述：必要的事件信息。
  - **[meta]**：必要的结构化数据，用于提供有关消息的元信息。其中的参数有：
    - **sequenceId**：事件标识符（达到最大值 2147483647 时，回转至 1）。
    - **sysUpTime**：当组件无法获取系统时间时，应包括此值（整数，包含自系统上次初始化以来所经过的时间（以百分之几秒计））。
- **STRUCTURED-DATA** 描述：事取决于事件类别的件信息。
  - **[authn@3833]**：用于身份验证事件的结构化数据。其中的参数有：
    - **itf**：用户所连接的接口，要么是网络端口，要么是本地接口（hmi、usb ...）。
    - **peer**：用户所连接的组件的 FQDN 或 IP 地址，以及其端口 (ipAddress:port)（如果是本地接口，则此选项为可选项）
    - **user**：用户名（组件或人），如果用户名未知，则为可选。
  - **[authz@3833]**:用于授权事件的结构化数据。其中的参数有：
    - **user**：用户名（组件或人）
    - **object**：用户的对象访问，对象取决于产品。
    - **action**：对对象执行的操作：创建、读取、更新、删除 (CRUD)
  - **[config@3833]**：用于配置事件的结构化数据。其中的参数有：
    - **object**：要配置的安全对象的名称（固件、RBAC、安全策略、设备设置、信任锚、产品相关对象）
    - **value**：新对象的可选版本或值
  - **[cred@3833]**：用于凭据管理事件的结构化数据。其中的参数有：
    - **name**：证书的公用名或用户登录名
  - **[system@3833]**：用于系统事件的结构化数据。其中的参数有：
    - **object**：更改的系统对象的名称（控制器、模块、旋转开关、SD 卡、产品相关对象）
  - **[backup@3833]**：用于备份的结构化数据。其中的参数有：
    - **object**：此对象作为已备份/还原的组件的一部分，且取决于产品。
  - 结构化数据也可由每个应用程序为特定事件定义。

Modicon M580 控制器（固件版本低于 4.10）、BMENUA0100（固件版本 1.10 和 2.0）和 BMENOR2200H（固件版本低于 3.01）的日志事件消息结构

Modicon M580 控制器固件和 BMENUA0100 的 Syslog 消息结构：

字段	描述
PRI	类别和严重性信息（下表提供说明）。
VERSION	Syslog 协议规范的版本（版本 = 1（对于 RFC 5424））。
TIMESTAMP	时间戳格式由 RFC 3339 发布，它推荐使用以下 ISO8601 互联网日期和时间格式：YYY-MM-DD**T**hh:mm:ss.nnn**Z** **注: -**、**T**、:、.、**Z** 是必要字符，它们是时间戳字段的一部分。**T** 和 **Z** 需要以大写格式写入。**Z** 指定时间为 UTC 时间。 时间字段内容说明： • YYY：年 • MM：月 • DD：日 • hh：时 • mm：分 • ss：秒 • nnn：秒的细分单位（毫秒）（如果没有，则为 0）
HOSTNAME	识别最初发送 Syslog 消息的机器。完全限定域名 (FQDN) 或源静态 IP 地址（如果不支持 FQDN）。
APP-NAME	识别发起 Syslog 消息的应用程序。它包含用于识别消息发送实体的信息（例如，商业型号的一部分）。
PROCID	发起消息的过程或协议名称（例如，Modbus、HTTPS、LocalHMI、...） 接收 NILVALUE（如果未使用）。
MSGID	识别与事件相关的消息的类型，例如 HTTP、FTP、Modbus。 接收 NILVALUE（如果未使用）。
MESSAGE TEXT	此字段包含： • 发布方地址：生成日志的实体的 IP 地址。 • 对等设备 ID：对等设备 ID，前提是，对等设备参与操作（例如，记录操作的用户名）。接收 null（如果未使用）。 • 对等设备地址：对等设备 IP 地址（如果对等设备参与操作）。未使用（空）。 • 类型：识别消息的唯一编号（请参见 Event Log Message Descriptions for Control Expert, 55 页）。 • 注释：描述消息的字符串（请参见 M580 控制器（固件版本不低于 V4.10）和 BMENOR2200H（固件版本不低于 3.01）的事件日志消息描述, 60 页）。

设置系统架构中的 Syslog 服务器

有多个 Syslog 服务器可用于不同操作系统。

注: Syslog 服务器必须符合 RFC 5424。

Syslog 服务器提供来源的示例：

- WinSyslog：用于 Windows 操作系统：

  链接：www.winsyslog.com/en/。
- Kiwi Syslog：用于 Windows 操作系统：

  链接：www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx。
- Splunk：用于 Windows 和 Unix 操作系统：

  链接：www.splunk.com/。
- Rsyslog：用于 Unix 操作系统：

  链接：www.rsyslog.com/。
- Syslog-ng：用于 Unix 操作系统的开源。

  链接：www.balabit.com/network-security/syslog-ng/opensource-logging-system。
- Syslog Server：用于 Windows 操作系统的开源。

  链接：sourceforge.net/projects/syslog-server/。

设置系统架构中的 Syslog 客户端

在 Control Expert 中未所有设备和设备类型管理器 (DTM) 管理事件记录。

事件记录功能、服务器地址和端口号以如下方式在 Control Expert 中配置，在执行了**生成**操作之后，这些参数将被发送到系统中的每个客户端：

步骤	操作
1	单击**工具 > 项目设置**。
2	单击**项目设置 > 常规 > PLC 诊断**。
3	选中**事件日志记录**复选框（缺省已取消选中）。 **注:** 只有从 Unity Pro 10.0 开始，才能打开选择了此设置的项目。 Unity Pro 是版本 13.1 或更高版本的 Control Expert 的原名。
4	输入有效的 **SYSLOG 服务器地址**和 **SYSLOG 服务器端口号**。
5	在配置了此设置后，执行**生成**（不需要选择**分析项目**）。

诊断事件记录

下表显示可用于各种设备的事件记录诊断的类型：

设备	诊断信息
Control Expert	如果与 Syslog 服务器的通讯出现错误，则会将检测到的错误记录在事件查看器中。如要在 Control Expert 中启用事件查看器，请在 Security Editor（请参阅 “EcoStruxure™ Control Expert Security Editor 操作指南”）的**策略**选项卡中，选中**审计**复选框。
BMENOC0301 and BMENOC0311 设备 DDT（*SERVICE_STATUS2* 参数）	有两个诊断信息可用： • EVENT_LOG_STATUS：值 = 1，如果事件日志服务正常运行。 值 = 0，如果事件日志服务不可操作。 • LOG_SERVER_NOT_REACHABLE：值= 1，如果 Syslog 客户端未收到 Syslog 服务器的 TCP 消息确认。 值 = 0，如果收到确认。
Modicon M580 控制器设备 DDT	
BMECXM 设备 DDT	

Event Log Message Descriptions for Control Expert

记录的事件：应用程序操作

下表显示当记录事件为以下事件时的消息描述：应用程序操作。

MSG(1)	类别	严重性	描述
创建新项目	10	6	创建新 Control Expert 应用程序
打开现有项目	10	6	打开现有 Control Expert 应用程序
保存项目	10	6	保存当前打开的应用程序
将项目另存为	10	6	使用其他文件保存当前打开的应用程序
导入项目	10	6	导入应用程序
离线生成	10	6	在在线模式下生成应用程序
在线停止状态下的生成	10	6	在在线模式控制器处于 Stop 状态时，生成应用程序
在线运行状态下的生成	10	6	在在线模式控制器处于 RUN 状态时，生成应用程序
启动、停止或初始化 PAC	10	6	启动/停止/初始化控制器
使用当前值更新初始值	10	6	使用当前值更新初始值
从 PAC 传输项目	10	6	从控制器上传应用程序

MSG(1)	类别	严重性	描述
将项目传输到 PAC	10	6	将应用程序下载到控制器
将数据值从文件传输到 PAC	10	6	将数据值从文件传输到控制器
在 PAC 中恢复项目备份	10	6	在控制器中恢复项目备份
保存到 PAC 中的项目备份	10	6	在控制器中保存项目备份
设置地址	10	6	更改控制器地址连接
修改选项	10	6	Control Expert 选项修改
修改变量值	10	6	控制器内部的变量值修改
强制内部位	10	6	控制器内部的变量强制值修改：内部位
强制输出	10	6	控制器内部的变量强制值修改：输出
强制输入	10	6	控制器内部的变量强制值修改：输入
任务管理	10	6	任务管理
任务循环时间修改	10	6	任务循环时间修改
在诊断查看器中禁用消息	10	6	在诊断查看器中禁用消息
调试可执行程序	10	6	调试可执行程序
替换项目变量	10	6	替换项目变量
创建库或系列	10	6	在库内部创建库或系列
删除库或系列	10	6	删除库内部的库或系列
将对象放入库中	10	6	将应用程序中的元素 (DFB/DDT) 复制到库中
从库中删除对象	10	6	删除库中的元素 (DFB/DDT)
从库获取对象	10	6	将库中的元素 (DFB/DDT/EF/EFB) 复制到应用程序
修改文档	10	6	修改文档（应用程序打印）
修改功能视图	10	6	修改功能视图
修改动态数据表	10	6	修改动态数据表
修改常量值	10	6	修改常量值
修改程序结构	10	6	修改程序结构
修改程序段	10	6	修改程序段
修改项目设置	10	6	修改项目设置

MSG(1)	类别	严重性	描述
变量添加删除	10	6	在数据编辑器中创建/删除变量
变量主属性修改	10	6	修改变量属性
变量次要属性修改	10	6	修改变量属性
DDT 添加删除	10	6	在数据编辑器中创建/删除 DDT
DDT 修改	10	6	在数据编辑器中修改 DDT
DFB 类型添加删除	10	6	在数据编辑器中创建/删除 DFB
DFB 类型结构修改	10	6	在数据编辑器中修改 DFB 结构
DFB 类型段修改	10	6	修改 DFB 段
DFB 实例修改	10	6	在数据编辑器中修改 DFB 实例
DFB 实例次要属性修改	10	6	在数据编辑器中修改 DFB 实例次要属性
修改配置	10	6	控制器配置修改
IO 嗅探	10	6	控制器 I/O 嗅探
修改 IO 配置	10	6	控制器 I/O 配置修改
调整 IO	10	6	控制器 I/O 配置调整
保存参数	10	6	控制器 I/O 配置从 I/O 屏幕保存参数
恢复参数	10	6	控制器 I/O 配置从 I/O 屏幕恢复参数
修改屏幕	10	6	操作员屏幕修改
修改消息	10	6	修改消息
添加/删除屏幕或系列	10	6	操作员屏幕：添加/删除系列/屏幕
移动组件	13	6	移动 FFB 块
移动组件	13	6	移动触点/线圈
插入组件	13	6	插入 FFB 块
插入组件	13	6	插入触点/线圈
删除组件	13	6	删除 FFB 块
删除组件	13	6	删除触点/线圈
添加变量	13	6	为 FFB 块设置有效参数
添加变量	13	6	为触点/线圈设置有效参数
删除变量	13	6	删除 FFB 块的有效参数
删除变量	13	6	删除触点/线圈的有效参数

MSG(1)	类别	严重性	描述
修改变量	13	6	更改 FFB 块的有效参数
修改变量	13	6	更改触点/线圈的有效参数
链路引脚	13	6	在两个引脚之间建立链路
缩放组件	13	6	更改可扩展 FFB 块的大小
缩放组件	13	6	更改垂直/水平链路的大小
重命名变量	13	6	重命名有效参数
删除行	13	6	删除一行
从...删除行	13	6	删除多行
删除列	13	6	删除一列
从...删除列	13	6	删除多列
插入行	13	6	插入一行
从...插入行	13	6	插入多行
插入列	13	6	插入一列
从...插入列	13	6	插入多列
(1) MSG 内容包括用户名、Control Expert 的 PID 以及消息的串联。			

注: HOSTNAME、APP-NAME、PROCID、MSGID 和 STRUCTURED-DATA 字段不适用于 Control Expert 消息。

记录的事件：DTM 操作

下表显示当记录事件为以下事件时的消息描述：DTM 操作。

MSG(1)	类别	严重性	描述
已完成将参数下载到设备服务，但存在错误	9	6	DTM 参数下载已完成，但存在错误
已完成将参数下载到设备服务，无错误	9	6	DTM 参数下载完成，无错误
已完成从设备服务上传参数，但存在错误	9	6	DTM 参数上传完成，但存在错误
已完成从设备服务上传参数，无错误	9	6	DTM 参数上传完成，无错误
服务上线失败	9	6	未建立到 DTM 的连接
服务上线成功	9	6	已成功连接到 DTM

MSG(1)	类别	严重性	描述
服务下线失败	9	6	未关闭到 DTM 的连接
服务下线成功	9	6	已成功关闭到 DTM 的连接
FDR 参数下载服务执行失败	9	6	未执行 DTM FDR 参数下载服务
已成功执行 FDR 参数下载服务	9	6	已成功执行 DTM FDR 参数下载服务
FDR 参数上传服务执行失败	9	6	未执行 DTM FDR 参数上传服务
已成功执行 FDR 参数上传服务	9	6	已成功执行 DTM FDR 参数上传服务
将参数下载到设备服务失败	9	6	未将参数下载到设备服务
已成功将参数下载到设备服务	9	6	已成功将参数下载到设备服务
从设备服务上传参数失败	9	6	未从设备服务上传参数
已成功从设备服务上传参数	9	6	已成功从设备服务上传参数
审计跟踪功能事件	9	6	审计跟踪功能事件
审计跟踪设备状态事件	9	6	审计跟踪设备状态事件
无设备状态消息	9	6	无设备状态消息
状态信息	9	6	状态信息
访问权限：读/写	9	6	访问权限：读/写
枚举器条目	9	6	枚举器条目
(1) MSG 内容包括用户名、Control Expert 的 PID 以及消息的串联。			

记录的事件：密码操作

下表显示当记录事件为以下事件时的消息描述：密码操作。

MSG(1)	类别	严重性	描述
网络安全 - 修改密码 > 密码不正确	2	6	更改应用程序密码时，出现问题
网络安全 - 验证密码 > 密码不正确	2	6	验证应用程序密码时，出现问题
网络安全 - 验证段密码 > 密码不正确	2	6	段密码验证出现问题
网络安全 - 数据存储密码已修改	2	6	更改了密码“DataStorage”
网络安全 - 固件密码已修改	2	6	更改了密码“FW Download”

MSG(1)	类别	严重性	描述
网络安全 - 验证密码 > 密码不正确	2	6	验证应用程序密码时，出现问题
(1) MSG 内容包括用户名、Control Expert 的 PID 以及消息的串联。			

记录的事件：更改了 SYSLOG 配置

下表显示当记录事件为以下事件时的消息描述：更改了 SYSLOG 配置。

MSG(1)	类别	严重性	描述
更改了 SYSLOG 地址	-	-	网络安全 - 更改了事件记录项目 - 事件记录、SYSLOG 服务器地址、端口或协议
(1) MSG 内容包括用户名、Control Expert 的 PID 以及消息的串联。			

记录的事件：文件操作

下表显示当记录事件为以下事件时的消息描述：文件操作。

MSG(1)	类别	严重性	描述
XXXXX 文件已打开	0	6	文件 XXXXX 已打开
与 PAC 断开连接 @=XXXXXX 驱动程序 = YYYYY	0	6	控制器已断开 = @XXXXXX 驱动程序 = YYYYYY
关闭应用程序 XXXXXX	0	6	应用程序 XXXXXX 关闭
项目已从 PAC 传输到 PC	0	6	从控制器传输到 PC
(1) MSG 内容包括用户名、Control Expert 的 PID 以及消息的串联。			

M580 控制器（固件版本不低于 V4.10）和 BMENOR2200H（固件版本不低于 3.01）的事件日志消息描述

本主题介绍了以下方面的事件日志消息：

- 固件版本不低于 4.10 的 M580 控制器（**设备**列中缩写为 **CPU**）

- 固件版本不低于 3.01 的 BMENOR2200H RTU 模块（**设备**列中缩写为“eNOR”）

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
成功连接	从用户（人或组件）到组件的所有成功连接 - 无论是通过加密协议还是通过非加密协议（如果客户安全策略允许）进行的连接	成功登录（通过 HTTPS 实现的 Web 服务器）	6	HTTPS	CONNECTION_SUCCESS	[metasequenceId=*num*] [-authn@3833 itf=*localPort* | *localInterfaceceer=peerFQDN:peerPort* user=*username*]	登录	CPU eNOR
		成功登录（通过 HTTPS 升级固件）	6	HTTPS	CONNECTION_SUCCESS	[metasequenceId=*num*] [-authn@3833 itf=*localPort* | *localInterfaceceer=peerFQDN:peerPort* user=*username*]	登录	CPU eNOR
		成功登录 (OPC-UA)	6	OPC-UA	CONNECTION_SUCCESS	[metasequenceId=*num*] [-authn@3833 itf=*localPort* | *localInterfaceceer=peerFQDN:peerPort* user=*username*]	插口连接	CPU
		成功登录（通过 Modbus-Umas 实现	6	MODBUS-UMAS	CONNECTION_SUCCESS	[metasequenceId=*num*]	登录	CPU

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
		的 Unity 应用程序密码）**仅标准模式**				[-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]		
		Modbus TCP 连接成功（无用户）	6	MODBUS	CONNECTION_SUCCESS	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]	插口连接	CPU eNOR
		HTTP/DPWS 连接成功	6	HTTP	CONNECTION_SUCCESS	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]	插口连接	CPU
		EIP 显式 TCP 连接成功（无用户）	6	EIP	CONNECTION_SUCCESS	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* |	插口连接	CPU

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
						*localInterface*peer=*peerFQDN:peerPort* user=*username*]		
		DNP3 连接成功（无用户）	6	DNP3	CONNECTION_SUCCESS	[meta sequenceId=num] [-auth-n@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=username]	插口连接	eNOR
		IEC 60870 连接成功（无用户）	6	IEC60870	CONNECTION_SUCCESS	[meta sequenceId=num] [-auth-n@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=username]	插口连接	eNOR
连接问题	从用户（人或组件）到组件的所有未成功的连接 - 无论是通过加密协议还是通过非加密协议（如果客户安全策略允	登录问题（通过 Modbus-Umas 实现的 Unity 应用程序密码）	5	MODBUS-UMAS	CONNECTION_FAILURE	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]	密码无效	CPU

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
	许）进行的连接	Modbus TCP 连接问题（无用户）	5	MODBUS	CONNECTION_FAILURE	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]	“已达到最大连接数”“过滤的数据流”	CPU eNOR
		EIP 显式 TCP 连接问题（无用户）	5	EIP	CONNECTION_FAILURE	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]	已达到最大连接数，过滤的数据流	CPU
		DNP3 连接问题（无用户）	5	DNP3	CONNECTION_FAILURE	[meta sequenceId=num] [-auth-n@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=username]	“已达到最大连接数”	eNOR
		IEC60870 连接问题（无用户）	5	IEC60870	CONNECTION_FAILURE	[meta sequenceId=num] [-auth-n@3833	已达到最大连接数	eNOR

