

## SIMATIC NET

### S7-1200 - TeleControl SIMATIC CP 1243-1

#### 操作说明

#### 前言

#### 应用和功能

**1**

#### LED 和连接器

**2**

#### 安装、接线、调试和拆卸

**3**

#### 组态

**4**

#### 程序块 (OUC)

**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 Siemens AG

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

### 责任免除

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

# 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**

订货号 6GK7 243-1BX30-0XE0

硬件版本 3

固件版本 V3.3

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。有关支持的遥控协议，请参见“CP 的属性 (页 13)”部分。

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 通信以太网接口。



图 1 CP 1243-1

在模块外壳铰接盖顶部的后方，可以看到在订货号右侧以占位符“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

本手册介绍此模块的属性，在您安装和调试设备时提供支持。

此外，还提供了操作说明以及设备诊断选项的相关信息。

#### 组态

必要的组态步骤以概述的形式进行介绍。

- **不使用遥控通信功能的 CP**

本手册中介绍了这些应用的相关组态步骤。

- **使用遥控通信功能的 CP**

有关这些应用的组态和诊断的完整说明，请参见相应的组态手册 /4/ (页 114)。

参见下文中“文档结构”部分的信息。

## 本版本新增内容

- 硬件版本 3
- 具有功能改进的固件版本 V3.3
- 新增认证 (CCC / UKEX)

### 限制：

按照协议 IEC 60870-5 进行遥控操作时，需遵守以下事项：

如果数值由两个设定值数据点几乎在同一时间发送，可能会忽略第二个设定值传输。两次设定值发送的间隔至少为 70 毫秒。

## 替换的手册版本

版本 12/2019

## Internet 上的最新版本手册

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>)

## 文档结构

CP 的文档包括以下手册和内容：

- **操作说明**
  - 应用和功能（不使用遥控功能）
  - 要求（CPU、组态软件等）
  - 硬件说明
  - 安装、接线、调试、操作
  - 组态

“组态”部分仅介绍了与遥控不相关的功能的组态。

如果使用遥控功能，请阅读相应的组态手册。
  - 诊断、维护
  - 技术规范、认证、附件

- **组态手册 TeleControl Basic**

在 STEP 7 Professional (TIA Portal) 下组态和诊断

适用于支持 TeleControl Basic 协议的所有 SIMATIC NET 通信模块。

- **DNP3 组态手册**

在 STEP 7 Professional (TIA Portal) 下组态和诊断

适用于支持 DNP3 协议的所有 SIMATIC NET 通信模块。

- **组态手册 IEC 60870-5**

在 STEP 7 Professional (TIA Portal) 下组态和诊断

适用于支持 IEC 60870-5-101/104 协议的所有 SIMATIC NET 通信模块。

可以在附录 参考文档 (页 113) 中找到手册的 Internet 链接。

## 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 系统
- SIMATIC STEP 7 Basic / Professional

## 有关本文档的说明

### 产品名称

- **CP / 模块 / 设备**

在本文档中，使用这些术语来表示产品全名 CP 1243-1。

### PDF 中的交叉引用

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

### 搜索

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

## 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。

---

您可在提供的数字介质中找到许可证条款：

- OSS\_CP1243x\_99.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。

## 固件/软件支持的说明

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

## 安全性信息

### Siemens

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

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

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

关于可采取的工业信息安全措施的更多信息，请访问

链接：<http://www.siemens.com/industrialsecurity>

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

要及时了解有关产品更新的信息，请订阅 Siemens 工业信息安全 RSS 源，网址为

链接：<https://www.siemens.com/cert>

## 设备故障

如果故障无法消除，请将设备送至西门子代表处进行维修。不提供现场维修服务。

## 解除调试

正确关闭设备，以防止未经授权的人员访问设备内存中的机密数据。

为此，需要恢复设备的出厂设置。

通过使用 STEP 7 的在线功能复位 CPU 来实现此操作。

## 回收和处置



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

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

请按照当地法规进行处理。

可在 Siemens 工业在线支持的 Internet 页面中找到产品的回收信息：

链接：<https://support.industry.siemens.com/cs/ww/zh/view/109479891>

## SIMATIC NET 词汇表

SIMATIC NET 词汇表描述了本文档中可能使用的术语。

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

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

## 培训、服务与支持

有关培训、服务和支持的信息，请参见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
<b>1 应用和功能 .....</b>	<b>13</b>
1.1 CP 的属性 .....	13
1.2 通信服务 .....	13
1.3 通过 SINEMA RC 通信 .....	15
1.4 其它服务和属性 .....	17
1.5 安全功能 .....	18
1.6 组态限制和性能数据 .....	21
1.7 组态示例 .....	24
1.8 使用要求 .....	26
1.8.1 硬件要求 .....	26
1.8.2 软件要求 .....	26
<b>2 LED 和连接器 .....</b>	<b>27</b>
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
<b>3 安装、接线、调试和拆卸 .....</b>	<b>33</b>
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 依据 ATEX / UKEX / IECEx / CCC-Ex 要求在危险区域使用的注意事项 .....	34
3.1.3 依据 UL HazLoc 和 FM 要求在危险区域使用的注意事项 .....	35
3.2 在危险区域安装、拆卸和维修 .....	35
3.3 安装、连接和调试 .....	37
3.4 操作注意事项 .....	42
3.5 拆卸 .....	42
<b>4 组态 .....</b>	<b>43</b>
4.1 安全建议 .....	43
4.2 STEP 7 中的组态 .....	47

4.3	通信类型 .....	48
4.4	时钟同步 .....	49
4.5	以太网接口 .....	53
4.5.1	以太网地址 .....	53
4.5.2	IPv6 .....	54
4.5.3	CP 标识 .....	54
4.5.4	时钟同步 .....	54
4.5.5	高级选项 .....	55
4.5.6	访问 Web 服务器 .....	55
4.6	伙伴站 .....	55
4.7	DNS 组态 .....	56
4.8	与 CPU 通信 .....	56
4.8.1	与 CPU 通信 .....	56
4.8.2	CP 诊断 .....	57
4.9	SNMP .....	59
4.10	安全性 .....	60
4.10.1	安全用户 .....	60
4.10.2	参数概述 .....	60
4.10.3	防火墙 .....	61
4.10.3.1	MAC 防火墙预检查消息。 .....	61
4.10.3.2	源 IP 地址的表示法（高级防火墙模式） .....	62
4.10.3.3	已组态 VPN 隧道连接的防火墙设置 .....	62
4.10.3.4	防火墙激活情况下的在线安全诊断和下载到站设置 .....	62
4.10.4	电子邮件组态 .....	63
4.10.5	日志设置 - 过滤系统事件 .....	65
4.10.6	SNMP .....	65
4.10.7	VPN .....	67
4.10.7.1	VPN (Virtual Private Network) .....	67
4.10.7.2	为各站间的 S7 通信创建 VPN 通道 .....	68
4.10.7.3	SOFTNET 安全客户端的 VPN 通信（工程师站） .....	70
4.10.7.4	在 CP 和 SCALANCE M 之间建立 VPN 隧道通信 .....	71
4.10.7.5	CP 作为 VPN 连接的被动用户 .....	71
4.10.7.6	SYSLOG .....	72
4.10.7.7	SINEMA Remote Connect .....	72
4.10.8	证书管理器 .....	75
4.10.9	处理证书 .....	75
4.11	数据点 .....	78
4.12	消息 .....	78
4.13	用于用户名、密码和消息的字符集 .....	84
5	程序块 (OUC) .....	85

5.1	用于 OUC 的程序块.....	85
5.2	在运行期间更改 IP 地址 .....	88
<b>6</b>	<b>诊断和保养 .....</b>	<b>91</b>
6.1	诊断选项 .....	91
6.2	Web 服务器 S7-1200：连接建立 .....	94
6.3	通过端口 8448 执行在线安全诊断 .....	96
6.4	SNMP .....	96
6.5	电子邮件的处理状态 .....	98
6.6	下载固件 .....	100
6.7	模块更换 .....	101
<b>7</b>	<b>技术数据 .....</b>	<b>103</b>
7.1	CP 1243-1 的技术规范 .....	103
7.2	以太网接口的引脚分配 .....	104
<b>A</b>	<b>认证 .....</b>	<b>105</b>
<b>B</b>	<b>尺寸图 .....</b>	<b>111</b>
<b>C</b>	<b>参考文档 .....</b>	<b>113</b>
	索引 .....	117



# 应用和功能

## 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

CP 也可用作 CPU 的接口扩展。在此角色中，它用于实现网络分离。

利用不同安全功能（如防火墙和数据加密协议）的组合，CP 可保护站甚至整个自动化单元免受未经授权的访问。并可保护站和通信伙伴之间的通信免受窃取和篡改。

## 1.2 通信服务

### 遥控通信

支持以下应用：

- **与控制中心的通信**

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 可以与冗余控制中心进行通信。

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 18) 部分。

- **站间通信**

通过主站实现站间通信 (TeleControl Basic)

在此应用中，CP

将通过移动无线网络建立与遥控服务器的连接。遥控服务器会将帧转发到目标站。

- **直接通信**

以下应用中，可实现站间直接通信：

- Open User Communication （通过程序块）
- 采用 DNP3 和 IEC 协议时，在为接口启用“主站功能”(Master function) 的情况下

## 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。

此功能在 STEP 7 中组态。无需使用程序块。

有关要求与功能，请参见电子邮件组态 (页 63)部分。

## 通过 SINEMA Remote Connect 通信

支持 V3.1 及以上固件版本。请参见通过 SINEMA RC 通信 (页 15)部分。

## S7 通信和 PG/OP 通信

如果在 CP 的组态中启用了 S7 通信，则可从 CPU 中读取数据或将数据写入 CPU 中。

CP 支持以下功能：

- **PUT/GET**

CP 支持客户端（程序块）和服务器形式的功能，用于与远程站 (S7-300/400/1200/1500) 进行数据交换。

有关程序块的详细信息，请参见 STEP 7 的信息系统。

- **PG 功能**

- **操作员监控功能 (HMI)**

- **S7 路由**

CP V2.1 及以上固件版本 (CPU ≥ V4.2)

对于 S7 通信，CP 需具备固定的 IP 地址。

## 通过 Open User Communication (OUC) 通信

通过 CP 的以太网接口和 CPU 上 Open User Communication 的程序块，CP 具有下列通信选项：

- 与 SIMATIC 站通信
- 发送电子邮件

与遥控通信的对应服务（见上文）不同，若要通过 OUC 传送电子邮件，则需要使用 TMAIL\_C 程序块，请参见用于 OUC 的程序块 (页 85)部分。

## 1.3 通过 SINEMA RC 通信

### 通过 SINEMA Remote Connect (SINEMA RC) 通信

“SINEMA RC Server”应用程序通过 Internet 为分布式网络提供端到端连接管理。其中也包括对下级站点的安全远程访问。考虑到已存储的访问权限，SINEMA RC 服务器和远程设备之间的通信通过 VPN 隧道进行。

