SIEMENS

SIMATIC NET

S7-1500 - 工业以太网 CP 1543-1

设备手册

12/2013

C79000-G8952-C289-05

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 ® 的都是西门子股份有限公司的注册商标。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
Industry Sector
Postfach 48 48
90026 NÜRNBERG
德国

C79000-G8952-C289-05
℗ 12/2013 本公司保留技术更改的权利

前言

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 CP。

另请参见文档指南 (页 7)

约定

请务必阅读以下特殊注意事项：

说明

注意事项包含有关本文档所述产品、使用该产品或文档中应特别关注的部分的重要信息。

名称

- 在本文档中，同样使用术语“CP”代替产品全称。
- 名称 STEP 7 是指 STEP 7 Professional 组态工具。

SIMATIC NET 词汇表

在 SIMATIC NET 词汇表部分针对本文档中所用的专业术语进行了解释。

用户可在以下位置找到 SIMATIC NET 词汇表：

- SIMATIC NET 手册集

  该 DVD 随一些 SIMATIC NET 产品一起提供。

- 请参见 Internet 上的以下条目 ID：

  50305045 (http://support.automation.siemens.com/WW/view/zh/50305045)

许可证条款

说明

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。 接受许可证条款包含的免责声明和担保是使用开源软件的具体前提条件。

在所提供的数据介质中，下列文档提供有许可证条款：

- DOC_OSS-Siemens_74.pdf
- DOC_OSS-CP1243-1DNP3_76.pdf

长版

西门子自动化和驱动产品具有某些工业安全功能，以支持工厂或设备安全操作。这些功能是整个工业安全机制的重要组成部分。基于此我们对产品进行持续开发。因此，建议您随时关注产品的更新信息并确保您仅使用最新版本。更多信息，请访问：
http://support.automation.siemens.com.

此外，要确保工厂或设备的安全操作，还须采取适当的预防措施（例如：设备单元保护机制），并将自动化和驱动组件纳入整个工厂或设备先进且全面的工业安全保护机制中。可能使用的任何第三方产品须一并考虑。更多信息，请访问：
http://www.siemens.com/industrialsecurity

目录

文档指南

1

简介

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、功能手册和设备手册组成。

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。

有关与 S7-1500 进行通信的文档概述

下表列出了其它文档，是 CP 1543-1 说明的补充文档，可以在 Internet 上查看。

表格 1- 1　CP 1543-1 的组态工具

主题	文档	重要内容
系统描述	系统手册： S7-1500 自动化系统 (http://support.automation.siemens.com/WW/view/zh/59191792)	• 应用规划 • 安装 • 连接 • 调试
系统诊断	功能手册：系统诊断 (http://support.automation.siemens.com/WW/view/zh/59192926)	• 概述 • 硬件/软件诊断评估
通信	功能手册：通信 (http://support.automation.siemens.com/WW/view/zh/59192925)	• 概述
	功能手册： Web 服务器 (http://support.automation.siemens.com/WW/view/zh/59193560)	• 功能 • 运行
	手册工业以太网安全 (http://support.automation.siemens.com/WW/view/zh/56577508)	• 工业以太网中安全功能的概述和说明

主题	文档	重要内容
	手册 SIMATIC NET：双绞线和光纤网络 (http://support.automation.siemens.com/WW/view/zh/8763736)	• 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 (http://support.automation.siemens.com/WW/view/zh/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 (http://support.automation.siemens.com/WW/view/zh/59193566)	• 基本信息 • 计算

SIMATIC 手册

有关 SIMATIC 产品的所有最新手册，可在 Internet (http://www.siemens.com/automation/service&support) 上免费下载。

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”提供到目前为止 SIMATIC S7（工业以太网）可用的所有 CP 的信息。

可以在 Internet (http://support.automation.siemens.com/WW/view/zh/9836605) 上找到此文档的最新版本

