Modicon 控制器平台

网络安全
参考手册

05/2015

EIO0000002004.01

www.schneider-electric.com

Schneider Electric

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

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

当设备用于具有技术安全要求的应用场合时，必须遵守有关的使用说明。

未能使用 Schneider Electric 软件或认可的软件配合我们的硬件，则可能导致人身伤害、损害或不正确的操作结果。

不遵守此信息可能导致人身伤害或设备损坏。

目录

安全信息

重要信息

声明

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

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

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

⚠ 危险

危险表示若不加以避免，将**会导致**严重人身伤害甚至死亡的危险情况。

⚠ 警告

警告表示若不加以避免，可能**会导致**严重人身伤害甚至死亡的危险情况。

⚠ 小心

小心表示若不加以避免，可能**会导致**轻微或中度人身伤害的危险情况。

注意

注意用于表示与人身伤害无关的危害。

请注意

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

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

关于本书

概览

文档范围

⚠ 警告

意外操作设备、失控、数据丢失

系统所有人、设计者、操作人员以及那些维护使用 Unity Pro 软件之设备的人员都必须阅读、理解并遵循本文档 *Modicon 控制器平台网络安全，参考手册*（部件号：EIO0000002004）中的说明。

不遵循上述说明可能导致人员伤亡或设备损坏。

本手册定义了网络安全要素，它们有助于您配置的系统不易受到网络攻击。

注意：本手册通篇使用关于网络安全主题的术语“ 安全性 ”。

有效性说明

此文档适用于 Unity Pro 10.0 或更高版本。

本文档中描述的设备技术特性在网站上也有提供。要在线访问此信息：

步骤	操作
1	访问 Schneider Electric 主页 *www.schneider-electric.com*。
2	在 **Search** 框中键入产品参考号或产品系列名称。 ● 型号 / 产品系列中不得包括空格。 ● 要获得有关类似模块分组的信息，请使用星号 (*)。
3	如果您输入参考号，则转到 **Product datasheets** 搜索结果，单击您感兴趣的参考号。 如果您输入产品系列的名称，则转到 **Product Ranges** 搜索结果，单击您感兴趣的产品系列。
4	如果 **Products** 搜索结果中出现多个参考号，请单击您感兴趣的参考号。
5	根据屏幕大小，您可能需要向下滚动查看数据表。
6	要将数据表保存为 .pdf 文件或打印数据表，请单击 **Download XXX product datasheet**。

本手册中介绍的特性应该与在线显示的那些特性相同。依据我们的持续改进政策，我们将不断修订内容，使其更加清楚明了，更加准确。如果您发现手册和在线信息之间存在差异，请以在线信息为准。

相关的文件

文件名称	参考编号
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cyber Security Recommendations	–
《Modicon M580 系统规划指南》	HRB62666 （英语）、 HRB65318 （法语）、 HRB65319 （德语）、 HRB65320 （意大利语）、 HRB65321 （西班牙语）、 HRB65322 （简体中文）
Modicon M580 硬件参考手册	EIO0000001578 （英语）、 EIO0000001579 （法语）、 EIO0000001580 （德语）、 EIO0000001582 （意大利语）、 EIO0000001581 （西班牙语）、 EIO0000001583 （简体中文）
Modicon M580 BME NOC 03•1 Ethernet 通讯模块安装和配置指南	HRB62665 (English), HRB65311 (French), HRB65313 (German), HRB65314 (Italian), HRB65315 (Spanish), HRB65316 (Chinese)
《用于以太网的 Modicon M340 通讯模块和处理器用户手册》	31007131 （英语）、 31007132 （法语）、 31007133 （德语）、 31007494 （意大利语）、 31007134 （西班牙语）、 31007493 （简体中文）
《使用 Unity Pro 的 Quantum TCP/IP 配置用户手册》	33002467 （英语）、 33002468 （法语）、 33002469 （德语）、 31008078 （意大利语）、 33002470 （西班牙语）、 31007110 （简体中文）

文件名称	参考编号
《使用 Unity Pro Ethernet 网络模块的 Premium 和 Atrium 用户手册》	35006192 （英语）、 35006193 （法语）、 35006194 （德语）、 31007214 （意大利语）、 35006195 （西班牙语）、 31007102 （简体中文）
Unity Pro 操作模式	33003101 （英语）、 33003102 （法语）、 33003103 （德语）、 33003696 （意大利语）、 33003104 （西班牙语）、 33003697 （简体中文）
采用 Unity Pro 的 Quantum 硬件参考手册	35010529 （英语）、 35010530 （法语）、 35010531 （德语）、 35010532 （西班牙语）、 35013975 （意大利语）、 35012184 （简体中文）
Modicon M580 BME CXM CANopen 模块，用户手册	EIO0000002129 （英语）、 EIO0000002130 （法语）、 EIO0000002131 （德语）、 EIO0000002132 （意大利语）、 EIO0000002133 （西班牙语）、 EIO0000002134 （简体中文）
MC80 可编程逻辑控制器，用户手册	EIO0000002071 （英语）

您可以从我们的网站下载这些技术出版物和其它技术信息，网址是：www.schneider-electric.com。

章 1
介绍

Schneider Electric 指南

简介

您的 PC 系统可运行各种应用程序来增强您的控制环境中的安全性。系统具有出厂默认设置，要求重新配置以与深度防御方法的 Schneider Electric 设备加强建议保持一致。

下面的指南介绍了 Windows 7 操作系统中的流程。这些仅作为示例提供。您的操作系统和应用程序可能有不同的要求或流程。

Schneider Electric website 的支持区域提供专用于网络安全的主题。

深度防御方法

除了本手册中介绍的解决方案，建议遵循以下 STN 指南中说明的 Schneider Electric 深度防御方法：

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

章 2
如何保护架构

简介

本章节说明 Modicon 控制器平台架构的完成操作，目的是使架构更加安全。

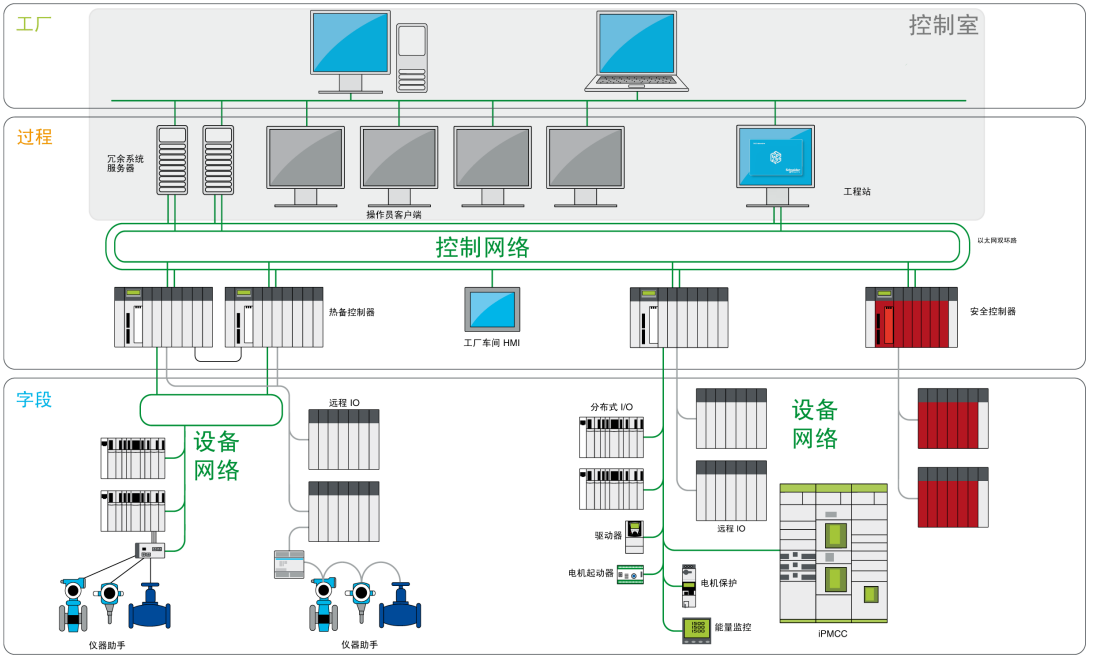
本章包含了哪些内容？

本章包含了以下主题：

系统查看

系统架构

以下 PlantStruxure 架构突出显示具备可进行保护的多层架构的必要性 （带控制网络和设备网络）。扁平化架构 （所有设备连接到同一网络）无法进行适当保护。



