SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet SIMATIC CP 1545-1

操作说明

前言

应用和功能 1

LED，连接器 2

连接、安装、调试、拆卸 3

组态 4

程序块 5

诊断和维护 6

技术规范 7

认证 8

尺寸图 9

附加信息 A

Syslog 消息 B

06/2022

C79000-G8952-C499-03

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-C499-03
Ⓟ 05/2022 本公司保留更改的权利

Copyright © Siemens AG 2019 - 2022.
保留所有权利

前言

注意

为防止人员受伤，请在使用前阅读本手册。

本文档的有效性

本文档适用于下列产品：

- CP 1545-1
  订货号 6GK7545-1GX00-0XE0
  硬件版本 1
  固件版本 V1.1

  用于将 SIMATIC S7-1500 连接到工业以太网的通信处理器
  通信功能：TCP/IP、UDP、S7、FTP 客户端/服务器、电子邮件、通过 MQTT 连接到云系统



图 1　　带 CP 1545-1 (右) 的 S7-1500

文档用途

本文档介绍了设备的应用和属性，可在组态期间为用户提供支持，并展示了维护和诊断选项。

本版本新增内容

固件版本 V1.1，包含以下新功能：

- CloudConnect 功能得到改进，例如：
  - 将时间触发器与主题/组相关联。
  - 导出/导入有效载荷格式
- 运行期间可组态 CP 诊断，请参见“CP 诊断 (页 50)”部分。
- 可组态 UDP 缓冲区，请参见“设置 (页 45)”部分。

请注意下文中关于 DHCP 和 LLDP 的限制。

- DHCP 的特性 (页 48)
- 安全性 (页 53)

替换的版本

版本 12/2019

Internet 上的文档

如需本文档的最新版本，可在西门子工业在线支持的 Internet 页面上获取：
链接： (https://support.industry.siemens.com/cs/ww/zh/ps/25625/man)

所需经验

要安装、调试和操作设备，需要具备以下领域的经验：

- 通用电气工程
- 自动化工程 / STEP 7 Professional

有关本文档的说明

缩写与名称

- **CP/设备/模块**

  指代通信处理器 CP 1545-1

- **ES**

  工程师站 (STEP 7 Professional)

- **站**

  SIMATIC S7 站

- **STEP 7**

  表示组态工具 STEP 7 Professional

交叉引用

在本手册中，经常会交叉引用其它部分。要在跳转至交叉引用后返回原始页面，某些 PDF 阅读器支持 <Alt>+<左箭头> 命令。

搜索

为在列表中显示某一搜索术语的所有实例，一些 PDF 阅读器支持命令 <Ctrl>+<Shift>+<F>。

信息资源和其它文档

见下文的文档指南。

可在以下页面上找到 CP 的应用示例：
链接：（https://support.industry.siemens.com/cs/ww/zh/ps/25625/ae）

更多关于 S7-1500 的文献，请参见“文档指南”部分。

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_CP15451_99.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：(https://www.siemens.com/cert)

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。

固件/软件支持的说明

定期检查新固件/软件版本或安全更新并加以应用。新版本发布后，先前版本不再受支持，也不再进行维护。

文档指南

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　　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	系统诊断 (https://support.industry.siemens.com/cs/ww/zh/view/59192926)功能手册	• 概述 • 硬件/软件诊断评估
通信	通信 (https://support.industry.siemens.com/cs/ww/zh/view/59192925)功能手册	• 概述
	Web 服务器 (https://support.industry.siemens.com/cs/ww/zh/view/59193560)功能手册	• 功能 • 运行
	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	设计无干扰控制器 (https://support.industry.siemens.com/cs/ww/zh/view/59193566)功能手册	• 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

DVD 上的 CP 文档

有关产品和组态的文档，请参见“SIMATIC NET Manual Collection”或“SIMATIC Communication Products”DVD。此 DVD 包含截至产品手册创建时有效的手册。

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。

解除调试

正确关闭设备，以防止未经授权的人员访问设备内存中的机密数据。

为此，需要恢复设备的出厂设置。

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)

SIMATIC NET 词汇表

SIMATIC NET 词汇表描述了本文档中可能使用的术语。

要获取完整的 SIMATIC NET 词汇表，请访问西门子工业在线支持，网址为：

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

培训、服务与支持

有关培训、服务和支持的信息，请参见 Internet 上 Siemens Industry Online Support 页面中的多语言文档“DC_support_99.pdf”：

链接：(https://support.industry.siemens.com/cs/cn/zh/view/38652101/en)

目录

前言 **3**

1 应用和功能 **13**

1.1 应用 13

1.2 通信服务 13

1.3 云通信 15

1.4 其它功能 17

1.5 工业以太网安全 19

1.6 组态限制和性能数据 20
1.6.1 通信模块的组态限制 20
1.6.2 常规特性数据 20
1.6.3 特性数据 CloudConnect 21
1.6.4 S7 通信的特性 21
1.6.5 OUC 和 FETCH/WRITE 的特性数据 22
1.6.6 用于 FTP/FTPS 模式的特性数据 24
1.6.7 安全特性 - 防火墙规则 24

1.7 使用要求 25
1.7.1 可用的 CPU 25
1.7.2 CP 25
1.7.3 软件要求 26

2 LED，连接器 **27**

2.1 LED 27

2.2 千兆位接口 29

3 连接、安装、调试、拆卸 **31**

3.1 使用设备时的重要注意事项 31
3.1.1 有关在危险场所使用的注意事项 31
3.1.2 依据 ATEX / UKEX / IECEx / CCC-Ex 要求在危险区域使用的注意事项 32
3.1.3 依据 UL HazLoc 和 FM 要求在危险区域使用的注意事项 33

3.2 在危险区域安装、拆卸和维修 34

3.3 安装 35

3.4 连接 38

3.5 调试 - 下载组态数据 39

3.6 CPU 的工作模式：CP 的响应 40

3.7 拆卸 40
4 组态 41
4.1 安全建议 41
4.2 STEP 7 Professional 45
4.3 设置 45
4.4 限制 CPU 中的通信服务 46
4.5 IP 组态 48
4.5.1 DHCP 的特性 48
4.5.2 在网络中检测重复 IP 地址后重新启动 48
4.5.3 IP 路由 49
4.5.4 已编程的连接：防火墙规则的限制 50
4.6 DNS 组态 50
4.7 与 CPU 通信 50
4.7.1 CP 诊断 50
4.8 SNMP 52
4.9 安全性 53
4.9.1 安全用户 53
4.9.2 防火墙 53
4.9.2.1 检查到达帧和离去帧时的防火墙顺序 53
4.9.2.2 源 IP 地址的表示法（高级防火墙模式） 54
4.9.2.3 HTTP 和 HTTPS 不可使用 IPv6 54
4.9.2.4 防火墙激活情况下的在线安全诊断和下载到站设置 54
4.9.3 时钟同步 55
4.9.4 日志设置 - 过滤系统事件 56
4.9.5 VPN 56
4.9.5.1 在 S7-1500 站之间建立 VPN 隧道通信 58
4.9.5.2 在 CP 和 SCALANCE M 之间建立 VPN 隧道通信 60
4.9.5.3 与 SOFTNET Security Client 进行 VPN 隧道通信 60
4.9.5.4 CP 作为 VPN 连接的被动用户 61
4.9.6 在线功能 61
4.9.7 证书 61
4.9.7.1 第三方证书 61
4.9.7.2 证书管理器 62
4.9.7.3 处理证书 62
4.10 FTP 服务器组态 65
4.10.1 组态 FTP 服务器功能 65
4.10.2 FTP 组态列表的布局和结构 67
4.10.3 FTPS 访问 68
4.11 CloudConnect 68

4.11.1 组态云访问 68
4.11.1.1 组态概述 68
4.11.1.2 数据结构和组态的注意事项 69
4.11.1.3 组态规则 70
4.11.1.4 “CloudConnect”参数组 74
4.11.1.5 MindConnect IoT Extension 中的 Onboarding 78
4.11.1.6 操作数区域和变量 79
4.11.2 组态主题、组和数据点 80
4.11.2.1 组态主题或组 80
4.11.2.2 组态数据点 81
4.11.2.3 数据类型 83
4.11.2.4 触发 84
4.11.2.5 有效载荷格式 89
4.11.2.6 导入/导出有效载荷 94
4.11.3 主题的属性对话框 102
4.11.3.1 打开属性对话框 102
4.11.3.2 Quality of Service (QoS) 102
4.11.4 附加信息 103
4.11.4.1 连接中止和数据缓冲 103
4.11.4.2 JSON 转义序列 105
4.11.4.3 允许的字符 107

5 程序块 111

5.1 用于通信的程序块 111
5.2 在运行期间更改 IP 地址 116
5.3 FTP 客户端功能块 117
5.3.1 FTP_CMD 117
5.3.2 输入参数 - FTP_CMD 119
5.3.3 FTP_CMD 的作业块 121
5.3.4 输出参数和状态信息FTP_CMD 128
5.3.5 用于 FTP 客户端操作的数据块（文件 DB）的结构 132

6 诊断和维护 137

6.1 诊断 137
6.1.1 诊断方法 137
6.1.2 通过端口 8448 执行在线安全诊断 139
6.1.3 在线连接 139
6.1.4 使用 SNMP 进行诊断 140
6.2 维护 143
6.2.1 更新固件 143
6.2.2 在没有编程设备的情况下更换模块 146

7 技术规范 147

7.1 技术规范 147
7.2 以太网接口的引脚分配 148
7.3 允许的电缆长度 - 以太网 149
7.4 允许的电缆长度 - 千兆以太网 149
8 认证 151
9 尺寸图 157
A 附加信息 159
A.1 通过 FETCH/WRITE 链接到其它系统 159
B Syslog 消息 163
B.1 Syslog 消息的结构 163
B.2 Syslog 消息中的变量 165
B.3 消息 167
B.3.1 Non-repudiation 167
索引 169

1 应用和功能

1.1 应用

应用

CP 适合在 S7-1500 自动化系统中运行，允许 S7-1500 与工业以太网和云系统相连接。

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。

1.2 通信服务

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。

  有关块的信息，请参见"程序块 (页 111)"部分。

- **MQTT**

  MQTT 用于将 S7-1500 连接到云系统。有关通信功能和云系统的信息，请参见"云通信 (页 15)"部分。

- **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。

    有关块的信息，请参见"程序块 (页 111)"部分。

- **电子邮件**

  请参见上文 (OUC)。

- **HTTP/HTTPS**

  – CPU 的 Web 服务器：通过 HTTP/HTTPS 监视设备和过程数据

    如果不需要该功能，可以在 STEP 7 组态中禁用此功能并禁用端口 80（"访问 Web 服务器"(Access to the Web server) 参数组）。

- **FETCH/WRITE**

  通过 ISO 传输、ISO-on-TCP 和 TCP 连接实现 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。

有关组态通信功能的详细信息，请参见 STEP 7 帮助系统。

1.3 云通信

云连接的协议

CP 支持以下与云 broker 或云服务器通信的协议：

- MQTT

  根据 OASIS 标准版 3.1 / 3.1.1

云系统和通信功能

CP 可连接到支持具有 broker 功能与 MQTT 协议的云系统。

云访问的组态（“云运营商”）适用于与以下云系统的通信：

- MindSphere (Siemens)

  服务： MindConnect IoT Extension

  CP 的功能：

  – 发布方

- 其它云

  其它云系统的配置文件

  CP 的功能：

  – 发布方

  – 订阅者

    有关详细信息，请参见下文。

  可能的云系统包括：

  – AWS (Amazon)

    服务： IoT Core

  – Azure (Microsoft)

    服务： IoT Hub

  – IBM Cloud (IBM)

    服务： Watson IoT Platform

CP 的云通信功能

下表概括了手册印刷之时支持的各家云提供商支持的功能。

请咨询您的云提供商，以了解其支持的功能。

符号含义：

- **+**：支持
- **-**：不支持

功能	MindSphere (Siemens)	AWS (Amazon)	Azure (Microsoft)	IBM Cloud (IBM)
CP 的发布方功能	+	+	+	+
CP 的订阅方功能	-	-	-	+
QoS = 2	+			
通过 TLS 实现的 MQTT	+	+	+	+

CP 的通信伙伴

- Publisher

  发布方将数据发布给云代理。

  以下设备可与作为订阅者的 CP 一起（仅当通过"其他云"进行通信时）充当发布方：

  – CP 1545-1

  – 第三方设备

    第三方设备，其消息的组态和有效载荷格式与 CP 兼容。

- Subscriber

  订阅者登录云代理并订阅发布方的数据。

  以下设备可与作为发布方的 CP 一起充当订阅者：

  – CP 1545-1

    （仅用于通过"其它云"进行的通信）

  – 第三方设备

    第三方设备，其消息的组态和有效载荷格式与 CP 兼容。

有关通信处理器与第三方设备兼容性的详细信息，请参见"组态规则 (页 70)"部分。

安全通信证书 -

如果要使用安全的云通信，请在“安全性 > CloudConnect > 代理组态”(Security > CloudConnect > Broker configuration) 下选择“基于 TLS 的 MQTT”(MQTT over TLS) 选项。

在此参数组中，可以指定要使用的代理证书（之前已在全局安全设置中导入并分配给 CP 的证书）。

如果通过云与 CP 通信的伙伴 (Publisher / Subscriber) 需要使用证书进行安全通信，则在 CP 上使用“客户端证书”(Client certificate) 下拉列表中的伙伴证书。

有关组态的信息，请参见“”CloudConnect”参数组 (页 74)”。

1.4 其它功能

通过 NTP (Network Time Protocol) 进行时钟同步

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。

CP 支持通过 NTP (secure) 实现安全时间传输。

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 MIB 对象的内容。

安全功能激活时，CP 支持 SNMPv3。

IP 组态 (IPv4 / IPv6)

- 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分配给 CP，请参见“程序块 (页 111)”部分。不适用于 S7 连接。

IP 路由

CP 支持静态 IP 路由 (IPv4) 到其它 CM/CP。

有关详细信息，请参见“IP 路由 (页 49)”部分。

IPv6 地址 - 在 CP 上的用途

IPv6 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。可以为组态中的以太网接口激活“访问 Web 服务器”(Access to the Web server)。

阅读 Web 服务器的文档；请参见 前言 (页 3)，文档指南。

说明

通过 HTTPS 访问 Web 服务器

SIMATIC S7-1500 站的 Web 服务器位于 CPU 中。因此，在使用 CP 的 IP 地址对站的 Web 服务器进行安全 HTTPS 访问时，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。

1.5 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 41)”部分中的信息。

1.6 组态限制和性能数据

1.6.1 通信模块的组态限制

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通信模块数量取决于正在使用的 CPU 型号。

  通过运行多个 CM/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 CPU 文档中的信息，参见文档指南中的“前言 (页 3)”。

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。

1.6.2 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。

1.6.3 特性数据 CloudConnect

云的连接数

- **与 broker 的会话数量**

  最多 1 个会话

云连接的过程数据量

- **S7 CPU 数据区域中的变量**
  - 最多 500 个变量

主题/组的数量

- **可组态的主题或组的数量**
  - 最多 500 个

1.6.4 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

特性	说明/值
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。

1.6.5 OUC 和 FETCH/WRITE 的特性数据

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

特性	说明/值
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，参见文档指南中的“前言 (页 3)”。

UDP 的限制

- UDP 广播/组播

  为避免由于广播/组播帧流量较高而导致 CP 过载，可限制在 CP 上接收 UDP 广播/组播；参见“设置 (页 45)”部分。

- 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。

1.6.6 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。

1.6.7 安全特性 - 防火墙规则

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 14.90.120.0/16）
- 最多 128 个具有传输速度限制的规则

1.7 使用要求

1.7.1 可用的 CPU

以下 CPU 可用作通信模块的本地 CPU：

- 兼容的 CPU

  对于以下产品系列，可在固件版本 V2.1 及更高版本的 STEP 7 中组态所有 CPU：

  – 标准 CPU (CPU 15xx)

  – 紧凑型 CPU (CPU 15xxC)

例外

- 以下 CPU 不兼容：

  – H-CPU (CPU 1517H-x PN)

  – R-CPU (CPU 151xR-x PN)

说明

确保通信模块的固件为最新版本

为避免将版本较新的 CPU
与版本较旧的通信模块同时使用时时出现问题，应保证通信模块的固件为最新版本。
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/25625/dl)

