SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet CP 1543-1

操作说明

前言

文档指南 1

产品总览、功能 2

安装、连接、调试、操作 3

组态、编程 4

诊断和保养 5

技术规范 6

认证 7

12/2019

C79000-G8952-C289-08

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

⚠危险
表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

⚠警告
表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

⚠小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。 由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用 Siemens 产品

请注意下列说明：

⚠警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号 ® 的都是 Siemens AG 的注册商标。本印刷品中的其他符号可能是一些其他商标。若第三方出于自身目的使用这些商标，将侵害其所有者的权利。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
德国

C79000-G8952-C289-08
℗ 12/2019 本公司保留更改的权利

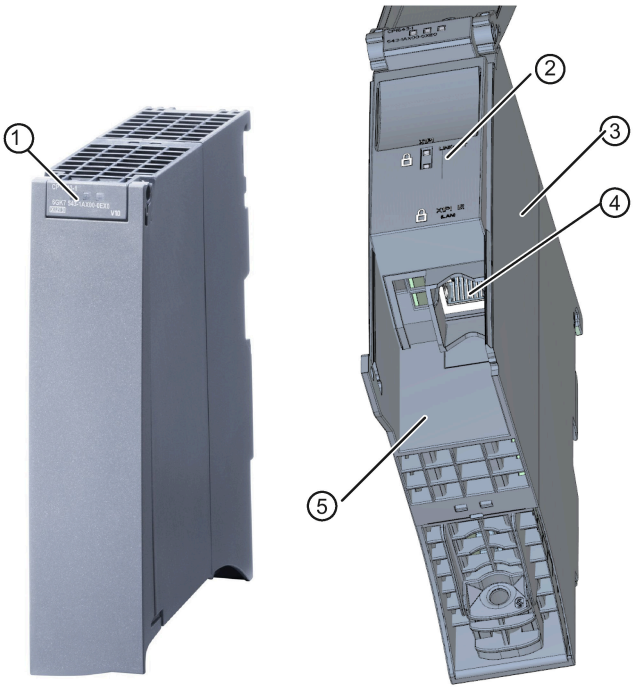
前言

部件编号、有效性和产品名称

本说明包含以下产品的相关信息：

CP 1543-1
部件编号 6GK7 543-1AX00-0XE0
硬件产品版本 2
固件版本 V2.2
用于 SIMATIC S7-1500 的通信处理器

CP 1543-1 的视图



① 显示状态和错误的 LED
② 以太网接口的 LED 指示灯，用于指示连接状态和工作状态
③ 型号牌
④ 以太网端口：1 个 8 针 RJ-45 插孔
挂锁图标表示到外部不安全子网的接口。
⑤ 标有 MAC 地址的标签

图 1 前盖关闭（左侧）和打开（右侧）的 CP 1543-1 的视图

地址标签：为 CP 预设的唯一 MAC 地址

CP 随附了默认 MAC 地址：

该 MAC 地址印于外壳上。

如果组态 MAC 地址（ISO 传输连接），建议使用印在模块上的 MAC 地址进行模块组态! 这可确保在子网中分配唯一的 MAC 地址！

本文档用途

本手册是 S7-1500 系统手册的补充。

利用本手册和系统手册中的信息，您将能够调试通信处理器。

本发布版本的新增内容

- 固件版本 V2.2 具有以下新功能：

  对 CPU 虚拟接口的支持，参见“CPU 的虚拟接口 (页 41)”部分。
- 新增 ATEX/IECEx 认证
- 编辑修订

版本历史

- 固件版本 V2.1 具有以下新功能：
  - 通过背板总线进行 IP 路由的扩展安全设置，参见“IP 路由 (页 41)”部分。
- 固件版本 V2.0 具有以下新功能：
  - 基于 TCP/IP 的 Secure OUC (Open User Communication)
  - Secure Mail：用于传送电子邮件的新系统数据类型 (SDT)

    备选：非安全传送（通过端口 25）或安全传送（通过端口 587）
  - 用作 FTP 服务器：访问 CPU 的 SIMATIC 存储卡
  - 通过背板总线进行 IP 路由

替换的版本

版本 05/2017

Internet 上的当前版本手册

如需本手册的最新版本，可在 Siemens 工业在线支持的 Internet 页面上获取：

链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15340/man)

信息资源和其它文档

请参见“文档指南 (页 11)：部分。

缩写与名称

在本文档中，使用以下缩写代替产品全称：

- CP

  代替产品全称 CP 1543-1。

- STEP 7

  表示组态工具 STEP 7 Professional

许可证条款

说明

开源软件

该产品包含开源软件。在使用本产品之前，请仔细阅读开源软件的许可证条款。

在所提供的数据介质中，下列文档提供有许可证条款：

- OSS_CP15431_86.pdf

安全性信息

Siemens 为其产品及解决方案提供了工业信息安全功能，以支持工厂、系统、机器和网络的安全运行。

为了防止工厂、系统、机器和网络受到网络攻击，需要实施并持续维护先进且全面的工业信息安全保护机制。Siemens 的产品和解决方案仅构成此类概念的其中一个要素。

客户负责防止其工厂、系统、机器和网络受到未经授权的访问。只有在必要时并采取适当安全措施（例如，使用防火墙和网络分段）的情况下，才能将系统、机器和组件连接到企业网络或 Internet。

关于可采取的工业信息安全措施的更多信息，请访问
链接： (http://www.siemens.com/industrialsecurity)

Siemens 不断对产品和解决方案进行开发和完善以提高安全性。Siemens 强烈建议您及时更新产品并始终使用最新产品版本。如果使用的产品版本不再受支持，或者未能应用最新的更新程序，客户遭受网络攻击的风险会增加。

要及时了解有关产品更新的信息，请订阅 Siemens 工业信息安全 RSS 源，网址为
链接： (http://www.siemens.com/industrialsecurity)

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

SIMATIC NET 词汇表

对于本文档中所用的许多专业术语，SIMATIC NET 词汇表部分都给出了解释。

相关 SIMATIC NET 词汇表，请访问以下 Internet 网址：

链接： (https://support.industry.siemens.com/cs/ww/zh/view/50305045)

设备故障

如果故障无法消除，请将设备送至西门子代表处进行维修。不提供现场维修服务。

回收和处置

该产品的污染物含量低，可以回收利用并且符合 WEEE 指令 2012/19/EU“废弃电子电气设备”的要求。

请勿将产品丢弃在公共场所。为了使旧设备的回收和处置更符合环境要求，请联系一家经认证的电子废料处理公司或联系西门子的联系人。

请按照当地法规进行处理。

可在 Siemens 工业在线支持的 Internet 页面中找到产品的回收信息：
链接： (https://support.industry.siemens.com/cs/ww/zh/view/109479891)

目录

前言 **3**

1 文档指南 **11**

2 产品总览、功能 **13**

2.1 通信服务 14

2.2 其它功能 15

2.3 工业以太网安全 17

2.4 组态限制和性能数据 18
2.4.1 常规特性数据 18
2.4.2 S7 通信的特性 20
2.4.3 用于 FTP/FTPS 模式的特性数据 21
2.4.4 安全特性 21

2.5 使用要求 22
2.5.1 组态限制 22
2.5.2 项目工程 22
2.5.3 程序块 - 概述 23

2.6 LED 25

2.7 千兆位接口 27

3 安装、连接、调试、操作 **29**

3.1 使用设备的重要注意事项 29
3.1.1 有关在危险场所使用的注意事项 29
3.1.2 符合 ATEX/IECEx 要求的危险场所使用注意事项 30
3.1.3 符合 UL Hazloc 要求的危险场所使用注意事项 31
3.1.4 符合 FM 要求的危险场所使用通用注意事项 31

3.2 安装和调试 CP 1543-1 32

3.3 CPU 的工作模式：CP 的响应 33

4 组态、编程 **35**

4.1 安全建议 35

4.2 限制 CPU 中的通信服务 38

4.3 网络设置 39

4.4 IP 组态 40
4.4.1 关于 IP 组态的注意事项 40
4.4.2 在网络中检测重复 IP 地址后重新启动 40

4.4.3 IP 路由 41
4.4.4 CPU 的虚拟接口 41
4.4.5 已编程的连接：防火墙规则的限制 45
4.5 时钟同步 45
4.6 DNS 组态 46
4.7 FTP 通信 46
4.7.1 FTP 服务器 47
4.7.1.1 组态 FTP 服务器功能 47
4.7.2 FTP 客户端 50
4.7.2.1 程序块 FTP_CMD（FTP 客户端功能） 50
4.7.2.2 输入参数 - FTP_CMD 53
4.7.2.3 FTP_CMD 的作业块 55
4.7.2.4 输出参数和状态信息 FTP_CMD 62
4.7.2.5 用于 FTP 客户端操作的数据块（文件 DB）的结构 66
4.8 安全性 69
4.8.1 安全用户 69
4.8.2 VPN 70
4.8.2.1 在 S7-1500 站之间建立 VPN 隧道通信 71
4.8.2.2 在 CP 和 SCALANCE M 之间建立 VPN 隧道通信 73
4.8.2.3 与 SOFTNET Security Client 进行 VPN 隧道通信 73
4.8.2.4 CP 作为 VPN 连接的被动用户 74
4.8.3 防火墙 75
4.8.3.1 检查到达帧和离去帧时的防火墙顺序 75
4.8.3.2 源 IP 地址的表示法（高级防火墙模式） 75
4.8.3.3 HTTP 和 HTTPS 不可使用 IPv6 75
4.8.3.4 连接的 VPN 隧道防火墙设置 75
4.8.4 在线功能 76
4.8.4.1 防火墙激活情况下的在线安全诊断和下载到站设置 76
4.8.4.2 通过端口 8448 执行在线安全诊断 77
4.8.5 日志设置 - 过滤系统事件 77
4.9 用于 OUC 的程序块 77
5 诊断和保养 81
5.1 诊断方法 81
5.2 在线连接 82
5.3 使用 SNMP 进行诊断 83
5.4 更新固件 86
5.5 在没有编程设备的情况下更换模块 89
6 技术规范 91
6.1 CP 技术规范 91

6.2 以太网接口的引脚分配 92
6.3 允许的电缆长度 - 以太网 92
6.4 允许的电缆长度 - 千兆以太网 93
7 认证 95
索引 101

文档指南

1

S7-1500 产品文档

SIMATIC 产品文档采用模块化结构，并涵盖了有关自动化系统的各类主题。

S7-1500 系统的完整文档由系统手册、功能手册、设备手册和操作说明组成。

STEP 7 信息系统（在线帮助）还可以在您组态和编程自动化系统时提供支持。

下表列出了其它文档，这些文档是本 CP 手册的补充文档，可以从 Internet 获取。

表格 1- 1　S7-1500 产品文档概述

主题	文档	重要内容
系统描述	系统手册：S7-1500 自动化系统 (https://support.industry.siemens.com/cs/ww/zh/view/59191792)	• 应用规划 • 安装 • 连接 • 调试
系统诊断	功能手册：系统诊断 (https://support.industry.siemens.com/cs/ww/zh/view/59192926)	• 概述 • 硬件/软件诊断评估
通信	功能手册：通信 (https://support.industry.siemens.com/cs/ww/zh/view/59192925)	• 概述
	功能手册：Web 服务器 (https://support.industry.siemens.com/cs/ww/zh/view/59193560)	• 功能 • 运行

主题	文档	重要内容
	SIMATIC NET - 工业以太网 / PROFINET - 系统手册 • 工业以太网 链接： (https://support.industry.siemens.com/cs/ww/de/view/27069465) • 无源网络组件 链接： (https://support.industry.siemens.com/cs/ww/zh/view/84922825)	• 以太网网络 • 网络组态 • 网络组件
控制系统的无干扰安装	功能手册：控制系统的无干扰安装 (https://support.industry.siemens.com/cs/ww/zh/view/59193566)	• 基本信息 • 电磁兼容性 • 避雷 • 外壳选择
周期和响应时间	功能手册：周期和响应时间 (https://support.industry.siemens.com/cs/ww/zh/view/59193558)	• 基本信息 • 计算

手册集（部件编号 A5E00069051）中的 CP 文档

“SIMATIC NET 手册集”DVD 中包含创建时当前所有 SIMATIC NET 产品的设备手册和描述。此 DVD 会定期更新。

SIMATIC NET S7 CP 的版本历史/最新下载

“SIMATIC NET S7 CP（工业以太网）的版本历史/最新下载”文档提供到目前为止 SIMATIC S7（工业以太网）可用的所有 CP 的信息。

可在 Internet 上找到该文档的最新版本：
链接： (https://support.industry.siemens.com/cs/ww/zh/view/109474421)

产品总览、功能

2

应用

CP 适合在 S7-1500 自动化系统中运行。它允许将 S7-1500 连接到工业以太网。

利用不同安全措施（如防火墙和数据加密协议）的组合，CP 可保护 S7-1500 甚至整个自动化单元免受未经授权的访问。它还可保护 S7 站和通信伙伴之间的通信不受刺探和操纵。

2.1 通信服务

CP 支持以下通信服务：

- **Open User Communication (OUC)**

  通过使用已编程或已组态的通信连接的 CP，Open User Communication 支持以下通信服务：

  – ISO 传输（符合 ISO/IEC 8073）

  – TCP (IPv4/IPv6)（符合 RFC 793 和 8200）

    利用通过 TCPv4/v6 连接实现的接口，CP 支持几乎每个终端系统都提供的 TCP/IP 套接字接口。

  – ISO-on-TCP（符合 RFC 1006）

  – UDP（符合 RFC 768）

  – 基于 UDP 连接组播

    组态连接时可通过选择合适的 IP 地址来实现组播模式。

  – 通过 SMTP（端口 25）或 SMTPS（端口 587）发送电子邮件，在电子邮件服务器上进行身份验证。

- **S7 通信**

  – PG 通信

  – 操作员监控功能（HMI 通信）

  – 通过 S7 连接进行的数据交换

- **FTP/FTPS**

  FTP 功能 (File Transfer Protocol)，用于管理文件以及访问 CPU 中的数据块

  – FTP 服务器

    可通过组态激活

  – FTP 客户端

    可通过程序块进行组态。

- **FETCH/WRITE**
  - 通过 ISO 传输、ISO-on-TCP 和 TCP 连接实现的 FETCH/WRITE 服务（作为服务器，对应于 S5 协议）

    带有 CP 的 S7-1500 始终为服务器（建立被动连接）。

    获取或写访问（建立主动连接的客户端功能）始终由 SIMATIC S5 或第三方设备/PC 执行。

2.2 其它功能

基于工业以太网使用 NTP 模式实现时钟同步（NTP：网络时间协议）

CP 定期向 NTP 服务器发送时钟查询并与当地时钟同步。

时间也会自动转发到 S7 站中的 CPU 模块，从而允许同步整个 S7 站中的时间。

安全功能：CP 支持使用 NTP (secure) 协议进行安全时钟同步和时钟传送。

可通过出厂设置 MAC 地址进行寻址

要将 IP 地址分配给新的 CP（由工厂直接提供），可使用正在使用的接口上的预设 MAC 地址进行寻址。在 STEP 7 中进行在线地址分配。

SNMP 代理

CP 支持通过 SNMP（简单网络管理协议）版本 V1 进行数据查询。它会根据 MIB II 标准和自动化系统 MIB 提供特定 MIB 对象的内容。

如果已启用安全，则 CP 支持通过 SNMPv3 传送网络分析信息以免遭窃听。

IP 组态 - IPv4 和 IPv6

CP 的 IP 组态的基本特性：

- CP 支持使用符合 IPv4 和 IPv6 的 IP 地址。
- 您可以组态为 CP 分配 IP 地址的方法和方式、子网掩码以及网关地址。
- IP 组态和连接组态 (IPv4) 也可以通过用户程序（有关程序块，请参见程序块 - 概述 (页 23)部分）分配到 CP。

