

SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-1

操作说明

前言

应用和属性

1

LED 和连接器

2

安装、连接、调试

3

组态

4

程序块

5

诊断和保养

6

技术数据

7

认证

A

尺寸图

B




参考文档

C

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

本手册的有效性

本文档包含以下遥控产品的信息：

- **CP 1243-1**
部件编号 6GK7 243-1BX30-0XE0
硬件产品版本 2
固件版本 V3.0

CP 1243-1 是一款通信处理器，用于通过公共基础设施（如 DSL）将 SIMATIC S7-1200 连接到的控制中心系统。

借助 VPN 技术和防火墙，CP 可为 S7-1200 提供访问保护。

CP 也可用作 CPU 的附加 S7 通信接口。



图 1 CP 1243-1

在模块外壳铰接盖顶部的后方，可以看到在部件编号右侧以占位符“X”形式印上的硬件产品版本。例如，如果印上的文本为“X 2 3 4”，那么“X”为硬件产品版本 1 的占位符。

您可在外壳铰接盖顶部的左后方，即 LED 区域下方找到 CP 的固件版本。

该 MAC 地址位于外壳的下铰链盖下方。

产品名称和缩写

- **CP/子模块/模块**

在下文中，该缩写用于代替产品全称 CP 1243-1:

- **TCSB**

下文将使用此缩写代替“TeleControl Server Basic”，版本 V3。

- **STEP 7**

下文中这一缩写将代替 STEP 7 Basic/Professional 组态工具。

- **ES**

含有 STEP 7 项目的 PC

本手册的用途

本手册介绍了该模块的特性，并且可在安装和调试时提供支持。

所需的组态步骤会以概述的形式进行介绍，还会对固件功能和组态之间的关系进行说明。

您还将找到有关设备诊断选项的信息。

本发布版本的新增内容

- 新硬件产品版本 2
- 上述固件版本的新功能包括：
 - 扩展了遥控协议 DNP3 和 IEC
 - 无遥控通信也可发送消息
 - 更改了时钟同步期间的行为，请参见时钟同步 (页 48)部分。
 - 扩展了支持的数据类型，请参见数据点类型 (页 100)部分。
- 自 STEP 7 V14 SP1 以来数据点组态的功能改进，请参见数据点组态 (页 93)部分。
- 编辑修订

替换的手册版本

版本 12/2016

Internet 上的当前版本手册

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

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/15922/man>)

所需经验

要安装、调试和操作 CP，您需要具备以下几个方面的经验：

- 自动化工程
- 设置 SIMATIC S7-1200
- SIMATIC STEP 7 Basic / Professional

交叉引用

在本手册中，经常交叉引用其它部分。

为能够在跳转至交叉引用后能够返回初始页面，某些 PDF 阅读器支持 <Alt>+<左箭头> 命令。

信息资源和其它文档

有关更多读物和参考资料的总览，请参见本手册的附录。

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。

在所提供的介质中，下列文档提供有许可证条款：

- OSS-CP1243-1_86.pdf

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。

安全提示:

Siemens 为其产品及解决方案提供了工业安全功能，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。

此外，应考虑遵循 Siemens

有关相应安全措施的指南。更多有关工业安全的信息，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 工业安全 RSS 源，网址为链接: (<http://www.siemens.com/industrialsecurity>)。

SIMATIC NET 词汇表

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

相关 SIMATIC NET 词汇表，请访问以下 Internet 网址:

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

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>)

培训、服务与支持

有关培训、服务和支持的信息，请参见本文档随附的数据媒体上的多语言文档“DC_support_99.pdf”。

目录

前言	3
1 应用和属性.....	13
1.1 CP 的属性	13
1.2 通信服务.....	13
1.3 其它服务和属性.....	14
1.4 安全功能.....	15
1.5 组态限制和性能数据	17
1.6 组态示例.....	20
1.6.1 发送电子邮件	20
1.6.2 TeleControl Basic.....	21
1.6.3 DNP3 / IEC	22
1.6.3.1 采用 1 个子网的组态	22
1.6.3.2 通过 Internet 进行连接的组态	23
1.6.3.3 采用冗余控制中心的组态	24
1.7 使用要求.....	25
1.7.1 硬件要求.....	25
1.7.2 软件要求.....	26
2 LED 和连接器	27
2.1 打开外壳盖	27
2.2 LED	28
2.3 电气连接器	32
2.3.1 电源	32
2.3.2 以太网接口 X1P1	32
3 安装、连接、调试.....	33
3.1 使用设备的重要注意事项	33
3.1.1 有关在危险场所使用的注意事项	33
3.1.2 IECEx/ATEX 要求的危险场所使用注意事项	34
3.1.3 符合 UL HazLoc 要求的危险场所使用注意事项.....	35
3.1.4 FM 要求的危险场所使用注意事项.....	35
3.2 安装、连接和调试	36
3.3 操作注意事项	39
4 组态	41

4.1	安全建议.....	41
4.2	STEP 7 中的组态	44
4.3	寻址和验证	46
4.3.1	TeleControl Basic	46
4.3.2	DNP3/IEC	46
4.4	时钟同步.....	48
4.5	通信类型.....	51
4.6	以太网接口	52
4.6.1	CP 标识.....	52
4.6.2	时钟同步.....	53
4.6.3	高级选项.....	53
4.6.4	传输设置 – TeleControl Basic.....	55
4.6.5	传输设置 – DNP3.....	56
4.6.6	传输设置 - IEC	58
4.7	SNMP.....	61
4.8	伙伴站	61
4.8.1	伙伴站 > 常规参数.....	62
4.8.2	TeleControl Basic	65
4.8.2.1	在冗余 TCSB 系统中寻址	65
4.8.2.2	高级设置.....	65
4.8.2.3	站间通信的伙伴.....	66
4.8.3	DNP3 / IEC	67
4.8.3.1	高级设置 (DNP3 / IEC)	67
4.9	安全性	72
4.9.1	参数概述.....	72
4.9.2	使用 TeleControl Basic 协议的 CP 标识.....	73
4.9.3	DNP3 安全选项.....	74
4.9.4	防火墙	77
4.9.4.1	MAC 防火墙预检查消息。.....	77
4.9.4.2	源 IP 地址的表示法（高级防火墙模式）	78
4.9.4.3	已组态 VPN 隧道连接的防火墙设置	78
4.9.4.4	防火墙激活情况下的在线安全诊断和下载到站设置.....	78
4.9.5	电子邮件组态	79
4.9.6	日志设置 - 过滤系统事件.....	80
4.9.7	SNMP.....	81
4.9.8	证书管理器.....	82
4.9.9	处理证书.....	82
4.9.10	VPN.....	85
4.9.10.1	VPN (Virtual Private Network)	85
4.9.10.2	为各站间的 S7 通信创建 VPN 通道	86
4.9.10.3	SOFTNET 安全客户端的 VPN 通信（工程师站）	89

4.9.10.4	创建 VPN 连接遥控服务器	89
4.9.10.5	在 CP 和 SCALANCE M 之间建立 VPN 隧道通信	90
4.9.10.6	CP 作为 VPN 连接的被动用户	90
4.9.10.7	SYSLOG	91
4.9.11	TeleService 访问的组态	91
4.10	数据点	93
4.10.1	数据点组态	93
4.10.2	数据点名称的语法	100
4.10.3	数据点类型	100
4.10.4	组态数据点索引	108
4.10.5	数据点的状态 ID	109
4.10.6	读取周期	111
4.10.7	过程映像、传输类型、事件类别、触发	112
4.10.8	“触发”(Trigger) 选项卡	115
4.10.9	阈值触发	117
4.10.10	模拟值预处理	119
4.10.11	命令输出	126
4.10.12	伙伴站	129
4.10.12.1	DNP3 和 IEC 数据点的伙伴组态	129
4.10.12.2	具有 TeleControl Basic 数据点的伙伴组态。	129
4.11	消息	130
4.12	访问 Web 服务器	133
5	程序块	135
5.1	用于 OUC 的程序块	135
5.2	在运行期间更改 IP 地址	138
6	诊断和保养	141
6.1	诊断选项	141
6.2	通过端口 8448 执行在线安全诊断	143
6.3	在线功能和 TeleService	144
6.4	SNMP	146
6.5	电子邮件的处理状态	147
6.6	下载固件	149
6.7	模块更换	152
7	技术数据	153
7.1	CP 1243-1 的技术规范	153
7.2	以太网接口的引脚分配	155
A	认证	157

B	尺寸图	161
C	参考文档.....	163
	索引.....	165

应用和属性

1.1 CP 的属性

应用

CP 旨在适用于 S7-1200 自动化系统。在 CP 的支持下，S7-1200 可连接到工业以太网，也可通过 Internet 连接下列控制中心系统：

- 遥控服务器（OPC 服务器应用程序 TCSB V3）
- DNP3 主站
- IEC 主站

由于集成了防火墙和数据加密协议等多种安全功能，CP 可以保护站点甚至整个自动化单元免受未经授权的访问，同时也可保护远程 S7 站与主站 (TCSB) 之间的通信不受刺探和操纵。

1.2 通信服务

通信服务

支持以下通信服务：

- **遥控通信**

CP 是 SIMATIC S7-1200 的通信处理器，可将系统连接到上述控制中心系统。CP 可以与冗余控制系统进行通信。

对于每个控制中心系统，在 CP（“通信类型”）上激活相关遥控协议。协议允许将基于 IP 的数据传输用于遥控应用。

有关可用安全功能，请参见安全功能 (页 15) 部分。

- **消息/电子邮件**

对于特殊事件，CP 可以发送电子邮件形式的消息。

有关要求与功能，请参见电子邮件组态 (页 79) 部分。

- 具有以下功能的 S7 通信和 PG/OP 通信：
 - 以客户端和服务器形式的 PUT/GET 可用于与 S7 站进行数据交换
 - PG 功能
 - 操作员监控功能 (HMI)

1.3 其它服务和属性

其它服务和属性

- 数据点组态

由于 STEP 7 中具有数据点组态功能，因此无需为传送过程数据而编程程序块。控制系统会一对一地处理各个数据点。
- IP 组态 - IPv4 和 IPv6
 - IPv4 / IPv6

CP 支持符合 IPv4 和 IPv6 的 IP 地址。

针对 IPv6 网络中的遥控应用，除 IPv4 地址外还可以使用 IPv6 地址。
 - 地址分配

可以在组态中手动设置 IP 地址、子网掩码和网关地址。

也可以从 DHCP 服务器或通过组态之外的其它方式获取 IP 地址。
- 时钟同步

CP 支持多种同步时钟的方法。请参见时钟同步 (页 48)部分了解相关信息。

有关时间标记格式的信息，请参见数据点类型 (页 100)部分。
- 事件存储

CP 可以按时间顺序存储不同类别的事件，并将它们自发地或一起传送到遥控服务器。
- 请求或触发数据传送

与通信伙伴的遥控通信可以通过两种方式触发：

 - 主站发出请求或 OPC 客户端连接到 TCSB
 - 主动，由多种可选条件触发

- **模拟值处理**

在 CP 中可以按各种方法预处理模拟值。
- **在线功能 / TeleService**

从工程师站，可以使用 STEP 7 的在线功能通过 CP 访问站。
可使用下列在线功能：

 - 将项目或程序数据从 STEP 7 项目下载到站
 - 查询站中的诊断数据
 - 向 CP 下载固件文件

有关各在线功能的信息，请参见在线功能和 TeleService (页 144)部分。
- **SNMP**

作为 SNMP 代理，CP 支持使用 SNMP（简单网络管理协议）进行数据查询。
有关详细信息，请参见SNMP (页 146)部分。

1.4 安全功能

Industrial Ethernet Security

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。经 CP 的数据传输受多种安全方法保护，可防止遭到以下攻击：

- 数据间谍
- 数据操纵
- 未授权访问

通过 CPU 的附加以太网/PROFINET 接口可实现安全的底层网络。

安全功能可独立于遥控通信使用。

遥控协议的安全功能

- **TeleControl Basic**
 - **加密遥控通信**

作为集成（不可组态）的安全功能，协议可以对传输的数据进行加密。

可在 STEP 7 的“以太网接口 (X1) > 高级选项 > 传输设置”(Ethernet interface (X1) > Advanced options > Transmission settings) 参数组中组态 CPU 与遥控服务器之间的密钥交换间隔。
 - **遥控密码**

使用遥控服务器对 CP 进行验证
- **DNP3**

可使用专用于 DNP3 的安全功能。
- **IEC 60870-5**

IEC 协议无协议特定的安全功能。

更多可组态的 CP 安全功能

通过使用 CP 作为安全模块，S7-1200 站便可通过外部网络接口实现以下安全功能：

- **防火墙**
 - 具有状态数据包检查功能的 IP 防火墙（第 3 层和第 4 层）
 - 根据 IEEE 802.3，也适用于“非 IP”以太网帧（第 2 层）的防火墙
 - 传输速度限制（“带宽限制”）
 - 全局防火墙规则
- **IPsec 隧道 (VPN) 确保通信安全**

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

组态过程中，可将 CP 与其它模块放在一起，以构成 VPN 组。在一个 VPN 组的所有安全模块之间创建 IPsec 隧道 (VPN)。这些安全模块的所有内部节点都可以通过这些隧道彼此安全地进行通信。
- **记录**

为允许监视，可将事件存储在日志文件中，日志文件可通过组态工具读出，也可以自动发送到 Syslog 服务器。

- **STARTTLS / SMTPS**
用于安全传送电子邮件
- **NTP (secure)**
用于时钟同步期间的安全传输
- **SNMPv3**
用于安全传送网络分析信息，使其免受窃听
- **设备和网段的保护**
防火墙提供的保护可覆盖单个设备、多个设备甚至整个网段。

说明

对安全有要求的工厂 - 建议

使用下列选项：

- 若您的系统对安全性要求很高，请使用安全协议 **NTP (secure)**、**HTTPS** 和 **SNMPv3**。
- 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。
另请参见安全建议 (页 41) 部分。

有关在运行期间更改 IP 地址，请参见安全性 (页 72) 部分。

有关安全功能的使用和组态的更多信息，请参见 **STEP 7** 信息系统和 **I/4** (页 164) 手册。

1.5 组态限制和性能数据

每站的 CMS/CP 数

在每个 S7-1200 站中，最多可以插入和组态 3 个 CM/CP；这允许 3 个 CP 1243-1 模块。

要使用遥控通信，可为每个站插入三个 CP 1243-1 模块。

连接资源

- **遥控连接**

CP 可通过多种遥控协议与以下主站类型建立连接：

- 非冗余或冗余遥控服务器 (TCSB)。
- 多达四个非冗余或冗余 DNP3 主站
- 多达四个非冗余或冗余 IEC 主站

此外，通过 Telecontrol Basic 协议，借助 CP 1243-1，遥控服务器可与多达 15 个 S7 站进行站间通信。

- **S7 连接和 TCP/UDP/ISO-on-TCP 连接**

最多 14 个连接资源，可按需分配：

- S7 连接 (PUT/GET)
- 通过程序块 (OUC) 连接到 S7 站

- **在线功能**

为在线功能保留了 1 个连接资源。

- **PG/OP 连接**

- PG 连接有 1 个连接资源
- OP 连接有 3 个连接资源

可进行数据点组态的数据点数量

可组态的数据点最多为 200 个。

用户数据

在 STEP 7 组态中，要通过 CP 传送的数据会分配给不同的数据点。

每个数据点的用户数据大小取决于相关数据点的数据类型。相关详细信息可参见数据点类型 (页 100) 部分。

帧存储器（发送缓冲区）

CP

带有一个帧存储器（发送缓冲区），用于存储组态为事件的数据点值以及发送至通信伙伴的值。

发送缓冲区最多可容纳 **64000**

个事件，并针对所有已组态的通信伙伴将其分为相等的部分。帧存储器的大小可在 **STEP 7** 中设置，相关信息请参见 **SNMP (页 61)** 部分。

通过 **Telecontrol Basic**

协议，可将发送缓冲区用于多达三个伙伴的站间通信。您可以在“伙伴”(Partner) 参数组中创建组态。

消息/ (电子邮件)

- 可通过消息编辑器组态发送多达 **10** 条消息 (电子邮件)。
- 通过 **TMAIL_C** 程序块发送电子邮件

IPsec 隧道 (VPN)

与其它安全模块进行安全通信时，最多可以建立 **8** 个 **IPsec** 端子。

防火墙规则

高级防火墙模式中防火墙规则的最大数目被限制为 **256** 个。

防火墙规则将按如下方式进行划分：

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

1.6 组态示例

1.6.1 发送电子邮件

发送电子邮件的组态：

以下示例显示了发送电子邮件的组态。CP 的遥控通信已禁用。

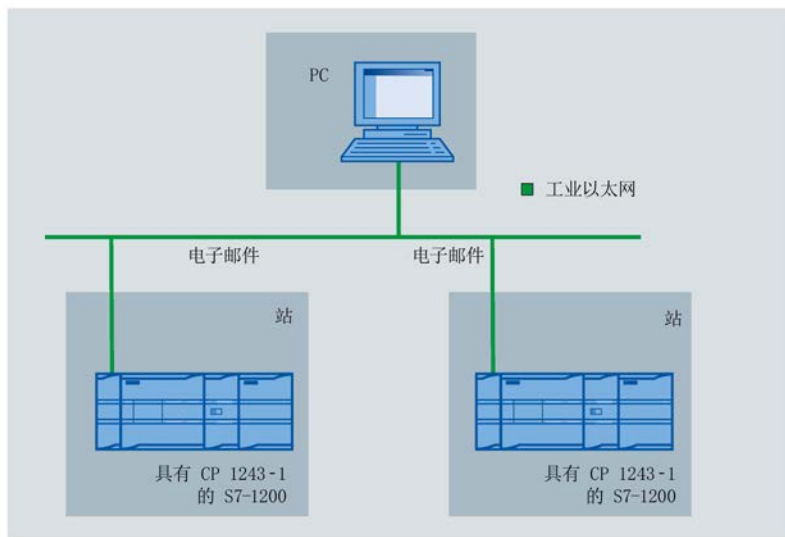


图 1-1 发送电子邮件

1.6.2 TeleControl Basic

基于非冗余主站 (TCSB) 的遥控

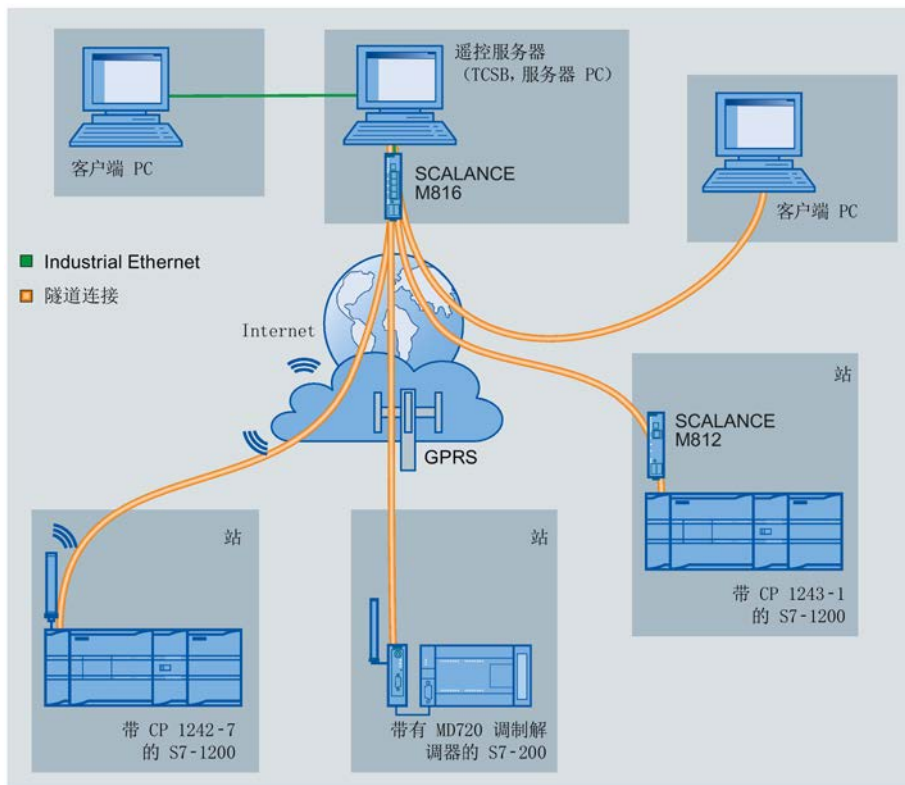


图 1-2 S7 站与主站 (TCSB) 之间的通信

在示例的遥控应用中，SIMATIC S7 站与主站中的非冗余遥控服务器 (TCSB) 进行通信。

- 各站与主站之间的遥控通信

通信通过以下路径和通信模块执行：

- 通过 Internet 进行的通信：带有 CP 1243-1 的 S7-1200
- 通过 GSM 网络和 Internet 进行的通信：带有 CP 1242-7 的 S7-1200 或带有 MD720 调制解调器的 S7-200

按照各通信模块所采用的遥控协议，端子之间将自动进行加密的连接。

可以选择在 CP 1243-1 和遥控服务器之间建立 VPN 连接。

遥控服务器监视由远程站建立的连接。

- 站间通信

同类型站（如带有 CP 1243-1 的 S7-1200）可以通过经遥控服务器发送帧的方式彼此进行通信。

基于冗余主站 (TCSB) 的遥控

下图显示了支持 S7 站与冗余主站 (TCSB) 进行通信的可能结构。

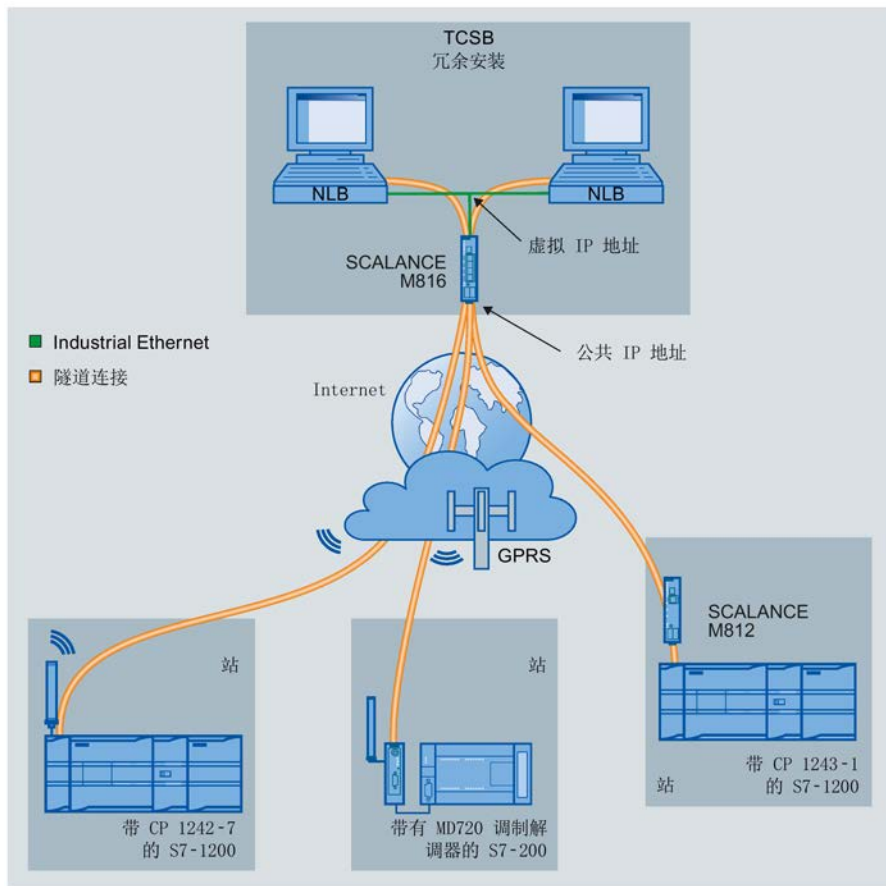


图 1-3 S7 站与冗余主站的通信

1.6.3 DNP3 / IEC

1.6.3.1 采用 1 个子网的组态

采用非冗余控制中心的组态示例

以下示例描述了采用非冗余控制中心的组态示例，其中的所有节点都位于 1 个 IP 子网内。

本例中，使用了 DNP3 协议；换句话说，从站配有 CP 1243-1。

而对于使用 IEC 协议的组态，设置均相同。

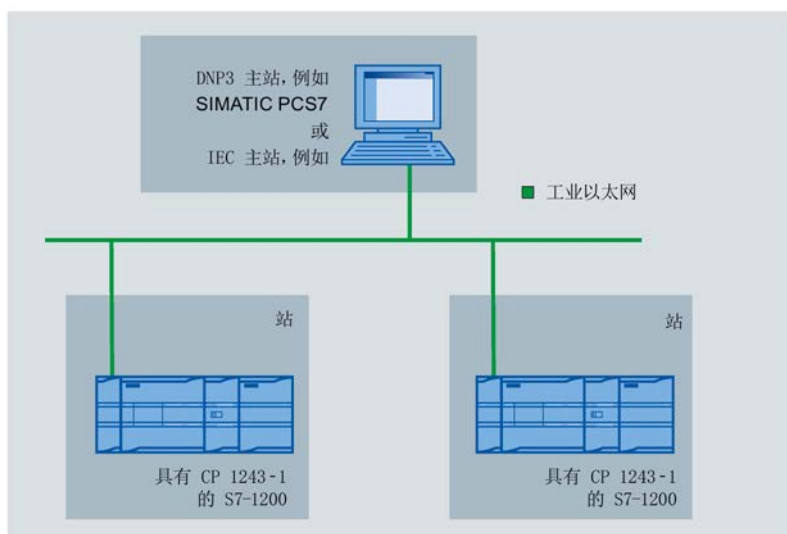


图 1-4 采用非冗余控制中心并且从站处于同一 IP 子网中的组态示例

S7-1200 站通过 CP 连接到 Internet，并与控制中心相连。

使用 DNP3 协议时，可将 SIMATIC PCS 7 TeleControl 或第三方提供商的系统用作控制中心。若使用 SIMATIC PCS 7 TeleControl 作为控制中心中的 DNP3 主站，则需要安装必要的 DNP3 驱动程序。