1.7.2 CP

兼容的通信模块

CP 1545-1 可用于 CP 1543-1 或 CM 1542-1 旁边的机架。

CP 1545-1 不能用作 CP 1543-1 的替换件。

1.7.3 软件要求

用于实现组态和在线功能的软件

要组态和使用 CP 的全部功能，需要以下组态工具：

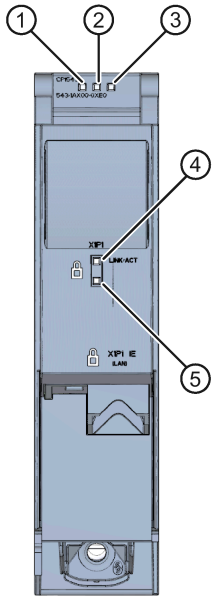
- STEP 7 Professional V17

LED，连接器

2

2.1 LED

LED



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

图 2-1 CP 1545-1 的 LED 指示灯（不带前盖）

LED 符号的含义

下表中的 LED 符号具有以下含义：

绿色 LED	红色 LED	黄色 LED	说明
□	□	□	LED 熄灭
■	■	■	LED 点亮（持续）
☼	☼	☼	LED 闪烁

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：下表列出了 LED 各种状态组合的含义。

表格 2- 1　LED“RUN”、“ERROR”、“MAINT”的含义

RUN（绿色）	ERROR（红色）	MAINT（黄色）	含义
□	□	□	CP 上无电源电压或电源电压过低
■	■	■	启动期间的 LED 测试
■	■	□	CP 启动
■	□	□	CP 处于 RUN 模式。无中断。
■	☼	□	发生了诊断事件。
■	□	■	要求维护
■	□	☼	下载用户程序
☼	□	□	• CP 组态丢失或不完整 • 正在加载固件
☼	☼	☼	模块故障 （LED 闪烁同步）

以太网接口 X1 P1 LED 指示灯的含义：

LED LINK/ACT（绿色/黄色）指示以太网接口的端口状态和活动：

表格 2- 2　“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 和通信伙伴之间无以太网连接 不通过以太网发送/接收数据
☼ 绿色闪烁	□ 黄灯熄灭	“LED 闪烁测试”，请参见 STEP 7 帮助（“硬件诊断”）
■ 绿灯点亮	□ 黄灯熄灭	连接到以太网 CP 和通信伙伴之间存在以太网连接
■ 绿灯点亮	■ 呈黄色闪烁	通过以太网发送/接收数据

2.2 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，请参见以太网接口的引脚分配 (页 148)部分。

连接、安装、调试、拆卸 3

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。

3.1 使用设备时的重要注意事项

3.1.1 有关在危险场所使用的注意事项

⚠警告

清洁外壳

- **在危险区域**

  只能用潮湿但不浸水的布来清洁外壳的外部。

- **在非危险区域**

  只能用干布来清洁外壳的外部。

不要使用任何液体或溶剂。

⚠警告

设备仅能在污染等级为 1 或 2 的环境中运行（如 EN/IEC 60664-1, GB/T 16935.1 中所述）。

⚠警告

电源

该设备专为在受限电源 (LPS) 提供的可直连安全超低电压 (SELV) 下工作而设计。

因此，电源需要满足至少以下条件之一：

- 只可将符合 IEC 60950-1/EN 60950-1/VDE 0805-1 或 IEC 62368-1/EN 62368-1/VDE 62368-1 的由受限电源 (LPS) 提供的安全超低电压 (SELV) 连接到电源端子上。
- 按照美国国家电气法规 (ANSI/NFPA 70)，设备的供电装置必须符合 NEC 2 类要求。

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。

⚠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。

3.1.2 依据 ATEX / UKEX / IECEx / CCC-Ex 要求在危险区域使用的注意事项

⚠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

机柜要求

为符合 EU 指令 2014/34 EU (ATEX 114)、UK Regulation SI 2016/1107 或者 IECEx 或 CCC-Ex 的条件，该机壳或机柜必须至少满足 EN IEC/IEC 60079-7 与 GB 3836.8 规定的最低 IP54（符合 EN/IEC 60529 与 GB/T 4208）要求。

⚠警告

DIN 导轨

在 ATEX、UKEX、IECEx 和 CCC-Ex 的应用领域中，仅可使用 Siemens DIN 导轨 6ES5 710-8MA11 来安装模块。

⚠警告

适用于危险区域中高环境温度的电缆

在环境温度 ≥ 60 °C 时，则选择可在至少高 20 °C
的环境温度中使用的专用耐高温电缆。外壳上使用的电缆入口必须符合 EN IEC/IEC 60079-0 与 GB 3836.1 要求的 IP 防护等级。

⚠警告

瞬态过电压

应采取措施以防止出现高出额定电压 40% 以上（或超过 119 V）的瞬态过电压。只有在使用 SELV（安全特低电压）操作设备时才会出现这种情况。

3.1.3 依据 UL HazLoc 和 FM 要求在危险区域使用的注意事项

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

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

在控制柜或外壳外进行墙式安装不满足 FM 认证的要求。

⚠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

如果将设备安装在机柜中，则机柜的内部温度与设备的环境温度要相对应。

⚠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 °C higher than maximum ambient temperature.

3.2 在危险区域安装、拆卸和维修

⚠警告

附件和备件不允许使用

危险区域中的爆炸风险

- 仅可使用原装附件和原装备件。
- 请遵循设备手册以及附件或备件随附的手册中介绍的所有相关安装和安全说明。

⚠警告

电缆或连接器不适用

危险区域中的爆炸风险

- 仅可使用符合相关防护类型要求的连接器。
- 如有必要，可按照指定的扭矩拧紧连接器螺钉连接、设备紧固螺钉、接地螺钉等。
- 使用未使用的电缆开孔进行电气连接。
- 安装后检查电缆是否牢固安装。

⚠警告

屏蔽电缆安装不当

存在因危险区域与非危险区域之间的均衡电流而引发爆炸的风险。

- 仅将穿过危险区域的屏蔽电缆一端接地。
- 两端接地时，布设等电位连接导线。

⚠警告

缺少等电位联结

如果危险区域中没有等电位联结，则存在因均衡电流或点火火花引发爆炸的风险。

- 确保为设备提供等电位联结。

⚠警告

电缆头未受保护

存在因危险区域中的电缆头未受保护而引发爆炸的风险。

- 按照 IEC/EN 60079-14 的规定对未使用的电缆头进行保护。

⚠警告

本安电路和非本安电路未充分隔离

危险区域中的爆炸风险

- 连接本安和非本安电路时，确保按照当地法规（例如 IEC 60079-14）正确执行电位隔离。
- 请留意您所在国家/地区适用的设备认证。

⚠警告

未授权对采用防爆设计的设备进行维修

危险区域中的爆炸风险

- 仅可由获得西门子授权的人员执行维修工作。

3.3 安装

注意

安装不当

安装不当可能导致设备损坏或危害设备操作。

- 安装设备之前，请务必确保设备没有可见损坏。
- 使用合适的工具安装设备。请留意关于安装的相应部分中的信息。

⚠警告

开放式设备

该设备为“open equipment”，符合标准 IEC 61010-2-201 或 UL 61010-2-201 / CSA C22.2
No. 61010-2-201。为符合关于机械稳定性、阻燃性、稳定性以及防接触保护的安全操作要求，下面指定了可选择的安装类型：

- 安装在合适的机柜中。
- 安装在合适的外壳中。
- 安装在配置适当的封闭控制室内。

安装

注意

仅在电源关闭后再安装和拆卸设备。

安装或拆卸模块之前，请关闭工作站的电源。在接通电源的情况下安装或拆卸模块可能导致模块损坏或数据丢失。

注意

安装位置 - 取决于温度范围

注意安装位置对所允许的温度范围的相关性：

- 水平安装机架（DIN 导轨）表示模块要垂直安装。
- 垂直安装机架（DIN 导轨）表示模块要水平安装。

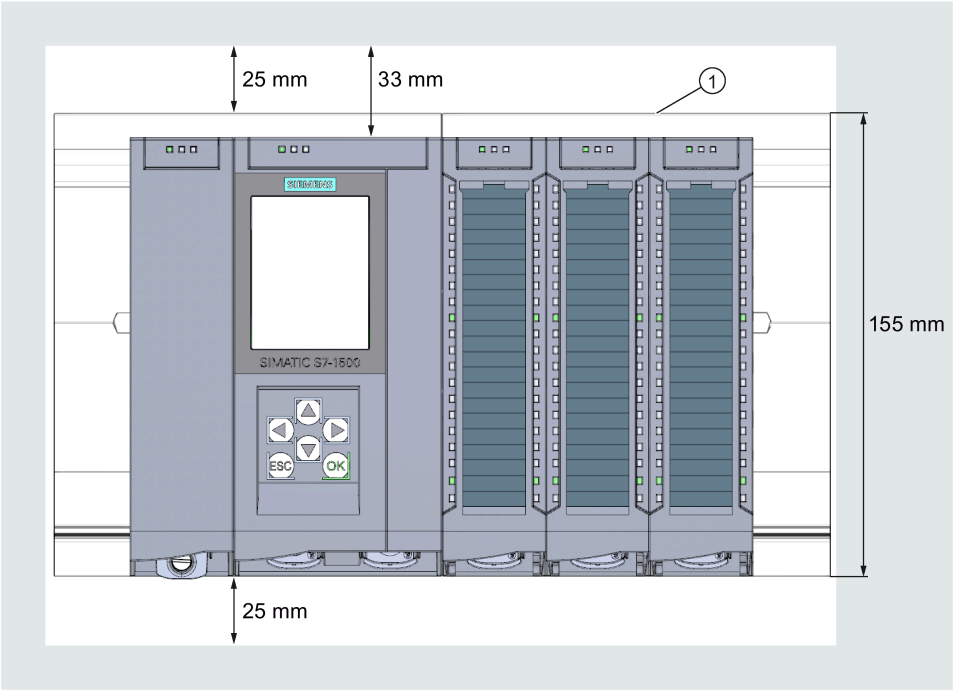
有关允许的温度范围的信息，请参见“技术规范 (页 147)”部分。

最小间隙

安装模块时，请勿遮盖其上下通风口，以确保充分通风，防止过热。

水平安装机架时，保持以下最小间隙，确保空气流通：

- 模块上方：至少 33 mm
- 模块下方：至少 25 mm



机架安装	模块安装位置
水平安装机架	
垂直安装机架	

⚠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，请参见 前言 (页 3)，文档指南。

操作步骤

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；参见 前言 (页 3)，文档指南。

3.4 连接

⚠警告

电源

该设备专为在受限电源 (LPS) 提供的可直连安全超低电压 (SELV) 下工作而设计。

因此，电源需要满足至少以下条件之一：

- 只可将符合 IEC 60950-1/EN 60950-1/VDE 0805-1 或 IEC 62368-1/EN 62368-1/VDE 62368-1 的由受限电源 (LPS) 提供的安全超低电压 (SELV) 连接到电源端子上。
- 按照美国国家电气法规 (ANSI/NFPA 70)，设备的供电装置必须符合 NEC 2 类要求。

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。

端子

⚠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，请参见 前言 (页 3)，文档指南。

电源断开

在连接设备时确保电源已关闭。

操作步骤

1. 通过 RJ-45 插座将 CP 连接到工业以太网（CP 底部）。

   关于以太网接口的引脚分配，请参见"以太网接口的引脚分配 (页 148)"部分。

2. 接通 S7 站的电源。
3. 关闭模块的前盖。

操作期间，请使铰接的前面板保持闭合状态。

3.5 调试 - 下载组态数据

要求：完成组态

仅当站的 STEP 7 项目数据完整时，才能完全调试 CP。

下载

调试的其余步骤涉及到下载 STEP 7 项目数据。

通过将组态数据下载到 CPU 来向 CP 提供相关组态数据。

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；要通过以太网加载站，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"

连接建立

如果使用 CP 进行云通信，并且 CP 的所有连接均已建立，则 CP 会在加载后自动与云建立连接。

3.6 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

3.7 拆卸

⚠警告

拆卸不当

拆卸不当可能导致危险区域中出现爆炸风险。

要正确拆卸，请遵循以下规则：

- 开始操作之前，确保电源已切断。
- 对剩余的连接采取相应安全措施，确保系统意外启动的情况下不会因拆卸而造成损坏。

组态

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：(https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security.html)
  - 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/25625/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。

  – 禁止访问 CPU 的 Web 服务器（CPU 组态）。

- 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 139)"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：

- 代理端口
  - 不受保护的 MQTT： 1883 (TCP)
  - 通过 TLS 实现的 MQTT： 8883 (TCP)

  可以在组态中设置端口号。
- 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）
- Syslog / 514 (UDP)

4.2 STEP 7 Professional

STEP 7 中的组态

在 STEP 7 Professional 中对 CP 进行组态。

有关所需 STEP 7 版本，请参见"软件要求 (页 26)"部分。

4.3 设置

FETCH/WRITE

可使用 FETCH/WRITE 服务访问 S7-CPU 中的系统存储区。

- FETCH：直接读取数据
- WRITE：直接写入数据

可从下列设备进行访问：

- SIMATIC S5
- SIMATIC PC 站
- 非 SIMATIC 设备

S7-1500 CP 是用于 FETCH/WRITE 服务的服务器。

以下协议支持 FETCH/WRITE 服务：

- TCP
- ISO-on-TCP
- ISO 传输

使用 FETCH/WRITE 服务时无需组态的连接。

CPU 组态要求

需要在 CPU 组态中启用 FETCH/WRITE 通信服务，请参见"限制 CPU 中的通信服务 (页 46)"部分。

系统存储器

可以使用 FETCH 或 WRITE 访问 S7-1500 CPU 的系统存储器中的下列操作数区域：

- 数据块 (DB)

  请注意以下内容：

  – 访问 DB 时，最大 DB 编号为 255。

  – 在 CP 的 TSAP 表中，激活用于访问 S5 或 S7 伙伴的"S7 寻址"(S7 addressing) 参数。

- 位存储器 (M)
- 过程映像输入 (PII)
- 过程映像输出 (PIQ)
- I/O 区域输入（PIW、PID、PIB）
- I/O 区域输出（PQW、PQD、PQB）
- 计数器 (C)
- 定时器 (T)

连接到非 SIMATIC 系统

FETCH/WRITE 服务可用于从任何非西门子设备访问 S7 系统存储器区。

例如，要对 PC 应用程序同样进行该类型的访问，需要了解作业的 PDU 结构。请参见附录 通过 FETCH/WRITE 链接到其它系统 (页 159)。

UDP 帧缓冲

禁用 UDP 数据报缓冲可防止模块过载。

禁用缓冲后，到达的 UDP 数据报如果在一个周期内未由用户程序获取，则将被丢弃。

4.4 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。

需要在 CPU 组态的以下位置为这些通信服务分配相应的权限：

- 参数组“保护和安全 > > 连接机制”(Protection & Security > Connection mechanisms)

  启用“允许来自远程对象的 PUT/GET 通信访问”(Permit access with PUT/GET communication from remote partner) 选项。

“允许来自远程对象的 PUT/GET 通信访问”(Permit access with PUT/GET communication from remote partner)

- 启用选项

  允许从客户端访问 CPU 数据。

  启用此选项的前提是在“访问级别”(Access level)
  参数组中启用访问选项。“无访问（完全保护）”(No access (complete protection))
  选项启用后，PUT/GET 通信也无法启用。

- 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

4.5 IP 组态

4.5.1 DHCP 的特性

说明

DHCP 不与 IPsec 搭配使用

“VPN (IPsec)”和“DHCP”功能都可以使用，但不能同时使用。

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。

DHCP：中止 ISO 传输连接

说明

通过 DHCP 获取 IP 地址时，如果因服务器暂时出现故障等情况导致 DHCP 服务器无法更新 CP 的 IP 地址，CP 会中止所有 ISO 传输连接。

4.5.2 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。

4.5.3 IP 路由

通过背板总线进行 IP 路由

此功能可通过背板总线在机架中的通信模块之间进行静态 Ipv4 路由。这意味着通过站的两个通信模块连接的两个子网之间的路由可通过站的背板总线进行操作。

以下模块支持此功能：

- CP 1545-1
- CM 1542-1

  固件版本 V2.0 及更高版本
- CP 1543-1
  - 固件版本 V2.0 及更高版本（禁用安全功能）
  - 固件版本 V2.1 及更高版本（启用安全功能）

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。

限制

不能通过站的 CPU 中的通信模块进行 IPv4 路由。

组态

可通过以下路径在 STEP 7 中搜索此功能：
"以太网接口 > 以太网地址 > 通信模块间的 IP 路由"

