

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200AL 通信

功能手册

前言

文档指南

1

产品概述

2

通信服务

3

PG 通信

4

HMI 通信

5

开放式通信

6

S7 通信

7

点对点链接

8

路由

9

连接资源

10

连接诊断

11

工业以太网安全

12

服务与支持

A

法律资讯

警告提示系统

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

 危险
表示如果不采取相应的小心措施， 将会 导致死亡或者严重的人身伤害。
 警告
表示如果不采取相应的小心措施， 可能 导致死亡或者严重的人身伤害。
 小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。
注意
表示如果不采取相应的小心措施，可能导致财产损失。

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

合格的专业人员

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

按规定使用 Siemens 产品

请注意下列说明：

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

商标

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

责任免除

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

前言

本文档的用途

在本功能手册中，简要介绍了 SIMATIC S7-1500、ET 200MP、ET 200SP 和 ET 200AL 系统中的通信选件、CPU、通信模块和处理器。本功能手册介绍面向连接的异步通信。

本文档中包含以下内容：

- 通信服务概述
- 通信服务的属性
- 设置通信服务等用户操作概述

所需的基本知识

要理解本功能手册中的内容，需要具备以下知识：

- 自动化技术的基本知识
- 工业自动化系统 SIMATIC 的知识
- 有关如何使用 STEP 7 (TIA Portal) 的基本知识

本文档的适用范围

本文档是 SIMATIC S7-1500、ET 200MP、ET 200SP 和 ET 200AL 系统中所有产品的基础性文档。产品文档基于本文档。

相对于先前版本的变更

本手册相对于先前版本（2014 年 6 月版）的具有以下变更/增添：

- 增加了用于 SIMATIC S7-1500 软控制器的通信协议和端口号
- 增加了 HMI 设备的最大连接资源数目
- 增加了数据记录路由功能

约定

STEP 7: 在本文档中，我们将版本从 V12 (TIA Portal) 起的 STEP 7 组态和编程软件统称为“STEP 7”。

本文档中包含所述设备的相关图片。这些图可能与提供的设备略有不同。

请特别关注以下注意事项的相关信息：

说明

这些注意事项包含有关产品、产品操作、应特别关注的文档部分的重要信息。

其它支持

有关技术支持的信息，请参见附录服务与支持 (页 92)。

有关各种 SIMATIC 产品和系统的技术文档，请访问 Internet (<http://www.siemens.com/simatic-tech-doku-portal>)。

Internet (<http://mall.industry.siemens.com>) 上还提供了在线目录和在线订购系统。

安全信息

西门子为其产品及解决方案提供工业安全功能，以支持工厂、解决方案、机器、设备和/或网络的安全运行。这些功能是整个工业安全机制的重要组成部分。有鉴于此，西门子不断对产品和解决方案进行开发和完善。西门子强烈建议您定期检查产品的更新和升级信息。

要确保西门子产品和解决方案的安全操作，还须采取适当的预防措施（例如：设备单元保护机制），并将每个组件纳入全面且先进的工业安全保护机制中。此外，还需考虑到可能使用的所有第三方产品。更多有关工业安全的信息，请访问 Internet (<http://www.siemens.com/industrialsecurity>)。

要及时了解有关产品的更新和升级信息，请订阅相关产品的实事信息。更多相关信息，请访问 Internet (<http://support.automation.siemens.com>)。

目录

前言	3
1 文档指南	7
2 产品概述	10
3 通信服务	15
3.1 通信选项概述	15
3.2 连接资源总览	18
3.3 建立连接	19
3.4 数据一致性	22
3.5 通信协议和使用的端口号	24
4 PG 通信	29
5 HMI 通信	32
6 开放式通信	35
6.1 开放式通信的概述	35
6.2 开放式通信的协议	36
6.3 开放式通信的指令	37
6.4 建立采用 TCP、ISO-on-TCP、UDP 和 ISO 协议的开放式通信	40
6.5 建立与 Modbus TCP 的通信	46
6.6 通过电子邮件建立通信	49
6.7 通过 FTP 建立通信	50
6.8 建立和终止通信关系	53
7 S7 通信	54
8 点对点链接	64
9 路由	71
9.1 S7 路由	71
9.2 数据记录路由	76
10 连接资源	78
10.1 连接资源分配	78
11 连接诊断	84

12 工业以太网安全 88

 12.1 防火墙 89

 12.2 日志记录..... 90

 12.3 NTP 客户端 90

 12.4 SNMP 91

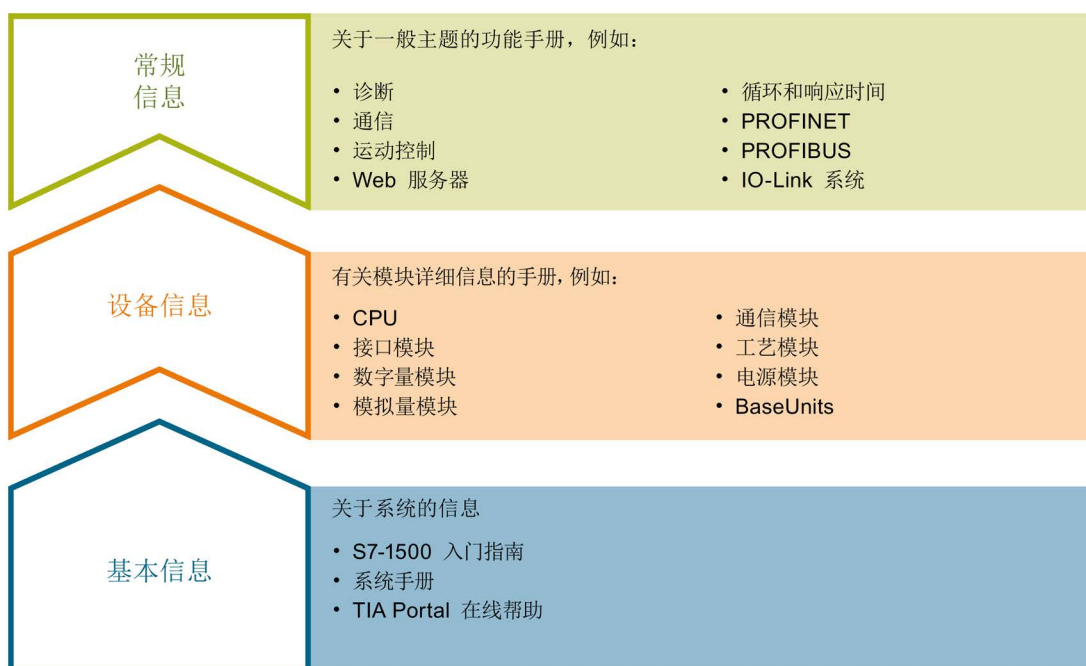
A 服务与支持 92

 术语表 96

 索引 107

SIMATIC S7-1500 自动化系统以及 SIMATIC ET 200MP、ET 200SP 和 ET 200AL 分布式 I/O 系统的文档分为 3 个部分。

这样用户可方便访问自己所需的特定内容。



基本信息

系统手册和入门指南中详细描述了 SIMATIC S7-1500、ET 200MP、ET 200SP 和 ET 200AL 系统的组态、安装、接线和调试。STEP 7 在线帮助用户提供了组态和编程方面的支持。

设备信息

产品手册中包含模块特定信息的简洁描述，如特性、端子图、功能特性、技术数据。

常规信息

功能手册包含各种常规主题的详细描述，如诊断、通信、运动控制、Web 服务器。

可以从 Internet (<http://w3.siemens.com/mcms/industrial-automation-systems-simatic/en/manual-overview/Pages/Default.aspx>) 上免费下载文档。

产品信息数据表中记录了对这些手册的更改和补充。

手册集

手册集中包含系统的完整文档，这些文档收集在一个文件中。

可以在 Internet 上找到手册集：

- S7-1500/ET 200MP (<http://support.automation.siemens.com/CN/view/zh/86140384>)
- ET 200SP (<http://support.automation.siemens.com/CN/view/zh/84133942>)
- ET 200AL (<http://support.automation.siemens.com/CN/view/zh/95242965>)

我的文档管理器

“我的文档管理器”用于将完整手册或部分手册组合成用户自己的手册。

用户可以将该手册导出为 PDF 文件或可供稍后进行编辑的格式。

可以在 Internet (<http://support.automation.siemens.com/CN/view/zh/38715968>) 上找到“我的文档管理器”。

应用程序和工具

“应用程序和工具”提供使用各种工具的支持和用于解决自动化任务的各种示例。自动化系统中的多个组件完美协作，从而组合成不同的解决方案，而用户则无需关注各个单独的产品。

可以在 Internet (<http://support.automation.siemens.com/WW/view/zh/20208582>) 上找到“应用程序和工具”。

CAX 下载管理器

CAX 下载管理器用于访问 CAX 或 CAe 系统的最新产品数据。

仅需几次单击用户即可组态自己的下载包。

用户可选择：

- 产品图片、2 维图、3 维模型、内部电路图、EPLAN 宏文件
- 手册、功能特性、操作手册、证书
- 产品主数据

可以在 Internet (<https://support.automation.siemens.com/CN/view/zh/42455541>) 上找到 CAX 下载管理器。

TIA Selection Tool

通过 TIA Selection Tool，用户可以为全集成自动化（TIA）选择、组态和订购设备。

该工具是 SIMATIC Selection Tool 的下一代产品，并将自动化技术的已知组态程序集成到一个工具中。

通过 TIA Selection Tool，用户可以从产品选择或产品组态中生成一个完整的订购列表。

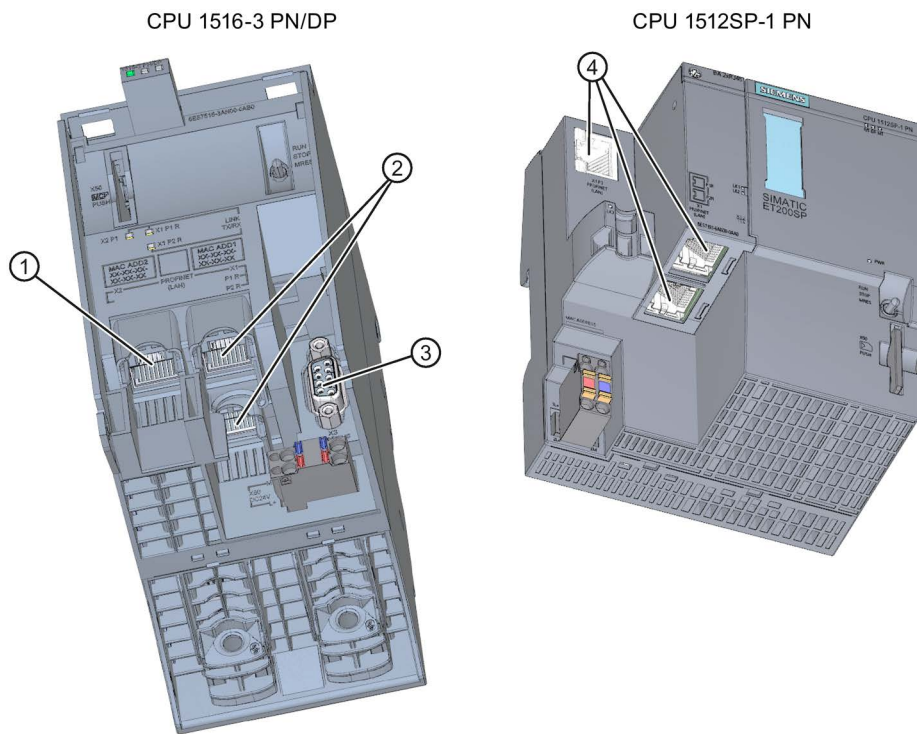
可以在 Internet (<http://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool>) 上找到 TIA Selection Tool。

产品概述

S7-1500、ET 200MP、ET 200SP 和 ET 200AL 系统的 CPU、通信模块和处理器以及 PC 系统提供了通过 PROFINET、PROFIBUS 和点对点连接进行通信的接口。

CPU、通信模块和通信处理器

PROFINET 和 PROFIBUS DP 接口集成在 S7-1500 CPU 中。例如，CPU 1516-3 PN/DP 上带有 2 个 PROFINET 接口和 1 个 PROFIBUS DP 接口。安装通信模块 (CM) 和通信处理器 (CP) 之后，还可以使用其它 PROFINET 和 PROFIBUS DP 接口。



- ① PROFINET 接口 (X1)，带一个端口
- ② PROFINET 接口 (X2)，带双端口交换机
- ③ PROFIBUS DP 接口 (X3)
- ④ PROFINET 接口 (X1)，带 3 端口交换机

图 2-1 CPU 1516-3 PN/DP 和 CPU 1512SP-1 PN 的接口

通信模块的接口

通信模块 (CM) 的接口特性与 S7-1500 CPU 上集成的同类型接口（例如，PROFIBUS DP）完全相同。可用来通过相应接口将系统进行扩展（例如，为 S7-1500 自动化系统的通信模块 CM 1542 5 添加 PROFIBUS 接口）。

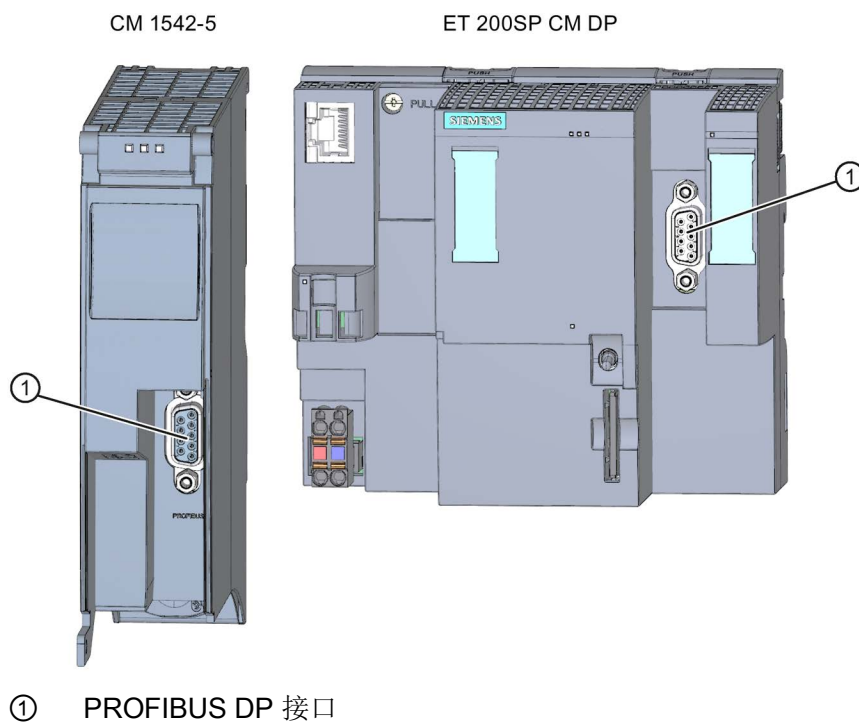
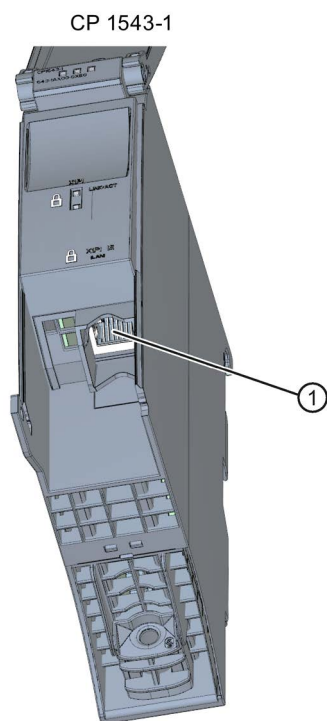


图 2-2 CM 1542-5 和 CM DP 的 PROFIBUS DP 接口

通信处理器的接口

通信处理器 (CP) 接口的功能与 CPU 中集成的接口不同。CP 具有一些特殊功能。例如，CP 1543-1 上具有工业以太网安全功能，可通过其工业以太网接口对工业以太网进行保护。



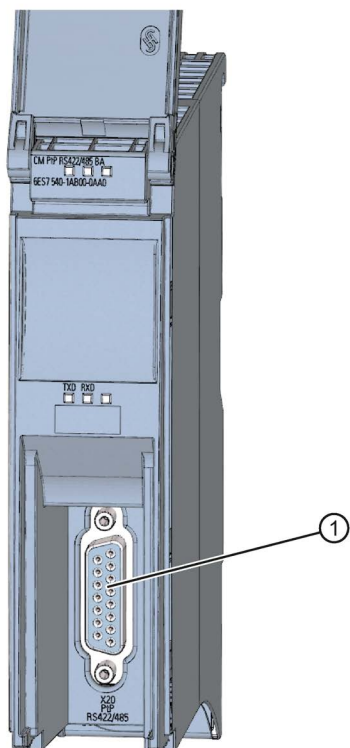
① 工业以太网接口

图 2-3 CP 1543-1 的工业以太网接口

进行点对点连接的通信模块接口

点对点连接的通信模块可通过 RS 232、RS 422 和 RS 485 接口进行通信，例如 Freeport 或 Modbus 通信。

CM PtP RS422/485 BA

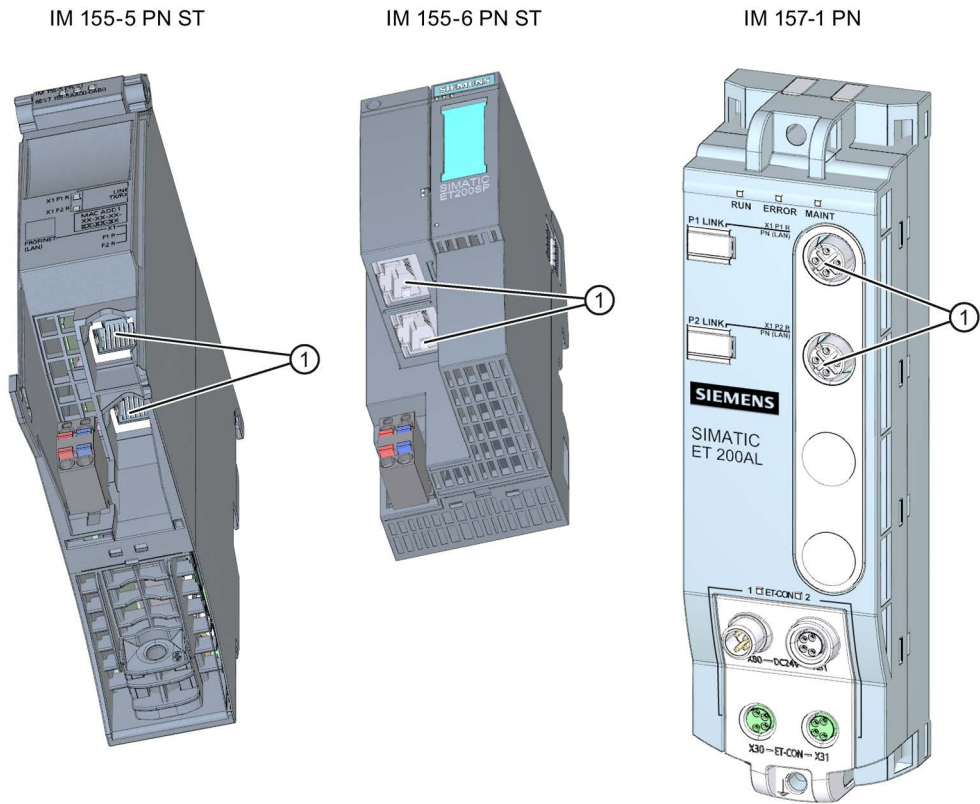


① 用于点对点连接的接口

图 2-4 CM PtP RS422/485 BA 的点对点连接接口

接口模块上的接口

ET 200MP、ET 200SP 和 ET 200AL 接口模块 (IM) 上的 PROFINET 和 PROFIBUS DP 接口用于将分布式 I/O ET 200MP、ET 200SP 和 ET 200AL 连接到上级 I/O 控制器或 DP 主站的 PROFINET 或 PROFIBUS。



① PROFINET 接口，带双端口交换机

图 2-5 PROFINET 接口 IM 155-5 PN ST (ET 200MP)、IM 155-6 PN ST (ET 200SP) 和 IM 157-1 PN (ET 200AL)

通信服务

下文中介绍的通信服务将使用系统中 CPU、通信模块和处理器所提供的接口和通信机制。

通信服务

3.1 通信选项概述

通信选项概述

以下通信选项可用于完成自动化任务。

表格 3-1 通信选项

通信选项	功能	通过接口：		
		PN/IE *	DP	串行
PG 通信	调试、测试、诊断	√	√	-
HMI 通信	操作员监控	√	√	-
通过 TCP/IP 实现开放式通信	使用 TCP/IP 协议通过 PROFINET/工业以太网进行数据交换 指令： • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	√	-	-
通过 ISO-on-TCP 实现开放式通信	使用 ISO-on-TCP 协议通过 PROFINET/工业以太网进行数据交换 指令： • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	√	-	-

3.1 通信选项概述

通信选件	功能	通过接口:		
		PN/IE *	DP	串行
通过 UDP 实现开放式通信	使用 UDP 协议通过 PROFINET/工业以太网进行数据交换 指令: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	√	-	-
通过 ISO 实现开放式通信（仅适用于带有 PROFINET/工业以太网接口的 CP）	使用 ISO 协议通过 PROFINET/工业以太网进行数据交换 指令: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	√	-	-
通过 Modbus TCP 进行通信	使用 Modbus TCP 协议通过 PROFINET 进行数据交换 指令: • MB_CLIENT • MB_SERVER	√	-	-
电子邮件	通过电子邮件发送过程报警 指令: • TMAIL_C	√	-	-
FTP（仅适于带有 PROFINET/工业以太网接口的 CP）	通过 FTP（文件传输协议）进行文件管理和文件访问，CP 既可以作为 FTP 客户端也可以作为 FTP 服务器 指令: • FTP_CMD	√	-	-
Fetch/Write（仅适于带有 PROFINET/工业以太网接口的 CP）	通过 TCP/IP、ISO-on-TCP 和 ISO 作为服务器 通过 Fetch/Write 的特殊指令	√	-	-

通信选项	功能	通过接口:		
		PN/IE *	DP	串行
S7 通信	客户端/服务器或客户端/客户端的数据交换 指令: • PUT/GET • BSEND/BRCV • USEND/URCV	√	√	-
串行点到点连接	使用 Freeport、3964 (R)、USS 或 Modbus 协议通过点对点连接进行数据交换 通过 PtP、USS 或 Modbus/RTU 的特定指令	-	-	√
Web 服务器	通过 HTTP(S) 进行数据交换, 例如进行诊断	√	-	-
SNMP (简单网络管理协议)	诊断 IP 网络的“网络运行状况”, 可通过标准 SNMP 协议对 IP 网络组件进行参数设置	√	-	-
时间同步	通过 PN/IE 接口: CPU 是 NTP 客户端 (网 络时间协议)	√	-	-
	通过 DP 接口: CPU/CM/CP 作为时间主站 或时间从站	-	√	-

