SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet CP 1543-1

Betriebsanleitung

Vorwort

Wegweiser Dokumentation 1

Produktübersicht, Funktionen 2

Montage, Anschluss, Inbetriebnahme, Betrieb 3

Projektierung, Programmierung 4

Diagnose und Instandhaltung 5

Technische Daten 6

Zulassungen 7

05/2017

C79000-G8900-C289-07

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
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C289-07
℗ 05/2017 Änderungen vorbehalten

Vorwort

Zweck der Dokumentation

Das vorliegende Handbuch ergänzt das Systemhandbuch S7-1500.

Die Informationen des vorliegenden Handbuchs und des Systemhandbuchs ermöglichen es Ihnen, den Kommunikationsprozessor in Betrieb zu nehmen.

Neu in dieser Ausgabe

- Firmware-Version V2.1 mit folgenden neuen Funktionen:
  - Erweiterte Security-Einstellungen bei IP-Routing über den Rückwandbus

    Siehe Kapitel IP-Routing (Seite 35).

Versionshistorie

Firmware-Version V2.0 mit folgenden neuen Funktionen:

- Secure OUC (Open User Communication) über TCP/IP
- Secure Mail: Neue Systemdatentypen (SDTs) für die Übertragung von E-Mails

  Alternativ: Ungesicherte Übertragung über Port 25 oder gesicherte Übertragung über Port 587
- Betrieb als FTP-Server: Zugriff auf die SIMATIC Memory Card der CPU
- IP-Routing über den Rückwandbus

Abgelöste Ausgabe

Ausgabe 10/2016

Aktuelle Handbuchausgabe im Internet

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

Link: (https://support.industry.siemens.com/cs/ww/de/ps/15340/man)

Weiterführende Literatur

Siehe Kapitel Wegweiser Dokumentation (Seite 9).

Abkürzungen und Bezeichnungen

- CP

  In diesem Dokument wird nachfolgend auch die Bezeichnung "CP" stellvertretend für die vollständige Produktbezeichnung verwendet.

- STEP 7

  Für das Projektierungswerkzeug STEP 7 Professional wird stellvertretend die Bezeichnung STEP 7 verwendet.

Konventionen

Beachten Sie auch die folgendermaßen gekennzeichneten Hinweise:

Hinweis

Ein Hinweis enthält wichtige Informationen zum in der Dokumentation beschriebenen Produkt, zur Handhabung des Produkts oder zu dem Teil der Dokumentation, auf den besonders aufmerksam gemacht werden soll.

Siehe auch

Programmbausteine für OUC (Seite 45)

Projektierung der FTP-Server-Funktion (Seite 51)

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 in folgendem Dokument, das sich auf dem mitgelieferten Datenträger befindet:

- OSS_CP15431_86.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 nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter folgender Adresse:
Link: (http://www.siemens.com/industrialsecurity)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter folgender Adresse:
Link: (http://www.siemens.com/industrialsecurity)

Firmware

Firmware

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

SIMATIC NET-Glossar

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

Sie finden das SIMATIC NET-Glossar im Internet unter folgender Adresse:

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

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)

Inhaltsverzeichnis

Vorwort ... **3**

1 Wegweiser Dokumentation ... **9**

2 Produktübersicht, Funktionen ... **11**

2.1 Produktdaten ... 11

2.2 Kommunikationsdienste ... 12

2.3 Weitere Funktionen ... 13

2.4 Industrial Ethernet Security ... 15

2.5 Mengengerüst und Leistungsdaten ... 16
2.5.1 Allgemeine Kenndaten ... 16
2.5.2 Kenndaten für die Open User Communication (OUC) und FETCH/WRITE ... 16
2.5.3 Kenndaten S7-Kommunikation ... 18
2.5.4 Kenndaten für den FTP / FTPS-Betrieb ... 19
2.5.5 Kenndaten Security ... 19

2.6 Voraussetzungen für den Einsatz ... 20
2.6.1 Mengengerüst ... 20
2.6.2 Projektierung ... 20
2.6.3 Programmierung ... 21

2.7 LEDs ... 22

2.8 Gigabit-Schnittstelle ... 24

3 Montage, Anschluss, Inbetriebnahme, Betrieb ... **25**

3.1 Wichtige Hinweise zum Geräteeinsatz ... 25
3.1.1 Hinweise für den Einsatz im Ex-Bereich ... 25
3.1.2 Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx ... 26
3.1.3 Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc ... 27
3.1.4 Hinweise für den Einsatz im Ex-Bereich gemäß FM ... 27

3.2 Montage und Inbetriebnahme des CP 1543-1 ... 28

3.3 Betriebszustand der CPU - Rückwirkung auf CP ... 30

4 Projektierung, Programmierung ... **31**

4.1 Security-Empfehlungen ... 31

4.2 Netzwerkeinstellungen ... 34

4.3 IP-Konfiguration ... 35
4.3.1 Besonderheiten zur IP-Konfiguration ... 35
4.3.2 Wiederanlauf nach Erkennen einer IP-Doppeladressierung im Netzwerk ... 35
4.3.3 IP-Routing ... 35

4.4 Security ... 36
4.4.1 VPN ... 36
4.4.1.1 VPN-Tunnelkommunikation zwischen S7-1500-Stationen anlegen ... 37

4.4.1.2 VPN-Tunnelkommunikation zwischen CP 1543-1 und SCALANCE M erfolgreich aufbauen 40
4.4.1.3 VPN-Tunnelkommunikation mit SOFTNET Security Client 40
4.4.1.4 CP als passiver Teilnehmer von VPN-Verbindungen 41
4.4.2 Firewall 41
4.4.2.1 Firewall-Reihenfolge bei der Prüfung ein- und ausgehender Telegramme 41
4.4.2.2 Schreibweise der Quell-IP-Adresse (erweiterter Firewall-Modus) 41
4.4.2.3 HTTP und HTTPS über IPv6 nicht möglich 41
4.4.2.4 Firewall-Einstellungen für Verbindungen über VPN-Tunnel 42
4.4.3 Online-Funktionen 42
4.4.3.1 Online-Diagnose über Port 8448 42
4.4.3.2 Online-Diagnose und Laden in Station bei aktivierter Firewall 43
4.4.4 Filtern der System-Ereignisse 43
4.5 Uhrzeitsynchronisation 44
4.6 Programmbausteine für OUC 45
4.7 Einrichten der FTP-Kommunikation 48
4.7.1 Der Programmbaustein FTP_CMD (FTP-Client-Funktion) 48
4.7.2 Projektierung der FTP-Server-Funktion 51
4.8 IP-Zugriffsschutz bei programmierten Kommunikationsverbindungen 54
5 Diagnose und Instandhaltung 55
5.1 Diagnosemöglichkeiten 55
5.2 Diagnose über SNMP 55
5.3 Baugruppentausch ohne PG 58
6 Technische Daten 59
7 Zulassungen 61
Index 67

Wegweiser Dokumentation

1

Einleitung

Die Dokumentation der SIMATIC Produkte ist modular aufgebaut und enthält Themen rund um Ihr Automatisierungssystem.

Die komplette Dokumentation für das System S7-1500 besteht aus dem Systemhandbuch, Funktionshandbüchern und Gerätehandbüchern.

Außerdem unterstützt Sie das Informationssystem von STEP 7 (Online-Hilfe) bei der Projektierung und Programmierung Ihres Automatisierungssystems.

Übersicht der Dokumentation zur Kommunikation bei S7-1500

Die folgende Tabelle zeigt weitere Dokumente, die die vorliegende Beschreibung zum CP 1543-1 ergänzen und im Internet erhältlich sind.

Tabelle 1- 1 Dokumentation für den CP 1543-1

Thema	Dokumentation	Wichtigste Inhalte
Beschreibung des Systems	Systemhandbuch Automatisierungssystem S7-1500 (https://support.industry.siemens.com/cs/ww/de/view/59191792)	• Einsatzplanung • Montage • Anschließen • Inbetriebnehmen
Systemdiagnose	Funktionshandbuch Systemdiagnose (https://support.industry.siemens.com/cs/ww/de/view/59192926)	• Überblick • Diagnoseauswertung Hardware/Software
Kommunikation	Funktionshandbuch Kommunikation (https://support.industry.siemens.com/cs/ww/de/view/59192925)	• Überblick
	Funktionshandbuch Webserver (https://support.industry.siemens.com/cs/ww/de/view/59193560)	• Funktion • Bedienung
	Handbuch Industrial Ethernet Security (https://support.industry.siemens.com/cs/ww/de/ps/15326/man)	• Überblick und Beschreibung der Security-Funktionen in Industrial Ethernet

Thema	Dokumentation	Wichtigste Inhalte
	SIMATIC NET - Industrial Ethernet / PROFINET - Systemhandbuch • Industrial Ethernet Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465) • Passive Netzkomponenten Link: (https://support.industry.siemens.com/cs/ww/de/view/84922825)	• Ethernet-Netze • Netzprojektierung • Netzwerkkomponenten
Steuerungen störsicher aufbauen	Funktionshandbuch Steuerungen störsicher aufbauen (https://support.industry.siemens.com/cs/ww/de/view/59193566)	• Grundlagen • Elektromagnetische Verträglichkeit • Blitzschutz • Gehäuseauswahl
Zyklus- und Reaktionszeiten	Funktionshandbuch Zyklus- und Reaktionszeiten (https://support.industry.siemens.com/cs/ww/de/view/59193558)	• Grundlagen • Berechnungen

SIMATIC-Handbücher

Im Internet finden Sie alle aktuellen Handbücher zu SIMATIC-Produkten zum kostenlosen Download:
Link: (http://www.siemens.com/automation/service&support)

CP-Dokumentation auf der Manual Collection (Artikelnummer A5E00069051)

Die DVD "SIMATIC NET Manual Collection" enthält die zum Erstellungszeitpunkt aktuellen Gerätehandbücher und Beschreibungen aller SIMATIC NET-Produkte. Sie wird in regelmäßigen Abständen aktualisiert.

Versionshistorie/aktuelle Downloads für die SIMATIC NET S7-CPs

Im Dokument "Versionshistorie/aktuelle Downloads für die SIMATIC NET S7-CPs (Industrial Ethernet)" finden Sie Informationen über alle bisher lieferbaren CPs für SIMATIC S7 (Industrial Ethernet).

Die aktuelle Ausgabe des Dokuments finden Sie im Internet:
Link: (https://support.industry.siemens.com/cs/ww/de/view/109474421)

Produktübersicht, Funktionen

2

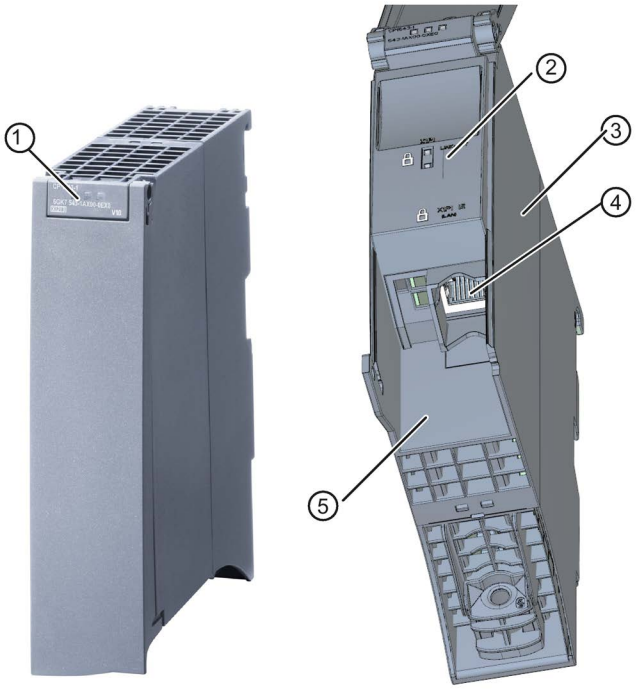
2.1 Produktdaten

Artikelnummer, Gültigkeit und Produktbezeichnungen

In dieser Beschreibung finden Sie Informationen zum Produkt

CP 1543-1
Artikelnummer 6GK7 543-1AX00-0XE0
Hardware-Erzeugnisstand 2
Firmware-Version V2.1
Kommunikationsprozessor für SIMATIC S7-1500

Ansicht des CP 1543-1



① LEDs für Status- und Fehleranzeigen
② LED-Anzeigen der Ethernet-Schnittstelle für Verbindungsstatus und Aktivität
③ Typenschild
④ Ethernet-Schnittstelle: 1 x 8-polige RJ45-Buchse
Schloss-Kennzeichnung symbolisiert Schnittstelle zum externen, unsicheren Subnetz.
⑤ Aufdruck MAC-Adresse

Bild 2-1 Darstellung des CP 1543-1 mit geschlossener (links) und geöffneter (rechts) Frontklappe

Adressaufdruck: Eindeutige MAC−Adresse für den CP voreingestellt

Der CP wird mit einer voreingestellten MAC-Adresse ausgeliefert:

Die MAC-Adresse ist auf dem Gehäuse aufgedruckt.