SINEMA RC 使用 OpenVPN 对数据加密。通信中心为 SINEMA RC 服务器，通过该服务器可实现用户间的通信及管理通信系统的组态。

SCALANCE M 路由器可用于连接用途，并且也支持 OpenVPN 和 SINEMA Remote Connect 的连接。

有关通过 SINEMA RC 进行通信所需的 CP 固件版本信息，请参见通信服务 (页 13)部分。

### 参数组

若要通过 SINEMA RC 通信以及通过 SINEMA RC 遥控通信，可在以下两个参数组中进行组态：

- 通过 SINEMA RC 通信：
  - > “安全 > VPN”(Security > VPN)
- 通过 SINEMA RC 遥控通信：
  - > “通信类型”(Communication types)

有关组态的信息，请参见遥控组态手册 I/4/ (页 114)。

## 应用

根据遥控通信参数和 SINEMA RC 参数的不同组合，有以下几种应用选项：

应用示例：

- (1) 没有遥控通信且没有 SINEMA RC （CP 无法连接网络）
- (2) CP 仅通过 SINEMA RC 进行远程维护
- (3) CP 仅进行遥控通信
- (4) CP 使用遥控通信，但 SINEMA RC 仅进行远程维护
- (5) CP 使用 SINEMA RC 进行遥控通信和远程维护。

下表提供了不同参数设置下的应用概览。

- “开”表示参数处于激活状态。
- “关”表示参数处于未激活状态。

表格 1-1 使用实例和待激活参数

使用实例	参数设置 (参数缩写) *		
	SRC	TC	TC-SRC
(1)	关	关	关
(2)	开	关	关
(3)	关	开	关
(4)	开	开	关
(5)	开	开	开

\* 参数缩写的说明：

**SRC** - 安全 > VPN（已激活）>“VPN 连接类型”：

“通过 SINEMA Remote Connect 服务器自动进行 OpenVPN 组态”

**TC** - 通信类型 > 已启用遥控通信

**TC-SRC** - 通信类型 >

“通过 SINEMA Remote Connect 激活遥控通信”



## 1.4 其它服务和属性

### 其它服务和属性

- **IP 组态 - IPv4 和 IPv6**

- IPv4 / IPv6

CP 支持符合 IPv4 和 IPv6 的 IP 地址。

在 IPv6 网络中，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 支持多种同步时钟方法。相关信息，请参见时钟同步 (页 49)部分。

- **在线功能**

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，请参见诊断选项 (页 91)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 96)部分。

### 遥控模式下的其它属性

- **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序块。控制系统会一对一地处理各个数据点。

- **发送缓冲区**

CP 将组态为事件的数据点的值保存在发送缓冲区中。

数据不会进行永久性保存，停电时会丢失。

- **过程数据的事件驱动型传输**

CP

将数据从发送缓冲区单独（自发地）或捆绑发送到通信伙伴。传输操作可由各种触发器触发。

- **模拟值处理**

在 CP 中可以按各种方法预处理模拟值。

## 1.5 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“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 STEP 7 中的 CP 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
  - 限制传输速度以限制通信过量和 DoS 攻击（“定义 IP 数据包过滤规则”）
  - 全局防火墙规则

- **VPN**

可使用以下备选方法：

- 通过 IPsec 隧道进行安全通信

利用 VPN 通信，可与一个或多个安全模块建立安全的 IPsec 隧道通信。在组态过程中，可将 CP 与其它模块组合在一起，以构成 VPN 组。在一个 VPN 组的所有安全模块之间创建 IPsec 隧道。

- 通过 SINEMA Remote Connect 进行远程维护

通过 SINEMA RC 服务器进行通信时无需创建 VPN 组，而且实际上也无法创建。SINEMA RC 服务器管理设备和安全装置 (OpenVPN) 之间的通信。

- **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 43) 部分。

---

有关在运行期间更改 IP 地址，请参见安全性 (页 60) 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。

## 1.6 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。

### 连接资源

- **S7 连接和 TCP/UDP/ISO-on-TCP 连接**

工业以太网上的连接总数：最多 14 个

其中：

- S7：最多 14 个（包括用于 S7 路由的连接）
- TCP/IP：最多 14 个
- ISO-on-TCP：最多 14 个
- UDP：最多 14 个

此外：

- **遥控连接**

CP 可通过多种遥控协议与以下伙伴建立连接：

**TeleControl Basic**

- 非冗余或冗余遥控服务器 (TCSB)。
- 其它站间通信

通过远程控制服务器在两个站的 CP 之间建立站间通信。该通信在“伙伴站 > 站间通信的伙伴”参数组中进行组态。

站间通信的组态限制，共计最多 15 个，其中：

- 发送到伙伴：最多 3 个（“发送缓冲区”(Send buffer) 参数已启用）
- 从伙伴接收：最多 15 个（“发送缓冲区”(Send buffer) 参数已禁用）

#### **DNP3 / IEC 60870-5**

- 最多可与 4 个伙伴进行通信

伙伴可以是一个单独或冗余主机，也可以是一个工作站（直接通信）。

可通过遥控连接在各站之间进行直接通信。

- **在线连接**

与工程师站 (STEP 7) 建立一个在线连接需使占用两个资源

- **编程设备和 HMI 连接 (OP)**

总数最多为 4 个，其中：

- 编程设备连接的资源：最多 1 个
- HMI 连接的资源：最多 3 个

#### **可进行数据点组态的数据点数量**

可组态数据点的最大数量

- TeleControl Basic: 200
- DNP3：500
- IEC：500

#### **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（参见“数据点类型”）。

#### **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要发送至通信伙伴的值。

发送缓冲区的最大大小如下：

- TeleControl Basic：64 000 个事件
- DNP3：100 000 个结果
- IEC：100 000 个结果

发送缓冲区的容量将均分给所有已组态的通信伙伴。帧存储器的大小可在 STEP 7 中进行设置（“与 CPU 进行通信”(Communication with the CPU) 参数组）。

### 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 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”)

1.7 组态示例

有关遥控应用的组态示例，请参见组态手册 /4/ (页 114)。

用于实现安全网络分离的 CP 组态

以下示例显示了用于保护站和下级自动化单元的 CP 1243-1 组态。

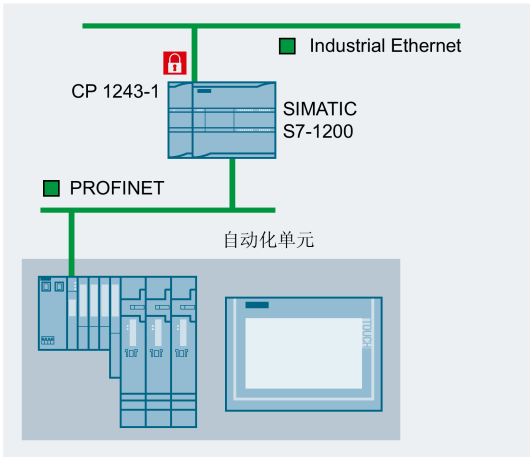


图 1-1 采用 CP 1243-1 的安全通信

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。

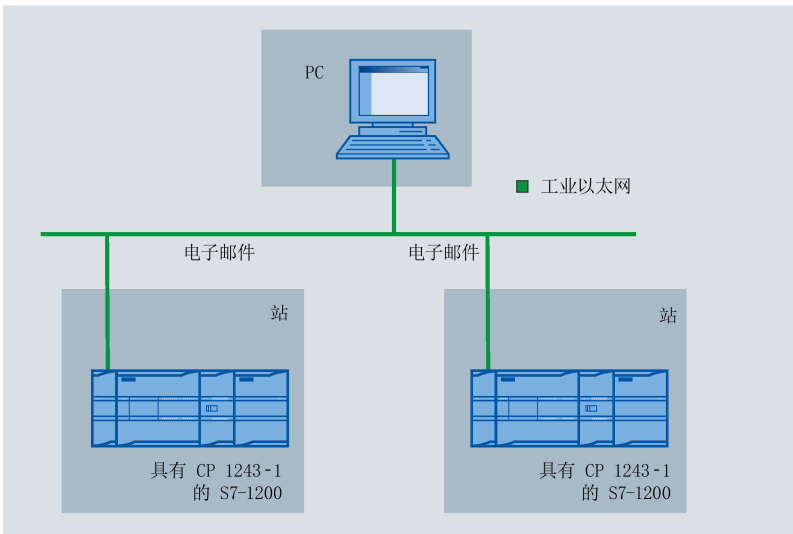


图 1-2 发送电子邮件



## 使用 SINEMA RC 进行远程维护

下图显示了各种具有安全 CP 的工作站通过 SINEMA Remote Connect - Server 与工程站的连接。

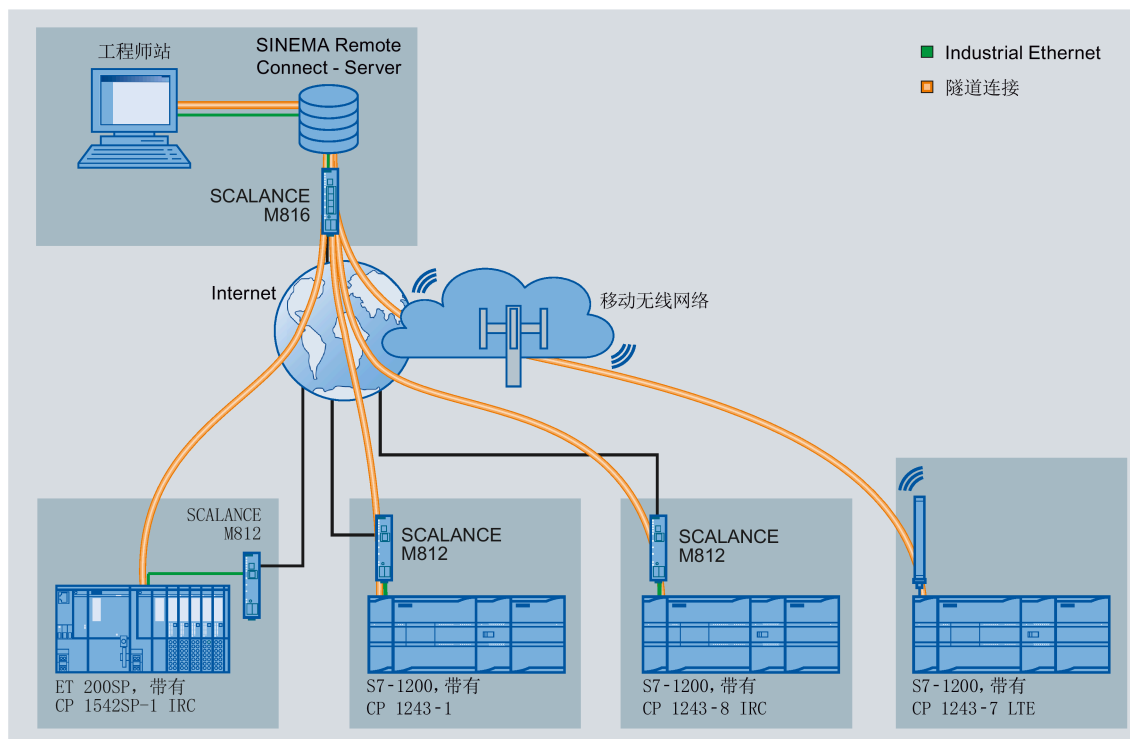


图 1-3 各工作站通过 SINEMA RC 与工程师站的连接

## 1.8 使用要求

### 1.8.1 硬件要求

#### CPU 1200

S7-1200 需使用以下硬件：

- CP  
固件版本 V3.3 的要求是使用硬件版本为 2 的 CP。
- CPU
  - 固件版本不高于 V2.1（硬件版本 1）的 CP 兼容固件版本不高于 V3.0 的 CPU。
  - 固件版本不高于 V3.0（硬件版本 2）的 CP 兼容版本不低于 V4.1 的 CPU。
  - CPU 版本不低于 V4.4 时，才能实现固件版本为 V3.3 的 CP 的所有功能。