  注意：不适用于 S7 连接。

IP 路由

CP 支持静态 IP 路由 (IPv4) 到其它 CM 1542-1 V2.0 / CP 1543-1 V2.0。

有关详细信息，请参见“IP 路由 (页 41)”部分。

IPv6 地址 - 在 CP 上的用途

符合 IPv6 的 IP 地址可用于以下通信服务：

- FETCH/WRITE 访问（CP 为服务器）
- FTP 服务器模式
- 通过程序块进行寻址的 FTP 客户端模式
- 通过程序块进行寻址的电子邮件传输
- 通过 OUC 块和以下 SDT 实现的 TCP： TCON_QDN, TCON_QDN_SEC
- SNMP

使用 IPv6 地址时，请务必对 DNS 服务器进行相应组态。

访问 CPU 的 Web 服务器

通过 CP 的 LAN 接口，可以访问 CPU 的 Web 服务器。借助于 CPU 的 Web 服务器，可以读出站中的模块数据。

注意 Web 服务器的特殊说明；请参见“文档指南 (页 11)”部分

说明

使用 HTTPS 协议进行 Web 服务器访问

SIMATIC S7-1500 站的 Web 服务器位于 CPU 中。因此，在使用 CP 1543-1 的 IP 地址对站的 Web 服务器进行安全访问 (HTTPS) 时，将显示 CPU 的 SSL 证书。

用于 FETCH/WRITE 的 S5/S7 寻址模式

FETCH/WRITE 访问的寻址模式可以组态为 S7 或 S5 寻址模式。寻址模式指定了在数据访问期间标识起始地址位置的方式（S7 寻址模式仅适用于数据块/DB）。

请阅读 STEP 7 在线帮助中的附加信息。

2.3 工业以太网安全

全面保护 - 工业以太网安全的任务

利用工业以太网安全，单个设备、自动化单元或以太网网段均可受到保护。通过以下各种安全措施，可对 CP 与外部网络之间的数据传输进行保护：

- 数据间谍（FTPS、HTTPS）
- 数据操纵
- 未授权访问

通过由 CPU 或者附加 CP 实现的附加以太网/PROFINET 接口，可做到运行安全的底层网络。

适用于 S7-1500 站的 CP 的安全功能

使用 CP 后，S7-1500 站便可通过外部网络接口实现以下安全功能：

- 防火墙
  - 具有状态数据包检查功能的 IP 防火墙（第 3 层和第 4 层）
  - 防火墙也适用于符合 IEEE 802.3 的非 IP 帧 (Layer 2)
  - 传输速度限制
  - 全局和用户专用防火墙规则集

  防火墙保护功能可应用于单个设备、多个设备或整个网段的运行。
- 记录

  为允许监视，可将事件存储在日志文件中，日志文件可通过 STEP 7 读出，也可以自动发送到 Syslog 服务器。
- FTPS （显式模式）

  用于加密传送文件。
- NTP (secure)

  用于安全的时钟同步

- SMTPS

  通过端口 587 安全传送电子邮件

- SNMPv3

  用于安全传送网络分析信息，使其免受窃听

请参见“安全建议 (页 35)”部分中的信息。

2.4 组态限制和性能数据

2.4.1 常规特性数据

特性	说明/值
工业以太网上可自由使用的连接总数	118 此值适用于以下类型的连接总数： • S7 连接 • 开放式通信服务的连接 • FTP（FTP 客户端）

说明

CPU 的连接资源

根据 CPU 型号，有不同数量的连接资源可用。连接资源的数量是可组态连接数量的决定性因素。这意味着实际可实现的值可能小于在介绍 CP 的部分中指定的值。

Open User Communication (OUC) 通过 TCP、ISO-on-TCP、ISO 传输协议和 UDP 连接提供通信访问。

以下特性非常重要 (OUC + FETCH/WRITE)：

特性	说明/值
连接数	已组态和已编程的连接数（ISO 传输 + ISO-on-TCP + TCP + UDP + FETCH/WRITE + 电子邮件）： • 总数最多 118 个 各项的最大值： – TCP 连接： 0...118 – ISO-on-TCP 连接： 0...118 – ISO 传输连接： 0...118 – UDP 连接总数（已指定和空闲）： 0...118 – 电子邮件连接： 0...1 – FETCH/WRITE 的连接： 0...16
程序块的最大数据长度	数据块允许传送以下长度的用户数据： • ISO-on-TCP、TCP 和 ISO 传输：1 到 64 kB • UDP：1 字节至 2 KB • 电子邮件 – 作业标题 + 用户数据：1 到 256 字节 – 电子邮件附件：最大 64 kB
LAN 接口 - 每个协议数据单元由 CP 生成的最大数据字段长度 (TPDU = transport protocol data unit)	• 发送 ISO 传输、ISOonTCP 和 TCP：1452 字节/TPDU • 接收 – ISO 传输：512 字节/TPDU – ISO-on-TCP：1452 字节/TPDU – TCP：1452 字节/TPDU

说明

CPU 的连接资源

根据 CPU 型号，有不同数量的连接资源可用。连接资源的数量是可组态连接数量的决定性因素。这意味着实际可实现的值可能小于在介绍 CP 的部分中指定的值。

有关连接资源主题的详细信息，请参见“通信”功能手册中的“文档指南 (页 11)”部分。

UDP 的限制

- UDP 广播/组播的限制

  为避免由于广播/组播帧流量较高而导致 CP 过载，将限制在 CP 上接收 UDP 广播/组播。

- UDP 帧缓冲

  帧缓冲的长度：至少 7360 个字节

  缓冲区溢出后，新到达的帧如果不是由用户程序获取，则将被丢弃。

2.4.2 S7 通信的特性

S7 通信通过 ISO 传输或 ISO-on-TCP 协议提供数据传输。

特性	说明/值
工业以太网上可自由使用的 S7 连接总数	最多 118
LAN 接口 - 每个协议数据单元由 CP 生成的数据字段长度(PDU = protocol data unit)	• 发送：480 字节/PDU • 接收：480 字节/PDU
可保留的 OP 连接数 *	最多 4 个
可保留的 PG 连接数 *	最多 4 个
Web 的 HTTP 连接数	最多 4 个

* CPU 保留连接资源。对于已编程的连接，也要考虑指定的值。

说明

S7-1500 站的最大值

根据正在使用的 CPU，S7-1500 站存在限值。请注意相关文档中的信息。

2.4.3 用于 FTP/FTPS 模式的特性数据

FTP 的 TCP 连接

通过 TCP 连接从 CP 传输 FTP 操作。下列特性适用：

- FTP 客户端模式

  最多可以使用 32 个 FTP 会话。

  每个已激活的 FTP 会话最多占用 2 个 TCP 连接（1 个控制连接和 1 个数据连接）。

- FTP 服务器模式

  最多可同时运行 16 个 FTP 会话。

  每个已激活的 FTP 会话最多占用 2 个 TCP 连接（1 个控制连接和 1 个数据连接）。

FTP 客户端模式的程序块 FTP_CMD

要进行通信，请使用程序块 FTP_CMD。

在 FTP 中的块执行时间取决于伙伴的响应时间和用户数据长度。因此不存在普遍有效的声明。

2.4.4 安全特性

IPsec 隧道 (VPN)

利用 VPN 隧道通信，可与一个或多个安全模块建立安全的 IPsec 隧道通信。

组态限制	值
IPsec 隧道数	最多 16 个

防火墙规则（高级防火墙模式）

高级防火墙模式中防火墙规则的最大数目被限制为 256 个。

防火墙规则将按如下方式进行划分：

- 最多为 226 个具有单独地址的规则
- 最多 30 个具有地址范围或网络地址的规则
  （如 140.90.120.1 - 140.90.120.20 或 140.90.120.0/16）
- 最多 128 个具有传输速度限制的规则（“带宽限制”）

2.5 使用要求

2.5.1 组态限制

使用此处描述的 CP 类型时，以下限制适用：

- 可以在机架中运行的 CP 数量取决于正在使用的 CPU 型号。

  通过运行多个 CP，可以针对整个站提高下文列出的组态限制。但是，CPU 已对整个组态设置了限制。通过在系统限制的框架内使用多个 CP，可增加 CP 提供的组态的大小。

  请注意文档中有关 CPU 的信息；请参见文档指南 (页 11)部分

说明

通过 CPU 提供的电源充足或需要更多电源模块

在 S7-1500 站中可运行一定数量的模块，无需增加电源。对于特定 CPU 型号，请确保为背板总线持续提供指定的馈电。根据 S7-1500 站的组态，您可能需要提供更多电源模块。

2.5.2 项目工程

组态和下载组态数据

将组态数据下载到 CPU 时，会向 CP 提供相关组态。 可通过存储卡或 S7-1500 站的任意以太网/PROFINET 接口将组态数据下载到 CPU；

需要以下版本的 STEP 7：

STEP 7 版本	CP 的功能
STEP 7 Professional V12 SP1 或更高版本	可以对 CP 1543-1 (6GK7 543-1AX00-0XE0) 的完整功能进行组态。

2.5.3 程序块 - 概述

程序块 - 概述

以下程序块（指令）可用于 CP。

表格 2- 1 Open User Communication 的块

协议	程序块（指令）	系统数据类型
TCP	• TSEND_C/TRCV_C 或 • TCON/TDISCON + TSEND/TRCV	• TCON_IP_v4 • TCON_QDN • TCON_QDN_SEC • TCON_Configured
ISO-on-TCP		• TCON_IP_RFC
ISO		• TCON_ISOnative
UDP	• TCON/TDISCON + TUSEND/TURCV	• TCON_IP_v4
电子邮件	• TMAIL_C	• TMAIL_V4 • TMAIL_QDN • TMAIL_QDN_SEC • TMAIL_V6 • TMAIL_V6_SEC

表格 2- 2　CP 的通信服务块

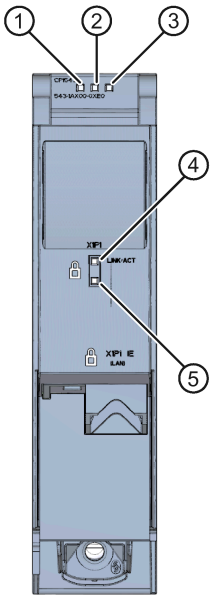
协议	程序块（指令）	系统数据类型
FTP	• FTP_CMD	• FTP_CONNECT_IPV4 • FTP_CONNECT_IPV6 • FTP_CONNECT_NAME • FTP_FILENAME • FTP_FILENAME_PART

表格 2- 3　以太网接口或 NTP/DNS 服务器的组态块

功能	程序块（指令）	系统数据类型
以太网接口的组态	• T_CONFIG	• IF_CONF_V4 • IF_CONF_V6 • IF_CONF_NTP • IF_CONF_DNS • IF_CONF_MAC

2.6 LED

LED



① RUN LED
② ERROR LED
③ MAINT LED
④ LINK/ACT LED
⑤ 预留 LED

图 2-1 CP 1543-1 的 LED 指示灯（不带前盖）

CP 的 LED 指示灯的含义

CP 使用以下 3 个 LED 来显示当前工作状态和诊断状态：

- RUN （单色 LED：绿色）
- ERROR （单色 LED：红色）
- MAINT （单色 LED：黄色）

下表列出了 RUN、ERROR 和 MAINT LED 各种颜色组合的含义。

表格 2- 4　LED“RUN”、“ERROR”、“MAINT”的含义

RUN	ERROR	MAINT	含义
LED 熄灭	LED 熄灭	LED 熄灭	CP 上无电源电压或电源电压过低。
LED 呈绿色亮起	LED 呈红色亮起	LED 呈黄色亮起	启动期间的 LED 测试
LED 呈绿色亮起	LED 呈红色亮起	LED 熄灭	启动（正在启动 CP）
LED 呈绿色亮起	LED 熄灭	LED 熄灭	CP 处于 RUN 模式。 无中断
LED 呈绿色亮起	LED 呈红色闪烁	LED 熄灭	发生了诊断事件。
LED 呈绿色亮起	LED 熄灭	LED 呈黄色亮起	维护，需要维护。
LED 呈绿色亮起	LED 熄灭	LED 呈黄色闪烁	需要维护。 下载用户程序
LED 呈绿色闪烁	LED 熄灭	LED 熄灭	不存在 CP 组态 正在加载固件
LED 呈绿色闪烁	LED 呈红色闪烁	LED 呈黄色闪烁	模块故障 （LED 闪烁同步）

以太网接口 LED 指示灯的含义： X1 P1

LED LINK/ACT（绿/黄两种颜色）分配给以太网接口。下表列出了 LED 模式。

表格 2- 5 “LINK/ACT”LED 的含义

LINK/ACT		含义
□ 绿灯熄灭	□ 黄灯熄灭	不存在以太网连接 CP 的以太网接口和通信伙伴之间不存在以太网连接。 当前没有通过以太网接口接收/发送数据。
☼ 绿色闪烁	□ 黄灯熄灭	正在执行“节点闪烁测试”。
■ 绿灯点亮	□ 黄灯熄灭	存在以太网连接。 CP 的以太网接口和通信伙伴之间存在以太网连接。
■ 绿灯点亮	■ 黄灯闪烁	当前正在通过以太网上通信伙伴的以太网设备的以太网接口接收/发送数据。

2.7 千兆位接口

符合千兆位规范并支持安全访问的以太网接口

CP 具有一个符合千兆位标准 IEEE 802.3 的以太网接口。该以太网接口支持自动跨接、自动协商和自动检测功能。

以太网接口允许通过防火墙安全连接到外部网络。CP 提供以下保护功能：

- 保护 CP 运行时所在的 S7-1500 站；
- 保护连接到 S7-1500 站其它接口的底层公司网络。

有关 D 型 RJ-45 插孔的引脚分配的信息，请参见安装和调试 CP 1543-1 (页 32)部分。

安装、连接、调试、操作 3

3.1 使用设备的重要注意事项

有关设备使用的安全须知

在设置和操作设备时，以及在所有相关工作（例如，安装、连接或更换设备）期间，注意以下安全须知。

注意
LAN 连接 LAN 或带有属于 LAN 的连接的 LAN 段应当处于单独的低压供电系统和单独的建筑中。 确保 LAN 处于符合 IEEE 802.3 标准的 A 类环境或符合 IEC TR 62101 标准的 0 类环境中。 从不建立到 TNV 网络（Telephone Network，电话网络）或 WAN（Wide Area Network，广域网）的直接电气连接。

3.1.1 有关在危险场所使用的注意事项

⚠警告
设备只能在污染等级 1 或 2 的环境中运行（请参见 IEC 60664-1）。

⚠警告
爆炸危险 请勿在易燃环境下从设备上连接或断开电缆。

⚠警告
爆炸危险 更换组件可能损害在 1 级 2 分区或 2 区的适用性。

⚠警告

在相当于 I 级 2 分区或 I 级 2 区的危险环境下使用本设备时，必须将其安装在机柜或适当的机壳内。

⚠警告

DIN 导轨

在应用程序的 ATEX 和 IECEx 区域，只可用 Siemens DIN 导轨 6ES5 710-8MA11 来安装模块。

3.1.2 符合 ATEX/IECEx 要求的危险场所使用注意事项

⚠警告

机柜/机壳要求

为符合 EU 指令 94/9 (ATEX95)，机壳或机柜必须至少满足 EN 60529 规定的 IP54 要求。

⚠警告

电缆

如果电缆或导线入口的温度超过 70 °C，或者导线分支点超过 80 °C，必须采取专门的预防措施。如果设备要在环境温度超过 50 °C 的情况下工作，则只能使用允许最高工作温度至少为 80 °C 的电缆。

⚠警告

应采取措施以防止出现高出额定电压 40% 以上的瞬变电压浪涌。只有在使用 SELV（safety extra-low voltage，安全超低电压）操作设备时才会出现这种情况。

3.1.3 符合 UL Hazloc 要求的危险场所使用注意事项

⚠警告

爆炸危险

只有当断开电源或设备所处环境不存在可燃气体时，才能带电连接电缆或断开电缆连接。

此设备仅适合在 I 类，2 分区，A、B、C 和 D 组或无危险位置使用。

此设备仅适合在 I 类，2 区，IIC 组或无危险位置使用。

3.1.4 符合 FM 要求的危险场所使用通用注意事项

⚠警告

爆炸危险

只有当断开电源或设备所处环境不存在可燃气体时，才能带电连接电缆或断开电缆连接。

此设备仅适合在 I 类，2 分区，A、B、C 和 D 组或无危险位置使用。

此设备仅适合在 I 类，2 区，IIC 组或无危险位置使用。

⚠警告

爆炸危险

The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 ºC higher than maximum ambient temperature.

