

# SIEMENS

## SIMATIC NET

### ET 200SP - Industrial Ethernet CP 154xSP-1

Betriebsanleitung

CP 1542SP-1  
CP 1542SP-1 IRC  
CP 1543SP-1

12/2019

C79000-G8900-C426-05

Vorwort

Anwendung und Funktionen

1

LEDs und Anschlüsse

2

Montage, Anschluss,  
Inbetriebnahme

3

Projektierung

4

Programmbausteine

5

Diagnose und  
Instandhaltung

6

Technische Daten

7

Zulassungen

A

Maßzeichnungen

B

Zubehör

C


Literaturverzeichnis


D


## Rechtliche Hinweise

### Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

 <b>GEFAHR</b>
bedeutet, dass Tod oder schwere Körperverletzung eintreten <b>wird</b> , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

 <b>WARNUNG</b>
bedeutet, dass Tod oder schwere Körperverletzung eintreten <b>kann</b> , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

 <b>VORSICHT</b>
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

<b>ACHTUNG</b>
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.


Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

### Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

### Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

 <b>WARNUNG</b>
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

### Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

### Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

# Vorwort

## Gültigkeit dieses Handbuchs

In diesem Dokument finden Sie Informationen zu den folgenden Modulen:

- **CP 1542SP-1**  
Artikelnummer **6GK7542-6UX00-0XE0**  
Hardware-Erzeugnisstand 1  
Firmware-Version V2.1  
Kommunikationsprozessor zum Anschluss einer SIMATIC ET 200SP-CPU an Industrial Ethernet
- **CP 1542SP-1 IRC**  
Artikelnummer **6GK7542-6VX00-0XE0**  
Hardware-Erzeugnisstand 1  
Firmware-Version V2.1  
Kommunikationsprozessor zum Anschluss einer SIMATIC ET 200SP-CPU über Industrial Ethernet an eine Leitstelle (TCSB, ST7, DNP3, IEC 60870-5-104)
- **CP 1543SP-1**  
Artikelnummer **6GK7543-6WX00-0XE0**  
Hardware-Erzeugnisstand 1  
Firmware-Version V2.1  
Kommunikationsprozessor zum Anschluss einer SIMATIC ET 200SP-CPU an Industrial Ethernet, Security



Bild 1 CP 1542SP-1 mit gestecktem BusAdapter (hier BA 2xRJ45)

Auf der Vorderseite der Baugruppe ist am rechten Rand der Hardware-Erzeugnisstand als Platzhalter "X" aufgedruckt. Bei einem Aufdruck von beispielsweise "X 2 3 4" ist X der Platzhalter für den Hardware-Erzeugnisstand 1.

Direkt darunter finden Sie die Angabe der Firmware-Version des CP im Auslieferungszustand.

Die MAC-Adresse der Schnittstelle ist auf der Vorderseite links unten aufgedruckt, oberhalb der Anschlüsse für die Spannungsversorgung:

- 00:1B:1B:xx:xx:01 (Schnittstelle)

Die MAC-Adressen der Ports können Sie über die Online-Funktionen von STEP 7 (Erreichbare Teilnehmer) erfahren:

- 00:1B:1B:xx:xx:02 (Port X1P1)
- 00:1B:1B:xx:xx:03 (Port X1P2)

## Produktbezeichnungen, Begriffe und Abkürzungen

Nachfolgend finden Sie Abkürzungen und Produktbezeichnungen, die häufig in diesem Handbuch verwendet werden.

- **CP / Modul / Gerät**

Wenn Eigenschaften in diesem Handbuch für alle drei CP-Typen gültig sind, werden diese Bezeichnungen stellvertretend für den vollständigen Produktnamen aller drei CP-Typen verwendet.

Wenn Informationen nur für bestimmte CP-Typen gelten, werden die jeweiligen CP-Namen im Text oder in der Kapitelüberschrift genannt.

## Neu in dieser Ausgabe

- Neue Firmware-Version V2.1, unter anderem mit folgenden Funktionen:
  - Unterstützung weiterer SDTs für OUC-Bausteine
  - Größere Anzahl projektierbarer Datenpunkte (Telecontrol), siehe Mengengerüst und Leistungsdaten (Seite 23).
  - Direkte Kommunikation des CP 1542SP-1 IRC zwischen Stationen (DNP3 / IEC 60870-5)
- Beschreibung der Funktionen der Firmware-Version V2.0:
  - Anbindung an SINEMA Remote Connect (CP 1542SP-1 IRC / CP 1543SP-1)
  - Projektierte E-Mails unabhängig von Telecontrol-Kommunikation (CP 1542SP-1 IRC / CP 1543SP-1)
  - Unterstützung des Fernwirkprotokolls SINAUT ST7 (CP 1542SP-1 IRC)
  - Uhrzeitsynchronisation über Uhrzeit des Kommunikationspartners (CP 1542SP-1 IRC)

Freigegebene CPUs für CP-Firmware V2.0: CPUs ab Firmware V2.0

Projektierbarkeit der Funktionen: STEP 7 Professional ab V15

- Neue ATEX-/IECEx-Zulassung
- Neuer Aufbau der Dokumentation

Die Dokumentation des CP besteht aus der vorliegenden Betriebsanleitung und zusätzlichen Projektierungshandbüchern für den CP 1542SP-1 IRC, siehe unten.

## Abgelöste Ausgabe

Ausgabe 02/2018

## Aufbau der Dokumentation

Die Dokumentation der drei CP-Typen besteht aus folgenden Handbüchern und Inhalten:

- **Betriebsanleitung**

Gültig für alle drei CP-Typen

- Anwendung und Funktionen
- Voraussetzungen (CPUs, Projektierungs-Software etc.)
- Hardware-Beschreibung
- Montage, Anschluss, Inbetriebnahme, Betrieb
- Projektierung des CP 1542SP-1 und CP 1543SP-1  
Zur Projektierung des CP 1542SP-1 IRC siehe Projektierungshandbücher.
- Diagnose, Instandhaltung
- Technische Daten, Zulassungen, Zubehör

- **Projektierungshandbücher (CP 1542SP-1 IRC)**

Die Projektierung des CP 1542SP-1 IRC wird in folgenden zusätzlichen Dokumenten beschrieben:

- **Systemhandbuch SINAUT ST7**  
**Band 3 - Projektierung unter STEP 7 Professional (TIA Portal)**
- **Projektierungshandbuch Telecontrol Basic**  
Projektierung und Diagnose in STEP 7 Professional (TIA Portal)
- **Projektierungshandbuch DNP3**  
Projektierung und Diagnose in STEP 7 Professional (TIA Portal)
- **Projektierungshandbuch IEC**  
Projektierung und Diagnose in STEP 7 Professional (TIA Portal)

Die Internet-Links der Handbücher finden Sie im Anhang Literaturverzeichnis (Seite 111).

## Vorausgesetzte Kenntnisse

Für Montage, Inbetriebnahme und Betrieb des CP werden Kenntnisse auf folgenden Gebieten vorausgesetzt:

- Automatisierungstechnik
- Aufbau des Systems SIMATIC ET 200SP
- SIMATIC STEP 7 Professional

## Aktuelle Handbuchausgabe im Internet

Die aktuelle Ausgabe dieses Handbuchs finden Sie auch auf den Internet-Seiten des Siemens Industry Online Support:

- CP 1542SP-1 / CP 1543SP-1  
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22144/man>)
- CP 1542SP-1 IRC  
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/man>)

## Querverweise

In diesem Handbuch werden häufig Querverweise zu anderen Kapiteln verwendet.

Um nach dem Sprung eines Querverweises wieder zurück zur Ausgangsseite zu gelangen, unterstützen einige PDF-Reader den Befehl <Alt>+<Links-Pfeil>.

## Lizenzbedingungen

---

### Hinweis

#### Open Source Software

Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie das Produkt nutzen.

---

Sie finden die Lizenzbedingungen in folgendem Dokument, das sich auf dem mitgelieferten Datenträger befindet:

- OSS\_CP-ET200SP\_99.pdf

## Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z. B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter folgender Adresse:

Link: (<http://www.siemens.com/industrialsecurity>)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen

Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter folgender Adresse:

Link: (<http://www.siemens.com/industrialsecurity>)

## Firmware

Die Firmware ist signiert und verschlüsselt. Es ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

## Gerät defekt

Bitte senden Sie das Gerät im Fehlerfall an Ihre Siemens-Vertretung zur Reparatur ein. Eine Reparatur vor Ort ist nicht möglich.

## Recycling und Entsorgung



Das Produkt ist schadstoffarm, recyclingfähig und erfüllt die Anforderungen der WEEE-Richtlinie 2012/19/EU "Elektro- und Elektronik-Altgeräte".

Entsorgen Sie das Produkt nicht bei öffentlichen Entsorgungsstellen. Für ein umweltverträgliches Recycling und die Entsorgung Ihres Altgeräts wenden Sie sich an einen zertifizierten Entsorgungsbetrieb für Elektronikschrott oder an Ihren Siemens-Ansprechpartner.

Beachten Sie die örtlichen Bestimmungen.

Informationen zur Produktrückgabe finden Sie auf den Internetseiten des Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/de/view/109479891>)

## SIMATIC NET-Glossar

Erklärungen zu vielen Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar hier:

- SIMATIC NET Manual Collection oder Produkt-DVD

Die DVD liegt einigen SIMATIC NET-Produkten bei.

- Im Internet unter folgender Adresse:

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

## Training, Service & Support

Informationen zu Training, Service & Support finden Sie in dem mehrsprachigen Dokument "DC\_support\_99.pdf" auf den Internet-Seiten des Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/de/view/38652101>)





# Inhaltsverzeichnis

	<b>Vorwort</b> .....	<b>3</b>
<b>1</b>	<b>Anwendung und Funktionen</b> .....	<b>13</b>
1.1	Lieferumfang .....	13
1.2	Anwendung .....	13
1.3	Kommunikationsdienste.....	14
1.4	Telecontrol-Kommunikation (CP 1542SP-1 IRC) .....	15
1.5	Kommunikation über SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1).....	18
1.6	Security-Funktionen (CP 1542SP-1 IRC, CP 1543SP-1).....	19
1.7	Weitere Dienste und Eigenschaften .....	22
1.8	Mengengerüst und Leistungsdaten .....	23
1.9	Voraussetzungen für den Einsatz.....	26
1.9.1	Hardware-Voraussetzungen .....	26
1.9.2	Software-Voraussetzungen .....	27
1.10	Konfigurationsbeispiele.....	27
<b>2</b>	<b>LEDs und Anschlüsse</b> .....	<b>35</b>
2.1	LEDs .....	35
2.2	Spannungsversorgung.....	36
2.3	Anschluss für den BusAdapter .....	37
<b>3</b>	<b>Montage, Anschluss, Inbetriebnahme</b> .....	<b>39</b>
3.1	Wichtige Hinweise zum Geräteeinsatz .....	39
3.1.1	Hinweise für den Einsatz im Ex-Bereich.....	39
3.1.2	Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx.....	41
3.1.3	Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc.....	41
3.1.4	Hinweise für den Einsatz im Ex-Bereich gemäß FM .....	42
3.2	CP montieren .....	42
3.3	CP anschließen.....	46
3.4	CP in Betrieb nehmen.....	47
<b>4</b>	<b>Projektierung</b> .....	<b>49</b>
4.1	Security-Empfehlungen.....	49
4.2	Projektierung in STEP 7.....	53
4.3	Kommunikationsarten (CP 1543SP-1).....	54
4.4	Ethernet-Schnittstelle.....	55
4.4.1	IPv6 .....	55
4.4.2	Erweiterte Optionen .....	55

4.4.3	Zugriff auf den Webserver .....	56
4.5	Uhrzeitsynchronisation.....	56
4.6	DNS-Konfiguration .....	58
4.7	Kommunikation mit der CPU.....	58
4.8	SNMP .....	60
4.9	Security (CP 1543SP-1).....	61
4.9.1	Security-Benutzer.....	61
4.9.2	Firewall.....	62
4.9.2.1	Vorgezogene Prüfung von Telegrammen durch die MAC-Firewall .....	62
4.9.2.2	Einstellungen für Online-Security-Diagnose und Laden in Station bei aktivierter Firewall.....	62
4.9.2.3	Schreibweise der Quell-IP-Adresse (erweiterter Firewall-Modus).....	63
4.9.2.4	Firewall-Einstellungen für S7-Verbindungen über VPN-Tunnel .....	63
4.9.3	Log-Einstellungen - Filtern der System-Ereignisse.....	64
4.9.4	E-Mail-Projektierung .....	64
4.9.5	VPN.....	65
4.9.5.1	VPN (Virtual Private Network).....	65
4.9.5.2	SINEMA Remote Connect .....	66
4.9.5.3	VPN-Tunnel für S7-Kommunikation zwischen Stationen anlegen.....	69
4.9.5.4	VPN-Kommunikation mit SOFTNET Security Client (Engineering-Station) .....	70
4.9.5.5	VPN-Tunnelkommunikation zwischen CP und SCALANCE M aufbauen.....	71
4.9.5.6	CP als passiver Teilnehmer von VPN-Verbindungen .....	71
4.9.6	SNMP .....	72
4.9.7	Zertifikatsmanager .....	73
4.10	Nachrichten: E-Mails (CP 1543SP-1) .....	75
<b>5</b>	<b>Programmbausteine.....</b>	<b>79</b>
5.1	Programmbausteine für OUC .....	79
5.2	Änderung der IP-Parameter zur Laufzeit .....	82
5.3	MODBUS-Bausteine .....	83
<b>6</b>	<b>Diagnose und Instandhaltung.....</b>	<b>85</b>
6.1	Diagnosemöglichkeiten.....	85
6.2	Online-Security-Diagnose über Port 8448 (CP 1542SP-1 IRC, CP 1543SP-1) .....	88
6.3	Diagnose über SNMP .....	88
6.4	Webserver der CPU.....	90
6.5	Bearbeitungsstatus von E-Mails (CP 1543SP-1).....	92
6.6	Firmware laden .....	94
6.7	Baugruppentausch.....	96
<b>7</b>	<b>Technische Daten.....</b>	<b>97</b>
<b>A</b>	<b>Zulassungen.....</b>	<b>99</b>
<b>B</b>	<b>Maßzeichnungen .....</b>	<b>105</b>
<b>C</b>	<b>Zubehör.....</b>	<b>107</b>

C.1	BusAdapter .....	107
C.2	Router SCALANCE M.....	109
<b>D</b>	<b>Literaturverzeichnis.....</b>	<b>111</b>
	<b>Index.....</b>	<b>115</b>



# Anwendung und Funktionen

## 1.1 Lieferumfang

Folgende Teile gehören zum Lieferumfang des Produkts:

- CP 154xSP-1
- Stecker für die Buchse der Spannungsversorgung (DC 24 V) des CP
- DVD mit Dokumentation und Lizenztexten

Ein BusAdapter für den Ethernet-Anschluss des CP ist nicht Teil des Lieferumfangs.

## 1.2 Anwendung

### Anwendung der CP-Varianten

Der CP dient dem Anschluss der ET 200SP an Industrial Ethernet über Kupferkabel oder Lichtwellenleiter. Er kann als zusätzliche Ethernet-Schnittstelle der CPU für die S7-Kommunikation genutzt werden.

Für den Ethernet-Anschluss benötigt der CP einen BusAdapter. Der BusAdapter ist nicht im Lieferumfang des CP enthalten. Zu den kompatiblen BusAdaptern siehe Kapitel BusAdapter (Seite 107).

Die drei CP-Typen sind für folgende Kommunikationsaufgaben vorgesehen:

- **CP 1542SP-1**

Der CP 1542SP-1 ermöglicht der ET 200SP einen weiteren Ethernet-Anschluss.

- **CP 1543SP-1**

Der CP 1543SP-1 verfügt über Security-Funktionen für die Netzwerksicherheit, wie zum Beispiel Firewall und VPN. Damit ist ein geschützter Zugriff auf die ET 200SP möglich.

- **CP 1542SP-1 IRC**

Der CP 1542SP-1 IRC unterstützt Telecontrol-Kommunikation zur Anbindung der ET 200SP-CPU an eine Leitstelle. Eines der folgenden Telecontrol-Protokolle kann alternativ verwendet werden:

- TeleControl Basic  
Zum Anschluss der ET 200SP-CPU an eine Leitstelle mit Telecontrol-Server (TCSB)
- ST7  
Zum Anschluss der ET 200SP-CPU an eine Leitstelle mit SINAUT ST7
- DNP3  
Zum Anschluss der ET 200SP-CPU an DNP3-Master
- IEC 60870-5-104  
Zum Anschluss der ET 200SP-CPU an IEC-Master

## 1.3 Kommunikationsdienste

### Kommunikationsdienste

Folgende Kommunikationsdienste werden unterstützt:

- **S7-Kommunikation und PG/OP-Kommunikation mit folgenden Funktionen:**
  - PUT/GET als Client und Server zum Datenaustausch mit S7-Stationen
  - USEND/URCV zum unkoordinierten Datenaustausch mit einem remoten Partner
  - BSEND/BRCV zum Austausch größerer Datenmengen mit einem Partner
  - PG-Funktionen
  - Bedien- und Beobachtungsfunktionen (HMI)

Für vollspezifizierte S7-Verbindungen benötigt der CP eine feste IP-Adresse.

- **S7-Routing**
  - Routing von S7-Verbindungen über den Rückwandbus und die CPU zu anderen S7-Stationen
- **SINEMA Remote Connect (SINEMA RC)**

Ab Firmware-Version V2.0 unterstützen die folgenden CP-Typen Kommunikation über SINEMA RC ab Software-Version V1.3:

- CP 1542SP-1 IRC
- CP 1543SP-1

Siehe Kapitel Kommunikation über SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1) (Seite 18).

Zum Handbuch siehe /8/ (Seite 113).

- **Open User Communication (OUC)**

OUC über Programmbausteine mit folgenden Protokollen:

- TCP/IP
- ISO-on-TCP
- UDP

Der CP 1543SP-1 unterstützt Secure OUC.

Die von den drei CP-Typen unterstützten Programmbausteine finden Sie im Kapitel Programmbausteine (Seite 79).

- **E-Mail über Programmbausteine**

- **HTTP / HTTPS**

Über HTTP / HTTPS können Sie auf den Webserver der CPU zugreifen.

Zur Telecontrol-Kommunikation des CP 1542SP-1 IRC siehe Kapitel Telecontrol-Kommunikation (CP 1542SP-1 IRC) (Seite 15).

Zu den Security-Funktionen des CP 1543SP-1 siehe Kapitel Security-Funktionen (CP 1542SP-1 IRC, CP 1543SP-1) (Seite 19).

## 1.4 Telecontrol-Kommunikation (CP 1542SP-1 IRC)

### Telecontrol-Protokolle

Zusätzlich zu den oben genannten Kommunikationsdiensten unterstützt der CP 1542SP-1 IRC die folgenden Fernwirkprotokolle zur Kommunikation mit einer Zentrale und anderen Telecontrol-Stationen:

- **TeleControl Basic \***

Proprietäres Protokoll für Fernwirkapplikationen. Das IP-basierte Protokoll dient der Anbindung des CP an die Applikation TCSB.

TCSB ist auf einem PC in der Zentrale installiert, dem Telecontrol-Server. Über den OPC-DA- bzw. OPC-UA-Server von TCSB kann ein OPC-Client auf die Prozessdaten des CP zugreifen.

TCSB wird ab folgender Version unterstützt: V3.0 + SP3

Zum Handbuch von TCSB siehe /4/ (Seite 112).

- **ST7**

Proprietäres Protokoll für Fernwirkapplikationen im System SINAUT ST7. Das Protokoll dient der Anbindung des CP an ST7-Leitstellen.

Das Protokoll SINAUT ST7 unterstützt unter anderem folgende Funktionen:

- Kommunikation mit der Zentrale
- Querkommunikation mit anderen Stationen
- Übertragungsprotokoll MSC

Unter SINAUT ST7 verwendet der CP auf der OSI-Schicht 3 das Übertragungsprotokoll MSC in folgenden Varianten:

- MSC (Standardeinstellung)
- MSCsec bei höheren Ansprüchen an die Sicherheit ("Security" aktiviert)
- Kommunikation über Mobilfunk

Die Kommunikation über ein Mobilfunknetz in Kombination mit dem Internet wird über einen Router SCALANCE M ermöglicht. Die Produktreihe SCALANCE M bietet verschiedene VPN-Router mit IPSec, Verschlüsselungssoftware und eigener Firewall.

Eine Auflistung der Router finden Sie im Anhang Router SCALANCE M (Seite 109).

- **DNP3 \***

Der CP fungiert als DNP3-Station (Outstation).

Die Kommunikation basiert auf der DNP3 SPECIFICATION Version 2.11 (2007/2009).

Eine ausführliche Übersicht der Attribute und Eigenschaften des DNP3-Protokolls, die vom CP unterstützt werden, finden Sie im DNP3-Geräteprofil, siehe:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/man>)

Kommunikationspartner des CP können sein:

DNP3-Master:

- SIMATIC PCS 7 TeleControl
- SIMATIC WinCC TeleControl
- SIMATIC WinCC OA
- Eine DNP3-fähige TIM-Baugruppe (TIM 3V IE DNP3 / TIM 4R IE DNP3)  
Zum Handbuch der TIM-Baugruppe siehe /5/ (Seite 112).
- Fremdsysteme, welche die oben genannte DNP3-Spezifikation unterstützen.

DNP3-Stationen (Outstation):

- CPs in Stationen

Für die Direkte Kommunikation wird beim sendenden Datenpunkt die "Master-Funktion" aktiviert.



- **IEC 60870-5-104 \***

Der CP fungiert als Unterstation (Slave).

Die Kommunikation basiert auf der Spezifikation IEC 60870-5 Teil 104 (2006).

Eine ausführliche Übersicht der Attribute und Eigenschaften der IEC-Spezifikation, die vom CP unterstützt werden, finden Sie im IEC-Geräteprofil, siehe:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/man>)

Kommunikationspartner des CP können sein:

IEC-Master:

- SIMATIC PCS 7 TeleControl
- SIMATIC WinCC TeleControl
- SIMATIC WinCC OA
- Fremdsysteme, welche die oben genannte IEC-Spezifikation unterstützen.

Stationen:

- CPs in Stationen

Für die Direkte Kommunikation wird beim sendenden Datenpunkt die "Master-Funktion" aktiviert.

\* Telecontrol-Kommunikation mit der Zentrale optional über SINEMA Remote Connect, siehe Kapitel Kommunikation über SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1) (Seite 18).

## Weitere Eigenschaften des CP 1542SP-1 IRC

- **Datenpunktprojektierung**

Die Prozesswerte werden für die Kommunikation als Datenpunkte projektiert.

Zur Übertragung von Nutzdaten zwischen Station und Kommunikationspartner ist beim CP 1542SP-1 IRC keine Programmierung von Programmbausteinen erforderlich.

Die Datenbereiche im Speicher der CPU, welche für die Kommunikation mit dem Partner vorgesehen sind, werden Datenpunkt-bezogen im CP projektiert. Dabei adressiert jeder Datenpunkt eine PLC-Variable oder ein Element in einem Datenbaustein der CPU.

Die Datenpunkte können individuell im Leitsystem verarbeitet werden.

- **Nachrichten / E-Mail**

Bei projektierbaren Ereignissen im Prozessabbild der CPU kann der CP Nachrichten als E-Mail versenden. Die per E-Mail versendeten Daten werden über PLC-Variablen projektiert.

- **Sendepuffer**

Der CP speichert Werte von Datenpunkten, die als Ereignis projektiert sind, im Sendepuffer. Er überträgt die Daten spontan oder gebündelt an den Kommunikationspartner.

Die Daten werden nicht remanent gespeichert. Bei Spannungsausfall gehen sie verloren.

- **Analogwertvorverarbeitung**

Analogwerte können im CP nach verschiedenen Methoden vorverarbeitet werden.

Weitere Informationen finden Sie in den Telecontrol-Projektierungshandbüchern, siehe /10/ (Seite 113).

## 1.5 Kommunikation über SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1)

### Gültigkeit

Folgende Kommunikationsarten über SINEMA Remote Connect werden von den CPs unterstützt:

- CP 1543SP-1
  - Fernwartung über SINEMA Remote Connect
- CP 1542SP-1 IRC
  - Fernwartung über SINEMA Remote Connect
  - Telecontrol-Kommunikation über SINEMA Remote Connect

Beachten Sie dies bei den unten beschriebenen Anwendungsfällen.

### Kommunikation über SINEMA Remote Connect (SINEMA RC)

Die Applikation "SINEMA RC Server" bietet ein durchgängiges Verbindungsmanagement von verteilten Netzwerken über das Internet. Dazu gehört auch der sichere Fernzugriff auf unterlagerte Stationen. Die Kommunikation zwischen SINEMA RC Server und den entfernten Teilnehmern läuft über VPN-Tunnel unter Berücksichtigung der hinterlegten Zugriffsrechte.

SINEMA RC verwendet OpenVPN zur Verschlüsselung der Daten. Zentrum der Kommunikation ist der SINEMA RC-Server, über den die Kommunikation zwischen den Teilnehmern läuft und der die Konfiguration des Kommunikationssystems verwaltet.