* IE - 工业以太网

附加信息

- 有关 Fetch/Write 服务的信息, 请参见 STEP 7 在线帮助。
- 有关 PtP 连接的其它信息, 请参见功能手册“CM PtP - 点对点连接组态 (<http://support.automation.siemens.com/WW/view/de/59057093/0/zh>)”。
- 有关 Web 服务器的功能介绍, 请参见功能手册“Web 服务器 (<http://support.automation.siemens.com/WW/view/zh/59193560>)”。
- 有关 SNMP 标准协议的信息, 请访问 Internet (<http://support.automation.siemens.com/WW/view/zh/15166742>) 上的服务与支持页面。
- 有关时间同步的信息, 请参见 S7-1500, ET 200MP (<http://support.automation.siemens.com/WW/view/zh/59191792>) 系统手册。

3.2 连接资源总览

连接资源

某些通信服务需要进行连接。连接需要占用所用 CPU、CP 和 CM 中的资源（例如，CPU 操作系统中的存储区域）。大多数情况下，每个 CPU/CP/CM 都需要一个连接资源。在 HMI 通信中，每个 HMI 连接最多需要 3 个连接资源。

可用的连接资源取决于所用的 CPU。CP 和 CM 的数量不能超出自动化系统中定义的上限。

站中的可用连接资源

站的最大资源数由 CPU 决定。

每个 CPU 都预留有一定数量的连接资源，用于编程设备、HMI 和 Web 服务器通信。另外，还提供了可用于 SNMP、电子邮件连接、HMI 和 S7 通信以及开放式通信的资源。

何时会分配连接资源？

连接资源的分配时间取决于连接的设置方式（自动、编程或组态）。请参见“建立连接 (页 19)”部分。

附加信息

有关连接资源分配和在 STEP 7 中显示连接资源的更多信息，请参见“连接资源 (页 78)”部分。

3.3 建立连接

自动连接

如果将 PG/PC 接口物理连接到 CPU 的接口，并通过 STEP 7 中的“转至在线”(Go online)对话框进行了接口分配，则 STEP 7 将自动建立连接（例如，PG 或 HMI 连接）。

建立编程的连接

在 STEP 7 的程序编辑器中，可根据所选 CPU 使用相应的通信指令（如 TSEND_C）建立编程连接。

指定连接参数（在巡视窗口、指令属性中）时，通过用户界面使得操作更为方便快捷。

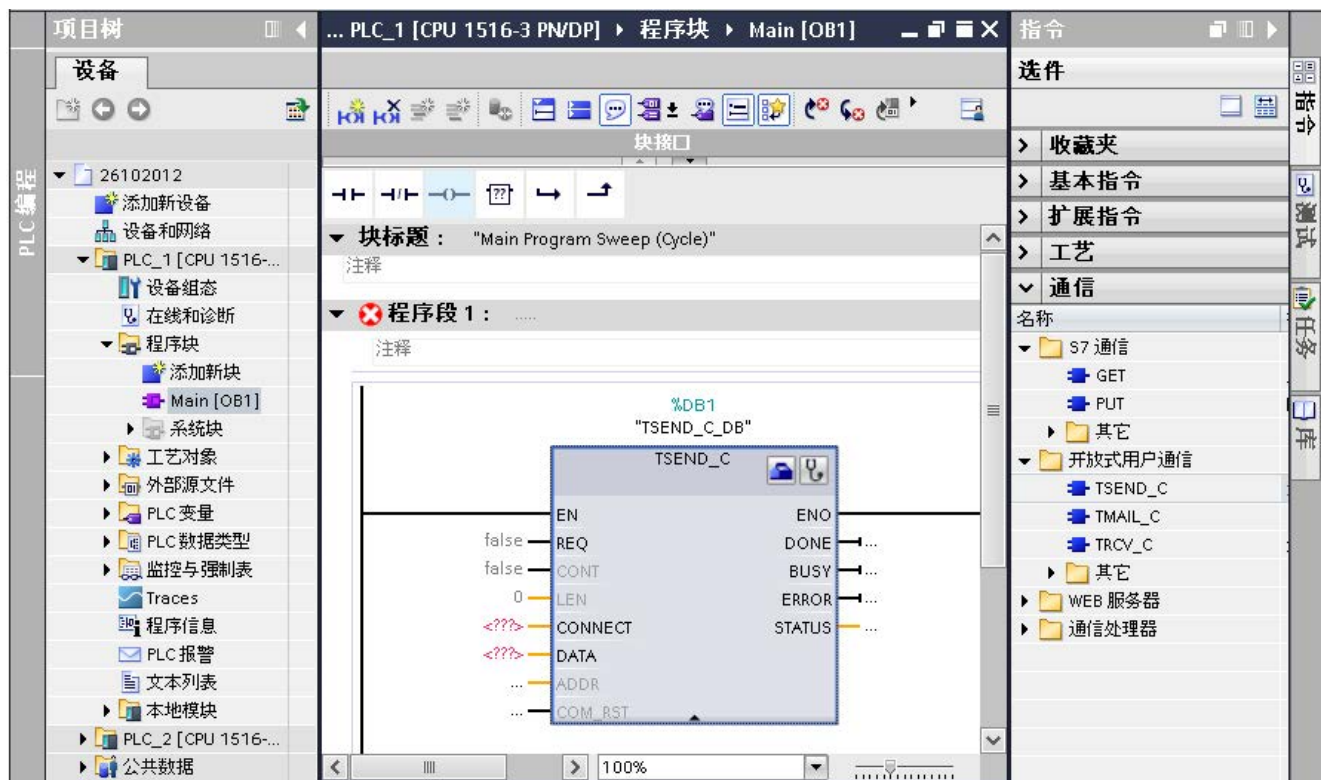


图 3-1 通过编程

建立组态的连接

根据所选的 CPU 或软控制器，可在 STEP 7 的“设备与网络”(Devices & networks) 编辑器中的网络视图内建立组态的连接。

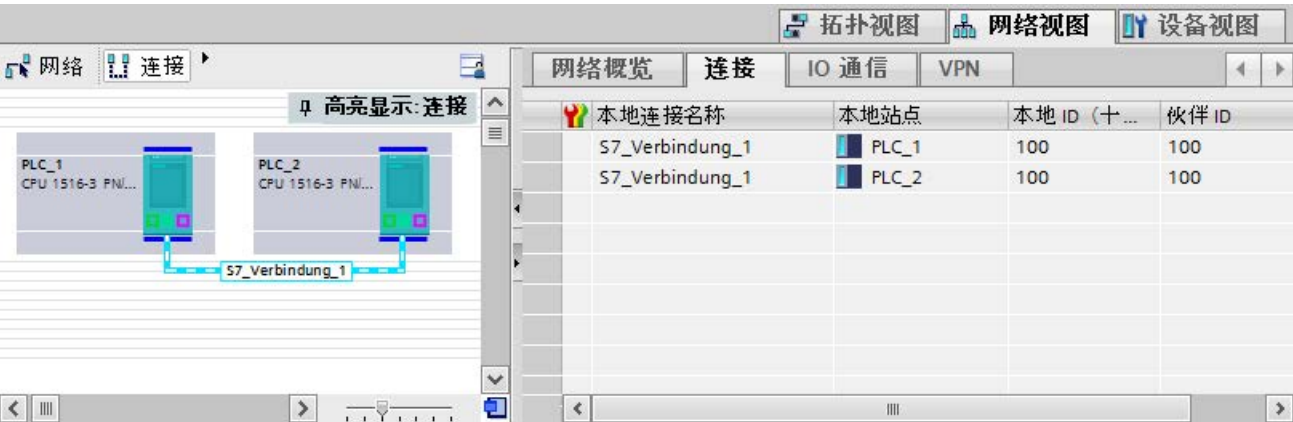


图 3-2 通过组态

总结

通常，可以选择通过组态建立连接或者通过编程建立连接。如果选择通过编程建立连接，则将在数据传输结束后释放连接资源。编程的连接不能保证路由的连接，也就是说，在可用的资源不足时不会建立这些连接。通过组态建立连接时，下载组态后资源仍处于已分配状态，直至组态再次更改。因此，通过组态的连接建立连接不能因缺乏资源而失败。CPU 的巡视窗口中的“连接资源”(Connection resources) 表显示了已使用的连接资源和仍可使用的连接资源的概览。

表格 3-2 设置连接

连接	自动	通过编程	通过组态
编程设备连接	√	-	-
HMI 连接	√	-	√
通过 TCP/IP 连接实现开放式通信	-	√	√
通过 ISO-on-TCP 连接实现开放式通信	-	√	√
通过 UDP 连接实现开放式通信	-	√	√
通过 ISO 连接实现开放式通信	-	√	√
通过 Modbus TCP 连接进行通信	-	√	-
电子邮件连接	-	√	-
FTP 连接	-	√	-
S7 连接	-	-	√

附加信息

有关连接资源分配和在 STEP 7 中显示连接资源的更多信息，请参见连接资源 (页 78) 部分。

3.4 数据一致性

数据一致性的定义

并发过程无法修改的数据块称为一致性数据区。这意味着，其大小超出一致性数据区的连续数据块中，可能同时包含新的和旧的数据。

示例

当一个通信指令中断时（例如，由高优先级的硬件中断 **OB** 进行中断），则会发生不一致性现象。如果该 **OB** 中的用户程序对该指令已部分处理的数据进行了更改，则所传送的数据包括：

- 一部分来自于发生硬件中断处理之前
- 一部分来自于发生硬件中断处理之后

这意味着日期不一致（在不同的时间点加以处理）。

结论

如果遵守系统中所指定的一致性数据的最大数量，则不会产生不一致现象。

S7-1500 CPU 中最大可以设置 **462** 个字节的一致性数据（请见下文）。

如果需要一致性传输的数据量大于系统中指定的一致性数据的最大值，则请务必确保应用程序中的数据保持一致，并通过延长 **CPU** 的中断响应时间等方式，避免传输过程发生中断。

S7-1500 的数据一致性

使用指令访问公共数据：

如果用户程序中包含访问公共数据的通信指令（如 TSEND/TRCV），则用户可以通过诸如“DONE”参数对该数据区进行访问。这样就可以在用户程序中确保使用通信指令进行本地数据传输的数据区中的数据保持一致。

使用 PUT/GET 指令或通过 HMI 通信进行 Write/Read 操作：

使用 PUT/GET 指令进行 S7 通信或通过 HMI 通信进行 Write/Read 操作时，需要考虑到编程或组态过程中一致性数据区域的大小。这是因为，目标设备（服务器）上的用户程序中没有可以执行源用户程序中数据传输的指令。

S7-1500 中系统指定的最大数据一致性：

在程序循环过程中，S7-1500 最多可以将块中 462 个字节的通信数据一致地传入或传出用户存储器。对于较大的数据区域将不能保证数据一致性。如果要求定义数据一致性，则 CPU 用户程序中通信数据的长度不能超过 462 个字节。之后，就可以从 HMI 设备使用 Read/Write 变量一致性地访问这些数据。

点对点 CM 的最大数据一致性：

通过 CM 进行点对点连接通信时，用户程序中的 Send/Receive 指令可确保数据的一致性。最大数据一致性为 4 KB，具体取决于模块类型。

附加信息

- 有关一致性数据的最大数量，请参见 CPU、CM 或 CP 手册中的技术规范。
- 有关数据一致性的更多信息，请参见 STEP 7 在线帮助中的指令说明。

3.5 通信协议和使用的端口号

本部分概述了各种协议和使用的端口号。对于每种协议，指定了地址参数、各自的通信层以及通信角色和通信方向。

通过这些信息，可以将自动化系统的安全保护措施与所用的协议进行匹配（例如防火墙）。由于安全措施仅限于以太网或 PROFINET 网络，因此这些表不包含任何 PROFIBUS 协议。

下表显示了所用的不同层和协议。

下表显示了 S7-1500 和 ET 200SP CPU 所支持的协议。S7-1500 软控制器还支持下表中列出的协议，这些协议适用于分配给软控制器的以太网接口。

表格 3-3 层和协议

协议	端口号	(2) 链路层 (4) 传输层	功能	说明
PROFINET 协议				
DCP 发现和组态协议	不相关	(2) Ethertype 0x8892 (PROFINET)	可访问设备 PROFINET 发 现和组态	DCP 由 PROFINET 用于发现 PROFINET 设备并提供基本设置。
LLDP 链路层发现协议	不相关	(2) Ethertype 0x88CC (LLDP)	PROFINET 链 路层发现协议	LLDP 由 PROFINET 用于发现和管理 PROFINET 设备间的邻近关系。 LLDP 使用特定的组播 MAC 地址： 01-80-C2-00-00-0E
MRP 介质冗余协议	不相关	(2) Ethertyp e 0x88E3 (IEC 62493- 2-2010)	PROFINET 介 质冗余	MRP 通过环形拓扑控制冗余传输路径。 MRP 根据标准使用组播 MAC 地址
PTCP 精确透明时钟协议	不相关	(2) Ethertype 0x8892 (PROFINET)	PROFINET 发送时钟和时 间同步，基于 IEEE 1588	PTC 提供 RJ45 端口之间的延时测量，并 随后发送时钟同步和时间同步。 PTCP 根据标准使用组播 MAC 地址
PROFINET IO 数据	不相关	(2) Ethertype 0x8892 (PROFINET)	PROFINET 周 期性 IO 数据传 送	PROFINET IO 帧用于通过以太网在 PROFINET IO 控制器和 IO 设备之间周期 性传送 IO 数据。
PROFINET 上下文管理器	34964	(4) UDP	无 PROFINET 连接的 RPC	PROFINET 上下文管理器可提供终点映射 器以建立应用关联 (PROFINET AR)。

协议	端口号	(2) 链路层 (4) 传输层	功能	说明
面向连接的通信协议				
SMTP 简单邮件传输协议	25	(4) TCP	简单邮件传输协议	SMTP 用于发送电子邮件和短消息（具体取决于提供商）。
HTTP 超文本传输协议	80	(4) TCP	超文本传输协议	HTTP 用于与 CPU 内部 Web 服务器通信。
ISO on TCP （遵循 RFC 1006 标准）	102	(4) TCP	ISO-on-TCP 协议	ISO on TCP（遵循 RFC 1006 标准）用于与远程 CPU 或软控制器进行面向消息的数据交换。 S7 与 ES、HMI、OPC Server 等通信。
NTP 网络时间协议	123	(4) UDP	网络时间协议	NTP 用于将 CPU 系统时间与 NTP 服务器的时间进行同步。
SNMP 简单网络管理协议	161 162 （陷阱）	(4) UDP	简单网络管理协议	SNMP 由 SNMP 管理器用于读取和设置网络管理数据（SNMP 管理的对象）。
HTTPS 安全超文本传输协议	443	(4) TCP	安全超文本传输协议	HTTPS 用于通过安全套接层 (SSL) 与 CPU 内部的 Web 服务器通信。
Modbus TCP Modbus 传输控制协议	502	(4) TCP	Modbus/TCP 协议	Modbus/TCP 由用户程序中的 MB_CLIENT/MB_SERVER 指令使用。

3.5 通信协议和使用的端口号

协议	端口号	(2) 链路层 (4) 传输层	功能	说明
OUC ¹ 开放式用户通信	1 ... 1999 使用范围有限 ²	(4) TCP (4) UDP	开放式用户通信 (TCP/UDP)	OUC 指令可以建立连接、终止连接并基于套接层传输数据。
	2000 ... 5000 推荐配置			
	5001 ... 49151 使用范围有限 ²			
预留	49152 .. 65535	(4) TCP (4) UDP	-	如果应用程序未确定本地端口号，将使用动态端口区域激活连接端点。

¹ 注： 用户可以通过开放式通信直接访问 UDP/TCP。 用户必须遵守 IANA (Internet Assigned Numbers Authority, 互联网数字分配机构) 的端口限制/定义。

² 请勿将已由其它协议使用的端口用于 OUC。

下表显示了 S7-1500 软控制器通过分配给 Windows 的以太网接口加以支持的协议。

表格 3-4 层和协议

协议	端口号	(2) 链路层 (4) 传输层	功能	说明
PROFINET 协议				
DCP 发现和组态 协议	不相关	(2) Ethertype 0x8892 (PROFINET)	可访问设备 PROFINET 发现和组态	DCP 由 PROFINET 用于发现 PROFINET 设备并提供基本设置。
面向连接的通信协议				
SMTP 简单邮件传 输协议	25	(4) TCP	简单邮件传 输协议	SMTP 用于发送电子邮件和短消息（具体取决于提供商）。
HTTP 超文本传输 协议	可调节 ¹	(4) TCP	超文本传输 协议	HTTP 用于与 CPU 内部 Web 服务器通信。为避免与 Windows 上的其它 Web 服务器冲突，可以更改端口号。 如果要使用 Web 服务器访问，必须在 Windows 防火墙中激活该端口。
ISO on TCP （遵循 RFC 1006 标准）	102	(4) TCP	ISO-on-TCP 协议	用于与编程设备/PC 或 HMI 通信的 ISO on TCP（遵循 RFC 1006 标准）。
OUC ² 开放式用户 通信	1 ... 1999 使用范围 有限 ^{3, 4}	(4) TCP (4) UDP	开放式用户 通信 (TCP/UDP)	OUC 指令可以建立连接、终止连接并基于套接层传输数据。 如果要使用 OUC，则必须在 Windows 防火墙中激活该端口。
	2000 ... 5000 推荐 ⁴			
	5001 ... 49151 使用范围 有限 ^{3, 4}			

3.5 通信协议和使用的端口号

协议	端口号	(2) 链路层 (4) 传输层	功能	说明
预留	49152 ... 65535	(4) TCP (4) UDP	-	如果应用程序不确定本地端口号，则是用于主动连接连接端点的动态端口范围。 如果要使用这种通信，则必须在 Windows 防火墙中激活端口。

- 1 Windows 分配的接口的默认设置： 81
- 2 注： 用户可以通过开放式用户通信直接访问 UDP/TCP。用户必须遵守 IANA (Internet Assigned Numbers Authority, 互联网数字分配机构) 的端口限制/定义。
- 3 请勿将已由其它协议使用的端口用于 OUC。
- 4 请勿将已由其它 Windows 应用程序使用的端口用于 OUC。

下表显示了除 S7-1500 通信模块（如 CP 1543-1）的表中列出的协议之外所支持的其它协议。

表格 3-5 层和协议

协议	端口号	(2) 链路层 (4) 传输层	功能	说明
PROFINET/工业以太网协议				
面向连接的通信协议				
FTP 文件传输协议	20（数据） 21（控制）	(4) TCP	文件传输协议	FTP 用于传输文件（仅与 CP 连接）。
SecureFTP 文件传输协议	20（数据） 21（控制）	(4) TCP	文件传输协议	SecureFTP 用于通过 TSL 连接传输文件（仅与 CP 连接）。
DHCP 动态主机配置协议	68	(4) UDP	动态主机配置协议	DHCP 用于在启动 IE 接口时从 DHCP 服务器检索 IP 地址套件。
安全 NTPv3 网络时间协议	123	(4) UDP	网络时间协议	NTP 用于将 CM/CP 内部系统时钟与 NTP 服务器同步。
SNMP 简单网络管理协议	161 162（陷阱）	(4) UDP	简单网络管理协议	SNMPv3 允许 CM/CP 在具有授权时从 SNMPv3 代理读取网络管理数据 (MIB)。

PG 通信

特性

使用 PG 进行通信时，CPU 或其它具备通信功能的模块可在工程师站进行数据交换（例如，PG、PC）。可以通过 PROFIBUS 和 PROFINET 子网进行数据交换。此外，还支持 S7 子网之间的网关。

PG 通信具有装载程序和组态数据、运行测试以及评估诊断信息所需的功能。这些功能集成在具有通信功能的模块的操作系统中。

PG/PC 可以在线连接到一个 CPU。PG/PC 同时可操作最多 4 个在线连接（例如，连接 4 个 CPU）。

要求

- 编程设备/PC 与具有通信功能的模块进行物理连接。
- 如果需要通过 S7 路由来访问具有通信功能的模块，则必须在参与的站（S7 路由器和端点）中装载硬件组态。

在线连接步骤

若要实现编程设备通信，必须建立与 CPU 的在线连接：

1. 在 STEP 7 的项目树中选择 CPU。
2. 选择“在线 > 转至在线”(Online > Go online) 菜单命令。

3. 在“转至在线”(Go online) 对话框中，针对在线连接进行以下设置：
- 在“编程设备/PC 接口类型”(Type of PG/PC interface) 下拉列表中，选择接口类型（如 PN/IE）。
 - 在“编程设备/PC 接口”(PG/PC interface) 下拉列表中，选择要用于建立在线连接的编程设备/PC 接口（如工业以太网卡）。
 - 从“连接到接口/子网”(Connection to interface/subnet) 下拉列表，选择用于将编程设备/PC 物理连接的接口或 S7 子网。
 - 如果可以通过 S7 路由器（网关）访问具有通信功能的模块，请从“第一网关”(1st Gateway) 下拉列表选择用于连接相关子网的 S7 路由器。

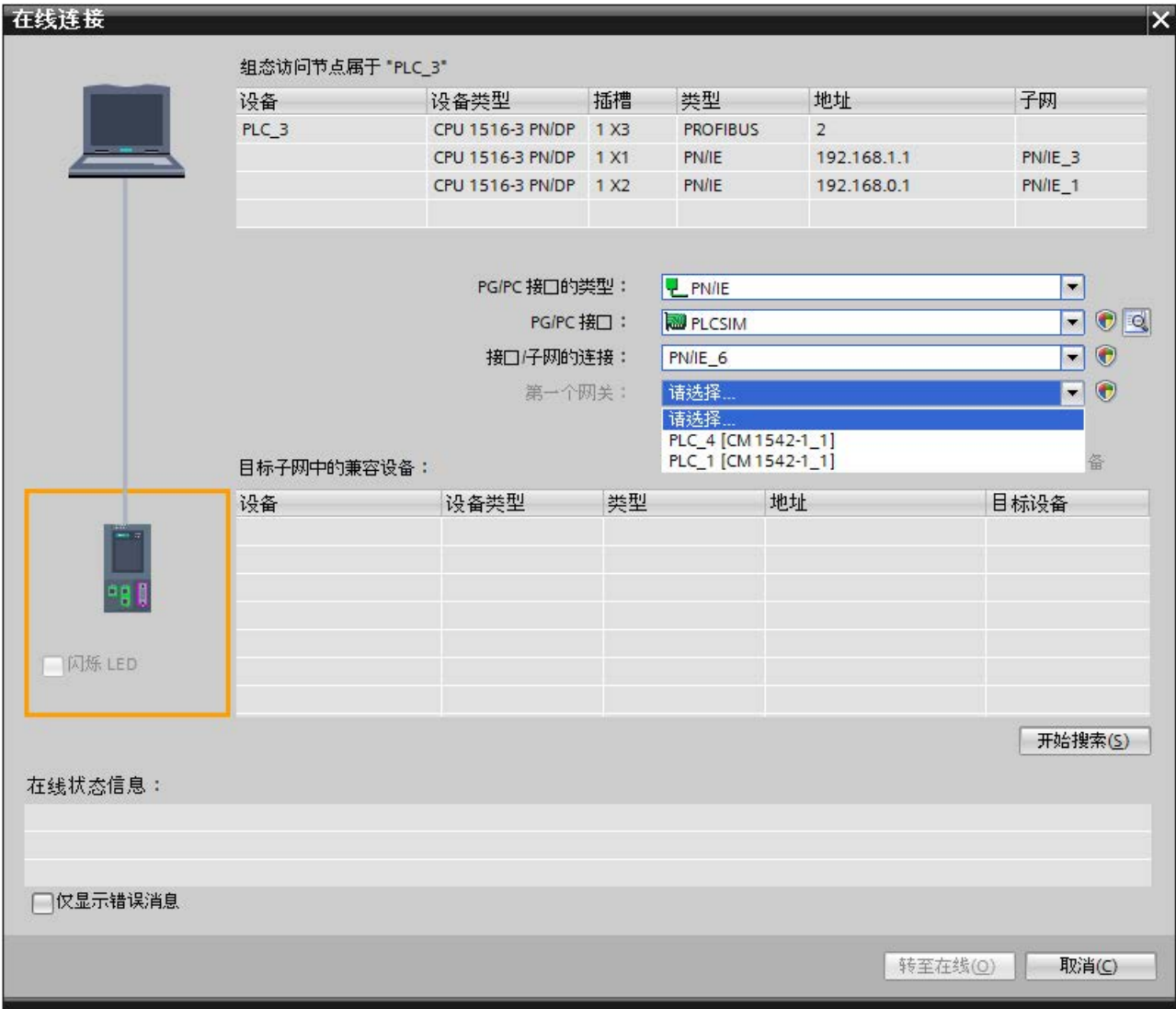


图 4-1 建立 PG 通信

4. 在表格“目标子网中的兼容设备”(Compatible devices in the target subnet) 中，选择相应的 CPU，并通过“转至在线”(Go online) 进行确认。