产品总览

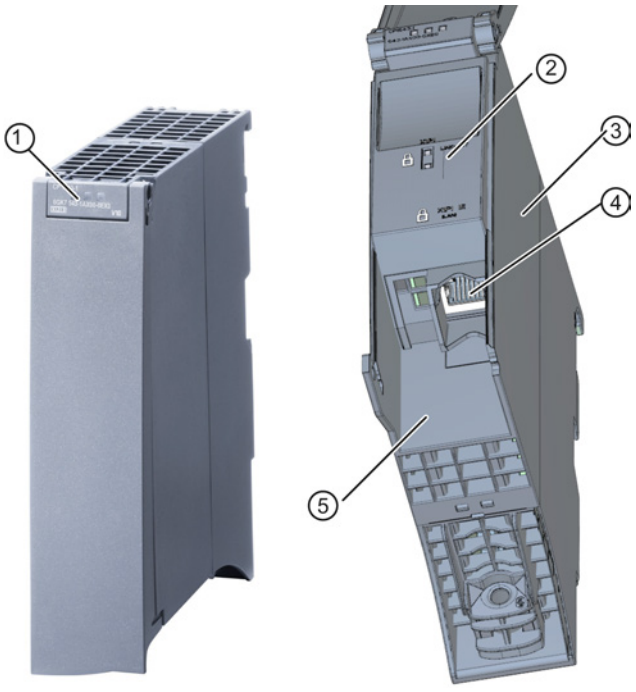
2

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 V1.1
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，表示“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 2-1 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！

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 可保护各 S7-1500 站甚至整个自动化单元免受未经授权的访问。

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。

说明

术语“以太网接口”

上文介绍的符合千兆位规范的 CP 接口在本手册的其余部分称为“以太网接口”。

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。

CP 支持以下通信服务：

- **开放式通信**

  通过使用已编程或已组态的通信连接的 CP，开放式通信支持以下通信服务：

  – ISO 传输（符合 ISO/IEC 8073）

  – TCP（符合 RFC 793）、ISO-on-TCP（符合 RFC 1006）和 UDP（符合 RFC 768）；

    利用通过 TCP 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。

  – 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 ISO 传输连接、ISOonTCP 连接和 TCP 连接实现的 FETCH/WRITE 服务（服务器服务；对应于 S5 协议）；

    此处，带有 CP 的 SIMATIC S71500 始终为服务器（建立被动连接），而获取或写访问（建立主动连接的客户端功能）始终由 SIMATIC S5 或第三方设备/PC 发起。

- **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

- **IT 功能**

  – FTP 功能（文件传输协议 FTP/FTPS），用于文件管理以及访问 CPU 中的数据块（客户端和服务器功能）

  – 通过 SMTP 或具有“SMTPAuth”的 ESMTP 在电子邮件服务器上发送用于验证的电子邮件。

2.1 其它功能

在工业以太网上使用 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（安全）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，请参见编程 (页 22)部分）分配到 CP。

  注意： 不适用于 S7 连接。

符合 IPv6 格式的 IP 地址 - CP 上的使用范围

符合 IPv6 的 IP 地址可用于以下通信服务：

- FTP 服务器模式
- FETCH/WRITE 访问（CP 为服务器）
- 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

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 7)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。

2.2 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的组合，可防御从连接到 CP 1543-1 的外部网络发来的数据：

- 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）
  - 根据 IEEE 802.3，也适用于以太网“非 IP”帧（第 2 层）的防火墙
  - 带宽限制
  - 全局防火墙规则
- 记录

  为允许监视，可将事件存储在日志文件中，日志文件可通过组态工具读出，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。

- 安全 NTP

  用于安全的时钟同步和传输。

- SNMPv3

  用于安全传送网络分析信息，使其免受窃听。

- 设备和网段的保护

  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。

注意
对安全有要求的工厂 - 建议 使用下列选项： • 若您的系统对安全性要求很高，请使用安全协议 NTP（安全）、FTPS、HTTPS 和 SNMPv3。 • 如果您连接到了公共网络，则应使用防火墙。 考虑下您要通过公共网络获取的服务。 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。

功能特性

3

3.1 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。

3.2 开放式通信的特性

使用开放式通信可通过 TCP、ISOonTCP、ISO 传输和 UDP 连接访问通信。

以下特性非常重要：

特性	说明/值
连接数	• 连接的最大总数（组态的与编程的： （ISO 传输和 ISOonTCP + TCP + UDP + FETCH/WRITE + 电子邮件）<= 118 其中： – TCP 连接： 1...118 1) – ISO-on-TCP 连接： 1...118 – ISO 传输连接： 1...118 – 可以组态的 UDP 连接总数（已指定和空闲）： 1...118 – 适用于 FETCH/WRITE 的连接： 1...16 – 电子邮件连接：1 注意： • 1) 避免接收端发生过载 TCP 连接的流控制**无法**控制接收方的永久性过载。 因此必须确保发送方不会永久超出接收 CP 的处理能力（大约每秒 150200 条消息）。
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： 1. ISO-on-TCP、TCP 和 ISO 传输：1 到 64 kB 2. UDP： 1 到 1452 字节 3. 电子邮件（作业标题 + 用户数据）：1 到 256 字节 电子邮件附件： 最多 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 7)部分