Falls Sie eine MAC-Adresse projektieren (ISO-Transportverbindungen), empfehlen wir Ihnen, die aufgedruckte MAC-Adresse bei der Baugruppenprojektierung zu übernehmen! Sie stellen damit eine eindeutige MAC-Adressvergabe im Subnetz sicher!

Anwendung

Der CP ist für den Betrieb in einem Automatisierungssystem S7-1500 vorgesehen. Der CP ermöglicht den Anschluss der S7–1500 an Industrial Ethernet.

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall und Protokolle zur Datenverschlüsselung schützt der CP die S7-1500 oder auch ganze Automatisierungszellen vor unberechtigten Zugriffen. Weiterhin schützt er die Kommunikation zwischen der S7-Station und den Kommunikationspartnern vor Spionage und Manipulation.

2.2 Kommunikationsdienste

Der CP unterstützt folgende Kommunikationsdienste:

- **Open User Communication (OUC)**

  Die Open User Communication unterstützt über programmierte oder projektierte Kommunikationsverbindungen folgende Kommunikationsdienste über den CP:

  – ISO-Transport (gemäß ISO/IEC 8073)

  – TCP (gemäß RFC 793), ISO-on-TCP (gemäß RFC 1006) und UDP (gemäß RFC 768)

    Mit der Schnittstelle über TCP-Verbindungen unterstützt der CP die auf nahezu jedem Endsystem vorhandene Socket-Schnittstelle zu TCP/IP.

  – Multicast über UDP-Verbindung

    Der Multicast-Betrieb wird über eine entsprechende IP-Adressierung bei der Verbindungsprojektierung ermöglicht.

  – E-Mail versenden über SMTP (Port 25) oder SMTPS (Port 587) mit "SMTP-Auth" zur Authentifizierung an einem E-Mail-Server.

- **S7-Kommunikation**

  – PG-Kommunikation

  – Bedien- und Beobachtungsfunktionen (HMI-Kommunikation)

  – Datenaustausch über S7-Verbindungen

- **IT-Funktionen**
  - FTP-Funktionen (File Transfer Protocol FTP/FTPS) für Dateiverwaltung und Zugriffe auf Datenbausteine in der CPU (Client- und Serverfunktion).
  - Zu E-Mail siehe oben (OUC)
- **FETCH/WRITE**
  - FETCH/WRITE-Dienste als Server (entsprechend S5-Protokoll) über ISO-Transport-, ISO-on-TCP- und TCP-Verbindungen

    Die S7-1500 mit dem CP ist hierbei immer Server (passiver Verbindungsaufbau).

    Den holenden oder schreibenden Zugriff (Client-Funktion mit aktivem Verbindungsaufbau) führt eine SIMATIC S5 oder ein Fremdgerät / PC aus.

2.3 Weitere Funktionen

Uhrzeitsynchronisierung über Industrial Ethernet nach NTP-Verfahren (NTP: Network Time Protocol)

Der CP sendet in regelmäßigen Zeitabständen Uhrzeitanfragen an einen NTP-Server und synchronisiert seine lokale Uhrzeit.

Zusätzlich wird die Uhrzeit automatisch an die CPU-Baugruppen in der S7-Station weitergeleitet und somit die Uhrzeit in der gesamten S7-Station synchronisiert.

Security-Funktion: der CP unterstützt das Protokoll NTP (secure) zur sicheren Uhrzeitsynchronisation und Uhrzeitübertragung.

Adressierbarkeit über werkseitig voreingestellte MAC-Adresse

Ein fabrikneuer CP kann zur IP-Adressvergabe an der jeweils genutzten Schnittstelle über die voreingestellte MAC-Adresse erreicht werden. Die Online-Adressvergabe erfolgt in STEP 7.

SNMP-Agent

Der CP unterstützt die Datenabfrage über SNMP in Version V1 (Simple Network Management Protocol). Er liefert dabei die Inhalte von bestimmten MIB-Objekten gemäß Standard-MIB II und Automation System MIB.

Bei aktivierter Security unterstützt der CP SNMPv3 zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.

IP-Konfiguration - IPv4 und IPv6

Die wesentlichen Merkmale der IP-Konfiguration für den CP:

- Der CP unterstützt die Nutzung von IP-Adressen gemäß IPv4 und IPv6.
- Es ist konfigurierbar, über welchen Weg bzw. über welches Verfahren dem CP die IP-Adresse, die Subnetzmaske und die Adresse eines Netzübergangs zugewiesen wird.
- Dem CP kann die IP-Konfiguration und die Verbindungsprojektierung (IPv4) auch über das Anwenderprogramm zugewiesen werden (Programmbausteine siehe Kapitel Programmierung (Seite 21)).

  Anmerkung: gilt nicht für S7-Verbindungen.

IP-Routing

Der CP unterstützt statisches IP-Routing (IPv4) zu weiteren CM 1542-1 V2.0 / CP 1543-1 V2.0.

Zu Details siehe Kapitel IP-Routing (Seite 35).

IPv6-Adressen - Nutzungsbereich im CP

Für folgende Kommunikationsdienste kann eine IP-Adresse gemäß IPv6 verwendet werden:

- FTP Serverbetrieb
- FETCH/WRITE-Zugriff (CP ist Server)
- FTP-Clientbetrieb mit Adressierung über Programmbaustein
- E-Mail Übertragung mit Adressierung über Programmbaustein

Zugang zum Webserver der CPU

Über die LAN-Schnittstelle des CP haben Sie Zugang zum Webserver der CPU. Mit Hilfe des Webservers der CPU können Sie Baugruppendaten aus einer Station auslesen.

Beachten Sie die spezielle Beschreibung zum Webserver; siehe Kapitel Wegweiser Dokumentation (Seite 9)

Hinweis

Webserverzugriff über das HTTPS-Protokoll

Der Webserver einer SIMATIC S7-1500-Station befindet sich in der CPU. Bei sicherem Zugriff (HTTPS) auf den Webserver der Station über die IP-Adresse des CP 1543-1 wird daher das SSL-Zertifikat der CPU angezeigt.

S5-/S7-Adressierungsmodus für FETCH/WRITE

Der Adressierungsmodus ist für den FETCH/WRITE-Zugriff als S7- oder S5-Adressierungsmodus projektierbar. Der Adressierungsmodus legt fest, wie die Position der Anfangsadresse beim Datenzugriff ermittelt wird (S7-Adressiermodus gilt nur für Datenbausteine / DBs).

Beachten Sie weitere Angaben in der Online-Hilfe von STEP 7.

2.4 Industrial Ethernet Security

Umfassender Schutz - Aufgabe von Industrial Ethernet Security

Mit Industrial Ethernet Security können einzelne Geräte, Automatisierungszellen oder Netzsegmente eines Ethernet-Netzwerks abgesichert werden. Die Datenübertragung aus dem am CP 1543-1 angeschlossenen externen Netz kann durch die Kombination unterschiedlicher Sicherheitsmaßnahmen geschützt werden vor:

- Datenspionage (FTPS, HTTPS)
- Datenmanipulation
- unberechtigten Zugriffen

Über zusätzliche Ethernet-/PROFINET-Schnittstellen, realisiert durch die CPU oder zusätzliche CPs, können sichere unterlagerte Netze betrieben werden.

Security-Funktionen des CP für die S7-1500-Station

Durch die Verwendung des CP werden für die S7-1500-Station folgende Security-Funktionen an der Schnittstelle zum externen Netz zugänglich:

- Firewall
  - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer2)
  - Bandbreitenbegrenzung
  - Globale Firewall-Regeln

  Die Schutzfunktion Firewall kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.
- Logging

  Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mit Hilfe des Projektierwerkzeugs ausgelesen werden oder automatisch an einen Syslog-Server gesendet werden können.
- FTPS (expliziter Modus)

  Zur verschlüsselten Übertragung von Dateien
- NTP (secure)

  Zur sicheren Uhrzeitsynchronisierung und -übertragung

- SMTPS

  Zur gesicherten Übertragung von E-mails über Port 587
- SNMPv3

  Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen

Beachten Sie die Hinweise im Kapitel Security-Empfehlungen (Seite 31).

2.5 Mengengerüst und Leistungsdaten

2.5.1 Allgemeine Kenndaten

Merkmal	Erläuterung / Werte
Anzahl frei nutzbarer Verbindungen über Industrial Ethernet insgesamt	118 Der Wert gilt für die Gesamtsumme der Verbindungen folgender Typen: • S7-Verbindungen • Verbindungen für Offene Kommunikationsdienste • FTP (FTP-Client)

Hinweis

Verbindungsressourcen der CPU

Abhängig vom CPU-Typ steht eine unterschiedliche Anzahl an Verbindungsressourcen zur Verfügung. Die Anzahl an Verbindungsressourcen ist letztendlich maßgeblich für die Anzahl projektierbarer Verbindungen. Daher können sich geringere Werte ergeben, als im vorliegenden Kapitel zum CP angegeben werden.

2.5.2 Kenndaten für die Open User Communication (OUC) und FETCH/WRITE

Die Open User Communication (OUC) bietet den Zugang zur Kommunikation über TCP-, ISO-on-TCP-, ISO-Transport- und UDP-Verbindungen.

Folgende Kenndaten sind von Bedeutung (OUC + FETCH/WRITE):

Merkmal	Erläuterung / Werte
Anzahl Verbindungen	• Anzahl projektierte und programmierte Verbindungen insgesamt (ISO-Transport + ISO-on-TCP + TCP + UDP + FETCH/WRITE + E-Mail): Max. 118 Davon jeweils maximal: – TCP-Verbindungen: 1...118 [1)] – ISO-on-TCP-Verbindungen: 1...118 – ISO-Transportverbindungen: 1...118 – UDP-Verbindungen (spezifizierte und freie) insgesamt projektierbar: 1...118 – Verbindung für E-Mail: 1 – Verbindungen für FETCH/WRITE: 1...16 Anmerkungen: [1)] Empfangsüberlast vermeiden Die Flusskontrolle bei TCP-Verbindungen kann eine dauerhafte Überlast des Empfängers nicht regulieren. Es ist daher darauf zu achten, dass die Verarbeitungsleistung eines empfangenden CP vom Sender nicht dauerhaft überschritten wird (ca. 150-200 Nachrichten/s).
Max. Datenlänge für Programmbausteine	Die Programmbausteine ermöglichen den Transfer von Nutzdaten folgender Längen: • ISO-on-TCP, TCP, ISO-Transport: 1 bis 64 kByte • UDP: 1 bis 1452 Byte • E-Mail – Auftragsheader + Nutzdaten: 1 bis 256 Byte – E-Mail Anlage: bis 64 kByte
LAN-Schnittstelle - vom CP erzeugte max. Datenblocklänge pro Protokolleinheit (TPDU = transport protocol data unit)	• für Senden ISO-Transport, ISO-on-TCP, TCP: 1452 Byte / TPDU • für Empfangen – ISO-Transport: 512 Byte / TPDU – ISO-on-TCP: 1452 Byte / TPDU – TCP: 1452 Byte / TPDU

Hinweis

Verbindungsressourcen der CPU

Abhängig vom CPU-Typ steht eine unterschiedliche Anzahl an Verbindungsressourcen zur Verfügung. Die Anzahl an Verbindungsressourcen ist letztendlich maßgeblich für die Anzahl projektierbarer Verbindungen. Daher können sich geringere Werte ergeben, als im vorliegenden Kapitel zum CP angegeben werden.