安全通讯

控制室内的设备相比连接到设备网络的设备会更多的暴露于攻击。因此，安全通讯需要在控制室和 PAC 以及设备之间实施。

在系统架构中，控制室区域为灰色，目的是将其与 PAC 和设备进行区分。

加强 PC

简介

位于控制室内的 PC 高度暴露于攻击。支持 Unity Pro 或 OFS 的这些 PC 需要加强。

加强工程工作站

客户会选择各种商业 PC 系统，满足自己的工程工作站需求。关键的加强技术包括：

- 强大的密码管理。
- 用户帐户管理。
- 应用到应用程序和用户帐户的最低特权方法。
- 删除或禁用不需要的服务。
- 删除远程管理特权。
- 系统补丁管理。

禁用未使用的网络接口卡

验证是否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 7 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**。

配置本地连接

各种 Windows 网络设置可增强与 Schneider Electric 建议的深度防御方法一致的安全性。

在 Windows 7 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 →本地连接 (x)** 来访问这些设设置。

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。
- 取消选择除 **QoS 数据包调度程序**和 **Internet 协议版本 4** 之外的所有**本地连接属性**条目。
- 在**高级 TCP/IP 设置**上的 **Wins** 选项卡下，取消选中**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 的深度防御建议还包括以下内容：

- 仅定义静态 IPv4 地址、子网掩码和网关。
- 在控制室内不要使用 DHCP 或 DNS。

禁用远程桌面协议

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

步骤	操作
1	在 Windows 2008R2 或 Windows 7 中，可通过**计算机 →系统属性 →高级系统设置禁用 RDP**。
2	在**远程**选项卡上，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。

更新安全策略

通过命令窗口中的 `gpupdate` 更新您系统中与 PC 相关的安全策略。有关详细信息，请参考与 `gpupdate` 上的 Microsoft 文档。

禁用 LANMAN 和 NTLM

Microsoft LAN Manager 协议（LANMAN 或 LM）及其后续 NT LAN Manager (NTLM) 具有使其在控制应用程序中的使用不合适的漏洞。

以下步骤介绍了如何在 Windows 7 或 Windows 2008R2 中禁用 LM 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。拒绝以下字段中的 LM & NTLM** 在**网络安全：LAN 管理器身份验证级别**字段中。
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` 以提交更改的安全策略。

管理更新

部署前，使用 Microsoft **Windows 更新** Web 页面上的实用程序更新所有 PC 的操作系统。要在 Windows 2008R2 或 Windows 7 中访问此工具，请选择**开始 →所有程序 →Windows 更新**。

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）。

描述

为了减少攻击字段，禁用任何未使用的嵌入式服务，以关闭潜在通讯门。

禁用 Unity Pro 中的 Ethernet 服务

可以在 Unity Pro 中使用 Ethernet 选项卡启用 / 禁用 Ethernet 服务。为下列每个平台提供的选项卡说明：

- Modicon M340 (参见第 *43* 页)
- Modicon M580 (参见第 *44* 页)
- Modicon Quantum (参见第 *45* 页)
- Modicon X80 modules (参见第 *47* 页)
- Modicon Premium/Atrium (参见第 *48* 页)

请在将应用程序下载到 CPU 之前设置 Ethernet 选项卡参数。

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。

注意：对于一些产品， ETH_PORT_CTRL *(参见 Unity Pro, 通讯 , 功能块库)* 功能块允许禁用在 Unity Pro 应用程序中配置后已启用的服务。服务可以使用同样的功能块再次启用。

限制控制网络的数据流 （访问控制）

控制网络的数据流

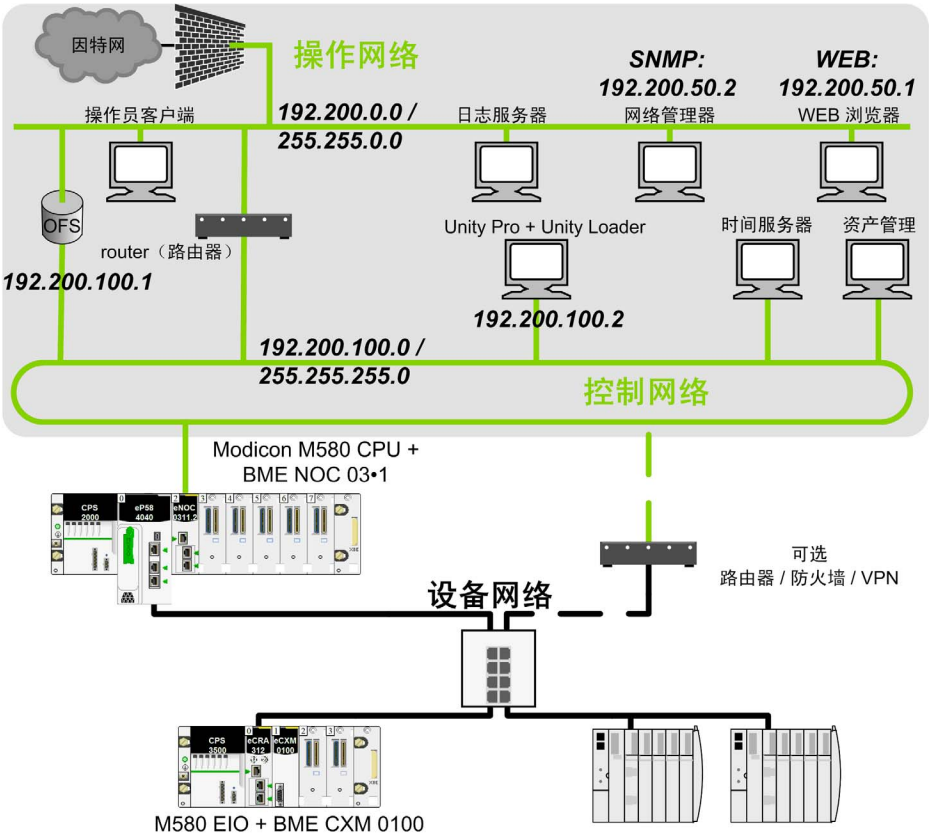
控制网络的数据流是基于 IP 的由控制网络启动的数据流。

描述

为了控制在嵌入式产品中访问通讯服务器，访问控制管理限制从控制网络到来源或子网 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。访问控制管理操作网络和控制网络 （位于灰色区域）上进行通讯的设备的 Ethernet 数据流。



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）能够访问 CPU Web 服务器。
- 连接到控制网络的任何设备 （IP 地址 = 192.200.100.x）能够使用 Modbus TCP 与 CPU 通讯，并能够访问 CPU Web 服务器。

要限制前一架构示例中的数据流，则授权地址和服务在 Unity Pro 访问控制表中如下设置：

来源	IP 地址	子网	子网掩码	FTP	TFTP	HTTP	端口 502	EIP	SNMP
网络管理器	192.200.50.2	否	–	–	–	–	–	–	X
操作网络	192.200.0.0	是	255.255.0.0	–	–	X	–	–	–
Unity Loader	192.200.100.2	否	–	X	–	–	–	–	–
控制网络	192.200.100.0	是	255.255.255.0	–	–	–	X	–	–
X 选中 **–** 未选中或无内容									