3.2 安装和调试 CP 1543-1

安装和调试

⚠警告

阅读系统手册“S7-1500 自动化系统”

在安装、连接和调试之前，请阅读《S7-1500 自动化系统》系统手册中的相关部分（有关文档的参考，请参见文档指南 (页 11)部分）。

在安装/拆卸设备时确保电源已关闭。

组态

仅当 STEP 7 项目数据完整时，才能完全调试 CP。

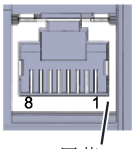
安装和调试步骤

步骤	执行	注意事项和说明
1	安装和连接时，请按照《S7-1500 自动化系统》系统手册中介绍的 I/O 模块安装步骤进行操作。	
2	通过 RJ45 插孔将 CP 连接到工业以太网。	CP 的底部
3	接通电源。	
4	关闭模块的前盖，保持其在运行过程中处于关闭状态。	
5	调试的其余步骤涉及到下载 STEP 7 项目数据。	在下载到站时传送 CP 的 STEP 7 项目数据。要加载站，请将项目数据所在的工程师站连接到 CPU 的以太网接口。 有关加载的详细信息，请参见 STEP 7 在线帮助的以下部分： • “编译和加载项目数据” • “使用在线和诊断功能”

以太网接口

下表列出了以太网接口（RJ-45 插孔）的引脚分配。分配对应于以太网标准 IEEE 802.3。

表格 3- 1　以太网接口的引脚分配

视图	引脚	10/100 Mbps 运行		10/100 Mbps 或者千兆运行	
		信号名称	引脚分配	信号名称	引脚分配
	1	TD	Transmit Data +	D1+	D1 双向 +
	2	TD_N	Transmit Data -	D1-	D1 双向 -
	3	RD	Receive Data +	D2+	D2 双向 +
	4	GND	Ground	D3+	D3 双向 +
	5	GND	Ground	D3-	D3 双向 -
	6	RD_N	Receive Data -	D2-	D2 双向 -
	7	GND	Ground	D4+	D4 双向 +
	8	GND	Ground	D4-	D4 双向 -

有关“连接”和“附件（RJ-45 插头）”主题的更多信息，请参见系统手册：
链接： (https://support.industry.siemens.com/cs/ww/zh/view/59191792)

3.3 CPU 的工作模式：CP 的响应

切换 CPU 的工作模式： RUN → STOP

可以使用 STEP 7 切换 CPU 的工作模式（RUN 和 STOP 之间）。

说明

CP 的 RUN/STOP LED

无论 CPU 是否处于 STOP 模式，CP 的绿色 RUN/STOP LED 都持续保持绿色点亮状态。

CPU 的状态为 STOP 时，CP 保持在 RUN 状态。以下行为适用于 CP：

- 适用于已建立的连接（ISO 传输、ISO-on-TCP、TCP、UDP）：
  - 保留已编程的连接。
  - 终止已组态的连接。
- 下列功能仍保持启用状态：
  - CP 的组态和诊断

    仍然存在用于组态、诊断和 PG 通道路由的系统连接。
  - Web 诊断
  - S7 路由功能
  - 时钟同步

组态、编程 4

4.1 安全建议

请遵循以下安全建议，以避免系统受到未授权访问。

常规

- 应定期进行检查以确保设备符合以下建议内容和其它适用的安全准则。
- 从安全角度对工厂进行整体评估。将单元保护机制与适当的产品配合使用。
- 请勿将设备直接连接到 Internet。请在受保护的网络区域内运行该设备。
- 定期在 Siemens Internet 页面上检查新功能。
  - 有关工业安全的信息，请参见以下链接：
    链接： (http://www.siemens.com/industrialsecurity)
  - 有关工业通信安全的信息，请参见以下链接：
    链接： (http://w3.siemens.com/mcms/industrial-communication/zh/ie/industrial-ethernet-security/Seiten/industrial-security.aspx)
  - 有关网络安全主题的一系列文档，请参见此处：
    链接： (https://support.industry.siemens.com/cs/cn/zh/view/92651441)
- 保持固件为最新。定期检查固件的安全更新，并使用这些更新。

  有关产品新闻和新固件版本的信息，请访问以下地址：
  链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15340/dl)

物理访问

应将该设备限制为仅允许合格人员进行物理访问。

网络连接

请勿将 PC 直接连接到 Internet。如需将 CP 连接到 Internet，则应启用安全功能或对 CP 进行适当的保护，例如带防火墙的 SCALANCE S。

产品的安全功能

在组态产品过程中，可使用安全设置选项。其中包括：

- 保护等级

  在“保护和安全”(Protection and Security) 下组态访问 CPU。

- 通信的安全功能
  - 启用 CP 的安全功能并建立防火墙。

    如果您连接到了公共网络，则应使用防火墙。请考虑您要允许哪些服务通过公共网络对站进行访问。通过使用防火墙的“带宽限制”功能，可以限制泛洪和 DoS 攻击。

    FETCH/WRITE 功能可用来访问 PLC 的各种数据。但若使用了公共网络时，就不应该使用 FETCH/WRITE 功能。
  - 使用变种安全协议 HTTPS, FTPS, NTP (secure) 和 SNMPv3。
  - 使用安全 OUC 通信 (Secure OUC) 的程序块。
  - 禁用对 CPU（CPU 组态）Web 服务器和对 CP 的 Web 服务器的访问。
- 保护访问程序块的密码

  防止存储于数据库的程序块的密码被查看。有关 STEP 7 信息系统中程序的信息，请参见关键词“了解保护方法”下的内容。

- 记录功能

  启用安全组态功能，并定期检查对未经授权的访问的记录事件。

密码

- 定义设备使用和密码分配规则。
- 定期更新密码以提高安全性。
- 仅使用密码强度高的密码。避免使用密码强度弱的密码，如“password1”、“123456789”或类似的密码。
- 确保所有密码都受到保护，未授权人员无法访问。

  相关信息，另请参见上述部分。

- 请勿将同一密码用于不同用户和系统。

协议

安全和非安全协议

- 仅激活使用系统所需的协议。
- 在物理保护措施未阻止设备访问时使用安全协议。
- 例如，在公共网络（如 Internet）接口上禁用 DHCP，以防止 IP 欺骗。

表格：各列标题和条目的含义：

下表总体地介绍了该设备上打开的端口。

- **协议/功能**

  设备支持的协议。

- **端口号（协议）**

  分配给协议的端口号。

- **端口的默认状态**

  – 打开

  组态开始时，该端口打开。

  – 关闭

  组态开始时，该端口关闭。

- **端口状态**

  – 打开

  端口始终处于打开状态且无法关闭。

  – 组态后打开

  端口在组态后打开。

  – 打开（登录时，组态后）

  默认情况下，端口打开。组态端口后，通信伙伴需要登录。

  – 通过块调用打开

  只有调用合适的程序块时，才会打开该端口。

- **身份验证**

  在访问期间，指定协议是否已对通信伙伴进行验证。

协议/ 功能	端口号（协议）	端口的默认状态	端口状态	身份验证
DCP	93 (UDP)	打开	打开	否
S7 和在线连接	102 (TCP)	打开	打开 *	否
在线安全诊断	8448 (TCP)	关闭	组态后打开	否
HTTP	80 (TCP)	关闭	组态后打开	否
HTTPS	443 (TCP)	关闭	组态后打开	是
FTP	20 (TCP) 21 (TCP)	关闭	组态后打开	否
FTPS	989 (TCP) 990 (TCP)	关闭	组态后打开	是
SNMP	161 (UDP)	打开	组态后打开	是（带 SNMPv3）

* 有关避免在诊断期间打开端口 102 的信息，请参见“通过端口 8448 执行在线安全诊断 (页 77)”部分。

通信伙伴和路由器的端口

确保在相应的防火墙中启用了通信伙伴和中介路由器所需的客户端端口。

其中包括：

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP) - 在块调用时在 CP 中打开（仅限传出）
- SMTPS / 587 (TCP) - 在块调用时在 CP 中打开（仅限传出）

4.2 限制 CPU 中的通信服务

无连接的通信服务

CPU 可用作一系列通信服务的服务器，而且无需组态连接。其它通信伙伴可以访问 CPU 数据。这意味着本地 CPU 不再能够控制与客户端的通信。

这些通信服务的可靠性由 CPU 的“保护和安全”(Protection & Security) 参数组中的“连接机制”(Connection mechanisms) 参数设置。

“允许来自远程伙伴的 PUT/GET 通信访问”

- 启用选项

  允许从客户端访问 CPU 数据。

- 禁用选项

  只有通信连接需要对本地 CPU 和通信伙伴进行组态或编程时，才能对 CPU 数据进行读写访问。

  本地 CPU 仅用作服务器（不对通信伙伴进行组态/编程）时，无法连接。

  CP 的以下通信服务要求 CPU 的固件版本 ≥ V2.

  如果禁用此选项，则无法执行以下操作：

  – 通过 CP 进行 PUT/GET 访问

  – 通过 CP 进行 FETCH/WRITE 访问

  如果禁用此选项，则可以执行以下操作：

  – 通过 CP 进行 FTP 访问

4.3 网络设置

自动设置

CPU 的以太网接口已永久设置为自动检测。

说明

正常情况下，基本设置便可确保正常通信。

自动跨接机制

利用集成的自动跨接机制，可以使用标准电缆连接 PC/PG。 无需使用跨接电缆。

说明

连接交换机

要连接不支持自动跨接机制的交换机，请使用跨接电缆。

4.4 IP 组态

4.4.1 关于 IP 组态的注意事项

如果使用 DHCP 分配 IP 地址，组态的 S7 和 OUC 连接将无法运行

说明

如果使用 DHCP 获取 IP 地址，组态的所有 S7 和 OUC 连接都会失效。 原因： 运行期间，已组态的 IP 地址被通过 DHCP 获取的地址代替。

4.4.2 在网络中检测重复 IP 地址后重新启动

为了减少排除网络故障所花费的时间，CP 可在启动期间检测网络中的重复地址。

CP 启动时的行为

如果在 CP 启动时检测到重复地址，CP 将切换到 RUN 模式并且无法通过以太网接口访问。 ERROR LED 闪烁。

4.4.3 IP 路由

通过背板总线进行 IP 路由

CP 支持静态 IP 路由 (IPv4) 到其它 CM/CP：

- CP 1545-1
- CM 1542-1 V2.0
- CP 1543-1 V2.0

例如，可以使用 IP 路由通过较低级别模块访问 Web 服务器。

使用 IP 路由时，数据吞吐量限制在 1 Mbps。选择模块数量和确定通过背板总线的预期数据流量时，请记住这一点。

组态

可通过以下参数在 STEP 7 中激活 IP 路由：
"以太网接口 > 以太网地址 > 通信模块间的 IP 路由"

请注意：
如果在某个站中使用多个 CP，并希望使用 IP 路由，则仅可为站中的一个 CP 组态一个路由器。

激活安全功能时，将创建附加 IP 防火墙规则，可以在全局安全设置的高级防火墙模式下修改这些规则。

4.4.4 CPU 的虚拟接口

CP 1543-1 支持 CPU 的虚拟接口。

要求

要使用 CPU 的虚拟接口，必须满足以下要求：

- S7-1500 CPU 固件版本 V2.8 或更高版本

  R/H CPU 不支持此功能。
- CP 1543-1 固件版本 V2.2 或更高版本

  CP 的安全功能已禁用。
- 可组态性：自 STEP 7 V16 起

CPU 的虚拟接口

自固件版本 V2.8 起，S7-1500 CPU 提供访问其基于 IP 的应用程序（如 OPC UA）的选项，不仅可通过其本地 PROFINET 接口访问，还可以通过同一站中的 CP 1543-1 的接口进行访问。

虚拟接口名为 W1。

虚拟接口的特性

虚拟接口不是具有传统接口常用属性的完全可诊断接口。由于通过背板总线实现的内部连接不代表 S7 子网，并且没有任何端口，因此虚拟接口不会在诊断视图中显示。因此，无法建立通过网络电缆实现的物理连接。

还可通过虚拟接口访问以下基于 IP 的服务：

- OPC UA（客户端和服务器）
- 编程的 OUC 连接
- S7 通信：ES/HMI 访问以及 S7 通信指令，如 PUT/GET

虚拟接口的 IP 地址显示在 STEP 7 中以及 CPU 显示中。

已激活的接口可用于通信伙伴组态中。

有关虚拟接口与物理接口相比的限制条件，请参见 STEP 7 信息系统。

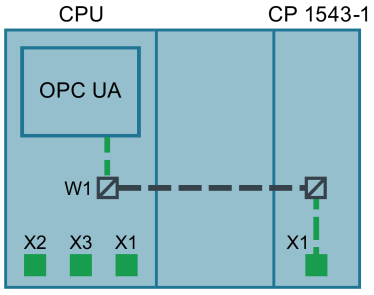


图 4-1　　虚拟接口的原理

虚拟接口 W1 的组态

虚拟接口在 STEP 7 中的参数组“高级组态 > 通过通信模块访问 PLC”(Advanced configuration > Access to PLC via communication module) 中组态。

在此，会将虚拟接口分配给站的 CP，可通过该虚拟接口对 CPU 进行外部访问。可以从下拉列表中选择站的已组态 CP。

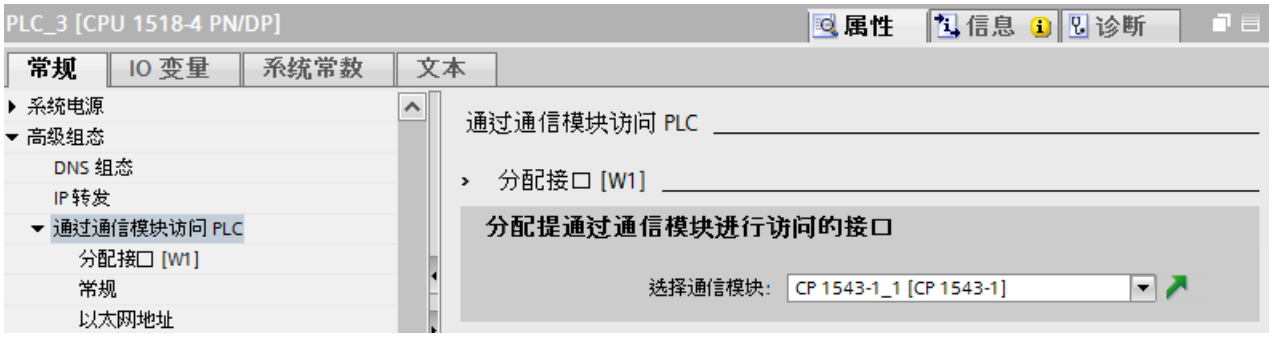


图 4-2　　在 CPU 属性中选择 CP

选择 CP 后，组态虚拟接口的 IP 和 PROFINET 参数。

请遵守以下规则：

- 虚拟接口的 IP 地址与 CPU 的 PROFINET 接口的 IP 地址必须位于不相连的单独地址段中。
- 虚拟接口的 IP 地址必须位于以太网接口的子网中，以便 CP 服务与 CPU 可实现相互访问。

加载组态数据后，可通过 CP 和虚拟接口访问 CPU 服务（如 OPC UA 服务器）。

虚拟接口的 IP 地址显示在 CPU 的 OPC UA 服务器属性对话框中的服务器地址列表中。已创建连接和 S7 通信（例如 HMI 和 BSEND、BRCV）通过此接口运行。