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
						itf=localPort | localInterface peer=peerFQDN:peerPort user=username]		
由于身份验证尝试过程中出现过多问题，导致的人员用户帐户被锁定	安全策略可以请求在经过可配置的尝试次数之后阻止人员用户帐户。此事件向管理员通知潜在攻击，并且必须锁定人员用户帐户。	登录问题（通过 HTTPS 实现的 Web 服务器）。由于身份验证尝试过程中出现过多问题，导致的人员用户帐户被锁定	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]	证书无效，密码无效	CPU eNOR
		登录问题（通过 HTTPS 升级固件）。由于身份验证尝试失败的次数过多，导致人员用户帐户被锁定	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*username*]	无效证书”“无效密码”	CPU eNOR
		登录问题 (OPC-UA)。由于身份验证尝试过程中出现过多问题，导致的人员用户帐户被锁定	1	OPC-UA	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort*	证书无效，密码无效	—

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
						user=*username*]		
拒绝登录（帐户被阻止）	人员用户尝试使用已被阻止的帐户进行连接。	登录问题（通过 HTTPS 实现的 Web 服务器）。拒绝登录（帐户被阻止）	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort* user=*username*]		CPU eNOR
		登录问题（通过 HTTPS 升级固件）。拒绝登录（帐户被阻止）	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort* user=*username*]		CPU
		登录问题 (OPC-UA)。拒绝登录（帐户被阻止）	1	OPC-UA	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort* user=*username*]		—
断开连接	在不活动时长超时后，手动	HTTPS 断开连接	6	HTTPS	DISCONNECTION	[meta sequenceId=*num*]	手动注销	CPU eNOR

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
	断开人员或组件的连接。	（Web 服务器）				[-auth-n@3833 itf=*localPort* | *localInterfa-ce*peer= *peerFQDN: peerPort* user= *username*]		
		HTTPS 断开连接（固件升级）	6	HTTPS	DISCON-NECTIO-N	[meta sequencel-d=*num*] [-auth-n@3833 itf=*localPort* | *localInterfa-ce*peer= *peerFQDN: peerPort* user= *username*]	手动注销	CPU eNOR
		OPC-UA 断开连接	6	OPC-UA	DISCON-NECTIO-N	[meta sequencel-d=*num*] [-auth-n@3833 itf=*localPort* | *localInterfa-ce*peer= *peerFQDN: peerPort* user= *username*]	插口断开连接	CPU
		Modbus 断开连接	6	MODBUS	DISCON-NECTIO-N	[meta sequencel-d=*num*] [-auth-n@3833 itf=*localPort* |	插口断开连接	CPU

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
						localInterfacepeer=peerFQDN:peerPort user=*username*]		
		EIP 显式断连	6	EIP	DISCONNECTION	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*username*]	插口断开连接	CPU
		HTTP 断开连接 (DPWS)	6	HTTP	DISCONNECTION	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*username*]	插口断开连接	CPU
		超时触发的 HTTPS 断连	6	HTTPS	DISCONNECTION	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*username*]	超时注销	CPU eNOR

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
		超时触发的 OPC-UA 断连	6	OPC-UA	DISCONNECTION	[meta sequenceId=*num*] [-auth-n@3833 itf=*localPort* | *localInterfacepeer*= *peerFQDN:peerPort* user= *username*]	超时注销	—
		DNP3 断开连接	6	DNP3	DISCONNECTION	[meta sequenceId=num] [-auth-n@3833 itf=localPort | localInterface peer= peerFQDN:peerPort user= username]	插口断开连接	eNOR
		IEC 60870 断开连接	6	IEC60870	DISCONNECTION	[meta sequenceId=num] [-auth-n@3833 itf=localPort | localInterface peer= peerFQDN:peerPort user= username]	插口断开连接	eNOR
运行时的重大参数更改	运行时的重大参数更改，此更改可能对系统造	控制器应用程序参数更改：循环时间	6	配置	PARAMETER_SET	[meta sequenceId=*num*] [-config@3833	扫描时间	CPU

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
	成重大影响					object="PLC 应用程序" value=*value*]		
备份操作	备份部分或整个组件	从控制器下载应用程序	6	备份	BACKUP	[meta sequenceId=*num*] [-backup@3833 object="PLC 应用程序"]		CPU
		从 BME NUA 或 BME NOR 网页导出网络安全配置	6	备份	BACKUP	[meta sequenceId=*num*] [-backup@3833 object="网络安全配置"]		eNOR
恢复操作	恢复部分或整个组件	将控制器应用程序/配置上传到控制器中	6	配置	CONFIGURATION_CHANGE	[meta sequenceId=*num*] [-config@3833 object=*Object Object* = "PLC 应用程序" 或 "PLC 配置"		CPU
		恢复控制器中的控制器应用程序	6	备份	恢复	[meta sequenceId=*num*] [-backup@3833 object="PLC 应用程序"]		CPU
		从 BME NUA 或 BME NOR	6	备份	恢复	[meta sequenceId=*num*]		eNOR

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
		网页导入网络安全配置				[-backup@3833 object="网络安全配置"]		
固件更新	新固件已成功验证并安装。	将新固件上传到设备控制器、Copro、网页中	6	配置	FIRMWARE_UPDATE	[meta sequenceId=*num*] [-config@3833 object=*Object* value=*version*]"Object = "固件"、"安全Copro"、"网页"		CPU eNOR
固件更新无效	由于出现错误，未安装新固件。	由于版本不兼容或签名无效，未安装新固件	1	配置	FIRMWARE_INVALID	[meta sequenceId=*num*] [-config@3833 object=*Object* value=*version*]"Object = "固件"、"安全Copro"、"网页"	版本不兼容，签名无效	CPU eNOR
修改设备时间	针对更改时间和日期的人员用户请求。	—	5	配置	TIME_CHANGE	[meta sequenceId=*num*] [-config@3833 object="时间" value=*datetime*]		CPU
时间信号不在容许范围内	组件应验证通过时间同步通道接收的	—	1	配置	TIME_UNEXPECTED	[meta sequenceId=*num*] [-	时间信号不在容许范围内	

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
	时间同步消息，并且如果时间同步消息不在组件内部/本地时钟的容许范围内（过去的时间、相差甚远...），则应报警					config@3833 object="时间" value=*datetime*]		
硬件更改	检测到网络拓扑更改	网络物理端口更改：端口链路接通/断开	6	系统	HARDWARE_CHANGE	[system@3833 object=*Object*] Object = "eth"，后接十进制数字	端口链路连通，端口链路断开	CPU
		从 RSTP / HSR / PRP 检测到的任何拓扑更改	6	系统	HARDWARE_CHANGE	[system@3833 object=*Object*] Object = "eth"，后接十进制数字	端口启用 端口禁用 端口学习 端口转发 端口阻止	CPU
	检测到硬件更改	M580 SD 卡插入/拔出	6	系统	HARDWARE_CHANGE	[system@3833 object="SD卡"]	插入，拔出	CPU
操作模式更改	程序操作模式更改（Run、Stop、Init、Halt）模式，维护模式，维护模式/SafeRun/停止 SAFE 任务	—	5	系统	OPERATING_MODE_CHANGE	[system@3833 object=Object] Object = "PLC" 或 "PLC safe 任务" 或 "模块"	“Init”“Run”“Stop”“Halt”“维护模式”“安全模式”“Hsby 主设备”“Hsby 辅助设备”“Hsby 等待”“主站”“非主站”	CPU

记录的事件	描述	附加描述	严重性	PROCID	MSGID	STRUCTURED-DATA	MSG	设备
配置无效（外部网络安全）	由于出现错误，未安装新（非网络安全）配置。	数据完整性错误（控制器应用程序、...）	1	配置	CONFIGURATION_INVALID	[meta sequenceId=*num*] [config@3833 object=*Object* value=*version*]"*Object*="PLC 应用程序" 或 "模块配置"	格式无效，版本不兼容	
重启	硬件复位，或者固件上传后自动复位	—	1	系统	REBOOT	—	固件更新，复位按钮	CPU
产品证书（和/或密钥）修改	证书管理：SL1 产品自签名证书创建	—	6	凭据	CERTIFICATE_CHANGE	[meta sequenceId=*num*] [cred@3833 name=*CommonName*]	证书创建	CPU

注: 除上述结构外，每条消息还将包含以下字段和值：

- 类别 = 10
- HOSTNAME = 完全限定域名 (FQDN) 或本地 IP 地址
- APPNAME = 商业型号名称，例如 BMEP584040

Syslog 服务器消息示例

Date	Time	Priority	Hostname	Message
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="331"][authn@3833 if="eth" peer="192.168.11.50:52470"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="330"][authn@3833 if="eth" peer="192.168.11.50:52468"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="329"][authn@3833 if="eth" peer="192.168.11.50:52466"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="328"][authn@3833 if="eth" peer="192.168.11.50:52464"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="327"][authn@3833 if="eth" peer="192.168.11.50:52462"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="326"][authn@3833 if="eth" peer="192.168.11.50:52460"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="325"][authn@3833 if="eth" peer="192.168.11.50:52458"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="324"][authn@3833 if="eth" peer="192.168.11.50:52456"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="323"][authn@3833 if="eth" peer="192.168.11.50:52454"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="322"][authn@3833 if="eth" peer="192.168.11.50:52452"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="321"][authn@3833 if="eth" peer="192.168.11.50:52450"] Socket connection
11-08-2021	11:54:33	System0.Info	192.168.11.1	1 2021-08-26T11:22:12.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="320"][authn@3833 if="eth" peer="192.168.11.50:52442"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:07.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="319"][authn@3833 if="eth" peer="192.168.1.100:34246"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="318"][authn@3833 if="eth" peer="192.168.11.50:52440"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="317"][config@3833 object="Module"]
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:04.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="316"][config@3833 object="Module"]
11-08-2021	11:54:24	System0.Notice	192.168.11.1	1 2021-08-26T11:22:03.000Z 192.168.11.1 BMEP585040 System OPERATING_MODE_CHANGE [meta sequenceId="315"][system@3833 object="PLC"] Init
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="314"][config@3833 object="PLC application"]
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Backup RESTORE [meta sequenceId="313"][backup@3833 object="PLC application"]
11-08-2021	11:54:07	System0.Info	192.168.11.1	1 2021-08-26T11:21:46.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="312"][authn@3833 if="eth" peer="192.168.1.100:34235"] Socket connection
11-08-2021	11:53:20	System0.Info	192.168.11.1	1 2021-08-26T11:20:59.000Z 192.168.11.1 BMEP585040 Backup BACKUP [meta sequenceId="311"][backup@3833 object="PLC application"]

M580 控制器（固件版本低于 4.10）、BMENUA0100 和 BMENOR2200H（固件版本低于 3.01）的事件日志消息描述

本主题介绍了以下方面的事件日志消息：

- 固件版本低于 4.10 的 M580 控制器（**设备**列中缩写为“CPU”）
- BMENUA0100 OPC UA 通讯模块（**设备**列中缩写为“NUA”）
- BMENOR2200H 远程终端单元（**设备**列中缩写为“eNOR”）

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
成功连接到工具或设备，或从工具或设备成功连接 * 成功登录 * TCP 连接成功	成功登录（通过 FTP 存储数据、通过 FTP 实现的 FDR 服务器、通过 FTP 上传固件）	10	6	FTP	远程 ip 地址	Li1：成功连接 (MNT_ENG_MSG_TYP_CNCTN_SUCCES-S)	“成功登录”	CPU
	成功登录（通过 HTTPS 实			HTTPS	“(null)”		“成功登录”	NUA

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
	现的 Web 服务器）							
	成功登录（通过 HTTPS 升级固件）			HTTPS	“(null)”		“成功登录”	NUA
	成功登录 (OPC-UA)			OPC-UA	“(null)”		“成功登录”	NUA
	成功登录（通过 Modbus-Umas 实现的 Unity 应用程序密码）			DEVICE_MANAGE-R	“(null)”		“成功登录”	CPU
	成功登录（通过 HTTP 实现的 Web 服务器）			HTTP	“(null)”		“成功登录”或“成功连接”（如果没有用户登录 M580 网页）	CPU
	TCP 连接成功（无用户）。			MODBUS	远程 ip 地址		“成功连接”	CPU
	TCP 连接成功（无用户）。			EIP	“(null)”		“成功连接”	CPU
	通过 DNP3 通讯协议（关于 DNP3 主站和外站）成功连接			DNP3	远程 ip 地址		“成功连接”	eNOR
	通过 IEC60870 通讯协议（关于 IEC60870 客户端和服务器）成功连接			IEC60870	远程 ip 地址		“成功连接”	eNOR

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
与工具或设备之间的连接所存在的问题： * 由于 ACL 检查导致的 TCP 连接问题（源 IP 地址/TCP 端口过滤） * 登录问题	登录问题（通过 FTP 存储数据、通过 FTP 实现的 FDR 服务器、通过 FTP 上传固件）	10	4	FTP	远程 ip 地址	Li2：连接失败（凭据错误）(MNT_ENG_MSG_TYP_CNCTN_FAILURE)	“登录失败”	CPU
	登录问题（通过 HTTPS 实现的 Web 服务器）			HTTPS	“(null)”		“登录失败”	NUA
	登录问题（通过 HTTPS 升级固件）			HTTPS	“(null)”		“登录失败”	NUA
	登录问题 (OPC-UA)			OPC-UA	“(null)”		“登录失败”	NUA
	登录问题（通过 HTTP 实现的 Web 服务器）			HTTP	远程 ip 地址		“登录失败”或“连接失败”（如果没有用户登录）	CPU
	登录问题（通过 Modbus-Umas 实现的 Unity 应用程序密码）			DEVICE_MANAGE-R	远程 ip 地址		“登录失败”	CPU
	TCP 连接问题（无用户）			MODBUS	远程 ip 地址		“连接失败”	CPU
	TCP 连接问题（无用户）			EIP	远程 ip 地址		“连接失败”	CPU
	DNP3 通讯协议（关于 DNP3 主站和外			DNP3	远程 ip 地址		“连接失败”	eNOR

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
	站）连接问题							
	IEC60870 通讯协议（关于 IEC60870 客户端和服务器）连接问题			IEC60870	远程 ip 地址		“连接失败”	eNOR
本地或对等设备触发的断连： * TCP 断开连接 * 按需注销	对等设备/用户/本地设备触发的断连	10	6	FTP	“(null)”	Li5：对等设备/用户触发的断连 (MNT_ENG_MSG_TYP_DINECTI-ON)	“断开连接”	—
	对等设备/用户/本地设备触发的断连			HTTPS	“(null)”		“断开连接”	NUA
	对等设备/用户/本地设备触发的断连			OPC-UA	“(null)”		“断开连接”	NUA
	对等设备/用户/本地设备触发的断连			MODBUS	远程 ip 地址		“断开连接”	CPU
	—			DNP3	“(null)”或远程 ip 地址		“断开连接”	eNOR
	—			IEC60870	“(null)”或远程 ip 地址		“断开连接”	eNOR
自动注销（不活动超时）HTTPS OPC-UA	超时触发的断连	10	6	HTTPS	“(null)”	Li6：超时触发触发的断连 (MNT_ENG_MSG_TYP_DSCNCT_	“自动注销”	NUA

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
						TIMEOU-T)		
	超时触发的断连			OPC-UA			“自动注销”	NUA
系统中的重大更改：配置外的参数运行时更改	循环时间或警戒时钟控制器应用程序参数（循环时间、警戒时钟）的重大更改	13	5	DEVICE_ MANAGE-R	“(null)”	Li87：系统参数更新 (MNT_ ENG_ MSG_ TYP_ PARAME-TER_ UPDATE)	“XXXX参数更新”（带有标识该参数的 XXXX） XXXX =“循环时间” 示例：循环时间参数更新	CPU
系统中的重大更改： * 从设备下载应用程序或配置 * 从设备导出（记录）网络安全配置文件	从设备下载配置文件	13	6	MODBUS	“(null)”	Li8：从设备下载配置文件 (MNT_ ENG_ MSG_ TYP_ CONF_ DL)	“应用程序下载”或“配置下载”	CPU
				HTTPS			“网络安全配置备份”	NUA
系统中的重大更改	仅将应用程序/配置或配置上传到设备（包括 CCOTF） 将网络安全配置文件导入（恢复）到设备中	13	6	MODBUS	“(null)”	Li9：将配置文件上传到设备 (MNT_ ENG_ MSG_ TYP_ CONF_ UL)	“应用程序上传”或“配置上传”	CPU NUA
				HTTPS			“网络安全配置恢复”	NUA
系统中的重大更改	将网页上传到设备	13	6	FTP	“(null)”	Li10：将新固件上传到设备中 (MNT_ ENG_ MSG_ TYP_	“网页上传”	CPU

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
						FIRMWA-RE_ UPDATE)		
	上传新安全 copro 固件			FTP			“安全 copro 固件上传”	CPU
	将新固件上传到设备中			FTP			“固件上传”	CPU
	将新固件上传到设备中			HTTPS			“固件上传”	NUA
系统中的重大更改	修改设备时间	13	6	DEVICE_ MANAGE-R	“(null)”	LI15：修改 IED 时间	“时间重大更改”	NUA
通讯参数运行时的配置外更改成功	启用/禁用通讯服务	10	4	DEVICE_ MANAGE-R	“(null)”	Li18：任何端口，物理（串行、USB）或逻辑（telnet、FTP）激活/停用 (MNT_ ENG_ MSG_ TYP_ PORT_ MANAGE-MENT)	“主要通讯参数更新：XXXX YYYY"XX-XX = "EIP" 或 "DHCP" 或 "FTP" 或 "-MODBUS" 或 "SNMP" 或 "HTTP" 或 "-SECURIT-Y" 或 "NTP" 或 "IPSEC" 或 "DEVICE_ MANAGE-R" 仅适用于 NUA：XXXX =“仅前往控制器的 Control	CPU NUA eNOR

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
							Expert 数据流”或“仅前往设备网络的 Control Expert 数据流”或“CPU 到 CPU 数据流”仅适用于 NOR：XXXX = "DNP3 over TLS 通道["通道名称"]" 或 "IEC60870 over TLS"YYYY= “启用”或“禁用” 示例：“主要通讯参数更新：FTP 启用”	
网络物理端口更改：端口链路接通/断开	任何网络物理端口状态更改。可以是以太网端口的简单状态，也可以是从冗余系统的 RSTP/HSR/PRP 算法收集的信息	10	4	DEVICE_MANAGE-R	“(null)”	LI19：任何网络物理端口状态更改。可以是以太网端口的简单状态，也可以是从冗余系统的 RSTP/HSR/PRP 算法收集的信息 (MNT_ENG_MSG_TYP_NETWK_PORT_CHG)	“主要网络物理端口状态更改：XXXX 链路 YYYY” XXXX =“ETH”，后接端口的十进制编号或“FRONT 端口” YYYY = “链路接通”或“链路断开” 示例：“主要网络物理端口状态更改：ETH1 链路连通）	CPU NUA