设施描述

针对使用 Modbus TCP 或 EtherNet/IP 授权与 CUP 进行通讯的设备已设置授权地址。

前一示例中每个 IP 地址的服务设置说明：

192.200.50.2 (SNMP): 设置为使用 SNMP 从网络管理器授权访问。

192.200.0.0 (HTTP): 操作网络子网设置为授权所有 Web 浏览器连接到操作网络以访问 CPU web 浏览器。

192.200.100.2 (FTP): 设置为使用 FTP 从 Unity Loader 授权访问。

192.200.100.0 (Port502): 控制网络子网设置为授权所有设备连接到控制网络 (OFS, Unity Pro, Unity Loader) 以通过 Port502 Modbus 访问 CPU。

注意：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 Unity Pro **安全性**屏幕中，在子网规则之前针对专用子网输入特定规则。例如：要给定特殊 SNMP 权限到设备 192.200.50.2，则在全局子网规则 192.200.0.0/255.255.0.0 之前输入规则，该子网允许 HTTP 访问子网的所有设备。

设置安全通讯

简介

安全通讯的目标是保护通讯通道，该通道允许远程访问系统的关键资源 （例如 PAC 嵌入式应用程序、固件）。 IPsec （因特网协议安全）是由 IETF 定义的开放标准，以在 IP 网络上提供受保护的专用通讯，该网络通过使用加密和协议安全机制组合来提供。我们的 IPsec 保护实施包括抗重放、消息完整性检查和消息初始验证。

IPsec 受 Microsoft Windows 7 支持，并可从 PC 操作系统启动。

描述

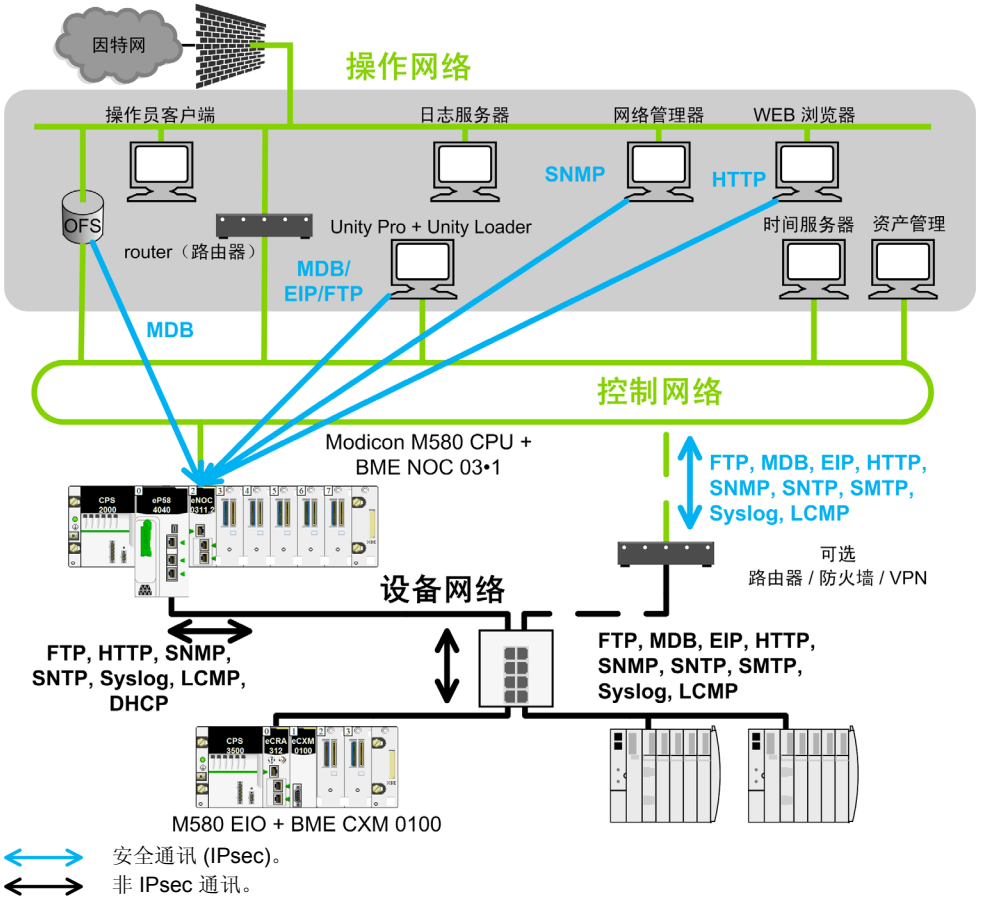
IPsec 功能允许确保：

- 控制室 Modbus 通过 BME NOC 03•1 模块访问 PAC CPU。
- 控制室以服务器模式 (Modbus, EtherNet/IP, HTTP, FTP, SNMP) 访问在 BME NOC 03•1 模块内运行的通讯服务。

注意：IPsec 旨在保护在 PAC 内以服务器模式运行的服务的安全。PAC 启动的安全客户端服务在该手册范围之外。

架构示例

下图的目的是通过示例说明从控制室到 Modicon M580 的安全通讯涉及的各种协议或服务 PAC。



带安全通讯功能的数据流

下表显示可从 IPsec 安全通讯获益的 Ethernet 服务：

因特网服务或流量	安全通讯
SNMP 代理	IPsec(1)
SNMP 陷阱	IPsec
EIP class 1 扫描器	否
EIP class 3 客户端	否 (2)
EIP class 3 服务器	IPsec(1)
Modbus 扫描器	否 (3)
Modbus 客户端 (port502)	否 (2)
Modbus 服务器 (port502)	IPsec(1)
HTTP	IPsec(1)
ICMP (ping, ...)	IPsec(1)
DHCP, BOOTP 客户端	否 (2)
DHCP, BOOTP 服务器	否
FTP 服务器 , TFTP 服务器	IPsec(1)
Syslog 客户端 (UDP)	否 (2)
(1) IKE/IPsec 由对等 (PC) 启动之前，该流量清零。一旦建立 IKE/IPsec，该流量受 IPsec 保护。 **(2)** IPsec 启用时，此客户端服务由 BME NOC 03•1 启动不可用。 **(3)** 无 IPsec 保护时，此客户端服务可用。	

注意：IPsec 为 OSI 3 层保护。 OSI 2 层保护 （ARP、 RSTP、 LLDP、回路检查协议）不受 IPsec 保护。

限制

架构中的 IPsec 限制：BME NOC 03•1 不支持 IP 转发到设备网络。

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 / 防火墙 /vpn （例如 ConneXium 防火墙）以在控制网络和设备网络之间提供安全通讯 （如上一张架构示例图 (参见第 *21* 页) 所示）。

从控制网络执行以下操作要求透明：

- 从 Unity Loader 到 FTP 服务升级 Modicon M580 CPU 固件。
- 从网络管理到 SNMP 服务执行 Modicon M580 CPU 网络诊断。
- 从 DTM 到 EIP 服务诊断 Modicon M580 CPU。
- 从 Web 浏览器到 HTTP 服务诊断 Modicon M580 CPU。

- 通过 syslog 服务记录 syslog 服务器中的 Modicon M580 CPU 网络安全事件。
- 通过 NTP 服务从全局时间服务器同步 Modicon M580 CPU 时间。

在系统架构中设置 IPsec 通讯

继续执行以下步骤以设置 IPsec 通讯：

- 在控制室内，识别要使用 Modbus （Unity Pro、 Unity Loader、 OFS、客户应用程序如 SGBackup...）与 PAC 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 BME NOC 03•1 模块的 Unity Pro DTM、Unity Loader、 SNMP 管理器、 Web 浏览器、Web designer）上配置的每个 BME NOC 03•1 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。
- 包含连接到控制网络的每个 PAC 背板上的带 IPsec 功能的 BME NOC 03•1 模块。
  要在 BME NOC 03•1 模块上配置 IPsec 功能，继续执行 2 个步骤：
  - 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。
    注意：由于 IPsec 依赖此共享密钥，所以它是安全政策的关键元素，必须由安全管理员管理。