1.6.3.2 通过 Internet 进行连接的组态

通过 Internet 进行连接的组态示例

以下示例包含采用非冗余控制中心的组态。

本例中，使用了 DNP3 协议。而对于使用 IEC 协议的组态，设置均相同。

S7-1200 站通过 CP 连接到 Internet，并与控制中心相连。

使用 DNP3 协议时，可将 SIMATIC PCS 7 TeleControl 或第三方提供商的系统用作控制中心。若使用 SIMATIC PCS 7 TeleControl 作为控制中心中的 DNP3 主站，则需要安装必要的 DNP3 驱动程序。

1.6 组态示例

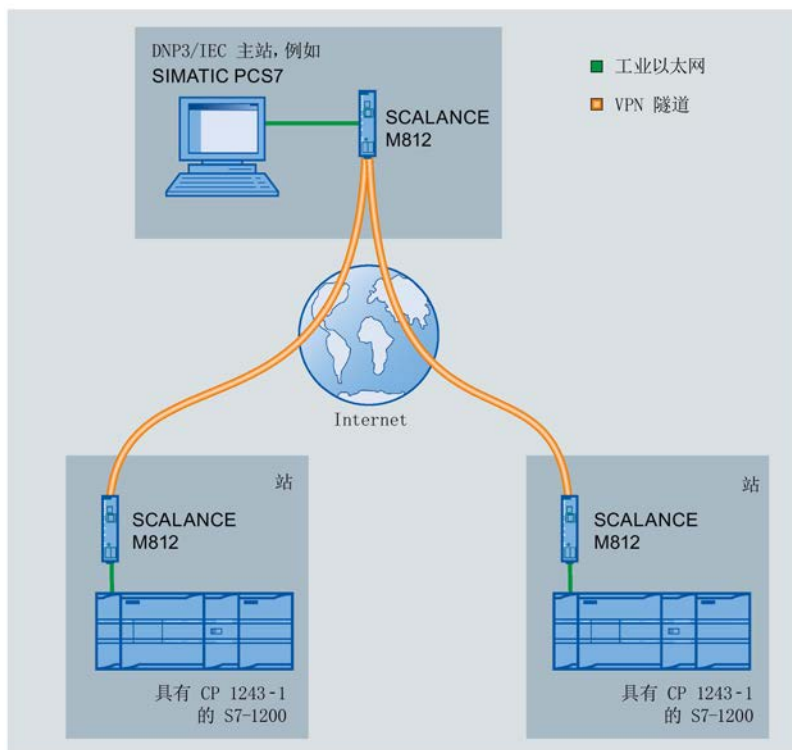


图 1-5 通过 Internet 进行连接的组态示例

作为路由器 SCALANCE 812 的替代方案，您还可以使用标准 DSL 调制解调器，并通过安全模块 SCALANCE S 建立 VPN 连接。

寻址

请参见DNP3/IEC (页 46)部分中的信息。

1.6.3.3 采用冗余控制中心的组态

采用冗余控制中心的组态示例

以下示例为采用冗余控制中心并通过 Internet 进行连接的组态。

本例中，使用了 DNP3 协议。而对于使用 IEC 协议的组态，设置均相同。

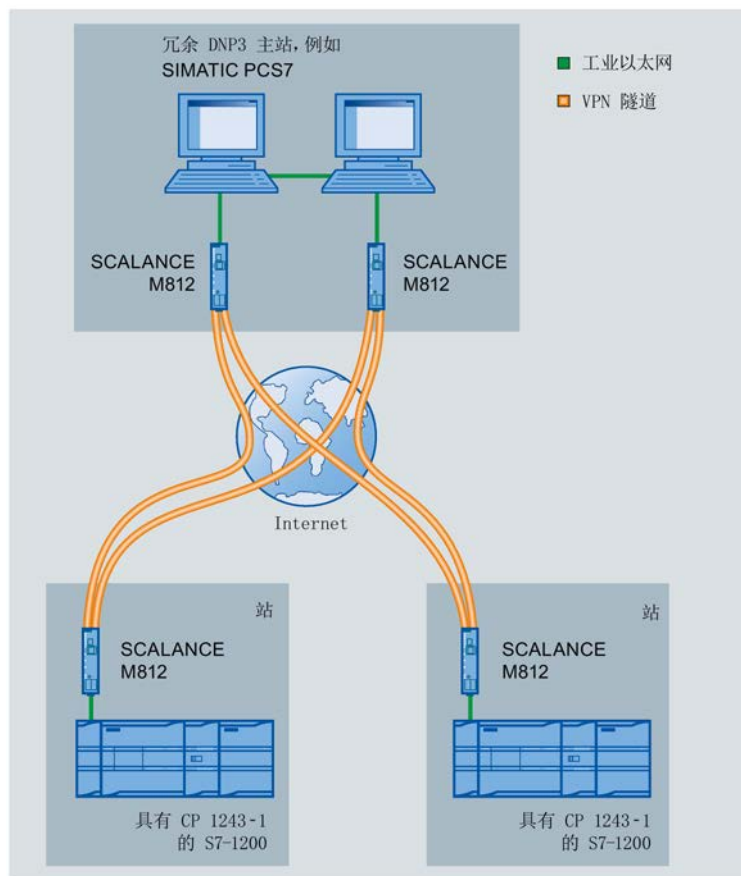


图 1-6 采用冗余 DNP3 主站的组态示例

冗余 DNP3 主站寻址

CP 通过同一个 DNP3 地址（实际是两个不同的 IP 地址）对控制中心中冗余 DNP3 主站的两台设备进行寻址。

1.7 使用要求

1.7.1 硬件要求

以下描述是关于遥控通信的组态。

不考虑导轨、外壳、电缆和其它附件。

根据工厂的具体组态，需要使用以下设备和固件版本。

1.7 使用要求

应用示例：与控制中心的遥控通信

在 S7-1200 站中：

- 自固件版本 V3 起的 CPU
CP 的完整功能仅适用于自 V4.2 起的 CPU。
- DSL 路由器 SCALANCE M812

在主站中：

- 带控制中心应用的 PC（备选）：
 - TCSB（版本 V3）
有关 TCSB 结构的更多详细信息，请参见/3/ (页 164)部分。
 - DNP3 主站
 - IEC 主站
- DSL 路由器 SCALANCE M812
- 使用在线功能时：带有 STEP 7 的工程师站（请参见软件要求 (页 26)部分）。

带有 CP 的 S7 站的组态：

装有 STEP 7 的工程师站

1.7.2 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，需要以下组态工具：

- STEP 7 Basic / Professional V14.0 SP1

LED 和连接器

2.1 打开外壳盖

显示元件和电气连接器的位置

用于具体显示模块状态的 LED 位于模块外壳上盖后面。

以太网连接器位于模块下铰链盖后面。

打开外壳盖

如图中箭头所示向上或向下拉可打开外壳的上盖或下盖。

保护盖伸到外壳外侧，使手有地方握。

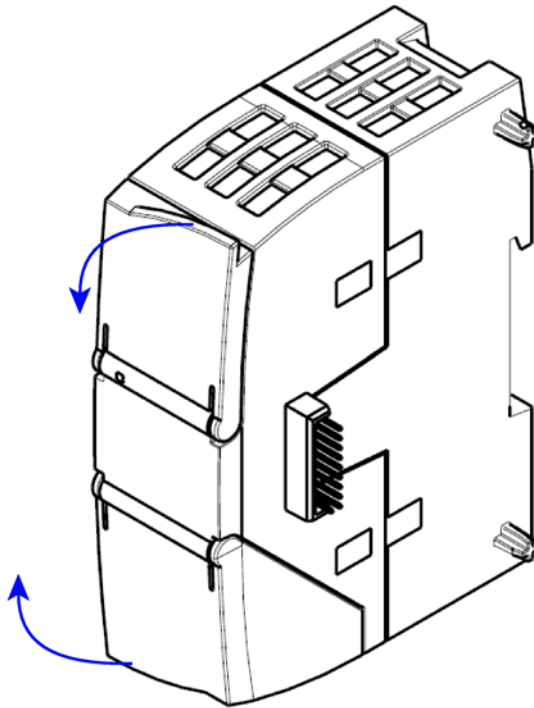


图 2-1 打开外壳盖

2.2 LED

模块的 LED

模块具有多个用于显示状态的 LED:


- **正面 LED**

始终可见的“DIAG”LED 显示模块的基本状态。





- **外壳上盖下方的 LED**

上盖下方的 LED 提供有关模块状态的详细信息。

表格 2-1 正面 LED

LED/颜色	名称	含义
 (红色/绿色)	DIAG	模块的基本状态




表格 2-2 外壳上盖下方的 LED

LED (颜色)	名称	含义
 (绿色)	LINK	与工业以太网的连接状态
 (绿色)	CONNECT	与通信伙伴的连接状态
 (绿色)	VPN	VPN 组态的状态
 (绿色)	SERVICE	用于实现在线功能的连接的状态

LED 状态的 LED 颜色和图示

下表中的 LED 符号具有以下含义：

表格 2-3 LED 符号的含义

符号				-
LED 状态	熄灭	亮起（常亮）	闪烁	不相关


说明

模块启动时的 LED 颜色

模块启动时，所有 LED 都短暂亮起。多色 LED 将显示混合颜色。此时，LED 的颜色不明确。

CP 的基本状态显示（“DIAG”LED）

表格 2-4 CP 的基本状态显示

DIAG (红色/绿色)	含义 (列出多条时可以表示多种不同的含义)
CP 的基本状态	
	<ul style="list-style-type: none"> • 断电 • 启动错误
 绿色	正在运行 (RUN)，无严重错误
 绿色闪烁	<ul style="list-style-type: none"> • 伙伴未连接 • 加载固件成功
 红色闪烁	<ul style="list-style-type: none"> • 正在启动 • 模块故障 • STEP 7 项目数据无效
 红绿闪烁	固件加载错误

2.2 LED

运行状态和通信状态的显示

LED 按以下方式指示模块的运行状态和通信状态：

表格 2-5 运行状态和通信状态的显示

DIAG (红色/绿色)	LINK (绿色)	CONNECT (绿色)	VPN (绿色)	SERVICE (绿色)	含义 (列出多条时可以表示多种不同的含义)
模块启动 (STOP → RUN) 或错误状态					
○	○	○	○	○	断电
● 红色	●	●	●	●	启动 - 阶段 1
● 红色闪烁	-	○	○	○	启动 - 阶段 2
● 绿色	-	-	-	-	正在运行 (RUN)，无严重错误
○		●	●	●	启动错误
● 红色	-	● 红色闪烁	-	-	STEP 7 项目数据无效
● 红色闪烁	-	○	-	-	缺少 STEP 7 项目数据
● 红色闪烁	●	● 红色闪烁	-	-	背板总线错误
与工业以太网的连接					
-	●	-	-	-	存在与工业以太网的连接
● 绿色	● 红色闪烁	-	-	-	<ul style="list-style-type: none"> 正在建立与工业以太网的连接。 正在获取 IP 地址。
-	○	-	-	-	与工业以太网无连接
与通信伙伴的连接					
● 绿色	●	●	-	-	建立了至少到一个通信伙伴的连接

DIAG (红色/绿色)	LINK (绿色)	CONNECT (绿色)	VPN (绿色)	SERVICE (绿色)	含义 (列出多条时可以表示多种不同的含义)
 绿色			-	-	可访问伙伴，CPU 处于 STOP 模式
 绿色闪烁			-	-	伙伴无法访问
用于实现在线功能的连接					
 绿色		-	-		已建立用于实现在线功能的连接
 绿色		-	-		尝试建立用于实现在线功能的连接
 绿色	-	-	-		未连接到工程师站
VPN 连接					
 绿色		-		-	已建立 VPN 连接
 绿色闪烁		-	 绿色闪烁	-	组态了 VPN 连接，但尚未建立。
-	-	-		-	在 CP 上未组态 VPN 连接
加载固件					
 红色和绿色交替闪烁					正在加载固件。DIAG LED 红色和绿色交替闪烁。
 绿色闪烁					已成功加载固件。
 红色闪烁					固件加载错误

2.3 电气连接器

2.3.1 电源

电源

CM 通过背板总线供电。不需要单独的电源。

2.3.2 以太网接口 X1P1

以太网接口

以太网连接器位于模块下铰链盖后面。接口是符合 IEEE 802.3 的 RJ-45 插孔。
有关引脚分配以及其它与以太网接口有关的数据，请参见技术数据 (页 153) 部分。

安装、连接、调试

3.1 使用设备的重要注意事项


有关设备使用的安全须知


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

过压保护

注意
<p>外部电源的保护</p> <p>如果通过较长的电源电缆或网络为模块或站供电，则电源电缆上可能会产生强电磁脉冲耦合效应。例如，雷击或开关较高负荷可产生这种现象。</p> <p>外部电源的连接无法抵御强电磁脉冲。</p> <p>要对其进行保护，必须使用外部过压保护模块。只有使用合适的保护元件时，才会满足 EN61000-4-5 对电源线路抗浪涌测试的要求。例如，Dehn Blitzductor BVT AVD 24（部件编号为 918 422）或类似的保护元件便是合适的设备。</p> <p>制造商： DEHN+SOEHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt, Germany</p>

3.1.1 有关在危险场所使用的注意事项

 警告
<p>爆炸危险</p> <p>请不要在设备通电时打开机壳。</p>

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

3.1 使用设备的重要注意事项



警告

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

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

如果设备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

请勿在易燃环境下连接或断开设备。



警告

爆炸危险

更换组件可能损害在 I 级 2 分区或 2 区的适用性。



警告

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。

3.1.2 IECEx/ATEX 要求的危险场所使用注意事项



警告

机柜/机壳要求

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



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



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

3.1.3 符合 UL HazLoc 要求的危险场所使用注意事项



爆炸危险

请勿在电路接通时断开连接，除非已知该区域不存在任何危险。

此设备仅适合在 I 类，2 分区，A、B、C 和 D 组或无危险位置使用。

此设备仅适合在 I 类，2 区，IIC 组或无危险位置使用。

3.1.4 FM 要求的危险场所使用注意事项




爆炸危险

请勿在电路接通时进行连接或断开连接，除非已知该区域不存在高浓度易燃气体。


此设备仅适合在 I 类，2 分区，A、B、C 和 D 组或无危险位置使用。

此设备仅适合在 I 类，2 区，IIC 组或无危险位置使用。

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

3.2 安装、连接和调试

安装和调试之前

 小心
阅读系统手册“S7-1200 可编程控制器” 在安装、连接和调试之前，先阅读系统手册“S7-1200 可编程控制器”中的相应部分，详细信息请参见本文档的附录。 安装和连接时，按照系统手册“S7-1200 可编程控制器”所述步骤操作。

拔出/插入模块

注意
插入/拔出模块时关闭工作站 在拔出或插入模块前，务必关闭工作站的电源。

安装尺寸

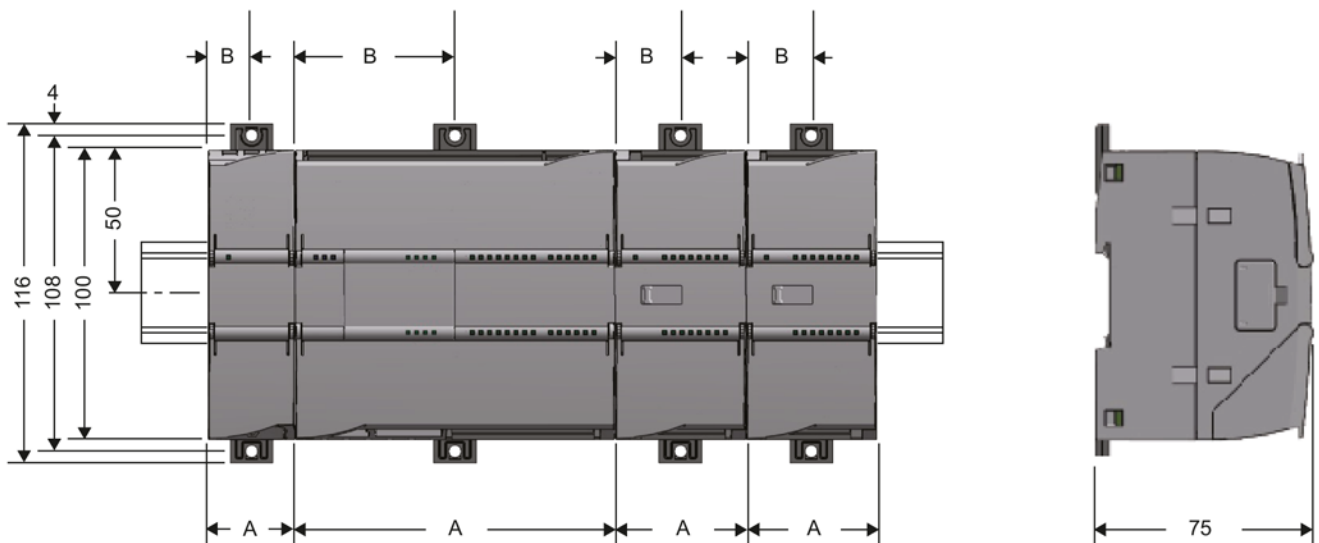


图 3-1 S7-1200 的安装尺寸

表格 3-1 安装尺寸 (mm)

S7-1200 设备		宽度 A	宽度 B *
CPU (示例)	CPU 1211C, CPU 1212C	90 mm	45 mm
	CPU 1214C	110 mm	55 mm
通信接口 (示例)	CM 1241, CM 1243-5, CM 1242-5	30 mm	15 mm
	CP 1242-7, CP 1243-1, CP 1243-7, CP 1243-8 IRC	30 mm	15 mm

* 宽度 B: 外壳边缘与 DIN 导轨安装夹孔的中心之间的距离

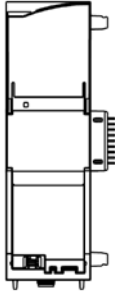
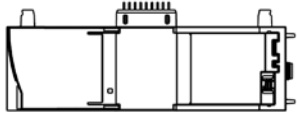
有关模块的详细尺寸, 请参见尺寸图 (页 161) 部分。

DIN 导轨夹, 控制面板安装

所有 CPU、SM、CM 和 CP 均可安装到机柜内的 35 mm DIN 导轨上。使用拉出式 DIN 导轨安装夹将设备固定在导轨上。这些安装夹在展开时也可锁定到位, 从而允许将设备安装在开关配电板中。DIN 导轨安装夹的孔的内部尺寸为 4.3 mm。

安装位置

注意
<p>安装位置</p> <p>安装模块时不能遮盖模块的上下通风口，以确保充分通风。在设备上方和下方必须留出 25 mm 的间隙，以使空气流通并防止过热。</p> <p>请记住，允许的温度范围取决于设备的安装位置。在CP 1243-1 的技术规范 (页 153)部分介绍了允许的温度范围。</p>

设备位置/允许的温度范围	安装位置
机架水平安装	
导轨垂直安装:	

要求： 调试前的组态

调试模块的一个要求是 STEP 7 项目数据完整无缺（请参见下文第 5 步）。

安装、连接和调试模块

说明

在电源关闭时连接

只有在 S7-1200 断电时才能接线。

表格 3-2 安装和连接步骤

步骤	执行的操作	备注和说明
1	将 CP 安装在 DIN 导轨上，并将其连接到右侧的模块。	使用 35 mm DIN 导轨。 允许使用 CPU 左侧的插槽。
2	固定 DIN 导轨。	
3	将以太网电缆连接到 CP。	有关接口的引脚分配，请参见技术数据 (页 153) 部分。
4	接通电源。	
5	剩余调试步骤涉及下载 STEP 7 项目数据。	在加载站时传送 CP 的 STEP 7 项目数据。 要加载站，请将项目数据所在的工程师站连接到 CPU 的以太网接口。 有关加载的详细信息，请参见 STEP 7 信息系统的以下部分： <ul style="list-style-type: none"> • "加载项目数据" • "使用在线和诊断功能"
6	合上模块前盖，并使其在运行期间保持闭合状态。	

3.3 操作注意事项

注意
<p>合上前面板</p> <p>为确保无干扰运行，运行期间应将模块的前面板保持闭合状态。</p>

3.3 操作注意事项

组态

4.1 安全建议

请遵循以下 Security 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。请在受保护的网路区域内运行该设备。
- 保持固件为最新。定期检查固件的安全更新，并相应安装。
- 定期在 Siemens Internet 页面上检查新功能。
 - 可以在以下链接中找到网络安全的相关信息：
链接：(<http://www.siemens.com/industrialsecurity>)
 - 可以在以下链接中找到工业以太网安全的相关信息：
链接：(<http://w3.siemens.com/mcems/industrial-communication/zh/ie/industrial-ethernet-security/Seiten/industrial-security.aspx>)
 - 可以在以下手册中找到关于工业安全主题的说明：
链接：
(http://w3app.siemens.com/mcems/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP02-0BA4_BR_Network_Security_en_112015.pdf)

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。如要要求将 CP 连接到 Internet 或使用 CP 1543SP-1，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

组态 CPU 的保护等级

有关信息，请参见 STEP 7 的信息系统。

- 安全通信功能

- 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。

- 使用变种安全协议 NTP (secure)和 SNMPv3。

- 使用遥控协议的安全功能。

- 离开对 CPU（CPU 组态）Web 服务器和对 CP 的 Web 服务器的访问。

- 记录功能

启用安全组态功能，并定期检查未经授权而进行访问的事件记录。

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。
 - 如果不使用遥控通信，NTP 协议提供 NTP (secure) 作为安全的备选方案。
 - 当访问 Web 服务器（CPU 的组态）时，HTTP 协议提供 HTTPS 作为安全的备选方案。