必须至少在站的 2 个模块中激活 IP 路由。

请注意：
如果希望使用 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。

4.5.4 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。

4.6 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 与 CPU 通信

4.7.1 CP 诊断

CP 诊断

通过 CP 诊断，可将 CPU 和 CP 某些功能的状态保存在 CPU 变量中，并将其用于其它平台和诊断用途。

诊断数据的最小更新周期为 1 秒。

- 启用高级 CP 诊断

  启用此选项便可使用以下诊断功能。

  如果启用该选项，则必须对“诊断触发变量”(Diagnostics trigger tag) 进行组态。

- 诊断触发变量

  如果 CPU 的用户程序将“诊断触发变量”(Diagnostics trigger tag) (BOOL) 设置为 1，则 CP 将更新用于高级诊断的已组态变量值。

  将当前值写入用于高级诊断的变量后，CP 会将“诊断触发变量”(Diagnostics trigger tag) 设为 0，指示 CPU 可以从变量中读取更新的值。

常规

- CPU 负载

  此变量 (Byte) 以百分比形式指定 CPU 处理器负载。

- 存储器资源

  此变量 (Byte) 以百分比形式指定 CP 工作存储器 (RAM) 的使用率。

CloudConnect

以下选项只能与 CP 的已启用 CloudConnect 功能搭配使用。

- 代理连接状态

  与代理建立连接后，此变量 (Bool) 设为 1。

  如果未建立连接，则值 = 0。

- 发送缓冲区使用情况

  此变量 (Byte) 以百分比形式指定消息缓冲区的分配。

  如果 CP 与 broker 之间的连接中断，则 CP 将帧保存在帧存储器中。

- CPU 采样错误

  此变量 (UDInt) 指定自上次复位诊断触发器变量起的扫描错误数。

  在组态的“扫描周期”内无法读取云通信的所有 DB
  变量的情况将计数，可能的原因有背板总线的通信负载偏高。

  如果有新的诊断请求（诊断触发器变量： 0 → 1），则计数器复位为零。

4.8 SNMP

SNMP

CP 支持以下 SNMP 版本：

- **SNMPv1**

  禁用了安全功能的情况下可用。

  注意，通过此协议可以实现对该模块的读写访问。在这种情况下，不能进行其它设置。

  只有在启用安全功能的情况下，才可以配置团体字符串。

  CP 使用以下团体字符串对通过 SNMPv1 访问其 SNMP 代理进行验证：

访问 CP 中的 SNMP 代理	**在 SNMPv1 中用于身份验证的团体字符串*)**
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，更改预设置和众所周知的字符串 "public" 和 "private"。

- **SNMPv3**

  仅当启用安全功能时可用

更多详细信息，请参见“使用 SNMP 进行诊断 (页 140)”部分。

组态

- **“启用 SNMP”**(Enable SNMP)

  如果启用该选项，则在 CP 上启用通过 SNMPv1 的通信。

  如果禁用此选项，则 CP 不会通过 SNMPv1 或 SNMPv3 应答来自 SNMP 客户端的查询。

4.9 安全性

说明

启用安全功能时将不发送 LLDP 帧
在启用安全功能时，即使 LLDP 模式已在 STEP 7 中启用，CP 也不会发送 LLDP 帧。

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 19)部分。

有关安全功能的组态限制，请参见安全特性 - 防火墙规则 (页 24)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 53)部分。

4.9.1 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">"用户"选项卡。

1. 创建用户并组态参数。
2. 在"分配的角色"下方区域为该用户分配角色"NET Standard"或"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。

4.9.2 防火墙

4.9.2.1 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 50)

4.9.2.2 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。

4.9.2.3 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。

4.9.2.4 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。

全局安全功能：

1. 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“Echo Reply”和一个类型为“Echo Request”的新条目。

CP 的本地安全功能：

现在选择 S7 站中的 CP。

1. 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。
2. 打开“IP 规则”(IP rules) 参数组。

3. 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：Accept；从：外部；至：站；服务 > ICMPv4/6 服务 > Echo Request（此前全局创建的服务）
   - 操作：Accept；从：站；至：外部；服务 > ICMPv4/6 服务 > Echo Reply（以前全局创建的服务）
4. 对于"Echo Request"服务的 IP 规则，在"源 IP 地址"(Source IP address) 下输入工程师站的 IP 地址。

基于这些规则，只能通过防火墙从包含 ICMP 数据包 (ping) 的工程师站访问 CP。

说明

在线安全诊断和下载的附加服务

如果希望使用"在线安全诊断"(Online security diagnostics) 或"下载到设备"(Download to device) 功能，则需要创建附加规则或禁用"Echo Request"/"Echo Reply"服务。

4.9.3 时钟同步

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

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，建议使用 NTP (secure) 方法。

同步方法

如果禁用安全功能，则 CP 支持 NTP 同步方法 (Network Time Protocol)。

如果已启用安全功能，则 CP 支持以下方法：

- NTP
- NTP (secure)

  在扩展 NTP 组态中，可以创建和管理其它 NTP 服务器。

有关组态的更多信息，请参见 STEP 7 在线帮助。

4.9.4 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。

4.9.5 VPN

说明

DHCP 不与 IPsec 搭配使用

“VPN (IPsec)”和“DHCP”功能都可以使用，但不能同时使用。

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

4.9.5.1 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。

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。
   已创建新的安全用户。现在，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。

结果

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。

4.9.5.2 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 58)”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。

4.9.5.3 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 58)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。

4.9.5.4 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”。

4.9.6 在线功能

4.9.7 证书

4.9.7.1 第三方证书

云提供商证书

要在 S7 站与代理之间进行加密通信（通过 TLS 实现的 MQTT），需要云提供商的 CA 根证书，还可能需要设备证书或私钥。

对不同云提供商的要求不同。

请从云提供商处获取所需文件，或访问其 Internet 页面下载。

有关所需文件和相关 Web 页面的说明，请参见 CP 的应用示例。在西门子工业在线支持的 Internet 页面中可找到此文档：
链接：(https://support.industry.siemens.com/cs/ww/zh/ps/25625/ae)

4.9.7.2 证书管理器

证书分配

如果使用需要 CP 身份验证的通信，则需要将通信伙伴的证书导入 STEP 7 项目，并将其与组态数据一起下载到 CP 中。

1. 使用全局安全设置中的证书管理器导入所有通信伙伴的第三方证书。
2. 然后将其所有通信伙伴的证书分配给 CP，或：
   - 使用全局安全设置中的“受信证书和根认证机构”(Trusted certificates and root certification authorities) 表
   - 使用模块（安全性）的本地证书管理器中的“伙伴设备的证书”(Certificates of the partner devices) 表

     该表还包括已在同一 STEP 7 项目中生成其证书的通信伙伴的证书。

有关操作步骤说明，请参见“处理证书 (页 62)”部分。

4.9.7.3 处理证书

验证证书

如果已为 CP 组态了需要身份验证的安全通信，则需要自己与通信伙伴双方的证书才能进行通信。

已启用安全功能的 STEP 7 项目的所有节点均由证书提供。STEP 7 项目是认证机构。

说明

安全功能被禁用时无证书。

如果在 STEP 7 项目中禁用了 CP 的安全功能，则不会为 CP 生成证书。

为请求证书的 CP 的每个应用程序创建证书。证书显示在 STEP 7 的“全局安全设置 > 证书管理器 > 设备证书”(Global security settings > Certificate manager > Device certificates) 中。除附加信息外，此处还提供相应证书的使用方法（服务/应用程序）。

可以通过在表中选择证书以及选择快捷菜单“显示”(Show) 来调用有关证书的更多信息。

启用安全功能后，CP 就可以与非 Siemens 伙伴进行通信，通信过程中必须交换伙伴的相关证书。要向 CP 提供第三方证书，请按以下步骤操作：

1. 从通信伙伴导入第三方证书

   ⇒ 项目的全局安全设置（证书管理器）

2. 分配证书，或：

   – 全局安全设置 > 证书管理器 > “受信证书和根认证机构”(Global security settings > Certificate manager > Trusted certificates and root certification authorities)

   – CP 的本地安全设置 > 证书管理器 > “伙伴设备的证书”(Local security settings of the CP > Certificate manager > Certificates of the partner devices)

以下部分介绍了这些步骤。

从通信伙伴导入第三方证书

使用 STEP 7 项目全局安全设置中的证书管理器导入第三方供应商的通信伙伴证书。请按照下面列出的步骤进行操作：

1. 将第三方证书保存到所连工程师站 PC 的文件系统中。
2. 在 STEP 7 项目中打开全局证书管理器：

   全局安全设置 > 证书管理器

3. 打开“受信证书和根认证机构”(Trusted certificates and root certification authorities) 选项卡。
4. 单击表中的行可选择快捷菜单“导入”(Import)。
5. 在打开的对话框中，将证书从工程师站的文件系统导入到 STEP 7 项目中。

在全局安全设置中分配证书

通过以下方式导入伙伴证书：全局安全设置 > 证书管理器 > 受信任证书（Global > security settings > Certificate manager > Trusted certificates） > 单击鼠标右键。然后将证书分配给 CP（选择证书 > 单击鼠标右键）。

1. 打开“受信证书和根认证机构”(Trusted certificates and root certification authorities) 选项卡。
2. 选择所需证书。

3. 在快捷菜单（点击鼠标右键）中选择“分配”(Assign)。
4. 在之后显示的对话框中，选择所需的模块。

   分配后，证书显示在模块的本地证书管理器中的“伙伴设备的证书”(Certificates of the partner devices) 表中。

本地分配证书

要为 CP 使用导入的证书，需要在 CP 的“安全”(Security) 参数组中显示相应证书。

该表还包括已在同一 STEP 7 项目中生成其证书的通信伙伴的证书。

请按以下步骤导入：

1. 在 STEP 7 项目中选择 CP。
2. 导航到参数组“安全 > 证书管理器”(Certificate manager)。
3. 在表中，双击具有条目“<新增>”的单元格。

   将显示“全局安全设置”(Global security settings) 的“证书管理器”(Certificate manager) 表。
4. 在表中，选择所需的第三方证书并单击表下方的绿色复选标记采用该证书。

   所选证书显示在 CP 的本地表中。

为第三方供应商应用程序（如记录服务器）导出证书

为与第三方供应商的应用程序通信，第三方应用程序通常也需要 CP 的证书。

采用与导入类似的方式，为来自第三方供应商的通信伙伴导出 CP 证书（见上文）。请按照下面列出的步骤进行操作：

1. 在 STEP 7 项目中打开全局证书管理器：

   全局安全设置 > 证书管理器
2. 打开“设备证书”(Device certificates) 选项卡。
3. 在表中选择具有所需证书的行，然后选择快捷菜单“导出”(Export)。
4. 将证书保存到所连工程师站 PC 的文件系统中。

现在可以将导出的 CP 证书传送到第三方供应商的系统中。

记录服务器的证书

如果在您的系统中使用了记录服务器，则导出服务器上用于 CP 验证的 SSL 证书。

更改证书：备用主题名

STEP 7 采用来自 STEP 7 组态数据中的"备用主题名"(SAN) 参数的"DNS 名称"(DNS name)、"IP 地址"(IP address) 和"URI"属性。

可以在全局安全设置的证书管理器中更改证书的这个参数。为此，请在设备证书表中选择证书，然后调用快捷菜单"更新"(Renew)。STEP 7 项目中未采在 STEP 7 中更改的"证书所有者的备用名称"(Alternative name of the certificate owner) 参数的属性。

4.10 FTP 服务器组态

4.10.1 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。

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：

- **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）。

有关文件 DB 结构的信息，请参见"用于 FTP 客户端操作的数据块（文件 DB）的结构 (页 132)"部分。

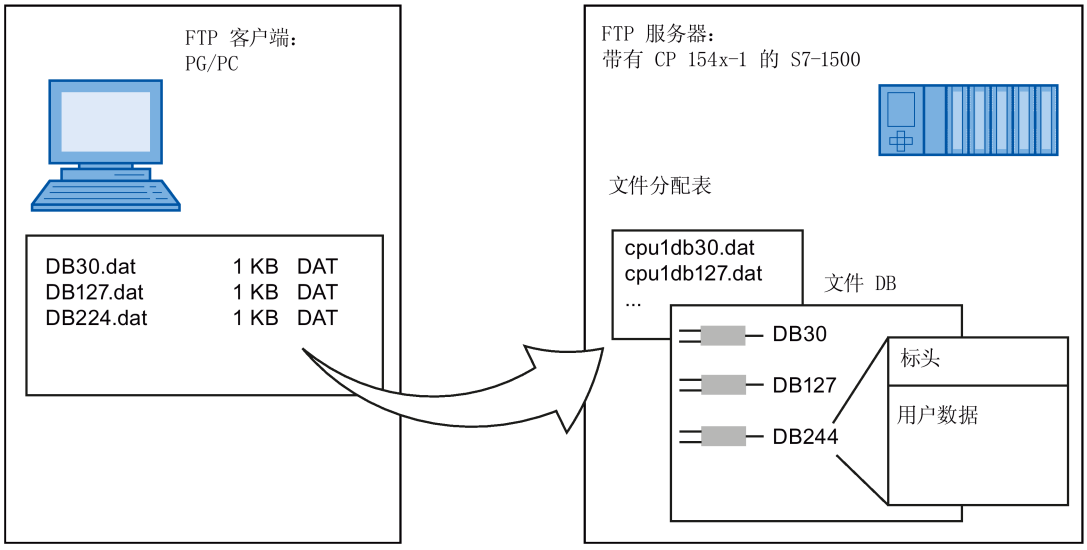


图 4-1 将配备 CP 154x-1 的 S7-CPU 作为 S7 CPU 数据的 FTP 服务器

4.10.2 FTP 组态列表的布局和结构

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”）

4.10.3 FTPS 访问

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。

4.11 CloudConnect

4.11.1 组态云访问

4.11.1.1 组态概述

组态云访问 - 概述

1. 要允许云应用程序访问过程映像，请在本地 CPU 中创建所需的 DB 和 DB 变量。

   主题/组的数据点（见下文）可访问这些 DB 变量；请参见“操作数区域和变量 (页 79)”部分。

2. 请在全局安全设置中至少创建一个角色为“NET Administrator”的用户。
3. 在参数组“安全”(Security) 下为 CP 启用“激活安全特性”(Activate security features) 选项。

4. 启用“激活 CloudConnect”(Activate CloudConnect) 选项，以实现 CP 的云通信功能。

   选择云提供商：

   – Siemens MindSphere - MindConnect IoT Extension

   – 其它云

   有关支持的云提供商，请参见“云通信 (页 15)”部分。

   组态其它参数；请参见““CloudConnect”参数组 (页 74)”部分。

5. 如果组态通过代理进行加密通信（通过 TLS 实现的 MQTT），则至少需要相关证书，并可能需要云提供商的密钥。

   请从云提供商处获取相关文件（也可访问其 Internet 页面获取），并将文件导入 STEP 7 项目和 CP。相关操作步骤，请参见“证书 (页 61)”部分。

6. 然后展开项目树：

   “站 > 本地模块 > CP 1545-1 > 云连接”(Station > Local modules > CP 1545-1 > Cloud connection)

   更多相关信息，请参见“组态主题或组 (页 80)”部分。

   创建组或主题。

7. 打开组或主题，插入数据点并进行组态。

8. 通过“属性”(Properties) 快捷菜单打开主题/组的属性对话框。

   – 组态主题/组的名称、“作者”和“注释”（后两项为可选项）。

   – 组态“所需的服务质量 (QoS)”(Required Quality of Service (QoS))。更多相关信息，请参见“Quality of Service (QoS) (页 102)”部分。