Zum Thema Verbindungsressourcen finden sie ausführliche Informationen im Funktionshandbuch "Kommunikation"; siehe Kapitel Wegweiser Dokumentation (Seite 9).

Einschränkungen bei UDP

- Einschränkungen UDP-Broadcast / Multicast

  Um Überlast des CP durch einen hohen Broadcast-/Multicast-Telegrammverkehr zu vermeiden, ist der Empfang von UDP-Broadcast/Multicast im CP begrenzt.

- UDP-Telegramm-Pufferung

  Länge des Telegrammpuffers: Mindestens 7360 Byte

  Nach einem Pufferüberlauf werden neu eintreffende Telegramme, die nicht vom Anwenderprogramm abgeholt werden, verworfen.

2.5.3 Kenndaten S7-Kommunikation

Die S7-Kommunikation bietet die Datenübertragung über die Protokolle ISO-Transport oder ISO-on-TCP.

Merkmal	Erläuterung / Werte
Anzahl frei nutzbarer S7-Verbindungen über Industrial Ethernet insgesamt	Max. 118
LAN-Schnittstelle - vom CP erzeugte Datenblocklänge pro Protokolleinheit (PDU = protocol data unit)	• für Senden: 480 Byte / PDU • für Empfangen: 480 Byte / PDU
Anzahl reservierte OP-Verbindungen	4
Anzahl reservierte PG-Verbindungen	4
Anzahl reservierte Verbindungen für Web	2

Hinweis

Maximalwerte für S7-1500 Station

Abhängig von der verwendeten CPU gibt es Grenzwerte für die S7-1500 Station. Beachten Sie die Angaben in der entsprechenden Dokumentation.

2.5.4 Kenndaten für den FTP / FTPS-Betrieb

TCP-Verbindungen für FTP

FTP-Aktionen werden vom CP über TCP-Verbindungen übertragen. Je nach Betriebsart gelten hierfür folgende Kenndaten:

- FTP im Client-Betrieb:

  Sie können maximal 32 FTP-Sitzungen belegen. Pro aktivierter FTP-Sitzung werden bis zu 2 TCP-Verbindungen belegt (1 Control-Verbindung und 1 Datenverbindung).

- FTP im Server-Betrieb:

  Sie können maximal 16 FTP-Sitzungen gleichzeitig betreiben. Pro aktivierter FTP-Sitzung werden bis zu 2 TCP-Verbindungen belegt (1 Control-Verbindung und 1 Datenverbindung).

Programmbaustein FTP_CMD (FB40) für FTP-Client Betrieb

Für die Kommunikation nutzen Sie den FTP-Programmbaustein FTP_CMD.

Die Baustein-Laufzeit hängt bei FTP von den Reaktionszeiten des Partners und von der Länge der Nutzdaten ab. Eine allgemein gültige Angabe ist daher nicht möglich.

2.5.5 Kenndaten Security

IPSec-Tunnel (VPN)

Die VPN-Tunnelkommunikation ermöglicht den Aufbau einer gesicherten IPSec-Tunnelkommunikation zu einem oder mehreren Security-Modulen.

Mengengerüst	Wert
Anzahl der IPSec-Tunnel	16 maximal

Firewall-Regeln (erweiterter Firewall-Modus)

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 14.90.120.0/16)
- Maximal 128 Regeln mit Begrenzung der Übertragungsgeschwindigkeit ("Bandbreitenbegrenzung")

2.6 Voraussetzungen für den Einsatz

2.6.1 Mengengerüst

Für den Einsatz des hier beschriebenen CP-Typs gelten folgende Begrenzungen:

- Die Anzahl betreibbarer CPs innerhalb eines Racks ist abhängig vom verwendeten CPU-Typ.

  Durch den Betrieb mehrerer CPs können Sie die nachfolgend genannten Mengengerüste für die Station insgesamt vergrößern. Durch die CPU sind jedoch Systemgrenzen für das Gesamtmengengerüst vorgegeben. Das durch einen CP zur Verfügung stehende Mengengerüst lässt sich durch Verwendung mehrerer CPs im Rahmen der Systemgrenzen vergrößern.

  Beachten Sie die Angaben in der Dokumentation zur CPU, siehe Kapitel Wegweiser Dokumentation (Seite 9).

Hinweis

Stromversorgung über CPU ausreichend oder zusätzliche Stromversorgungsmodule erforderlich

Sie können eine bestimmte Anzahl Baugruppen ohne zusätzliche Stromversorgung in der S7 1500-Station betreiben. Beachten Sie die für den jeweiligen CPU-Typ angegebene Einspeiseleistung in den Rückwandbus. Abhängig vom Ausbau der S7 1500-Station müssen Sie zusätzliche Stromversorgungsmodule vorsehen.

2.6.2 Projektierung

Projektierung und Laden der Projektierungsdaten

Der CP wird beim Laden der Projektierungsdaten in die CPU mit den relevanten Projektierungsdaten versorgt. Das Laden der Projektierungsdaten in die CPU ist über eine Speicherkarte oder eine beliebige Ethernet-/PROFINET-Schnittstelle der S7-1500-Station möglich.

Erforderlich ist STEP 7 in folgender Version:

Version STEP 7	Funktion des CP
STEP 7 Professional ab V12 SP1	Die vollständige Funktionalität des CP 1543-1 (6GK7 543-1AX00-0XE0) ist projektierbar.

2.6.3 Programmierung

Programmbausteine

Für Kommunikationsdienste stehen vorgefertigte Programmbausteine (Anweisungen) als Schnittstelle in Ihrem STEP 7-Anwenderprogramm zur Verfügung.

Tabelle 2- 1 Anweisungen für Kommunikationsdienste

Protokoll	Programmbaustein (Anweisung)	Systemdatentyp
TCP	Verbindung herstellen und Daten senden/empfangen über: • TSEND_C/TRCV_C oder • TCON, TSEND/TRCV (Abbau der Verbindung über TDISCON möglich)	• TCON_IP_v4 • TCON_Configured
ISO-on-TCP		• TCON_IP_RFC
ISO		• TCON_ISOnative
UDP	• TCON, TUSEND/TURCV(Abbau der Verbindung über TDISCON möglich)	• TCON_IP_v4
E-Mail	• TMAIL_C	• TMail_v4***** • TMail_v6***** • TMAIL_FQDN*****
FTP	• FTP_CMD	• FTP_CONNECT_IPV4***** • FTP_CONNECT_IPV6***** • FTP_CONNECT_NAME***** • FTP_FILENAME* • FTP_FILENAME_PART*

*****Anwenderdefinierter Datentyp

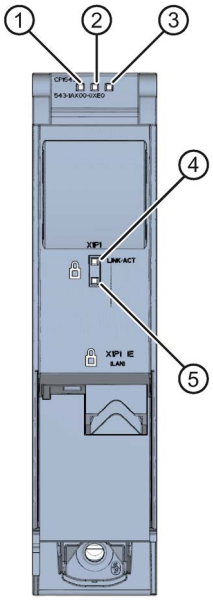
Tabelle 2- 2 Anweisungen für Konfigurationsaufgaben

Funktion	Programmbaustein (Anweisung)	Systemdatentyp
Konfiguration der Ethernet-Schnittstelle	• T_CONFIG	• CONF_DATA

Beachten Sie die Dokumentation der Programmbausteine in der Online-Hilfe von STEP 7.

2.7 LEDs

LEDs



① RUN-LED
② ERROR-LED
③ MAINT-LED
④ LINK/ACT-LED
⑤ Reserve-LED

Bild 2-2 LED-Anzeige des CP 1543-1 (ohne Frontklappe)

Bedeutung der LED-Anzeigen des CP

Der CP besitzt zur Anzeige des aktuellen Betriebszustandes und des Diagnosezustandes die folgenden 3 LEDs:

- RUN (einfarbige LED: grün)
- ERROR (einfarbige LED: rot)
- MAINT (einfarbige LED: gelb)

Die folgende Tabelle zeigt die Bedeutung der verschiedenen Kombinationen der Farben der RUN-, ERROR- und MAINT-LED.

Tabelle 2- 3 Bedeutung der LEDs "RUN", "ERROR", "MAINT"

RUN	ERROR	MAINT	Bedeutung
LED aus	LED aus	LED aus	Keine oder zu geringe Versorgungs-spannung am CP.
LED leuchtet grün	LED leuchtet rot	LED leuchtet gelb	LED-Test im Anlauf
LED leuchtet grün	LED leuchtet rot	LED aus	Anlauf (Booten des CP)
LED leuchtet grün	LED aus	LED aus	CP befindet sich im Betriebszustand RUN.
			Keine Störung
LED leuchtet grün	LED blinkt rot	LED aus	Ein Diagnoseereignis liegt vor.
LED leuchtet grün	LED aus	LED leuchtet gelb	Maintenance, eine Wartungsanforderung liegt vor.
LED leuchtet grün	LED aus	LED blinkt gelb	Ein Wartungsbedarf liegt vor.
			Laden des Anwenderprogramms
LED blinkt grün	LED aus	LED aus	Keine CP-Projektierung vorhanden
			Firmware wird geladen
LED blinkt grün	LED blinkt rot	LED blinkt gelb	Baugruppenfehler (LEDs blinken synchron)

Bedeutung der LED-Anzeigen der Ethernet-Schnittstelle: X1 P1

Die LED LINK/ACT (zweifarbig grün/gelb) ist dem Port der Ethernet-Schnittstelle zugeordnet. Die folgende Tabelle zeigt die LED-Bilder.

Tabelle 2- 4 Bedeutung der LED "LINK/ACT"

LINK/ACT		Bedeutung
grün aus	gelb aus	Keine Verbindung zu Ethernet Eine Ethernet-Verbindung zwischen Ethernet-Schnittstelle des CP und dem Kommunikationspartner besteht nicht. Zum aktuellen Zeitpunkt werden keine Daten über die Ethernet-Schnittstelle empfangen/gesendet.
grün blinkt	gelb aus	Der "Teilnehmer-Blinktest" wird durchgeführt.
grün ein	gelb aus	Verbindung zu Ethernet vorhanden Eine Ethernet-Verbindung zwischen der Ethernet-Schnittstelle Ihres CP und einem Kommunikations-partner besteht.
grün ein	gelb flackert	Zum aktuellen Zeitpunkt werden Daten über die Ether-net-Schnittstelle des Ethernet-Geräts von einem Kom-munikationspartner im Ethernet empfangen/gesendet.

2.8 Gigabit-Schnittstelle

Ethernet-Schnittstelle mit Gigabit-Spezifikation und Security-Zugang

Der CP besitzt eine Ethernet-Schnittstelle nach den Gigabit-Standards IEEE 802.3. Die Ethernet-Schnittstelle unterstützt Autocrossing, Autonegotiation und Autosensing.

Die Ethernet-Schnittstelle ermöglicht den über Firewall gesicherten Anschluss an externe Netzwerke. Der CP bietet die Schutzfunktion wie folgt:

- Schutz der S7-1500 Station, in welcher der CP betrieben wird;
- Schutz der an weiteren Schnittstellen der S7-1500-Station angeschlossenen unterlagerten Firmennetzwerke.

Die Pin-Belegung der Sub-RJ45-Buchse finden Sie im Kapitel Montage und Inbetriebnahme des CP 1543-1 (Seite 28).