Router SCALANCE M, die Sie für die Verbindung einsetzen können, unterstützen auch OpenVPN und die Anbindung an SINEMA Remote Connect.

Zur erforderlichen Firmware-Version des CP für die Kommunikation über SINEMA RC siehe Kapitel Kommunikationsdienste (Seite 14).

### Parametergruppen

Die Projektierung der Kommunikation über SINEMA RC und der Telecontrol-Kommunikation über SINEMA RC führen Sie in zwei Parametergruppen durch:

- Kommunikation über SINEMA RC:
  - > "Security > VPN"
- Telecontrol-Kommunikation über SINEMA RC:
  - > "Kommunikationsarten"

Zur Projektierung siehe Telecontrol-Projektierungshandbücher /10/ (Seite 113).

## Anwendungen

Aus der Kombination der Parameter für Telecontrol-Kommunikation und SINEMA RC ergeben sich folgende Anwendungsmöglichkeiten.

Anwendungsfall:

- (1) Kein Telecontrol und kein SINEMA RC (CP nur für Netzwerktrennung)
- (2) CP nur für Fernwartung über SINEMA RC
- (3) CP nur für Telecontrol-Kommunikation
- (4) CP nutzt Telecontrol-Kommunikation, SINEMA RC aber nur für Fernwartung.
- (5) CP nutzt SINEMA RC für Telecontrol-Kommunikation und Fernwartung.

Die Tabelle gibt einen Überblick über die Anwendungsfälle mit den jeweiligen Parameter-Einstellungen.

- "Ein" bedeutet Parameter aktiviert.
- "Aus" bedeutet Parameter deaktiviert.

Tabelle 1- 1 Anwendungsfälle und zu aktivierende Parameter

Anwendungsfall	Parameter-Einstellungen (Parameter abgekürzt) *		
	SRC	TC	TC-SRC
(1)	Aus	Aus	Aus
(2)	Ein	Aus	Aus
(3)	Aus	Ein	Aus
(4)	Ein	Ein	Aus
(5)	Ein	Ein	Ein

\* Bedeutung der Parameter-Abkürzungen:

**SRC** - Security > VPN (aktiviert) > "VPN-Verbindungstyp":

"Automatische OpenVPN-Konfiguration über SINEMA Remote Connect Server"

**TC** - Kommunikationsarten > Telecontrol-Kommunikation aktiviert

**TC-SRC** - Kommunikationsarten >

"Telecontrol-Kommunikation über SINEMA Remote Connect aktivieren"

## 1.6 Security-Funktionen (CP 1542SP-1 IRC, CP 1543SP-1)

Security-Funktionen stehen für folgende CP-Typen zur Verfügung:

- CP 1543SP-1

Die Security-Funktionen werden in der Projektierung des CP aktiviert.

- CP 1542SP-1 IRC

Die Beschreibung der Security-Funktionen finden Sie in den Telecontrol-Projektierungshandbüchern, siehe /10/ (Seite 113).

Zu den Security-Funktionen der Programmbausteine der Open User Communication siehe Kapitel Programmbausteine (Seite 79).

---

**Hinweis**

**Empfehlung für sicherheitskritische Anlagen**

Beachten Sie die Hinweise im Kapitel Security-Empfehlungen (Seite 49).

---

**CP 1543SP-1**

Mit Industrial Ethernet Security können einzelne Geräte, Automatisierungszellen oder Netzsegmente eines Ethernet-Netzwerks abgesichert werden. Die Datenübertragung über den CP 1543SP-1 kann durch die Kombination unterschiedlicher Sicherheitsmaßnahmen vor folgenden Angriffen geschützt werden:

- Datenspionage
- Datenmanipulation
- Unberechtigte Zugriffe

Über zusätzliche Ethernet-/PROFINET-Schnittstellen der CPU können sichere unterlagerte Netze betrieben werden.

Durch die Verwendung des CP als Security-Modul werden für die ET 200SP-Station folgende Security-Funktionen an der Schnittstelle zum Ethernet-Netz zugänglich:

- **Firewall**

Die Firewall schützt das Gerät über:

- IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
- Firewall auch für "Non-IP"-Ethernet-Frames gemäß IEEE 802.3 (Layer 2)
- Begrenzung der Übertragungsgeschwindigkeit zur Einschränkung von Flooding- und DoS-Angriffen ("IP-Paketfilter-Regeln definieren")

- **Zertifikate**

Für die sichere Authentifizierung der Kommunikationspartner werden Zertifikate genutzt.

- **VPN**

Folgende Alternativen sind nutzbar:

- Gesicherte Kommunikation durch IPsec-Tunnel

Die VPN-Kommunikation ermöglicht den Aufbau von gesicherten IPsec-Tunneln für die Kommunikation mit einem oder mehreren Security-Modulen. Der CP kann mit anderen Baugruppen per Projektierung zu VPN-Gruppen zusammengefasst werden. Zwischen allen Security-Modulen einer VPN-Gruppe werden IPsec-Tunnel aufgebaut.

- Fernwartung über SINEMA Remote Connect

Für die Kommunikation über einen SINEMA RC-Server ist das Anlegen einer VPN-Gruppe nicht erforderlich und nicht möglich. Der SINEMA RC-Server verwaltet die Kommunikation zwischen den Teilnehmern und die Security-Mechanismen (OpenVPN).

Zur Projektierung siehe Kapitel SINEMA Remote Connect (Seite 66).

- **Logging**

Zur Überwachung kann das Versenden von Ereignissen aktiviert werden. Die Ereignisse können mithilfe von STEP 7 ausgelesen oder an einen Syslog-Server gesendet werden.

- **Verschlüsselte E-Mails**

Für die gesicherte Übertragung von Informationen mithilfe verschlüsselter E-Mails können Sie alternativ verwenden:

- SSL/TLS
- STARTTLS

Zur Projektierung siehe Kapitel E-Mail-Projektierung (Seite 64).

- **NTP (secure)**

Zur sicheren Übertragung bei der Uhrzeitsynchronisation

- **SNMPv3**

Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen

Hinweise zur Projektierung der Security-Funktionen finden Sie im Kapitel Security (CP 1543SP-1) (Seite 61).

Weitere Informationen zur Funktionalität und Projektierung der Security-Funktionen finden Sie im Informationssystem von STEP 7.

## CP 1542SP-1 IRC

Der CP unterstützt folgende Security-Funktionen:

- **Verschlüsselte E-Mails**

Für die gesicherte Übertragung von Informationen mithilfe verschlüsselter E-Mails können Sie alternativ verwenden:

- SSL/TLS
- STARTTLS

Zur Projektierung siehe Kapitel E-Mail-Projektierung (Seite 64).

- **Zertifikate**

Für die sichere Authentifizierung der Kommunikationspartner werden Zertifikate genutzt.

- **Gesicherte Telecontrol-Kommunikation**

Die Telecontrol-Protokolle bieten folgende Security-Funktionen:

- **TeleControl Basic**

Als integrierte Security-Funktion verschlüsselt das Telecontrol-Protokoll die Daten bei der Übermittlung zwischen CP und Telecontrol-Server. Das Intervall des Schlüsselaustausches zwischen CP und Telecontrol-Server ist einstellbar.

Das Telecontrol-Passwort dient zur Authentifizierung des CP beim Telecontrol-Server.

Bei aktivierten Security-Funktionen kann der CP Telecontrol-Kommunikation über SINEMA Remote Connect abwickeln.

- **SINAUT ST7**

Die vom CP für die Telecontrol-Kommunikation über das ST7-Protokoll anwendbaren Übertragungsprotokolle unterstützen folgende Security-Funktionen:

- MSC

Das MSC-Protokoll unterstützt die Authentifizierung der Kommunikationspartner und eine einfache Verschlüsselung der Daten. In die Verschlüsselung gehen ein Benutzername und ein Passwort ein. Zwischen MSC-Station und MSC-Zentrale wird ein Tunnel aufgebaut.

- MSCsec

Zusätzlich zu MSC wird bei MSCsec der gemeinsame automatisch generierte Schlüssel in einem projektierbaren Intervall zwischen den Kommunikationspartnern erneuert.

- **DNP3**

Der CP unterstützt Authentifizierung gemäß der Spezifikation "Secure Authentication V5".

Bei aktivierten Security-Funktionen kann der CP Telecontrol-Kommunikation über SINEMA Remote Connect abwickeln.

- **IEC 60870-5-104**

Bei aktivierten Security-Funktionen kann der CP Telecontrol-Kommunikation über SINEMA Remote Connect abwickeln.

Zur Kommunikation über SINEMA Remote Connect siehe Kapitel Kommunikation über SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1) (Seite 18).

## 1.7 Weitere Dienste und Eigenschaften

### Weitere Dienste und Eigenschaften des CP

- **IP-Konfiguration**

- Adresstypen

Der CP unterstützt IP-Adressen gemäß IPv4 und IPv6.

- Adressierung

Die IP-Adresse, die Subnetzmaske und die Adresse eines Netzübergangs können manuell in der Projektierung eingestellt werden. Alternativ kann die IP-Adresse über Programmbausteine bezogen werden.

- DHCP: Alternativ kann die IP-Adresse von einem DHCP-Server bezogen werden.

- DCP (Discovery and Configuration Protocol) wird unterstützt.

- **Uhrzeitsynchronisation**
  - NTP  
Der CP kann seine Uhrzeit über NTP synchronisieren.  
CP 1543SP-1: Bei aktivierten Security-Funktionen kann das gesicherte Verfahren NTP (secure) verwendet werden.
  - CP 1542SP-1 IRC: Uhrzeit vom Partner  
Bei aktivierter Telecontrol-Kommunikation kann der CP seine Uhrzeit auch vom Kommunikationspartner beziehen.  
Bei TeleControl Basic und DNP3 wird UTC-Zeit verwendet.  
Bei ST7 und IEC wird die Lokalzeit des Partner-PC verwendet.
  - Der CP kann die Uhrzeit der CPU über eine PLC-Variable zur Verfügung stellen.  
Weitere Informationen finden Sie im Kapitel Uhrzeitsynchronisation (Seite 56).
- **SNMP**  
Der CP unterstützt als SNMP-Agent Abfragen über SNMPv1.  
Der CP 1543SP-1 unterstützt zusätzlich SNMPv3.  
Weitere Informationen finden Sie im Kapitel SNMP (Seite 60).
- **E-Mail**  
Der CP 1542SP-1 IRC und der CP 1543SP-1 unterstützen das Versenden von E-Mails.

## 1.8 Mengengerüst und Leistungsdaten

### Anzahl der CPs pro Station

Pro ET 200SP-Station können bis zu drei Sonderbaugruppen gesteckt und projiziert werden, davon maximal zwei CP 154xSP-1.

Zu Details der erlaubten Sonderbaugruppen und den Steckplatzregeln siehe Kapitel CP montieren (Seite 42).

### Verbindungs-Ressourcen

#### Verbindungs-Ressourcen - gültig für alle CP-Varianten

Anzahl Verbindungen über Industrial Ethernet insgesamt maximal 32, davon:

- S7: Max. 16
- TCP/IP: Max. 32
- ISO-on-TCP: Max. 32
- UDP: Max. 32

**Zusätzlich:**

- Online-Verbindungen der Engineering-Station (STEP 7): Max. 2
- TCP-Verbindungen für HTTP

Für HTTP-Zugriffe stehen bis zu 12 TCP-Verbindungsressourcen zur Verfügung, die von einem oder mehreren Webbrowsern genutzt werden, um Daten des CP anzuzeigen.

- PG/OP-Verbindungen (HMI): Insgesamt maximal 16, davon:
  - Verbindungs-Ressourcen für PG-Verbindungen: Max. 16
  - Verbindungs-Ressourcen für OP-Verbindungen: Max. 16

## CP 1543SP-1

### Security-Funktionen des CP 1543SP-1

- **VPN-Tunnel (IPsec)**

Es können maximal vier **IPsec**-Tunnel für die gesicherte Kommunikation mit weiteren Security-Modulen aufgebaut werden.

- **Firewall-Regeln**

Die maximale Anzahl der Firewall-Regeln im erweiterten Firewall-Modus ist auf 256 begrenzt. Die Firewall-Regeln teilen sich wie folgt auf:

- Maximal 226 Regeln mit einzelnen Adressen
- Maximal 30 Regeln mit Adressbereichen oder Netzadressen (z. B. 140.90.120.1 - 140.90.120.20 oder 140.90.120.0/16)
- Maximal 128 Regeln mit Begrenzung der Übertragungsgeschwindigkeit ("Bandbreitenbegrenzung")

- **E-Mail (über Nachrichteneditor)**

Es können bis zu 10 zu versendende E-Mails projiziert werden.

Maximale Anzahl an Zeichen, die pro E-Mail übertragen werden kann: 256 ASCII-Zeichen inklusive eines evtl. mitgeschickten Werts



## CP 1542SP-1 IRC

### Telecontrol-Funktionen des CP 1542SP-1 IRC

- **Telecontrol-Verbindungen**

- TeleControl Basic

Es kann eine Verbindung zu einem einfach oder redundant aufgebauten Telecontrol-Server aufgebaut werden.

- SINAUT ST7

Der CP kann bis zu 8 ST7-Verbindungen aufbauen, davon maximal:

- 8 Einzel-Verbindungen mit Partnern
- 4 redundante Verbindungen mit Partnern
- 8 Verbindungen zur Querkommunikation zwischen ST7-Stationen
- Eine Mischung der drei Möglichkeiten

- DNP3 / IEC 60870-5-104

Es können Verbindungen mit bis zu 4 einfachen oder redundanten Mastern aufgebaut werden.

- **E-Mail (über Nachrichteneditor)**

Bis zu 10 zu versendende E-Mails können projiziert werden.

Maximale Anzahl an Zeichen, die pro E-Mail übertragen werden kann: 256 ASCII-Zeichen inklusive eines evtl. mitgeschickten Werts

- **Telegrammspeicher (Sendepuffer)**

Der CP besitzt einen Telegrammspeicher (Sendepuffer) für die Werte von Datenpunkten, die als Ereignis projiziert sind.

Das Volumen des Sendepuffers teilt sich auf alle projizierten Kommunikationspartner zu gleichen Teilen auf. Die Größe des Sendepuffers ist in STEP 7 projektierbar (Parametergruppe "Kommunikation mit der CPU").

Die maximale Größe des Sendepuffers beträgt beim jeweiligen Fernwirkprotokoll:

- TeleControl Basic  
64000 Ereignisse
- SINAUT ST7  
32000 Ereignisse
- DNP3  
100000 Ereignisse
- IEC 60870-5-104  
100000 Ereignisse

Zu Details zur Funktion des Sendepuffers wie dem Speichern von Ereignissen und den Übertragungsmöglichkeiten der Daten siehe /10/ (Seite 113).

- **Datenpunkte**

Die vom CP zu übertragenden Daten werden in der STEP 7-Projektierung verschiedenen Datenpunkten zugeordnet. Die Größe der Nutzdaten pro Datenpunkt hängt vom Datentyp des jeweiligen Datenpunkts ab. Zu Details siehe /10/ (Seite 113).

- Telecontrol Basic: 500
- ST7: 1500
- DNP3: 1500
- IEC: 1500

## 1.9 Voraussetzungen für den Einsatz

### 1.9.1 Hardware-Voraussetzungen

#### BusAdapter

Für den Anschluss an das Ethernet-Netz benötigt der CP einen BusAdapter. Ein BusAdapter ist nicht Teil des Lieferumfangs des CP.

Der CP unterstützt folgende BusAdapter:

- BA 2xRJ45
- BA 2xFC
- BA 2xSCRJ
- BA SCRJ/RJ45
- BA SCRJ/FC

Weitere Details zu den BusAdaptoren finden Sie im Anhang BusAdapter (Seite 107) und im Handbuch /3/ (Seite 112).

#### CPUs und weitere Komponenten der ET 200SP

Der CP unterstützt den Betrieb in Stationen, die eine der folgenden CPUs enthalten:

- CPU 1510SP-1 PN  
Artikelnummer: 6ES7510-1DJ01-0AB0
- CPU 1510SP F-1 PN  
Artikelnummer: 6ES7510-1SJ01-0AB0

- CPU 1512SP-1 PN  
Artikelnummer: 6ES7512-1DK01-0AB0
- CPU 1512SP F-1 PN  
Artikelnummer: 6ES7512-1SK01-0AB0

Weitere Teile und Module, die zusätzlich für den Aufbau der ET 200SP-Station benötigt werden, wie Schienen, Peripheriemodule oder Verkabelung, werden hier nicht aufgeführt. Siehe hierzu /3/ (Seite 112).

### Komponenten der Kommunikationspartner

Komponenten, die von den Kommunikationspartnern des CP 1542SP-1 IRC benötigt werden, sind hier nicht aufgeführt. Verweise zur Dokumentation weiterer Produkte (bspw. TCSB) finden Sie im Literaturverzeichnis im Anhang des Handbuchs.

## 1.9.2 Software-Voraussetzungen

### Projektierungs-Software

Für die Projektierung der gesamten Funktionalität der in diesem Dokument beschriebenen Firmware-Version des CP ist das folgende Projektierungswerkzeug erforderlich:

- STEP 7 Professional V16

### Software für Online-Funktionen

Für die Nutzung der Online-Funktionen ist folgende Software erforderlich:

- STEP 7 in der oben angegebenen Version.

### CPU-Firmware

Für den Einsatz des CP wird eine CPU 151xSP mit einer Firmware-Version  $\geq$  V2.0 benötigt.

## 1.10 Konfigurationsbeispiele

Nachfolgend finden Sie Konfigurationsbeispiele für den Einsatz der drei CP-Typen.

### CP 1542SP-1 - Netzwerktrennung

Der CP wird in der ET 200SP verwendet, um unterlagerte Netzwerke getrennt zu betreiben oder eine Trennung vom überlagerten Netzwerk zu erreichen.

Die ET 200SP kann flexibel um weitere Ethernet-Schnittstellen über den CP erweitert werden. Durch die Netzwerktrennung wird der Aufbau identischer Maschinen mit gleichen IP-Adresse ermöglicht. Der CP übernimmt die Kommunikation und entlastet die CPU.

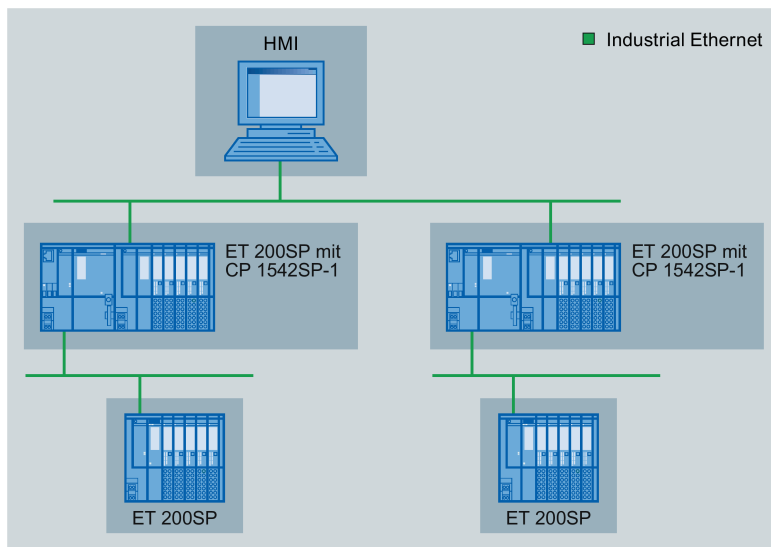


Bild 1-1 Konfigurationsbeispiel einer ET 200SP mit CP 1542SP-1

### CP 1543SP-1 - Zellschutz durch Security-Funktionen

Der CP kommuniziert verschlüsselt mit Kommunikationspartnern im angeschlossenen Netzwerk. Die Firewall überwacht den Zugriff auf die ET 200SP und schützt damit unterlagerte Netzwerke. Dadurch werden Datenverlust, Störungen der Produktion und Schäden an Maschinen vermieden.

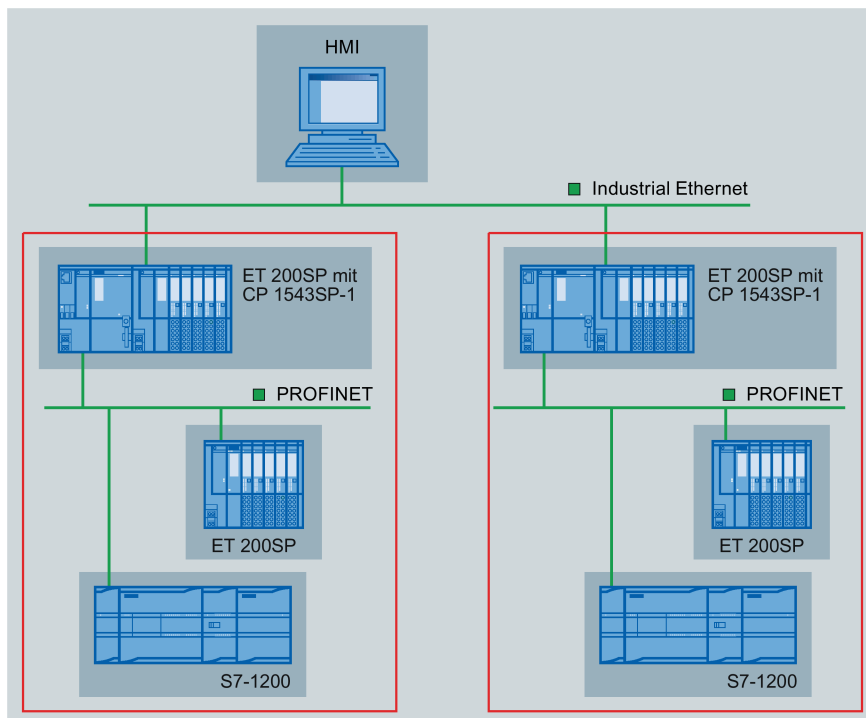


Bild 1-2 Konfigurationsbeispiel einer ET 200SP mit CP 1543SP-1

## CP 1542SP-1 IRC - Anbindung an Leitzentralen

Durch den Einsatz des CP kann die ET 200SP als Remote Terminal Unit eingesetzt werden. Für die Telecontrol-Kommunikation können folgende Protokolle eingesetzt werden:

- TeleControl Basic
- SINAUT ST7
- IEC 60870-5-104
- DNP3

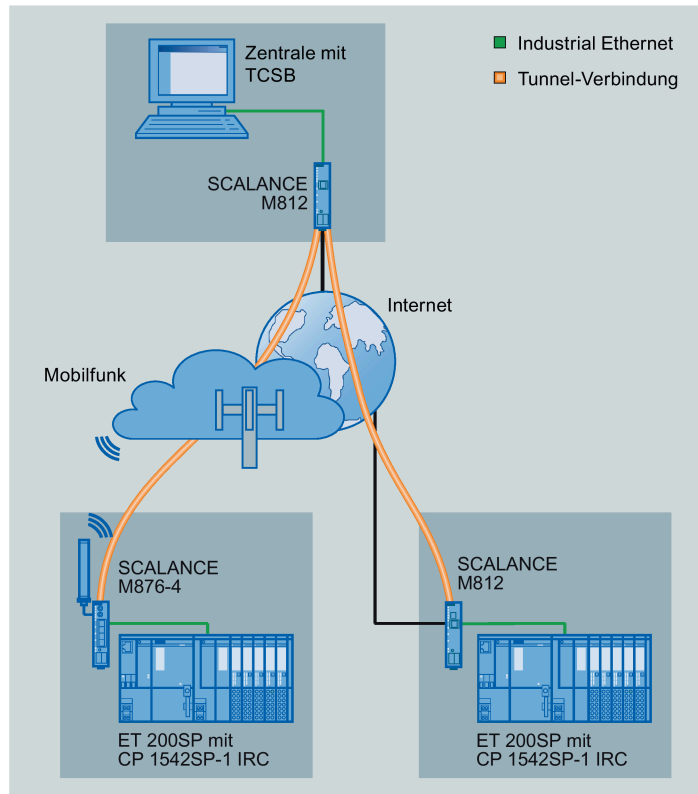


Bild 1-3 Konfigurationsbeispiel einer ET 200SP mit CP 1542SP-1 IRC; Protokoll: TeleControl Basic

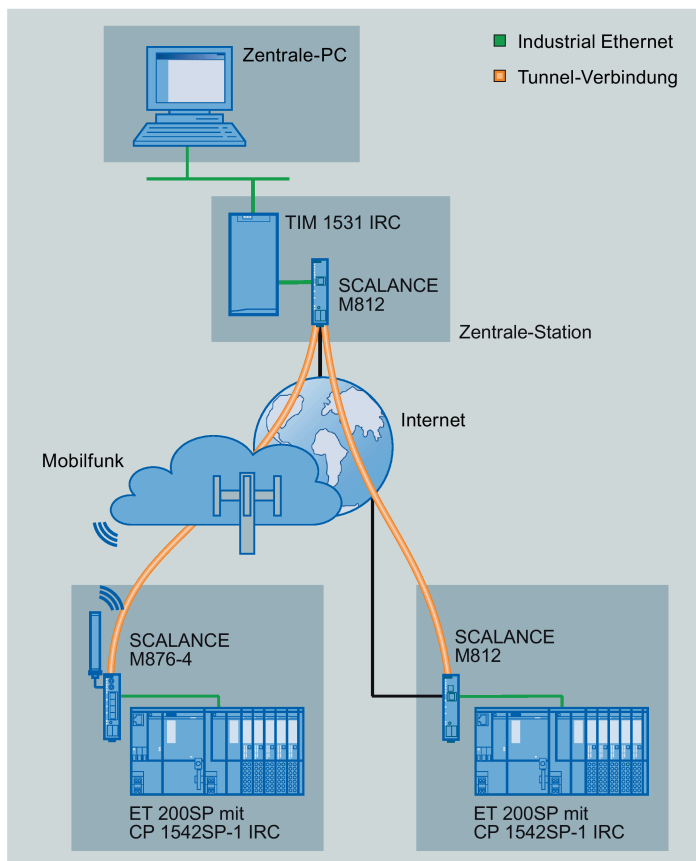


Bild 1-4 Konfigurationsbeispiel einer ET 200SP mit CP 1542SP-1 IRC; Protokoll: ST7

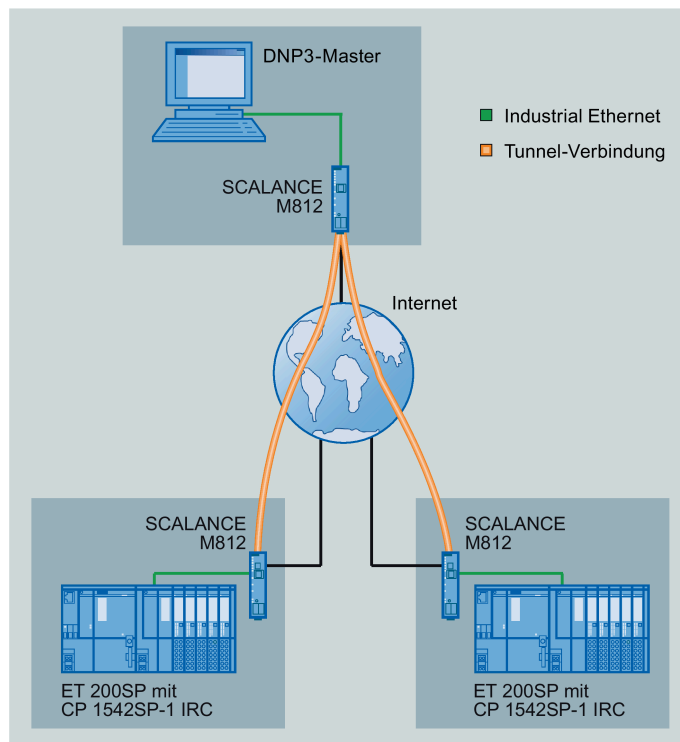


Bild 1-5 Konfigurationsbeispiel einer ET 200SP mit CP 1542SP-1 IRC; Protokoll: DNP3

Eine Konfiguration, bei dem das Protokoll IEC 60870-5-104 eingesetzt wird, könnte ähnlich aussehen.

