SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-7 LTE

Betriebsanleitung

CP 1243-7 LTE-EU
CP 1243-7 LTE-US

05/2021
C79000-G8900-C381-06

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.

⚠ **GEFAHR**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **WARNUNG**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **VORSICHT**
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
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:

⚠ **WARNUNG**
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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C381-06
Ⓟ 05/2021 Änderungen vorbehalten

Vorwort

Gültigkeit dieses Handbuchs

In diesem Dokument finden Sie Informationen zu folgendem Produkt:

- CP 1243-7 LTE-EU
  Artikelnummer 6GK7 243-7KX30-0XE0
  Hardware-Erzeugnisstand 3
  Firmware-Version V3.3
  Kommunikationsprozessor zum Anschluss der SIMATIC S7-1200 über LTE-, UMTS- oder GSM-Mobilfunknetze, europäischer Standard
- CP 1243-7 LTE-US

  Artikelnummer 6GK7 243-7SX30-0XE0
  Hardware-Erzeugnisstand 3
  Firmware-Version V3.3
  Kommunikationsprozessor zum Anschluss der SIMATIC S7-1200 über LTE- oder UMTS-Mobilfunknetze, nordamerikanischer Standard (AT&T-zertifiziert)

Bild 1 CP 1243-7 LTE

Hinter der oberen Gehäuseklappe der Baugruppe ist rechts neben der Artikelnummer der Hardware-Erzeugnisstand als Platzhalter "X" aufgedruckt (z. B. X 2 3 4). "X" wäre in diesem Fall der Platzhalter für den Hardware-Erzeugnisstand 1.

Die Firmware-Version des CP im Auslieferungszustand finden Sie hinter der oberen Gehäuseklappe links unter dem LED-Feld.

Die IMEI finden Sie hinter der unteren Gehäuseklappe.

Zweck des Handbuchs

Dieses Handbuch beschreibt die Eigenschaften dieser Baugruppe und unterstützt Sie bei der Montage und Inbetriebsetzung des Geräts. Weiterhin finden Sie Hinweise für den Betrieb und Diagnosemöglichkeiten des Geräts.

Die Projektierung wird abhängig von der Nutzung des CP beschrieben:

- **CP ohne Telecontrol-Kommunikation**

  Für diese Anwendungsfälle sind alle relevanten Projektierungsschritte in der vorliegenden Betriebsanleitung beschrieben.

- **CP mit Telecontrol-Kommunikation**

  Für diese Anwendungsfälle finden Sie die komplette Beschreibung der Projektierung und Diagnose im jeweiligen Projektierungshandbuch, siehe unten.

Beachten Sie die Angaben unten im Abschnitt "Aufbau der Dokumentation".

Neu in dieser Ausgabe

- Hardware-Erzeugnisstand 3, unter anderem mit folgenden neuen Funktionen:
  - Neues Mobilfunkmodul
  - Unterstützung von IPv6

  Beachten Sie den nachfolgenden Hinweis zu den Antennen.
- Firmware-Version V3.3, unter anderem mit folgenden neuen Funktionen:
  - Unterstützung des Telecontrol-Protokolls DNP3
  - Unterstützung des Telecontrol-Protokolls IEC 60870-5

  Beachten Sie hierzu den Aufbau der Dokumentation.

Hinweis

Zugelassene Antennen abhängig vom Hardware-Erzeugnisstand

Abhängig vom Hardware-Erzeugnisstand wurde der CP mit unterschiedlichen Antennen zugelassen.

Beachten Sie hierzu die Angaben im Anhang Zubehör (Seite 115).

Abgelöste Handbuchausgabe

Ausgabe 12/2019

Aufbau der Dokumentation

Die Dokumentation des CP besteht aus folgenden Handbüchern und Inhalten:

- **Betriebsanleitung**
  - Anwendung und Funktionen
  - Voraussetzungen (CPUs, Projektierungs-Software etc.)
  - Hardware-Beschreibung
  - Montage, Anschluss, Inbetriebnahme, Betrieb
  - Projektierung

    Dieses Kapitel der Betriebsanleitung beschreibt die Projektierung ohne Nutzung der Telecontrol-Funktionen.

    Wenn Sie Telecontrol-Funktionen nutzen, dann lesen Sie das betreffende Projektierungshandbuch, siehe unten.
  - Diagnose, Instandhaltung
  - Technische Daten, Zulassungen, Zubehör
- **Projektierungshandbuch**

  Projektierung und Diagnose in STEP 7 Professional (TIA Portal)

  Die Projektierungshandbücher beschreiben jeweils die komplette Projektierung des CP bei Nutzung der Telecontrol-Funktionen.
  - **Projektierungshandbuch TeleControl Basic**

    Gültig für alle SIMATIC NET-Kommunikationsmodule, die das Protokoll TeleControl Basic unterstützen.
  - **Projektierungshandbuch DNP3**

    Gültig für alle SIMATIC NET-Kommunikationsmodule, die das Protokoll DNP3 unterstützen.
  - **Projektierungshandbuch IEC 60870-5**

    Gültig für alle SIMATIC NET-Kommunikationsmodule, die das Protokoll IEC 60870-5-101/104 unterstützen.

Die Internet-Links der Handbücher finden Sie unter /3/ (Seite 118).

Aktuelle Handbuchausgabe im Internet

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

Link: (https://support.industry.siemens.com/cs/ww/de/ps/15924/man)

Vorausgesetzte Kenntnisse

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

- Automatisierungstechnik
- Aufbau des Systems SIMATIC S7-1200
- SIMATIC STEP 7 Basic / Professional
- Datenübertragung über Mobilfunknetze und Internet

Hinweise zum vorliegenden Dokument

Begriffe

- **CP / Modul / Gerät / Baugruppe**

  Vereinfachte Bezeichnung des CP 1243-7 LTE-EU / CP 1243-7 LTE-US, gültig für beide CPs.

  Wenn eine Funktion im jeweiligen Kontext nur für einen der beiden CPs relevant ist, wird dies durch Nennung des vollständigen Namens kenntlich gemacht.

- **TCSB**

  TeleControl Server Basic V3, OPC-Server für Telecontrol-Kommunikation

- **Mobilfunknetz**

  Das bzw. die Mobilfunknetze, welche der jeweilige CP unterstützt bzw. nutzt.

  Die genauen Standards und Frequenzbänder, welche die beiden CPs unterstützen, finden Sie in den Kapiteln Anschluss der S7-1200 an ein Mobilfunknetz (Seite 11) und Technische Daten (Seite 101).

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>.

Suche

Um alle Fundstellen eines gesuchten Begriffs in einer Liste anzuzeigen, unterstützen einige PDF-Reader den Befehl <Strg>+<Shift>+<F>.

Weiterführende Literatur

Eine Übersicht weiterführender Literatur finden Sie im Anhang dieses Handbuchs.

Lizenzbedingungen

Hinweis

Open Source Software

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

Sie finden die Lizenzbedingungen auf dem mitgelieferten Datenträger:

- OSS_CP124x7_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)

Security-Projektierung

Die neuesten Sicherheitsstandards werden nur mit der aktuellen Firmware-Version und bei Nutzung des aktuellen Projektierungswerkzeugs unterstützt.

Bei Austausch des Geräts gegen ein neueres werden nicht die neuesten Sicherheitsstandards unterstützt, sondern diejenigen des ausgetauschten Geräts.

Firmware

Die Firmware ist signiert und verschlüsselt. Damit 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.

Außerbetriebnahme

Nehmen Sie das Gerät ordnungsgemäß außer Betrieb, um zu verhindern, dass unbefugte Personen an vertrauliche Daten im Gerätespeicher gelangen.

Setzen Sie das Gerät hierzu auf Werkseinstellungen zurück.

Dies erreichen Sie durch Rücksetzen der CPU über die Online-Funktionen von STEP 7.

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", welches sich auf dem mitgelieferten Datenträger mit Dokumentation befindet.

Inhaltsverzeichnis

Anwendung und Funktionen

1

1.1 Anschluss der S7-1200 an ein Mobilfunknetz

Der CP ist für den Einsatz in Industrieumgebungen vorgesehen.

Mobilfunkstandards, Frequenzbänder

Mithilfe des CP lässt sich die SIMATIC-Steuerung S7-1200 an Mobilfunknetze der folgenden Standards anschließen:

- **CP 1243-7 LTE-EU**

  Der CP unterstützt folgende Mobilfunkstandards:

  – LTE

  – UMTS

  – GSM

- **CP 1243-7 LTE-US**

  Der CP ist von AT&T zertifiziert und unterstützt folgende Mobilfunkstandards:

  – LTE

  – UMTS

Die unterstützten Frequenzbänder finden Sie im Kapitel Technische Daten (Seite 101).

Umschaltung des Mobilfunkstandards bei nicht verfügbarem Netz

Wenn der Aufbau einer Verbindung über ein Mobilfunknetz mit LTE-Standard fehlschlägt, dann versucht der CP, sich in ein verfügbares Netz mit dem nächst niedrigeren Mobilfunkstandard einzuwählen. Es gilt das folgende Rückfallverhalten:

- CP 1243-7 LTE-EU: LTE → UMTS → GSM
- CP 1243-7 LTE-US: LTE → UMTS

Voraussetzung ist die Aktivierung der entsprechenden Mobilfunkstandards in der Projektierung des CP.

Länderzulassungen

Die Länder, in denen der CP zugelassen ist, finden Sie im Internet auf den Seiten des Siemens Industry Online Support. Den Link finden Sie im Kapitel Zulassungen (Seite 107).

1.2 Kommunikationsdienste

IP-basierte WAN-Kommunikation über Mobilfunknetze

Der CP ermöglicht die WAN-Kommunikation von entfernten Stationen mit einer Zentrale, die Kommunikation zwischen Stationen über eine Zentrale (Querkommunikation) und die direkte Kommunikation zwischen Stationen.

Der CP unterstützt folgende Dienste für die Kommunikation über das Mobilfunknetz bzw. über das Mobilfunknetz und das Internet:

- **Datendienste**

  Übertragung von Prozessdaten über Mobilfunknetze der folgenden Standards:

  – **GPRS / EDGE**

    (General Packet Radio Service) / (Enhanced Data Rates for GSM Evolution)

    Nur CP 1243-7 LTE EU

    Die paketorientierten Dienste der Datenübertragung GPRS/EDGE werden über das GSM-Netz abgewickelt.

    Hinweis
    Kein CDMA

    Der CP ist nicht geeignet für GSM-Netze, in denen das Code-Multiplex-Verfahren "Code Division Multiple Access" (CDMA) verwendet wird.

  – **UMTS / HSPA**

    (Universal Mobile Telecommunications System) / (High Speed Packet Access)

    UMTS ermöglicht deutlich höhere Übertragungsgeschwindigkeiten als GSM.

    HSPA ist eine Weiterentwicklung von UMTS und ermöglicht wiederum höhere Übertragungsgeschwindigkeiten.

  – **LTE**

    (Long Term Evolution)

    Mobilfunk-Spezifikation mit höherer Übertragungsgeschwindigkeit als UMTS.

- **SMS**

  (Short Message Service)

  Der CP kann SMS versenden und empfangen.

- **E-Mail**

  Der CP kann E-Mails über Mobilfunk und das Internet versenden.

Kommunikationsarten

Die folgenden Kommunikationsarten werden ermöglicht:

- **Telecontrol-Kommunikation mit einer Leitzentrale**

  Die S7-1200-Station mit Mobilfunk-CP kommuniziert über Mobilfunk und das Internet mit einer Zentrale.

- **Ereignisgesteuertes Versenden von Nachrichten (SMS / E-Mail)**

  Über das Mobilfunknetz verschickt der CP SMS an Mobiltelefone oder E-Mails an PCs mit Internetanschluss.

  Beide Nachrichtenarten werden im Nachrichteneditor von STEP 7 projektiert. Der Einsatz von Programmbausteinen ist nicht erforderlich.

  Zur Projektierung siehe Kapitel E-Mail-Projektierung (Seite 60) und Nachrichten (Seite 72).

- **Direkte Kommunikation**

  Direkte Kommunikation zwischen Stationen ist in folgenden Anwendungen möglich:

  – Open User Communication über Programmbausteine

  – Senden von Daten an Partnerstationen bei Telecontrol-Kommunikation DNP3 / IEC bei aktivierter "Master-Funktion" der Datenpunkte

Telecontrol

Der CP unterstützt folgende Arten der WAN-Kommunikation:

- **Telecontrol-Kommunikation**

  Anschluss der S7–1200 über Mobilfunk und das Internet an folgende Leitstellen-Systeme:

  – Telecontrol-Server (TeleControl Basic / TCSB)

  – DNP3-Zentrale

  – IEC-Zentrale

- **Querkommunikation**

  Kommunikation zwischen Stationen über die Zentrale (TeleControl Basic)

  In dieser Anwendung baut der CP über das Mobilfunknetz eine Verbindung mit dem Telecontrol-Server auf. Der Telecontrol-Server leitet die Telegramme an die Zielstation weiter.

E-Mail

Unabhängig von der Aktivierung der Telecontrol-Kommunikation kann der CP ereignisgesteuert projektierte E-Mails an PCs mit Internetanschluss versenden. Der Einsatz von Programmbausteinen ist hierfür nicht erforderlich. Zur Projektierung siehe unten.

Kommunikation über SINEMA Remote Connect

Unterstützung ab Firmware-Version V3.1. Siehe Kapitel Kommunikation über SINEMA RC (Seite 15).

Direkte Kommunikation über Open User Communication (OUC)

Über die Programmbausteine der Open User Communication stehen dem CP folgende Kommunikationsmöglichkeiten zur Verfügung:

- Direkte Kommunikation zwischen S7-1200-Stationen über das Mobilfunknetz

  Dazu muss dem CP eine feste IP-Adresse zugewiesen sein, siehe Kapitel Weitere Dienste und Eigenschaften (Seite 16).

- SMS und E-Mail über das Mobilfunknetz
  - Senden und Empfangen von SMS an Mobiltelefone oder S7-Stationen
  - Senden von E-Mails an PCs mit Internetanschluss

  Im Unterschied zu den beiden entsprechenden Diensten der Telecontrol-Kommunikation (siehe oben) müssen für die Übertragung von SMS/E-Mails über OUC Programmbausteine eingesetzt werden, siehe Kapitel Programmbausteine für OUC (Seite 79).

Anwendungsbeispiele finden Sie im Kapitel Konfigurationsbeispiele (Seite 23).

S7-Kommunikation

Das Lesen / Schreiben von Daten aus / in eine CPU über das Mobilfunknetz wird ermöglicht, wenn in der Projektierung des CP die S7-Kommunikation aktiviert ist.

Der CP unterstützt folgende Funktionen:

- PUT / GET

  Der CP unterstützt die Funktion als Client (Programmbausteine) und Server zum Datenaustausch mit entfernten Stationen (S7-300/400/1200/1500).

  Details zu den Programmbausteinen finden Sie im Informationssystem von STEP 7

- S7-Routing

  Ab CP-Firmware V2.1 mit CPU ≥ V4.2

Für die S7-Kommunikation benötigt der CP eine feste IP-Adresse, siehe Kapitel Weitere Dienste und Eigenschaften (Seite 16).

TeleService über das Mobilfunknetz

TeleService wird ermöglicht, wenn der CP die Telecontrol-Kommunikation "TeleControl Basic" nutzt und wenn in der Projektierung des CP die Online-Funktionen aktiviert sind.

Zwischen einer Engineering-Station (PC mit STEP 7) und einer entfernten S7-1200-Station kann eine TeleService-Verbindung über das Mobilfunknetz und das Internet aufgebaut werden.

Die TeleService-Verbindung können Sie für folgende Zwecke nutzen:

- Laden von Projekt- oder Programmdaten aus dem STEP 7-Projekt in die Station
- Abfragen von Diagnosedaten aus der Station

Weitere Informationen finden Sie im Projektierungshandbuch /3/ (Seite 118).

1.3 Kommunikation über SINEMA RC

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 12).

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 /3/ (Seite 118).

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"

1.4 Weitere Dienste und Eigenschaften

Weitere Dienste und Eigenschaften

- **IP-Konfiguration**

  Der CP bekommt vom Mobilfunk-Netzbetreiber eine dynamische oder eine feste IP-Adresse zugewiesen:

  – Dynamische IP-Adresse

    Bei Nutzung der Telecontrol-Kommunikation vergibt der Mobilfunk-Netzbetreiber dem CP in der Regel eine dynamische IP-Adresse. Dies stellen Sie in STEP 7 in der Parametergruppe "Ethernet-Schnittstelle > Ethernet-Adressen" ein.

  – Feste IP-Adresse

    Zur Nutzung der S7-Kommunikation oder zum Empfang von Daten über die Open User Communication muss der CP über eine feste IP-Adresse erreichbar sein. In diesem Fall geben Sie die vom Mobilfunk-Netzbetreiber zugewiesene feste IP-Adresse in der gleichen Parametergruppe ein.

- **Uhrzeitsynchronisation**

  Der CP unterstützt verschiedene Verfahren der Uhrzeitsynchronisation. Informationen finden Sie im Kapitel Uhrzeitsynchronisation (Seite 51).

- **Zugang zum Webserver der CPU**

  Mithilfe des Webservers der CPU können Sie Baugruppendaten aus der Station auslesen.

- **Diagnose-SMS**

  Auf Anforderung durch ein Mobiltelefon sendet der CP eine SMS mit Diagnosedaten an dieses Mobiltelefon.

Weitere Eigenschaften im Telecontrol-Betrieb

- **Datenpunktprojektierung**

  Durch die Datenpunktprojektierung in STEP 7 entfällt das Anlegen von Programmbausteinen zur Übertragung der Prozessdaten. Die einzelnen Datenpunkte werden eins-zu-eins im Leitsystem verarbeitet.

- **Sendepuffer**

  Der CP speichert Werte von Datenpunkten, die als Ereignis projektiert sind, im Sendepuffer.

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

- **Datenübertragung nach Anforderung oder getriggert**

  Die Telecontrol-Kommunikation mit TCSB wird über zwei Wege ausgelöst:

  – Nach Anforderung durch TCSB bzw. einen an TCSB angeschlossenen OPC-Client

  – Getriggert nach verschiedenen einstellbaren Kriterien

  Protokollierung von Statusdaten und deren Übertragung an den Telecontrol-Server

  z. B.:

  – Übertragene Datenvolumina

  – ID der Funkzelle im Bereich der Station

  – GSM-Signalstärke

  – Kommunikationsstatus

  etc.

- **Analogwertvorverarbeitung**

  Analogwerte können im CP nach verschiedenen Methoden vorverarbeitet werden.

1.5 Security-Funktionen

Industrial Ethernet Security - Security-Funktionen des CP

Die nachfolgenden Security-Funktionen sind unabhängig von der Telecontrol-Kommunikation nutzbar.

Mit Industrial Ethernet Security können einzelne Geräte, Automatisierungszellen oder Netzsegmente eines IP-basierten Netzwerks abgesichert werden. Die Datenübertragung über den CP 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 S7-1200-Station zusätzlich folgende Security-Funktionen an der Schnittstelle zum externen Netz zugänglich:

- **Firewall**
  - 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
  - Globale Firewall-Regeln
- **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).
- **Logging**

  Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mit Hilfe des Projektierungswerkzeugs ausgelesen werden oder automatisch an einen Syslog-Server gesendet werden können.
- **STARTTLS / SMTPS**

  Zur sicheren Übertragung von E-Mails
- **NTP (secure)**

  Zur sicheren Übertragung bei der Uhrzeitsynchronisation bei deaktivierter Telecontrol-Kommunikation
- **HTTPS**

  Für den sicheren Zugriff auf den Webserver der CPU

Hinweise zur Projektierung der Security-Funktionen finden Sie im Kapitel Security (Seite 58).

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

Security-Funktionen der Telecontrol-Protokolle

Der CP unterstützt folgende Security-Funktionen:

- **TeleControl Basic**
  - **Verschlüsselte Telecontrol-Kommunikation**

    Als integrierte (nicht projektierbare) Security-Funktion verschlüsselt das Protokoll TeleControl Basic die Daten bei der Übermittlung.

    Das Intervall des Schlüsselaustausches zwischen CP und Telecontrol-Server projektieren Sie in STEP 7 in der Parametergruppe "Ethernet-Schnittstelle (X1) > Erweiterte Optionen > Übertragungseinstellungen".
  - **Autorisierte Rufnummern**

    Zur Autorisierung von Teilnehmern, die einen Verbindungsaufbau des CP veranlassen dürfen (bspw. Mobiltelefone), wird für jeden Teilnehmer eine autorisierte Rufnummer projektiert.
  - **Telecontrol-Passwort**

    Zur Authentifizierung des CP beim Telecontrol-Server
- **DNP3**

  Secure Authentication

1.6 Mengengerüst und Leistungsdaten

Verbindungs-Ressourcen

- **Telecontrol-Verbindungen**
  - DNP3 / IEC

    Der CP kann Verbindungen mit bis zu 4 Kommunikationspartnern aufbauen.