Montage, Anschluss, Inbetriebnahme, Betrieb 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.

⚠ WARNUNG

Anschlüsse am LAN (Local Area Networks)

Ein LAN oder LAN-Segment mit den zugehörenden Anschlüssen sollte sich innerhalb einer einzigen Niederspannungsversorgungseinrichtung und innerhalb eines einzigen Gebäudes befinden. Es ist sicherzustellen, dass sich das LAN in einer "Umgebung vom Typ A" gemäß IEEE802.3 oder in einer "Umgebung vom Typ 0" gemäß IEC TR 62101 befindet.

Stellen Sie nie eine direkte elektrische Verbindung her zu TNV-Netzen (Telephon-Netzwerk) oder WAN (Wide Area Network).

3.1.1 Hinweise für den Einsatz im Ex-Bereich

⚠ WARNUNG

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

⚠ WARNUNG

EXPLOSIONSGEFAHR

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

⚠WARNUNG

EXPLOSIONSGEFAHR

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

⚠WARNUNG

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

⚠WARNUNG

Hutschiene

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

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

⚠WARNUNG

Anforderungen an den Schaltschrank

Um die EU-Richtlinie 94/9 (ATEX 95) zu erfüllen, muss das Gehäuse oder der Schaltschrank mindestens die Anforderungen von IP54 nach EN 60529 erfüllen.

⚠WARNUNG

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

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

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

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

3.1.4 Hinweise für den Einsatz im Ex-Bereich gemäß FM

⚠ WARNUNG

EXPLOSIONSGEFAHR

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

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

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

⚠WARNUNG

EXPLOSIONSGEFAHR

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

3.2 Montage und Inbetriebnahme des CP 1543-1

Montage und Inbetriebnahme

⚠WARNUNG

Lesen Sie das Systemhandbuch "Automatisierungssystem S7-1500"

Lesen Sie vor der Montage, dem Anschließen und der Inbetriebnahme die entsprechenden Abschnitte im Systemhandbuch "Automatisierungssystem S7-1500" (Literaturverweis siehe Kapitel Wegweiser Dokumentation (Seite 9)).

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

Projektierung

Voraussetzung für die komplette Inbetriebnahme des CP ist die Vollständigkeit der STEP 7-Projektdaten.

Vorgehensweise zur Montage und Inbetriebnahme

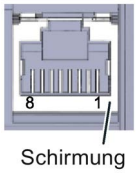
Schritt	Ausführung	Hinweise und Erläuterungen
1	Gehen Sie bei der Montage und dem Anschließen entsprechend den Beschreibungen zur Montage von Peripheriemodulen im Systemhandbuch "Automatisierungssystem S7 1500" vor.	
2	Schließen Sie den CP über die RJ-45-Buchse an Industrial Ethernet an.	Unterseite des CP
3	Schalten Sie die Spannungsversorgung ein.	

Schritt	Ausführung	Hinweise und Erläuterungen
4	Schließen Sie die Frontklappen der Baugruppe und halten Sie diese im Betrieb geschlossen.	
5	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 übersetzen und laden" • "Online- und Diagnosefunktionen nutzen"

Ethernet-Schnittstelle

Die folgende Tabelle zeigt die Anschlussbelegung bei der Ethernet-Schnittstelle (RJ45-Buchse). Die Belegung entspricht dem Ethernet-Standard IEEE 802.3.

Tabelle 3- 1 Anschlussbelegung Ethernet-Schnittstelle

Ansicht	Pin	10/100 Mbit-Betrieb		10/100 Mbit- oder Gigabit-Betrieb	
		Signalname	Steckerbelegung	Signalname	Steckerbelegung
	1	TD	Transmit Data +	D1+	D1 bidirektional +
	2	TD_N	Transmit Data -	D1-	D1 bidirektional -
	3	RD	Receive Data +	D2+	D2 bidirektional +
	4	GND	Ground	D3+	D3 bidirektional +
	5	GND	Ground	D3-	D3 bidirektional -
	6	RD_N	Receive Data -	D2-	D2 bidirektional -
	7	GND	Ground	D4+	D4 bidirektional +
	8	GND	Ground	D4-	D4 bidirektional -

Weitere Informationen zum Thema "Anschließen" und zum Thema "Zubehör (RJ45-Stecker)" finden Sie im Systemhandbuch:
Link: (https://support.industry.siemens.com/cs/ww/de/view/59191792)

3.3 Betriebszustand der CPU - Rückwirkung auf CP

Sie haben die Möglichkeit, den Betriebszustand der CPU über die Projektiersoftware STEP 7 zwischen RUN und STOP umzuschalten.

Abhängig vom Betriebszustand der CPU zeigt der CP das nachfolgend beschriebene Verhalten.

Umschalten der CPU von RUN auf STOP:

Im Zustand STOP der CPU bleibt der CP im Zustand RUN und es gilt folgendes Verhalten:

- Für aufgebaute Verbindungen (ISO-Transport-, ISO-on-TCP-, TCP-, UDP-Verbindungen) gilt abhängig von der Konfiguration:
  - Programmierte Verbindungen bleiben bestehen.
  - Projektierte Verbindungen werden abgebaut.
- Aktiviert bleiben folgende Funktionen:
  - Die Projektierung und Diagnose des CP (entsprechende Systemverbindungen für Projektierung, Diagnose und PG Kanal-Routing bestehen weiterhin);
  - Die Webdiagnose
  - S7-Routing-Funktion
  - Uhrzeitsynchronisation

Hinweis

RUN/STOP-LED des CP

Die grüne RUN/STOP-LED des CP leuchtet unabhängig vom STOP-Zustand der CPU weiterhin grün.

Projektierung, Programmierung

4

4.1 Security-Empfehlungen

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

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.
- Halten Sie die Firmware aktuell. Informieren Sie sich regelmäßig über Sicherheits-Updates der Firmware und wenden Sie diese an.
- Informieren Sie sich regelmäßig über Neuigkeiten auf den Siemens-Internetseiten.
  - Hier finden Sie informationen zu Netzwerksicherheit:

    Link: (http://www.siemens.com/industrialsecurity)
  - Hier finden Sie informationen zu Industrial Ethernet Security:

    Link: (http://w3.siemens.com/mcms/industrial-communication/de/ie/industrial-ethernet-security/Seiten/industrial-security.aspx)
  - Eine Einführung in das Thema Industrial Security finden Sie in folgender Druckschrift:

    Link: (http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP01-0BA4_BR_Netzwerksicherheit_de_112015.pdf)

Physikalischer Zugang

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

Netzanschluss

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

Security-Funktionen des Produkts

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

- Schutzstufen

  Projektieren Sie unter "Schutz und Security" den Zugriff auf die CPU.

- Security-Funktion der Kommunikation
  - Aktivieren Sie die Security-Funktionen des CP und richten Sie die Firewall ein.

    Beim Anschluss an öffentliche Netze sollten Sie die Firewall einsetzen. Bedenken Sie, mit welchen Diensten Sie über öffentliche Netze einen Zugriff auf die Station ermöglichen wollen. Indem Sie die "Bandbreitenbegrenzung" der Firewall verwenden, nutzen Sie die Möglichkeit, Flooding- und DoS-Angriffe einzuschränken.

    Die Funktionalität FETCH/WRITE bietet die Möglichkeit, auf beliebige Daten Ihrer PLC zuzugreifen. In Verbindung mit öffentlichen Netzen sollte die Funktionalität FETCH/WRITE nicht verwendet werden.
  - Verwenden Sie die sicheren Protokollvarianten HTTPS, FTPS, NTP (secure) und SNMPv3.
  - Nutzen Sie die Programmbausteine für die gesicherte OUC-Kommunikation (Secure OUC).
  - Lassen Sie den Zugriff auf den Webserver der CPU (CPU-Projektierung) und auf den Webserver des CP deaktiviert.
- Schutz der Passwörter für den Zugriff auf Programmbausteine

  Schützen Sie Passwörter, die für Programmbausteine in Datenbausteinen abgelegt werden, vor Einsicht. Hinweise zur Vorgehensweise finden Sie im STEP 7-Informationssystem unter dem Stichwort "Know-how-Schutz".
- Logging-Funktion

  Aktivieren Sie die Funktion über die Security-Projektierung und prüfen Sie die protokollierten Ereignisse regelmäßig auf unautorisierte Zugriffe.

Passwörter

- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Aktualisieren Sie regelmäßig die Passwörter, um die Sicherheit zu erhöhen.
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter wie z. B. "passwort1", "123456789" oder dergleichen.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.

  Siehe hierzu auch den vorstehenden Abschnitt.
- Verwenden Sie ein Passwort nicht für verschiedene Benutzer und Systeme.

Protokolle

Sichere und unsichere Protokolle

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

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.
  - Offen bei Bausteinaufruf

    Der Port wird nur geöffnet, wenn ein entsprechender Programmbaustein aufgerufen wird.

- **Authentifizierung**

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

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
DHCP	68 (UDP)	Offen	Offen nach Konfiguration (nur ausgehend)	Nein
DCP	93 (UDP)	Offen	Offen	Nein
DCE	135 (TCP)	Offen	Offen	Ja, wenn Security aktiviert ist.

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
S7-Kommunikation	102 (TCP)	Offen	Offen	Nein
Online-Security-Diagnose	8448 (TCP)	Geschlossen	Offen nach Konfiguration	
NTP	123 (UDP)	Geschlossen	Offen nach Konfiguration (nur ausgehend)	Nein
HTTP	80 (TCP)	Geschlossen	Offen nach Konfiguration	Nein
HTTPS	443 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
FTP	20 (TCP) 21 (TCP)	Geschlossen	Offen nach Konfiguration	Nein
FTPS	989 (TCP) 990 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
SNMP	161 (UDP)	Offen	Offen nach Konfiguration	Ja (unter SNMPv3)
SMTP	25 (TCP)	Geschlossen	Offen bei Bausteinaufruf (nur ausgehend)	Nein
SMTPS	587 (TCP)	Geschlossen	Offen bei Bausteinaufruf (nur ausgehend)	Nein

4.2 Netzwerkeinstellungen

Automatische Einstellung

Die Ethernet-Schnittstelle des CP ist fest auf automatische Erkennung (Autosensing) eingestellt.

Hinweis

Die Grundeinstellung gewährleistet im Normalfall eine problemlose Kommunikation.

Autocrossing-Mechanismus

Durch den integrierten Autocrossing-Mechanismus ist es möglich, die Verbindung von PC / PG direkt über Standardkabel herzustellen. Ein gekreuztes Kabel ist nicht notwendig.

Hinweis

Anschluss eines Switch

Verwenden Sie zum Anschluss eines Switch, der seinerseits keinen Autocrossing-Mechanismus beherrscht, ein gekreuztes Kabel.

4.3 IP-Konfiguration

4.3.1 Besonderheiten zur IP-Konfiguration

Projektierte S7- und OUC-Verbindungen bei IP-Adresse über DHCP nicht betreibbar

Hinweis

Wenn Sie die IP-Adresse über DHCP beziehen, sind evtl. projektierte S7- und OUC-Verbindungen nicht funktionsfähig. Grund: die projektierte IP-Adresse wird im Betrieb durch die von DHCP bezogene IP-Adresse ersetzt.

4.3.2 Wiederanlauf nach Erkennen einer IP-Doppeladressierung im Netzwerk

Um Ihnen eine schwierige Suche nach Fehlern im Netzwerk zu ersparen, erkennt der CP beim Anlauf eine Doppeladressierung im Netzwerk.

Verhalten beim Anlauf des CP

Wenn beim Anlauf des CP eine Doppeladressierung erkannt wird, dann geht der CP in RUN und ist über die Ethernet-Schnittstelle nicht erreichbar. Die ERROR-LED blinkt.

4.3.3 IP-Routing

IP-Routing über den Rückwandbus

Der CP unterstützt statisches IP-Routing (IPv4) zu weiteren CM 1542-1 / CP 1543-1. Das IP-Routing können Sie beispielsweise für den Webserver-Zugriff von unterlagerten Modulen nutzen.