### 1.8.2 软件要求

#### 用于实现组态和在线功能的软件

要组态模块，需要具备以下组态工具：

- 对于固件版本为 V3.2 的 CP：  
STEP 7 Basic V16
- 要使用固件版本 V3.3 的全部功能：  
STEP 7 Basic V17

## 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。

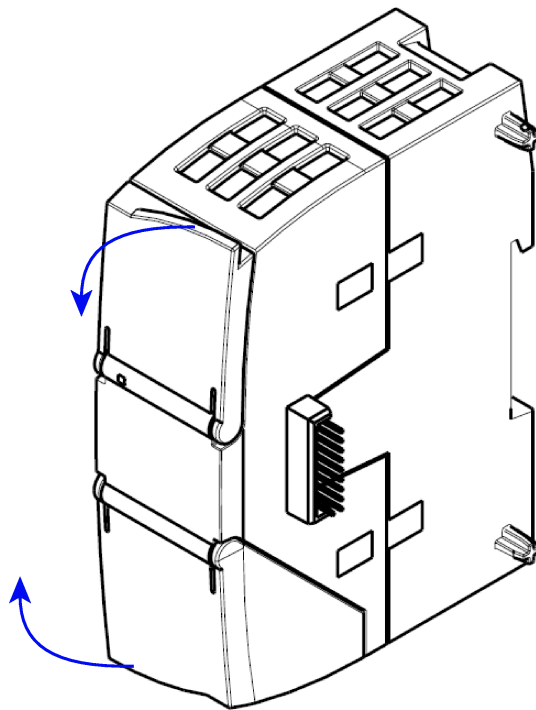


图 2-1 打开外壳盖

## 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)	<b>DIAG</b>	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)	<b>LINK</b>	与工业以太网的连接状态
 (绿色)	<b>CONNECT</b>	与通信伙伴的连接状态
 (绿色)	<b>VPN</b>	VPN 或 SINEMA Remote Connect 组态的状态
 (绿色)	<b>SERVICE</b>	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)
<b>CP 的基本状态</b>	
	<ul style="list-style-type: none"> <li>断电</li> <li>启动错误</li> </ul>
 绿色	正在运行 (RUN)，无严重错误
 绿色闪烁	<ul style="list-style-type: none"> <li>伙伴未连接</li> <li>加载固件成功</li> </ul>
 红色闪烁	<ul style="list-style-type: none"> <li>正在启动</li> <li>模块故障</li> <li>STEP 7 项目数据无效</li> </ul>
 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)
<b>模块启动 (STOP → RUN) 或错误状态</b>						
						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		-		-	-	STEP 7 项目数据无效
 红色闪烁		-		-	-	缺少 STEP 7 项目数据
 红色闪烁				-	-	背板总线错误
<b>与工业以太网的连接</b>						
-			-	-	-	存在与工业以太网的连接
 绿色			-	-	-	<ul style="list-style-type: none"> <li>正在建立与工业以太网的连接。</li> <li>正在获取 IP 地址。</li> </ul>
-			-	-	-	与工业以太网无连接
<b>与通信伙伴的连接</b>						
 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
<b>用于实现在线功能的连接</b>						
 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
<b>VPN/SINEMA Remote Connect 连接</b>						
 绿色			-		-	已建立 VPN/SINEMA Remote Connect 连接
 绿色闪烁			-	 绿色闪烁	-	尝试建立已组态的 VPN/SINEMA Remote Connect 连接
-		-	-		-	尚未在 CP 上组态或建立 VPN/SINEMA Remote Connect 连接
<b>正在加载固件</b>						
						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 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 103)部分。



## 安装、接线、调试和拆卸

### 有关设备使用的安全须知

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

### 3.1 使用设备的重要注意事项

#### 过压保护

##### 注意

##### 外部电源的保护

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。

外部电源的连接器的连接器无法抵御强电磁脉冲。

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。

制造商：

DEHN+SOEHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt, Germany

#### 3.1.1 有关在危险场所使用的注意事项



##### 警告

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

### 3.1 使用设备的重要注意事项



#### 警告

##### 爆炸危险

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

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



#### 警告

##### 机柜要求

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



#### 警告

##### 适用于危险区域中高环境温度的电缆

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



#### 警告

如果电缆或导线入口的温度超过  $70^{\circ}\text{C}$ ，或者导线分支点超过  $80^{\circ}\text{C}$ ，必须采取专门的预防措施。如果设备要在环境温度超过  $60^{\circ}\text{C}$  的情况下工作，则只能使用允许的最高工作温度至少为  $80^{\circ}\text{C}$  的电缆。



#### 警告

##### 瞬态过电压

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

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

此设备仅适合在 I 类，2 分区，A、B、C 和 D 组或无危险位置使用。

此设备仅适合在 I 类，2 区，IIC 组或无危险位置使用。



**警告**

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



**警告**

如果将设备安装在机柜中，则机柜的内部温度与设备的环境温度要相对应。



**警告**

#### 爆炸危险

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

## 3.2 在危险区域安装、拆卸和维修



**警告**

#### 附件和备件不允许使用

危险区域中的爆炸风险

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

### 3.2 在危险区域安装、拆卸和维修



#### 警告

##### 电缆或连接器不适用

危险区域中的爆炸风险

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



#### 警告

##### 屏蔽电缆安装不当

存在因危险区域与非危险区域之间的均衡电流而引发爆炸的风险。

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



#### 警告

##### 缺少等电位联结

如果危险区域中没有等电位联结，则存在因均衡电流或点火火花引发爆炸的风险。

- 确保为设备提供等电位联结。



#### 警告

##### 电缆头未受保护

存在因危险区域中的电缆头未受保护而引发爆炸的风险。

- 按照 IEC/EN 60079-14 的规定对未使用的电缆头进行保护。

**警告****本安电路和非本安电路未充分隔离**

危险区域中的爆炸风险

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

**警告****未授权对采用防爆设计的设备进行维修**

危险区域中的爆炸风险

- 仅可由获得西门子授权的人员执行维修工作。

### 3.3 安装、连接和调试

**注意****安装不当**

安装不当可能导致设备损坏或危害设备操作。

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

### 3.3 安装、连接和调试



#### 警告

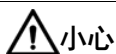
#### 开放式设备

该设备为“open equipment”，符合标准 IEC 61010-2-201 或 UL 61010-2-201 / CSA C22.2

No. 61010-2-201。为符合关于机械稳定性、阻燃性、稳定性以及防接触保护的安全操作要求，下面指定了可选择的安装类型：

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

### 安装和调试之前



#### 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

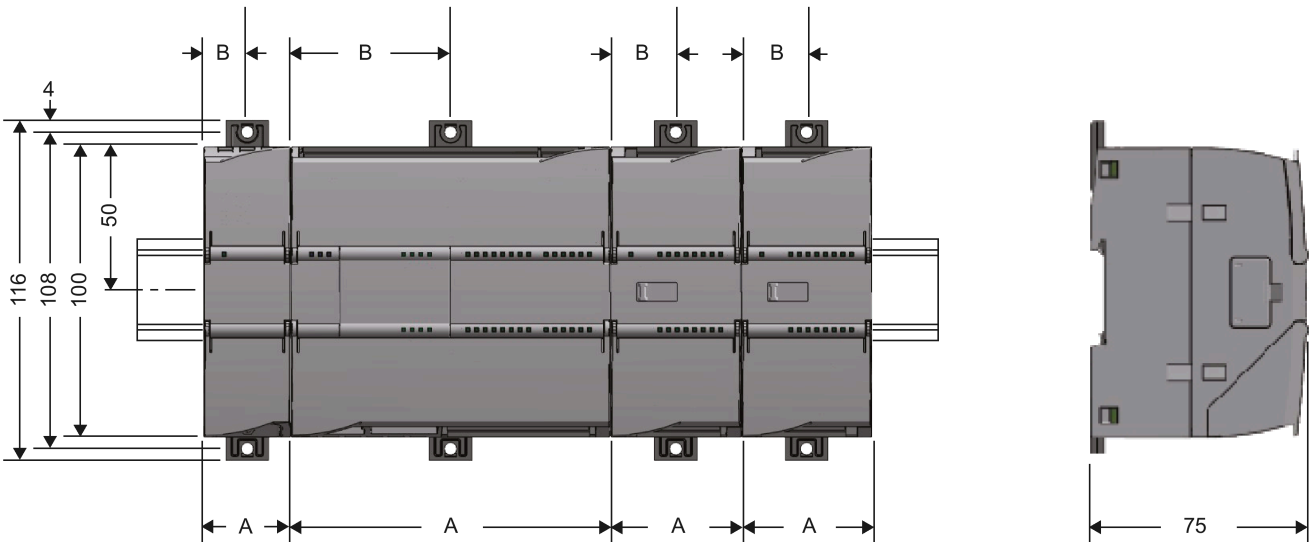


图 3-1 S7-1200 的安装尺寸

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 111)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。

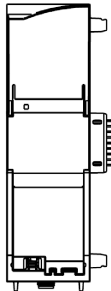
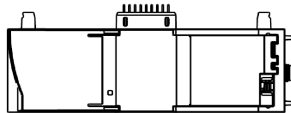
## 安装位置

### 注意

#### 安装位置

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。

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 103) 部分介绍了允许的温度范围。

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：	

### 警告

#### 电源

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

因此，电源需要满足至少以下条件之一：

- 只可将符合 IEC 60950-1/EN 60950-1/VDE 0805-1 或 IEC 62368-1/EN 62368-1/VDE 62368-1 的由受限电源 (LPS) 提供的安全超低电压 (SELV) 连接到电源端子上。
- 按照美国国家电气法规 (ANSI/NFPA 70)，设备的供电装置必须符合 NEC 2 类要求。如果设备连接有一个冗余电源（两个独立的电源），则两个电源都必须满足这些要求。

## 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 103)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"> <li>“加载项目数据”</li> <li>“使用在线和诊断功能”</li> </ul>

## 调试期间手动设置时钟

### 说明

#### 使用 Security/SINEMA RC 时的时钟同步

使用安全功能（例如 SINEMA Remote Connect）时，CP 需要当前时间以在伙伴或 SINEMA RC 服务器上进行验证。

首次建立连接之前，CP 会从 CPU 或 NTP 服务器接收时间。

#### 建议：

在调试期间，至少使用 STEP 7 在线功能手动设置一次 CPU 时间。如果已经为时间同步组态了“伙伴时间”(Time from partner)选项，这一点尤为重要。这样，可以确保站启动时 CPU 的时钟是有效的，并且 CP 可以与伙伴或 SINEMA RC 服务器交换所需的证书。