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
检测到的任何拓扑更改：	从 RSTP / HSR / PRP 检测到的任何拓扑更改	10	4	RSTP	“(null)”	LI20：从冗余系统的 RSTP / HSR / PRP 算法检测到的任何拓扑更改 (MNT_ ENG_ MSG_ TYP_ NTWK_ TPLGY_ CHG)	“检测到拓扑更改”或“检测到拓扑更改：XXXX YYYY” XXXX =“ETH”，后接端口的十进制编号或“FRONT 端口” YYYY =“启用”、“禁用”、“学习”、“转发”、“阻止”	CPU NUA
完整性检查错误： * 数字签名错误， * 仅完整性（哈希 mac）	固件完整性错误	10	6	DEVICE_ MANAGE-R	“(null)”	LI84：数据完整性错误 MNT_ ENG_ MSG_ DATA_ INTEGRI-TY_ ERROR	“固件完整性错误”	CPU NUA
	数据完整性错误：CS 配置、证书、白名单或 RBAC）			DEVICE_ MANAGE-R			“数据完整性错误”	NUA
系统中的重大更改：重新启动	固件上传后重新启动	13	4	DEVICE_ MANAGE-R	“(null)”	LI14：MNT_ ENG_ MSG_ TYP_ REBOO-T_ ORDER	“重启”	CPU NUA
系统中的重大更改	控制器运行模式更改（Run、Stop、Init、Halt） 维护模式	13	5	DEVICE_ MANAGE-R	“(null)”	LI85：操作模式更改 MNT_ ENG_ MSG_ OPERATI-NG_ MODE_ CHANGE	“XXXX 状态更新：YYYY”（-XXXX 表示状态更改的对象，YYYY 表示新状态）XXXX =“PLC”或	CPU

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
	安全相关运行模式更改（SafeRun、停止 Safe 任务）						“PLC 安全任务”或“设备”YYYY =“INIT”或“STOP”或“RUN”或“HALT”或“维护模式”或“安全模式”示例：“PLC 状态更新：RUN”“PLC 状态更新：维护模式”	
系统中的重大更改：硬件更改	对 SD 卡执行操作	13	6	DEVICE_MANAGER	“(null)”	LI26：硬件更改 MNT_ENG_MSG_HARDWARE_CHANGE	“硬件更新：XXXX”（-XXXX 用于描述更新）XXXX =“SD卡插入”或“SD 卡拔出”	CPU
	转轮位置更改：复位、高级			DEVICE_MANAGER			“硬件更新：XXXX”（-XXXX 用于描述更新）XXXX =“恢复出厂模式”或“安全模式”	NUA
网络安全 RBAC 的重大更改（通过网络安全配置网页完成）。	创建用户帐户 删除用户帐户 更新用户帐户			HTTPS	“(null)”	Li11：MNT_ENG_MSG_TYP_RBAC_UPDATE	“更新 RBAC”	NUA
网络安全策略的重大更改（通过网	网络服务 事件日志 安全策略	10	4	HTTPS	“(null)”	Li12：MNT_ENG_MSG_	“主要网络安全参数更新：网络服务”“主	NUA

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
络安全配置网页完成）。	安全横幅					TYP_ SECURIT-Y_ UPDATE_ UPDATE	要网络安全参数更新：事件日志”“主要网络安全参数更新：安全策略”“主要网络安全参数更新：安全横幅”	
网络安全设备特有参数的重大更改（通过网络安全配置网页完成）。	启用/禁用和配置 IPSEC 启用/禁用和配置 OPC-UA 启用/禁用和配置 DNP3	10	4	HTTPS	“(null)”	Li13：MNT_ ENG_ MSG_ TYP_ DSS_ UPDATE	“主要网络安全参数更新：IPSEC”“主要网络安全参数更新：OPC-UA”	NUA
授权问题	不允许对用户或计算机的资源执行操作	10	4	HTTPS	“(null)”	Li21：MNT_ ENG_ MSG_ TYP_ AUTH_ REQ	“授权失败”	—
证书管理	添加/删除客户端证书	10	4	HTTPS	“(null)”	Li89：证书管理 (MNT_ ENG_ MSG_ TYP_ CERT_ MGT)	“添加客户端证书”“删除客户端证书”	NUA
证书管理： * 证书已过期	重新启动时检测服务器证书是否过期	10	3	DEVICE_ MANAGE-R	“(null)”	Li29：证书管理 (MNT_ ENG_ MSG_ TYP_ CERT_ EXPIRE)	“证书已过期”	NUA

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
eNOR 项目特有：								
身份验证问题	—	10	4	“DNP3_ Master”或“DNP3_ Outstation”	远程 ip 地址	Li100：MNT_ ENG_ MSG_ TYPE_ AUTHENTICATION_ FAILURE	“通道[“通道名称”]身份验证失败”	eNOR
非预期响应	—	10	4	“DNP3_ Master”或“DNP3_ Outstation”	远程 ip 地址	Li101：MNT_ ENG_ MSG_ TYPE_ UNEXPECTED_ RESPONSE	“通道[“通道名称”]非预期响应”	eNOR
无响应	—	10	4	“DNP3_ Master”或“DNP3_ Outstation”	远程 ip 地址	Li102：MNT_ ENG_ MSG_ TYPE_ NO_ RESPONSE	“通道[“通道名称”]无响应”	eNOR
不支持积极模式	—	10	4	“DNP3_ Master”或“DNP3_ Outstation”	远程 ip 地址	Li103：MNT_ ENG_ MSG_ TYPE_ ACGRESSIVE_ MODE_ NOT_ SUPPORTED	“通道[“通道名称”]不支持积极模式”	eNOR
不支持 MAC 算法	—	10	4	“DNP3_ Master”或“DNP3_ Outstation”	远程 ip 地址	Li104：MNT_ ENG_ MSG_ TYPE_ MAC_ ALGORITHM_ NOT_	“通道[“通道名称”]不支持 MAC 算法”	eNOR

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
						SUPPOR-TED		
不支持密钥封装算法	—	10	4	“DNP3_ Master”或“DNP3_ Outstatio-n”	远程 ip 地址	Li105：MNT_ ENG_ MSG_ TYPE_ KEYWRA-P_ ALGORIT-HM_ NOT_ SUPPOR-TED	“通道[“通道名称”]不支持密钥封装算法”	eNOR
授权问题	—	10	4	“DNP3_ Master”或“DNP3_ Outstatio-n”	远程 ip 地址	Li86：MNT_ ENG_ MSG_ TYP_ AUTHOR-IZATION_ FAILURE)	“通道[“通道名称”]授权失败”	eNOR
不允许更新密钥更改方法	—	10	4	“DNP3_ Master”或“DNP3_ Outstatio-n”	远程 ip 地址	Li106：MNT_ ENG_ MSG_ TYPE_ UPDATE_ KEY_ CHANG-E_ METHO-D_NOT_ APPORT-ED	“通道[“通道名称”]不允许更新密钥更改方法”	eNOR
签名无效	—	10	4	“DNP3_ Master”或“DNP3_ Outstatio-n”	远程 ip 地址	Li107：MNT_ ENG_ MSG_ TYPE_ INVALID_ SIGNATU-RE	“通道[“通道名称”]签名无效”	eNOR
证书数据无效	—	10	4	“DNP3_ Master”或“DNP3_	远程 ip 地址	Li108：MNT_ ENG_ MSG_	“通道[“通道名称”]证书数据无效”	eNOR

记录的事件	描述	类别	严重性	MSGID	MSG：对等设备地址	MSG：类型	MSG：应用程序消息	设备
				Outstation”		TYPE_ INVALID_ CERTIFI-CATION_ DATA		
未知用户	—	10	4	“DNP3_ Master”或 “DNP3_ Outstation”	远程 ip 地址	Li109：MNT_ ENG_ MSG_ TYPE_ UNKNO-WN_ USER	“通道[“通道名称”]未知用户”	eNOR
超过最大会话密钥状态请求	—	10	4	“DNP3_ Master”或 “DNP3_ Outstation”	远程 ip 地址	Li110：MNT_ ENG_ MSG_ TYPE_ MAX_ SESSIO-N_KEY_ STATUS_ REQ_ EXCEUD-E	“通道[“通道名称”]超过最大会话密钥状态请求”	eNOR
会话密钥更改成功	—	10	6	“DNP3_ Master”或 “DNP3_ Outstation”	远程 ip 地址	Li111：MNT_ ENG_ MSG_ TYPE_ SESSIO-N_KEY_ CHANG-E_ SUCCES-S	“通道[“通道名称”]会话密钥更改成功”	eNOR

注: 除上述结构外，每条消息还将包含以下字段和值（位于“严重性”字段后）：

- HOSTNAME = 本地 IP 地址或为空。
- APPNAME = 商业型号名称，例如 BMEP584040。
- 未使用 PROCID。
- MSG:IssuerAdress = 本地 IP 地址。
- 未使用 MSG:Peer。

控制识别和身份验证

管理帐户

以下是帐户管理的最佳做法：

- 创建没有管理权限的标准用户帐户。
- 使用标准用户帐户启动应用程序。仅在应用程序要求更高的权限级别执行其在系统中的角色时，才使用具有更多权限的帐户启动应用程序。
- 使用管理级别帐户安装应用程序。

使用 Windows 10 管理用户帐户控制 (UAC)

为了帮助尽量减少未经授权的 PC 操作系统更改，Windows 10 针对无管理权限的普通用户为应用程序授予特定权限级别。如果没有管理权限，应用程序无法更改系统。UAC 会提示用户向应用程序授予或拒绝授予其他权限。将 UAC 设置为最高级别。在最高级别下，在允许应用程序进行需要管理权限的任何更改之前，UAC 会提示用户。

如要访问 windows 10 中的 UAC 设置，请打开**控制面板 > 用户帐户和家庭安全 > 用户帐户 > 更改用户帐户控制设置**，或在 Windows 10 **开始菜单**搜索字段中输入 **UAC**。

管理密码

密码管理是加强设备的基本工具之一，是对设备进行配置以防止基于通讯的威胁的过程。建议应用以下密码管理准则：

- 在所有电子邮件以及 Web 服务器、控制器和 Ethernet 接口模块上启用密码验证。
- 安装后立即更改所有缺省密码，包括以下内容的密码：
  - Windows、SCADA、HMI 和其他系统上的用户和应用程序帐户
  - 脚本和源代码
  - 网络控制设备
  - 具有用户帐户的设备
  - FTP 服务器
  - SNMP 和 HTTP 设备
  - Control Expert
- 仅对需要访问权限的人授予密码。禁止共享密码。

- 密码输入过程中不要显示密码。
  - 要求使用很难猜测的密码。允许时，密码应该至少包含 8 个字符，并且由大小写字母、数字和特殊字符组成。
- 要求用户和应用程序根据计划间隔时间更改密码。
- 合同终止时，删除员工的访问权限帐户。
- 要求不同的帐户、系统和应用程序使用不同的密码。
- 维护管理员帐户密码的安全主列表，以便在紧急情况下可快速访问这些密码。
- 实施密码管理，以免干扰操作员对事件（如紧急关机）的响应能力。
- 请勿通过电子邮件或通过非安全互联网执行的其他方式传输密码。

管理 HTTP

超文本传输协议 (HTTP)是 Web 使用的基础协议。它用于控制系统，以支持控制产品中的嵌入式 Web 服务器。Schneider ElectricWeb 服务器使用 HTTP 通讯来藉由网页显示数据并发送命令。

如果不需要 HTTP 服务器，请将其禁用。否则，请使用安全超文本传输协议 (HTTPS)，它是 HTTP 和加密协议的组合，而不要使用 HTTP（如果可能）。通过实施访问控制机制（如限制从特定设备到特定设备的访问权限的防火墙规则），只允许特定设备的流量。

在支持此功能的产品上，您可以将 HTTPS 配置作为缺省 Web 服务器。

从可信网络将 M580 控制器的自签名证书导入至 Web 浏览器中。这有助于在连接到可信控制器的网页时防止显示通知。

注: 在续订控制器的证书时，比如在从应用程序更改控制器的 IP 地址时，必须执行此操作。

管理 FTP

文件传输协议 (FTP) 通过基于 TCP/IP 的网络（如 Internet）提供远程文件传输服务。FTP 在客户端和服务器之间使用客户端-服务器架构以及单独的控制和数据连接。

请考虑 Schneider Electric 提供的 FTP 服务的以下行为：

- FTP 协议已缺省禁用。
- FTP 协议仅是特定维护和配置活动所必需的。建议客户在不需要时禁用 FTP 服务。

- FTP 协议是非安全协议，因此必须谨慎使用，以避免敏感信息泄露以及控制器遭到未授权访问：
  - 如果可能，应更改支持 FTP 的所有设备的缺省密码。
  - 使用访问控制列表来限制与授权 IP 地址的通讯。有关相关模块的详细信息，请参阅“每个系统的网络安全服务”。
  - 使用 BMENOC 模块时，应配置 IPSEC 功能 (设置加密通讯, 33 页)。
  - 在控制室的企业网络和操作网络的范围内，阻止 FTP 的所有入站和出站通讯流。
  - 筛选特定主机的控制网络和操作网络之间的 FTP 命令，或通过单独、安全的管理网络进行传送。
  - 使用外部模块在受 Modicon 控制器影响的模块与控制网络上的工程站之间建立 VPN。
- BMENOC0301 and BMENOC0311 模块不支持到设备网络的 IP 转发。

  如果控制网络和设备网络之间需要透明，则需要外部路由器/VPN 在控制网络和设备网络之间提供加密通讯（请参阅 CSPN 安全目标, 39 页 中的示意图）。

在 FTP 协议中，从控制网络执行以下操作要求透明：

- 从 Automation Device Maintenance 更新 M580 控制器固件。
- 通过 SNMP 服务从网络管理工具执行的 Modicon M580 控制器网络诊断

管理 SNMP

简单网络管理协议协议 (SNMP) 可在集中管理控制台和网络设备（如路由器、打印机和控制器）之间提供网络管理服务。该协议包括以下三个部分：

- 管理器：一种应用程序，用于通过发出请求、获取响应以及监听和处理代理发出的陷阱，来管理网络上的 SNMP 代理。
- 代理：位于受管理设备中的网络管理软件模块。代理允许管理器更改配置参数。受管理设备可以是任何类型的设备：路由器、访问服务器、交换机、网桥、集线器、控制器、驱动器。
- 网络管理系统 (NMS)：管理员用来执行管理任务的终端。

Schneider Electric Ethernet 设备具有用于网络管理的 SNMP 服务能力。

通常会自动安装 SNMP，其中 **public** 作为读取字符串、**private** 作为写入字符串。此类安装允许攻击者在系统上进行侦查以拒绝服务。

使用 SNMP 来帮助降低攻击风险：

- 如果需要使用 SNMP v1，请使用访问设置限制可访问交换机的设备（IP 地址）。将不同的读取以及读取/写入密码分配给设备。
- 更改支持 SNMP 的所有设备的缺省密码。

- 在控制室的企业网络和操作网络的范围内，阻止 SNMP 的所有入站和出站通讯流。
- 筛选特定主机的控制网络和操作网络之间的 SNMP v1 命令，或通过单独、安全的管理网络进行传送。
- 通过识别有权查询 SNMP 设备的 IP 地址来控制访问。
- 使用外部模块在受 Modicon 控制器影响的模块与控制网络上的工程站之间建立 VPN。

管理 Control Expert 应用程序、段、数据存储和固件密码

在 Control Expert 中，密码适用于以下情形（取决于控制器）：

- **应用程序**

  通过密码进行 Control Expert 和控制器应用程序保护，有助于防止意外的应用程序修改、下载或打开（.STU、.STA and .ZEF 文件）。密码加密存储在应用程序中。

  除密码保护外，您还可以对 .STU、.STA 和 .ZEF 文件加密。Control Expert 中的文件加密功能有助于防止遭到无权限人员的非法更改，并加强了知识产权的防盗保护以及对其他恶意意图的防护。文件加密选项受密码机制保护。

  注: 当将控制器作为系统项目的一部分进行管理时，应用程序密码和文件加密在 Control Expert 编辑器中处于禁用状态，并且需要使用拓扑管理器来管理。

  有关更多详情，请参见应用程序保护 主题（请参阅“EcoStruxure™ Control Expert 操作模式”）。

- **段**

  可在离线模式下，从项目的**属性**屏幕访问段保护功能。此功能用于帮助保护程序段。有关更多详情，请参见段和子程序保护主题（请参阅“EcoStruxure™ Control Expert 操作模式”）。

  注: 只要项目中的保护未激活，段保护就处于未激活状态。

- **数据存储/Web**

  通过密码进行的数据存储保护有助于防止对 SD 存储卡数据存储区域的意外访问（如果控制器中已插入有效的存储卡）。它还可有助于防止对 Web 诊断数据的意外访问（M580 控制器固件 ≥ 4.0 时）。有关更多详细信息，请参见数据存储保护主题（请参阅“EcoStruxure™ Control Expert 操作模式”）。

- **固件**

  通过密码进行的下载保护有助于防止下载恶意固件。有关更多详情，请参见固件保护主题（请参阅“EcoStruxure™ Control Expert 操作模式”）。

控制授权

Control Expert Security Editor

使用安全配置工具来定义软件用户及其相应授权。EcoStruxure Control Expert 访问安全性只影响安装软件的终端，不影响项目，因为项目有自己的安全保护系统。

有关详细信息，请参阅 *EcoStruxure™ Control Expert, Security Editor, Operation Guide*。

建议为安全管理员 (*SecurityAdmin*) 设置专门密码，并用限制性用户类型限制其他用户权限。

编程和监控模式

可通过两种模式在**在线**模式下访问控制器：

- **编程**模式：可修改控制器程序。当终端首次连接到控制器时，控制器变为保留状态，只要控制器为保留状态，就无法连接别的终端。
- **监控**模式：控制器程序无法修改，但变量可以修改。监控模式不会保留控制器，可以在监控模式下访问已保留的控制器。

如要在 EcoStruxure Control Expert 中选择模式，轻选择：**工具 > 选项... > 连接 > 缺省连接模式**。

有关这些模式的更多详细信息，请参见在线模式下的服务主题（请参阅“EcoStruxure™ Control Expert 操作模式”）。

如果可能，建议将**在线**控制器访问模式设置为**监控**。

程序段保护

在离线模式下，可以从项目的**属性**屏幕访问段保护功能。此功能用于保护程序段。有关更多详情，请参见段和子程序保护主题（请参阅“EcoStruxure™ Control Expert 操作模式”）。

注: 只要未在项目中激活段保护，则该保护就一直处于非活动状态。

建议激活段保护。

控制器存储器保护

对于任意通讯通道，存储器保护功能禁止在在线模式下将项目传输至控制器以及进行修改。

注: 控制器存储器保护不能用热备控制器来配置。在这种情况下，请使用 IPsec 加密通讯。

存储器保护的激活方式如下：

- Modicon M340 控制器：输入位。有关详细信息，请参阅配置 *Modicon M340* 处理器章节（请参阅“EcoStruxure™ Control Expert 操作模式”）。
- Modicon M580 控制器：输入位。有关详细信息，请参阅 管理运行/停止输入章节（请参阅“Modicon M580 硬件参考手册”）。
- Modicon Quantum 控制器：控制器模块上的物理键开关（对于低端（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum 硬件参考手册”）或高端（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum 硬件参考手册”）控制器）。
- Modicon Premium 控制器：输入位。有关更多详细信息，请参阅配置 *Premium* 处理器章节（请参阅“EcoStruxure™ Control Expert 操作模式”）。
- Modicon MC80 控制器：输入位。有关详细信息，请参阅 Modicon MC80 Program Logic Controller (PLC) User Manual。
- Modicon Momentum MDI 控制器：输入位。有关详细信息，请参阅“EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide”。

建议尽可能激活控制器存储器保护。

控制器远程运行/停止访问

远程运行/停止访问管理定义如何远程启动或停止控制器，并且这种管理取决于系统。

注: 无法使用热备控制器来配置控制器远程运行/停止访问。在这种情况下，请使用 IPsec 加密通讯。

控制器	访问
Modicon M580:	控制器远程运行/停止访问允许执行以下其中一项操作： • 通过请求远程停止或运行控制器。 • 通过请求远程停止控制器。拒绝远程运行控制器的请求。当配置了有效输入时，只能运行由输入控制的运行。 • 拒绝通过请求远程停止或运行控制器的请求。 请参阅管理运行/停止输入章节，以了解有助于防止远程命令访问运行/停止模式的控制器配置选项（请参阅“Modicon M580 硬件参考手册”）。