虚拟接口 W1 的 IP 地址不会列于当前在设备显示中显示的本地接口 (Xn) 下，但会显示在“设置”(Settings) 部分中的“地址”(Addresses) 下。未插入任何 CP 或虚拟接口已禁用的情况下，也会显示虚拟接口。如果未组态 IP，则 IP 地址和子网掩码会显示为 0.0.0.0。

虚拟接口 W1 显示在“在线和诊断”(Online & Diagnostics) 下的诊断视图中。

虚拟接口的硬件 ID 显示在 CPU 属性的系统常量中。

说明

运行和重启时的地址更改

加载虚拟接口的 IP 参数后，即可通过 CPU 显示屏、通过 T_CONFIG 或在线更改这些参数。

但需要注意的是，最初加载的组态将在 CPU 重启后再次生效。

组态更改

更改已分配 CP 可能会影响虚拟接口的组态：

- 组态中的更改
  - 分配其它 CP

    该组态用于新 CP。
  - 取消选择已分配 CP

    取消激活虚拟接口 W1 且组态丢失。

    再次分配 CP 时，需要再次组态虚拟接口。
- 更改站组态
  - 移动 CP

    如果 CP 只是移动到设备的其它插槽，则组态保持有效。
  - 取出 CP

    如果将 CP 从站中取出，则组态会保留在 CPU 中。

    在 CPU 参数组下拉列表中，CP 显示为丢失，编译组态会提示错误。可以取消选择缺失的 CP 或将其分配给另一个 CP。

CP 的安全设置

内部 CP 的防火墙设置不会影响通过虚拟接口进行数据通信。即，通信模块的安全功能无法保护数据通过虚拟接口进行通信。

注意
连接到非安全网络 仅当 CP 的安全功能已禁用时，才能通过 CP 使用虚拟接口。 如果将 CP 连接到非安全网络，则务必要将额外的防火墙连接到 CP 与非安全网络之间的接口。为此，应使用安全模块，例如 SCALANCE S602 V3 或 S623。

4.4.5 已编程的连接：防火墙规则的限制

已编程连接和已组态安全功能的限制

原则上，可以使用程序块 TCON 并同时组态防火墙来设置程序控制的通信连接。

说明

伙伴 IP 地址不在防火墙规则内

在 STEP 7 中组态指定连接（主动端点）时，伙伴的 IP 地址不会自动输入到防火墙组态中。

4.5 时钟同步

一般规则

CP 支持以下时钟同步模式：

- NTP 模式（NTP：网络时间协议）

说明

时间设置建议

建议每隔大约 10 秒就与外部时钟同步一次。这会使内部时间和绝对时间的偏差尽可能小。

说明

NTP 同步时钟的特性

如果未选中“接受非同步 NTP 服务器的时间”(Accept time from non-synchronized NTP servers) 选项，则响应如下：

如果 CP 接收来自未与 16 层同步的 NTP 服务器的时钟帧，则时钟不会根据相应帧进行设置。在这种情况下，诊断中没有任何 NTP 服务器显示为“NTP 主站”(NTP master)；而只显示为“可访问”。

安全性

在扩展 NTP 组态中，可以创建和管理其它 NTP 服务器。

说明

确保有效时钟

如果使用安全功能，则有效的时钟极其重要。如果不能从站 (CPU) 获得时钟，建议您使用 NTP (secure) 方法。

组态

有关组态的详细信息，请参见“时钟同步”参数组的 STEP 7 在线帮助。

4.6 DNS 组态

DNS 服务器

在模块自身、通信伙伴或 FTP 服务器等应通过主机名称 (FQDN) 访问时可能需要 DNS 服务器。如果将设备地址指定为 FQDN，则需要组态 DNS 服务器。在这种情况下，通过组态的 DNS 服务器确定设备的 IP 地址。

最多可为 CP 组态 3 个 DNS 服务器。不会对组态的第 4 个 DNS 服务器进行评估。

4.7 FTP 通信

仅启用安全功能的 FTPS 访问

只有在 STEP 7 项目中创建了拥有适当权限的用户时，才能通过 FTPS 方式访问作为 FTP 服务器的 S7-1500 站。这意味着必须启用 CP 上的安全功能。这样，全局用户管理中的安全设置才可用。

4.7.1 FTP 服务器

4.7.1.1 组态 FTP 服务器功能

CP 组态

在下列参数组中组态 CP 的 FTP 服务器功能。

- 禁用安全功能：“FTP 服务器组态”(FTP server configuration)
- 启用安全功能:“安全 > FTP 服务器组态”(Security > FTP server configuration)

CPU 组态和编程要求

使用以下设置启用 FTP 访问：

- 在“保护和安全 > 连接机制”(Protection & Security > Connection mechanisms) 的 CPU 组态中：

  禁用“通过 PUT/GET 通信访问...”(Access via PUT/GET communication...) 选项。
- 作为文件 DB，创建“字节数组”类型的数据块。

仅适用于固件版本 ≤ V2.0 的 CP 1543-1：

- 针对所有用作文件 DB 的数据块，禁用“优化块访问”(Optimized block access) 属性。

S7-1500 CP 作为 FTP 服务器

借助此处所述的功能，可使用 FTP 命令以文件形式与 S7-1500 站交换数据。同时，还可以使用读取、写入和管理文件等常规 FTP 命令。

可以访问 S7-1500 的下列数据：

- **CP 的 RAM**

  目录名称：

  /ram

- **CPU 的数据块**

  目录名称：

  /cpu1 / DBx

  “DBx”是相关数据块的名称，例如 DB10。

- **CPU 的 SIMATIC 存储卡**

  自以下固件版本起支持该功能：

  – CPU： V2.0

  – CP 1543-1： V2.0

  – CP 1545-1： V1.0

  目录名称：

  /mmc_cpu1

  可以访问 SIMATIC 存储卡的下列文件夹：

  – /DATALOGS

    日志文件的目录

  – /RECIPES

    配方文件的目录

说明

对 CPU 的 SIMATIC 存储卡进行 FTP 访问：CPU 可切换到 STOP 模式

请注意，存储卡的容量有限。如果 SIMATIC 存储卡的存储空间因存储大量数据而被完全占满，则 CPU 会切换到 STOP 模式。

- 更换一个具有足够存储容量的存储卡。
- 避免经常使用 FTP 向 SIMATIC 存储卡写入大量数据。

通过 CPU 的 DB 进行读取/写入

要通过数据块使用 FTP 传送数据，请在 CPU 中创建需要的 DB。因为结构特殊，所以将其称为文件 DB。

在收到 FTP 命令时，充当 FTP 服务器的 CP 会查询分配表以找出 CPU 中用于文件传送的数据块与文件的映射关系。在 CP 的 STEP 7 组态中进行数据块分配（FTP 组态）。

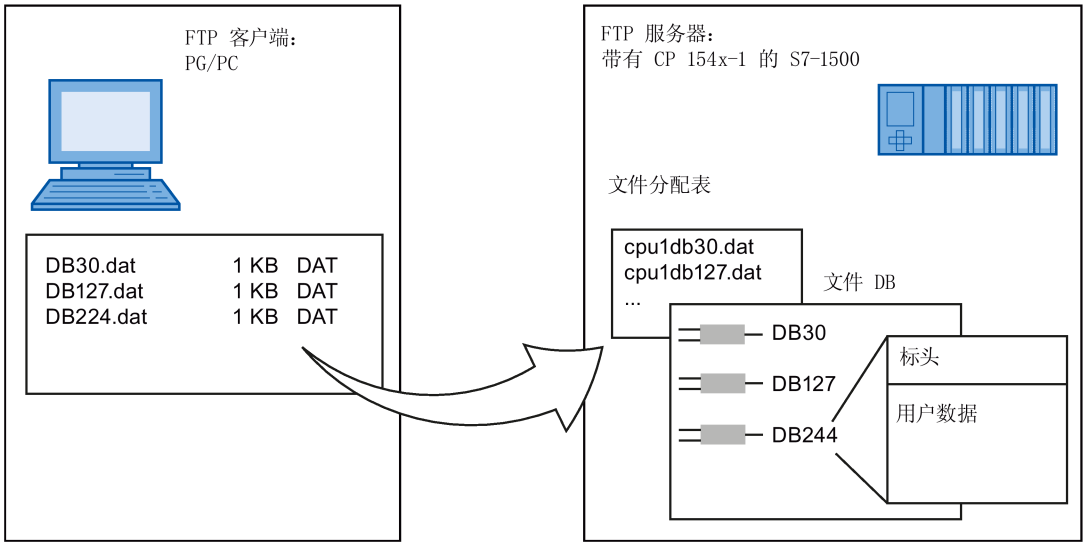


图 4-3 将配备 CP 154x-1 的 S7-CPU 作为 S7 CPU 数据的 FTP 服务器

STEP 7 中的 DB 分配

STEP 7 数据块分配表中的字段的含义和语法如下：

列标题	CPU	DB	文件名	注释
含义	CPU 分配 可从下拉列表中选择	数据块（文件 DB）的编号 可从下拉列表中选择	分配给文件 DB 的文件名 自动名称推荐；条目可以编辑。	简略的注释
示例	cpu1 [PLC_1]	20	cpu1_db20.dat	测量值设备 1

有关语法的注意事项

下列内容适用于文件数据块的文件名：

- 文件名以“cpuX”开始（对于 S7-1500，其中的 X = 1）。

  说明

  请遵循适当的表示法（“cpu”小写，行开头没有前导空格）。否则，文件将无法识别。

- 长度：最多 64 个字符（包括“cpuX”）

4.7.2 FTP 客户端

4.7.2.1 程序块 FTP_CMD（FTP 客户端功能）

FTP_CMD

通过 FTP_CMD 指令，可以建立 FTP 连接，并从 FTP 服务器传送文件或将文件传送到 FTP 服务器。

可以通过 FTP 或 FTPS（安全 SSL 连接）传送数据。

当 Main [OB1] 打开时，可在 STEP 7 中“指令”(Instructions) 任务卡的“通信 > 通信处理器 > SIMATIC NET CP”(Communication > Communications processor > SIMATIC NET CP) 下找到块。

说明

块版本

在工作站中，V2.x 版的 FTP_CMD 必须结合 CPU V2.x 和 CP V2.x 一起使用。

只要工作站采用 CPU V1.x 或 CP V1.x，就必须在旧版 V1.x（例如 V1.4）中使用 FTP_CMD。为此，需将“SIMATIC NET CP”库的版本更改为 V3.4。之后，便可以选择旧版的块。

下表列出了兼容性。

表格 4- 1　程序块 FTP_CMD 与 CPU 和 CP 版本的兼容性

FTP_CMD	CPU	CP 1543-1
V1.5	V1.x	任意
V1.5	任意	V1.x
V2.0	V2.x	V2.x

可以通过 FTP 或 FTPS（安全 SSL 连接）传送数据。

说明

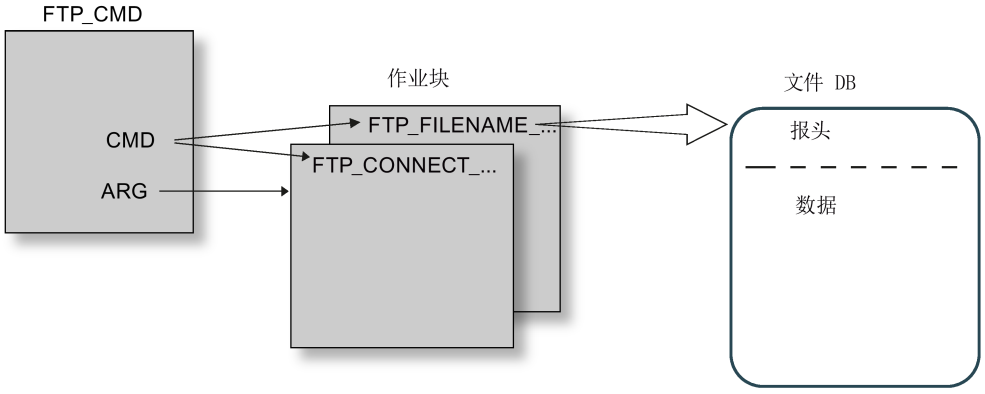
FTPS：比较证书

FTPS 需要对 FTP 服务器和 FTP 客户端之间的证书进行比较。如果在 FTP 客户端的 STEP 7 项目外组态 FTP 服务器，则需要导入 FTP 服务器的证书。将 FTP 服务器的证书作为受信任证书导入证书管理器。

工作原理

FTP_CMD 指令引用指定了 FTP 命令的作业块 (ARG)。根据 FTP 命令 (CMD) 的类型，此作业块使用不同的数据结构执行参数分配。这些不同的结构可以使用适当的数据类型 (UDT)。

下图显示了调用结构：



作业块 (UDTs)

以下数据结构用于作业块：

- 连接建立

  基于以下访问类型的连接建立可使用不同数据结构：

  – FTP_CONNECT_IPV4：基于 IPv4 通过 IP 地址建立连接

  – FTP_CONNECT_IPV6：基于 IPv6 通过 IP 地址建立连接

  – FTP_CONNECT_NAME：通过服务器名称 (DNS) 建立连接

- 数据传送

  有两种不同的数据结构可用于实现数据传送：

  – FTP_FILENAME：用于访问整个文件的数据结构

  – FTP_FILENAME_PART：用于读取数据区的数据结构

File_DB 中的数据传送

数据传送通过包含作业数据报头和用户数据区域的数据块实现。该数据块在作业缓冲区中加以指定。

有关示例文件 DB 的描述，请参见 STEP 7 信息系统。

CPU 组态要求

使用以下设置启用 FTP 访问：

- 针对所有用作文件 DB 的数据块，禁用“优化块访问”(Optimized block access) 属性。
- 仅当使用 CPU V1.x 和 CP V1.1.x 时：
  在“保护和安全”(Protection & Security) 下的 CPU 组态数据中，启用“通过 PUT/GET 通信访问...”(Access via PUT/GET communication...) 选项（必须释放 PUT/GET）。

4.7.2.2 输入参数 - FTP_CMD

输入参数的说明

将以下输入参数提供给 FTP_CMD 指令：

表格 4- 2 FTP_CMD 指令的形式参数 - 输入参数

参数	声明	数据类型	存储区	含义/说明
REQ	Input	BOOL	E, A, M, DB, L	在上升沿启动发送作业。
ID *	INPUT	INT	1, 2 ... 64	在 FTP 连接上处理 FTP 作业。该参数可识别所用的连接。
CMD *	INPUT	BYTE	请参见下表“命令”。	调用该指令时要执行的 FTP 命令。可在此表后找到 FTP 命令类型的值范围。 此处指定的 FTP 命令必须与作业块中指定的命令相同（ARG 参数）。 如果 CP 固件不支持命令，则输出一条带 STATUS = $8F6B_H$ 的出错消息。
ARG *	INPUT	VARIANT	请参见下表“命令”。	作业块 引用具有适合于 FTP 命令的执行参数的数据区。 根据不同的 FTP 命令，使用特定的数据类型 (UDT)。这些 UDT 如下所示。 此处指定的指针不允许使用 ANY 数据类型！

* 输入参数“ID”和“CMD”的值将覆盖输入参数“ARG”的值。

“CMD”参数中的 FTP 命令

下表显示了“CMD”参数命令的含义以及提供给作业块所用的 UDT。

表格 4- 3　命令类型

CMD（命令类型）	相关作业块/UDT	含义/处理
0 (NOOP)	*	调用的 FC 不执行任何动作。当提供这些参数时，按如下规定设置状态代码： DONE=1; ERROR=0; STATUS=0
1 (CONNECT)	FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME	建立 FTP 连接 通过该命令，FTP 客户端将与 FTP 服务器建立 FTP 连接(端口 21)。 在此处为所有其他 FTP 命令指定的连接 ID 下，该连接可用。然后与为该用户指定的 FTP 服务器交换数据。
2 (STORE)	FTP_FILENAME	该函数调用将一个数据块(文件 DB)从 FTP 客户端(S7-CPU)传送到 FTP 服务器。 注意：如果该文件(文件 DB)已经存在于 FTP 服务器上，则该文件将被覆盖。
3 (RETRIEVE)	FTP_FILENAME	该函数调用将文件从 FTP 服务器传送到 FTP 客户端(S7-CPU)。 注意：如果 FTP 客户端上的数据块(文件 DB)已经包含一个文件，则该文件被覆盖。
4 (DELETE)	FTP_FILENAME	通过该函数调用，删除 FTP 服务器上的文件。
5 (QUIT)	*	通过该函数调用，可关闭在“ID”中指定的 FTP 连接。