附加信息

有关“转至在线”(Go online) 的信息，请参见 STEP 7 的在线帮助。

HMI 通信

特性

使用 HMI 通信，一个或多个 HMI 设备（例如，HMI 精简面板/精智面板/移动面板）可通过 PROFINET 或 PROFIBUS DP 接口与 CPU 进行数据交换，以便操作员进行监控。通过 HMI 连接进行数据交换。

如果要设置与 CPU 之间的多个 HMI 连接，可使用：

- CPU 的 PROFINET 和 PROFIBUS DP 接口
- 带相关接口的 CP 和 CM

建立 HMI 通信的步骤

1. 在 STEP 7“设备与网络”(Devices & networks) 编辑器的网络视图中，可以在 CPU 的当前组态中组态 HMI 设备。
2. 选择“连接”(Connections) 按钮，并从下拉列表中选择“HMI 连接”(HMI connection)。
3. 在连接的断点（HMI 设备和 CPU）之间拖出一条线。端点用颜色突出显示。如果所需的 S7 子网尚不存在，则系统将自动创建。

4. 在“连接”(Connections) 选项卡中，选择 HMI 连接所在的行。

在“属性”(Properties) 选项卡的“常规”(General) 区域中，将显示 HMI 连接的属性，其中一些属性可以更改。

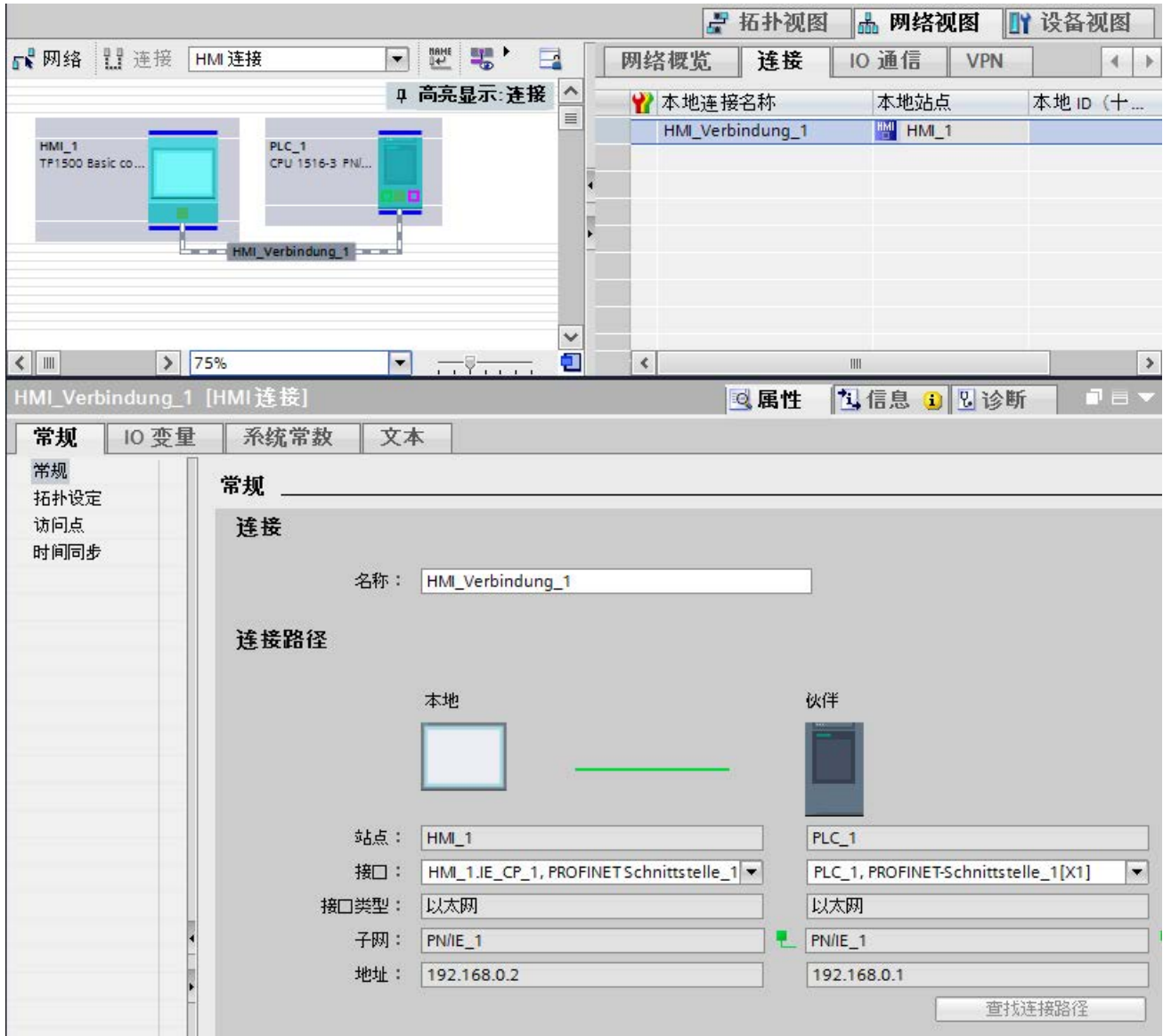


图 5-1 建立 HMI 通信

5. 将硬件组态下载到 CPU。

6. 将硬件组态下载到 HMI 设备。

附加信息

有关 HMI 的 S7 路由的信息，请参见“S7 路由 (页 71)”部分。

有关设置 HMI 连接的信息，请参见 STEP 7 的在线帮助。

开放式通信

6.1 开放式通信的概述

开放式通信的特点

通过开放式通信，CPU 可以与具有通信功能的其它模块进行数据交换。开放式通信具有以下主要特点：

- 开放式标准（通信伙伴可以是两个 SIMATIC CPU，也可以是 SIMATIC CPU 和适当的第三方设备）。
- 通过各种协议（在 STEP 7 中称为“连接类型”）进行通信
- 可传输的数据结构上具有高度灵活性。因此，通信设备只要支持这些连接类型，都可以进行开放式数据交换。
- 开放式通信可在各种自动化系统中实现，请参见相应手册的技术数据。

示例：

- CPU（S7-1500、ET 200SP CPU、S7-1500 软控制器）的集成式 PROFINET/工业以太网接口
- 通信模块（如 CP 1543-1、CM 1542-1）的 PROFINET 工业以太网接口

6.2 开放式通信的协议

开放式通信的协议

以下协议适用于开放式通信：

表格 6-1 开放式通信的传输协议

传输协议	所用接口
TCP ，遵循 RFC 793 标准	PROFINET/工业以太网
ISO-on-TCP ，遵循 RFC 1006 (Class 4) 标准	PROFINET/工业以太网
ISO ，遵循 ISO/IEC 8073 标准	工业以太网（仅 CP 1543-1）
UDP ，遵循 RFC 768 标准	PROFINET/工业以太网

表格 6-2 开放式通信的应用协议

应用协议	使用的传输协议
Modbus TCP	TCP ，遵循 RFC 793 标准
电子邮件	TCP ，遵循 RFC 793 标准
FTP	TCP ，遵循 RFC 793 标准

TCP、ISO-on-TCP、ISO、UDP

在进行数据传输之前，这些协议（UDP 除外）首先会建立与通信伙伴的传输连接。如果需防止数据丢失，则可以使用面向连接的协议。

采用 UDP 协议时，可以：

- 通过 CPU 的 PROFINET 接口或 CP 1543-1 的工业以太网接口，向 PROFINET 上的一个设备进行单播或向所有设备进行广播。
- 通过 CP 1543-1 的 PROFINET/工业以太网接口向组播组的所有接收方进行组播。

Modbus TCP

Modbus 协议是是一种基于主站/从站架构的通信协议，采用总线型拓扑。在 Modbus TCP（传输控制协议）中，数据作为 TCP/IP 数据包进行传输。

只有用户程序中的相关指令才能对通信进行控制。

电子邮件和 FTP

例如，可使用邮件来发送数据块内容的附件（如过程数据）。

可以使用 FTP 连接（FTP = 文件传输协议）与 S7 设备之间双向传输文件。

通信由客户端用户程序中的指令控制。

6.3 开放式通信的指令

简介

可通过以下方式建立相关连接（例如，TCP 连接）的开放式通信：

- 通过对通信伙伴的用户程序进行编程
- 通过在 STEP 7 的硬件和网络编辑器中组态连接

无论是通过编程建立连接还是通过组态建立连接，都需要在通信双方的用户程序中使用相应的指令发送和接收数据。

通过用户程序建立连接

如果通过编程建立连接，则需在用户程序中使用相应的指令建立和终止连接。

在某些应用领域中，通过用户程序建立连接而非通过硬件组态中的组态静态建立连接，反而更具有优势。这样，在需要建立连接时，只需通过一个特定的应用程序指令即可建立连接。如果选择通过编程建立连接，则将在数据传输结束后还将释放连接资源。

每个通信连接中都需要一个数据结构，用于保存建立连接的参数（例如，TCP 中的系统数据类型“TCON_IP_v4”）。

系统数据类型 (SDT) 由系统提供，这种数据类型预定义的结构不能更改。

各个协议都有自己的数据结构（见下表）。这些参数将保存在系统数据类型（如，TCON_IP_v4）的数据块中（“连接描述 DB”）。

可以通过两种方式创建带有这种数据结构的数据块：

- 手动创建这种数据块，并为其分配参数，然后再将该数据块直接写入指令中（建立电子邮件和 FTP 连接时，需要使用）
- 建议：在组态 TSEND_C、TRCV_C 和 TCON 指令的连接期间，在程序编辑器中的属性中自动创建数据块。

可以在“连接描述 DB”中修改连接的参数。

6.3 开放式通信的指令

通过编程建立连接时的协议、系统数据类型和可用指令

表格 6-3 通过编程建立连接时的指令

协议	系统数据类型	用户程序的指令
TCP	• TCON_IP_v4	建立连接并收/发数据: • TSEND_C/TRCV_C 或 • TCON、TSEND/TRCV (可通过 TDISCON 终止连接)
ISO-on-TCP	• TCON_IP_RFC	
ISO, 遵循 ISO/IEC 8073 (Class 4) 标准	• TCON_ISOOnative¹ • TCON_Configured	
UDP	• TCON_IP_v4 • TADDR_Param	建立连接并收/发数据: • TSEND_C/TRCV_C • TUSEND/TURCV (可通过 TDISCON 来终止连接)
Modbus TCP	• TCON_IP_v4	• MB_CLIENT • MB_SERVER
电子邮件	• TMAIL_v4 • TMAIL_v6 • TMAIL_FQDN	• TMAIL_C
FTP	• FTP_CONNECT_IPV4² • FTP_CONNECT_IPV6² • FTP_CONNECT_NAME²	• FTP_CMD

¹ 此协议只能与 CP 1543-1 一起使用

² 自定义数据类型

通过连接组态建立连接

通过连接组态建立连接时，将在 STEP 7 的硬件和网络编辑器中指定连接的地址参数。

发送和接收数据的指令与通过编程建立连接的指令相同：

表格 6-4 通过组态建立连接时的发送/接收指令

协议	通过组态建立连接时进行发送/接收
支持的指令：	
TCP	发送/接收数据： • TSEND_C/TRCV_C 或 • TSEND/TRCV
ISO-on-TCP	
ISO, 遵循 ISO/IEC 8073 (Class 4) 标准	
UDP	发送/接收数据： • TSEND_C/TRCV_C • TUSEND/TURCV
Modbus TCP	不支持
电子邮件	不支持
FTP	不支持

开放式通信的其它指令

可针对在用户程序中建立的连接以及组态的连接使用以下指令：

- T_RESET：终止和建立连接
- T_DIAG：检查连接

附加信息

STEP 7 在线帮助介绍了：

- 用户数据类型和系统数据类型
- 开放式通信的指令
- 连接参数

有关连接资源的分配和释放的信息，请参见连接资源分配 (页 78) 部分。

6.4 建立采用 TCP、ISO-on-TCP、UDP 和 ISO 协议的开放式通信

组态 TSEND_C、TRCV_C 或 TCON 指令的连接

要求：TSEND_C、TRCV_C 或 TCON 指令是在程序编辑器中创建的。

1. 在程序编辑器中，选择开放式用户通信的 TCON、TSEND_C 或 TRCV_C 块。
2. 在巡视窗口中，打开“属性 > 组态”(Properties > Configuration) 选项卡。

3. 选择“连接参数”(Connection parameters) 组。在选择连接伙伴之前，只启用了伙伴端点的空下拉列表。其它所有输入选项均被禁用。

同时显示一些已知的连接参数：

- 本地端点的名称
- 本地端点的接口
- 本地端点的 IPv4 地址（以太网子网）或 PROFIBUS 地址（PROFIBUS 子网）。

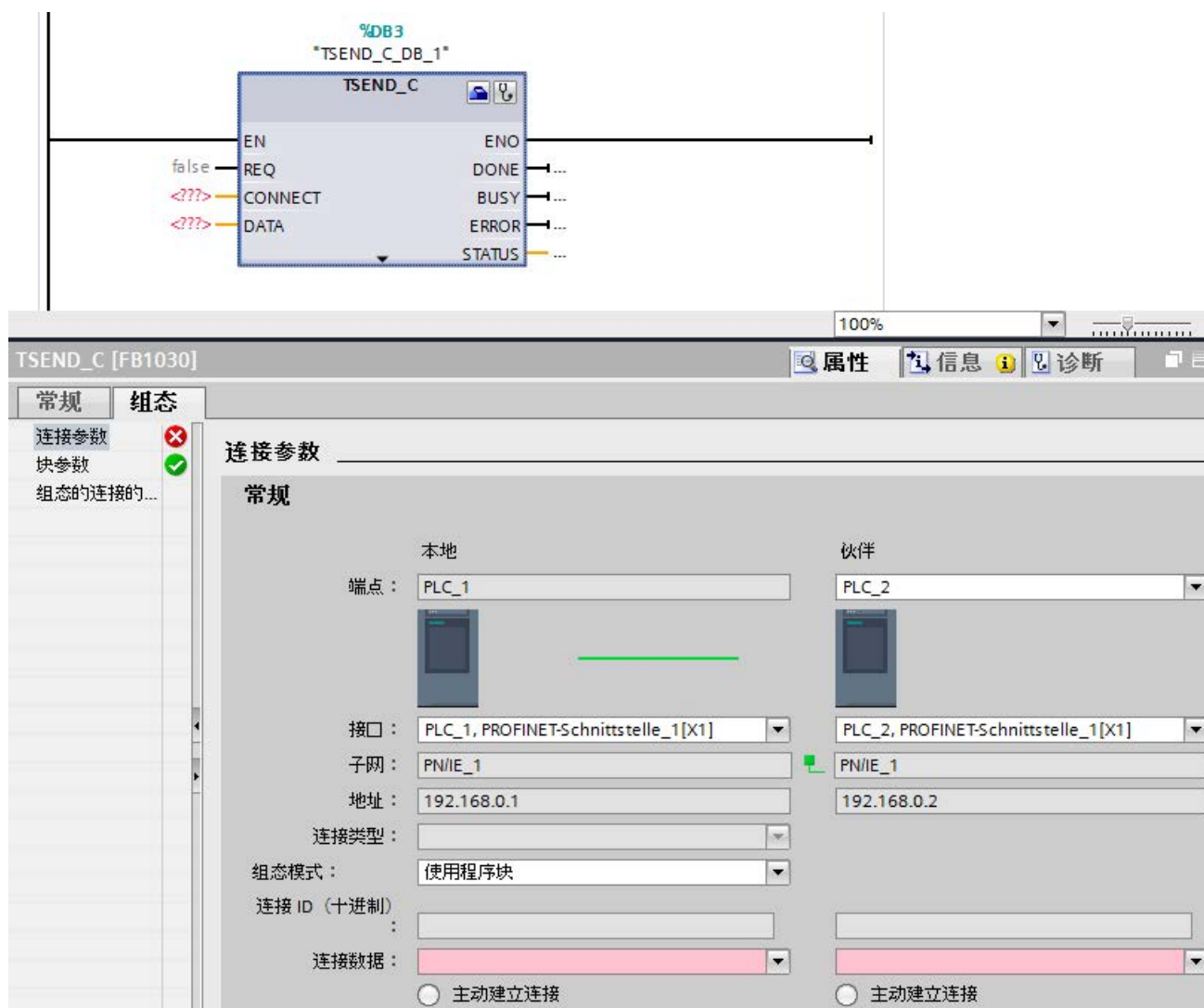


图 6-1 TSEND_C 的连接参数

4. 从伙伴端点的下拉列表框中，选择一个连接伙伴。可以选择项目中未指定的设备或 CPU 作为通信伙伴。随后会自动输入一些特定的连接参数。

用户需要设置以下参数：

- 伙伴端点的名称
- 伙伴端点的接口
- 伙伴端点的 IPv4 地址（以太网子网）或 PROFIBUS 地址（PROFIBUS 子网）。

如果连接伙伴已联网，则显示子网名称。

5. 在“组态类型”(Configuration type) 下拉列表中，选择使用程序块或使用组态的连接。
6. 在“连接数据”(Connection data) 下拉列表中选择现有连接描述 DB，或者对于已组态的连接，在“连接名称”(Connection name) 下选择现有连接。也可以新建连接描述 DB 或已组态的连接。之后，仍可以选择其它连接描述 DB 或已组态的连接，或者更改连接描述 DB 的名称，从而新建数据块：
 - 用户也可以在所选 TCON、TSEND_C 或 TRCV_C 指令的 CONNECT 输入参数互连中查看所选的数据块。
 - 如果已使用 TCON、TSEND_C 或 TRCV_C 指令的 CONNECT 参数为连接伙伴指定了连接描述 DB，则可使用此 DB 或创建一个新 DB。
 - 如果编辑下拉列表中所显示的数据块的名称，则会生成一个新数据块用于该连接，新数据块使用更改的名称，但结构和内容不变。
 - 更改的数据块名称在通信伙伴环境中必须唯一。
 - 连接描述 DB 必须具有结构 TCON_Param、TCON_IP_v4 或 TCON_IP_RFC，具体取决于 CPU 类型和连接。
 - 无法为未指定的伙伴选择数据块。

在选择或创建连接描述 DB 或已组态的连接后确定并输入其它值。

以下适用于指定的连接伙伴：

- ISO-on-TCP 连接类型
- 默认值为 1 的连接 ID
- 由本地伙伴方创建的主动连接建立
- TSAP ID
 - 对于 S7-1200/1500: E0.01.49.53.4F.6F.6E.54.43.50.2D.31
 - 对于 S7-300/400: E0.02.49.53.4F.6F.6E.54.43.50.2D.31

以下适用于未指定的连接伙伴：

- TCP 连接类型
- 伙伴端口 2000

以下适用于带有指定连接伙伴的已组态连接：

- TCP 连接类型
- 默认值为 257 的连接 ID
- 由本地伙伴方创建的主动连接建立
- 伙伴端口 2000

以下适用于带有未指定连接伙伴的已组态连接：

- TCP 连接类型
- 本地端口 2000

7. 输入连接伙伴所需的连接 ID。不能为未指定的伙伴分配任何连接 ID。

说明

必须为已知连接伙伴的连接 ID 输入一个唯一值。连接参数的设置不会检查连接 ID 是否唯一，在创建新连接时不会为连接 ID 输入默认值。

8. 从相关的下拉列表中选择所需的连接类型。根据连接类型设定详细地址信息的默认值。可在以下类型中选择：

- TCP
- ISO-on-TCP
- UDP
- ISO（仅适用于组态模式“使用已组态的连接”(Use configured connection)）

可以编辑地址详细信息中的输入框。根据所选的协议，可以编辑端口（TCP 和 UDP）或 TSAP（ISO-on-TCP 和 ISO）。

9. 使用“主动连接建立”(Active connection establishment) 复选框来设置 TCP、ISO 和 ISO-on-TCP 的连接建立特性。用户可以决定主动建立连接的通信伙伴。

连接组态将立即检查更改后的值是否存在输入错误，然后将值输入连接描述数据块中。

说明

只有在将伙伴端点的程序段下载到硬件后，两个通信伙伴之间才能进行开放式用户通信。要实现功能完整的通信，应确保在设备上不仅装载了本地 CPU 的连接描述，而且还装载了伙伴 CPU 的连接描述。

组态连接，例如，针对 TSEND/TRCV

如果要将 TSEND/TRCV 指令用于开放式通信，首先需要组态连接（例如，TCP 连接）。

要组态 TCP 连接，请按以下步骤操作：

1. 在 STEP 7 的“设备与网络”(Devices & networks) 编辑器的网络视图中，组态通信伙伴。
2. 单击“连接”(Connections) 按钮，然后从下拉列表中选择“TCP 连接”(TCP connection) 连接类型。
3. 使用拖放操作，将通信伙伴相互连接（通过接口或本地端点）。如果所需的 S7 子网尚不存在，则系统将自动创建。
还可以设置与未指定伙伴的连接。
4. 从网络视图中选择已创建的连接。
5. 在“属性”(Properties) 选项卡的“常规”(General) 区域中，设置连接的属性（例如，连接名称和将使用的通信伙伴接口）。
若要连接到未指定的伙伴，请设置该伙伴的地址。
可在“本地 ID”(Local ID) 区域中查找本地 ID（用户程序中的连接参考）。
6. 在项目树中，选择用于 1 个 CPU 的“程序块”(Program blocks) 文件夹。双击文件夹，打开文件夹中的 OB1。将打开程序编辑器。
7. 从“指令”(Instructions) 任务卡中“通信”(Communication) 区域内的“开放式通信”(Open communication) 中，选择所需的指令（如 TSEND）并拖放到 OB1 中的程序段中。
8. 通过该指令的 ID 参数，指定要用于数据传输的已组态连接的本地 ID。
9. 互连 TSEND 指令的“DATA”参数和数据块中的用户数据。
10. 将硬件组态和用户程序下载到 CPU。

