

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

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.

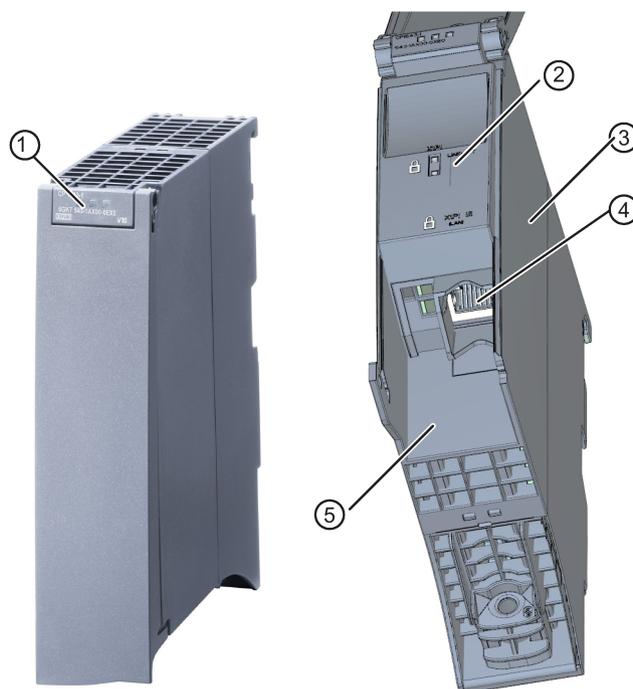
Vorwort

Artikelnummer, Gültigkeit und Produktbezeichnungen

In dieser Beschreibung finden Sie Informationen zu folgendem Produkt:

CP 1543-1
Artikelnummer 6GK7 543-1AX00-0XE0
Hardware-Erzeugnisstand 2
Firmware-Version V2.2
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 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!

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 V2.2 mit folgenden neuen Funktionen:
 - Unterstützung der virtuellen Schnittstelle der CPU, siehe Kapitel Die virtuelle Schnittstelle der CPU (Seite 37).
- Neue ATEX-/IECEX-Zulassung
- Redaktionelle Überarbeitung

Versionshistorie

- Firmware-Version V2.1 mit folgenden neuen Funktionen:
 - Erweiterte Security-Einstellungen bei IP-Routing über den Rückwandbus, siehe Kapitel IP-Routing (Seite 36).
- 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 05/2017

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

In diesem Dokument werden folgende Abkürzungen stellvertretend für die jeweils vollständige Bezeichnung verwendet:

- CP
Verwendung für die vollständige Produktbezeichnung CP 1543-1
- STEP 7
Verwendung für das Projektierungswerkzeug STEP 7 Professional

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 einen Bestandteil eines solchen Konzepts.

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

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

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

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

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

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

Firmware

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

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>)

Gerät defekt

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

Recycling und Entsorgung



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

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

Beachten Sie die örtlichen Bestimmungen.

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

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

Inhaltsverzeichnis

	Vorwort	3
1	Wegweiser Dokumentation	9
2	Produktübersicht, Funktionen	11
2.1	Kommunikationsdienste.....	11
2.2	Weitere Funktionen.....	12
2.3	Industrial Ethernet Security.....	14
2.4	Mengengerüst und Leistungsdaten	15
2.4.1	Allgemeine Kenndaten.....	15
2.4.2	Kenndaten S7-Kommunikation	17
2.4.3	Kenndaten für den FTP / FTPS-Betrieb	17
2.4.4	Kenndaten Security.....	18
2.5	Voraussetzungen für den Einsatz.....	18
2.5.1	Mengengerüst.....	18
2.5.2	Projektierung.....	19
2.5.3	Programmbausteine - Übersicht	19
2.6	LEDs	21
2.7	Gigabit-Schnittstelle	23
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 den CP	30
4	Projektierung, Programmierung	31
4.1	Security-Empfehlungen	31
4.2	Einschränken von Kommunikationsdiensten in der CPU	34
4.3	Netzwerkeinstellungen.....	35
4.4	IP-Konfiguration	36
4.4.1	Besonderheiten zur IP-Konfiguration.....	36
4.4.2	Wiederanlauf nach Erkennen einer IP-Doppeladressierung im Netzwerk	36
4.4.3	IP-Routing	36
4.4.4	Die virtuelle Schnittstelle der CPU.....	37
4.4.5	Programmierte Verbindungen: Einschränkung der Firewall-Regeln	40
4.5	Uhrzeitsynchronisation	41

4.6	DNS-Konfiguration	42
4.7	FTP-Kommunikation	42
4.7.1	FTP-Server.....	42
4.7.1.1	Projektierung der FTP-Server-Funktion.....	42
4.7.2	FTP-Client.....	45
4.7.2.1	Der Programmbaustein FTP_CMD (FTP-Client-Funktion).....	45
4.7.2.2	Eingangsparameter FTP_CMD.....	47
4.7.2.3	Auftragsblöcke für FTP_CMD	49
4.7.2.4	Ausgangsparameter und Statusinformationen FTP_CMD	54
4.7.2.5	Aufbau des Datenbausteins (File-DB) für den FTP-Client-Betrieb	58
4.8	Security	61
4.8.1	Security-Benutzer	61
4.8.2	VPN.....	61
4.8.2.1	VPN-Tunnelkommunikation zwischen S7-1500-Stationen anlegen	63
4.8.2.2	VPN-Tunnelkommunikation zwischen CP und SCALANCE M aufbauen.....	65
4.8.2.3	VPN-Tunnelkommunikation mit SOFTNET Security Client	65
4.8.2.4	CP als passiver Teilnehmer von VPN-Verbindungen.....	66
4.8.3	Firewall.....	66
4.8.3.1	Firewall-Reihenfolge bei der Prüfung ein- und ausgehender Telegramme	66
4.8.3.2	Schreibweise der Quell-IP-Adresse (erweiterter Firewall-Modus).....	66
4.8.3.3	HTTP und HTTPS über IPv6 nicht möglich	67
4.8.3.4	Firewall-Einstellungen für Verbindungen über VPN-Tunnel	67
4.8.4	Online-Funktionen.....	67
4.8.4.1	Einstellungen für Online-Security-Diagnose und Laden in Station bei aktivierter Firewall.....	67
4.8.4.2	Online-Security-Diagnose über Port 8448	68
4.8.5	Log-Einstellungen - Filtern der System-Ereignisse.....	68
4.9	Programmbausteine für OUC	68
5	Diagnose und Instandhaltung	73
5.1	Diagnosemöglichkeiten.....	73
5.2	Online verbinden	74
5.3	Diagnose über SNMP	75
5.4	Firmware aktualisieren.....	77
5.5	Baugruppentausch ohne PG.....	80
6	Technische Daten.....	81
6.1	Technische Daten des CP	81
6.2	Belegung der Ethernet-Schnittstelle	82
6.3	Zulässige Leitungslängen - Ethernet	82
6.4	Zulässige Leitungslängen - Gigabit-Ethernet.....	82
7	Zulassungen	83
	Index.....	89