    Als Partner gilt ein einfach oder redundant aufgebauter Master oder eine Station (Direkte Kommunikation).
  - TeleControl Basic

    1 reservierte Verbindung für den Nutzdatenaustausch mit dem Telecontrol-Server

    Zusätzlich Querkommunikation: Die Querkommunikation zwischen den CPs zweier Stationen läuft über den Telecontrol-Server. Sie wird in der Parametergruppe "Partnerstationen" > "Partner für Querkommunikation" projektiert.

    Mengengerüst für Querkommunikation: Insgesamt max. 15, davon:

    - Senden an Partner: Max. 3 (Parameter "Sendepuffer" aktiviert)

    - Empfangen von Partnern: Max. 15 (Parameter "Sendepuffer" deaktiviert)

- **S7-Verbindungen und TCP- / UDP- / ISO-on-TCP-Verbindungen**

  Max. 14 Verbindungs-Ressourcen, beliebig aufteilbar für:

  – S7-Verbindungen (PUT/GET)

    Inklusive Verbindungen für S7-Routing

  – Verbindungen über Programmbausteine (OUC) mit S7-Stationen
- **PG/OP-Verbindungen**
  – 1 Verbindungs-Ressource für PG-Verbindungen
  – 3 Verbindungs-Ressourcen für OP-Verbindungen
- **Online-Funktionen**

  1 Verbindungs-Ressource ist für Online-Funktionen reserviert.
- **TeleService-Verbindungen**
  – Max. 1 TeleService-Verbindung
- **Verbindungen zu NTP-Servern**

  Max. 1 Verbindung zu einem NTP-Server

Nutzdaten

Bei den nachfolgend aufgeführten Verbindungstypen stellen die Nutzdaten eines Telegramms hinsichtlich des Übertragungszeitpunkts einen konsistenten Datenbereich dar.

Nutzdaten pro Telegramm bei den unterschiedlichen Verbindungstypen:

- Bei TCP-Verbindungen: Max. 8192 Byte
- Bei ISO-on-TCP-Verbindungen: Max. 1452 Byte
- Bei UDP-Verbindungen: Max. 1472 Byte

Bei Telegrammen der Telecontrol-Kommunikation sind die einzelnen Werte der Datenpunkte zeitgestempelt.

Anzahl der Datenpunkte für die Datenpunktprojektierung

Die maximale Anzahl der projektierbaren Datenpunkte unter den Telecontrolprotokollen beträgt:

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

Telegrammspeicher (Sendepuffer)

Der CP besitzt einen Telegrammspeicher (Sendepuffer) für die Werte von Datenpunkten, die als Ereignis projektiert sind und an die Kommunikationspartner gesendet werden sollen.

Der Sendepuffer hat folgende maximale Größe:

- TeleControl Basic: 64000 Telegramme
- DNP3: 100000 Ereignisse
- IEC: 100000 Ereignisse

Der Sendepuffer teilt sich auf alle projektierten Kommunikationspartner zu gleichen Teilen auf. Die Größe des Telegrammspeichers ist in STEP 7 einstellbar (Parametergruppe "Kommunikation mit der CPU").

Nachrichten: E-Mail / SMS

Bis zu 10 Nachrichten , die als E-Mail oder SMS versendet werden, können in STEP 7 projektiert werden.

Maximale Anzahl an Zeichen, die pro SMS übertragen werden kann: 160 ASCII-Zeichen inklusive eines evtl. mitgeschickten Werts

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

IPSec-Tunnel (VPN)

Es kann ein IPSec-Tunnel für die gesicherte Kommunikation mit einem weiteren Security-Modul 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

1.7 Voraussetzungen für den Betrieb

Hardware-Voraussetzungen

Für die Nutzung ist an Hardware in der S7-1200 erforderlich:

- CP

  Voraussetzung für die Firmware-Version V3.3 ist ein CP mit Hardware-Erzeugnisstand 2 oder 3.

- Eine CPU

  Die volle Funktionalität des CP steht nur mit einer CPU ab V4.4 zur Verfügung.

- Eine externe Antenne für den CP

  Verwenden Sie die Antenne aus dem Zubehörprogramm für den CP, siehe Anhang Zubehör (Seite 115).

Projektierungs-Software

Für die Nutzung des vollen Funktionsumfangs ist für die Projektierung der Baugruppe das folgende Projektierungswerkzeug erforderlich:

STEP 7 Basic V17

Programmbausteine für Open User Communication und S7-Kommunikation

Für die Open User Communication und die S7-Kommunikation werden Programmbausteine benötigt, siehe Kapitel Kommunikationsdienste (Seite 12).

Voraussetzungen für die Nutzung von Mobilfunkdiensten

- Lokale Verfügbarkeit eines Mobilfunknetzes im Bereich der Station.
- Ein Vertrag mit einem geeigneten Mobilfunk-Netzbetreiber

  Der Vertrag muss die Übermittlung von Daten ermöglichen.

- IP-Adresse:
  - Für die Kommunikation mit dem Telecontrol-Server kann eine vom Mobilfunk-Netzbetreiber vergebene private (feste) oder öffentliche (dynamische) IP-Adresse verwendet werden.
  - Für die direkte Kommunikation zwischen S7-Stationen (S7-Kommunikation) muss der Mobilfunk-Netzbetreiber dem CP eine feste IP-Adresse zuweisen und die Telegramme an die Zielteilnehmer weiterleiten.

  Die Anwendungen, welche eine feste IP-Adresse benötigen, finden Sie im Kapitel Ethernet-Adressen (Seite 50).

- Die zum Mobilfunkvertrag gehörende SIM-Karte mit zugehöriger PIN

  Die SIM-Karte wird in den CP gesteckt.

  Bei Abschluss von Mobilfunkverträgen, bei denen der Netzbetreiber keine PIN vergibt, wird für die Projektierung des CP auch keine PIN benötigt.

- Zugangspunkt (Access Point)

  Für den Übergang zwischen Mobilfunknetz und Internet benötigen Sie einen Zugangspunkt. Der Name des Zugangspunkts (APN) und die Zugangsdaten werden in STEP 7 für den CP projektiert.

  In der Regel stellen die Mobilfunk-Netzbetreiber einen Zugangspunkt zur Verfügung.

  Beachten Sie den Hinweis zu APNs im Kapitel Mobilfunk-Kommunikationseinstellungen (Seite 48).

Voraussetzungen für E-Mail

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

Software für die Telecontrol-Kommunikation und TeleService

Voraussetzung: Die Telecontrol-Kommunikation ist aktiviert.

- Für die Telecontrol-Kommunikation

  Für den Telecontrol-Server in der Zentrale wird die Software "TCSB" (TeleControl Server V3) benötigt.

  Zur Dokumentation der Applikationen siehe /4/ (Seite 118).

- Für TeleService

  Für TeleService können Sie die Applikation SINEMA Remote Connect verwenden.

Weitere Informationen finden Sie in den Projektierungshandbüchern TeleControl Basic, DNP3, IEC 60870-5, siehe /3/ (Seite 118).

1.8 Konfigurationsbeispiele

Im Folgenden finden Sie Konfigurationsbeispiele für Stationen mit CP 1243-7 LTE.

Konfigurationsbeispiele zu Telecontrol-Anwendungen finden Sie in den Projektierungshandbüchern /3/ (Seite 118).

Versenden von SMS und E-Mails

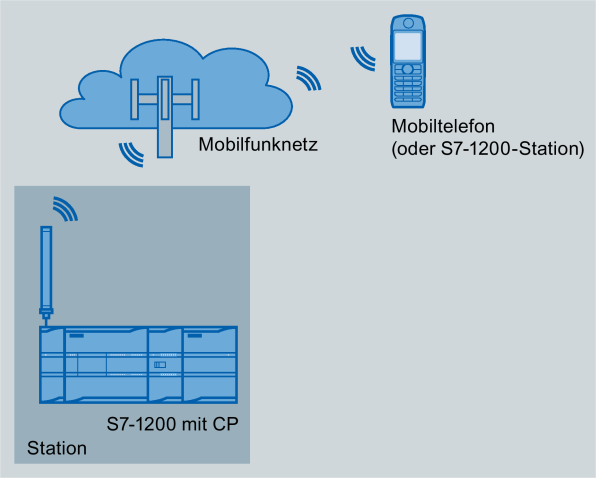


Bild 1-1 SMS-Versand einer S7-1200-Station

SMS

Ein Mobilfunk-CP kann SMS an ein Mobiltelefon oder eine projektierte S7-Station versenden. Hierzu gibt es folgende Mechanismen:

- SMS, die aufgrund eines Ereignisses generiert und versendet werden. Sie werden im Nachrichten-Editor projektiert.
- SMS, die Aufruf der entsprechenden Programmbausteine der Open User Communication gesendet bzw. empfangen werden.

  Siehe hierzu Abschnitt "Direkte Kommunikation zwischen Stationen".
- Durch ein Mobiltelefon kann eine Diagnose-SMS angefordert werden, siehe Kapitel Diagnosemöglichkeiten (Seite 93).

  Für alle Mobiltelefone, welche SMS an den CP senden, muss in der STEP 7-Projektierung des CP die autorisierte Rufnummer angegeben werden (Parametergruppe "Security > Autorisierte Rufnummer").

E-Mails

Der CP kann E-Mails an einen PC mit Internetanschluss oder ein Mobiltelefon versenden. Hierzu gibt es folgende Mechanismen:

- E-Mails, die aufgrund eines Ereignisses generiert und versendet werden. Sie werden im Nachrichten-Editor projektiert.
- E-Mails, die durch Aufruf des Programmbausteins TMAIL_C gesendet werden.

Für die gesicherte Übertragung von E-Mail muss der CP die aktuelle Uhrzeit haben.

Direkte Kommunikation zwischen Stationen

Direkte Kommunikation zwischen S7-Stationen wird über die Programmbausteine der Open User Communication (OUC) ermöglicht

In dieser Konfiguration kommunizieren zwei SIMATIC S7-1200-Stationen mithilfe des CP über das Mobilfunknetz direkt miteinander. Jeder CP hat eine feste IP-Adresse. Der entsprechende Dienst des Netzbetreibers muss dies ermöglichen.

Für alle Mobiltelefone, welche SMS an den CP senden, muss in der STEP 7-Projektierung des CP die autorisierte Rufnummer angegeben werden (Parametergruppe "Security > Autorisierte Rufnummer").

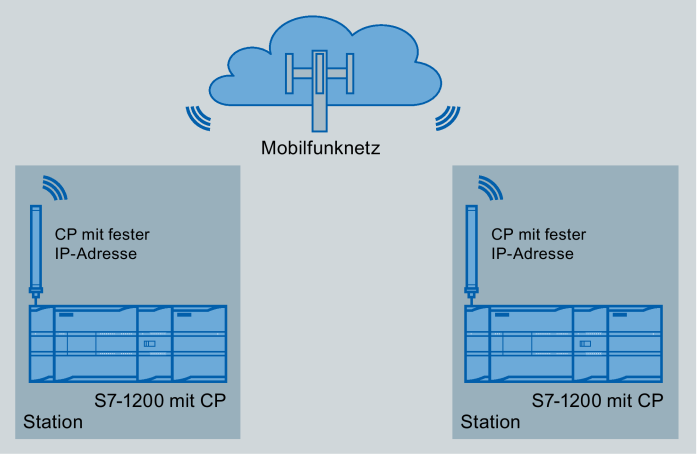


Bild 1-2 Direkte Kommunikation von zwei S7-1200-Stationen

Fernwartung mit SINEMA RC

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

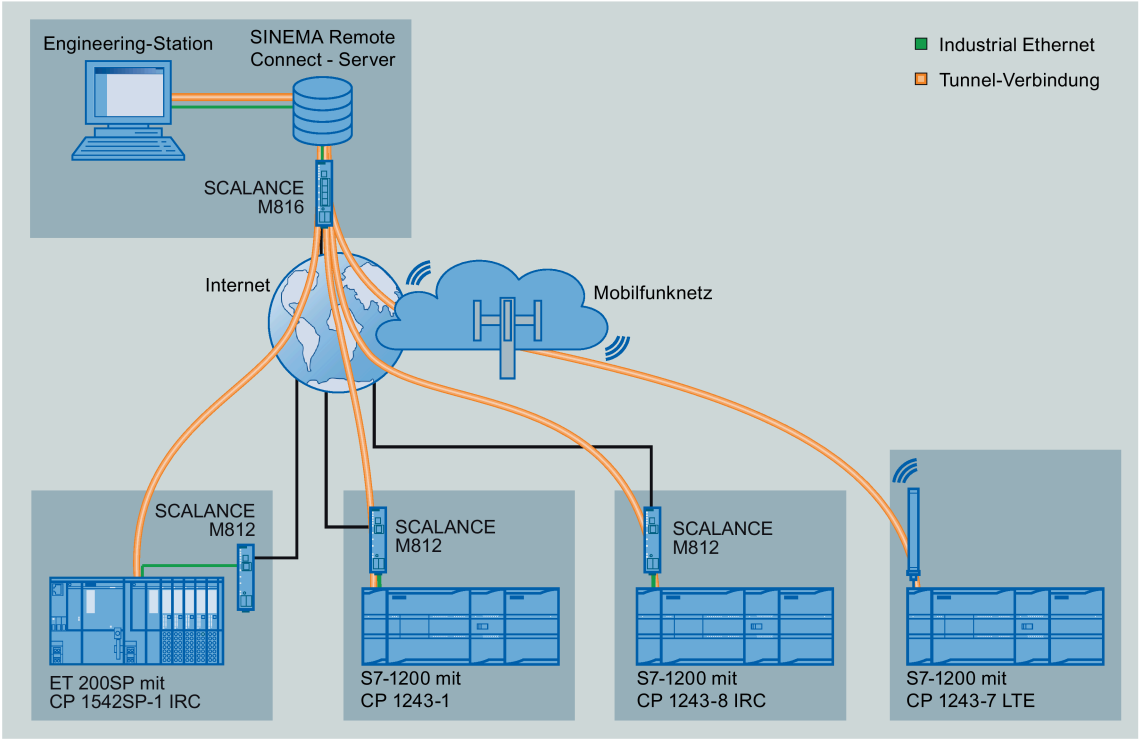


Bild 1-3 Anbindung von Stationen an Engineering-Station über SINEMA RC

LEDs und Anschlüsse

2

2.1 Öffnen der Gehäuseabdeckungen

Lage der Anzeigeelemente und der elektrischen Anschlüsse

Die LEDs für die detaillierte Anzeige der Baugruppenzustände befinden sich hinter der oberen Gehäuseklappe der Baugruppe.

Die Buchse für die Spannungsversorgung befindet sich auf der Oberseite der Baugruppe.

Der Anschluss für die externe Antenne befindet sich auf der Unterseite der Baugruppe.

Der Schacht zum Einlegen der SIM-Karte befindet sich hinter der unteren Gehäuseklappe der Baugruppe.

Öffnen der Gehäuseabdeckungen

Öffnen Sie die obere bzw. untere Gehäuseklappe, indem Sie diese wie in der Abbildung nach unten bzw. oben drehen. Die Gehäuseklappen sind hierfür zu einem Griff verlängert.

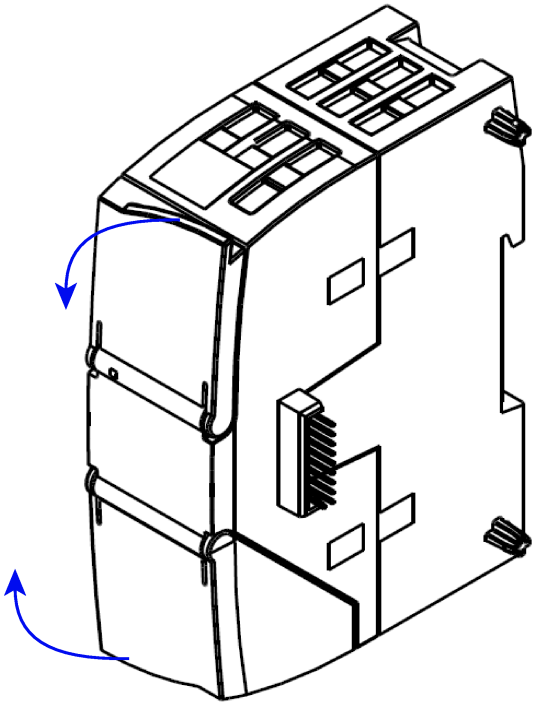


Bild 2-1 Öffnen der Gehäuseabdeckungen

2.2 LEDs

LEDs der Baugruppe

Der CP besitzt folgende LEDs zur Zustandsanzeige:

- LED "DIAG" auf der Frontplatte

  Die immer sichtbare LED "DIAG" zeigt die Grundzustände der Baugruppe an.

- LEDs unter der oberen Gehäuseklappe

  Diese LEDs zeigen weitere Details zum Zustand der Baugruppe an.

Tabelle 2- 1 LED auf der Frontplatte

LED / Farben	Bezeichnung	Bedeutung
rot / grün	DIAG	Grundzustand der Baugruppe

Tabelle 2- 2 LEDs unter der oberen Gehäuseklappe

LED / Farben	Bezeichnung	Bedeutung
rot / grün	NETWORK	Zustand der Verbindung mit dem Mobilfunknetz
grün	CONNECT	Zustand der Verbindung mit der Zentrale
gelb / grün	SIGNAL QUALITY	Signalqualität des Mobilfunknetzes
grün	VPN	Zustand der VPN- bzw. SINEMA Remote Connect-Projektierung

Hinweis

LED-Farben beim Anlauf der Baugruppe

Beim Anlauf der Baugruppe leuchten alle LEDs für kurze Zeit auf. Mehrfarbige LEDs zeigen dabei eine Mischfarbe. In diesem Moment ist die Farbe der LEDs nicht eindeutig.

Anzeige des Betriebs- und Kommunikationszustands

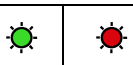
Die LED-Symbole in den nachfolgenden Tabellen haben folgende Bedeutung:

Tabelle 2- 3 Bedeutung der LED-Symbole

Symbol	○	● ● ●	☼ ☼ ☼	-
LED-Zustand	AUS	EIN (Ruhelicht)	Blinkend	Nicht relevant

Die LEDs zeigen nach folgenden Schemata den Betriebs- und Kommunikationszustand der Baugruppe an:

DIAG (rot / grün)	**NETWORK** (rot / grün)	**CONNECT** (grün)	**SIGNAL QUALITY** (gelb / grün)	**VPN** (grün)	**Bedeutung**
Anzeige der Grundzustände der Baugruppe					
○	○	○	○	○	Spannung AUS
● rot	●	●	●	●	Anlauf
☼ rot blinkend	-	○	-	-	Fehler: • Ungültige CP-Projektierung oder • CP-Typ passt nicht zu den Projektierungsdaten in der CPU.
● grün	-	-	-	-	Laufend (RUN) ohne Fehler
☼ rot blinkend	-	☼	-	-	Rückwandbusfehler
☼ rot blinkend	●	-	-	-	Fehlende SIM-Karte
☼ rot blinkend	☼	-	-	-	Fehlende oder falsche PIN
Verbindung mit dem Mobilfunknetz					
-	●	-	-	-	Bestehende Verbindung zum Dienst im Mobilfunknetz
-	○	-	-	-	Keine Verbindung zum Dienst im Mobilfunknetz
Verbindung zu Kommunikationspartnern					
● grün	●	●	-	-	Verbindung zu mindestens einem Partner aufgebaut, CPU in RUN
● grün	●	☼	-	-	Verbindung zu mindestens einem Partner aufgebaut, CPU in STOP
☼ grün blinkend	●	●	-	-	Kein Partner erreichbar, CPU in RUN
☼ grün blinkend	●	☼	-	-	Kein Partner erreichbar, CPU in STOP
☼ grün blinkend	○	●	-	-	Telecontrol-Projektierung vorhanden, Partner nicht erreichbar, CPU in RUN
☼ grün blinkend	○	☼	-	-	Telecontrol-Projektierung vorhanden, Partner nicht erreichbar, CPU in STOP

DIAG (rot / grün)	**NETWORK** (rot / grün)	**CONNECT** (grün)	**SIGNAL QUALITY** (gelb / grün)	**VPN** (grün)	**Bedeutung**
Qualität der Mobilfunkverbindung					
-	-	-		-	Gutes Netz (-73 ... ≥ -51 dBm)
-	-	-		-	Mittelstarkes Netz (-89 ... -74 dBm)
-	-	-		-	Schwaches Netz (-109 ... -90 dBm)
-	-	-		-	Kein Netz (≤ -110 dBm)
 rot blinkend	-	-		-	Fehlende externe Spannungsversorgung
VPN- / SINEMA Remote Connect-Verbindung					
-		-	-		VPN- / SINEMA Remote Connect-Verbindung aufgebaut
-		-	-		Aufbauversuch einer projektierten VPN- / SINEMA Remote Connect-Verbindung
-	-	-	-		Keine VPN- / SINEMA Remote Connect-Verbindung im CP projektiert oder momentan nicht aufgebaut
Firmware laden					
					Firmware wird geladen. Die LED "DIAG" blinkt abwechselnd rot und grün.
 grün blinkend					Firmware wurde erfolgreich geladen.
 rot blinkend					• Fehler beim Laden der Firmware oder • Interner Fehler des CP; Abhilfe: Spannung AUS → EIN

2.3 Elektrische Anschlüsse

2.3.1 Spannungsversorgung

Spannungsversorgung

Die 3-polige Buchse für die externe Spannungsversorgung DC 24 V befindet sich auf der Oberseite der Baugruppe. Der passende Stecker ist Teil des Lieferumfangs.