Modicon M340:	控制器远程运行/停止访问允许执行以下其中一项操作： • 通过请求远程停止或运行控制器。 • 通过请求远程停止控制器。拒绝远程运行控制器的请求。当配置了有效输入时，只能运行由输入控制的运行。 请参阅“配置 *Modicon M340* 处理器”章节（请参阅“EcoStruxure™ Control Expert 操作模式”）。
Modicon Premium:	控制器远程运行/停止访问允许执行以下其中一项操作： • 通过请求远程停止或运行控制器。 • 通过请求远程停止控制器。拒绝远程运行控制器的请求。当配置了有效输入时，只能运行由输入控制的运行。 请参阅“配置 *Premium* 处理器”章节（请参阅“EcoStruxure™ Control Expert 操作模式”）。
Modicon Quantum:	控制器远程运行/停止访问允许： • 通过请求远程停止或运行控制器。
Modicon MC80:	控制器远程运行/停止访问允许执行以下其中一项操作： • 通过请求远程停止或运行控制器。 • 通过请求远程停止控制器。拒绝远程运行控制器的请求。当配置了有效输入时，只能运行由输入控制的运行。 • 拒绝通过请求远程运行或停止控制器。 请参阅 Modicon MC80 Program Logic Controller (PLC) User Manual 中的配置 *Modicon MC80* 处理器章节。
Modicon Momentum MDI	控制器远程运行/停止访问允许执行以下其中一项操作： • 通过请求远程停止或运行控制器。 • 通过请求远程停止控制器。拒绝远程运行控制器的请求。当配置了有效输入时，只能运行由输入控制的运行。 请参阅 Modicon Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide 中的 配置 *Modicon Momentum MDI* 处理器章节。

建议拒绝通过请求远程运行或停止控制器。

控制器变量访问

为了有助于保护控制器数据免受未授权的读取或写入访问，尽可能使用以下最佳做法：

- 使用非定位数据。
- 配置 EcoStruxure Control Expert 以仅存储 HMI 变量：**工具 > 项目设置... > PLC 嵌入式数据 > 数据字典 > 仅 HMI 变量。**

  只有在选择了**数据字典**的情况下，才能选择**仅 HMI 变量。**

- 将通过 HMI 或 SCADA 访问的变量标记为 *HMI*。未标记为 *HMI* 的变量无法通过外部客户端访问。
- 与 SCADA 的连接必须依靠 OFS。

数据存储器保护

您可以在 EcoStruxure Control Expert 中激活数据存储器保护，方法是：导航到**工具 > 项目设置 > PLC 嵌入式数据**，然后选择**应用**。此功能有助于同时保护定位和非定位数据。

有关数据存储器保护功能的更多信息，请参阅“EcoStruxure Control Expert 操作模式”文档中的主题数据存储器保护。

管理数据完整性检查

简介

Control Expert 中的自动完整性检查功能有助于防止 Control Expert 文件和软件遭到病毒或恶意软件篡改。您也可以手动启动完整性检查。

自动完整性检查。

包含拓扑管理器的 Control Expert 基于客户端/服务器架构。

服务器被配置为在计算机通电或重启时自动启动。在服务器启动之前，会对这两者执行完整性检查。

服务器仅在完整性检查完成且未检测到数据损坏时启动。如果完整性检查检测到数据损坏，则会记录错误，您可以使用**事件查看器**来查看此错误。

出现一个消息框，指示损坏的文件。单击**确定**，Control Expert 实例随即关闭。有关详细信息，请参阅 *EcoStruxure Control Expert* 安装手册，以及主题启用与远程客户端的通讯并增强安全性。

使用 Control Expert Classic 执行手动完整性检查

如要在启动 Control Expert Classic 的实例时执行手动完整性检查，请执行以下步骤：

步骤	操作
1	单击**帮助 > 关于 Control Expert XXX。**
2	在**完整性检查**字段中，单击**执行自检。** **结果**：完整性检查在后台运行。Control Expert 会创建成功和失败组件登录的日志。日志文件包含登录的 IP 地址、日期和时间以及结果。 **注:** 如果完整性检查显示组件登录失败，**事件查看器**会显示一条消息。单击**确定。**手动修复日志中的条目。

使用 Control Expert 执行手动完整性检查

如要在启动 Control Expert 的实例时执行手动完整性检查，请执行以下步骤：

步骤	操作
1	单击拓扑管理器工具栏中的**帮助 > 关于...。**
2	在**关于**框中，单击链接**执行自检。** **结果**：完整性检查在后台运行。扫描在客户端所连接的本地客户端（本地或远程）上执行。客户端和服务器将一直运行，直到返回完整性检查结果。 有关完整性检查结果的相应后果，请参见下表。

如果	则
未检测到数据损坏	显示消息自检成功完成。单击**确定。**
在客户端上检测到数据损坏	出现一个消息框，指示损坏的文件。单击**确定**，Control Expert 客户端随即关闭。
在其中一个服务器上检测到数据损坏	服务器停止。会记录错误，您可以使用**事件查看器**来查看此错误。

M580 固件完整性检查

M580 控制器固件完整性检查在新固件上传或 Modicon M580 PAC 重启之后将自动执行。

SD 卡管理

激活应用程序签名，以避免从 SD 卡运行不正确的应用程序。

使用 SIG_WRITE 和 SIG_CHECK 函数（请参阅 *EcoStruxure™ Control Expert, Communication, Block Library*）管理 SD 卡签名。

配置 SD 卡端口保护

SD 卡保护机制适用于固件版本不低于 4.30 的控制器。

此功能可通过控制器网页上的**配置**选项卡来启用或禁用。

打开**主页**。

步骤	操作
1	打开因特网浏览器。
2	在地址栏中，输入分配给控制器的 IP 地址。
3	输入用户名 **modbususer** 和应用程序密码。
4	按 **Enter**，等待页面打开。
5	选择**配置 > 网络安全**。
6	在下拉列表中，选择 **SD 卡端口**以配置此功能： • **已启用**（控制器不考虑 SD 卡）。 • **已禁用**（控制器考虑 SD 卡）。 **注:** 如果 SD 卡已插入控制器中，则在移除 SD 卡或对控制器执行电源重置时，会激活保护。 **注:** 启用了 SD 卡端口保护后，控制器备份存储区为控制器 NAND。因此，如果启用了保护，则在清除备份区时，会清除控制器 NAND。

配置 Control Expert 与 M580 以太网控制器之间的安全工程链路

兼容性

- M580 PV < 25（白色控制器），PV >= 25（灰色控制器）。
- Control Expert Classic 和 Control Expert Topology Manager V16.0 及更高版本。
- M580 固件 V4.20 及更高版本。
- Control Expert应用程序 V4.20 及更高版本。

安全连接的用途

使用上文所述的软件、硬件和应用程序版本，您可以配置 Control Expert 与 M580 以太网控制器之间的安全连接。此连接基于传输层安全 (TLS) 协议，并提供端到端加密通讯。

安全工程链路通过提供以下功能来帮助保护 M580 控制器免受网络攻击：

- 依赖于自签名 M580 证书的控制器身份验证。
- 对 Control Expert 与 M580 控制器之间的数据流加密。
- 通过要求登录名/密码来提供 Control Expert 客户端身份验证，以建立 HTTPS 通道。

安全连接有助于防止以下网络攻击：

- 重播攻击。
- 密码恢复（散列）。
- 应用程序二进制恢复。
- 可能修改数据或应用程序的中间人 (MITM) 攻击。

安全连接的相关功能

下列功能已被添加到 **Security Editor**、M580 控制器固件和 Control Expert，以支持安全工程链路的创建：

- 安全通讯协议驱动程序, 98 页
- 三种工程链路模式, 98 页

通讯协议驱动程序

HTTPS 和 **HTTPS via USB** 是支持安全工程链路的新驱动程序。

注: 为了清晰起见，两个先前存在的驱动程序已被重命名：

- **TCPIP** 现在为 **Modbus TCP**
- **USB** 现在为 **Modbus TCP via USB**

工程链路模式

根据要达到的网络安全级别，可以选择以下三种**工程链路模式**中的一种：

- **完全访问**：

  控制器的工作方式与在以前的固件版本中一样。接受安全和非安全通讯。

  - 对于 Control Expert 通讯，控制器接受 **Modbus TCP** 和 **Modbus TCP via USB** 非安全驱动程序或 **HTTPS** 和 **HTTPS via USB** 安全驱动程序。
  - 对于 SCADA 或控制器到控制器通讯，接受 **Modbus TCP**（端口 502）。

- **已过滤**（缺省）：

  一种混合模式，藉由它，您可以在工程链路上应用网络安全，并在连接到 SCADA 或其他控制器的链路上应用非安全连接。

  - 对于 Control Expert 通讯，控制器接受 **HTTPS** 和 **HTTPS via USB** 安全驱动程序。
  - 对于 SCADA 或控制器到控制器通讯，接受 **Modbus TCP**（端口 502）或 **UMAS** (OFS)。

    注: 在**已过滤**模式中，控制器接受 **Modbus TCP** 和 **Modbus TCP via USB** 非安全驱动程序，但在项目的选项中，**连接模式**必须设置为**监控**。监控模式为只读模式，在这种模式下，无法将应用程序下载到控制器，也无法停止控制器。

- **已强制**（缺省）：

  此模式提供最高安全级别。控制器仅接受安全协议。

  - 对于 Control Expert 通讯，控制器仅接受 **HTTPS** 和 **HTTPS via USB** 安全驱动程序。
  - 对于 SCADA 或控制器到控制器通讯，**不**接受 **Modbus TCP**（端口 502）或 **UMAS** (OFS)。

注: 如果配置了**完全访问**模式且使用 **HTTPS** 或 **HTTPS via USB** 安全驱动程序，可能会对应用程序下载时间产生重大影响。如果您希望使用安全驱动程序，请考虑使用**已过滤**或**已强制**模式，以保持性能。

协议可用性概述

每个**工程链路模式**选项都支持逻辑端口和通讯协议组合，具体如下：

链路用途：		**安全工程链路**	**非安全工程链路**		**HMI / SCADA**
驱动程序：		**HTTPS 或 HTTPS via USB**	**Modbus TCP 或 Modbus TCP via USB**		Modbus TCPIP 或 UMAS
通讯逻辑端口：		443	502		502
连接模式：		**监测或编程**	**编程**	**监控**	不适用
工程链路模式：	已强制	✓	✗	✗	✗
	已过滤	✓	✗	✓	✓
	完全访问	✓	✓	✓	✓

Security Editor 证书白名单

Security Editor 中引入了**证书白名单**，它包括以下功能：

- **添加**：使用此命令，可配置要创建安全工程链路的 M580 控制器的 IP 地址。
- **获取证书**：使用此命令，可从设备获取 HTTPS 证书。
- 它会打开一个对话框，让您能够信任证书并将其添加到 Windows 证书存储库。
- **查看证书**：使用此命令，可显示和验证证书。
- **删除**：使用此命令，可从列表中删除证书。

注: 在此版本中，仅支持自签名证书。

配置安全连接程序

使用 Control Expert 和 Security Editor，通过执行下述任务，来完成安全工程链路的配置。

初步任务

1. 将控制器升级至：
   a. V4.20 或更高版本（对于标准控制器）。
   b. V4.21 或更高版本（对于安全控制器）。

2. 将 Control Expert 升级到 V16.0 或更高版本。
3. 打开现有项目并将应用程序级别更改为 V4.20 或更高版本，或者创建应用程序级别为 V4.20 或更高版本的新项目。
4. 在控制器的“安全”选项卡中启用 HTTPS（如已禁用）。
5. 选择工程链路模式设置（请参阅工程链路模式）。
6. 如果先前未配置最终的 M580 以太网控制器 IP 地址设置，则配置这些设置。

   注: 由于 M580 控制器的证书包含其 IP 地址，因此每次更改 IP 地址设置时，控制器都会续订其证书。每次都必须在 Security Editor 中信任证书。
7. 为新项目创建应用程序密码。
8. 为新项目创建固件和 Web 密码。
9. 使用 **Modbus TCP** 或 **Modbus TCP via USB**将应用程序下载到控制器。

任务 1：在 Security Editor 中信任 M580 证书

1. 打开 Security Editor。
2. 首次启动 Security Editor 时，请为 SecurityAdmin 配置密码，然后等待 Security Editor 安装。
3. 使用配置的密码以 SecurityAdmin 身份登录。
4. 选择**证书白名单**选项卡。
5. 单击**添加**。**添加连接配置**对话框随即打开。
6. 选择 **HTTPS** 或 **HTTPS over USB** 作为 **通讯协议**。然后将 **IP 地址**设置为控制器的已配置的 IP 地址。
7. 单击**确定**。
8. 选择与控制器对应的行。
9. 单击**信任证书**，然后单击**是**以添加证书。

   “证书状态”列将更新，并指示：
   - 有效：已成功添加证书。
   - 未知：未添加证书。使用工具提示查看检出错误详细信息。
10. 如果证书有效，请单击省略号 (...) 以显示其设备名称和详细信息。

任务 2：配置安全连接

1. 在 Control Expert 中，选择 **PLC > 设置地址...**。

2. 在 PLC 区域中，输入 M580 控制器的 IP 地址，或者如果正使用 USB 电缆，则输入 SYS。
3. 在**通讯协议**区域中，选择 **HTTPS** 或 **HTTPS via USB**。
4. 单击**确定**。
5. 在 Control Expert 中，选择 **PLC > 连接**。
6. 输入应用程序密码。

运行模式注意事项

开箱即用通讯

首次启动新开箱的 M580 控制器时，将适用以下限制：

- 不支持 Control Expert 与 M580 控制器之间的 HTTPS 连接。
- 只能使用 USB 或 TCPIP 进行通讯。

将 M580 控制器复位为 NOCONF

可以通过以下方式将 M580 控制器切换到 NOCONF：

- 设置旋钮以复位热备 M580 控制器。
- 按照以下方式使用 SD 卡：
  1. 在不使用密码的情况下，创建应用程序。
  2. 将应用程序加载到同型号的其他 M580 控制器中。
  3. 将 SD 卡插入此控制器。
  4. 将 %S66 设置为 TRUE，以将应用程序备份到 SD 卡上。
  5. 将 SD 卡插入原 M580 控制器中，并重置控制器电源。

复位应用程序密码

在**已过滤**和**完全访问工程链路模式**中，仍然可以通过技术支持复位应用程序密码。

支持在线更改应用程序密码。

强制安全性编程兼容性和限制

兼容性

请参阅主题配置 Control Expert 与 M580 以太网控制器之间的安全工程链路, 97 页。

工程链路模式限制

对于任何物理连接，**已强制工程链路模式**选项适用以下限制：

- 数据字典功能无效。
- “已强制”工程链路模式不支持 BMENUA0100••。
- 升级到产品版本 (PV) 不低于 3 的 M580。
- 无法使用以下功能块来访问控制器：
  - READ_VAR
  - WRITE_VAR
  - DATA_EXCH
  - READ_REMOTE
- Modbus 扫描器无法扫描控制器。
- M580 控制器的 Modbus 扫描器无法扫描 Modbus 设备。
- 根据所选的通讯协议（Modbus TCP 或 EtherNet/IP），某些 DTM 诊断服务不可用，具体如下：

DTM 服务	协议	可用性
EtherNet/IP DTM 连接	EtherNet/IP	✓
EtherNet/IP DTM 断开	EtherNet/IP	✓
Modbus DTM 连接	Modbus TCP	✗
Modbus DTM 断开	Modbus TCP	✗
以太网诊断	EtherNet/IP	✓
带宽诊断	Modbus TCP	✗
RSTP 诊断	Modbus TCP	✗
网络时间服务诊断	EtherNet/IP	✓

通讯适配器兼容性

下表总结了根据所选择的工程模式控制器或通讯适配器可用的服务。

行对应于可用的服务：

- 工程链路：Control Expert 与控制器之间的连接。
- 客户端模式通讯：扫描器、Modbus、EtherNet/IP（隐式或显式）、OPCUA、DNP3、IEC 61850。
- 服务器模式通讯：Modbus、EtherNet/IP、OPCUA、DNP3、IEC 61850。

列对应于不同的可能配置。例如：

- 仅控制器：控制器在使用时不搭配任何通讯适配器。
- 控制器 + NOC（背板开）：主机架中存在控制器和 BMENOC03••；BMENOC03•• 的背板端口已启用；Control Expert 连接到 BMENOC03••。
- 控制器 + NOC（背板关）：主机架中存在控制器和 BMENOC03••；BMENOC03•• 的背板端口已禁用；Control Expert 连接到 BMENOC03••。

使用通讯适配器时，某些服务在通讯适配器本身上提供，或者通过通讯适配器从控制器提供。为了区分这两种情况，需要使用字母“C”表示控制器，使用字母“M”表示模块。例如：

- 如果可以使用控制器的 IP 地址建立从 Control Expert 到控制器的连接，则使用字母“C”。
- 如果使用 BMENUA0100 的 IP 地址建立源自 Control Expert 的连接，则应用与该模块相关的列中的字母“M”。

Modicon M580 系统		仅控制器			控制器 + NOC（NOC301、NOC311、NOC321）			控制器 + NOC（NOC301、NOC311、NOC321）			控制器 + NOC321			控制器 + NUA（安全模式）			控制器 + BMXNOR			控制器 + BMENOR			控制器 + NOP			控制器 + NOP		
通讯适配器参数					背板 端口已启用			背板 端口已禁用			背板 端口已禁用 IP 转发			IP 转发			背板 隔离			背板 端口已禁用			背板 端口已启用 无 IP 转发			背板 端口已禁用 IP 转发		
拓扑																												
安全模式																												
工程链路	HTTPS	C	C	C	C	C	C	X	X	X	C	C	C	C* M	C* M	X	X	X	X	X	X	X	C	C	C	X	X	X
	Modbus TCP 监控	C	C	X	C M	C M	X	C	C	X	C	C	X	C* M	C* M	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X
	Modbus TCP 编程	C	X	X	C M	X	X	C	X	X	C	X	X	C* M	X	X	M	X	X	M**	X	X	C M	X	X	M	X	X
客户端模式	Modbus IO 扫描器	C	C	X	C M	C M	M	M	M	M	C M	C M	M	C*	C*	X	-	-	-	-	-	-	C	C	X	-	-	-
	EIP 扫描器	C	C	C	C M	C M	C M	M	M	M	C M	C M	C M	C*	C*	C*	-	-	-	-	-	-	C	C	C	-	-	-
	EFB Modbus	C	C	X	C	C	X	C	C	X	C	C	X	C*	C*	X	C	C	X	C	C	X	C	C	X	C	C	X
	EFB EIP	C	C	C	C	C	C	C	C	C	C	C	C	C*	C*	C*	C	C	C	C	C	C	C	C	C	C	C	C
	EFB OPCUA	C	C	C	-	-	-	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	-	C	C	C	C	C	C
	DNP3 IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X