Wegweiser Dokumentation

Dokumentation für die S7-1500

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 oder Betriebsanleitungen.

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

Die folgende Tabelle zeigt weitere Dokumente, welche das vorliegende Handbuch zum CP ergänzen und im Internet erhältlich sind.

Tabelle 1- 1 Übersicht der Dokumentation für die S7-1500

Thema	Dokumentation	Wichtigste Inhalte
Beschreibung des Systems	Systemhandbuch Automatisierungssystem S7-1500 (https://support.industry.siemens.com/cs/ww/de/view/59191792)	<ul style="list-style-type: none"> • Einsatzplanung • Montage • Anschließen • Inbetriebnehmen
Systemdiagnose	Funktionshandbuch Systemdiagnose (https://support.industry.siemens.com/cs/ww/de/view/59192926)	<ul style="list-style-type: none"> • Überblick • Diagnoseauswertung Hardware/Software
Kommunikation	Funktionshandbuch Kommunikation (https://support.industry.siemens.com/cs/ww/de/view/59192925)	<ul style="list-style-type: none"> • Überblick
	Funktionshandbuch Webserver (https://support.industry.siemens.com/cs/ww/de/view/59193560)	<ul style="list-style-type: none"> • Funktion • Bedienung
	SIMATIC NET - Industrial Ethernet / PROFINET - Systemhandbuch <ul style="list-style-type: none"> • Industrial Ethernet Link: (https://support.industry.siemens.com/cs/w/de/view/27069465) • Passive Netzkomponenten Link: (https://support.industry.siemens.com/cs/w/de/view/84922825) 	<ul style="list-style-type: none"> • Ethernet-Netze • Netzprojektierung • Netzwerkkomponenten

Thema	Dokumentation	Wichtigste Inhalte
Steuerungen störsicher aufbauen	Funktionshandbuch Steuerungen störsicher aufbauen (https://support.industry.siemens.com/cs/ww/de/view/59193566)	<ul style="list-style-type: none"> • Grundlagen • Elektromagnetische Verträglichkeit • Blitzschutz • Gehäuseauswahl
Zyklus- und Reaktionszeiten	Funktionshandbuch Zyklus- und Reaktionszeiten (https://support.industry.siemens.com/cs/ww/de/view/59193558)	<ul style="list-style-type: none"> • Grundlagen • Berechnungen

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

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.

2.1 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 (IPv4/IPv6) (gemäß RFC 793 und 8200)

Mit der Schnittstelle über TCPv4/v6-Verbindungen unterstützt der CP die auf nahezu jedem Endsystem vorhandene Socket-Schnittstelle zu TCP/IP.

- ISO-on-TCP (gemäß RFC 1006)
- UDP (gemäß RFC 768)
- 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 Authentifizierung an einem E-Mail-Server.

- **S7-Kommunikation**

- PG-Kommunikation
- Bedien- und Beobachtungsfunktionen (HMI-Kommunikation)
- Datenaustausch über S7-Verbindungen

- **FTP/FTPS**

FTP-Funktionen (File Transfer Protocol) für Dateiverwaltung und Zugriffe auf Datenbausteine in der CPU

- FTP-Server

Aktivierbar über die Projektierung

- FTP-Client

Parametrierbar über Programmbausteine.

- **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.

2.2 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 Verbindungsprojektion (IPv4) auch über das Anwenderprogramm zugewiesen werden (Programmbausteine siehe Kapitel Programmbausteine - Übersicht (Seite 19)).

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 36).

IPv6-Adressen - Nutzungsbereich im CP

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

- FETCH/WRITE-Zugriff (CP ist Server)
- FTP-Server-Betrieb
- FTP-Client-Betrieb mit Adressierung über Programmbaustein
- E-Mail-Übertragung mit Adressierung über Programmbaustein
- TCP über OUC-Bausteine mit folgenden SDTs: TCON_QDN, TCON_QDN_SEC
- SNMP

Beachten Sie bei Verwendung von IPv6-Adressen, den DNS-Server entsprechend zu konfigurieren.

Zugang zum Webserver der CPU

Über die LAN-Schnittstelle des CP haben Sie Zugang zum Webserver der CPU. Mit Hilfe des Webserver 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.

2.3 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 angeschlossenen externen Netz kann durch unterschiedliche Sicherheitsmaßnahmen geschützt werden vor:

- Datenspionage (FTPS, HTTPS)
- Datenmanipulation
- Unberechtigte Zugriffe

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 Nicht-IP-Frames gemäß IEEE 802.3 (Layer 2)
 - Begrenzung der Übertragungsgeschwindigkeit
 - Globale und benutzerspezifische Firewall-Regeln

Die Schutzfunktion der Firewall kann sich über den Betrieb einzelner oder mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.