CMD（命令类型）	相关作业块/UDT	含义/处理
6 (APPEND)	FTP_FILENAME	与“STORE”类似，“APPEND”命令将文件保存在 FTP 服务器上。但“APPEND”命令不会覆盖 FTP 服务器上的文件。为现有文件添加新内容。 如果 FTP 服务器上不包含该文件(文件 DB)，则创建该文件。
7 (RETR_PART)	FTP_FILENAME_PART	使用“RETR_PART”命令(检索部分)，可以从 FTP 服务器请求文件的一部分。 如果涉及非常大的文件，则该命令允许仅限于读取当前要求的部分。 为此，需要获知文件的结构。 在 FB40 中，使用“OFFSET”和“LEN”两个参数输入所要求的文件部分。

* 对于命令类型 0 (NOOP) 和 5 (QUIT)，必须指定可自由选择的作业块 (UDT)。不进行评估。

4.7.2.3 FTP_CMD 的作业块

含义

为 FTP_CMD 指令提供使用 ARG 参数的作业块。结构取决于 FTP 命令类型。通过使用默认数据类型 (UDT)，该指令可识别作业块类型。您将在下文中找到下列作业块的相关数据类型 (UDT)：

- 基于 IPv4 通过 IP 地址建立 FTP 连接
- 基于 IPv6 通过 IP 地址建立 FTP 连接
- 通过服务器名称建立 FTP 连接
- 读写访问和其它 FTP 命令
- FTP 命令 RETR_PART

基于 IPv4 通过 IP 地址建立 FTP 连接的作业块

对于基于 IPv4 通过 IP 地址建立的 FTP 连接，将使用以下数据结构。

表格 4- 4　FTP_CONNECT_IPV4

参数	类型	取值范围	含义/说明
InterfaceID	HW_ANY		模块起始地址 调用指令时，在 LADDR 参数中传送 CP 的模块起始地址。 在“属性 > 地址 > 输入”(Properties > Addresses > Inputs) 下，可以找到 CP 组态中 CP 的模块起始地址。
ID	CONN_OUC	1, 2...64	在 FTP 连接上处理 FTP 作业。该参数可识别所用的连接。
ConnectionType	BYTE	0	连接类型“FTP”
ActiveEstablishment	BOOL	TRUE	TRUE = 主动连接建立
FTPCmd	BYTE	1	FTP 命令 "CONNECT" 调用该指令时执行的 FTP 命令。关于命令类型的取值范围，可参见“输入参数 - FTP_CMD (页 53)”部分。 注意： 此处指定的 FTP 命令必须与在 CMD 输入参数中指定的命令相同。
CertIndex	BYTE	0 = FTP 1 = FTPS	在此处选择协议类型 FTP 或 FTPS。 有关 FTPS 的注意事项： 如果在 FTP 客户端的 STEP 7 项目外组态 FTP 服务器，则必须导入 FTP 服务器的证书。
UserName	STRING[32]	’benutzer’	用于登录 FTP 服务器的用户名
Password	STRING[32]	’passwort’	用于登录 FTP 服务器的密码
FTPserverIPaddr	IP_V4	ADDR(1) ... ADDR(4)	Array[1..4] of Byte 形式的 FTP 服务器的 IP 地址，其中 1 个字节指定一个地址块。 示例：ADDR(1) 指定第一个地址块（地址的第一个字节）。

基于 IPv6 通过 IP 地址建立 FTP 连接的作业块

对于基于 IPv6 通过 IP 地址建立的 FTP 连接，将使用以下数据结构。

表格 4- 5　FTP_CONNECT_IPV6

参数	类型	取值范围	含义/说明
InterfaceID	HW_ANY		模块起始地址 调用指令时，在 LADDR 参数中传送 CP 的模块起始地址。 在“属性 > 地址 > 输入”(Properties > Addresses > Inputs) 下，可以找到 CP 组态中 CP 的模块起始地址。
ID	CONN_OUC	1, 2...64	在 FTP 连接上处理 FTP 作业。该参数可识别所用的连接。
ConnectionType	BYTE	0	连接类型“FTP”
ActiveEstablishment	BOOL	TRUE	TRUE = 主动连接建立
FTPCmd	BYTE	1	FTP 命令 "CONNECT" 调用该指令时执行的 FTP 命令。关于命令类型的取值范围，可参见“输入参数 - FTP_CMD (页 53)”部分。 注意： 此处指定的 FTP 命令必须与在 CMD 输入参数中指定的命令相同。
CertIndex	BYTE	0 = FTP 1 = FTPS	在此处选择协议类型 FTP 或 FTPS。 有关 FTPS 的注意事项： 如果在 FTP 客户端的 STEP 7 项目外组态 FTP 服务器，则必须导入 FTP 服务器的证书。
UserName	STRING[32]	‘用户’	用于登录 FTP 服务器的用户名
Password	STRING[32]	‘密码’	用于登录 FTP 服务器的密码
FTPserverIPaddr	IP_V6	ADDR(1) ... ADDR(16)	Array[1..16] of Byte 形式的 FTP 服务器的 IP 地址，其中 2 个字节指定一个地址块。 示例：ADDR(1) + ADDR(2) 指定第一个地址块。

通过服务器名称建立 FTP 连接的作业块

对于建立指定了服务器名称的 FTP 连接，将使用以下数据结构。使用 DNS 将服务器名称分配给 IP 地址。

表格 4- 6 FTP_CONNECT_NAME

参数	类型	取值范围	含义/说明
InterfaceID	HW_ANY		模块起始地址 调用指令时，在 LADDR 参数中传送 CP 的模块起始地址。 在“属性 > 地址 > 输入”(Properties > Addresses > Inputs) 下，可以找到 CP 组态中 CP 的模块起始地址。
ID	CONN_OUC	1, 2...64	在 FTP 连接上处理 FTP 作业。该参数可识别所用的连接。
ConnectionType	BYTE	0	连接类型“FTP”
ActiveEstablishment	BOOL	TRUE	TRUE = 主动连接建立
FTPcmd	BYTE	1	FTP 命令 "CONNECT" 调用该指令时执行的 FTP 命令。关于命令类型的取值范围，可参见“输入参数 - FTP_CMD (页 53)”部分。 注意： 此处指定的 FTP 命令必须与在 CMD 输入参数中指定的命令相同。
CertIndex	BYTE	0 = FTP 1 = FTPS	在此处选择协议类型 FTP 或 FTPS。 有关 FTPS 的注意事项： 如果在 FTP 客户端的 STEP 7 项目外组态 FTP 服务器，则必须导入 FTP 服务器的证书。
UserName	STRING[32]	’benutzer’	用于登录 FTP 服务器的用户名
Password	STRING[32]	’passwort’	用于登录 FTP 服务器的密码
FTPserverName	STRING[254]		FTP 服务器的 IP 地址

读写访问和其它 FTP 命令的作业块

以下数据结构可用于 FTP 命令 store、retrieve、delete 和 append。

表格 4- 7　FTP_FILENAME

参数	类型	取值范围	含义/说明
InterfaceID	HW_ANY		模块起始地址 调用指令时，在 LADDR 参数中传送 CP 的模块起始地址。 在“属性 > 地址 > 输入”(Properties > Addresses > Inputs) 下，可以找到 CP 组态中 CP 的模块起始地址。
ID	CONN_OUC	1, 2...64	在 FTP 连接上处理 FTP 作业。该参数可识别所用的连接。
ConnectionType	BYTE	0	连接类型“FTP”
ActiveEstablishment	BOOL	TRUE	TRUE = 主动连接建立
FTPcmd	BYTE	2, 3, 4, 6	FTP 命令 "STORE / RETRIEVE / DELETE / APPEND" 调用该指令时执行的 FTP 命令。关于命令类型的取值范围，可参见“输入参数 - FTP_CMD (页 53)”部分。 注意： 此处指定的 FTP 命令必须与在 CMD 输入参数中指定的命令相同。
CertIndex	BYTE	0 = FTP 1 = FTPS	在此处选择协议类型 FTP 或 FTPS。 有关 FTPS 的注意事项： 如果在 FTP 客户端的 STEP 7 项目外组态 FTP 服务器，则必须导入 FTP 服务器的证书。
DataBlockNumber	UINT		在此指定的数据块包含要读取/写入的文件 DB。

参数	类型	取值范围	含义/说明
LenFilename	UINT	0...1000	不评估用于指定文件名总长度的参数“LenFilename”。 而是评估“Filename”参数字符串中的长度信息。
Filename	ARRAY[0..3] OF STRING[254]		目标文件或源文件的文件名。 文件名的四个字符串连在一起，作为一个完整字符串传输给服务器。

RETR_PART FTP 命令的作业块

以下数据结构用于 RETR_PART FTP 命令。

表格 4- 8 FTP_FILENAME_PART

参数	类型	取值范围	含义/说明
InterfaceID	HW_ANY		模块起始地址 调用指令时，在 LADDR 参数中传送 CP 的模块起始地址。 在“属性 > 地址 > 输入”(Properties > Addresses > Inputs) 下，可以找到 CP 组态中 CP 的模块起始地址。
ID	CONN_OUC	1, 2...64	在 FTP 连接上处理 FTP 作业。该参数可识别所用的连接。
ConnectionType	BYTE	0	连接类型“FTP”
ActiveEstablishment	BOOL	TRUE	TRUE = 主动连接建立
FTPcmd	BYTE	7	FTP 命令 "RETR_PART" 调用该指令时执行的 FTP 命令。关于命令类型的取值范围，可参见“输入参数 - FTP_CMD (页 53)”部分。 此处指定的 FTP 命令必须与在 CMD 输入参数中指定的命令相同。
CertIndex	BYTE	0 = FTP 1 = FTPS	在此处选择协议类型 FTP 或 FTPS。 有关 FTPS 的注意事项：如果在 FTP 客户端的 STEP 7 项目外组态 FTP 服务器，则必须导入 FTP 服务器的证书。

参数	类型	取值范围	含义/说明
Offset	DWORD		从将要读取的那个文件算起的偏移量(以字节计)。
Length	DWORD		在“OFFSET”中指定的数值处开始读取的子长(以字节计)。 特性： • 如果指定“DW#16#FFFFFFFF”，将读取文件的可用剩余部分。 如果没有出现其它错误，则结果“正确”(DONE = 1，STATUS = 0)。 • 当 OFFSET > 原始文件长度时： 目标文件长度(文件 DB 中的 ACT_LENGTH)：CPU 上的 0 字节。 如果没有出现其它错误，则结果“正确”(DONE = 1，STATUS = 0)。 • 当 OFFSET + LEN > 原始文件长度(且 LEN ≠ 0xFFFFFFFF)时： 目标文件长度(文件 DB 中的 ACT_LENGTH)：从“OFFSET”开始的可用字节。 如果没有出现其它错误，则结果“正确”(DONE = 1，STATUS = 0)。
DataBlockNumber	UINT		在此指定的数据块包含要读取/写入的文件 DB。
LenFilename	UINT	0...1000	不评估用于指定文件名总长度的参数“LenFilename”。 而是评估“Filename”参数字符串中的长度信息。
Filename	ARRAY[0..3] OF STRING[254]		目标文件或源文件的文件名。 文件名的四个字符串连在一起，作为一个完整字符串传输给服务器。

命令类型 NOOP 和 QUIT 的参数提供

同时为 FTP_CMD 提供对具有以下命令类型的作业块的引用：

CMD = 0 (NOOP)

CMD = 5 (QUIT)

由于这些命令类型执行时，不对作业块的内容进行评估，因此指定作业块的类型 (UDT) 不重要。

说明

对 FTP 作业块的引用丢失时的响应

如果未提供引用，则不执行命令。指令将在保持锁定在明显的执行状态下，不会为接口上的用户程序提供任何反馈。

4.7.2.4 输出参数和状态信息 FTP_CMD

参数 BUSY、DONE 和 ERROR

使用参数 BUSY、DONE、ERROR 和 STATUS 控制执行状态。BUSY 参数指示处理状态。使用 DONE 参数检查作业是否已正确执行。如果在执行 "FTP_CMD" 的期间出错，则会设置 ERROR 参数。错误信息在 STATUS 参数中输出。

下表列出了参数 BUSY、DONE 和 ERROR 之间的关系：

BUSY	DONE	ERROR	说明
1	-	-	正在处理作业。
0	1	0	作业已成功完成。
0	0	1	出错，作业终止。STATUS 参数中指定了错误的产生原因。
0	0	0	未分配新作业。

评估状态代码

说明

评估

- 评估 BUSY = 0

  BUSY = 0 之前，请勿评估状态显示。

- 状态 $8Fxx_H$

  有关以状态 $8Fxx_H$ 编码的条目，请参见“STEP 7 标准和系统函数”参考手册中的信息。描述通过 RET_VAL 输出参数进行错误评估的章节含详细信息。

表格 4- 9　FTP_CMD：STATUS 参数与 DONE 和 ERROR 一起使用时的含义

DONE	ERROR	STATUS	含义
0	0	0000_H	没有任何作业在执行中。
1	0	0000_H	无错完成了作业。
0	0	7001_H	第一次发起作业。
0	0	7002_H	作业仍在运行。
0	1	$80C4_H$	通信错误(临时发生，通常建议在用户程序中重复执行该作业)。
0	1	8183_H	组态与作业参数不匹配。
0	1	8401_H	未知错误 可能的原因： • 检测到连接超时。 • FTP 服务器已中止连接。 解决方法：再次发送 QUIT 和 CONNECT 命令以重新建立连接。
0	1	8402_H	连接处于出错状态。 可能已超出连接的超时时间或 FTP 服务器已终止连接。 解决方法：发送 QUIT 和 CONNECT 命令以重新建立连接。
0	1	8403_H	登录失败。
0	1	8404_H	无法获取 FTP 服务器。
0	1	8405_H	传送失败。
0	1	8406_H	当前操作超时
0	1	8407_H	FTP 服务器上未找到文件。
0	1	8408_H	无法传送。
0	1	8409_H	无法获取文件。
0	1	8410_H	数据连接的 TCP 端口设置失败。
0	1	8411_H	偏移量信息不匹配。
0	1	8412_H	更改指定目录时出错
0	1	8413_H	接收数据时出错
0	1	8414_H	发送数据时出错
0	1	8415_H	客户端拒绝指定 CMD（命令类型）。

DONE	ERROR	STATUS	含义
0	1	8416_H	FTP 服务器已关闭连接。
0	1	8418_H	用户数据错误。可能的原因： • 文件名为空。 • 数据长度为“0”。 • 等
0	1	8419_H	没有套接字资源可用来打开数据连接。
0	1	8420_H	没有套接字资源可用来打开控制连接。
0	1	8421_H	打开要读取的文件 DB 时出错
0	1	8422_H	打开要写入的文件 DB 时出错
0	1	8423_H	无法与 FTP 服务器建立连接。
0	1	8424_H	内部错误
0	1	8425_H	域名格式错误
0	1	8426_H	未决的 DNS 查询过多。
0	1	8427_H	指定的 DNS 服务器无法分配指定的域名。
0	1	8428_H	没有可用的连接资源。
0	1	8429_H	未知通道 ID
0	1	8430_H	文件 DB 过短。
0	1	8431_H	写入到文件 DB 时出错。
0	1	8432_H	从文件 DB 读取时出错。
0	1	8433_H	访问文件 DB 时出错。
0	1	8434_H	操作中止。
0	1	8435_H	通道将复位。
0	1	8436_H	意外的服务器应答
0	1	8437_H	无法验证证书。
0	1	8438_H	发生未知错误。
0	1	8439_H	FTP 命令导致错误。必须在 FTP 服务器上查找原因（REST 命令）。
0	1	8440_H	FTP 服务器不支持请求的 SSL 协议。
0	1	8446_H	FTP 密码发送到 FTP 服务器后，FTP 服务器返回了一个意外代码。