BME NOC 03•1 模块配置使用 Unity Pro 执行。应用程序通过 USB 链路进行初始下载，未来下载通过以太网使用 IPsec 功能执行 （如果 IPsec 已启用）。

支持 IPsec 需求的每台 PC 要符合以下 IPsec 配置的要求：

- 使用 Microsoft Windows 7 OS。
- 有管理员权限以配置 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** (参见第 *15* 页) 主题中的说明加强 PC。

参阅配置 IP 安全通讯 *(参见 Modicon M580, BME NOC 03•1 Ethernet 通讯模块，安装和配置指南)* 主题，了解更多有关配置的详情。

在系统架构中诊断 IPsec 通讯

配置 IP 安全通讯 *(参见 Modicon M580, BME NOC 03•1 Ethernet 通讯模块，安装和配置指南)* 主题提供系统架构中的 IPsec 诊断信息。

设置网络安全审计 （事件记录）

简介

记录事件和记录分析对安全系统来说很重要。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。网络安全相关的事件会进行局部记录，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 （Ethernet 网络安全事件受到监控的连接点：设备、 Unity Pro 或 DTM）。

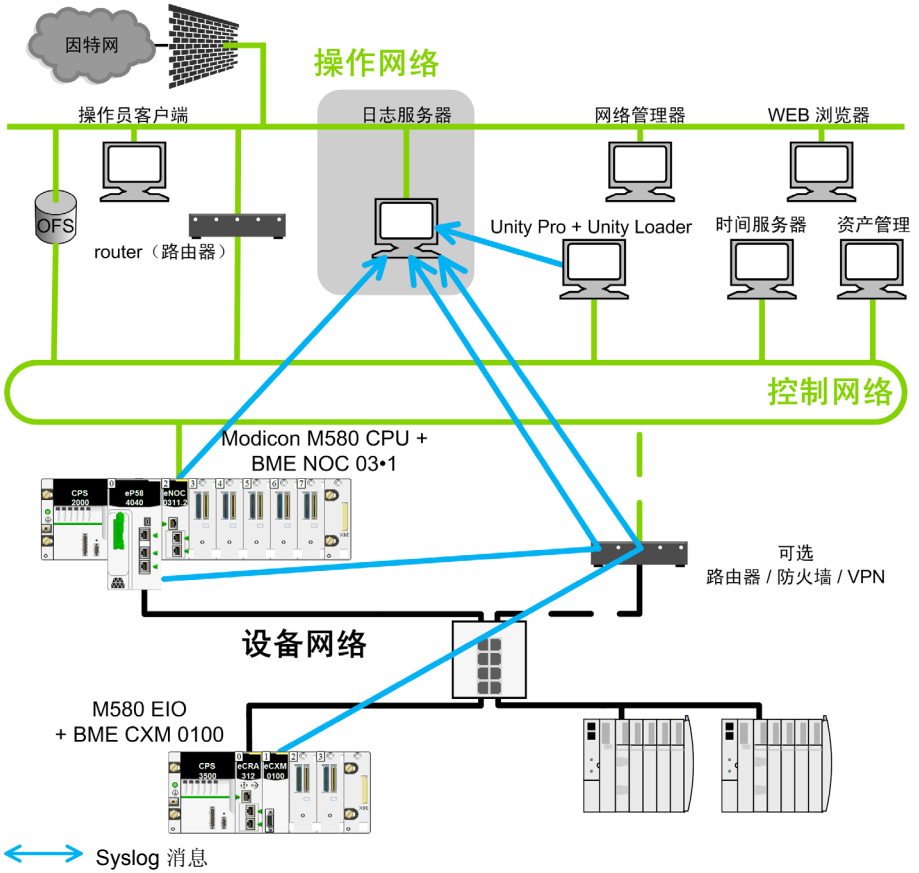
事件日志服务说明

每个日志客户端的角色为：

- 检测事件并记录事件的时标。
  单个 NTP 参考需要在系统中配置，从而记录网络安全事件的时标。
- 发送已检测的事件到事件记录服务器。
  事件使用 syslog 协议 （RFC 5424 规格）在客户端和服务器之间交换。
  syslog 消息遵循 RFC 5424 规格描述的格式。
  Syslog 交换通过 TCP 协议完成。
  设备发生瞬态网络故障时，事件不会丢失。设备复位时，事件将丢失。

架构示例

下图突出显示系统架构中记录服务器的位置：



事件已记录

Syslog 消息结构：

字段	说明
PRI	类别和严重性信息 （下表提供说明）。
版本	syslog 协议规格的版本 （RFC 5424 版本 = 1）。
时标	时标格式由推荐以下 ISO8601 因特网日期和时间格式的 RFC 3339 发布：YYY-MM-DD**T**hh:mm:ss.nnn**Z** **注意：-**、 **T**、 **:**、 **.**、 **Z** 是强制必需的字符，它们是时标字段的一部分。 **T** 和 **Z** 需要以大写字母写入。 **Z** 指定时间为 UTC。 时间字段内容说明： **YYY** 年 **MM** 月 **DD** 日 **hh** 时 **mm** 月 **ss** 秒 **nnn** 秒的细分单位为毫秒 （如果没有则为 0）
HOSTNAME	识别最初发送 syslog 消息的机器：完全合格的域名 (FQDN) 或源静态 IP 地址（如果 FQDN 不受支持）。
APP-NAME	识别发起 syslog 消息的应用程序。它包含允许识别发送消息的实体的信息 （例如商业参考的子集）。
PROCID	识别发送事件的过程、实体或组件。 接收 NILVALUE （如果未使用）。
MSGID	识别事件相关消息的类型，例如 HTTP、 FTP、 Modbus。 接收 NILVALUE （如果未使用）。
MESSAGE TEXT	该字段包含以下信息： ● 发出者地址：生成日志的实体的 IP 地址。 ● 对等 ID：对等 ID，如果对等涉及操作 （例如，记录操作的用户名）。接收 null （如果未使用）。 ● 对等地址：对等 IP 地址，如果对等涉及操作。接收 null （如果未使用）。 ● 类型：识别消息的唯一编号 （下表提供说明）。 ● 内容：描述消息的字符串 （下表提供描述）。

下表介绍链接到能够在 syslog 服务器中进行记录的 PAC 的事件：

事件描述	类别	安全性 (1)	类型	注释
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。 例如：通过 FTP 的数据存储、通过 Modbus 的 Unity Pro 应用程序密码、通过 FTP 的固件上载、FDR ... ● 用户成功登录到工具。 例如：Unity Pro 安全编辑器。 ● 成功的 TCP 连接 （无用户）。 例如：M580 CPU 的 Port502 Modbus TCP/IP 显示消息传递	10	信息类	1	Successful login, 或 successful connection.
从工具或设备连接失败 ● 因错误访问控制列表 (ACL) 检查导致失败连接（源 IP 地址或 TCP 端口过滤）。 ● 失败的登录 （ACL 检查正确）。 例如：通过 FTP 的数据存储、通过 Modbus 的 Unity Pro 应用程序、通过 FTP 的 FDR 服务器 ... ● 用户登录软件工具失败。 例如 : Unity Pro。 ● 失败的 TCP 连接 （无用户）。 例如：M580 CPU 的 Port502 Modbus TCP/IP 显示消息传递	10	警告	2	Failed login, 或 failed connection。
局部或由对等触发断开连接： ● 注销请求 (FTP)。	10	信息类	5	Disconnection。
自动注销 （例如不活动超时）。	10	信息类	6	Auto logout。
系统中的主要更改： ● 配置范围外的参数运行时间更改：CPU 应用程序参数更改 （例如循环时间或警戒时钟）。	13	通知	87	XXXX parameter update （XXXX 识别参数）。 例如 : cycle time parameter update。
系统中的主要更改： ● 配置范围外处理数据运行时间更改。	13	通知	88	XXXX process update （XXXX 识别参数）。
系统中的主要更改： ● 应用程序和配置上载，或配置仅上载到设备（包括 CCOTF 功能）。	13	信息类	9	XXXX upload （XXXX 识别上载的对象）。 例如 : application upload, configuration upload.
系统中的主要更改： ● 下载设备的应用程序和配置。	13	信息类	8	XXXX download （XXXX 识别下载的对象）。 例如 : application download, configuration download。
(1) 注：项目严重性、 Emergency、 Alert、 Critical、 Error、 Warning、 Notice、 Informational、 Debug 在此表中用作 syslog 事件消息的属性，并在 Internet Engineering Task Force (IETF) 的 RFC 5424 规格中定义。				