### Telecontrol über SINEMA Remote Connect

Die folgende Abbildung zeigt eine Konfiguration, in welcher der CP 1542SP-1 IRC über einen SINEMA Remote Connect-Server mit der Zentrale kommuniziert. In diesem Beispiel verwendet der CP das Protokoll IEC 60870-5-104.

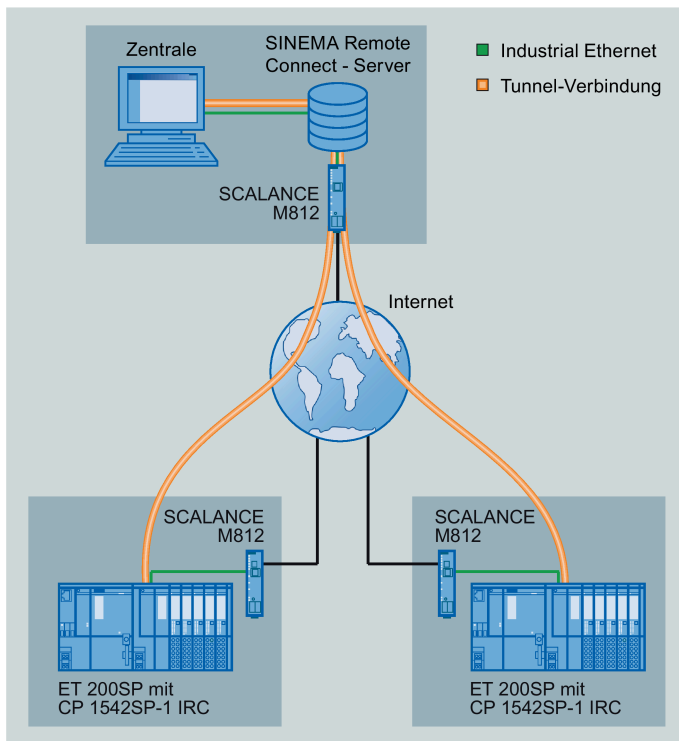


Bild 1-6 Konfigurationsbeispiel einer ET 200SP mit CP 1542SP-1 IRC für Telecontrol-Kommunikation über SINEMA RC



## Fernwartung mit SINEMA RC

Die folgende Abbildung zeigt die Anbindung verschiedener Stationen mit Security-CP an eine Engineering-Station über SINEMA Remote Connect - Server.

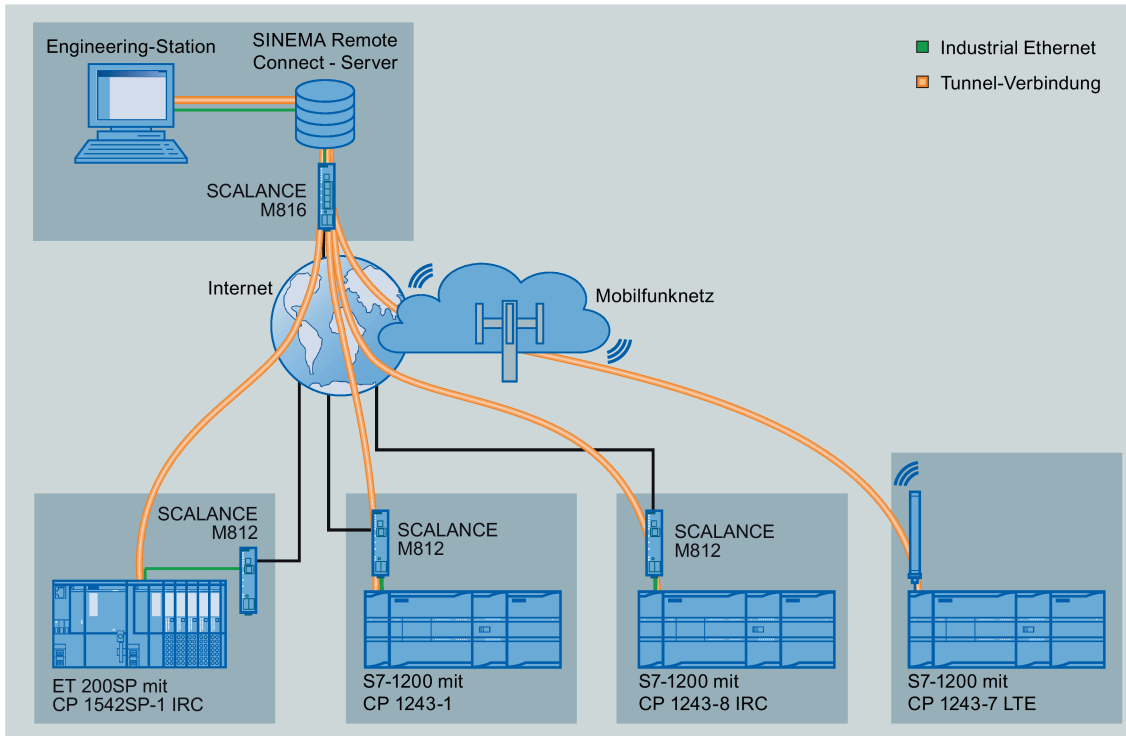


Bild 1-7 Anbindung von Stationen an Engineering-Station über SINEMA RC



## LEDs und Anschlüsse

### 2.1 LEDs

#### Bedeutung der LED-Anzeigen des CP

Der CP hat auf der Vorderseite folgende Leuchtdioden (LEDs):

LED-Name	Bedeutung
PWR	Spannungsversorgung
RN	Betriebszustand
ER	Fehler
MT	Wartung

Tabelle 2- 1 Legende zu den nachfolgenden Tabellen







































Symbol	  		  	-
Bedeutung / LED-Zustand	EIN (LED leuchtet)	AUS	LED blinkt	Beliebig

Tabelle 2- 2 Bedeutung der LED-Anzeigen des CP

PWR (grün)	RN (grün)	ER (rot)	MT (gelb)	Bedeutung
				Keine oder zu geringe Versorgungsspannung am CP
				Anlauf des CP
				CP im Betriebszustand RUN
	-			Fehler. LED-Bild bei folgenden Ereignissen: <ul style="list-style-type: none"> <li>Doppelte IP-Adresse</li> <li>Nicht gesteckter oder gezogener BusAdapter</li> <li>Keine Telecontrol-Verbindung (CP 1542SP-1 IRC)</li> </ul>
				Fehler: CP defekt
				<ul style="list-style-type: none"> <li>Anlauf</li> <li>Fehlende Projektierungsdaten</li> </ul>
				Firmware-Aktualisierung läuft.
				Eine Wartungsanforderung des CP liegt vor. Beispiel: <ul style="list-style-type: none"> <li>Ende der Firmware-Aktualisierung</li> </ul>

## LEDs der BusAdapter

Jeder Port eines BusAdapters verfügt über eine LED "LKx", die über den Verbindungszustand mit Ethernet und den Telegrammverkehr des Ports informieren.

Tabelle 2-3 Bedeutung der LED-Anzeigen der BusAdapter

LK (grün)	Bedeutung
○	Keine Ethernet-Verbindung. Mögliche Ursachen: <ul style="list-style-type: none"> <li>Keine physikalische Verbindung mit dem Netz</li> <li>Port in der Projektierung deaktiviert</li> </ul>
⦿	LED-Blinktest
●	Ethernet-Verbindung zwischen Port und Kommunikationspartner besteht.

## 2.2 Spannungsversorgung

### Externe Spannungsversorgung erforderlich

Der Anschluss für die externe Spannungsversorgung DC 24 V befindet sich auf der Vorderseite des CP.

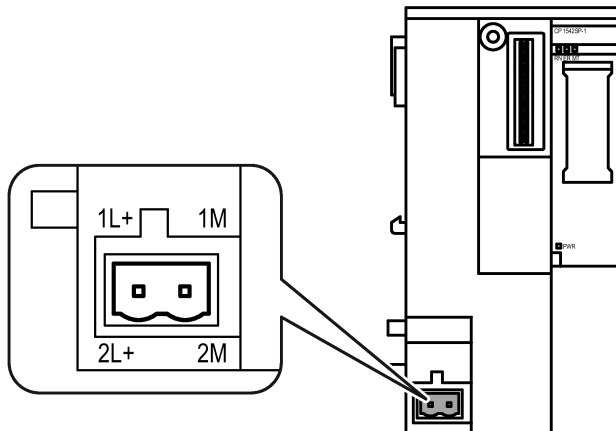


Bild 2-1 Spannungsversorgung des CP

Anschluss X80 ist für den Anschluss an eine einfache oder redundant ausgeführte Spannungsversorgung vorgesehen. Die Spannungsversorgung wird an den mit dem CP mitgelieferten steckbaren Klemmenblock angeschlossen. Der Klemmenblock wird in die Buchse X80 des CP gesteckt.

Informationen zur Montage und zum Anschluss finden Sie in den Kapiteln CP montieren (Seite 42) und CP anschließen (Seite 46).

## Verpolschutz

Der steckbare Klemmenblock für Anschluss X80 ist so ausgeführt, dass er nur in einer Position gesteckt werden kann. Hierdurch ergibt sich ein konstruktiver Verpolschutz.

Der Anschluss X80 besitzt außerdem einen elektronischen Verpolschutz.

Weitere Daten zur Spannungsversorgung finden Sie im Kapitel Technische Daten (Seite 97).

## 2.3 Anschluss für den BusAdapter

### Betrieb des Geräts nur mit BusAdapter

Für den Anschluss an Ethernet benötigt der CP einen BusAdapter. Ein BusAdapter ist nicht Teil des Lieferumfangs des CP.

Der Steckplatz befindet sich auf der Vorderseite des Geräts.

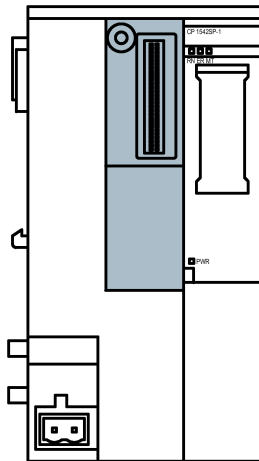


Bild 2-2 Frontseite des CP, der Steckplatz des BusAdapters ist grau gekennzeichnet.

Die vom CP unterstützten BusAdapter finden Sie im Kapitel BusAdapter (Seite 107).

Informationen zur Montage und zum Anschluss finden Sie in den Kapiteln CP montieren (Seite 42) und CP anschließen (Seite 46).

Die Belegung der Ethernet-Schnittstelle finden Sie im Kapitel BusAdapter (Seite 107). Weitere technische Daten der BusAdapter finden Sie im Handbuch /3/ (Seite 112).



# Montage, Anschluss, Inbetriebnahme

## 3.1 Wichtige Hinweise zum Geräteinsatz


### Sicherheitshinweise für den Geräteinsatz


Beachten Sie die folgenden Sicherheitshinweise für Aufstellung und Betrieb des Geräts und alle damit zusammenhängenden Arbeiten wie Montieren und Anschließen des Geräts oder Geräte austausch.

### Überspannungsschutz

<b>ACHTUNG</b>
<b>Schutz der externen Spannungsversorgung</b>
Wenn die Baugruppe oder die Station über ausgedehnte Versorgungsleitungen oder Netze gespeist wird, dann sind Einkopplungen starker elektromagnetischer Pulse auf die Versorgungsleitungen möglich, die z. B. durch Blitzschlag oder das Schalten großer Lasten entstehen können.
Der Anschluss der externen Spannungsversorgung ist nicht gegen starke elektromagnetische Pulse geschützt. Hierfür ist ein externes Überspannungsschutz-Modul erforderlich. Die Anforderungen nach EN61000-4-5, Surge-Prüfung auf Spannungsversorgungsleitungen, werden nur erfüllt bei Einsatz eines geeigneten Schutzelements. Geeignet ist der Dehn Blitzductor BVT AVD 24, Artikelnummer 918 422 oder ein gleichwertiges Schutzelement.
Hersteller: DEHN+SOEHNE GmbH+Co.KG, Hans-Dehn-Str.1, Postfach 1640, D-92306 Neumarkt

### 3.1.1 Hinweise für den Einsatz im Ex-Bereich

 <b>WARNUNG</b>
<b>EXPLOSIONSGEFAHR</b>
Öffnen Sie das Gerät nicht bei eingeschalteter Versorgungsspannung.

 <b>WARNUNG</b>
Das Gerät darf nur in einer Umgebung der Verschmutzungsstufe 1 oder 2 betrieben werden (vgl. IEC 60664-1).

 **WARNUNG**

Das Gerät ist für den Betrieb mit einer direkt anschließbaren Sicherheitskleinspannung (Safety Extra Low Voltage, SELV) durch eine Spannungsversorgung mit begrenzter Leistung (Limited Power Source, LPS) ausgelegt.

Deshalb dürfen nur Sicherheitskleinspannungen (SELV) mit begrenzter Leistung (Limited Power Source, LPS) nach IEC 60950-1 / EN 60950-1 / VDE 0805-1 mit den Versorgungsanschlüssen verbunden werden oder das Netzteil für die Versorgung des Geräts muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

Wenn das Gerät an eine redundante Spannungsversorgung angeschlossen wird (zwei getrennte Spannungsversorgungen), müssen beide die genannten Anforderungen erfüllen.

 **WARNUNG**

**EXPLOSIONSGEFAHR**

In einer leicht entzündlichen oder brennbaren Umgebung dürfen keine Leitungen an das Gerät angeschlossen oder vom Gerät getrennt werden.

 **WARNUNG**

**EXPLOSIONSGEFAHR**

Der Austausch von Komponenten kann die Eignung für Class I, Division 2 oder Zone 2 beeinträchtigen.

 **WARNUNG**

Bei Einsatz in explosionsgefährdeter Umgebung entsprechend Class I, Division 2 oder Class I, Zone 2 muss das Gerät in einen Schaltschrank oder in ein Gehäuse eingebaut werden.


 **WARNUNG**


**Hutschiene**


Im Anwendungsbereich von ATEX und IECEx darf nur die Siemens Hutschiene 6ES5 710-8MA11 zur Montage der Module verwendet werden.




### 3.1.2 Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx

 <b>WARNUNG</b>
<b>Anforderungen an den Schaltschrank</b> Um die EU-Richtlinie 2014/34 EU (ATEX 114) oder die Bedingungen von IECEx zu erfüllen, muss das Gehäuse oder der Schaltschrank mindestens die Anforderungen von IP54 (gemäß EN 60529) nach EN 60079-7 erfüllen.

 <b>WARNUNG</b>
<b>Kabel</b> Wenn am Kabel oder an der Gehäusebuchse Temperaturen über 70 °C auftreten oder die Temperatur an den Adernverzweigungsstellen der Leitungen über 80 °C liegt, müssen besondere Vorkehrungen getroffen werden. Wenn das Gerät bei Umgebungstemperaturen von über 50 °C betrieben wird, müssen Sie Kabel mit einer zulässigen Betriebstemperatur von mindesten 80 °C verwenden.

 <b>WARNUNG</b>
Treffen Sie Maßnahmen, um transiente Überspannungen von mehr als 40% der Nennspannung zu verhindern. Das ist gewährleistet, wenn Sie die Geräte ausschließlich mit SELV (Sicherheitskleinspannung) betreiben.


### 3.1.3 Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc

 <b>WARNUNG</b>
<b>EXPLOSIONSGEFAHR</b> Sie dürfen spannungsführende Leitungen nur trennen oder anschließen, wenn die Spannungsversorgung ausgeschaltet ist oder wenn sich das Gerät in einem Bereich ohne entflammbare Gas-Konzentrationen befindet.

Dieses Gerät ist nur für den Einsatz in Bereichen gemäß Class I, Division 2, Groups A, B, C und D und in nicht explosionsgefährdeten Bereichen geeignet.


Dieses Gerät ist nur für den Einsatz in Bereichen gemäß Class I, Zone 2, Group IIC und in nicht explosionsgefährdeten Bereichen geeignet.

### 3.1.4 Hinweise für den Einsatz im Ex-Bereich gemäß FM

 <b>WARNUNG</b>
<b>EXPLOSIONSGEFAHR</b>
Sie dürfen spannungsführenden Leitungen nur trennen oder anschließen, wenn die Spannungsversorgung ausgeschaltet ist oder wenn sich das Gerät in einem Bereich ohne entflammbare Gas-Konzentrationen befindet.

Dieses Gerät ist nur für den Einsatz in Bereichen gemäß Class I, Division 2, Groups A, B, C und D und in nicht explosionsgefährdeten Bereichen geeignet.

Dieses Gerät ist nur für den Einsatz in Bereichen gemäß Class I, Zone 2, Group IIC und in nicht explosionsgefährdeten Bereichen geeignet.

 <b>WARNUNG</b>
<b>EXPLOSIONSGEFAHR</b>
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 CP montieren

<b>ACHTUNG</b>
<b>Montage und Demontage des CP nur im spannungslosen Zustand!</b>
Schalten Sie die Spannungsversorgung der ET 200SP und des CP aus, bevor Sie die Module montieren oder demontieren. Montage oder Demontage bei eingeschalteter Versorgungsspannung kann zu einer Beschädigung der Module und zu Datenverlust führen.

### Hinweis

#### Aufbauhinweise beachten

Beachten Sie bei der Montage und beim Anschluss des CP die Ausführungen im Handbuch /3/ (Seite 112).

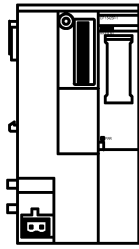
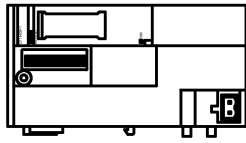
**ACHTUNG****Einbaulage - Abhängigkeit des Temperaturbereichs**

Die Montage muss so erfolgen, dass die oberen und unteren Lüftungsschlitze der Module nicht verdeckt werden und eine gute Durchlüftung möglich ist. Ober- und unterhalb der Module muss ein Freiraum von 25 mm für die Luftzirkulation als Schutz vor Überhitzung eingehalten werden.

Beachten Sie die Abhängigkeit des zulässigen Temperaturbereichs von der Einbaulage:

- Waagerechter Aufbau des Baugruppenträgers (Hutschiene) bedeutet senkrechte Lage des CP.
- Senkrechter Aufbau des Baugruppenträgers (Hutschiene) bedeutet waagerechte Lage des CP.

Die zulässigen Temperaturbereiche finden Sie im Kapitel Technische Daten (Seite 97).

Aufbau des Baugruppenträgers	Einbaulage des CP
Waagerechter Aufbau des Baugruppenträgers	
Senkrechter Aufbau des Baugruppenträgers	

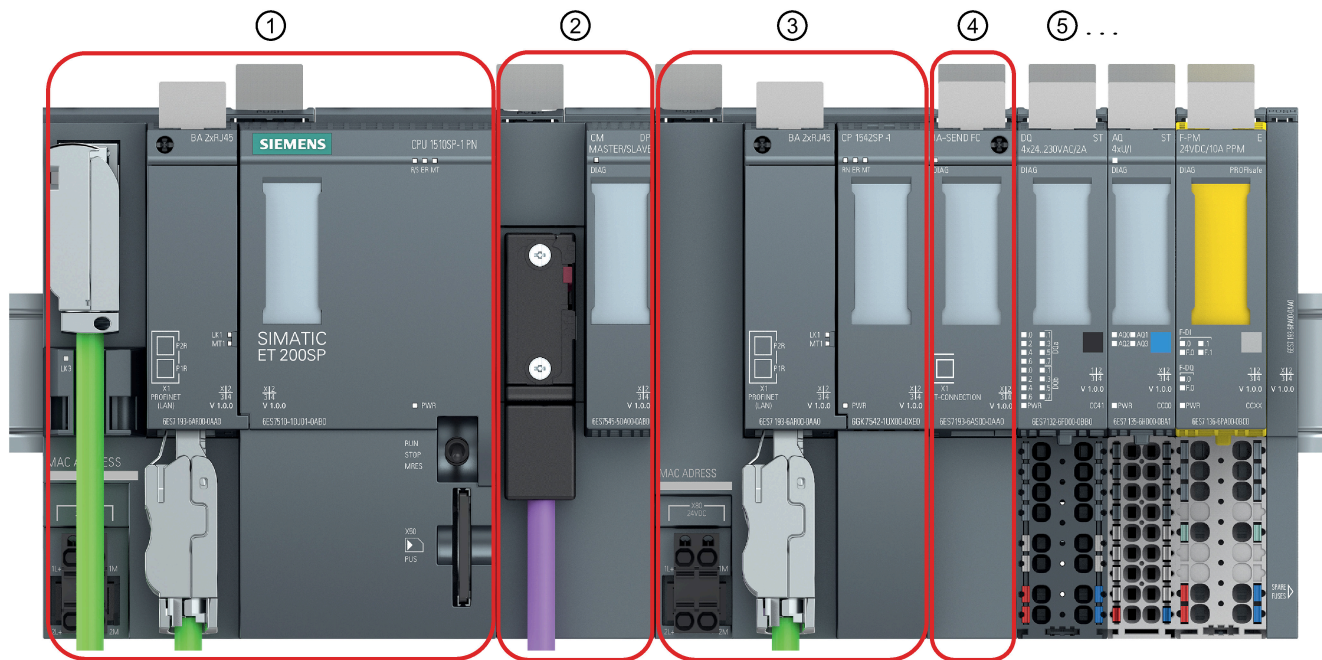
**Steckplatzregeln**

Die CPU belegt immer den Steckplatz 1. In einer ET 200SP können Sie auf den Steckplätzen 2 .. 4 (vgl. Abbildung) rechts neben der CPU bis zu drei der folgenden Module stecken:

- CMs
- CPs
- BusAdapter Send

Von diesen drei Modulen dürfen bis zu zwei CP 154xSP-1 gesteckt werden. Diese beiden CPs können vom gleichen Typ sein oder unterschiedlich.

Das CM DP darf nur direkt neben der CPU stecken.



- ① Steckplatz 1 - nur für die CPU zugelassen.
- ② Steckplatz 2 - für CM / CP / BusAdapter Send \*  
Wenn Sie ein PROFIBUS-CM nutzen, müssen Sie dieses direkt neben die CPU auf Steckplatz 1 stecken.
- ③ Steckplatz 3 - für CM / CP / BusAdapter Send \*
- ④ Steckplatz 4 - für CM / CP / BusAdapter Send \*
- ⑤ Steckplatz 5 ff - für Peripherie

\* Wenn Sie einen BusAdapter Send verwenden, dann muss dieser auf den Steckplatz direkt neben die Peripheriemodule gesteckt werden.