按照以上步骤，通过接收指令 TRCV 建立与伙伴 CPU 的连接，并将下载到该 CPU 上。

使用 CP 1543-1 进行 ISO 连接时的注意事项

使用“ISO 连接”(ISO connection) 连接类型时，如果要通过 MAC 地址进行寻址，则需在 CP 的属性中选中复选框“使用 ISO 协议”(Use ISO protocol)。



图 6-2 选择 CP 1543-1 ISO 协议

附加信息

STEP 7 在线帮助介绍了：

- 开放式通信的指令
- 连接参数

6.5 建立与 Modbus TCP 的通信

通过用户程序建立 Modbus TCP 连接

使用指令 MB_CLIENT 或 MB_SERVER，可以在程序编辑器中分配参数。

设置通过 Modbus TCP 进行通信的步骤

MB_CLIENT 指令作为 Modbus TCP 客户端通过 TCP 连接进行通信。通过该指令，可以在客户端和服务器之间建立连接、向服务器发送 Modbus 请求并接收相应的 Modbus 响应。用户还可以使用该指令控制 TCP 连接的设置。

MB_SERVER 指令作为 Modbus TCP 服务器通过 TCP 连接进行通信。该指令将处理 Modbus 客户端的连接请求、接收并处理 Modbus 请求并发送响应。用户还可以控制 TCP 连接的设置。

要求： 只要涉及到 IP，客户端和服务器就需要通过一个 S7 子网 (PROFINET) 来连接。

1. 在 STEP 7 的“设备与网络”(Devices & Networks) 编辑器的网络视图中，组态带有 CPU 的 S7-1500 自动化系统。
2. 在项目树中，选择“程序块”(Program blocks) 文件夹。双击该文件夹，打开文件夹中的 OB1。将打开程序编辑器。
3. 从“指令”(Instructions) 任务卡中“通信”(Communication) 区域内的“其它”(Other) 中的“MODBUS TCP”，选择所需的指令（如 MB_CLIENT）并拖放到 OB1 的程序段中。

4. 分配 MB_CLIENT 或 MB_SERVER 指令的参数。请遵守以下规则：

必须为每个 MB_CLIENT 连接指定 IPv4 服务器地址。

每个 MB_CLIENT 或 MB_SERVER 连接都必须使用具有数据结构 TCON_IP_v4 的唯一背景数据块。

连接 ID 与背景数据块组合成对，对于每个连接，组合对都必须唯一。

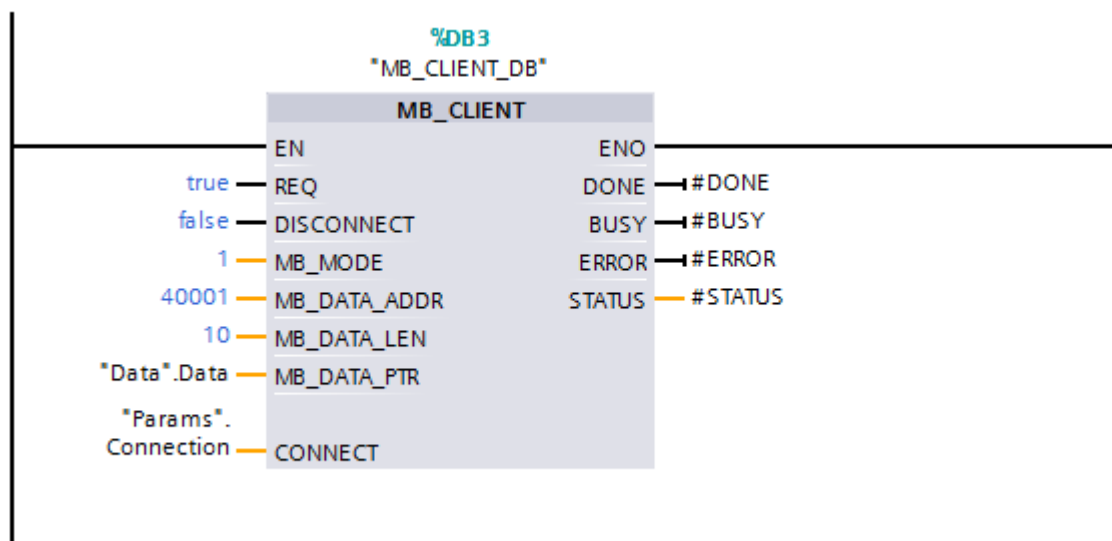


图 6-3 MB_CLIENT

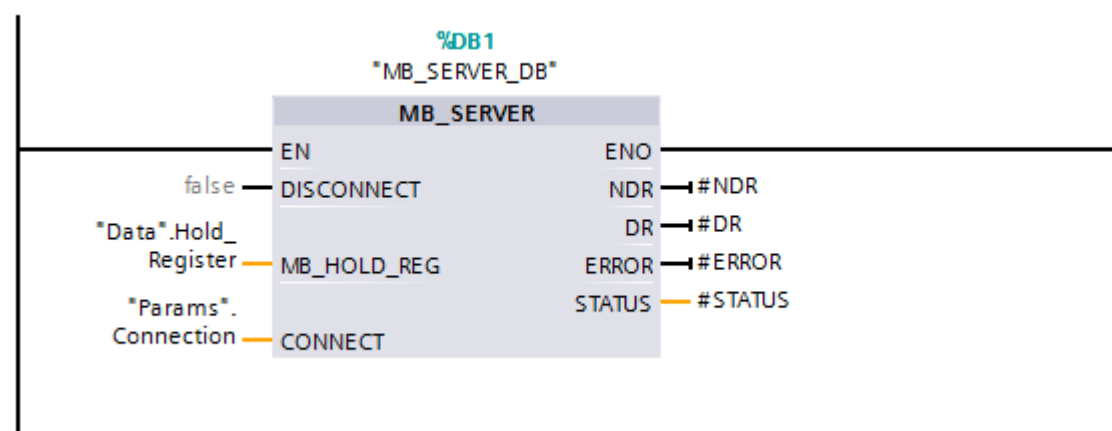


图 6-4 MB_SERVER

5. 将硬件组态和用户程序下载到 CPU。

Modbus TCP 服务器作为连接到 Modbus RTU 的网关

如果使用 Modbus TCP 服务器作为连接到 Modbus RTU 协议的网关，请使用静态参数 MB_UNIT_ID 对串行网络中的从站设备编址。MB_UNIT_ID 参数对应于 Modbus RTU 协议中该从站地址的字段。在此情况下，MB_UNIT_ID 参数会将请求转发到正确的 Modbus RTU 从站地址。

用户不必自己对网关功能编程。

可以在与 MB_CLIENT 指令关联的背景数据块中找到 MB_UNIT_ID 参数。

有关 MB_UNIT_ID 参数的更多信息，请参见 STEP 7 在线帮助。

6.6 通过电子邮件建立通信

通过用户程序建立电子邮件连接

在通过电子邮件进行通信时，需要手动创建相关系统数据类型的数据块并分配参数和直接调用指令。以下将介绍具体的操作步骤。

建立通过电子邮件进行通信的步骤

CPU 可以发送电子邮件。通过 TMAIL_C 指令，从 CPU 的用户程序发送电子邮件。

要求： 可通过 IPv4 网络访问 SMTP 服务器。

1. 在 STEP 7 的“设备与网络”(Devices & Networks) 编辑器的网络视图中，组态带有 CPU 的 S7-1500 自动化系统。
2. 在指令 TMAIL_C 中设置 SMTP 服务器的地址参数。（建议：指定附录名称。）
3. 创建一个全局数据块，并在此数据块内创建类型为 TMAIL_v4、TMAIL_v6（仅限 CP 1543-1）或 TMAIL_FQDM（仅限 CP 1543-1）的变量。
4. 将该变量连接到 TMAIL_C 指令的 MAIL_ADDR_PARAM 参数。
5. 将硬件组态和用户程序下载到 CPU。

附加信息

STEP 7 在线帮助介绍了：

- 系统数据类型
- 开放式通信的指令
- 连接参数

6.7 通过 FTP 建立通信

通过用户程序建立 FTP 连接

在通过 FTP 进行通信时，必须手动创建相关系统数据类型的数据块，并分配参数和直接调用指令。以下将介绍具体的操作步骤。

FTP 客户端和服务器的功能

CPU 可以将文件发送到 FTP 服务器，也可以从 FTP 服务器接收文件。S7-1500 中只能通过 CP 1543-1 进行 FTP 通信。该 CP 既可以作为 FTP 服务器，也可以作为 FTP 客户端，或者可以同时作为服务器和客户端。FTP 客户端可以是第三方系统/PC。

在 STEP 7 中对 CP 进行相应的组态后，FTP 服务器才能正常运行。

使用 FTP 的客户端功能，可以建立和终止 FTP 连接、传输以及删除服务器上的文件。

FTP 的客户端功能将调用 FTP_CMD 指令。

设置 FTP 服务器功能的步骤

要求： 可通过 IPv4 网络访问 FTP 服务器。

1. 在 STEP 7 的“设备与网络”(Devices & Networks) 编辑器的设备视图中，组态带有 CPU 和 CP 1543-1 的 S7-1500 自动化系统。

同时，用户需要在“连接机制”(Connection mechanisms) 部分的“保护”(Protection) 区域导航下 S7-1500 CPU 的硬件组态内选中复选框“允许借助 PUT/GET 通信从远程伙伴 (PLC、HMI、OPC...) 访问”(Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...))。

2. 在“FTP 组态”(FTP configuration) 中的 CP 属性内，进行以下设置：

- 选择复选框“使用 FTP 服务器传送 S7 CPU 数据”(Use FTP server for S7 CPU data)。
- 指定要存储 FTP DB 的 CPU、数据块和文件名称。

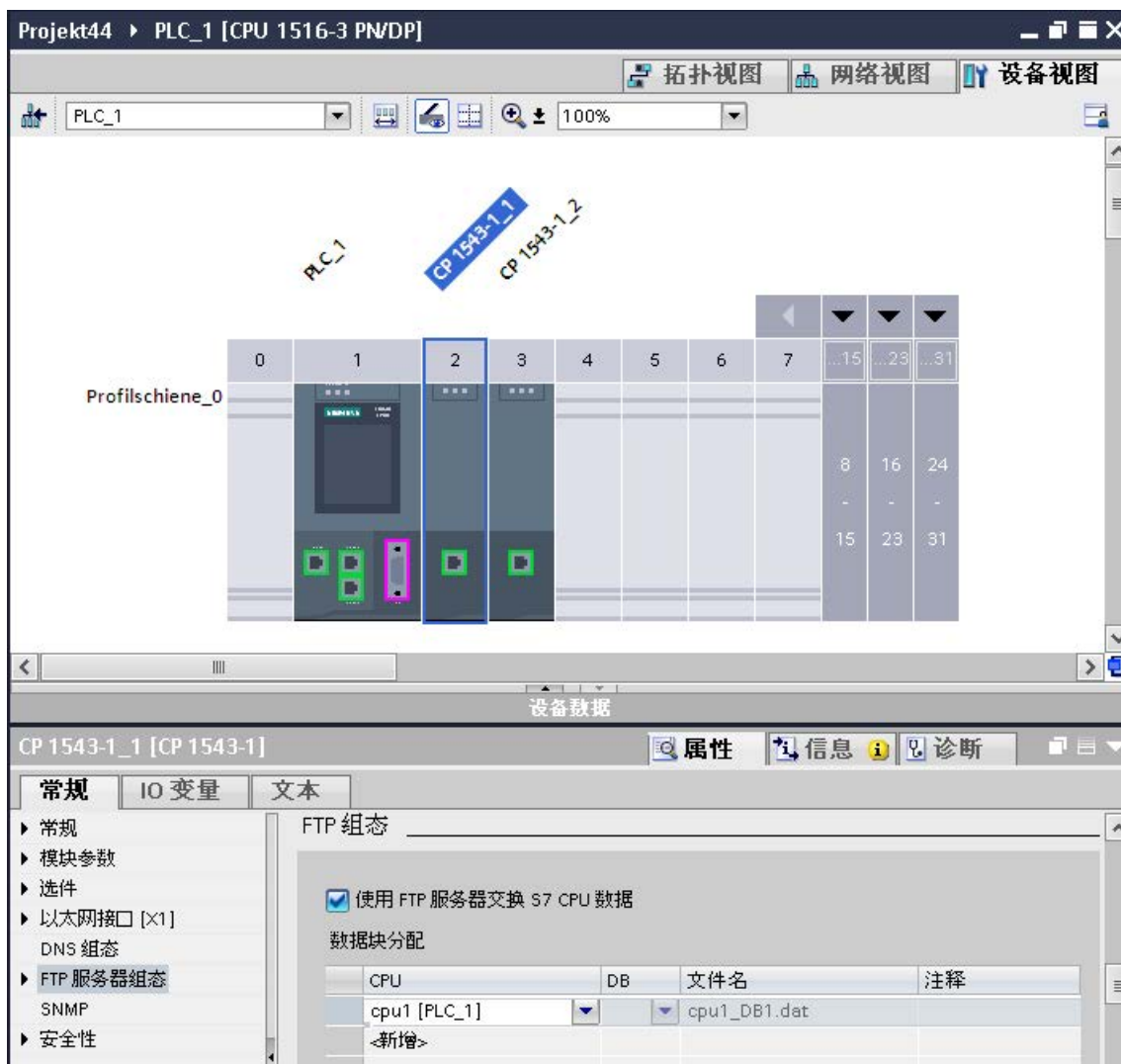


图 6-5 设置 FTP 组态

3. 将硬件组态下载到 CPU。

设置 FTP 客户端功能的步骤

要求： 可通过 IPv4 网络访问 FTP 服务器。

1. 在 STEP 7 的“设备与网络”(Devices & Networks) 编辑器的设备视图中，组态带有 CPU 和 CP 1543-1 的 S7-1500 自动化系统。

同时，用户需要在“连接机制”(Connection mechanisms) 部分的“保护”(Protection) 区域导航下 S7-1500 CPU 的硬件组态内选中复选框“允许借助 PUT/GET 通信从远程伙伴 (PLC、HMI、OPC...) 访问”(Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...))。

2. 在 CPU 的用户程序中调用 FTP_CMD 指令。
3. 在指令 FTP_CMD 中设置 FTP 服务器的连接参数。
4. 创建一个全局数据块，并在此数据块内创建一个 FTP_CONNECT_IPV4、FTP_CONNECT_IPV6 或 FTP_CONNECT_NAME 类型的变量。
5. 将数据块内的变量与 FTP_CMD 指令互连。
6. 要连接 FTP 服务器，需要在 DB 中指定以下参数：
 - 进行 FTP 访问的相关数据类型 (FTP_CONNECT_IPV4、FTP_CONNECT_IPV6 或 FTP_CONNECT_NAME) 的用户名、密码和 IP 地址
7. 将硬件组态和用户程序下载到 CPU。

附加信息

STEP 7 在线帮助介绍了：

- 系统数据类型
- 开放式通信的指令
- 连接参数

6.8 建立和终止通信关系

建立和终止通信

下表显示了如何建立和终止开放式通信中的通信。

表格 6-5 建立和终止通信

设置连接	建立通信	终止通信
通过用户程序	将用户程序下载到 CPU 之后： 通信被动方将通过调用 TSEND_C/TRCV_C 或 TCON 建立本地通信访问。通信主动方则通过调用 TSEND_C/TRCV_C 或 TCON 开始建立连接。如果无法建立连接，则将向用户程序中的指令发送一条正反馈。 在终止与 T_RESET 指令的连接后，将会重新建立连接。 如果连接中止，则通信主动方将尝试重新建立连接。仅当事先与 TCON 成功建立了连接时，才会这样。	• 使用 TSEND_C/TRCV_C、TDISCON 和 T_RESET 指令 • 将 CPU 从 RUN 模块切换到 STOP 模式时 • CPU 断电/通电
通过组态建立连接时	将连接组态和用户程序下载到 CPU 之后。	删除 STEP 7 中的连接组态并将更改后的组态下载到 CPU 中。

S7 通信

S7 通信的特点

S7 通信作为 SIMATIC 的同构通信，属于 SIMATIC CPU 之间进行供应商相关的通信（非开放式标准）。在移植和连接现有系统（S7-300、S7-400）进行通信时通常使用 S7 通信。

对于两个 S7-1500 自动化系统之间的数据传输，建议使用开放式通信（请参见开放式通信 (页 35) 部分）。

S7 通信的属性

通过 S7 通信，CPU 可与另一个 CPU 交换数据。一旦用户在接收端接收到数据，就将自动向发送端 CPU 确认已接收到数据。

通过所组态的 S7 连接进行数据交换。S7 连接可以在一端或者同时在两端进行组态。

S7 通信可通过以下方式进行：

- CPU 的集成 PROFINET 或 PROFIBUS DP 接口
- CP/CM 的接口

在一端组态 S7 连接

对于在一端组态的 S7 连接，仅在一个通信伙伴中组态此连接并且仅下载到此伙伴。

可以组态一个连接到一台 CPU 的单向 S7 连接，该 CPU 仅作为 S7 连接的服务器（例如，CPU 315-2 DP）。该 CPU 已组态，因此其地址参数和接口也是已知的。

另外，还可以组态一个连接到伙伴的单向 S7 连接，该伙伴不在项目中，其地址参数和接口都未知。因此，需要输入地址；STEP 7 不对其进行检查。开始时未指定伙伴（创建 S7 连接时未注册伙伴地址）。输入地址后，该地址是“未知”的（即虽然已命名，但项目是未知的）。

这样便可在项目之外使用 S7 连接。本地项目将无法识别该通信伙伴（未指定），将在另一个 STEP 7 或第三方项目中进行组态。

在两端组态 S7 连接

在两端同时组态 S7 连接时，将同时在两个通信伙伴中组态和下载所组态的 S7 连接参数。

S7 通信的指令

与 S7-1500 进行 S7 通信时，可以使用以下指令：

- PUT/GET

可使用指令“PUT”，将数据写入一个远程 CPU。使用指令“GET”从远程 CPU 读取数据。PUT 和 GET 指令是单向指令，也就是说，只需在一个通信伙伴中有该指令即可。通过连接组态，可方便地设置 PUT 和 GET 指令。

说明

PUT/GET 指令的数据块

使用 PUT/GET 指令时，只能使用进行绝对寻址的数据块。不能使用进行符号寻址的数据块。

用户还必须在“保护”(Protection) 区域启用此服务以保护 CPU 组态。

- BSEND/BRCV

指令“BSEND”可将数据发送到类型为“BRCV”的远程伙伴指令。指令“BRCV”从类型为“BSEND”的远程伙伴指令接收数据。可通过指令对“BSEND/BRCV”进行 S7 通信，以实现安全数据传输。

- USEND/URCV

指令“USEND”可将数据发送到类型为“URCV”的远程伙伴指令。指令“URCV”从类型为“USEND”的远程伙伴指令接收数据。无论通信伙伴的处理时间如何，用户都可通过指令对“BSEND/BRCV”进行 S7 通信，以实现快速的非安全数据传输，例如，传输操作和维护消息。

从站模式下的 PROFIBUS DP 接口

在 STEP 7 中的通信模块（如 CM 1542-5）PROFIBUS DP 接口属性中，有一个“测试、调试和路由”(Test, commissioning, routing) 复选框。通过该复选框，可以确定将 DP 从站上的 PROFIBUS DP 作为 PROFIBUS 上的主动设备或被动设备。

- 选中复选框：该从站将作为 PROFIBUS 上的主动设备。只能为该 DP 从站建立两端组态的 S7 连接。
- 禁用复选框：DP 从站将作为 PROFIBUS 上的被动设备。只能为该 DP 从站建立一端组态的 S7 连接。



图 7-1 “测试、调试和路由”(Test, commissioning, routing) 复选框

组态 PUT/GET 指令的 S7 连接

可以创建 S7 连接并在指定 PUT/GET 指令的连接参数时分配这些连接的参数。分配连接参数时，会立即检查更改的值有无输入错误。

要求：PUT 或 GET 指令是在程序编辑器中创建的。

要使用 PUT/GET 组态 S7 连接，请按以下步骤操作：

1. 在程序编辑器中，选择调用 PUT 或 GET 指令。
2. 在巡视窗口中，打开“属性 > 组态”(Properties > Configuration) 选项卡。

3. 选择“连接参数”(Connection parameters) 组。在选择连接伙伴之前，只启用了伙伴端点的空下拉列表。其它所有输入选项均被禁用。

同时显示一些已知的连接参数：

- 本地端点的名称
- 本地端点的接口
- 本地端点的 IPv4 地址

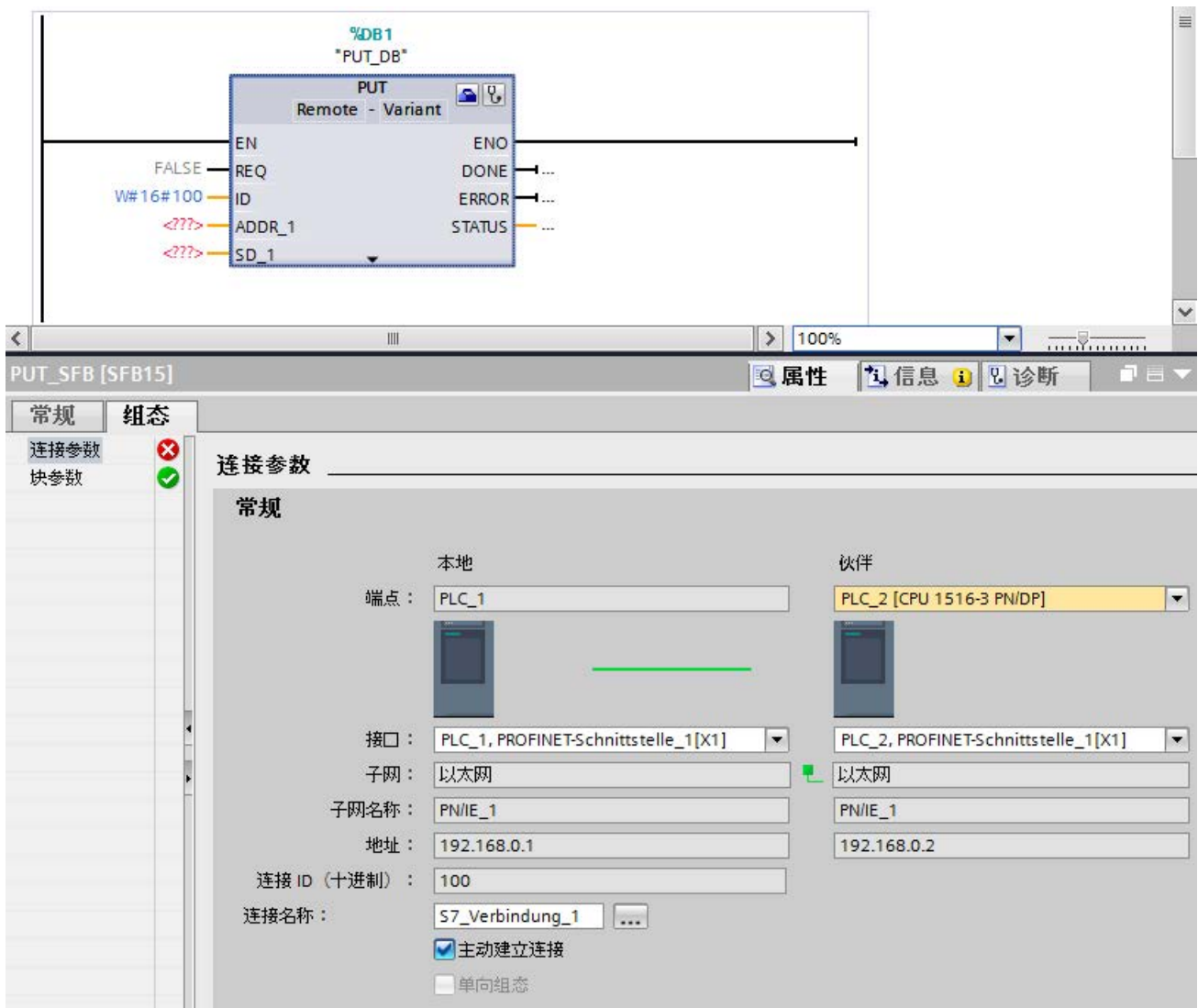


图 7-2 PUT 指令的连接组态

4. 从伙伴端点的下拉列表框中，选择一个连接伙伴。可以选择项目中未指定的设备或 CPU 作为通信伙伴。

选择连接伙伴后，会自动输入以下参数：

- 伙伴端点的名称
- 伙伴端点的接口。如果有多个接口，则可根据需要更改接口。
- 伙伴端点的接口类型
- 两个端点的子网名称
- 伙伴端点的 IPv4 地址
- 用于通信的连接的名称。