   – 如果需要，为组或主题组态时间触发器。

4.11.1.2 数据结构和组态的注意事项

数据结构

要访问云通信的过程数据，CP 需访问 CPU 的 DB 变量。DB 变量中引用的数据通过数据点在 CP 中进行组态。

针对不同的云提供商，将采用不同的数据结构来传送到代理：

- 其它云 (AWS / Azure / IBM Cloud)
  - 主题

    主题是用于传输一个或多个数据点值的通道。

    可创建多个主题。

    无法组态组。
- Siemens MindSphere - MindConnect IoT Extension
  - 组

    一个组可以包含一个或多个数据点。

    可创建一个或多个组。
  - 主题

    所有组都永久分配到 MindConnect IoT Extension 的标准主题“s/us”。

主题和组名

主题名称的组态：

- 对于云提供商 MindConnect IoT Extension，主题名称“s/us”为固定名称。
- 对于所有其它云提供商，主题名称可组态。

4.11.1.3 组态规则

组态规则

请遵循以下组态规则：

- **数据块**
  - 大小

    DB 中的变量数量不受限制。

    在创建数组时，只有最大元素数量 < 10000 的数组的元素/变量可以发布。

- **主题/组**
  - 数量

    每个 CP 的最大数量： 500
  - 名称

    在云应用程序中，主题名称必须唯一。

    这一点适用于所有相关发布方和订阅者。

    还应阅读"允许的字符 (页 107)"一节中的信息。
  - 大小

    主题或组可包含的数据点的数量还受到有效载荷总量的限制，具体参见下文。

  数据点
  - 数量

    每个 CP 的最大数据点数： 500

    每个主题/组的最大数据点数： 500

    主题或组可包含的数据点的数量还受到有效载荷总量的限制，具体参见下文。
  - 名称

    在主题中，数据点名称必须唯一。

    还应阅读"允许的字符 (页 107)"一节中的信息。

  有效载荷量
  - 每个主题/组的有效载荷总量

    最大 500000 Byte（相当于 500000 个 ASCII 字符）
  - 每个 CP 的有效载荷总量

    最大 500000 Byte（相当于 500000 个 ASCII 字符）

  配置中的有效载荷量取决于所使用的有效载荷格式。包含一个数据点且数据点名称长度为 21 个 ASCII 字符的标准有效载荷格式的大小如下：
  - JSON : 258 Byte
  - XML : 363 Byte
  - MindSphere - MindConnect IoT Extension : 160 Byte

  如果使用更长名称或更多代码组件（例如更多属性），则需要加上这些内容。

有效载荷量计算示例：
，数据点的有效载荷量为 500 个 ASCII 字符，每个主题有一个数据点，组态了 500 个主题，则有效载荷总量为 250000 字节。

注：
由于发布消息时会用数值代替变量，因此网络中的有效载荷量可能与配置中的有效载荷量不同。

用户一致性检查

说明

发布方和订阅者参数的一致性检查

如果作为订阅者的 CP
在运行时接收来自发布方的数据，则订阅者会在用户数据中针对接收到的每个值检查发布方提供的以下参数：

- 主题名称
- 数据点名称
- 数据类型

作为订阅者的 CP 不会评估发布方的站名称。

评估

一致性检查结果：

- 参数相同

  如果发布方提供的这三个参数与订阅者中组态的参数完全相同，并且消息的 QualityCode 为“GOOD”，则订阅者会将接收的数据写入其 CPU 数据块中。

- 参数不相同

  如果发布方提供的这三个参数中有一个或多个与订阅者中组态的参数不匹配，订阅者会丢弃该数据。

建议

在层级结构系统中传输数据时，一般建议根据此层级结构为组件命名。

如果所发布数据的名称参考了站的过程数据，则有利于后续对这些数据进行分配和评估。

示例：

- 主题/组名称

  假设要为组或主题“Motor5”命名，数据分配到 S7 站“Station1”。

  主题名称示例：

  “Station1_Motor5”

- 数据点示例

  “Plant1_Unit1_Aggregate1_DB_1_Signal1”

数据点和 DB

在云应用程序中，单独的发布方可向多个订阅者发布数据。各个订阅者可以订阅来自多个发布方的数据。

为了使数据更加一目了然并降低发生重名的概率，建议按照以下程序进行组态：

- 数据块

  在 CPU 中，仅为发布者功能和订阅者功能创建单独的 DB。

- 数据点名称/DB 编号

  如果使用数据点访问的数据块 (DB)
  的编号作为数据点名称的一部分，分配数据点会更加简单。

- 发布方

  – 针对每个订阅者，为作为发布者的 CP 创建一个单独的数据块。

  – 如果 CP
  订阅来自多个发布方的数据，则针对专用于此订阅（基于不同发布方）的相应 DB 组态一个不同的 DB 编号。

  如果数据点名称使用 DB
  编号作为名称的一部分，这可以防止来自不同发布方的变量具有相同的数据点名称。

- 订阅者

  针对每个发布方，为作为订阅者的 CP 创建一个单独的数据块。

  注释：
  订阅的数据只能写入数据块变量。对于更多执行动作，用户程序必须访问数据块变量。这可防止订阅数据在接收过程中直接更改过程映像。

所述建议并非强制要求，但可增加分配数据时的清晰度，并能够减少重名。

4.11.1.4 “CloudConnect”参数组

要求

组态云通信时要求激活安全功能。

请注意，如果稍后禁用安全功能，则除了数据点和主题或组之外，之前组态的所有云数据都将丢失。

常规

- **激活 CloudConnect**

  通过 CP 的以太网接口激活与云系统的通信。

- **云提供商**

  选择所需的云提供商：

  – Siemens MindSphere - MindConnect IoT Extension

  – 其它云（用于其它云系统的配置文件）

- **设备名称**

  有效性：仅限 MindConnect IoT Extension

  有关含义，请参见“MindConnect IoT Extension 中的 Onboarding (页 78)”。

  不要在名称中使用引号 (")；这会导致消息被发送两次。另请参见“允许的字符 (页 107)”。

- **变量扫描周期**

  查询 CPU 的 DB 变量的周期 (ms)。

  取值范围： 100..4294967295 ms

说明

传输的数据量

参数值会对传输的数据量产生直接影响。

当满足值触发器的触发条件时，数据将以每个变量的扫描周期传输到代理。另请参见“触发 (页 84)”部分中的说明。

数据丢失

如果组态的变量扫描周期非常短，同时组态的数据点数量非常多，则一些代理可能无法从云服务器的输入缓冲区读取所有已发布数据。

还需要注意帧存储器的功能，参见“连接中止和数据缓冲 (页 103)”部分。

- **带时间戳的主题**

  启用此选项后，会在每次发布时将当前时间戳添加至每个值。

代理组态

- **MQTT / 通过 TLS 实现的 MQTT**

  或者，也可以选择以下协议之一：

  – MQTT （未加密的传输）

  – 通过 TLS 实现的 MQTT（加密传输）

- **最低 TLS 版本**

  定义 CP 和伙伴使用的 TLS 版本。

- **代理证书**

  仅当启用加密传输"通过 TLS 实现的 MQTT"(MQTT via TLS)
  后，该参数才有效。在这种情况下，需要来自云提供商的证书。

  默认设置："自动"(Automatic)。通过"自动"(Automatic)
  设置，分配来自受信任证书的证书。

  要手动分配证书，请按以下步骤操作。

  – 导入伙伴证书：

    全局安全设置 > 证书管理器 > 受信任证书 (Global security settings > Certificate manager > Trusted certificates) > 单击鼠标右键

  – 将证书分配到 CP：

    在"受信任证书"(Trusted certificates) 列表中选择证书 > 单击鼠标右键

    证书随即显示在参数组"安全 > 证书管理器"(Security > Certificate manager) 中 CP 上的"伙伴设备的证书"(Certificates of the partner devices) 列表中。

  – 此时，在"代理证书"(Broker certificate) 下拉列表中选择导入的证书。

- **代理地址**

  代理服务器的地址（IPv4 地址或主机名）

- **代理端口**

  代理服务器的端口号

  – 端口 1883 预设用于未加密传输 (MQTT)。

  – 端口 8883 预设用于加密传输（通过 TLS 实现的 MQTT）。

- **客户端 ID**

  输入服务提供商分配的或用户定义的客户端 ID。

  ASCII 段中的最多 255 个字符（十六进制）0x20 .. 0x7F

- **客户端证书**

  CP 证书仅适用于安全的云通信（通过 TLS 实现的 MQTT）。

  如果 CP 的通信伙伴（云/Publisher / Subscriber）需要安全通信证书，则使用 CP 的证书。客户端证书将自动由 STEP 7 创建，供 CP 使用，并会显示在参数的输出域中。

  处理证书：

  只有在交换相应证书后才可进行安全通信：

  – 导出 STEP 7 项目或 CP 的证书

    对于待使用的 CP 证书，TIA 项目的 CA 证书必须导入到云服务器并作为受信的证书。为此，按照散列算法从全局安全设置中导出 CA 证书：
    “安全设置 > 安全功能 > 证书管理器 > 证书颁发机构 (CA)”(Security settings > Security features > Certificate manager > Certificate Authority (CA)) > 选择证书 > 快捷菜单“导出”(Export)。

    然后将证书传送到云服务器。

  – 导入通信伙伴的证书

    必须将通信伙伴的相应证书作为受信证书导入到 STEP 7 项目。为此，按以下步骤执行：

    将证书保存到 STEP 7 项目计算机的文件系统中。在全局安全设置中导入证书：
    “安全设置 > 安全功能 > 证书管理器 > 受信任的证书和根证书颁发机构”(Security settings > Security features > Certificate manager > Trusted certificates and root certification authorities) > 选择空白表格行 > 快捷菜单“导入”(Import)。

    具体步骤取决于所用的云。

    对于部分云，例如 AWS 等，必须将此证书作为设备证书分配给 CP。为此，按以下步骤执行：

– 将云证书分配到 CP（取决于云）

要求：已按上述方式将全局安全设置中的云证书导入。

在"受信任的证书和根证书颁发机构"(Trusted certificates and root certification authorities) 列表中选择证书，单击快捷菜单"分配"(Assign)
并在下一个对话框中选择 CP。

至此，证书显示在"伙伴设备的证书"(Certificates of the partner devices) 列表下 CP 的本地证书管理器中。

- **清理会话**

启用该选项后，将在终止连接时删除会话信息。

禁用该选项后，将在终止连接时保留会话信息。

说明

建议：启用"清理会话"(Clean session)

建议启用此参数。
如果组态的 QoS 值> 0，且"清理会话"(Clean session)
已禁用，在连接因确认处于未决状态而中止的情况下，会出现不确定的情况。

代理监视

- **保持连接间隔**

与代理之间连接的监视时间

如果在发送数据后的组态监视时间 内没有其它数据等待传输，或者 CP
未接收到代理发送的数据包，则 CP 会向代理发送保持连接数据包
(PINGREQ)，代理必须进行确认 (PINGRESP)。

请注意该参数对连接中止响应的影响，参见"连接中止和数据缓冲 (页 103)"部分。

调试后对值进行的更改将在下一次"下载到设备"之后生效。

代理验证

- **启用验证 (Enable authentication)**

  启用此选项后，会通过身份验证与代理建立连接。如果可能，请使用 TLS 传送用户名和密码。

  如果禁用此选项，则会匿名建立连接。

- **用户名** (User name)

  输入服务提供商分配的用户名或用户定义的用户名。

- **密码 (Password)**

  输入服务提供商分配的密码或用户定义的密码。

4.11.1.5 MindConnect IoT Extension 中的 Onboarding

Device 参数

连接到 Siemens MindSphere - MindConnect IoT Extension 时，在 CP 和 MindConnect IoT Extension 间建立连接后，在 Onboarding 过程期间将使用两个参数来识别设备。

- **设备名称 (Device Name)**

  CP 在 Onboarding 过程中使用此名称进行注册。

  设备名称显示在 MindConnect IoT Extension 的以下位置：
  Device > Device profile > "NAME"

  可以在 CP 的“安全 > CloudConnect > 常规” (Security > CloudConnect > General) 参数组中指定名称。

  默认名称的组成方式如下：
  <PLC 名称>.<CP 名称>

  不受允许的字符将从名称的组成部分中删除。注意指定名称的规则，请参见“允许的字符 (页 107)”。

- **设备类型 (Device Type)**

  此参数无法组态，可永久设置为以下字符串：

  – c8y_MQTTDevice

  MindConnect IoT Extension 中需要此参数来确定设备类型。

  设备类型显示在 MindConnect IoT Extension 的以下位置：
  Device > Device profile > "Type"

有关设置 IoT Extension 的更多信息，请访问以下 Internet 网址：
链接：(https://support.industry.siemens.com/cs/ww/zh/ps/25625)

4.11.1.6 操作数区域和变量

操作数区域

来自 CPU 的以下操作数区域的变量可用于传输 S7 站的数据：

- 数据块（全局 DB）

  在 DB 的属性对话框中组态时，请注意：

  – 启用“可从 OPC UA 访问 DB”(DB accessible from OPC UA) 属性。

组态 DB 变量

组态 DB 变量时选择以下选项：

- “可从 HMI/OPC UA 访问”(Accessible from HMI/OPC UA)
- “可从 HMI/OPC UA写入”(Writable from HMI/OPC UA)（写访问时需要选择此项）

有关可用于云连接的数据类型，请参见“数据类型 (页 83)”部分。

4.11.2 组态主题、组和数据点

4.11.2.1 组态主题或组

不同云运营商下的组态

通过选择云提供商，可以确定是否为数据传输组态主题或组。

- MindConnect IoT Extension

  可创建多个组。

  一个组可以包含多个数据点。

  在 IoT Extension
  中，组对应于结构特性“Series”。所有组都永久分配到标准主题“s/us”。

  在项目树中选择站并将其展开：

  “> 站 > 本地模块 > CP 1545-1 > 云连接 > 组”(Station > Local modules > CP 1545-1 > Cloud connection > Groups)

  单击“添加组”(Add group)。发布方组已创建，主题编辑器打开。

- 其它云

  可创建多个主题。

  一个主题可以包含多个数据点。

  在项目树中选择站并将其展开：

  “> 站 > 本地模块 > CP 1545-1 > 云连接 > 发布的主题 / 订阅的主题”(Station > Local modules > CP 1545-1 > Cloud connection > Published topics/Subscribed topics)

  请注意您的云提供商支持的功能（发布方 / 订阅者），参见“云通信 (页 15)”部分。

  单击“添加主题”(Add topic)。主题已创建，主题编辑器打开。

更多关于组或主题组态的信息，请参见“组态数据点 (页 81)”部分。

打开主题编辑器

按照以下方式打开主题编辑器：

1. 展开项目树：

   “站 > 本地模块 > CP 1545-1 > 云连接 > 发布的主题或组 / "订阅的主题”(Station > Local modules > CP 1545-1 > Cloud connection > Published topics or groups/Subscribed topics)

2. 可通过两种方式打开主题编辑器：
   – 双击“添加主题”(Add topic) 或“添加组”(Add group)”
   – 双击已有的主题或组

打开有效载荷编辑器

“主题编辑器”(Topic editor) 打开后，在右上角显示以下两个选项卡：

- “主题编辑器”(Topic editor)
- 有效载荷编辑器

可以单击对应选项卡以在这两个编辑器之间进行切换。

在“有效载荷编辑器”(Payload editor)
中，定义要发布的有效载荷的格式，参见“有效载荷格式 (页 89)”部分。

要在 STEP 7 之外编辑有效载荷格式，请参见“导入/导出有效载荷 (页 94)”部分。

说明

仅组态发布者的有效载荷格式
请注意，将只为已发布的数据组态有效载荷格式。

4.11.2.2 组态数据点

在主题/组中插入数据点

双击打开主题/组。

在主题或组中，单击表格第一个空行的“PLC 变量”(PLC tag) 单元格。

通过对象选择对话框，选择所需的 CPU DB 的 DB 变量。有关 DB
变量的信息，请参见“操作数区域和变量 (页 79)”部分。

DB 变量作为数据点传输到表中，属性和参数显示如下。

下表列出了可组态的所有数据点。

组态数据点

- **名称**

  数据点的组态名称

- **PLC 变量**

  DB 变量的组态名称

- **数据类型**

  数据点的组态数据类型

  有关支持的数据类型，请参见"数据类型 (页 83)"部分。

- **属性**

  ⇒ 有效性： MindConnect IoT Extension

  该属性作为 <ADDITIONAL_ATTRIBUTE> 应用到用户数据；请参见"有效载荷格式 (页 89)"部分。

  连接到 IoT Extension 后，属性可理解为相应数据点物理单位的标签。标准单位为：

  – C = 以摄氏度为单位的温度

  – P = 以巴为单位的压力

  – mm = 以米为单位的长度

  – km/h = 以 km/h 为单位的速度

  – m/s2 = 以 m/s^2 为单位的加速度

  – % = 以百分比为单位的大小

  – %RH = 以百分比为单位的相对湿度

  – A = 以安培为单位的电流

  – V = 以伏特为单位的电压

  – W = 以瓦特为单位的功率

  – kWh = 以千瓦时为单位的能量

  – VAh = 以伏安小时为单位的视在能量

  – dBm = 以分贝毫瓦为单位的发射功率（对数比）

  – lux = 以勒克斯 (lm/m^2) 为单位的照度

  也可以指定 SI 系统的其它复合单位，例如：

  m/h, m/s, m, km, mW, kW, mWh, mA, VArh

- **触发器**

  有关组态的信息，请参见"触发 (页 84)"。

4.11.2.3 数据类型

支持的数据类型

下表列出了可组态的数据类型。

如有需要，检查代理是否支持这些数据类型。

<DATAPOINT_TYPE> 表示发布时的数据类型。关于有效载荷和变量 <DATAPOINT_TYPE> 的发布，请参见"有效载荷格式 (页 89)"部分。

表格 4- 1　可用于云访问的数据类型

S7 数据类型（位）	<DATAPOINT_TYPE>	备注
BOOL (1)	BOOL	传输的值： 0, 1
BYTE (8)	UINT8	
CHAR (8)	CHAR	无 WCHAR
USINT (8)	UINT8	
INT (16)	INT16	
UINT (16)	UINT16	
WORD (16)	UINT16	
REAL (32)	SINGLE_FLOAT	
DWORD (32)	UINT32	
DINT (32)	INT32	
UDINT (32)	UINT32	
LREAL (64)	DOUBLE_FLOAT	
STRING (2..256 Char) *	S7_STRING *	无 WSTRING
DATE_AND_TIME (64) *	S7_DT *	
DTL (96) *	S7_DTL *	