Die Pin-Belegung der Buchse finden Sie im Kapitel Belegung der Buchse für die externe Spannungsversorgung (Seite 104).

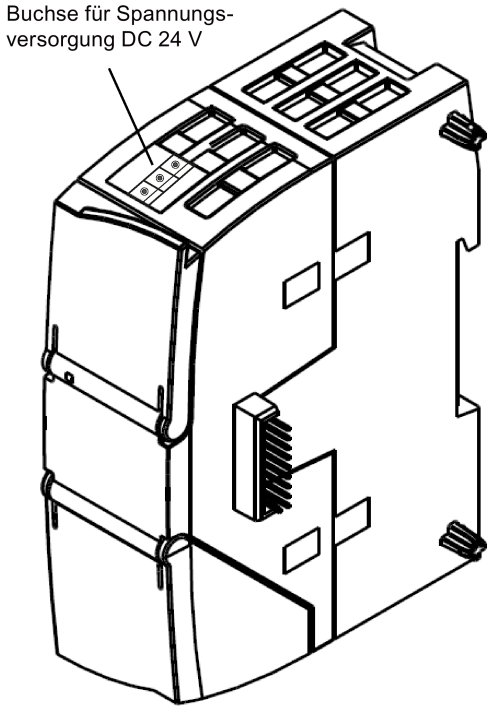


Bild 2-2 Anschlussbuchse für die Spannungsversorgung DC 24 V

2.3.2 Funkschnittstelle

Funkschnittstelle für das Mobilfunknetz

Für die Kommunikation im Mobilfunknetz ist eine externe Antenne erforderlich. Diese wird über die SMA-Buchse des CP angeschlossen. Die SMA-Buchse befindet sich hinter der unteren Frontklappe des CP.

Die zugelassene Antenne finden Sie im Kapitel Zubehör (Seite 115).

Weitere Informationen zu den elektrischen Anschlüssen

Technische Details zu den elektrischen Anschlüssen finden Sie im Kapitel Technische Daten (Seite 101).

Montage, Anschluss, Inbetriebnahme 3

3.1 Wichtige Hinweise zum Geräteeinsatz

Sicherheitshinweise für den Geräteeinsatz

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

Überspannungsschutz

ACHTUNG
Schutz der externen Spannungsversorgung 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

⚠ **WARNUNG**
EXPLOSIONSGEFAHR ÖFFNEN SIE DAS GERÄT NICHT BEI EINGESCHALTETER VERSORGUNGSSPANNUNG.

⚠WARNUNG

Das Gerät darf nur in einer Umgebung der Verschmutzungsklasse 1 oder 2 betrieben werden (vgl. IEC60664-1).

⚠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.

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

⚠ WARNUNG

Anforderungen an den Schaltschrank

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.

⚠ WARNUNG

Kabel

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.

⚠ WARNUNG

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

⚠ WARNUNG

EXPLOSIONSGEFAHR

Trennen Sie das Gerät nicht von spannungsführenden Leitungen, solange nicht sichergestellt ist, dass in der Umgebung keine explosionsgefährdete Atmosphäre vorherrscht.

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.

3.2 Montieren, anschließen und in Betrieb nehmen

Vor der Montage und Inbetriebnahme

⚠ WARNUNG

Lesen Sie das Systemhandbuch "S7-1200 Automatisierungssystem"

Lesen Sie vor der Montage, dem Anschließen und der Inbetriebnahme die entsprechenden Abschnitte im Systemhandbuch "S7-1200 Automatisierungssystem", siehe Literaturverweis im Anhang.

Gehen Sie bei der Montage und dem Anschließen entsprechend den Beschreibungen im Systemhandbuch "S7-1200 Automatisierungssystem" vor.

Projektierung

Voraussetzung für die komplette Inbetriebnahme des CP ist die Vollständigkeit der STEP 7-Projektdaten (siehe unten). Lesen Sie hierzu das Kapitel Projektierung (Seite 41).

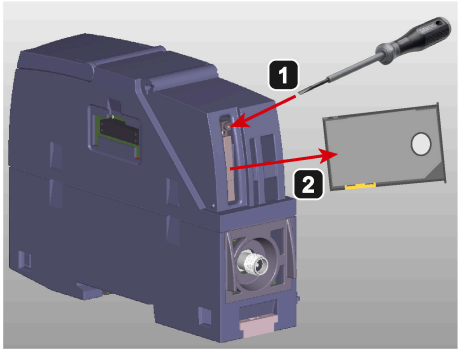
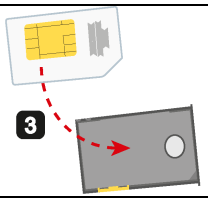
Einlegen der SIM-Karte

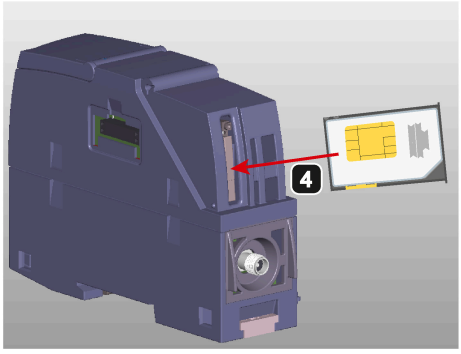
Hinweis

Stecken und ziehen der SIM-Karte

Stecken oder ziehen Sie die SIM-Karte nicht während des laufenden Betriebs des CP.

Legen Sie vor der Montage die SIM-Karte in den CP ein.

Schritt	Ausführung	Hinweise und Erläuterungen
1	Schalten Sie die Spannungsversorgung der Station aus.	
2	Entriegeln Sie den Schlitten für die SIM-Karte an der Unterseite des CP hinter der unteren Gehäuseklappe durch leichten Druck auf den Entriegelungsstift.	
3	Ziehen Sie den Schlitten aus dem Gehäuse.	
4	Legen Sie die SIM-Karte wie abgebildet in den Schlitten.	

Schritt	Ausführung	Hinweise und Erläuterungen
5	Schieben Sie den Schlitten wieder in das Gehäuse, bis er leicht einrastet.	
6	Schalten Sie die Spannungsversorgung der Station ein.	

Abmessungen für die Montage

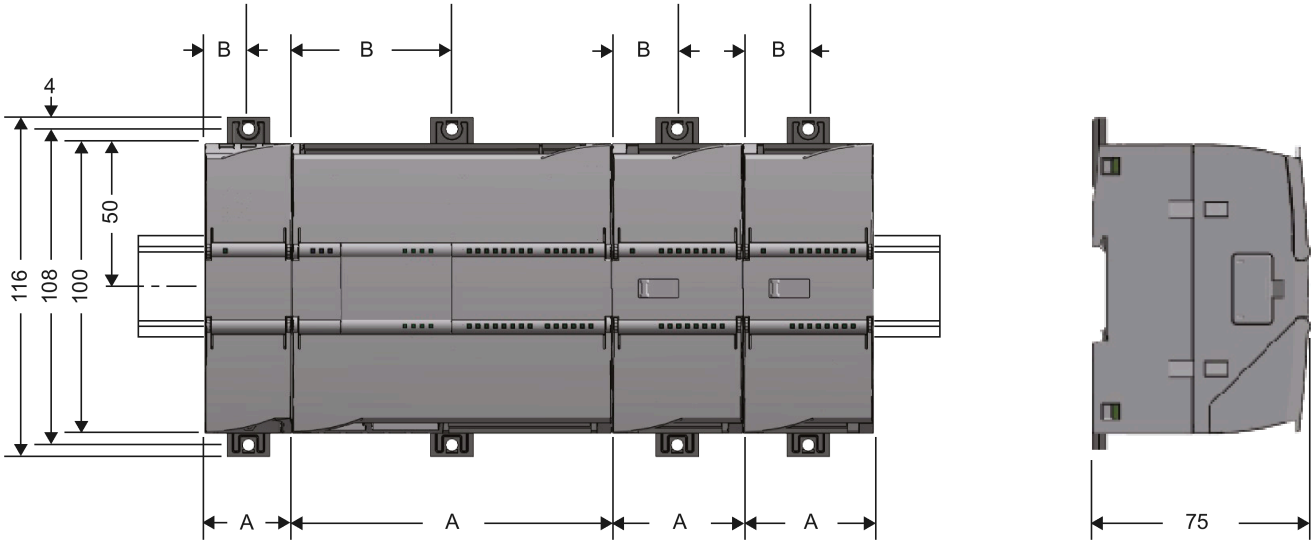


Bild 3-1 Einbaumaße der S7-1200

Tabelle 3- 1 Abmessungen für die Montage (mm)

S7-1200-Geräte		Breite A	Breite B *
CPU (Beispiele)	CPU 1211C, CPU 1212C	90 mm	45 mm
	CPU 1214C	110 mm	55 mm
Signalmodule (Beispiele)	8 oder 16 digitale E/A 2, 4 oder 8 analoge E/A Thermoelement, 4 oder 8 E/A RTD, 4 E/A	45 mm	22,5 mm
	16 analoge E/A RTD, 8 E/A	70 mm	35 mm
Kommunikations-Schnittstellen (Beispiele)	CM 1241 RS232 / CM 1241 RS485	30 mm	15 mm
	CM 1243-5 (PROFIBUS-Master) CM 1242-5 (PROFIBUS-Slave)	30 mm	15 mm
	CP 124x-7	30 mm	15 mm

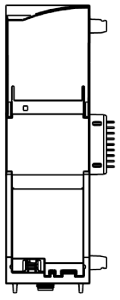
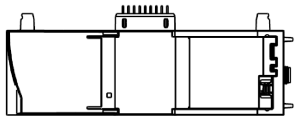
* Breite B: Maß zwischen Gehäusekante und Mitte der Bohrung der Hutschienenklemme

Hutschienenklemmen

Alle CPUs, SMs, CMs und CPs können auf der DIN-Hutschiene im Schaltschrank montiert werden. Verwenden Sie die herausziehbaren Hutschienenklemmen für die Befestigung des Geräts auf der Hutschiene. Diese Klemmen rasten auch in herausgezogener Position ein, um den Einbau des Geräts in einer Schalttafel zu ermöglichen. Das Innenmaß der Bohrung der Hutschienenklemmen beträgt 4,3 mm.

Vorgehensweise zur Montage und Inbetriebnahme

ACHTUNG
Einbaulage Die Montage muss so erfolgen, dass die oberen und unteren Lüftungsschlitze der Baugruppe nicht verdeckt werden und eine gute Durchlüftung möglich ist. Ober- und unterhalb des Geräts 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. Die zulässigen Temperaturbereiche finden Sie im Kapitel Allgemeine technische Daten (Seite 101).

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

Hinweis

Anschluss im spannungslosen Zustand

Verdrahten Sie die S7-1200 nur im spannungslosen Zustand.

Hinweis

Spannungsversorgung aus den Spannungsausgängen der CPU

Die externe Spannungsversorgung des CP muss aus den Spannungsausgängen der CPU gespeist werden.

Beachten Sie die maximale Belastbarkeit der Spannungsausgänge der CPU.

Daten zur Stromaufnahme und Verlustwirkleistung des CP finden Sie im Kapitel Allgemeine technische Daten (Seite 101).

Hinweis

Ausschalten der Station bei Ziehen/Stecken des CP

Trennen Sie nicht alleine die Versorgungsspannung des CP. Schalten Sie immer die Versorgungsspannung der ganzen Station aus.

Tabelle 3- 2 Vorgehensweise zu Montage und Anschluss

Schritt	Ausführung	Hinweise und Erläuterungen
1	Stecken Sie den CP auf die Hutschiene und verbinden Sie ihn mit der benachbarten Baugruppe rechts davon.	Verwenden Sie eine 35 mm DIN Hutschiene. Zulässig sind die Steckplätze links neben der CPU.
2	Befestigen Sie die Hutschiene.	
3	Befestigen Sie die Leitungen der Spannungsversorgung an dem Spannungsausgang der CPU.	
4	Befestigen Sie die Leitungen der Spannungsversorgung an dem mit dem CP mitgelieferten Stecker und stecken Sie den Stecker in die Buchse auf der Oberseite des CP.	Die Belegung ist neben der Buchse auf der Gehäuseoberseite aufgedruckt. Sie finden Sie auch im Kapitel Belegung der Buchse für die externe Spannungsversorgung (Seite 104).
5	Schließen Sie die Antenne an der SMA-Buchse des CP.	Unterseite des CP
	Achtung • Sichern Sie den Antennenanschluss mit einer geeigneten Überspannungsschutzvorrichtung ab, wenn das Antennenkabel länger als 30 m ist. • Sichern Sie den Antennenanschluss mit einem geeigneten Blitzschutz ab, wenn Sie die Antenne im Außenbereich installieren. • Wenn Sie mehrere CPs in räumlicher Nähe installieren, dann halten Sie zwischen den Antennen einen Mindestabstand von 50 cm.	
6	Schalten Sie die Spannungsversorgung ein.	
7	Schließen Sie die Frontklappen der Baugruppe und halten Sie diese während des Betriebs geschlossen.	
8	Die weitere Inbetriebnahme umfasst das Laden der STEP 7-Projektdaten.	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 Ethernet-Schnittstelle der CPU an. Weitere Details zum Laden entnehmen Sie folgenden Kapiteln der Online-Hilfe von STEP 7: • "Projektdaten laden" • "Online- und Diagnosefunktionen nutzen"

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" projektiert 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.

3.3 Hinweise zum Betrieb

⚠ VORSICHT

Mindestabstand zum Gerät

Das Gerät darf nur betrieben werden, wenn der Abstand zwischen Gerät (bzw. Antenne) und Benutzer mindestens 20 cm beträgt.

ACHTUNG

Schließen der Frontklappen

Halten Sie zur Sicherstellung eines störungsfreien Betriebs die Frontklappen der Baugruppe während des Betriebs geschlossen.

Projektierung

4

4.1 Security-Empfehlungen

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

Beachten Sie bei aktivierter Telecontrol-Kommunikation auch die Hinweise im Projektierungshandbuch.

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 Zellenschutzkonzept 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 folgender Adresse:
  Link: (https://support.industry.siemens.com/cs/ww/de/ps/15924/dl)

Physikalischer Zugang

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

APNs von Mobilfunk-Netzbetreibern

Wenn Sie für den Mobilfunk-CP einen APN des Netzbetreibers projektieren, dann kann es - abhängig vom verwendeten APN - sein, dass der CP öffentlich im Internet erreichbar ist.

Beachten Sie dieses Sicherheitsrisiko bei der Auswahl des APN.

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.
- Security-Funktion der Kommunikation
  - Aktivieren Sie die Security-Funktionen des CP.
  - Verwenden Sie die sichere Open User Communication über die entsprechenden Programmbausteine.
  - Deaktivieren Sie den Zugriff auf den Webserver der CPU (CPU-Projektierung) und auf den CP.
- Schutz der Passwörter von Programmbausteinen

  Schützen Sie Passwörter, die für Programmbausteine in Datenbausteinen abgelegt werden, vor Einsicht. Die Vorgehensweise ist im STEP 7-Informationssystem beschrieben.

  Wenn Sie in einem DB nachträglich Parameter, bspw. ein Passwort; verändern möchten, dann beachten Sie folgendes: Die Inhalte eines DB mit Know-How-Schutz sind nicht mehr sichtbar und nur noch über die Quelle oder über die direkte Zuweisung von Parametern veränderbar.
- 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.
- **Authentifizierung**

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

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	2404 (TCP) einstellbar	Geschlossen	Offen	Nein
S7- und Online-Verbindungen	102 (TCP)	Geschlossen	Offen nach Konfiguration *	Nein

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
Kommunikation über SINEMA RC	443 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
HTTP	80 (TCP)	Geschlossen	Offen nach Konfiguration	Nein
HTTPS	443 (TCP)	Geschlossen	Offen nach Konfiguration	Ja

***** Manche Dienstbetreiber beanstanden das Öffnen von Port 102 als Sicherheitslücke. Zur Vermeidung des Öffnens von Port 102 bei der Online-Diagnose siehe Kapitel Online-Security-Diagnose über Port 8448 (Seite 96).

Ports von Kommunikationspartnern und Routern

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

Dies können sein:

- TeleControl Basic / 55097 (TCP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- SINEMA RC Autokonfiguration / 443 (TCP) - einstellbar
- SINEMA RC und OpenVPN / 1194 (UDP) - einstellbar in SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)

4.2 Projektierung in STEP 7

Projektierung in STEP 7

Die Projektierung der Baugruppen, Netze und Verbindungen führen Sie an einer Engineering-Station in SIMATIC STEP 7 durch. Die erforderliche Version finden Sie im Kapitel Voraussetzungen für den Betrieb (Seite 22).

Sie können maximal drei CMs/CPs pro Station projektieren. Wenn Sie mehrere CPs in einer S7-1200 stecken, lassen sich beispielsweise redundante Kommunikationspfade aufbauen.

Die nachfolgende Beschreibung gilt für Anwendungsfälle ohne Telecontrol-Kommunikation.

Projektierung der Telecontrol-Kommunikation

Die Beschreibung zur Projektierung der Telecontrol-Kommunikation finden Sie im Projektierungshandbuch /3/ (Seite 118).

Übersicht der Projektierungsschritte in STEP 7

Hinweise:

- Für die Kommunikation über das Mobilfunknetz muss kein Ethernet-Netz angelegt werden.
- Bei Aktivierung der Security-Funktionen müssen Sie ein Netz anlegen und die Schnittstelle zumindest vernetzen, damit der Projektierungsdaten übersetzt werden können.

Gehen Sie bei der Projektierung folgendermaßen vor:

1. Legen Sie ein STEP 7-Projekt an.
2. Legen Sie die erforderlichen SIMATIC-Stationen mit den erforderlichen Modulen und CPs an.
3. Projektieren Sie die CPs inklusive der Nachrichten (E-Mail / SMS).
4. Legen Sie - falls gewünscht - die Programmbausteine für die S7-Kommunikation und die Open User Communication an und parametrieren Sie diese.
5. Speichern und übersetzen Sie das Projekt.
6. Laden Sie die Projektdaten in die Stationen

   Über die Funktion "Laden in Gerät" werden die STEP 7-Projektdaten inklusive der Projektierungsdaten der CPs in die jeweilige CPU geladen.

Weitere Informationen zu den einzelnen Schritten finden Sie in den nachfolgenden Kapiteln und im Hilfesystem von STEP 7.

Benötigte Informationen für die Projektierung

Benötigte Informationen für die Telecontrol-Kommunikation

Die Informationen, die Sie für diesen Anwendungsfall benötigen, finden Sie im Projektierungshandbuch /3/ (Seite 118).

Benötigte Informationen für die Mobilfunk-Kommunikation

Folgende Informationen werden für die Projektierung eines Mobilfunk-CP benötigt, welcher E-Mail und SMS nutzt, aber keine Telecontrol-Kommunikation:

- Eigene Rufnummer des CP
- APN

  Name des Zugangspunkts (APN) vom Mobilfunknetz zum Internet

  (Information vom Mobilfunk-Netzbetreiber)
- APN-Benutzername

  Benutzername für den Zugangspunkt des Mobilfunk-Netzwerkbetreibers
- APN-Passwort

  Passwort für den Zugangspunkt des Mobilfunk-Netzwerkbetreibers
- Teilnehmernummer der SMS-Zentrale (SMSC) - bei Nutzung von SMS
- PIN der SIM-Karte

Hinweis

Projektierte PIN und PIN auf der SIM-Karte müssen übereinstimmen.

Wenn Sie die PIN der SIM-Karte des CP bei der STEP 7-Projektierung des CP falsch eingeben und die Station laden, dann speichert der CP die falsche PIN. Eine falsch eingegebene PIN wird vom CP nur einmal übergeben, damit die SIM-Karte nicht gesperrt wird.

Wenn Sie die PIN der SIM-Karte extern in die falsch projektierte PIN ändern (neue PIN der SIM-Karte = zuvor in STEP 7 falsch projektierte PIN), dann lehnt der CP diese PIN erneut ohne Prüfung ab.