Modicon M580 系统		仅控制器			控制器 + NOC（NOC301、NOC311、NOC321）			控制器 + NOC（NOC301、NOC311、NOC321）			控制器 + NOC321			控制器 + NUA（安全模式）			控制器 + BMXNOR			控制器 + BMENOR			控制器 + NOP			控制器 + NOP		
通讯适配器参数					背板端口已启用			背板端口已禁用			背板端口已禁用IP 转发			IP 转发			背板隔离			背板端口已禁用			背板端口已启用无 IP 转发			背板端口已禁用IP 转发		
拓扑																												
安全模式																													
服务器模式	Modbus 服务器 / UMAS	C	C	X	M	M	X	M	M	X	C	C	X	C* M-*	C* M*	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X
SCADA 通讯	OPCUA 服务器	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	-	-	-	-	-	-	-	-	-	-	-	-
	EtherNet/IP 适配器（本地服务器）	C	C	C	M	M	M	M	M	M	C M	C M	C M	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	控制器的 HTTPS Web 服务器	C	C	C	C	C	C	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	-	C	C	C	-	-	-
	DNP3 - IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X

符号	描述
	工程链路模式设置为**完全访问**
	工程链路模式设置为**已过滤**
	工程链路模式设置为**已强制**
C	• 在客户端模式“C”下，表示通讯由控制器发起。 • 在服务器模式“C”下，表示目标 IP 地址为控制器。
M	• 在客户端模式“M”下，表示通讯由通讯适配器发起。 • 在服务器模式“M”下，表示目标 IP 地址为通讯适配器。 在这两种情况下，模块都通过 XBUS 与控制器通讯。
X	不支持
*	取决于 BMENUA0100 模块中配置的转发规则。
**	如果 BMENOR00200 中启用了 Modbus 服务器
-	不适用

M580 以太网服务和端口

本主题介绍可用的 M580 以太网服务及其在 Control Expert 应用程序中的缺省状态。

“开箱”表示配置适用于未安装任何应用程序的出厂控制器。在控制器上安装应用程序后，将再也无法实现这种“开箱”配置。

“缺省”表示该配置适用于缺省 Control Expert 应用程序。

固件版本不低于 4.10 的 M580 控制器

服务	端口号	开箱	缺省	备注
HTTP	80/tcp	已关闭	已关闭	Web 服务器
Modbus TCP	502/tcp	已打开	已打开	-
EtherNet/IP	44818/tcp-udp	已关闭	已关闭	EtherNet/IP 显式（3 类）
DHCP	67/udp	已关闭	已关闭	-
FTP	21/tcp	已打开	已关闭	固件、数据存储、FDR
TFTP	69/udp	已关闭	已关闭	FDR (X80)
SNMP	161/udp	已关闭	已关闭	-
EtherNet/IP	2222/udp	已关闭	已关闭	EtherNet/IP 隐式（1 类）
NTP/SNTP	123/udp	已关闭	已关闭	NTPV4 或 SNTP

固件版本低于 4.10 的 M580 控制器

服务	端口号	开箱	缺省	备注
HTTPS	443/tcp	已打开	已打开	Web、固件、数据存储
Modbus TCP	502/tcp	已打开	已打开	注(1)
EtherNet/IP	44818/tcp-udp	已关闭	已关闭	EtherNet/IP 显式（3 类）
DHCP	67/udp	已关闭	已关闭	-
FTP	21/tcp	已关闭	已关闭	FDR
TFTP	69/udp	已关闭	已关闭	FDR (X80)

服务	端口号	开箱	缺省	备注
SNMP	161/udp	已关闭	已关闭	-
EtherNet/IP	2222/udp	已关闭	已关闭	EtherNet/IP 隐式（1 类）
NTP/SNTP	123/udp	已关闭	已关闭	NTPV4 或 SNTP
DPWS	9867/tcp	已打开	已打开	固件更新，注(1)
WS-Discovery	3702/udp	已关闭	已关闭	与 SNMP 的状态同步
注(1)：端口和相关服务是客户的首要需求，用以确保基本功能可以在所需的工业环境下运行。该端口保持打开，以保证安全性和可用性。用户无法禁用该端口。				

每个系统的网络安全服务

简介

本章列出了每个系统可用的网络安全服务，并指明在 Control Expert 帮助中的何处查看详细信息。

网络安全服务

概述

软件、DTM 或设备是在全局系统中提供网络安全服务的元素。针对以下元素列出了可用的网络安全服务：

- Control Expert , 110 页 软件
- Modicon M340 , 110 页控制器
- Modicon M580 , 111 页控制器
- Modicon Quantum 控制器和通讯模块, 112 页
- Modicon X80 模块, 113 页
- Modicon Premium/Atrium 控制器和通讯模块, 113 页
- Modicon Momentum MDI, 114 页
- Modicon MC80, 115 页

下面列出的网络安全服务在上一章节中进行了说明：

- 禁用未使用的服务, 29 页
- 访问控制, 30 页
- 设置加密通讯, 33 页
- 事件记录, 48 页
- 身份验证, 87 页
- 授权, 91 页
- 完整性检查, 94 页

Unity Pro/Control Expert 软件中的网络安全服务

Unity Pro 是版本 13.1 或更高版本的 Control Expert 的原名。

网络安全服务可用性

软件	网络安全服务							
版本	禁用未使用的服务	访问控制	加密通讯	保密的加密通讯	事件记录	身份验证	授权	完整性检查
Unity Pro v8.1	–	N.A.	–	–	–	X	X	X
Unity Pro≥v10.0	–	N.A.	X	–	X	X	X	X
Unity Pro≥v13.0	–	N.A.	X	X	X	X	X	X
Control Expert≥-v14.0	X	X	X	X	X	X	X	X

X 可用，至少一个服务已实现。

- 不可用

N.A. 不适用

在为不低于 v4.01 的 M580 固件版本使用不低于 v.15.1 的 Control Expert 版本时，有更强大的密码恢复机制可用。

Modicon M340 控制器中的网络安全服务

Modicon M340 控制器中的最低固件版本和网络安全服务可用性：

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
BMX P34 1000	2.60	–	–	–	–	X	X	–
BMX P34 2000	2.60	–	–	–	–	X	X	–
BMX P34 2010	2.60	–	–	–	–	X	X	–
BMX P34 20102	2.60	–	–	–	–	X	X	–
BMX P34 2020	2.60	X	X	–	–	X	X	–

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–
X 可用，至少一个服务已实现。 **-** 不可用								

Modicon M580 控制器中的网络安全服务

Modicon M580 控制器中的最低固件版本和网络安全服务可用性：

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
BME P58 1020	1.00	X	X	–	X	X	X	X
BME P58 2020	1.00	X	X	–	X	X	X	X
BME P58 2040	1.00	X	X	–	X	X	X	X
BME P58 3020	1.00	X	X	–	X	X	X	X
BME P58 3040	1.00	X	X	–	X	X	X	X
BME P58 4020	1.00	X	X	–	X	X	X	X
BME P58 4040	1.00	X	X	–	X	X	X	X
BME P58 5040	2.10	X	X	–	X	X	X	X
BME P58 6040	2.10	X	X	–	X	X	X	X
BME H58 2040	2.10	X	X	–	X	X	X	X
BME H58 4040	2.10	X	X	–	X	X	X	X
BME H58 6040	2.10	X	X	–	X	X	X	X
X 可用，至少一个服务已实现。 **-** 不可用								

Modicon Quantum 控制器和模块中的网络安全服务

Modicon Quantum 控制器中的最低固件版本和网络安全服务可用性：

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
140CPU31110	3.20	–	–	–	–	X	X	–
140CPU43412•	3.20	–	–	–	–	X	X	–
140CPU53414•	3.20	–	–	–	–	X	X	–
140CPU651•0	3.20	X	X	–	–	X	X	–
140CPU65260	3.20	X	X	–	–	X	X	–
140CPU65860	3.20	X	X	–	–	X	X	–
140CPU67060	3.20	X	X	–	–	X	X	–
140CPU67160	3.20	X	X	–	–	X	X	–
140CPU6726•	3.20	X	X	–	–	X	X	–
140CPU67861	3.20	X	X	–	–	X	X	–

X 可用，至少一个服务已实现。

- 不可用

支持 网络安全服务的 Modicon Quantum 模块：

模块		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
140NOC7710•	1.00	–	X	–	–	X	–	–
140NOC78000	2.00	X	X	–	–	X	–	–
140NOC78100	2.00	X	X	–	–	X	–	–
140NOE771••	X	X	–	–	–	X	–	–
140NWM10000	–	X	–	–	–	–	–	–

X 可用，至少一个服务已实现。

- 不可用

Modicon X80 模块中的网络安全服务

支持 网络安全服务的 Modicon X80 模块：

模块		网络安全服务							
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	保密的加密通讯	事件记录	身份验证	授权	完整性检查
BMECXM0100	1.01	X	X	–	–	X	–	–	X
BMENOC0301	1.01	X	X	X	–	X	X	–	X
BMENOC0311	1.01	X	X	X	–	X	X	–	X
BMXNOC0401.2	2.05	X	X	–	–	–	–	–	–
BMXNOE0100.2	2.90	X	X	–	–	–	–	–	–
BMXNOE0110.2	6.00	X	X	–	–	–	–	–	–
BMXPRA0100	2.60	X	X	–	–	–	X	–	–
BMENOC0301	2.11	X	X	X	X	X	X	–	X
BMENOC0311	2.11	X	X	X	X	X	X	–	X

X 可用，至少一个服务已实现。

- 不可用

Modicon Premium/Atrium 控制器和模块中的网络安全服务

Modicon Premium/Atrium 控制器中的最低固件版本和网络安全服务可用性：

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
TSXH57•4M	3.10	–	–	–	–	X	X	–
TSXP570244M	3.10	–	–	–	–	X	X	–
TSXP57•04M	3.10	–	–	–	–	X	X	–
TSXP57•54M	3.10	–	–	–	–	X	X	–
TSXP571634M TSXP572634M TSXP573634M	3.10	X	X	–	–	X	X	–

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
（通过 ETY 端口）								
TSXP574634M TSXP575634M TSXP576634M （嵌入式 Ethernet 端口）	3.10	X	X	–	–	X	X	–
X 可用，至少一个服务已实现。 **-** 不可用								

支持 网络安全服务的 Modicon Premium/Atrium 模块：

模块		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
TSXETC101.2	2.04	X	X	–	–	–	–	–
TSXETY4103	5.70	X	X	–	–	–	–	–
TSXETY5103	5.90	X	X	–	–	–	–	–
X 可用，至少一个服务已实现。 **-** 不可用								

Modicon Momentum MDI 控制器和模块中的网络安全服务

Modicon Momentum MDI: 控制器中的最低固件版本和网络安全服务可用性

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
171CBU78090	1.0	X	X	–	–	X	X	–
171CBU98090	1.0	X	X	–	–	X	X	–

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
171CBU98091	1.0	X	X	–	–	X	X	–
X 可用，至少一个服务已实现。 **-** 不可用								

Modicon MC80 控制器和模块中的网络安全服务

Modicon MC80: 控制器中的最低固件版本和网络安全服务可用性

控制器		网络安全服务						
版本	最低固件	禁用未使用的服务	访问控制	加密通讯	事件记录	身份验证	授权	完整性检查
BMKC8020301	1.2	X	X	–	–	X	X	–
BMKC8020310	1.0	X	X	–	–	X	X	–
BMKC8030311	1.2	X	X	–	–	X	X	–
X 可用，至少一个服务已实现。 **-** 不可用								

Modicon M340 安全服务

概述

在不同手册中，以如下主题所述的那样，为 Modicon M340 控制器提供了通讯安全服务设置描述。

带嵌入式 Ethernet 端口的 Modicon M340 控制器

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全章节（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。
访问控制：	请参阅消息传送配置参数章节（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。

Modicon M580 安全服务

Modicon M580 控制器

在介绍“安全”选项卡（请参阅“Modicon M580 硬件参考手册”）的主题中提供了与网络安全相关的通讯参数描述。

Modicon Quantum 安全服务

概述

在不同手册中，以如下主题所述的那样，为 Modicon Quantum 控制器和 Ethernet 模块提供了通讯安全服务设置描述。

带嵌入式 Ethernet 端口的 Modicon Quantum 控制器

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全（启用/禁用 *HTTP*、*FTP* 和 *TFTP*）章节（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum Ethernet 网络模块用户手册”）。
访问控制：	请参阅带 *Control Expert* 的 *Modicon Quantum* 以太网控制器消息传送配置章节（请参阅“使用 Quantum 的 EcoStruxure™ Control Expert Ethernet 网络模块用户手册”）。

140 NOC 771 0x 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全（启用/禁用 *HTTP*、*FTP* 和 *TFTP*）章节（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum Ethernet 网络模块用户手册”）。
访问控制：	请参阅配置访问控制章节（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum 140 NOC 771 01 以太网通讯模块用户手册”）。

140 NOC 780 00 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全章节（请参阅“Quantum EIO 控制网络安装和配置指南”）。
访问控制：	请参阅配置访问控制章节（请参阅“Quantum EIO 控制网络安装和配置指南”）。

140 NOC 781 00 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全章节（请参阅“Quantum EIO 控制网络安装和配置指南”）。
访问控制：	请参阅配置访问控制章节（请参阅“Quantum EIO 控制网络安装和配置指南”）。

140 NOE 771 xx 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全（启用/禁用 *HTTP*、*FTP* 和 *TFTP*）章节（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum Ethernet 网络模块用户手册”）、安全章节（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum Ethernet 网络模块用户手册”），和 建立*HTTP*和写入密码章节（请参阅“ 使用 EcoStruxure™ Control Expert 的 Quantum Ethernet 网络模块用户手册”）。

140 NWM 100 00 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全（启用/禁用 *HTTP*、*FTP* 和 *TFTP*）章节（请参阅“使用 EcoStruxure™ Control Expert 的 Quantum Ethernet 网络模块用户手册”）。

Modicon X80 安全服务

概述

在不同手册中，以如下主题所述的那样，为 Modicon X80 Ethernet 模块提供了通讯安全服务设置描述。

BMXNOC0401.2 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

Ethernet 通讯：	请参阅安全章节（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。
访问控制：	请参阅配置访问控制章节（请参阅“Modicon M340 BMX NOC 0401 以太网通讯模块用户手册”）。

BMXNOE0100.2 和 BMXNOE0110.2 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

Ethernet 通讯：	请参阅安全章节（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。
访问控制：	请参阅消息传送配置参数章节（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。

BMXPRA0100 模块

BMXPRA0100 模块被配置作为 Modicon M340 控制器。在以下主题中提供了与网络安全相关的通讯参数描述：

Ethernet 通讯：	请参阅安全主题（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。
访问控制：	请参阅消息传送配置参数主题（请参阅“用于 Ethernet 的 Modicon M340 通讯模块和处理器用户手册”）。

BMXNOR0200H 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

Ethernet 通讯：	请参阅安全主题（请参阅“Modicon X80 BMXNOR0200H RTU模块用户手册”）。
访问控制：	请参阅消息传送配置参数主题。

BMENOR2200H 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

Ethernet 通讯：	请参阅安全主题。
访问控制：	请参阅消息传送配置参数主题。

BMECXM0100 模块

在以太网服务配置章节（请参阅“Modicon M580 BMECXM CANopen 模块用户手册”）中提供了与网络安全相关的通讯参数描述。

BMENOC0301 and BMENOC0311 模块

在配置安全服务主题（请参阅 Modicon M580 BMENOC0301 / BMENOC0311 Ethernet 通讯模块安装和配置指南）中提供了与网络安全相关的通讯参数描述。

BMENUA0100 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅“网络安全设置”主题（请参阅 M580 BMENUA0100 OPC UA 嵌入式模块安装和配置指南”）。
访问控制：	请参阅访问控制主题。

Modicon Premium/Atrium 安全服务

概述

在不同手册中，以如下主题所述的那样，为 Modicon Premium/Atrium 控制器和 Ethernet 模块提供了通讯安全服务设置描述。

带嵌入式 Ethernet 端口的 Modicon Premium/Atrium 控制器

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全服务配置参数章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium 和 Atrium Ethernet 网络模块用户手册”）。
访问控制：	请参阅配置 *TCP/IP* 消息传送 *(TSX P57 6634/5634/4634)* 章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium 和 Atrium Ethernet 网络模块用户手册”）。

带 ETY 端口的 Modicon Premium/Atrium 控制器

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全服务配置参数章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium 和 Atrium Ethernet 网络模块用户手册”）。
访问控制：	请参阅配置 *TCP/IP* 消息传送章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium 和 Atrium Ethernet 网络模块用户手册”）。

TSX ETC 101.2 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium TSX ETC 101 以太网通讯模块用户手册”）。
访问控制：	请参阅配置访问控制章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium TSX ETC 101 以太网通讯模块用户手册”）。

TSX ETY x103 模块

在以下主题中提供了与网络安全相关的通讯参数描述：

以太网通讯：	请参阅安全服务配置参数章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium 和 Atrium Ethernet 网络模块用户手册”）。
访问控制：	请参阅配置 *TCP/IP* 消息传送章节（请参阅“使用 EcoStruxure™ Control Expert 的 Premium 和 Atrium Ethernet 网络模块用户手册”）。

Modicon Momentum MDI 安全服务

在 *Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide* 中为 Modicon Momentum MDI 控制器提供了通讯安全服务设置描述。

Modicon MC80 安全服务

在 *Modicon MC80 Program Logic Controller (PLC) User Manual* 中为 MC80 控制器提供了通讯安全服务设置描述。

如何使用 EAGLE40 藉由 VPN 保护 M580、M340、Momentum MDI 和 MC80 架构

简介

本章介绍如何依靠被配置用于建立 VPN 连接的防火墙设备（如来自 Belden 的 EAGLE40-07），来帮助增强控制器的针对网络攻击的防护。在架构中部署此类设备可有助于减轻设备中存在的漏洞，并有助于减少不同产品的攻击面。

建议对网络、工作站和设备进行强化，如 *Modicon* 控制器系统网络安全用户指南中所述，此文档可从以下网址下载：https://www.se.com/us/en/download/document/EIO0000001999/

EAGLE40 防火墙

为什么使用防火墙？

依靠防火墙来增强现有架构的网络安全具有以下优点：

- 控制网络和设备的网络安全得到加强。
- 增强的网络安全依赖于 IPSEC 协议。
- 可将对现有架构和性能的影响降至最低。

EAGLE40 主要功能

EAGLE40 防火墙是一种覆盖或缓解网络安全残余问题的解决方案。

- 通过功能强大的 IPSEC VPN，EAGLE40 防火墙为网络通讯提供预期的保密性，以帮助防止中间人攻击。它通过帮助防止欺骗攻击来确保发送方的身份验证。消息完整性通过加密方法加强，无法被篡改。
- 此外，还有常用的过滤功能可用，允许基于 IP、Mac 地址和网络设备端口控制通讯流和协议。
- EAGLE40 防火墙是一款可扩展产品，能够纳入多点架构中，其速率和带宽性能有助于确保网络透明性。