* Siemens MindSphere 不支持

4.11.2.4 触发

传输数据的时间和数量

数据传输到云的要求

要传输一个值，必须满足以下条件：

- 数据点已分配给组态中的主题。
- 至少满足一个触发条件。

传输时间

使用"触发器"(Trigger) 指定将数据点的值传输到每个数据点的代理的时间。

组态值触发器和时间触发器时，两者具有同等权限。只要满足两个触发条件之一，就会触发传输。

传输的数据量

一旦数据点的值进入待传输状态，以下数据就会一起传输到代理：

- 其它云

  传输主题的所有数据点的值

- MindConnect IoT Extension

  传输组的所有数据点的值

传输持续时间（值触发）

说明

传输的数据量

请注意，所有触发器的设置都会影响传输的数据量。

值触发

只要满足触发条件，就会传输主题或组的数据。

值触发器 + 时间触发器

不同的值触发器和附加的时间触发器均会发起整个主题或组的传输。

说明

以“变量扫描周期”传输

当满足值触发器的触发条件时，数据将以每个变量的扫描周期传输到代理。

在参数组“安全 > CloudConnect > ”(Security > CloudConnect) 中组态 CP 上的“变量扫描周期”(scan cycle of variables)，参见“”CloudConnect”参数组 (页 74)”部分。

触发器

可使用触发指定开始将已保存的值传输到云或 broker 所需的条件。

提供以下触发器类型：

- **时间触发**

  时间触发器用于主题/组的所有数据点。

  时间触发器是在主题/组的属性对话框中组态的。

  可以使用以下类型的触发器：

  – 循环

  – 时间（每日 / 每周 / 每月）

  说明

  CP V1.0 迁移后的时间触发器

  当 CP 从固件版本 V1.0 迁移到固件版本 V1.1 之后，旧版项目中的时间触发器行为如下：

  在旧版本中组态的数据点的时间触发器会传输到采用 CP V1.1 的主题或组。如果在主题或组中组态了多个时间触发器，则会应用第一个发现的时间触发器。

- **值触发**

  可以为每个变量组态一个值触发器：

  可以使用以下类型的触发器：

  – 偏差（偏差传输）

  – 阈值下限 / 阈值上限

  – 范围内 / 范围外

  有关含义，请参见下文。

触发类型

时间触发

- 循环

  循环传输 - 在几毫秒内组态

  值循环传输。

- 每天一次

  值在每日的组态时间传送一次。

- 每周一次

  值每周传送一次。

- 每月一次

  值每月传送一次。

  注意：
  如果某个月份的天数少于组态的天数（例如第 31 天），则在月底不会传输任何值。

值触发

对于所有值触发器，请注意相应数据点的数据类型的取值范围。相应触发值是根据取值范围组态的。

- 偏差

  只要组态的值偏离了存储在 CPU 中的上一个值，就会立即传输该值。

  在发生以下情况时触发传输：

  – 新值 >（上次保存的值 + 正偏差）
  – 新值 <（上次保存的值 - 正偏差）
  – 新值 >（上次保存的值 - 负偏差）
  – 新值 <（上次保存的值 + 负偏差）

- 阈值下限

  低于组态值时立即传输值。

  在发生以下情况时触发传输：

  – 新值 < 组态的阈值下限

- 阈值上限

  高于组态值时立即传输值。

  在发生以下情况时触发传输：

  – 新值 > 组态的阈值上限

- 范围内

  在组态范围内时立即传输值。

  在发生以下情况时触发传输：

  – 范围下限 < 新值 < 范围上限

- 超出范围

  超出组态范围时立即传输值。

  在发生以下情况时触发传输：

  – 范围下限 > 新值

  – 范围上限 < 新值

值触发的取值范围取决于数据点的数据类型。

数据和触发类型

并非每种数据类型都支持所有触发类型。下表列出了可组态的数据类型，并为每种数据类型指定了支持的触发类型。

符号含义：

- **+**：支持
- **-**：不支持

表格 4- 2　数据类型支持的触发

S7 数据类型 类型（位/字节）	**支持的触发**	
	时间触发	**值触发**
Bool (1)	**+**	**x** (仅限值 0)
Byte (8)	**+**	**+**
Char (8)	**+**	**+**
USInt (8)	**+**	**+**

S7 数据类型 类型（位/字节）	支持的触发	
	时间触发	值触发
Int (16)	+	+
UInt (16)	+	+
Word (16)	+	+
Real (32)	+	+
DWord (32)	+	+
DInt (32)	+	+
UDInt (32)	+	+
LReal (64)	+	+
String (*2..256 Char*)	+	-
Date_And_Time (*8*)	+	-
DTL (*12*)	+	-

数据类型的取值范围

为数据类型"偏差"、"阈值下限""阈值上限"、"范围内"和"超出范围"组态阈值。

适用于阈值触发的最重要数据类型的取值范围如下：

- Bool: 0 / 1
- Byte: 0...255 / -128...+127
- Char: 0...255
- USInt: 0...255
- Int: -32768...+32767
- UInt: 0...65535
- Word: -32768...+32767 / 0...65535
- DInt: -2147483648...+2147483647
- UDInt: 0...4294967295
- DWord: -2147483647...+2147483647 / 0...4294967295
- Real: +1.175495e-38...+3.402823e+38
- LReal: +12.2250738585072014e-308...+1.7976931348623157e+308

S7 模拟量输入模块的值范围

值为正整数 (Int: 0...32767) 时，270 对应于 S7 模拟量输入模块原始值的 1% (27648 = 100%)。

4.11.2.5 有效载荷格式

固件版本 V1.0 与 V1.1 的 CP 之间的兼容性

如果使用固件版本为 V1.1 的 CP 的订阅方功能，则可使用固件版本为 V1.0 的 CP 的发布方数据 (JSON) 来订阅数据。

用户数据格式

不同的云系统使用不同格式来传输用户数据。CP 根据所连接的云系统（“云提供商”(Cloud provider) 参数）输出以下格式的用户数据：

- MindConnect IoT Extension

  MindSphere / IoT Extension (Siemens) 的格式

- JSON

  其它云的格式

  预期使用 JSON 格式处理主题的云服务。

- XML

  （未使用）

CP 使用 UTF-8 字符编码格式化用户数据。

有效载荷格式 "MindConnect IoT Extension"

```
200, "{{Pub_data point_1.NAME}}", "{{GROUP}}", "{{Pub_data
point_1.VALUE}}", "{{Pub_data point_1.ADDITIONAL_ATTRIBUTE}}",
"{{PUBLISH_TIMESTAMP}}"
```

有效载荷格式 "JSON"

```
{
    "Timestamp" : "{{PUBLISH_TIMESTAMP}}",
    "DataItems" : [
    {
        "Variable" : "{{Pub_data point_1.NAME}}",
        "Type" : "{{Pub_data point_1.TYPE}}",
        "Value" : "{{Pub_data point_1.VALUE}}",
        "QualityCode" : "{{Pub_data point_1.QUALITY_CODE}}"
    },
    {
        "Variable" : "{{Pub_data point_2.NAME}}",
        "Type" : "{{Pub_data point_2.TYPE}}",
        "Value" : "{{Pub_data point_2.VALUE}}",
        "QualityCode" : "{{Pub_data point_2.QUALITY_CODE}}"
    }]
}
```

代码组件

用于格式化用户数据的代码包含下面列出的组件。

对各个代码组件的结构描述如下所示：

- **代码组件**

  <Syntax>

  含义

  – 示例（不适用于所有组件）

代码组件：语法和含义

- **200**

  200

  函数代码 (MindConnect IoT Extension)

- **时间戳**

  {{PUBLISH_TIMESTAMP}}

  含义：发布时间

  – 示例：

    语法："{{PUBLISH_TIMESTAMP}}"
    字符串结果："2018-08-20T13:58:16.192313634+00:00"

- **数据点/变量**

  {{Pub_data point_n.NAME}}

  数据点名称

- **组**

  {{GROUP}}

  组名称 (MindConnect IoT Extension)

- **值**

  {{Pub_data point_n.VALUE}}

  数据点值

- **属性**

  {{Pub_data point_n.ADDITIONAL_ATTRIBUTE}}

  属性 (MindConnect IoT Extension)

- **数据类型**

  {{Pub_data point_n.TYPE}}

  设备输出的数据点的数据类型

  有关数据类型的输出，请参见“操作数区域和变量 (页 79)”部分。

- **QualityCode**

  {{Pub_data point_n.QUALITY_CODE}}

  值的质量状态

  有关含义，请参见下文。

有效载荷内容中不允许的序列

有效载荷内容中不允许下列序列：

- {{#
- {{^
- {{/
- {{>
- {{&
- {{{

已传输有效载荷示例 (JSON)

下面是主题传输的用户数据示例。

S7 站的主题包含数据点“DP1”、“DP2”和“DP3”的三个变量。

“DataItems”密钥的值是一个数组，其中含有这三个变量的对象。

```
{
   "Timestamp" : "{{PUBLISH_TIMESTAMP}}",
   "DataItems" : [
   {
      "Variable" : "{{DP1.NAME}}",
      "Type" : "{{DP1.TYPE}}",
      "Value" : "{{DP1.VALUE}}",
```

```
      "QualityCode" : "{{DP1.QUALITY_CODE}}"
    },
    {
      "Variable" : "{{DP2.NAME}}",
      "Type" : "{{DP2.TYPE}}",
      "Value" : "{{DP2.VALUE}}",
      "QualityCode" : "{{DP2.QUALITY_CODE}}"
    },
    {
      "Variable" : "{{DP3.NAME}}",
      "Type" : "{{DP3.TYPE}}",
      "Value" : "{{DP3.VALUE}}",
      "QualityCode" : "{{DP3.QUALITY_CODE}}"
    }]
}
```

转义序列

转义序列根据所用协议修改代码，可用来转换某些特殊字符。

以下名称组件中可能包含特殊字符，例如：

- 站名称
- 主题名称
- 组名称

CP 支持以下转义序列：

- JSON PubSub

  标准 JSON 转义序列

  有关使用的转义序列，请参见“JSON 转义序列 (页 105)”。

- XML

  标准 XML 转义序列

- CSV

  标准 CSV 转义序列

发布者将相应的特殊字符转换为转义序列。

对于订阅者，则将转义序列转换为反向序列。

QualityCode

传输与 QualityCode

数据点的"QualityCode"质量状态也随用户数据一起传输。该状态指示值的有效性。

该状态由作为发布方的 CP 设置，值范围如下：

- GOOD

  值有效。

- BAD

  变量的值无效或不是最新的。可能的原因：

  – CPU 处于 STOP 状态

  – 值不是最新的

  – 读取变量时出错

该状态的值会对传输产生以下影响：

- 发布方 → 云

  作为发布方的 CP 独立于该状态值发布消息。

- 云 → 订阅者

  作为订阅者的 CP 独立于该状态值接收消息。

  但是，当收到状态为"BAD"的消息时，作为订阅者的 CP 不会将该值写入 CPU。

4.11.2.6 导入/导出有效载荷

在 STEP 7 之外编辑有效载荷格式

如果要在 STEP 7 之外定义有效载荷的格式，或者要继续使用或编辑在 STEP 7 项目中定义的格式，可导入并导出格式。

可以通过 XML 格式导入/导出数据。

导出和导入有效载荷

先检查是否在 CP 的“CloudConnect”参数组中选择了正确的 cloud operator：

- 对于主题：其它云
- 对于组：Siemens MindSphere - MindConnect IoT Extension

请按以下步骤进行导出/导入：

1. 展开项目树：

   “站 > 本地模块 > CP 1545-1”(Station > Local Modules > CP 1545-1)

2. 选择“云连接”(Cloud connection) 条目。
3. 在快捷菜单中，单击“导出 CloudConnect 数据”(Export CloudConnect Data) 或“导入 CloudConnect 数据”(Import CloudConnect data)。

   用于导入或导出 *.XML 格式文件的窗口会打开。

注意：

- 如果忽略可选元素/属性，则将使用相应默认值。
- 如果 *.XML 文件包含无效条目，则将显示相应的错误消息。
- 只有已发布的主题（可能是订阅主题）或订阅的组可以存在。

  但不能同时导入或导出主题和组。

- 要将变量导入数据点，这些变量必须在目标设备的 CPU 中可用。

  如果在导入过程中未找到 XML
  文件中所含的变量名，则相应的字段将在导入后保留为空。为仍然能够使用数据点，必须为数据点选择一个变量。

说明

无语法检查

导入的用户数据文件未经过 STEP 7 或 CP
的语法检查。有语法错误时，将无法进行云通信。
如果自行编辑用户数据，务必确保语法准确。

XML 语法和允许的值

语法	元素/ 属性	允许的数据类型/取值范围	含义/说明
<PublishedGroups> 或 <PublishedTopics>			
<General Comment>	• Comment • Author • Name	• 字符串 • 字符串 • 字符串	• 可选 • 可选 • 必选
<QoS>		整型 / 0...2	可选
<TimeTrigger> <Cyclic> 或 <TimeTrigger> <Date>	• CycleTime • Frequency • TimeOfTheDay • Weekday • DayOfTheMonth	• 整型 / 10...4294967295 ms • 字符串 / Daily, Weekly, Monthly • 整型 / 0...1439 分钟 (00:00 ... 23:59) • 字符串 / Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday • 整型 / 1...31	• 必选，针对元素 TimeTrigger > Cyclic • 必选，针对元素 TimeTrigger > Date • 可选 • 可选 • 可选
<DataPoints> <DataPoint> <General Name> <DataPoints> <DataPoint> <General> <Tag>	• Name	• 字符串 • 字符串	• 必选 • 可选
<DataPoints> <DataPoint> <ValueTrigger>	• Type • Value • RangeLow • RangeHigh	• 字符串 / Deviation, Lower Threshold, Upper Threshold, Outside Range, Inside Range • 字符串 • 字符串 • 字符串	• 必选，针对元素 ValueTrigger • 可选 • 可选 • 可选

语法	元素/ 属性	允许的数据类型/取值范围	含义/说明
<Payload>	• Format • Customize	• 字符串 / XML, JSON, MindConnect IoT Extension, Custom • 布尔型 / true, false • <![CDATA[内容]]> 要允许内容，请参见"有效载荷格式 (页 89)"部分。	• 必选 • 可选 • 可选
<SubscribedTopics>			
<General>	• Comment • Author • Name	• 字符串 • 字符串 • 字符串	• 可选 • 可选 • 必选
<QoS>		整型 / 0...2	可选
<DataPoints> <DataPoint> <General> <DataPoints> <DataPoint> <General> <Tag>	• Name	• 字符串 • 字符串	• 必选 • 可选