- Logging

Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mithilfe von STEP 7 ausgelesen oder automatisch an einen Syslog-Server gesendet werden können.
- FTPS (expliziter Modus)

Zur verschlüsselten Übertragung von Dateien
- NTP (secure)

Zur gesicherten Uhrzeitsynchronisation

- 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).

2.4 Mengengerüst und Leistungsdaten

2.4.1 Allgemeine Kenndaten

Merkmal	Erläuterung / Werte
Anzahl frei nutzbarer Verbindungen über Industrial Ethernet insgesamt	118 Der Wert gilt für die Gesamtsumme der Verbindungen folgender Typen: <ul style="list-style-type: none"> • 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.

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 (ISO-Transport + ISO-on-TCP + TCP + UDP + FETCH/WRITE + E-Mail): <ul style="list-style-type: none"> • Insgesamt max. 118 Davon jeweils maximal: <ul style="list-style-type: none"> – TCP-Verbindungen: 0...118 – ISO-on-TCP-Verbindungen: 0...118 – ISO-Transportverbindungen: 0...118 – UDP-Verbindungen (spezifizierte und freie) insgesamt: 0...118 – Verbindung für E-Mail: 0...1 – Verbindungen für FETCH/WRITE: 0...16

Merkmal	Erläuterung / Werte
Max. Datenlänge für Programmbausteine	Die Programmbausteine ermöglichen den Transfer von Nutzdaten folgender Längen: <ul style="list-style-type: none"> • ISO-on-TCP, TCP, ISO-Transport: 1 bis 64 kB • UDP: 1 Byte bis 2 kB • E-Mail <ul style="list-style-type: none"> – Auftragsheader + Nutzdaten: 1 bis 256 Byte – E-Mail-Anhang: bis 64 kB
LAN-Schnittstelle - vom CP erzeugte max. Datenblocklänge pro Protokolleinheit (TPDU = transport protocol data unit)	<ul style="list-style-type: none"> • für Senden <ul style="list-style-type: none"> – ISO-Transport, ISO-on-TCP, TCP: 1452 Byte / TPDU • für Empfangen <ul style="list-style-type: none"> – 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.

2.4.2 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)	<ul style="list-style-type: none">Für Senden: 480 Byte / PDUFür Empfangen: 480 Byte / PDU
Anzahl reservierbare OP-Verbindungen *	Max. 4
Anzahl reservierbare PG-Verbindungen *	Max. 4
Anzahl HTTP-Verbindungen für Web	Max. 4

* Die CPU reserviert Verbindungsressourcen. Berücksichtigen Sie die angegebenen Werte auch für programmierte Verbindungen.

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.

2.4.3 Kenndaten für den FTP / FTPS-Betrieb

TCP-Verbindungen für FTP

FTP-Aktionen werden vom CP über TCP-Verbindungen übertragen. Es gelten folgende Kenndaten:

- FTP-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-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 für FTP-Client-Betrieb

Für die Kommunikation nutzen Sie den 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.

2.4.4 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")

2.5 Voraussetzungen für den Einsatz

2.5.1 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.

2.5.2 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.

2.5.3 Programmbausteine - Übersicht

Programmbausteine - Übersicht

Folgende Programmbausteine (Anweisungen) stehen für den CP zur Verfügung.

Tabelle 2- 1 Bausteine der Open User Communication

Protokoll	Programmbaustein (Anweisung)	Systemdatentyp
TCP	<ul style="list-style-type: none"> • TSEND_C/TRCV_C oder • TCON/TDISCON + TSEND/TRCV 	<ul style="list-style-type: none"> • TCON_IP_v4 • TCON_QDN • TCON_QDN_SEC • TCON_Configured
ISO-on-TCP		<ul style="list-style-type: none"> • TCON_IP_RFC
ISO		<ul style="list-style-type: none"> • TCON_ISOnative
UDP	<ul style="list-style-type: none"> • TCON/TDISCON + TUSEND/TURCV 	<ul style="list-style-type: none"> • TCON_IP_v4
E-Mail	<ul style="list-style-type: none"> • TMAIL_C 	<ul style="list-style-type: none"> • TMAIL_V4 • TMAIL_QDN • TMAIL_QDN_SEC • TMAIL_V6 • TMAIL_V6_SEC

Tabelle 2- 2 Baustein für Kommunikationsdienste des CP

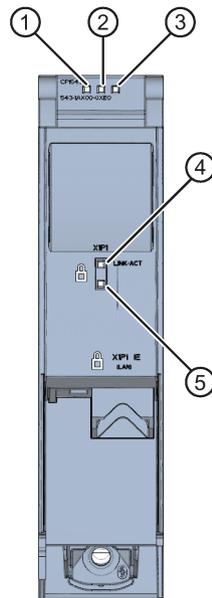
Protokoll	Programmbaustein (Anweisung)	Systemdatentyp
FTP	<ul style="list-style-type: none"> FTP_CMD 	<ul style="list-style-type: none"> FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME FTP_FILENAME FTP_FILENAME_PART

Tabelle 2- 3 Baustein für die Konfiguration der Ethernet-Schnittstelle oder eines NTP-/DNS-Servers

Funktion	Programmbaustein (Anweisung)	Systemdatentyp
Konfiguration der Ethernet-Schnittstelle	<ul style="list-style-type: none"> T_CONFIG 	<ul style="list-style-type: none"> IF_CONF_V4 IF_CONF_V6 IF_CONF_NTP IF_CONF_DNS IF_CONF_MAC

2.6 LEDs

LEDs



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

Bild 2-1 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.