DONE	ERROR	STATUS	含义
0	1	8451_H	尝试将传输模式从二进制更改为 ASCII 时发出了出错信号。
0	1	8455_H	CM/CP 上的存储器请求失败。
0	1	8460_H	处理 SSL/TLS 时出现问题。
0	1	8469_H	接口错误 无法使用指定的输出接口。 解决方法： 设置要用于出站连接的接口。
0	1	8475_H	SSL 证书或 SSH md5 指纹未被视为可信。
0	1	8476_H	未从 FTP 服务器接收到任何内容。在当前状态下，必须假定一个错误响应。
0	1	8477_H	未找到指定的“加密引擎”（加密模块）。
0	1	8478_H	将所选 SSL“加密引擎”设置为默认值的尝试失败。
0	1	8480_H	FTP 客户端的证书出现问题。
0	1	8481_H	无法使用指定的编号。
0	1	8482_H	FTP 服务器使用了不受支持的编码。
0	1	8484_H	超出了最大文件大小。
0	1	8485_H	文件 DB 在处理成待发送时被修改或文件 DB 的结构错误。
0	1	8489_H	无法发送数据。FTP 服务器上没有足够的存储空间用于此操作。
0	1	8492_H	文件已经存在。文件不会被覆盖。
0	1	8496_H	读取 SSL CA 证书时出现问题。
0	1	8497_H	SSH 会话出现意外错误。
0	1	8498_H	无法终止 SSL 连接。
0	1	8499_H	套接字未准备好发送/接收。请等待至就绪，然后重试。
0	1	8501_H	FTP 服务器执行的 SSL 证书检查失败。
0	1	8507_H	在活动 FTP 会话期间建立连接的同时等待 FTP 服务器时发生超时。
0	1	$8F54_H$	文件 DB 标题中的“EXIST”位未置位。
0	1	$8F55_H$	标题状态位：已锁定
0	1	$8F56_H$	复位文件 DB 标题中的 NEW 位未复位。

DONE	ERROR	STATUS	含义
0	1	$8F6B_H$	可能的原因： • CMD 参数的数值错误 允许使用 0 至 15 范围内的数值。 • 不支持 FB40 命令。 可能原因：CP 的固件不正确 解决方法：固化程序更新(对于较早的 CP，使用函数 FC 40...FC 44，而不是 FB 40。)
0	1	$8F7F_H$	内部错误；例如非法 ANY 引用。

4.7.2.5 用于 FTP 客户端操作的数据块（文件 DB）的结构

工作原理

要使用 FTP 传送数据，请在 S7 站的 CPU 上创建数据块（文件 DB）。这些数据块必须具有特定结构，以便作为可传送文件由 FTP 服务进行处理。它们由下列部分组成：

- 部分 1：文件 DB 报头(具有固定长度，20 字节)
- 部分 2：“Array [..] of Byte”或“Array [..] of Char”类型的用户数据（具有可变的长度和结构）

数据一致性

确保不在同一时间多次访问同一文件 DB。

创建文件 DB

1. 在 STEP 7 中创建一个新数据块。
2. 打开块编辑器。
3. 在 DB 的块编辑器中，选择要用作文件 DB 起始行的行。
4. 在“数据类型”(Data type) 列中，使用键盘输入类型“FILE_DB_HEADER”。

   将创建文件 DB 所需的带报头结构的数据结构。
5. 将“WRITEACCESS”参数设置为“true”以启用访问。
6. 在“MAX_LENGTH”参数中输入用户数据长度的值。

7. 之后，为要发送的用户数据创建一个“Array [..] of Byte”或“Array [..] of Char”类型的数据字段。

   字段的大小必须与报头中所规定的“MAX_LENGTH”相匹配。

用于 FTP 客户端模式的文件 DB 报头

此处描述的文件 DB 报头与服务器模式的文件 DB 报头相同。

参数	类型	数值/含义	电源
EXIST	BOOL	EXIST 位指示用户数据区是否包含有效的数据。 只有在 EXIST=1 时，retrieve FTP 命令才执行作业。 • 0：文件 DB 不包含有效的用户数据（文件不存在）。 • 1：文件 DB 包含有效的用户数据（文件存在）。	DELETE FTP 命令设置 EXIST=0。 STORE FTP 命令设置 EXIST=1。
LOCKED	BOOL	LOCKED 位用于限制对文件 DB 的访问。 • 0：可以访问文件 DB。 • 1：文件 DB 被锁定。	如果该位之前为 0，则在执行“STORE”和“RETRIEVE”FTP 命令后，会设置 LOCKED=1。 在为了取得数据一致性而进行的写访问期间，S7 CPU 上的用户程序还可以置位或复位 LOCKED。 这样可使用户程序与 FTP 处理互锁，从而确保一致性。 建议在用户程序中按下列顺序执行： 1. 检查 LOCKED 位（是否为 0） 2. 置位 WRITEACCESS = 0 3. 检查 LOCKED 位（是否为 0） 4. 置位 LOCKED = 1 5. 写数据 6. 置位 LOCKED = 0

参数	类型	数值/含义	电源
NEW	BOOL	NEW 位指示自上一次读操作到现在，数据是否被修改。 • 0：自上次写访问以来，文件 DB 的内容没有发生改变。S7 CPU 的用户程序已经记录最近一次修改。 • 1：S7 CPU 的用户程序尚未记录上次写访问。	执行以后，“RETRIEVE”FTP 命令设置 NEW=1。 读取数据后，S7 CPU 中的用户程序必须设置 NEW=0 以允许新的“RETRIEVE”命令。
WRITEACCESS	BOOL	• 0：用户程序对 S7 CPU 上的文件 DB 具有写访问权限。 • 1：用户程序对 S7 CPU 上的文件 DB 不具有写访问权限。	在组态 DB 期间，将此位置位为初始值。 建议： 如有可能，应该保持此位不变！在特殊情况下，可以在操作期间对此进行调整。
ACT_LENGTH	DINT	用户数据区的当前长度。 只有在 EXIST = 1 时，该字段的内容才有效。	在进行写入操作以后更新当前长度。
MAX_LENGTH	DINT	用户数据区的最大长度（整个 DB 的长度减去 20 个字节的文件头）。	应在 DB 组态期间指定最大长度。还可在操作期间通过用户程序修改该数值。
FTP_REPLY_CODE	INT	无符号整型(16 位)，包含最后一个来自 FTP 的返回代码，代码为二进制数值。 只有当 EXIST=1 时，此字段的内容才有效。	通过 FTP 协议句柄及服务器的 FTP 命令处理更新。
DATE_TIME	DATE_AND_TIME	文件最近一次修改的日期和时间。 只有当 EXIST=1 时，此字段的内容才有效。	在写访问以后更新当前日期。 如果使用了转发时钟的功能，则输入对应于已传递的时间。 如果未使用转发时钟的功能，则输入相对时间。参考为 CP 的启动时间（初始值： 01.01.1994 00:00h）。

从 FTP_CMD 程序块评估“LOCKED”和“NEW”状态位

- 在版本为 1.2 的“FTP_CMD”程序块中，不会评估 FILE_DB_HEADER 的“LOCKED”和“NEW”状态位。

  使用 FTP 服务器的功能或者使用同一文件 DB 时，不能排除同时多次访问同一数据区的可能性。这将导致数据不一致。

- 在版本 1.5 或更高版本的“FTP_CMD”程序块中，正确设置 FILE_DB_HEADER 的状态位“LOCKED”和“NEW”。评估这两个状态位。自 STEP 7 Professional V12 SP1 开始提供版本 1.5。

说明

避免数据不一致

确保不在同一时间多次访问同一文件 DB。

4.8 安全性

有关安全功能的范围和使用的概览信息，请参见工业以太网安全 (页 17)部分。

有关安全功能的组态限制，请参见安全特性 (页 21)部分。

要组态安全功能，需要创建一个安全用户，请参见安全用户 (页 69)部分。

4.8.1 安全用户

创建安全用户

组态安全功能需要具备相关的组态权限。为此，需要通过相应权限创建至少一个安全用户。

导航到全局安全设置 > “用户和角色”(User and roles) >“用户”(Users) 选项卡。

1. 创建用户并组态参数。
2. 在“分配的角色”(Assigned roles)下方区域为该用户分配角色“NET 标准”(NET Standard)或“NET 管理员”(NET Administrator)。

登录后，该用户可以在 STEP 7 项目中进行所需的设置。

在以后使用安全参数时，请继续以该用户身份登录。

4.8.2 VPN

仅当将模块分配给全局安全功能中的 VPN 组时，才会显示模块的“VPN”参数组。

什么是 VPN？

虚拟专用网络 (VPN) 是用于在公共 IP 网络（例如 Internet）中安全传输保密数据的技术。利用 VPN，可通过非安全网络在两个安全 IT 系统或网络间建立安全连接（= 隧道）并进行操作。

VPN 隧道的主要特性之一是，无论是否使用高层协议（HTTP，FTP），它都能转发所有网络数据包。

两个网络组件间的数据通信实际上是通过其它网络进行无限制传输。这样便可通过相邻网络将整个网络连接在一起。

属性

- VPN 构成了一个嵌入到相邻（已分配）网络中的逻辑子网。VPN 使用已分配网络的通常寻址机制，但就数据而言，其传输自己的网络数据包，因此独立于该网络的其余部分运行。
- VPN 允许 VPN 伙伴通过分配的网络进行通信。
- VPN 基于隧道技术，可单独进行组态，并且是客户特定且独立的。
- 使用密码、公钥或数字证书（= 身份验证）可保护 VPN 伙伴间的通信免遭窃听或操纵。

应用领域

- 可通过 Internet 将局域网安全地连接在一起（“站点到站点”连接）。
- 对公司网络进行安全访问（“端到站点”连接）。
- 对服务器进行安全访问（“端到端”连接）。
- 无需访问第三方即可在两个服务器间进行通信（“端到端”连接或“主机到主机”连接）。
- 确保联网的自动化系统中的信息安全性。
- 保护包含自动化网络中或通过 Internet 进行的安全远程访问中的相关数据通信的计算机系统。
- 可通过公共网络从 PC/编程设备对受安全模块保护的自动化设备或网络进行安全远程访问。

单元保护概念

利用工业以太网安全，单个设备、自动化单元或以太网网段均可受到保护：

- 允许对受安全模块保护的各个设备甚至整个自动化单元进行访问。
- 通过非安全网络结构实现安全连接成为可能。

借助不同安全措施（例如防火墙、NAT/NAPT 路由器和 IPsec 隧道上的 VPN）的组合，安全模块可防止：

- 数据间谍
- 数据操纵
- 不希望的访问

4.8.2.1 在 S7-1500 站之间建立 VPN 隧道通信

要求

要在 S7-1500 站之间创建 VPN 隧道，必须满足以下要求：

- 已组态两个 S7-1500 站。
- 相关 CP 1543-1 组态 V1.1 及以上版本的固件。
- 两个站的以太网接口位于统一子网中。

说明

也可通过 IP 路由器进行通信

也可通过 IP 路由器在两个 S7-1500 站之间进行通信。但是，要使用此通信路径，需要进行进一步设置。

操作步骤

要创建 VPN 隧道，需要完成以下步骤：

1. 创建安全用户。

   如果已创建安全用户：请以该用户身份登录。

2. 选中“激活安全特性”(Activate security features) 复选框。
3. 创建 VPN 组并分配安全模块。
4. 组态 VPN 组的属性。

   组态两个 CP 的本地 VPN 属性。

有关各步骤的详细说明，请参见本部分的以下段落。

创建安全用户

要创建 VPN 隧道，需要相应的组态权限。要激活安全功能，需要至少创建一个安全用户。

1. 在 CP 的本地安全设置中，单击“用户登录”(User logon) 按钮。
   结果：打开一个新窗口。
2. 输入用户名、密码和密码确认。
3. 单击“用户登录”(User login) 按钮。
   您已创建新的安全用户。现在，您可以使用安全功能。

对于所有其它登录，请以该用户身份登录。

启用“激活安全特性”选项

- 登录后，必须将两个 CP 的“激活安全特性”(Activate security features) 选项都选中。
  现在，两个 CP 均可使用安全功能。

创建 VPN 组并分配安全模块

说明

安全模块上的当前日期和时钟

使用安全通信（例如 HTTPS、VPN...）时，确保涉及的安全模块具有当前时钟和当前日期。否则，使用的证书将无法评估为有效，安全通信不会工作。

1. 在全局安全设置中，选择条目“防火墙 > VPN 组 > 添加新 VPN 组”(Firewall > VPN groups > Add new VPN group)。
2. 双击条目“添加新 VPN 组”(Add new VPN group) 来创建 VPN 组。
   结果：新的 VPN 组显示在所选条目下。
3. 在全局安全设置中，双击条目“VPN 组 > 将模块分配给 VPN 组”(VPN groups > Assign module to a VPN group)。
4. 分配将在其间建立到 VPN 组的 VPN 隧道的安全模块。

组态 VPN 组的属性

1. 双击新创建的 VPN 组。
   结果：VPN 组的属性显示在“身份验证”(Authentication) 下。
2. 输入 VPN 组的名称。在属性中组态 VPN 组的设置。
   通过这种方式，可以定义 VPN 组的基本属性。

说明

指定 CP 的 VPN 属性

请在模块的本地属性中指定所需 CP 的 VPN 属性（“安全性 > 防火墙 > VPN”(Security > Firewall > VPN)）

结果

您已创建 VPN 隧道。CP 的防火墙将自动激活：创建 VPN 组时，已默认选中“激活防火墙”(Activate firewall) 选项。无法禁用此选项。

- 将组态下载到属于该 VPN 组的所有模块。

4.8.2.2 在 CP 和 SCALANCE M 之间建立 VPN 隧道通信

在 CP 和 SCALANCE M 之间建立 VPN 隧道通信的步骤实际上与“适用于 S7-1500 站的步骤 (页 71)”中的说明相同。

只有在已创建的 VPN 组（“VPN 组 > 身份验证”(VPN groups > Authentication)）的全局安全设置中启用“Perfect Forward Secrecy”选项，才能建立 VPN 隧道通信。

如果禁用此选项，则 CP 会拒绝建立连接。

4.8.2.3 与 SOFTNET Security Client 进行 VPN 隧道通信

在 SOFTNET 安全客户端和 CP 之间设置 VPN 隧道通信的步骤实际上与适用于 S7-1500 站的步骤 (页 71)中的说明相同。

只有禁用了内部节点，VPN 隧道通信才会工作

在某些情况下，在 SOFTNET Security Client 与 CP 之间建立 VPN 隧道通信会失败。

SOFTNET Security Client 也尝试建立与低级别内部节点的 VPN 隧道通信。与不存在的节点建立通信将妨碍与 CP 建立所需的通信。

要成功建立与 CP 的 VPN 隧道通信，需要禁用内部节点。

只有出现所描述的问题时，才会使用下述节点禁用步骤。

在 SOFTNET Security Client 通道概述中禁用节点：

1. 移除“启用主动学习”(Enable active learning) 复选框中的复选标记。

   低级别节点在初始时从隧道列表中消失。

2. 在隧道列表中，选择所需的 CP 连接。
3. 使用鼠标右键，在快捷菜单中选择“启用所有成员”(Enable all members)。

   低级别节点暂时再次出现在隧道列表中。

4. 在隧道列表中选择低级别节点。
5. 使用鼠标右键，在快捷菜单中选择“删除条目”(Delete entry)。

结果：现在已完全禁用低级别节点。成功建立与 CP 的 VPN 隧道通信。

4.8.2.4 CP 作为 VPN 连接的被动用户

设置通过被动用户建立 VPN 连接的权限

如果 CP 通过网关连接另一个 VPN 用户，则需要将建立 VPN 连接的权限设置为“Responder”。

以下典型组态中会出现这种情况：

VPN 用户（主动）⇔ 网关（动态 IP 地址）⇔ Internet ⇔ 网关（固定 IP 地址）⇔ CP（被动）

按如下方法，组态将 CP 作为被动用户建立 VPN 连接的权限：

1. 在 STEP 7 中，转到设备和网络视图。
2. 选择 CP。
3. 在本地安全设置中，打开“VPN”参数组。
4. 对于每个将 CP 作为被动 VPN 用户的 VPN 连接，将默认设置“Initiator/Responder”更改为设置“Responder”。