### 3.4 操作注意事项

## 3.4 操作注意事项

#### 注意

##### 合上前面板

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。

## 3.5 拆卸



#### 警告

##### 拆卸不当

拆卸不当可能导致危险区域中出现爆炸风险。

要正确拆卸，请遵循以下规则：

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

## 拆卸

1. 断开电源前，请先拔掉数据电缆的连接器，从而断开设备的接地。
2. 关闭工作站的电源。
3. 使用一字螺丝刀将设备背面的两个 DIN 导轨下方卡件拆下，使其卡入扩展位置。  
这将释放锁紧机构。
4. 将设备从 DIN 导轨侧面旋至前面。

## 组态

### 4.1 安全建议

请遵循以下安全建议，以免系统受到未授权访问。

启用遥控通信后，还应参考相关组态手册中的信息。

#### 常规

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

有关产品新闻和新固件版本的信息，请访问以下地址：  
链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/21764/dl>)

#### 物理访问

应将该设备限制为仅允许合格人员进行物理访问。

#### 网络连接

请勿将 PC 直接连接到 Internet。如需将 CP 连接到 Internet，则要对 CP 进行适当的保护，例如使用带防火墙的 SCALANCE S，或者使用 CP。

## 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

相关信息，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。在防火墙中通过 IP 数据包过滤规则限制“传输速度”，可以限制通信过量和 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。

- 将对 CPU 的 Web 服务器的访问保持禁用状态。

- 保护访问程序块的密码

防止存储在数据库的程序块的密码被查看。有关 STEP 7 信息系统中程序的信息，请参见关键词“专有技术保护”下的内容。

- 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。

## 4.1 安全建议

- 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	20000 (TCP/UDP) 可设置	关闭	组态后打开	是，已启用 Secure Authentication 时。
IEC	2404 (TCP) 可设置	关闭	打开	否
S7 和在线连接	102 (TCP)	关闭	组态后打开 *	否
在线安全诊断 (若受支持)	102 (TCP)	打开	组态后打开 *	否
通过 SINEMA RC 通信（若受支持）	443 (TCP)	关闭	组态后打开	是
HTTP	80 (TCP)	关闭	组态后打开	是
HTTPS	443 (TCP)	关闭	组态后打开	是
SNMP（若受支持）	161 (UDP)	打开	组态后打开	是（带 SNMPv3）
Syslog	514 (UDP)	关闭	组态后打开	否

\* 一些服务提供商认为开放的端口 102 是一个安全漏洞。

为避免在线诊断期间开放端口 102，请参见“通过端口 8448 执行在线安全诊断 (页 96)”部分。

## 通信伙伴和路由器的端口

确保在相应的防火墙中启用了通信伙伴和中介路由器所需的客户端端口。

这些端口包括（如果使用并受支持）：

- TeleControl Basic / 55097 (TCP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- NTP / 123 (UDP)

- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- SINEMA RC 自动组态 / 443 (TCP) - 可以设置
- SINEMA RC 和 OpenVPN / 1194 (UDP) - 可以在 SINEMA RC 中设置
- IPSec / 500 (TCP) / 4500 (UDP)
- Syslog / 514 (UDP)

## 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。

每个站最多可组态三个 CM/CP。

以下内容适用于不使用遥控通信功能的应用。

### 遥控通信组态

有关组态遥控通信的描述，请参见组态手册 /4/ (页 114)。

### STEP 7 中的组态步骤概述

组态时按照以下步骤操作：

1. 创建 STEP 7 项目。
2. 使用所需的模块和 CP 创建必备的 SIMATIC 站。
3. 创建以太网网络。
4. 将站连接到以太网子网。
5. 组态包括消息（电子邮件）的 CP。
6. 如有需要，可为 S7 通信和 Open User Communication 创建程序块，并根据需要对这些程序块进行组态。

7. 保存并编译项目。

8. 将项目数据下载到站中。

使用“下载到设备”(Download to device) 功能，可将包含 CP 组态数据的 STEP 7 项目数据下载至相关 CPU 中。

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 通信类型

### “通信类型”(Communication types) 参数组

在此参数组中，可以启用 CP 的通信服务。

为最大程度降低未经授权的用户访问工作站的风险，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。

- **启用遥控通信**

在 CP 上启用遥控通信。

通过下拉列表“协议类型”(Protocol type) 选择遥控协议。

- TeleControl Basic
- DNP3
- IEC 60870-5

请注意，如果之后更改遥控协议，将会删除所有协议特定数据。其中包括数据点和伙伴信息。

更多信息，请参见组态手册 /4/ (页 114)。



- **通过 SINEMA Remote Connect 激活遥控通信**

通过 SINEMA RS 在 CP 中启用通信。

有关 SINEMA Remote Connect 的应用案例以及这些应用的组态说明，请参见“SINEMA Remote Connect (页 72)”部分。

更多信息，请参见组态手册 I/4/ (页 114)。

有关 SINEMA Remote Connect - Server 手册的 I/6/ (页 115)。

- **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**

启用工程师站与工作站 CPU 之间的 S7 通信功能以及 S7 路由。

如果组态与该站之间的 S7

连接，并且通过通信模块来运行这些连接，则需要为通信模块启用该选项。

**请注意：**

禁用此功能意味着不会采取任何安全措施。为了保护工作站，请使用适当的安全功能，如防火墙、VPN 或 CPU 密码保护等。

无需启用 Open User Communication，因为随后需要创建相关程序块。因此无法对 CP 进行意外访问。

## 4.4 时钟同步

---

### 说明

#### 使用 SINEMA RC 时的时钟同步

如果 CP 从 CPU 获取时间，则使用 SINEMA Remote Connect 时可在调试期间手动设置 CPU 时间；请参见“安装、连接和调试 (页 37)”部分中的说明。

---

---

**说明****CP 的时钟同步**

对于需要时钟同步的应用，您需要定期同步 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。这会尽可能缩小内部时间和 UTC 时间的偏差。

---

**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。

---

**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。

---

对于 S7-1200，不会将时钟从站转发至子网。

**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**

安全功能启用后可在此进行组态。

## 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

## CP 的同步方法

CP 支持以下同步时钟的方法：

- **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)**

安全功能启用后，可使用 NTP (secure) 方法。该方法使用对称密钥进行验证。各种可组态的散列算法可用于完整性检查。

可以在全局设置中，创建和管理 NTP (secure) 类型的 NTP 服务器。

在 CP 上指定使用的服务器。

- **从 CPU 获取时间**

自 V4.2 起, CPU 可以 10 秒为同步周期同步站的所有 CM/CP。

CPU 的参数:

如果启用了“CPU 同步设备的模块”(CPU synchronizes the modules of the device)

选项, 则可使站的所有遥控 CP (固件版本  $\geq$  V2.1.77) 以 10 秒为同步周期开始与 CPU 时间进行同步。

- **未组态时钟同步**

如果未在 CP 上组态时间同步, 则可在以下条件下同步 CP 的时间:

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 CM/CP 将与 CPU 时间进行同步。

- **从伙伴获取时间**

启用遥控通信后: CP 采用通信伙伴的时钟。

相关说明, 请参见组态手册 I/4/ (页 114)。

## 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:

- 使用 PLC 变量将 CP 时间转发至 CPU
  - 通过背板总线将 CP 时间转发至 CPU
-

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 < V3**

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 ≥ V3.0 和 CPU 固件 ≥ V4.2**

如果站中的两个模块均具备上述固件版本之一，会将 CP 的时间自动转发给 CPU。

此操作的条件为：在“PROFINET 接口 > 时钟同步”(PROFINET Interface > Time-of-day synchronization) 下为 CPU 选择了“CPU 同步设备的模块”(CPU synchronizes the modules of the device) 选项。

随后，站的所有智能模块将与 CPU 时间进行同步。

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。

## 4.5 以太网接口

### 4.5.1 以太网地址

#### 以太网地址

在以下参数组中，将以太网接口联网并组态 IP 地址参数。

**请注意：**

以下应用需要使用固定 IP 地址 (IPv4/IPv6)：

- 使用 S7 通信时
- 通过 Open User Communication 接收数据时
- 使用 VPN 时
- 使用 SINEMA Remote Connect 时

可以在参数组中的“高级选项 > 端口 [Xn P1]”(Advanced options > Port [Xn P1]) 下组态端口互连和传输特性。

更多相关信息，请参见 STEP 7 信息系统。

## 4.5 以太网接口

### 4.5.2 IPv6

#### 手动组态 IPv6 地址

如果组态其它 IPv6 地址（“手动组态”(Manual configuration) 选项），请确保两个 IPv6 地址分属不同的子网。

有关组态的信息，请参见 STEP 7 信息系统。

#### 通信伙伴和 IPv6

---

##### 说明

##### 通过 IPv6 进行 Internet 通信

如果要使用 IPv6 地址并将 CP 连接到 Internet，请确保已连接到 Internet 的路由器和所用 Internet 服务（例如，电子邮件）的提供商也支持 IPv6 地址。

##### 通过 IPv6 进行 OUC 通信

使用 Open User Communication 块并激活 IPv6 时，应确保通信伙伴支持 IPv6。如果对 DNS 服务器进行查询，则返回的地址首先使用 IPv6 地址，然后再使用 IPv4 地址。

---

### 4.5.3 CP 标识

只有启用遥控通信后，此参数组才可用。更多信息，请参见组态手册 /4/ (页 114)。

### 4.5.4 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 49)部分。

## 4.5.5 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。

- **TCP 连接监视时间**

功能：如果 TCP

连接监视期间无数据通信，则通信模块会向通信伙伴发送保持连接帧，并且应在 TCP 保持连接监视时间内获得响应。

默认设置：180 s。允许的范围：1...65535 s

- **TCP 保持连接超时**

通信模块发送保持连接帧后，应在保持连接监视时间内收到通信伙伴的响应。如果模块在组态时间内未收到响应，其将关闭连接并尝试重新建立连接。

默认设置：10 s。允许的范围：1...65535 s

### 传输设置

仅当启用了遥控通信后，协议特定的传输设置才可见。更多信息，请参见组态手册 /4/ (页 114)。

## 4.5.6 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。

可通过 PC 基于 LAN 访问站的 Web 服务器。

有关 Web 服务器的信息，请参见手册 /1/ (页 113)。

组态手册 /4/ (页 114) 中介绍了使用 TeleControl Basic 时访问 Web 服务器的特性。

有关 S7-1200 的 Web 服务器的信息，请参见手册 《/1/ (页 113)》。

## 4.6 伙伴站

只有启用遥控通信后，此参数组才会显示出来。

## 4.7 DNS 组态

### DNS 服务器

当模块、通信伙伴、NTP 或电子邮件服务器等应通过主机名称 (FQDN) 访问时，可能需要 DNS 服务器。

以 FQDN 方式寻址通信伙伴时，需要组态 DNS 服务器。随后通过组态的 DNS 服务器确定通信伙伴的 IP 地址 (IPv4/IPv6)。

使用 IPv6 地址时，请务必对 DNS 服务器进行相应组态。

## 4.8 与 CPU 通信

### 4.8.1 与 CPU 通信

#### 与 CPU 通信

前四个参数只与遥控通信有关。

#### 看门狗位

- CP 监视

CP 通过看门狗位检查与 CPU 的连接。

CP 每 5 秒将该位向 CPU 传送一次，然后在下一个 CPU 采样周期内将其复位。发生连接故障时不会传送该位。这将向 CPU 发出连接故障信号。

看门狗位的 PLC 变量必须由用户程序进行评估。



## CP 时间

- **CP 时间同步到 CPU**

通过该功能，CPU 可读取 CP 的时钟。使用此方法，CP 可与 CPU 时间同步。

步骤：

- CPU 通过用户程序将输入“时间触发变量”(Time trigger variable) (BOOL) 设为 1。
- 然后，CP 将其时间写入“CP 时间变量”(CP time variable) (DTL) 并将“时间触发变量”(Time trigger variable) 值复位为 0。
- 用户程序读取“CP 时间变量”(CP time variable) 以设置 CPU 时间。