Bild 3-1 Steckplätze der ET 200SP

### Hutschienenmontage

#### Hinweis

#### Sicherung der Module vor Verrutschen auf der Hutschiene

Wenn Sie die Module in einem Bereich mit mechanischer Belastung montieren, dann verwenden Sie zur Sicherung der Module auf der Hutschiene geeignete Klemmvorrichtungen an beiden Enden der Gerätegruppe, z. B. Siemens-Endhalter 8WA1808.

Die Endhalter verhindern, dass die Module bei mechanischer Belastung auseinanderrutschen.

Beachten Sie bei Einsatz in Einsatzbereichen von ATEX oder IECEx den Hinweis zur Hutschiene im Kapitel Hinweise für den Einsatz im Ex-Bereich (Seite 39).

Das System ET 200SP ist geeignet für die Montage auf einer Profilschiene gemäß EN 60715 (35 × 7,5 mm oder 35 × 15 mm)

1. Hängen Sie die CPU / das Interfacemodul in die Profilschiene ein.
2. Schwenken Sie die CPU / das Interfacemodul nach hinten, bis die Profilschienenentriegelung hörbar einrastet.
3. Hängen Sie den CP rechts neben der CPU ein.
4. Schwenken Sie den CP nach hinten, bis die Profilschienenentriegelung hörbar einrastet.
5. Verschieben Sie den CP nach links, bis er hörbar in die CPU einrastet.
6. Montieren Sie die weiteren BaseUnits und Module entsprechend.

Siehe hierzu Handbuch /3/ (Seite 112).

### Stecken des BusAdapters

<b>ACHTUNG</b>
<b>Berühren der Steckkontakte</b>
Berühren Sie nicht die Steckkontakte, wenn kein BusAdapter gesteckt ist.

1. Schließen Sie die entsprechende Leitung am BusAdapter an, wenn Sie einen BusAdapter mit optischem oder direktem elektrischem Anschluss (ohne Stecker) verwenden.
2. Stecken Sie den BusAdapter in den Steckplatz des CP.

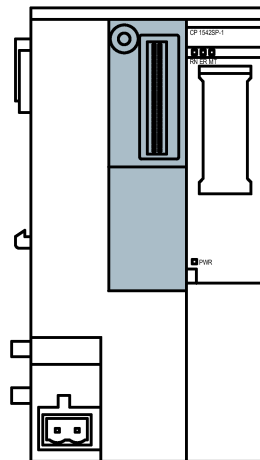


Bild 3-2 Vorderseite des CP; der Steckplatz des BusAdapters ist grau gekennzeichnet.

3.3 CP anschließen

3. Verschrauben Sie den BusAdapter mit dem CP.

Die Sicherungsschraube befindet sich links oben auf der Vorderseite des BusAdapters.

Verwenden Sie dazu einen Schraubendreher mit 3 bis 3,5 mm Klingenbreite oder einen passenden Torx-Schraubendreher (T15).

Das maximale Anzugsmoment beträgt 0,25 Nm.

4. Stecken Sie den Stecker der Anschlussleitung in die Buchse des BusAdapters, wenn Sie einen BusAdapter mit Stecker verwenden.

Zum Stecken der BusAdapter und zum Konfektionieren von Leitungen siehe auch Handbuch /3/ (Seite 112).

### Demontage von der Hutschiene

Führen Sie die folgenden Schritte durch, um einen CP von der Hutschiene zu demontieren:

1. Schalten Sie die Versorgungsspannung der gesamten Station inklusive CP und CPU aus.
2. Betätigen Sie die Profilschienenentriegelung der zu verschiebenden Module (CPU, CPs) und verschieben Sie diese parallel nach links, bis sie sich vom restlichen Modulverbund lösen (Freiraum ca. 16 mm).

Drücken Sie grundsätzlich den mit "PUSH" gekennzeichneten Verriegelungsschieber auf der Oberseite eines Moduls nach unten, um das betreffende Modul auf der Hutschiene bewegen zu können.

3. Betätigen Sie die Profilschienenentriegelung am CP und verschieben Sie ihn nach rechts, bis er sich von der CPU löst (Freiraum ca. 8 mm).
4. Schwenken Sie den CP bei gedrückter Profilschienenentriegelung am CP aus der Profilschiene heraus.

## 3.3 CP anschließen

### Reihenfolge der Arbeiten

<b>ACHTUNG</b>
<b>Anschluss nur im spannungslosen Zustand</b>
Schließen Sie den CP nur im spannungslosen Zustand an. Beachten Sie die Vorgaben im Systemhandbuch, siehe /2/ (Seite 112).

Der BusAdapter ist bereits an der entsprechenden Leitung angeschlossen, siehe Kapitel CP montieren (Seite 42).

1. Schließen Sie die externe Spannungsversorgung am Klemmenblock von Anschluss X80 an.

Verwenden Sie die gleiche Spannungsversorgung wie die CPU.

2. Schalten Sie die Spannungsversorgung erst ein, nachdem der CP komplett verdrahtet und angeschlossen ist.

### Spannungsversorgung am Anschluss X80

Die Lage des Anschlusses X80 für die Spannungsversorgung des CP finden Sie im Kapitel Spannungsversorgung (Seite 36). Dort finden Sie auch Hinweise zum Verpolschutz.

Der 2-polige steckbare Klemmenblock für die Buchse X80 hat folgende Belegung:

Klemme	Belegung
1L+ / 2L+	DC 24 V
1M / 2M	Masse

Die beiden Klemmen 1L+/L2+ sowie 1M/2M des Klemmenblocks sind jeweils intern gebrückt, so dass Sie entweder eine einfache oder eine redundante Spannungsversorgung anschließen können.

Anschließbare Leitungsquerschnitte:

- Ohne Adernendhülle: 0,2 .. 2,5 mm<sup>2</sup> / AWG 24 .. 13
- Mit Adernendhülle: 0,25 .. 1,5 mm<sup>2</sup> / AWG 24 .. 16
- Mit TWIN-Adernendhülle: 0,5 .. 1,0 mm<sup>2</sup> / AWG 20 .. 17

Angaben zu Leistungsaufnahme und weiteren technischen Details der Anschlüsse finden Sie im Kapitel Technische Daten (Seite 97).

## 3.4 CP in Betrieb nehmen

### Voraussetzung: Projektierung vor Inbetriebnahme

Voraussetzung für die komplette Inbetriebnahme der Baugruppe ist die Vollständigkeit der STEP 7-Projektdateien.

## Baugruppe in Betrieb nehmen

Die weitere Inbetriebnahme umfasst folgende Schritte:

1. Übersetzen der Projektdaten
2. Laden der STEP 7-Projektdaten in das Gerät

Die STEP 7-Projektdaten des CP werden beim Laden der Station mit übertragen.

Schließen Sie zum Laden der Station die Engineering-Station, auf der sich die Projektdaten befinden, an die CPU an.

Weitere Details finden Sie im STEP 7-Informationssystem im Kapitel "Projektdaten übersetzen und laden".

---

### Hinweis

#### Uhrzeitsynchronisation bei Nutzung von SINEMA RC

Wenn der CP die Uhrzeit von der CPU bezieht, dann stellen Sie bei Nutzung von SINEMA Remote Connect während der Inbetriebnahme manuell die Uhrzeit der CPU, siehe Hinweis in Kapitel CP in Betrieb nehmen (Seite 47).

---

## Uhrzeit bei der Inbetriebnahme manuell stellen

---

### Hinweis

#### Uhrzeitsynchronisation bei Nutzung von Security / SINEMA RC

Bei Nutzung von Security-Funktionen, beispielsweise SINEMA Remote Connect, benötigt der CP die aktuelle Uhrzeit für die Authentifizierung beim Partner bzw. am SINEMA RC-Server.

Der CP bezieht die Uhrzeit vor dem ersten Verbindungsaufbau von der CPU oder von einem NTP-Server.

#### Empfehlung:

Stellen Sie bei der Inbetriebnahme zumindest einmal die Uhrzeit der CPU manuell über die Online-Funktionen von STEP 7. Dies ist insbesondere dann notwendig, wenn Sie für die Uhrzeitsynchronisation die Option "Uhrzeit vom Partner" projiziert haben. Damit stellen Sie sicher, dass die CPU beim Anlauf der Station eine gültige Uhrzeit hat und der CP die erforderlichen Zertifikate mit dem Partner bzw. dem SINEMA RC-Server austauschen kann.

---



# Projektierung

## 4.1 Security-Empfehlungen

Beachten Sie folgende Security-Empfehlungen, um nicht autorisierte Zugriffe auf das System zu unterbinden.

---

### Hinweis

#### Security-Funktionen der CP-Typen

Die nachfolgenden Hinweise gelten - je nach unterstützter Funktion - nicht für jeden CP-Typ.

---

### Allgemein

- Stellen Sie regelmäßig sicher, dass das Gerät diese Empfehlungen und ggf. weitere interne Security-Richtlinien erfüllt.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellschutzkonzept mit entsprechenden Produkten.
- Verbinden Sie das Gerät nicht direkt mit dem Internet. Betreiben Sie das Gerät innerhalb eines geschützten Netzwerkbereichs.
- Informieren Sie sich regelmäßig über Neuigkeiten auf den Siemens-Internetseiten.
  - Hier finden Sie Informationen zu Industrial Security:  
Link: (<http://www.siemens.com/industrialsecurity>)
  - Eine Auswahl an Dokumenten zum Thema Netzwerksicherheit finden Sie hier:  
Link: (<https://support.industry.siemens.com/cs/ww/de/view/92651441>)
- Halten Sie die Firmware aktuell. Informieren Sie sich regelmäßig über Sicherheits-Updates der Firmware und wenden Sie diese an.

Hinweise auf Produktneuigkeiten und neue Firmware-Versionen finden Sie unter folgenden Adressen:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22144/dl>)

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/dl>)

### Physikalischer Zugang

Beschränken Sie den physikalischen Zugang zu dem Gerät auf qualifiziertes Personal.

### Netzanschluss

Schließen Sie den CP nicht direkt an das Internet an. Wenn ein Anschluss des CP an das Internet gewünscht ist, schalten Sie entsprechende Schutzvorrichtungen vor den CP, bspw. ein SCALANCE S mit Firewall, oder nutzen Sie den CP 1543SP-1.

## Security-Funktionen des Produkts

Nutzen Sie die Möglichkeiten der Security-Einstellungen in der Projektierung des Produkts. Hierzu zählen unter anderem:

- Schutzstufen  
Projektieren Sie eine Schutzstufe der CPU.  
Hinweise hierzu finden Sie im Informationssystem von STEP 7.
- Deaktivierung von BusAdapter-Ports  
Deaktivieren Sie in der Projektierung einen nicht benötigten Port des verwendeten BusAdapters.
- Security-Funktion der Kommunikation
  - Aktivieren Sie die Security-Funktionen des CP und richten Sie die Firewall ein.  
Beim Anschluss an öffentliche Netze sollten Sie die Firewall einsetzen. Bedenken Sie, mit welchen Diensten Sie über öffentliche Netze einen Zugriff auf die Station ermöglichen wollen. Indem Sie die "Übertragungsgeschwindigkeit" über die IP-Paketfilter-Regeln in der Firewall begrenzen, nutzen Sie die Möglichkeit, Flooding- und DoS-Angriffe einzuschränken.
  - Verwenden Sie die sicheren Protokollvarianten NTP (secure) und SNMPv3.
  - Nutzen Sie die Security-Funktionen der Telecontrol-Protokolle, bspw. die DNP3-Security-Optionen.
  - Verwenden Sie die gesicherte Open User Communication (Secure OUC) über die entsprechenden Programmbausteine.
  - Lassen Sie den Zugriff auf den Webserver der CPU deaktiviert.
- Schutz der Passwörter für den Zugriff auf Programmbausteine  
Schützen Sie Passwörter, die für Programmbausteine in Datenbausteinen abgelegt werden, vor Einsicht. Hinweise zur Vorgehensweise finden Sie im STEP 7-Informationssystem unter dem Stichwort "Know-how-Schutz".
- Logging-Funktion  
Aktivieren Sie die Funktion über die Security-Projektierung und prüfen Sie die protokollierten Ereignisse regelmäßig auf unautorisierte Zugriffe.

## Passwörter

- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Aktualisieren Sie regelmäßig die Passwörter, um die Sicherheit zu erhöhen.
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter wie z. B. "passwort1", "123456789" oder dergleichen.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.  
Siehe hierzu auch den vorstehenden Abschnitt.
- Verwenden Sie ein Passwort nicht für verschiedene Benutzer und Systeme.

## Protokolle

### Sichere und unsichere Protokolle

- Aktivieren Sie nur Protokolle, die Sie für den Einsatz des Systems benötigen.
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physikalische Schutzvorkehrungen gesichert ist.

Das Protokoll NTP bietet mit NTP (secure) eine sichere Alternative.

### Tabelle: Bedeutung der Spaltentitel und Einträge

Die folgende Tabelle gibt Ihnen einen Überblick über die offenen Ports in diesem Gerät.

- **Protokoll / Funktion**

Protokolle, die das Gerät unterstützt.

- **Portnummer (Protokoll)**

Portnummer, die dem Protokoll zugeordnet ist.

- **Voreinstellung des Ports**

- Offen

Der Port ist zu Beginn der Projektierung offen.

- Geschlossen

Der Port ist zu Beginn der Projektierung geschlossen.

- **Portzustand**

- Offen

Der Port ist immer offen und kann nicht geschlossen werden.

- Offen nach Konfiguration

Der Port ist offen, wenn er konfiguriert wurde.

- Offen (Anmeldung, wenn konfiguriert)

Der Port ist standardmäßig offen. Nach der Konfiguration des Ports ist eine Anmeldung des Kommunikationspartners erforderlich.

- Geschlossen nach Konfiguration

Der Port ist geschlossen, da der CP immer Client für diesen Dienst ist.

- **Authentifizierung**

Gibt an, ob das Protokoll den Kommunikationspartner während des Zugriffs authentifiziert.

Tabelle 4- 1 Server-Ports (alle drei CP-Typen)

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
DHCP	68 (UDP)	Geschlossen	Offen nach Konfiguration (während der CP eine neue Adresse bezieht)	Nein
S7- und Online-Verbindungen	102 (TCP)	Geschlossen	Offen nach Konfiguration *	Nein
HTTP	80 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
HTTPS	443 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
SNMP	161 (UDP)	Offen	Offen nach Konfiguration	Ja (unter SNMPv3)

\* Manche Dienstbetreiber beanstanden das Öffnen von Port 102 als Sicherheitslücke. Zur Vermeidung des Öffnens des Ports bei der Online-Diagnose siehe Kapitel Online-Security-Diagnose über Port 8448 (CP 1542SP-1 IRC, CP 1543SP-1) (Seite 88).

Tabelle 4- 2 Server-Ports - nur CP 1542SP-1 IRC und CP 1543SP-1

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
Online-Diagnose	102 (TCP)	Geschlossen	Offen nach Konfiguration	Nein
Kommunikation über SINEMA RC	443 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
Syslog	514 (UDP)	Geschlossen	Offen nach Konfiguration	Nein

Tabelle 4- 3 Server-Ports - nur CP 1542SP-1 IRC

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
DNP3	20000 (TCP/UDP) einstellbar	Geschlossen	Offen nach Konfiguration	Ja, wenn Secure Authentication aktiviert ist.
IEC 60870-5-104	2404 (TCP) einstellbar	Geschlossen	Offen nach Konfiguration	Nein

### Ports von Kommunikationspartnern und Routern

Achten Sie darauf, in den Kommunikationspartnern des CP und in zwischengeschalteten Routern die benötigten Client-Ports in der entsprechenden Firewall freizuschalten.

Dies können sein:

- TeleControl Basic / 55097 (TCP) - einstellbar
- ST7 mit MSC-Protokoll / 26382 (TCP) - einstellbar
- DHCP / 67, 68 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- NTP / 123 (UDP)

- DNS / 53 (UDP)
- SINEMA RC Autokonfiguration / 443 (TCP) - einstellbar
- SINEMA RC und OpenVPN / 1194 (UDP) - einstellbar in SINEMA RC
- IPSec / 500 (TCP)
- Syslog / 514 (UDP)

## 4.2 Projektierung in STEP 7

### Projektierung in STEP 7

Die Projektierung der Baugruppen und Netze führen Sie in SIMATIC STEP 7 durch. Die erforderliche Version finden Sie im Kapitel Software-Voraussetzungen (Seite 27).

---

#### Hinweis

##### Projektierung des CP 1542SP-1 IRC

Die Beschreibung der Basis-Projektierung des CP 1542SP-1 IRC finden Sie in den nachfolgenden Kapiteln.

Die Beschreibung der Projektierung der Telecontrol-Kommunikation des CP 1542SP-1 IRC finden Sie im jeweiligen Projektierungshandbuch, siehe /10/ (Seite 113).

---

### Übersicht der Projektierung des CP

Gehen Sie bei der Projektierung folgendermaßen vor:

1. Legen Sie ein STEP 7-Projekt an.
2. Fügen Sie die erforderlichen SIMATIC-Stationen aus folgendem Katalog-Verzeichnis ein:

Controller > SIMATIC ET200 CPU > ET 200SP CPU

3. Fügen Sie die CPs und Eingangs- und Ausgangsbaugruppen aus folgendem Katalog-Verzeichnis in die Stationen ein:

Dezentrale Peripherie > ET 200SP

Sie können für eine ET 200SP maximal zwei CP 154xSP-1 projektieren.

4. Legen Sie ein Ethernet-Netz an.
5. Verbinden Sie die Stationen mit dem Ethernet-Subnetz.
6. Projektieren Sie die eingefügten CPs.

Die BusAdapter finden Sie bei geöffneter Gerätesicht des CP in einem eigenen Katalog-Verzeichnis.

Details zu den Security-Funktionen finden Sie im Kapitel Security (CP 1543SP-1) (Seite 61).

7. Optional: Legen Sie Programmbausteine für die Open User Communication an.
8. Speichern und übersetzen Sie das Projekt.

In den nachfolgenden Kapiteln finden Sie Informationen zu einzelnen Parametergruppen. Informationen zu Parametern, die nicht in diesem Handbuch beschrieben sind, finden Sie im Informationssystem von STEP 7.

### Laden der Projektierungsdaten

Beim Laden der Station werden die Projektdaten der Station inklusive der Projektierungsdaten des CP auf der CPU gespeichert.

Informationen zum Laden der Station finden Sie im STEP 7-Informationssystem.

## 4.3 Kommunikationsarten (CP 1543SP-1)

Gültigkeit: CP 1543SP-1

Die Beschreibung für den CP 1542SP-1 IRC finden Sie im jeweiligen Projektierungshandbuch.

### Parametergruppe "Kommunikationsarten"

Um das Risiko unerlaubter Zugriffe über Ethernet auf die Station zu minimieren, müssen Sie die nachfolgenden Kommunikationsdienste für den CP aktivieren.

- **Online-Funktionen aktivieren**

Gibt im CP den Zugang zur CPU für die Online-Funktionen frei (Diagnose, Projektdaten laden etc.). Bei aktivierter Funktion kann von der Engineering-Station über den CP auf die CPU zugegriffen werden.

Wenn die Option deaktiviert ist, dann haben Sie mit den Online-Funktionen über den CP keinen Zugriff auf die CPU. Die Online-Diagnose der CPU mit direktem Anschluss an die Schnittstelle der CPU ist jedoch weiterhin möglich.

- **S7-Kommunikation aktivieren**

Gibt im CP die Funktionen der S7-Kommunikation mit einer SIMATIC S7 frei.

Wenn Sie S7-Verbindungen mit der betreffenden Station projektieren, die über den CP laufen, dann müssen Sie diese Option aktivieren.

Die Open User Communication muss nicht freigegeben werden, da Sie hierzu aktiv die entsprechenden Programmbausteine anlegen müssen. Ein unbeabsichtigter Zugriff auf den CP ist somit nicht möglich.

## 4.4 Ethernet-Schnittstelle

Projektieren Sie die allgemein verfügbaren Parameter wie für jede andere Ethernet-Schnittstelle auch:

- Allgemeine Daten (Name etc.)
- Adressen und ggf. Router
- Port-Einstellungen
- Zugriff auf den Webserver

### 4.4.1 IPv6

#### Manuelle Konfiguration von IPv6-Adressen

Wenn Sie zusätzliche IPv6-Adressen projektieren (Option "Manuelle Konfiguration"), dann stellen Sie sicher, dass die beiden IPv6-Adressen unterschiedlichen Subnetzen zugehören.

Informationen zur Projektierung finden Sie im Informationssystem von STEP 7.

#### Kommunikationspartner und IPv6

---

##### Hinweis

##### Internet-Kommunikation über IPv6

Wenn Sie IPv6-Adressen verwenden möchten und den CP an das Internet anschließen, dann stellen Sie sicher, dass der am Internet angeschlossene Router und die Betreiber der genutzten Internet-Dienste (bspw. E-Mail) ebenfalls IPv6-Adressen unterstützen.

##### OUC-Kommunikation über IPv6

Wenn Sie Bausteine der Open User Communication verwenden und IPv6 aktivieren, dann stellen Sie sicher, dass auch die Kommunikationspartner IPv6 unterstützen. Bei Anfragen an DNS-Server werden von zurückgelieferten Adressen die IPv6-Adressen vorrangig vor IPv4-Adressen verwendet.

---

### 4.4.2 Erweiterte Optionen

#### Telecontrol-spezifische Übertragungseinstellungen des CP 1542SP-1 IRC

Die Beschreibung der Telecontrol-spezifischen Übertragungseinstellungen des CP 1542SP-1 IRC finden Sie im jeweiligen Projektierungshandbuch, siehe Literaturverzeichnis (Seite 111).

## BA ... (BusAdapter)

Für den Anschluss an das Ethernet-Netz benötigt der CP einen BusAdapter. Ein BusAdapter ist nicht Teil des Lieferumfangs des CP.

Die unterstützten BusAdapter finden Sie im Anhang BusAdapter (Seite 107).

### Einfügen eines BusAdapters

In der Voreinstellung verwendet der CP einen BusAdapter "BA 2xRJ45".

Wenn Sie einen anderen BusAdapter verwenden, dann gehen Sie zunächst in die Gerätesicht des CP.

Öffnen Sie rechts im Katalog das Verzeichnis "BusAdapter" und ziehen den zu verwendenden BusAdapter auf die Schnittstelle des CP. Über den Dialog "Gerät tauschen" fügen Sie den neuen BusAdapter ein.

### Projektieren des BusAdapters

In der Parametergruppe "Ethernet-Schnittstelle > Erweiterte Optionen > BA ..." des CP projektieren Sie die Einstellungen des Netzanschlusses über den BusAdapter.

Wenn Sie nicht beide Ports des BusAdapters verwenden, können Sie einen der beiden Ports in der Parametergruppe "Aktivieren" deaktivieren.

## 4.4.3 Zugriff auf den Webserver

### Zugang zum Webserver der CPU

Der Webserver befindet sich in der CPU. Über den CP haben Sie Zugang zum Webserver der CPU.

Von einem PC aus können Sie auf den Webserver der Station zugreifen, wenn der PC über LAN am Anlagennetz angeschlossen ist.

Informationen zum Webserver der ET 200SP finden Sie im Handbuch /2/ (Seite 112).

## 4.5 Uhrzeitsynchronisation

---

### Hinweis

#### Empfehlung für die Zeitvorgabe

Die Synchronisation mit einer externen Uhr wird bei Ethernet-Verbindungen im zeitlichen Abstand von ca. 10 Sekunden empfohlen. Sie erreichen damit eine möglichst geringe Abweichung der internen Uhrzeit von der UTC-Uhrzeit.

---



**Hinweis****Konsistente Uhrzeitsynchronisation über NTP / NTP (secure)**

Bis Firmware-Version V2.0 des CP können CPU und CP beide die Uhrzeit über NTP synchronisieren lassen. Lassen Sie in diesem Fall die Uhrzeit der Station von einer externen Uhrzeitquelle nur durch ein einziges Modul der Station synchronisieren, um innerhalb der Station eine konsistente Uhrzeit vorzuhalten. Wenn Sie dennoch die Uhrzeitsynchronisation bei beiden Modulen aktivieren, dann verwenden Sie möglichst dieselben NTP-Server, um innerhalb der Station eine konsistente Uhrzeit vorzuhalten.

Ab Firmware-Version V2.1 des CP kann nur noch 1 Modul in der Station Uhrzeit-Client sein. Dieses Modul verteilt die Uhrzeit innerhalb der Station.

---

**Uhrzeitsynchronisation der CPs**

Die CPs unterstützen folgende Verfahren der Uhrzeitsynchronisation:

- CP 1542SP-1
  - NTP
  - Von lokaler StationProjektierbar an der Ethernet-Schnittstelle
- CP 1543SP-1
  - NTP
  - NTP (secure)
  - Von lokaler StationBei aktivierten Security-Funktionen projektierbar unter "Security"
- CP 1542SP-1 IRC
  - NTP
  - Von lokaler StationSowie - abhängig vom Telecontrol-Protokoll:
  - Uhrzeit von Partner / Von WANZu Details siehe Projektierungshandbücher Literaturverzeichnis (Seite 111).