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。
 - 组态后关闭
由于 CP 始终为此服务的客户端，所以关闭端口。
- 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
DNP3 监听器端口	20000 (TCP)	关闭	组态后打开	否
IEC 监听器端口	102 (TCP)	关闭	组态后打开	否
S7 和在线连接	2404 (TCP)	打开	组态后打开 *	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
SNMP	161 (UDP)	打开	组态后打开	是（带 SNMPv3）

* 有关在诊断期间避免打开端口的信息，请参见通过端口 8448 执行在线安全诊断 (页 143)部分。

4.2 STEP 7 中的组态

STEP 7 中的组态

在 SIMATIC STEP 7 中组态模块和网络。可以在软件要求 (页 26)部分中找到所需版本。

在机架中安装 CP

每个站最多可组态三个 CM/CP。

组态通信的要求

组态 CP 和通信伙伴之间通信的一个要求是，对分配的 CPU 以及站的输入和输出数据进行编程。

还必须创建 PLC 变量以将用户数据分配到数据点。

有关详细信息，请参见以下各部分。

如何在 STEP 7 中组态遥控通信

组态时按照以下步骤操作：

1. 创建 STEP 7 项目。
2. 插入所需的 SIMATIC 站。

无法亦无需组态控制中心设备、应用以及 CP 和伙伴之间的连接。

3. 在站中插入 CP 以及所需的输入和输出模块。
4. 创建以太网网络。
5. 将站连接到以太网子网。
6. 组态插入的 CP。

有关组态通信的详细信息，请参见以下部分。

7. 保存项目。

有关组态 CP 的详细信息，请参见 STEP 7 的信息系统及以下部分。

加载和存储组态数据

加载站时，站的项目数据（包括 CP 的组态数据）存储在 CPU 中。

有关加载站的信息，请参见 STEP 7 信息系统。

4.3 寻址和验证

4.3.1 TeleControl Basic

CP 的 IP 地址

由于 CP 始终会建立与 TCSB 的连接，因此可通过 Internet 服务提供商向 CP 分配动态 IP 地址。

若要在运行期间更改 IP 地址，另请参见在运行期间更改 IP 地址 (页 138)部分。

与 TCSB 通信的地址和验证数据

要对 CP 的 TCSB 通信进行 STEP 7 组态，需要以下信息：

- “伙伴站”参数组中的参数
 - 伙伴 IP 地址
遥控服务器连接到 Internet 时所需的 DSL 路由器的 IP 地址或主机名称。
建议使用固定 IP 地址。
 - 伙伴端口（TCSB 监听端口的端口号）
- “安全 > CP 标识”(Security > CP identification) 参数组中的参数
 - 项目编号
 - 站编号
 - 密码（用于验证）

4.3.2 DNP3/IEC

要组态和调试 CP，需要以下信息：

主站的地址信息

CP 的 STEP 7 组态需要以下信息：

- 主站的地址
 - IP 地址
 - 或
 - 可由 DNS 解析的名称

若要使用 DNS，则必须有 DNS 服务器（请参见下文），而且 CP 必须可以访问该 DNS 服务器。

- 主站监听端口的端口号
- DNS 服务器地址

如果使用可由 DNS 解析的名称对主站寻址，则需使用 DNS 服务器地址。

通过 Internet 进行连接的组态：VPN 连接

对于通过 Internet 进行的连接，可使用动态 IP 地址。

为了实现双向通信并确保数据在传送过程中受到保护，必须通过 VPN 通道进行连接。为此，可以使用 SCALANCE S 或 SCALANCE M 系列安全模块。

在组态时请记住以下几点：

- 可按正常情况组态主站 IP 地址。
- 在组态 CP 接口时，应组态路由器的 IP 地址。
- 应在 STEP 7 中针对从站和控制中心创建 SCALANCE S/M 的 VPN 组态。

4.4 时钟同步

CP 的同步方法

说明

CP 的时钟同步

对于需要时钟同步的应用（例如遥控），需要定期同步 CP 的时钟。如果不定期同步 CP 的时钟，则 CP 的时间信息中每天可能有几秒的偏差。

启用安全功能后，需要启用时钟同步。

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。

CP 支持以下同步时钟的方法：

- **从伙伴获取时间**

CP 采用主站内通信伙伴的时钟。

仅适用于启用遥控通信后。

- **NTP**

通过所连接网络中的 NTP 服务器同步时钟。

在启用遥控通信时也可以使用该方法。

通过自固件版本 V3 起的 CP，NTP 服务器的地址也可以作为 URL 输入，例如 <ntp.server.com>。为此，需要 DNS 服务器。

- **NTP (secure)**

NTP (secure) 安全方法根据散列算法 MD5 或 SHA-1 使用对称密钥。

在 CP 上指定使用的服务器。

在 STEP 7 全局安全设置中组态类型为 NTP (secure) 的 NTP 服务器。

- **从 CPU 获取时间**

自 V4.2 起，CPU 以 10 秒为同步周期同步站的所有 CM/CP。

CPU 的参数：

如果为 CPU 启用了“CPU 同步设备的模块”(CPU synchronizes the modules of the device) 选项，则站的所有智能模块（固件版本 \geq V2.1.77 的 CP）将以 10 秒的同步周期与 CPU 时间进行同步。

时钟同步的参数组

您可以在以下参数组中组态时钟同步：

- **以太网接口**

可在下列条件下，在此处创建组态：

- 遥控通信已禁用。
- 安全功能已禁用。

- **安全性**

可在下列条件下，在此处创建组态：

- 安全功能已启用。

同步方法对使用 CP 的依赖性

根据使用的遥控通讯或安全功能情况，可选择以下同步方法：

- 遥控通信已禁用，安全已禁用
 - NTP
 - 从 CPU 获取时间
- 遥控通信已禁用，安全已启用
 - NTP
 - NTP (secure)
 - 从 CPU 获取时间
- 遥控通信和安全均已启用
 - 从伙伴获取时间
 - NTP
 - NTP (secure)
 - 从 CPU 获取时间

通过 S7-1200 进行时钟同步

使用外部时间源时，S7-1200 站可以通过 CPU 或 CP 获取当前时间。

对于 S7-1200，不会将始终从站转发至子网。

说明

建议：只由 1 个模块进行时钟同步

仅由单个模块对站中来自外部时间源的时间进行同步，以便使站内的时间保持一致。

当 CPU 从 CP 获取时间后，禁用 CPU 的时钟同步。

CPU 的时钟同步

CPU 可以使用以下同步方法：

- **NTP**

只可为 CPU 主动组态此选项：

- **从 CP 获取时间**

如果启用从 CP 向 CPU 的转发时间（见下文），CPU 将采用站 CP 的时钟。

将时间从 CP 转发至 CPU

说明

将时间转发到 CPU

根据所涉及模块的固件版本，可采用以下方式将 CP 的时间转发至 CPU：

- 通过 PLC 变量转发 CP 时间（可选）
 - 通过背板总线转发 CP 时间（强制）
-

将 CP 时间转发至 CPU 的操作取决于 CP 和 CPU 的固件版本。请注意以下行为。

- **CP 固件 ≤ V2.1.6x**

采用该固件版本时，CP 可以选择通过 PLC 变量为 CPU 提供时间。当 CPU 周期性地读取该 PLC 变量时，CPU 会采用 CP 时间。

在“与 CPU 通信”(Communication with the CPU) 参数组中，可设置 CP 当前的时钟是否可通过 PLC 变量提供给 CPU。有关 PLC 变量，请参见 CP 的参数组“与 CPU 通信”(Communication with the CPU)。

- **CP 固件 ≥ V2.1.77 和 CPU 固件 ≥ V4.2**

如果站中的两个模块均具备上述固件版本，则会将 CP 的时间自动转发给 CPU。

由于 CPU 自动采用 CP 时间，因此不再需要通过 PLC 变量进行转发。

如果在“PROFINET 接口 > 时间同步”(PROFINET interface > Time synchronization) 中为 CPU 启用了“CPU 同步设备的模块”(CPU synchronizes the modules of the device) 选项，则站的所有智能模块将与 CPU 时间进行同步。

4.5 通信类型

在此参数组中，可以启用 CP 的通信类型。

为最大程度降低未经授权的用户通过以太网访问工作站的风险，您需要启用通信服务，CP 将分别执行这些服务。用户可以不启用以下所有选项，但至少应启用其中一个选项。

“通信类型”参数组

- 启用遥控通信
 - TeleControl Basic
 - DNP3
 - IEC 60870-5

请注意，如果之后更改遥控通信类型，则会删除所有特定参数。此外，还包括数据点和伙伴信息等。

- 激活在线功能

允许通过 CP 访问 CPU 的在线功能（诊断、加载项目数据等）。如果启用此功能，工程师站可通过 CP 访问 CPU。

如果禁用此选项，无法通过 CP 访问 CPU 的在线功能。不过，仍然可以通过直接连接到 CPU 的接口在线诊断 CPU。

- 启用 S7 通信

在 CP 上启用与 SIMATIC S7 之间的 S7 通信功能。

如果组态了与相关站之间的 S7 连接，并且要通过 CP 来运行，则需要启用该选项。

4.6 以太网接口

4.6.1 CP 标识

只有启用遥控通信后，此参数组才可用。

CP 寻址

参数组用于网络中 CP 的寻址和标识。

- TeleControl Basic

您将在“安全”(Security) 中找到 TeleControl Basic 协议的参数，请参见使用 TeleControl Basic 协议的 CP 标识 (页 73)部分。

- DNP3

站地址是 DNP 地址。

输入站地址（仅限数字）。允许的值范围：1...65519。

- IEC

站地址是“ASDU 的公共地址”或信息对象的地址。

输入站地址（仅限数字）。允许的值范围：1...65534。

4.6.2 时钟同步

时钟同步

有关时钟同步的组态，请参见时钟同步 (页 48)部分。

4.6.3 高级选项

TCP 连接监视

在此进行的设置全局适用于 CP 已组态的全部 TCP 连接。

使用 TeleControl Basic 和 DNP3:

注意可为各个通信伙伴覆盖此处组态的值的选项，请参见伙伴站 (页 61)部分。

• TCP 连接监视时间

功能：如果在 TCP 连接监视时间内无数据通信，则 CP 向通信伙伴发送保持连接消息。

默认设置： 180 s。允许的范围： 1...65535 s。

– 以太网接口下的参数

为以太网接口组态的监视时间全局适用于所有 TCP 连接。该参数预设为 180 s（默认值）。

– “伙伴站”(Partner stations) 下的参数

将再次出现“伙伴连接”(Connection to partner) 参数组中各伙伴的“TCP 连接监视时间”(TCP connection monitoring time)

参数。该参数仅适用于对应的单个伙伴。在以太网接口上预设的 180 s 参数值适用于各个伙伴。

如果想要更改各个伙伴的“TCP 连接监视时间”(TCP connection monitoring time) 值，可在“伙伴站”(Partner stations)

中单独为每个伙伴调整该值。例如，如果想要以更短的时间间隔检查连接，则需减小该值。

• TCP 保持连接监视时间

CP 发送保持连接消息后，应在保持连接监视时间内收到通信伙伴的响应。如果 CP 在组态时间内未收到响应，它将终止连接。

默认设置： 10 s。允许的范围： 1...65535 s。

– 以太网接口下的参数

为以太网接口组态的监视时间设置全局适用于所有 TCP 连接。

– “伙伴站”(Partner stations) 下的参数

与 TCP 连接监视时间 (TCP connection monitoring time) 参数一样，可单独为每个伙伴调整“伙伴站”(Partner stations) 的值。

4.6.4 传输设置 – TeleControl Basic

传输设置 – TeleControl Basic

- **连接建立延迟**

在此进行的设置适用于遥控服务器的连接。

重连延迟是指，当无法访问遥控服务器或连接已中止时，CP 重复尝试建立连接之间的等待时间。

该等待时间避免在存在连接问题时以较短间隔连续尝试建立连接。

为下一次尝试建立连接之前的等待时间组态一个基准值。从该基准值开始，每经过 3 次重试失败后当前等待时间将加倍，直到最大值 900 s。

默认设置： 10 s。基准值的取值范围为： 10...300 s

例如：

已组态的基准值为 20 时尝试重新建立连接之间的间隔（等待时间）如下：

- 3 次 20 s
- 3 次 40 s
- 3 次 80 s
- 依此类推，直到最大值 900 s

说明

如果该伙伴无法连接，则通过移动无线网络建立连接可能需要几分钟。这可能取决于具体的网络以及当前的网络负载。

根据合约要求，每次尝试建立连接都可能产生一定费用。

- **发送监视时间**

从主动发送帧后到收到伙伴（遥控服务器）确认所经过的时间。主动发送帧后即开始计时。若发送监视时间结束后，仍未收到伙伴的确认，则最多重复发送此帧三次。三次尝试失败后，连接终止并重新开始建立。

默认设置： 60 s。允许的范围： 1...65535 s。

- **看门狗监视时间**

在看门狗周期内，CP 会检查与遥控服务器之间的连接。看门狗周期是指 CP 与遥控服务器之间无数据交换的一段时间间隔，经过该时间间隔后，CP 会向遥控服务器发送看门狗帧。看门狗周期仅可通过

TCSB（参数“保持连接监视时间”(Keepalive monitoring)

time) 进行组态。首次建立连接后，在 TCSB 中组态的值会由遥控服务器传送到 CP。

CP 每次将数据传送到 TCSB

并收到遥控服务器发出的确认消息后，就会启动看门狗周期。看门狗周期溢出时，CP 会向遥控服务器发送看门狗帧。

发送看门狗帧后，CP 会启动看门狗监视时间(watchdog monitoring time)，然后在这段时间内等待遥控服务器的响应。如果 CP 在监视时间内未收到遥控服务器的响应，它将终止并重新建立连接。

默认设置：30 s。允许的范围：0...65535 s。如果输入 0（零），则会禁用该功能。

- **密钥交换间隔**

在此处输入 CP 和遥控服务器交换密钥的时间间隔（单位为小时）。密钥是 CP 和 TCSB V3 使用的遥控协议的安全功能。

默认设置：8 s。允许的范围：0...65535 s。如果输入 0（零），则会禁用该功能。

4.6.5 传输设置 – DNP3

传输设置 – DNP3

- **干扰位**

干扰位可用作“Internal Indication Bytes”的位 1.6 (IIN1.6)，以在 CPU 处于 STOP 模式时通知主站。

- **选择和操作之间的最长时间**

选择和操作之间的最长持续时间（秒）。若将“选择”命令传送到 CPU 并要该命令生效，则在“选择”与“操作”之间不能再向该站发送其它帧。

允许的范围：1..65535

默认设置：1

- **帧重复**

在未接收到主站确认的情况下，数据链路层的重复帧数目。

允许的范围：0 ... 255

默认设置：0

如果输入 0（零），则会禁用该功能。

- **连接确认**

CP 请求主站发送连接确认的情况（从不、始终、仅限分段帧）。

- **连接监视时间**

期望收到主站确认的时间（单位为秒）。

允许的范围：0...65535

默认设置：2

如果输入 0（零），则会禁用该功能。

- **传送模式“主动”**

事件的传输模式

- 自发

立即传输事件帧。

- 有条件自发

事件消息仅在发送自发帧或伙伴建立连接时发送。

- **主动帧的最大数量**

在未接收到通信伙伴确认的情况下，重复主动帧的最大数目。

允许的范围：0...255

默认设置：3

- **主动帧的监视时间**

期望从主站接收到主动帧确认的时间（单位为秒）。

允许的范围：1...65535

默认设置：5

- **1/2/3 类事件缓冲**

在此，对于三个事件类别的任一个，指定在出现多少事件后将存储的事件发送至通信伙伴。

允许的范围：1 ... 255。

- **1/2/3 类事件延迟时间**

在此，对于三个事件的任一个，指定在将事件发送至通信伙伴前，可将其保存在发送缓冲区的最长时间（单位为秒）。

允许的范围： 0 ... 65535

如果输入 0（零），则会禁用该功能。

- **映像存储器的事件类别**

选择只将最新的当前值存储于发送缓冲区中的事件类别。

在默认设置中，1 类和 2 类事件的所有值都存储在发送缓冲区中，3 类事件仅存储当前值（映像存储器过程）。

有关映像缓冲区和发送缓冲区工作方式以及传送数据选项的详细信息，请参见过程映像、传输类型、事件类别、触发 (页 112) 部分。

4.6.6 传输设置 - IEC

传输设置 - IEC 60870-5

- **选择和操作之间的最长时间**

选择和操作之间的最长持续时间（秒）。若将“选择”命令传送到 CPU 并要使该命令生效，则在“选择”与“操作”之间不能再向该站发送其它帧。

允许的范围： 1..65535

默认设置： 1

- **连接建立的监视时间 (t_0)**

连接建立的监视时间 (t_0)，单位为秒。如果通信伙伴在该监视时间内未确认连接建立，CP 将尝试再次建立连接。

允许的范围： 1..255

默认设置： 30

- **帧监视时间 (t_1)**

通信伙伴确认 CP 发送帧的监视时间（单位为秒）。该监视时间适用于 CP 发送所有 I、S 和 U 格式的帧。

如果在监视时间内伙伴未发送确认，CP 终止与该伙伴的连接。

允许的范围：1..255

默认设置： 15

说明

主站设置

组态监视时间 t_1 和 t_2

时，确保在主站上进行相应的设置，以避免产生意外的错误消息或连接中止。

- **S 和 U 帧的监视时间 (t_2)**

CP 确认主站数据帧的监视时间（单位为秒）。

从主站接收到数据后，CP 按如下方式确认接收到数据：

- 如果 CP 在 t_2 内将数据发送至主站本身，它将在发送数据帧（I 格式）的同时确认在 t_2 内接收到从主站发来数据帧。
- t_2 过去后，CP 向最新的主站发送确认帧（S 格式）。

允许的范围： 1 ... 255

默认设置： 10

t_2 的值应小于 t_1 的值。

- **测试帧的空闲时间 (t_3)**

CP 未从主站接收到任何帧时的监视时间（单位为秒）。

t_3 过去后，CP 向主站发送测试/控制帧（U 格式）。

此参数适合空闲时段（即没有数据通信的时间）较长的情况。

允许的范围： 1 ... 255

默认设置： 30

- **发送序号 N(S) 和接收序号 N(R) (k) 的差值**

帧的发送序号和接收序号之差。

主站返回 CP 发来的帧的发送序号，发送 CP

随后会将该序号作为接收序号保存。加上此处组态的差值后，发送序列号还小于接收序列号的帧会被视为已成功传送并从 CP 的发送缓冲区中删除。

允许的范围： 1 ... 64

默认设置： 12

- **未确认数据帧的最大数量 (w)**

w: 收到的数据帧 (I-APDU) 的最大数量，必须确认此后最早从主站接收的帧。

允许的范围： 1..8

默认设置： 8

该值必须小于“发送和接收序号之差” (k) 的值。

IEC 协议的确认机制

对于发送的每个数据帧，CP

都会发送连续的发送序号。数据帧起初存储在发送缓冲区中。

主站接收到数据帧后，会发送该帧（如果收到多个帧，则为最后一个帧）中的发送序号作为对 CP 的发送确认。CP

会将主站返回的发送序号作为接收序号存储起来，并将其用作接收确认。

发送序号小于或等于当前接收序号的帧会被视为已成功传送并从 CP 的发送缓冲区中删除。

推荐规范值：

- w 不得高于 k 的 2/3。
- 推荐的 k 值： 12
- 推荐的 w 值： 8

4.7 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!

- **SNMPv3**

仅当启用安全功能时可用

有关配置 SNMPv3 的信息, 请参见SNMP (页 81)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。

4.8 伙伴站

只有启用遥控通信后, 此参数组才会显示出来。

4.8.1 伙伴站 > 常规参数

监听器端口

仅限于 DNP3/IEC

此处显示模块的监听器端口和通信伙伴连接请求的端口。

- DNP3 协议默认值：20000
- IEC 协议默认值：2404

您可以更改模块的端口号。请记住通讯伙伴（主站）上的设置。

允许的范围： 1024...65535

伙伴'X' / 通信服务器

- 激活伙伴
 - TeleControl Basic
在默认设置中，启用遥控服务器作为唯一可能的伙伴。
 - DNP3/IEC
启用该选项后，可启用可组态主站进行通信。
- 伙伴编号
伙伴编号由系统分配。数据点组态期间需要向其通信伙伴分配数据点。
- 站地址 / 主站地址
 - TeleControl Basic
如果启用了遥控通信，则系统会自动分配遥控服务器的站地址。
 - DNP3
为进行标识，必须在主站上组态站地址。
 - IEC
公共 ASDU 地址

与伙伴连接

- **伙伴 IP 地址**

伙伴的 IP 地址或主机名称 (FQDN)。例如，可也为 DynDNS 服务的 FQDN。

- **TeleControl Basic 的注意事项**

如果 CP 连接到 TCSB 冗余组 (TCSB V3)，则在此组态 DSL 路由器的公共 IP 地址，从而可通过 Internet 访问遥控服务器。在 DSL 路由器上设置端口转发，这样公共 IP 地址（外部网络）就会成为 TCSB 服务器 PC 的虚拟 IP 地址（内部网络）。因此，该站也不会接收到告知其连接到冗余组两台计算机中哪一台的任何信息。

另请参见在冗余 TCSB 系统中寻址 (页 65)部分。

- **连接监视**

仅适用于 TeleControl Basic 和 DNP3

启用该功能时，将通过发送保持连接帧来监视与通信伙伴的连接。

在以太网接口参数组中为 CP 的所有 TCP 连接设置 TCP 连接监视时间。该设置适用于 CP 的所有 TCP 连接。

在参数组“伙伴站”(Partner stations) 的此处，可以为伙伴单独设置全局设置的 TCP 连接监视时间。此处为伙伴设置的值会覆盖在参数组“以太网接口 (X1) > 高级选项 > TCP 连接监视”(Ethernet interface (X1) > Advanced options > TCP connection monitoring) 中设置的全局值。

- **TCP 连接监视时间**

仅适用于 TeleControl Basic 和 DNP3

功能：如果 TCP 连接监视期间无数据通信，则 CP 向通信伙伴发送保持连接消息。

默认设置： 180 s。允许的范围： 1...65535 s。

在更高级别为以太网接口指定的监视时间默认适用于所有已组态 TCP 连接。

- **以太网接口下的参数**

为以太网接口组态的监视时间全局适用于所有 TCP 连接。将该参数预设为 180 s（默认值）。

- **“伙伴站”(Partner stations) 下的参数**

会再次出现“连接到伙伴”(Connection to partner) 参数组中各个伙伴的“TCP 连接监视时间”(TCP connection monitoring time)

参数。该参数仅适用于对应的单个伙伴。在以太网接口上预设的 180 s 参数值适用于各个伙伴。

如果想要更改各个伙伴的“TCP 连接监视时间”(TCP connection monitoring time) 值, 可在“伙伴站”(Partner stations)

中单独为每个伙伴调整该值。例如, 如果想要以更短的时间间隔检查连接, 则需减小该值。

- **TCP 保持连接监视时间**

仅适用于 **TeleControl Basic** 和 **DNP3**

如果在此处组态的值与以太网接口参数组中组态的值不同, 则将使用“伙伴站”(Partner stations) 参数组的监视时间。

CP 发送保持连接消息后, 应在保持连接监视时间内收到通信伙伴的响应。如果 CP 在组态时间内未收到响应, 它将终止连接。

默认设置: 10 s。允许的范围: 1...65535 s。

- **以太网接口下的参数**

为以太网接口组态的监视时间设置全局适用于所有 TCP 连接。

- **“伙伴站”(Partner stations) 下的参数**

与 TCP 连接监视时间 (TCP connection monitoring time) 参数一样, 可单独为每个伙伴调整“伙伴站”(Partner stations) 的值。