前提条件

软件安装

在客户端与防火墙之间基于 IPSEC 协议建立 VPN 隧道时，必须使用兼容的 VPN 客户端软件。

EAGLE40 防火墙要求使用 VPN 客户端 IPSEC/IKEV2。

注: 使用 TheGreenBow 提供的 VPN 客户端解决方案。

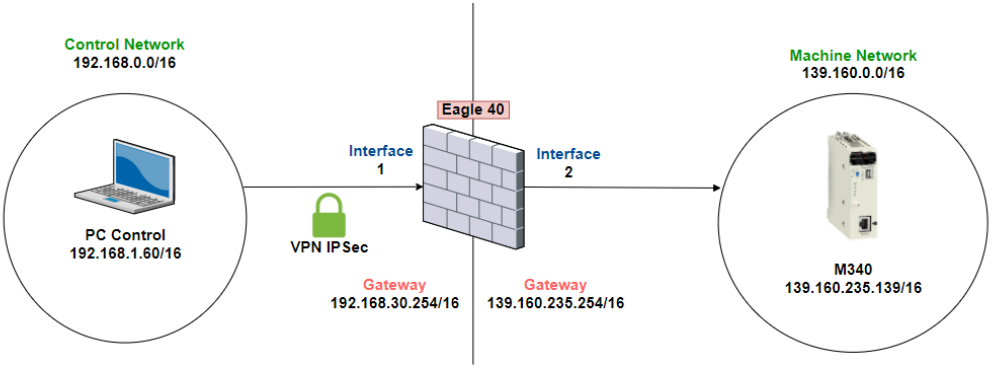
在下述配置过程中，我们使用了此软件，您可以通过以下 URL 下载：

https://www.thegreenbow.com/en/

机器和操作系统

在配置防火墙之前，您需要准备架构中使用的所有 IP 地址。

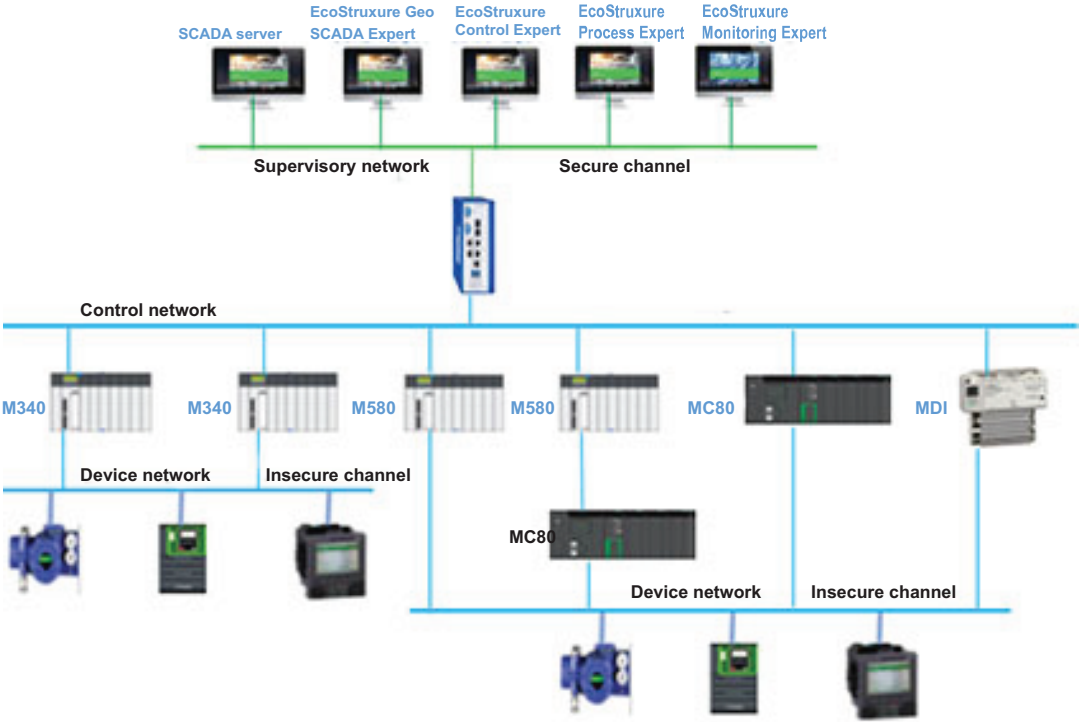
下图为示例：



典型架构

本文档中的架构和配置说明作为示例提供，可以适应不同的架构和系统。

例如，将 Modicon M340、M580、Momentum MDI 和 MC80 控制器组合在一起的以下混合架构便是典型架构：



注: 在控制器附近安装 EAGLE40 防火墙。

配置防火墙

Web 配置

如要配置防火墙，请打开互联网浏览器并输入以下 URL：

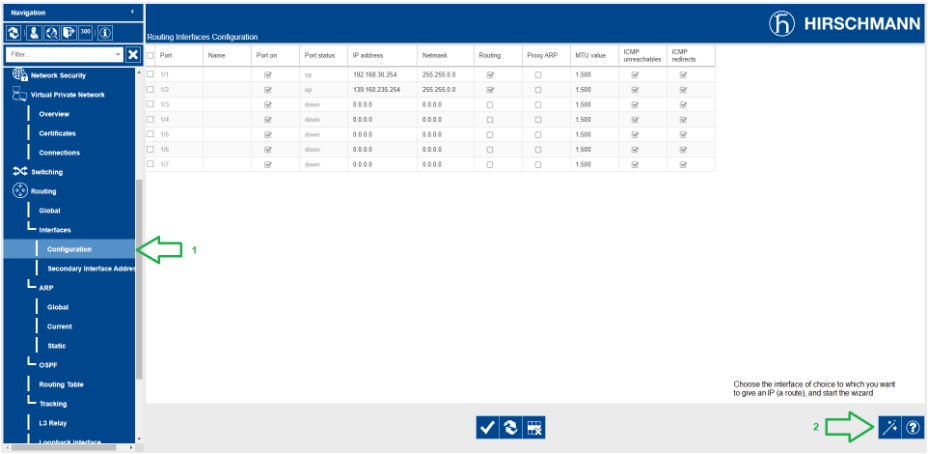
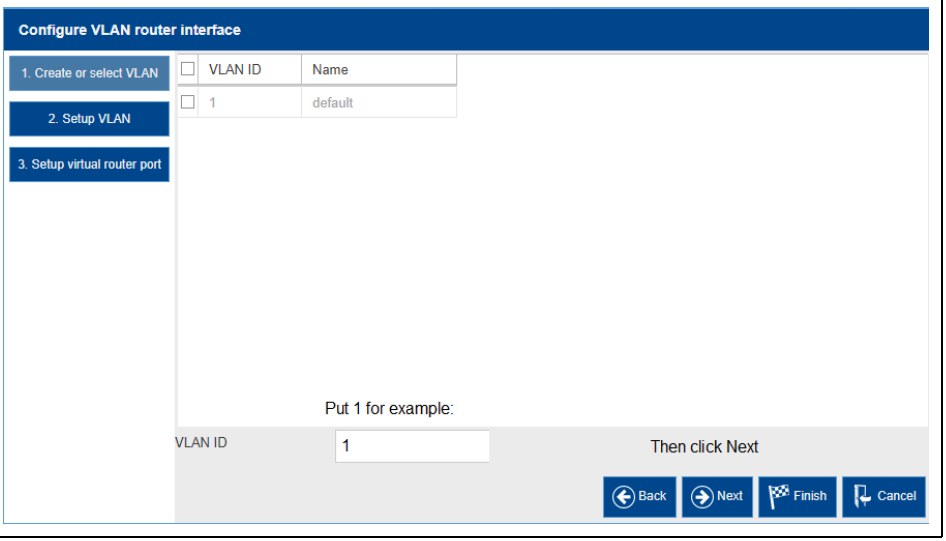
`https://[IPFirewall]/admin`

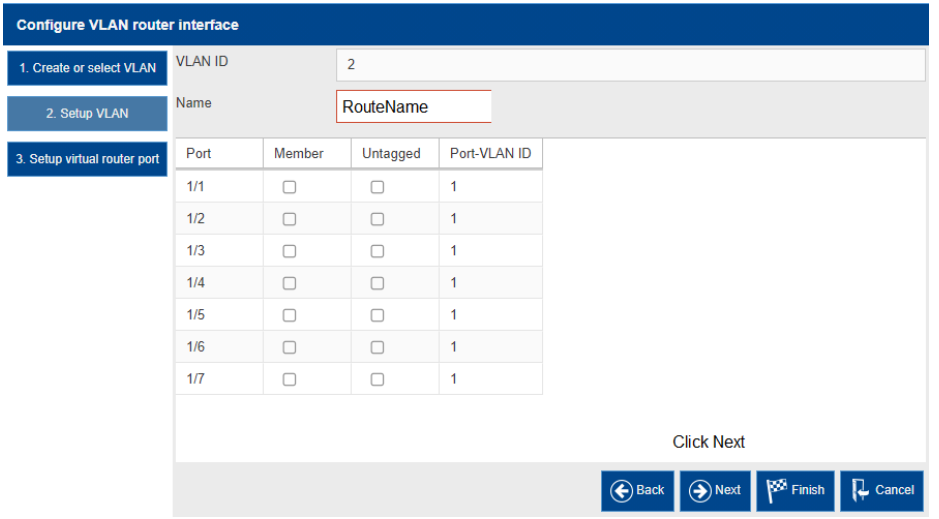
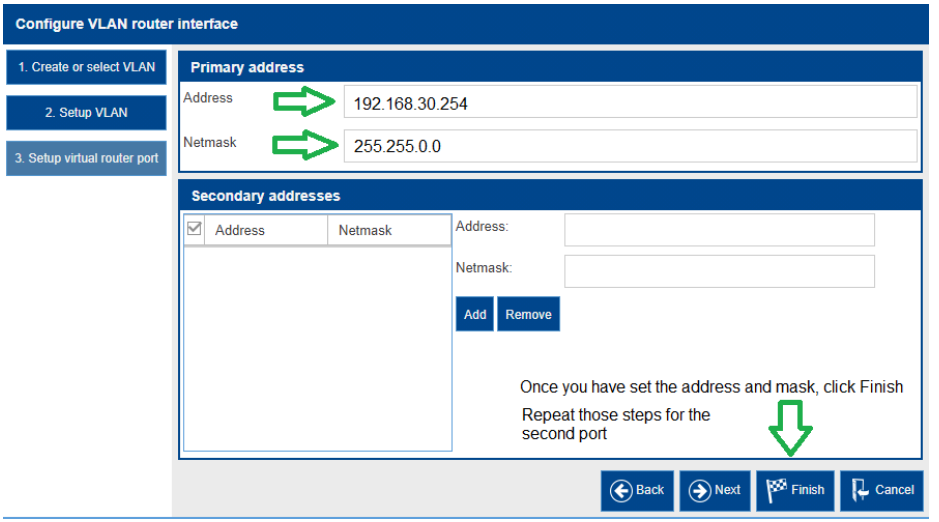
单击 **Enter**，然后使用缺省用户名/密码组合 `admin/private` 登录。

注: 首次登录时，需要更改密码。

配置路由

如要配置路由，请执行以下操作：

步骤	操作
1	 **1.** 在**导航**左窗格中，打开**路由 > 接口 > 配置**网页。选择要配置的以太网接口。 **2.** 单击  图标，以启动 **Configure VLAN Router Interface**（配置 VLAN 路由器接口）窗口。
2	为要配置的 VLAN 设置 ID 编号（示例中为 1），然后单击**下一步**。 

步骤	操作
3	为要配置的 VLAN 设置路由器名称（示例中为 RouteName），然后单击**下一步**。 
4	设置控制网络的 IP 地址及其掩码（示例中为 `192.168.30.254/16`），然后单击**完成**。 
5	对使用第二个以太网接口的机器网络重复步骤 1 至 4。

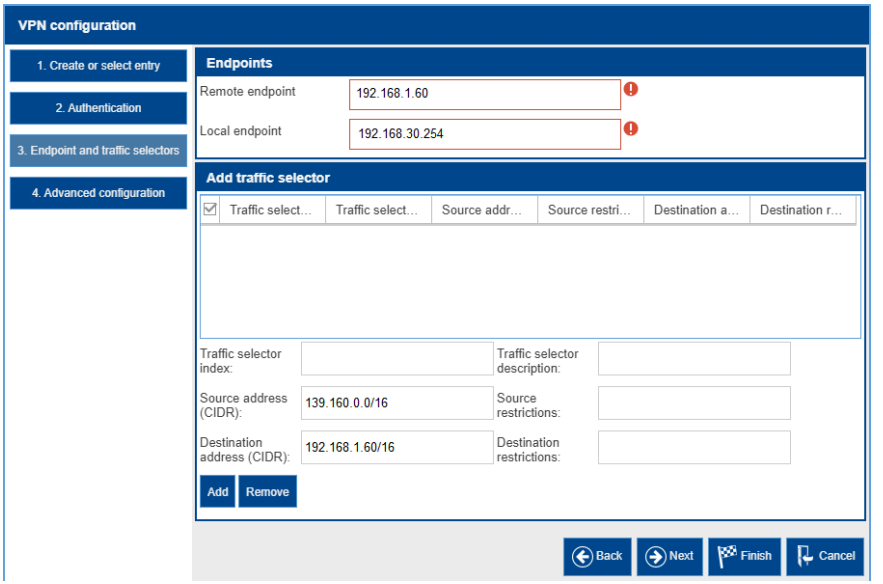
在下例中，我们将第一个物理端口上的防火墙的控制网络网关接口设置为 `192.168.30.254/16`，将第二个物理端口上的机器网络设置为 `139.160.235.254/16`。

Port	Name	Port on	Port status	IP address	Netmask	Routing	Proxy ARP	MTU value	ICMP unreachables	ICMP redirects
1/1		☑	up	192.168.30.254	255.255.0.0	☑	☐	1,500	☑	☑
1/2		☑	up	139.160.235.254	255.255.0.0	☑	☐	1,500	☑	☑
1/3		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/4		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/5		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/6		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/7		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑

在防火墙中配置 VPN

如要配置 VPN，请执行以下操作：

步骤	操作
1	在网页的左侧窗格中，单击 **Virtual Private Network > Connections** 菜单。单击  图标。
2	选择索引编号和名称，然后单击**下一步。**
3	选择密码 (PSK)，然后单击**下一步。**

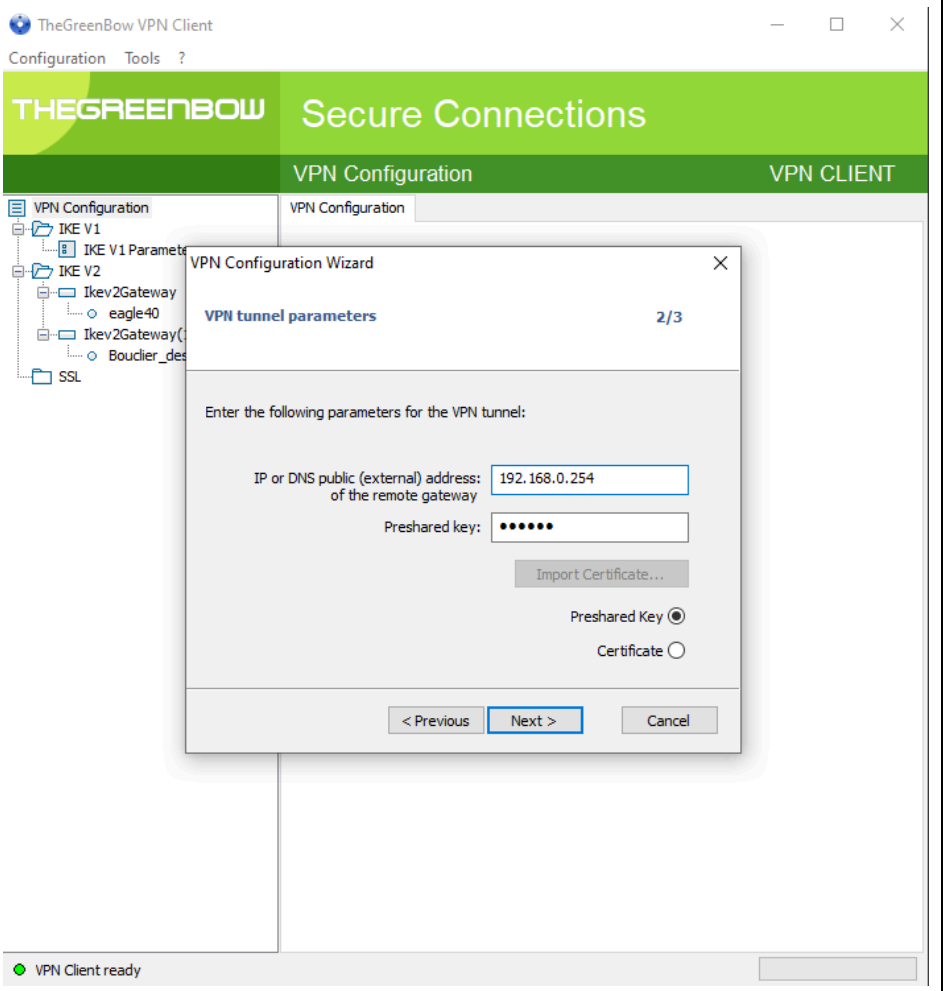
步骤	操作
4	根据您的网络填写 IP 地址和掩码。 • **Remote endpoint**：通过 VPN 连接到防火墙的计算机。 • **Local endpoint**：路由中配置的网关。 • **Source address (CIDR)**：受保护的计算机网络仅在通过 VPN 连接后可访问。 • **Destination address (CIDR)**：通过 VPN 连接到防火墙的计算机。  单击 **Next**。
5	设置余裕时间。缺省值是 150。 将 **IKE Version** 设置为 ikev2，然后单击 **Finish**。

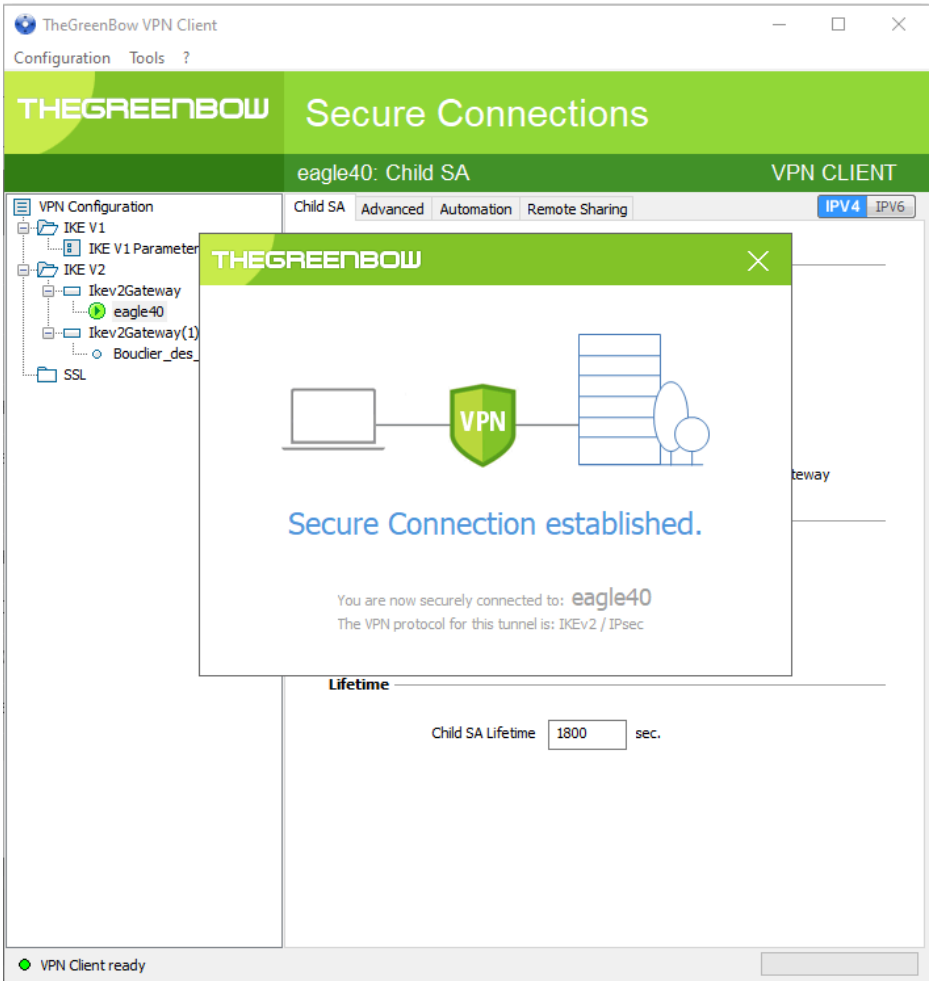
配置 VPN 客户端

注: 在我们的示例中，使用了 TheGreenBow 提供的 VPN 客户端解决方案。

如要配置 VPN 客户端，请执行以下操作：

步骤	操作
1	下载并安装 VPN 客户端软件。
2	在“VPN 客户端”窗口的左窗格中，右键单击 **VPN Configuration**，然后选择 **Wizard**。
3	选择 **IKEv2 Tunnel**，然后单击 **Next**。