2.6 LEDs

Tabelle 2- 4 Bedeutung der LEDs "RUN", "ERROR", "MAINT"

RUN	ERROR	MAINT	Bedeutung
 LED aus	 LED aus	 LED aus	Keine oder zu geringe Versorgungsspannung 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 (zweifarbige grün/gelb) ist dem Port der Ethernet-Schnittstelle zugeordnet. Die folgende Tabelle zeigt die LED-Bilder.

Tabelle 2- 5 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 Kommunikationspartner besteht.
 grün ein	 gelb flackert	Zum aktuellen Zeitpunkt werden Daten über die Ethernet-Schnittstelle des Ethernet-Geräts von einem Kommunikationspartner im Ethernet empfangen/gesendet.

2.7 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

3.1 Wichtige Hinweise zum Geräteinsatz

Sicherheitshinweise für den Geräteinsatz

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

ACHTUNG
<p>Anschlüsse am LAN (Local Area Networks)</p> <p>Ein LAN oder LAN-Segment mit den zugehörigen Anschlüssen sollte sich innerhalb einer einzigen Niederspannungsversorgungseinrichtung und innerhalb eines einzigen Gebäudes befinden.</p> <p>Stellen Sie sicher, 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.</p> <p>Stellen Sie nie eine direkte elektrische Verbindung her zu TNV-Netzen (Telefon-Netzwerk) oder WAN (Wide Area Network).</p>

3.1.1 Hinweise für den Einsatz im Ex-Bereich

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

 WARNUNG
<p>EXPLOSIONSGEFAHR</p> <p>In einer leicht entzündlichen oder brennbaren Umgebung dürfen keine Leitungen an das Gerät angeschlossen oder vom Gerät getrennt werden.</p>

 **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**

Kabel

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

 **WARNUNG**

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

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

 **WARNUNG**

EXPLOSIONSGEFAHR

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 °C 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-Projektdateien.

Vorgehensweise zur Montage und Inbetriebnahme

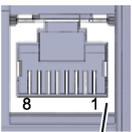
Schritt	Ausführung	Hinweise und Erläuterungen
1	Gehen Sie bei der Montage und dem Anschließen entsprechend den Beschreibungen zur Montage von Peripheriemodulen im Systemhandbuch "Automatisierungssystem S7 1500" vor.	
2	Schließen Sie den CP über die RJ-45-Buchse an Industrial Ethernet an.	Unterseite des 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-Projektdateien.	<p>Die STEP 7-Projektdateien des CP werden beim Laden der Station mit übertragen. Schließen Sie zum Laden der Station die Engineering-Station, auf der sich die Projektdateien befinden, an die Ethernet-Schnittstelle der CPU an.</p> <p>Weitere Details zum Laden entnehmen Sie folgenden Kapiteln der Online-Hilfe von STEP 7:</p> <ul style="list-style-type: none"> • "Projektdateien 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
 <p>Schirmung</p>	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 den CP

Umschalten der CPU: RUN → STOP

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

Hinweis

RUN/STOP-LED des CP

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

Im Zustand STOP der CPU bleibt der CP im Zustand RUN. Für den CP gilt das folgende Verhalten:

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

Projektierung, Programmierung

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 Zellschutzkonzept mit entsprechenden Produkten.
- Verbinden Sie das Gerät nicht direkt mit dem Internet. Betreiben Sie das Gerät innerhalb eines geschützten Netzwerkbereichs.
- Informieren Sie sich regelmäßig über Neuigkeiten auf den Siemens-Internetseiten.
 - Hier finden Sie Informationen zu Industrial Security:
Link: (<http://www.siemens.com/industrialsecurity>)
 - Hier finden Sie Informationen zu Security in der industriellen Kommunikation:
Link: (<http://w3.siemens.com/mcms/industrial-communication/de/ie/industrial-ethernet-security/Seiten/industrial-security.aspx>)
 - Eine Auswahl an Dokumenten zum Thema Netzwerksicherheit finden Sie hier:
Link: (<https://support.industry.siemens.com/cs/ww/de/view/92651441>)
- Halten Sie die Firmware aktuell. Informieren Sie sich regelmäßig über Sicherheits-Updates der Firmware und wenden Sie diese an.

Hinweise auf Produktneuigkeiten und neue Firmware-Versionen finden Sie unter folgender Adresse:

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

Physikalischer Zugang

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

Netzanschluss

Schließen Sie den CP nicht direkt an das Internet an. Wenn ein Anschluss des CP an das Internet gewünscht ist, dann aktivieren Sie die Security-Funktionen oder 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.
- Deaktivieren Sie DHCP an Schnittstellen zu öffentlichen Netzen wie bspw. dem Internet, um IP-Spoofing vorzubeugen.

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
DCP	93 (UDP)	Offen	Offen	Nein
S7- und Online-Verbindungen	102 (TCP)	Offen	Offen *	Nein
Online-Security-Diagnose	8448 (TCP)	Geschlossen	Offen nach Konfiguration	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)

* Zur Vermeidung des Öffnens von Port 102 bei der Diagnose siehe Kapitel Online-Security-Diagnose über Port 8448 (Seite 68).

Ports von Kommunikationspartnern und Routern

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

Dies können sein:

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP) - im CP offen bei Bausteinaufruf (nur ausgehend)
- SMTPS / 587 (TCP) - im CP offen bei Bausteinaufruf (nur ausgehend)

4.2 Einschränken von Kommunikationsdiensten in der CPU

Kommunikationsdienste ohne Verbindungen

Die CPU kann Server für eine Reihe von Kommunikationsdiensten sein, ohne dass für die CPU Verbindungen projektiert sind. Andere Kommunikationsteilnehmer können auf CPU-Daten zugreifen. Damit entfällt für die lokale CPU als Server die Möglichkeit, die Kommunikation zu den Clients zu kontrollieren.