- **连接模式 (Connection mode)**

在“永久”(Permanent) 连接模式下, 与通信伙伴间存在永久连接。

CP 仅支持该连接模式。

- **连接建立**

指定将建立连接的通信伙伴 (始终为 CP)。

- **协议类型**

仅适用于 **DNP3**

选择传输层的协议类型: TCP / UDP

- **伙伴端口**

仅限于 **TeleControl Basic**

遥控服务器的监听端口号。

4.8.2 TeleControl Basic

4.8.2.1 在冗余 TCSB 系统中寻址

冗余遥控服务器的寻址

- 站使用一个 IP 地址对 TCSB 冗余组进行寻址

在 LAN 中的 TCSB 服务器 PC 与 DSL 路由器（如 SCALANCE M）所连接的主站上，计算机操作系统的网络负载平衡 (NLB) 功能将为两个服务器 PC 分配一个公共的虚拟 IP 地址。

该 IP 地址根据网络设置进行组态：

- 如果仅连接一个没有 DSL 路由器的 CP，则必须在 CP 中将 NLB 分配的虚拟地址组态为遥控服务器的 IP 地址。
- 如果使用 DSL 路由器，对站中的冗余遥控服务器进行寻址时只需组态一个 IP 地址，即 DSL 路由器的公共地址。

在 DSL 路由器上设置端口转发，这样公共 IP 地址（外部网络）就会成为 TCSB 服务器 PC 的虚拟 IP 地址（内部网络）。通过 Internet 只能访问公共 IP 地址。因此，该站也不会接收到告知其连接到冗余组两台计算机中哪一台的任何信息。

4.8.2.2 高级设置

遥控服务器 > 高级设置

- 报告伙伴状态

如果启用了“报告伙伴状态”(Report partner status) 功能，CP 将会向远程伙伴报告通信状态。

- 如果可与伙伴连接，则“伙伴状态的 PLC 变量”(PLC tag for partner status)（数据类型 WORD）的位 0 置为 1。
- 如果到远程伙伴的所有路径均正常（对冗余路径有用），则位 1 置 1。

- 位 2-3 指示发送缓冲区（帧存储器）的状态。

可能的值包括：

- 0：发送缓冲区正常
- 1：发送缓冲区将要溢出（充满超过 80 %）。
- 3：发送缓冲区已溢出（充满到 100 %）。

一旦填充量降到 50% 以下，位 2 和位 3 就复位为 0。

PLC 变量的位 4 到 15 未使用且不需要在程序中进行评估。

4.8.2.3 站间通信的伙伴

站间通信

在此表格中，指定当前站使用站间通信的 S7 站。站间通信的连接通过遥控服务器实现。

伙伴

伙伴编号由系统分配。数据点组态期间需要向其通信伙伴分配数据点。

对于站间通信，通过参数“项目”、“站”和“插槽”对伙伴进行寻址。

项目

在此处输入伙伴站中的 CP 的项目号。（伙伴上的参数组“Security > CP 标识”(Security > CP identification)）

站

在此处输入伙伴站中的 CP 的站编号。（伙伴上的参数组“Security > CP 标识”(Security > CP identification)）

插槽

在此处输入伙伴站中用来建立连接的 CP 的插槽号。

帧存储器

激活启用站间通信的选项。

如果连接受到干扰，帧将存储在 CP 的发送缓冲区（帧存储器）中。请注意，所有通信伙伴共用帧存储器的容量。

访问 ID

此处显示的访问 ID 由项目号、站号和插槽的十六进制值组成。DWORD 类型的参数分配如下：

- 位 0 - 7：插槽
- 位 8 - 20：站编号
- 位 21 - 31：项目编号

4.8.3 DNP3 / IEC

4.8.3.1 高级设置 (DNP3 / IEC)

高级设置

- 伙伴监视时间

如果 CP 未在组态的时间内接收到来自通信伙伴的生命迹象信号，则 CP 会将此解释为伙伴故障/错误。CP 将中止连接并尝试重新建立该连接。

如果输入 0，则会禁用此功能。

- DNP3 等级

仅适用于 DNP3

指示 CP 支持的 DNP3 implementation level

在 DNP3

规范中定义了各种等级的协议符合性，这些等级描述了主站或站的受支持的功能范围 (subset)。这些等级 (implementation levels) 称为“DNP3 Application Layer protocol Level”，其缩写为 DNP3-L1 至 DNP3-L4。

对于 CP 和主站之间的通信，主站支持的 DNP3 等级必须已知。

所选的 DNP3 CP 使用的等级需要在 STEP 7 中为每个通信伙伴（DNP3 主站）单独进行设置，必须与相应连接的主站使用的等级一致。

CP 支持以下 implementation levels:

- Level 1
- Level 2
- Level 3
- Level 4
- Level 4+

在标准中未指定的实现层（本文称为 Level 4+）包含 Level 4 的各种功能，此外还支持下列 DNP3 数据类型/变量：

- 不带时钟的 64 位浮点数模拟值
- 带时钟的 64 位浮点数模拟值
- 带时钟 16 位格式的 Counter event
- 带时钟 32 位格式的 Counter event

- **事件传送模式**

仅适用于 DNP3

向此通信伙伴传送 DNP 事件所采用的模式：

- 按时间顺序传送帧
- 或
- 将每个数据点的收集帧作为块进行传送。

- **报告伙伴状态**

如果启用了“报告伙伴状态”(Report partner status) 功能，CP 将会向远程伙伴报告通信状态。

- 如果可与伙伴连接，则“伙伴状态的 PLC 变量”(PLC tag for partner status)（数据类型 WORD）的位 0 置为 1。
- 如果到远程伙伴的所有路径均正常（对冗余路径有用），则位 1 置 1。
- 位 2 指示发送缓冲区（帧存储器）的状态。
可能的值包括：
 - 0: 发送缓冲区正常
 - 1: 发送缓冲区将要溢出（充满超过 80 %）。
 - 3: 发送缓冲区已溢出（充满到 100 %）。只要填充水平降到 50% 以下，位 3 就复位为 0。

PLC 变量的位 3 到位 15 未使用且不需要在程序中进行评估。

与 CPU 通信

使用前三个参数在 CPU 扫描周期中指定 CP 的 CPU 访问权限。有关 CPU 扫描周期的结构，请参见读取周期 (页 111)部分。

第四个参数“帧存储器大小”(Frame memory size) 决定用于存储组态为事件的数据点帧的 CP 发送缓冲区的大小。

- **周期暂停时间**

CPU 存储区两个扫描周期之间的等待时间

- **写作业的最大数目**

一个 CPU 扫描周期内向 CPU 存储区写入的作业的最大数目

- **读作业的最大数目**

一个 CPU 扫描周期内从 CPU 存储区读取的低优先级作业的最大数目。

- **帧存储器大小**

在此，设置事件的帧存储器的大小（发送缓冲区）。

帧存储器的大小将均分给所有已组态的通信伙伴。有关帧存储器大小的信息，请参见组态限制和性能数据 (页 17)部分。

有关发送缓冲区工作方式（存储和发送事件）以及传送数据选项的详细信息，请参见过程映像、传输类型、事件类别、触发 (页 112)部分。

看门狗位

- **CP 监视**

通过看门狗位，可将 CP 的遥控通信状态发送给 CPU。

CP 时钟

- **到 CPU 的 CP 时间**

使用此功能，CP 可将其时钟用于 CPU。

有关详细信息，请参见 STEP 7 信息系统。

CP 诊断

通过参数组，可以选择使用 PLC 变量从 CP 中读出高级诊断数据。

- **启用高级 CP 诊断**

启用该选项以使用高级 CP 诊断。

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

可选择性启用下列用于诊断数据各个项的 PLC 变量。

- **诊断触发变量**

如果 CPU 用户程序中的 PLC 变量 (BOOL) 设置为 1，则 CP 将更新稍后可组态用于高级诊断的 PLC 变量的值。

将当前值写入下列 PLC 变量后，CP 会将“诊断触发变量”(Diagnostics trigger tag) 设为 0，指示 CPU 可以从 PLC 变量读取更新的值。

说明

诊断触发变量的快速设置

不得将触发设置为快于 500 毫秒的最小间隔。

- **帧存储器溢出**

用于发送缓冲区溢出预警的 PLC 变量（数据类型字节）。当发送缓冲区的填充量达到 80% 时位 0 置 1。

- **帧存储器大小**

用于表示发送缓冲区占用量的 PLC 变量（DWord 数据类型）。显示保存的帧数。

- **最后一次成功登录 TCSB 的日期**

仅适用于 TeleControl Basic 协议

用于表示 CP 最后一次登录遥控服务器的日期的 PLC 变量（DTL 数据类型）。

- **最后一次未成功登录 TCSB 的日期**

仅适用于 TeleControl Basic 协议

用于表示 CP 最后一次未能登录遥控服务器的日期的 PLC 变量（DTL 数据类型）。

- **TeleService 状态**

PLC 变量 (BOOL) 指示 TeleService 会话是否为激活状态。

- 0 = 无激活状态的 TeleService 会话
- 1 = TeleService 会话处于激活状态

- **VPN 状态**

PLC 变量 (BOOL) 指示是否已建立 VPN 隧道。

- 0 = 无已建立的 VPN 隧道
- 1 = VPN 隧道已建立

4.9 安全性

有关安全功能的范围和使用的概览信息，请参见安全功能 (页 15)部分。

有关安全功能的组态限制，请参见组态限制和性能数据 (页 17)部分。

4.9.1 参数概述

参数组

如果启用了 CP 的安全功能，则可以找到用于组态 CP 的以下参数组：

- **CP 标识**

仅限 TeleControl Basic 协议

在此组态相关参数，以使用遥控服务器对 CP 进行验证。有关上述参数的详细信息，请参见下文。

- **DNP3 安全选项**

仅限 DNP3 协议

在此处，可以组态协议特定的安全功能。有关上述参数的详细信息，请参见下文。

- **防火墙**

请参见防火墙 (页 77)部分。

- **时间同步**

有关时钟同步的组态，请参见时钟同步 (页 48)部分。

- **电子邮件组态**

请参见电子邮件组态 (页 79)。

- **日志设置**

在此处对安全相关事件的记录事宜进行设置。

请参见日志设置 - 过滤系统事件 (页 80)部分。

- **SNMP**

在此处，可对 CP 上的 SNMP 代理进行设置。

请参见SNMP (页 81)部分。

- **证书管理器**

请参见证书管理器 (页 82)。

此外，在 STEP 7 全局安全设置中，您将找到以下参数组：

- **VPN 组**

在此处组态 VPN 通信，请参见VPN (页 85)部分。

- **用户管理**

在此处组态有关 TeleService 访问的用户、角色和权限，请参见TeleService 访问的组态 (页 91)部分。

4.9.2 使用 TeleControl Basic 协议的 CP 标识

在“CP 标识”(CP identification) 参数组中，可以组态以下信息以使用遥控服务器验证 CP：

- **项目编号**

STEP 7 项目中所有遥控 CP 的项目编号均相同。TCSB 从 1 到 2000 之间估计项目编号。

如果更改了项目号，则 STEP 7 项目中所有 CP 的此参数都将更改。

- **站编号**

对于具有遥控 CP 的每个 S7-1200 站，将组态单独的站编号。TCSB 从 1 到 8000 之间估计站编号。

- 遥控密码

用于对遥控服务器上的 CP 进行验证的密码。

ASCII 字符集 0x20 ... 0x7e 的 8 ... 29 个字符

可以对 STEP 7 项目的所有 CP 使用相同密码。在 TCSB 中为该站组态相同的密码。

- 访问 ID

显示的访问 ID 由项目号、站号和插槽的十六进制值组成。该 DWORD 类型的参数分配如下：

- 位 0 - 7：插槽
- 位 8 至 20：站编号
- 位 21 至 31：项目编号

4.9.3 DNP3 安全选项

伙伴'X'

初步说明：验证和密钥交换

如果启用安全选项，DNP3 主站和 CP 通过私密密钥（预共享密钥）对自身进行验证。

借助公用的预共享密钥在主站与 CP

之间建立第一个连接后，商定会话密钥并周期性更新会话密钥。通常由主站启动会话密钥的更新操作。在下列参数中指定更新密钥的标准。

- 密钥交换间隔
- 密钥交换前的验证请求次数

只要满足这其中任何一个条件，就会更新会话密钥。

参数

- **启用 DNP3 安全选项**

如果要使用安全机制，请启用此选项。

- **IKE 模式**

选择密钥交换模式。取值范围：

- **Aggressive Mode**

Aggressive Mode 更快一些但不会加密传送身份。

- **Main Mode**

Main Mode 为标准模式。

默认设置： **Aggressive Mode**

- **安全统计信息**

指定是否将安全事件的统计信息发送到主站。安全事件是 CP 的验证请求。如果启用该选项，含日期、时间和结果的所有验证请求将保存在 CP 中并发送至主站进行进一步评估。

取值范围：

- 不发送安全统计信息

- 发送安全统计信息

默认设置： 不发送安全统计信息

- **SHA-1 互锁**

已将“SHA-256”组态为安全散列算法，但主站不支持 SHA-256 时，此设置用于选择 CP 是否可使用安全散列算法 SHA-1。

取值范围：

- 不允许使用 SHA-1 模式

CP 可能不会使用 SHA-1。主站不支持 SHA-256 时，将不会建立连接。

- 允许使用 SHA-1 模式

主站不支持 SHA-256 时，CP 可以使用 SHA-1。

默认设置： 不允许使用 SHA-1 模式

- **安全散列算法 (SHA)**

选择 Secure Hash Algorithm (SHA)

取值范围:

- SHA-1
- SHA-256

默认设置: 256

- **加密算法**

选择 Advanced Encryption Standard (AES)

取值范围:

- AES-128
- AES-256

默认设置: AES-128

- **密钥长度**

指定预共享密钥的长度（字节）。

允许的范围: 16 - 128 根据 STEP 7 中组态的上述安全散列算法, 预设了以下长度:

- 对于 SHA-1: 16
- 对于 SHA-256: 32

不允许值 0（零）。

- **统计请求的最大次数**

如果在密钥交换间隔内超出组态的主站统计查询次数, CP 会在 CPU 诊断缓冲区中输入一条消息。

取值范围: 2...255 默认设置: 5

- **密钥交换前的验证请求次数**

CP 向主站请求验证的最大次数。达到此数目时, 更新会话密钥。

取值范围: 1...10000 默认设置: 1000

建议: 将 CP 的验证次数设置为主站验证次数的两倍。

- **密钥交换间隔**

CP 和主站之间再次交换密钥的时间间隔。通信伙伴双方的间隔必须匹配。

取值范围：0...65535 分钟。若输入

0（零），则绝不会更改密钥（禁用功能）。默认设置：15 分钟。

建议：将 CP 的密钥交换间隔设置为主站密钥交换间隔的两倍时长。

- **验证超时**

主站响应 CP 验证请求时的最长等待时间。

超出等待时间时，CP 将视之为错误。在这种情况下，CP 生成安全事件并将其发送至主站。

取值范围：1... 65535 s 默认设置：5

- **预共享密钥**

可以通过两种方式组态预共享密钥：

- 手动组态

在 STEP 7 中以十六进制值形式手动输入预共享密钥。

- 以文件形式导入

如果通过主站或另一个工程组态系统生成预共享密钥，则从工程师站的文件系统导入预共享密钥。

CP 与主站的预共享密钥必须相同。

4.9.4 防火墙

4.9.4.1 MAC 防火墙预检查消息。

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。

4.9.4.2 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。

4.9.4.3 已组态 VPN 隧道连接的防火墙设置

高级防火墙模式中的 IP 规则

如果在 CP 和通信伙伴之间通过 VPN 隧道建立组态连接，则需要调整 CP 的本地防火墙设置：

在高级防火墙模式（“安全 > 防火墙 > IP 规则”(Security > Firewall > IP rules)）下，为 VPN 隧道的两个通信方向选择“Allow*”操作。

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 78)

4.9.4.4 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：

1. 在全局安全设置（参见项目树）中，选择条目“防火墙 > 服务 > 为 IP 规则定义服务”(Firewall > Services > Define services for IP rules)。
2. 选择“ICMP”选项卡。
3. 插入一个类型为“回送应答”(Echo Reply) 和一个类型为“回送请求”(Echo Request) 的新条目。
4. 现在选择 S7 站中的 CP。
5. 在 CP 的本地安全设置中，在“Security > 防火墙”(Security > Firewall) 参数组中启用防火墙的高级模式。

6. 打开“IP 规则”(IP rules) 参数组。
7. 在表中, 按如下方式为之前已创建的全局服务插入新的 IP 规则:
 - 操作 (Action): 允许; 全局创建的“回送请求”(Echo request) 服务“从外部 -> 到站”(From external -> To station) 通信
 - 操作 (Action): 允许; 全局创建的“回送应答”服务“从站 -> 到外部”通信
8. 对于“回送请求”的 IP 规则, 在“源 IP 地址”(Source IP address) 中输入工程师站的 IP 地址。这可确保只有来自您的工程师站的 ICMP 帧 (ping) 可以通过防火墙。

4.9.5 电子邮件组态

在 STEP 7 中组态电子邮件

对于特殊事件, 例如, CPU STOP, CP 可以发送电子邮件形式。这与是否使用遥控通信无关。

当使用遥控通信时, 在 CPU

过程映像中额外组态的事件可以触发发送电子邮件。过程数据也可以随电子邮件发送。

在消息编辑器 (“消息”(Messages) 条目) 中, 可分别组态各个电子邮件, 请参见消息 (页 130) 部分。

要求

在发送电子邮件的组态中必须满足以下要求:

- 安全功能已启用。
- CP 的时间已同步。
- 在“电子邮件组态”(E-mail configuration) 条目中, 已组态访问电子邮件服务器要使用的协议和数据。

电子邮件组态

对于 SMTP 端口 25 的默认设置, 模块将传送未加密电子邮件。

如果您的电子邮件服务提供商仅支持加密传送，请使用以下选项之一：

- 端口号 587

通过使用 STARTTLS，模块会将加密电子邮件发送到您的电子邮件服务提供商的 SMTP 服务器。

建议：如果您的电子邮件服务提供商同时提供两种选项 (STARTTLS / SSL/TLS)，应使用 STARTTLS 及端口 587。

- 端口号 465

通过使用 SSL/TLS (SMTPS)，模块会将加密电子邮件发送到您的电子邮件服务提供商的 SMTP 服务器。

请向您的电子邮件服务提供商询问可以支持哪种选项。

导入加密传送所需的证书

为能够使用加密传送，您需要在 STEP 7 的证书管理器中加载电子邮件帐户的证书。该证书可从您的电子邮件服务提供商处获取。请执行以下步骤以使用证书：

1. 将电子邮件服务提供商提供的证书保存到工程师站的文件系统中。
2. 使用“全局安全设置 > 证书管理器”(Global security settings > Certificate manager) 将证书导入 STEP 7 项目中。
3. 通过本地“安全”(Security) 参数组中的“证书管理器”(Certificate manager) 表，将导入的证书用于每一个使用加密电子邮件的模块。

相关操作步骤，请参见处理证书 (页 82)部分

4.9.6 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。

4.9.7 SNMP

SNMP

有关 SNMP 的 CP 功能范围，请参见SNMP (页 146)部分。

如果启用了安全功能，则用户有以下选择和设置选项。

SNMP

- “启用 SNMP”(Enable SNMP)

如果启用该选项，则释放设备上通过 SNMP 进行的通信。默认情况下启用 SNMPv1。

如果禁用此选项，则不应答来自 SNMP 客户端的查询（无论是通过 SNMPv1 还是通过 SNMPv3）。

- “使用 SNMPv1”(Use SNMPv1)

启用对 CP 使用 SNMPv1。有关组态所需团体字符串的信息，请参见下文 (SNMPv1)。

- “使用 SNMPv3”(Use SNMPv3)

启用对 CP 使用 SNMPv3。有关组态所需算法的信息，请参见下文 (SNMPv3)。

SNMPv1

团体字符串需要与查询一起通过 SNMPv1 发送到 CP。

- “读取团体字符串”(Reading community string)

读访问需要该字符串。

请保留预设字符串"public"或组态新字符串。

- “允许写访问”(Allow write access)

如果启用该选项，则释放对 CP 的写访问，并且可以编辑相应的团体字符串。

- “写团体字符串”(Writing community string)

写访问需要该字符串，该字符串也可用于读访问。

请保留预设字符串"private"或组态新字符串。

注意对预设团体字符串使用小写字母！

SNMPv3

需要组态以下算法以通过 SNMPv3 对 CP 进行加密访问。

- “验证算法”(Authentication algorithm)

从下拉列表中选择要使用的验证方法。

- “加密算法”(Encryption algorithm)

从下拉列表中选择要使用的加密方法。

请注意 SCT 在线帮助以了解可能算法的安全信息。

用户管理

用户管理可在全局安全设置中找到，可在其中为各用户分配角色。

在角色的属性下，可以查看特定角色的权限列表，例如使用 SNMP 的各种访问类型。对于新角色，可以自由组态个人权限。

可在 STEP 7 的信息系统中找到有关用户、角色和密码策略的信息。

4.9.8 证书管理器

证书分配

如果对模块通信采用身份验证，例如采用 SSL/TLS

以实现安全传送电子邮件，则需要证书。您需要将非 Siemens 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模块：

1. 使用全局安全设置中的证书管理器导入通信伙伴的证书。
2. 然后在模块的本地安全设置下面的表中将导入的证书分配给模块。

有关操作步骤说明，请参见处理证书 (页 82)部分。

更多相关信息，请参见 STEP 7 信息系统。

4.9.9 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。

为了通过 SSL/TLS 安全传送电子邮件，需要为 CP 创建 SSL 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。“设备证书”(Device certificates) 表显示签发者、有效性、证书（服务/应用程序）使用和密钥使用情况。可以通过在表中选择证书并选择快捷菜单“显示”(Show) 来调用有关证书的更多信息。该表还显示 STEP 7 生成的所有其它证书和所有导入的证书。

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. 本地分配证书
 - ⇒ CP 的本地安全设置（“证书管理器”表）

这两个步骤分别在接下来的两部分中说明。

从通信伙伴导入第三方证书

使用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。

本地分配证书

要为 CP 使用导入的证书，需要在 CP 的“安全”(Security) 参数组中指定相应证书。请按照下面列出的步骤进行操作：

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。

只有此时才会将第三方证书用于 CP。

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“备用主题名”(Subject Alternative Name) 参数（Windows：“备用应用程序名称”）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。

4.9.10 VPN

4.9.10.1 VPN (Virtual Private Network)

VPN 隧道

Virtual Private Network (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，它会转发所有帧，甚至可以转发来自更高层级协议（HTTP，FTP 等）的帧。

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。这样便可通过相邻或中间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，其传输自己的帧，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。
- 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，单个设备或以太网网段均可受到保护：

- 允许访问安全模块保护的各个设备和网段。
- 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

4.9.10.2 为各站间的 S7 通信创建 VPN 通道

要求

要允许使用安全 **CP**（如 **CP 1628**）为两个 **S7** 站间的 **S7** 通信，或为 **S7** 站与工程师站间的 **S7** 通信创建 **VPN** 隧道，则必须满足以下要求：

- 已组态这两个站。
- 两个站中的 **CP** 必须都支持安全功能。
- 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
5. 组态两个 CP 的本地 VPN 属性