Hinweis

Abhilfe nach Eingabe einer falschen PIN:

Um eine weitere Ablehnung der PIN durch den CP zu beheben, müssen Sie eine PIN verwenden, die ungleich der falsch eingegebenen PIN ist. Vorgehensweise:

- Wenn die PIN der SIM-Karte nicht geändert wurde:
  - Projektieren Sie die PIN in STEP 7 mit der PIN der SIM-Karte.
  - Laden Sie die Station erneut.
- Wenn die ursprüngliche PIN der SIM-Karte extern in diejenige PIN geändert wurde, die zuvor falsch in STEP 7 projektiert wurde:
  - Ändern Sie extern die PIN der SIM-Karte in eine neue PIN, die in STEP 7 noch nicht falsch projektiert wurde.
  - Ändern Sie die projektierte PIN im STEP 7-Projekt in die neu vergebene PIN der SIM-Karte.
  - Laden Sie die Station erneut.

4.3 Kommunikationsarten

In dieser Parametergruppe aktivieren Sie die Kommunikationsarten des CP.

Um das Risiko unerlaubter Zugriffe über den CP auf die Station zu minimieren, müssen Sie die Kommunikationsdienste, die der CP durchführen soll, einzeln aktivieren. Sie können alle Optionen aktivieren, es sollte aber mindestens eine Option aktiviert sein.

Parametergruppe "Kommunikationsarten"

- **Telecontrol-Kommunikation aktivieren**

  Gibt im CP die Telecontrol-Kommunikation frei.

  Über die Klappliste "Protokolltyp" wählen Sie das Telecontrol-Protokoll aus.

  - TeleControl Basic
  - DNP3
  - IEC 60870-5

Beachten Sie, dass bei einer nachträglichen Änderung des Telecontrol-Protokolls alle protokollspezifischen Daten gelöscht werden. Dazu gehören unter anderem die Datenpunkt- und Partner-Informationen.

Weitere Informationen finden Sie in den Projektierungshandbüchern /3/ (Seite 118).

- **Telecontrol-Kommunikation über SINEMA Remote Connect aktivieren**

  Gibt im CP die Kommunikation über SINEMA RS frei.

  Die Anwendungsfälle von SINEMA Remote Connect und Projektierungshinweise zu diesen Anwendungen finden Sie im Kapitel Kommunikation über SINEMA RC (Seite 15).

  Weitere Informationen finden Sie in den Projektierungshandbüchern /3/ (Seite 118).

  Zum Handbuch SINEMA Remote Connect - Server siehe /5/ (Seite 118).

- **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 zur CPU aktivieren**

  Gibt die Funktionen der S7-Kommunikation zwischen Engineering-Station und Stations-CPU sowie das S7-Routing frei.

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

  Beachten Sie:
  Die Deaktivierung der Funktion bedeutet keine Security-Maßnahme. Verwenden Sie zum Schutz der Station geeignete Security-Funktionen wie Firewall, VPN oder den Passwort-Schutz der CPU.

- **SMS aktivieren**

  Gibt das Empfangen und Versenden von SMS frei.

  Die Funktion ist unabhängig von der Aktivierung der Telecontrol-Kommunikation aktivierbar.

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 Mobilfunk-Kommunikationseinstellungen

"Mobilfunk-Einstellungen"

In dieser Parametergruppe projektieren Sie folgende Parameter:

- **CP-Rufnummer**

  Telefonnummer des CP

- **PIN aktivieren**

  Wenn Ihr Dienstbetreiber eine PIN verlangt, dann aktivieren Sie diese Option.

- **PIN**

  PIN der SIM-Karte

- **Datendienste aktivieren**

  Aktiviert für den CP die Nutzung von Datendiensten im Mobilfunknetz.

  Hinweis
  Nachträgliche Deaktivierung

  Wenn Sie Datendienste bereits im Betrieb genutzt haben und diese nachträglich deaktivieren, dann müssen Sie die Projektierungsdaten neu laden und die CPU in STOP und anschließend wieder in RUN setzen.

- **GPRS (2G) / UMTS (3G) / LTE**

  Aktivieren Sie den oder diejenigen Mobilfunkdienste, die Sie nutzen möchten. Sie können einzelne Mobilfunkdienste freischalten oder alle.

  "GPRS (2G)" wird nur vom CP 1243-7 LTE EU unterstützt.

- **SMSC**

  Telefonnummer der SMS-Zentrale (Short Message Service Center)

  Das Feld hat folgende Optionen:

  – Keine Nummer

    In der Voreinstellung übernimmt der CP die SMSC-Daten des Dienstbetreibers direkt von der gesteckten SIM-Karte. Wenn Sie die SMSC-Nummer der SIM-Karte nutzen möchten, dann lassen Sie das Feld frei.

  – Projektierte Nummer

    Wenn Sie ein anderes SMSC nutzen möchten, dann geben Sie die Telefonnummer dieses SMSC ein.

    Beachten Sie Folgendes:

Hinweis

Feste Speicherung der SMSC-Nummer

Wenn Sie eine SMSC-Nummer projektieren, dann greift der CP nicht mehr auf die SMSC-Daten der SIM-Karte zurück. Dies gilt auch dann, wenn Sie die SMSC-Nummer wieder aus der Projektierung löschen.

Empfehlung:
Wenn Sie eine SMSC-Nummer projektieren, dann notieren Sie sich vorher die SMSC-Nummer Ihres Dienstbetreibers, die sich auch auf der SIM-Karte befindet. Sie können dann das SMSC Ihres Betreibers später, wenn Sie dieses nutzen möchten, wiederverwenden, indem Sie die SMSC-Nummer projektieren.

"APN-Einstellungen"

In dieser Parametergruppe projektieren Sie die Daten des Zugangspunkts. Den APN benötigen Sie für das Versenden von E-Mails.

Der CP unterstützt APNs mit IPv4- und IPv6-Adresse.

Beachten Sie den Sicherheitshinweis im Kapitel Security-Empfehlungen (Seite 41).

Über die Eingabe Ihres Landes im Feld "Land" können Sie einen der vorbelegten APNs aus der Klappliste auswählen.

Alternativ projektieren Sie den APN manuell.

Hinweis

Projektierung von APN-Benutzername und Passwort

Wenn Ihr Dienstbetreiber einen APN-Benutzernamen und ein Passwort verlangt, erhalten Sie diese Informationen von ihm.

Wenn Ihr Dienstbetreiber keinen APN-Benutzernamen und kein Passwort verlangt, kann es erforderlich sein, Platzhalter für die beiden Parameter zu projektieren. Dies ist beispielsweise der Fall, wenn Ihr Betreiber das Provider Password Authentication Protocol (PAP) zur Authentifizierung verwendet. Erkundigen Sie sich in diesem Fall bei Ihrem Betreiber nach den erforderlichen Angaben.

Benutzernamen und Passwörter können bis zu 64 Zeichen enthalten. Die zugelassenen Zeichen finden Sie im Kapitel Zeichensatz für Passwörter und Nachrichten (Seite 78).

Wenn Ihr Dienstbetreiber keinen APN-Benutzernamen und kein Passwort verlangt, kann es in manchen Fällen dennoch sinnvoll sein, Platzhalter für die beiden Parameter einzugeben.

"Liste der bevorzugten Netzwerke"

In dieser Parametergruppe legen Sie das Einwahlverhalten des CP in verschiedene Mobilfunknetze fest.

"TeleService-Einstellungen"

TeleService ist nur bei aktivierter Telecontrol-Kommunikation nutzbar. Die Beschreibung der TeleService-Funktionen finden Sie im Projektierungshandbuch, siehe /3/ (Seite 118).

4.5 Ethernet-Schnittstelle [X1]

4.5.1 Ethernet-Adressen

Die Ethernet-Schnittstelle bei Mobilfunk-CPs

Mobilfunk-CPs haben keine physische Ethernet-Schnittstelle.

In STEP 7 wird die Ethernet-Schnittstelle als Platzhalter für die Projektierung verschiedener Adress- und Überwachungs-Parameter verwendet.

Ethernet-Adressen

Hier projektieren Sie die IP-Adresse des CP und den Netzanschluss.

Wenn Sie die Security-Funktionen aktivieren, beispielsweise bei Nutzung der Telecontrol-Kommunikation, dann müssen Sie den CP aus Konsistenzgründen vernetzen. Legen Sie hierzu ein beliebiges Ethernet-Netz an.

IP-Protokoll

- **Dynamische IP-Adresse**

  Aktivieren Sie diese Option, wenn der CP die IP-Adresse vom Netzbetreiber dynamisch zugewiesen bekommt.

- **Feste IP-Adresse vom Mobilfunk-Netzbetreiber**

  Aktivieren Sie diese Option, wenn Sie einen Mobilfunkvertrag haben, bei dem der Netzbetreiber dem CP eine feste IP-Adresse zuweist.

  Beachten Sie:
  Für folgende Anwendungen ist eine feste IP-Adresse (IPv4/IPv6) erforderlich:

  – Bei Nutzung von S7-Kommunikation
  – Bei Empfang von Daten über die Open User Communication
  – Bei Nutzung von VPN
  – Bei Nutzung von SINEMA Remote Connect

- **IPv6-Protokoll verwenden**

  Zusätzlich zu IPv4 können Sie optional IPv6 für den CP aktivieren.

  IPv6 wird ab Hardware-Erzeugnisstand 3 des CP unterstützt.

4.5.2 Erweiterte Optionen

TCP-Verbindungsüberwachung

Die hier vorgenommenen Einstellungen gelten global für alle projektierten TCP-Verbindungen des CP.

- **TCP-Verbindungs-Überwachungszeit**

  Funktion: Wenn innerhalb der TCP-Verbindungs-Überwachungszeit kein Datenverkehr stattfindet, sendet das Kommunikationsmodul ein Keep-alive-Telegramm an den Kommunikationspartner und erwartet dessen Antwort innerhalb der TCP-Keep-alive-Überwachungszeit.

  Voreinstellung: 180 s. Zulässiger Bereich: 1...65535 s

- **TCP-Keep-alive-Überwachungszeit**

  Nach dem Senden eines Keep-alive-Telegramms erwartet das Kommunikationsmodul innerhalb der Keep-alive-Überwachungszeit eine Antwort vom Kommunikationspartner. Wenn das Modul innerhalb der projektierten Zeit keine Antwort empfängt, baut es die Verbindung ab und versucht, sie neu aufzubauen.

  Voreinstellung: 10 s. Zulässiger Bereich: 1...65535 s

4.5.3 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.

Über Ethernet bzw. das Internet können Sie auf den Webserver der Station zugreifen.

Empfehlung bei langsamen Übertragungswegen: Stellen Sie den Aktualisierungszyklus des Webbrowsers größer ein.

4.6 Uhrzeitsynchronisation

Hinweis

Uhrzeitsynchronisation des CP

Bei Anwendungen, die eine Uhrzeitsynchronisation erfordern, müssen Sie die Uhrzeit des CP regelmäßig synchronisieren. Wenn Sie die Uhrzeit des CP nicht regelmäßig synchronisieren, kann es in der Zeitangabe des CP zu Abweichungen von einigen Sekunden pro Tag kommen.

Bei aktivierten Security-Funktionen müssen Sie die Uhrzeitsynchronisation aktivieren.

Hinweis

Empfehlung für die Zeitvorgabe

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

Uhrzeitsynchronisation bei der S7-1200

Bei Verwendung einer externen Uhrzeitquelle kann die S7-1200-Station die aktuelle Uhrzeit sowohl über die CPU als auch über einen CP beziehen.

Hinweis

Empfehlung: Uhrzeitsynchronisation nur durch 1 Modul

Lassen Sie 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 die CPU die Uhrzeit vom CP übernimmt, dann deaktivieren Sie die Uhrzeitsynchronisation der CPU.

Eine Weiterleitung der Uhrzeit von der Station an das Subnetz findet bei S7-1200 nicht statt.

Parametergruppen für die Uhrzeitsynchronisation

Die Uhrzeitsynchronisation können Sie in folgenden Parametergruppen projektieren:

- **Ethernet-Schnittstelle**

  Hier nehmen Sie die Projektierung unter folgenden Bedingungen vor:

  – Die Telecontrol-Kommunikation ist deaktiviert.

  – Die Security-Funktionen sind deaktiviert.

- **Security**

  Hier nehmen Sie die Projektierung vor, wenn die Security-Funktionen aktiviert sind.

Abhängigkeit der Synchronisationsverfahren von CP-Nutzung

Abhängig von der Nutzung der Telecontrol-Kommunikation oder den Security-Funktionen sind folgende Synchronisationsverfahren auswählbar:

- **Telecontrol-Kommunikation deaktiviert, Security deaktiviert**

  – NTP

  – Uhrzeit von CPU

- **Telecontrol-Kommunikation deaktiviert, Security aktiviert**
  - NTP
  - NTP (secure)
  - Uhrzeit von CPU
- **Telecontrol-Kommunikation und Security aktiviert**
  - Uhrzeit vom Partner
  - NTP
  - NTP (secure)
  - Uhrzeit von CPU

Synchronisationsverfahren des CP

Der CP unterstützt folgende Verfahren der Uhrzeitsynchronisation:

- **NTP**

  Die Uhrzeit wird von einem NTP-Server im angeschlossenen Netz bezogen.

  Das Verfahren kann auch genutzt werden, wenn die Telecontrol-Kommunikation aktiviert ist.

  Bei CPs ab Firmware-Version V3 kann die Adresse des NTP-Servers auch als URL eingegeben werden, bspw. <ntp.server.com>. Hierfür wird ein DNS-Server benötigt.

- **NTP (secure)**

  Bei aktivierten Security-Funktionen steht auch das gesicherte Verfahren NTP (secure) zur Verfügung. Es 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.

  Die genutzten Server legen Sie beim CP fest.

- **Uhrzeit von CPU**

  Die CPU ab V4.2 kann alle CMs/CPs der Station in einem Synchronisationszyklus von 10 Sekunden synchronisieren.

  Parameter der CPU:
  Über die Option "CPU synchronisiert die Module des Geräts" können Sie veranlassen, dass alle Telecontrol-CPs der Station mit Firmware ≥ V2.1.77 in einem Synchronisationszyklus von 10 Sekunden mit der CPU-Zeit synchronisiert werden.

- **Keine Uhrzeitsynchronisation projektiert**

  Wenn beim CP keine Uhrzeitsynchronisation projektiert ist, kann die Uhrzeit des CP unter folgender Bedingung synchronisiert werden:

  Wenn bei der CPU unter "PROFINET-Schnittstelle > Uhrzeitsynchronisation" die Option "CPU synchronisiert die Module des Geräts" aktiviert ist, werden alle CMs/CPs der Station mit der Uhrzeit der CPU synchronisiert.

- **Uhrzeit vom Partner**

  Bei aktivierter Telecontrol-Kommunikation: Der CP übernimmt die Uhrzeit vom Kommunikationspartner.

  Die Beschreibung finden Sie im Projektierungshandbuch /3/ (Seite 118).

Uhrzeitweiterleitung vom CP an die CPU

Hinweis

Uhrzeitweiterleitung an die CPU

Abhängig von der Firmware-Version der beteiligten Module wird die Uhrzeit des CP unterschiedlich an die CPU weitergeleitet:

- Weiterleitung der CP-Zeit an die CPU über eine PLC-Variable
- Weiterleitung der CP-Zeit über den Rückwandbus an die CPU

Die Weiterleitung der CP-Zeit an die CPU ist abhängig von der Firmware-Version des CP und der CPU. Beachten Sie das nachfolgende Verhalten.

- **CP-Firmware < V3**

  Mit dieser Firmware-Version kann die CP-Uhrzeit optional der CPU über eine PLC-Variable zur Verfügung gestellt werden. Wenn diese PLC-Variable zyklisch von der CPU gelesen wird, übernimmt die CPU die CP-Zeit.

  In der Parametergruppe "Kommunikation mit der CPU" können Sie einstellen, ob die aktuelle Uhrzeit des CP der CPU über eine PLC-Variable zur Verfügung gestellt werden soll. Zur PLC-Variablen siehe Parametergruppe "Kommunikation mit der CPU" des CP.

- **CP-Firmware ≥ V3.0 und CPU-Firmware ≥ V4.2**

  Wenn beide Module in einer Station eine der genannten Firmware-Versionen aufweisen, kann die Uhrzeit des CP automatisch an die CPU weitergeleitet werden.

  Bedingung hierfür ist: Bei der CPU ist unter "PROFINET-Schnittstelle > Uhrzeitsynchronisation" die Option "CPU synchronisiert die Module des Geräts" aktiviert.

  Dann werden alle intelligenten Module der Station mit der CPU-Zeit synchronisiert.

  Da die CPU automatisch die CP-Zeit übernimmt, benötigen Sie die Weiterleitungsoption über die PLC-Variable nicht mehr.

4.7 DNS-Konfiguration

DNS-Server projektieren

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.

Wenn der CP Mobilfunkdienste nutzt und der Mobilfunknetz-Betreiber einen DNS-Server in seinem Netz betreibt, hat die Projektierung folgende Auswirkungen:

- Keine Projektierung eines DNS-Servers

  IP-Adressen werden automatisch vom DNS-Server des Netzbetreibers bezogen (empfohlene Vorgehensweise).

- Projektierung eines DNS-Servers

  IP-Adressen werden vom projektierten DNS-Server bezogen. DNS-Server des Netzwerkbetreibers werden nicht berücksichtigt.

4.8 Kommunikation mit der CPU

Kommunikation mit der CPU

Die ersten 4 Parameter sind nur für Telecontrol-Kommunikation relevant.

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 51).

CP-Diagnose

In der Parametergruppe "CP-Diagnose" haben Sie die Möglichkeit, der CPU erweiterte Diagnosedaten des CP über PLC-Variablen zur Verfügung zu stellen.

Die Zustände der PLC-Variablen können Sie über den Webserver der CPU anzeigen.

- **Erweiterte CP-Diagnose aktivieren**

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

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

Je nach CP-Typ und unterstützten Funktionen können PLC-Variablen für folgende Diagnosedaten projektiert werden:

- **Telegrammspeicher-Überlaufwarnung**

  - Nur relevant für Telecontrol-Kommunikation -

- **Telegrammspeicher-Belegung**

  - Nur relevant für Telecontrol-Kommunikation -

- **Aktuelle IP-Adresse**

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

- **Mobilfunk-Signalqualität (LED)**

  PLC-Variable (Datentyp UInt) für die Signalqualität des lokalen Mobilfunknetzes, wie diese von der LED "SIGNAL QUALITY" angezeigt wird.

- **Mobilfunk-Signalqualität (dBm)**

  PLC-Variable (Datentyp INT) für die Signalqualität des lokalen Mobilfunknetzes als dBm-Wert.

- **LED 'NETWORK'**

  PLC-Variable (Datentyp UInt) für den Zustand der Verbindung zum Datendienst im Mobilfunknetz.

  Bedeutung der Werte (dezimal):

  – 0 = Aus dem Netz ausgebucht

  – 1 = Falsche PIN

  – 2 = Falsche, defekte oder nicht gesteckte SIM-Karte

  – 3 = Warten auf PIN / keine PIN projektiert

  – 4 = In Netz eingebucht

- **Datum erfolgreiche Netzanmeldung**

  PLC-Variable (Datentyp DTL) für das Datum, an dem sich der CP zuletzt erfolgreich am Mobilfunknetz angemeldet hat.

- **Datum nicht erfolgreiche Netzanmeldung**

  PLC-Variable (Datentyp DTL) für das Datum, an dem sich der CP das letzte Mal nicht am Mobilfunknetz anmelden konnte.

- **Datum erfolgreiche TCSB-Anmeldung**

  - Nur relevant für Telecontrol-Kommunikation -

- **Datum nicht erfolgreiche TCSB-Anmeldung**

  - Nur relevant für Telecontrol-Kommunikation -

- **TeleService-Status**

  - Nur relevant für Telecontrol-Kommunikation -

- **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

4.9 Security

Die Beschreibung der Telecontrol-spezifischen Parameter finden Sie im jeweiligen Projektierungshandbuch /3/ (Seite 118).

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 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.

4.9.2.3 Firewall-Einstellungen für projektierte Verbindungen über VPN-Tunnel

IP-Regeln im erweiterten Firewall-Modus

Wenn Sie projektierte Verbindungen 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.

Siehe hierzu Kapitel Einstellungen für Online-Security-Diagnose und Laden in Station bei aktivierter Firewall (Seite 59).

4.9.2.4 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 erstekllen oder die Dienste "Echo Request" / "Echo Reply" deaktivieren.

4.9.3 Uhrzeitsynchronisation

Die Beschreibung der Parameter finden Sie im Kapitel Uhrzeitsynchronisation (Seite 51).

4.9.4 Autorisierte Rufnummern

SMS-Empfang nur von Teilnehmern mit autorisierter Rufnummer

Voraussetzung dafür, dass der CP eine SMS akzeptiert, ist die Autorisierung des sendenden Kommunikationspartners mithilfe seiner Rufnummer. Diese Rufnummern projektieren Sie in der Liste "Autorisierte Rufnummern".