建议：

设置“时间触发变量”(Time trigger variable)

的频率不得超过每秒一次，以避免在背板总线上产生不必要的通信负载。

---

### 说明

请参见时钟同步 (页 49)部分中的信息。

---

## 4.8.2 CP 诊断

固件版本为 V3 及以上版本的 CP 支持这些功能。

### CP 诊断

在“CP 诊断”(CP diagnostics) 参数组中，可选择使用 PLC 变量为 CPU 提供 CP 的高级诊断数据。

可以通过 CPU 的 Web 服务器显示 PLC 变量的状态。

- **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 将更新以下用于高级诊断的 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**

触发器的设置频率不应超过每秒一次。

---

根据 CP 类型和支持的功能，可为以下诊断数据组态 PLC 变量：

- **帧存储器溢出警告**

- 只与遥控通信有关 -

- **帧存储器占用率**

- 只与遥控通信有关 -

- **当前 IP 地址**

用于表示 CP 接口的当前 IP 地址的 PLC 变量（字符串数据类型）。

- **最后一次成功登录 TCSB 的日期**

- 只与遥控通信有关 -

- **最后一次未成功登录 TCSB 的日期**

- 只与遥控通信有关 -

- **TeleService 状态**

- 只与遥控通信有关 -

- **VPN IPsec 状态**

PLC 变量 (BOOL) 指示是否已建立 VPN IPsec 隧道：

– 0 = 未建立隧道

– 1 = 已建立隧道

- **连接到 SINEMA Remote Connect**

PLC 变量 (BOOL) 指示到 SINEMA RC 的 OpenVPN 隧道是否已建立：

– 0 = 未建立隧道

– 1 = 已建立隧道

## 4.9 SNMP

### SNMP

CP 支持以下 SNMP 版本：

- **SNMPv1**

启用和禁用安全功能时均可用

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。

在默认设置中，CP 使用以下团体字符串验证通过 SNMPv1 对其 SNMP 代理进行的访问：

访问 CP 中的 SNMP 代理	在 SNMPv1 中用于身份验证的团体字符串*)
读访问	public
读和写访问	private

\*) 注意使用小写字母！

#### 说明

##### 访问的安全性

出于安全原因，更改预设置和众所周知的字符串 "public" 和 "private"。  
如果启用安全功能，则可以组态团体字符串。

- **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 65) 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。

## 4.10 安全性

独立选项的组态取决于所用的遥控协议。

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 18)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 21)部分。

要组态安全功能，需要创建一个安全用户，请参见安全用户 (页 60)部分。

### 4.10.1 安全用户

#### 创建安全用户

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

导航到全局安全设置 >“用户和角色”>“用户”选项卡。

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

登录后，该用户可以在 STEP 7 项目中进行所需的设置。

在以后使用安全参数时，请继续以该用户身份登录。

### 4.10.2 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 61)部分。

- **时钟同步**

有关时钟同步的组态，请参见时钟同步 (页 49)部分。

- **电子邮件组态**

请参见电子邮件组态 (页 63)部分。

- **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 65)部分。

- **SNMP**

在此处，可对 CP 上的 SNMP 代理进行设置。

请参见SNMP (页 65)部分。

- **证书管理器**

请参见证书管理器 (页 75)部分。

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 67)部分。

- **用户管理**

在此处组态用户、角色和权限。

### 4.10.3 防火墙

#### 4.10.3.1 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。

#### 4.10.3.2 源 IP 地址的表示法（高级防火墙模式）

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

- 仅使用连字符来分隔两个 IP 地址。

正确：192.168.10.0-192.168.10.255

- 不要在两个 IP 地址之间输入任何其它符号。

错误：192.168.10.0 - 192.168.10.255

如果错误地输入范围，则不会使用防火墙规则。

#### 4.10.3.3 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。

相关信息，请参见防火墙激活情况下的在线安全诊断和下载到站设置 (页 62)部分。

#### 4.10.3.4 防火墙激活情况下的在线安全诊断和下载到站设置

##### 针对在线功能设置防火墙

若已启用安全功能，请按照下面列出的步骤进行操作。

**全局安全功能：**

1. 选择条目“防火墙 > 服务 > 为 IP 规则定义服务”(Firewall > Services > Define services for IP rules)。
2. 选择“ICMP”选项卡。
3. 插入一个类型为“Echo Reply”和一个类型为“Echo Request”的新条目。

**CP 的本地安全功能：**

现在选择 S7 站中的 CP。

1. 在 CP 的本地安全设置中，在“安全 > 防火墙”(Security > Firewall) 参数组中启用高级防火墙模式。
2. 打开“IP 规则”(IP rules) 参数组。
3. 在表中，按如下方式为之前已创建的全局服务插入新的 IP 规则：
  - 操作：Accept；从：外部；至：站；服务 > ICMPv4/6 服务 > Echo Request（此前全局创建的服务）
  - 操作：Accept；从：站；至：外部；服务 > ICMPv4/6 服务 > Echo Reply（以前全局创建的服务）
4. 对于“Echo Request”服务的 IP 规则，在“源 IP 地址”(Source IP address) 下输入工程师站的 IP 地址。

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

---

**说明****在线安全诊断和下载的附加服务**

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

---

#### 4.10.4 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 78) 部分。

## 电子邮件要求

注意 CP 组态中对于传送电子邮件的以下要求：

- 安全功能已启用。
- CP 的时间已同步。

要进行组态，则需要 SMTP 服务器和用户帐户的有关数据：

- 服务器地址、端口号、用户名、密码、发件人 (CP) 的电子邮件地址
- 通过加密传送：服务器证书

## 电子邮件组态

使用 SMTP 端口 25 的默认设置时，模块将传输未加密电子邮件。

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 75) 部分



## 4.10.5 日志设置 - 过滤系统事件

### 系统事件值设置太高时产生的通信问题

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

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

## 4.10.6 SNMP

### SNMP

有关 SNMP 的 CP 功能范围，请参见SNMP (页 96)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！

---

**说明****访问安全**

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

---

**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。

请注意在线帮助中有关可能的算法的安全信息。

**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。

## 4.10.7 VPN

### 4.10.7.1 VPN (Virtual Private Network)

#### VPN - IPsec

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（IPsec 隧道）并进行操作。

IPsec 隧道转发所有数据，甚至包括来自更高层协议（HTTP、FTP 等）的数据。

两个网络组件间的数据通信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

#### 4.10.7.2 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. 启用“激活安全特性”(Activate security features) 选项
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。

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

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。

#### 4.10.7.3 SOFTNET 安全客户端的 VPN 通信（工程师站）

有关在 SOFTNET 安全客户端和 CP 之间建立 VPN 隧道通信的信息，请参见“为各站间的 S7 通信创建 VPN 通道 (页 68)”部分。

### 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”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”。

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”。

结果：现在已完全禁用低级别节点。可以建立 VPN 隧道通信。

#### 4.10.7.4 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。

#### 4.10.7.5 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”。

#### 4.10.7.6 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，则这仅限于一个已组态的 VPN 连接。

#### 4.10.7.7 SINEMA Remote Connect

##### 使用 SINEMA Remote Connect (SINEMA RC) 进行远程维护

应用程序“SINEMA Remote Connect”(SINEMA RC) 可用于远程维护。

SINEMA RC 使用 OpenVPN 对数据加密。通信中心为 SINEMA RC 服务器，通过该服务器可实现用户间的通信及管理通信系统的组态。

##### 准备步骤

在 STEP 7 中开始组态模块的 SINEMA RC 连接之前，请执行以下步骤。这是确保 STEP 7 项目一致性的先决条件。

- 组态 SINEMA Remote Connect Server

根据需要组态 SINEMA RC Server（不在 STEP 7 中）。必须在 SINEMA RC 服务器中组态通信模块及其通信伙伴。

- 导出 CA 证书（可选）

如果要在建立连接期间使用服务器证书作为通信模块的身份验证方式，请从 SINEMA RC Server 中导出 CA 证书。

然后将 CA 证书从 SINEMA RC Server 导入工程师站。

或者，也可以使用服务器证书的识别码作为通信模块的身份验证方式。识别码的有效期限可能短于证书的有效期限。

请注意，更换模块时需要重复导入证书。



## 组态 SINEMA Remote Connect

### 导入自己的证书

1. 在 CP 上，导航到参数组“安全 > 证书管理器 > 伙伴设备的证书”。
2. 双击第一个表格空行以打开证书选择对话框。
3. 选择 SINEMA RC Server 的 CA 证书。

然后导航到参数组“安全 > VPN”(Security > VPN)。

### VPN > 常规

1. 激活 VPN
2. 对于“VPN 连接类型”，如果要通过 SINEMA Remote Connect 进行通信，则选择“通过 SINEMA 远程连接服务器进行的自动 OpenVPN 组态”选项。

### SINEMA 远程连接服务器

输入该服务器的地址和端口号。

### 服务器验证

在此可以选择建立连接期间的通信模块身份验证方式。

- CA 证书

在“CA 证书”下，从之前导入并在本地证书管理器中进行分配的 SINEMA RC Server 中选择 CA 证书。

模块通常会检查服务器的 CA 证书及其有效期。这两个选项无法更改。

- 识别码

选择这种身份验证方式时，应输入 SINEMA RC Server 服务器证书的识别码。

### 身份验证

- 设备 ID

输入在 SINEMA RC 中为模块生成的设备 ID。

- 设备密码

输入在 SINEMA RC 中组态的模块的设备密码。

最大字符数：127

### 可选设置

在“安全 > VPN > 可选设置”参数组中通过参数“连接类型”对连接建立进行组态。

- **更新间隔**

可通过此参数设置 CP 在 SINEMA RC 服务器上查询组态的间隔。

请注意，如果将 SINEMA RC 服务器的组态设置更改为 0（零），则 CP 将无法再与 SINEMA RC 服务器建立连接。

- **“连接类型”**

该参数的两个选项将在连接建立中具有以下作用：

- 自动

模块建立与 SINEMA RC 服务器的连接。在连接参数由 SINEMA 远程连接服务器更改之前，OpenVPN 连接都会保持。如果连接中断，则 CP 会自动重新建立连接。