有关各步骤的详细说明，请参见本部分的以下段落。

创建安全用户

要创建 VPN

隧道，需要相应的组态权限。要激活安全功能，需要至少创建一个安全用户。

1. 在 CP 的本地安全设置中，单击“用户登录”(User logon) 按钮。

结果：打开一个新窗口。

2. 输入用户名、密码和密码确认。
3. 单击“登录”(Logon) 按钮。

已创建一个新的安全用户。现在，您可以使用安全功能。

对于所有其它登录，请以该用户身份登录。

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

登录后，需要在两个 CP 的组态中选中“激活安全特性”(Activate security features) 复选框。

这样，您就可以使用两个 CP 的安全功能。

创建 VPN 组并分配安全模块

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。

说明

CP 上 VPN 连接的当前日期和时间

通常，为建立 VPN

连接和能够相应识别待交换的证书，将需要获取连接双方工作站的当前日期和时间。

与工程师站建立 VPN 连接时，若该工程师站同时又是遥控服务器（装有 TCSB），则会按以下方式建立并伴随 CP 的时钟同步操作：

在工程师站（装有 TCSB）中，使用 CP 来建立 VPN 连接。即使该 CP 尚不具有当前时间，也将建立 VPN 连接。

若具有当前时间，所用的证书将评估为有效，从而可进行安全通信。

在连接建立后，CP 会与 PC

同步其时钟，因为遥控通信启用后，遥控服务器为时间主站。

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。

这些属性定义 VPN 组的默认设置，可以随时进行更改。

说明

指定 CP 的 VPN 属性

请在相关模块的参数组“Security > 防火墙 > VPN”(Security > Firewall > VPN) 中指定 CP 的 VPN 属性。

结果

您已创建 VPN 隧道。CP 的防火墙将自动激活：创建 VPN

组时，已默认选中“激活防火墙”(Activate firewall) 复选框。无法取消选择该复选框。

将组态下载到属于该 VPN 组的所有模块。

4.9.10.3 SOFTNET 安全客户端的 VPN 通信（工程师站）

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为各站间的 S7 通信创建 VPN 通道 (页 86)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。可以建立 VPN 隧道通信。

4.9.10.4 创建 VPN 连接遥控服务器

CP 与 TCSB 间 VPN 连接的组态

为了保证 VPN 隧道的通信安全，通信伙伴被分配到一个公共 VPN 组。不可直接组态 CP 与 TCSB 间的 VPN 连接，因为遥控服务器无法在 STEP 7 中进行组态。

要组态 CP 1243-1 与 TCSB 间基于 VPN 连接的通信，请遵循以下步骤：

- 创建一个 PC 站来代替遥控服务器。

该 PC 站的作用仅是临时代替遥控服务器来组态安全组，没有任何其它用途。

- 要设置安全功能，可选择以下方法：
 - 在遥控服务器的计算机上安装 CP 1628（安全模块），并将 CP 1243-1 和 CP 1628 分配至组态过程中的同一安全组。
 - 在遥控服务器的计算机上安装 SOFTNET Security Client（需要许可证），并在 STEP 7 项目中组态安全功能。

通过这两个选项，您都可以在 TCSB 端实现相应的连接需求，保证远程站的 CP 和遥控服务器之间能够通过安全 VPN 连接进行安全通信。

请按上述内容组态 CP 的安全功能。

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

按照对各个站的描述，在 CP 和 SCALANCE M 路由器之间建立 VPN 隧道。

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

如果未选中该复选框，CP 会拒绝建立隧道。

4.9.10.6 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”。

4.9.10.7 SYSLOG

仅对 1 个 VPN 连接使用 SYSLOG

如果要通过 VPN 连接使用级别 7 (debug) 的 SYSLOG，则这仅限于一个已建立的 VPN 连接。

4.9.11 TeleService 访问的组态

使用 TeleService 时的相关组态

为满足 CP 使用 TeleService 功能时的要求，您需要在 STEP 7 中针对以下各项进行必要设置。

CP 的“通信类型”(Communication types) 参数组

选择下列选项：

- 启用遥控通信
- 激活在线功能

CP 的“伙伴站”(Partner stations) 下的遥控服务器

可以在此处组态以下信息：

- 遥控服务器的地址
可由 DNS 解析的遥控服务器的 IP 地址或名称
- 端口
遥控服务器的端口号

全局安全设置中的用户和角色

1. 在项目树中打开以下页面：

“全局安全设置 > 用户管理”(Global security settings > User management)

2. 角色

打开“角色”(Roles) 选项卡

随即显示“角色”(Roles) 和“角色的权限”(Rights of the role) 这两个表格。

如果“角色视图”(Roles view) 被“角色的权限”(Rights of the role) 表格隐藏，则可根据需要打开该视图。

在“角色”(Roles) 表格中（位于顶部），为 **TeleService** 新建一个用户自定义的角色。

3. 在“用户”(User) 选项卡中，创建一个用户，允许其在以后执行 CP 的 **TeleService** 功能。

组态以下参数：

- 用户名

分配将具有 **TeleService** 权限的用户名。

在启动 **TeleService** 会话时需要该用户名。

- 验证方法

为该用户选择验证方法“密码”(Password)。

- 密码

分配密码。

在启动 **TeleService** 会话时需要该密码。

注：

安全功能的密码属性在“密码策略”(Password policies) 选项卡中指定。

启动 **TeleService** 会话时，需要在工程师站中输入该密码。

- 最长会话时间

此处组态的时间只有在访问 **SCALANCE S** 模块时需要。如果所创建的用户仅适用于 **TeleService** 会话，则可保留默认值不变。

4. 单击“角色”(Roles) 选项卡。

5. 在“模块权限”(Module rights) 组的下方列表“角色的权限”(Rights of the role) 中选择 CP。

6. 可用的权限将显示在“权限列表”(List of rights) 表格中。
显示“使用 TeleService”(Use TeleService) 权限。
7. 启用模块的“使用 TeleService”(Use TeleService) 权限。
8. 随后，在防火墙中将 S7 协议设为“允许”(allow)。

4.10 数据点

4.10.1 数据点组态

与 CPU 进行数据点相关通信

对于带数据点组态的遥控模块，要在站和通信伙伴之间传送用户数据，无需编程任何程序块。

CPU

存储器中用于与通信伙伴进行通信的数据区在模块上组态为数据点相关。每个数据点都链接到一个 PLC 变量或数据块变量。

要求：已创建 PLC 变量和/或数据块 (DB)

必须先在 CPU 程序中创建 PLC 变量或 DB，才允许组态数据点。

可以在标准变量表或用户自定义变量表中创建用于数据点组态的 PLC 变量。所有要用于数据点组态的 PLC 变量都必须具有属性“HMI 中可见”。

PLC 变量的地址区是 CPU 上的输入、输出或位存储器区。

说明

PLC 变量数

请记住组态限制和性能数据 (页 17)部分中可用于数据点组态的 PLC 变量的最大数目。

与模块协议特定的数据点类型兼容的 PLC 变量格式和 S7 数据类型，请参见数据点类型 (页 100)部分。

访问 CPU 的存储区

数据点引用的 PLC 变量或 DB 的值由模块读取并传送到通信伙伴。

从通信伙伴接收到的数据由模块通过 PLC 变量或 DB 写入 CPU。

在 STEP 7 中组态数据点和消息

在 STEP 7 中的数据点和消息编辑器中组态数据点。若要找到此内容，可使用项目树：

“项目 > 相关站的目录 > 本地模块 > CP”(Project > directory of the relevant station > Local modules > CP)

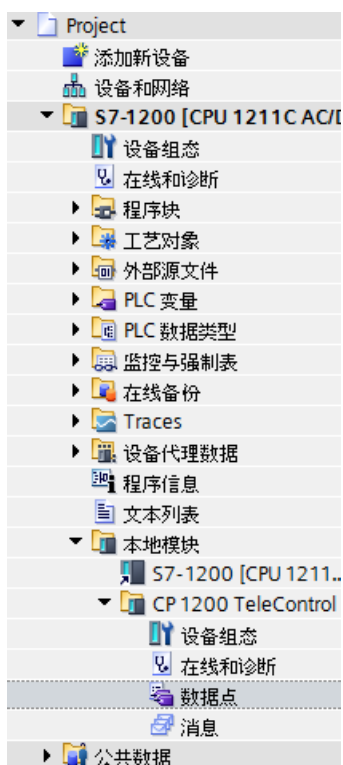


图 4-1 组态数据点和消息

通过双击条目、数据点或消息编辑器。

使用表格右上方的两个条目在数据点和消息编辑器之间进行切换。

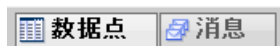


图 4-2 在两个编辑器之间切换

创建对象

在数据点或消息编辑器打开的状态下，通过双击带灰显条目的第一个表格行中的“<添加对象>”(<Add object>) 创建一个新对象。

单元中会写入预设名称。可根据需要更改该名称，但该名称在模块中必须唯一。

	名称	PLC 变量
1	DataPoint	"Tag_1-BI"
2	DataPoint_1	"Tag_2-BQ"
3	DataPoint_2	"Tag_1-BI"


图 4-3 数据点表格


通过使用其它表格列的下拉列表和屏幕底部显示的参数框组态每个对象的其余属性。

将数据点分配给其数据源

创建完成后，将新的数据点分配给其数据源。根据数据点的数据类型，PLC 变量可以作为数据源。

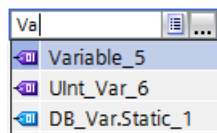
分配时，提供以下选项：

- 单击“PLC 变量”(PLC tag) 列单元中的表格符号 。

随即显示所有已组态的 PLC 变量和已创建数据块的变量。通过鼠标或键盘选择所需数据源。
- 单击符号 。

随即显示已组态的 PLC 变量和块的选择列表。从相关列表中选择所需数据源。
- 在 PLC 变量的名称框中，输入所需数据源名称的一部分。

随即显示名称中包含所输入字母的所有已组态 PLC 变量和数据块的变量。



选择所需数据源。

说明

为 PLC 变量分配参数值

此处所述的机制在需要将参数值分配给 PLC 变量时同样适用。PLC 变量的输入框（例如，伙伴状态的 PLC 变量支持此处所述用于选择 PLC 变量的功能。

排列和复制对象

与数据点或消息编辑器中的许多其它程序一样，您还可以根据需要排列列、对表格排序以及复制和插入对象。

- 排列列

如果用鼠标左键单击列标题，则可以移动该列。

- 排序对象

如果用鼠标左键短暂单击列标题，则可以根据该列中的条目对表格中的对象进行升序或降序排列。排序顺序由列标题中的箭头指示。

对列降序排列后，可以通过再次单击列标题对列进行反向排序。

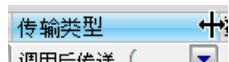
- 调整列宽

可使用以下操作实现此功能：

- 使用通过鼠标右键单击列标题时打开的快捷菜单。

“优化宽度”(Optimize width)， “优化所有列宽”(Optimize width of all columns)

- 如果将光标移动至列标题的边缘，将出现以下符号：



如果出现该符号，请立即单击列标题。列宽将根据本列中最宽的条目自行调整。

- 显示/隐藏列

用鼠标右键单击列标题，使用打开的快捷菜单调用该功能。

- 复制、粘贴、剪切和删除对象

如果用鼠标右键单击表格中某个对象的参数框，则可以使用以快捷菜单命名的功能（复制、粘贴、剪切、删除）。

可在表格中或表格下方第一个空行对对象进行粘贴、剪切或复制操作。

导出和导入数据点

要简化较大型工厂的工程，可以将已组态模块的数据点导出，然后将其导入项目中其它模块中。这点对于具备众多相同或相似站或数据点模块的项目来说特别有利。

例如，当在网络或设备视图中选择模块并选择相应快捷菜单时，导出/导入功能可用。



图 4-4 模块的快捷菜单

导出的模块数据点信息写入 CSV 文件中。

导出

当调用导出功能时，导出对话框打开。在其中选择需要导出数据点信息的项目的单个或多个模块。如有必要，可以一次性导出项目中所有模块的数据点。

在导出对话框中，可以在文件目录中选择存储位置。当导出模块数据时，还可以更改预设的文件名。

从多个模块导出时，文件由预设名称构成，预设名称由站名称和模块名称组成。

除了数据点信息之外，文件本身还包含有以下信息：

- 模块名称
- 模块类型
- CPU 名称
- CPU 类型

编辑数据点信息

可以在导出的 CSV

文件中编辑数据点信息。这样您便可将该文件用作许多其它站的组态模板。

如果项目中存在许多类型相同的站，可以为其它尚未组态的站点复制包含已完全组态模块的数据点的 CSV 文件，然后修改特定站点的各个参数。这样便不必在 STEP 7

中为每个模块组态数据点。只需将复制和修改的 CSV

文件导入其它相同类型的模块中。将该文件导入另一个模块时，CSV

文件的已修改参数值将被应用到该模块的数据点组态中。

CSV 文件的行包含以下内容：

- 行 1: ,Name,Type,
不能修改此行。
- 行 2: PLC,<CPU 名称>、<CPU 类型>
含义：PLC（站类别名称）、CPU 名称、CPU 类型
只能修改 <CPU 名称> 和 <CPU 类型> 元素。
CPU 类型必须完全对应于目录中 CPU 的名称。
- 行 3: Module,<模块名称>、<模块类型>
含义：Module（模块类别名称）、模块类型、模块名称
只能修改 <模块名称> 和 <模块类型> 元素。
如果要将在数据点导入多个模块，则修改模块名称时需要注意（见下文）。
模块类型必须完全对应于目录中模块的名称。
- 行 4: 数据点的参数名称（英语）
不能修改此行。
- 行 5..n: 对应于行 4 中各个数据点的参数值
您可以为特定站更改这些参数值。

导入模块中

导入数据点前，请确保已创建数据点所需的 PLC 变量。

注意，当导入 CSV

文件时，模块中存在的所有数据点都将被删除，并替换为导入的数据点。

选择一个模块，然后从该模块的快捷菜单中选择导入功能。导入对话框随即打开，可在其中选择文件目录下的所需 CSV 文件。

如果各个数据点到相关 PLC

变量的分配信息与原始模块中的分配相匹配，则会将数据点分配给相应的 PLC 变量。

当您想要向模块中导入数据点，但某些必需的 PLC 变量尚未在 CPU 中创建时，将无法分配相应的数据点信息。在这种情况下，您可以稍后创建缺失的 PLC 变量并为其分配导入的数据点信息。为此，可以使用“分配修复”功能（见下文）。

如果导入的模块中和所导出模块中的 PLC

变量名称不同，则无法将相应的数据点分配给您的 PLC 变量。

导入到多个模块

您可以将多个模块中的数据点导入到不同项目的模块中。为此，在导入对话框中选择所有带控制密钥的所需 CSV 文件。

导入数据点前，请确保已相应创建带有同名 CPU、同名模块和同名 PLC 变量的站。

导入项目的对应站时，将基于 CSV

文件中的模块名称搜索这些站。如果项目中不存在目标站或模块的名称不同，将忽略特定 CSV 文件的导入。

数据点导入的限制

在以下情况下将中止导入数据点：

- 待导入的 CSV 文件中模块所需的属性缺失。

示例：如果待导入的数据点使用时间触发，则在没有为模块组态时钟同步时将中止导入。

- 模块使用的遥控协议和初始模块使用的协议不同。

仅在导入到多个模块时：

- 当模块或 CPU 的名称与 CSV 文件中的数据不同时，将中止导入操作。

注意：

使用相同协议的模块互相兼容：

- TeleControl Basic

使用 TeleControl Basic 协议的所有 SIMATIC NET 模块：

CP 1243-1, CP 1242-7 GPRS V2, CP 1243-7 LTE, CP 1542SP-1 IRC

- ST7

CP 1243-8 IRC, 具有 ST7 功能的 TIM 模块

- DNP3

CP 1243-1, CP 1243-8 IRC, 具有 DNP3 功能的 TIM 模块


- IEC

CP 1243-1, CP 1243-8 IRC

可在兼容模块之间导入和导出数据点。

分配修复

如果您期望在不同于导出 CSV 文件的某个站中进行导入操作，并且已对该站中的 PLC 进行命名，则导入过程中数据点和 PLC 变量之间的分配将丢失。

此时，可以选择适当地为现有 PLC 变量进行重命名，或者也可以选择添加缺失的 PLC 变量。之后，可以修复未分配的数据点和 PLC 变量之间的分配。该功能既可以通过模块的快捷菜单（见上文）调用，也可以通过数据点编辑器左上角的如下图标调用：。

如果通过修复功能找到了名称与数据点匹配的 PLC 变量，则分配将恢复。但不会检查变量的数据类型。

对分配进行修复后，务必检查新分配的 PLC 变量是否正确。

4.10.2 数据点名称的语法

数据点名称的字符集

创建数据点时，采用预设名称“DataPoint_n”。可以在数据点表格和数据点的“常规”(General) 选项卡中更改数据点名称。

分配名称时，可能仅使用范围在 0x20 ... 0x7e（编号 32-126）的 ASCII 字符，例外情况在下文列出。

禁用的字符：

- .'[]/\|
句号、省略号、方括号、斜线、反斜线、竖线 (pipe)

4.10.3 数据点类型

将从 CPU 传送的用户数据（通过 CP 上的 CPU 的 PLC 变量引用）组态为数据点。

针对各种遥控协议，CP 支持的数据点类型及可兼容的 S7 数据类型均在下文列出。

方向与传送方向：

- “in”：监视方向：
- “out”：控制方向

说明

修复数据点的数组后的影响

如果之后修改数组，必须重新创建数据点。

“TeleControl Basic”协议的数据点类型

表格 4-1 支持的数据点类型和兼容的 S7 数据类型

格式（存储要求）	数据点类型	方向	S7 数据类型	操作数区域
位	数字量输入	in	Bool	I, Q, M, DB
	数字量输出	in	Bool	Q, M, DB
字节	数字量输入	in	Byte, Char, USInt	I, Q, M, DB
	数字量输出	out	Byte, Char, USInt	Q, M, DB
有符号整数（16 位）	模拟量输入	in	Int	I, Q, M, DB
	模拟量输出	out	Int	Q, M, DB
计数器（16 位）	计数器输入	in	Word, UInt	I, Q, M, DB
有符号整数（32 位）	模拟量输入	in	DInt	Q, M, DB
	模拟量输出	out	DInt	Q, M, DB
计数器（32 位）	计数器输入	in	UDInt, DWord	I, Q, M, DB
有符号浮点数（32 位）	模拟量输入	in	Real	Q, M, DB
	模拟量输出	out	Real	Q, M, DB
有符号浮点数（64 位）	模拟量输入	out	LReal	Q, M, DB
	模拟量输出	out	LReal	Q, M, DB
数据块（1 .. 64 字节）	数据	in / out	ARRAY ¹⁾	DB
	数据	in / out	ARRAY ¹⁾	DB

¹⁾ 有关 ARRAY 数据类型的可能格式，请参见以下部分。

数据块 (ARRAY)

使用 ARRAY 数据类型，最多可以传送 64 字节的连续存储区。ARRAY 兼容以下 S7 数据类型：

- Byte, UInt (每个数据块最多总共 64 个)
- Char (每个数据块最多总共 64 个) - 固件版本 2.1.77 及以上的 CP
- Int, UInt, Word (每个数据块最多总共 32 个)
- DInt, UDInt, DWord (每个数据块最多总共 16 个)

如果之后修改数组，必须重新创建数据点。

时间戳的格式

时间戳由 OPC 服务器应用程序以 UTC 格式 (48 位) 输出，其中包含毫秒数。

“DNP3”协议的数据点类型

表格 4-2 支持的数据点类型、DNP3 对象组、变型和兼容的 S7 数据类型

格式 (存储要求)	数据点类型 CP [数据点类型 TIM]	DNP3 数据组 [variations]	方向	S7 数据类型	操作数区域
位	Binary Input	1 [1, 2]	in	Bool	I, Q, M, DB
	Binary Input Event	2 [1, 2]	in	Bool	I, Q, M, DB
	Binary Output ¹⁾	10 [2]	out	Bool	Q, M, DB
	Binary Output Event ¹⁾	11 [1, 2]	out	Bool	Q, M, DB
	Binary Command	12 [1]	out	Bool	Q, M, DB
16 位整型	Counter Static	20 [2]	in	UInt, Word	I, Q, M, DB
	Frozen Counter ²⁾	21 [2, 6]	in	UInt, Word	I, Q, M, DB
	Counter Event	22 [2, 6]	in	UInt, Word	I, Q, M, DB
	Frozen Counter Event ³⁾	23 [2, 6]	in	UInt, Word	I, Q, M, DB
	Analog Input	30 [2]	in	Int	I, Q, M, DB
	Analog Input Event	32 [2]	in	Int	I, Q, M, DB
	Analog Output Status ⁴⁾	40 [2]	out	Int	Q, M, DB

格式（存储要求）	数据点类型 CP [数据点类型 TIM]	DNP3 数据组 [variations]	方向	S7 数据类型	操作数区域
	Analog Output	41 [2]	out	Int	Q, M, DB
	Analog Output Event ⁴⁾	42 [2, 4]	out	Int	Q, M, DB
32 位整型	Counter Static	20 [1]	in	DWord	I, Q, M, DB
	Frozen Counter ²⁾	21 [1, 5]	in	DWord	I, Q, M, DB
	Counter Event	22 [1, 5]	in	DWord	I, Q, M, DB
	Frozen Counter Event ³⁾	23 [1, 5]	in	DWord	I, Q, M, DB
	Analog Input	30 [1]	in	DInt	Q, M, DB
	Analog Input Event	32 [1]	in	DInt	Q, M, DB
	Analog Output Status ⁴⁾	40 [1, 3]	out	DInt	Q, M, DB
	Analog Output	41 [1]	out	DInt	Q, M, DB
	Analog Output Event ⁴⁾	42 [1]	out	DInt	Q, M, DB
浮点数（32 位）	Analog Input	30 [5]	in	Real	Q, M, DB
	Analog Input Event	32 [5, 7]	in	Real	Q, M, DB
	Analog Output Status ⁴⁾	40 [3]	out	Real	Q, M, DB
	Analog Output	41 [3]	out	Real	Q, M, DB
	Analog Output Event ⁴⁾	42 [5, 7]	out	Real	Q, M, DB
浮点数（64 位）	Analog Input	30 [6]	in	LReal	Q, M, DB
	Analog Input Event	32 [6, 8]	in	LReal	Q, M, DB
	Analog Output	41 [4]	out	LReal	Q, M, DB
	Analog Output Event ⁴⁾	42 [6, 8]	out	LReal	Q, M, DB

格式 (存储要求)	数据点类型 CP [数据点类型 TIM]	DNP3 数据组 [variations]	方向	S7 数据类型	操作数区域
数据块 (1...64 字节) ⁵⁾	Octet String / Oc- tet String Output	110 [-]	in, out	⁵⁾	DB
	Octet String Event ⁵⁾	111 [-]	in, out	⁵⁾	DB

1) 此对象组可以使用替换对象组 12 在 STEP 7 的数据点编辑器中组态。

2) 此对象组可以使用替换对象组 20 在 STEP 7 的数据点编辑器中组态。

3) 此对象组可以使用替换对象组 22 在 STEP 7 的数据点编辑器中组态。

4) 此对象组可以使用替换对象组 41 在 STEP 7 的数据点编辑器中组态。

5) 使用这些数据点类型，最多可以传送 64 字节的连续存储区。所有大小在 1 到 64 字节的 S7 数据类型都可兼容。

(表格脚注^{1), 2), 3), 4)} 的替换对象组

可使用上述替换对象组来组态以下对象组的初始数据点类型：

- 10 [2]
- 11 [1, 2]
- 21 [1, 2, 5, 6]
- 23 [1, 2, 5, 6]
- 40 [1, 2, 3]
- 42 [1, 2, 4, 5, 6, 7, 8]

若要组态 DNP3 CP，应使用指定的替换对象组。

在 STEP 7 中可使用可组态的数据点索引分配主站上的各个数据点。DNP3 CP 的数据点随即会分配给主站上的相应数据点。

组态数据点 Binary Output (10 [2]) 的示例

数据点将进行以下组态：

在 DNP3 CP 上组态为 Binary Command (12 [1])

在主站上组态为 Binary Output (10 [2])

对于数据点类型二进制输出事件 (11) 和模拟量输出事件 (42)，还需要启用镜像；请参见下一部分。

输出事件（对象组 11 和 42）的反向镜像组态

首先，按上文所述创建类型为二进制输出事件（对象组 11）和模拟量输出事件（对象组 42）的数据点作为对象组 12 或 41 的数据点。

可监视这两个对象组的本地值的变化情况，并将变化情况传送至主站（）。本地值改变的原因有多种，例如操作员现场手动输入会导致本地值改变。

为使来源于本地事件或干预的值传送至主站，需要为相关数据点提供进行反向镜像的通道。在“常规”(General) 选项卡中，使用数据点组态中的“值监视”(Value monitoring) 选项组态该反向镜像功能。