步骤	操作
4	设置可通过控制网络接口访问的防火墙的 IP 地址（示例中为 192.168.0.254）。 输入先前选择的 PSK。  单击 **Next**，然后单击 **Finish**。
5	在“VPN 客户端”窗口的左侧窗格中，右键单击刚创建的 Ikev2 隧道，然后对其重命名。

步骤	操作
6	右键单击刚重命名的 Ikev2 隧道，然后选择 **Open Tunnel**。 随后便会以通知形式确认已建立安全连接。 

术语

1 类连接:

CIP 传输 1 类连接，用于通过隐式消息传送在 EtherNet/IP 设备之间传输 I/O 数据。

3 类连接:

CIP 传输 3 类连接，用于在 EtherNet/IP 设备之间传输显式消息。

802.1Q:

适用于虚拟局域网 (VLAN) 的 IEEE 协议标志符。本标志提供 VLAN 识别和服务质量 (QoS) 等级。

主环路:

Ethernet RIO 网络的主环路。此环路包含 RIO 模块、本地机架（包含带 Ethernet I/O 扫描器服务的控制器）和电源模块。

交换机:

用于对网络进行分段并可以减少冲突发生可能性的多端口设备。交换机根据数据包的源地址和目标地址过滤或转发数据包。交换机可以全双工运行，并能向各个端口提供全部网络带宽。交换机的输入/输出速度可以不同（如 10、100 或 1000Mbps）。交换机被视为 OSI 2 层（数据链接层）设备。

全双工:

两个网络设备彼此间同时进行独立双向通讯的能力。

分布式设备:

支持与控制器或其他 Ethernet I/O 扫描器服务进行交换的任何 Ethernet 设备（Schneider Electric 设备、PC、服务器或第三方设备）。

功能块图:

请参见 FBD。

变量:

`BOOL`、`WORD`、`DWORD` 和类似类型的内存实体，包含可被当前运行的程序修改的内容。

域名:

标识互联网中设备的字母数字字符串，是网站统一资源定位符 (URL) 的主要组成部分。例如，域名 *schneider-electric.com* 是 URL *www.se.com* 的主要组成部分。

每个域名都被指定为域名系统的一部分，并与 IP 地址关联。

也称为主机名。

多点传送:

广播的特殊形式，其中数据包的副本仅发送到网络目标的指定子网。隐式消息通常使用多点传送格式实现 EtherNet/IP 网络的通讯。

子环路:

基于 Ethernet 的网络，使用主环路上的双环路交换机 (DRS) 或 BMENOS0300 网络选项开关模块将回路连接到主环路。此网络包含 RIO 或分布式设备。

子网掩码:

32 位值，用于隐藏（或屏蔽）IP 协议网络上某台设备 IP 地址的网络部分，从而只显示主机地址。

就绪设备:

Ethernet 就绪设备向以太网/IP 或 Modbus 模块提供其他服务，例如：单个参数输入、总线编辑器声明、系统传输、确定的扫描容量、提示修改的警告消息以及 Control Expert 和设备 DTM 间共享的用户权限。

广播:

发送至广播域中所有设备的消息。

应用性时间戳:

使用应用性时间戳解决方案来藉由不支持 OPC DA 接口的 SCADA 系统访问时间戳事件缓冲区。这时，Control Expert 应用程序中的功能块会读取缓冲区中的事件，并将这些事件格式化以便发送至 SCADA 系统。

扫描器:

扫描器是 EtherNet/IP 中隐式消息的 I/O 连接请求的起始，也是 Modbus TCP 消息请求的起始。

扫描器类设备:

扫描器类设备由 ODVA 定义为 EtherNet/IP 节点，可以启动 I/O 与网络中的其他节点之间的数据交换。

控制器间网络:

基于 Ethernet 的网络，属于控制网络的一部分，提供控制器与工程工具（编程、资产管理系统 (AMS)）之间的数据交换。

控制网络:

基于 Ethernet 的网络，包含 PAC、SCADA 系统、NTP 服务器、PC、AMS 和交换机等。支持以下两种拓扑：

- 扁平：此网络中的所有模块和设备都属于同一个子网。
- 2 层：网络分为操作网络和控制器间网络。这两个网络可以在物理上独立，但通常通过路由设备链接。

操作网络:

基于 Ethernet 的网络，包含操作员工具（SCADA、客户端 PC、打印机、批处理工具和 EMS 等）。控制器直接连接或通过控制器间网络的路由来连接。此网络是控制网络的一部分。

整数的数值:

整数的数值用于在十进制系统中输入整数值。值的前面可以有符号“+”和“-”。分隔数字的下划线符号 (_) 没有意义。

示例：

```
-12,0,123_456,+986
```

无连接:

描述两个网络设备之间的通讯，在这种通讯状态下，无需预先排列，即可在两个设备之间发送数据。每段传输数据中还包含路由信息（包括源地址和目标地址）。

显式消息客户端:

(显式消息客户端) 设备类，由仅支持显式消息作为客户端的 EtherNet/IP 节点的 ODVA 定义。此设备类中常见的示例是 HMI 和 SCADA 系统。

显式消息:

用于 Modbus TCP 和 EtherNet/IP 的基于 TCP/IP 的消息。它用于包含数据（通常是客户端与服务器之间的非预定信息）和路由信息的点对点客户端/服务器消息。在 EtherNet/IP 中，显式消息视为 3 类消息，可以基于连接，也可以无连接。

服务端口:

M580 RIO 模块上的专用 Ethernet 端口。该端口可支持以下主要功能（具体取决于模块类型）：

- 端口镜像：用于诊断用途
- 访问：用于将 HMI/Control Expert/ConneXview 连接到控制器
- 扩展：用于将设备网络扩展到另一个子网
- 禁用：禁用该端口，在此模式下不转发任何通讯。

本地从站:

Schneider Electric EtherNet/IP 通讯模块提供的功能允许扫描器充当适配器角色。本地从站使模块能够使用隐式消息传送连接来发布数据。本地从站通常用于 PAC 之间的点对点交换。

本地机架:

包含控制器和电源的 M580 机架。本地机架包含一个或两个机架：主机架和扩展机架（与主机架属于同一个系列）。扩展机架是可选的。

机架优化连接:

来自多个 I/O 模块的数据合并在一个数据包中，通过 EtherNet/IP 网络的隐式消息提供给扫描器。

架构:

架构描述了由以下组件构成的网络规格的框架：

- 物理组件及其功能组织和配置
- 操作原理和过程
- 其操作中使用的数据格式

热备:

热备系统使用一个主 PAC (PLC) 和一个备用 PAC。两个 PAC 机架具备相同的硬件和软件配置。备用 PAC 监控主 PAC 的当前系统状态。如果主 PAC 无法操作，当备用 PAC 控制系统时，保持高可用控制。

独立 DIO 网络:

基于 Ethernet 的网络，包含不参与 RIO 网络的分布式设备。

目标:

在 EtherNet/IP 中，如果某台设备接收隐式或显式消息通讯连接请求，或者接收非连接显式消息的消息请求，它将被视为目标。

确定性:

对于定义的应用程序和架构，您可以预测到事件（输入值的更改）与控制器输出的对应更改之间的延迟是有限时间 *t*，小于过程所需的期限。

端口 502:

TCP/IP 堆栈的端口 502 是为 Modbus TCP 通讯保留的常见端口。

端口镜像:

在此模式下，与网络交换机上的源端口相关的数据通讯会复制到另一个目标端口。这使连接的管理工具可以监控和分析通讯。

简单菊花链回路:

简单菊花链回路通常称为 SDCL，仅包含 RIO 模块（不包含分布式设备）。此拓扑由本地机架（包含带 Ethernet I/O 扫描器服务的控制器）、以及一个或多个 RIO 子站（每个子站包含 RIO 适配器模块）组成。

网关:

网关设备有时通过不同的网络协议与两个不同的网络互连。连接基于不同协议的网络时，网关可将数据报从一个协议堆栈转换到另一个协议堆栈。用于连接两个基于 IP 的网络时，网关（也称作路由器）有两个单独的 IP 地址，每个网络使用一个地址。

网络时间服务:

使用此服务来通过互联网同步计算机时钟，以记录事件（顺序事件）、同步事件（触发同时发生的事件）或同步报警和 I/O（时标报警），

网络:

有两种含义：

- 在梯形图中：

  网络是一组相互连接的图形元素。网络的作用域对于包含该网络的程序组织单元（段）而言是局部的。

- 对于专用通讯模块：

  网络是一组相互通讯的工作站。网络这个术语还用于定义一组相互连接的图形元素。然后这个元素组再构成可能包含一组网络的程序的一部分。

网络融合:

在网络丢失的情况下重新配置网络，以确保系统可用性。

苛刻环境:

抗碳氢化合物、工业用油、清洁剂和焊接芯片。高达 100% 的相对湿度、含盐空气、显著温度变化、- 10°C 和 + 70°C 之间的工作温度、或在移动安装情况下。对于加强型（H）设备，相对湿度高达 95%，工作温度在 -25°C 和 + 70°C 之间。

虚拟局域网:

(虚拟局域网) 扩展到单个 LAN 以外的一组 LAN 段的局域网 (LAN)VLAN 是使用相关软件特别创建和配置的逻辑实体。

设备网络:

远程 I/O 网络中基于 Ethernet 的网络，包含远程 I/O 和分布式 I/O 设备。此网络上连接的设备遵循特定规则，以便可以确定远程 I/O。

起始:

在 EtherNet/IP 中，如果某台设备发起 CIP 连接以进行隐式或显式消息通讯，或者发起消息请求以获取非连接显式消息时，它将被视为起始。

连接发起方:

发起连接请求以传输 I/O 数据或显式消息的 EtherNet/IP 网络节点。

连接消息:

在 EtherNet/IP 中，连接消息使用 CIP 连接进行通讯。连接消息是指不同节点上两个或多个应用对象之间的逻辑关系。此连接为实现某种目的而提前创建虚拟电路，例如频繁显式消息或实时 I/O 数据传输等目的。

连接:

两个或多个网络设备之间的虚拟电路，在传输数据前建立。建立连接后，一系列数据通过同一通讯路径传输，而不必在每段数据中都包含路由信息（包括源地址和目标地址）。

适配器:

适配器是扫描器发出的实时 I/O 数据连接请求的目标。只有在扫描器将适配器配置为发送或接收实时 I/O 数据时，适配器才能执行这类操作，并且它不存储或创建建立连接所需的数据通讯参数。适配器接受来自其他设备的显式消息请求（已连接或未连接）。

陷阱:

陷阱是指 SNMP 代理引导的事件，表示以下事件之一：

- 代理的状态发生变化。
- 有未经授权的 SNMP 管理器设备试图从 SNMP 代理获取数据（或试图更改该代理上的数据）。

隐式消息:

基于 UDP/IP 的 1 类连接消息，用于 EtherNet/IP。隐式消息旨在维护用于生产者与消费者之间控制数据的预定传输的打开连接。由于打开的连接受到维护，所以每个消息基本上都包含数据（不含对象信息的开销）和连接标识符。

高容量菊花链回路:

高容量菊花链回路通常称为 HCDL，使用双环路交换机 (DRSs) 将设备子环路（包含 RIO 子站或分布式设备）和/或 DIO 云连接到 Ethernet RIO 网络。

高级模式:

在 Control Expert 中，选择高级模式可以显示有助于定义 Ethernet 连接的专用级配置属性。对于这些属性，只有非常熟悉 EtherNet/IP 通讯协议的人员才能进行编辑，因此可根据特定用户的资格选择隐藏还是显示这些属性。

A

ARRAY:

`ARRAY` 是包含单一类型的元素的表。语法如下：`ARRAY [<limits>] OF <Type>`

示例：`ARRAY [1..2] OF BOOL` 是一个一维表，由两个 `BOOL` 类型的元素组成。

`ARRAY [1..10, 1..20] OF INT` 是二维表，由 10x20 个 `INT` 类型的元素组成。

ART:

（应用程序响应时间）控制器应用程序对单个输入做出反应所需的时间。ART 的测量时段为从控制器中的物理信号打开并触发写入命令直到远程输出打开以指示接收到数据。

AUX:

(AUX) 任务是一种可选的周期性处理器任务，通过其编程软件运行。AUX 任务用于执行需要低优先级的应用程序部分。仅当 MAST 和 FAST 任务没有可执行的任务时，才会执行此任务。AUX 任务有两段：

- IN：在 AUX 任务执行之前，将输入复制到 IN 段。
- OUT：在 AUX 任务执行完后，将输出复制到 OUT 段。

B

BCD:

二进制编码的十进制数 十进制数的二进制编码。

BOOL:

布尔类型 这是计算中的基本数据类型。BOOL 变量可以是以下两个值之一：0 (FALSE) 或 1 (TRUE)。

从字提取的位属于 BOOL 类型，例如：%MW10.4。

BOOTP:

(引导程序协议) 一种 UDP 网络协议，可由网络客户端用于从服务器自动获取 IP 地址。客户端使用客户端的 MAC 地址向服务器标识自己。服务器会维护预先配置的客户端设备 MAC 地址及关联的 IP 地址表，从而向客户端发送其定义的 IP 地址。BOOTP 服务使用 UDP 端口 67 和 68。

C

CCOTF:

（动态更改配置）Control Expert 的一项功能，允许在系统运行期间在系统配置中进行模块硬件更改。此更改不影响活动操作。

CIP™:

（公共工业协议）为各种制造自动化应用提供的一整套全面的消息和服务（包括控制、安全、同步、运动、配置和信息）。CIP 允许用户将这些制造应用与企业级 Ethernet 网络和因特网相集成。CIP 是 EtherNet/IP 的核心协议。

CPU:

（中央处理单元）CPU，也称为处理器或控制器，是工业制造过程的控制中心。它与继电器控制系统相对，可实现过程的自动化。CPU 是适合在条件苛刻的工业环境中使用的计算机。

D

DDT:

(导出的数据类型) 导出的数据类型是具有相同类型 (ARRAY) 或不同类型（结构）的一组元素。

Device DDT (DDDT):

设备 DDT 是由制造商预定义的 DDT，用户不可进行修改。它包含 I/O 模块的 I/O 语言元素。

DFB:

（导出的功能块）DFB 类型是可以由用户使用 ST、IL、LD 或 FBD 语言定义的功能块。

在应用程序中使用这些 DFB 类型，可以：

- 简化程序的设计和输入
- 使程序更便于阅读
- 使程序更易于调试
- 减少生成的代码量

DHCP:

（动态主机配置协议）BOOTP 通讯协议的扩展，可以自动分配 IP 寻址设置，包括 IP 地址、子网掩码、网关 IP 地址和 DNS 服务器名称。DHCP 不需要维护用于标识各个网络设备的表。客户端使用其 MAC 地址或唯一分配的设备标识符向 DHCP 服务器标识自己。DHCP 服务使用 UDP 端口 67 和 68。

DIO 云:

一组分布式设备，不需要它们，亦可支持 RSTP。DIO 云只需要单一（非环路）铜线连接。它们可以连接到 DRS 上的某些铜缆端口，或者也可以直接连接到本地机架中的控制器或 Ethernet 通讯模块。DIO 云**无法**连接到子环路。

DIO 网络:

包含分布式设备的网络，其中由本地机架上的带 DIO 扫描器服务的控制器执行 I/O 扫描。DIO 网络通讯流在 RIO 通讯流之后传输，后者在 RIO 网络中优先传输。

DIO:

（分布式 *I/O*）也称为分布式设备。DRSs 使用 DIO 端口连接分布式设备。

DNS:

(域名服务器/服务) 一种将字母数字域名转换为 IP 地址（设备在网络中的唯一标识符）的服务。

DRS:

双环路交换机ConneXium 扩展可管理交换机，经过配置可在 Ethernet 网络中运行。Schneider Electric 提供的预定义配置文件可下载到 DRS，以支持主环路/子环路架构的特殊功能。

DSCP:

（差分服务代码点）此 6 位字段位于 IP 数据包的标头中，以对流量进行分类和优先级排序。

DST:

(夏令时) DST 也称为夏令时间 ，是指在春天即将开始时将时钟向前调整并在秋天即将开始时将时钟向后调整的做法。

DT:

(日期和时间) 采用 64 位格式的 BCD 编码的 DT 类型，包含以下信息：

- 在 16 位字段编码的年
- 以 8 位字段编码的月
- 以 8 位字段编码的日
- 以 8 位字段编码的时间
- 以 8 位字段编码的分
- 以 8 位字段编码的秒

注: 八个最低有效位未使用。

DT 类型采用以下格式输入：

DT#<年>**-**<月>**-**<日>**-**<时>**:**<分>**:**<秒>

下表显示每个字段的上限/下限：

字段	限制	注释
年	[1990,2099]	年
月	[01,12]	显示前导 0；输入数据时可以忽略它。
日	[01,31]	用于月 01/03/05/07/08/10/12
	[01,30]	用于月 04/06/09/11
	[01,29]	用于月 02（闰年）
	[01,28]	用于月 02（非闰年）
时	[00,23]	显示前导 0；输入数据时可以忽略它。
分	[00,59]	显示前导 0；输入数据时可以忽略它。
秒	[00,59]	显示前导 0；输入数据时可以忽略它。

DTM:

（设备类型管理器）DTM 是一种在主机 PC 上运行的设备驱动程序。它为访问设备参数、配置和操作设备以及排除设备故障提供了统一的结构。从用于设置设备参数的简单图形用户界面 (GUI)，到用于诊断和维护目的而执行复杂实时计算的高度复杂的应用程序，都属于 DTM。在 DTM 环境中，设备既可以是通讯模块，也可以是网络中的远程设备。

请参阅 FDT。

E

EDS:

(电子数据表) EDS 是描述设备配置能力的简单文本文件。EDS 文件由设备制造商生成和维护。

EFB:

(基本功能块) 这是在执行预定义逻辑功能的程序中使用的功能块。

EFB 具有状态和内部参数。即使输入完全相同，输出值也可能不同。例如，计数器有一个输出，指示已达到预选值。当值等于预选值时，此输出设置为 1。

EF:

(基本功能) 这是在执行预定义逻辑功能的程序中使用的功能块。

此功能不具有有关内部状态的任何信息。如果使用相同的输入参数多次调用同一功能，将返回相同的输出值。[功能块（实例）] 中提供了有关功能调用的图形形式的信息。与功能块调用不同，功能调用仅包括未命名且名称与功能名称完全相同的输出。在 FBD 中，每个调用都使用图形块通过唯一[编号]来指示。此编号自动进行管理，无法修改。

需要在程序中定位并配置这些功能，以便执行应用程序。

您还可以使用 SDKC 开发工具包开发其他功能。

EIO 网络:

(Ethernet I/O) 基于 Ethernet 的网络，包含以下三种类型的设备：

- 本地机架
- X80 远程子站（使用 BM•CRA312•0 适配器模块）或 BMENOS0300 网络选项交换机模块
- ConneXium 扩展双环路交换机 (DRS)

  注: 分布式设备也可以通过与 DRSs 或 X80 远程模块的服务端口连接来参与 Ethernet I/O 网络。

EN:

EN 表示 **EN**able（启用）；是可选功能块输入。启用 EN 输入时，则自动设置 ENO 输出。

如果 EN = 0，则不启用功能块；不执行其内部程序且 ENO 设置为 0。

如果 EN = 1，则功能块的内部程序会运行且 ENO 设置为 1。如果检测到运行时错误，则 ENO 设置为 0。

如果 EN 输入未连接，则会自动设置为 1。

ENO:

ENO 表示 **E**rror **NO**tification（错误通知）；这是与可选输入 EN 关联的输出。

如果 ENO 设置为 0（因为 EN=0 或如果检测到运行时错误）：

- 功能块输出的状态保持正确执行的前一个扫描循环过程中的相同状态。
- 功能（以及过程）的输出设置为 0。

Ethernet DIO 扫描器服务:

M580 控制器的嵌入式 DIO 扫描器服务管理 M580 设备网络上的分布式设备。

Ethernet I/O 扫描器服务:

M580 控制器的该嵌入式 Ethernet I/O 扫描器服务管理 M580 设备网络上的分布式设备 **和** RIO 子站。

EtherNet/IP™:

用于工业自动化应用的网络通讯协议，它将 TCP/IP 的标准互联网传输协议与应用层通用工业协议 (CIP) 相结合，支持高速数据交换和工业协议。EtherNet/IP 采用电子数据表 (EDS) 来为各网络设备及其功能分类。

Ethernet:

基于 CSMA/CD 和帧的 10 Mb/s、100 Mb/s 或 1 Gb/s LAN，可以借助铜双绞线或光缆运行或无线运行。IEEE标准 802.3 定义用于配置有线 Ethernet 网络的规则；IEEE 标准 802.11 定义用于配置无线 Ethernet 网络的规则。常见形式包括 10BASE-T、100BASE-TX 和 1000BASE-T，其可以利用类别 5e 铜双绞线电缆和 RJ45 模块化连接器。

F

FAST:

FAST 任务是可选的周期性处理器任务，可标识高优先级和多个扫描请求，通过其编程软件运行。FAST 任务可将所选 I/O 模块安排为每次扫描多次解析其逻辑。FAST 任务有两段：

- IN：在 FAST 任务执行之前，将输入复制到 IN 段。
- OUT：在 FAST 任务执行完后，将输出复制到 OUT 段。

FBD:

（功能块图）工作原理类似于流程图的 IEC 61131-3 图形编程语言。通过添加简单逻辑功能块（例如，AND、OR），程序的每个功能或功能块均使用此图形形式来表示。每个功能块的输入位于左侧，输出位于右侧。可将功能块输出链接到其他功能块的输入来创建复杂表达式。

FDR:

(*FAST* 设备更换) 一种使用配置软件更换无法操作的产品的服务。

FDT:

(现场设备工具) 协调现场设备和系统主机之间的通讯的技术。

FTP:

(文件传输协议) 通过基于 TCP/IP 的网络（如因特网）将文件从一个主机复制到另一个主机的协议。FTP 在客户端和服务器之间使用客户端-服务器架构以及单独的控制和数据连接。

G

GPS:

(*global positioning system*) GPS 标准由在全球范围内提供的民用和军用的基于空间的定位、导航和定时信号组成。标准定位服务性能取决于卫星广播信号参数、GPS 星群设计、可见卫星数量和各种环境参数。

H

HART:

(可寻址远程传感器高速通道) 双向通讯协议，用于通过模拟量电线在控制或监控系统与智能设备之间发送和接收数字信息。

HART 是提供主机系统与智能现场仪器之间数据访问的全球标准。主机可以是技术人员的手持式设备或笔记本电脑上的任何软件应用程序，乃至可以是工厂的过程控制、资产管理、或使用任何控制系统的其他系统。

HMI（人机界面）：

(人机界面) 允许人机交互的系统。

HTTP:

(超文本传输协议) 用于分布式和协作信息系统的网络协议。HTTP 是 web 数据通讯的基础。

I

I/O 扫描器:

不断轮询 I/O 模块以收集数据、状态、事件及诊断信息的 Ethernet 服务。这一过程用于监控输入和控制输出。此服务支持 RIO 和 DIO 逻辑扫描。

%I:

根据 CEI 标准，`%I` 表示离散量输入类型的语言对象。

IEC 61131-3:

国际标准：可编程逻辑控制器

第 3 部分：编程语言

IGMP:

（因特网组管理协议）此因特网标准用于多点传送，允许主机订阅特定的多点传送组。

IL:

（指令列表）包含一系列基础指令的 IEC 61131-3 编程语言。与用于对处理器编程的汇编语言非常相似。每个指令由一个指令代码和一个操作数组成。

INT:

(整数)（采用 16 位编码）其上限/下限如下：-（2 的 15 次幂）到（2 的 15 次幂）- 1。

示例：`-32768`, `32767`, `2#1111110001001001`, `16#9FA4`。

IODDT:

（输入/输出导出数据类型）一种结构化数据类型，表示模块或控制器通道。每个应用程序专用模块都有自己的 IODDT。

IP 地址:

分配给连接 TCP/IP 网络的设备的 32 位标识符，由网络地址和主机地址组成。

IPsec:

（因特网协议安全）一组开放的协议标准，使用 IPsec 保护模块间通讯的 IP 通讯会话的隐私性并对此会话加密，由因特网工程工作组 (IETF) 开发。IPsec 身份验证和加密算法需要用户定义的用于处理 IPsec 会话中每个通讯数据包的密钥。

%IW:

根据 CEI 标准，`%IW` 表示模拟量输入类型的语言对象。

L

LD:

（梯形图）一种 IEC 61131-3 编程语言，表示要作为图形图（非常类似于电路图（例如，触点、线圈）执行的指令。

M

%M:

根据 CEI 标准，`%M` 表示存储器位类型的语言对象。

M580 Ethernet I/O 设备:

提供自动网络恢复和确定性 RIO 性能的 Ethernet 设备。可以计算解析 RIO 逻辑扫描所需的时间，系统可以从通讯中断中快速恢复。M580 EthernetI/O 设备包括：

- 本地机架（包括带 Ethernet I/O 扫描器服务的控制器）
- RIO 子站（包括 X80 适配器模块）
- 具有预定义配置的 DRS 交换机

MAST:

主 (MAST) 任务是一种确定性处理器任务，通过其编程软件运行。MAST 任务可将 RIO 模块逻辑安排为在每次 I/O 扫描中解析。MAST 任务有两段：

- IN：在 MAST 任务执行之前，将输入复制到 IN 段。
- OUT：在 MAST 任务执行完后，将输出复制到 OUT 段。

MB/TCP:

（*TCP* 协议上的 *Modbus*）这是用于通过 TCP/IP 网络进行通讯的 Modbus 变体。

MIB:

(管理信息库) 用于管理通讯网络中的对象的虚拟数据库。请参见 SNMP。

Modbus:

Modbus 是一种应用层消息传递协议。 Modbus 可为不同类型的总线或网络上连接的设备提供客户端与服务器通讯。Modbus 可提供功能代码指定的多种服务。

%MW:

根据 CEI 标准，`%MW` 表示存储器字类型的语言对象。

N

NIM:

(网络接口模块) NIM 位于 STB 岛的第一个位置中（物理设置的最左侧）。NIM 提供 I/O 模块和现场总线主站之间的接口。它是岛上与现场总线相关的唯一模块 — 每个现场总线使用不同的 NIM。

NTP:

(网络时间协议) 用于同步计算机系统时钟的协议。该协议使用抖动缓存区来消除可变延迟的影响。

O

O -> T:

(起始到目标) 请参见起始和目标。

ODVA:

（开放式设备网络供应商协会）ODVA 支持基于 CIP 的网络技术。

OFS:

(*OPC Factory Server*) OFS 用于实现与 Control Expert 系列 PLC 的实时 SCADA 通讯。OFS 采用标准 OPC 数据访问协议。

OPC DA:

（面向过程控制数据访问的 *OLE*）在为客户端与服务器之间的实施数据通讯提供规范 OPC 标准中，这个数据访问规范是最常实施的规范。

P

PAC:

可编程自动控制器。PAC 是工业制造过程的控制中心。它与继电器控制系统相对，可实现过程的自动化。PAC 是适合在条件苛刻的工业环境中使用的计算机。

PTP:

（精度时间协议）使用此协议来在整个计算机网络中同步时钟。在局域网中，PDP 实现次微秒级别的时钟准确度，从而适合用于测量和控制系统。

Q

%Q:

根据 CEI 标准，%Q 表示离散量输出类型的语言对象。

QoS:

(服务质量) 将不同优先权分配给各种通信量类型以管理网络数据流的做法。在工业网络中，QoS 用于实现可预测级别的网络性能。

%QW:

根据 CEI 标准，%QW 表示模拟量输出类型的语言对象。

R

RIO 子站:

Ethernet RIO 网络中三种 RIO 模块类型之一。RIO 子站是连接到 Ethernet RIO 网络并由 Ethernet RIO 适配器模块管理的 I/O 模块的 M580 机架。子站可以是单个机架或是带有扩展机架的主机架。

RIO 网络:

基于 Ethernet 的网络，包含 3 种类型的 RIO 设备：本地机架、RIO 子站和 ConneXium 扩展双环路交换机 (DRS)。分布式设备也可以通过与 DRSs 或 BMENOS0300 网络选项开关模块的连接来参与 RIO 网络。

RPI:

（请求数据包间隔）扫描器请求的各次循环数据传输之间的时间段。EtherNet/IP 设备将按照 RPI（由扫描器分配给它们）指定的速率发布数据，并在 RPI 期间接收来自扫描器的消息请求。

RSTP:

（快速生成树协议）允许网络设计包括备用（冗余）链路以便在活动链路停止运行时提供自动备份路径，无需回路或手动启用/禁用备份链路。

S

S908 RIO:

使用同轴电缆和接线端子的Quantum RIO 系统。

SCADA:

（监督控制和数据采集）SCADA 系统是用于控制和监视工业、基础设施或基于设施的过程（如输电、通过管线输送油气和供水）的计算机系统。

SFC:

（顺序功能图）IEC 61131-3一种编程语言，用于以图形和结构化方式表示顺序控制器的操作。控制器的顺序行为和各种最终情形的相关图形描述使用简单图形符号进行创建。

SFP:

（小型可插拔）SFP 收发器充当模块和光缆之间的接口。

SMTP:

(简单邮件传输协议) 允许基于控制器的项目报告报警或事件的电子邮件通知服务。控制器监控系统，并可以自动创建包含数据、报警和/或事件的电子邮件消息警告。邮件收件人可以为本地或远程收件人。

SNMP:

(简单网络管理协议) 网络管理系统中使用的协议，用于监控附加到网络的设备。该协议是因特网工程工作组 (IETF) 定义的因特网协议套件 (IP) 的一部分，该套件由网络管理指南组成，包括应用层协议、数据库方案以及一组数据对象。

SNTP:

(简单网络时间协议) 请参见 NTP。

SOE:

（事件序列）SOE 软件帮助用户理解可能引起不安全过程状况和关机的一系列事件。SOE 对于解决或预防此类状况可能非常重要。

ST:

（结构化文本）一种 IEC 61131-3 编程语言，它表示结构化书面语言，是一种类似于计算机编程语言的开发语言。它可用于组织一系列指令。

%SW:

根据 CEI 标准，`%SW` 表示系统字类型的语言对象。

T

T->O:

(目标到起始) 请参见目标和起始。

TCP/IP:

也称为因特网协议套件，TCP/IP 是用于执行网络事务的协议的集合。该套件的名称源自两个常用协议：传输控制协议和互联网协议。TCP/IP是面向连接的协议，供 Modbus TCP 和 EtherNet/IP 用于发送显式消息。

TCP:

(传输控制协议) 因特网协议套件的一个关键协议，支持面向连接的通讯，方法是建立必要的连接，通过同一个通讯路径传输排序数据。

TFTP:

（小型文件传输协议）文件传输协议 (FTP) 的简化版本，TFTP 使用客户端-服务器架构在两个设备之间建立连接。从 TFTP 客户端，单个文件可以上载到服务器或从服务器下载，使用用户数据报协议 (UDP) 传输数据。

TIME_OF_DAY:

请参见 `TOD`。

TOD:

(时间) 采用 32 位格式的 BCD 编码的TOD 类型，包含以下信息：

- 以 8 位字段编码的时
- 以 8 位字段编码的分
- 以 8 位字段编码的秒

注: 八个最低有效位未使用。

TOD 类型采用以下格式输入 ：xxxxxxxx: TOD#<时>:<分>:<秒>

下表显示每个字段的上限/下限：

字段	限制	注释
时	[00,23]	显示前导 0；输入数据时可以忽略它。
分	[00,59]	显示前导 0；输入数据时可以忽略它。
秒	[00,59]	显示前导 0；输入数据时可以忽略它。

示例：TOD#23:59:45。

TR:

(透明就绪) 支持 Web 的配电设备，包括中压和低电压开关装置、开关板、配电板、电机控制中心以及成套变电站。通过透明就绪设备可以使用标准 Web 浏览器从网络上的任何 PC 访问仪表和设备状态。

U

UDP:

(用户数据报协议) 支持无连接通讯的传输层协议。在网络节点上运行的应用程序可以使用 UDP 互相发送数据报。与 TCP 不同，UDP 不包括用于建立数据路径或提供数据排序和检查的初步通讯。但是，由于消除了提供这些功能所需的开销，因此 UDP 比 TCP 更快。对于时间要求比较高的应用，即宁愿丢弃数据报也不希望数据报延迟的情况，UDP 可能是更好的选择。对于 EtherNet/IP 中的隐式消息，UDP 是主要传输协议。

UMAS:

（统一消息应用服务）UMAS 是管理 Control Expert 和控制器之间通讯的一项专有的系统协议。

UTC:

(世界协调时间) 用于管理全球时钟和时间的主要时间标准（接近以前的 GMT 时间标准）。

索引

事件日志消息.....60
BMENOR2200H.....74
BMENUA0100.....74
Control Expert.....55
M580 控制器（固件 V4.10 和任何后续支持版本）.....60
M580 控制器（固件版本低于 V4.10）.....74
事件记录
网络安全.....109
保护
存储器.....92
段.....91
关键资产
PAC，M580 CSPN.....45
环境，M580 CSPN.....45
内存，控制器
CSPN.....46
加强
PC.....22
固件
安全.....109
网络安全.....109
固件签名
CSPN.....46
固件篡改
CSPN.....46
存储器
保护.....92
存储器保护
安全.....94
存储器程序篡改
CSPN.....46
安全
ACL.....30
CSPN.....39
CSPN，M580 运行模式.....44
M580 Control Expert Security Editor.....43
M580 CSPN 参数.....44
Syslog.....48
固件.....109
存储器保护.....94
完整性检查.....94
审计跟踪.....48
授权.....91
服务.....109
记录.....48
访问控制.....30
运行/停止.....92
安全通讯
CSPN.....46
网络安全.....109
完整性检查
安全.....94
网络安全.....109
审计跟踪
安全.....48
密码
Control Expert.....90
网络安全.....87
密码存储
CSPN.....46
帐户
网络安全.....87
执行模式，控制器
CSPN.....46
执行模式篡改
CSPN.....46
授权
安全.....91
网络安全.....109
接口，管理
CSPN.....46
控制器内存
CSPN.....46
控制器执行模式
CSPN.....46
数据流篡改
CSPN.....46
文献
网络安全.....16
服务
安全.....109
网络安全.....109
服务拒绝
CSPN.....46
架构.....18
段
保护.....91
漏洞
网络安全.....16
用户类型
M580 Control Expert Security Editor.....43

安全， M580 Control Expert Security Editor 43
禁用
通讯服务 29
禁用未使用的服务
网络安全 109
签名，固件
CSPN 46
管理接口
CSPN 46
网络安全 16
CSPN 39
CSPN，M580 39
CSPN，M580 运行模式 44
FTP 88
HTTP 88
LANMAN / NTLM 25
M340 115
M580 116
M580 Control Expert Security Editor 43
M580 CSPN 参数 44
Premium/Atrium 120
Quantum 116
SNMP 89
X80 118
事件记录 109
固件 109
安全通讯 109
完整性检查 109
密码 87
局域连接 26
帐户 87
指南 16
授权 109
文献 16
服务 109
漏洞 16
禁用未使用的服务 109
网络接口卡 26
访问控制 109
身份验证 109
远程桌面 25
通知 16
网络接口卡
网络安全 26
认证
CSPN 39
记录
安全 48
访问
USB 19
访问控制
安全 30
网络安全 109
访问控制策略
CSPN 46
资产
关键，M580 CSP 环境 45
关键，M580 CSPN 控制器 45
身份验证
网络安全 109
输入管理，不正确
CSPN 46
运行/停止
安全 92
运行模式
CSPN，M580 44
远程桌面
网络安全 25
通知
网络安全 16
通讯，安全
CSPN 46
通讯服务
禁用 29

A

ACL
安全 30

C

Control Expert
password 90
Control Expert Security Editor 43
CSPN 39
M580 网络安全参数 44
M580 运行模式 44
M580，不正确的输入管理 46
M580，加密通讯 46
M580，固件签名 46
M580，固件篡改 46
M580，存储器程序篡改 46
M580，安全的密码存储 46

M580，执行模式篡改 46
M580，控制器内存的完整性和可靠性 46
M580，控制器执行模式的完整性 46
M580，数据流篡改 46
M580，服务拒绝 46
M580，管理接口的加密授权 46
M580，访问控制策略 46
关键资产，控制器 45
关键资产，环境 45

F

FTP
cybersecurity 88

H

HTTP
cybersecurity 88

L

LAN
网络安全 26
LANMAN / NTLM
网络安全 25

M

M340
cybersecurity 115
M580
cybersecurity 116

O

Operate
M580 Control Expert Security Editor 用户类型 43

P

PC
加强 22
Premium/Atrium
cybersecurity 120
Program
M580 Control Expert Security Editor 用户类型 43

Q

Quantum
cybersecurity 116

R

ReadOnly
M580 Control Expert Security Editor 用户类型 43

S

SNMP
cybersecurity 89
Syslog
BMENOR2200H 74
BMENUA0100 74
Control Expert 55
M580 控制器（固件 V4.10 和任何后续支持版本） 60
M580 控制器（固件版本低于 V4.10） 74
security 48

U

USB
访问 19

X

X80
cybersecurity 118

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。

© 2024 Schneider Electric. 版权所有。

EIO0000002004.10