事件描述	类别	安全性 (1)	类型	注释
系统中的主要更改： ● 固件上载。	13	信息类	10	XXXX upload。 例如：firmware upload、 web pages upload。
配置范围外的通讯参数运行时间更改。 ● 通讯服务启用或禁用（M580 PAC 设备中的 FTP、TFTP、 HTTP、功能块）。	10	警告	18	Major communication parameter update: XXXX YYYY（XXXX = 通讯参数 ID、YYYY = 值）。 例如：major communication parameter update: FTP enable。
嵌入式交换机端口状态更改： ● 端口链路连通、端口链路断开， ...	10	警告	19	ETHXX YYYY （XX = 端口号，YYYY = 端口状态）。 例如：ETH3 link down （端口 3 电缆断开连接之后）。
已检测到的拓扑更改： ● 从 RSTP：端口角色更改或根更改。	10	警告	20	topology change detected。
完整性检查错误： ● 数字签名错误。 ● 仅完整性 （散列）错误。	10	错误	84	XXXX integrity error（XXXX 识别带已检测到错误的对象）。 例如：firmware integrity error。
系统中的主要更改： ● 程序操作模式更改 (run, stop, init, ...)。	13	通知	85	XXXX state update: YYYY（XXXX 识别带更改状态的对象，YYYY 识别新状态）。 例如：PLC state update: RUN。
系统中的主要更改： ● 硬件更改 （SD 卡插入、模块更换 ...）。	13	信息类	26	XXXX hardware update: YYYY（XXXX 识别带更改状态的硬件，YYYY 识别升级）。 例如：PLC hardware update: SD card insertion。
(1) 注：项目严重性、 Emergency、 Alert、 Critical、 Error、 Warning、 Notice、 Informational、 Debug 在此表中用作 syslog 事件消息的属性，并在 Internet Engineering Task Force (IETF) 的 RFC 5424 规格中定义。				

注意：前表中未说明的 Unity Pro 特定事件在 **安全编辑器** 用户配置文件 *(参见 Unity Pro, 操作模式)* 审计列中定义，并通过 syslog 发送。

每个 RFC 5424 事件类型相关联的规格的 Syslog 消息类别值：

类别值	说明
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。
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。

每个 RFC 5424 事件类型相关联的规格的 Syslog 消息安全值：

安全值	关键字	说明
0	紧急	系统不可用。
1	警报	必须立即采取操作。
2	关键	关键条件。
3	错误	错误条件。
4	警告	警告条件。
5	通知	正常但重要的条件。
6	信息类	非正式消息。
7	调试	调试级消息。

在系统架构中设置 Syslog 服务器

各种操作系统可使用多种 syslog 服务器。 syslog 服务器提供者的示例：

WinSyslog: 用于 Windows 操作系统。

链路 : *www.winsyslog.com/en/*。

Kiwi Syslog 用于 Windows 操作系统。

链路 : *www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx*。

Splunk 用于 Windows 和 Unix 操作系统。

链路 : *www.splunk.com/*。

Rsyslog 用于 Unix 操作系统。

链路 : *www.rsyslog.com/*。

Syslog-ng 用于 Unix 操作系统的开放源码。

链路 : *www.balabit.com/network-security/syslog-ng/opensource-logging-system*。

Syslog Server 用于 Windows 操作系统的开放源码。

链路 : *sourceforge.net/projects/syslog-server/*。

在系统架构中设置 Syslog 客户端

所有设备、 DTM 和 Unity Pro 在 Unity Pro 中管理事件记录。

事件记录功能、服务器地址和端口号在 Unity Pro 中配置，如下所示，并且这些参数在 **生成** 操作后会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**事件记录**复选框 （缺省情况为不选中）。 **注意：** 选中此设置的项目仅可以在 Unity Pro 10.0 或更高版本中打开。
4	输入有效的 **SYSLOG 服务器地址**和 **SYSLOG 服务器端口号**。
5	配置此设置后执行**生成** （不要求选择**分析项目**）。

诊断事件记录

下表显示各种设备可用的事件记录诊断的类型：

设备	诊断信息
Unity Pro	如果 syslog 服务器发生通讯错误，则检测到的错误会记录在事件查看器中。
BME NOC 03•1 设备 DDT （SERVICE_STATUS2 参数）	两个诊断信息可用： **EVENT_LOG_STATUS:** 值 = 1，如果事件日志服务可操作或已禁用。 值 = 0，如果事件日志服务不可操作。 **LOG_SERVER_NOT_REACHABLE:** 值 = 1，如果 syslog 客户端不接收 syslog 服务器的 TCP 消息确认。 值 = 0，如果确认已接收。
Modicon M580 CPU 设备 DDT	
BME CXM 设备 DDT	

控制识别和身份验证

管理帐户

关于帐户管理， Schneider Electric 有以下建议：

- 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。

管理用户帐户控制 (UAC) (Windows 7)

为了阻止未经授权而试图对系统进行更改的行为， Windows 7 对应用程序授予普通用户的许可级别 （无管理权限）。在此级别，应用程序不能对系统进行更改。 UAC 提示用户授予或拒绝向应用程序分配其他权限。将 UAC 设置为其最高级别。在最高级别时， UAC 在允许应用程序进行要求管理权限的更改之前会提示用户。

要访问 Windows 7 中的 UAC 设置，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 7 **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。
Schneider Electric 建议采用以下密码管理准则：

- 对所有邮件和 Web 服务器、 CPU 和 Ethernet 界面模块启用密码身份验证。
- **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
  - Unity Pro
- 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。
- 不要通过电子邮件或其他通过因特网的不安全方式传输密码。

管理 HTTP

超文本传输协议 (HTTP) 是供 Web 使用的底层协议。该协议用于控制系统，以支持控制产品中的嵌入式 Web 服务器。Schneider Electric Web 服务器通过 Web 页面使用 HTTP 通讯显示数据和发送命令。

如果不需要 HTTP 服务器，请将其禁用。否则，如果可能，请使用*安全超文本传输协议* (HTTPS)，它是由 HTTP 和加密协议组合而成的，而不是 HTTP。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。

可将 HTTPS 配置为支持此功能的产品上的缺省 Web 服务器。

管理 SNMP

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

- 管理器：通过发出请求、获取响应以及侦听和处理代理发出的陷阱来管理网络上 SNMP 代理的应用程序
- 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、桥接器、集线器、 PAC、驱动器。
- 网络管理系统 (NMS)：管理员执行管理任务所使用的终端

对于网络管理， Schneider ElectricEthernet 设备具有 SNMP 服务功能。

SNMP 常常会随作为读取字符串的 **public** 和作为写入字符串的 **private** 一起自动安装。此类安装允许攻击者在系统上进行侦查以拒绝服务。

通过 SNMP 帮助减少攻击风险：

- 如果可能，停用 SNMP v1 和 v2，并使用 SNMP v3，这可将密码和消息进行加密。
- 如果需要使用 SNMP v1 或 v2，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量。
- 筛选特定主机的控制网络和操作网络之间的 SNMP v1 和 v2 命令，或通过单独、安全的管理网络进行传送。
- 通过识别有权限查询 SNMP 设备的 IP 地址来控制访问。