请记住，在使用反向镜像功能时，需要将控制器中的本地值和数据点的相关 PLC 变量互连。

时间戳的格式

时间戳以 UTC 格式（48 位）传送，其中包含毫秒数。

“IEC”协议的数据点类型

表格 4-3 支持的数据点类型、IEC 类型和兼容的 S7 数据类型

格式（存储要求）	数据点类型	IEC 类型	方向	S7 数据类型	操作数区域
位	Single-point information	<1>	in	Bool	I, Q, M, DB
	Single-point information with time tag CP56Time2a ¹⁾	<30>	in	Bool	I, Q, M, DB
	Single command	<45>	out	Bool	Q, M, DB
	Single command with time tag CP56Time2a ¹⁾	<58>	out	Bool	Q, M, DB
	Double command with time tag CP56Time2a ¹⁾	<59>	out	Bool	Q, M, DB
字节	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag CP56Time2a ¹⁾	<32>	in	Byte, USInt	I, Q, M, DB
	Regulating step command with time tag CP56Time2a ¹⁾	<60>	out	Byte, USInt	Q, M, DB

格式（存储要求）	数据点类型	IEC 类型	方向	S7 数据类型	操作数区域
16 位整型	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag CP56Time2a ¹⁾	<34>	in	Int	I, Q, M, DB
	Measured value, scaled value	<11>	in	Int	I, Q, M, DB
	Measured value, scaled value with time tag CP56Time2a ¹⁾	<35>	in	Int	I, Q, M, DB
	Set point command, normalised value	<48>	out	Int	Q, M, DB
	Set point command, scaled value	<49>	out	Int	Q, M, DB
	Set point command, normalised value with time tag CP56Time2a ¹⁾	<61>	out	Int	Q, M, DB
	Set point command, scaled value with time tag CP56Time2a ¹⁾	<62>	out	Int	Q, M, DB
32 位整型	Bitstring of 32 bits	<7>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a ¹⁾	<33>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals	<15>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals with time tag CP56Time2a ¹⁾	<37>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits	<51>	out	UDInt, DWord	Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a ¹⁾	<64>	out	UDInt, DWord	Q, M, DB
浮点数（32 位）	Measured value, short floating point number	<13>	in	Real	Q, M, DB

格式（存储要求）	数据点类型	IEC 类型	方向	S7 数据类型	操作数区域
	Measured value, short floating point number with time tag CP56Time2a ¹⁾	<36>	in	Real	Q, M, DB
	Set point command, short floating point number	<50>	out	Real	Q, M, DB
	Set point command, short floating point with time tag CP56Time2a ¹⁾	<63>	out	Real	Q, M, DB
数据块 (1...2 Bit) ²⁾	Double-point information	<3>	in	²⁾	DB
	Double-point information with time tag CP56Time2a ¹⁾	<31>	in	²⁾	DB
	Double command	<46>	out	²⁾	DB
	Regulating step command	<47>	out	²⁾	DB
	Double command with time tag CP56Time2a ¹⁾	<59>	out	²⁾	DB
	Regulating step command with time tag CP56Time2a ¹⁾	<60>	out	²⁾	DB
数据块 (1...32 Bit) ³⁾	Bitstring of 32 bits ³⁾	<7>	in	³⁾	DB
	Bitstring of 32 bits with time tag CP56Time2a ^{1) 3)}	<33>	in	³⁾	DB
	Bitstring of 32 bits ³⁾	<51>	out	³⁾	DB
	Bitstring of 32 bits with time tag CP56Time2a ^{1) 3)}	<64>	out	³⁾	DB

1) 关于时间戳的格式，请参见后续部分。

2) 对于这些数据点类型，创建的数据块中包含具有 2 个布尔型值的数组。

3) 使用这些数据点类型，最多可以传送 32 位的连续存储区。仅兼容 S7 布尔数据类型。

时间戳的格式

时间戳会根据 IEC

规范，以“CP56Time2a”格式进行传送。请注意，只会传送帧中表示毫秒和分钟的前 3 个字节。

4.10.4 组态数据点索引

组态数据点索引

以下所述是为组态数据点索引的规则。

使用 TeleControl Basic 协议的数据点索引

在 CP 中，数据点类别的索引必须符合以下规则：

- 输入

所有数据点类型（数字量输入、模拟量输入等）中输入数据点的索引必须唯一。

- 输出

所有数据点类型（数字量输入、模拟量输入等）中输出数据点的索引必须唯一。

说明

站间通信的数据点索引

请注意，对于与另一个 S7 站的 CP 之间的站间通信，发送和接收 CP 的两个相应数据点（数据点对）的索引必须相同。

有关组态的信息，请参见具有 TeleControl Basic 数据点的伙伴组态。（页 129）部分。

使用 DNP3 协议的数据点索引

在 CP 上，以下每个对象组中的数据点索引都必须唯一：

- Binary Input / Binary Input Event
- Binary Output / Binary Command
- Counter / Counter Event
- Analog Input / Analog Input Event
- Analog Output
- Octet String / Octet String Event

不同对象组中的两个数据点的索引可以相同。

使用 IEC 协议的数据点索引

CP 中的数据点索引必须唯一。

如果数据点索引分配两次，则在一致性检查中会指示错误并会阻止保存项目。

4.10.5 数据点的状态 ID

状态标识符

下表中的列出的数据点的状态标识符将随各帧中的值一同传送到通信伙伴。通信伙伴可对它们进行评估。

“意义”表格行中的条目与“位状态”表格行中的条目相对应。

在数据点状态变化时生成事件

对于组态为事件的数据点，下述状态标识符的状态位如发生更改，则也会导致事件生成。

例如：站启动时，如果以事件方式组态的数据点的“RESTART”状态值从 1（值还没有更新）更改为 0（值已更新），将引起事件生成。

使用 TeleControl Basic 协议的状态标识

根据其状态，状态位（见下表）由 TCSB 转换为 OPC 质量代码。

- Quality = BAD
位 2 或 7 = 1
- Quality = UNCERTAIN
位 1、3 或 5 = 1
- Quality = GOOD
位 1、2、3、5 和 6 = 0

4.10 数据点

表格 4-4 状态字节 0 的位分配

位	7	6	5	4	3	2	1	0
标记名称	-	NON_ EXISTEN T	Substitute d	LOCAL_ FORCED	CARRY	OVER_ RANGE	RESTART	ONLINE
含义	-	数据点不存在或 S7 地址不可访问	替换值	本地操作员控制	在读取值之前计数值上溢	模拟预处理过冲/下冲的限值	启动后尚未更新值	值有效
位状态	(始终为 0)	1	1	1	1	1	1	1

使用 DNP3 协议的状态标识符

状态 ID 对应于以下规范中的以下元素：

OBJECT FLAGS - DNP3 Specification, Volume 6, Data Object Library - Part 1

表格 4-5 状态字节的位分配

位	7	6	5	4	3	2	1	0
标记名称	-	-	-	LOCAL_ FORCED	DISCONTI NUITY	OVER_ RANGE	RESTART	ONLINE
含义	-	-	-	本地操作员控制	在读取值之前计数值上溢	模拟预处理过冲/下冲的限值	启动后尚未更新值	值有效
位状态	(始终为 0)	(始终为 0)	(始终为 0)	1	1	1	1	1

使用 IEC 协议的状态标识符

状态 ID 对应于以下规范中的以下元素：

Quality descriptor - IEC 60870 Part 5-101

表格 4-6 状态字节的位分配

位	7	6	5	4	3	2	1	0
标记名称	-	-	SB substituted	-	CY carry	OV overflow	NT not topical	IV invalid
含义	-	-	替换值	-	在读取值之前计数值上溢	超出值范围，模拟值	值未更新	值有效
位状态	(始终为0)	(始终为0)	1	(始终为0)	1	1	1	0

4.10.6 读取周期

数据点的优先级

通过 CPU 上已分配的 PLC

变量来周期性读取输入数据点的值时，可按优先级顺序进行。

无需在每个 CPU

扫描周期中都读取次要输入数据点。而对于重要的输入数据点，可在每个 CPU 扫描周期中按优先级进行更新。

可以在 STEP 7 数据点组态的“常规”(General) 选项卡中，通过“读取周期”(Read cycle) 参数指定数据点的优先级。其中存在以下两个输入数据点选项：

- “快速周期”(Fast cycle)
- “正常周期”(Normal cycle)

可以按照下述方法读取数据点。

CPU 扫描周期的结构

CP 扫描 CPU 存储区所遵循的周期（包括暂停）由以下阶段组成：

- **高优先级读取作业**

扫描优先级为“高优先级”的输入数据点值在每个扫描周期中均会被读取。

- **低优先级读取作业**

某些扫描优先级为“低优先级”的输入数据点值会在每个扫描周期中被读取。

CP 每个周期读取的值的数目会通过“与 CPU 通信”(Communication with the CPU) 参数组中的“读取作业最大数量”(Max. number of read jobs)

参数来指定。超过该值而无法在一个周期中读取的值将在下一周期或后续周期之一中读取。

- **写入作业**

每个周期都会将一定数量的主动写入作业的值写入到 CPU 中。CP 每个周期写入的值的数目会通过“与 CPU 通信”(Communication with the CPU) 参数组中的“写入作业最大数量”(Max. number of write jobs) 参数来指定。数量超出此值的值将在下一周期或后续某一周期中写入。

- **周期暂停时间**

这是两个扫描周期之间的等待时间。用于为其它通过站背板总线访问 CPU 的过程预留足够的时间。

4.10.7 过程映像、传输类型、事件类别、触发

保存数据点值

数据点的值存储在 CP 的映像存储器中，仅在通信伙伴查询时才传送。

事件还存储在帧存储器（发送缓冲区）中并可以主动传送。

使用“传输类型”(Type of transmission) 参数将数据点组态为静态值或事件（参见下文）：

- **调用后传送：无事件/静态值**

静态值输入到映像存储器中（CP 的过程映像）。

- **触发：事件**

组态为事件的数据点值也输入到 CP 的映像存储区中。

事件的值也输入到 CP 的发送缓冲区中。

如果具有 DNP3

功能，则当主站启用了主动发送功能后，事件的值将主动发送给通信伙伴。

映像存储器，CP 的过程映像

映像存储器是 CP

的过程映像。所有组态数据点的最新值存储在映像存储器中。数据点的新值会覆盖映像存储器中上一次存储的值。

在查询通信伙伴后发送该值，请参见下面“传输类型”部分的“调用后传送”。

发送缓冲区（帧存储器）

CP

的发送缓冲区用作组态为事件的各数据点值的存储器。有关发送缓冲区的最大大小，请参见组态限制和性能数据 (页 17)部分。

组态的事件数将均分给所有已组态和启用的通信伙伴。有关组态的信息，请参见SNMP (页 61)部分中的“帧存储器大小”(Frame memory size) 参数。

如果与通信伙伴的连接中断，则事件的各个值会存储在 CP 的 RAM

中。在连接恢复后会发送缓冲的值。帧存储器按时间顺序运行；也就是说，首选发送最早的帧（FIFO 原则）。

将帧传送给通信伙伴后，已传送的值将从缓冲区中删除。

如果在较长时间内都无法传送帧，且发送缓冲区将要溢出，则响应如下：

采用 TeleControl Basic 的强制映像模式

如果发送缓冲区充满到 80%，则 CP

将切换到强制映像模式。事件的新值将不再添加到发送缓冲区，而是会覆盖映像存储器中现有的旧值。

当恢复通信伙伴的连接后，一旦发送缓冲区的填充比例已降至 50% 以下，CP 就会切换回发送缓冲区模式。

传输类型/事件类别

可以使用下列传输类型：

- **调用后传送**

数据点的当前值输入到 CP 的映像存储区中。数据点的新值会覆盖映像存储器中上一次存储的值。通信伙伴进行调用后，将传输当前值。

- **触发（事件）**

组态为事件的数据点的值输入到 CP 的映像存储器和发送缓冲区中。

在下列情况下，将保存事件的值：

- 当满足组态的触发条件时（数据点组态 >“触发器”(Trigger) 选项卡，参见下文）
- 数据点状态标识符的状态位的值发生变化时，另请参见数据点的状态 ID (页 109)部分。

例如：当组态为事件的数据点的值在启动站的过程中通过首次读取 CPU 数据进行更新时，此数据点的状态“RESTART”将发生变化（位状态从 1 变为 0）。这将导致事件的生成。

使用“传输类型”(Type of transmission)

参数将数据点组态为事件时，可选用以下事件类别：

- **触发每个值**

按时间顺序将各值变化输入到发送缓冲区中。

- **触发当前值**

只有最新的当前值才会输入到发送缓冲区中。该值会覆盖此处以前保存的值。

触发器

触发类型

对于事件驱动的传送，存在多种触发类型：

- **阈值触发**

在达到某一阈值时传送数据点的值。通过比较当前值与上一次存储的值之差来计算阈值，请参见阈值触发 (页 117) 部分。

- **时间触发**

按组态的时间间隔或指定的时间传送数据点的值。

- **事件触发**

在可组态的触发信号激活时传送数据点的值。对于触发信号，将评估触发位的沿变化 (0 → 1)，通过用户程序将触发位置位。必要时，可以为每个数据点组态一个触发位。

复位位存储区/DB 中的触发变量：

如果触发变量的存储区在位存储器或数据块中，则传送数据点值时，触发变量将复位为零。

帧的传输时间（传输模式）

数据点的值是在触发后立即传送到通信伙伴还是在延迟后传送到通信伙伴取决于数据点的“触发”(Trigger) 选项卡中参数“传输模式”(Transmission mode) 的设置：

- **自发**

立即传送值。

- **有条件自发**

只有满足以下两个条件之一时才传送值：

- 遥控服务器查询站。
- 传送传输模式为“主动”(Unsolicited) 的另一个事件的值。

4.10.8 “触发”(Trigger) 选项卡

触发

使用“传输类型”(Type of transmission) 参数将数据点组态为静态值或事件：

保存组态为事件的数据点的值

将组态为事件的数据点的值保存到发送缓冲区（消息存储器）的操作可以由多个触发类型进行触发：

- **阈值触发**

在数据点的值达到某一阈值时保存数据点的值。通过比较当前值与上一次存储的值得之差来计算阈值，请参见阈值触发 (页 117)部分。

- **时间触发**

按组态的时间间隔或指定的时间保存数据点的值。

- **事件触发（触发变量）**

在可组态的触发信号激活时保存数据点的值。对于触发信号，将评估触发变量的沿变化 (0 → 1)，通过用户程序将触发位置位。必要时，可以为每个数据点组态一个触发变量。

复位位存储区/DB 中的触发变量：

如果触发变量的存储区位于位存储区或数据块中，则传送数据点的值时，CP 会将触发变量本身重置为 0（零）。这一过程最多需要 500 毫秒的时间。

说明

触发的快速设置

不得将触发设置为快于 500 毫秒的最小间隔。这同样适用于硬件触发器（输入区域）。

说明

硬件触发器

需要通过用户程序重置硬件触发器

传输组态为事件的数据点的值

在“传输模式”(Transmission mode)

参数中指定数据点的值是在触发后立即传送到通信伙伴还是在延迟后传送到通信伙伴。

传输模式

帧的传输模式可在数据点的“触发器”(Trigger)

选项卡中进行设置。可以通过该选项指定是立即发送事件消息还是延迟发送事件消息：

- 立即传送 - 自发

立即传送值。

- 缓冲传输 - 有条件自发

只有满足以下任一条件时才传送值：

- 通信伙伴查询站。
- 传送传输模式为“自发”(Spontaneous) 的另一个事件的值。

4.10.9 阈值触发

说明

阈值触发：仅在“模拟值预处理”之后进行计算

注意，在检查和计算已组态的阈值之前执行模拟值预处理。

这会影响到阈值触发组态的值。

说明

组态了生成平均值功能时不支持阈值触发

如果组态了生成平均值功能，则无法为所涉及的模拟值事件组态阈值触发。

关于模拟值预处理的时间顺序，请参见模拟值预处理 (页 119)部分。

阈值触发

功能

如果过程值与阈值偏离，则保存该过程值。

可使用以下两种方法计算阈值偏差：

- **绝对方法**

对于已组态生成平均值的二进制和计数器值以及模拟值，可使用绝对方法计算阈值偏差。

- **集成方法**

对于未组态生成平均值的模拟值，可使用集成方法计算阈值偏差。

在进行集成阈值计算时，不是计算当前过程值与上次存储值的绝对偏差，而是计算集成偏差。

绝对方法

对于各个二进制值，需进行检查以确定当前（可能已经过滤波）值是否超出阈值范围。当前阈值范围由最后一次保存的值和所组态的阈值数量确定：

- 阈值范围上限：最后一次保存的值 + 阈值
- 阈值范围下限：最后一次保存的值 - 阈值

过程值达到阈值范围的上限或下限后，将立即保存该值。新保存的值将作为计算新阈值范围的基础。

集成方法

集成阈值计算通过周期性比较集成的当前值与上次存储的值来实现。对两个值进行比较的计算周期为 500 毫秒。

（注意：不可将计算周期与 CPU 存储区的扫描周期相混淆）。

在每个计算周期中求取当前过程值的偏差总和。仅当合计的值达到组态的阈值触发值时，才进行触发并在发送缓冲区中输入新过程值。

我们以下面的示例来说明该方法，其中组态的阈值为 2.0。

表格 4-7 组态为 2.0 的阈值的集成计算示例

时间 [s] (计算周期)	存储在发送缓冲区中的过程值	当前过程值	与存储值的绝对偏差	集成偏差
0	20.0	20.0	0	0
0.5		20.3	+0.3	0.3
1.0		19.8	-0.2	0.1
1.5		20.2	+0.2	0.3

时间 [s] (计算周期)	存储在发送缓冲区中的过程值	当前过程值	与存储值的绝对偏差	集成偏差
2.0		20.5	+0.5	0.8
2.5		20.3	+0.3	1.1
3.0		20.4	+0.4	1.5
3.5	20.5	20.5	+0.5	2.0
4.0		20.4	-0.1	-0.1
4.5		20.1	-0.4	-0.5
5.0		19.9	-0.6	-1.1
5.5		20.1	-0.4	-1.5
6.0	19.9	19.9	-0.6	-2.1

按示例所示的过程值变化，组态为 2.0 的阈值触发激活两次：

- 在 3.5 s 时刻：集成偏差值为 2.0。存储在发送缓冲区的新过程值为 20.5。
- 在 6.0 s 时刻：集成偏差值为 2.1。存储在发送缓冲区的新过程值为 19.9。

本例中，如果约为 0.5

的过程值偏差应激活触发，则根据此处所示的过程值特性，需要组态一个约为 1.5 ...2.5 的阈值。

4.10.10 模拟值预处理

带数据点组态的 CP

支持模拟值预处理。对于模拟值数据点，可以组态下面介绍的部分或全部功能。

要求和限制

有关组态预处理选项的要求和相关限制，请参见与特定功能相关的部分。

说明

因组态触发器引起的限制

如果未为相关数据点组态阈值触发，将不能执行模拟值预处理选项“故障抑制时间”(Fault suppression time)、“限值计算”(Limit value calculation)和“滤波”(smoothing)。在这种情况下，读取的数据点的过程值将在阈值计算的预处理周期(500 ms) 结束前输入到 CP 的映像存储区中。

模拟值预处理选项的顺序

组态为事件的模拟量输入的值在 CPU 上按以下流程处理：

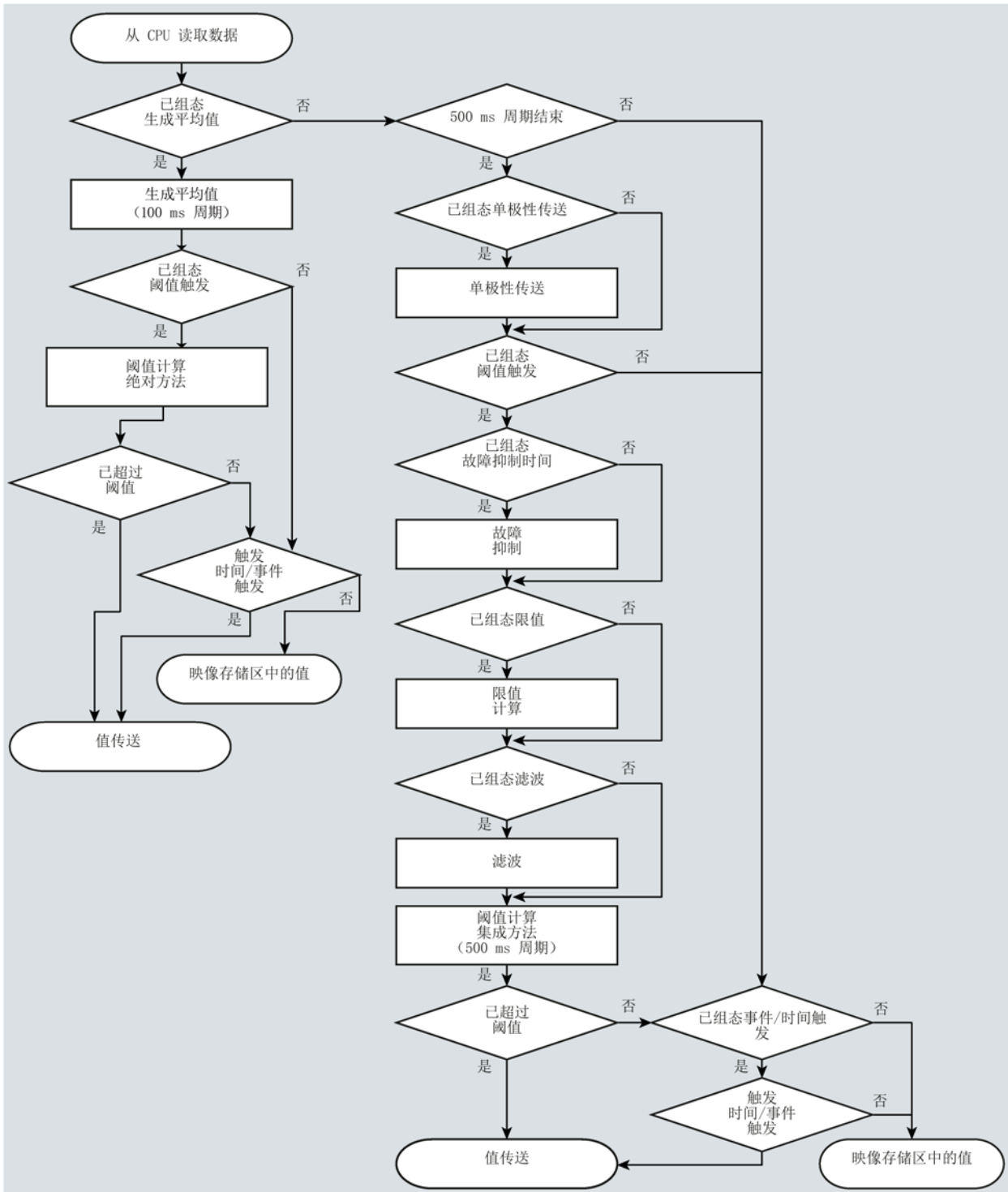


图 4-5 模拟值预处理的顺序

500

毫秒的周期由集成阈值计算启动。在此周期中，即使启用以下预处理选项时，也会保存这些值：

- “单极性传送”(Unipolar transfer)
- “故障抑制时间”(Fault suppression time)
- “限值计算”(Limit value calculation)
- “滤波”(Smoothing)

生成平均值

说明

组态了生成平均值功能时的预处理选项限制

如果为模拟值事件组态了生成平均值功能，则会有以下预处理选项不可用：

- 单极性传送
- 故障抑制时间
- 滤波

功能

通过该参数，将采集到的模拟值作为平均值进行传送。

如果生成平均值功能已激活，将对组态时间触发发挥作用。

将在 100

毫秒的周期内读取模拟数据点的当前值并进行求和。每个时间单位读取的值的数量取决于 CP 的 CPU 读取周期和 CPU 扫描周期。

只要触发器触发传送，就根据累加值计算出平均值。然后，再次开始累加，以便计算下一个平均值。

如果模拟值消息传输是由通信伙伴的请求触发的，则也可以计算平均值。此时平均值计算的持续时间为从上次传输（例如，由触发器触发）开始至请求发出时。同样，累加再一次重新开始，以便计算下一个平均值。