4.8.3 防火墙

4.8.3.1 检查到达帧和离去帧时的防火墙顺序

每个到达帧或离去帧都会经过 MAC 防火墙（第 2 层）。 如果帧在此层级被丢弃，则 IP 防火墙（第 3 层）不会对其进行检查。 这表示，通过合适的 MAC 防火墙规则，可以限制或阻止 IP 通信。

参见

已编程的连接：防火墙规则的限制 (页 45)

CPU 的虚拟接口 (页 41)

4.8.3.2 源 IP 地址的表示法（高级防火墙模式）

如果在 CP 的高级防火墙设置中指定源 IP 地址的地址范围，请确保表示法正确无误：

- 仅使用连字符来分隔两个 IP 地址。

  正确：192.168.10.0-192.168.10.255

- 不要在两个 IP 地址之间输入任何其它符号。

  错误：192.168.10.0 - 192.168.10.255

如果错误地输入范围，则不会使用防火墙规则。

4.8.3.3 HTTP 和 HTTPS 不可使用 IPv6

在工作站的 Web 服务器上无法通过 IPv6 协议使用 HTTP 和 HTTPS 通信。

如果在本地安全设置的“防火墙 > 预定义的 IPv6 规则”(Firewall > Predefined IPv6 rules) 条目中启用防火墙： 所选复选框“允许 HTTP”(Allow HTTP) 和“允许 HTTPS”(Allow HTTPS) 没有作用。

4.8.3.4 连接的 VPN 隧道防火墙设置

高级防火墙模式中的 IP 规则

如果已组态 CP 间的连接，则在高级防火墙模式下操作 CP 时，请注意以下设置。

在“安全 > 防火墙 > IP 规则”(Security > Firewall > IP rules) 参数组中，选择“Accept”设置进行两个 CP 的隧道连接。

如果不启用该选项，则将终止并重新建立 VPN 隧道连接。

这适用于 CP 154x-1 与 CP 343-1 Advanced、CP 443-1 Advanced、CP 1628 或 CP 1243-1 等之间的连接。

参见

防火墙激活情况下的在线安全诊断和下载到站设置 (页 76)

4.8.4 在线功能

4.8.4.1 防火墙激活情况下的在线安全诊断和下载到站设置

针对在线功能设置防火墙

若已启用安全功能，请按照下面列出的步骤进行操作：

1. 在全局安全设置（参见项目树）中，选择条目“防火墙 > 服务 > 为 IP 规则定义服务”(Firewall > Services > Define services for IP rules)。
2. 选择“ICMP”选项卡。
3. 插入一个类型为“回送应答”(Echo Reply) 和一个类型为“回送请求”(Echo Request) 的新条目。
4. 现在选择 S7 站中的 CP。
5. 在 CP 的本地安全设置中，在“安全 > 防火墙”(Security > Firewall) 参数组中启用高级防火墙模式。
6. 打开“IP 规则”(IP rules) 参数组。
7. 在表中，按如下方式为之前已创建的全局服务插入新的 IP 规则：
   - 操作 (Action)：允许；全局创建的“回送请求”(Echo request) 服务“从外部 -> 到站”(From external -> To station) 通信
   - 操作 (Action)：允许；全局创建的“回送应答”服务“从站 -> 到外部”通信
8. 对于“回送请求”的 IP 规则，在“源 IP 地址”(Source IP address) 中输入工程师站的 IP 地址。这可确保只有来自您的工程师站的 ICMP 帧 (ping) 可以通过防火墙。

4.8.4.2 通过端口 8448 执行在线安全诊断

通过端口 8448 执行安全诊断

要求：通过 HTTPS 激活对 CP 的 Web 服务器的访问。

如果要在 STEP 7 Professional 中执行安全诊断，请按下列步骤进行操作：

1. 在 STEP 7 中选择 CP。
2. 打开“在线和诊断”(Online & Diagnostics) 快捷菜单。
3. 在“安全性”(Security) 参数组中，单击“在线连接”(Connect online) 按钮。

这样，即可通过端口 8448 执行安全诊断。

4.8.5 日志设置 - 过滤系统事件

系统事件值设置太高时产生的通信问题

如果过滤系统事件的值设置得过高，则您可能无法实现最佳通信性能。 大量输出错误消息可延迟或阻止通信连接的处理。

在“Security > 日志设置 > 组态系统事件”(Security > Log settings > Configure system events) 中，将“等级：”(Level:) 参数设为值“3（错误）”(3 (Error))，以便确保建立可靠的通信连接。

4.9 用于 OUC 的程序块

编程 Open User Communication (OUC)

如要通过以太网获得以下通信服务，需使用下面列出的各个指令（程序块）。

- ISO 传输
- TCP (IPv4 / IPv6)
- ISO-on-TCP
- UDP (Multicast)
- 电子邮件

为此，创建适当的程序块。此程序块可在 STEP 7 的“指令 > 通信 > Open user communication”(Instructions > Communication > Open User Communication) 窗口中找到。

有关程序块的详细信息，请参见 STEP 7 的信息系统。

说明

不同程序块版本

请注意，在 STEP 7 中，不能在一个站中使用一个程序块的不同版本。

支持用于 OUC 的程序块

以下特定的最低版本指令可用于 Open User Communication 编程：

- **TSEND_C V3.1 / TRCV_C V3.1**

  紧凑型程序块，用于建立/终止连接和发送/接收数据

  或

- **TCON V4.0 / TDISCON V2.1**

  建立连接/终止连接

- **TUSEND V4.0 / TURCV V4.0**

  通过 UDP 发送和接收数据

- **TSEND V4.0 / TRCV V4.0**

  通过 TCP 或 ISOonTCP 发送和接收数据

- **TMAIL_C V4.0**

  发送电子邮件

  请注意 STEP 7 信息系统中 V4.0 及以上版本 TMAIL_C 的描述。

建立和终止连接

各个连接通过程序块 TCON 建立。请注意，必须为每个连接调用单独的程序块 TCON。

必须为每个通信伙伴建立单独的连接，即使发送相同数据块。

成功传输数据之后，可以终止连接。还可以通过调用 TDISCON 终止连接。

说明

连接中止

如果现有连接被通信伙伴中止或由于网络上的干扰而中止，则同样必须通过调用 TDISCON 来终止连接。编程时确保考虑到这一点。

系统数据类型 (SDT) 的连接描述

对于连接描述，上述程序块使用参数 CONNECT（对于 TMAIL_C 则使用 MAIL_ADDR_PARAM）。连接描述以数据块形式存储，此数据块的结构由系统数据类型 (SDT) 定义。

创建数据块 SDT

为每个数据块形式的连接描述创建所需的 SDT。SDT 类型在 STEP 7 中生成，具体方式是在程序块声明表中的“数据类型”(Data type) 框中手动输入名称（如“TCON_IP_V4”），而不是从“数据类型”(Data type) 下拉列表中选择一个条目。随后，相应的 SDT 与其参数一并创建出来。

可使用如下 SDT：

- **TCON_Configured**

  基于 TCP 传送帧

- **TCON_IP_V4**

  基于 TCP 或 UDP 传送帧

- **TCON_IP_V4_SEC**

  基于 TCP 安全传送帧

- **TCON_QDN**

  基于 TCP 或 UDP 传送帧 (IPv4 / IPv6)

- **TCON_QDN_SEC**

  基于 TCP 安全传送帧 (IPv4 / IPv6)

- **TCON_IP_RFC**

  基于 ISO-on-TCP 传送帧

- **TCON_ISOnative**

  基于 ISO 传输传送帧

- **TMail_V4**

  基于 IPv4 地址式电子邮件服务器寻址来传送电子邮件

- **TMail_V6**

  基于 IPv6 地址式电子邮件服务器寻址来传送电子邮件

- **TMail_FQDN**

  基于主机名式电子邮件服务器寻址来传送电子邮件

- **TMail_V4_SEC**

  基于 IPv4 地址式电子邮件服务器寻址来安全传送电子邮件

- **TMail_V6_SEC**

  基于 IPv6 地址式电子邮件服务器寻址来安全传送电子邮件

- **TMail_QDN_SEC**

  基于主机名式电子邮件服务器寻址来安全传送电子邮件

有关 SDT 及其参数的说明，请参见 STEP 7 信息系统中 SDT 的相应名称下的内容。

有关 SDT TMail_V4_SEC、TMail_V6_SEC 和 TMail_QDN_SEC 的参数的说明，请参见 TCON_IP_V4_SEC 的在线帮助部分。

诊断和保养

5

5.1 诊断方法

可对模块使用以下诊断方法：

模块的 LED

有关 LED 指示灯的信息，请参见 LED (页 25)部分。

STEP 7：“巡视”(Inspector) 窗口中的“诊断”(Diagnostics) 选项卡

如果工程师站通过以太网连接到模块，则可以在此处找到有关 ES 与模块间连接状态的信息。

STEP 7：通过“在线和诊断”(Online & Diagnostics) 快捷菜单启用诊断功能

可以使用在线功能从存储 STEP 7 项目的工程师站中读取模块的各种诊断信息并执行维护功能。

有关 STEP 7 诊断功能的其它信息，请参见 STEP 7 信息系统。

诊断

可在此处找到有关所选模块的以下静态信息：

- 常规

  模块的常规信息

- 诊断状态

  有关诊断状态的信息

- 以太网接口

  地址和统计信息

- 时间

  指定模块中的当前时间和时间源

- 安全性

  状态信息和日志条目

功能

可在此处运行以下功能：

- 固件更新

  有关说明，请参见“更新固件 (页 86)”部分。
- 分配 IP 地址
- 分配 PROFINET 设备名称
- 保存服务数据

STEP 7：在线连接

通过“在线连接”(Connect online) 快捷菜单建立与模块的在线连接。

相关操作步骤，请参见“在线连接 (页 82)”部分。

Web 服务器

在 PC 上，可以通过 HTTP/HTTPS 访问 CPU 的 Web 页面。这些页面提供各种信息。

要访问内容，请参见“文档指南 (页 11)”。

SNMP

有关所支持的功能的详细信息，请参见使用 SNMP 进行诊断 (页 83)部分。

5.2 在线连接

在线功能

CP 与 STEP 7 共同在工程师站 (ES) 上提供各种诊断和维护功能。为此，ES 和 CP 必须位于同一子网中。

通过以太网建立在线连接

步骤：

1. 将 ES 连接到网络。
2. 在 ES 上打开相关的 STEP 7 项目。

3. 选择 CP。
4. 使用“在线连接”(Connect online) 图标启用在线功能。
5. 在“在线连接”(Connect online) 对话框的“PG/PC 接口类型”(Type of PG/PC interface) 下拉列表中，选择“PN/IE”条目。
6. 在“PG/PC 接口”(PG/PC interface) 下拉列表中，选择 ES 的接口。

   可使用下拉列表右侧的  图标来检查接口的设置。
7. 在“与接口/子网连接”(Connect with interface/subnet) 下拉列表中，选择站的接口。
8. 单击“开始搜索”(Start search)。

   如果可以进行连接，则显示该站。
9. 在目标设备表中选择站。

   通过 CP 或 CPU 的路径均可行。
10. 单击“连接”(Connect)。

终止在线连接

完成在线会话后，使用“断开连接”(Disconnect) 按钮再次终止在线连接。

参见

在线功能 (页 76)

5.3 使用 SNMP 进行诊断

要求

要使用 SNMP，需要在组态中启用该功能。

SNMP (Simple Network Management Protocol)

SNMP 是用于诊断、管理网络和网络中节点的协议。SNMP 使用无连接 UDP 协议发送数据。

有关 SNMP 兼容设备属性的信息在 MIB 文件中输入 (MIB = Management Information Base)。

关于 SNMP 和 Siemens Automation MIB 的详细信息，请参见 Internet 上的手册《基于 SNMP 的诊断和组态》：
链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15392/man)

CP 的性能应用范围

CP 支持以下 SNMP 版本：

- SNMPv1
- SNMPv3 (Security 功能已激活)

CP 不支持陷阱。

SNMPv1 中支持的 MIB

CP 支持以下 MIB：

- **MIB II （根据 RFC1213）**

  CP 支持以下 MIB 对象组：

  – System
  – Interfaces
  – IP
  – ICMP
  – TCP
  – UDP
  – SNMP

- **LLDP MIB**
- **Siemens Automation MIB**

  注意 MIB 对象的写入权限，请参见下一部分 (SNMPv3)。

SNMPv3 中支持的 MIB 对象

若启用了 SNMPv3，则 CP 将返回如下 MIB 对象的内容：

- **MIB II （根据 RFC1213）**

  CP 支持以下 MIB 对象组：

  – System

  – Interfaces

    “接口”MIB 对象提供有关 CP 接口的状态信息。

  – IP (IPv4/IPv6)

  – ICMP

  – TCP

  – UDP

  – SNMP

  不支持以下标准 MIB II 组：

  – Adress Translation (AT)

  – EGP

  – Transmission

- **LLDP MIB**

- **Siemens Automation MIB**

  请注意，只允许对“System”组的以下 MIB 对象进行写访问：

  – sysContact

  – sysLocation

  – sysName

    使用 DHCP 选项 12 将设置的 sysName 作为主机名发送到 DHCP 服务器以注册 DNS 服务器。

  出于安全原因，对于所有其它 MIB 对象和 MIB 对象组，只能进行读访问。

使用团体名称的访问权限 (SNMPv1)

TCP 使用以下团体字符串控制对 SNMP 代理的访问权限：

表格 5- 1　SNMP 代理中的访问权限

访问类型	团体字符串 *)
读访问	public
读和写访问	private

*) 注意使用小写字母！

说明

访问的安全性

出于安全原因，请更改众所周知的字符串 "public" 和 "private"。

5.4　更新固件

CP 的新固件版本

如果 CP 有新的固件版本可以使用，则可在 Siemens 工业在线支持的以下 Internet 页面上找到：

链接：（https://support.industry.siemens.com/cs/ww/zh/ps/15340/dl）

固件文件具有 *.upd 的文件格式。

在 PC 上保存固件文件。

有不同的方法可在 CP 上加载新的固件文件：

- 通过以太网使用 STEP 7 的在线功能
- 将固件文件从 SD 卡加载到 CPU 中

说明

固件文件专用 SD 卡

对于固件文件，需要一个 SIMATIC SD 存储卡，例如（订货号）：

- 6AV6671-8XB10-0AX1
- 6AV2181-8XP00-0AX0
- 6AV2181-8AQ10-0AX0

固件更新卡可能不包含任何其它文件。无法使用含有组态数据的 SD 卡。

说明

固件更新的持续时间

下载新的固件文件可能需要几分钟的时间。
务必稍作等待，直到可以从 LED 显示判断出固件更新已结束（如下所示）。

通过以太网使用 STEP 7 的在线功能加载固件

要求：

- 可通过以太网访问站的 CPU。
- 工程师站和 CPU 位于同一子网中。
- 新的固件文件存储在工程师站上。
- 工程师站连接至网络。
- 相关的 STEP 7 项目在工程师站上打开。

步骤：

1. 选择要使用新固件进行更新的站。
2. 使用“在线连接”(Connect online) 图标启用在线功能。
3. 在“在线连接”(Connect online) 对话框的“PG/PC 接口类型”(Type of PG/PC interface) 列表框中选择以太网接口。
4. 选择站的 CPU。
5. 单击“开始搜索”(Start search) 搜寻网络中的模块并指定连接路径。