管理 Unity Pro 应用程序、段、数据存储和固件密码

在 Unity Pro 中，密码应用到以下方面 （取决于 CPU）：

- **应用程序**
  Unity Pro 和 CPU 应用程序密码保护可防止意外的应用程序修改、下载或打开 （.STU 和 .STA 文件）。查阅应用程序保护 *(参见 Unity Pro, 操作模式)* 主题，了解更多详情。
- **段**
  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。查阅段和子程序保护 *(参见 Unity Pro, 操作模式)* 主题，了解更多详情。
  注意：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。
- **数据存储**
  通过密码进行的数据存储保护可防止对 SD 存储卡数据存储区域的意外访问 （如果 CPU 中已插入有效的存储卡）。查阅数据存储保护 *(参见 Unity Pro, 操作模式)* 主题，了解更多详情。
- **固件**
  通过密码进行的下载保护可防止对 CPU 内的恶意固件下载。

控制授权

Unity Pro 安全性编辑器

安全配置工具用于定义软件用户及其相应授权。 Unity Pro 访问安全性只与安装软件的终端有关，不涉及项目，因为项目有自己的安全保护系统。

访问安全性管理 *(参见 Unity Pro, 操作模式)* 部分提供更多有关安全性编辑器的详细信息。

编程和监控模式

两种模式可用于访问**在线**模式的 CPU：

- **编程**模式：CPU 程序可修改。当终端首次连接到 CPU 时， CPU 变成已保留，只要 CPU 为已保留，则另一终端将无法进行连接。
- **监控**模式：CPU 程序无法修改，但变量可以修改。监控模式无法保留 CPU，可在监控模式中访问已保留的 CPU。

要在 Unity Pro 中选择模式，选择：**工具 →选项 ... →连接 →缺省连接模式**。

参阅在线模式服务 *(参见 Unity Pro, 操作模式)* 主题，了解更多有关这些模式的详情。

程序选择保护

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。参阅段和子程序保护 *(参见 Unity Pro, 操作模式)* 主题，了解更多详情。

注意：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。

CPU 存储器保护

对于任意通讯通道，存储器保护禁止在在线模式下将项目传输至 CPU 以及进行修改。

存储器保护按如下所示激活：

- Modicon M340 CPU：输入位。参阅 Modicon M340 处理器配置 *(参见 Unity Pro, 操作模式)* 章节，了解更多详情。
- Modicon M580 CPU：输入位。参阅管理运行 / 停止输入 *(参见 Modicon M580, 硬件, 参考手册)*，了解更多详情。
- Modicon Quantum CPU：CPU 模块上的物理键开关，可用于低端 *(参见 采用 Unity Pro 的 Quantum, 硬件, 参考手册)* 或高端 *(参见 采用 Unity Pro 的 Quantum, 硬件, 参考手册)* CPU。
- Modicon Premium CPU：输入位。参阅 Premium 处理器配置 *(参见 Unity Pro, 操作模式)* 章节，了解更多详情。
- Modicon MC80 CPU：输入位。 Modicon MC80 CPU 手册提供更多详细信息。

CPU 远程运行 / 停止访问

远程运行 / 停止访问管理定义 CPU 如何远程启动或停止，并取决于平台：

Modicon M580： CPU 远程访问运行 / 停止允许执行下列操作之一：

- 通过请求远程停止或运行 CPU。
- 通过请求远程停止 CPU。通过请求拒绝远程运行 CPU，只有在配置有效的输入时才能通过输入控制运行。
- 通过请求拒绝远程运行或停止 CPU。

请参阅有关有助于防止远程命令访问运行 / 停止模式的 CPU 配置选项的*管理运行 / 停止输入 (参见 Modicon M580, 硬件，参考手册)* 的章节。

Modicon M340： CPU 远程访问运行 / 停止允许执行下列操作之一：

- 通过请求远程停止或运行 CPU。
- 通过请求远程停止 CPU。通过请求拒绝远程运行 CPU，只有在配置有效的输入时才能通过输入控制运行。

请参阅有关 *Modicon M340 处理器配置 (参见 Unity Pro, 操作模式)* 的章节。

Modicon Premium： CPU 远程访问运行 / 停止允许执行下列操作之一：

- 通过请求远程停止或运行 CPU。
- 通过请求远程停止 CPU。通过请求拒绝远程运行 CPU，只有在配置有效的输入时才能通过输入控制运行。

请参阅有关 *Premium\Atrium 处理器配置 (参见 Unity Pro, 操作模式)* 的章节。

Modicon Quantum： CPU 远程访问运行 / 停止允许：

- 通过请求远程停止或运行 CPU。

Modicon MC80： CPU 远程访问运行 / 停止允许执行下列操作之一：

- 通过请求远程停止或运行 CPU。
- 通过请求远程停止 CPU。通过请求拒绝远程运行 CPU，只有在配置有效的输入时才能通过输入控制运行。
- 通过请求拒绝远程停止 CPU。

请参阅 MC80 用户手册中有关 **Modicon MC80 处理器配置**的章节。

CPU 变量访问

要保护 CPU 数据在运行时防止非法读取或写入访问，请执行以下步骤：

- 使用非定位数据。
- 配置 Unity Pro 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**。
  仅在选择**数据字典**时，才能选择**仅 HMI 变量**。
- 标记为从 HMI 或 SCADA 访问的 *HMI* 变量。未标记为 *HMI* 的变量无法通过外部客户端访问。
- 与 SCADA 的连接必须依赖 OFS。

管理数据完整性检查

简介

您可使用获得授权 PC 上 Unity Pro 中的完整性检查功能，以防止通过 Internet 上的病毒 / 恶意软件更改 Unity Pro 文件和软件。

执行完整性检查

仅首次启动 Unity Pro 时，Unity Pro 自动执行完整性检查。PAC 固件完整性检查在新固件升级或 PAC 重启之后将自动完成。要在 Unity Pro 中手动执行完整性检查，请遵循以下步骤：

步骤	操作
1	单击**帮助 →关于 Unity Pro XXX**。
2	在**完整性检查**字段中，单击**执行自检**。 **结果**：完整性检查会在后台运行，不会影响应用程序的性能。 Unity Pro 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。 **注意**：如果完整性检查显示组件登录未成功，则**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。

章 3
平台的网络安全服务

简介

本章节列出平台可用的主要网络安全服务，并指示在 Unity Pro 帮助中能够找到详细信息的位置。

本章包含了哪些内容？

本章包含了以下主题：

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。所列可用网络安全服务用于以下元素：

- Unity Pro (参见第 *38* 页) 软件。
- Modicon M340 (参见第 *39* 页) CPU。
- Modicon M580 (参见第 *39* 页) CPU。
- Modicon Momentum （尚未实施的网络安全服务）。
- Modicon Quantum (参见第 *40* 页) CPU 和通讯模块。
- Modicon X80 (参见第 *41* 页) 模块。
- Modicon Premium/Atrium (参见第 *41* 页) CPU 和通讯模块。

以下所列网络安全服务在前一章中已说明：

- 禁用未使用的服务 (参见第 *17* 页)
- 访问控制 (参见第 *18* 页)
- 安全通讯 (参见第 *20* 页)
- 事件记录 (参见第 *24* 页)
- 身份验证 (参见第 *31* 页)
- 授权 (参见第 *34* 页)
- 完整性检查 (参见第 *36* 页)

Unity Pro 软件中的网络安全服务

Unity Pro 软件中的网络安全服务可用性：

软件		网络安全服务						
参考	版本	禁用未使用的服务	访问控制	安全 com	事件记录	身份验证	授权	完整性检查
Unity Pro	8.1	–	N.A.	–	–	X	X	X
Unity Pro	10.0	–	N.A.	X	X	X	X	X
X 可用，至少一个服务已实施。 **–** 不可用 **N.A.** 不适用								