Der Datendurchsatz beim IP-Routing ist auf 1 MBit/s beschränkt. Beachten Sie dies bezüglich der Anzahl der teilnehmenden Module und des erwarteten Datenverkehrs über den Rückwandbus.

Projektierung

Sie können das IP-Routing in STEP 7 über die Funktion "IP-Routing zwischen Kommunikationsmodulen" aktivieren. In den Security-Einstellungen heißt die entsprechende Funktion "IP-Routing über den Rückwandbus". Bei Aktivierung der Funktion werden zusätzlich IP-Firewall-Regeln angelegt, die Sie im erweiterten Firewall-Modus der Security-Einstellungen anpassen können.

Das IP-Routing läuft über den projektierten Default-Router. Wenn Sie mehrere CPs in einer Station verwenden, dann darf unter den Modulen in der Station nur eines als Router projektiert sein.

4.4 Security

Beachten Sie den Umfang und die Anwendung der Security-Funktionen des CP im Kapitel Industrial Ethernet Security (Seite 15).

Zum Mengengerüst siehe Kapitel Kenndaten Security (Seite 19).

Die Security-Funktionen werden in STEP 7 projektiert.

4.4.1 VPN

Was ist VPN?

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 unabhängig von höheren Protokollen (HTTP, FTP) sämtliche Netzwerkpakete weiterleitet.

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

Eigenschaften

- VPN bildet ein logisches Teilnetz, das sich in ein benachbartes (zugeordnetes) Netz einbettet. VPN nutzt die üblichen Adressierungsmechanismen des zugeordneten Netzes, transportiert datentechnisch aber eigene Netzwerkpakete und arbeitet so vom Rest dieses Netzes losgelöst.
- VPN ermöglicht die Kommunikation der darin befindlichen VPN-Partner mit dem zugeordneten Netz.
- VPN basiert auf einer Tunneltechnik, ist individuell konfigurierbar, kundenspezifisch und in sich geschlossen.
- 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 Server möglich, ohne dass die Kommunikation durch Dritte eingesehen werden kann („Ende-zu-Ende“- oder „Host-to-Host"-Verbindung).
- Gewährleistung von Informationssicherheit in vernetzten Anlagen der Automatisierungstechnik.
- Absicherung von Rechnersystemen einschließlich der dazugehörigen Datenkommunikation innerhalb eines Automatisierungsnetzes oder den sicheren Fernzugriff über das Internet.
- Gesicherte Fernzugriffe vom PC/Programmiergerät auf Automatisierungsgeräte oder Netzwerke, die durch Security-Module geschützt sind, über öffentliche Netze hinweg möglich.

Zellenschutzkonzept

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

- Der Zugriff auf einzelne Geräte oder auch ganze Automatisierungszellen, die durch Security-Module geschützt sind, wird erlaubt.
- Gesicherte Verbindungen über unsichere Netzwerkstrukturen werden ermöglicht.

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

- Datenspionage
- Datenmanipulation
- Unerwünschten Zugriffen

4.4.1.1 VPN-Tunnelkommunikation zwischen S7-1500-Stationen anlegen

Voraussetzungen

Um einen VPN-Tunnel zwischen zwei S7-1500-Stationen anzulegen, müssen folgende Voraussetzungen erfüllt sein:

- Zwei S7-1500-Stationen sind projektiert.
- Beide CPs sind mit einer Firmware-Version ≥ V1.1 projektiert.
- Die Ethernet-Schnittstellen der beiden Stationen befinden sich im gleichen Subnetz.

Hinweis

Kommunikation auch über einen IP-Router möglich

Die Kommunikation zwischen den beiden S7-1500-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 Benutzer an.
2. Kontrollkästchen "Aktiviere Security-Funktionen" anwählen.
3. VPN-Gruppe anlegen und Security-Module zuweisen.
4. Eigenschaften der VPN-Gruppe projektieren.

   Lokale VPN-Eigenschaften der beiden CPs projektieren.

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

Security-Benutzer anlegen

Um einen VPN-Tunnel anzulegen, benötigen Sie entsprechende Projektierungsrechte. Um die Security-Funktionen zu aktivieren, müssen Sie mindestens einen Security-Benutzer anlegen.

1. Klicken Sie in den lokalen Security-Einstellungen des CPs auf die Schaltfläche "Benutzeranmeldung".
   Ergebnis: Ein neues Fenster öffnet sich.
2. Geben Sie Benutzernamen, Passwort und die Bestätigung des Passworts ein.
3. Klicken Sie auf die Schaltfläche "Anmelden".
   Sie haben einen neuen Security-Benutzer angelegt. Die Security-Funktionen stehen Ihnen zur Verfügung.

Bei allen weiteren Anmeldungen melden Sie sich als Benutzer an.

Kontrollkästchen "Aktiviere Security-Funktionen" anwählen

- Nach dem Anmelden müssen Sie bei beiden 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

Hinweis

Aktuelles Datum und aktuelle Uhrzeit auf den Security-Modulen

Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Security-Module über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

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.

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 des CP festlegen

Die VPN-Eigenschaften des jeweiligen CP legen Sie in den lokalen Eigenschaften der Baugruppe fest ("Security" > "Firewall" > "VPN")

Ergebnis

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

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

4.4.1.2 VPN-Tunnelkommunikation zwischen CP 1543-1 und SCALANCE M erfolgreich aufbauen

Das Anlegen der VPN-Tunnelkommunikation zwischen CP 1543-1 und SCALANCE M erfolgt entsprechend der beschriebenen Vorgehensweise bei S7-1500-Stationen (Seite 37).

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

Wenn das Kontrollkästchen nicht angewählt ist, lehnt der CP 1543-1 den Verbindungsaufbau ab.

4.4.1.3 VPN-Tunnelkommunikation mit SOFTNET Security Client

Das Anlegen der VPN-Tunnelkommunikation zwischen SOFTNET Security Client und dem CP 1543-1 erfolgt entsprechend der beschriebenen Vorgehensweise bei S7-1500-Stationen (Seite 37).

VPN-Tunnelkommunikation gelingt nur bei deaktiviertem internen Teilnehmer

Unter bestimmten Bedingungen gelingt der Aufbau einer VPN-Tunnelkommunikation zwischen SOFTNET Security Client und dem CP 1543-1 nicht.

SOFTNET Security Client versucht zusätzlich, eine VPN-Tunnelkommunikation zu einem unterlagerten internen Teilnehmer aufzubauen. Dieser Kommunikationsaufbau zu einem nicht vorhandenen Teilnehmer verhindert den gewünschten Kommunikationsaufbau zum CP 1543-1.

Um eine erfolgreiche VPN-Tunnelkommunikation zum CP 1543-1 aufzubauen, müssen Sie den internen Teilnehmer deaktivieren.

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

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

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

   Der unterlagerte Teilnehmer verschwindet vorerst aus der Tunnelliste.
2. Selektieren Sie in der Tunnelliste die gewünschte Verbindung zum CP 1543-1.
3. Wählen Sie im Kontextmenü über die rechte Maustaste "Aktiviere Verbindung zu den internen Knoten" aus.

   Der unterlagerte Teilnehmer erscheint vorübergehend wieder in der Tunnelliste.
4. Selektieren Sie in der Tunnelliste den unterlagerten Teilnehmer.
5. Wählen Sie im Kontextmenü über die rechte Maustaste "Lösche Eintrag" aus

Ergebnis: Der unterlagerte Teilnehmer ist endgültig deaktiviert. Der Aufbau einer VPN-Tunnelkommunikation zum CP 1543-1 gelingt.

4.4.1.4 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".

4.4.2 Firewall

4.4.2.1 Firewall-Reihenfolge bei der Prüfung ein- und ausgehender Telegramme

Jedes eingehende oder ausgehende Telegramm durchläuft zunächst die MAC-Firewall (Layer 2). Wird das Telegramm bereits auf dieser Ebene verworfen, 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.

4.4.2.2 Schreibweise der Quell-IP-Adresse (erweiterter Firewall-Modus)

Wenn Sie in den erweiterten Firewall-Einstellungen des CP 1543-1 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.

4.4.2.3 HTTP und HTTPS über IPv6 nicht möglich

Die HTTP- und HTTPS-Kommunikation über das IPv6-Protokoll auf den Webserver der Station ist nicht möglich.

Bei aktivierter Firewall in den lokalen Security-Einstellungen im Eintrag "Firewall > Vordefinierte IPv6-Regeln": Die angewählten Kontrollkästchen "Erlaube HTTP" und "Erlaube HTTPS" sind ohne Funktion.

4.4.2.4 Firewall-Einstellungen für Verbindungen über VPN-Tunnel

IP-Regeln im erweiterten Firewall-Modus

Beachten Sie bei projektierten Verbindungen zwischen CPs die folgende Einstellung, wenn Sie die CPs im erweiterten Firewall-Modus betreiben.

Wählen Sie bei beiden CPs in der Parametergruppe "Security > Firewall > IP-Regeln" für Tunnelverbindungen die Einstelllung "Allow" aus.

Wenn Sie die Option nicht aktivieren, wird die VPN-Verbindung abgebaut und wieder neu aufgebaut.

Dies gilt für Verbindungen zwischen CP 1543-1 und beispielsweise CP 343-1 Advanced, CP 443-1 Advanced, CP 1628 oder CP 1243-1.

Siehe auch

Online-Diagnose und Laden in Station bei aktivierter Firewall (Seite 43)

4.4.3 Online-Funktionen

4.4.3.1 Online-Diagnose über Port 8448

Security-Diagnose ohne Öffnen von Port 102

Wenn Sie Security-Diagnose durchführen möchten, ohne den Port 102 zu öffnen, dann gehen Sie folgendermaßen vor:

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

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

4.4.3.2 Online-Diagnose und Laden in Station bei aktivierter Firewall

Firewall für Online-Funktionen einstellen

Gehen Sie bei aktivierten Security-Funktionen wie folgt vor:

1. Wählen Sie in den globalen Security-Einstellungen (siehe Projektnavigation) 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.
4. Wählen Sie nun den CP in der S7-Station aus.
5. Aktivieren Sie den erweiterten Firewall-Modus in den lokalen Security-Einstellungen des CP in der Parametergruppe "Security > Firewall".
6. Öffnen Sie die Parametergruppe "IP-Regeln".
7. Fügen Sie in der Tabelle jeweils eine neue IP-Regel für die zuvor global angelegten Dienste wie folgt ein:
   - Aktion: Allow; "Von Extern -> Nach Station" mit dem global angelegten Dienst "Echo Request"
   - Aktion: Allow; "Von Station -> Nach Extern" mit dem global angelegten Dienst "Echo Reply"
8. Tragen Sie für die IP-Regel zum Echo Request unter "Quell-IP-Adresse" die IP-Adresse der Enineering-Station ein. So sorgen Sie dafür, dass ICMP-Telegramme (Ping) nur von Ihrer Enineering-Station aus die Firewall passieren können.

4.4.4 Filtern der System-Ereignisse

Kommunikationsprobleme bei zu hoch eingestelltem Wert für System-Ereignisse

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

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

4.5 Uhrzeitsynchronisation

Verfahren

Der CP unterstützt das folgende Verfahren zur Uhrzeitsynchronisation:

- NTP-Verfahren (NTP: Network Time Protocol)

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 absoluten Uhrzeit.

Hinweis

Besonderheit bei Uhrzeitsynchronisation über NTP

Wenn die Option "Uhrzeit von nicht synchronisierten NTP-Servern annehmen" nicht aktiviert ist, gilt folgendes Verhalten:

Wenn der CP ein Uhrzeit-Telegramm von einem nicht synchronisiertem NTP-Server mit Stratum 16 empfängt, dann wird die Uhrzeit nicht danach gestellt. In diesem Fall wird in der Diagnose keiner der NTP-Server als "NTP-Master" angezeigt, sondern nur als "erreichbar".