5. 如果需要，请在“连接名称”(Connection name) 输入框中更改连接名称。如果要创建新连接或编辑现有连接，请单击“创建新连接”(Create new connection) 图标。

说明

仅当已将伙伴端点的硬件配置和程序部分加载到硬件中后，两个通信伙伴之间的 PUT 和 GET 指令才能运行。要实现功能完整的通信，应确保在设备上不仅装载了本地 CPU 的连接描述，而且还装载了伙伴 CPU 的连接描述。

组态 BSEND/BRCV 的 S7 连接

例如，如果要使用 BSEND/BRCV 指令进行 S7 通信，首先需要组态 S7 连接。

要组态 S7 连接，请按以下步骤操作：

1. 在 STEP 7 的“设备与网络”(Devices & networks) 编辑器的网络视图中，组态通信伙伴。
2. 选择“连接”(Connections) 按钮，并从下拉列表中选择“S7 连接”(S7 connection) 条目。
3. 使用拖放操作，将通信伙伴相互连接（通过接口或本地端点）。如果所需的 S7 子网尚不存在，则系统将自动创建。

还可以设置与未指定伙伴的连接。

4. 在选项卡“连接”(Connections) 中，选择 S7 连接所在的行。
5. 在“属性”(Properties) 选项卡的“常规”(General) 区域中，设置 S7 连接的属性（例如，连接名称和将使用的通信伙伴接口）。

若要建立与未指定的伙伴间的 S7 连接，请设置该伙伴的地址。

可在“本地 ID”(Local ID) 区域中找到本地 ID（用户程序中的 S7 连接参考）。

6. 在项目树中，选择用于 1 个 CPU 的“程序块”(Program blocks) 文件夹。双击文件夹，打开文件夹中的 OB1。将打开程序编辑器。
7. 在程序编辑器中，如果在一端组态 S7 连接，则在通信伙伴的用户程序中调用相关的指令进行 S7 通信；如果在两端组态，则在通信伙伴的用户程序中调用。例如，从“指令”(Instructions) 任务卡中的“通信”(Communication) 区域内，选择 BSEND 和 BRCV 指令，并将其拖放到 OB1 的一个程序段中。
8. 通过该指令的 ID 参数，指定要用于数据传输的已组态连接的本地 ID。
9. 指定指令的参数，以标识待读取/写入的数据以及数据的来源和目的地。
10. 将硬件组态和用户程序下载到 CPU。

通过 CP 1543-1 进行 S7 通信

如果通过 CP 1543-1 的工业以太网接口建立 S7 通信，则可以在 S7 连接属性的“常规”(General) 区域中选择数据传输的传输协议：

- 选中“TCP/IP”复选框（默认选中）：ISO-on-TCP (RFC1006)：在 S7-1500 CPU 间进行 S7 通信
- 禁用“TCP/IP”复选框：ISO 协议 (IEC8073)：使用 MAC 地址进行寻址

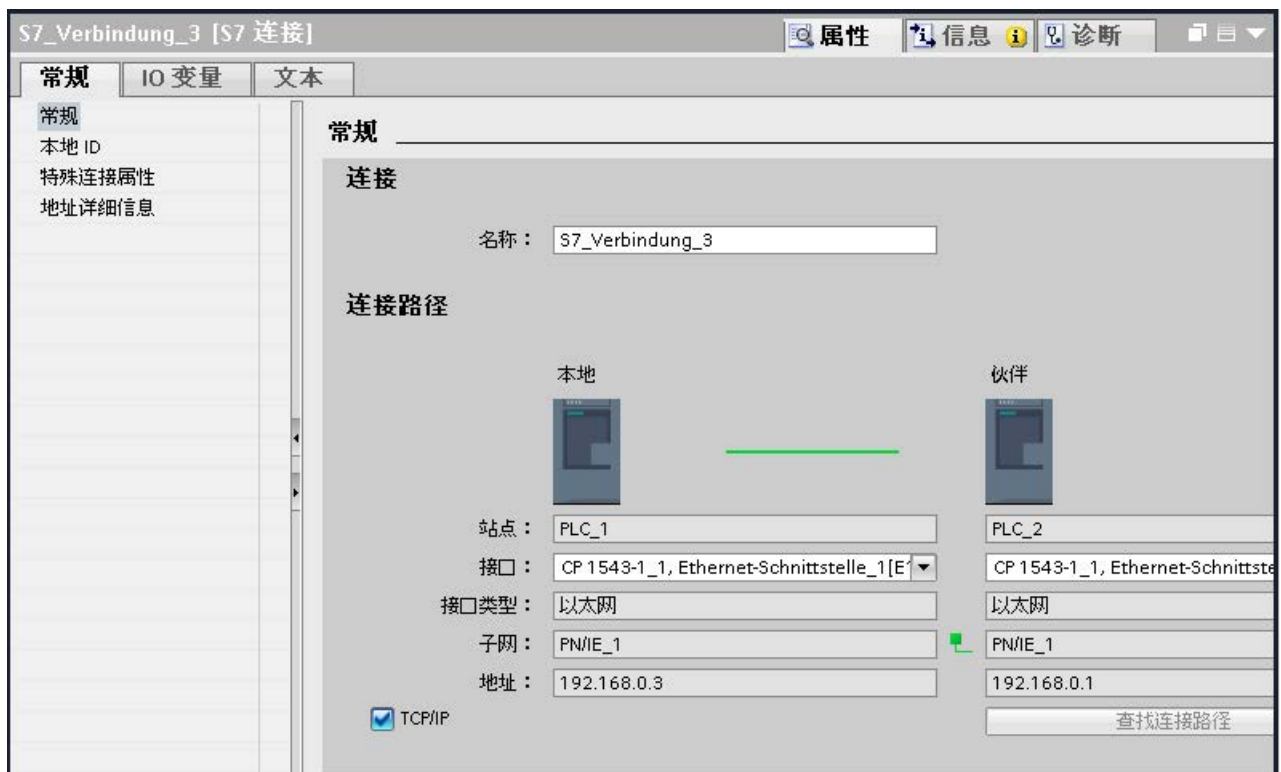


图 7-3 选择 CP 1543-1 的传输协议

建立不同 S7 子网间 S7 连接的步骤

可以在多个 S7 子网间（PROFIBUS、PROFINET/工业以太网）建立 S7 连接（S7 路由）。

1. 在 STEP 7 的“设备与网络”(Devices & networks) 编辑器的网络视图中，组态通信伙伴。
2. 选择“网络”(Network) 按钮。
3. 通过拖放操作，连接 S7 子网（PROFIBUS、PROFINET/工业以太网）中的相应接口。

4. 选择“连接”(Connections) 按钮，并从下拉列表中选择“S7 连接”(S7 connection) 条目。
5. 在本例中，通过拖放操作将左侧 S7 子网 (PROFIBUS) 中的 PLC_1 连接到右侧 S7 子网 (PROFINET) 中的 PLC_3。

已组态 CPU 1 和 CPU 3 之间的 S7 连接。

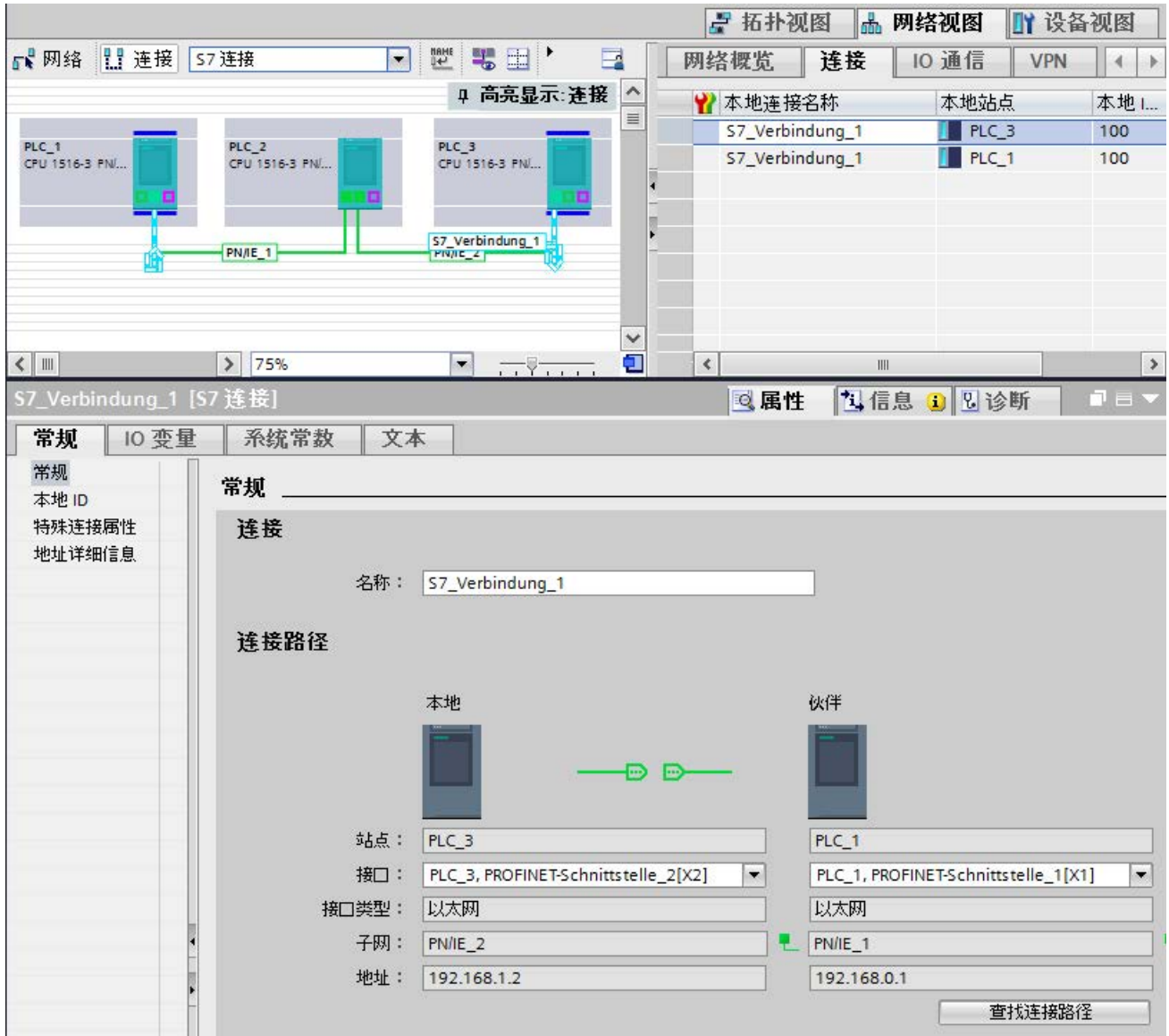


图 7-4 通过不同子网进行 S7 连接

CPU 1515SP PC 作为 S7 连接的路由器

如果将 "PROFINET onboard [X2]" 接口分配给 SIMATIC PC 站的 CPU 1515SP PC，CPU 1515SP PC 便可用作 S7 连接的路由器。在 CP 接口 "PROFINET onboard [X2]" 上设置“无，或其它 Windows 设置”(None, or a different Windows setting) 时，CPU 1515SP PC 无法用作路由的 S7 连接的路由器。

如果 CPU 1515SP PC 分配的接口从“SIMATIC PC 站”(SIMATIC PC station) 更改为“无，或其它 Windows 设置”(None, or a different Windows setting)，CPU 1515SP PC 路由的现有 S7 连接将失效。由于 PLC 现在不再处理此连接的路由功能，因此在编译 CPU 1515SP PC 时，将不会显示与无效连接相关的消息。在编译连接的端点时，将仅显示路由的无效 S7 连接。

路由的 S7 连接所需的接口必须在 CPU 1515SP PC 上明确指定。可以在“PROFINET 内置 [X2] > 接口分配”(PROFINET onboard [X2] > Interface assignment) 下的属性中编辑 CPU 1515SP PC 的接口分配。

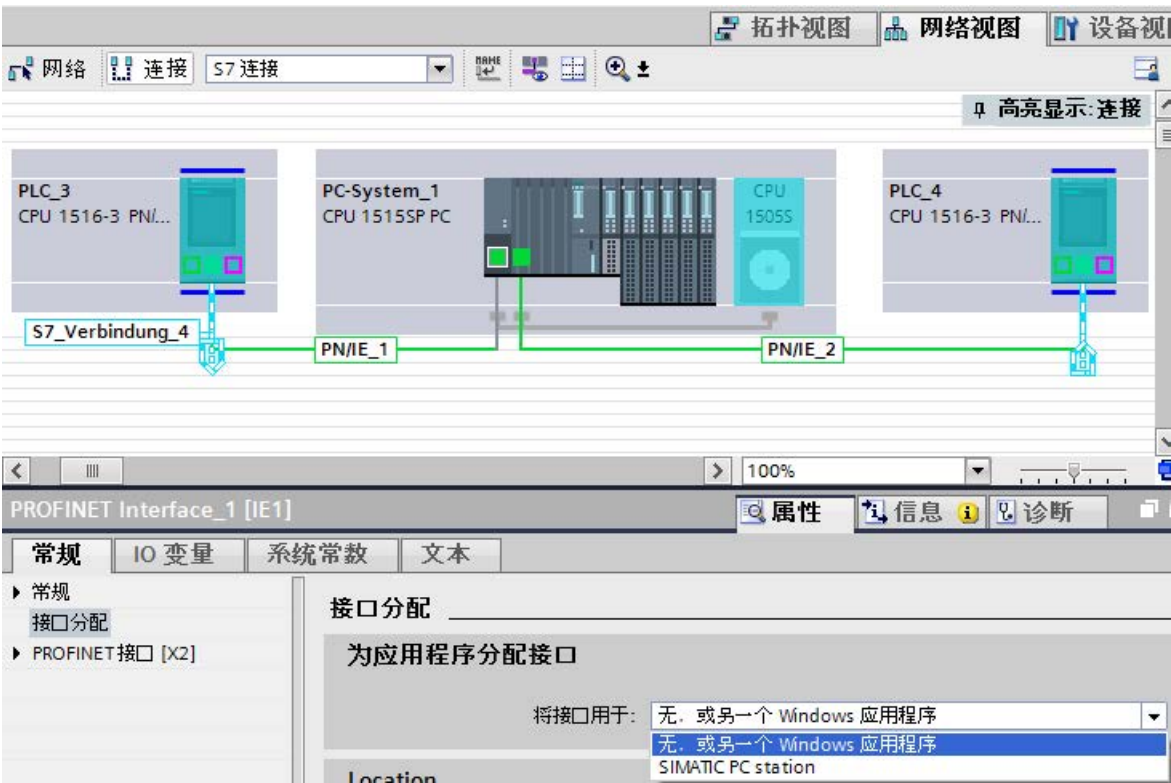


图 7-5 S7 路由 PC 站

附加信息

有关 S7 连接组态和如何在用户程序中使用 S7 通信指令的详细信息，请参见 STEP 7 在线帮助。

点对点链接

功能

可通过带有串口（RS232、RS422 或 RS485）的通信模块 (CM) 建立 S7-1500、ET 200MP 和 ET 200SP 的点对点连接。

- S7-1500/ET 200MP:
 - CM PtP RS232 BA
 - CM PtP RS422/485 BA
 - CM PtP RS232 HF
 - CM PtP RS422/485 HF
- ET 200SP:
 - CM PtP

通过点对点连接，通信模块与具有通信能力的第三方系统或设备之间可以进行双向数据交换。点对点通信需要至少两个通信伙伴。通过 RS422 和 RS485，可以在两个以上通信伙伴间进行通信。

点对点连接的通信协议

- Freeport 协议（也称为 ASCII 协议）
- 3964(R) 协议
- RTU 格式的 Modbus 协议（RTU：远程终端设备）
- USS 协议（通用串行接口协议）

根据 ISO/OSI 参考模型，这些协议将使用不同层：

- Freeport：使用第 1 层（物理层）
- 3964 (R)、USS 和 Modbus：使用第 1 层和第 2 层（物理层和数据链路层。因此，与 Freeport 相比，传输的可靠性更高）。USS 和 Modbus 还另外使用第 4 层。

Freeport 协议的特性

- 通过一个可选的结束条件（例如，超出字符延时时间、收到结束字符、收到一定数量的数据），接收方可以识别出数据传输是否结束。
- 但发送方无法识别接收方所接收到的发送数据有无错误。

3964 (R) 程序的特性

- 发送数据时，将添加一些控制字符（起始、结束和块校验字符）。请确保这些控制字符不作为数据包含在帧中。
- 可通过这些控制字符建立和终止连接。
- 如果发生传输错误，则将自动重新传输数据。

通过 Freeport 或 3964 (R) 通信进行数据交换

待发送的数据将存储在相应 CPU 数据块的用户程序（发送缓冲区）中。通信模块上的接收缓冲区将用于存储接收数据。检查接收缓冲区的属性，必要时进行调整。必须创建用于在 CPU 中接收的数据块。

在 CPU 的用户程序中，可通过“Send_P2P”和“Receive_P2P”指令在 CPU 和 CM 间进行数据传输。

建立 Freeport 或 3964 (R) 通信的步骤

1. 在 STEP 7 的硬件和网络编辑器的设备视图中，组态一个带有 CPU 和 CM 的 S7-1500 组态。
2. 在“属性”(Properties) 选项卡的“常规”(General) 区域内，指定 CP 接口的参数（协议、端口参数）。

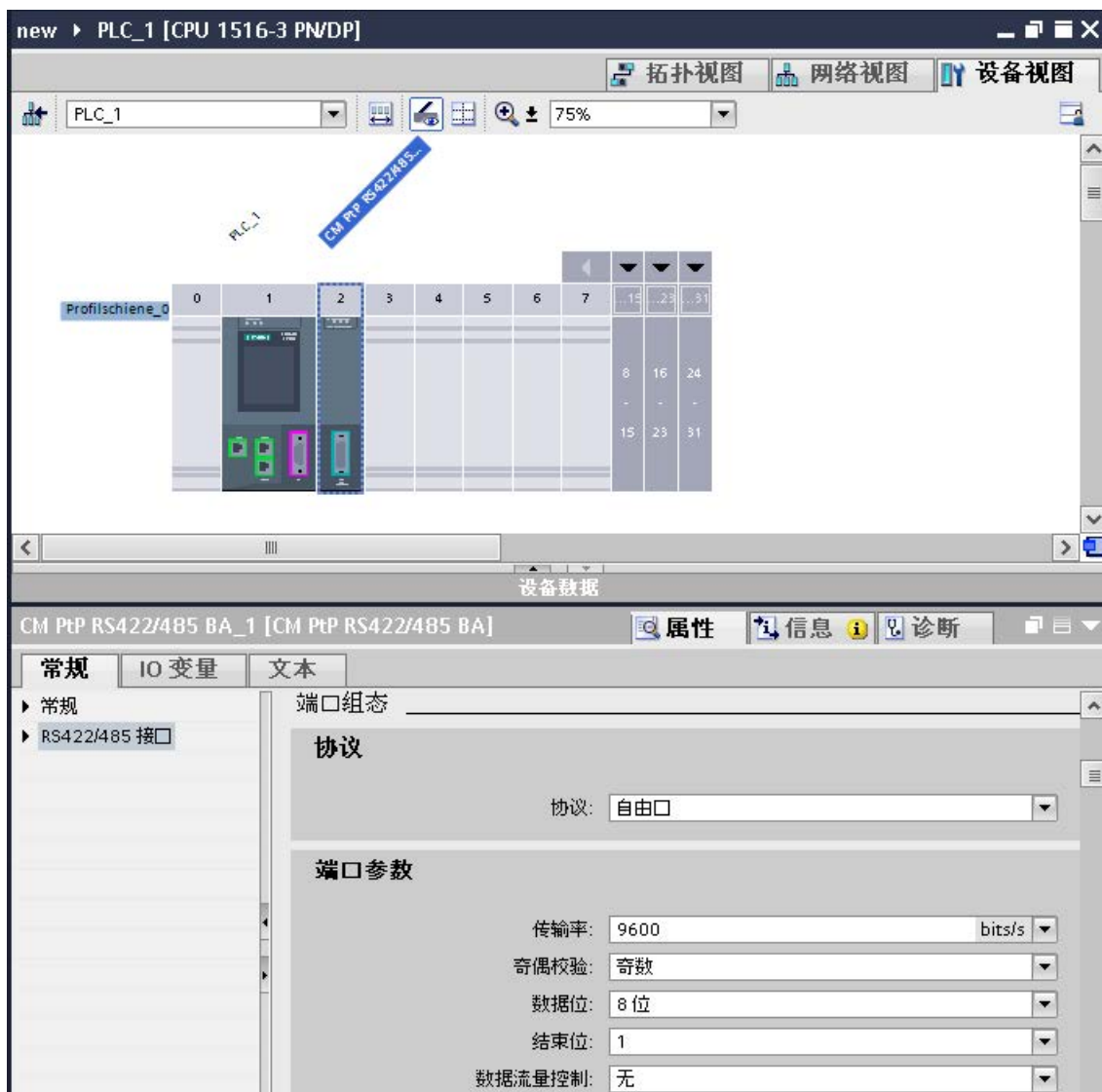


图 8-1 建立 PtP 通信

3. 在项目树中，选择“程序块”(Program blocks) 文件夹。双击该文件夹，打开文件夹中的 OB1。将打开程序编辑器。
4. 从“指令”(Instructions) 任务卡中的“通信” (Communication) 区域内，选择 Send_P2P 和 Receive_P2P 指令，将它们拖放到 OB1 中的一个程序段中。