包含示例值的 XML 结构

```
<?xml version="1.0" encoding="UTF-8"?>
<CloudConnectData>
  <PublishedTopics>
    <PublishedTopic>
      <General Name="Published Topic_1" Author="Ben Utzer"
                  Comment="My published topic"/>
      <QoS>1</QoS>
      <TimeTrigger>
        <Date Frequency="Daily" TimeOfTheDay="720"/>
      </TimeTrigger>
```

```
        <DataPoints>
          <DataPoint>
            <General Name="Published_datapoint_1">
              <Tag>"Data_block_1"."Enabled"</Tag>
            </General>
          </DataPoint>
          <DataPoint>
            <General Name="Published_datapoint_2">
              <Tag>"Data_block_1"."LastStatusMsg"</Tag>
            </General>
          </DataPoint>
          <DataPoint>
            <General Name="Published_datapoint_3">
              <Tag>"Data_block_1"."ErrorCount"</Tag>
            </General>
            <ValueTrigger Type="Deviation" Value="1"/>
          </DataPoint>
        </DataPoints>
        <Payload Format="XML" Customize="true">
          <![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<root>
    <!-- Custom plant identification number -->
    <MyCustomXMLTag>0123456789</MyCustomXMLTag>
 <DataItems>
  <DataItem>
   <Variable>{{Published_datapoint_1.NAME}}</Variable>
   <Type>{{Published_datapoint_1.TYPE}}</Type>
   <Value>{{Published_datapoint_1.VALUE}}</Value>
```

```
  </DataItem>
  <DataItem>
   <Variable>{{Published_datapoint_2.NAME}}</Variable>
   <Type>{{Published_datapoint_2.TYPE}}</Type>
   <Value>{{Published_datapoint_2.VALUE}}</Value>
  </DataItem>
  <DataItem>
   <Variable>{{Published_datapoint_3.NAME}}</Variable>
   <Type>{{Published_datapoint_3.TYPE}}</Type>
   <Value>{{Published_datapoint_3.VALUE}}</Value>
   <QualityCode>{{Published_datapoint_3.QUALITY_CODE}}</QualityCo
de>
  </DataItem>
 </DataItems>
</root>]]>
      </Payload>
    </PublishedTopic>
    <PublishedTopic>
      <General Name="Published Topic_2" Author="Ben Utzer"
                    Comment="Another published topic"/>
      <QoS>2</QoS>
      <TimeTrigger>
        <Cyclic CycleTime="500"/>
      </TimeTrigger>
      <DataPoints>
        <DataPoint>
          <General Name="Published_datapoint_1">
            <Tag>"Data_block_1"."Actuation_Speed"</Tag>
          </General>
```

```
            <ValueTrigger Type="Inside Range" RangeLow="150"
                        RangeHigh="300"/>
          </DataPoint>
          <DataPoint>
            <General Name="Published_datapoint_2">
              <Tag>"Data_block_1"."X-Position"</Tag>
            </General>
            <ValueTrigger Type="Outside Range" RangeLow="0"
RangeHigh="200"/>
          </DataPoint>
        </DataPoints>
        <Payload Format="XML"/>
      </PublishedTopic>
      <PublishedTopic>
        <General Name="Published Topic_3" Author="Ben Utzer"
                        Comment="Yet another published topic"/>
        <QoS>0</QoS>
        <TimeTrigger>
          <Date Frequency="Weekly" Weekday="Wednesday"/>
        </TimeTrigger>
        <DataPoints>
          <DataPoint>
            <General Name="Published_datapoint_1">
              <Tag>"Data_block_2"."ManufacturedItems"</Tag>
            </General>
            <ValueTrigger Type="Lower Threshold" Value="50"/>
          </DataPoint>
          <DataPoint>
            <General Name="Published_datapoint_2">
```

```
            <Tag>"Data_block_1"."RejectedQuality"</Tag>
          </General>
          <ValueTrigger Type="Upper Threshold" Value="3"/>
        </DataPoint>
      </DataPoints>
    </PublishedTopic>
  </PublishedTopics>
  <SubscribedTopics>
    <SubscribedTopic>
      <General Name="Subscribed Topic_3" Author="Ben Utzer"
                    Comment="My subscribed topic"/>
      <QoS>2</QoS>
      <DataPoints>
        <DataPoint>
          <General Name="Subscribed_datapoint_1">
            <Tag>"Data_block_2"."In_Storage"</Tag>
          </General>
        </DataPoint>
        <DataPoint>
          <General Name="Subscribed_datapoint_2">
            <Tag>"Data_block_2"."Required"</Tag>
          </General>
        </DataPoint>
      </DataPoints>
    </SubscribedTopic>
  </SubscribedTopics>
</CloudConnectData>
```

4.11.3 主题的属性对话框

4.11.3.1 打开属性对话框

在本地模块下的导航区域中打开 CP 时，可通过两种方式打开属性对话框：

- 通过快捷菜单选择主题/组时（右键单击）
- 当主题编辑器打开时，使用数据点表格上方的"属性"(Properties) 按钮

以下参数组可用：

- 常规
- Quality of Service (QoS)

  有关组态的信息，请参见和"Quality of Service (QoS) (页 102)"部分。
- 触发器

  时间触发器用于主题/组的所有数据点。

  有关时间触发器的组态，请参见"触发 (页 84)"部分。

4.11.3.2 Quality of Service (QoS)

- Quality of Service (QoS) 主题的属性

在本地模块下的导航区域中展开
CP，并通过快捷菜单打开主题的属性对话框时，可以访问该参数。

- **所需的服务质量 (QoS)**

  可在此定义该主题的传输行为 (Quality of Service)。

  如果可能，应由代理完成组态的值。如果所用代理不符合所需的 QoS 级别，则检查其执行的响应。在这种情况下，一些代理会选择最接近所需级别的级别。其它代理会输出错误消息。

  – QoS 0

    传输不超过一次

    CP 向 broker 发送一次主题。CP 不需要确认。

    如果 broker 未收到该主题，则该主题将丢失。

– QoS 1

至少传输一次

CP 将主题发送给 broker，直至收到来自 broker 作为确认的PUBACK 数据包。

– QoS 2

传输一次

CP 发送主题并等待，直到从指定的 broker 接收到两步确认。

此版本代表了最高的质量等级，但也与客户端以及服务器的最高管理负载相关。

默认设置： 0

4.11.4 附加信息

4.11.4.1 连接中止和数据缓冲

CP 对连接中止的响应

对连接中止的响应如下：

- **CP 与 CPU（CPU 处于 STOP 模式）之间的连接中止**
  – 连接中止期间：

    CP 发布含空字符串值和 QualityCode“BAD”的消息。

  – 连接恢复后：

    当满足触发条件时，CP 发布包含当前值和 QualityCode“GOOD”的消息。

- **CP 和云之间的连接中止 - CP 上的电缆拔出**
  – 连接中止期间：

    CP 不发布任何消息。

  – 连接恢复后：

    有关该行为的信息，请参见以下部分。

- **CP 和云之间的连接中止 - 云服务器不可访问**

  有关该行为的信息，请参见以下部分。

根据 QoS 值对连接中止作出响应

CP 对与云服务器的连接中止作出的响应取决于组态的 QoS 值。

- QoS = 0
  - 连接中止期间：

    CP 发布包含当前值的消息。

    每次发送消息后，CP 均会启动"保持连接时间间隔"，以监视与代理的连接。如果 CP 在该监视时间内未收到 CP 发送的数据包，则会向代理发送 PINGREQ 数据包。

    如果 CP 未收到代理发送的 PINGRESP 数据包，则将在 1.5 倍的保持连接时间间隔后终止连接。CP 随后会再次尝试建立连接。

    CP 不缓存任何已发布消息。
  - 连接恢复后：

    CP 发布包含当前值的消息。
- QoS = 1 / 2
  - 连接中止期间：

    CP 发布包含当前值的消息，并等待代理确认每条消息。代理确认后，CP 仅会将已发布消息从其发送缓冲区中删除。

    根据代理使用的 QoS 值，CP 会发送以下确认：

    - QoS = 1： PUBACK

    - QoS = 2： PUBREC + PUBREL

    如果 CP 未收到代理对最近发布的任何消息的确认（最多 16 条消息），则 CP 不会继续发送任何消息。

    如果 CP 在监视时间（保持连接时间间隔）内未收到代理发送的数据包，则会向代理发送 PINGREQ 数据包。如果 CP 未收到代理发送的 PINGRESP 数据包，则将在 1.5 倍的保持连接时间间隔后终止连接。CP 随后会再次尝试建立连接。
  - 连接恢复后：

    连接重新建立后，CP 会等待仍处于未决状态的确认。

    收到确认后，CP 会先发布帧存储器中的消息，然后再发布新累积的消息。

帧存储器中的数据缓冲

CP 将尚未发布的累积消息保存在其帧存储器中。帧存储器的容量为 3500 条消息。

帧存储器按时间顺序运行；换言之，首先发送最早的数据（FIFO 原则）。超出最大容量时，时间最早的消息会被覆盖。

4.11.4.2 JSON 转义序列

JSON 转义序列

对有效载荷使用 JSON 格式时，作为发布者的 CP 会将以下字符转换为转义序列。

对于作为订阅者的 CP，则将转义序列转换为反向序列。

字符	JSON 转义序列	说明
\n	\\n	新行 *
\r	\\r	换行符 *
\t	\\t	制表符 *
\"	\\"	引号
\\	\\\\	双反斜杠
\u0000	\\u0000	
\u0001	\\u0001	
\u0002	\\u0002	
\u0003	\\u0003	
\u0004	\\u0004	
\u0005	\\u0005	
\u0006	\\u0006	
\u0007	\\u0007	
\b	\\u0008	
\t	\\u0009	
\n	\\u000A	
\u000b	\\u000B	
\f"	\\u000C	
\r	\\u000D	

字符	JSON 转义序列	说明
\\u000e	\\u000E	
\u000f	\\u000f	
\u0010	\\u0010	
\u0011	\\u0011	
\u0012	\\u0012	
\u0013	\\u0013	
\u0014	\\u0014	
\u0015	\\u0015	
\u0016	\\u0016	
\u0017	\\u0017	
\u0018	\\u0018	
\u0019	\\u0019	
\u001a	\\u001a	
\u001b	\\u001b	
\u001c	\\u001c	
\u001d	\\u001d	
\u001e	\\u001e	
\u001f	\\u001f	
\u007F	\\u007F	

***** 在 STEP 7 中作为名称组件不可组态

4.11.4.3 允许的字符

名称中禁止使用的字符

不允许在名称中使用下列字符：

- 0x22 (")

  通常不允许使用引号。

- 0x20 (SP)

  大多数名称中都允许使用空格。例外情况：CloudConnect 数据点

  头尾的空格会被自动删除。

允许的字符

有关 ASCII 字符集，请参见下文。

参数	字符	字符数
以下内容的名称： • DB 变量 *	允许的字符： • 标准字符（数字、字母） • 特殊字符 0x21 .. 0x7E • 特殊字符 ≥ 0x80	
CloudConnect * • 数据点名称	允许的字符： • 标准字符（数字、字母） • 特殊字符 ≥ 0x80 • 特殊字符 0x21 .. 0x60 及例外情况 不允许使用以下字符： • 空格 • ! / . < > ^ \ # ! & = { } • Tab 制表符 也不允许下列字符串： • PUBLISH_TIMESTAMP • DATAPOINT_ARRAY • GROUP	

参数	字符	字符数
CloudConnect * • 主题名称 （不适用于组）	允许的字符： • 标准字符（数字、字母） • 特殊字符 ≥ 0x80 • 特殊字符 0x21 .. 0x7E 及例外情况 不允许使用以下字符： • # + / • 名称首字符 $	
CloudConnect * • 设备名称	允许的字符： • 标准字符（数字、字母） • 特殊字符 ≥ 0x80 • 特殊字符 0x60 • 特殊字符 0x21 .. 0x7E 及例外情况 不允许使用以下字符： • " ' /	1 ... 128
以下内容的名称： • NTP 服务器 • 主机 • S7 站、CPU、CP	RFC1035 和 RFC1123 的允许字符： • 标准字符（数字、字母） 不能使用只包含数字的站名称 • 0x2D (-) .. 0x2E (.)	
用户名、密码	允许的字符： • 标准字符（数字、字母） • 以下特殊字符： – 0x2D (-) – 0x2E (.) – 0x40 (@) – 0x5F (_)	

***** JSON 格式的云消息：JSON
标准的转义序列适用于站名称、主题名称和数据点名称中的特殊字符。

ASCII 字符集

下面列出的 ASCII 字符包含十六进制代码和相应字符。

标准字符

- **0x30 .. 0x39**

  0 1 2 3 4 5 6 7 8 9

- **0x41 .. 0x5A**

  A B C D E F G H I J KL M N O P Q R S T U V W X Y Z

- **0x61 .. 0x7A**

  a b c d e f g h i j k l m n o p q r s t u v w x y z

特殊字符 < 0x80

- **0x21 .. 0x2F**

  ! " # $ % & ' ( ) * + , - . /

- **0x3A .. 0x40**

  : ; < = > ? @

- **0x5B .. 0x60**

  [\ ] ^ _ `

- **0x7B .. 0x7E**

  { | } ~

特殊字符 ≥ 0x80 (ISO/IEC 8859-1)

- **0x80, 0x82 .. 0x89, 0x8A .. 0x8C, 0x8E, 0x91 .. 0x9C, 0x9E .. 0x9F**

  € , ƒ „ … † ‡ ˆ ‰ Š ‹ Œ Ž ‘ ’ “ ” • – — ˜ ™ š › œ ž Ÿ

- **0xA1 .. 0xAC, 0xAE .. 0xB5, 0xB8 ..0xBF**

  ¡ ¢ £ ¤ ¥ ¦ § ¨ © ª « ¬ - ® ¯ ° ± ² ³ ´ µ ¸ ¹ º » ¼ ½ ¾ ¿

- **0xC0 .. 0xFF**

  À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

程序块

5

5.1 用于通信的程序块

使用程序块

下面列出的程序块（指令）可用于 S7 站之间的通信。

未组态通过程序块进行通信。可组态的程序块可用作 STEP 7 用户程序中的接口。

有关程序块的详细信息，请参见 STEP 7 的信息系统。

建议：如果可能，请使用最新版本的模块。

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 Open User Communication (OUC) 的程序块

可在“指令 > 通信 > Open User Communication”(Instructions > Communication > Open User Communication) 任务卡中找到 STEP 7 中的程序块。

可使用以下块：

- **TSEND_C / TRCV_C**

  紧凑型块，用于：

  – 连接建立/终止和发送数据

  – 连接建立/终止和接收数据

使用替代块建立/断开连接，并使用单独的块来发送/接收数据：

- **TCON / TDISCON**

  建立连接/终止连接

- **TUSEND / TURCV**

  通过 UDP 发送和接收数据

- **TSEND / TRCV**

  通过 TCP 或 ISOonTCP 发送和接收数据

- **TMAIL_C**

  发送电子邮件

  要传送加密的电子邮件，CP 需要使用精准的时钟。组态时钟同步。

用于在运行期间更改 CP 组态数据：

- **T_CONFIG**

  IP 参数的程序控制组态

  有关 T_CONFIG 和 SDT 的信息，请参见"在运行期间更改 IP 地址 (页 116)"部分中的"IF_CONF_..."。

说明

CP 组态要求

为能够以程序控制方式更改 IP 参数，必须在组态 CP 以太网接口的 IP 地址时，启用"直接在设备上设置 IP 地址"选项。

CP 的 FTP 客户端块

可在"指令 > 通信 > 通信处理器 > SIMATIC NET CP"(Instructions > Communication > Communication processor > SIMATIC NET CP) 中找到 STEP 7 中的程序块。

- **FTP_CMD**

  FTP 客户端功能块

  设置 FTP 连接并与 FTP 服务器之间进行文件传输

  请参见"FTP 客户端功能块 (页 117)"部分中的相关说明。

系统数据类型 (SDT) 的连接描述

上述所列的块将 CONNECT 参数用于相关连接描述。

TMAIL_C 使用参数 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（全局 DB）形式的连接描述创建所需的 SDT。

SDT
类型不是通过从程序块声明表的"数据类型"下拉列表中选择一个条目进行创建，而是通过在"数据类型"框中手动输入名称（例如"TCON_IP_V4"）进行创建。随后，相应的 SDT 与其参数一并创建出来。