Security

Sie können in der erweiterten NTP-Konfiguration zusätzliche NTP-Server anlegen und verwalten.

Hinweis

Gültige Uhrzeit sicherstellen

Wenn Sie Security-Funktionen nutzen, ist eine gültige Uhrzeit von erheblicher Bedeutung. Sofern Sie die Uhrzeit nicht von der Station (CPU) beziehen, wird empfohlen, auf das Verfahren NTP (secure) zurückzugreifen.

Projektierung

Weitere Hinweise zur Projektierung finden Sie in der Online-Hilfe von STEP 7 in der Parametergruppe "Uhrzeitsynchronisation".

4.6 Programmbausteine für OUC

Programmierung der Open User Communication (OUC)

Die unten aufgeführten Anweisungen (Programmbausteine) sind erforderlich für folgende Kommunikationsdienste über Ethernet:

- ISO-Transport
- TCP
- ISO-on-TCP
- UDP (Multicast)
- E-Mail

Legen Sie hierfür die entsprechenden Programmbausteine an. Die Programmbausteine finden Sie in STEP 7 im Fenster "Anweisungen > Kommunikation > Open user communication".

Details zu den Programmbausteinen finden Sie im Informationssystem von STEP 7.

Hinweis

Unterschiedliche Programmbaustein-Versionen

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

Unterstützte Programmbausteine für OUC

Die folgenden Anweisungen in der angegebenen Mindestversion stehen für die Programmierung der Open User Communication zur Verfügung:

- **TSEND_C V3.1 / TRCV_C V3.1**

  Kompakte Bausteine für Verbindungsauf-/abbau sowie Senden und Empfangen von Daten

  bzw.

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

  Verbindungsaufbau / Verbindungsabbau

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

  Senden bzw. Empfangen von Daten über UDP

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

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

- **TMAIL_C V4.0**

  Senden von E-Mails

  Beachten Sie die Beschreibung zum TMAIL_C ab Version V4.0 im STEP 7-Informationssystem.

Verbindungs-Auf- und Abbau

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

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

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

Hinweis

Verbindungsabbruch

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

Verbindungsbeschreibungen in Systemdatentypen (SDTs)

Für die jeweilige Verbindungsbeschreibung verwenden die oben genannten Bausteine den Parameter CONNECT (bzw. MAIL_ADDR_PARAM bei TMAIL_C). Die Verbindungsbeschreibung wird in einem Datenbaustein abgelegt, dessen Struktur durch einen Systemdatentyp (SDT) festgelegt wird.

Anlegen eines SDT für die Datenbausteine

Den zu jeder Verbindungsbeschreibung erforderlichen SDT legen Sie als Datenbaustein an. Der SDT-Typ wird erzeugt, indem Sie in STEP 7 in der Deklarationstabelle des Bausteins nicht einen Eintrag aus der Klappliste "Datentyp" wählen, sondern in das Feld "Datentyp" manuell den Namen eingeben (z. B. "TCON_IP_V4"). Der entsprechende SDT wird dann mit seinen Parametern angelegt.

Die folgenden SDTs können verwendet werden.

- **Konfigurierte Verbindungen:**
  - **TCON_Configured**

    Für die Übertragung von Telegrammen über TCP
- **Programmierte Verbindungen:**
  - **TCON_IP_V4**

    Für die Übertragung von Telegrammen über TCP oder UDP
  - **TCON_IP_V4_SEC**

    Für die gesicherte Übertragung von Telegrammen über TCP
  - **TCON_QDN**

    Für die Übertragung von Telegrammen über TCP oder UDP
  - **TCON_QDN_SEC**

    Für die gesicherte Übertragung von Telegrammen über TCP
  - **TCON_IP_RFC**

    Für die Übertragung von Telegrammen über ISO-on-TCP
  - **TCON_ISOnative**

    Für die Übertragung von Telegrammen über ISO-Transport
  - **TMail_V4**

    Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv4-Adresse
  - **TMail_V6**

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

    Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über den Host-Namen
  - **TMail_V4_SEC**

    Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv4-Adresse
  - **TMail_V6_SEC**

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

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

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

Die Parameterbeschreibung der SDTs TMail_V4_SEC, TMail_V6_SEC und TMail_QDN_SEC finden Sie im Online-Hilfe-Kapitel zu TCON_IP_V4_SEC.

4.7 Einrichten der FTP-Kommunikation

4.7.1 Der Programmbaustein FTP_CMD (FTP-Client-Funktion)

Bedeutung

Mit der Anweisung FTP_CMD können Sie FTP-Verbindungen aufbauen und Dateien von und zu einem FTP-Server übertragen.

Hinweis
Bausteinversionen

Die Version V2.x des FTP_CMD können Sie in einer Station nur zusammen mit einer CPU V2.x und einem CP V2.x verwenden.

Sobald die Station eine CPU V1.x oder einen CP V1.x enthält, müssen Sie den FTP_CMD in der älteren Version V1.x verwenden (bspw. V1.4). Schalten Sie hierzu die Version der Bibliothek "SIMATIC NET CP" auf V3.4. Sie können dann eine ältere Version des Bausteins auswählen.

Die folgende Tabelle zeigt die Kompatibilitäten.

Tabelle 4- 1 Kompatibilität des Bausteins FTP_CMD mit Versionen der CPU und des CP

FTP_CMD	CPU	CP 1543-1
V1.5	V1.x	Beliebig
V1.5	Beliebig	V1.x
V2.0	V2.x	V2.x

Der Datentransfer ist über FTP oder FTPS (gesichterte SSL-Verbindungen) möglich.

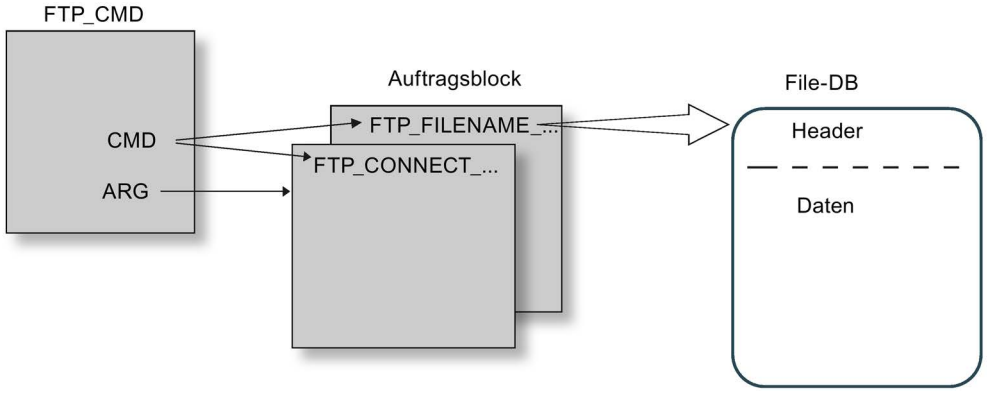
Hinweis
FTPS: Zertifikate abgleichen

FTPS erfordert den Abgleich der Zertifikate zwischen FTP-Server und FTP-Client. Wenn der FTP-Server außerhalb des STEP 7-Projekts des FTP-Client konfiguriert wird, dann ist der Import des Zertifikates vom FTP-Server erforderlich. Importieren Sie im Zertifikatsmanager das Zertifikat des FTP-Servers als vertrauenswürdiges Zertifikat.

Funktionsweise

Die Anweisung FTP_CMD verweist auf einen Auftragsblock (ARG), in dem das FTP-Kommando spezifiziert wird. Je nach Typ des FTP-Kommandos (CMD) verwendet dieser Auftragsblock unterschiedliche Datenstrukturen zur Parametrierung. Für diese unterschiedlichen Strukturen stehen jeweils passende Datentypen (UDTs) zur Verfügung.

Die folgende Darstellung zeigt die Aufrufstruktur:



Auftragsblöcke

Für die Auftragsblöcke werden folgende Datenstrukturen verwendet:

- Verbindungsaufbau

  Für den Verbindungsaufbau stehen unterschiedliche Datenstrukturen für folgende Zugriffsarten zur Verfügung:

  – FTP_CONNECT_IPV4: Verbindungsaufbau mit IP-Adressen gemäß IPv4

  – FTP_CONNECT_IPV6: Verbindungsaufbau mit IP-Adressen gemäß IPv6

  – FTP_CONNECT_NAME: Verbindungsaufbau mit Server-Namen (DNS)

- Datentransfer

  Für den Datentransfer stehen zwei unterschiedliche Datenstrukturen zur Verfügung:

  – FTP_FILENAME: Datenstruktur für den Zugriff auf eine vollständige Datei

  – FTP_FILENAME_PART: Datenstruktur für den lesenden Zugriff auf einen Datenbereich

Datenübertragung im File_DB

Der Datentransfer erfolgt über Datenbausteine, die einen Header für Auftragsdaten sowie den Bereich für die Nutzdaten enthalten. Der Datenbaustein wird im Auftragspuffer angegeben.

Voraussetzungen in der CPU-Projektierung

Verwenden Sie folgende Einstellungen, um den FTP-Zugriff zu ermöglichen:

- Deaktivieren Sie bei allen als File-DB verwendeten Datenbausteinen das Attribut "Optimierter Bausteinzugriff".
- Nur bei Verwendung einer CPU V1.x und eines CP V1.1.x:
  Aaktivieren Sie in den Projektierungsdaten der CPU unter "Schutz & Security" die Option "Zugriff über PUT/GET-Kommunikation ..." (PUT/GET muss freigegeben sein).

FTP-Zugriff über Anweisung FTP_CMD - Parameterversorgung bei Kommandotypen NOOP und QUIT

Versorgen Sie die Anweisung FTP_CMD auch bei folgenden Kommandotypen mit Verweis auf einen Auftragsblock:

CMD = 0 (NOOP)

CMD = 5 (QUIT)

Der Inhalt des Auftragsblocks wird bei Ausführung dieser Kommandotypen nicht ausgewertet, der Typ (UDT) des angegebenen Auftragsblockes ist daher unerheblich.

Hinweis

Verhalten bei fehlendem Verweis auf den FTP-Auftragsblock

Bei fehlender Versorgung wird das Kommando nicht ausgeführt. Die Anweisung verharrt in einem scheinbaren Ausführungszustand ohne Rückmeldung an der Schnittstelle zum Anwenderprogramm.

Auswerten der Statusbits "LOCKED" und "NEW" vom Programmbaustein FTP_CMD

- In der Version 1.2 des Programmbausteins "FTP_CMD" werden die Statusbits "LOCKED" und "NEW" des FILE_DB_HEADER nicht ausgewertet.

  Über die Funktion des FTP-Servers oder durch die Nutzung des selben File DB sind mehrfache gleichzeitige Zugriffe auf den jeweils selben Datenbereich nicht ausgeschlossen. Dadurch kann es zu Dateninkonsistenz kommen.
- Ab der Version 1.5 des Programmbausteins "FTP_CMD" sind die Statusbits "LOCKED" und "NEW" des FILE_DB_HEADER richtig gesetzt. Die beiden Statusbits werden ausgewertet. Die Version 1.5 ist verfügbar ab STEP 7 Professional V12 SP1.

Hinweis

Dateninkonsistenz vermeiden

Achten Sie darauf, dass Sie nicht gleichzeitig mehrfach auf den selben File DB zugreifen.

4.7.2 Projektierung der FTP-Server-Funktion

CP-Projektierung

Projektieren Sie die FTP-Server-Funktion des CP in folgender Parametergruppe.

- Bei deaktivierten Security-Funktionen: "FTP-Server-Konfiguration"
- Bei aktivierten Security-Funktionen: "Security > FTP-Server-Konfiguration"

Voraussetzungen in der CPU-Projektierung und Programmierung

Verwenden Sie folgende Einstellungen, um den FTP-Zugriff zu ermöglichen:

- In der CPU-Projektierung unter "Schutz & Security > Verbindungsmechanismen":

  Deaktivieren Sie die Option "Zugriff über PUT/GET-Kommunikation ...".
- Legen Sie als File-DBs Datenbausteine vom Typ "Array-of-Byte" an.
- Deaktivieren Sie bei allen als File-DB verwendeten DBs das Attribut "Optimierter Bausteinzugriff".