**Uhrzeitweiterleitung an die CPU**

Die CPs bieten der CPU die Möglichkeit, ihre Uhrzeit über eine PLC-Variable vom CP zu übernehmen. Siehe hierzu Kapitel Kommunikation mit der CPU (Seite 58).

Wenn die CPU die Uhrzeit vom CP über eine PLC-Variable übernimmt, dann deaktivieren Sie die eigene Uhrzeitsynchronisation der CPU.

## Verfahren der Uhrzeitsynchronisation

Nachfolgend sind die Uhrzeitsynchronisationsverfahren des jeweiligen CP-Typs beschrieben.

- **NTP**

Sie projektieren die Adressen des oder der NTP-Server, das Synchronisierungsintervall und die Option "Uhrzeit von nicht synchronisierten NTP-Servern annehmen".

- **NTP (secure)**

Das gesicherte Verfahren NTP (secure) nutzt Authentifizierung über symmetrische Schlüssel. Für die Integritätsprüfung stehen verschiedene projektierbare Hash-Algorithmen zur Verfügung.

Unter den globalen Security-Einstellungen können Sie NTP-Server vom Typ NTP (secure) anlegen und verwalten.

---

### Hinweis

#### Gültige Uhrzeit sicherstellen

Wenn Sie Security-Funktionen nutzen, dann ist eine gültige Uhrzeit erforderlich. Es wird empfohlen, auf das Verfahren NTP (secure) zurückzugreifen.

---

### Hinweis

#### Manuelles Stellen der Uhrzeit bei der Inbetriebnahme

Wenn Sie Security-Funktionen oder SINEMA RC nutzen, dann stellen Sie die Uhrzeit bei der Inbetriebnahme manuell, siehe Kapitel CP in Betrieb nehmen (Seite 47).

---

## 4.6 DNS-Konfiguration

### DNS-Server

Ein DNS-Server kann erforderlich sein, wenn das Modul selbst, ein Kommunikationspartner oder bspw. ein NTP- oder E-Mail-Server über den Host-Namen (FQDN) erreichbar sein soll.

Bei Adressierung eines Kommunikationspartners als FQDN müssen Sie einen DNS-Server projektieren. Die IP-Adresse (IPv4/IPv6) des Kommunikationspartners wird dann über den projektierten DNS-Server ermittelt.

Achten Sie bei Verwendung von IPv6-Adressen auf die entsprechende Projektierung der DNS-Server.

## 4.7 Kommunikation mit der CPU

Gültigkeit: CP 1542SP-1 / CP 1543SP-1

Die Beschreibung für den CP 1542SP-1 IRC finden Sie im jeweiligen Projektierungshandbuch.

## Watchdog-Bit

- **CP-Überwachung**

Über das Watchdog-Bit prüft der CP die Verbindung mit der CPU.

Der CP überträgt das Bit alle 5 Sekunden an die CPU und setzt es im darauffolgenden CPU-Abtastzyklus wieder zurück. Bei Verbindungsstörungen wird das Bit nicht übertragen. Damit wird der CPU die Verbindungsstörung signalisiert.

Die PLC-Variable des Watchdog-Bits muss vom Anwenderprogramm ausgewertet werden.

## CP-Uhrzeit

- **CP-Uhrzeit an CPU**

Die Funktion ermöglicht der CPU, die Uhrzeit des CP zu lesen. Über diesen Weg kann der CP die CPU-Uhrzeit synchronisieren.

Ablauf:

- Die CPU setzt den Eingang "Uhrzeit-Trigger-Variable" (BOOL) über das Anwenderprogramm auf 1.
- Der CP schreibt daraufhin seine Uhrzeit in die "CP-Uhrzeitvariable" (DTL) und setzt den Wert von "Uhrzeit-Trigger-Variable" zurück auf 0.
- Das Anwenderprogramm liest die "CP-Uhrzeitvariable" zum Stellen der CPU-Uhrzeit aus.

Empfehlung:

Setzen Sie die "Uhrzeit-Trigger-Variable" nicht öfter als einmal pro Sekunde, um den Rückwandbus nicht unnötig mit Kommunikation zu belasten.

---

### Hinweis

Beachten Sie die Hinweise im Kapitel Uhrzeitsynchronisation (Seite 56).

---

## CP-Diagnose

Über die Parametergruppe haben Sie die Möglichkeit, erweiterte Diagnosedaten aus dem CP auszulesen.

- **Erweiterte CP-Diagnose aktivieren**

Aktivieren Sie die Option, um die erweiterte CP-Diagnose zu nutzen.

Bei aktivierter Option muss zumindest die "Diagnose-Trigger-Variable" projiziert werden.

Die nachfolgenden PLC-Variablen für die einzelnen Diagnosedaten können selektiv aktiviert werden.

- **Diagnose-Trigger-Variable**

Wenn die PLC-Variable (BOOL) aus dem Anwenderprogramm der CPU auf 1 gesetzt wird, dann aktualisiert der CP die Werte der folgenden PLC-Variablen für die erweiterte Diagnose.

Nach dem Schreiben der aktuellen Werte in die folgenden PLC-Variablen setzt der CP die "Diagnose-Trigger-Variable" auf 0 und signalisiert damit der CPU, dass die aktualisierten Werte aus den PLC-Variablen gelesen werden können.

---

**Hinweis**

**Schnelles Setzen der Diagnose-Trigger-Variable**

Trigger sollten nicht öfter als einmal pro Sekunde gesetzt werden.

---

**Variable für CP 1542SP-1 und CP 1543SP-1:**

- **Aktuelle IP-Adresse**

PLC-Variable (Datentyp String) für die aktuelle IP-Adresse der Schnittstelle des CP

**Variablen nur für CP 1543SP-1:**

- **VPN-IPsec-Status**

Die PLC-Variable (BOOL) gibt an, ob ein VPN-IPsec-Tunnel aufgebaut ist:

- 0 = Kein Tunnel aufgebaut
- 1 = Tunnel aufgebaut

- **Verbindung mit SINEMA Remote Connect**

Die PLC-Variable (BOOL) gibt an, ob ein OpenVPN-Tunnel zu SINEMA RC aufgebaut ist:

- 0 = Kein Tunnel aufgebaut
- 1 = Tunnel aufgebaut

## 4.8 SNMP

### Parametergruppe "SNMP"

- **SNMP aktivieren**

Gibt im CP die Funktion des SNMP-Agenten frei.

## Leistungsumfang der CPs

Die CPs unterstützen folgende SNMP-Versionen:

- **CP 1542SP-1**
  - SNMPv1
- **CP 1543SP-1, CP 1542SP-1 IRC**
  - SNMPv1
  - SNMPv3 (bei aktivierten Security-Funktionen)

Wenn die Security-Funktionen aktiviert sind, finden Sie die Parametergruppe "SNMP" unter "Security".

Traps werden vom CP nicht unterstützt.

Details zu den unterstützten Funktionen finden Sie im Kapitel Diagnose über SNMP (Seite 88).

## 4.9 Security (CP 1543SP-1)

### Security-Funktionen des CP 1542SP-1 IRC

Die Beschreibung der Security-Funktionen des CP 1542SP-1 IRC finden Sie im Projektierungshandbuch des jeweiligen Telecontrol-Protokolls, siehe Literaturverzeichnis (Seite 111).

### Security-Funktionen des CP 1543SP-1

Die nachfolgende Beschreibung der Security-Funktionen gilt nur für den CP 1543SP-1.

Zu den Funktionen in der Übersicht siehe Kapitel Anwendung und Funktionen (Seite 13).

Um die Security-Funktionen projektieren zu können, müssen Sie einen Security-Benutzer anlegen, siehe Kapitel Security-Benutzer (Seite 61).

### 4.9.1 Security-Benutzer

#### Security-Benutzer anlegen

Um Security-Funktionen projektieren zu können, benötigen Sie entsprechende Projektierungsrechte. Hierzu müssen Sie mindestens einen Security-Benutzer mit den entsprechenden Rechten anlegen.

Navigieren Sie zu den globalen Security-Einstellungen > "Benutzer und Rollen" > Register "Benutzer".

1. Legen Sie einen Benutzer an und projektieren Sie die Parameter.
2. Weisen Sie diesem Benutzer in dem darunterliegenden Bereich "Zugewiesene Rollen" die Rolle "NET Standard" oder "NET Administrator" zu.

Dieser Benutzer kann nach dem Anmelden am STEP 7-Projekt die erforderlichen Einstellungen vornehmen.

Melden Sie sich auch künftig bei Arbeiten an Security-Parametern als dieser Benutzer an.

## 4.9.2 Firewall

### 4.9.2.1 Vorgezogene Prüfung von Telegrammen durch die MAC-Firewall

Jedes eingehende oder ausgehende Telegramm durchläuft zunächst die MAC-Firewall (Layer 2). Wenn das Telegramm bereits auf dieser Ebene verworfen wird, dann wird es nicht zusätzlich durch die IP-Firewall (Layer 3) geprüft. Somit kann durch entsprechende MAC-Firewall-Regeln die IP-Kommunikation eingeschränkt oder geblockt werden.

### 4.9.2.2 Einstellungen für Online-Security-Diagnose und Laden in Station bei aktivierter Firewall

#### Firewall für Online-Funktionen einstellen

Gehen Sie bei aktivierten Security-Funktionen wie folgt vor.

##### **Globale Security-Funktionen:**

1. Wählen Sie den Eintrag "Firewall > Dienste > Dienste für IP-Regeln definieren".
2. Wählen Sie das Register "ICMP".
3. Fügen Sie jeweils einen neuen Eintrag vom Typ "Echo Reply" und "Echo Request" ein.

##### **Lokale Security-Funktionen des CP:**

Wählen Sie nun den CP in der S7-Station aus.

1. Aktivieren Sie den erweiterten Firewall-Modus in den lokalen Security-Einstellungen des CP in der Parametergruppe "Security > Firewall".
2. Öffnen Sie die Parametergruppe "IP-Regeln".

3. Fügen Sie in der Tabelle jeweils eine neue IP-Regel für die zuvor global angelegten Dienste wie folgt ein:
  - Aktion: Accept; Von: Extern; Nach: Station; Dienst > ICMPv4/6-Dienst > Echo Request (der zuvor global angelegte Dienst)
  - Aktion: Accept; Von: Station; Nach: Extern; Dienst > ICMPv4/6-Dienst > Echo Reply (der zuvor global angelegte Dienst)
4. Tragen Sie für die IP-Regel zum Dienst "Echo Request" unter "Quell-IP-Adresse" die IP-Adresse der Engineering-Station ein.

Mit diesen Regeln kann der CP von der Engineering-Station aus nur mit ICMP-Paketen (Ping) über die Firewall erreicht werden.

---

**Hinweis****Weitere Dienste für Online-Security-Diagnose und Laden**

Wenn Sie die Funktionen "Online-Security-Diagnose" oder "Laden in Gerät" nutzen möchten, müssen Sie zusätzliche Regeln erstellen oder die Dienste "Echo Request" / "Echo Reply" deaktivieren.

---

#### 4.9.2.3 Schreibweise der Quell-IP-Adresse (erweiterter Firewall-Modus)

Wenn Sie in den erweiterten Firewall-Einstellungen des CP bei der Quell-IP-Adresse einen Adressbereich angeben, achten Sie auf die richtige Schreibweise:

- Trennen Sie die beiden IP-Adressen nur durch einen Bindestrich.  
Richtig: 192.168.10.0-192.168.10.255
- Geben Sie keine weiteren Zeichen zwischen die beiden IP-Adressen ein.  
Falsch: 192.168.10.0 - 192.168.10.255

Wenn Sie den Bereich falsch eingeben, wird die Firewall-Regel nicht angewendet.

#### 4.9.2.4 Firewall-Einstellungen für S7-Verbindungen über VPN-Tunnel

##### IP-Regeln im erweiterten Firewall-Modus

Wenn Sie projektierte Verbindungen (S7, OUC) mit VPN-Tunnel zwischen dem CP und einem Kommunikationspartner einrichten, dann müssen Sie die lokalen Firewall-Einstellungen des CP anpassen:

Wählen Sie für die Verbindungen im erweiterten Firewall-Modus ("Security > Firewall > IP-Regeln") für beide Kommunikationsrichtungen des VPN-Tunnels die Aktion "Allow\*" aus.

### 4.9.3 Log-Einstellungen - Filtern der System-Ereignisse

#### Kommunikationsprobleme bei zu hoch eingestelltem Wert für System-Ereignisse

Bei zu hoch eingestelltem Wert für die Filterung der System-Ereignisse können Sie eventuell nicht den maximale Leistungsumfang der Kommunikation nutzen. Die hohe Anzahl an ausgegebenen Fehlermeldungen kann die Bearbeitung der Kommunikationsverbindungen verzögern oder verhindern.

Stellen Sie unter "Security > Log-Einstellungen > System-Ereignisse konfigurieren" den Parameter "Ebene:" auf den Wert "3 (Error)" ein, um den sicheren Aufbau der Kommunikationsverbindungen zu gewährleisten.

### 4.9.4 E-Mail-Projektierung

#### Voraussetzungen und benötigte Informationen

Beachten Sie folgende Voraussetzungen in der CP-Projektierung für die Übertragung von E-Mails:

- Die Security-Funktionen sind aktiviert.
- Die Uhrzeit des CP ist synchronisiert.

Für die Projektierung benötigen Sie die Daten des SMTP-Servers und des Benutzerkontos:

- Server-Adresse, Port-Nummer, Benutzername, Passwort, E-Mail-Adresse des Absenders (CP)
- Bei verschlüsselter Übertragung: Server-Zertifikat

#### E-Mail-Projektierung

- **Keine Konfiguration**

In der Voreinstellung ist das Versenden von E-Mails deaktiviert.

- **SMTP aktivieren**

Aktivieren Sie diese Option, wenn Sie das Versenden unverschlüsselter E-Mails über den SMTP-Port 25 nutzen möchten.

- **SSL/TLS aktivieren**

Wenn Ihr E-Mail-Dienst-Betreiber nur verschlüsselte Übertragung unterstützt, dann aktivieren Sie diese Option. Über die Port-Nummer wählen Sie das Protokoll:

- Port-Nr. 587

Unter Verwendung von STARTTLS sendet der CP verschlüsselte E-Mails.

- Port-Nr. 465

Unter Verwendung von SSL/TLS (SMTPS) sendet der CP verschlüsselte E-Mails.

Erkundigen Sie sich bei Ihrem E-Mail-Dienst-Betreiber, welche Option unterstützt wird.

Wenn Sie einen Internetanschluss mit IPv6-Infrastruktur nutzen wollen, dann beachten Sie den Hinweis im Kapitel IPv6 (Seite 55).



## 4.9.5 VPN

### 4.9.5.1 VPN (Virtual Private Network)

#### VPN - IPsec

Virtual Private Network (VPN) ist eine Technologie für den sicheren Transport von vertraulichen Daten über öffentliche IP-Netzwerke, z. B. das Internet. Mit VPN wird eine sichere Verbindung (IPsec-Tunnel) zwischen zwei sicheren IT-Systemen oder Netzen über ein unsicheres Netz hinweg eingerichtet und betrieben.

Der IPsec-Tunnel leitet sämtliche Daten weiter, auch von Protokollen höherer Schichten (HTTP, FTP etc.).

Der Datenverkehr zweier Netzkomponenten wird uneingeschränkt durch ein anderes Netz transportiert. Damit können komplette Netzwerke über ein benachbartes oder zwischengeschaltetes Netz hinweg miteinander verbunden werden.

#### Eigenschaften

- VPN bildet ein logisches Teilnetz, das sich in ein benachbartes (zugeordnetes) Netz einbettet. VPN nutzt die üblichen Adressierungsmechanismen des zugeordneten Netzes, transportiert datentechnisch aber eigene Telegramme und arbeitet so vom Rest dieses Netzes losgelöst.
- VPN ermöglicht die Kommunikation der darin befindlichen VPN-Partner mit dem zugeordneten Netz.
- VPN basiert auf einer Tunneltechnik und ist individuell konfigurierbar.
- Die abhör- und manipulationssichere Kommunikation zwischen den VPN-Partnern wird durch die Verwendung von Passwörtern, öffentlichen Schlüsseln oder durch ein digitales Zertifikat (Authentifizierung) gewährleistet.

#### Anwendungsgebiete/Einsatzgebiete

- Lokale Netze können über das Internet auf sichere Art miteinander verbunden werden (Site-to-Site-Verbindung).
- Gesicherter Zugriff auf ein Firmennetz (End-to-Site-Verbindung)
- Gesicherter Zugriff auf einen Server (End-to-End-Verbindung)
- Kommunikation zwischen zwei Servern, ohne dass die Kommunikation durch Dritte eingesehen werden kann (Ende-zu-Ende- oder Host-to-Host-Verbindung).
- Gewährleistung von Informationssicherheit in vernetzten Anlagen der Automatisierungstechnik
- Absicherung von Rechnersystemen einschließlich der dazugehörigen Datenkommunikation innerhalb eines Automatisierungsnetzes oder den sicheren Fernzugriff über das Internet
- Gesicherte Fernzugriffe vom PC/Programmiergerät auf Automatisierungsgeräte oder Netzwerke, die durch Security-Module geschützt sind, über öffentliche Netze hinweg.

## Zellenschutzkonzept

Mit Industrial Ethernet Security können einzelne Geräte oder Netzsegmente eines Ethernet-Netzwerks abgesichert werden:

- Der Zugriff auf einzelne Geräte und Netzsegmente, die durch Security-Module geschützt sind, wird erlaubt.
- Gesicherte Verbindungen über unsichere Netzwerkstrukturen werden ermöglicht.

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall, NAT-/NAPT-Router und VPN über IPsec-Tunnel schützen Security-Module vor:

- Datenspionage
- Datenmanipulation
- Unerwünschte Zugriffe

### 4.9.5.2 SINEMA Remote Connect

#### Fernwartung mit SINEMA Remote Connect (SINEMA RC)

Die Applikation "SINEMA Remote Connect" (SINEMA RC) steht für Fernwartungszwecke zur Verfügung.

SINEMA RC verwendet OpenVPN zur Verschlüsselung der Daten. Zentrum der Kommunikation ist der SINEMA RC-Server, über den die Kommunikation zwischen den Teilnehmern läuft und der die Konfiguration des Kommunikationssystems verwaltet.

#### Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie die Projektierung der SINEMA RC-Anbindung des Moduls in STEP 7 beginnen. Sie sind Voraussetzung für ein konsistentes STEP 7-Projekt.

- Projektierung von SINEMA Remote Connect Server

Nehmen Sie die erforderliche Projektierung von SINEMA RC Server vor (nicht in STEP 7). Das Kommunikationsmodul und dessen Kommunikationspartner müssen im SINEMA RC-Server projiziert werden.

- Exportieren des CA-Zertifikats (optional)

Wenn Sie als Authentifizierungsmethode des Kommunikationsmoduls beim Verbindungsaufbau das Zertifikat des Servers nutzen möchten, dann exportieren Sie das CA-Zertifikat von SINEMA RC Server.

Importieren Sie anschließend das CA-Zertifikat von SINEMA RC Server in die Engineering-Station.

Alternativ können Sie als Authentifizierungsmethode des Kommunikationsmoduls den Fingerabdruck des Server-Zertifikats verwenden. Die Gültigkeitsdauer des Fingerabdrucks kann kürzer sein als die des Zertifikats.

Beachten Sie, dass Sie den Import des Zertifikats im Fall eines Baugruppentauschs wiederholen müssen.

## Projektierung von SINEMA Remote Connect

### Importieren des eigenen Zertifikats

1. Navigieren Sie beim CP zur Parametergruppe "Security > Zertifikatsmanager > Zertifikate der Partnergeräte".
2. Öffnen Sie den Dialog zur Auswahl des Zertifikats durch Doppelklick auf die erste freie Tabellenzeile.
3. Wählen Sie das CA-Zertifikat von SINEMA RC Server aus.

Navigieren Sie anschließend zur Parametergruppe "Security > VPN".

### VPN > Allgemein

1. Aktivieren Sie VPN
2. Wählen Sie als VPN-Verbindungstyp die Option "Automatische OpenVPN-Konfiguration über SINEMA Remote Connect Server" aus, wenn Sie Kommunikation über SINEMA Remote Connect nutzen möchten.

Bei Auswahl von "Internet Key Exchange (IKE) ..." können Sie Kommunikation über IPsec-Tunnel nutzen.

### SINEMA Remote Connect Server

Tragen Sie die Adresse und Portnummer des Servers ein.

### Serverüberprüfung

Hier wählen Sie die Authentifizierungsmethode des Kommunikationsmoduls beim Verbindungsaufbau aus.

- CA-Zertifikat

Wählen Sie unter "CA-Zertifikat" das zuvor importierte und im lokalen Zertifikatsmanager zugewiesene CA-Zertifikat von SINEMA RC Server aus.

Das Modul prüft grundsätzlich das CA-Zertifikat des Servers und dessen Gültigkeitsdauer. Die beiden Optionen können nicht geändert werden.

- Fingerabdruck

Wenn Sie diese Authentifizierungsmethode wählen, dann geben Sie den Fingerabdruck des Server-Zertifikats von SINEMA RC Server ein.

### Authentifizierung

- Geräte-ID

Tragen Sie die in SINEMA RC erzeugte Geräte-ID für das Modul ein.

- Gerätepasswort

Tragen Sie das in SINEMA RC projektierte Gerätepasswort des Moduls ein.

Max. Anzahl an Zeichen: 127

### Optionale Einstellungen

Der Verbindungsaufbau wird in der Parametergruppe "Security > VPN > Optionale Einstellungen" über den Parameter "Verbindungsart" projektiert.

- **Aktualisierungsintervall**

Über den Parameter stellen Sie das Intervall ein, in dem der CP die Konfiguration beim SINEMA RC-Server abfragt.

Beachten Sie bei der Einstellung 0 (null), dass Änderungen der Konfiguration des SINEMA RC-Servers dazu führen können, dass vom CP keine Verbindung mehr zum SINEMA RC-Server aufgebaut werden kann.

- **"Verbindungsart"**

Die beiden Optionen des Parameters haben folgende Auswirkung auf den Verbindungsaufbau:

- Auto

Das Modul baut eine Verbindung zum SINEMA RC-Server auf. Die OpenVPN-Verbindung bleibt bis zum Ändern der Verbindungsparameter durch den SINEMA Remote Connect-Server bestehen. Bei Verbindungsabbruch baut der CP die Verbindung automatisch wieder auf.

Bei Änderung der Verbindungsparameter durch den SINEMA Remote Connect-Server fragt der CP die neuen Verbindungsdaten nach Ablauf des oben projektierten Aktualisierungsintervalls ab.

- PLC-Trigger

Die Option ist vorgesehen für sporadische Kommunikation des Moduls über den SINEMA RC-Server.

Diese Option können Sie nutzen, wenn Sie temporäre Verbindungen zwischen dem Modul und einem PC aufbauen möchten. Die temporären Verbindungen werden über eine PLC-Variable aufgebaut und können beispielsweise für Service-Fälle genutzt werden.

---

### Hinweis

#### Verbindungsabbruch

Bei einem STOP der CPU, beispielsweise durch Firmware-Update oder "Laden in Gerät", wird die OpenVPN-Verbindung abgebrochen.

Diese Funktionen können nur bei Aktivierung der Option "Auto" genutzt werden.

---

- **PLC-Variable für Verbindungsaufbau**

Das Modul baut bei ausgewählter Option "PLC-Trigger" eine Verbindung auf, wenn die PLC-Variable (Bool) den Wert 1 annimmt. Im laufenden Betrieb kann die PLC-Variable bei Bedarf gesetzt werden, beispielsweise über ein HMI-Panel.

Beim Rücksetzen der PLC-Variable auf 0 wird die Verbindung wieder abgebaut.

### 4.9.5.3 VPN-Tunnel für S7-Kommunikation zwischen Stationen anlegen

#### Voraussetzungen

Um einen VPN-Tunnel für S7-Kommunikation zwischen zwei S7-Stationen oder zwischen einer S7-Station und einer Engineering-Station mit Security-CP (bspw. CP 1628) anzulegen, müssen folgende Voraussetzungen erfüllt sein:

- Die zwei Stationen sind projektiert.
- Die CPs in beiden Stationen müssen die Security-Funktionen unterstützen.
- Die Ethernet-Schnittstellen der beiden Stationen müssen vernetzt sein.

---

#### Hinweis

##### Kommunikation auch über einen IP-Router möglich

Die Kommunikation zwischen den beiden Stationen ist auch über einen IP-Router möglich. Für diesen Kommunikationsweg müssen Sie jedoch weitere Einstellungen vornehmen.