"Autorisierte Rufnummern"

Eine hier eingetragene Rufnummer berechtigt den Absender, der diese Rufnummer mit überträgt, einen Verbindungsaufbau durch den CP auszulösen.

- Wenn in der Liste nur ein Stern (*) eingetragen wird, dann akzeptiert der CP SMS von allen Absendern.
- Ein Stern (*) nach einem Rufnummern-Rumpf berechtigt alle an den Rumpf angeschlossenen Teilnehmer (Durchwahlnummern) zum Verbindungsaufbau.

  Beispiel: +49123456* berechtigt +49123456101, +49123456102, +49123456207 etc.

Wenn die Liste "Autorisierte Rufnummern" leer ist, dann kann der CP nicht zu einem Verbindungsaufbau durch ein Mobiltelefon veranlasst werden.

4.9.5 E-Mail-Projektierung

Projektierung von E-Mails

Unter dem Eintrag "E-Mail-Projektierung" projektieren Sie das zu verwendende Protokoll sowie die Zugangsdaten zum E-Mail-Server.

Im Nachrichteneditor (Eintrag "Nachrichten") projektieren Sie die einzelnen E-Mails, siehe Kapitel Nachrichten (Seite 72).

Voraussetzungen für E-Mail

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

Wenn Sie die sichere Übertragung von E-Mail nutzen möchten, muss die Baugruppe das aktuelle Datum und die aktuelle Uhrzeit haben.

In der Standardeinstellung des SMTP-Ports 25 überträgt die Baugruppe unverschlüsselte E-Mails.

Wenn Ihr E-Mail-Dienst-Betreiber nur verschlüsselte Übertragung unterstützt, dann verwenden Sie eine der folgenden Optionen:

- Port-Nr. 587

  Unter Verwendung von STARTTLS sendet die Baugruppe verschlüsselte E-Mails an den SMTP-Server Ihres E-Mail-Dienst-Betreibers.

  Empfehlung: Wenn Ihr E-Mail-Betreiber beide Möglichkeiten (STARTTLS / SSL/TLS) anbietet, dann sollten Sie STARTTLS mit Port 587 verwenden.

- Port-Nr. 465

  Unter Verwendung von SSL/TLS (SMTPS) sendet die Baugruppe verschlüsselte E-Mails an den SMTP-Server Ihres E-Mail-Dienst-Betreibers.

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

Zur Projektierung der Passwörter siehe Zeichensatz für Passwörter und Nachrichten (Seite 78).

Zertifikat importieren bei verschlüsselter Übertragung

Um eine verschlüsselte Übertragung nutzen zu können, müssen Sie das Zertifikat Ihres E-Mail-Kontos in den Zertifikatsmanager von STEP 7 laden. Das Zertifikat erhalten Sie von Ihrem E-Mail-Dienst-Betreiber.

Verwenden Sie das Zertifikat über folgende Schritte:

1. Speichern Sie das Zertifikat Ihres E-Mail-Dienst-Betreibers im Dateisystem der Engineering-Station.
2. Importieren Sie das Zertifikat in Ihr STEP 7-Projekt über "Globale Security-Einstellungen > Zertifikatsmanager".
3. Verwenden Sie das importierte Zertifikat bei jeder Baugruppe, welche verschlüsselte E-Mails nutzt, über die Tabelle "Zertifikatsmanager" in der lokalen Parametergruppe "Security".

Zur Vorgehensweise siehe Kapitel Zertifikatsmanager (Seite 69).

4.9.6 VPN

4.9.6.1 VPN (Virtual Private Network)

VPN-Tunnel

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 (Tunnel) zwischen zwei sicheren IT-Systemen oder Netzen über ein unsicheres Netz hinweg eingerichtet und betrieben.

Der VPN-Tunnel zeichnet sich dadurch aus, dass er sämtliche Telegramme weiterleitet, auch von Protokollen höherer Schichten (HTTP, FTP, Telecontrol-Protokolle der Applikationsschicht etc.).

Der Datenverkehr zweier Netzkomponenten wird uneingeschränkt durch ein physikalisches Netz abgewickelt. Damit können Netzwerke über ein zwischengeschaltetes Netz hinweg miteinander verbunden werden.

VPN-Tunnel gewährleisten Integrität und Vertraulichkeit bei der Datenübertragung.

Eigenschaften

- VPN bildet ein logisches Netz, das sich in ein physikalisches Netz einbettet. VPN nutzt die üblichen Adressierungsmechanismen des physikalischen Netzes, transportiert aber nur die Telegramme der VPN-Teilnehmer und arbeitet so vom Rest des physikalischen Netzes losgelöst.
- VPN ermöglicht die Kommunikation der im VPN-Netz befindlichen Teilnehmer mit dem physikalischen Netz.
- VPN basiert auf einer Tunneltechnik und ist für einzelne Teilnehmer projektierbar.
- 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).
- Absicherung von Rechnern und deren Kommunikation innerhalb eines Automatisierungsnetzes
- Gesicherte Fernzugriffe vom PC/PG über öffentliche Netze auf Automatisierungsgeräte oder Netzwerke, die durch Security-Module geschützt sind.

4.9.6.2 Adressierung des CP bei Nutzung von VPN

IP-Adressen und VPN-Ports

In den üblichen Mobilfunknetzen ist es nicht möglich, eine dynamische IP-Adresse, welche dem CP vom Mobilfunk-Netzbetreiber zugewiesen wurde, aus dem Internet zu erreichen. Daher ist für eingehende Verbindungen sicherzustellen, dass dem CP vom Mobilfunk-Netzbetreiber eine feste öffentliche IP-Adresse vergeben wird.

Zusätzlich muss gewährleistet sein, dass neben dieser IP-Adresse auch die für VPN notwendigen Ports aus dem Internet erreichbar sind.

4.9.6.3 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 befinden sich im gleichen Subnetz.
- Alle empfangenden Stationen benötigen eine feste IP-Adresse, um über die öffentlichen Netze erreichbar zu sein. Hierzu ist für den Mobilfunk-CP in der Regel ein spezieller Mobilfunkvertrag erforderlich.

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.

"Aktiviere Security-Funktionen" anwählen

Nach dem Anmelden müssen Sie in der Projektierung beider CPs das Kontrollkästchen "Aktiviere Security-Funktionen" anwählen.

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

VPN-Gruppe anlegen und Security-Module zuweisen

1. Wählen Sie in den globalen Security-Einstellungen den Eintrag "Firewall" > "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 in den globalen Security-Einstellungen 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

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

Der Aufbau einer VPN-Verbindung zu einer Engineering-Station, die gleichzeitig Telecontrol-Server ist (TCSB installiert), läuft zusammen mit der Uhrzeitsynchronisation des CP folgendermaßen ab:

Sie wollen an der Engineering-Station (mit TCSB) eine VPN-Verbindung durch den CP aufbauen lassen. Auch wenn der CP noch nicht die aktuelle Uhrzeit hat, wird die VPN-Verbindung aufgebaut. Die verwendeten Zertifikate werden als gültig ausgewertet und die gesicherte Kommunikation funktioniert.

Nach dem Verbindungsaufbau synchronisiert der CP seine Uhrzeit mit dem PC, da der Telecontrol-Server bei aktivierter Telecontrol-Kommunikation Uhrzeit-Master ist.

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: Das Kontrollkästchen "Firewall aktivieren" wird beim Anlegen einer VPN-Gruppe automatisch aktiviert. Sie können das Kontrollkästchen nicht deaktivieren.

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

4.9.6.4 Kommunikationspartner in einer VPN-Gruppe

Projektierung der Kommunikationspartner

Wenn ein Teilnehmer mit mehreren CPs über VPN-Verbindungen kommunizieren soll, dann müssen alle Kommunikationspartner der gleichen VPN-Gruppe zugeordnet werden.

Der CP selbst kann nur mit einem einzigen Kommunikationspartner über VPN kommunizieren.

4.9.6.5 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".

4.9.6.6 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 projektiert 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.

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.

4.9.7 Zertifikatsmanager

Zuordnung von Zertifikaten

Wenn Sie für die Baugruppe Kommunikation mit Authentifizierung nutzen, beispielsweise SSL/TLS für die gesicherte Übertragung von E-Mails, dann werden Zertifikate benötigt. Sie müssen Zertifikate von Nicht-Siemens-Kommunikationspartnern in das STEP 7-Projekt importieren und diese mit den Projektierungsdaten in die Baugruppe laden:

1. Importieren Sie die Zertifikate des Kommunikationspartners über den Zertifikatsmanager in den Globalen Security-Einstellungen.
2. Ordnen Sie anschließend der Baugruppe die importierten Zertifikate zu, wahlweise:
   - Über die Tabelle "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen" den Globalen Security-Einstellungen
   - Über die Tabelle "Zertifikate der Partner-Geräte" im lokalen Zertifikatsmanager der Baugruppe (Security)

     Nehmen Sie in diese Tabelle auch die Zertifikate von Kommunikationspartnern auf, deren Zertifikate im selben STEP 7-Projekt generiert wurden.

Die Beschreibung der Vorgehensweise finden Sie im Kapitel Handhabung von Zertifikaten (Seite 69).

Weitere Informationen finden Sie im STEP 7-Informationssystem.

4.9.8 Handhabung von Zertifikaten

Zertifikate für die Authentifizierung

Wenn Sie für das Kommunikationsmodul gesicherte Kommunikation mit Authentifizierung projektiert haben, dann werden eigene Zertifikate und Zertifikate des Kommunikationspartners für das Zustandekommen der Kommunikation benötigt.

Alle Teilnehmer eines STEP 7-Projekts mit aktivierten Security-Funktionen werden mit Zertifikaten versorgt. Das STEP 7-Projekt ist dabei die Zertifizierungsstelle.

Hinweis

Kein Zertifikat bei deaktivierten Security-Funktionen

Wenn im STEP 7-Projekt die Security-Funktionen des CP deaktiviert sind, dann wird auch kein Zertifikat für den CP erzeugt.

Für die gesicherte Übertragung von E-Mails über SSL/TLS wird für den CP ein SSL-Zertifikat erstellt. Es wird in STEP 7 unter "Globale Security-Einstellungen > Zertifikatsmanager > Gerätezertifikate" sichtbar. In der Tabelle "Gerätezertifikate" werden Aussteller, Gültigkeit, Verwendung eines Zertifikats (Dienst/Applikation) und die Verwendung eines Schlüssels angezeigt. Weitere Informationen eines Zertifikats können Sie aufrufen, wenn Sie das Zertifikat in der Tabelle selektieren und das Kontextmenü "Anzeigen" wählen. In der Tabelle sehen Sie auch alle weiteren von STEP 7 erzeugten sowie alle importierten Zertifikate.

Damit das Modul bei aktivierten Security-Funktionen mit Nicht-Siemens-Partnern kommunizieren kann, müssen die entsprechenden Zertifikate der Partner bei der Kommunikation ausgetauscht werden. Gehen Sie für die Versorgung des Moduls mit Fremdzertifikaten folgendermaßen vor:

1. Fremdzertifikate von Kommunikationspartnern importieren

   ⇒ Globale Security-Einstellungen des Projekts (Zertifikatsmanager)

2. Zertifikate zuordnen, alternativ:

   – Globale Security-Einstellungen > Zertifikatsmanager > "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen"

   – Lokale Security-Einstellungen des Moduls > Zertifikatsmanager > "Zertifikate der Partner-Geräte"

Die Schritte sind in den folgenden Abschnitten beschrieben.

Fremdzertifikate von Kommunikationspartnern importieren

Importieren Sie die Zertifikate der Kommunikationspartner von Drittherstellern über den Zertifikatsmanager in den Globalen Security-Einstellungen des STEP 7-Projekts. Gehen Sie hierzu folgendermaßen vor:

1. Speichern Sie das Fremdzertifikat im Dateisystem des PC der angeschlossenen Engineering-Station.
2. Öffnen Sie im STEP 7-Projekt den globalen Zertifikatsmanager:

   Globale Security-Einstellungen > Zertifikatsmanager
3. Öffnen Sie das Register "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen".
4. Klicken Sie in eine Zeile der Tabelle und wählen Sie das Kontextmenü "Importieren".
5. Importieren Sie über den sich öffnenden Dialog das Zertifikat aus dem Dateisystem der Engineering-Station in das STEP 7-Projekt.

Zertifikate in den Globalen Security-Einstellungen zuordnen

Importieren Sie das Partner-Zertifikat über: Globale Security-Einstellungen > Zertifikatsmanager > Vertrauenswürdige Zertifikate > rechte Maustaste. Weisen Sie das Zertifikat dem CP zu (Zertifikat selektieren > rechte Maustaste).

1. Öffnen Sie das Register "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen".
2. Selektieren Sie das gewünschte Zertifikat.
3. Wählen Sie das Kontextmenü "Zuweisen" (rechte Maustaste).
4. Markieren Sie im Folgedialog die gewünschte Baugruppe.

   Nach dem Zuweisen taucht das Zertifikat im lokalen Zertifikatsmanager der Baugruppe in der Tabelle "Zertifikate der Partner-Geräte" auf.

Zertifikate lokal zuordnen

Um ein importiertes Zertifikat für das Modul nutzen zu können, muss das Zertifikat in der Parametergruppe "Security" des Moduls angezeigt werden. Gehen Sie hierzu folgendermaßen vor:

1. Selektieren Sie im STEP 7-Projekt das Modul.
2. Navigieren Sie zur Parametergruppe "Security > Zertifikatsmanager".
3. Doppelklicken Sie in der Tabelle auf die Zelle mit dem Eintrag "<Neu hinzufügen>".

   Die Tabelle "Zertifikatsmanager" der Globalen Security-Einstellungen wird angezeigt.
4. Selektieren Sie in der Tabelle das gewünschte Fremdzertifikat und klicken Sie zur Übernahme auf das grüne Häkchen unter der Tabelle.

   Das ausgewählte Zertifikat wird in der lokalen Tabelle des Moduls angezeigt.

Erst jetzt wird das Fremdzertifikat für das Modul verwendet.

Nehmen Sie in diese Tabelle auch die Zertifikate von Kommunikationspartnern auf, deren Zertifikate im selben STEP 7-Projekt generiert wurden.

Zertifikate für Applikationen von Drittherstellern exportieren (z. B. Logging-Server)

Für die Kommunikation mit Applikationen von Drittherstellern benötigt die Fremd-Applikation in der Regel auch das Zertifikat des Moduls.

Den Export des Zertifikats des Moduls für Kommunikationspartner von Drittherstellern führen Sie ähnlich wie den Import durch (vgl. oben). Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie im STEP 7-Projekt den globalen Zertifikatsmanager:

   Globale Security-Einstellungen > Zertifikatsmanager
2. Öffnen Sie das Register "Gerätezertifikate".
3. Selektieren Sie in der Tabelle die Zeile mit dem gewünschten Zertifikat und wählen Sie das Kontextmenü "Exportieren".
4. Speichern Sie das Zertifikat im Dateisystem des PC der angeschlossenen Engineering-Station.

Jetzt können Sie das exportierte Zertifikat des Moduls in das System des Drittherstellers übertragen.

Zertifikat für Logging-Server

Wenn Sie einen Logging-Server in Ihrer Anlage verwenden, dann exportieren Sie für die Authentifizierung des Moduls am Server das SSL-Zertifikat.

Zertifikat ändern: Alternativer Name des Zertifikatsinhabers

STEP 7 übernimmt die Eigenschaften "DNS-Name", "IP-Adresse" und "URI" des Parameters "Alternativer Name des Zertifikatsinhabers" (Windows: "Alternativer Antragstellername") aus den STEP 7-Projektierungsdaten.

Sie können diesen Parameter eines Zertifikats im Zertifikatsmanager der Globalen Security-Einstellungen ändern. Selektieren Sie hierzu in der Tabelle der Gerätezertifikate ein Zertifikat

und rufen Sie das Kontextmenü "Erneuern" auf. In STEP 7 geänderte Eigenschaften des Parameters "Alternativer Name des Zertifikatsinhabers" werden nicht vom STEP 7-Projekt übernommen.

4.10 Datenpunkte

Die Beschreibung der Telecontrol-spezifischen Parameter finden Sie im jeweiligen Projektierungshandbuch /3/ (Seite 118).

4.11 Nachrichten

Projektierung von Nachrichten

Bei wichtigen Ereignissen kann der CP Nachrichten absetzen. Projektierbar sind:

- E-Mails

  Empfänger kann ein PC mit Internetanschluss oder eine S7-Station sein.

- SMS (nur Mobilfunk-CPs)

  Empfänger kann ein Mobiltelefon oder eine S7-Station sein.

Die Nachrichten projektieren Sie im Nachrichteneditor des CP. Diesen finden Sie alternativ über:

- Das Kontextmenü des CP
- Über die Projektnavigation: Verzeichnis der Station > Lokale Module > CP

Die Zugangsdaten zum Mobilfunknetz und zu einem APN für die Übertragung von E-Mails erhalten Sie von Ihrem Netzbetreiber. Diese projektieren Sie in der Parametergruppe "Mobilfunk-Kommunikationseinstellungen", siehe Kapitel Mobilfunk-Kommunikationseinstellungen (Seite 48).

Die zugelassenen Zeichen für Nachrichtentexte und weitere Parameter finden Sie im Kapitel Zeichensatz für Passwörter und Nachrichten (Seite 78).

Projektierungsübersicht und benötigte Informationen

Für die Übertragung von Nachrichten muss die Telecontrol-Kommunikation (Parametergruppe "Kommunikationsarten") nicht mehr aktiviert werden. Sie können mit dem CP Nachrichten versenden, ohne Telecontrol-Kommunikation zu nutzen.

Weitere benötige Informationen für SMS und E-Mails, die Sie von Ihrem Dienstbetreiber erhalten, finden Sie in den folgenden Abschnitten.

E-Mails

Benötigte Informationen:

- Zugangsdaten des SMTP-Servers: Adresse, Port-Nummer, Benutzername, Passwort
- Bei Nutzung von STARTTLS oder SSL/TLS: Zertifikat des E-Mail-Dienst-Betreibers
- E-Mail-Adressen der Empfänger

Die Projektierung nehmen Sie in folgenden Parametergruppen vor:

- Aktivierung der Security-Funktionen

  Für die Nutzung von E-Mails müssen Sie die Security-Funktionen des CP aktivieren, Parametergruppe "Security".
- Projektierung des Dienstes / Protokolls:

  "E-Mail-Projektierung", siehe Kapitel E-Mail-Projektierung (Seite 60).
- Bei Nutzung von STARTTLS oder SSL/TLS:
  - Import des Zertifikats des E-Mail-Dienst-Betreibers:

    "Globale Security-Einstellungen"
  - Verwendung des importierten Zertifikats für den CP:

    Parametergruppe "Security" > "Zertifikatsmanager"

SMS

Benötigte Informationen:

- Nummer des SMSC

Die Projektierung nehmen Sie in folgenden Parametergruppen vor:

- Aktivierung der SMS-Funktion:

  "Kommunikationsarten" > "SMS aktivieren"
- Projektierung des SMSC

  "Mobilfunk-Kommunikationseinstellungen", siehe oben.
- Projektierung der SMS

  Nachrichteneditor, siehe oben.

Projektierung im Nachrichteneditor

Die Projektierung der Nachrichten nehmen Sie in STEP 7 im Datenpunkt- und Nachrichten-Editor vor. Sie können den Editor alternativ öffnen über:

- Selektion der Kommunikationsbaugruppe

  Kontextmenü "Datenpunkt- und Nachrichten-Editor öffnen"
- Über die Projektnavigation:

  Projekt > Verzeichnis der jeweiligen Station > Lokale Baugruppen > gewünschte Kommunikationsbaugruppe

  Durch Doppelklick auf den Eintrag öffnet sich der Datenpunkt- bzw. Nachrichten-Editor.

Bild 4-1 Öffnen des Nachrichten-Editors über die Projektnavigation

Nach Öffnen des Editors können Sie über die beiden Einträge rechts oben über der Tabelle zwischen dem Datenpunkt- bzw. Nachrichten-Editor umschalten.

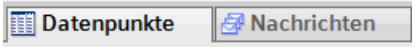


Bild 4-2 Umschaltung zwischen den zwei Editoren

Der Datenpunkteditor ist nur für die Telecontrol-Kommunikation relevant.

Anlegen von Objekten

Legen Sie ein neues Objekt (Nachricht) an, indem Sie in die erste Tabellenzeile mit dem gegrauten Eintrag "<Objekt hinzufügen>" doppelklicken.

Den vorbelegten Namen können Sie nach Ihren Bedürfnissen anpassen, er muss aber innerhalb des Moduls eindeutig sein.