如果 SINEMA 远程连接服务器更改了连接参数，则 CP 将在上述组态的更新间隔结束后请求获取新的连接数据。

- PLC 触发器

该选项用于模块通过 SINEMA RC 服务器进行的偶发通信。

如果要在模块和 PC 之间建立临时连接，则可使用该选项。例如，临时连接通过 PLC 变量建立，可用于提供服务。

---

### 说明

#### 连接中止

如果由于固件更新或“下载到设备”而导致 CPU 停止，则 OpenVPN 连接将中止。  
仅在启用“自动”选项后才能使用这些功能。

---

- **建立连接的 PLC 变量**

如果已选择选项“PLC 触发器”，则当 PLC 变量 (Bool) 变为值 1 时模块会建立一个连接。操作期间可根据需要通过使用 HMI 面板等方式设置 PLC 变量。

将 PLC 变量重置为 0 后，会再次终止连接。

## 4.10.8 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. 然后通过以下任一方式将导入的证书分配给模块：
  - 使用全局安全设置中的“受信任的证书和根证书颁发机构”表
  - 使用模块（安全性）的本地证书管理器中的“伙伴设备的证书”表该表还包括已在同一 STEP 7 项目中生成其证书的通信伙伴的证书。

有关操作步骤说明，请参见处理证书 (页 75) 部分。

更多相关信息，请参见 STEP 7 信息系统。

## 4.10.9 处理证书

### 验证证书

如果已为通信模块组态了需要身份验证的安全通信，则自身与通信伙伴双方都具有证书才能进行通信。

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，模块就可以与非西门子伙伴进行通信，通信过程中必须交换伙伴的相关证书。要向模块提供第三方证书，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. 通过以下任一方式分配证书：

- 全局安全设置 > 证书管理器 > “受信证书和根认证机构”(Global security settings > Certificate manager > Trusted certificates and root certification authorities)
- 模块的本地安全设置 > 证书管理器 > “伙伴设备的证书”(Local security settings of the module > Certificate manager > Certificates of the partner devices)

以下部分介绍了这些步骤。

### 从通信伙伴导入第三方证书

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

1. 将第三方证书保存到所连工程师站 PC 的文件系统中。
2. 在 STEP 7 项目中打开全局证书管理器：  
全局安全设置 > 证书管理器
3. 打开“受信证书和根认证机构”(Trusted certificates and root certification authorities) 选项卡。
4. 单击表中的行可选择快捷菜单“导入”(Import)。
5. 在打开的对话框中，将证书从工程师站的文件系统导入到 STEP 7 项目中。

### 在全局安全设置中分配证书

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

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

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

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

## 本地分配证书

要在模块中使用导入的证书，需要在模块的“安全”(Security) 参数组中显示相应证书。请按照下面列出的步骤进行操作：

1. 在 STEP 7 项目中选择模块。
2. 导航到参数组“安全 > 证书管理器”(Security > 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。

所选证书显示在模块的本地表中。

此时第三方证书才可以用于模块。

该表还包括已在同一 STEP 7 项目中生成其证书的通信伙伴的证书。

## 为第三方供应商应用程序（如记录服务器）导出证书

在与第三方供应商的应用程序通信时，第三方应用程序通常也需要模块的证书。

导出模块证书，用于第三方供应商的通信伙伴，操作步骤与导入类似（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。

现在可以将导出的模块证书传送到第三方供应商的系统中。

### 记录服务器的证书

如果在用户系统中使用了记录服务器，则导出服务器上用于模块验证的 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 项目中未采用在 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。

## 4.11 数据点

可以在组态手册中找到有关遥控特定参数的说明，具体请参见“/4/ (页 114)”。

## 4.12 消息

### 组态电子邮件

如果发生重要事件，CP 可发送消息。电子邮件可组态：接收方可以是连接 Internet 的 PC 或 S7 站。

可以使用 CP 的消息编辑器组态消息。或者，可通过以下方式找到消息：

- CP 的快捷菜单（使用所选模块）
- 通过项目导航：“站目录 > 本地模块 > CP”(Directory of the station > Local modules > CP)

有关消息文本和其它参数中允许的字符的信息，请参见“用于用户名、密码和消息的字符集 (页 84)”部分。

### 项目概述和必要信息

要传输消息，不再需要启用遥控通信（参数组“通信类型”(Communication types)）。通过 CP 无需使用遥控通信即可发送消息。

使用电子邮件所需的信息：

- SMTP 服务器的访问数据：地址、端口号、用户名、密码
- 使用 STARTTLS 或 SSL/TLS 时：电子邮件服务提供商的证书
- 收件人的电子邮件地址

可以在以下参数组中执行组态：

- 启用安全功能

要使用电子邮件，需要启用 CP 的安全功能（参数组“安全”(Security)）。

- 服务/协议的组态：

“电子邮件组态”(E-mail configuration)，请参见电子邮件组态 (页 63)部分。

- 使用 STARTTLS 或 SSL/TLS 时：

– 导入电子邮件服务提供商的证书：

“全局安全设置”(Global security settings)

– 将导入的证书用于 CP：

参数组“安全 > 证书管理器”(Security > Certificate manager)

## 消息编辑器中的组态

可在 STEP 7 中的数据点和消息编辑器中组态消息。或者，可打开编辑器：

- 通过选择通信模块

快捷菜单“打开数据点和消息编辑器”(Open the data point and messages editor)

- 通过项目导航：

“项目 > 相关站的目录 > 本地模块 > 所需通信模块”(Project > directory of the relevant station > Local modules > required communications module)

通过双击条目，数据点或消息编辑器打开。

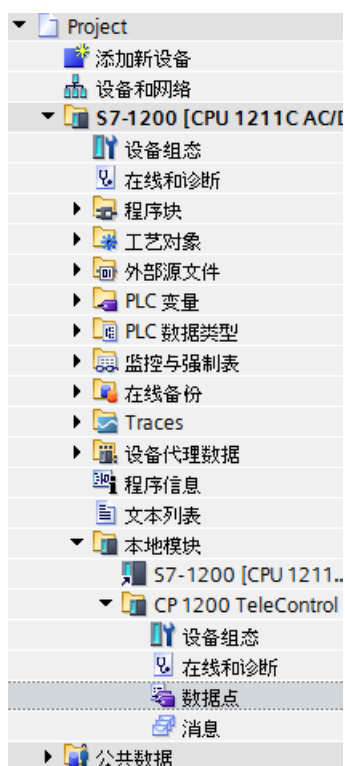


图 4-1 通过项目导航打开消息编辑器

打开编辑器之后，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

数据点编辑器仅与遥控通信相关。

### 创建对象

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（消息）。

可根据需要更改默认名称，但该名称在模块中必须唯一。



### 排列列和行，显示/隐藏列

与许多其它程序一样，还可以根据需要排列各列并对表格排序：

- 排列列

如果用鼠标左键按住列标题，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右边缘附近，将出现以下符号：



出现该符号后，即可双击列标题。列宽将根据本列中最宽的条目自行调整。

- 显示/隐藏列

使用右键单击列标题时打开的快捷菜单调用此功能：

### 复制消息

可以复制和粘贴消息。如果右键单击表格中某个对象的行，则可从快捷菜单访问下面列出的功能：

- 剪切
- 复制
- 粘贴

可在表格中或表格下方第一个空行处粘贴事先剪切或复制的对象。

对于同一类型且采用相同遥控协议的其它通信模块，也可以将剪切或复制的对象粘贴到表格中。

- 删除

按住 <Ctrl> 键，可选择多个不连续的行。

如果按住 <Shift> 键，则可选择连续区域的起点和终点。

### 用于组态消息的选项卡

在“消息”(Messages) 表中选择消息。可以在表格下方的选项卡中组态所选消息的参数。

#### “消息参数”(Message parameter)

在此处组态电话号码或收件人、主题（电子邮件）和消息文本。

#### “触发器”(Trigger)

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**

指定触发消息发送的事件。

- **使用 PLC 变量**

要通过触发信号发送电子邮件，需评估用户程序设置的触发位“触发器 PLC 变量”(PLC tag for trigger) 的沿变化 (0 →

1)。必要时，可以为每条消息组态一个单独的触发位。有关触发位的信息，请参见下文。

**触发位复位：**

如果触发位的存储区在存储区或数据块中，则在消息发送后，触发位复位为零。在所有其它情况下，需要通过用户程序将触发位复位。

---

#### 说明

##### 诊断触发变量的快速设置

触发器的设置频率不应超过每秒一次。

---

- **CPU 切换到 STOP 模式**

- **CPU 切换到 RUN 模式**

- **与伙伴的连接已中断**

与伙伴的遥控连接中断时，触发消息发送。

- **与伙伴的连接已建立**

当遥控连接恢复时，触发消息发送。

- **与伙伴的连接建立失败**

无法与遥控服务器建立连接时，触发消息发送。

- **远程服务会话已启动**

当启用 TeleControl Basic 通信类型且 TeleService 连接已建立时，触发消息发送。

- **远程服务会话已结束**

当启用 TeleControl Basic 通信类型且 TeleService 连接已终止时，触发消息发送。

- **VPN 连接已建立**

当 VPN 连接已建立或恢复时，触发消息发送。

- **VPN 连接已终止**

当 VPN 连接中断时，触发消息发送。

- **SINEMA RC 连接已建立**

当 OpenVPN 连接已建立或恢复时，触发消息发送。

- **SINEMA RC 连接已终止**

当 OpenVPN 连接中断时，触发消息发送。

- **触发器的 PLC 变量**

触发器“使用 PLC 变量”(Use PLC tag) 的 PLC 变量

- **启用处理状态标识符**

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

该状态将写入“获取处理状态的 PLC 变量”。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 98)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**

启用该选项后，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 \$\$。

\$\$ 用作表示数据点值的占位符，支持以下数据类型：

- Bool, Byte, Char, Int, UInt, Word, DWord, UInt, DInt, Real, String,
- 以上数据类型的数组

#### 4.13 用于用户名、密码和消息的字符集

- 值的 PLC 变量

要写入待发送值的 PLC 变量。

### 4.13 用于用户名、密码和消息的字符集

#### 用于用户名、密码和消息文本的字符集

下文中允许的字符适用于：

- 电子邮件服务器：
  - 用户名和密码
- 消息编辑器中的消息：
  - 消息文本

作为 ASCII 字符集（十六进制值和字符名称）输入：

- 0x20  
空格
- 0x21 ... 0x5F  
!"#\$%&'()\*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNO PQ  
RSTUVWXYZ[\]^\_
- 0x61 ... 0x7E  
abcdefghijklmnopqrstuvwxyz{|}~
- 0x7C, 0x7E  
|~

此外，对于消息文本：

- 手动换行符 (↵)