Modicon M340 CPU 中的网络安全服务

Modicon M340 CPU 中的最低固件版本和网络安全服务可用性：

CPU		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	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	–
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon M580 CPU 中的网络安全服务：

Modicon M580 CPU 中的最低固件版本和网络安全服务可用性：

CPU		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	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
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon Quantum CPU 和模块中的网络安全服务

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

CPU		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	事件记录	身份验证	授权	完整性检查
140 CPU 311 10	3.20	–	–	–	–	X	X	–
140 CPU 434 12•	3.20	–	–	–	–	X	X	–
140 CPU 534 14•	3.20	–	–	–	–	X	X	–
140 CPU 651 •0	3.20	X	X	–	–	X	X	–
140 CPU 652 60	3.20	X	X	–	–	X	X	–
140 CPU 658 60	3.20	X	X	–	–	X	X	–
140 CPU 670 60	3.20	X	X	–	–	X	X	–
140 CPU 671 60	3.20	X	X	–	–	X	X	–
140 CPU 672 6•	3.20	X	X	–	–	X	X	–
140 CPU 678 61	3.20	X	X	–	–	X	X	–
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon Quantum 模块支持网络安全服务：

模块		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	事件记录	身份验证	授权	完整性检查
140 NOC 771 0•	1.00	–	X	–	–	X	–	–
140 NOC 780 00	2.00	X	X	–	–	X	–	–
140 NOC 781 00	2.00	X	X	–	–	X	–	–
140 NOE 771 ••	X	X	–	–	–	X	–	–
140 NWM 100 00	–	X	–	–	–	–	–	–
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon X80 模块中的网络安全服务

Modicon X80 模块支持网络安全服务：

模块		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	事件记录	身份验证	授权	完整性检查
BME CXM 0100	1.01	X	X	–	X	–	–	X
BME NOC 0301	1.01	X	X	X	X	X	–	X
BME NOC 0311	1.01	X	X	X	X	X	–	X
BMX NOC 0401.2	2.05	X	X	–	–	–	–	–
BMX NOE 0100.2	2.90	X	X	–	–	–	–	–
BMX NOE 0110.2	6.00	X	X	–	–	–	–	–
BMX PRA 0100	2.60	X	X	–	–	X	–	–
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon Premium/Atrium CPU 和模块中的网络安全服务

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

CPU		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	事件记录	身份验证	授权	完整性检查
TSX H57 •4M	3.10	–	–	–	–	X	X	–
TSX P57 0244M	3.10	–	–	–	–	X	X	–
TSX P57 •04M	3.10	–	–	–	–	X	X	–
TSX P57 •54M	3.10	–	–	–	–	X	X	–
TSX P57 1634M TSX P57 2634M TSX P57 3634M （通过 ETY 端口）	3.10	X	X	–	–	X	X	–
TSX P57 4634M TSX P57 5634M TSX P57 6634M （嵌入式 Ethernet 端口）	3.10	X	X	–	–	X	X	–
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon Premium/Atrium 模块支持网络安全服务：

模块		网络安全服务						
参考	最低固件	禁用未使用的服务	访问控制	安全 com	事件记录	身份验证	授权	完整性检查
TSX ETC 101.2	2.04	X	X	–	–	–	–	–
TSX ETY 4103	5.70	X	X	–	–	–	–	–
TSX ETY 5103	5.90	X	X	–	–	–	–	–
X 可用，至少一个服务已实施。 **–** 不可用								

Modicon M340 安全服务

概述

在不同手册中为 Modicon M340 CPU 提供的通讯安全服务设置说明如以下主题所述。

Modicon M340 CPU 与嵌入式 Ethernet 端口

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器, 用户手册)* 的章节。

访问控制： 请参阅有关*消息传递配置参数 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器, 用户手册)* 的章节。

Modicon M580 安全服务

Modicon M580 CPU

描述*安全选项卡 (参见 Modicon M580, 硬件 , 参考手册)* 的主题提供与网络安全相关的通讯参数说明。

Modicon Quantum 安全服务

概述

在不同手册中为 Modicon Quantum CPU 和 Ethernet 模块提供的通讯安全服务设置说明如以下主题所述。

Modicon Quantum CPU 与嵌入式 Ethernet 端口

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全（启用 / 禁用 HTTP、FTP 和 TFTP）(参见 Modicon Quantum 及 Unity, Ethernet 网络模块，用户手册)* 的章节。

访问控制： 请参阅有关 *Modicon Quantum Unity 以太网控制器消息传递配置 (参见 Modicon Quantum 及 Unity, Ethernet 网络模块，用户手册)* 的章节。

140 NOC 771 0x 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全（启用 / 禁用 HTTP、FTP 和 TFTP）(参见 Modicon Quantum 及 Unity, Ethernet 网络模块，用户手册)* 的章节。

访问控制： 请参阅有关*配置访问控制 (参见 Quantum, 140 NOC 771 01 以太网通讯模块，用户手册)* 的章节。

140 NOC 780 00 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 Quantum EIO, 控制网络，安装和配置指南)* 的章节。

访问控制： 请参阅有关*配置访问控制 (参见 Quantum EIO, 控制网络，安装和配置指南)* 的章节。

140 NOC 781 00 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 Quantum EIO, 控制网络，安装和配置指南)* 的章节。

访问控制： 请参阅有关*配置访问控制 (参见 Quantum EIO, 控制网络，安装和配置指南)* 的章节。

140 NOE 771 xx 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全（启用 / 禁用 HTTP、FTP 和 TFTP）(参见 Modicon Quantum 及 Unity, Ethernet 网络模块，用户手册)*、*安全 (参见 Modicon Quantum 及 Unity, Ethernet 网络模块，用户手册)* 和*建立 HTTP 和写入密码 (参见 Modicon Quantum 及 Unity, Ethernet 网络模块，用户手册)* 的章节。

140 NWM 100 00 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全（启用 / 禁用 HTTP、 FTP 和 TFTP）(参见 Modicon Quantum 及 Unity, Ethernet 网络模块 , 用户手册)* 的章节。

Modicon X80 安全服务

概述

在不同手册中为 Modicon X80 Ethernet 模块提供的通讯安全服务设置说明如以下主题所述。

BME CXM 0100 模块

可选配置章节提供与网络安全相关的通讯参数说明。

BME NOC 03•1 模块

配置安全服务 *(参见 Modicon M580, BME NOC 03•1 Ethernet 通讯模块，安装和配置指南)* 章节提供与网络安全相关的通讯参数说明。

BMX NOC 0401.2 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器，用户手册)* 的章节。

访问控制： 请参阅有关*配置访问控制 (参见 Modicon M340, BMX NOC 0401 以太网通讯模块，用户手册)* 的章节。

BMX NOE 0100.2 和 BMX NOE 0110.2 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器，用户手册)* 的章节。

访问控制： 请参阅有关*消息传递配置参数 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器，用户手册)* 的章节。

BMX PRA 0100 模块

将 BMX PRA 0100 配置为 Modicon M340 CPU。所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器，用户手册)* 的章节。

访问控制： 请参阅有关*消息传递配置参数 (参见 用于 Ethernet 的 Modicon M340, 通讯模块和处理器，用户手册)* 的章节。

Modicon Premium/Atrium 安全服务

概述

在不同手册中为 Modicon Premium/Atrium CPU 和 Ethernet 模块提供的通讯安全服务设置说明如以下主题所述。

Modicon Premium/Atrium CPU 与嵌入式 Ethernet 端口

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全服务配置参数 (参见 使用 Unity Pro 的 Premium 和 Atrium, Ethernet 网络模块 , 用户手册)* 的章节。