输入模块：上溢范围/下溢范围

若采集的值处于上溢或下溢范围内，则将立即停止生成平均值。当前平均值计算周期中将 32767 / 7FFF_h 或 -32768 / 8000_h 值保存为无效平均值，并通过下一条消息发送。

然后开始进行新的平均值计算。如果模拟值仍在上溢或下溢范围内，则会再次将命名的两个值其中之一保存为无效平均值，并在下一条消息触发时发送。

说明

组态的故障抑制时间 > 0

如果已组态误差抑制时间并随后启用了生成平均值功能，则错误抑制时间的值显示为灰色且不再使用。如果启用生成平均值功能，则内部会将错误抑制时间设置为 0。

单极性传送

限制

无法在生成平均值的同时组态单极性传送。当激活生成平均值功能时，启用单极性传送将不起作用。

功能

对于单极性传送，会将负值更正为零。如果不应将来自欠范围的值当作实际的测量值传送，则需要这一操作。

例外情况：对于输入模块的过程数据，用于指示非零最小输入断线状态的值 **-32768 / 8000_h** 可以传送。

但对于软件输入，所有负值都将更正为零。

故障抑制时间

功能要求

为该数据点组态阈值触发

限制

无法在生成平均值的同时组态故障抑制时间。当激活生成平均值功能时，组态的值将不起作用。

功能

该参数的典型应用是，抑制大功率电机启动时产生电流峰值，要不然会向控制中心发出干扰信号。

在指定的时间段内，将抑制位于上溢范围 (7FFF_h) 或下溢范围 (8000_h) 的模拟值的传送。超出此故障抑制时间后，如果值 7FFF_H 或 8000_H 仍处于未决状态，才会发送该值。

如果该值在故障抑制时间结束前返回到测量范围，将传送当前值。

输入模块

根据 S7

模拟量输入模块直接采集到的模拟值作为原始值完成抑制调整。这些模块将返回针对所有输入范围（也包括非零最小输入）指定的上溢或下溢范围值。

上溢范围 (32767 / 7FFF_h) 或下溢范围 (-32768 / 8000_h)

内的模拟值不会在故障抑制时间内进行传送。这同样适用于非零最小输入。若在故障抑制时间结束后，上溢/下溢范围内的值仍处于未决状态，才会进行传送。

针对由 CPU 预处理完成后的值的建议：

如果 CPU

的位存储区或数据块中提供了预处理完成后的值，则只有当这些值也具有上述上溢或下溢范围内的 32767 / 7FFF_h 或 -32768 / 8000_h

时，抑制才可行或有意义。如果不是这种情况，则不应为预处理的值组态该参数。

对于在 CPU 中预处理完成的值，可自由指定上溢和下溢的限值。

滤波系数

功能要求

为该数据点组态阈值触发

限制

无法在生成平均值的同时组态滤波系数。当激活生成平均值功能时，组态的值将不起作用。

功能

使用滤波功能可以使快速波动的模拟值稳定。

与 S7 模拟量输入模块一样，根据以下公式计算滤波系数。

$$y_n = \frac{x_n + (k-1) y_{n-1}}{k}$$

其中

y_n = 当前周期中的滤波值

x_n = 当前周期 n 中采集的值

k = 滤波系数

可将下列值组态为模块的滤波系数。

- 1 = 无滤波
- 4 = 弱滤波
- 32 = 中滤波
- 64 = 强滤波

设置限值“低” / 设置限值“高”

功能要求

- 为该数据点组态阈值触发
- PLC 变量位于位存储器操作数区域或数据区域中

模拟值数据点必须链接到位存储器或数据区域（数据块）中的 PLC 变量。对于硬件模块的 PLC 变量（输入操作数区域），无法进行限值组态。

限值的组态对于已经过 CPU 预处理的测量值毫无意义。

功能

在这两个输入框中，可以在测量范围起点方向和测量范围终点的方向上设置限值。还可以评估限值，例如，作为测量范围的起点或终点。

状态标识符“OVER_RANGE” / “overflow”

通过支持状态标识符的协议，如果超出或低于限值，则将数据点的状态标识符设置为测量范围违例，即下文所述的“OV”。这些状态标识符将在数据点的状态 ID (页 109)部分中介绍。

传递相关模拟值时，数据点状态标识符的“OV”位的设置如下：

- 限值“高”：
 - 如果超出此限值：OV = 1
 - 如果值低于此限值：OV = 0
- 限值“低”：
 - 如果值低于此限值：OV = 1
 - 如果值超出此限值：OV = 0

限值的组态

限值将完全以十进制数形式组态。值的范围基于模拟输入模块原始值的值范围。

十进制数字条目对应于位存储器或数据区域中已分配 PLC 变量的值范围。

值 0（零）的条目为禁用的限值。

范围	PLC 变量的原始值（16 位）		模块输出 [mA]			测量范围 [%]
	十进制	十六进制	0 .. 20 (单极)	-20 .. +20 (双极)	4 .. 20 (非零最小)	
上溢	32767	7FFF	> 23.515	> 23.515	> 22.810	> 117.593
过范围	32511 ... 27649	7EFF ... 6C01	23.515 ... 20.001	23.515 ... 20.001	22.810 ... 20.001	117.593 ... 100.004
额定范围 (单极/非零最小)	27648 ... 0	6C00 ... 0000	20 ... 0		20 ... 4	100 ... 0
额定范围 (双极)	27648 ... 0 ... -27648	6C00 ... 0000 ... 9400		20 ... 0 ... -20		100 ... 0 ... -100
欠范围 (单极/非零最小)	-1 ... -4864	FFFF ... ED00	-0.001 ... -3.518		3.999 ... 1.185	-0.004 ... -17.59

范围	PLC 变量的原始值 (16 位)		模块输出 [mA]			测量范围 [%]
	十进制	十六进制	0 .. 20 (单极)	-20 .. +20 (双极)	4 .. 20 (非零最小)	
欠范围 (双极)	-27649	93FF		-20.001		-100.004

	-32512	8100		-23.516		-117.593
下冲/断线	-32768	8000	< -3.518		< 1.185	< -17.593

说明

选项被禁用时的值评估

如果启用上述一个或两个选项并组态值，后来再禁用该选项，则仍然会评估灰色显示的值。

要禁用这两个选项，需先从输入框中删除之前组态的限值，然后禁用相关选项。

针对快速波动的模拟值的建议：

模拟值波动较快时，如果已组态限值，则先对模拟值滤波会有所帮助。

4.10.11 命令输出

命令输出的参数

使用 DNP3 和 IEC 协议，可为命令输出组态以下参数：

- LATCH_ON / LATCH_OFF
- PULSE_ON

可为下列数据点类型组态参数：

- DNP3
Binary Command Output
- IEC
Single command

组态

该数据点类型允许接收带有以下控制信息（控制代码）的命令：

- **LATCH_ON / LATCH_OFF**

或

- **PULSE_ON**

当主站接收到与功能“PULSE_ON”一起发出的“Control Code”字节时，则对“Count”、“On-time”和“Off-time”进行评估，并与对象参数“最大脉冲宽度”(Max. pulse duration)、“脉冲宽度替换时间”(Pulse duration replacement time)和“最大脉冲数”(Max. number of pulses) 进行比较（见下文）。

将评估由主站发送的以下控制代码。

表格 4-8 数据对象功能

接收:			对象的反应取决于组态	
Control Code	TCC *	Op Type **	输出模式 = Pulse on	输出模式 = Latch on/off
0x01	NUL	PULSE_ON	将“On-time”持续时间的输出设置为 1。	拒绝命令。
0x03	NUL	LATCH_ON	拒绝命令。	输出永久设置为 1。
0x04	NUL	LATCH_OFF	拒绝命令。	输出永久设置为 0。
0x41	CLOSE	PULSE_ON	输出永久设置为 1（同 LATCH_ON）。	拒绝命令。
0x81	TRIP	PULSE_ON	输出永久设置为 0（同 LATCH_OFF）。	拒绝命令。

* Trip-Close Code field

** Operation Type field

参数

名称: 最大脉冲数 (Max. number of pulses)

取值范围: 0 ... 255

默认值:	0
说明:	监视主站发送的脉冲数 (Count)。如果所接收的来自主站的脉冲数超出此处的组态值，则拒绝命令。 如果输入 0（零），则会禁用此监视。
名称:	最大脉冲宽度 (Max. pulse duration)
取值范围:	0 ... 65535
默认值:	0
说明:	监视主站发送的脉冲宽度 (On-time)。如果接收来自主站的脉冲的持续时间超出此处的组态值，则使用可组态的“脉冲宽度替换时间”(Pulse duration replacement time)。如果将“脉冲宽度替换时间”(Pulse duration replacement time) 组态为零，则拒绝该命令。 通过 0（零），“脉冲宽度替换时间”(Pulse duration replacement time) 可用于每个脉冲。
名称:	脉冲宽度等效时间 (Pulse duration equivalent time)
取值范围:	0 ... 65535
默认值:	0
说明:	如果所接收的来自主站的脉冲宽度超出“最大脉冲宽度”(Max pulse duration) 中的组态值，则替换脉冲宽度值。仅当组态了“最大脉冲宽度”(Max. pulse duration) 时，该参数可用。 如果该值为 0（零），则无可用替换值。 如果“最大脉冲宽度”(Max. pulse duration) 和“脉冲宽度替换时间”(Pulse duration replacement time) 组态为零，则拒绝该命令。

4.10.12 伙伴站

4.10.12.1 DNP3 和 IEC 数据点的伙伴组态

启用数据点的伙伴 - DNP3/IEC

启用所选数据点可用于交换数据的所有已组态伙伴。可在“伙伴站”(Partner stations) 参数组中指定 CP 的通信伙伴。

- 启用伙伴 1

在数据点的概览表格中，将默认伙伴 1 设置为数据点的伙伴。

此时，在“伙伴站”(Partner stations) 选项卡中，会启用伙伴 1，该选项呈灰显。

- 启用伙伴 n

如果您在概览表格中为此数据点启用不同伙伴或多个伙伴，将会在“伙伴站”(Partner stations) 选项卡中启用，且可以选择或取消选择全部 4 个伙伴。

4.10.12.2 具有 TeleControl Basic 数据点的伙伴组态。

启用数据点的伙伴 - TeleControl Basic

启用所选数据点可用于交换数据的伙伴。

可组态通信。不能同时选择遥控服务器和 S7 站作为数据点的伙伴。

通信伙伴可以为：

- 遥控服务器

由于遥控服务器始终作为 CP 的通信伙伴启用，因此在此选项卡中默认使用。

已选择“遥控服务器已启用”(Telecontrol server enabled) 选项并灰显。

- S7 站

必须通过“TeleControl Basic”协议访问此站。

可在“伙伴站”(Partner stations) 参数组中指定 CP 的通信伙伴。

激活两个选项之一：

- 遥控服务器已启用

仅遥控服务器是数据点的通信伙伴。

- 站间通信的伙伴

仅 S7 站是数据点的通信伙伴。

伙伴编号（站间通信）

通过从下拉列表中选择所需伙伴，为所选数据点的站间通信指定伙伴 CP。相关伙伴的访问 ID 显示在括号中。

可以选择在“伙伴站 > 站间通信伙伴”(Partner stations > Partner for inter-station communication) 中指定的伙伴。

数据点索引

通信伙伴上相应数据点的索引。

注意：

- 发送和接收 CP 的数据对必须具有相同的数据点索引。CP 2 的接收数据点与具有相同数据点索引的 CP 1 发送数据点相对应。
- 对于相反的通信方向，必须创建第二对数据点。CP 2 的发送数据点与具有相同数据点索引的 CP 1 接收数据点相对应。同样，两者具有相同的数据点索引。

4.11 消息

组态电子邮件

如果发生了重要事件，CP 可向通信伙伴发送电子邮件。

关于使用电子邮件的要求，请参见电子邮件组态 (页 79)部分。

可在 STEP 7

中用于组态数据点和消息的编辑器中组态电子邮件。若要找到此内容，可使用项目树：

“项目 > 相关站的目录 > 本地模块 > CP”(Project > directory of the relevant station > Local modules > CP)

有关 STEP 7 中的视图，请参见数据点组态 (页 93)部分。

消息编辑器的常规功能（如复制或列设置）与数据点编辑器的功能相对应。

要求和必要信息

请记住 CP 组态中对于传送电子邮件的以下要求：

- 组态“电子邮件组态”(E-mail configuration) 参数组（请参见“安全性”参数组）

为此，需要以下信息：

- SMTP 服务器的访问数据：地址、端口号、用户名、密码
- CP 自己的电子邮件地址
- 收件人的电子邮件地址

“消息参数”

在此处组态消息的收件人、主题和文本。

“触发器”

在“触发器”(Trigger) 参数组中，组态发送消息和其它参数的触发机制。

- 电子邮件触发器

指定触发电子邮件发送的事件。

- 使用 PLC 变量

要通过触发信号实现电子邮件发送，需评估触发位“触发器的 PLC 变量”(PLC tag for trigger) 的沿变化 (0 →

1)。必要时，可以为每个电子邮件组态一个触发位。有关触发位的信息，请参见以下部分。

- CPU 切换到 STOP 模式
- CPU 切换到 RUN 模式
- 与伙伴的连接中断

在与伙伴的连接中断时，触发电子邮件发送。

- 建立与伙伴的连接

连接恢复时触发电子邮件发送。

仅可通过 TeleControl Basic 触发以下各项：

- 建立与伙伴的连接失败
无法建立与伙伴的连接时，触发电子邮件发送。
- Teleservice 会话开始
- Teleservice 会话结束

- **触发器的 PLC 变量**

用作电子邮件触发器“使用 PLC 变量”(Use PLC tag) 的 PLC 变量

如果该触发位的存储区是在位存储区或数据块中，则触发位在电子邮件发送后复位为零。

- **启用处理状态标识符**

如果启用此选项，则每次尝试发送都返回一个状态，并提供有关已发送消息处理状态的信息。

该状态将写入“处理状态的 PLC 变量”(PLC tag for processing status)。如果传送消息时出现问题，可以通过在 CPU 的 Web 服务器上显示该 PLC 变量的值来确定状态。

有关十六进制状态输出的意义，请参见电子邮件的处理状态 (页 147)部分。

- **处理状态的 PLC 变量**

用于反映处理状态的 DWORD 类型的 PLC 变量

- **包括值**

如果启用该选项，则 CP 会向消息中的占位符 \$\$ 发送 CPU 存储区中的值。为此，可输入“\$\$”作为占位符，以便在消息文本中显示待发送的值。

请选择一个 PLC

变量，该变量的值将集成在消息中。借此，将该值输入到消息文本中，代替占位符 \$\$。

\$\$ 可以是数据点类型（最多 32 位的简单数据类型）的占位符。

- **值关联的 PLC 变量**

要写入待发送值的 PLC 变量。

4.12 访问 Web 服务器

访问 CPU 的 Web 服务器

S7-1200 站的 Web 服务器位于 CPU 中。通过 CP，可以访问 CPU 的 Web 服务器。

如果已通过 LAN 将 PC 连接到遥控服务器，则可通过 PC 使用 TCSB 访问站的 Web 服务器。

相关要求请参见手册/3/ (页 164)。

有关 Web 服务器的信息，请参见手册/1/ (页 163)。

程序块

5.1 用于 OUC 的程序块

使用 Open User Communication (OUC) 的程序块

若要在 S7 站之间直接通信，可使用下述指令（程序块）。

与其它通信类型不同，Open User Communication 无需在 CP 组态中启用，因为需要为此创建相应的程序块。有关程序块的详细信息，请参见 STEP 7 的信息系统。

说明

不同程序块版本

请注意，在 STEP 7 中，不能在一个站中使用一个程序块的不同版本。

支持用于 OUC 的程序块

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

- TSEND_C V3.0 / TRCV_C V3.0

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

或者：

- TCON V4.0 / TDISCON V2.1

建立连接/终止连接

- TUSEND V4.0 / TURCV V4.0

通过 UDP 发送和接收数据

- TSEND V4.0 / TRCV V4.0

通过 TCP 或 ISOonTCP 发送和接收数据

- TMAIL_C V4.0

发送电子邮件

要通过该块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 V1.0

IP 参数的程序控制组态

此程序块可在 STEP 7 的“指令 > 通信 > Open User Communication”(Instructions > Communication > Open User Communication) 窗口中找到。

系统数据类型 (SDT) 的连接描述

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

创建数据块 SDT

为每个数据块（全局 DB）形式的连接描述创建所需的 SDT。

SDT 类型生成的具体方式是在程序块声明表中的“数据类型”(Data type) 框中手动输入名称（例如“TCON_Param”），而不是从“数据类型”(Data type) 下拉列表中选择一个条目。随后，相应的 SDT 与其参数一并创建出来。

使用 SDT

- TCON_IP_v4

基于 TCP 或 UDP 传送帧

- TADDR_Param

基于 UDP 传送帧

- TCON_IP_RFC

基于 ISO-on-TCP 传送帧（两个 S7-1200 站间直接通信）

- **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
- **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。注意：必须为每个连接调用单独的程序块 TCON。

必须为每个通信伙伴建立单独的连接，即使发送相同数据块。

成功传输数据之后，可以终止连接。还可以通过调用“TDISCON”终止连接。

说明

连接中止

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

5.2 在运行期间更改 IP 地址

在运行期间更改 IP 地址

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

说明

使用动态 IP 地址更改 IP 参数

如果 CP 从 Internet 服务提供商获得动态 IP 地址，请注意程序控制的 IP 参数更改的影响：在这种情况下，通信伙伴无法再访问 CP。

要求 - 固体版本

对程序控制的 IP 参数更改存在如下要求：

- CP 固件 \geq V2.1.7x
以及
- CPU 固件 \geq V4.2

要求 - 程序块/STEP 7 版本

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。

根据 STEP 7 版本，可以使用以下程序块和系统数据类型：

- **STEP 7 Basic ≥ V14**

T_CONFIG

配合：

- IF_CONF_V4
- IF_CONF_NTP
- IF_CONF_V6
- IF_CONF_DNS

- **STEP 7 Basic ≤ V14**

TC_CONFIG

配合：

- IF_CONF_V4

有关块编程的详细信息，请参见 STEP 7 信息系统。

要求 - CP 编程

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。

5.2 在运行期间更改 IP 地址

诊断和保养

6.1 诊断选项

可使用以下诊断选项。

模块的 LED

有关 LED 显示的详细信息，请参见LED (页 28)部分。

STEP 7: 巡视窗口中的“诊断”(Diagnostics) 选项卡。

可在此处找到有关所选模块在线状态的以下信息：

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

使用在线功能，可以从存储了 CP 项目的工程师站中读取 CP 的诊断信息。

如果想通过 CP 对工作站运行在线诊断，则需要激活“通信类型”(Communication types) 参数组的在线功能，请参见通信类型 (页 51)部分。

“诊断”(Diagnostics) 组

可在此处找到有关所选模块的以下静态信息：

- 模块的常规信息
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

- **Industrial Remote Communication**

在此处，可获取有关 CP 的 WAN 接口和其他参数的具体信息。该条目下具有下列子条目：

- 伙伴
 - 有关伙伴地址设置的信息，连接统计信息，伙伴的组态数据以及其它诊断信息。
- 数据点列表
 - 有关数据点的各种信息，例如：组态数据、值、连接状态等
- 协议诊断
 - 使用“启用协议跟踪”(Enable protocol trace) 功能，将复制模块接收和发送的帧几秒钟。
 - 使用“禁用协议跟踪”(Disable protocol trace) 功能，将停止记录并将数据写入记录文件。
 - 使用“保存”(Save) 功能，可将日志文件保存在工程师站，然后再进行分析。
- 设备特定事件
 - 有关 CP 内部事件的信息

- **时间**

有关设备上时间的信息

“功能”(Functions) 组

- **保存服务数据**

该功能用于记录您无法自行消除预期之外或不必要的模块行为时的内部过程。

使用“保存服务数据”(Save service data) 按钮创建日志文件。数据保存在格式为“*.dmp”的文件中，可通过 Siemens 热线进行评估。

STEP 7: 伙伴状态

CP 可以通过 PLC 变量向 CPU 发送通信伙伴的连接状态。可以通过 CPU 的 Web 服务器显示 PLC 变量的状态

有关组态的信息，请参见伙伴站 (页 61)部分。

CPU 的 Web 服务器

通过 CP 可访问 CPU 的 Web 服务器以及其中的可见信息。要进行相应访问，请参见访问 Web 服务器 (页 133)部分。

SNMP

有关各功能的信息，请参见SNMP (页 146)部分。

6.2 通过端口 8448 执行在线安全诊断

在不打开端口 102 的情况下执行安全诊断

如果想在不开端口 102 的情况下执行安全诊断，请按下列步骤进行操作：

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

这样，即可通过端口 8448 执行安全诊断。

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 78)

6.3 在线功能和 TeleService

在线功能和 TeleService

CP 与工程师站 (ES) 上的 STEP 7 一起，以如下术语的名义提供诸多诊断和维护功能：

- 在线功能

从 ES 通过 LAN 访问站

要求：ES 和 CP 位于同一子网中。

- TeleService

从 ES 通过 WAN (Internet) 访问站

要求：CP 连接到遥控服务器，并且可以通过此路径到达，请参见访问 Web 服务器 (页 133)部分中的信息。

对于位于不同 IP 子网，或者可通过 Internet 访问的远程站，只有在通过 VPN 通道将 ES（具有 CP 1628 或通过 SCALANCE S）连接到该站时才能使用这些功能。

用于传输用户数据的 CP 和遥控服务器之间用于传送用户数据的连接不会被 TeleService 连接中断。

这些功能和连接的建立在很大程度上与在线功能和 TeleService 相同。

说明

TeleService 的传输时间

请注意，通过 WAN (Internet) 传输大量数据可能需要很长时间。

如果传输路径中断，将导致数据传输被中止。

通过以太网建立使用在线功能的连接

步骤：

1. 将 ES 连接到网络。
2. 在 ES 上打开相关的 STEP 7 项目。
3. 选择要通过新固件更新的 CP 或站（要更新其 CP）的 CPU。
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) 对话框中，转到“PG/PC 接口类型”(Type of PG/PC interface) 下拉列表中，选择条目“通过遥控实现 TeleService”(TeleService via telecontrol)。
6. 在“PG/PC 接口”(PG/PC interface) 下拉列表中选择条目“TeleService board”。
7. 如果尚未选择 CP，则在表中选择 CP。

通过 CP 或 CPU 的路径均可行。

8. 单击“PG/PC 接口”(PG/PC interface) 下拉列表旁的  图标。

将打开“通过遥控建立远程连接”(Establish remote connection via telecontrol) 对话框。

9. 在此对话框中进行必要的输入（见下文），然后单击“连接”(Connect)。

“通过遥控建立远程连接”(Establish remote connection via telecontrol) 对话框中的信息。

在该对话框中，输入之前在 STEP 7 的以下标题中组态的数据：

- **遥控服务器/TeleService 网关...**

选择 TeleService 交换站是位于工程师站的 PC 上还是网络中，以及可否通过 Internet 进行访问。

TeleService 网关不能仅用作遥控服务器的交换站。

- 输入遥控服务器的地址。

可由 DNS 解析的遥控服务器的 IP 地址或名称以及端口号

- 个人服务器密码

输入使用遥控服务器对 CP 进行验证时使用的遥控密码

CP 的遥控密码在安全设置中的“CP 标识”(CP identification) 下组态，另请参见使用 TeleControl Basic 协议的 CP 标识 (页 73)部分。

- **验证...**

- Teleservice 用户名和密码

在此处，输入在 STEP 7 的全局 TeleService 设置中组态的 Security 用户数据，另请参见 TeleService 访问的组态 (页 91)部分。