使用 SDT

- **TCON_IP_v4**

  基于 TCP 或 UDP 传送数据

- **TCON_QDN**

  通过完全限定域名 (FQDN) (IPv4 / IPv6) 进行 TCP 或 UDP 通信

- **TCON_Configured**

  用于通过组态的 TCP 连接传送数据

- **TCON_IP_RFC**

  基于 ISO-on-TCP 传送数据（两个 S7 站间直接通信）

- **TCON_ISOnative**

  用于通过 ISO 传输连接传送数据

- **TADDR_Param**

  基于 UDP 传送数据

- **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**

  如果要传送电子邮件，则使用其名称 (FQDN) 寻址电子邮件服务器

对于安全传输：

- **TCON_IP_V4_SEC**

  用于基于 TCP 或 UDP 安全传送数据

- **TCON_QDN_SEC**

  通过完全限定域名 (FQDN) (IPv4 / IPv6) 进行安全 TCP 或 UDP 通信

- **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 信息系统中相应名称下的内容。

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。

成功传送数据后可以终止连接。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。

程序块 - 概述

以下程序块（指令）可用于 CP。

表格 5- 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_Configured • TCON_QDN • TCON_IP_V4_SEC • TCON_QDN_SEC
ISO-on-TCP		• TCON_IP_RFC
ISO		• TCON_ISOnative
UDP	• TCON/TDISCON + TUSEND/TURCV	• TCON_IP_v4 • TCON_QDN • TADDR_Param • TCON_IP_V4_SEC • TCON_QDN_SEC
电子邮件	• TMAIL_C	• TMAIL_V4 • TMAIL_V6 • TMAIL_V6_SEC • TMail_FQDN • TMAIL_V4_SEC • TMAIL_QDN_SEC

表格 5- 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 5- 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

5.2 在运行期间更改 IP 地址

在运行时更改地址参数

可在运行时更改以下受程序控制的 CP 地址参数：

- IP 地址
- 子网掩码
- 路由器地址

可通过程序块支持受程序控制的 IP 参数更改。程序块访问以适当的系统数据类型 (SDT) 存储的地址数据。

除 CP 的地址参数外，使用 T_CONFIG 还可以通过程序控制来更改 DNS 服务器 (IF_CONF_DNS) 和 NTP 服务器 (IF_CONF_NTP) 的地址参数。

可以使用以下程序块和系统数据类型：

- **T_CONFIG**

  与 SDT：

  – IF_CONF_V4

  – IF_CONF_V6

  – IF_CONF_MAC

  – IF_CONF_DNS

  – IF_CONF_NTP

  组态的地址参数在 CP 中只能是暂时有效。在相应的“IF_CONF_...”SDT 中，必须设置 "Mode" = 2 参数。

说明

不支持来自 CP 的反馈

"T_CONFIG"不支持 CP 对 CPU
的反馈。块调用或设置地址参数时出现的错误不会报告。无论是否已设置地址参数，块都输出"BUSY"或"DONE"。

有关块编程的详细信息，请参见 STEP 7 信息系统。

CP 组态要求

为能够更改程序控制的 IP 参数，必须在组态 CP 以太网接口的 IP
地址时，启用"直接在设备上设置 IP 地址"(IP address is set directly at the device) 选项。

5.3 FTP 客户端功能块

5.3.1 FTP_CMD

FTP_CMD

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。

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。

说明

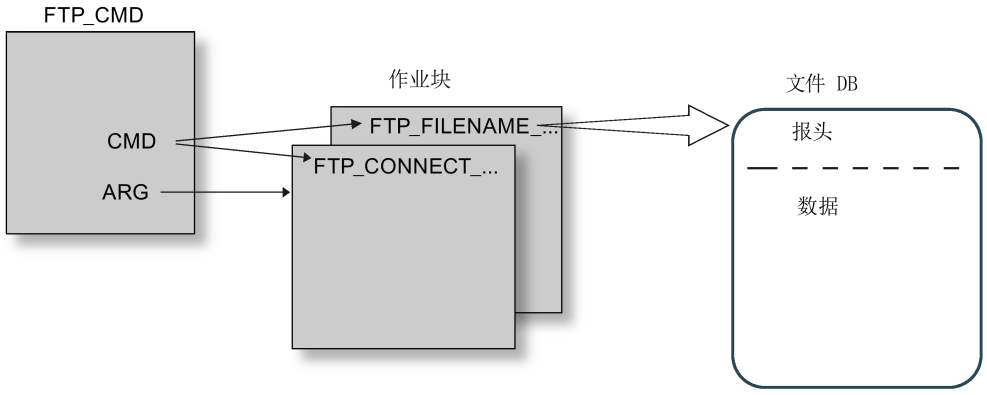
FTPS：比较证书

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

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

文件 DB 中的数据传输

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。

5.3.2 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 5- 4 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 5- 5　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。

5.3.3 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 5- 6　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 119)"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 5- 7　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 119)”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 5- 8　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 119)”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 5- 9　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 119)”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 5- 10　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 119)"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。

参数	类型	取值范围	含义/说明
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。
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。

5.3.4 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 5- 11　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。

DONE	ERROR	STATUS	含义
0	1	8405H	传送失败。
0	1	8406H	当前操作超时
0	1	8407H	FTP 服务器上未找到文件。
0	1	8408H	无法传送。
0	1	8409H	无法获取文件。
0	1	8410H	数据连接的 TCP 端口设置失败。
0	1	8411H	偏移量信息不匹配。
0	1	8412H	更改指定目录时出错
0	1	8413H	接收数据时出错
0	1	8414H	发送数据时出错
0	1	8415H	客户端拒绝指定 CMD（命令类型）。
0	1	8416H	FTP 服务器已关闭连接。
0	1	8418H	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	8419H	没有套接字资源可用来打开数据连接。
0	1	8420H	没有套接字资源可用来打开控制连接。
0	1	8421H	打开要读取的文件 DB 时出错
0	1	8422H	打开要写入的文件 DB 时出错
0	1	8423H	无法与 FTP 服务器建立连接。
0	1	8424H	内部错误
0	1	8425H	域名格式错误
0	1	8426H	未决的 DNS 查询过多。
0	1	8427H	指定的 DNS 服务器无法分配指定的域名。
0	1	8428H	没有可用的连接资源。
0	1	8429H	未知通道 ID
0	1	8430H	文件 DB 过短。
0	1	8431H	写入到文件 DB 时出错。

DONE	ERROR	STATUS	含义
0	1	8432H	从文件 DB 读取时出错。
0	1	8433H	访问文件 DB 时出错。
0	1	8434H	操作中止。
0	1	8435H	通道将复位。
0	1	8436H	意外的服务器应答
0	1	8437H	无法验证证书。
0	1	8438H	发生未知错误。
0	1	8439H	FTP 命令导致错误。必须在 FTP 服务器上查找原因（REST 命令）。
0	1	8440H	FTP 服务器不支持请求的 SSL 协议。
0	1	8446H	FTP 密码发送到 FTP 服务器后，FTP 服务器返回了一个意外代码。
0	1	8451H	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	8455H	CM/CP 上的存储器请求失败。
0	1	8460H	处理 SSL/TLS 时出现问题。
0	1	8469H	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	8475H	SSL 证书或 SSH md5 指纹未被视为可信。
0	1	8476H	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	8477H	未找到指定的"加密引擎"（加密模块）。
0	1	8478H	将所选 SSL"加密引擎"设置为默认值的尝试失败。
0	1	8480H	FTP 客户端的证书出现问题。
0	1	8481H	无法使用指定的编号。
0	1	8482H	FTP 服务器使用了不受支持的编码。
0	1	8484H	超出了最大文件大小。
0	1	8485H	文件 DB 在处理成待发送时被修改或文件 DB 的结构错误。

DONE	ERROR	STATUS	含义
0	1	8489H	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	8492H	文件已经存在。文件不会被覆盖。
0	1	8496H	读取 SSL CA 证书时出现问题。
0	1	8497H	SSH 会话出现意外错误。
0	1	8498H	无法终止 SSL 连接。
0	1	8499H	套接字未准备好发送/接收。请等待至就绪，然后重试。
0	1	8501H	FTP 服务器执行的 SSL 证书检查失败。
0	1	8507H	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	8F54H	文件 DB 标题中的“EXIST”位未置位。
0	1	8F55H	标题状态位：已锁定
0	1	8F56H	复位文件DB标题中的NEW位未复位。
0	1	8F6BH	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	8F7FH	内部错误；例如非法 ANY 引用。

5.3.5 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。

参数	类型	数值/含义	电源
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
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。

参数	类型	数值/含义	电源
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）。

诊断和维护

6

6.1 诊断

6.1.1 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 27)部分。

运行期间的 CP 诊断

通过组态，可允许向 CPU 变量中写入诊断信息；参见“CP 诊断 (页 50)”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 143)”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 139)”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，请参见文档指南中的“前言 (页 3)”。

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 140)部分。

6.1.2 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：

- 激活防火墙后，必须启用访问权限。

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”快捷菜单。
3. 在“安全性”参数组中，单击“在线连接”按钮。

这样，即可通过端口 8448 执行安全诊断。

有关详细信息，请参见“防火墙激活情况下的在线安全诊断和下载到站设置 (页 54)”部分。

6.1.3 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 61)

6.1.4 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 6- 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"。

6.2 维护



⚠小心

表面高温

对表面温度超过 70 °C (158 °F) 的部件执行维护作业期间存在灼伤风险。

- 请采取适当的防护措施，比如佩戴防护手套。
- 维护作业完成后，请恢复触点防护措施。

⚠警告

清洁外壳

- **在危险区域**

  只能用潮湿但不浸水的布来清洁外壳的外部。
- **在非危险区域**

  只能用干布来清洁外壳的外部。

不要使用任何液体或溶剂。

⚠警告

未授权对采用防爆设计的设备进行维修

危险区域中的爆炸风险

- 仅可由获得西门子授权的人员执行维修工作。

6.2.1 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/25625/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（“固件更新程序”(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》，参见文档指南中的“前言 (页 3)”。

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 27)”部分。

6.2.2 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

7

7.1 技术规范

技术规范 - CP 1545-1		
订货号	6GK7545-1GX00-0XE0	
工业以太网连接		
数量	1 个千兆位接口 (X1 P1)	
设计	RJ-45 插头，光电隔离	
属性		
• 标准	• 1000BASE-T, IEEE 802.3ab	
• 传输速度	• 10 / 100 / 1000 Mbps	
• 其它属性	• 半双工/全双工，自动跨接，自动协商	
电源		
设计	通过 S7-1500 背板总线 (15 V)	
更多电气数据		
电流消耗（典型值）	S7-1500 背板总线 300 mA	
有效功耗（典型值）	4.5 W	
绝缘	经测试达到：	DC 780 V (type test)
符合 IEC/EN 60664-1 的过压类别	类别 II	
允许的环境条件		
环境温度	导轨水平安装的运行期间	0 °C ... +60 °C
	导轨垂直安装的运行期间	0 °C ... +40 °C
	存储期间	-40 °C ... +70 °C
	运输期间	-40 °C ... +70 °C
相对湿度	运行期间	25 °C 时 ≤ 95 %，无冷凝
允许的污染物浓度	按照 ISA-S71.04 severity level G1, G2, G3 进行的腐蚀性气体测试	
	• SO_2	• < 0,5 ppm
	• H_2S	• < 0,1 ppm

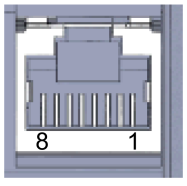
技术规范 - CP 1545-1	
设计、尺寸和重量	
模块规格	紧凑型模块 S7-1500，单宽度
防护等级	IP20
重量	320 g
尺寸 (W x H x D)	35 x 147 x 129 mm
安装类型	S7-1500 标准导轨安装

更多数据，请参见"应用和功能 (页 13)"部分和《S7-1500 系统手册》，可在 前言 (页 3)，文档指南中查找该文档。

7.2 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

7.3 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)

7.4 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

8

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)

Internet 上的文档

有关下列符合性声明以及产品证书，请访问以下 Internet 地址：
链接：(https://support.industry.siemens.com/cs/ww/zh/ps/25625/cert)

可在相关证书中找到标准的当前版本，有关证书的信息，请访问上述 Internet 地址。

符合性声明地址

EU 和 UK 符合性声明适用于以下区域的所有主管部门：

Siemens Aktiengesellschaft
Digital Industries
P.O.Box 48 48
90026 Nuremberg
Germany

EC 符合性声明



CP
满足以下欧盟指令的要求和安全目标，并符合欧盟公文中有关可编程控制器的欧洲协调标准 (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

UK 符合性声明



Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

产品满足以下指令的相关要求：

- UKEX Regulations

  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.

- EMC Regulations

  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

- RoHS Regulations

  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX / IECEx / UKEX / CCC-Ex

注意文档"Use of subassemblies/modules in a Zone 2 Hazardous Area"中的信息，文档位置如下：

- 在产品随附的文档 DVD 中的：
  "所有文档">"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- Internet 地址：
  链接：(https://support.industry.siemens.com/cs/ww/zh/view/78381013)

必须满足"依据 ATEX / UKEX / IECEx / CCC-Ex 要求在危险区域使用的注意事项 (页 32)"部分中的相关条件，才能安全使用本产品。

产品满足下列防爆保护要求。

IECEx

分类： Ex ec IIC T4 Gc，证书编号： IECEx DEK 18.0019X

产品满足以下标准的要求：

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

ATEX

分类： II 3 G Ex ec IIC T4 Gc，证书编号：DEKRA 18ATEX0027 X

产品满足以下标准的要求：

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

UKEX

分类： II 3 G Ex ec IIC T4 Gc，证书编号：DEKRA 21UKEX0003 X

产品满足以下标准的要求：

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

Importer UK: Siemens plc (请参见上文)

CCC-Ex

分类：Ex na IIC T4 Gc，证书编号：2020322310002625

产品满足以下标准的要求：

- GB 3836.1

  危险区域 - 第 0 部分：设备 - 常规要求

- GB 3836.8

  爆炸性气体环境 - 第 15 部分：保护类型"n"的设备保护

EMC

CP 满足以下指令的相关要求：

- EU 指令 2014/30/EU"电磁兼容性"（EMC 指令）
- EMC Regulations SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

应用标准：

- 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

- 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

RoHS

CP 满足以下指令的相关要求：

- EU 指令 2011/65/EU 对电气和电子设备中特定危险物质的使用限制。
- SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

应用标准：EN IEC 63000

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:请参见模块铭牌上的温度等级信息

Report / UL file: E223122 (NRAG, NRAG7)

注意，需满足链接：(https://support.industry.siemens.com/cs/ww/zh/view/78381013)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

A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 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。

关税同盟标志

EAC (Eurasian Conformity)

俄罗斯、白俄罗斯、亚美尼亚、哈萨克斯坦和吉尔吉斯斯坦的欧亚经济联盟

基于关税同盟技术规范的符合性声明 (TR ZU)

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/25625/cert)