5. 根据组态，指定这些指令的参数。
6. 将硬件组态和用户程序下载到 CPU。

或者：通过用户程序进行动态组态

在某些类型的应用中，动态建立通信连接更有优势。即，通过一个特定的应用中的程序建立通信。

这种应用的典型示例有串行计算机生产商。为了用户更为便捷地使用用户接口，这些制造商可以按照特定的操作要求对通信服务进行调整。

Freeport 的通信指令

一共有 3 条指令可在用户程序中动态组态 **Freeport** 通信。以下情况适用于所有 3 条指令：之前有效的组态数据将被覆盖，但不会在目标系统中永久保存。

- “Port_Config”指令可用于对通信模块的相关端口进行程序控制的组态。
- “Send_Config”指令可用于对相关的端口进行动态组态。例如，传输的时间间隔和中断（串行传输参数）。
- “Receive_Config”指令可用于对相关的端口进行动态组态。例如，消息传输的开始和结束条件（串行接收参数）

3964 (R) 通信的指令

一共有 2 种指令可在用户程序中动态组态 **3964 (R)** 通信。以下情况适用于这些指令：之前有效的组态数据将被覆盖，但不会在目标系统中永久保存。

- “Port_Config”指令可用于对通信模块的相关端口进行程序控制的组态。
- “P3964_Config”指令可用于对协议的参数进行动态组态。

USS 协议的特性

- 一种简单的串行数据传输协议，采用半双工模式并通过循环帧进行数据传输，为驱动技术量身定制。
- 根据主站/从站模式进行数据传输。
 - 主站可以访问驱动器的功能，并可以控制驱动器，读取状态值，对驱动器参数进行读/写操作。

通过 USS 通信进行数据交换

该通信模块将作为主站。主站可以向最多 16 个驱动器连续发送帧（任务帧），并将收到每个所寻址驱动器的响应帧。

在以下条件下，驱动器发送一个响应帧：

- 接收到的帧无错误
- 驱动器在此帧中寻址

如果不满足以上这些条件，或者在广播帧中对驱动器进行寻址，则驱动器将不发送响应帧。

如果主站在一定的处理时间（响应延时时间）之后从驱动器接收到一条响应帧，则主站与相应的驱动器之间存在连接。

建立 USS 通信的步骤

1. 在 STEP 7 的硬件和网络编辑器的设备视图中，组态一个带有 CPU 和 CM 的 S7-1500 组态。
2. 在项目树中，选择“程序块”(Program blocks) 文件夹。双击该文件夹，打开文件夹中的 OB1。将打开程序编辑器。
3. 从“指令”(Instructions) 任务卡的“通信”(Communication) 区域中的“通信处理器”(Communications processor) 文件夹，根据当前的任务选择 USS 通信的指令，并将其拖放到 OB1 的一个程序段中：
 - 使用“USS_Port_Scan”指令，可通过 USS 程序段进行通信。
 - “USS_Drive_Control”指令为驱动器准备发送数据并评估驱动器的响应数据。
 - “USS_Read_Param”指令可用于读出驱动器的参数。
 - “USS_Write_Param”指令可用于更改驱动器的参数。
4. 根据组态，指定这些指令的参数。
5. 将硬件组态和用户程序下载到 CPU。

Modbus 协议 (RTU) 的特性

- 采用串行、异步传输的通信方式，传输速率高达 115.2 kbps，半双工。
- 根据主站/从站模式进行数据传输。
- Modbus 主站可发送向 Modbus 从站进行读写操作的作业：
 - 读取输入、定时器、计数器、输出、存储位、数据块
 - 写入输出、存储位、数据块
- 还可以向所有从站进行广播。

通过 Modbus 通信 (RTU) 进行数据交换

通信模块可以作为 Modbus 主站，也可以作为 Modbus 从站。Modbus 主站可与一个或多个 Modbus 从站进行通信（具体数量取决于物理接口）。只允许 Modbus 主站通过对 Modbus 从站进行显式寻址，向 Modbus 主站返回数据。从站将检测数据传输是否终止，并进行确认。如果发生错误，将向主站发送一个错误代码。

建立 Modbus 通信 (RTU) 的步骤

1. 在 STEP 7 的硬件和网络编辑器的设备视图中，组态一个带有 CPU 和 CM 的 S7-1500 组态。
2. 在项目树中，选择“程序块”(Program blocks) 文件夹。双击该文件夹，打开文件夹中的 OB1。将打开程序编辑器。
3. 从“指令”(Instructions) 任务卡的“通信”(Communication) 区域中的“通信处理器”(Communications processor) 文件夹，根据当前的任务选择 Modbus 通信的指令，并将其拖放到 OB1 的一个程序段中：
 - “Modbus_Comm_Load”指令将对 Modbus 通信的 CM 端口进行组态。
 - “Modbus_Master”指令可用于调用 Modbus 主站的功能。
 - “Modbus_Slave”指令可用于调用 Modbus 从站的功能。
4. 根据组态，指定这些指令的参数。
5. 将硬件组态和用户程序下载到 CPU。

附加信息

- 有关通过点对点连接进行通信的更多详细信息以及串行数据传输基本知识，请参见“CM PtP 通信模块 - 点对点连接的组态 (<http://support.automation.siemens.com/WW/view/zh/59057093>)”功能手册。
- 有关如何在用户程序中使用点对点连接指令的说明，请参见 **STEP 7** 在线帮助。
- 有关带有串行接口的通信模块的信息，请参见特定的通信模块手册。

路由

9.1 S7 路由

S7 路由的定义

S7 路由就是跨 S7 子网传输数据。可以跨越几个 S7 子网将信息从发送方传送到接收方。S7 路由器提供从一个 S7 子网到一个或多个其它子网的网关。S7 路由器具有连接至相应 S7 子网的接口。S7 路由可通过各种 S7 子网 (PROFINET/工业以太网和/或 PROFIBUS) 实现。

S7 路由的要求

- 在 STEP 7 的项目中已对网络中可访问的所有设备进行了组态和下载。
- S7 路由中涉及的所有设备必须接收有关可通过特定 S7 路由器访问的 S7 子网的信息。由于 CPU 扮演着 S7 路由器的角色，这些设备通过将硬件组态下载到 CPU 来获取路由信息。

在具有多个连续 S7 子网的拓扑中，必须按照以下顺序进行下载：首先，将硬件组态下载到同一 S7 子网中作为编程器/PC 的 CPU；然后，按照 S7 子网自近到远的顺序，逐一下载到 S7 子网的 CPU。
- 必须将用于通过 S7 路由器建立连接的编程器/PC 分配给与其物理连接的 S7 子网。可以根据菜单命令“在线诊断 > 在线访问 > 连接到接口/子网(Online & Diagnostics > Online accesses > Connection to interface/subnet)，将该编程器/PC 指定为 STEP 7 中的编程器/PC。
- 对于类型为 PROFIBUS 的 S7 子网：CPU 必须组态为 DP 主站。如果要组态为 DP 从站，则必须选中 DP 从站上 DP 接口属性内的“测试、调试、路由”(Test, commissioning, routing) 复选框。
- 从 STEP 7 V13 SP1 起，支持 HMI 连接的 S7 路由。

用于在线连接的 S7 路由

通过编程器/PC，可以访问 S7 子网以外的设备，例如，可执行以下操作：

- 下载用户程序
- 下载硬件组态
- 执行测试和诊断功能

在下图中，CPU 1 是 S7 子网 1 和 S7 子网 2 间的 S7 路由器。

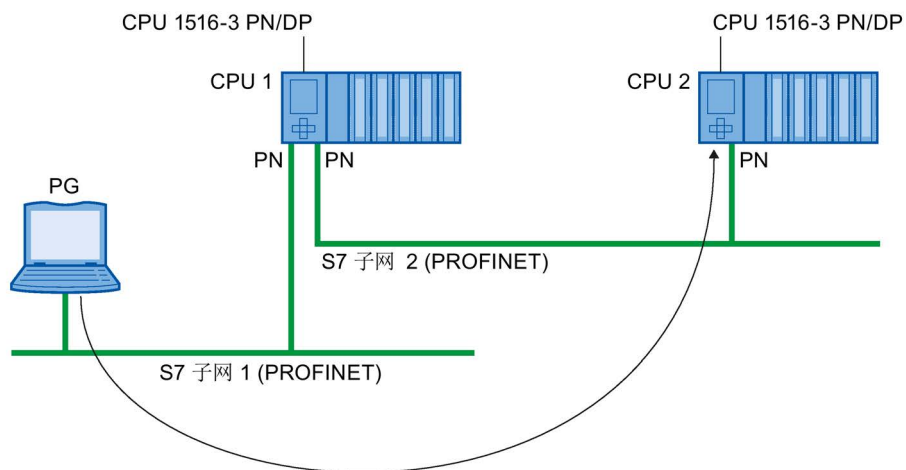


图 9-1 S7 路由：PROFINET - PROFINET

下图举例说明了从 PG 通过 PROFINET 访问 PROFIBUS 的过程。CPU 1 是 S7 子网 1 和 S7 子网 2 间的 S7 路由器；CPU 2 是 S7 子网 2 和 S7 子网 3 间的 S7 路由器。

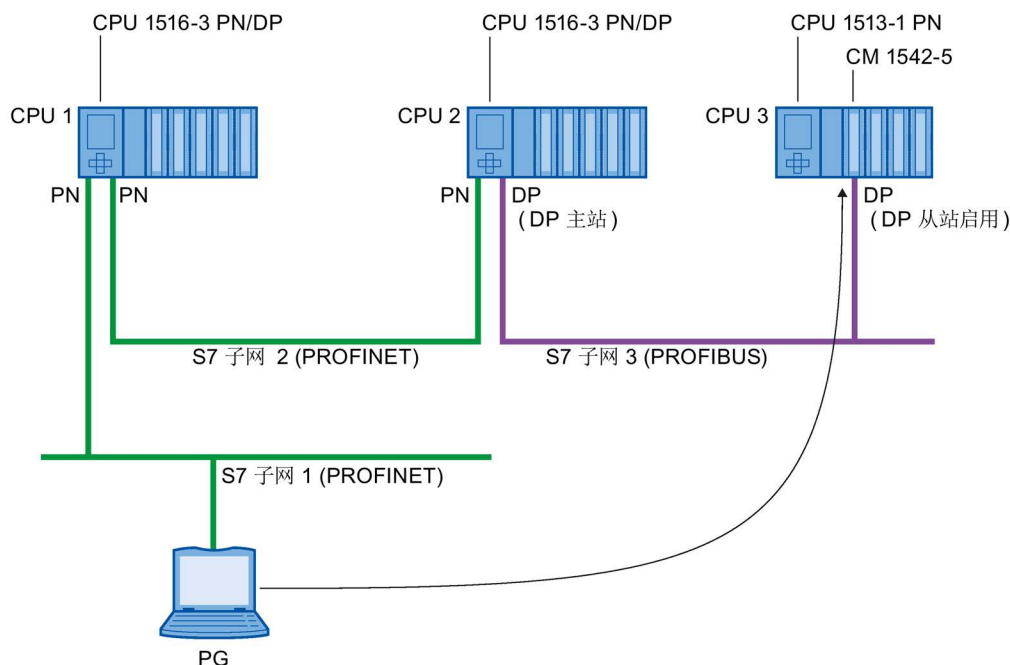


图 9-2 S7 路由：PROFINET - PROFIBUS

用于 HMI 连接的 S7 路由

可以在不同 S7 子网（PROFIBUS 和 PROFINET 或工业以太网）中的 HMI 和 CPU 之间建立 S7 连接。在下图中，CPU 1 是 S7 子网 1 和 S7 子网 2 间的 S7 路由器。

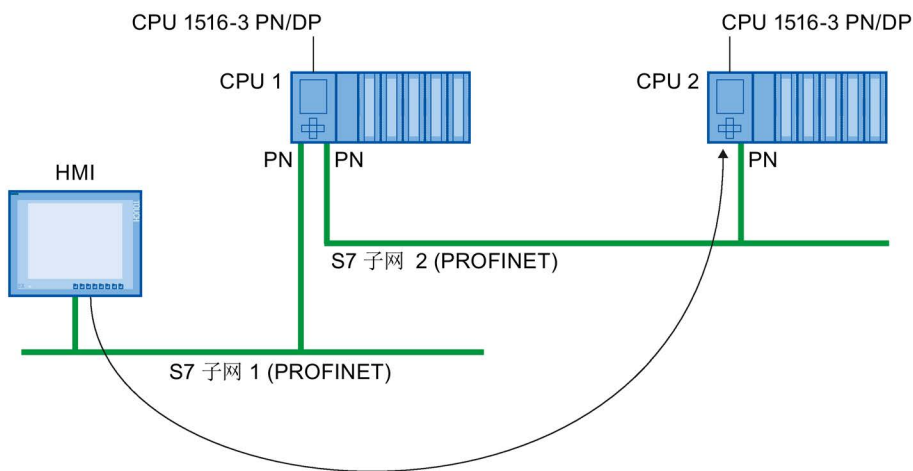


图 9-3 通过 HMI 连接实现的 S7 路由

用于 CPU-CPU 通信的 S7 路由

可以为不同子网（PROFIBUS 和 PROFINET 或工业以太网）中的两个 CPU 建立 S7 连接。连接的建立步骤，请参见“S7 通信 (页 54)”部分中的示例。

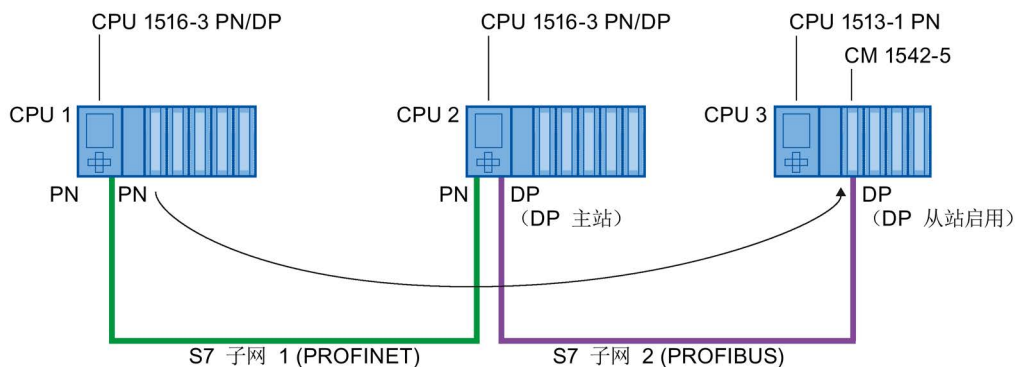


图 9-4 通过 CPU-CPU 通信实现的 S7 路由

使用 S7 路由

对于 CPU，在 STEP 7 的“转至在线”(Go online) 对话框中，选择编程器/PC 接口和 S7 子网。S7 路由自动执行。

S7 路由的连接数量

有关 S7 路由器（CPU、CM 或 CP）上 S7 路由的连接数量，请参见相关 CPU/CM/CP 手册中的技术规范。

S7 路由：应用示例

下图举例说明了如何使用编程器对系统进行远程维护。这里，两个 S7 子网之间的连接是通过调制解调器实现的。

可以在 STEP 7 的“在线访问”(Online access) 或“转至在线”(Go online) 中组态一个通过 TeleService 的远程连接。

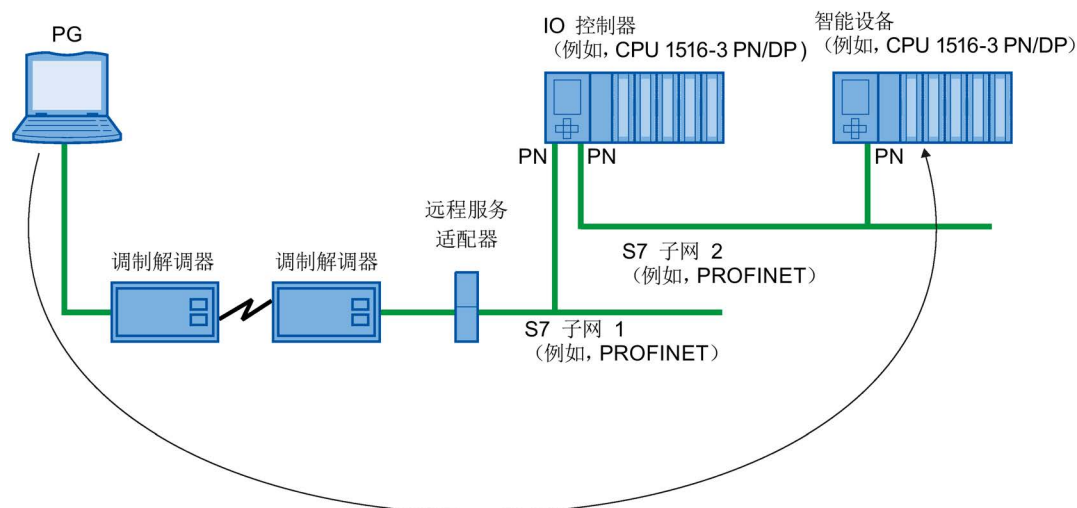


图 9-5 使用 TeleService 对设备进行远程维护

附加信息

- 有关 S7 路由的连接资源分配，请参见“连接资源分配 (页 78)”部分。
- 有关设置 TeleService 连接的信息，请参见 STEP 7 的在线帮助。
- 有关 S7 路由和 TeleService 适配器的更多信息，可通过以下链接访问 Internet。
 - 设备手册“工业软件工程组态工具 TS Adapter 的 IE 基础知识”
(<http://support.automation.siemens.com/WW/view/ch/51311100>)”
 - TS Adapter
(<http://support.automation.siemens.com/WW/view/zh/10805406/133100>) 的下载内容

参见

HMI 通信 (页 32)

9.2 数据记录路由

数据记录路由的定义

可以通过 **PROFINET**，从工程师站将数据发送到多个网络中的现场设备。由于工程师站使用标准化的记录对现场设备寻址且这些记录通过 **S7** 设备来路由，因此使用“数据记录路由”这个术语来表示这种路由。

通过数据记录路由发送的数据包括使用的现场设备（从站）的参数分配，以及设备的特定信息（如，设定值、限值等）。

例如，在使用不同厂商的现场设备时，可使用数据记录路由。为进行组态和诊断，将使用标准数据记录 (**PROFINET**) 来寻址现场设备。

使用 STEP 7 实现数据记录路由

通过借助于 **TCI** 接口（工具调用接口）调用设备工具（如 **PCT**）并传递调用参数，可使用 **STEP 7** 执行数据路由。设备工具使用的通信路径也可供 **STEP 7** 用来与现场设备通信。

除了在 **STEP 7 PC** 上安装 **TCI** 工具外，这种路由不需要其它组态。

示例：通过 Port Configuration Tool (PCT) 实现的数据记录路由

可以使用端口组态工具 (PCT) 来组态 ET200 的 IO Link 主站，并向连接的 IO Link 设备分配参数。子网通过数据记录路由器来连接。例如，数据记录路由器可以是 CPU、CP、IM 或 IO Link 主站。

有关 PCT 支持的数据记录路由器的配置，请点击此处

(<http://support.automation.siemens.com/WW/view/zh/87611392>)。

下图显示了通过 PCT 实现数据记录路由的组态示例。

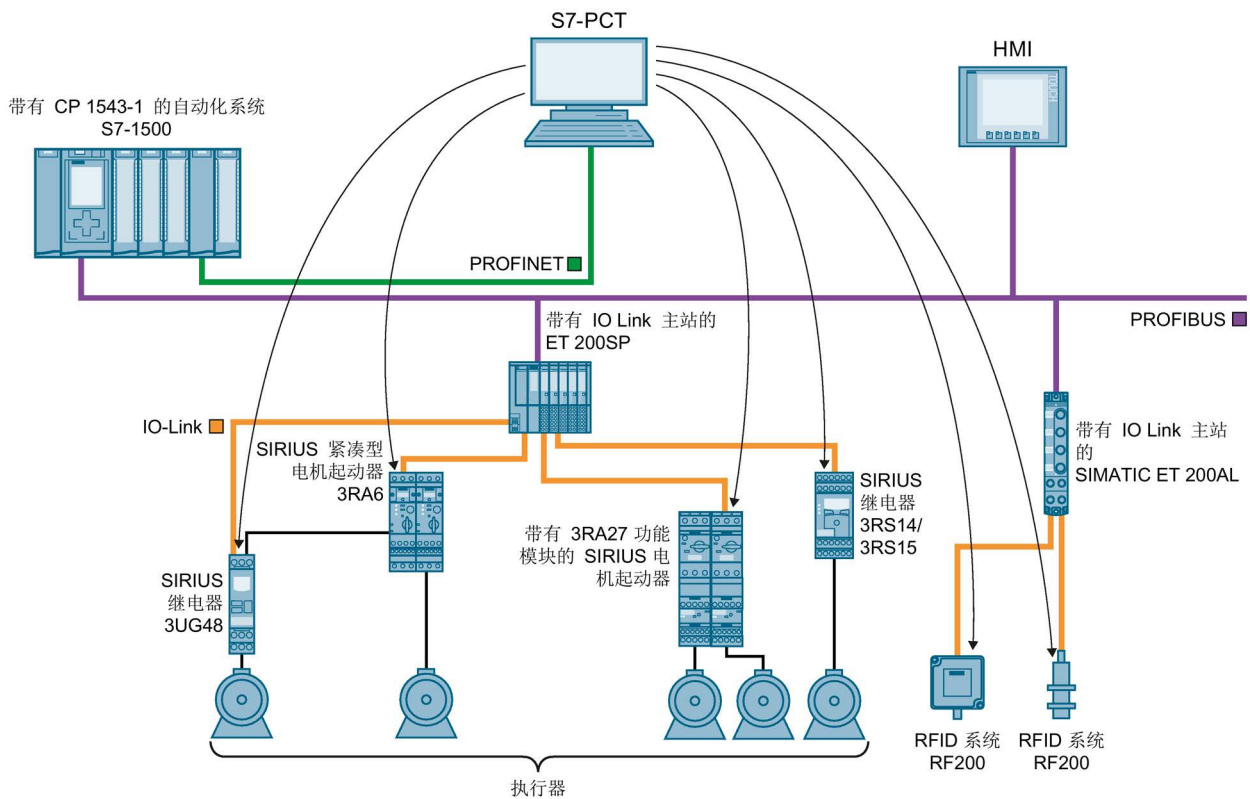


图 9-6 通过 PCT 实现数据记录路由的组态示例

附加信息

- 有关 CPU、CP 或 CM 是否支持数据记录路由，请参见相关手册。
- 有关数据记录路由的连接资源分配的信息，请参见“连接资源分配 (页 78)”部分。
- 有关使用 STEP 7 进行组态的更多信息，请参见 STEP 7 在线帮助。

连接资源

10.1 连接资源分配

自动连接时的连接资源分配

一旦将 PG 或 HMI 设备物理连接到一个 CPU 并且 STEP 7 中设置为转至在线，将立即分配连接资源。

通过编程方式建立连接时的连接资源分配

通过编程建立连接时，在调用建立连接的指令（TSEND_C/TRCV_C 或 T_CON）时，开始分配连接资源。

通过为 TSEND_C/TRCV_C 指令的 CONT 参数分配相应的参数或者调用 TDISCON 指令，可以在数据传输结束后终止连接，同时释放连接资源。如果连接终止，则 CPU/CP/CM 中的连接资源将再次可用。如果继续保留连接，则会因无需重新建立连接，而缩短下一次数据传输中指令的执行时间。如果 CPU 转入 STOP 模式，将会释放连接资源。