Die Zulässigkeit dieser Kommunikationsdienste wird durch den Parameter "Verbindungsmechanismen" in der Parametergruppe "Schutz & Security" der CPU eingestellt.

"Zugriff über PUT/GET-Kommunikation durch entfernten Partner erlauben"

- Option aktiviert

Der Client-seitige Zugriff auf CPU-Daten ist erlaubt.

- Option deaktiviert

Lesender und schreibender Zugriff auf CPU-Daten ist nur möglich bei Kommunikationsverbindungen, die eine Projektierung bzw. Programmierung sowohl für die lokale CPU als auch für den Kommunikationspartner voraussetzen.

Verbindungen, für welche die lokale CPU nur Server ist (keine Projektierung/Programmierung der Kommunikation zum Partner), sind nicht möglich.

Die folgenden Kommunikationsdienste des CP beziehen sich auf eine CPU \geq V2.

Bei deaktivierter Option sind nicht möglich:

- PUT/GET-Zugriff über den CP
- FETCH/WRITE-Zugriff über den CP

Bei deaktivierter Option ist möglich:

- FTP-Zugriff über den CP

4.3 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.

4.4 IP-Konfiguration

4.4.1 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.

4.4.2 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.

4.4.3 IP-Routing

IP-Routing über den Rückwandbus

Der CP unterstützt statisches IP-Routing (IPv4) zu weiteren CMs/CPs:

- CP 1545-1
- CM 1542-1 V2.0
- CP 1543-1 V2.0

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 folgenden Parameter aktivieren:
"Ethernet-Schnittstelle > Ethernet-Adressen > IP-Routing zwischen Kommunikationsmodulen"

Beachten Sie:

Wenn Sie mehrere CPs in einer Station verwenden und IP-Routing nutzen möchten, dann dürfen Sie in der Station nur für einen CP einen Router projektieren.

Bei Aktivierung der Security-Funktion werden zusätzlich IP-Firewall-Regeln angelegt, die Sie im erweiterten Firewall-Modus in den globalen Security-Einstellungen anpassen können.

4.4.4 Die virtuelle Schnittstelle der CPU

Der CP 1543-1 unterstützt die virtuelle Schnittstelle der CPU.

Voraussetzung

Für die Nutzung der virtuellen Schnittstelle der CPU müssen folgende Voraussetzungen erfüllt sein:

- S7-1500-CPU ab Firmware V2.8
R/H-CPU's unterstützen die Funktion nicht.
- CP 1543-1 ab Firmware V2.2
Die Security-Funktionen des CP sind deaktiviert.
- Projektierbarkeit: Ab STEP 7 V16

Die virtuelle Schnittstelle der CPU

Die S7-1500 CPU bietet ab Firmware Version V2.8 die Möglichkeit, ihre IP-basierten Anwendungen wie z. B. OPC UA nicht nur über ihre lokalen PROFINET-Schnittstellen zu erreichen, sondern auch über die Schnittstelle eines CP 1543-1 in derselben Station.

Die virtuelle Schnittstelle hat die Bezeichnung W1.

Merkmale der virtuellen Schnittstelle

Die virtuelle Schnittstelle ist keine voll diagnosefähige Schnittstelle mit den bekannten Eigenschaften herkömmlicher Schnittstellen. In den grafischen Sichten wird die virtuelle Schnittstelle nicht angezeigt, da die interne Verbindung über den Rückwandbus kein S7-Subnetz darstellt und keine Ports hat. Eine physikalische Verbindung durch ein Netzkabel kann daher nicht hergestellt werden.

Die folgenden IP-basierten Dienste können auch über die virtuelle Schnittstelle erreicht werden:

- OPC UA (Client und Server)
- Programmierte OUC-Verbindungen
- S7-Kommunikation: ES/HMI-Zugriff und Anweisungen für S7-Kommunikation wie z. B. PUT/GET

Die IP-Adresse der virtuellen Schnittstelle wird in STEP 7 und im Display der CPU angezeigt.

Die aktivierte Schnittstelle kann in der Projektierung der Kommunikationspartner verwendet werden.

Zu Einschränkungen der virtuellen Schnittstelle gegenüber physischen Schnittstellen siehe STEP 7-Informationssystem.

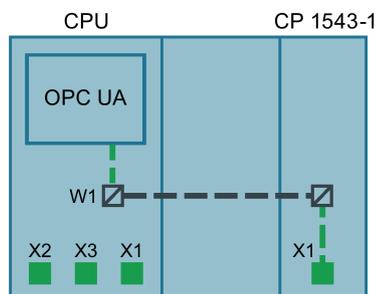


Bild 4-1 Prinzip der virtuellen Schnittstelle

Konfiguration der virtuellen Schnittstelle W1

Die virtuelle Schnittstelle wird in STEP 7 in der Parametergruppe "Erweiterte Konfiguration > Zugriff auf PLC über Kommunikationsmodul" projektiert.

Dort wird die virtuelle Schnittstelle einem CP der Station zugewiesen, über den von außen auf die CPU zugegriffen werden kann. In der Klappliste sind die projektierten CPs der Station auswählbar.