---

#### Vorgehensweise

Um einen VPN-Tunnel anzulegen, müssen Sie die folgenden Schritte durchführen:

1. Security-Benutzer anlegen  
Wenn der Security-Benutzer schon angelegt ist: Melden Sie sich als dieser Benutzer an.
2. Option "Aktiviere Security-Funktionen" aktivieren
3. VPN-Gruppe anlegen und Security-Module zuweisen
4. Eigenschaften der VPN-Gruppe projektieren
5. Lokale VPN-Eigenschaften der beiden CPs projektieren

Die genaue Beschreibung der einzelnen Handlungsschritte finden Sie in den nachfolgenden Abschnitten dieses Kapitels.

#### Security-Funktionen aktivieren

Aktivieren Sie nach dem Anmelden bei beiden CPs unter "Security" die Option "Aktiviere Security-Funktionen".

Für beide CPs stehen Ihnen jetzt die Security-Funktionen zur Verfügung.

#### VPN-Gruppe anlegen und Security-Module zuweisen

1. Navigieren Sie in den globalen Security-Einstellungen zu "VPN-Gruppen" > "Neue VPN-Gruppe hinzufügen".
2. Doppelklicken Sie auf den Eintrag "Neue VPN-Gruppe hinzufügen", um eine VPN-Gruppe anzulegen.

Ergebnis: Eine neue VPN-Gruppe wird unterhalb des ausgewählten Eintrags angezeigt.

3. Doppelklicken Sie auf den Eintrag "VPN-Gruppen" > "Modul einer VPN-Gruppe zuweisen".
4. Ordnen Sie der VPN-Gruppe die Security-Module zu, zwischen denen VPN-Tunnel aufgebaut werden sollen.

---

**Hinweis**

**Aktuelles Datum und aktuelle Uhrzeit im CP für VPN-Verbindungen**

Zum Aufbau einer VPN-Verbindung und die damit verbundene Anerkennung der auszutauschenden Zertifikate wird das aktuelle Datum und die aktuelle Uhrzeit in beiden Stationen vorausgesetzt.

---

**Eigenschaften der VPN-Gruppe projektieren**

1. Doppelklicken Sie auf die neu angelegte VPN-Gruppe.  
Ergebnis: Die Eigenschaften der VPN-Gruppe werden unter "Authentifizierung" angezeigt.
2. Geben Sie der VPN-Gruppe einen Namen. Projektieren Sie in den Eigenschaften die Einstellungen der VPN-Gruppe.  
Diese Eigenschaften definieren die Standardeinstellungen der VPN-Gruppe, die Sie jederzeit ändern können.

---

**Hinweis**

**VPN-Eigenschaften der CPs festlegen**

Die VPN-Eigenschaften der CPs legen Sie in der Parametergruppe "Security" > "Firewall" > "VPN" der jeweiligen Baugruppe fest.

---

**Ergebnis**

Sie haben einen VPN-Tunnel angelegt. Die Firewall der CPs wird automatisch aktiviert: Die Option "Firewall aktivieren" wird beim Anlegen einer VPN-Gruppe automatisch aktiviert. Sie können die Option nicht deaktivieren.

Laden Sie die Konfiguration in alle Module, die zur VPN-Gruppe gehören.

**4.9.5.4 VPN-Kommunikation mit SOFTNET Security Client (Engineering-Station)**

**VPN-Tunnelkommunikation gelingt nur bei deaktiviertem internen Teilnehmer**

Unter bestimmten Bedingungen gelingt der Aufbau einer VPN-Tunnelkommunikation zwischen SOFTNET Security Client und dem CP nicht.

SOFTNET Security Client versucht zusätzlich, eine VPN-Tunnelkommunikation zu einem unterlagerten internen Teilnehmer aufzubauen. Dieser Kommunikationsaufbau zu einem

nicht vorhandenen Teilnehmer verhindert den gewünschten Kommunikationsaufbau zum CP.

Um eine erfolgreiche VPN-Tunnelkommunikation zum CP aufzubauen, müssen Sie den internen Teilnehmer deaktivieren.

Nur wenn das beschriebene Problem vorliegt, müssen Sie die nachfolgende Vorgehensweise der Deaktivierung des Teilnehmers anwenden.

Deaktivieren Sie den Teilnehmer in der SOFTNET Security Client - Tunnelübersicht:

1. Entfernen Sie den Haken im Kontrollkästchen "Lernen der internen Knoten der Tunnelpartner aktivieren".

Der unterlagerte Teilnehmer verschwindet vorerst aus der Tunnelliste.

2. Selektieren Sie in der Tunnelliste die gewünschte Verbindung zum CP.

3. Wählen Sie im Kontextmenü über die rechte Maustaste "Aktiviere Verbindung zu den internen Knoten" aus.

Der unterlagerte Teilnehmer erscheint vorübergehend wieder in der Tunnelliste.

4. Selektieren Sie in der Tunnelliste den unterlagerten Teilnehmer.

5. Wählen Sie im Kontextmenü über die rechte Maustaste "Lösche Eintrag" aus

Ergebnis: Der unterlagerte Teilnehmer ist endgültig deaktiviert. Der Aufbau einer VPN-Tunnelkommunikation zum CP gelingt.

#### 4.9.5.5 VPN-Tunnelkommunikation zwischen CP und SCALANCE M aufbauen

Legen Sie einen VPN-Tunnel zwischen CP und einem Router SCALANCE M entsprechend der bei den Stationen beschriebenen Vorgehensweise an.

Nur wenn Sie in den globalen Security-Einstellungen der angelegten VPN-Gruppe ("VPN-Gruppen > Authentifizierung") das Kontrollkästchen "Perfect Forward Secrecy" angewählt haben, wird eine VPN-Tunnelkommunikation aufgebaut.

Wenn das Kontrollkästchen nicht angewählt ist, lehnt der CP den Verbindungsaufbau ab.

#### 4.9.5.6 CP als passiver Teilnehmer von VPN-Verbindungen

##### Erlaubnis zum VPN-Verbindungsaufbau bei passivem Teilnehmer einstellen

Wenn der CP über ein Gateway mit einem anderen VPN-Teilnehmer verbunden ist und der CP ein passiver Teilnehmer ist, dann müssen Sie die Erlaubnis zum VPN-Verbindungsaufbau auf "Responder" einstellen.

Dies ist der Fall bei folgender typischer Konfiguration:

VPN-Teilnehmer (aktiv) ⇔ Gateway (dyn. IP-Adresse) ⇔ Internet ⇔ Gateway (feste IP-Adresse) ⇔ CP (passiv)

Projektieren Sie für den CP als passivem Teilnehmer die Erlaubnis zum VPN-Verbindungsaufbau folgendermaßen:

1. Gehen Sie in STEP 7 in die Geräte- und Netzansicht.
2. Selektieren Sie den CP.
3. Öffnen Sie unter den lokalen Security-Einstellungen die Parametergruppe "VPN".
4. Ändern Sie für jede VPN-Verbindung mit dem CP als passivem VPN-Teilnehmer die Standardeinstellung "Initiator/Responder" in die Einstellung "Responder".

## 4.9.6 SNMP

### SNMP

Den Leistungsumfang des Geräts zu SNMP finden Sie im Kapitel Diagnose über SNMP (Seite 88).

Bei aktivierten Security-Funktionen haben Sie folgende Auswahl und Einstellmöglichkeiten.

#### SNMP

- **"SNMP aktivieren"**

Bei aktivierter Option wird im Gerät die Kommunikation über SNMP freigegeben. In der Voreinstellung ist SNMPv1 aktiviert.

Bei deaktivierter Option werden Anfragen von SNMP-Clients weder über SNMPv1 noch über SNMPv3 beantwortet.

- **"SNMPv1 verwenden"**

Aktiviert die Nutzung von SNMPv1 für das Gerät. Zur Projektierung der erforderlichen Community-Strings siehe unten (SNMPv1).

- **"SNMPv3 verwenden"**

Aktiviert die Nutzung von SNMPv3 für das Gerät. Zur Projektierung der erforderlichen Algorithmen siehe unten (SNMPv3).

#### SNMPv1

Die Community-Strings müssen bei Anfragen an das Gerät über SNMPv1 mitgeschickt werden.



Beachten Sie die Schreibweise der voreingestellten Community-Strings mit Kleinbuchstaben!

- **"Community String lesend"**

Der String ist für den lesenden Zugriff erforderlich.

Belassen Sie den voreingestellten String "public" oder projektieren Sie einen String.

- **"Erlaube schreibenden Zugriff"**

Bei Aktivierung der Option wird der schreibende Zugriff auf das Gerät freigegeben und der zugehörige Community-String wird editierbar.

- **"Community String schreibend"**

Der String ist für den schreibenden Zugriff erforderlich und kann auch für den lesenden Zugriff verwendet werden.

Belassen Sie den voreingestellten String "private" oder projektieren Sie einen String.

---

### Hinweis

#### Sicherheit des Zugriffs

Ändern Sie aus Sicherheitsgründen die voreingestellten und allgemein bekannten Strings "public" und "private" ab.

---

### SNMPv3

Die Algorithmen müssen für den verschlüsselten Zugriff auf das Gerät über SNMPv3 projiziert werden.

- **"Authentifizierungsalgorithmus"**

Selektieren Sie in der Klappliste das zu verwendende Authentifizierungsverfahren.

- **"Verschlüsselungsalgorithmus"**

Selektieren Sie in der Klappliste das zu verwendende Verschlüsselungsverfahren.

### Benutzerverwaltung

In der Benutzerverwaltung, die Sie unter den Globalen Security-Einstellungen finden, weisen Sie den verschiedenen Benutzern ihre Rolle zu.

Unter den Eigenschaften der Rollen sehen Sie die Rechtestliste der jeweiligen Rolle, beispielsweise die verschiedenen Zugriffsarten über SNMP. Für neue Rollen können Sie die einzelnen Rechte frei projektieren.

Informationen zu Benutzern, Rollen und den Passwort-Richtlinien finden Sie im Informationssystem von STEP 7.

## 4.9.7 Zertifikatsmanager

Bei aktivierten Security-Funktionen werden im STEP 7-Projekt automatisch für alle betroffenen Security-Module die benötigten Zertifikate erzeugt, um beispielsweise über VPN-Verbindungen kommunizieren zu können.

Von STEP 7 erzeugte Zertifikate wie SSL-Zertifikate oder VPN-Gruppen-Zertifikate werden automatisch den zugehörigen Modulen zugeordnet und müssen diesen nicht über die lokalen Security-Einstellungen zugeordnet werden.

### Der lokale Zertifikatsmanager

Zertifikate, die über den Zertifikatsmanager in den globalen Security-Einstellungen importiert wurden, werden nicht automatisch den zugehörigen Modulen zugeordnet. Importierte Zertifikate müssen manuell über den Eintrag "Zertifikatsmanager" in den lokalen Security-Einstellungen in die Liste der vertrauenswürdigen Partnerzertifikate aufgenommen werden. Beim Zuordnen eines CA-Zertifikats werden dem Modul auch die davon abgeleiteten Zertifikate zugeordnet.

### Hinzufügen von Zertifikaten

Über den lokalen Zertifikatsmanager ordnen Sie dem CP Zertifikate der Partner für bestimmte Dienste zu, z. B. für gesichertes Versenden von E-Mails.

1. Klicken Sie hierzu in die Tabellenzelle "Neu hinzufügen".
2. Klicken Sie auf die weiß hinterlegte Schaltfläche "...".
3. Fügen Sie in der sich öffnenden Zertifikatliste entweder ein neues Zertifikat über die Schaltfläche "Hinzufügen" ein oder wählen Sie ein bestehendes Zertifikat des Projekts über das Haken-Symbol aus.

Den Typ und die Eigenschaften der angezeigten Zertifikate können Sie im globalen Zertifikatsmanager erkennen.

### Zertifikate für den CP 1543SP-1

Bevor Zertifikate in Programmbausteinen für Secure Communication referenziert werden können, müssen diese Zertifikate dem Security-Modul über den lokalen Zertifikatsmanager als Gerätezertifikate zugeordnet werden.

#### Voraussetzung in den globalen Security-Einstellungen

Um dem CP Zertifikate eines Kommunikationspartners zuordnen zu können, müssen Sie die Zertifikate des Partners zuvor im globalen Zertifikatsmanager importieren (Globale Security-Einstellungen).

Um das zugeordnete Zertifikat dem Partnermodul bekanntzumachen, muss dieses Zertifikat nach dem Import in die Liste der vertrauenswürdigen Partnerzertifikate aufgenommen werden.

#### Zertifikate in der CP-Projektierung zuweisen

Wählen Sie folgende Zertifikate in der CP-Projektierung aus:

- Tabelle "Gerätezertifikate":  
Das vom STEP 7-Projekt erzeugte Geräte-Zertifikat des CP
- Tabelle "Zertifikate der Partner-Geräte":  
Das importierte Zertifikat des Partners

## 4.10 Nachrichten: E-Mails (CP 1543SP-1)

### Gültigkeit

Gültigkeit: CP 1543SP-1

Die Beschreibung für den CP 1542SP-1 IRC finden Sie im jeweiligen Projektierungshandbuch.

---

#### Hinweis

##### **E-Mails über den Nachrichten-Editor**

Die nachfolgenden Ausführungen gelten für E-Mails, die über den Nachrichten-Editor projiziert werden.

Das Versenden von E-Mails über OUC-Programmbausteine ist unabhängig davon.

---

### Voraussetzungen

Bei wichtigen Ereignissen kann der CP E-Mails an Kommunikationspartner absetzen.

Beachten Sie folgende Voraussetzungen in der CP-Projektierung für die Übertragung von E-Mails:

- Die Security-Funktionen sind aktiviert.
- Die Uhrzeit des CP ist synchronisiert.
- Projektierung der Parametergruppe "E-Mail-Projektierung"

Für die Projektierung der Nachrichten benötigen Sie die Empfänger-Adressen.

### Öffnen des Nachrichten-Editors

Die Projektierung der einzelnen Nachrichten (E-Mails) nehmen Sie in STEP 7 im Nachrichten-Editor vor. Sie können den Editor alternativ öffnen über:

- Selektion des CP  
Kontextmenü "Datenpunkt- und Nachrichten-Editor öffnen"
- Über die Projektnavigation:  
Station > "Lokale Module" > CP > Nachrichten  
Durch Doppelklick auf den Eintrag "Nachrichten" öffnet sich der Editor.

### Anlegen von Nachrichten

Legen Sie eine neue Nachricht an, indem Sie im Nachrichten-Editor in die erste Tabellenzeile mit dem grauten Eintrag "<Hinzufügen>" doppelklicken.

Den vorgelegten Namen "Alarm" einer E-Mail können Sie anpassen, er muss aber innerhalb des Moduls eindeutig sein.

## Nachrichtenparameter

Hier projektieren Sie die Empfänger, den Betreff und den Text der Nachricht.

### Trigger: Auslösen der E-Mail-Übertragung

Im Register "Trigger" projektieren Sie, wann das Versenden der E-Mail ausgelöst wird und ob zusätzliche Informationen mitgeschickt werden.

- **E-Mail-Trigger**

Legt das Ereignis fest, bei dem das Versenden der E-Mail ausgelöst wird:

- PLC-Variable verwenden

Als Trigger-Signal für das Versenden der E-Mail wird der Flankenwechsel (0 → 1) des Trigger-Bits "PLC-Variable für Trigger" ausgewertet, das vom Anwenderprogramm gesetzt wird. Für jede E-Mail kann bei Bedarf ein separates Trigger-Bit projektiert werden. Zum Trigger-Bit siehe unten.

**Rücksetzen des Trigger-Bits:**

Wenn der Speicherbereich des Trigger-Bits im Merkerbereich oder in einem Datenbaustein liegt, dann wird das Trigger-Bit mit dem Versenden der Nachricht auf Null zurückgesetzt.

In allen anderen Fällen müssen Sie das Trigger-Bit über das Anwenderprogramm zurücksetzen.

---

**Hinweis**

**Schnelles Setzen der Diagnose-Trigger-Variable**

Trigger sollten nicht öfter als einmal pro Sekunde gesetzt werden.

---

- CPU geht in STOP
- CPU geht in RUN

Abhängig von der VPN-Projektierung sind weiterhin folgende Einträge auswählbar:

- VPN-Verbindung aufgebaut
- VPN-Verbindung abgebaut

oder

- SINEMA RC-Verbindung aufgebaut
- SINEMA RC-Verbindung abgebaut

- **PLC-Variable für Trigger**

Variable (Bool) für den E-Mail-Trigger "PLC-Variable verwenden"

- **Kennung für Bearbeitungsstatus aktivieren**

Bei Aktivierung der Option wird nach jedem Sendeversuch ein Status zurückgegeben, der Auskunft über den Bearbeitungszustand der gesendeten Nachricht gibt.

Der Status wird in die "PLC-Variable für Bearbeitungsstatus" (DWORD) geschrieben. Bei Problemen mit der Zustellung der Nachrichten können Sie den Status über den Webserver der CPU feststellen, indem Sie dort den Wert der PLC-Variable anzeigen.

Zur Bedeutung der einzelnen Status siehe Kapitel Bearbeitungsstatus von E-Mails (CP 1543SP-1) (Seite 92).

- **Wert mitschicken**

Bei Aktivierung der schickt der CP in der Nachricht für den Platzhalter \$\$ einen Wert aus dem Speicherbereich der CPU mit.

Wählen Sie eine PLC-Variable, deren Wert in die Nachricht integriert wird. \$\$ kann Platzhalter sein für eine Variable mit einfachem Datentyp bis zur Größe von 32 Bit.

Der jeweils aktuelle Wert wird im Nachrichtentext an der Stelle des Platzhalters \$\$ eingesetzt. Hierzu geben Sie im Nachrichtentext "\$\$" als Platzhalter für den mitzuschickenden Wert ein.

## Editor-Ansicht: Anordnen von Spalten und Zeilen

Wie bei vielen anderen Programmen können Sie auch im Nachrichten-Editor die Spalten anordnen und die Tabelle nach Ihren Bedürfnissen sortieren:

- **Spalten anordnen**

Wenn Sie auf einen Spaltenkopf mit gedrückter linker Maustaste klicken, können Sie die Spalte verschieben.

- **Objekte sortieren**

Wenn Sie kurz mit der linken Maustaste auf einen Spaltenkopf klicken, können Sie die Objekte der Tabelle aufsteigend bzw. absteigend nach den Einträgen dieser Spalte sortieren. Die Sortierung wird über einen Pfeil im Spaltenkopf angezeigt.

Nach absteigender Sortierung einer Spalte lässt sich die Sortierung durch wiederholten Klick auf den Spaltenkopf wieder ausschalten.

- Spaltenbreite anpassen

Diese Funktion erreichen Sie über folgende Aktionen:

- Über das Kontextmenü, das sich bei Klicken mit der rechten Maustaste auf einen Spaltenkopf öffnet:

"Breite optimieren", "Breite aller Spalten optimieren"

- Wenn Sie den Cursor in die Nähe der Begrenzung eines Spaltenkopfs führen, erscheint das folgende Symbol:



Doppelklicken Sie in diesem Moment auf den Spaltenkopf. Die Spaltenbreite passt sich dem breitesten Eintrag in dieser Spalte an.

- Spalten ein-/ausblenden

Diese Funktion erreichen Sie über das Kontextmenü, das sich bei Klicken mit der rechten Maustaste auf einen Spaltenkopf öffnet.

## Nachrichten kopieren

Wenn Sie mit der rechten Maustaste in die Zeile eines Objekts in der Tabelle klicken, dann erreichen Sie die folgenden Kopierfunktionen über das Kontextmenü:

- Ausschneiden
- Kopieren
- Einfügen

Einfügen können Sie ausgeschnittene oder kopierte Objekte innerhalb der Tabelle oder in der ersten freien Zeile unterhalb der Tabelle.

Sie können ausgeschnittene oder kopierte Objekte auch in Tabellen anderer Kommunikationsmodule vom gleichen Typ einfügen.

- Löschen

Bei gedrückter <Strg>-Taste können Sie mehrere Zeilen selektieren, die nicht zusammenhängen.

Bei gedrückter <Shift>-Taste können Sie den Anfang und das Ende eines zusammenhängenden Bereichs selektieren.

# Programmbausteine

## 5.1 Programmbausteine für OUC

### Programmbausteine für die Open User Communication (OUC)

Verbindungen der Open User Communication werden nicht projiziert.

Für die TCP-/UDP-/ISO-on-TCP-Kommunikation über Ethernet werden die unten aufgeführten Bausteine der Open User Communication (OUC) eingesetzt. Hierfür legen Sie die entsprechenden Programmbausteine an. Details zu den Programmbausteinen finden Sie im Informationssystem von STEP 7.

---

#### Hinweis

#### Programmbaustein-Versionen

Beachten Sie, dass Sie in STEP 7 in einer Station nicht verschiedene Versionen eines Programmbausteins verwenden dürfen.

---

### Programmbausteine

Zusammen mit den drei CP-Typen stehen der CPU die folgenden OUC-Bausteine in der angegebenen Mindestversion zur Verfügung:

- **TSEND\_C V3.0 / TRCV\_C V3.0**

Kompakte Bausteine für:

- Verbindungsauf-/abbau und Senden von Daten
- Verbindungsauf-/abbau und Empfangen von Daten

Verwenden Sie alternativ:

- **TCON V4.0 / TDISCON V2.1**

Verbindungsaufbau / Verbindungsabbau

- **TUSEND V4.0 / TURCV V4.0**

Senden bzw. Empfangen von Daten über UDP

- **TSEND V4.0 / TRCV V4.0**

Senden bzw. Empfangen von Daten über TCP oder ISO-on-TCP

- **TMAIL\_C V4.0**

Senden von E-Mails

Für die Übertragung von verschlüsselten E-Mails mit diesem Baustein ist die genaue Uhrzeit im CP erforderlich. Projizieren Sie die Uhrzeitsynchronisation.

Zum Ändern der Projektierungsdaten des CP zur Laufzeit:

- **T\_CONFIG V1.0**

Programmgesteuerte Konfiguration der IP-Parameter

Siehe hierzu Kapitel Änderung der IP-Parameter zur Laufzeit (Seite 82).

Die Programmbausteine finden Sie in STEP 7 im Fenster "Anweisungen > Kommunikation > Open User Communication".

## Verbindungsbeschreibungen in Systemdatentypen (SDTs)

Für die jeweilige Verbindungsbeschreibung verwenden die oben genannten Bausteine den Parameter CONNECT (bzw. MAIL\_ADDR\_PARAM bei TMAIL\_C). Die Verbindungsbeschreibung wird in einem Datenbaustein abgelegt, dessen Struktur durch einen Systemdatentyp (SDT) festgelegt wird.

### Anlegen eines SDT für die Datenbausteine

Legen Sie zu jeder Verbindungsbeschreibung den erforderlichen SDT als Datenbaustein (Global-DB) an.

Der SDT-Typ wird erzeugt, indem Sie in der Deklarationstabelle des Bausteins nicht einen Eintrag aus der Klappliste "Datentyp" wählen, sondern in das Feld "Datentyp" manuell den Namen eingeben, beispielsweise "TCON\_IP\_V4". Der entsprechende SDT wird dann mit seinen Parametern angelegt.

### SDTs

Abhängig von den CP-spezifischen Security-Funktionen unterstützen die drei CP-Typen folgende SDTs:

- **SDTs für alle drei CP-Typen**

- **TCON\_IP\_V4**

Für die Übertragung von Daten über TCP oder UDP

- **TCON\_QDN**

Für die TCP- oder UDP-Kommunikation über den voll qualifizierten Domänen-Namen (FQDN) (IPv4 / IPv6)

- **TCON\_IP\_RFC**

Für die Übertragung von Daten über ISO-on-TCP (direkte Kommunikation zwischen zwei S7-Stationen)

- **TADDR\_Param**

Für die Übertragung von Daten über UDP

- **TMail\_V4**

Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv4-Adresse

- **TMail\_V6**

Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv6-Adresse



– **TMail\_FQDN**

Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über dessen Namen (FQDN)

• **Zusätzlich für CP 1542SP-1 IRC und CP 1543SP-1**

– **TMail\_V4\_SEC**

Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv4-Adresse

– **TMail\_V6\_SEC**

Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv6-Adresse

– **TMail\_QDN\_SEC**

Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über den Host-Namen

Hinweis zu TMail\_Vx\_SEC / TMail\_QDN\_SEC:

Bei diesen SDTs wird das Mailserver-Zertifikat geprüft, die ID des Zertifikats "TLSServerCertRef" (STEP 7-interne Referenz) jedoch nicht.

• **Zusätzlich für CP 1543SP-1**

– **TCON\_IP\_V4\_SEC**

Für die gesicherte Übertragung von Daten über TCP

– **TCON\_QDN\_SEC**

Für die gesicherte Übertragung von Daten über den Host-Namen

Die Beschreibung der SDTs mit ihren Parametern finden Sie im STEP 7-Informationssystem unter dem jeweiligen Namen des SDT.

## Verbindungs-Auf- und Abbau

Mit dem Programmbaustein TCON werden Verbindungen aufgebaut. Beachten Sie, dass für jede Verbindung ein eigener Programmbaustein TCON aufgerufen werden muss.

Für jeden Kommunikationspartner muss eine eigene Verbindung aufgebaut werden, auch wenn identische Datenblöcke gesendet werden.