通过组态方式建立连接时的连接资源分配

通过组态建立连接时，在硬件配置下载到 CPU 时开始分配连接资源。

使用组态的连接传输数据后不会终止连接。将永久分配这些连接资源。如果再次释放连接资源，则需要删除 STEP 7 中所组态的连接，并将修改后的组态下载到 CPU。

监视可用的最大连接资源

自动建立连接时，CPU 将监视自动化系统上连接资源的使用情况。预留的连接资源耗尽后，可以使用其它资源（只要自动化系统中有可用的连接资源）。

如果在用户程序中通过编程方式建立和终止连接，则需确保不超出自动化系统的连接资源限制。如果使用比自动化系统提供的连接资源更多的连接资源，则 CPU 会确认用于建立连接的指令并显示错误。

如果在 STEP 7 中通过组态方式建立连接，则 STEP 7 将监视连接资源的使用情况，以确保不超出自动化系统中的最大值。超过该限值时，STEP 7 将发出一条相应的警告。

通过组态建立连接：在 STEP 7 的离线视图中显示连接资源

在硬件组态中，可以显示自动化系统中预留的连接资源和可用连接资源。并在 CPU 属性的巡视窗口中显示连接资源。

1516-3 PN/DP]						
IO 变量 文本						
连接资源						
	站资源		模块资源	模块资源	模块资源	
	预留	动态 	PLC_2 [CPU 1516..	CP 1543-1_1..	CM 1542-5_1..	
最大资源数：	10	246	128	118	48	
	最大	已组态	已组态	已组态	已组态	已组态
PG 通信：	4	-	-	-	-	-
HMI 通信：	4	4	6	4	0	
S7 通信：	0	-	23	2	0	21
开放式用户通信：	0	-	118	39	52	27
Web 通信：	2	-	-	-	-	-
其它通信：	-	-	-	-	-	-
使用的总资源：	4	147	47	56	48	
可用资源：	6	99	81	62	0	

图 10-1 预留和可用的连接资源（离线视图）

模块特定的连接资源（离线视图）

模块特定的连接资源列包含有关自动化系统的 CPU、CP 和 CM 的以下信息：

- CPU/CP/CM 可用的最大连接资源数
- 为通信连接组态的连接资源数
- 已组态和已使用的连接资源数
- 仍可用的连接资源数

将按模块而非接口显示连接资源。

在本示例中，CPU 最多可以使用 128 个连接资源。在该 CPU 中，通过接口组态了 6 个 HMI、2 个 S7 和 39 个开放式通信连接，总计占用了 CPU 上的 47 个资源。CPU 中仍有 81 个可用资源。在 CP 1543-1 中共有 118 个可用资源，其中 56 个资源已分配，还有 62 个空闲资源。所有 48 个可用资源都将用于 CM 1542-5。

站特定的连接资源（离线视图）

自动化系统中（站内）可用连接资源的最大数量取决于所使用的 CPU。如果达到 CPU 中设定的限值，则将不会考虑 CPU、CP 和 CM 是否还包含与模块相关的其它连接资源。对于该站而言，连接资源已经用尽。

在本示例中，自动化系统预留了 246 + 10 个连接资源。

其中，预留的 10 个连接资源包括：

- 4 个连接资源用于 STEP 7 要求的 PG 通信。例如，执行测试和诊断功能或下载到 CPU 中
- 4 个连接资源用于 HMI 通信，由 STEP 7 中组态的第一个 HMI 连接分配
- 2 个连接资源用于与 Web 服务器通信。如果激活了 CPU 的 Web 服务器，则在连接 Web 浏览器后分配这两个连接资源。

换句话说，最多可以有 246 个动态连接资源，可用于自动化系统中的各种通信服务。在本示例中，其中的 147 个连接资源已组态为可用于各种通信服务和模块。剩下的 99 个连接资源将用于自动化系统。

由于 CPU、CP 和 CM 中可用连接资源的最大数（294 个连接资源）超出了站的限值 256 个，因此将在动态站资源列中显示一个三角形警告标志。

说明

超出可用的连接资源数

STEP 7 通过一个警告表示超出站特定的连接资源数量。此时，可以使用具有较大连接资源数最大值的 CPU，也可以减少通信连接的数量。

在 STEP 7 的在线视图中显示连接资源

如果在 STEP 7 的“设备与网络”(Devices & networks) 编辑器的网络视图选择一个在线连接的 CPU，则将在巡视窗口的“连接信息”(Connection information) 选项卡的“诊断”(Diagnostics) 区域中显示该自动化系统连接资源的已分配和未分配状态。



图 10-2 连接资源 - 在线

“连接资源”(Connection resources) 表格的在线视图中，还包含有离线视图列中所预留和组态的连接资源，以及 CPU 中当前已分配的连接资源。无论是通过自动、编程方式还是组态方式建立连接，将在在线视图中显示自动化系统中所有已分配的连接资源。在“其它通信”(Other communication) 行中，将显示与第三方设备通信以及通过数据记录路由进行通信时所分配的连接资源。该表格将自动进行更新。

说明

如果路由的 S7 连接经过某一 CPU，则该 CPU 所需的连接资源不出现在连接资源表中！

HMI 通信的连接资源

有关 HMI 连接中可用的和分配的连接资源信息，请参见相关 HMI 设备的离线视图（在巡视窗口中属性内的“连接资源”(Connection resources) 区域中）。

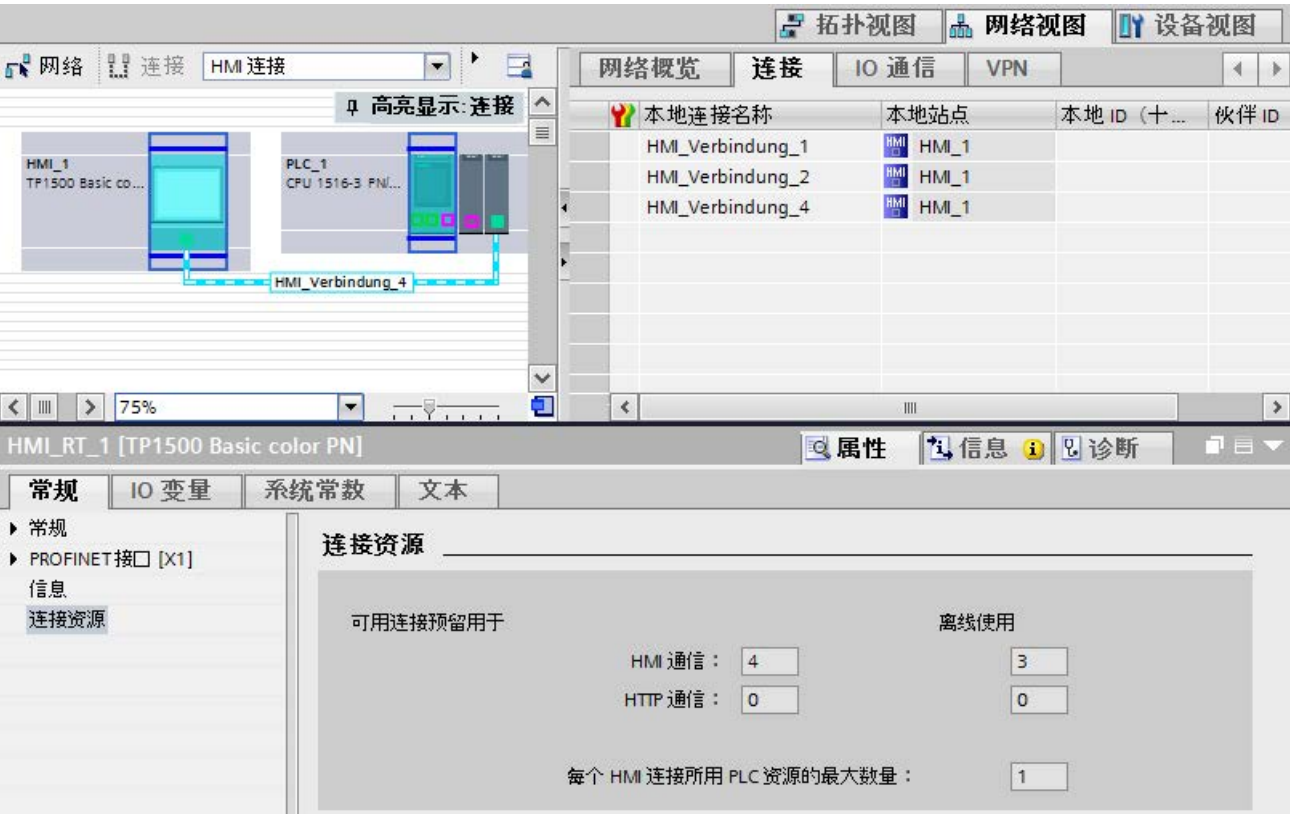


图 10-3 连接资源 - HMI 通信

以下信息将显示在“离线使用”(Offline used) 中。

- 用于 HMI 通信的连接资源数目

如果超出 HMI 设备可用连接资源的最大数，STEP 7 将输出一条相关消息。

- 已组态 HMI 连接所分配的连接资源的最大数量

对于 HMI 通信，CPU 中连接资源的分配取决于 HMI 设备。

下表显示了所用的 HMI 设备和每个 HMI 连接所分配的最大连接资源数之间的关系。

HMI 设备	每个 HMI 连接的 CPU 所需的最大连接资源数
精简面板	1
精智面板	2 ¹
RT Advanced	2 ¹
RT Professional	3

¹ 如果不使用系统诊断和消息组态，那么每个 HMI 连接的 CPU 仅需要一个连接资源。

S7 路由的连接资源

要在 S7 子网间传输数据（“S7 路由”），需在两个 CPU 之间建立 S7 连接。S7 子网将通过称为 S7 路由器的网关进行连接。S7-1500 中的 CPU、CM 和 CP 是 S7 路由器。

下面的情况适用于路由 S7 连接：

- 在每个端点中分配连接资源并显示在连接资源表中。
- 在 S7 路由器中，将会分配两个连接资源，但这两个连接资源不显示在连接资源表中。

数据记录路由的连接资源

数据记录路由还可以跨 S7 子网进行数据传输，通过 PROFIBUS 从连接到 PROFINET 的工程师站将数据传输到各种现场设备。

为实现数据记录路由，每个数据记录路由器中将分配两个连接资源。

说明

数据记录路由的连接资源

在数据记录路由器中，将为数据记录路由分配两个连接资源。数据记录连接和分配的连接资源都不会显示在连接资源表中。

附加信息

- 有关 S7 路由的信息，请参见“S7 路由 (页 71)”部分。
- 有关 HMI 设备所需的 CPU 连接资源数量，请参见 HMI 设备文档。

连接诊断

在线视图中的连接表

在 STEP 7 的“设备与网络”(Devices & networks) 编辑器中选择一个 CPU 后，将在连接表的在线视图中显示连接的状态。

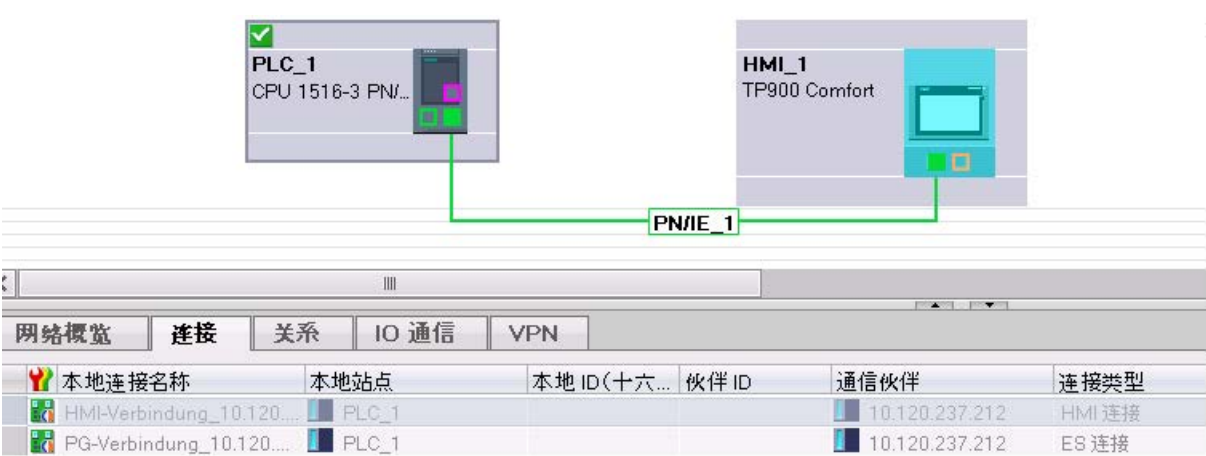


图 11-1 连接表的在线视图

在连接表中选择连接之后，可在“连接信息”(Connection information) 选项卡中查看详细诊断信息。

“连接信息”(Connection information) 选项卡： 连接的详细信息

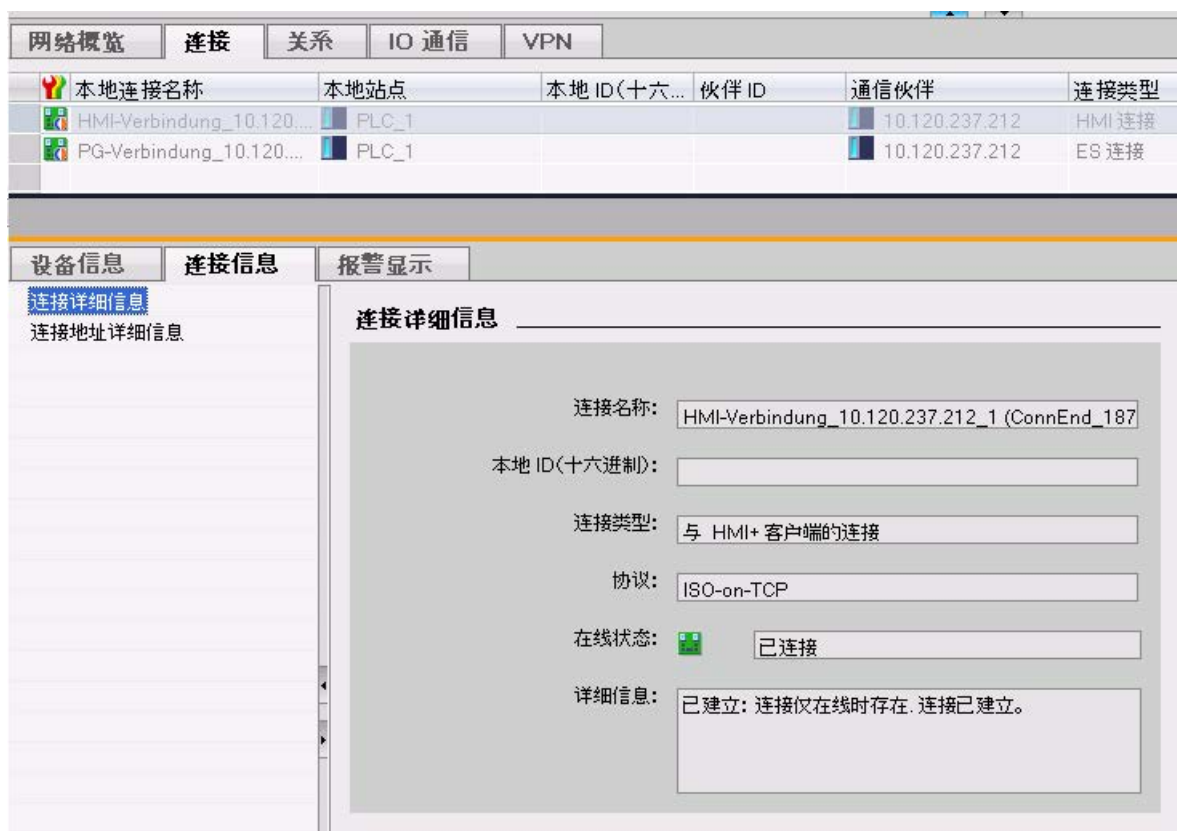


图 11-2 连接诊断 - 连接的详细信息

“连接信息”(Connection information) 选项卡： 地址详细信息

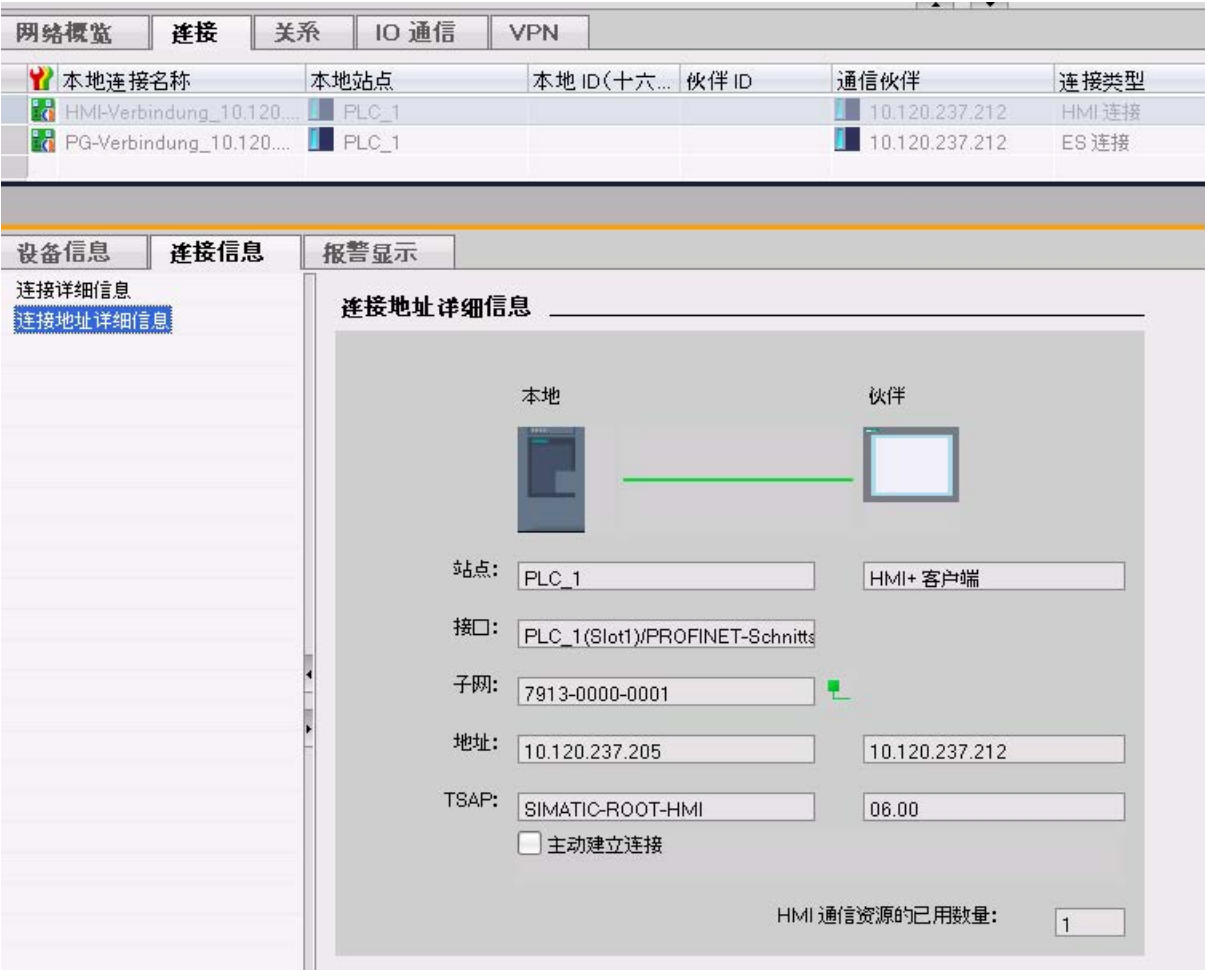


图 11-3 连接诊断 - 地址的详细信息

通过 Web 服务器进行诊断

通过 CPU 的集成 Web 服务器并使用 Web 浏览器，可以从 CPU 分析诊断信息。

在“通信”(Communication) 网页中，可在各个选项卡中查看通过 PROFINET 进行通信的以下信息：

- 有关 CPU 的 PROFINET 接口的信息（例如，地址、子网、物理属性）。
- 有关数据传输质量的信息（例如，正确发送/接收的数据包数量）。
- 有关分配的/可用的连接资源的信息。
- “连接”(Connections) 页面类似于 STEP 7 中的视图，还通过详细视图提供所有连接的概览。

用户程序中的诊断

在编程 T_DIAG 指令时，可使用用户程序来评估有关 CPU 的已组态和已编程连接的诊断信息。

附加信息

有关 Web 服务器的功能介绍，请参见功能手册“Web 服务器 (<http://support.automation.siemens.com/WW/view/zh/59193560>)”。

工业以太网安全

全方位保护 - 工业以太网安全的任务

通过工业以太网安全，可以对以太网中的单个设备、自动化单元或网段进行保护。此外，还可以通过组合其它不同的安全措施，对数据传输提供如下保护：

- 数据侦听
- 数据操纵
- 未经授权的访问

安全措施

- 防火墙
 - 全状态数据包检测型 IP 防火墙（第 3 层和第 4 层）
 - 符合 IEEE 802.3 标准的以太网“非 IP”帧的防火墙（第 2 层）
 - 带宽限制
 - 全局防火墙规则

防火墙将保护 CP 1543-1 内网段中的所有网络节点。

- 日志记录

在监视过程中，事件将存储在日志文件中，可通过组态工具进行读取或者自动发送到 Syslog 服务器中。

- HTTPS

对 Web 页面的传输进行加密。例如，在进行过程监视时。

- FTPS（显式模式）

对文件传输进行加密。

- 安全 NTP

对时间同步和传输进行保护

- SNMPv3

对网络分析信息的传输进行安全保护，以防窃听。

- 对设备和网段进行保护

通过防火墙的保护功能，对单个设备、多个设备，甚至整个网段进行保护。

12.1 防火墙

防火墙的任务

防火墙的目的是保护网络和站点免受外部的影响和干扰。这意味着，只能与之前指定的通信伙伴进行通信。

可通过 IPv4 地址、IPv4 子网、端口号或 MAC 地址等信息对数据流进行过滤。

可以为以下协议层组态防火墙功能：

- 全状态数据包检测型 IP 防火墙（第 3 层和第 4 层）
- 符合 IEEE 802.3 标准的以太网“非 IP”帧的防火墙（第 2 层）

防火墙的规则

在防火墙规则中将介绍允许或禁止传输的数据包以及传输的方向。

12.2 日志记录

功能

安全模块可以通过诊断和日志功能进行测试和监视。

- 诊断功能

包括各种可在线使用的系统和状态功能。

- 记录功能

记录系统和安全事件。根据事件类型的不同，记录的信息将包含在 CP 1543-1 的易失性或非易失性的本地缓冲区中。此外，也可以存储在网络服务器中。

只能通过网络连接对这些功能进行参数分配和评估。

通过日志功能记录事件

通过日志设置，指定待记录的事件。在此，可组态以下记录方式：

- 本地日志记录

通过这种记录方式，可以将事件记录在 CP 1543-1 的本地缓冲区中。并通过安全组态工具的在线对话框访问和显示这些记录，并在服务站中进行归档。

- 网络 Syslog

使用网络 Syslog，可以记录到网络中的 Syslog 服务器上。使用这种方式时，将根据日志设置中的组态信息对事件进行记录。

12.3 NTP 客户端

功能

要检查证书时间的有效性以及日志条目的时间戳，则需在 CPU 上对 CP 1543-1 中的日期和时间进行维护。时间可以与 NTP 同步。CP 1543-1 通过自动化系统的背板总线将同步的时间转发到 CPU。这样 CPU 还可以在执行程序时接收时间事件的同步时间。