UDP 的限制

- 不对传输进行确认

  不对 UDP 帧的传送情况进行确认，换言之，发送程序块检测不到也不会显示丢失的消息。

- UDP 帧缓冲

  帧缓冲的长度：

  至少 7360 个字节。

  注意：

  缓冲区溢出后，新到达的帧将被丢弃。

3.3 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)	• 针对发送：480 字节/PDU • 针对接收：480 字节/PDU
保留的 OP 连接数	4
保留的 PG 连接数	4
保留给 Web 的连接数	2

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。

3.4 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。 根据相应模式，以下特性数据适用：

- 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 (FB40)

要进行通信，请使用 FTP 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。

3.5 VPN 隧道通信的特性

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

使用要求

4

4.1 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。

  注意 CPU 的文档中的信息，请参见文档指南 (页 7)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。

4.2 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。

4.3 编程

程序块

针对通信服务，STEP 7 用户程序中提供了接口形式的预编程程序块（指令）。

表格 4- 1　通信服务指令

协议	程序块（指令）	系统数据类型
TCP	通过以下指令建立连接和发送/接收数据： • TSEND_C/TRCV_C 或 • TCON、TSEND/TRCV（可以使用 TDISCON 终止连接）	• TCON_IP_v4 • TCON_Configured
ISO-on-TCP		• TCON_IP_RFC
ISO		• TCON_ISOnative
UDP	• TCON、TUSEND/TURCV（可以使用 TDISCON 终止连接）	• TCON_IP_v4
电子邮件	• TMAIL_C	• TMail_v4* • TMail_v6* • TMAIL_FQDN*
FTP	• FTP_CMD	• FTP_CONNECT_IPV4* • FTP_CONNECT_IPV6* • FTP_CONNECT_NAME* • FTP_FILENAME* • FTP_FILENAME_PART*

*用户定义的数据类型

表格 4- 2　组态任务的指令

功能	程序块（指令）	系统数据类型
以太网接口的组态	• T_CONFIG	• CONF_DATA

请参见 STEP 7 在线帮助中的程序块文档。

连接/调试

5

5.1 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，以及在执行所有相关的工作（例如，安装、接线、更换设备或打开设备）期间，必须遵守以下安全须知。

通用注意事项

⚠警告

安全超低电压

本设备适用于在受限电源 (LPS, Limited Power Source) 提供的安全超低电压 (SELV, Safety Extra-Low Voltage) 下工作。（这不适用于 100 V...240 V 设备。）

这表示只能将符合 IEC 60950-1/EN 60950-1/VDE 0805-1 的 SELV/LPS 连接到电源端子上。 用作设备电源的供电单元必须符合美国国家电气法规 (r) (ANSI/NFPA 70) 中所述的 NEC 2 级标准。

如果设备使用冗余电源，还需另外满足以下要求：

如果设备连接有一个冗余电源（两个独立的电源），则两个电源都必须满足这些要求。

有关在危险场所使用的通用注意事项

⚠警告

连接或断开本设备时有爆炸风险

爆炸危险

请勿在易燃环境下连接或断开设备。

⚠警告

更换组件

爆炸危险

更换组件可能损害在 I 级 2 分区或 2 区的适用性。

⚠警告

机柜/机壳要求

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

受限应用领域

此设备仅适合在 I 类、2 分区、A、B、C 和 D 组别或无危险位置使用。

⚠警告

受限应用领域

此设备仅适合在 I 类、2 区、IIC 组别或无危险位置使用。

⚠警告

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。

符合 ATEX 要求的危险场所使用通用注意事项

⚠警告

机柜/机壳要求

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

⚠警告

温度超过 70 °C 情况下的适用电缆

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。 如果设备在 50°C 以上的环境温度下工作，则所选电缆的允许温度范围必须适合于实际测得的温度。

⚠警告

瞬变电压浪涌防护

应采取预防措施，防止瞬变电压浪涌超出额定电压 40% 以上。 仅当通过 SELV（安全超低电压）供电时，才满足该标准。

5.2 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 7)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。