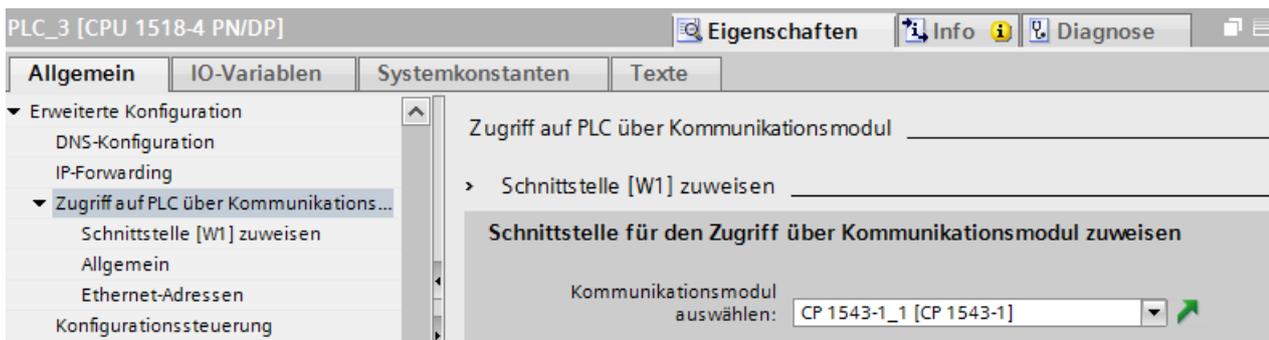


Bild 4-2 Auswahl des CP in den Eigenschaften der CPU

Nach der Auswahl des CP projektieren Sie die IP- und PROFINET-Parameter der virtuellen Schnittstelle.

Beachten Sie folgende Regeln:

- Die IP-Adresse der virtuellen Schnittstelle und die IP-Adressen der PROFINET-Schnittstellen der CPU müssen in unterschiedlichen, disjunkten Adressbändern liegen.
- Die IP-Adresse der virtuellen Schnittstelle muss im Subnetz der Ethernet-Schnittstelle des CP liegen, damit die Dienste des CP von der CPU aus erreicht werden können und umgekehrt.

Nach dem Laden der Projektierungsdaten sind die CPU-Dienste wie der OPC UA-Server über den CP und die virtuelle Schnittstelle erreichbar.

Die IP-Adresse der virtuellen Schnittstelle erscheint im Eigenschaftsdialog des OPC UA-Servers der CPU in der Liste der Server-Adressen. Angelegte Verbindungen und S7-Kommunikation (z. B. HMI und BSEND, BRCV) laufen über diese Schnittstelle.

Die IP-Adresse der virtuellen Schnittstelle W1 steht im Geräte-Display nicht unter den aktuell angezeigten lokalen Schnittstellen (Xn), sondern unter "Adressen" im Abschnitt "Einstellungen". Die virtuelle Schnittstelle ist auch dann sichtbar, wenn kein CP gesteckt oder die virtuelle Schnittstelle deaktiviert ist. Wenn keine IP-Projektierung vorhanden ist, werden IP-Adresse und Subnetzmaske mit 0.0.0.0 angezeigt.

Die virtuelle Schnittstelle W1 wird in der Diagnosesicht unter "Online & Diagnose" angezeigt.

In den CPU-Eigenschaften wird die Hardware-Kennung der virtuellen Schnittstelle in den Systemkonstanten angezeigt.

Hinweis

Adressänderung zur Laufzeit und Neustart

Wenn die IP-Parameter der virtuellen Schnittstelle geladen sind, können Sie diese anschließend über das Display der CPU, über T_CONFIG oder online ändern.

Beachten Sie aber, dass nach einem Neustart der CPU wieder die ursprünglich geladene Konfiguration aktiv ist.

Konfigurationsänderungen

Eine Änderung des zugewiesenen CP kann sich auf die Konfiguration der virtuellen Schnittstelle auswirken:

- Änderungen in der Projektierung
 - Zuweisung eines anderen CP
Die Konfiguration wird für den neuen CP übernommen.
 - Abwahl des zugewiesenen CP
Die virtuelle Schnittstelle W1 wird deaktiviert und die Konfiguration geht verloren.
Bei erneuter Zuweisung eines CP müssen Sie die virtuelle Schnittstelle erneut projektieren.

- Änderungen an der Stationskonfiguration
 - Verschieben des CP

Wenn der CP auf einen anderen Steckplatz des Geräts verschoben wird, bleibt die Konfiguration gültig.
 - Entfernen des CP

Wenn der CP aus der Station gezogen wird, bleibt die Konfiguration in der CPU erhalten.

In der Klappliste der Parametergruppe der CPU wird der CP als fehlend angezeigt und beim Übersetzen der Konfiguration ein Fehler ausgegeben. Zur Behebung kann der fehlende CP abgewählt oder ein anderer CP zugewiesen werden.

Security-Einstellungen des CP

Die Einstellungen der CP-internen Firewall nehmen keinen Einfluss auf die Kommunikation über die virtuelle Schnittstelle. Die Security-Funktionen des Kommunikationsmoduls können daher nicht den Datenverkehr über die virtuelle Schnittstelle absichern.

ACHTUNG
Verbindung mit unsicheren Netzen
Die Nutzung der virtuellen Schnittstelle über den CP ist nur möglich, wenn die Security-Funktionen des CP deaktiviert sind.
Wenn Sie den CP mit einem unsicheren Netz verbinden, müssen Sie eine zusätzliche Firewall an die Schnittstelle des CP zum unsicheren Netz schalten. Verwenden Sie hierfür ein Security-Modul, zum Beispiel SCALANCE S602 V3 oder S623.

4.4.5 Programmierte Verbindungen: Einschränkung der Firewall-Regeln

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.

Hinweis

Partner-IP-Adressen nicht in Firewall-Regeln

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

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 synchronisierten 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 DNS-Konfiguration

DNS-Server

Ein DNS-Server kann erforderlich sein, wenn die Baugruppe selbst, ein Kommunikationspartner oder bspw. ein FTP-Server über den Host-Namen (FQDN) erreichbar sein soll. Bei der Angabe der Adresse eines Geräts als FQDN müssen Sie einen DNS-Server projektieren. Die IP-Adresse des Geräts wird dann über den projektierten DNS-Server ermittelt.

Für den CP dürfen max. 3 DNS-Server projektiert werden. Der 4. projektierte DNS-Server wird nicht ausgewertet.