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。

6.4 SNMP

SNMP (Simple Network Management Protocol)

SNMP 是用于管理和诊断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)。

CP 作为 SNMP 代理时的性能范围

CP 支持在以下版本的 SNMP 中进行数据查询：

- SNMPv1 (标准版)
- SNMPv3 (Security)

它根据 RFC 1213 和 Siemens 自动化 MIB 返回标准 MIB II 的 MIB 对象的内容。

- **MIB II**

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
- ICMP
- TCP
- UDP
- SNMP

不支持以下组的 MIB II 标准：

- Adress Translation (AT)
- EGP
- Transmission

- **Siemens Automation MIB**

以下例外/限制适用于 CP。

只允许对系统组的以下 MIB 对象进行写访问：

- sysContact
- sysLocation
- sysName

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

出于安全原因，对于所有其它 MIB 对象/MIB 对象组，只能进行读访问。

CP 不支持陷阱。

有关 MIB 文件和 SNMP 的更多详细信息，请参见 /5/ (页 164) 手册。

组态

有关组态的信息，请参见：

- 禁用安全功能 (SNMPv1)：SNMP (页 61)
- 启用安全功能 (SNMPv1 / SNMPv3)：SNMP (页 81)

6.5 电子邮件的处理状态

组态电子邮件的处理状态

以下状态标识符适用于通过 CP 的消息编辑器组态的电子邮件。状态标识符的输出通过选项“启用处理状态标识符”(Enable identifier for processing status) 启用。状态标识符将写入 CPU 中的“处理状态的 PLC 变量”(PLC tag for processing status)。

有关组态的信息，请参见消息 (页 130)部分。

输出电子邮件的处理状态

处理状态由 CP 本身或相关服务的服务器在发送消息之后返回。

如果传送消息时出现问题，可以通过 CPU 的 Web 服务器确定状态。

6.5 电子邮件的处理状态

电子邮件的处理状态

“处理状态的 PLC 变量”(PLC tag for processing status) 状态标识符的含义如下：

表格 6-1 以十六进制格式输出的状态 ID 的含义

状态	含义
0000	传送已完成且未出错
82xx	来自电子邮件服务器的其它错误消息 除了前导“8”外，该消息还对应于 SMTP 协议的三位错误编号。
8401	无可用的通道可能原因：已存在通过 CP 的电子邮件连接。不能同时建立另一个连接。
8403	无法建立到 SMTP 服务器的 TCP/IP 连接。
8405	SMTP 服务器已拒绝登录请求。
8406	由 SMTP 客户端检测到内部 SSL 错误或证书结构问题。
8407	使用 SSL 的请求被拒绝。
8408	客户端无法获得用来与邮件服务器建立 TCP/IP 连接的套接字。
8409	无法通过连接进行写入。可能原因：通信伙伴复位了连接或连接已中止。
8410	无法通过连接进行读取。可能原因：通信伙伴终止了连接或连接已中止。
8411	发送电子邮件失败。原因：无足够的存储空间用于发送。
8412	组态的 DNS 服务器无法解析指定的域名。
8413	由于 DNS 子系统出现内部错误，导致域名无法被解析。
8414	域名为空字符串。
8415	cURL 模块发生内部错误。执行已中止。
8416	SMTP 模块发生内部错误。执行已中止。
8417	通过已经使用的通道向 SMTP 发出请求或通道 ID 无效。执行已中止。
8418	发送电子邮件已中止。可能原因：超出执行时间。
8419	通道已中断且在连接终止前无法使用。
8420	无法用 CP 的根证书验证来自服务器的证书链。
8421	发生内部错误。执行已停止。
8450	操作未执行：邮箱不可用/不可访问。以后再重试。
84xx	来自电子邮件服务器的其它错误消息 除了前导“8”外，该消息还对应于 SMTP 协议的三位错误编号。

状态	含义
8500	语法错误：命令未知。 还包括命令链过长的错误。原因可能是电子邮件服务器不支持 LOGIN 验证方法。 尝试不经过验证而发送电子邮件（无用户名）。
8501	语法错误。请检查以下组态数据： 报警组态 > 电子邮件数据 (Content): <ul style="list-style-type: none"> 收件人地址（“收件人”或“抄送”）。
8502	语法错误。请检查以下组态数据： 报警组态 > 电子邮件数据 (Content): <ul style="list-style-type: none"> 电子邮件地址（发送方）
8535	SMTP 验证未完成。请检查 CP 组态中的“用户名”和“密码”参数。
8550	无法访问 SMTP 服务器。没有访问权限。请检查以下组态数据： <ul style="list-style-type: none"> CP 组态 > 电子邮件组态： <ul style="list-style-type: none"> 用户名 密码 电子邮件地址（发送方） 报警组态 > 电子邮件数据 (Content): <ul style="list-style-type: none"> 收件人地址（“收件人”或“抄送”）。
8554	传送失败
85xx	来自电子邮件服务器的其它错误消息 除了前导“8”外，该消息还对应于 SMTP 协议的三位错误编号。

6.6 下载固件

CP 的新固件版本

如果模块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/15922/dl>)

请注意，无法将 V3 及以上的固件版本加载至硬件产品版本为 1 的 CP 上。

在工程师站 (ES) 上保存新的固件文件后，可使用以下方法加载固件文件：

- 将固件文件保存在 CPU 的存储卡上（推荐方法）
有关该过程的说明，请参见 S7-1200 系统手册。
- 通过以太网使用 STEP 7 的在线功能加载固件
有关将 ES 连接如何连接到站，请参见在线功能和 TeleService (页 144)部分。
- 通过 CPU（CPU 固件版本 V4.0 及更高版本）的 Web 服务器下载固件
此方法将在后文进行介绍。

说明

对 CPU 的保持性存储器的影响

- 如果使用 SIMATIC 存储卡安装固件文件，则会保留保持性存储器。
 - 如果使用 Web 服务器或在线功能安装固件文件，保持性存储器将丢失。
-

通过 CPU 的 Web 服务器下载固件

按照以下步骤将 ES 连接到 CPU 的 Web 服务器，并将 CP 的新固件文件下载到站中。

网络组态期间的要求

- CP 连接到遥控服务器，并且可以通过此路径到达。

请参见访问 Web 服务器 (页 133)部分中的信息。

CPU 组态要求

1. 在 ES 上打开相应项目。
2. 在 STEP 7 中选择所涉及站的 CPU。
3. 选择“Web 服务器”(Web server) 条目。
4. 在参数组“常规”(General) 中，选择“为此接口启用 Web 服务器”(Enable Web server for this interface) 选项。
5. 使用 CPU V4.0 或更高版本，在用户管理中创建具有所需权限的用户。

您需要分配根据访问级别执行固件更新的权限。

建立一个到 Web 服务器的连接时所需的步骤取决于您是启用还是禁用了“常规”(General) 参数组中的“仅允许通过 HTTPS 访问”(Allow access only using HTTPS) 选项:

- **通过 HTTP 建立连接**

禁用了“仅允许通过 HTTPS 访问”(Allow access only using HTTPS) 选项时步骤

- **通过 HTTPS 建立连接**

启用了“仅允许通过 HTTPS 访问”(Allow access only using HTTPS) 选项时的步骤

这两种情况在以下部分中进行说明。

要求: 新的固件文件存储在工程师站上。

在 STEP 7 信息系统中通过关键字“Web 服务器的相关信息”可找到访问 CPU 的 Web 服务器的要求 (允许的 Web 浏览器) 和步骤说明。

通过 HTTP 建立连接

1. 通过以太网接口将新固件文件所在的 PC 连接到 CPU。
2. 在 Web 浏览器的地址框中输入 CPU 的地址: `http://<IP 地址>`
3. 按回车键。

将打开 Web 服务器的起始页。

4. 单击窗口右上部的“下载证书”(Download certificate) 条目。

将打开“证书”(Certificate) 对话框。

5. 单击“安装证书...”(Install certificate ...) 按钮将证书下载到 PC。

证书将加载到 PC 上。

在 Web 浏览器的帮助中以及在 STEP 7 信息系统中通过关键字“HTTPS”或“使用 HTTPS 访问 (S7-1200)”可找到有关下载证书的信息。

6. 若连接已切换到安全模式 HTTPS (Web 服务器地址框中的“`https://<IP 地址>/...`”) 时, 可以按照下一部分“下载固件”(Downloading firmware) 中的描述继续操作。

如果终止到 Web 服务器的连接, 则下一次可 Web 服务器登录而不使用 HTTP 下载证书。

通过 HTTPS 建立连接

1. 通过以太网接口将新固件文件所在的 PC 连接到 CPU。
2. 在 Web 浏览器的地址框中输入 CPU 的地址: `https://<IP 地址>`

6.7 模块更换

3. 按回车键。

将打开 Web 服务器的起始页。

4. 按照下文“加载固件”部分所述继续操作。

加载固件

1. 以具有必要权限的用户身份登录 Web 服务器的起始页。

使用在 CPU 的 Web 服务器用户管理中所组态的用户数据。

2. 登录后，在 Web 服务器的导航面板中选择条目“模块状态”(Module status)。

3. 在模块列表中选择 CP。

4. 选择窗口下方的“固件”(Firmware) 选项卡。

5. 使用“浏览...”(Browse...) 按钮浏览到 PC 上的固件文件并使用“运行更新”(Run update) 按钮将文件下载到站中。

说明

关闭 Web 服务器

如果在固件更新期间关闭 Web 服务器，则无法将 CPU 的操作状态切换为 RUN。在这种情况下，需要先关闭 CPU 并再次打开，将 CPU 切换为 RUN 工作状态。

6.7 模块更换

模块更换



小心

阅读系统手册“S7-1200 可编程控制器”

在安装、连接和调试之前，先阅读系统手册“S7-1200 可编程控制器”中的相应部分（请参见本文档的附录）。

安装和连接时，按照系统手册“S7-1200 可编程控制器”所述步骤操作。

安装/卸载设备时，确保关闭电源。

CP 的 STEP 7 项目数据存储在本地的 CPU 中。如果设备有故障，只需更换 CP，而不必重新将项目数据下载到站。

站再次启动时，新 CP 将从 CPU 中读取项目数据。

技术数据

7.1 CP 1243-1 的技术规范

表格 7-1 CP 1243-1 的技术规范

技术规范		
部件编号	6GK7 243-1BX30-0XE0	
工业以太网连接		
数量	1	
设计	RJ-45 插孔	
属性	100BASE-TX, IEEE 802.3-2005, 半双工/全双工, 自动跨接, 自动协商, 光电隔离	
传输速度	10/100 Mbps	
允许的电缆长度 (以太网)	(每个长度范围的备选组合) *	
0 ... 55 m	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	
电气数据		
电源	来自 S7-1200 背板总线	5 VDC
电流消耗 (典型值)	来自 S7-1200 背板总线	250 mA
有效功耗 (典型值)	来自 S7-1200 背板总线	1.25 W
允许的环境条件		
环境温度	导轨水平安装的运行期间	-20 °C 至 +70 °C

技术规范		
	导轨垂直安装的运行期间	-20 °C 至 +60 °C
	存储期间	-40 °C 到 +70 °C
	运输期间	-40 °C 到 +70 °C
相对湿度	运行期间	25 °C 时 ≤ 95 %，无冷凝
设计、尺寸和重量		
模块规格	用于 S7-1200 的紧凑型模块，单宽度	
防护等级	IP20	
重量	122 g	
尺寸 (W x H x D)	30 x 110 x 75 mm	
安装选件	标准 DIN 导轨 开关配电板	
产品功能 **		

* 有关详细信息，请参见 IK PI 目录的“接线技术”

**有关更多特性和性能数据，请参见应用和属性 (页 13)部分。

7.2 以太网接口的引脚分配

以太网接口的引脚分配

下表列出了以太网接口的引脚分配。引脚分配符合以太网标准 802.3-2005，100BASE-TX 版本。

表格 7-2 以太网接口的引脚分配

RJ-45 插孔的视图	引脚	信号名称	分配
	1	TD	发送数据 +
	2	TD_N	发送数据 -
	3	RD	接收数据 +
	4	GND	接地
	5	GND	接地
	6	RD_N	接收数据 -
	7	GND	接地
	8	GND	接地

7.2 以太网接口的引脚分配

指定的认证

说明

设备铭牌上指定的认证

在产品上会印有指定认证的相应标志。

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。

CP 已通过以下认证并符合以下标准：

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

可以从下面的地址获取需要提供给所有责任机构的 EC 符合性声明：

Siemens Aktiengesellschaft
Division Process Industries and Drives
Process Automation
DE-76181 Karlsruhe
Germany

有关该产品的 EC 符合性声明，请访问以下 Internet 地址：

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/15922/cert>) >“EC 符合性声明”

IECEX

CP 满足 IECEX 的防爆要求。

IECEX 分类： Ex nA IIC T4 Gc

IECEX 证书： IECEX DEK 14.0088X

CP 满足以下标准的相关要求：

- EN 60079-0
危险区域 - 第 0 部分：设备 - 常规要求
- EN 60079-15
易爆环境 - 第 15 部分：防护类型“n”的设备保护

可在 IECEX 证书中找到标准的当前版本，请访问以下 Internet 地址获取 IECEX 证书：

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/15922/cert>)

必须满足IECEX/ATEX 要求的危险场所使用注意事项
(页 34)部分中的相关条件，才能安全部署 CP。

此外，也应注意文档“Use of subassemblies/modules in a Zone 2 Hazardous Area”中的信息，请访问以下 Internet 地址获取该文档：

链接：(<https://support.industry.siemens.com/cs/ww/zh/view/78381013>)

ATEX



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

ATEX 认证： II 3 G Ex nA IIC T4 Gc

Type Examination Certificate: KEMA 10ATEX0166 X


相关标准：

- EN 60079-0:2006: 潜在爆炸环境 - 一般要求
- EN 60079-15:2005: 用于爆炸性气体环境的电气设备；防护类型“n”

设备适合在污染等级 2 的环境中使用。

设备适合仅可在符合以下条件的环境中使用：

- Class I, Division 2, Group A, B, C, D 以及没有爆炸危险的区域
- Class I, Zone 2, Group IIC 以及没有爆炸危险的区域

 警告
<p>安装准则</p> <p>如果在安装和运行期间遵守以下规则，则产品符合要求：</p> <ul style="list-style-type: none"> • 使用设备的重要注意事项 (页 33)部分中的注意事项 • /I/ (页 163)文档中的安装说明

请注意，需满足链接：

(<https://support.industry.siemens.com/cs/ww/zh/ps/15922/cert>)部分中的相关条件，才能安全部署 CP。

此外，也应注意文档“Use of subassemblies/modules in a Zone 2 Hazardous Area”中的信息，请访问以下 Internet 地址获取该文档：

链接：(<https://support.industry.siemens.com/cs/ww/zh/view/78381013>)

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)

File Number: E223122

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 T4A; Ta = -20 °C...60 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...60 °C

Report / UL file: E223122 (NRAG.E223122)

请注意，需满足符合 UL HazLoc 要求的危险场所使用注意事项 (页 35)部分中的相关条件，才能安全部署 CP。

FM



Factory Mutual Approval Standard Class Number 3600, 3611, 3810, ANSI/ISA-61010-1

Equipment rating:

Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C

Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

Report Number: 3049779, 3049925

请注意，需满足FM 要求的危险场所使用注意事项 (页 35)部分中的相关条件，才能安全部署 CP。

澳大利亚 - RCM



CP 满足 AS/NZS 2064 标准 (A 类) 的要求。

EAC (Eurasian Conformity)



俄罗斯、白俄罗斯和哈萨克斯坦关税同盟

基于关税同盟 (TR CU) 技术规范的符合性声明

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/15922/cert>)

尺寸图

说明

CP 图中的所有尺寸均以毫米为单位。

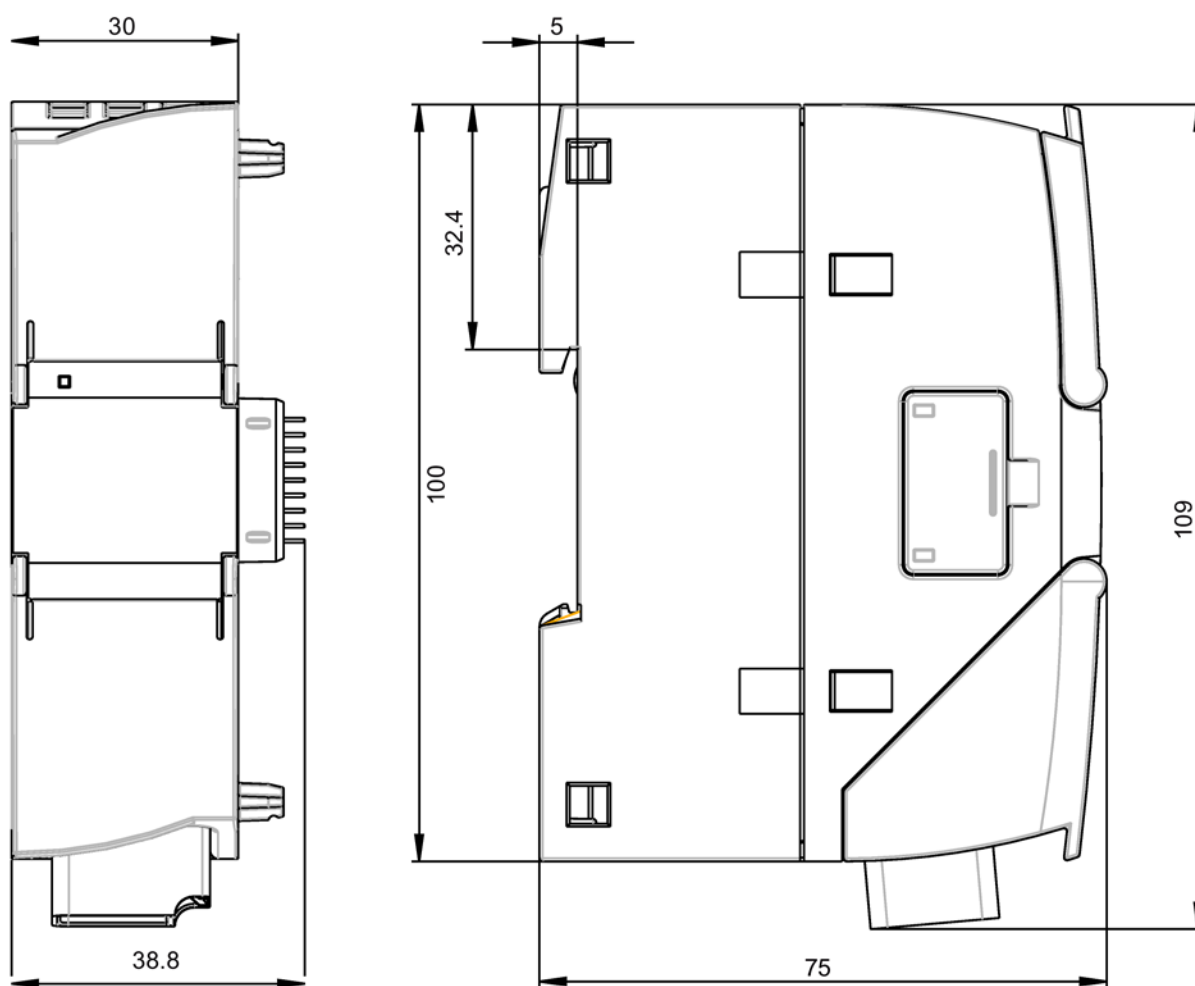


图 B-1 正视图与左侧视图



图 B-2 俯视图

参考文档

在哪里能找到Siemens文档

- 部件编号

可以在以下目录中找到 **Siemens** 相关产品的部件编号：

- SIMATIC NET - 工业通信/工业标识，目录 IK PI
- SIMATIC - 用于全集成自动化和小型自动化的产品，目录 ST 70

可以从 **Siemens** 代表处获得这些目录和其它信息。还可在 **Siemens Industry Mall** 的以下地址中找到相关产品信息：

链接：(<https://mall.industry.siemens.com>)

- Internet 上的手册

在 **Siemens** 工业在线支持的 **Internet** 页面中可找到 **SIMATIC NET** 手册：

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/15247/man>)

转到产品树中的所需产品并进行以下设置：

条目类型“手册”

- 数据介质上的手册

可以在 **SIMATIC NET** 产品随附的数据介质中找到相应的 **SIMATIC NET** 产品手册。

/1/

SIMATIC

S7-1200 可编程控制器

系统手册

Siemens AG

访问以下地址可获得当前版本：

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/13683/man>)

/2/

SIMATIC NET

CP 1243-1

操作说明

Siemens AG

链接: (<https://support.industry.siemens.com/cs/ww/zh/view/103948898>)

/3/

SIMATIC NET

TeleControl Server Basic (版本 V3)

操作说明

Siemens AG

链接: (<https://support.industry.siemens.com/cs/ww/zh/ps/15918/man>)

/4/

SIMATIC NET

Industrial Ethernet Security

安全基本知识和应用

组态手册

Siemens AG

链接: (<https://support.industry.siemens.com/cs/ww/zh/ps/15326/man>)

/5/

SIMATIC NET

SNMP 的诊断和组态

诊断手册

Siemens AG

链接: (<https://support.industry.siemens.com/cs/ww/zh/ps/15392/man>)

索引

C

CPU 固件, 26

D

DNP3 实现层, 74

DNP3 寻址, 47

DNP3 主站, 通过 Internet 寻址, 24

DNS 服务器, 47

DNS 服务器 - 程序控制的更改, 138

I

IEC 寻址, 47

Internet 连接, 47

IP 地址 - 程序控制的更改, 138

IP 地址 (主站), 47

IP 组态

IPv4, IPv6, 14

IP_CONF_V4, 138

IPsec 隧道: 数量, 19

M

MAC 地址, 3

MIB, 146

N

NTP, 48

NTP (secure), 49

NTP 服务器 - 程序控制的更改, 138

O

OPC quality code, 109

OUC (Open User Communication), 135

OUC 连接

资源, 18

P

PG/OP 连接, 18

PUT/GET, 18

S

S7 连接

启用, 52

资源, 18

Security, 15

SIMATIC NET 词汇表, 6

SMS

编程 (OUC), 135

SMTPS, 79

SNMP, 15, 61, 146

SNMPv3, 17, 81

SSL/TLS, 79

STARTTLS, 79

STEP 7 - 版本, 26

SYSLOG, 91

T

T_CONFIG, 138

TC_CONFIG, 138

TeleService, 15

V

VPN, 19, 47, 85

W

Web 服务器, 133

A

安全须知, 33

B

被动建立 VPN 连接, 90

部件编号, 3

C H

产品名称, 4

尺寸, 37

处置, 6

触发变量 - 复位, 115

传输模式, 115, 117

C

词汇表, 6

D

导入证书 - 电子邮件, 80

电子邮件

 编程 (OUC), 135

 数量, 19

 组态, 130

端口 8448, 143

F

发送缓冲区, 18, 113

防火墙, 16

服务和支持, 6

复位触发位, 115

G

更换模块, 152

固件版本, 3

过程映像, 113

H

回收, 6

J

记录服务器, 84

加密, 13

交叉引用 (PDF), 5

静态值, 113

镜像, 105

L

连接资源, 18

P

培训, 6

Q

强制映像模式, 113

R

冗余 DNP3 主站, 寻址, 25

S H

时间戳, 102

时钟同步, 14

事件, 113

数据点类型, 101

数据点组态, 93

数据缓冲, 18

说明 (OUC), 135

S

缩写/缩略语, 4

W

网关, 90

X

虚拟 IP 地址, 65

Y

以太网接口

分配, 155

映像存储器, 113

硬件产品版本, 3

有条件自发, 115, 117

运行状态 (LED 显示), 30

Z

在不打开端口 102 的情况下执行安全诊断, 143

在线功能, 15, 141

在线诊断, 52, 141

Z H

站间通信, 108

帧存储器, 18, 113

主动, 115, 117