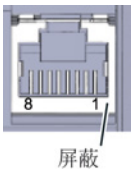
安装和调试步骤

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。	
3	通过 RJ45 插孔将 CP 连接到工业以太网。	CP 的底部
4	接通电源。	
5	关闭模块的前盖，保持其在运行过程中处于关闭状态。	
6	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的引脚分配。 分配对应于 RJ45 插头的以太网标准。

表格 5- 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	发送数据 +	D1+	D1 双向 +
	2	TD_N	发送数据 -	D1-	D1 双向 -
	3	RD	接收数据 +	D2+	D2 双向 +
	4	GND	接地	D3+	D3 双向 +
	5	GND	接地	D3-	D3 双向 -
	6	RD_N	接收数据 -	D2-	D2 双向 -
	7	GND	接地	D4+	D4 双向 +
	8	GND	接地	D4-	D4 双向 -

参考

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 S7-1500 自动化系统 (http://support.automation.siemens.com/WW/view/zh/59191792)。

5.3 在没有编程设备的情况下更换模块

常规步骤

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。

模块更换： 通过 DHCP 服务器分配 IP 地址的特殊功能 (IPv4)

组态 CP 时，可在属性对话框中指定 IP 组态；其中可选择从 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。 将新模块出厂时设置的 MAC 地址发送到 DHCP 服务器时，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。 这样可确保在更换模块后，始终从 DHCP 服务器获得相同的 IP 地址。

在个别情况下，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。 在这种情况下，新的 CP 也会收到与先前模块相同的 IP 地址。

5.4 CPU 模式 - 对 CP 的影响

可以使用 STEP 7 组态软件切换 CPU 的模式（RUN 和 STOP 之间）。

根据 CPU 的工作状态，CM 的行为如下所述。

将 CPU 从 RUN 切换到 STOP：

当 CPU 处于 STOP 模式时，CP 将保持 RUN 模式，其行为如下：

- 对于已建立的连接（ISO 传输、ISOonTCP、TCP、UDP 连接），根据组态，以下行为适用：
  - 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（用于组态、诊断和 PG 通道路由的系统连接得到保留）；
  - Web 诊断
  - S7 路由功能
  - 时钟同步

说明

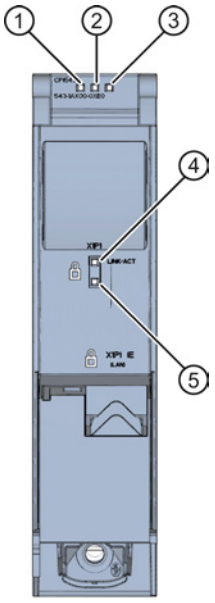
CP 的 RUN/STOP LED

无论 CPU 是否处于 STOP 模式，CP 的绿色 RUN/STOP LED 都持续绿色点亮。

中断、诊断消息、错误和系统报警 6

6.1 CP 的状态和错误显示

LED 指示灯



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

图 6-1 CP 1543-1 的 LED 指示灯（不带前盖）

LED 指示灯的含义

CP 1543-1 使用 3 个 LED 来显示当前工作状态和诊断状态，这些 LED 具有以下含义：

- RUN LED （单色 LED：绿色）
- ERROR LED （单色 LED：红色）
- MAINT LED （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 6- 1　LED 的含义

RUN LED	ERROR LED	MAINT LED	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

该端口的 LED 指示灯表示以下含义：

- LINK/ACT　存在连接/正在传送数据　（双色 LED：绿色/黄色）

下表显示了 CP 1543-1 的以太网接口各种 LED 组合。

表格 6- 2　LED 的含义

LINK/ACT LED		含义
绿灯熄灭	黄灯熄灭	无链接 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	存在链接 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。