   找到该模块后，模块将显示在表格中。

6. 使用“连接”(Connect) 按钮进行连接。

   “在线连接”向导将指导您完成剩余的安装步骤。

7. 在网络视图中选择 CPU，然后选择“在线和诊断”(Online & Diagnostics) 快捷菜单（右键单击）。

8. 在“在线和诊断”(Online & Diagnostics) 视图的导航面板中，选择条目“功能 > 固件更新”(Functions > Firmware update)。

9. 使用“浏览”(Browse) 按钮（“固件装载器”(Firmware loader) 参数组）在工程师站的文件系统中搜索新的固件文件。

10. 当“状态”(Status) 输出框显示签名固件的正确版本时，使用“开始更新”(Start update) 按钮开始下载固件。

有关在线功能的更多信息，请参见 STEP 7 信息系统。

通过 SD 卡加载固件

有关使用 SD 卡的详细信息，请参见《S7-1500 系统手册》，可在“文档指南 (页 11)”部分查找该文档。

要求：

- 已经使用合适的读卡器从 PC 中将新固件文件复制到 SD 卡。
- 可选：已为当前正在使用的固件文件保存了备份文件。

步骤：

1. 设置将 CPU 操作模式切换到 STOP 模式。

   确保在 STOP 状态下未激活写入功能（例如在线或测试功能）。

2. 从 CPU 插槽中删除包含组态数据的 SIMATIC Memory Card。

3. 将包含固件文件的 SD 卡插入 CPU 的卡槽中。

   插入卡后不久就会启动固件更新。显示屏上将显示以下内容： "STOP - FW UPDATE"

   如果发生错误，则显示相应的消息。

   完成固件更新后，显示屏将显示结果页面。

   可以通过 CPU 的以下 LED 模式识别固件是否成功更新：

   – RUN 指示灯呈黄色点亮。

   – MAINT 指示灯呈黄色闪烁。

4. 取出 SD 卡并再次插入 SIMATIC Memory Card。
5. 设置将 CPU 操作模式切换到 RUN 模式。

   CP 在启动过程中将使用新固件。

有关启动过程中 CP 的 LED 模式的信息，请参见“LED (页 25)”部分。

5.5 在没有编程设备的情况下更换模块

交换模块时的组态数据

CP 的组态数据存储在 CPU 中。这样便可在没有 PG 的情况下使用相同类型（相同的部件编号）的模块替换该模块。

说明

采用组态的 MAC 地址

设置 ISO 协议时，记住先前组态期间设置的 MAC 地址已由 CPU 传送到新的 CP 模块。

通过 DHCP (IPv4) 交换地址引用模块

CP 的 IP 组态选项之一是从 DHCP 服务器获取 IP 地址。

说明

建议：组态客户端 ID

更换模块时，注意新模块出厂时设置的 MAC 地址有别于旧模块。

将新模块出厂默认的 MAC 地址发送到 DHCP 服务器时，DHCP 服务器会返回一个与之前不同的 IP 地址，或不返回 IP 地址。

因此，最好按以下方式组态 IP：

- 始终组态客户端 ID 并相应组态 DHCP 服务器。这可确保在交换模块后，CP 始终接收来自 DHCP 服务器的同一 IP 地址。

如果组态新的 MAC 地址而不使用出厂时设置的 MAC 地址，则组态的 MAC 地址将始终传送到 DHCP 服务器。此时，新的 CP 具有与之前的模块相同的 IP 地址。

技术规范

6

6.1 CP 技术规范

注意 SIMATIC S7-1500 的系统描述 (页 11)中的信息。

除了系统描述中的信息外，下面的技术规范也适用此模块。

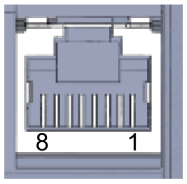
技术规范 - CP 1543-1	
产品名称	CP 1543-1
部件编号	6GK7 543-1AX00-0XE0
工业以太网连接	
• 数量	1 个以太网（千兆位）接口
• 设计	RJ-45 插孔
• 传输速度	10/100/1000 Mbps
电气数据	
电源	
• 通过 S7-1500 背板总线	15 V
电流消耗	
• 来自背板总线	350 mA
• 功率损耗	5.3 W
绝缘	
绝缘测试电压	707 VDC（型式测试）
设计、尺寸和重量	
模块规格	紧凑型模块 S7-1500，单宽度
防护等级	IP20
重量	约 350 g
尺寸 (W x H x D)	35 x 142 x 129 mm
安装选项	安装在 S7-1500 机架中
产品功能 *	

** 有关产品功能，请参见“产品总览、功能 (页 13)”部分。

6.2 以太网接口的引脚分配

千兆以太网接口的引脚

下表列出了以太网接口 X1 的引脚分配。

RJ-45 插孔的视图	引脚	信号名称	分配
	1	D1+	D1+ 双向
	2	D1-	D1- 双向
	3	D2+	D2+ 双向
	4	D3+	D3+ 双向
	5	D3-	D3- 双向
	6	D2-	D2- 双向
	7	D4+	D4+ 双向
	8	D4-	D4- 双向

6.3 允许的电缆长度 - 以太网

允许的电缆长度 - 以太网	各长度范围的备选组合
0 ... 55 m	• 最长 55 m 带有 IE FC RJ45 Plug 180 的 IE TP Torsion Cable • 最长 45 m 带有 IE FC RJ45 的 IE TP Torsion Cable + 10 m 通过 IE FC RJ45 Outlet 的 TP Cord
0 ... 85 m	• 最长 85 m 带有 IE FC RJ45 Plug 180 的 IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable • 最长 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m 通过 IE FC RJ45 Outlet 的 TP Cord
0 ... 100 m	• 最长 100 m 带有 IE FC RJ45 Plug 180 的 IE FC TP Standard Cable • 最长 90 m IE FC TP Standard Cable + 10 m 通过 IE FC RJ45 Outlet 的 TP Cord

另请参见西门子网上商城： (https://mall.industry.siemens.com)

6.4 允许的电缆长度 - 千兆以太网

允许的电缆长度 - 千兆以太网	备选组合：
0 ... 60 m	• 最长 60 m IE FC TP Flexible Cable GP 4x2 + 10 m 通过 IE FC RJ45 Modular Outlet Insert 1GE 的 TP Cord RJ45/RJ45 4x2
0 ... 100 m	• 最长 90 m IE FC TP Standard Cable GP 4x2 + 10 m 通过 IE FC RJ45 Modular Outlet Insert 1GE 的 TP Cord RJ45/RJ45 4x2

另请参见西门子网上商城： (https://mall.industry.siemens.com)

认证

7

指定的认证

说明

设备铭牌上指定的认证

仅当产品上印有相应标志时，才表示已获得指定的认证（船级社证书除外）。可通过铭牌上的标志了解已为该产品授予了以下认证中的哪些认证。船级社认证对此不适用。

船级社证书和国家认证

有关船级社设备证书和特殊国家认证的信息，请参见 Internet 上的 Siemens 工业在线支持：

链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15340/cert)

EC 符合性声明

CE

本产品满足下列 EC 指令的要求和安全目标，并符合欧盟官方文档中针对可编程逻辑控制器发布的协调欧洲标准 (EN)。

- **2014/34/EU（ATEX 防爆指令）**

  有关协调各成员国拟用于潜在爆炸性环境的设备和保护系统方面法律的 2014 年 2 月 26 日欧洲议会和理事会指令，EU L96 公文，2014 年 3 月 29 日，第 309-356 页

- **2014/30/EU (EMC)**

  2014 年 2 月 26 日欧洲议会和理事会 EMC 指令，用于协调各成员国电磁兼容性方面的法律；EU L96 公文，2014 年 3 月 29 日，第 79-106 页

- **2011/65/EU (RoHS)**

  有关电气和电子设备中特定危险物质的使用限制的 2011 年 6 月 8 日欧洲议会和理事会指令

向所有主管机关出具的 EC 符合标准声明可从以下地址获取：

Siemens Aktiengesellschaft
Digital Industries

P.O.Box 48 48
90026 Nuernberg
Germany

有关 EC 符合性声明，请访问以下 Internet 地址：
链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15340/cert)

可在 EC 符合性声明和证书中找到标准的当前版本。

IECEx

产品符合 IECEx 的防爆要求。

IECEx 分类：

- Ex nA IIC T4 Gc

  证书： IECEx DEK 14.0089X

  应用标准：

  – EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
  – EN 60079-15 - 爆炸性气体环境 - 第 15 部分：防护类型“n”的设备保护

- Ex ec IIC T4 Gc

  证书：IECEx DEK 18.0019X

  应用标准：

  – EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
  – EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

可在 IECEx 证书中找到标准的最新版本，请访问以下 Internet 地址获取 IECEx 证书：
链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15340/cert)

必须满足“符合 ATEX/IECEx 要求的危险场所使用注意事项 (页 30)”部分中的相关条件，才能安全使用本产品。

此外，也应注意文档“Use of subassemblies/modules in a Zone 2 Hazardous Area”中的信息，请访问以下 Internet 地址获取该文档：
链接： (https://support.industry.siemens.com/cs/ww/zh/view/78381013)

ATEX

本产品满足 EC 指令：2014/34/EC“在潜在易爆环境中使用的设备和防护设备”的要求。

ATEX 认证：

- II 3 G Ex nA IIC T4 Gc

  Type Examination Certificate: DEKRA 12 ATEX 0240X

  应用标准：

  – EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
  – EN 60079-15 -爆炸性气体环境 - 第 15 部分：防护类型“n”的设备保护

- II 3 G Ex ec IIC T4 Gc

  Type Examination Certificate: DEKRA 18 ATEX 0027X

  应用标准：

  – EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
  – EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

如上所述，可在 EC 符合性声明中找到标准的当前版本。

必须满足“符合 ATEX/IECEx 要求的危险场所使用注意事项 (页 30)”部分中的相关条件，才能安全使用本产品。

另外也应注意文档“Use of subassemblies/modules in a Zone 2 Hazardous Area”中的信息，此文档可在此处找到：

- 在“所有文档”(All documents) >"Use of subassemblies/modules in a Zone 2 Hazardous Area"下的
  SIMATIC NET 手册集 DVD 中
- Internet 地址：
  链接： (https://support.industry.siemens.com/cs/ww/zh/view/78381013)

EMC

产品满足 EC 指令 2014/30/EU“电磁兼容性”的相关要求（EMC 指令）。

应用标准：

- EN 61000-6-4

  电磁兼容性 (EMC) - 第 6-4 部分：通用标准 - 工业环境中的辐射标准

- EN 61000-6-2

  电磁兼容性 (EMC) - 第 6-2 部分：通用标准 - 工业环境中的抗扰性

RoHS

产品在电气和电子设备中特定危险物质的使用限制方面符合 EC 指令 2011/65/EU 的要求。

应用标准：

- EN 50581

c(UL)us

应用标准：

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E 85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

应用标准：

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta:请参见 CP 铭牌上的温度等级信息

Report / UL file: E223122 (NRAG, NRAG7)

注意，需满足符合 UL Hazloc 要求的危险场所使用注意事项 (页 31)部分中的相关条件，才能安全部署该产品。

说明

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

CSA

CSA Certification Mark Canadian Standard Association (CSA) nach Standard C 22.2 No. 142:

- Certification Record 063533–C-000

FM

Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

有关温度等级的信息，请参见模块铭牌。

澳大利亚 - RCM

本产品满足 AS/NZS 2064 标准（A 类）的要求。

加拿大

本 A 类数字设备符合加拿大标准 ICES-003 的要求。

AVIS CANADIEN

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

MSIP 요구사항 - For Korea only

A 급 기기(업무용 방송통신기자재)

이 기기는 업무용(A 급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

请注意，该设备符合针对干扰发射的 A 类规定。该设备可用于除住宅区以外的所有区域。

当前认证

SIMATIC NET 产品会定期提交到相关机构和认证中心，以获得与特定市场和应用有关的认证。

如果需要各个设备当前所获认证的列表，请咨询 Siemens 联系人或查阅 Siemens 工业在线支持的 Internet 页面：

链接： (https://support.industry.siemens.com/cs/ww/zh/ps/15340/cert)

索引

C

CPU 的工作模式, 33
CPU 的连接资源, 18

D

DHCP, 89

E

EMC - 电磁兼容性, 95

F

FETCH/WRITE, 15, 39
    S5/S7 寻址模式, 16
FETCH/WRITE 连接, 19
FTP, 39
    对 FTP 作业块的引用丢失时的响应, 62
FTP 的 TCP 连接, 21
FTP 服务器
    组态限制, 21
FTP 客户端
    组态限制, 21
FTP（FTP 客户端）, 18
FTP_CMD, 50
    块执行时间, 21
FTPS, 17
FTPS - Security, 46

H

HMI 通信, 14

I

IP 地址
    IPv6, 16
    通过 DHCP, 40
IP 组态
    IPv4 / IPv6, 15
IP 路由, 41
IPsec 隧道
    数量, 21
ISO 传输（符合 RFC 8073）, 14
ISO 传输连接, 19
ISO-on-TCP 连接, 19
ISO-on-TCP（符合 RFC 1006）, 14

L

LED 指示灯, 25

M

MAC 地址, 3, 15
MIB, 83

N

NTP (secure), 17, 46
NTP 服务器, 46
NTP 模式, 15

O

OP 连接
    数量, 20

Open User Communication (OUC), 14
OUC (Open User Communication), 77

P

PG 连接
  数量, 20
PG 通信, 14
PUT/GET, 39

R

RUN → STOP, 33

S

S5/S7 寻址模式, 16
S7 连接, 14, 18
  可自由使用数, 20
S7 通信, 14
SIMATIC NET, 12
SIMATIC NET 词汇表, 6
SMTPS, 18
SNMP, 83
SNMP 代理, 15
SNMPv3, 18
STEP 7, 5, 23
STEP 7 在线帮助, 32

T

TCP 连接, 19
TCP（符合 RFC 793）, 14

U

UDP
  限制, 20
UDP 连接, 19
UDP 帧缓冲, 20
UDP（符合 RFC 768）, 14

V

VPN, (??????)
  应用领域, 70
  单元保护概念, 71

W

Web 的连接
  数量, 20
Web 服务器, 16

X

下载, 12
下载项目数据, 32

Q

千兆位规范, 27

Y

已编程的连接
  数量, 20
已编程通信连接, 45

S H

手册集, 12

Y

以太网接口, 3, 27
    引脚分配, 33
    通过 T_CONFIG 组态, 24

D

电子邮件, 14
电子邮件连接, 19
电源模块
    更多, 22

C H

处置, 6

J

记录, 17

Z

在线功能, 82
在线诊断, 81

H

回收, 6

W

网关 (VPN), 74
网络中的重复地址, 40

Z

自动检测, 39
自动跨接机制, 40

A

安全诊断, 77
安全须知, 29
安装和调试, 32
    步骤, 32

F

防火墙, 17

L

连接交换机, 40

S H

时间同步, 15

X

系统数据类型
    FTP_..., 24
    TCON_..., 23
    TMail_..., 23
系统数据类型 (SDT), 79

C

词汇表, 6

G

固件版本, 3

B

版本历史, 12

D

单元保护概念
VPN, 71

Z

组态, 32
组态和下载组态数据, 22
组播
通过 UDP, 14

Z H

指令
FTP_CMD, 24
T_CONFIG, 24
TCON、TSEND/TRCV, 23
TDISCON, 23
TMAIL_C, 23
TSEND_C/TRCV_C, 23
TUSEND/TURCV, 23

Z

总体组态限制, 22

T

特殊注意事项
连接交换机, 40
时间设置建议, 45
确保有效时钟, 46

B

被动建立 VPN 连接, 74

D

调试
STEP 7 项目数据的完整性, 32

X

虚拟专用网络
定义, 70

Y

硬件产品版本, 3

C H

程序块 - 最大数据长度, 19

K

跨接电缆, 40

S H

数据管理 - 组态数据, 89
数量
可运行 CP, 22

D

端口 8448, 77