4.7 FTP-Kommunikation

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.

4.7.1 FTP-Server

4.7.1.1 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.

Nur beim CP 1543-1 mit Firmware-Version ≤ V2.0:

- 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 folgenden Firmware-Versionen:

- CPU: V2.0
- CP 1543-1: V2.0
- CP 1545-1: V1.0

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 Datenbausteinzusordnung nehmen Sie in der STEP 7-Projektierung des CP vor (FTP-Konfiguration).

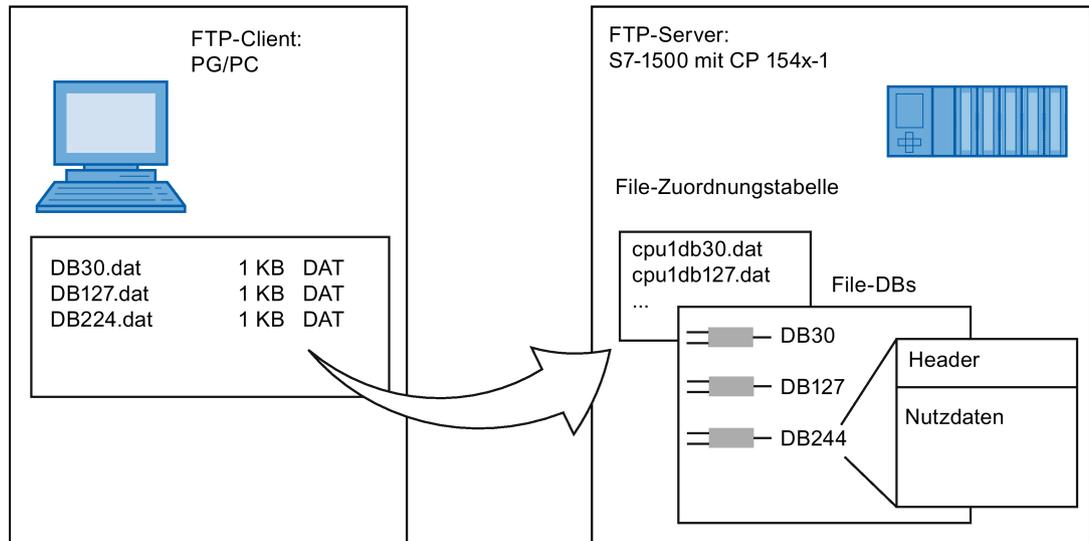


Bild 4-3 S7-CPU mit CP 154x-1 als FTP-Server für die S7-CPU-Daten

DB-Zuordnung in STEP 7

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

Spaltentitel	CPU	DB	Dateiname	Kommentar
Bedeutung	Zuordnung der CPU Auswählbar über Klapp- liste	Nr. des Datenbausteins (File-DB) Auswählbar über Klapp- liste	Dem File-DB zugewie- sener Dateiname Automatischer Na- mensvorschlag, 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")

4.7.2 FTP-Client

4.7.2.1 Der Programmbaustein FTP_CMD (FTP-Client-Funktion)

FTP_CMD

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

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

Sie finden den Baustein in STEP 7 bei geöffnetem Main [OB1] in der Task Card "Anweisungen" unter "Kommunikation > Kommunikationsprozessor > SIMATIC NET CP".

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 (gesicherte SSL-Verbindungen) möglich.

Hinweis

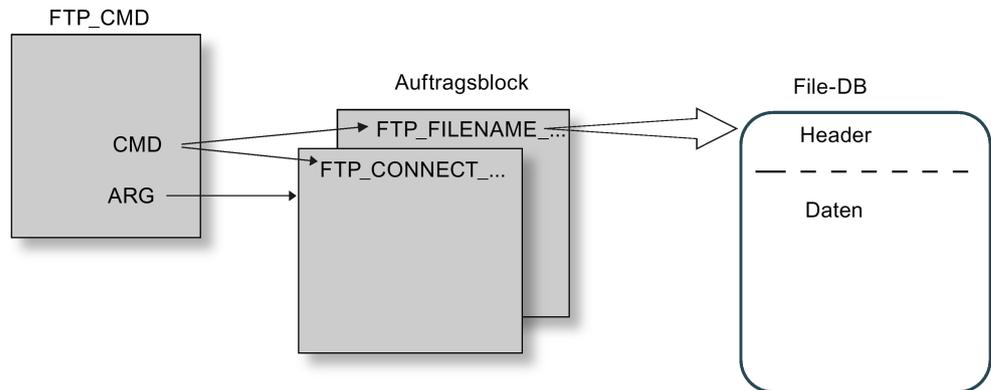
FTPS: Zertifikate abgleichen

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 vertrauenswürdigen 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 (UDTs)

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.

Die Beschreibung eines Beispiel-File-DB finden Sie im STEP 7 Informationssystem.

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:
Aktivieren Sie in den Projektierungsdaten der CPU unter "Schutz & Security" die Option "Zugriff über PUT/GET-Kommunikation ..." (PUT/GET muss freigegeben sein).