Anordnen von Spalten und Zeilen, Ein-/Ausblenden von Spalten

Wie bei vielen anderen Programmen können Sie 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 rechten 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

Sie können Nachrichten kopieren und einfügen. Wenn Sie mit der rechten Maustaste in die Zeile eines Objekts in der Tabelle klicken, erreichen Sie die genannten Funktionen 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 und mit gleichem Telecontrol-Protokoll 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.

Register zur Projektierung der Nachrichten

Selektieren Sie der Tabelle "Nachrichten" eine Nachricht. Die Parameter dieser selektierten Nachricht projektieren Sie in den Registern unterhalb der Tabelle.

"Nachrichtenparameter"

Hier projektieren Sie die Rufnummer bzw. die Empfänger, den Betreff (E-Mail) und den Text der Nachricht.

"Trigger"

Über die Parametergruppe "Trigger" projektieren Sie das Auslösen des Versendens der Nachricht sowie weitere Parameter.

- **E-Mail-Trigger / SMS-Trigger**

  Legt das Ereignis fest, bei dem das Versenden der Nachricht ausgelöst wird.

  Abhängig vom verwendeten Modul und den aktivierten Diensten können Sie folgende Trigger auswählen:

  – **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 Nachricht 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**

  – **Verbindung zu einem Partner unterbrochen**

    Löst das Senden der Nachricht aus, wenn die Telecontrol-Verbindung zu einem Partner unterbrochen wird.

  – **Verbindung zu einem Partner aufgebaut**

    Löst das Senden der Nachricht aus, wenn die Telecontrol-Verbindung wiederkehrt.

  – **Verbindungsaufbau zu einem Partner fehlgeschlagen**

    Löst das Senden der Nachricht aus, wenn die Telecontrol-Verbindung zu einem Partner nicht aufgebaut werden konnte.

  - **TeleService-Sitzung begonnen**

    Löst das Senden der Nachricht aus, wenn Telecontrol-Kommunikation aktiviert ist und eine TeleService-Verbindung aufgebaut ist.

  - **TeleService-Sitzung beendet**

    Löst das Senden der Nachricht aus, wenn Telecontrol-Kommunikation aktiviert ist und eine TeleService-Verbindung beendet worden ist.

  - **Schwaches Mobilfunknetz**

    (Nur SMS)

    Wenn die Mobilfunkverbindung für die Telecontrol-Kommunikation zu schwach ist, wird eine SMS ausgelöst und an den projektierten Empfänger geschickt.

  - **VPN-Verbindung aufgebaut**

    Löst das Senden der Nachricht aus, wenn die VPN-Verbindung aufgebaut ist oder wiederkehrt.

  - **VPN-Verbindung abgebaut**

    Löst das Senden der Nachricht aus, wenn die VPN-Verbindung unterbrochen wird.

  - **SINEMA RC-Verbindung aufgebaut**

    Löst das Senden der Nachricht aus, wenn die OpenVPN-Verbindung aufgebaut ist oder wiederkehrt.

  - **SINEMA RC-Verbindung abgebaut**

    Löst das Senden der Nachricht aus, wenn die OpenVPN-Verbindung unterbrochen wird.

- **PLC-Variable für Trigger**

  PLC-Variable für den 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 die "PLC-Variable für Bearbeitungsstatus" 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 hexadezimal ausgegebenen Status siehe Kapitel Bearbeitungsstatus von Nachrichten (Seite 96).

- **PLC-Variable für Bearbeitungsstatus**

  PLC-Variable vom Typ DWORD für den Bearbeitungsstatus

- **Wert mitschicken**

  Bei aktivierter Option schickt der CP in der Nachricht für den Platzhalter $$ einen Wert aus dem Speicherbereich der CPU mit. Hierzu geben Sie im Nachrichtentext "$$" als Platzhalter für den mitzuschickenden Wert ein.

  Wählen Sie eine PLC-Variable, deren Wert in die Nachricht integriert wird. Der Wert wird im Nachrichtentext an der Stelle des Platzhalters $$ eingesetzt.

  $$ als Platzhalter für die Werte von Datenpunkten unterstützt folgende Datentypen:

  – Bool, Byte, Char, Int, UInt, Word, DWord, UDInt, DInt, Real, String,

  – Arrays der vorgenannten Datentypen

  Beachten Sie, dass sich durch den Wert die Anzahl der Zeichen erhöht. Zur max. Anzahl der Zeichen siehe Mengengerüst.

- **PLC-Variable für Wert**

  PLC-Variable, in die der mitzuschickende Wert zu schreiben ist.

4.12 Zeichensatz für Passwörter und Nachrichten

Zeichensatz für APNs, E-Mail-Server, Nachrichtentexte und das Telecontrol-Passwort

Die nachfolgenden zugelassenen Zeichen gelten für:

- APN, E-Mail-Server:

  Benutzernamen und Passwörter

- CP-Identifikation:

  Telecontrol-Passwort

- Nachrichten im Nachrichteneditor:

  Nachrichtentexte

Angabe als ASCII-Zeichensätze (Hexadezimalwert und Zeichenname):

- 0x20

  Leerzeichen

- 0x21 ... 0x5F

  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _

- 0x61 ... 0x7E

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

- 0x7C, 0x7E

  | ~

Zusätzlich für Nachrichtentexte:

- Manueller Zeilenumbruch (↵)

  In Nachrichtentexten können Sie einen Zeilenumbruch über <Shift>+<Enter> einfügen.

Programmbausteine

5

5.1 Programmbausteine für OUC

Verwendung der Programmbausteine für die Open User Communication (OUC)

Die unten aufgeführten Anweisungen (Programmbausteine) sind erforderlich für die direkte Kommunikation zwischen S7-Stationen über das Mobilfunknetz.

Im Unterschied zur Telecontrol-Kommunikation muss die Open User Communication nicht in der Projektierung aktiviert werden, da hierfür aktiv die entsprechenden Programmbausteine angelegt werden müssen. Details zu den Programmbausteinen finden Sie im Informationssystem von STEP 7.

Für den Empfang von Daten über Programmbausteine benötigt der CP vom Mobilfunk-Netzbetreiber die Zuweisung einer festen IP-Adresse.

Hinweis

Keine unterschiedlichen Programmbaustein-Versionen

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

Voraussetzungen für Secure OUC

Voraussetzungen für die Nutzung der gesicherten Übertragung über Secure OUC:

- STEP 7: Ab V16
- CPU-Firmware: Ab V4.4
- CP-Firmware: Ab V3.2

Unterstützte Programmbausteine für OUC

Folgende Anweisungen in der angegebenen Mindestversion stehen für die Open User Communication 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
  - Senden bzw. Empfangen von SMS

- **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. Projektieren Sie die Uhrzeitsynchronisation.

Zum Ändern der Projektierungsdaten des CP zur Laufzeit:

- **T_CONFIG V1.0**

  Programmgesteuerte Konfiguration der IP-Parameter des CP

  Beachten Sie die Hinweise zu T_CONFIG und zu den SDTs "IF_CONF_..." im Kapitel TC_CONFIG zum Ändern der Projektierungsdaten des CP (Seite 85).

  Die Adressparameter können nur mit temporärer Gültigkeit konfiguriert werden. Im jeweiligen SDT "IF_CONF_..." muss der Parameter "Mode" = 2 gesetzt werden.

  Hinweis

  Keine Rückmeldung des CP

  "T_CONFIG" unterstützt keine Rückmeldung des CP an die CPU. Fehler im Bausteinaufruf oder beim Setzen des Adressparameters werden nicht zurück gemeldet. Unabhängig davon, ob der Adressparameter gesetzt wurde, gibt der Baustein "BUSY" oder "DONE" aus.

Die Programmbausteine finden Sie in STEP 7 in der Task Card "Anweisungen > Kommunikation > Open User Communication".

Verbindungsbeschreibungen in Systemdatentypen (SDTs)

Für die jeweilige Verbindungsbeschreibung verwenden die oben genannten Bausteine den Parameter CONNECT. TMAIL_C verwendet den Parameter MAIL_ADDR_PARAM.

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.

Verwendbare SDTs

- **TCON_IP_V4**

  Für die Übertragung von Telegrammen über TCP oder UDP

- **TCON_QDN**

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

- **TCON_IP_RFC**

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

- **TADDR_Param**

  Für die Übertragung von Telegrammen über UDP

- **TMail_V4**

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

  Empfehlung Für Mobilfunk-Anwendungen:
  Setzen Sie den Parameter "WatchdogTime" von "MAIL_ADDR_PARAM" auf einen Wert größer 3 Minuten.

- **TMail_FQDN**

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

- **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

- **TMail_V4_SEC**

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

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

Weitere Hinweise zum Versenden von SMS finden Sie im Kapitel SMS über OUC (Seite 82).

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 Parametrierung.

5.2 SMS über OUC

Verschicken von E-Mails / SMS über OUC

Die nachfolgend beschriebenen Programmbausteine und Systemdatentypen (SDTs) benötigen Sie bei Mobilfunk-CPs nur für die Übertragung von SMS über Open User Communication (OUC).

Das ereignisgesteuerte Versenden von E-Mails oder SMS dagegen ist unabhängig von Programmbausteinen und wird in STEP 7 im Nachrichteneditor des jeweiligen Moduls projektiert.

SMS über Programmbausteine

SMS an einen Partner senden

Legen Sie hierzu alternativ folgende Bausteine bzw. Systemdatentypen an:

- TCON + TDISCON + TSEND + TCON_Phone
- TSEND_C + TCON_Phone

SMS von einem Partner empfangen

Legen Sie hierzu alternativ folgende Bausteine bzw. Systemdatentypen an:

- TCON + TDISCON + TRCV + TCON_Phone
- TRCV_C + TCON_Phone

Wenn Sie im Parameter "PhoneNumber" des Systemdatentyps TCON_Phone keine Rufnummer parametrieren, kann der CP keine SMS empfangen.

SMS von mehreren Partnern empfangen

Sie können alternativ für jeden Partner einen separaten Bausteinsatz, wie oben für 1 Partner beschrieben, anlegen oder einen einzigen Bausteinsatz mit folgender Besonderheit im Baustein TCON_PHONE:

Wenn Sie im Parameter "PhoneNumber" des Bausteins TCON_Phone nach dem Rufnummern-Rumpf einen Stern (*) eingeben, dann dann wirkt der Stern als Platzhalter für alle autorisierten Rufnummern mit diesem Rufnummern-Rumpf.

Die für den Zugriff auf den CP autorisierten Rufnummern projektieren Sie in STEP 7 in der Parametergruppe "Security" des CP.

Zu sendender Nachrichtentext am Parameter "DATA"

Den Nachrichtentext geben Sie als String am Parameter "DATA" von TSEND bzw. TSEND_C ein.

Eine Nachricht kann bis zu 160 Zeichen enthalten. Wenn der Nachrichtentext mehr als 160 Zeichen enthält, wird der Text auf zwei oder mehr SMS aufgeteilt.

Auslesen des Nachrichtentextes am Parameter "DATA"

Für den Empfang einer SMS parametrieren Sie den auszulesenden Nachrichtentext bei den Bausteinen TRCV / TRCV_C am Parameter "DATA" über einen Datenbaustein (DB).

Legen Sie einen DB vom Datentyp "Struct" an. Öffnen Sie den Eigenschaftendialog des DB (Kontextmenü des DB) und deaktivieren Sie in der Parametergruppe "Attribute" den optimierten Bausteinzugriff.

Legen Sie in der Struktur des DB für die SMS folgende Datentypen an:

- DTL

  12 Byte für den Zeitstempel der empfangenen SMS (Zeitstempel vom Netz)

- String[22]

  String von 22 Byte für den Rufnummer des Absenders (+ 2 Byte String-Header)

- String[160]

  String von 160 Byte für den Nachrichtentext (+ 2 Byte String-Header)

  Der SMS-Text darf max. 160 Zeichen enthalten.

Die Struktur benötigt pro SMS einen Speicherplatz von 198 Byte.

Speichern der letzten 10 empfangenen SMS

Sie können bis zu 10 empfangene SMS vom Empfangsbaustein ausgeben, indem Sie beim TCON_PHONE am Parameter "PhoneNumber" den Eintrag "SMSSTORE" eingeben.

Für die Speicherung der Empfangsdaten von 10 SMS müssen Sie für den Parameter "DATA" des Empfangsbausteins eine ausreichend große Struktur (2000 Byte) anlegen. Wie oben beschrieben hat die Struktur folgenden Aufbau:

- Empfangsdaten SMS 1 (DTL, String[22], String[160], Byte)
- Empfangsdaten SMS 2 (DTL, String[22], String[160], Byte)

  ... bis
- Empfangsdaten SMS 10 (DTL, String[22], String[160], Byte)

Die Empfangsdaten jeder SMS haben folgenden Aufbau:

- DTL

  12 Byte für den Zeitstempel der empfangenen SMS (Zeitstempel vom Netz)

- String[22]

  String von 22 Byte für den Rufnummer des Absenders (+ 2 Byte String-Header)

- String[160]

  String von 160 Byte für den Nachrichtentext (+ 2 Byte String-Header)

- Byte

  Status der SMS

  Wenn mehr als eine SMS empfangen wird, dann wird für jede SMS der Status in diesem Status-Byte gespeichert:

  – 0 = Ungültig

    1 = Ungelesen

    2 = Gelesen

Beim Empfang von mehreren SMS benötigt die Struktur pro SMS einen Speicherplatz von 200 Byte.

Längenangaben an "LEN" und "DATA" bei Bausteinen "TRCV" / "TRCV_C"

Wenn Sie beim Empfang von SMS über die Bausteine TRCV oder "TRCV_C" die Längenangabe am Parameter "LEN" angeben, kann dies zu falschen Informationen in der Datenablage der empfangenen Informationen führen.

Empfehlung: Setzen Sie LEN = 0 und machen Sie die Längenangabe am Parameter "DATA".

Zeichensatz für den SMS-Text

Der CP unterstützt den folgenden ASCII-Zeichensatz (Hexadezimalwert und Zeichenname) für SMS-Texte, die über Programmbausteine gesendet werden:

- 0x0A

  LF (Zeilenvorschub)

- 0x0D

  CR (Carriage Return)

- 0x20

  Leerzeichen

- 0x21 ... 0x5A

  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- 0x61 ... 0x7A

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

5.3 TC_CONFIG zum Ändern der Projektierungsdaten des CP

Bedeutung

Mit dem Programmbaustein TC_CONFIG können Sie die in STEP 7 projektierten Parameter des CP ändern. Die projektierten Werte werden nicht remanent überschrieben. Die überschriebenen Werte bleiben gültig bis zum erneuten Aufruf von TC_CONFIG oder bis zum nächsten Anlauf der Station (Kaltstart durch Spannung AUS → EIN).

Wenn die STEP 7-Projektierungsdaten des CP dauerhaft geändert werden sollen, dann muss der Baustein nach jedem Anlauf der Station (Kaltstart) neu aufgerufen werden oder ein geändertes Projekt muss in die Station geladen werden.

Der Parameter CONFIG zeigt auf den Speicherbereich mit den Projektierungsdaten. Die Projektierungsdaten werden in einem Datenbaustein (DB) gespeichert. Der DB kann nicht mit optimiertem Bausteinzugriff angelegt werden. Die Struktur des DB wird durch den Systemdatentyp (SDT) IF_CONF vorgegeben.

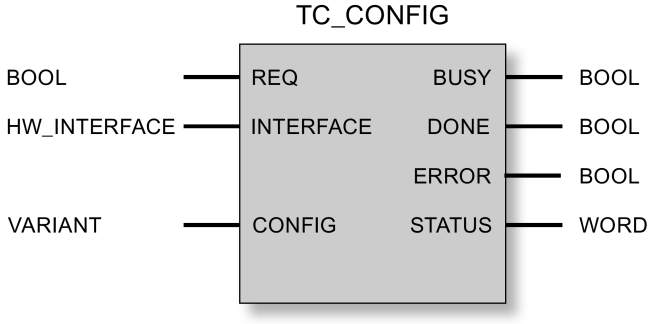
Diejenigen Projektierungsdaten, die im CP geändert werden sollen, werden im IF_CONF als Blöcke "IF_CONF_..." für die einzelnen Parameter nach Bedarf zusammengestellt.

Parameter, die sich durch den Baustein nicht ändern sollten, werden im IF_CONF nicht eingetragen. Sie behalten dann den in STEP 7 projektierten Wert.

Details zur Parametrierung von IF_CONF enthält der Abschnitt IF_CONF: SDT für Projektierungsdaten des CP (Seite 87).

Der Parameter INTERFACE referenziert den Namen der Schnittstelle des Mobilfunk-CP. Den Namen der Schnittstelle finden Sie im STEP 7-Projekt in der Standardvariablentabelle der Station im Register "Systemkonstanten" unter dem Eintrag mit dem Wert der "HW-Kennung" des CP.

Aufrufschnittstelle in FUP-Darstellung



Erläuterung der Formalparameter

Die folgende Tabelle erläutert die Formalparameter der Anweisung TC_CONFIG

Parameter	Deklaration	Datentyp	Wertebereich	Beschreibung
REQ	INPUT	BOOL	0, 1	Bei steigender Flanke wird die Bearbeitung des Bausteins gestartet und die Statusanzeigen initialisiert. Aktualisierung der Statusanzeigen DONE, ERROR und STATUS, wenn keine positive Flanke ansteht.
INTERFACE	INPUT	HW_Interface (WORD)		Referenz auf die Schnittstelle des lokalen CP
CONFIG	INOUT	VARIANT	Siehe auch "IF_CONF: SDT für Telecontrol-Projektierungsdaten"	Referenz auf den Speicherbereich mit der Zusammenstellung der zu ändernden Projektierungsdaten
ENO	OUTPUT	BOOL	0: Fehler 1: Fehlerfrei	Freigabeausgang Bei Auftreten eines Laufzeitfehlers der Anweisung wird ENO = 0 gesetzt.
BUSY	OUTPUT	BOOL	0: Bearbeitung der Anweisung noch nicht begonnen, abgeschlossen oder abgebrochen 1: Bearbeitung der Anweisung läuft	Anzeige des Bearbeitungs-Status des Bausteins
DONE	OUTPUT	BOOL	0: - 1: Bearbeitung der Anweisung erfolgreich beendet	Der Zustandsparameter zeigt an, ob der Auftrag fehlerfrei abgewickelt wurde. Zur Bedeutung im Zusammenhang mit den Parametern ERROR und STATUS siehe unter Anzeigen des Bausteins.
ERROR	OUTPUT	BOOL	0: - 1: Fehler	Fehleranzeige Zur Bedeutung im Zusammenhang mit den Parametern DONE und STATUS siehe unter Anzeigen des Bausteins.
STATUS	OUTPUT	WORD		Statusanzeige Zur Bedeutung im Zusammenhang mit den Parametern DONE und ERROR siehe unter Anzeigen des Bausteins.

Die Anzeigen BUSY, DONE und ERROR

Die Anzeigen von DONE und ERROR sind nur relevant bei BUSY = 0.

BUSY	DONE	ERROR	Bedeutung
0	0	0	Kein Auftrag in Bearbeitung

Alle weiteren Anzeigenkombinationen von DONE und ERROR finden Sie in der nachfolgenden Tabelle.

Die Anzeigen DONE, ERROR und STATUS

Die folgende Tabelle informiert über die vom Anwenderprogramm auszuwertende Anzeige, gebildet aus DONE, ERROR und STATUS.

DONE	ERROR	STATUS	Bedeutung
1	0	0000H	Auftrag fehlerfrei ausgeführt
0	0	7000H	Keine Auftragsbearbeitung aktiv (Erstaufruf des Bausteins)
0	0	7001H	Auftragsbearbeitung gestartet (Erstaufruf des Bausteins)
0	0	7002H	Auftragsbearbeitung läuft bereits (erneuter Aufruf des Bausteins bei BUSY = 1)
0	1	80E0H	Interner Fehler
0	1	80E6H	Keine Anfrage in Bearbeitung (Aufruf des Bausteins nicht gestartet)
0	1	80EBH	Anfrage vorübergehend zurückgewiesen (der CP wird momentan von STEP 7 konfiguriert.)
0	1	80F6H	Formatfehler eines Parameters im aufgerufenen Datenbaustein (falsche Länge, falsches Format oder ungültiger Wert) Prüfen Sie den SDT "IF_CONF".
0	1	80F7H	Falsche ID in den Parameterblöcken der Projektierungsdaten: Prüfen Sie den SDT "IF_CONF".

5.4 IF_CONF: SDT für Projektierungsdaten des CP

Aufbau des Systemdatentyps IF_CONF für den Programmbaustein TC_CONFIG

Der Parameter CONFIG des Programmbausteins TC_CONFIG referenziert den Speicherbereich mit den zu ändernden Projektierungsdaten des CP. Die in einem Datenbaustein abgelegten Projektierungsdaten werden als Struktur vom Systemdatentyp (SDT) IF_CONF beschrieben.