Nach erfolgter Datenübermittlung kann eine Verbindung abgebaut werden. Eine Verbindung wird durch Aufruf von TDISCON abgebaut.

---

### Hinweis

#### Verbindungsabbruch

Wenn eine bestehende Verbindung durch den Kommunikationspartner oder durch netzbedingte Störungen abgebrochen wird, dann muss die Verbindung auch durch den Aufruf von TDISCON abgebaut werden. Berücksichtigen Sie dies bei der Programmierung.

---

## 5.2 Änderung der IP-Parameter zur Laufzeit

### Änderung der IP-Adresse zur Laufzeit

Ab STEP 7 V14 können Sie mit T\_CONFIG die folgenden Adressparameter des CP zur Laufzeit programmgesteuert ändern:

- IP-Adresse
- Subnetzmaske
- Router-Adresse

---

#### Hinweis

##### Änderung der IP-Parameter bei dynamischer IP-Adresse

Beachten Sie die Auswirkungen der programmgesteuerten Änderung der IP-Parameter in dem Fall, dass der CP eine dynamische IP-Adresse durch den angeschlossenen Router bezieht: In diesem Fall ist der CP nicht mehr durch Kommunikationspartner zu erreichen.

---

#### Hinweis

##### Voraussetzung in der CP-Projektierung

Um die IP-Parameter programmgesteuert ändern zu können, muss in der Projektierung der IP-Adresse der Ethernet-Schnittstelle des CP die Option "Anpassen der IP-Adresse direkt am Gerät erlauben" aktiviert sein.

---

### Programmbausteine

Die programmgesteuerte Änderung der IP-Parameter wird durch Programmbausteine unterstützt. Die Programmbausteine greifen auf Adressdaten zu, die in einem passenden Systemdatentyp (SDT) hinterlegt sind.

Außer den Adress-Parametern des CP können mit T\_CONFIG auch die Adress-Parameter von DNS-Servern (IF\_CONF\_DNS) und NTP-Servern (IF\_CONF\_NTP) programmgesteuert geändert werden.

Folgende Programmbausteine und Systemdatentypen können verwendet werden:

- **T\_CONFIG**

Zusammen mit folgenden SDTs:

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

Detaillierte Informationen zu den Bausteinen und SDTs finden Sie im STEP 7-Informationssystem.

## **5.3 MODBUS-Bausteine**

### **MODBUS (TCP)**

Alle drei CP-Typen unterstützen die Programmbausteine für MODBUS (TCP):

- MB\_CLIENT
- MB\_SERVER

Detaillierte Informationen finden Sie im Informationssystem von STEP 7.



# Diagnose und Instandhaltung

## 6.1 Diagnosemöglichkeiten

Folgende Diagnosemöglichkeiten stehen Ihnen zur Verfügung.

### LEDs der Baugruppe

Informationen zu den LED-Anzeigen finden Sie im Kapitel LEDs (Seite 35).

### STEP 7: Das Register "Diagnose" im Inspektorfenster

Hier erhalten Sie folgende Informationen zum Online-Status der selektierten Baugruppe.

### STEP 7: Diagnosefunktionen im Menü "Online > Online und Diagnose"

Über die Online-Funktionen können Sie von einer Engineering-Station, auf welcher das Projekt mit dem CP gespeichert ist, Diagnoseinformationen aus dem CP lesen.

CP 1542SP-1 IRC / CP 1543SP-1: Wenn Sie Online-Diagnose mit der Station über den CP betreiben möchten, dann müssen Sie als Voraussetzung unter "Kommunikationsarten" die Option "Online-Funktionen aktivieren" freischalten.

#### Gruppe "Diagnose"

Die Diagnosesseiten sind in folgende Gruppen aufgeteilt:

- **Allgemein**

Diese Gruppe zeigt allgemeine Angaben zur Baugruppe an.

- **Diagnosestatus**

Diese Gruppe zeigt Statusinformationen des Moduls aus Sicht der CPU an.

- Gerätespezifische Ereignisse

Bei Modulen mit Security- oder Telecontrol-Funktionen werden Angaben zu Modul-internen Ereignissen angezeigt.

- **Ethernet-Schnittstelle**

Adress- und statistische Angaben

- **Industrial Remote Communication**

Für den CP 1542SP-1 IRC erhalten Sie hier Telecontrol-spezifische Informationen. Die Gruppe hat folgende Diagnoseseiten:

- Partner

Angaben zu Adressangaben des Partners, Verbindungsstatistik, Projektierungsdaten des Partners und weitere Diagnoseinformationen

- Datenpunktliste

Verschiedene Informationen zu den Datenpunkten wie Projektierungsdaten, Wert, Verbindungszustand etc.

- Protokolldiagnose

Über die Schaltfläche "Protokoll-Trace aktivieren" werden die Telegramme, die von der Baugruppe empfangen und gesendet werden, für einige Sekunden mitgeschrieben.

Über "Protokoll-Trace deaktivieren" werden die Protokollierung angehalten und die Daten in eine Protokollierungsdatei geschrieben.

Über "Speichern" können Sie die Protokollierungsdatei auf der Engineering-Station speichern und anschließend analysieren.

- **Uhrzeit**

Angaben zur Uhrzeit im Gerät

- **Security**

Die Gruppe steht bei den Modulen mit Security-Funktionen zur Verfügung.

- Zustand

Diese Diagnoseseite zeigt die wichtigsten Security-Einstellungen, die Uhrzeit und Daten zur Konfiguration an.

- System-Log

Auf dieser Diagnoseseite können Sie bei bestehender Verbindung zu einem SCALANCE S-Modul die Protokollierung der System-Einträge starten. Sie können die Einträge speichern.

- Audit-Log

Auf dieser Diagnoseseite können Sie die Protokollierung der Log-Daten des Moduls starten. Sie können die Einträge speichern.

- Kommunikationszustand

Diese Diagnoseseite zeigt die Zustände der bekannten Security-Module der VPN-Gruppe, deren Endpunkte und der Tunneleigenschaften an.

- SINEMA RC - Automatische VPN-Konfiguration

Diese Diagnoseseite zeigt den Status der automatischen OpenVPN-Konfiguration und der OpenVPN-Verbindungen an.

### Gruppe "Funktionen"

- **Firmware-Update**

Zur Beschreibung siehe Kapitel Firmware laden (Seite 94).

- **IP-Adresse zuweisen**

- **PROFINET-Gerätenamen vergeben**

- **Servicedaten speichern**

Die Funktion dient der Protokollierung von internen Prozessen der Baugruppe in Situationen, in denen Sie unerwartetes oder unerwünschtes Verhalten der Baugruppe nicht selbständig beheben können.

Über die Schaltfläche "Servicedaten speichern" wird die Protokollierungsdatei angelegt. Die Daten werden in eine Datei vom Format "\*.dmp" gespeichert, die vom Siemens Customer Support ausgewertet werden kann.

### Webserver der CPU

Über den CP können Sie auf den Webserver der CPU und die dort verfügbaren Informationen zugreifen. Zum Zugriff siehe Kapitel Webserver der CPU (Seite 90).

### SNMP

Zu den Funktionen siehe Kapitel Diagnose über SNMP (Seite 88).

### Diagnose-E-Mail

Gültigkeit: CP 1542SP-1 IRC / CP 1543SP-1

Die beiden CPs können bei projektierbaren Ereignissen wie bspw. dem Ausfall der Erreichbarkeit eines Partners oder beim STOP der CPU eine Diagnose-E-Mail verschicken.

Die Projektierung ist im Kapitel Nachrichten: E-Mails (CP 1543SP-1) (Seite 75) beschrieben.

### Telecontrol-Diagnose

Gültigkeit: CP 1542SP-1 IRC

- **Partnerstatus**

Der CP kann der CPU den Zustand der Verbindung zum Kommunikationspartner über eine PLC-Variable signalisieren.

Zur Projektierung siehe Telecontrol-Projektierungshandbücher /10/ (Seite 113).

- **CP-Diagnose**

Der CP kann erweiterte Diagnosedaten in PLC-Variablen ablegen.

Zur Projektierung siehe Kapitel Kommunikation mit der CPU (Seite 58).

Die Zustände der PLC-Variablen können Sie beispielsweise über den Webserver der CPU oder über eine Beobachtungstabelle anzeigen.

## 6.2 Online-Security-Diagnose über Port 8448 (CP 1542SP-1 IRC, CP 1543SP-1)

### Security-Diagnose über Port 8448

Voraussetzungen:

- Der Zugriff auf den Webserver der Station über HTTPS ist aktiviert.
- Bei aktivierter Firewall muss der Zugang freigegeben sein.

Wenn Sie in STEP 7 Professional eine Security-Diagnose durchführen möchten, dann gehen Sie folgendermaßen vor:

1. Selektieren Sie in STEP 7 den CP.
2. Öffnen Sie das Kontextmenü "Online & Diagnose".
3. Klicken Sie in der Parametergruppe "Security" auf die Schaltfläche "Online verbinden".

Über diesen Weg führen Sie die Security-Diagnose über Port 8448 aus.

### Siehe auch

Einstellungen für Online-Security-Diagnose und Laden in Station bei aktivierter Firewall (Seite 62)

## 6.3 Diagnose über SNMP

### Voraussetzung

Voraussetzung für die Nutzung von SNMP ist die Aktivierung der Funktion in der Projektierung, siehe Kapitel SNMP (Seite 60).

### SNMP (Simple Network Management Protocol)

SNMP ist ein Protokoll für die Diagnose und Verwaltung von Netzwerken und Teilnehmern im Netzwerk. Für die Datenübertragung verwendet SNMP das verbindungslose Protokoll UDP.

Informationen über die Eigenschaften von SNMP-fähigen Geräten sind in MIB-Dateien (MIB = Management Information Base) hinterlegt.

Ausführliche Informationen zu SNMP und der Siemens Automation MIB finden Sie im Handbuch /6/ (Seite 112).

### Leistungsumfang der CPs

Die CPs unterstützen folgende SNMP-Versionen:

- **CP 1542SP-1**
  - SNMPv1



- **CP 1543SP-1, CP 1542SP-1 IRC**
  - SNMPv1
  - SNMPv3 (bei aktivierten Security-Funktionen)Zur Projektierung von SNMPv3 siehe Kapitel SNMP (Seite 72).  
Traps werden vom CP nicht unterstützt.

### Unter SNMPv1 unterstützte MIBs

Die CPs unterstützen folgende MIBs:

- **MIB II (gemäß RFC1213)**

Der CP unterstützt folgende Gruppen von MIB-Objekten:

  - System
  - Interfaces
  - IP
  - ICMP
  - TCP
  - UDP
  - SNMP
- **LLDP MIB**

### Unter SNMPv3 unterstützte MIB-Objekte

Bei aktiviertem SNMPv3 liefert der CP die Inhalte folgender MIB-Objekte:

- **MIB II (gemäß RFC1213)**

Der CP unterstützt folgende Gruppen von MIB-Objekten:

  - System
  - Interfaces  
Das MIB-Objekt "Interfaces" liefert Zustandsinformationen über die CP-Schnittstellen.
  - IP (IPv4/IPv6)
  - ICMP
  - TCP
  - UDP
  - SNMPFolgende Gruppen der Standard-MIB II werden nicht unterstützt:
  - Adress Translation (AT)
  - EGP
  - Transmission
- **LLDP MIB**

### Zugriffsrechte über Community-Namen (SNMPv1)

Der CP verwendet in der Voreinstellung folgende Community-Strings zur Steuerung der Rechte zum Zugriff auf den SNMP-Agenten:

Tabelle 6- 1 Zugriffsrechte im SNMP-Agenten

Zugriffsart	Community String *)
Lesezugriff	public
Lese- und Schreibzugriff	private

\*) Beachten Sie die Schreibweise mit Kleinbuchstaben!

Bei aktivierten Security-Funktionen sind die Community-Strings projektierbar.

## 6.4 Webserver der CPU

### Der Webserver der CPU

Die CPU hat einen Webserver, auf den Sie von einem PC aus mittels HTTP/HTTPS über den CP zugreifen können.

Der Webserver der CPU bietet vielfältige Funktionen zur Diagnose und für Service-Zwecke. Detaillierte Informationen finden Sie im Systemhandbuch /2/ (Seite 112) und im Informationssystem von STEP 7 unter dem Stichwort "Webserver".

### Voraussetzungen für den Zugriff auf den Webserver

#### Zugelassene Webbrowser

Die unterstützten Webbrowser auf dem PC für den Zugriff auf den Webserver der CPU finden Sie im STEP 7-Informationssystem unter dem Stichwort "Webserver".

#### Voraussetzungen in der Projektierung der CPU

1. Öffnen Sie an der Engineering-Station das entsprechende Projekt.
2. Selektieren Sie in STEP 7 die CPU der betreffenden Station.
3. Selektieren Sie den Eintrag "Webserver".
4. Aktivieren Sie in der Parametergruppe "Allgemein" die Option "Webserver auf dieser Baugruppe aktivieren".

5. Legen Sie bei der CPU in der Benutzerverwaltung einen Benutzer mit den entsprechenden Rechten an.  
Zu Laden von Firmware müssen Sie diesem Benutzer unter der Zugriffsstufe das Recht zuweisen, Firmware-Updates durchzuführen.  
Benutzername und Passwort werden später für den Zugriff benötigt.
6. Projektierung der Option "Zugriff nur über HTTPS zulassen" in der Parametergruppe "Allgemein"  
Abhängig davon, ob Sie über HTTP oder über HTTPS auf den Webserver zugreifen möchten, unterscheidet sich die Projektierung des Parameters:
  - "Zugriff nur über HTTPS zulassen" aktiviert  
Der Verbindungsaufbau ist nur über HTTPS möglich.
  - "Zugriff nur über HTTPS zulassen" deaktiviert  
Der Verbindungsaufbau ist über HTTP und HTTPS möglich.

#### **Zusätzliche Voraussetzungen in der Projektierung des CP 1543SP-1**

Aktivieren Sie die Firewall in der Parametergruppe "Security".

Abhängig vom verwendeten Protokoll müssen Sie folgende weitere Einstellungen in der Parametergruppe der Firewall "Von Extern nach Station" vornehmen.

- Bei Verbindungsaufbau über HTTP
  - Aktivieren Sie die Option "Erlaube HTTP"
  - Aktivieren Sie die Option "Erlaube HTTPS"  
Begründung: Nach der Authentifizierung am Webserver wird auf HTTPS umgeschaltet.
- Bei Verbindungsaufbau über HTTPS
  - Deaktivieren Sie die Option "Erlaube HTTP"
  - Aktivieren Sie die Option "Erlaube HTTPS"

### **Verbindung mit dem Webserver aufbauen**

Gehen Sie folgendermaßen vor, um sich von dem PC aus mit dem Webserver der CPU zu verbinden.

Die beiden Varianten sind in den folgenden Abschnitten beschrieben.

#### **Verbindungsaufbau über HTTP**

1. Verbinden Sie den PC über die Ethernet-Schnittstelle mit dem CP.
2. Geben Sie die Adresse des CP in das Adressfeld Ihres Webbrowsers ein:  
http://<IP-Adresse>
3. Drücken Sie die Eingabetaste <Enter>.

Die Startseite des Webservers öffnet sich.

4. Klicken Sie auf den Eintrag "Download-Zertifikat" rechts oben im Fenster.

Das Dialogfeld "Zertifikat" öffnet sich.

5. Laden Sie das Zertifikat auf Ihren PC, indem Sie auf die Schaltfläche "Zertifikat installieren ..." klicken.

Das Zertifikat wird auf Ihren PC geladen.

Informationen zum Laden eines Zertifikats finden Sie in der Hilfe Ihres Webbrowsers und im STEP 7-Informationssystem unter dem Stichwort "Zertifikate für Webserver".

Wenn die Verbindung in den sicheren Modus HTTPS gewechselt ist ("https://<IP-Adresse>/..." im Adressfeld des Webrowsers), dann können Sie den Webserver bedienen, beispielsweise eine Firmware-Datei laden (siehe nachfolgender Abschnitt).

Wenn Sie die Verbindung zum Webserver trennen, dann können Sie sich das nächste mal ohne das Laden des Zertifikats über HTTP am Webserver anmelden.

#### Verbindungsaufbau über HTTPS

1. Verbinden Sie den PC über die Ethernet-Schnittstelle mit dem CP oder der CPU.
2. Geben Sie die Adresse des CP in das Adressfeld Ihres Webbrowsers ein:  
https://<IP-Adresse>
3. Drücken Sie die Eingabetaste <Enter>.

Die Startseite des Webrowsers öffnet sich.

Sie können den Webserver bedienen.

## 6.5 Bearbeitungsstatus von E-Mails (CP 1543SP-1)

### Bearbeitungsstatus von E-Mails

Die nachfolgenden Statuskennungen gelten für E-Mails, die über den Nachrichteneditor des CP projiziert wurden, vgl. Kapitel Nachrichten: E-Mails (CP 1543SP-1) (Seite 75).

E-Mails, die über Programmbausteine der Open User Communication versendet werden, geben über den Baustein andere Status zurück (siehe Bausteinhilfen).

### Bearbeitungsstatus der E-Mails des Nachrichteneditors

Die gelieferten Status der "PLC-Variable für Bearbeitungsstatus" haben folgende Bedeutung:

Tabelle 6-2 Bedeutung der hexadezimal ausgegebenen Statuskennung

Status	Bedeutung
0000	Übertragung fehlerfrei abgeschlossen
82xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht die Meldung der dreistelligen Fehlernummer des Protokolls SMTP.

Status	Bedeutung
8401	Kein Kanal verfügbar. Mögliche Ursache: Es besteht bereits eine E-Mail-Verbindung über den CP. Eine zweite Verbindung kann nicht parallel eingerichtet werden.
8403	Es konnte keine TCP/IP-Verbindung zum SMTP-Server aufgebaut werden.
8405	Der SMTP-Server hat die Login-Anfrage verweigert.
8406	Ein interner SSL-Fehler oder ein Problem mit der Struktur des Zertifikats wurde durch den SMTP-Client festgestellt.
8407	Anfrage zur Verwendung von SSL wurde verweigert.
8408	Der Client konnte kein Socket zur Erstellung einer TCP/IP-Verbindung zum Mail-Server ermitteln.
8409	Über die Verbindung kann nicht geschrieben werden. Mögliche Ursache: Durch den Kommunikationspartner wurde ein Reset der Verbindung durchgeführt oder die Verbindung wurde abgebrochen.
8410	Über die Verbindung kann nicht gelesen werden. Mögliche Ursache: Durch den Kommunikationspartner wurde die Verbindung abgebaut oder die Verbindung wurde abgebrochen.
8411	Senden der E-Mail fehlgeschlagen. Ursache: Speicherplatz war nicht ausreichend, um den Sendevorgang durchzuführen.
8412	Konfigurierter DNS-Server konnte den angegebenen Domain-Namen nicht auflösen.
8413	Aufgrund eines internen Fehlers im DNS-Subsystem konnte der Domain-Name nicht aufgelöst werden.
8414	Als Domain-Name wurde eine leere Zeichenkette angegeben.
8415	Ein interner Fehler ist im Curl-Modul aufgetreten. Ausführung wurde abgebrochen.
8416	Ein interner Fehler ist im SMTP-Modul aufgetreten. Ausführung wurde abgebrochen.
8417	Anfrage an SMTP auf bereits verwendetem Kanal oder ungültige Kanal-ID. Ausführung wurde abgebrochen.
8418	Senden der E-Mail wurde abgebrochen. Mögliche Ursache: Überschreitung der Ausführungszeit.
8419	Der Kanal wurde unterbrochen und kann nicht verwendet werden, bevor die Verbindung abgebaut wird.
8420	Zertifikatskette vom Server konnte nicht mit dem Root-Zertifikat des CP verifiziert werden.
8421	Interner Fehler aufgetreten. Ausführung wurde gestoppt.
8450	Aktion nicht ausgeführt: Mailbox nicht verfügbar / nicht erreichbar. Versuchen Sie es später noch einmal.
84xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht die Meldung der dreistelligen Fehlernummer des Protokolls SMTP.
8500	Syntax-Fehler: Kommando unbekannt. Das schließt auch den Fehler einer zu langen Befehlskette ein. Ursache kann sein, dass der E-Mail-Server das Authentifizierungsverfahren LOGIN nicht unterstützt. Versuchen Sie, E-Mails ohne Authentifizierung zu versenden (kein Benutzername).
8501	Syntax-Fehler. Überprüfen Sie die folgenden Projektierungsdaten: Meldungskonfiguration > E-Mail-Daten (Content): <ul style="list-style-type: none"> <li>• Empfängeradresse ("An" bzw. "Cc").</li> </ul>
8502	Syntax-Fehler. Überprüfen Sie die folgenden Projektierungsdaten: Meldungskonfiguration > E-Mail-Daten (Content): <ul style="list-style-type: none"> <li>• E-Mail-Adresse (Absender)</li> </ul>

Status	Bedeutung
8535	SMTP-Authentifizierung unvollständig. Überprüfen Sie in der CP-Projektierung die Parameter "Benutzername" und "Passwort".
8550	SMTP-Server kann nicht erreicht werden. Sie haben keine Zugriffsrechte. Überprüfen Sie die folgenden Projektierungsdaten: <ul style="list-style-type: none"><li>• CP-Projektierung &gt; E-Mail-Projektierung:<ul style="list-style-type: none"><li>– Benutzername</li><li>– Passwort</li><li>– E-Mail-Adresse (Absender)</li></ul></li><li>• Meldungskonfiguration &gt; E-Mail-Daten (Content):<ul style="list-style-type: none"><li>– Empfängeradresse ("An" bzw. "Cc").</li></ul></li></ul>
8554	Übertragung fehlgeschlagen
85xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht die Meldung der dreistelligen Fehlernummer des Protokolls SMTP.

## 6.6 Firmware laden

### Neue Firmware-Versionen des CP

Wenn für den CP eine neue Firmware-Version zur Verfügung steht, dann finden Sie diese auf den Internet-Seiten des Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22144/dl>)

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/dl>)

Zum Laden einer neuen Firmware-Datei in den CP stehen Ihnen drei Wege zur Verfügung:

- Speichern der Firmware-Datei auf der Memory Card der CPU  
Eine Beschreibung der Vorgehensweise zum Laden auf die Memory Card der CPU finden Sie auf der oben angegebenen Internetseite des Industry Online Support.
- Laden der Firmware mit den Online-Funktionen von STEP 7 über Ethernet / Internet  
Die Beschreibung finden Sie nachfolgend.

---

#### Hinweis

##### Dauer der Firmware-Aktualisierung

Das Laden einer neuen Firmware-Datei kann mehrere Minuten dauern.

Beachten Sie, dass der Vorgang umso länger dauert, je größer der Ausbau der Station mit Peripheriemodulen ist.

Warten Sie immer so lange, bis der Abschluss der Firmware-Aktualisierung an den LEDs erkennbar ist (LED-Bild "Wartungsanforderung" - Ende der Firmware-Aktualisierung).

---

## Laden der Firmware mit den Online-Funktionen von STEP 7 über Ethernet

### Voraussetzungen:

- Der CP oder die CPU ist über die IP-Adresse erreichbar.
- Die Engineering-Station und der CP liegen im gleichen Subnetz.
- Die neue Firmware-Datei ist auf Ihrer Engineering-Station gespeichert.
- Die Engineering-Station ist mit dem Netz verbunden.
- Auf der Engineering-Station ist das betreffende STEP 7-Projekt geöffnet.

### Vorgehensweise:

1. Selektieren Sie den CP oder die CPU derjenigen Station, dessen CP Sie mit einer neuen Firmware aktualisieren möchten.
  2. Aktivieren Sie die Online-Funktionen über das Symbol "Online verbinden".
  3. Selektieren Sie im Dialog "Online verbinden" in der Auswahlliste "Typ der PG/PC-Schnittstelle" die Ethernet-Schnittstelle.
  4. Selektieren Sie den Steckplatz des CP oder der CPU.  
Beide Wege sind möglich.
  5. Klicken Sie auf "Suche starten", um das Modul im Netz zu suchen und den Verbindungsweg festzulegen.  
Wenn das Modul gefunden wurde, wird es in der Tabelle angezeigt.
  6. Verbinden Sie sich über die Schaltfläche "Verbinden".  
Der Assistent "Online verbinden" führt Sie durch die weiteren Schritte.
  7. Selektieren Sie in der Netzsicht den CP und wählen Sie das Kontextmenü "Online & Diagnose" (rechte Maustaste).
  8. Wählen Sie in der Navigation der Online & Diagnose-Sicht den Eintrag "Funktionen > Firmware-Update".
  9. Suchen Sie über die Schaltfläche "Durchsuchen" (Parametergruppe "Firmware-Lader") die neue Firmware-Datei im Dateisystem der Engineering-Station.
  10. Starten Sie das Laden der Firmware über die Schaltfläche "Starte Aktualisierung", wenn im Ausgabefeld "Status" die richtige Version der signierten Firmware angezeigt wird.
- Weitere Hilfe zu den Online-Funktionen bietet Ihnen das STEP 7-Informationssystem.