在消息文本中，可以使用 <Shift>+<Enter> 插入换行符。

## 程序块 (OUC)

### 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。

---

#### Secure OUC 要求

通过 Secure OUC 使用安全传输的要求：

- STEP 7：V16 及更高版本
- CPU 固件：自 V4.4 起
- CP 固件：V3.2 及更高版本

#### 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

## 5.1 用于 OUC 的程序块

或者使用：

- **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

有关 T\_CONFIG 和 SDT 的信息，请参见在运行期间更改 IP 地址  
(页 88)部分中的“IF\_CONF\_...”。

---

### 说明

#### 不支持来自 CP 的反馈

“T\_CONFIG”不支持 CP 对 CPU

的反馈。块调用或设置地址参数时出现的错误不会报告。无论是否已设置地址参数，块都输出“BUSY”或“DONE”。

---

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

## 系统数据类型 (SDT) 的连接描述

上述所列的块将 CONNECT 参数用于相关连接描述。TMAIL\_C 使用参数 MAIL\_ADDR\_PARAM。

连接描述以数据块形式存储，此数据块的结构由系统数据类型 (SDT) 定义。

### 创建数据块 SDT

为每个数据块（全局 DB）形式的连接描述创建所需的 SDT。

SDT 类型不是通过从程序块声明表的“数据类型”(Data type) 下拉列表选择一个条目进行创建, 而是通过在“数据类型”(Data type) 框中手动输入名称 (例如“TCON\_IP\_V4”) 进行创建。

随后, 相应的 SDT 与其参数一并创建出来。

#### 可用的 SDT

- **TCON\_IP\_V4**  
基于 TCP 或 UDP 传送帧
- **TCON\_QDN**  
通过完全限定域名 (FQDN) (IPv4 / IPv6) 进行 TCP 或 UDP 通信
- **TCON\_IP\_RFC**  
基于 ISO-on-TCP 传送帧 (两个 S7 站间直接通信)
- **TADDR\_Param**  
基于 UDP 传送帧
- **TMail\_V4**  
基于 IPv4 地址式电子邮件服务器寻址来传送电子邮件
- **TMail\_V6**  
基于 IPv6 地址式电子邮件服务器寻址来传送电子邮件
- **TMail\_FQDN**  
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
- **TCON\_IP\_V4\_SEC**  
用于基于 TCP 安全传送数据
- **TCON\_QDN\_SEC**  
用于基于主机名安全传送数据
- **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

## 5.2 在运行期间更改 IP 地址

有关 TMail\_Vx\_SEC/TMail\_QDN\_SEC 的说明：

对于这些 SDT，检查邮件服务器的证书，而不是“TLSServerCertRef”（STEP 7 内部引用）证书的 ID。

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

### 在运行时通过 T\_CONFIG 更改地址参数

可在运行时使用 T\_CONFIG 以程序控制方式更改以下地址参数：

- CP 的 IP 地址
- CP 的子网掩码
- CP 的路由器地址
- DNS 服务器的地址参数 (IF\_CONF\_DNS)
- NTP 服务器的地址参数 (IF\_CONF\_NTP)



**CP 组态要求**

为能够以程序控制方式更改 IP 参数，必须在组态 CP 以太网接口的 IP 地址时，启用“直接在设备上设置 IP 地址”(IP address is set directly at the device) 选项。

**说明****使用动态 IP 地址更改 IP 参数**

如果 CP 从相连的路由器获得动态 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。

**程序块/STEP 7 版本**

T\_CONFIG 程序块支持以程序控制的方式更改 IP 参数，更改时会访问以适当的系统数据类型 (SDT) 存储的地址数据。

可将 T\_CONFIG 与以下系统数据类型 (SDT) 结合使用：

- IF\_CONF\_V4
- IF\_CONF\_V6
- IF\_CONF\_DNS
- IF\_CONF\_NTP

组态的地址参数在 CP 中只能是暂时有效。

在相应的“IF\_CONF\_...”SDT 中，必须设置 "Mode" = 2 参数。

**说明****不支持来自 CP 的反馈**

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

有关块和 SDT 参数分配的详细信息，请参见 STEP 7 信息系统。

**要求****STEP 7 版本**

自 STEP 7 Basic V14 起，可使用 T\_CONFIG。

## 5.2 在运行期间更改 IP 地址

### 组态的 IP 地址

为能够以程序控制方式更改 IP 参数，必须在组态 CP 以太网接口的 IP 地址时，启用“直接在设备上设置 IP 地址”(IP address is set directly at the device) 选项。

### 固件版本

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

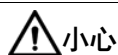
## 诊断和保养



### 警告

#### 清洁外壳

- **在危险区域**  
只能用潮湿但不浸水的布来清洁外壳的外部。
- **在非危险区域**  
只能用干布来清洁外壳的外部。  
不要使用任何液体或溶剂。



### 小心

#### 表面高温

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

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

## 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 Basic : “在线 > 在线和诊断”(Online > Online and diagnostics) 菜单的诊断功能

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。

如果要通过 CP 对工作站运行在线诊断，则需要选择通信类型“启用在线功能”(Enable online functions)，请参见通信类型 (页 48)部分。

### “诊断”(Diagnostics) 组

诊断页面分为以下几组：

- **常规**

该组显示模块的常规信息。

- **诊断状态**

该组显示 CPU 视图中模块的状态信息。

- 设备特定事件

此处显示有关内部模块事件的信息。

- **以太网接口**

地址和统计信息

- **Industrial Remote Communication**

该组具有以下诊断页面：

- 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)

按钮，记录模块接收和发送的帧并持续几秒钟。

使用“禁用协议跟踪”(Disable protocol trace)

功能，将停止记录并将数据写入日志文件。

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。

- **时钟**

有关设备上时间的信息

- **安全性**

该组具有以下诊断页面：

- 状态

此诊断页面显示最重要的安全设置、时间，以及与组态有关的数据。

- 系统日志

如果建立了与 SCALANCE S 模块的连接，则可在该诊断页面上开始记录系统条目。可以保存条目。

- 审计日志

可开始在此诊断页面上记录模块的日志数据。可以保存条目。

- 通信状态

此诊断页面显示 VPN 组已知安全模块的状态、其终点以及隧道属性。

- SINEMA RC - 自动 VPN 组态

该诊断页面显示自动 OpenVPN 组态和 OpenVPN 连接的状态。

**“功能”(Functions) 组**

- **固件更新**

有关说明，请参见下载固件 (页 100) 部分。

- **分配 IP 地址**

- **分配 PROFINET 设备名称**

- **保存服务数据**

该功能用于记录在用户无法自行消除预期之外或不必要的模块行为时的内部模块过程。

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。

## 诊断电子邮件

如果发生 CPU STOP 等可组态事件，则 CP 可以发送诊断电子邮件。有关组态的信息，请参见“消息”。

## 6.2 Web 服务器 S7-1200：连接建立

### 伙伴状态

使用遥控通信时，CP 可通过变量向 CPU 发送通信伙伴的连接状态。可以通过 CPU 的 Web 服务器显示变量的状态。可在以下参数组中组态变量：

- TeleControl Basic：“伙伴站”(Partner stations)
- DNP3/IEC：“与 CPU 进行通信”(Communication with the CPU)

### CP 诊断

CP 可以将扩展诊断数据存储在 PLC 变量中。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“CP 诊断 (页 57)”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 55)部分。

### SNMP

有关各功能的信息，请参见SNMP (页 96)部分。

## 6.2 Web 服务器 S7-1200：连接建立

### 建立与 CPU 的 Web 服务器的连接

按照以下步骤将 PC 连接到 CPU 的 Web 服务器。

#### CPU 组态要求

1. 在工程师站上打开相应项目。
2. 在 STEP 7 中选择所涉及站的 CPU。
3. 选择“Web 服务器”条目。
4. 在参数组“常规”中，选择“为该接口启用 Web 服务器”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。

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”参数组中的“仅允许通过 HTTPS 访问”选项：

- **通过 HTTP 建立连接**

禁用了“仅允许通过 HTTPS 访问”选项时步骤

- **通过 HTTPS 建立连接**

启用了“仅允许通过 HTTPS 访问”选项时的步骤

这两种情况在以下部分中进行说明。

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 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”条目。

将打开“证书”对话框。

5. 单击“安装证书...”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. 当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，可以按照下一部分中所述继续操作。

如果终止到 Web 服务器的连接，则下一次可通过 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 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>
3. 按回车键。

将打开 Web 服务器的起始页。

### 6.3 通过端口 8448 执行在线安全诊断

4. 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。
5. 登录后，在 Web 服务器的导航面板中选择条目“模块状态”。
6. 在模块列表中选择 CP。  
将显示 CP 特定的内容。

## 6.3 通过端口 8448 执行在线安全诊断

### 通过端口 8448 执行安全诊断

要求：

- 激活防火墙后，必须启用访问权限。

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

1. 在 STEP 7 中选择 CP。
2. 打开“在线和诊断”快捷菜单。
3. 在“安全性”参数组中，单击“在线连接”按钮。

这样，即可通过端口 8448 执行安全诊断。

有关详细信息，请参见“防火墙激活情况下的在线安全诊断和下载到站设置 (页 62)”部分。

## 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储存在 MIB 文件中 (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 (安全)

它根据 RFC1213 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：

- Address Translation (AT)
- EGP
- Transmission

- **LLDP MIB**

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 114) 手册。

## 组态

有关组态的信息，请参见：

- 禁用安全功能 (SNMPv1)：SNMP (页 59)
- 启用安全功能 (SNMPv1 / SNMPv3)：SNMP (页 65)

## 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，请参见电子邮件组态 (页 63) 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。

### 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	无可可用通道可能原因：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。

状态	含义
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。
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)： • 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)： • 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。

状态	含义
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"> <li>• CP 组态 &gt; 电子邮件组态： <ul style="list-style-type: none"> <li>– 用户名</li> <li>– 密码</li> <li>– 电子邮件地址（发送方）</li> </ul> </li> <li>• 报警组态 &gt; 电子邮件数据 (Content)： <ul style="list-style-type: none"> <li>– 收件人地址（“收件人”或“抄送”）。</li> </ul> </li> </ul>
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，则可在西门子工业在线支持 Internet 页面上通过以下地址找到：

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

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

有三种不同的方法可在 CP 上加载新的固件文件：

- 将固件文件保存在 CPU 的存储卡上  
可以在西门子工业在线支持的 Internet 页面中找到有关在 CPU 的存储卡上进行下载的步骤描述。
- 通过 WAN 使用 STEP 7 的在线功能加载固件

### 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。
- 如果使用在线功能安装固件文件，保持性存储器将丢失。

CP 的 LED 闪烁表示正在加载固件，请参见“LED (页 28)”。

## 通过 WAN 使用 STEP 7 的在线功能加载固件

### 要求：

- 可通过 CP 的 IP 地址对其进行访问。
- 工程师站和 CP 位于同一子网中。
- 新的固件文件存储在工程师站上。

### 步骤：

1. 将工程师站连接到网络。
2. 在工程师站上打开相关的 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”图标启用在线功能。
5. 在“在线连接”对话框的“PG/PC 接口类型”列表框中选择以太网接口“PN/IE”。
6. 选择 CP 或 CPU 的插槽。