Um den (SDT) IF_CONF nutzen zu können, müssen in der STEP 7-Basisprojektierung des CP bereits projektierte Werte vorhanden sein.

IF_CONF setzt sich aus einem Header und nachfolgenden Blöcken zusammen, die den Parametern oder Parameterbereichen des CP in den Geräteeigenschaften des STEP 7-Projekts entsprechen.

Die zu ändernden Projektierungsdaten des CP werden als IF_CONF-Blöcke zusammengestellt. Nicht zu ändernde Parameter werden in der IF_CONF-Struktur nicht berücksichtigt und bleiben so, wie sie im STEP 7-Projekt konfiguriert wurden.

Anlegen des DB und der IF_CONF-Strukturen

Die Parameter des CP können Sie innerhalb des IF_CONF-DB in einer oder in mehreren Strukturen mit jeweils einem oder mehreren Blöcken anlegen.

Die Datentypen der jeweiligen Blöcke müssen Sie über die Tastatur eintippen. Sie werden nicht in der Auswahlliste angezeigt. Groß-/Kleinschreibung spielt bei der Eingabe der Datentypen keine Rolle.

Gehen Sie zum Anlegen von IF_CONF folgendermaßen vor:

1. Legen Sie einen Datenbaustein vom Typ "Global-DB" mit Bausteinzugriff "Standard" an.
2. Legen Sie in der Tabelle der Parameterkonfiguration des DB eine Struktur an (Datentyp "Struct").

   Den Name können Sie frei festlegen.
3. Fügen Sie unter dieser Struktur einen Header ein, indem Sie den Namen des Headers vergeben und in die Zelle des Datentyps "IF_CONF_Header" eintippen.

   Der Header der Struktur mit seinen drei Parametern (siehe unten) wird angelegt.
4. Legen Sie einen Block für den ersten zu ändernden Parameter an, indem Sie den gewünschten Datentyp (bspw. "IF_CONF_APN") in die Zelle des Datentyps eintippen.
5. Wiederholen Sie den letzten Schritt für all diejenigen Parameter, die Sie mithilfe der Anweisung TC_CONFIG im CP ändern wollen.
6. Aktualisieren Sie abschließend im Header die Blockanzahl im Parameter "subfieldCnt".

Header von IF_CONF

Tabelle 5- 1 IF_CONF_Header

Byte	Parameter	Datentyp	Anfangswert	Beschreibung
0 ... 1	fieldType	UINT		Blocktyp: Muss immer 0 sein.
2 ... 3	fieldId	UINT		Block-ID: Muss immer 0 sein.
4 ... 5	subfieldCnt	UINT		Gesamtanzahl der in der Struktur enthaltenen Blöcke

Allgemeine Parameter der Parameterblöcke

Jeder Block enthält folgende allgemeine Parameter:

- Id

  Dieser Parameter kennzeichnet den jeweiligen Block und darf nicht verändert werden.
- Length

  Dieser Parameter gibt die Länge des Blocks an. Der Wert dient nur Informationszwecken.

  Blöcke mit Strings und / oder Arrays haben eine variable Länge. Durch versteckte Bytes kann die tatsächliche Länge von Blöcken größer als die Summe der angezeigten Parameter sein.
- Mode

  Für diesen Parameter sind die folgenden Werte zulässig:

Tabelle 5- 2 Werte von "Mode"

Wert	Bedeutung
1	Permanente Gültigkeit der Projektierungsdaten Nicht relevant beim CP
2	Temporäre Gültigkeit der Projektierungsdaten einschließlich Löschen vorhandener permanenter Projektierungsdaten Die permanenten Projektierungsdaten werden durch die Parameterblöcke von IF_CONF ersetzt.

"APN-Einstellungen"

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Mobilfunk-Kommunikationseinstellungen".

Tabelle 5- 3 IF_CONF_APN

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	4	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 174
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
AccesspointGPRS	STRING [98]		APN: Name des Zugangspunkts vom Mobilfunknetz zum Internet
AccesspointUser	STRING [42]		APN-Benutzername
AccesspointPassword	STRING [22]		APN-Passwort

"CP-Identifikation"

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Security".

Tabelle 5- 4 IF_CONF_Login

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	5	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 54
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
ModemName	STRING [22]		Zugangs-ID
ModemPassword	STRING [22]		Telecontrol-Passwort

"Telecontrol-Server"

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Partnerstationen".

Dieser Block ist zu verwenden, wenn der Telecontrol-Server mit einem über DNS auflösbaren Namen adressiert wird oder wenn die IP-Adresse als String hinterlegt werden soll.

Tabelle 5- 5 IF_CONF_TCS_Name

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	6	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 266
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
TcsName	-	-	- reserviert -
	STRING [254]		Durch DNS auflösbarer Name des Telecontrol-Servers oder IP-Adresse als String
RemotePort	UINT		Port des Telecontrol-Servers
Rank	UINT		Priorität des Servers [1, 2] 1 = Erster Telecontrol-Server, 2 = Zweiter Telecontrol-Server (zweiter Server nicht relevant)

"SMSC"

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Mobilfunk-Kommunikationseinstellungen" > "Dienste und Einstellungen".

Tabelle 5- 6 IF_CONF_SMS_Provider

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	10	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 28
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
SMSProvider	STRING [20]		Teilnehmernummer der SMS-Zentrale (SMSC) des Mobilfunk-Netzwerkbetreibers, mit dem der Mobilfunk-Vertrag für diese Station abgeschlossen wurde.

"PIN"

In STEP 7 befinden sich die PIN im Parameterbereich "Mobilfunk-Kommunikationseinstellungen" > "Dienste und Einstellungen".

Tabelle 5- 7 IF_CONF_PIN

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	11	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 16
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
Pin	STRING [8]		PIN der im CP gesteckten SIM-Karte Der Parameter ist nicht relevant, wenn die PIN richtig projektiert wurde. Bei falsch projektierter PIN kann die richtige PIN hiermit eingegeben werden.

"Autorisierte Rufnummer"

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Security".

Tabelle 5- 8 IF_CONF_WakeupList

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	13	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 246
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
WakeupPhone [1...10]	ARRAY [1...10] of STRING [22]		Rufnummer des zum Wecken autorisierten Teilnehmers Der Stern (*) am Ende einer Rufnummer dient als Platzhalter für Durchwahlnummern.

"Bevorzugte Mobilfunknetze"

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Mobilfunk-Kommunikationseinstellungen".

Tabelle 5- 9 IF_CONF_PrefProvider

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	14	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 46
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
Provider [1...5]	ARRAY [1...5] of STRING [6]		Alternative Mobilfunknetze mit Priorität 1 bis 5, in die sich der CP bevorzugt einwählt. Bis zu 5 Netze sind projektierbar. Nr. 1 mit höchster Priorität, Nr. 5 mit niedrigster Priorität. Eingabe des Public Land Mobile Network (PLMN) des Netzwerkbetreibers, bestehend aus Mobile Country Code (MCC) und Mobile Network Code (MNC). Beispiel (Testnetz der Siemens AG): 26276

TeleService-Zugang (DNS-Name / IP-Adresse des Servers)

Zugangsdaten des TeleService-Servers (Vermittlerstation).

In STEP 7 befinden sich die entsprechenden Daten im Parameterbereich "Mobilfunk-Kommunikationseinstellungen".

Mit IF_CONF_TS_Name kann nur ein in STEP 7 projektierter TeleService-Server geändert werden, aber kein neuer angelegt werden. Beim Versuch, die Konfiguration eines TeleService-Servers mit dem Baustein anzulegen, wird an TC_CONFIG der interne Fehler 80E0 ausgegeben.

Tabelle 5- 10 IF_CONF_TS_Name

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	20	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 266
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
ts_name	String [254]		Durch DNS auflösbarer Name des TeleService-Servers oder IP-Adresse als String
RemotePort	UINT		Port der Engineering-Station
Rank	UINT		Priorität des Servers [1] oder [2]: • 1 = Server 1 • 2 = Server 2 (nicht relevant)

Diagnose und Instandhaltung

6

6.1 Diagnosemöglichkeiten

Nachfolgende Diagnosemöglichkeiten stehen Ihnen zur Verfügung.

LEDs der Baugruppe

Informationen zu den LED-Anzeigen finden Sie im Kapitel LEDs (Seite 28).

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.

Wenn Sie Online-Diagnose mit der Station über den CP betreiben wollen, dann müssen die Online-Funktionen in der Parametergruppe "Kommunikationsarten" aktiviert sein.

Gruppe "Diagnose"

Hier erhalten Sie folgende statische Informationen zur selektierten Baugruppe:

- Allgemeine Informationen zur Baugruppe

  Allgemeine Angaben zur Baugruppe
- Diagnosestatus

  Angaben zum Diagnosestatus
- Ethernet-Schnittstelle

  Adress- und statistische Angaben

- Industrial Remote Communication

  Hier erhalten Sie spezifische Informationen zur WAN-Schnittstelle und weiteren Parametern des CP. Der Eintrag hat folgende Untereinträge:

  – Partner

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

  – Mobilfunk-Schnittstelle

    Diagnoseinformationen zum Netz, statistische Verbindungsinformationen, Angaben zu empfangenen/gesendeten Nachrichten

  – Datenpunktliste

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

  – Protokolldiagnose

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

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

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

  – Gerätespezifische Ereignisse

    Angaben zu CP-internen Ereignissen

- Uhrzeit

  Angaben zur Uhrzeit im Gerät

Gruppe "Funktionen"

- 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 von der Siemens-Hotline ausgewertet werden kann.

Diagnosemöglichkeiten über den Webserver der CPU

Details zu den Diagnosemöglichkeiten des Webservers finden Sie im S7-1200-Systemhandbuch, siehe /1/ (Seite 117).

Diagnose-SMS

Der CP schickt eine Diagnose-SMS an ein Telefon mit autorisierter Rufnummer, wenn er von diesem Telefon eine SMS mit folgendem Text erhält:

`CPDIAG`

Die daraufhin gesendete Diagnose-SMS enthält folgende Daten der S7-Station:

- Firmware-Version des CP
- Betriebszustand der CPU (RUN / STOP)
- Status der Mobilfunknetz-Verbindung

  Wertebereich und Bedeutung:

  – 0 = Aus dem Netz ausgebucht
  – 1 = Falsche PIN
  – 2 = Falsche SIM-Karte
  – 3 = Wartet auf PIN / keine PIN projektiert
  – 4 = In das Netz eingebucht
- Datum und Uhrzeit der letzten Einwahl in das Mobilfunknetz

  Die Daten werden im ISO 8601-Format angegeben ("Attach: JJJJ-MM-TT hh:mm:ss").

  Wenn die Uhrzeit des CP zum Zeitpunkt der Einwahl noch nicht synchronisiert war, dann wird als Zeitpunkt das voreingestellte Datum des CP (01.01.2000) übertragen.

  Wenn der letzte Einwahlversuch in das Mobilfunknetz nicht erfolgreich war, dann wird "Attach: -" übertragen.
- Name des aktuellen Mobilfunknetzes
- IP-Adresse des CP
- Signalstärke des Mobilfunknetzes
  – good: Gute Signalqualität (-73 ... -51 dBm)
  – medium: Mittlere Signalqualität (-89 ... -74 dBm)
  – weak: Schlechte Signalqualität (-109 ... -90 dBm)
  – no signal: Signal zu schwach für Empfang (≤ -110 dBm)
- Received Signal Strength Indication (RSSI) - Empfangsfeldstärke an der Station [0 ... 31]
- Verbindungszustand zum Telecontrol-Server

Wenn die zu sendenden Daten die Standardgröße einer SMS übersteigen, dann werden mehrere SMS versendet.

Diagnosemöglichkeiten des Telecontrol-Servers

Zur Telecontrol-Kommunikation bietet TCSB einige Diagnosemöglichkeiten, die Sie bei Problemen im Produktivbetrieb nutzen sollten.

Bei Verbindungsproblemen zwischen Station und Telecontrol-Server können Sie über die folgenden Systemvariablen schrittweise die Verbindung prüfen:

- ConnectionState
- PLCConnected
- PLCCpuState

Ausgefallene Mobilfunkübertragung

Wenn die Mobilfunkübertragung nicht funktioniert, aber alle anderen Einstellungen und Anschlüsse korrekt sind, dann prüfen Sie die externe Spannungsversorgung des CP.

TeleService

Die Beschreibung der TeleService-Funktionen finden Sie im jeweiligen Projektierungshandbuch, siehe /3/ (Seite 118).

6.2 Online-Security-Diagnose über Port 8448

Security-Diagnose über Port 8448

Voraussetzungen:

- 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.

6.3 Bearbeitungsstatus von Nachrichten

Bearbeitungsstatus

Wenn die Option "Kennung für Bearbeitungsstatus aktivieren" im Nachrichteneditor für eine Nachricht aktiviert ist, dann wird ein Status am CP ausgegeben, der Auskunft über den Bearbeitungszustand der gesendeten Nachricht gibt. Der Status wird in eine PLC-Variable vom Typ DWORD geschrieben. Wählen Sie diese Variable über das Feld "PLC-Variable für Bearbeitungsstatus" aus.

Der Bearbeitungsstatus wird nach der Übergabe einer zu sendenden Nachricht vom Modul selbst oder den Servern des Dienstes zurückgeliefert.

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

Die gelieferten Status der im Nachrichteneditor projektierten Nachrichten haben folgende Bedeutung:

Tabelle 6- 1 SMS: Bedeutung der hexadezimal ausgegebenen Statuskennung

Status	Bedeutung
0000	Übertragung fehlerfrei abgeschlossen
0001	Fehler bei der Übertragung; mögliche Ursachen: • SIM-Karte nicht gültig • Kein Netz • Falsche Zielrufnummer (Nummer nicht erreichbar)

Tabelle 6- 2 E-Mails: Bedeutung der hexadezimal ausgegebenen Statuskennung

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

Status	Bedeutung
84xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht der Status 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: Nachrichtenkonfiguration > Nachrichtenparameter: • Empfängeradresse ("An" bzw. "Cc").
8502	Syntax-Fehler. Überprüfen Sie die folgenden Projektierungsdaten: Nachrichtenkonfiguration > Nachrichtenparameter: • E-Mail-Adresse (Absender)
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: • CP-Projektierung > E-Mail-Projektierung: – Benutzername – Passwort – E-Mail-Adresse (Absender) • Nachrichtenkonfiguration > Nachrichtenparameter: – Empfängeradresse ("An" bzw. "Cc").
8554	Übertragung fehlgeschlagen
85xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht der Status der dreistelligen Fehlernummer des Protokolls SMTP.

6.4 Firmware laden

Hinweis

CPU-STOP

Setzen Sie die CPU immer in den Betriebszustand STOP, bevor Sie eine neue Firmware-Datei in den CP laden.

Neue Firmware-Versionen des CP

Wenn für die Baugruppe eine neue Firmware-Version zur Verfügung steht, dann finden Sie diese auf den Internet-Seiten des Siemens Industry Online Support unter folgender Adresse: Link: (https://support.industry.siemens.com/cs/ww/de/ps/15924/dl)

Beachten Sie, dass Firmware-Versionen ab V3 nicht auf CPs mit Hardware-Erzeugnisstand 1 geladen werden können.

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 Internetseite des Siemens Industry Online Support.

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

Hinweis

Auswirkungen auf den remanenten Speicher der CPU

- Wenn Sie für die Installation der Firmware-Datei eine SIMATIC Memory Card verwenden, bleibt der remanente Speicher erhalten.
- Wenn Sie die Online-Funktionen für die Installation der Firmware-Datei verwenden, geht der remanente Speicher verloren.

Den Vorgang des Firmware-Ladens erkennen Sie am Blinken der LEDs des CP, siehe LEDs (Seite 28).

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

Voraussetzungen:

- Der CP ist über seine IP-Adresse erreichbar.
- Die Engineering-Station und der CP liegen im gleichen Subnetz.
- Die neue Firmware-Datei ist auf Ihrer Engineering-Station gespeichert.

Vorgehensweise:

1. Verbinden Sie die Engineering-Station mit dem Netz.
2. Öffnen Sie auf der Engineering-Station das betreffende STEP 7-Projekt.
3. Selektieren Sie den CP oder die CPU derjenigen Station, dessen CP Sie mit einer neuen Firmware aktualisieren wollen.
4. Aktivieren Sie die Online-Funktionen über das Symbol "Online verbinden".
5. Selektieren Sie im Dialog "Online verbinden" in der Auswahlliste "Typ der PG/PC-Schnittstelle" die Ethernet-Schnittstelle "PN/IE".
6. Selektieren Sie den Steckplatz des CP oder der CPU.

   Beide Wege sind möglich.

7. Verbinden Sie sich über die Schaltfläche "Verbinden".

Der Wizard "Online verbinden" führt Sie durch die weiteren Schritte.

Weitere Hilfe zu den Online-Funktionen bietet Ihnen das STEP 7-Informationssystem.

6.5 Baugruppentausch

Baugruppentausch

⚠WARNUNG

Lesen Sie das Systemhandbuch "S7-1200 Automatisierungssystem"

Lesen Sie vor der Montage, dem Anschließen und der Inbetriebnahme die entsprechenden Abschnitte im Systemhandbuch "S7-1200 Automatisierungssystem" (siehe Literaturverweis im Anhang).

Gehen Sie bei der Montage und dem Anschließen entsprechend den Beschreibungen im Systemhandbuch "S7-1200 Automatisierungssystem" vor.

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

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

Beim Wiederanlauf der Station liest der neue CP die Projektdaten 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.

Bei Austausch des Geräts gegen ein neueres werden nicht die neuesten Sicherheitsstandards unterstützt, sondern diejenigen des ausgetauschten Geräts.

Denken Sie beim Baugruppentausch daran, die SIM-Karte vom alten in den neuen CP zu übernehmen.

Technische Daten

7

7.1 Allgemeine technische Daten

Tabelle 7- 1 Allgemeine technische Daten

Technische Daten		
Modulnamen	**Artikelnummern**	
• CP 1243-7 LTE-EU	• 6GK7 243-7KX30-0XE0	
• CP 1243-7 LTE-US	• 6GK7 243-7SX30-0XE0	
Antennenanschluss		
Antennenanschluss	Anzahl	1
	Ausführung	SMA-Buchse
	Impedanz nominal	50 Ω
	Antennenkabel, maximal zulässige Länge	≤ 30 m
Elektrische Daten		
Externe Spannungsversorgung	Versorgungsspannung	DC 24 V
	Zulässiger Bereich	19,2 ... 28,8 V
	Ausführung	Klemmenblock mit Stecker, 3-polig
	Leitungsquerschnitt	
	• Minimal	• 0,14 mm^2 (AWG 25)
	• Maximal	• 1,5 mm^2 (AWG 15)
	Max. Anzugsmoment der Schraubklemmen	0,45 Nm (4 lb.in.)
	Potenzialtrennung:	
	Netzteil gegen interne Schaltung	DC 710 V für 1 Minute
Stromaufnahme (typisch)	Aus DC 24 V (extern)	120 mA
	Aus dem S7-1200-Rückwandbus	150 mA
Verlustwirkleistung (typisch)	Aus DC 24 V (extern)	1,8 W
	Aus dem S7-1200-Rückwandbus	0,5 W
Zulässige Umgebungsbedingungen		
Umgebungstemperatur	Während Betrieb bei waagerechtem Aufbau des Baugruppenträgers (Hutschiene waagerecht)	-20 °C ... +70 °C
	Während Betrieb bei senkrechtem Aufbau des Baugruppenträgers (Hutschiene senkrecht)	-20 °C ... +60 °C
	Während Lagerung	-40 °C ... +70 °C
	Während Transport	-40 °C ... +70 °C
Relative Luftfeuchte	Während Betrieb	≤ 95 % bei 25 °C, ohne Kondensation
Bauform, Maße und Gewicht		
Baugruppenformat	Kompaktbaugruppe S7-1200, einfach breit	
Schutzart	IP20	

Technische Daten	
Gewicht	
• Nettogewicht	• 133 g
• Gewicht inklusive Verpackung	• 170 g
Abmessungen (B x H x T)	30 x 100 x 75 mm
Montagemöglichkeiten	• 35 mm DIN-Hutschiene • Schalttafel

Weitere Funktionen und Leistungsdaten finden Sie im Kapitel Anwendung und Funktionen (Seite 11).