6.2 诊断方法

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 CP 的状态和错误显示 (页 31)部分。

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

  在此可找到有关所选模块的以下信息：

  – 有关模块的在线状态的信息

- STEP 7： “在线 > 在线和诊断”(Online > Online and diagnostics) 菜单中的诊断功能

  在此可找到所选模块的状态信息：

  – 模块的常规信息

  – 诊断状态

  – 以太网接口的信息

  – 安全（已启用安全）

  有关 STEP 7 诊断功能的详细信息，请参见 STEP 7 在线帮助。

操作注意事项 7

7.1 网络设置

7.1.1 快速以太网

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。

7.2 IP 组态

7.2.1 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。

7.2.2 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。

7.3 安全性

7.3.1 过滤系统事件

避免因系统事件的高输出而在生产通信中出现问题

如果过滤系统事件的值设置得过高，则您可能无法使用最大数目的通信连接。 大量输出错误消息可延迟或阻止通信连接的处理。

为确保通信连接的可靠建立： 在 CP 1543-1 的本地安全设置（“安全性 > 日志设置 > 过滤系统事件”(Security > Log settings > Filtering of system events)）中，我们建议您设置级别值“3（错误）(3 (Error))”。

7.3.2 CP 1543-1 和 CP x43-1 之间用于组态连接的 VPN 隧道通信（高级防火墙模式）

如果您建立 CP 1543-1 和 CP x43-1 之间用于组态连接的 VPN 隧道通信，则将需要调整 CP 1543-1 的本地防火墙设置：

- 对于 VPN 隧道的两个通信方向，选择高级防火墙模式中的“允许”(Allow) 操作（“安全性 > 防火墙 > IP 规则”(Security > Firewall > IP rules)）。

如果不选择此设置，则将终止并重新建立 VPN 隧道连接。

7.3.3 防火墙

7.3.3.1 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。

7.3.3.2 防火墙激活情况下的在线诊断和下载

使用 STEP 7 和 Windows XP 时的特性

当要求通过 STEP 7 在线访问 S7-1500 站时，在尝试建立连接之前会向模块发送 ping 命令，这是 Windows XP 防火墙的特点所致。 ping 包将检查通信伙伴是否可用。 仅当 STEP 7 安装在运行 Windows XP 的 PG 上时存在此特性。 如果基于 Windows 7 运行 STEP 7，则不会发送 ping 包。

若 CP 防火墙激活，要允许 STEP 7 通过 CP 的以太网接口建立在线连接以进行诊断和下载，则要求在防火墙中进行一些特殊设置。 只有防火墙允许，才能成功确认这样的 ping 命令。

设置防火墙 - 涉及的步骤

若已启用安全，请按照下面列出的步骤进行操作：

1. 在全局安全设置中，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”和一个类型为“回送请求”的新条目。
4. 现在选择 S7-1500 站中的 CP。

5. 在 CP 的本地安全设置中，打开参数组“属性 > 常规 > 安全 > 防火墙”(Properties > General > Security > Firewall) 并激活高级防火墙模式。
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：
   - 动作： 允许；全局创建的“回送请求”服务“从外部 -> 到站”通信
   - 动作： 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 PG/PC 的 IP 地址。 这可确保只有来自您的 PG/PC 的 PING 数据包可以通过防火墙。

7.3.3.3 带宽限制 < 1 Mbps 没有任何作用（高级防火墙模式）

带宽限制值不能 < 1 Mbps。

这意味着，带宽限制的可用选项被限制为下列值范围： 1 至 100 Mbps。

7.3.3.4 防火墙规则的最大数目（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：

- 226 个具有单独地址的规则
- 30 个具有地址范围或网络地址的规则（例如 140.90.120.1-140.90.120.20 或 14.90.120.0/16）
- 具有已输入的带宽限制的规则数目被限制为 128 个。

7.3.3.5 源 IP 地址/地址范围的正确表示法（高级防火墙模式）

如果在 CP 1543-1 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。

7.3.3.6 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。

7.3.4 VPN

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

7.3.4.1 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。
- 两个 CP 必须在固件版本 V1.1 下组态。
- 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。

选中“激活安全特性”(Activate security features) 复选框

- 登录后，请将两个 CP 的“激活安全特性”(Activate security features) 复选框都选中。
  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。 组态 VPN 组的属性设置。
   这些属性定义了 VPN 组的默认设置，您可以随时进行更改。

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) 复选框。 无法取消选择该复选框。

- 将组态下载到属于该 VPN 组的所有模块。

7.3.4.2 在 CP 1543-1 和 SCALANCE M 之间成功建立 VPN 隧道通信

在 CP 1543-1 和 SCALANCE M 之间建立 VPN 隧道通信的步骤与“适用于 S7-1500 站的步骤 (页 40)”中的说明相同。

只有在已创建的 VPN 组（“VPN 组 > 身份验证”(VPN groups > Authentication)）的全局安全设置中选中“完美前向安全性”(Perfect Forward Secrecy) 复选框，才能建立 VPN 隧道通信。