访问控制： 请参阅有关 *TCP/IP 消息传递配置 (TSX P57 6634/5634/4634) (参见 使用 Unity Pro 的 Premium 和 Atrium, Ethernet 网络模块 , 用户手册)* 的章节。

通过 ETY 端口的 Modicon Premium/Atrium CPU

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全服务配置参数 (参见 使用 Unity Pro 的 Premium 和 Atrium, Ethernet 网络模块 , 用户手册)* 的章节。

访问控制： 请参阅有关 *TCP/IP 消息传递配置 (参见 使用 Unity Pro 的 Premium 和 Atrium, Ethernet 网络模块 , 用户手册)* 的章节。

TSX ETC 101.2 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全 (参见 Premium, TSX ETC 101 以太网通讯模块 , 用户手册)* 的章节。

访问控制： 请参阅有关*配置访问控制 (参见 Premium, TSX ETC 101 以太网通讯模块 , 用户手册)* 的章节。

TSX ETY x103 模块

所列主题提供与网络安全相关的通讯参数说明：

以太网通讯： 请参阅有关*安全服务配置参数 (参见 使用 Unity Pro 的 Premium 和 Atrium, Ethernet 网络模块 , 用户手册)* 的章节。

访问控制： 请参阅有关 *TCP/IP 消息传递配置 (参见 使用 Unity Pro 的 Premium 和 Atrium, Ethernet 网络模块 , 用户手册)* 的章节。

术语

%I

根据 CEI 标准， %I 表示离散量输入类型的语言对象。

%IW

根据 CEI 标准， %IW 表示模拟量输入类型的语言对象。

%M

根据 CEI 标准， %M 表示存储器位类型的语言对象。

%MW

根据 CEI 标准， %MW 表示存储器字类型的语言对象。

%Q

根据 CEI 标准， %Q 表示离散量输出类型的语言对象。

%QW

根据 CEI 标准， %QW 表示模拟量输出类型的语言对象。

%SW

根据 CEI 标准， %SW 表示系统字类型的语言对象。

1 类连接

CIP 传输 1 类连接，用于通过隐式消息在 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。

主环路

Ethernet RIO 网络的主环路。此环路包含 RIO 模块和本地机架 （包含具有 Ethernet I/O 通讯服务器服务的 CPU）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。

以太网 DIO 通讯服务器服务

M580 CPU (BME P58 1020, BME P58 2020, BME P58 3020, BME P58 4020) 的嵌入式通讯服务器服务，仅在 M580 设备网络中管理分布式设备

以太网 I/O 通讯服务器服务

M580 CPU (BME P58 2040, BME P58 3040, BME P58 4040) 的嵌入式通讯服务器服务，在 M580 设备网络中管理分布式设备**和** RIO 子站

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

支持使用 CPU 或其他 Ethernet 通讯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 等类型的存储器实体，其内容可由当前运行的程序进行修改。

域名

标识因特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.schneider-electric.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，通过主环路上的双环路交换机 (DRS) 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 Unity Pro 和设备 DTM 间共享的用户权限。

广播

发送给子网中所有设备的消息。

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、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、 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

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。

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。

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/Unity Pro/ConneXview 连接到 CPU
- 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 ElectricEtherNet/IP 通讯模块提供的功能，允许扫描器充当适配器的角色。本地从站使模块能够通过隐式消息连接发布数据。本地从站通常用于 PAC 之间的点对点交换。

本地机架

包含 CPU 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

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 （无分布式设备）。此拓扑由本地机架 （包含具有 Ethernet I/O 通讯服务器服务的 CPU）以及一个或多个 RIO 子站（每个子站包含一个 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

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。

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。

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

RIO 网络内包含 RIO 和分布式设备的基于 Ethernet 的网络。此网络上连接的设备遵循特定规则以便可以确定 RIO。

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

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）。

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。

连接起始

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。

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 Unity Pro 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。

ARRAY

ARRAY 是由单一类型的元素组成的表。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*)CPU 应用程序对提供的输入进行响应的时间。 ART 的测量是从 CPU 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。

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。

CCOTF

（*动态更改配置*） Unity Pro 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。

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。

通过在应用程序中使用 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

(*分布式 I/O*) 分布式设备的传统术语。 DRSs 使用 DIO 端口连接分布式设备。

DIO 云

一组不需要支持 RSTP 的分布式设备。 DIO 云只需要单一（非环路）铜缆连接。它们可以连接到 DRS 上的某些铜缆端口，也可以直接连接到*本地机架*中的 CPU 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，其中由本地机架中的 CPU DIO 通过通讯服务器服务执行 I/O 扫描。 DIO 网络流量在 RIO 流量 （这些流量在 RIO 网络中具有更高的优先级）之后传递。

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：

- 以 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

注意：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。

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。

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，每个调用通过图形功能块，由唯一的 [编号] 指示。此编号自动进行管理，无法修改。

在程序中定位和配置这些功能以执行您的应用程序。

您还可以使用 SDKC 开发工具包开发其他功能。

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。如果当前值等于预选值，则此输出将设置为 1。

EIO 网络

(*Ethernet I/O*) 基于 Ethernet 的网络，包含 3 种类型的设备：本地机架、 X80 EIO 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 X80 EIO 适配器模块的服务端口连接参与 EIO 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

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。

EtherNet/IP™

用于工业自动化应用的网络通讯协议，它将 TCP/IP 和 UDP 的标准因特网传输协议与应用层公共工业协议 (CIP) 组合在一起，以支持高速数据交换和工业控制。 EtherNet/IP 使用电子数据表 (EDS) 对各个网络设备及其功能进行分类。

FAST

事件触发的 (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图形编程语言。通过添加简单逻辑块 （AND、 OR 等），程序的每个功能或功能块均使用此图形形式表示。每个功能块的输入位于左侧，输出位于右侧。功能块输出可链接到其他功能块的输入，从而创建复合表达式。

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。

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或工厂的流程控制、资产管理或使用任何控制平台的其他系统中的任何软件应用程序。

HMI

(*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/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。

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*) 此语言由一系列基本指令组成。与用于对处理器编程的汇编语言非常相似。每个指令都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 / 输出导出的数据类型*）结构化的数据类型，用来表示一个模块或 CPU 的一个通道。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，保护使用 IPsec （因特网工程工作组 (IETF) 开发）的模块间流量的 IP 通讯会话。 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。

LD

（*梯形图*）一种编程语言，以非常类似于电路图 （触点、线圈等）的图形化方式表示要执行的指令。

M580 Ethernet I/O 设备

Ethernet 设备，提供自动网络恢复和确定性 RIO 性能。可计算解析 RIO 逻辑扫描所需的时间，系统可以从通讯中断中快速恢复。 M580Ethernet I/O 设备包括：

- 本地机架 （包括具有 Ethernet I/O 通讯服务器服务的 CPU）
- RIO 子站 （包括 Ethernet X80 EIO 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。

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。该协议使用抖动缓冲区来消除可变延迟的影响。

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。

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。

QoS

(*服务质量*) 将不同优先权分配给各种通讯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。

RIO 子站

Ethernet RIO 网络中三种类型 RIO 模块中的一种（*请参阅* **RIO 网络** *中的其他两种类型*）。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 的连接参与 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。

SFC

（*顺序功能图*）用于以图形和结构化方式表示顺序 CPU 的操作。 CPU 顺序行为和产生的各种情况的这一图形表示使用简单图形符号进行创建。

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*) 确定工业系统中的事件顺序并将这些事件与实时时钟关联的过程。

ST

(*结构化文本*) 该结构化文字语言是与计算机编程语言类似的开发语言。它可用于组织一系列指令。

T->O

(*目标到起始*) 请参见目标和起始。

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。

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：传输控制协议和因特网协议。 TCP/IP 是面向连接的协议，供 Modbus TCP 和 EtherNet/IP 用于发送显式消息。

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

注意：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。

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。

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