7.2 Technische Daten - Funkschnittstelle (CP 1243-7 LTE-EU)

Tabelle 7- 2 Technische Daten der Funkschnittstelle

Technische Daten - CP 1243-7 LTE-EU		
Artikelnummer	6GK7 243-7KX30-0XE0	
Funkschnittstelle		
Unterstützte Frequenzbänder	Mobilfunkstandard	Band-Nr. / Frequenz
	LTE FDD	• 1 / 2100 MHz • 3 / 1800 MHz • 7 / 2600 MHz • 8 / 900 MHz • 20 / 800 MHz • 28A / 700 MHz
	HSDPA+	• 1 / 2100 MHz • 3 / 1800 MHz • 8 / 900 MHz
	GSM / GPRS / EDGE	3 / 1800 MHz 8 / 900 MHz
Maximale Sendeleistung	4G / LTE FDD	+23 dBm (Class 3)
	3 G / WCDMA	+21 dBm (Class 3)
	EDGE LB	+27 dBm (Class E2)
	EDGE HB	+26 dBm (Class E2)
	GSM LB	+33 dBm (Class 4)
	GSM HB	+30 dBm (Class 4)
	TD-SCDMA	+21 dBm (Class 3)
LTE	Übertragungsgeschwindigkeit (maximal)	• Downlink: 150 Mbit/s • Uplink: 50 Mbit/s
HSPA+	Übertragungsgeschwindigkeit (maximal)	• Downlink (HSDPA): 42 Mbit/s • Uplink (HSUPA): 42 Mbit/s

Technische Daten - CP 1243-7 LTE-EU		
EDGE	Eigenschaften	• Multislot-Klasse 10 Endgeräteklasse B Kodierungsschema 1 ... 9 (GMSK)
	Übertragungsgeschwindigkeit (maximal)	• Downlink: 236,8 kbit/s • Uplink: 236,8 kbit/s
GPRS	Eigenschaften	• Multislot-Klasse 10 Endgeräteklasse B Kodierungsschema 1...4 (GMSK)
	Übertragungsgeschwindigkeit (maximal)	• Downlink: 85,6 kbit/s • Uplink: 85,6 kbit/s
SMS	Betriebsmodus abgehend	MO
	Dienst	Punkt zu Punkt

7.3 Technische Daten - Funkschnittstelle (CP 1243-7 LTE-US)

Tabelle 7- 3 Technische Daten der Funkschnittstelle

Technische Daten - CP 1243-7 LTE-US		
Artikelnummer	6GK7 243-7SX30-0XE0	
Unterstützte Frequenzbänder	Mobilfunkstandard	Band-Nr. / Frequenz
	LTE FDD	2 / 1900 MHz 4 / 1700 MHz 5 / 850 MHz 12 / 700 MHz 13 / 700 MHz 14 / 700 MHz 66 / 1700 MHz 71 / 617-698 MHz
	HSDPA+	2 / 1900 MHz 4 / 1700 MHz 5 / 850 MHz
Maximale Sendeleistung	4G / LTE FDD	+23 dBm (Class 3)
	3 G / WCDMA	+21 dBm (Class 3)
	TD-SCDMA	+21 dBm (Class 3)
LTE	Übertragungsgeschwindigkeit (maximal)	• Downlink: 100 Mbit/s • Uplink: 50 Mbit/s
HSPA+	Übertragungsgeschwindigkeit (maximal)	• Downlink (HSDPA): 42 Mbit/s • Uplink (HSUPA): 42 Mbit/s
SMS	Betriebsmodus abgehend	MO
	Dienst	Punkt zu Punkt

7.4 Belegung der Buchse für die externe Spannungsversorgung

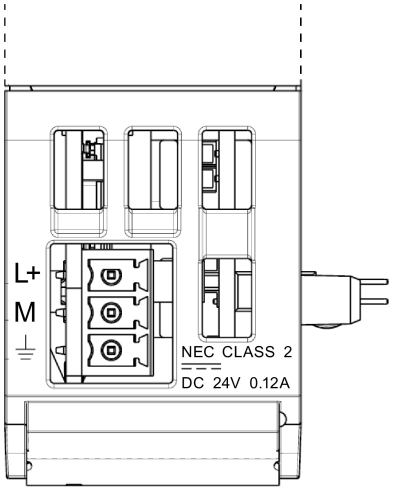


Bild 7-1 Buchse für die externe Spannungsversorgung DC 24 V (Draufsicht)

Tabelle 7- 4 Belegung der Buchse für die externe Spannungsversorgung

Pin	Beschriftung	Funktion
1	L+	DC + 24 V
2	M	Bezugsmasse zu DC + 24 V
3	⏚	Erdungsanschluss

Maßzeichnungen

A

Hinweis

Alle Maßangaben in den Zeichnungen des CP in Millimetern.

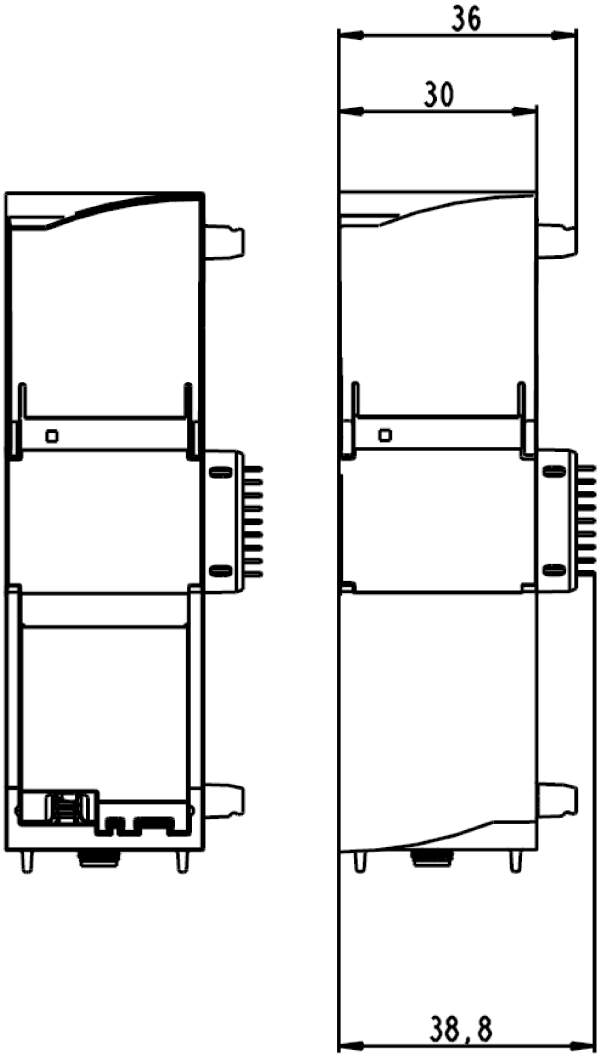


Bild A-1 Vorderansicht

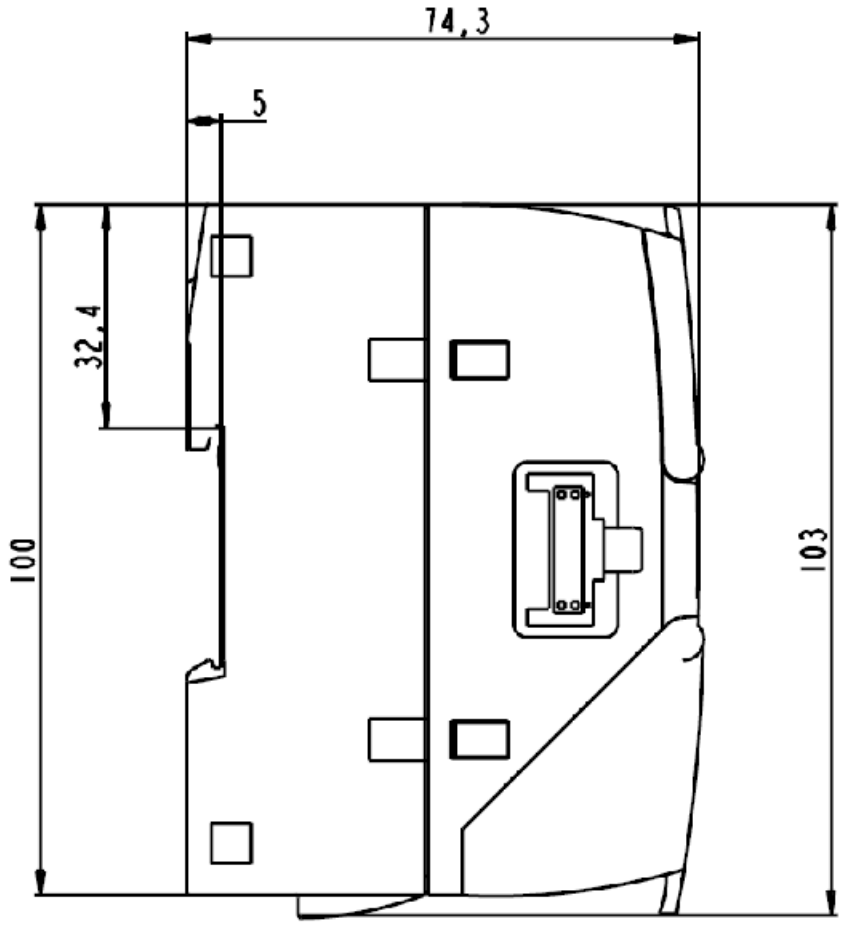


Bild A-2 Seitenansicht links

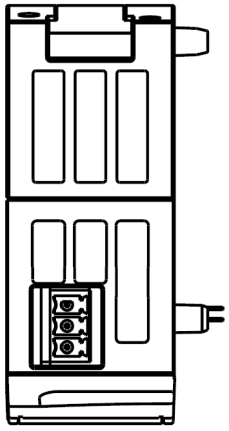


Bild A-3 Draufsicht

Zulassungen

B

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.

EU-Konformitätserklärung

CE

Gültig nur für CP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

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

- **2014/53/EU (Funkanlagen / Telekommunikations-Richtlinie)**

  Richtlinie des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG

- **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

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 Nürnberg
Deutschland

Die EU-Konformitätserklärung zu diesem Produkt finden Sie im Internet unter folgender Adresse:

Link: (https://support.industry.siemens.com/cs/ww/de/ps/15924/cert)
Filtereinstellungen: Zertifikatart: "EU-Konformitätserklärung"

IECEx

Das Produkt erfüllt die Anforderungen an den Explosionsschutz nach IECEx.

IECEx-Klassifikation:

- Ex ec IIC T4 Gc

  Zertifikat: IECEx DEK 18.0018X

  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/15924/cert)

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx (Seite 35) 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 0026X

  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 Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx (Seite 35) 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)

R&TTE

Der CP erfüllt die Anforderungen der EG-Richtlinie 1999/5/EG "Funkanlagen und Telekommunikations-Endeinrichtungen" gemäß den Anforderungen nach Art. 3 (1) a, 3 (1) b und 3 (2).

Art. 3 (1) a - Gesundheit und Sicherheit

Harmonisierte Normen:

- EN 60950-1+A11+A1+A12+A2

  Einrichtungen der Informationstechnik - Sicherheit - Teil 1: Allgemeine Anforderungen

- EN 62311

  Bewertung von elektrischen und elektronischen Einrichtungen in Bezug auf Begrenzungen der Exposition von Personen in elektromagnetischen Feldern (0 Hz ... 300 GHz)

Art. 3 (1) b - EMV

Harmonisierte Normen:

- ETSI EN 301 489-1 V1.9.2

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Elektromagnetische Verträglichkeit für Funkeinrichtungen und -dienste - Teil 1: Gemeinsame technische Anforderungen

- ETSI EN 301 489-3 V1.6.1

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Elektromagnetische Verträglichkeit (EMV) für Funkeinrichtungen und -dienste - Teil 3: Spezifische Bedingungen für Funkgeräte geringer Reichweite (SRD) für den Einsatz auf Frequenzen zwischen 9 kHz und 246 GHz

- ETSI EN 301 489-7 V1.3.1

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Elektromagnetische Verträglichkeit für Funkeinrichtungen und -dienste - Teil 7: Spezifische Bedingungen für mobile und transportable Funk- und Zusatz-/Hilfseinrichtungen digitaler zellularer Funk-Telekommunikationssysteme (GSM und DCS)

- ETSI EN 301 489-24 V1.5.1

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Elektromagnetische Verträglichkeit für Funkeinrichtungen und -dienste - Teil 24: Spezifische Bedingungen für mobile und transportable IMT-2000 CDMA-Direkt-Spreizspektrum-(UTRA-)Funkeinrichtungen und Zusatz-/Hilfseinrichtungen

- EN 61000-6-1

  Elektromagnetische Verträglichkeit (EMV) - Teil 6-1: Fachgrundnormen - Störfestigkeit für Wohnbereich, Geschäfts- und Gewerbebereiche sowie Kleinbetriebe

- EN 61000-6-2+AC

  Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche

- EN 61000-6-3+A1+AC

  Elektromagnetische Verträglichkeit (EMV) - Teil 6-3: Fachgrundnormen - Störaussendung für Wohnbereich, Geschäfts- und Gewerbebereiche sowie Kleinbetriebe

- EN 61000-6-4+A1

  Elektromagnetische Verträglichkeit (EMV) - Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche

- EN 55022+AC Class A / B

  Einrichtungen der Informationstechnik - Funkstöreigenschaften - Grenzwerte und Messverfahren

- EN 55024

  Einrichtungen der Informationstechnik - Störfestigkeitseigenschaften - Grenzwerte und Prüfverfahren

Art. 3 (2) - Maßnahmen zur effizienten Nutzung des Frequenzspektrums

Harmonisierte Normen:

- ETSI EN 300 440-2 V1.4.1

  Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Funkanlagen mit geringer Reichweite - Funkgeräte zum Betrieb im Frequenzbereich von 1 GHz bis 40 GHz. Teil 2: Harmonisierte Norm, welche die wesentlichen Anforderungen nach Artikel 3.2 der R&TTE-Richtlinie enthält.

- ETSI EN 301 511 V9.0.2

  Globales System für mobile Kommunikation (GSM). Harmonisierte Norm für Mobiltelefone im GSM 900- und GSM 1800-Band, welche die wesentlichen Anforderungen nach Artikel 3.2 der R&TTE- Richtlinie enthält.

- ETSI EN 301 908-1 V6.2.1

  IMT zellulare Netze - Harmonisierte Norm, welche die wesentlichen Anforderungen nach Artikel 3.2 der R&TTE-Richtlinie enthält. Teil 1: Einleitung und gemeinsame Anforderungen

- ETSI EN 301 908-2 V6.2.1

  IMT zellulare Netze. Harmonisierte Norm, welche die wesentlichen Anforderungen nach Artikel 3.2 der R&TTE-Richtlinie enthält. Teil 2: CDMA Direct Spread (UTRA FDD) Endgeräte (UE)

- ETSI EN 301 908-13 V6.2.1

  IMT zellulare Netze. Harmonisierte Norm, welche die wesentlichen Anforderungen nach Artikel 3.2 der R&TTE-Richtlinie enthält. Teil 13: Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment (UE)

Maximaler Antennengewinn

Benutzer und Installateure müssen Installationshinweise für die Antenne und die Bedingungen für den Betrieb der Sendeanlage erhalten, die einzuhalten sind, um der zulässigen HF-Exposition zu genügen.

Beachten Sie hierzu die technischen Daten der Antenne, siehe Anhang Zubehör (Seite 115).

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

cULus

Underwriters Laboratories, Inc. erfüllt

- 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. 61010-1-12 / CSA-IEC 61010-2-201

cULus HAZ.LOC.

Underwriters Laboratories, Inc. erfüllt

- ANSI ISA 12.12.01

  Nonincendive Electrical Equipment for Use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations
- CAN CSA C22.2 No. 213-M1987, 1st Ed. (R2013)
- Non-Incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4A; Ta = -20 °C...70 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...70 °C

FM

Factory Mutual Research (FM)
Zertifizierungsnorm-Klasse Nr. 3600 und 3611
Zugelassen für den Einsatz in:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 70 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 70 °C

Antennen

Die zugelassenen Antennen für den Mobilfunkbetrieb hängen ab vom Hardware-Erzeugnisstand des CP. Die zugelassenen Antennen finden Sie im Anhang Zubehör (Seite 115).

Nationale Funkzulassungen

Für den Betrieb des CP in einigen Ländern müssen Zulassungen für den Funkbetrieb vorliegen, die vereinbarte Kennzeichnung auf dem Typschild vorhanden sein und spezielle Hinweise für das jeweilige Land beachtet werden. Einige Länderzulassungen und Hinweise sind nachfolgend aufgeführt.

USA

Gültig nur für CP 1243-7 LTE-US (6GK7 243-7SX30-0XE0)

- **FCC**

  7layers Report Reference: MDE_SIEM_1308_FCCb

  Test Specification:

  – PART 2 - GENERAL RULES AND REGULATIONS

  – PART 15 - RADIO FREQUENCY DEVICES

  FCC statement:
  "This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
  (1) This device may not cause harmful interference, and
  (2) this device must accept any interference received, including interference that may cause undesired operation.
  Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment."

  Additional statement for Digital Devices / Computer Peripheral Devices
  FCC §15.105 statement:
  "This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help."

- **Network Compatibility**

  AT&T-Zulassung

Kanada

Gültig nur für CP 1243-7 LTE-US (6GK7 243-7SX30-0XE0)

Approval IDs:

- ICTA: 5131-LE910NA
- FCC: RI7LE910NA

IC statement:

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received,
including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi,
même si le brouillage est susceptible d'en compromettre le fonctionnement.

Südafrika

Gültig nur für CP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

Approval Number TA-2015/1864

EAC (Eurasian Conformity)

Gültig nur für CP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

Zollunion von Russland, Weißrussland und Kasachstan

Deklaration der Konformität gemäß technischer Vorschriften der Zollunion:

- TR CU
- RF Telecom

Mexico

Gültig nur für CP 1243-7 LTE-US (6GK7 243-7SX30-0XE0)

La operación de este equipo está sujeta a las siguientes dos condiciones:

(1) es posible que este equipo o dispositivo no cause interferencia perjudicial y

(2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Länderspezifische Mobilfunkzulassungen von SIMATIC NET-Geräten

Eine Übersicht der länderspezifischen Mobilfunkzulassungen von SIMATIC NET-Geräten finden Sie hier:
Link: (www.siemens.de/mobilfunkzulassungen)

Weitergehende Auskünfte zu länderspezifischen Mobilfunkzulassungen von SIMATIC NET-Geräten bekommen Sie beim Siemens Industry Online Support:
Link: (http://www.siemens.de/automation/support-request)

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: (https://support.industry.siemens.com/cs/ww/de/ps/15924/cert)

Zubehör

C

Abhängig vom Hardware-Erzeugnisstand ist der CP zusammen mit den folgenden Antennen für den Mobilfunkbetrieb zugelassen.

C.1 Antenne für CP ab Hardware-Erzeugnisstand 3

Für den Einsatz in Mobilfunknetzen steht folgende Antenne zur Montage im Innen- oder Außenbereich zur Verfügung. Die Antenne ist separat zu bestellen.

Antenne ANT896-4ME

Bild C-1 Antenne ANT896-4ME

Kurzbezeichnung	Bestell-Nr.	Erläuterung
ANT896-4ME	6GK5896-4ME00-0AA0	Rundstrahlantenne für LTE-Netze (4G), GSM-Netze (2G) und UMTS-Netze (3G), omnidirektional, witterungsbeständig für Innen- und Außenbereich, IP68, - 40 °.. + 70 °C, N-Connect female, inkl. Dichtung, Zahnscheibe und Mutter.

Das Anschlusskabel ist separat zu bestellen, siehe Antennenzubehör.

Detaillierte Informationen finden Sie in der Dokumentation des Geräts. Diese finden Sie im Internet auf den Seiten des Siemens Industry Online Support unter folgender Adresse:

Link: (https://support.industry.siemens.com/cs/ww/de/view/100699507)

C.2 Antenne für CP bis Hardware-Erzeugnisstand 2

Antenne ANT794-4MR

Für den Einsatz in Mobilfunknetzen steht die Quadband-Antenne ANT794-4MR zur Verfügung. Sie kann innerhalb und außerhalb von Gebäuden installiert werden.

Die Antenne ist separat zu bestellen.

Bild C-2 GSM/GPRS-Antenne ANT794-4MR

Kurzbezeichnung	Bestell-Nr.	Erläuterung
ANT794-4MR	6NH9 860-1AA00	Rundstrahlantenne für LTE-Netze (4G), GSM-Netze (2G) und UMTS-Netze (3G), omnidirektional, witterungsbeständig für Innen- und Außenbereich, 5 m Anschlusskabel fest mit der Antenne verbunden, SMA-Stecker, inkl. Montagewinkel, Schrauben, Dübel.

Detaillierte Informationen finden Sie in der Dokumentation des Geräts. Diese finden Sie im Internet auf den Seiten des Siemens Industrial Automation Customer Support:
Link: (https://support.industry.siemens.com/cs/ww/de/view/23119005)

Literaturverzeichnis

D

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
S7-1200 Automatisierungssystem
Systemhandbuch
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/de/ps/13683/man)

/2/

SIMATIC NET
CP 1243-7 LTE
Betriebsanleitung
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/de/ps/15924/man)

/3/

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/21764/man)

/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
SINEMA Remote Connect - Server
Betriebsanleitung
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/de/ps/21816/man)

Index

T

U

V

W

Z