S7-1500 CP als FTP-Server

Die hier beschriebene Funktion ermöglicht Ihnen, Daten in Form von Dateien (Files) über FTP-Kommandos in oder aus der S7-1500-Station zu übertragen. Dabei können die üblichen FTP-Kommandos genutzt werden, um Dateien zu lesen, zu schreiben und zu verwalten.

Der Zugriff ist auf folgende Daten der S7-1500 möglich:

- **RAM des CP**

  Name des Verzeichnisses:

  /ram

- **Datenbausteine der CPU**

  Name des Verzeichnisses:

  /cpu1 / DBx

  "DBx" ist der Name des entsprechenden Datenbausteins, bspw. BD10.

- **SIMATIC Memory Card der CPU**

  Die Funktion wird unterstützt ab CP-Firmware V2.0 und CPU-Firmware V2.0.

  Name des Verzeichnisses:

  /mmc_cpu1

  Der Zugriff ist auf folgende Ordner der SIMATIC Memory Card möglich:

  – /DATALOGS

    Verzeichnis für Log-Dateien

  – /RECIPES

    Verzeichnis für Rezeptdateien

Hinweis

FTP-Zugriff auf die SIMATIC Memory Card der CPU: CPU-STOP möglich

Beachten Sie, dass die Karten eine begrenzte Kapazität haben. Wenn der Speicherplatz der SIMATIC Memory Card durch Speichern großer Datenmengen komplett belegt ist, geht die CPU in STOP.

- Verwenden Sie eine Karte mit ausreichender Speicherkapazität.
- Vermeiden Sie häufiges Schreiben großer Datenmengen per FTP auf die SIMATIC Memory Card.

Lesen/Schreiben über DBs der CPU

Für die FTP-Übertragung von Daten über Datenbausteine legen Sie in der CPU die entsprechenden DBs an. Wegen ihrer speziellen Struktur werden diese hier als File-DBs bezeichnet.

Der CP als FTP-Server ermittelt bei einem FTP-Kommando aus seiner Zuordnungstabelle, wie die in der CPU für den File-Transfer genutzten Datenbausteine auf Dateien abgebildet werden sollen. Die Datenbausteinzuordnung nehmen Sie in der STEP 7-Projektierung des CP vor (FTP-Konfiguration).

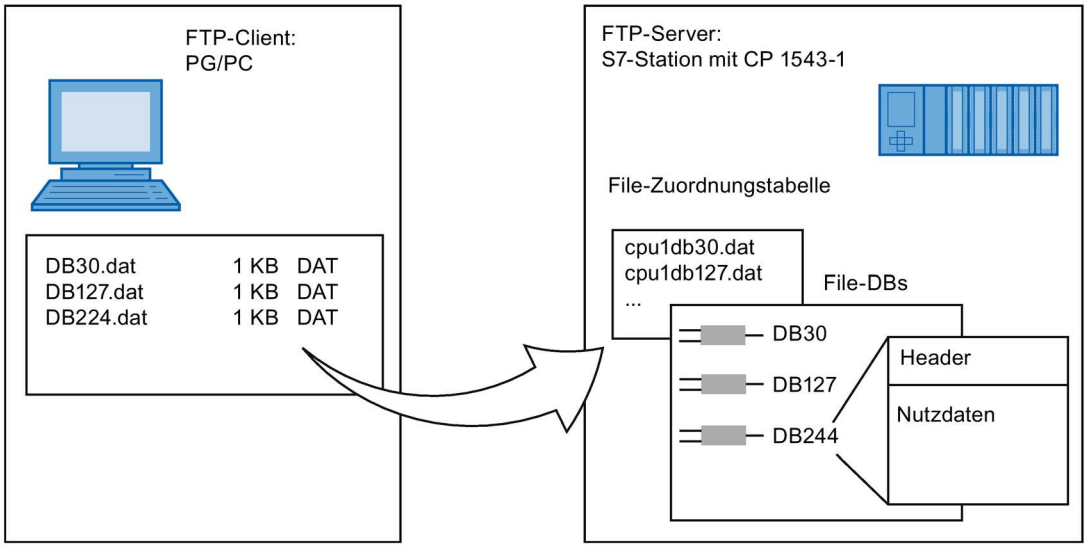


Bild 4-1 S7-CPU mit CP 1543-1 als FTP-Server für die S7-CPU-Daten

DB-Zuordnung in STEP 7

Die Felder der Tabelle der Datenbausteinzuordnung in STEP 7 haben folgende Bedeutung und Syntax:

Spaltentitel	CPU	DB	Dateiname	Kommentar
Bedeutung	Zuordnung der CPU Auswählbar über Klappliste	Nr. des Datenbausteins (File-DB) Auswählbar über Klappliste	Dem File-DB zugewiesener Dateiname Automatischer Namensvorschlag, Eintrag editierbar.	Informeller Kommentar
Beispiel	cpu1 [PLC_1]	20	cpu1_db20.dat	Messwerte Anlage 1

Hinweise zur Syntax

Für den Dateinamen eines File-DB gilt:

- Der Dateiname beginnt mit "cpuX" (mit X=1 bei S7-1500).

  Hinweis

  Beachten Sie die Schreibweise (Kleinbuchstaben für "cpu" und keine führenden Leerzeichen am Zeilenbeginn). Die Dateien werden sonst nicht erkannt.

- Länge: maximal 64 Zeichen (einschließlich der Angabe "cpuX")

FTPS-Zugriff nur bei aktivierten Security-Funktionen

Der Zugriff auf die S7-1500-Station als FTP-Server über FTPS setzt voraus, dass im STEP 7-Projekt ein Benutzer mit entsprechenden Rechten eingerichtet ist. Es ist daher erforderlich, dass beim CP die Security-Funktionen aktiviert sind. Damit stehen die Security-Einstellungen in der Globalen Benutzerverwaltung zur Verfügung.

4.8 IP-Zugriffsschutz bei programmierten Kommunikationsverbindungen

Einschränkungen bei programmierten Verbindungen und projektierten Security-Funktionen

Es ist prinzipiell möglich, Kommunikationsverbindungen über den Programmbaustein TCON programmgesteuert einzurichten und gleichzeitig über die Projektierung eine Firewall-Konfiguration vorzunehmen.

Bei der Projektierung von spezifizierten Verbindungen (aktive Endpunkte) in STEP 7 werden die IP-Adressen der Partner nicht automatisch in die Firewall-Konfiguration übernommen.

Die Projektierung des IP-Zugriffsschutzes sowie die Aspekte bei aktivierter Security sind in der Online-Hilfe von STEP 7 beschrieben.

Diagnose und Instandhaltung 5

5.1 Diagnosemöglichkeiten

Diagnosemöglichkeiten

Für die Baugruppe stehen Ihnen folgende Diagnosemöglichkeiten zur Verfügung:

- Die LEDs der Baugruppe

  Informationen zu den LED-Anzeigen finden Sie im Kapitel LEDs (Seite 22).

- STEP 7: Das Register "Diagnose" im Inspektorfenster

  Hier erhalten Sie folgende Informationen zur selektierten Baugruppe:

  – Informationen zum Online-Status der Baugruppe

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

  Hier erhalten Sie statische Informationen zur selektierten Baugruppe:

  – Allgemeine Informationen zur Baugruppe

  – Diagnosestatus

  – Informationen zur Ethernet-Schnittstelle

  – Security (bei aktivierter Security)

  Weitergehende Informationen zu den Diagnosefunktionen von STEP 7 erhalten Sie in der Online-Hilfe von STEP 7.

- SNMP

  Details zu den unterstützten Funktionen finden Sie im Kapitel Diagnose über SNMP (Seite 55).

5.2 Diagnose über SNMP

Voraussetzung

Voraussetzung für die Nutzung von SNMP ist die Aktivierung der Funktion in der Projektierung.

SNMP (Simple Network Management Protocol)

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

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

Ausführliche Informationen zu SNMP und der Siemens Automation MIB finden Sie im Handbuch "Diagnose und Projektierung mit SNMP", das Sie im Internet finden:
Link: (https://support.industry.siemens.com/cs/ww/de/ps/15392/man)

Leistungsumfang des CP

Der CP unterstützt folgende SNMP-Versionen:

- SNMPv1
- SNMPv3 (bei aktivierten Security-Funktionen)

Traps werden vom CP nicht unterstützt.

Unter SNMPv1 unterstützte MIBs

Der CP unterstützt folgende MIBs:

- **MIB II (gemäß RFC1213)**

  Der CP unterstützt folgende Gruppen von MIB-Objekten:

  – System
  – Interfaces
  – IP
  – ICMP
  – TCP
  – UDP
  – SNMP

- **LLDP MIB**
- **Siemens Automation MIB**

  Beachten Sie die Schreibrechte auf die MIB-Objekte, siehe nächster Abschnitt (SNMPv3).

Unter SNMPv3 unterstützte MIB-Objekte

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

- **MIB II (gemäß RFC1213)**

  Der CP unterstützt folgende Gruppen von MIB-Objekten:

  – System

  – Interfaces

    Das MIB-Objekt "Interfaces" liefert Zustandsinformationen über die CP-Schnittstellen.

  – IP (IPv4/IPv6)

  – ICMP

  – TCP

  – UDP

  – SNMP

  Folgende Gruppen der Standard-MIB II werden nicht unterstützt:

  – Adress Translation (AT)

  – EGP

  – Transmission

- **LLDP MIB**
- **Siemens Automation MIB**

  Beachten Sie, dass Schreibzugriffe nur für folgende MIB-Objekte der Gruppe "System" erlaubt sind:

  – sysContact

  – sysLocation

  – sysName

    Ein gesetzter sysName wird als Host-Name über die DHCP-Option 12 an den DHCP-Server zur Registrierung bei einem DNS-Server gesendet.

  Für alle anderen MIB-Objekte und Gruppen ist aus Sicherheitsgründen nur lesender Zugriff möglich.

Zugriffsrechte über Community-Namen (SNMPv1)

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

Tabelle 5- 1 Zugriffsrechte im SNMP-Agenten

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

*) Beachten Sie die Schreibweise mit Kleinbuchstaben!

5.3 Baugruppentausch ohne PG

Allgemeines Verfahren

Die Datenhaltung der Projektierungsdaten des CP erfolgt in der CPU. Damit ist der Austausch dieser Baugruppe gegen eine Baugruppe des selben Typs (identische Artikelnummer) ohne PG möglich.

Hinweis

Projektierte MAC-Adresse wird übernommen

Beachten Sie, dass bei Einstellung des ISO-Protokolls die zuvor in der Projektierung eingestellte MAC-Adresse von der CPU auf die neue CP-Baugruppe übertragen wird.

Baugruppentausch: Besonderheit bei IP-Adresse über DHCP-Server (IPv4)

Sie können bei der Projektierung im Eigenschaftendialog für den CP die IP-Konfiguration festlegen; eine Möglichkeit ist hierbei, dass der CP die IP-Adresse von einem DHCP-Server bezieht.

Hinweis

Empfehlung: Client-ID projektieren

Beachten Sie für den Baugruppentausch, dass sich bei der neuen Baugruppe die werkseitig eingestellte MAC-Adresse von der vorherigen unterscheidet. Wenn also dem DHCP-Server von der neuen Baugruppe die werkseitig eingestellte MAC-Adresse übermittelt wird, liefert dieser eine andere oder keine IP-Adresse zurück.

Vorzugsweise sollten Sie daher bei der Projektierung der IP-Konfiguration so vorgehen:

- Projektieren Sie immer eine Client-ID und konfigurieren Sie Ihren DHCP-Server entsprechend. Damit stellen Sie sicher, nach einem Austausch der Baugruppe immer die gleiche IP-Adresse vom DHCP-Server zu erhalten.