如果未选中该复选框，CP 1543-1 会拒绝建立隧道。

7.3.4.3 与 SOFTNET Security Client 进行 VPN 隧道通信

在 CP SOFTNET Security Client 和 CP 1543-1 之间建立 VPN 隧道通信的步骤与“适用于 S7-1500 站的步骤 (页 40)”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，于 SOFTNET Security Client 和 CP 1543-1 之间建立 VPN 隧道通信失败。

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此通信将防止与 CP 1543-1 建立所需的通信。

要成功建立与 CP 1543-1 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，选择与 CP 1543-1 之间的所需连接。
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。 可建立与 CP 1543-1 的 VPN 隧道通信。

7.4 FTP

仅在启用安全时进行 FTP 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 FTP 方式访问作为 FTP 服务器的 S7-1500 站。 这意味着必须激活 CP 上的“安全”(Security) 属性。这才可以用全局用户管理使全局安全设置可用。

使用 FTP_CMD 指令进行 FTP 访问 - 命令类型 NOOP 和 QUIT 的参数

与 STEP 7 在线帮助中有关 FTP_CMD 指令的信息不同，注意以下说明：

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。

注意
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。

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。

注意
避免数据不一致 确保不在同一时间多次访问同一文件 DB。

7.5 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 模式下时钟同步的特性

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

如果 CP 检测到 NTP 帧“不精确”(not exact)（示例： NTP 服务器不进行外部同步），则不会进行转发。 如果出现此问题，则诊断中没有 NTP 服务器显示为“NTP 主站”(NTP master)；而是所有 NTP 服务器都只显示为“可访问”(accessible)。

安全性

在扩展 NTP 组态中，可创建并管理其它 NTP 服务器，包括 NTP（安全）类型的服务器。

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（安全）类型的 NTP 服务器。

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。

7.6 SNMP 代理

SNMP（简单网络管理协议）

SNMP 是用于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 = 管理信息库）。

CP 支持通过 SNMP 版本 V1（标准）和 V3（安全）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。

更多信息

有关使用 MIB 文件的详细信息，请参见所使用的 SNMP 客户端的文档（SNMP 客户端示例： SIMATIC NET 中的 SNMP OPC 服务器）。

您可以在 Internet (http://support.automation.siemens.com/WW/view/zh/15177711) 上找到有关 MIB 的更多信息

可通过以下条目 ID 获取 MIB 文件： 67637278 (http://support.automation.siemens.com/WW/view/zh/67637278)

支持的 MIB

CP 支持以下几组 MIB II 标准（符合 RFC1213）的 MIB 对象：

- 系统
- 接口
- IP（IPv4 和 IPv6）
- ICMP
- TCP
- UDP
- SNMP
- 地址转换 (AT)

不支持其它组的 MIB II 标准：

- EGP
- 传输

CP 继续支持自动化系统 MIB。

例外/限制：

- 只允许对系统组的以下 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/MIB 对象组，只能进行读访问。
- CP 不支持陷阱。

MIB 组“接口”

“接口”MIB 对象提供有关 CP 接口的状态信息。

使用团体名称的访问权限

CP 使用以下团体名称控制 SNMP 代理中的访问权限：

表格 7- 1　SNMP 代理中的访问权限

访问类型	团体名称 *)
读访问	公有
读和写访问	私有

*) 注意使用小写字母！

7.7 用户程序中的接口

7.7.1 使用已编程通信连接的 IP 访问保护

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。

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。

STEP 7 的在线帮助介绍了 IP 访问保护的组态和已激活安全的各个方面。

技术规范

8

注意 SIMATIC S7-1500 的系统描述 (页 7)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。

	6GK7 543-1AX00-0XE0
产品型号名称	CP 1543-1
工业以太网连接	
• 数量	1 个以太网（千兆位）接口
以太网接口的设计	
• 连接器	1 个 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

	6GK7 543-1AX00-0XE0
允许的电缆长度	**（每个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
产品功能 **	

* 有关详细信息，请参见 IK PI 目录的“接线技术”

** 有关产品功能，请参见“功能特性 (页 15)”部分。

认证 9

9.1 认证 - 注意事项

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

在 Internet (http://support.automation.siemens.com/WW/news/zh/10805878) 上的 Siemens 自动化客户支持页面可找到船级社设备证书和特殊国家认证