可通过安全型或非安全型 NTP 服务器对时间进行自动设置和定期同步。最多可为 CP 1543-1 分配 4 个 NTP 服务器。但不能混合使用非安全型和安全型 NTP 服务器的组态。

12.4 SNMP

功能

CP 1543-1 支持通过简单网络管理协议 (SNMP) 传输管理信息，就像在 CPU 上一样。为此，需要在 CP 上安装一个“SNMP 代理”，用于接收和响应 SNMP 查询。有关具有 SNMP 功能设备的属性信息保存在 MIB（管理信息库）文件中，需要具有相应权限才能访问。

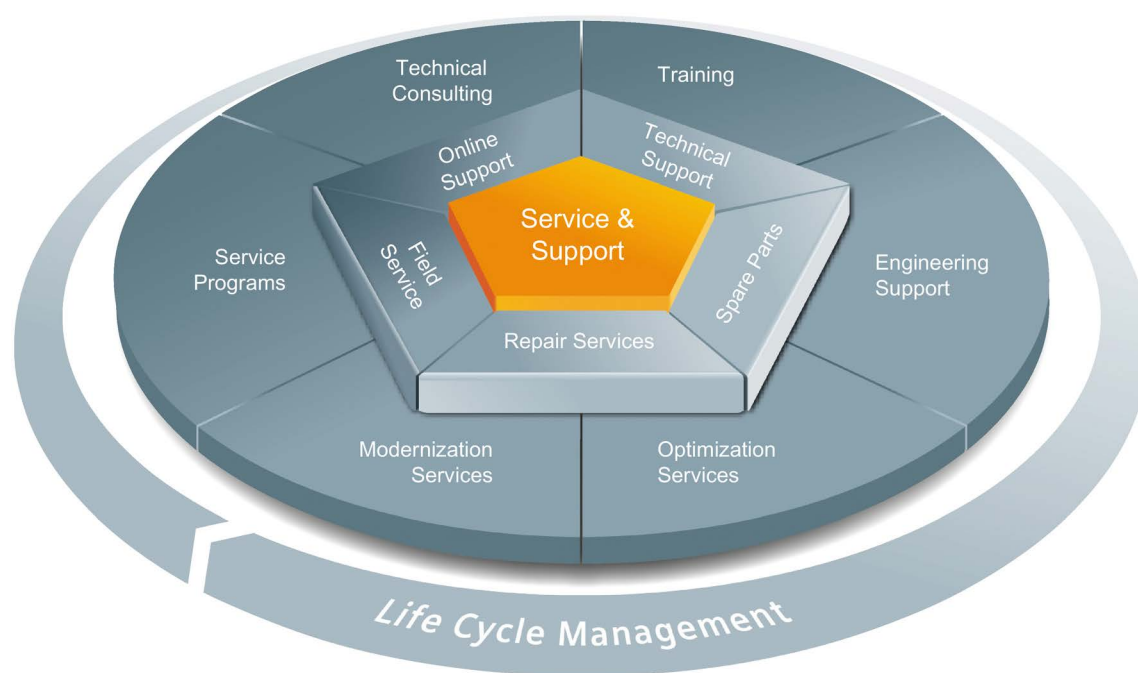
在使用 SNMPv1 安全措施时，还将发送“社区字符串”。“社区字符串”类似于一个密码，与 SNMP 查询一起发送。在“社区字符串”正确时，发送请求的信息。在此字符串不正确时，丢弃该请求。

在使用 SNMPv3 安全措施时，将对数据进行加密传输。为此，需要选择一种认证方法或者一种认证和加密方法。

可选择：

- 认证算法：无、MD5、SHA-1
- 加密算法：无、AES-128、DES

服务与支持



整个生命周期内的全面非凡服务

对于设备制造商、解决方案供应商以及工厂操作员而言，西门子工业自动化与驱动技术集团将为制造和加工行业内所有领域中的各种不同用户提供全面服务。

为了配合我们的产品和系统，我们提供有集成的结构化服务，以便在您设备或工厂生命周期的每个阶段都提供有高质量的服务和支持：从规划和实施到调试，以及维护和现代化改造，一应俱全。

我们的服务和支持时刻伴在您的左右，为您解决所有的西门子自动化和驱动技术问题。我们在 100 多个国家为设备和工厂生命周期的所有阶段都提供有现场支持。

在您的身边，将有一支由经验丰富的专家所组成的团队，为您提供积极的支持和专业技术。即使您与我们横跨多个大陆，我们的员工也将定期为您开展各种培训课程并与您保持密切的联系，以确保在各种领域为您提供可靠的服务。

在线支持

全面的在线信息平台，可以随时随地为您提供全面的服务与支持。

您可以在 Internet 上找到在线支持，地址如下：Internet
(<http://www.siemens.com/automation/service&support>)。

技术咨询

全面地为您的项目进行规划和设计：我们的规划和设计内涵盖了实际状态的详细分析、目标定义、产品和系统问题咨询，以及自动化解决方案的创建，无所不及。

技术支持

除了为客户提供有关技术问题的专家建议，我们还提供大量针对我们产品和系统的按需服务。

您可以在 Internet 上找到技术支持，地址如下：Internet
(<http://www.siemens.com/automation/support-request>)。

培训

我们为您提供的各种实践专业知识，助您在激烈的竞争中处于不败之地。

您可以在 Internet 上找到我们提供的培训课程，地址如下：Internet
(<http://www.siemens.com/sitrain>)。

工程组态支持

在项目工程组态和开发阶段，我们将专门针对您的要求进行量身定制的服务支持，涵盖了从自动化项目组态到实施的所有阶段。

现场服务

我们的现场服务为您提供调试和维护服务，以确保您的设备和工厂始终处于运行状态。

备件

在全世界的每个行业中，持久的可靠性是工厂和系统在运作时的必要条件。我们通过遍布全球的网络和最优秀的物流链，从一开始就为您提供所需的支持，使工厂和系统运行通畅。

维修

停机会在工厂中导致各种问题的产生并由此引发不必要的成本。我们通过遍布全球的维修设施，可以帮助您将这两者的成本降至最低。

优化

在设备和工厂的服务寿命期间，通常有很大的空间来提高生产力或降低成本。

为了帮助您实现这一终极目标，我们提供了全面的优化服务。

现代化改造

在需要现代化改造时，您也将得到我们的支持，我们将提供有从规划阶段直到调试完成的全面服务。

服务计划

我们的服务计划是针对自动化和驱动系统或产品组特选的各种服务包。各个服务之间相互协调以确保全面覆盖整个生命周期并对产品和服务的使用进行优化。

服务计划中的服务可以随时灵活更改并单独使用。

服务计划示例：

- 服务合同
- 工厂 IT 安全服务
- 驱动工程组态的生命周期服务
- SIMATIC PCS 7 的生命周期服务
- SINUMERIK 机床增效及制造信息化
- SIMATIC 远程支持服务

优势一瞥：

- 减少停机时间，提高生产力
- 量身定制各种服务，降低了维护成本
- 可预先计算并规划的成本
- 响应时间和备件交付时间有保障，服务十分可靠
- 客户服务人员将为额外任务提供支持以及解决方案
- 一站式全面服务，更少的联络，更多的专业技术

联系方式

在全球范围内就近为您提供各种服务：针对工业自动化和驱动技术集团提供的所有产品，我们都为您提供咨询、销售、培训、服务、支持、备件等服务。

要查找联系人数据库中的联系信息，请访问 Internet
(<http://www.siemens.com/automation/partner>)。

术语表

CM

→ 通信模块

CP

→ 通信处理器

CPU

中央处理单元 (**CPU**) - S7 自动化系统的核心模块，带有控制和算术逻辑运算单元、存储器、操作系统以及编程设备的接口。

DP 从站

PROFIBUS 上分布式 I/O 中的从站，采用 PROFIBUS DP 协议且符合 EN 50170 标准的第 3 部分。

→ 另请参见 *DP 主站*

DP 主站

在 PROFIBUS DP 中，分布式 I/O 中的主站符合 EN 50170 标准的第 3 部分。

→ 另请参见 *DP 从站*

FETCH/WRITE

使用 TCP/IP、ISO-on-TCP 和 ISO 协议的服务器服务，用于访问 S7 CPU 的系统存储区。可以从 SIMATIC S5 或第三方设备/PC 进行访问（客户端功能）。**FETCH**：直接读取数据；**WRITE**：直接写入数据。

Freeport 协议

可任意编程的 ASCII 协议；使用该协议可通过点对点连接进行数据传输。

FTP

文件传输协议 (**FTP**) 是一种网络协议，用于通过 **IP** 网络进行文件传输。**FTP** 用于服务器与客户端间的文件上传或下载。可创建并读取 **FTP** 目录，也可对目录和文件进行重命名或删除。

HMI

人机界面 (**HMI**)，用于显示和控制自动化过程的设备。

IE

→ 工业以太网

IM

→ 接口模块

IO 控制器、PROFINET IO 控制器

PROFINET 系统中的中央设备，通常为典型的可编程逻辑控制器或 **PC**。**IO** 控制器将建立与 **IO** 设备的连接，与这些设备进行数据交换，并对系统进行监控。

IO 设备、PROFINET IO 设备

PROFINET 系统中分布式 **I/O** 内的设备，通过 **IO** 控制器（例如，分布式 **I/O**、阀岛、变频器和交换机）进行监控。

IP 地址

用作采用 **Internet** 协议 (**IP**)、**PC** 网络中唯一地址的二进制数。根据该二进制数，可对这些设备进行唯一寻址和单独访问。使用可分离网络部分或主机部分结构的子网掩码来分析 **IPv4** 地址。例如，**IPv4** 地址由 4 个范围为 0 至 255 的十进制数组成。各数字间使用句点进行分隔。

IPv4 子网掩码

用来将 **IPv4** 地址（二进制数）划分为“网络部分”和“主机部分”的二进制掩码

ISO 协议

以太网中对消息或数据包进行数据传输的通信协议。该协议面向硬件、速度快、支持动态数据长度，ISO 协议适用于大中型数据传输。

ISO-on-TCP 协议

支持 S7 路由功能的通信协议，用于在以太网中对数据包进行数据传输，支持网络寻址，ISO-on-TCP 协议适用于大中型数据传输，并支持动态数据长度。

MAC 地址

所有以太网设备在全球范围内都唯一的设备标识码。MAC 地址由制造商分配，其中 3 字节为供应商 ID，另外 3 字节（以连续数字表示）为设备 ID。

Modbus RTU

远程终端单元 (**Remote Terminal Unit**)；基于主站/从站架构的开放式串行接口通信协议。

Modbus TCP

传输控制协议 (**Transmission Control Protocol**)；基于主站/从站架构的开放式以太网通信协议。数据以 TCP/IP 数据包的形式传输。

NTP

网络时间协议 (**Network Time Protocol, NTP**) 规定了由工业以太网建立的自动化系统中同步时钟的标准。NTP 采用适用于 Internet 的 UDP 传输协议。

PG

→ 编程设备

PNO

→ PROFIBUS 用户组织

PROFIBUS

过程现场总线 (**Process Field Bus**) - 欧洲现场总线标准。

PROFIBUS DP

使用 DP 协议且符合 EN 50170 的 PROFIBUS。DP 表示分布式 I/O，可实现快速、实时、循环的数据交换。从用户程序的角度来看，分布式 I/O 与集中式 I/O 的寻址方式完全相同。

PROFIBUS 地址

连接到 PROFIBUS 上的设备的唯一标识符。PROFIBUS 地址通过帧形式发送，用于寻址一个设备。

PROFIBUS 设备

该设备上至少有 1 个 PROFIBUS 接口为电气接口（如 RS-485）或光纤接口（如聚合物光纤）。

PROFIBUS 用户组织

该技术委员会致力于 PROFIBUS 和 PROFINET 标准的定义和开发。

PROFINET

基于组件的开放式工业通信系统，以分布式自动化系统的以太网为基础。这种通信技术由 PROFIBUS 用户组织推出。

PROFINET 接口

模块的 PROFINET 接口具备通信功能（如 CPU、CP），带有 1 个或多个端口。出厂前已为该接口分配有 MAC 地址。接口地址与 IP 地址和设备名称（来自各个组态）一起使用，可确保在网络中唯一识别 PROFINET 设备。该接口可以是电气接口、光学接口或者是无线接口。

PROFINET 设备

始终带有一个 PROFINET 接口（电气、光学或无线）的设备。

PROFINET IO

IO 即为输入/输出，分布式 I/O 可进行快速实时的周期性数据交换。从用户程序的角度来看，分布式 I/O 与集中式 I/O 的寻址方式完全相同。

PROFINET IO 作为 PROFIBUS 和 PROFINET International 基于以太网的自动化标准，它定义了跨厂商的通信、自动化系统和工程组态模式。

借助 PROFINET IO，实现一种允许所有设备随时访问网络的交换技术。因此，通过多个设备的并行数据传输，可以更为高效地使用网络。数据的并行发送和接收通过交换式以太网的全双工操作来实现。

PROFINET IO 基于交换式以太网的全双工操作，其带宽为 100 Mbps。

PtP

点对点 (PtP)，是两个（只能是两个）通信伙伴间进行双向数据交换的接口和/或传输协议。

RS232、RS422 和 RS485

串行接口标准。

RTU

Modbus RTU (RTU: 远程终端设备 (RTU))，用于传输二进制格式的数据，具有较高的数据吞吐率。在对数据进行评估之前，必须将其转换为一种可读取的格式。

S7 路由

通过作为 S7 路由器的一个或多个网络节点，可以在不同 S7 子网中的 S7 自动化系统、S7 应用或 PC 站之间进行通信。

SDA 服务

发送数据，需要进行确认。SDA 是一种基本服务。通过这种该服务，发起方（例如，DP 主站）可以向其它设备发送一条消息，并在之后接收从接收方发回的确认消息。

SDN 服务

发送数据，无需进行确认。该服务主要用于向多个站发送数据，但无需进行确认。该服务适用于发送同步任务和状态消息。

SNMP

简单网络管理协议 (**SNMP**)，使用无线 **UDP** 传输协议。**SNMP** 的工作模式与客户端/服务器的非常类似。**SNMP** 管理器对网络节点进行监视。**SNMP** 代理收集各网络节点中的各种网络特定信息，并以一种以结构化的形式将这种信息存储在管理信息库 (**Management Information Base**) 中。网络管理系统可以使用该信息进行详细的网络诊断。

TCP/IP

传输控制协议/因特网协议 (**TCP / IP**)，一种面向连接的网络协议，通常作为异构网络中数据传输的标准。

UDP

用户数据报协议 (**UDP**)，适用于快速简单数据传输的通信协议，无需进行确认。**TCP/IP** 中未定义错误检查机制。

USS

通用串行接口协议 (**USS**)，根据主站/从站原理定义了一种通过一根串行总线进行通信的访问方式。

Web 服务器

通过因特网进行数据交换的软件/通信服务。**Web** 服务器通过标准传输协议 (**HTTP**、**HTTPS**) 将文档传输到 **Web** 浏览器。文档可以是静态文档，也可以是由 **Web** 服务器根据 **Web** 浏览器的请求从不同的数据源动态生成的文档。

安全性

为防止以下各项丢失而采取的所有措施的统称

- 对数据进行未经授权的访问而导致机密性缺失
- 因数据操作而导致的完整性缺失
- 因数据破坏而导致的可用性缺失

编程设备

编程设备实质上是一种适用于工业应用的紧凑型便携式 **PC**。它们通过用于可编程逻辑控制器的特定硬件和软件组态进行识别。

操作系统

使用和操作计算机的软件。操作系统将对诸如内存、输入和输出设备等资源进行管理，并控制程序的执行。

从站

现场总线系统中的分布式设备，只有在主站提出请求后才能与主站进行数据交换。

→ 另请参见 *DP 从站*

点对点连接

通过通信模块上的串行接口，在两个通信伙伴（只能是两个）间进行双向数据交换。

端口

用于将设备连接到 **PROFINET** 的物理连接器。**PROFINET** 接口具有一个或多个端口。

服务器

可提供某些特定服务的设备或（广义上的）对象，并根据客户端的请求执行这些服务。

工业以太网

在工业环境中以太网络的构建指南。它与标准以太网的最大区别在于各组件的机械性能的鲁棒性和抗干扰性。

过程映像

过程映像是可编程逻辑控制器 (**PLC**) 的地址区域，用于以数字形式存储所连接模块上输入的信号状态和输出的逻辑状态。

环形拓扑

网络中的所有设备彼此连接形成一个环。

交换机

用于连接局域网 (LAN) 中多个终端或网段的网路组件。

接口模块

分布式 I/O 系统中的模块。接口模块通过现场总线将分布式 I/O 系统连接到 CPU (IO 控制器/DP 主站) 并提供用于 I/O 模块的数据。

客户端

一种网络设备，需要网络中的其它设备（服务器）将为其提供服务。

路由器

具有唯一标识符（名称和地址）的网络节点，用于将子网连接在一起，以便将数据传输到网络中唯一标识的网络通信节点。

设备

通用术语，适用于：

- 自动化系统（例如 PLC、PC）
- 分布式 I/O 系统
- 现场设备（例如 PLC、PC、液压设备、气动设备）以及
- 有源网络组件（例如交换机、路由器）
- PROFIBUS 的网关、AS Interface 或其它现场总线系统

时间同步

可以将一个单源标准系统时间传送给系统中的所有设备，以便这些设备可根据该标准时间设置自己的时钟。

树形拓扑结构

具有分支结构的一种网络拓扑结构：每个总线节点上连接有 2 或更多个总线节点。

双工

数据传输系统，分为全双工和半双工。

半双工： 使用一个通道交替地进行数据交换（可交替地发送或接收数据，但不能同时进行）。

全双工： 使用 2 个通道同时双向地进行数据交换（可双向同时发送和接收数据）。

双绞线

使用双绞线电缆连接的快速以太网基于 IEEE 802.3u 标准 (100 Base-TX)。传输介质是阻抗为 100 欧姆的 2x2 屏蔽双绞线电缆 (22 AWG)。这种电缆的传输特性必须符合类别 5 的要求。

终端设备和网络组件之间的最大连接长度不可超过 100 m。带 RJ-45 连接器系统的连接接口设计符合 100Base-TX 标准的要求。

通信处理器

执行其它通信任务的模块，可实现诸如区域安全之类的特殊应用。

通信模块

自动化系统中执行通信任务的模块，作为 CPU（例如 PROFIBUS）的接口扩展并具有附加通信功能 (PtP)。

网络

网络由 1 或多个相互连接的子网组成，可以包含任意数量的设备。各个网络可以彼此独立共存。

现场设备

→ 设备

线性总线形拓扑结构

一种网络拓扑结构，各种设备都连接到一个总线上。

协议

有关在两个或更多通信伙伴之间进行通信所遵循的规则协议。

一致性数据

这些数据属于一个整体，在传输时不能分开。

以太网

基于帧的局域网 (LAN)，采用国际标准技术。其中对电缆类型、物理层的信号发送、数据包的格式以及介质访问控制的协议进行定义。

以太网适配器

电子线路器件，用于将计算机接入以太网。以便在以太网中进行数据交换/通信。

用户程序

在 SIMATIC 中，对 CPU 操作系统和用户程序做了区分。用户程序中包含用于控制一个系统或过程的所有指令、声明和数据。用户程序可分配给可编程模块（例如，CPU 和 FM），并可由更小的单元构成。

指令

用户程序中最小的独立单元，并根据结构、功能或目的分为单个的用户程序部分。一条指令可代表处理器重的一个操作过程。

主站

通信/PROFIBUS 子网的上一层主动参与者。主站有权访问总线（令牌）、请求和发送数据。

→ 另请参见 DP 主站

子网

网络的一部分，子网的参数必须与设备（例如，PROFINET 中的）相匹配。子网中包含总线组件和所有连接的站。通过网关或路由器，子网可以进行互连从而构成一个网络。

自动化系统

可编程逻辑控制器，用于对过程工程组态行业和制造技术的过程链进行开环和闭环控制。自动化系统可包含各种组件和集成系统功能，具体取决于自动化任务。

总线

一种传输介质，用于连接多个设备。可通过电缆或光缆以串行或并行方式进行数据传输。

索引

3

3964(R) 程序, 64

B

BRCV, 55

BSEND, 55

C

CM, 10

CP, 10

F

Freeport 协议, 64

FTP, 15, 37, 49, 50

G

GET, 55

H

HMI 通信, 15, 32

I

IM, 14

ISO, 15, 36

ISO-on-TCP, 36, 40

M

Modbus TCP, 36

Modbus 协议 (RTU), 64

N

NTP, 15, 90

P

PCT, 77

PG 通信, 15, 29

PUT, 55

S

S7 路由, 71

 连接资源, 83

S7 通信, 15, 54, 83

SNMP, 15, 91

Syslog, 90

T

TCON, 37

TCP, 15, 36, 40

TDISCON, 37

TRCV, 37

TRCV_C, 37

TSEND, 37

TSEND_C, 37

U

UDP, 15, 36, 40

URCV, 55

USEND, 55

USS 协议, 64

W

Web 服务器, 15

A

安全措施, 88

 NTP, 90

 SNMP, 91

 防火墙, 89

 日志记录, 90

安全性, 88

D

点对点连接, 15, 64

电子邮件, 15, 37, 49

读取, 15

F

防火墙, 89

G

工业以太网安全, 88

J

建立和终止通信, 53

建立连接, 19

 CP 1543-1 的 ISO 连接, 45

 通过组态, 44

接口模块, 14

K

开放式通信

 建立 FTP, 50

 建立 TCP、ISO-on-TCP、UDP 连接, 40

 建立电子邮件, 49

 连接组态, 40

 特性, 35

 协议, 36

 指令, 37

开放式通信的协议, 36

开放式通信的指令, 37

L

连接

 开放式通信的指令, 37

 诊断, 84

连接诊断, 84

连接资源

 HMI 通信, 82

 S7 路由, 83

 概述, 18

 模块特定的, 79

 数据记录路由, 83

 引脚分配, 78

 在 STEP 7 中显示, 79

 站特定的, 80

连接资源分配, 78

R

日志记录, 90

S H

时间同步, 15

数据记录路由, 76

 连接资源, 83

数据一致性, 22, 22

T

通过 PUT/GET 指令进行通信

 创建和组态连接, 56

通信

 HMI 通信, 32

 PG 通信, 29

 S7 路由, 71

 S7 通信, 54

 点对点连接, 64

 建立和终止, 53

 开放式通信, 35

 数据记录路由, 76

 通信协议, 36

通信处理器, 10

通信处理器的接口, 12

通信服务

 连接资源, 18

通信接口, 11

通信模块, 10

通信模块的接口

 点对点连接, 13

通信选项

 概述, 15

X

系统数据类型, 38

写入, 15