尺寸图

9

尺寸图中所有尺寸均以毫米为单位。

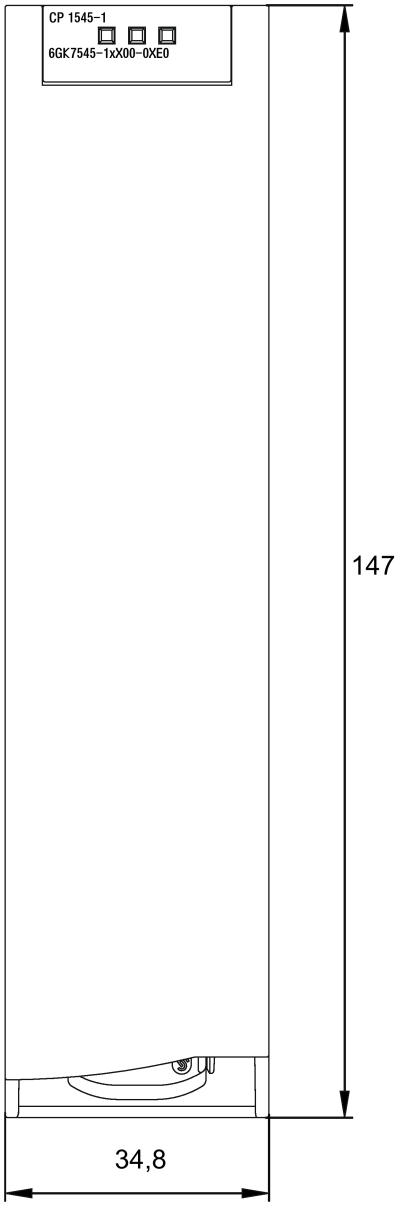


图 9-1　　正视图

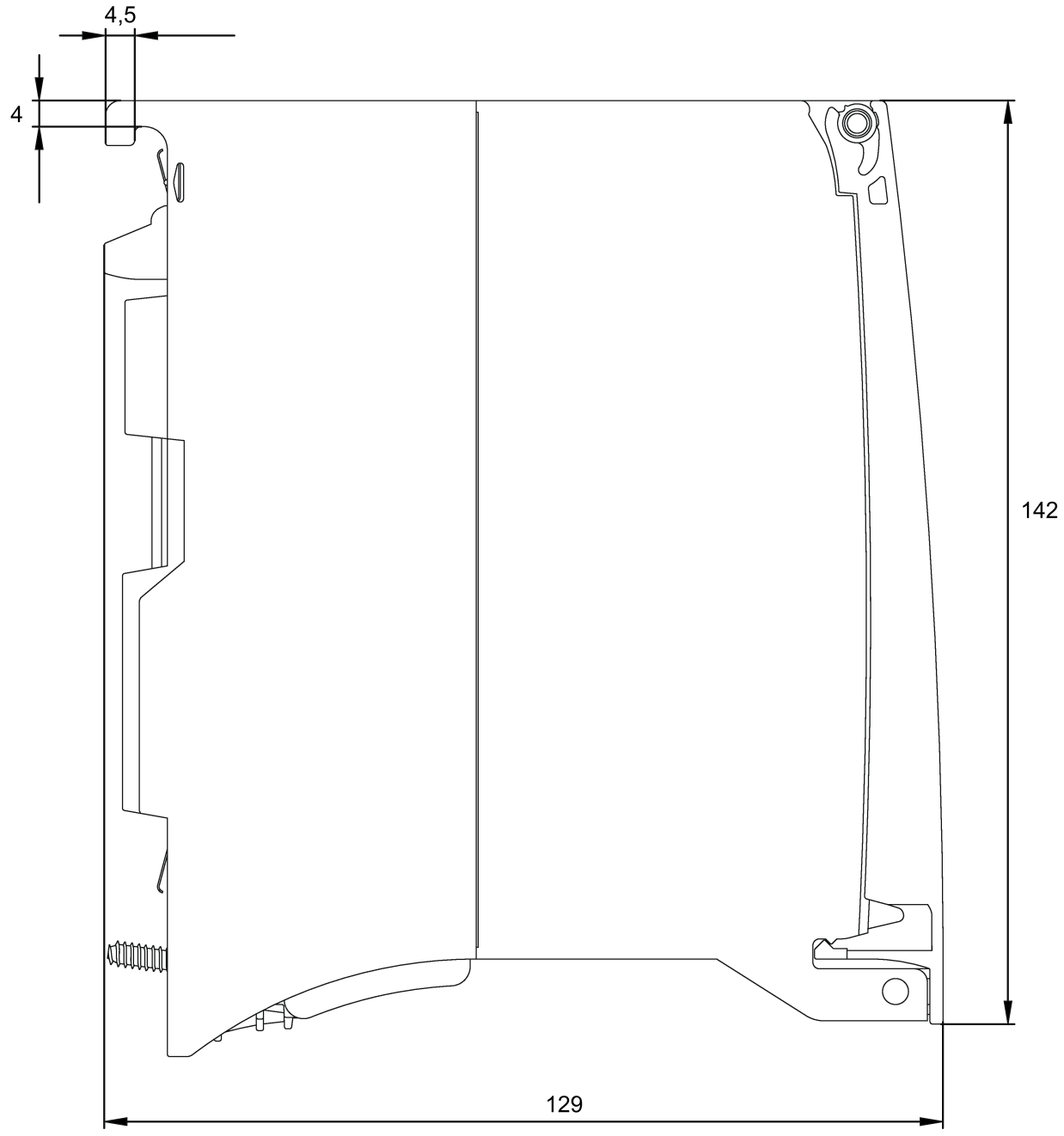


图 9-2 侧视图

附加信息

A

A.1 通过 FETCH/WRITE 链接到其它系统

可使用通过 ISO 传输连接、TCP 和 ISO-on-TCP 连接支持的 FETCH/WRITE 模式通过非西门子设备访问 S7 系统存储区。

为了能够使用这种类型的访问（例如用于 PC 应用程序），需要了解作业的 PDU 结构。请求和响应帧所需的 S7 特定或 S5 特定报头的长度为 16 字节。具体结构如下。

WRITE 帧的结构

下表中显示的不带固定值的参数的含义和值可以在"参数值"部分中找到。

WRITE 请求帧			**WRITE 确认帧**		
0	系统 ID	="S"	0	系统 ID	="S"
1		="5"	1		="5"
2	报头的长度（以字节为单位）	=16d。	2	报头长度	=16d。
3	ID OP 代码	=01	3	ID OP 代码	=01
4	长度 OP 代码	=03	4	长度 OP 代码	=03
5	OP 代码	=03	5	OP 代码	=04
6	ORG 字段	=03	6	Ack 字段	=0Fh
7	长度 ORG 字段	=08	7	长度 ack 字段	=03
8	**ORG ID**		**8**	**错误字段**	**=No**
9	**DBNR**		**9**	**空字段**	**=FFh**
A	**起始地址**	**高位字节**	**A**	**长度空字段**	**=07**
B		**低位字节**	**B**		
C	**长度**	**高位字节**	**C**		
D		**低位字节**	**D**	**空闲**	
I	**空字段**	**=FFh.**	**I**		
F	**长度空字段**	**=02**	**F**		
	数据字段最大为 64 K				

FETCH 帧的结构

下表中显示的不带固定值的参数的含义和值可以在"参数值"部分中找到。

FETCH 请求帧			**FETCH 响应帧**		
0	系统 ID	="S"	0	系统 ID	="S"
1		="5"	1		="5"
2	报头长度	=0x10	2	报头长度	=0x10
3	ID OP 代码	=0x01	3	ID OP 代码	=0x01
4	长度 OP 代码	=0x03	4	长度 OP 代码	=0x03
5	OP 代码	=0x05	5	OP 代码	=0x06
6	ORG 字段	=0x03	6	Ack 字段	=0x0F
7	长度 ORG 字段	=0x08	7	长度 ack 字段	=0x03
8	ORG ID		8	错误字段	=No
9	DBNR		9	空字段	=0xFF
A	起始地址	高位字节	A	长度空字段	=0x07
B		低位字节	B	空闲	
C	长度	高位字节	C		
D		低位字节	D		
I	空字段	=0xFF	I		
F	长度空字段	=0x02	F		
				仅当错误编号 = 0 时，数据才能达到 64 K	

参数值

S7 地址区	**DB**	**M**	**I**	**A**
ORG ID	01H	02H	03H	04H
	来自/到主存储器中的数据块的源/目标数据	来自/到位存储区的源/目标数据	来自/到输入过程图像 (PII) 的源/目标数据	来自/到输出过程图像 (PIQ) 的源/目标数据

DBNR	提供源数据或接收目标数据的 DB	不相关	不相关	不相关
允许范围	1...255			
起始地址	读取或写入数据的起始 DW 编号。	读取或写入数据的起始存储器字节编号。	读取或写入数据的起始输入字节编号。	读取或写入数据的起始输出字节编号。
允许范围	0...2047	CPU 可使所有存储器字节可用。	0...127	0...127
长度	源/目标数据块的长度（以字为单位）	源/目标数据块的长度（以字节为单位）	源/目标数据块的长度（以字节为单位）	源/目标数据块的长度（以字节为单位）
允许范围	最多 8192 个字节	最多 8192 个字节	1...128	1...128

S7 地址区	**PI/PQ**	**C**	**T**
ORG ID	05H	06H	07H
	来自/到 I/O 模块的源/目标数据 对应源数据输入模块、 目标数据输出模块	来自/到计数器单元的源/目标数据	来自/到定时器单元的源/目标数据
DBNR	不相关	不相关	不相关
起始地址	读取或写入数据的起始 I/O 字节编号。	读取或写入数据的起始计数器单元编号。	读取或写入数据的起始时间定时器单元编号。
允许范围	0...127 数字量 I/O 128...255 模拟量I/O	0...255	0...255

数量	源/目标数据块的长度（以字节为单位）	源/目标数据块的长度（以字为单位，计数器单元 = 1 个字）	源/目标数据块的长度（以字为单位，计数器单元 = 1 个字）
允许范围	1...256	1	1

Syslog 消息

B

产品输出的 Syslog 消息符合 RFC 5424。这类消息基于 IEC 62443-3-3。

有关每条消息的详细说明，请参见下文。

B.1 Syslog 消息的结构

Syslog 消息将设备状态中的更改记录为状态信息。符合 RFC 5424 或 RFC 5426 的 Syslog 消息由设备输出并通过设置的 UDP 端口传送到服务器（标准：514）。Syslog 服务器收集设备的信息并通知用户关于这些事件的信息。

Syslog 协议规定了可能参数的固定顺序和结构。符合 RFC5424 的 Syslog 消息具有以下结构：

部分/参数	说明
HEADER	
PRI	Syslog 消息的优先级，分为以下几种： • Severity（严重程度） 可能值： – 0 Emergency – 1 Alert – 2 Critical – 3 Error – 4 Warning – 5 Notice – 6 Information – 7 Debug • Facility（来源） 可能值包括：子系统、服务、用户等
VERSION	Syslog 规范的版本号
TIMESTAMP	设备的时间戳作为本地时间，包括时区和夏令时/标准时间校正 格式： YYYY-MM-DDThh:mm:ss.msmsmsms+xx:yy 示例： 2010-01-01T02:03:15.0003+02:00

部分/参数	说明
HOSTNAME	通过以下任一方式标识源设备： • FQDN • IPv4 地址（符合 RFC1035）：十进制格式的字节： XXX.XXX.XXX.XXX • IPv6 地址（符合 RFC4291 第 2.2 部分） • 主机名称 如果信息丢失，则输出“-”。 在产品中：过程接口 P2 的已组态 IPv4 地址
APP-NAME	消息源自的设备或应用程序。如果信息丢失，则输出“-”。 在产品中： "-"
PROCID	过程 ID 用于明确标识各个过程，例如分析和故障排除过程。如果信息丢失，则输出“-”。 在产品中： "-"
MSGID	用于标识消息的 ID。如果信息丢失，则输出“-”。 在产品中： "-"
STRUCTURED-DATA	
timeQuality	结构化数据元素“timeQuality”通过两个参数“tzKnown”和“isSynced”提供有关系统时间的信息。 示例： [timeQuality tzKnown="0" isSynced="0"] • tzKnown 此参数指定源设备中的时区是否已知。 – 1 = 已知 – 0 = 未知 • isSynced 此参数指定源设备是否与可靠的外部时间源同步，例如通过 NTP。 – 1 = 已同步 – 0 = 未同步
MSG	
MESSAGE	消息文本为 ASCII 字符串（英文）

有关 Syslog 消息结构以及 RFC 中参数含义的更多详细信息，敬请访问以下网址：

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

B.2 Syslog 消息中的变量

变量显示在大括号 {variable} 内“消息文本”(Message text) 字段的“Syslog 消息”(Syslog messages) 部分中。

输出消息可包含以下变量：

变量	说明	格式	可能值或示例
{IP address}	IPv4 地址（符合 RFC1035） IPv6 地址（符合 RFC4291 第 2.2 部分）	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{FQHN}	Fully Qualified Host Name：完全指定的主机名；完全限定域名 (FQDN) 或 IP 地址。	FQDN： host1.com IPv4：%d.%d.%d.%d	server1 192.168.1.105
{Src port} {Dest port}	端口号（小数）	%d	0 ... 65535
{Src mac} {Dest mac}	源/目标 MAC 地址	%02x:%02x:%02x; %02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	用于生成事件的第 4 层协议或服务。	%s	UDP | TCP | WBM | Telnet | SSH | Console | PNIO | PB | OPC | TFTP | SFTP
{Group}	用于标识组的名称（不带空格的字符串）	%s	IT 服务
{User name}	根据他/她的姓名识别经验证的用户的字符串（无空格）。	%s	<名称>
{Local interface}	本地接口的符号名称	%s	Console
{Action user name} 或 {Destination user name}	根据他/她的姓名识别目标用户。此用户不是经验证的用户。	%s	<名>.<姓名>
{Role}	角色的符号名称	%s	管理员

变量	说明	格式	可能值或示例
{Time minute} {Timeout}	分钟数	%d	44
{Time second}	秒数	%d	44
{Failed login count}	登录尝试失败次数	%d	10
{Max sessions}	最大会话数	%d	10
{Trigger pin}	已触发事件的 IO 引脚的字符串（无空格）。	%s	DI1
{Firewall rule}	用于防火墙规则集的字符串（带空格）	%s	Rule1
{Subject}	用于证书中的主题的字符串（无空格）。用作基于证书的验证的一部分（带空格），还必须包含 Unicode 字符。	%s UTF8 代码： %S	主题
{Config detail}	用于标识组态部分的字符串（无空格）	%s	OpenVPN
{Connection name}	VPN 连接的名称		Connection_1
{Firewall accept}	执行的防火墙操作（已接受数据包）		ACCEPT
{Firewall action reject}	执行的防火墙操作（已拒绝数据包）		REJECT DROP
{Length}	网络数据包长度（以字节为单位）	%d	52
{Network interface}	网络接口的符号名称	%s	vlan 1

B.3 消息

该产品输出以下 SYSLOG 消息（按类别排序）。

B.3.1 Non-repudiation

消息文本	{Protocol}: User {User name} has changed configuration.
示例	Console: User admin has changed configuration.
说明	用户已通过下载新组态数据更改了组态数据。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 Reference: SR 2.12

索引

C

CLoudConnect, 68
CPU 的工作模式, 40
CPU 的连接资源, 21

D

DHCP, 146
DNS 服务器 - 程序控制的更改, 116

F

FETCH/WRITE, 14
    S5/S7 寻址模式, 18
    功能, 45
    在 CPU 中启用, 47
FETCH/WRITE 连接, 22
FTP
    对 FTP 作业块的引用丢失时的响应, 128
    在 CPU 中启用, 47
FTP 的 TCP 连接, 24
FTP 服务器
    组态限制, 24
FTP 客户端
    组态限制, 24
FTP（FTP 客户端）, 20
FTP_CMD, 115, 117
    块执行时间, 24
FTPS, 19
FTPS - Security, 68

H

HMI 通信, 14

I

IP 地址
    通过 DHCP, 48
IP 地址 - 程序控制的更改, 116
IP 组态
    IPv4 / IPv6, 17
IP 路由, 49
IPv6 地址
    使用, 18
ISO 传输连接, 22
ISO-on-TCP (RFC 1006), 13
ISO-on-TCP 连接, 22
ISO-Transport (RFC 8073), 13

M

MAC 地址, 17
MIB, 140
Multicast (UDP), 13

N

NTP, 17
NTP (secure), 19, 55
NTP 服务器 - 程序控制的更改, 116

O

OP 连接
    数量, 21
Open User Communication (OUC), 13
OUC (Open User Communication), 111

P

PG 连接
    数量, 21
PG 通信, 14
PUT/GET
    在 CPU 中启用, 47

Q

QoS, 104
QualityCode, 94

R

RUN → STOP, 40

S

S7 连接, 20
    可自由使用数, 21
S7 通信, 14
SIMATIC NET 词汇表, 8
SMTPS, 20
SNMP, 52, 140
SNMPv3, 20
STEP 7 - 版本, 26

T

T_CONFIG, 116
TCON, 115
TCP (RFC 793), 13
TCP 连接, 22
TDISCON, 115
TRCV, 115
TSEND, 115

U

UDP, 23
UDP (RFC 768), 13
UDP 连接, 22

V

VPN, (??????)
    应用领域, 57
    单元保护概念, 57

W

Web 的连接
    数量, 21
Web 服务器, 18

Q

千兆位规范, 29

Y

已编程的连接
    数量, 21
已编程通信连接, 50

D

订货号, 3

Y

以太网接口, 29
    通过 T_CONFIG 组态, 116

D

电子邮件, 13
电子邮件连接, 22
电源模块
    更多, 20

C H

处置, 8

J

记录, 19
记录服务器, 64

Z

在线功能, 138
在线诊断, 137

H

回收, 8

W

网关 (VPN), 61
网络中的重复地址, 48

J

交叉引用 (PDF), 5

C H

产品名称, 4

A

安全诊断, 139
安全须知, 31

F

防火墙, 19

L

连接中止, 94

S H

时钟同步, 17
    建议, 55

X

系统数据类型
    FTP_..., 115
    TCON_..., 115
    TMail_..., 115

C

词汇表, 8

G

固件
    版本, 3

F

服务和支持, 8

D

单元保护概念
VPN, 57

Z

组态限制
通信模块, 20

S H

说明 (OUC), 111

J

兼容性
V1.0 - V1.1, 89

B

被动建立 VPN 连接, 61

P

培训, 8

X

虚拟专用网络
定义, 56

T

替换件, 25

Y

硬件版本, 3

C H

程序块 - 最大数据长度, 23

S H

数据传输（云）, 84
数据缓冲, 105
数据管理 - 组态数据, 146
数量
通信模块, 20

D

端口 8448, 139

S

缩写/缩略语, 4