在该条目下，转到所需产品并选择以下设置： “条目列表”(Entry list) 选项卡 >“证书”(Certificates) 条目类型。

标准和测试规范

本设备满足以下标准和测试规范。 模块的测试标准基于这些标准和测试规范。

IEC 61131–2

本手册中介绍的 SIMATIC NET S7 CP 符合 IEC 61131-2 标准（可编程逻辑控制器，第 2 部分：设备要求和验证）的要求和条件。

CE 标志

本手册中介绍的 SIMATIC NET S7-CP 符合以下 EC 指令的要求和保护目标，并且符合欧盟公文中有关可编程逻辑控制器的欧洲协调标准 (EN)：

- 2004/108/EEC“电磁兼容性”（EMC 指令）
- 94/9/EC“用于潜在爆炸环境的设备和保护系统”（防爆指令）

可以从位于以下地址的责任机构获取满足上述 EC 指令的 EC 符合性声明：

- Siemens Aktiengesellschaft
  Industry Automation
  Industrielle Kommunikation SIMATIC NET
  Postfach 4848
  D-90327 Nürnberg

有关 EC 符合性声明，请访问 Internet (http://support.automation.siemens.com/WW/view/zh/50302933) 上的以下地址/条目 ID

EMC 指令

上面列出的 SIMATIC NET S7 CP 旨在用于工业环境。

应用领域	要求	
	辐射	抗干扰
工业	EN 61000–6–4	EN 61000–6–2

防爆指令

符合 EN 60079（潜在易爆环境中的电气设备；防护类型“n”）

EN 60079-15，EN 60079-0

II 3 G Ex nA IIC T4 Gc

DEKRA 12 ATEX 0240X

说明

在危险区域（2 区）中使用（安装）SIMATIC NET 产品时，必须确保符合相关条件！
可在以下位置找到这些条件：

- 在 SIMATIC NET 手册集的
  “所有文档”(All Documents) > "Use of subassemblies/modules in a Zone 2 Hazardous Area"

针对澳大利亚的注意事项 - C-TICK

上面列出的 SIMATIC NET S7 CP 符合标准 AS/NZS 2064（A 类）的要求。

针对加拿大的注意事项

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.

UL 和 CSA 认证

说明

可通过铭牌上的标志确认产品通过的 UL/CSA 或 cULus 认证。

UL 认证

UL Recognition Mark Underwriters Laboratories (UL) nach Standard UL 508:

- Report E 85972

CSA 认证

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

- Certification Record 063533–C-000

cULus 认证，危险位置

CULUS Listed 7RA9 IND. CONT. EQ. FOR HAZ. LOC.

美国保险商实验室，符合

- UL 508（工业控制设备）
- CSA C22.2 No. 142（过程控制设备）
- ANSI ISA 12.12.01，CSA C22.2 No. 213-M1987（危险位置）
- CSA-213（危险位置）

授权使用在

- 1 类，2 分区。组 A、B、C、D T3...T6
- 1 类、2 区、组 IIC T3...T6

有关温度等级的信息，请参见模块铭牌。

⚠警告

爆炸危险 -

Do not disconnect while circuit is live unless area is known to be non hazardous.

Explosion Hazard -

Substitution of components may impair suitability for Class I, Division 2.

说明

This equipment is suitable for use in Class I, Division 2, Group A, B, C, D or non-hazardous locations only.

说明

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

说明

本设备必须依照 NEC（美国国家电气规程）的规定来安装。

在符合 I 类、2 分区的环境（见上文）中使用时，必须将 SIMATIC NET S7 CP 安装在机壳中。

FM 认证

美国工厂联研会许可标准类别号 3611，

I 类，2 分区，A、B、C、D 分组，T3...T6 或

I 类，2 区，IIC 组，T3...T6。

有关温度等级的信息，请参见模块铭牌。

⚠警告

可能导致人身伤害和财产损失。

在危险区域中，如果在 SIMATIC NET S7 CP 操作过程中连通或中断电路（例如，通过插入式连接、保险丝、开关），则可能导致人身伤害或财产损失。

警告 - 爆炸危险： 请勿在可燃或易燃环境中断开设备的连接。

在危险位置（2 分区或 2 区）使用时，必须将设备安装在机壳中。

索引