Wenn Sie in Ausnahmefällen statt der werkseitig eingestellten MAC-Adresse eine neue MAC-Adresse projektiert haben, dann wird dem DHCP-Server immer die projektierte MAC-Adresse übermittelt. In diesem Fall erhält der neue CP ebenfalls die selbe IP-Adresse wie bei der vorherigen Baugruppe.

Technische Daten

6

Beachten Sie die Angaben in der Systembeschreibung zu SIMATIC S7-1500 (Seite 9).

Zusätzlich zu den Angaben in der Systembeschreibung gelten für die Baugruppe die nachfolgenden technischen Daten.

Technische Daten - CP 1543-1	
Produktbezeichnung	CP 1543-1
Artikelnummer	6GK7 543-1AX00-0XE0
Anschluss an Industrial Ethernet	
• Anzahl	1 x Ethernet (Gigabit)-Schnittstelle
• Ausführung	RJ45-Buchse
• Übertragungsgeschwindigkeit	10 / 100 / 1000 Mbit/s
Elektrische Daten	
Spannungsversorgung	
• über S7-1500 Rückwandbus	15 V
Stromaufnahme	
• Aus Rückwandbus	350 mA
• Verlustleistung	5,3 W
Isolation	
Isolation geprüft mit	DC 707 V (Type Test)
Bauform, Maße und Gewicht	
Baugruppenformat	Kompaktbaugruppe S7-1500, einfach breit
Schutzart	IP20
Gewicht	ca. 350 g
Abmessungen (B x H x T)	35x 142 x 129 mm
Montagemöglichkeiten	Montage im S7-1500 Rack
Zulässige Leitungslängen	**(Alternative Kombinationen pro Längenbereich) ***
0 ... 55 m	• Max. 55 m IE TP Torsion Cable mit IE FC RJ45 Plug 180 • Max. 45 m IE TP Torsion Cable mit IE FC RJ45 + 10 m TP Cord über IE FC RJ45 Outlet

Technische Daten - CP 1543-1	
0 ... 85 m	• Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable mit IE FC RJ45 Plug 180 • Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord über IE FC RJ45 Outlet
0 ... 100 m	• Max. 100 m IE FC TP Standard Cable mit IE FC RJ45 Plug 180 • Max. 90 m IE FC TP Standard Cable + 10 m TP Cord über IE FC RJ45 Outlet
Produktfunktionen **	

* Zu Details siehe Katalog IK PI, Verkabelungstechnik

** Die Produktfunktionen finden Sie im Kapitel Produktübersicht, Funktionen (Seite 11).

Zulassungen

7

Erteilte Zulassungen

Hinweis

Erteilte Zulassungen auf dem Typenschild des Geräts

Die angegebenen Zulassungen - mit Ausnahme der Zertifikate für den Schiffbau - 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. Eine Ausnahme bilden die Zulassungen für den Schiffbau.

Zertifikate für den Schiffbau und Länderzulassungen

Die für das Gerät erteilten Zertifikate für den Schiffbau und spezielle Länderzulassungen finden Sie beim Siemens Industry Online Support im Internet:
Link: (https://support.industry.siemens.com/cs/ww/de/ps/15340/cert)

EU-Konformitätserklärung

CE

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

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

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

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

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

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

  Richtlinie des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten

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

Siemens Aktiengesellschaft
Division Process Industries and Drives

Process Automation
DE-76181 Karlsruhe
Deutschland

Die EU-Konformitätserklärung finden Sie auch im Internet unter folgender Adresse:
Link: (https://support.industry.siemens.com/cs/ww/de/ps/15340/cert)

Die aktuellen Fassungen der Normen können in der EU-Konformitätserklärung und in den Zertifikaten eingesehen werden.

IECEx

Das Produkt erfüllt die Anforderungen an den Explosionsschutz nach IECEx.

IECEx-Klassifikation: Ex nA IIC T4 Gc

Das Produkt erfüllt die Anforderungen der nachfolgenden Normen:

- EN 60079-0

  Explosionsgefährdete Bereiche - Teil 0: Betriebsmittel - Allgemeine Anforderungen

- EN 60079-15

  Explosionsfähige Atmosphäre - Teil 15: Geräteschutz durch Zündschutzart 'n'

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/15340/cert)

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx (Seite 26) 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".

Angewandte Normen:

- EN 60079-0

  Explosionsgefährdete Bereiche - Teil 0: Betriebsmittel - Allgemeine Anforderungen

- EN 60079-15

  Explosionsfähige Atmosphäre - Teil 15: Geräteschutz durch Zündschutzart 'n'

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

ATEX-Zulassung: II 3 G Ex nA IIC T4 Gc

Prüfnummer: DEKRA 12 ATEX 0240X

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx (Seite 26) müssen erfüllt sein.

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

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

EMV

Das Produkt erfüllt bis 19.04.2016 Anforderungen der EU-Richtlinie 2014/30/EU "Elektromagnetische Verträglichkeit" (EMV-Richtlinie).

Angewandte Normen:

- EN 61000-6-4

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

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

RoHS

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

Angewandte Norm:

- EN 50581:2012

c(UL)us

Angewandte Normen:

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

Report / UL file: E 85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

HAZ. LOC.

Angewandte Normen:

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

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta: Siehe Temperaturklasse auf dem Typenschild des CP

Report / UL file: E223122 (NRAG, NRAG7)

Beachten Sie die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß UL HazLoc (Seite 27).

Hinweis

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

CSA

CSA Certification Mark Canadian Standard Association (CSA) nach Standard C 22.2 No. 142:

- Certification Record 063533–C-000

FM

Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

Entnehmen Sie die Temperaturklasse dem Typenschild auf der Baugruppe.

Australien - RCM

Das Produkt erfüllt die Anforderungen der Normen nach AS/NZS 2064 (Klasse A).

Kanada

Dieses Digitalgerät Klasse A erfüllt die Anforderungen der Norm Canadian ICES-003.

AVIS CANADIEN

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

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

Beachten Sie, dass dieses Gerät bezüglich der Emission von Funkstörungen der Grenzwertklasse A entspricht. Dieses Gerät ist einsetzbar in allen Bereichen außer dem Wohnbereich.

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/15340/cert)

Index

A

Anschluss eines Switch, 34
Anweisung
  FTP_CMD, 19, 21
  T_CONFIG, 21
  TCON, TSEND/TRCV, 21
  TDISCON, 21
  TMAIL_C, 21
  TSEND_C/TRCV_C, 21
  TUSEND/TURCV, 21
Anzahl
  betreibbarer CPs, 20
Anzahl Verbindungen, 17
Autocrossing-Mechanismus, 34
Autosensing, 34

B

Bandbreitenbegrenzung, 15
Baugruppentausch
  Besonderheit bei IP-Adresse über DHCP-Server (IPv4), 58
Baustein-Laufzeit, 19
Besondere Hinweise
  Anschluss eines Switch, 34
  Empfehlung für die Zeitvorgabe, 44
  Gültige Uhrzeit sicherstellen, 44
  Verhalten bei fehlendem Verweis auf den FTP-Auftragsblock, 50

D

Datenhaltung der Projektierungsdaten des CP, 58
DHCP-Server, 58
Diagnosemöglichkeiten, 55
Doppeladressierung im Netzwerk, 35
Downloads, 10

E

E-Mail, 12, 17, 21
EMV - Elektromagnetische Verträglichkeit, 61
Entsorgung, 5
Ethernet-Schnittstelle, 11, 24
Etherrnet-Schnittstelle
  Anschlussbelegung, 29

F

FETCH/WRITE, 13, 17
  S5-/S7-Adressierungsmodus, 15
Firewall, 15
Firewall-Konfiguration, 54
Firmware-Version, 11
FTP, 21, 48
FTP (FTP-Client), 16
FTP im Client-Betrieb
  Mengengerüst, 19
FTP im Server-Betrieb
  Mengengerüst, 19
FTP_CMD, 48
FTPS, 48
FTPS - Security, 53
FTPS (expliziter Modus), 15

G

Gateway, 41
gekreuztes Kabel, 34
Gesamtmengengerüst, 20
Gigabit-Spezifikation, 24
Globale Firewall-Regeln, 15
Glossar, 5

H

Hardware-Erzeugnisstand, 11
HMI-Kommunikation, 12

I

Inbetriebnahme
  Vollständigkeit der STEP 7-Projektdaten, 28
IP-Adresse
  IPv6, 14
  über DHCP, 35
IP-Konfiguration
  IPv4 / IPv6, 14
IP-Routing, 35

IPSec-Tunnel
Anzahl, 19
IP-Zugriffsschutz, 54
ISO, 21
ISO-on-TCP, 21
ISO-on-TCP (gemäß RFC 1006), 12
ISO-on-TCP-Verbindungen, 17
ISO-Transport (gemäß RFC 8073), 12
ISO-Transportverbindungen, 17
IT-Funktionen, 13

K

Konfiguration der Ethernet-Schnittstelle, 21
Anweisung, 21

L

Laden der Projektdaten, 29
LED-Anzeige, 22
Logging, 15

M

MAC-Adresse, 11, 13, 58
Manual Collection, 10
Max. Datenlänge für Programmbausteine, 17
MIB, 55
Montage und Inbetriebnahme, 28
Vorgehensweise, 28
Multicast
über UDP, 12

N

NTP (secure), 15, 44
NTP-Server, 44
NTP-Verfahren, 13

O

Online-Hilfe von STEP 7, 29
Open User Communication (OUC), 12
OP-Verbindungen
Anzahl, 18
OUC (Open User Communication), 45

P

Passiver VPN-Verbindungsaufbau, 41
PG-Kommunikation, 12
PG-Verbindungen
Anzahl, 18
Port 8448, 42
PROFINET-Schnittstelle
LED-Anzeigen, 24
Programmbaustein, (Anweisung)
Programmierte Kommunikationsverbindung, 54
Projektierung, 28
Projektierung und Laden der Projektierungsdaten, 20

R

Recycling, 5

S

S5-/S7-Adressierungsmodus, 15
S7-Kommunikation, 12
S7-Routing-Funktion, 30
S7-Verbindungen, 12, 16
Anzahl frei nutzbarer, 18
Security-Diagnose ohne Port 102, 42
Security-SDTs, 46
Sicherheitshinweise, 25
SIMATIC NET, 10
SIMATIC NET-Glossar, 5
SMTPS, 16
SNMP, 55
SNMP-Agent, 13
SNMPv3, 16
Stateful Packet Inspection (Layer 3 und 4), 15
STEP 7, 4, 20
Stromversorgungsmodule
zusätzliche, 20
Systemdatentyp
CONF_DATA, 21
FTP_CONNECT_IPV4, 21
FTP_CONNECT_IPV6, 21
FTP_CONNECT_NAME, 21
FTP_FILENAME, 21
FTP_FILENAME_PART, 21
TCON_Configured, 21
TCON_IP_v4, 21, 21
TCON_ISOnative, 21, 21
TMAIL_FQDN, 21
TMail_v4, 21
TMail_v6, 21
Systemdatentypen (SDTs), 46

T

TCON, 54
TCP, 21
TCP (gemäß RFC 793), 12
TCP-Verbindungen, 17
TCP-Verbindungen für FTP, 19

U

UDP
    Einschränkungen, 18
UDP (gemäß RFC 768), 12
UDP-Telegramm-Pufferung, 18
UDP-Verbindungen, 17
Uhrzeitsynchronisation, 30
Uhrzeitsynchronisierung, 13
Umschalten der CPU
    von RUN auf STOP, 30

V

Verbindungen für Web
    Anzahl, 18
Verbindungsressourcen der CPU, 16
Versionshistorie, 10
Virtual Private Network
    Definition, 36
VPN, (Virtual Private Network)
    Anwendungsgebiete, 37
    Zellenschutzkonzept, 37

W

Webdiagnose, 30
Webserver, 14

Z

Zellenschutzkonzept
    VPN, 37