两种方式均可。

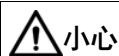
7. 使用“连接”按钮进行连接。

“在线连接”向导将指导您完成剩余的安装步骤。

有关在线功能的更多信息，请参见 STEP 7 信息系统。

## 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 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。

## 6.7 模块更换

站再次启动时，新 CP 将从 CPU 中读取项目数据。

**例外：**

SINEMA RC 组态的数据和 SINEMA RC 服务器的证书保存在 CP 中。这些信息无法从 CPU 中读取。

## 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"><li>最长 55 m 带有 IE FC RJ45 Plug 180 的 IE TP Torsion Cable</li><li>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</li></ul>	
0 ... 85 m	<ul style="list-style-type: none"><li>最长 85 m 带有 IE FC RJ45 Plug 180 的 IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable</li><li>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</li></ul>	
0 ... 100 m	<ul style="list-style-type: none"><li>最长 100 m 带有 IE FC RJ45 Plug 180 的 IE FC TP Standard Cable</li><li>最长 90 m IE FC TP Standard Cable + 10 m 通过 IE FC RJ45 Outlet 的 TP Cord</li></ul>	
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
	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

## 7.2 以太网接口的引脚分配

技术规范		
	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, 请参见应用和功能 (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	Transmit Data +
	2	TD_N	Transmit Data -
	3	RD	Receive Data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive Data -
	7	GND	Ground
	8	GND	Ground



# 认证

## 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。

---

## Internet 上的文档

有关下列符合性声明以及产品证书，请访问以下 Internet 地址：

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

可在相应证书中查看考虑的标准，可访问上述 Internet 地址获取证书。

## 符合性声明地址

EU 和 UK 符合性声明适用于以下区域的所有主管部门：

Siemens Aktiengesellschaft

Digital Industries

P.O.Box 48 48

90026 Nuremberg

Germany

## EC 符合性声明



CP

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

- **2014/34/EU (ATEX 防爆指令)**

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

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

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

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

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

## UK 符合性声明



Importer UK:

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

产品满足以下指令的相关要求：

- **UKEX Regulations**

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

- **EMC Regulations**

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

- **RoHS Regulations**

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

## ATEX / IECEx / UKEX / CCC-Ex

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

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

必须满足“依据 ATEX / UKEX / IECEx / CCC-Ex 要求在危险区域使用的注意事项 (页 34)”部分中的相关条件，才能安全使用本产品。

产品满足下列防爆保护要求。



**警告**

### 遵循安装准则

如果在安装和运行期间遵守以下规则，则产品符合要求：

- “使用设备的重要注意事项 (页 33)”部分中的注意事项
- /I/ (页 113)文档中的安装说明

## IECEx

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

产品满足以下标准的要求：

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

## ATEX

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

产品满足以下标准的要求：

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





#### UKEX

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

产品满足以下标准的要求：

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

Importer UK: Siemens plc (请参见上文)



#### CCC-Ex

分类：Ex na IIC T4 Gc (不在铭牌上), 证书编号：2020322310002625

产品满足以下标准的要求：

- GB 3836.1  
危险区域 - 第 0 部分：设备 - 常规要求
- GB 3836.8  
爆炸性气体环境 - 第 15 部分：保护类型“n”的设备保护

#### EMC

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

应用标准：

- EN 61000-6-4  
电磁兼容性 (EMC) - 第 6-4 部分：通用标准 - 工业环境中的辐射标准
- EN 61000-6-2  
电磁兼容性 (EMC) - 第 6-2 部分：通用标准 - 工业环境中的抗扰性

#### RoHS

CP 满足以下指令的相关要求：

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

应用标准：

- EN IEC 63000

## c(UL)us



应用标准：

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

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)

需满足依据 UL HazLoc 和 FM 要求在危险区域使用的注意事项  
(页 35)部分中的相关条件，才能安全使用 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

(Ta reduced to 50 °C when mounted vertically)

Report Number: 3040919

需满足依据 UL HazLoc 和 FM 要求在危险区域使用的注意事项  
(页 35)部分中的相关条件，才能安全使用 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

基于关税同盟技术规范的符合性声明 (TR CU)

#### MSIP 요구사항 - For Korea only



A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기  
바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

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

#### 当前认证

SIMATIC NET

产品会定期提交到相关机构和认证中心，以获得与特定市场和应用有关的认证。

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

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

## 尺寸图

## 说明

CP 图中的所有尺寸均以毫米为单位。

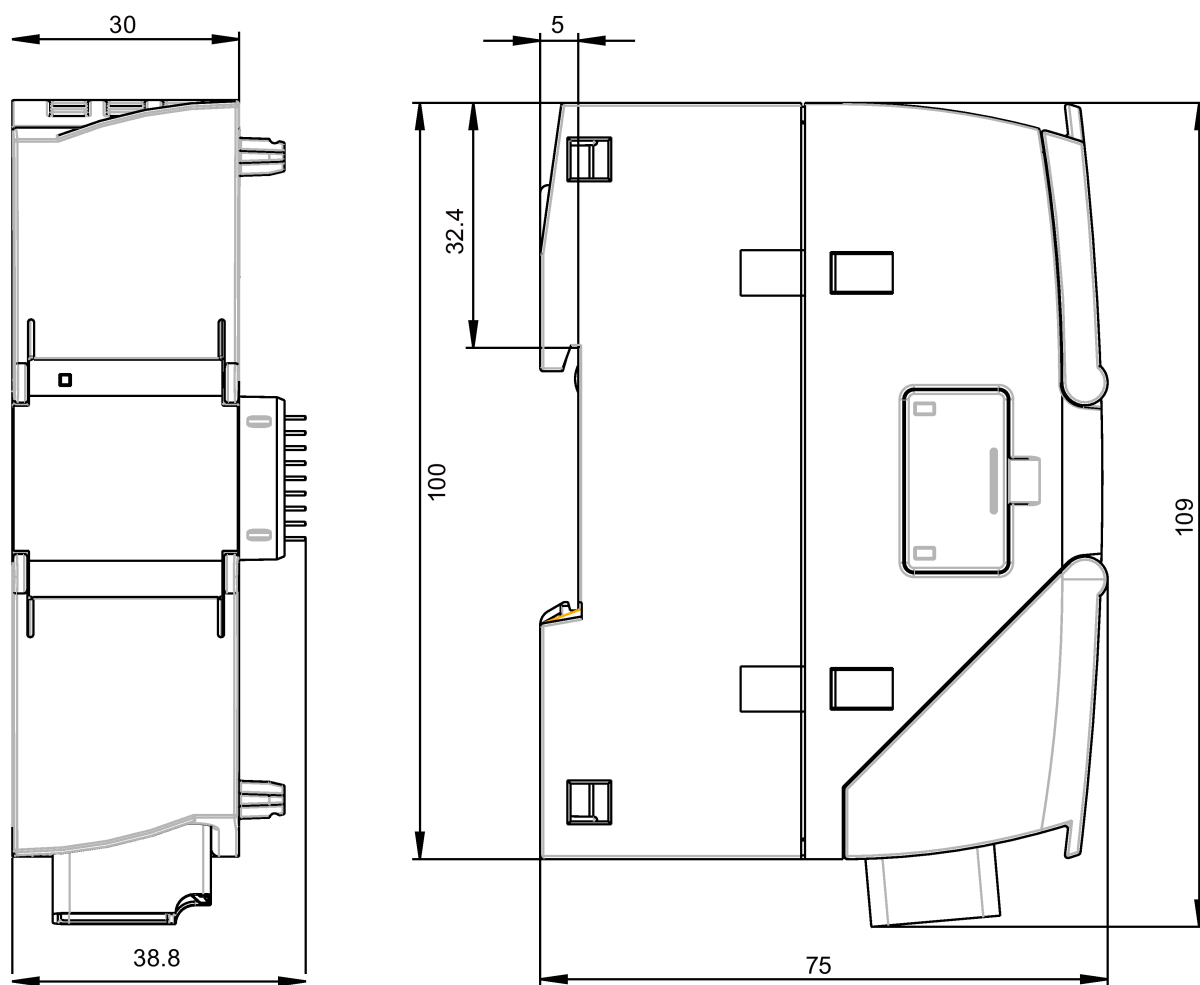


图 B-1 正视图与左侧视图

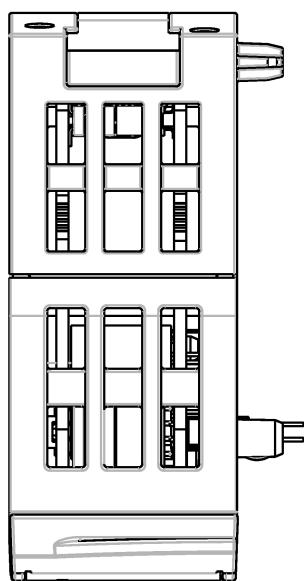


图 B-2 俯视图



## 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 自动化系统

系统手册

Siemens AG

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

/2/

**/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 - TeleControl

Siemens AG

协议的组态手册：

- TeleControl Basic

- SINAUT ST7

- DNP3

- IEC 60870-5

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/21764/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>)

**/6/**

SIMATIC NET

SINEMA Remote Connect - Server

操作说明

Siemens AG

链接：(<https://support.industry.siemens.com/cs/ww/zh/ps/21816/man>)



# 索引

## C

CPU 固件, 26

## D

DNS 服务器 - 程序控制的更改, 88

## I

IP 地址 - 程序控制的更改, 88

IP 地址 - 固定, 53

IP 组态

IPv4, IPv6, 17

IP\_CONF\_V4, 88

IPsec, 67

IPsec 隧道；数量, 23

## M

MAC 地址, 3

MIB, 97

## N

NTP, 51

NTP (secure), 51

NTP 服务器 - 程序控制的更改, 88

## O

OUC (Open User Communication), 85

OUC 连接

资源, 21

## P

PG/OP 连接, 22

## S

S7 连接

启用, 49

资源, 21

S7 路由, 14

Security, 18

SIMATIC NET 词汇表, 8

SMS

编程 (OUC), 85

SMTPS, 64

SNMP, 17, 59, 96

SNMPv3, 20, 65

SSL/TLS, 64

STARTTLS, 64

STEP 7 - 版本, 26

SYSLOG, 72

## T

T\_CONFIG, 88

TC\_CONFIG, 88

## V

VPN, 23, 67

## W

Web 服务器, 55

## D

订货号, 3

## CH

尺寸, 39

## Y

以太网接口  
分配, 104

## D

电子邮件  
组态, 78  
编程 (OUC), 85  
数量, 23

## CH

处置, 8

## J

记录服务器, 77

## F

发送缓冲区, 22

## Z

在线功能, 17, 49, 93  
在线诊断, 92

## H

回收, 8

## W

网关 (VPN), 71

## J

交叉引用 (PDF), 6

## CH

产品名称, 4

## A

安全诊断, 96  
安全须知, 33

## D

导入证书 - 电子邮件, 64

## F

防火墙, 19

## Y

运行状态 (LED 显示) , 30

## G

更换模块, 101

**L**

连接资源, 21

**S H**

时钟同步, 17

**C**

词汇表, 8

**C H**

拆卸, 42

**Z H**

直接通信, 14

**G**

固件版本, 3

**F**

服务和支持, 8

**Z H**

帧存储器, 22

**S H**

说明 (OUC), 85

**Z H**

站间通信, 14

**B**

被动建立 VPN 连接, 71

**P**

培训, 8

**Y**

硬件版本, 3

**C H**

程序块, 15

**S H**

数据缓冲, 22

**D**

端口 8448, 96

**S**

缩写/缩略语, 4