## 6.7 Baugruppentausch

 **VORSICHT**

**Lesen Sie das Systemhandbuch "SIMATIC ET 200SP Dezentrales Peripheriesystem"**

Lesen Sie vor der Montage, dem Anschließen und der Inbetriebnahme die entsprechenden Abschnitte im Systemhandbuch "SIMATIC ET 200SP Dezentrales Peripheriesystem" (siehe Literaturverweis im Anhang).

Gehen Sie bei der Montage und dem Anschließen entsprechend den Beschreibungen im Systemhandbuch "SIMATIC ET 200SP Dezentrales Peripheriesystem" vor.

Stellen Sie sicher, dass während der Montage/Demontage der Geräte die Spannungsversorgung ausgeschaltet ist.

### Baugruppentausch

Die STEP-7-Projektdateien des CP werden auf der jeweils lokalen CPU gespeichert. Dies ermöglicht im Ersatzteilfall einen einfachen Austausch des CP, ohne die Projektdateien erneut in die Station laden zu müssen.

Beim Wiederanlauf der Station liest der neue CP die Projektdateien von der CPU.

**Ausnahme:**

Die Daten der SINEMA RC-Projektierung und das Zertifikat des SINEMA RC-Servers sind im CP gespeichert. Sie können nicht von der CPU gelesen werden.



# Technische Daten

<b>Technische Daten</b>		
<b>Artikelnummern</b>	CP 1542SP-1	6GK7542-6UX00-0XE0
	CP 1542SP-1 IRC	6GK7542-6VX00-0XE0
	CP 1543SP-1	6GK7543-6WX00-0XE0
<b>Anschluss an Industrial Ethernet</b>		
Anzahl	1	
Ausführung	Steckplatz für BusAdapter	
Eigenschaften	Zu den Eigenschaften der BusAdapter und den zulässigen Leitungslängen siehe /3/ (Seite 112).	
<b>Elektrische Daten</b>		
Externe Spannungsversorgung (X80), Ausführung	Buchse Klemmenblock für Buchse	Zweipolig mit Verpolschutz 2 x zweipolig für einfache oder redundante Spannungsversorgung
Versorgungsspannung (extern)	<ul style="list-style-type: none"> <li>• Spannungsart</li> <li>• Zulässige untere Grenze</li> <li>• Zulässige obere Grenze</li> </ul>	<ul style="list-style-type: none"> <li>• DC 24 V</li> <li>• 19,2 V</li> <li>• 28,8 V</li> </ul>
Stromaufnahme	Aus Rückwandbus (3,3 V)	4 mA (typ.)
	Aus DC 24 V (extern)	Gesteckter BusAdapter:
	<ul style="list-style-type: none"> <li>• Mit BusAdapter BA 2xRJ45               <ul style="list-style-type: none"> <li>– typ.</li> <li>– max.</li> </ul> </li> <li>• Mit BusAdapter BA 2xLC               <ul style="list-style-type: none"> <li>– typ.</li> <li>– max.</li> </ul> </li> <li>• Mit BusAdapter BA SCRJ               <ul style="list-style-type: none"> <li>– typ.</li> <li>– max.</li> </ul> </li> <li>• Mit BusAdapter BA 2xVD               <ul style="list-style-type: none"> <li>– typ.</li> <li>– max.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• BA 2xRJ45               <ul style="list-style-type: none"> <li>– 115 mA</li> <li>– 140 mA</li> </ul> </li> <li>• BA 2xLC               <ul style="list-style-type: none"> <li>– 185 mA</li> <li>– 225 mA</li> </ul> </li> <li>• BA SCRJ               <ul style="list-style-type: none"> <li>– 150 mA</li> <li>– 240 mA</li> </ul> </li> <li>• BA 2xVD               <ul style="list-style-type: none"> <li>– 150 mA</li> <li>– 180 mA</li> </ul> </li> </ul>
Maximaler Einschaltstrom	(Nennwert)	12 A
Verlustwirkleistung	(typisch)	6 W
Überspannungskategorie gemäß IEC / EN 60664-1	Kategorie I	
<b>Zulässige Umgebungsbedingungen</b>		
Umgebungstemperatur	Während Betrieb bei waagerechtem Aufbau des Baugruppenträgers	-30 .. + 60 °C

---

**Technische Daten**

---

	Während Betrieb bei senkrechtem Aufbau des Baugruppenträgers	-30 .. + 50 °C
	Während Lagerung	-40 .. +70 °C
	Während Transport	-40 .. +70 °C
Relative Luftfeuchte	Während Betrieb	≤ 95 % bei 25 °C, ohne Kondensation

---

**Bauform, Maße und Gewicht**

---

Baugruppenformat	Kompaktbaugruppe ET 200SP
Schutzart	IP20
Gewicht	
• Ohne BusAdapter	• 180 g
• Mit BusAdapter 2xRJ45	• 230 g
Abmessungen (B x H x T)	60 x 117 x 74 mm
Montagemöglichkeiten	DIN-Hutschiene (35 mm)

---

**Mean Time Between Failures (MTBF)**

---

• Bei + 40 °C	• 56,87 Jahre
• Bei + 60 °C	• 24,78 Jahre

---

<b>Produktfunktionen</b>	Weitere Eigenschaften und Leistungsdaten finden Sie im Kapitel Anwendung und Funktionen (Seite 13).
--------------------------	---

---

# Zulassungen

## Erteilte Zulassungen

---

### Hinweis

#### Erteilte Zulassungen auf dem Typenschild des Geräts

Die angegebenen Zulassungen gelten erst dann als erteilt, wenn auf dem Produkt eine entsprechende Kennzeichnung angebracht ist. Welche der nachfolgenden Zulassungen für Ihr Produkt erteilt wurde, erkennen Sie an den Kennzeichnungen auf dem Typenschild.

---

## Gültigkeitsbereich der Zulassungen

Die nachfolgend aufgeführten Zulassungen sind gültig für den CP.

Die für die Zulassungen erforderlichen Prüfungen wurden mit gestecktem BusAdapter durchgeführt.

Die BusAdapter besitzen eigene Zulassungen, die hier nicht aufgeführt sind.

## EU-Konformitätserklärung



Der CP erfüllt die Anforderungen und sicherheitsrelevanten Ziele der folgenden EU-Richtlinien und entspricht den harmonisierten europäischen Normen (EN) für speicherprogrammierbare Steuerungen, die in den Amtsblättern der EU aufgeführt sind.

- **2014/34/EU (ATEX-Explosionsschutzrichtlinie)**

Richtlinie des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen; Amtsblatt der EU L96, 29/03/2014, S. 309-356

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

EMV-Richtlinie des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit; Amtsblatt der EU L96, 29/03/2014, S. 79-106

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

Richtlinie des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten; Amtsblatt der EU L174, 01/07/2011, S. 88-110

Die EU-Konformitätserklärung steht allen zuständigen Behörden zur Verfügung bei:

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

Die EU-Konformitätserklärung finden Sie auch im Internet unter folgender Adresse:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/>)

> Zertifikatart: "EU-Konformitätserklärung"

## IECEX

Das Produkt erfüllt die Anforderungen an den Explosionsschutz nach IECEX.

IECEX-Klassifikation:

- Ex ec IIC T4 Gc

Zertifikat: IECEX DEK 18.0017X

Angewandte Normen:

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

Die aktuellen Fassungen der Normen können im IECEX-Zertifikat eingesehen werden, das Sie im Internet unter der folgenden Adresse finden:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/>)

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEX (Seite 41) müssen erfüllt sein.

Beachten Sie auch die Angaben im Dokument "Use of subassemblies/modules in a Zone 2 Hazardous Area", das Sie im Internet unter der folgenden Adresse finden:

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

## ATEX



Das Produkt erfüllt die Anforderungen der EU-Richtlinie 2014/34/EU "Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen".

ATEX-Zulassung:

- II 3 G Ex ec IIC T4 Gc

Type Examination Certificate: DEKRA 18 ATEX 0025X

Angewandte Normen:

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

Die aktuellen Fassungen der Normen können in der EU-Konformitätserklärung eingesehen werden, siehe oben.

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitelhinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx (Seite 41) müssen erfüllt sein.

Beachten Sie auch die Angaben im Dokument "Use of subassemblies/modules in a Zone 2 Hazardous Area", das Sie hier finden:

- Auf der SIMATIC NET Manual Collection unter "Alle Dokumente" > "Use of subassemblies/modules in a Zone 2 Hazardous Area"
- Im Internet unter der folgenden Adresse:  
Link: (<https://support.industry.siemens.com/cs/ww/de/view/78381013>)

## EMV

Der CP erfüllt die Anforderungen der EU-Richtlinie 2014/30/EU "Elektromagnetische Verträglichkeit" (EMV-Richtlinie).

Angewandte Normen:

- EN 61000-6-4  
Elektromagnetische Verträglichkeit (EMV) - Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche
- EN 61000-6-2  
Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche

## RoHS

Der CP erfüllt die Anforderungen der EU-Richtlinie 2011/65/EU zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten.

Angewandte Norm:

- EN 50581:2012

## c(UL)us



Angewandte Normen:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment) Report / UL file: E85972 (NRAG, NRAG7)

### cULus Hazardous (Classified) Locations



Underwriters Laboratories, Inc.: CULUS Listed E223122 IND. CONT. EQ. FOR HAZ. LOC.

Angewandte Normen:

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4
- Cl. 1, Zone 2, GP. IIC T4

Ta: Siehe Temperaturklasse auf dem Typenschild des CP

Report / UL file: E223122 (NRAG, NRAG7)

Beachten Sie die Bedingungen für den sicheren Einsatz des CP gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc (Seite 41).

### 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 T4, Ta = 60 °C

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

Ta: Siehe Temperaturklasse auf dem Typenschild des CP

Beachten Sie die Bedingungen für den sicheren Einsatz des CP gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß FM (Seite 42).

### Australien - RCM



Der CP erfüllt die Anforderungen der Normen nach AS/NZS 2064 (Klasse A).

### Kennzeichnung für eurasische Zollunion



EAC (Eurasian Conformity)

Zollunion von Russland, Weißrussland und Kasachstan

Deklaration der Konformität gemäß technischer Vorschriften der Zollunion (TR CU)

### MSIP 요구사항 - For Korea only



Registration Number: MSIP REI S7M ET200SP

**A급 기기(업무용 방송통신기자재)**

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

## Aktuelle Zulassungen

SIMATIC NET-Produkte werden regelmäßig für die Zulassungen hinsichtlich bestimmter Märkte und Anwendungen bei Behörden und Zulassungsstellen eingereicht.

Wenden Sie sich an Ihre Siemens-Vertretung, wenn Sie eine Liste mit den aktuellen Zulassungen für die einzelnen Geräte benötigen, oder informieren Sie sich auf den Internet-Seiten des Siemens Industry Online Support:

Link: (<http://support.automation.siemens.com/WW/view/de/45605894>)





## Maßzeichnungen

Maßangaben in den Maßzeichnungen in Millimetern.

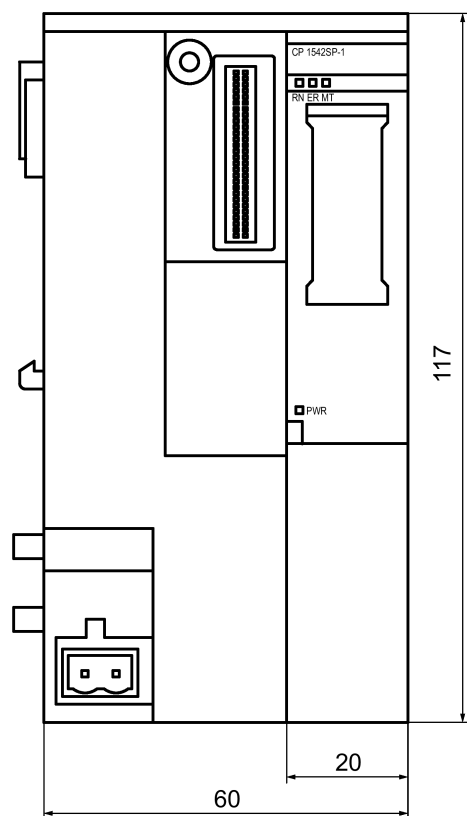


Bild B-1 Vorderansicht des CP

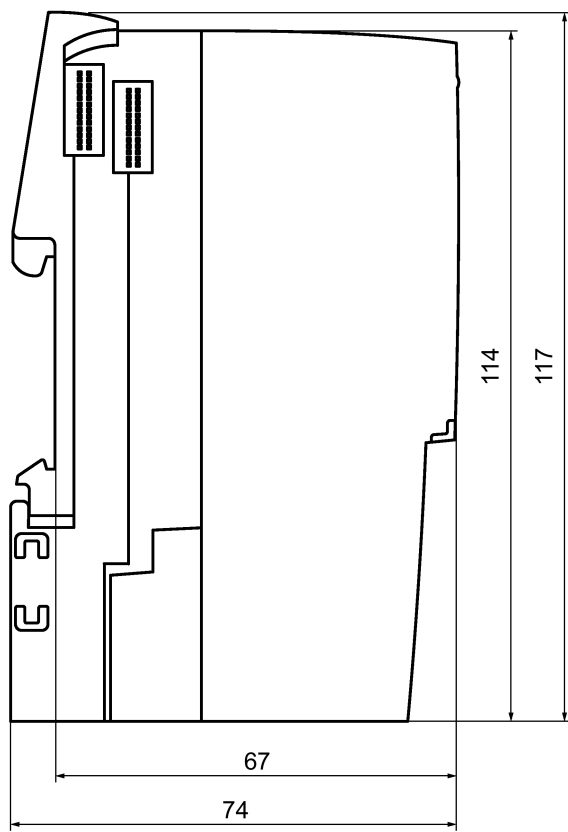


Bild B-2      Seitenansicht (links) des CP

# Zubehör

## C.1 BusAdapter

### Kompatible BusAdapter

Für den Anschluss an das Ethernet-Netz benötigt der CP einen BusAdapter. Ein BusAdapter ist nicht Teil des Lieferumfangs des CP.



Bild C-1 Beispiel eines BusAdapters, hier: BA SCRJ/RJ45

Der CP unterstützt folgende BusAdapter:

- BA 2×RJ45  
PROFINET-BusAdapter mit folgenden Anschlüssen:
  - 2 x Ethernet-Buchse RJ45Artikelnummer: 6ES7193-6AR00-0AA0
- BA 2×FC  
PROFINET-BusAdapter mit folgenden Anschlüssen:
  - 2 x direkter Anschluss des Buskabels (FastConnect)Artikelnummer: 6ES7193-6AF00-0AA0
- BA 2×SCRJ  
PROFINET-BusAdapter mit folgenden Anschlüssen:
  - 2 x Lichtwellenleiter POF/PCFArtikelnummer: 6ES7193-6AP00-0AA0

- BA SCRJ/RJ45  
PROFINET-BusAdapter, Medienkonverter LWL - Kupfer, mit folgenden Anschlüssen:
  - 1 x Lichtwellenleiter POF/PCF
  - 1 x Ethernet-Buchse RJ45
 Artikelnummer: 6ES7193-6AP20-0AA0
- BA SCRJ/FC  
PROFINET-BusAdapter, Medienkonverter LWL - Kupfer, mit folgenden Anschlüssen:
  - 1 x Lichtwellenleiter POF/PCF
  - 1 x direkter Anschluss des Buskabels (FastConnect)
 Artikelnummer: 6ES7193-6AP40-0AA0

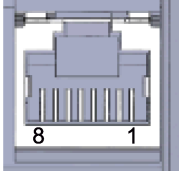
Weitere Details finden Sie im Handbuch /2/ (Seite 112) und in der Siemens Industry Mall unter:

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

## Belegung der Ethernet-Schnittstelle

Die folgende Tabelle zeigt die Anschlussbelegung der Ethernet-Schnittstelle. Die Belegung entspricht dem Ethernet-Standard 802.3-2005 in der Ausführung 100BASE-TX.

Tabelle C- 1 Anschlussbelegung Ethernet-Schnittstelle

Ansicht der RJ45-Buchse	Pin	Signalname	Belegung
	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

## C.2 Router SCALANCE M

### Router für IP-basierte Kommunikation

Für den Anschluss eines Kommunikationsmoduls an IP-basierte Infrastrukturnetze bieten sich folgende Router an:

- SCALANCE M812  
ADSL-Router für die drahtgebundene IP-Kommunikation über das Internet, VPN, Firewall, NAT, 1 Ethernet-Schnittstelle RJ45, 1 Digitaleingang, 1 Digitalausgang, ADSL2T oder ADSL2+
  - ADSL2T (analoger Telefonanschluss - Annex A)  
Artikelnummer: 6GK5812-1AA00-2AA2
  - ADSL2+ (ISDN-Anschluss - Annex B)  
Artikelnummer: 6GK5812-1BA00-2AA2
- SCALANCE M816  
ADSL-Router für die drahtgebundene IP-Kommunikation über das Internet, VPN, Firewall, NAT, 1 Ethernet-Schnittstelle RJ45 mit 4-Port-Switch, 1 Digitaleingang, 1 Digitalausgang, ADSL2T oder ADSL2+
  - ADSL2T (analoger Telefonanschluss - Annex A)  
Artikelnummer: 6GK5816-1AA00-2AA2
  - ADSL2+ (ISDN-Anschluss - Annex B)  
Artikelnummer: 6GK5816-1BA00-2AA2
- SCALANCE M826-2  
SHDSL-Router für die IP-Kommunikation über 2- und 4-Draht-Leitungen, ITU-T-Standard G.991.2 / SHDSL.biz, SHDSL-Topologie: Punkt-zu-Punkt, Bonding, Linie Bridge-Mode; Routing-Modus mit VPN, Firewall, NAT, 1 Ethernet-Schnittstelle mit 4-Port Switch, 1 Digitaleingang, 1 Digitalausgang  
Artikelnummer: 6GK5826-2AB00-2AB2
- SCALANCE M874-2  
2.5G-Router für die drahtlose IP-Kommunikation über 2.5G-Mobilfunk, VPN, Firewall, NAT, 1 Ethernet-Schnittstelle RJ45 mit 2-Port Switch, SMA-Antennenanschluss, 1 Digitaleingang, 1 Digitalausgang  
Artikelnummer: 6GK5874-2AA00-2AA2
- SCALANCE M874-3  
3G-Router für die drahtlose IP-Kommunikation über 3G-Mobilfunk HSPA+, VPN, Firewall, NAT, 1 Ethernet-Schnittstelle RJ45 mit 2-Port Switch, SMA-Antennenanschluss, 1 Digitaleingang, 1 Digitalausgang  
Artikelnummer: 6GK5874-3AA00-2AA2

- SCALANCE M876-3  
3G-Router für die drahtlose IP-Kommunikation über 3G-Mobilfunk HSPA+/EV-DO, VPN, Firewall, NAT, 1 Ethernet-Schnittstelle RJ45 mit 4-Port-Switch, SMA-Antennenanschluss, Antenna Diversity, 1 Digitaleingang, 1 Digitalausgang  
Netzbetreiber-Zulassungen beachten!
  - Internationale Ausführung  
Artikelnummer: 6GK5876-3AA02-2BA2
  - Ausführung für Korea  
Artikelnummer: 6GK5876-3AA02-2EA2
- SCALANCE M876-4  
4G-Router für die drahtlose IP-Kommunikation über LTE-Mobilfunk, VPN, Firewall, NAT, 1 Ethernet-Schnittstelle RJ45 mit 4-Port-Switch, 2 SMA-Antennenanschlüsse, MIMO-Technologie, 1 Digitaleingang, 1 Digitalausgang
  - Ausführung für Europa  
Artikelnummer: 6GK5876-4AA00-2BA2
  - Ausführung für Nordamerika  
Artikelnummer: 6GK5876-4AA00-2DA2

Informationen zu den Geräten finden Sie auf den Internetseiten des Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/15982>)

# Literaturverzeichnis

## Aufbau der Dokumentation

Beachten Sie den Aufbau der Dokumentation für die Geräte, siehe Vorwort (Seite 3).

## Auffinden der Siemens-Literatur

- Artikelnummern

Die Artikelnummern für die hier relevanten Siemens-Produkte finden Sie in den folgenden Katalogen:

- SIMATIC NET - Industrielle Kommunikation / Industrielle Identifikation, Katalog IK PI
- SIMATIC - Produkte für Totally Integrated Automation und Micro Automation, Katalog ST 70

Die Kataloge sowie zusätzliche Informationen können Sie bei Ihrer Siemens-Vertretung anfordern. Die Produktinformationen finden Sie auch in der Siemens Industry Mall unter der folgenden Adresse:

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

- Handbücher im Internet

Die SIMATIC NET-Handbücher finden Sie auf den Internet-Seiten des Siemens Industry Online Support:

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

Navigieren Sie dort im Produktbaum zum gewünschten Produkt und nehmen Sie folgende Einstellungen vor:

Beitragstyp "Handbücher"

- Handbücher auf Datenträger

Handbücher von SIMATIC NET-Produkten finden Sie auch auf dem Datenträger, der vielen SIMATIC NET-Produkten beiliegt.

/1/

SIMATIC

CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1

Betriebsanleitung

Siemens AG

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22144/man>)

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/man>)

0 /2/

**/2/**

SIMATIC  
ET 200SP - Dezentrales Peripheriesystem  
Systemhandbuch  
Siemens AG  
Link: (<http://support.automation.siemens.com/WW/view/de/58649293>)

**/3/**

SIMATIC  
ET 200SP  
Manual Collection  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/de/view/84133942>)

**/4/**

SIMATIC NET  
TeleControl Server Basic (Version V3)  
Betriebsanleitung  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/15918/man>)

**/5/**

SIMATIC NET  
TIM DNP3  
Systemhandbuch  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/15940/man>)

**/6/**

SIMATIC NET  
Diagnose und Projektierung mit SNMP  
Diagnosehandbuch  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/15392/man>)



**/17/**

SIMATIC NET  
Industrial Ethernet / PROFINET  
Systemhandbuch  
Siemens AG

- Industrial Ethernet  
Link: (<https://support.industry.siemens.com/cs/ww/de/view/27069465>)
- Passive Netzkomponenten  
Link: (<https://support.industry.siemens.com/cs/ww/de/view/84922825>)

**/18/**

SIMATIC NET  
SINEMA Remote Connect - Server  
Betriebsanleitung  
Siemens AG

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

**/19/**

SIMATIC NET  
SINAUT ST7  
Systemhandbuch  
- Band 1: System und Hardware  
- Band 2: Projektierung unter STEP 7 V5  
- Band 3: Projektierung unter STEP 7 Professional  
Siemens AG

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/21771/man>)

**/10/**

SIMATIC NET - TeleControl  
Siemens AG  
Projektierungshandbücher für die Protokolle:

- TeleControl Basic
- SINAUT ST7
- DNP3
- IEC 60870-5

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/22143/man>)



# Index

## A

Abkürzungen, 4  
IPSec-Tunnel,  
Artikelnummer, 3

## B

BusAdapter, 37  
BusAdapter - Projektierung, 53

## C

CPU-Firmware, 27

## D

Datenpufferung, 25  
DNP3  
    Geräteprofil, 16  
    Protokoll, 16  
DNS-Server - programmgesteuerte Änderung, 82  
Dokumentation - Aufbau, 5

## E

E-Mail  
    Anzahl, 24  
    Projektierung, 75  
Entsorgung, 7  
Ersatzteilfall, 96  
Ethernet-Schnittstelle  
    Belegung, 108

## F

Firewall, 20  
Firmware-Version, 3

## G

Gateway (VPN), 71  
Glossar, 7

## H

Hardware-Erzeugnisstand, 3

## I

IEC 60870-5-104  
    Geräteprofil, 17  
    Protokoll, 17  
IP\_CONF\_V4, 82  
IP-Adresse - programmgesteuerte Änderung, 82  
IP-Adresse - zuweisen, 87  
IPsec, 65  
IPv4, 22  
IPv6, 22

## L

Laden, 54

## M

MAC-Adresse, 3  
MIB, 88  
MODBUS (TCP), 83

## N

NTP, 58  
NTP (secure), 58  
NTP-Server - programmgesteuerte Änderung, 82

## O

Online-Diagnose, 54, 85  
Online-Funktionen, 87  
OUC (Open User Communication), 79

## P

Passiver VPN-Verbindungsaufbau, 71  
Port 8448, 88  
Produktbezeichnung, 4

## Q

Querkommunikation, 16  
Querverweise (PDF), 6

## R

Recycling, 7

## S

S7-Verbindungen  
  freigeben, 54  
Security-Diagnose, 88  
Security-Funktionen, 21  
Sendepuffer, 25  
Service & Support, 7  
Sicherheitshinweise, 39  
SIMATIC NET-Glossar, 7  
SINEMA Remote Connect, 14  
SMTPS, 64  
SNMP, 23, 88  
SNMPv3, 21, 72  
Spannungsversorgung, 36  
STARTTLS, 64  
Steckplatzregeln, 43  
STEP 7-Version, 27

## T

T\_CONFIG, 82  
TC\_CONFIG, 82  
TCSB  
  Version, 15  
TeleControl Basic, 15  
Telegrammspeicher, 25  
TLS, 64  
Training, 7

## U

Uhrzeitweiterleitung, 57

## V

Verbindungs-Ressourcen, 23  
VPN, 24, 65

## W

Webserver, 56