4.7.2.2 Eingangsparmeter FTP_CMD

Erläuterung der Eingangsparmeter

Sie versorgen die Anweisung FTP_CMD mit folgenden Eingangsparmetern:

Tabelle 4- 2 Formalparameter der Anweisung FTP_CMD - Eingangsparmeter

Parameter	Deklaration	Datentyp	Speicherbereich	Bedeutung / Bemerkung
REQ	Input	BOOL	E, A, M, DB, L	Startet den Sendeauftrag bei einer steigenden Flanke.
ID *	INPUT	INT	1, 2 ... 64	Die FTP-Aufträge werden über FTP-Verbindungen abgewickelt. Der Parameter identifiziert die genutzte Verbindung.
CMD *	INPUT	BYTE	Siehe nachfolgende Tabelle "Kommandos".	FTP-Kommando, das beim Aufruf der Anweisung ausgeführt werden soll. Wertebereiche für die FTP-Kommandotypen finden Sie im Anschluss an die Tabelle. Das hier angegebene FTP-Kommando muss identisch im Auftragsblock (Parameter ARG) angegeben werden. Wenn ein Kommando nicht von der CP-Firmware unterstützt wird, dann wird eine Fehlermeldung mit STATUS = 8F6B _H ausgegeben.
ARG *	INPUT	VARIANT	Siehe nachfolgende Tabelle "Kommandos".	Auftragsblock Verweist auf den Datenbereich mit den zum FTP-Kommando passenden Ausführungsparametern. Abhängig vom FTP-Kommando werden spezifische Datentypen (UDT) verwendet. Die UDTs werden nachfolgend angegeben. Für den hier anzugebenden Zeiger ist der Datentyp ANY nicht zulässig!

* Die Werte der Eingangsparmeter "ID" und "CMD" überschreiben den Wert des Eingangsparmeters "ARG".

FTP-Kommandos im Parameter "CMD"

Entnehmen Sie der folgenden Tabelle, welche Bedeutung die Kommandos des Parameters "CMD" haben und welche UDTs Sie zur Versorgung der Auftragsblöcke verwenden.

Tabelle 4- 3 Kommandotypen

CMD (Kommandotyp)	Relevante Auftragsblöcke / UDT	Bedeutung / Handhabung
0 (NOOP)	*	Der aufgerufene FB führt keine Aktionen aus. Die Statusanzeigen werden bei dieser Parameterversorgung wie folgt gesetzt: DONE=1; ERROR=0; STATUS=0
1 (CONNECT)	FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME	FTP-Verbindungsaufbau Mit diesem Kommando baut der FTP-Client eine FTP-Verbindung zu einem FTP-Server auf (Port 21). Die Verbindung steht unter der hier zugewiesenen Verbindungs-ID für alle weiteren FTP-Kommandos zur Verfügung. Daten werden dann mit dem für diesen Benutzer angegebenen FTP-Server ausgetauscht.
2 (STORE)	FTP_FILENAME	Mit diesem Funktionsaufruf wird ein Datenbaustein (File-DB) vom FTP-Client (S7-CPU) zum FTP-Server übertragen. Achtung: Falls die Datei (File-DB) auf dem FTP-Server schon vorhanden ist, wird diese überschrieben.
3 (RETRIEVE)	FTP_FILENAME	Mit diesem Funktionsaufruf wird eine Datei vom FTP-Server zum FTP-Client (S7-CPU) übertragen. Achtung: Falls der Datenbaustein (File-DB) beim FTP-Client schon eine Datei enthält, wird diese überschrieben.
4 (DELETE)	FTP_FILENAME	Mit diesem Funktionsaufruf löschen Sie eine Datei auf dem FTP-Server.
5 (QUIT)	*	Mit diesem Funktionsaufruf bauen Sie die in "ID" angegebene FTP-Verbindung ab.
6 (APPEND)	FTP_FILENAME	Ähnlich wie "STORE" speichert das Kommando "APPEND" (anhängen) eine Datei auf dem FTP-Server. Bei "APPEND" wird die Datei auf dem FTP-Server aber nicht überschrieben, sondern der neue zu speichernde Inhalt wird an die Datei angehängt. Falls die Datei auf dem FTP-Server nicht vorhanden ist, wird sie angelegt.
7 (RETR_PART)	FTP_FILENAME_PART	Mit dem Kommando "RETR_PART" (Teillänge lesen) können Sie einen Ausschnitt einer Datei vom FTP-Server anfordern. Bei sehr großen Dateien können Sie damit das Lesen auf den Teil beschränken, den Sie gerade benötigen. Dazu müssen Sie die Struktur dieser Datei kennen. Geben Sie den gewünschten Ausschnitt der Datei mithilfe der zwei Parameter "OFFSET" und "LEN" am FB 40 an.

* Bei den Kommandotypen 0 (NOOP) und 5 (QUIT) muss ein beliebiger Auftragsblock (UDT) angegeben werden. Dieser wird nicht ausgewertet.

4.7.2.3 Auftragsblöcke für FTP_CMD

Bedeutung

Sie versorgen die Anweisung FTP_CMD über den Parameter ARG mit einem Auftragsblock. Die Struktur ist abhängig vom FTP-Kommandotyp. Indem Sie die vorgegebenen Datentypen (UDT) verwenden, erkennt die Anweisung den Typ des Auftragsblocks. Nachfolgend werden die jeweiligen Datentypen (UDT) für folgende Auftragsblöcke angegeben:

- FTP-Verbindungsaufbau mit IP-Adresse gemäß IPv4
- FTP-Verbindungsaufbau mit IP-Adresse gemäß IPv6
- FTP-Verbindungsaufbau mit Server-Name
- Schreib- und Lesezugriff sowie übrige FTP-Kommandos
- FTP-Kommando RETR_PART

Auftragsblock für FTP-Verbindungsaufbau mit IP-Adresse gemäß IPv4

Für den FTP-Verbindungsaufbau mit IP-Adresse gemäß IPv4 wird die folgende Datenstruktur verwendet.

Tabelle 4- 4 FTP_CONNECT_IPV4

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
InterfaceID	HW_ANY		Baugruppen-Anfangsadresse Beim Aufruf eine Anweisung übergeben Sie im Parameter LADDR die Baugruppen-Anfangsadresse des CP. Die Baugruppen-Anfangsadresse des CP können Sie in der Projektierung des CP entnehmen unter: "Eigenschaften>Adressen>Eingänge"
ID	CONN_OUC	1, 2...64	Die FTP-Aufträge werden über FTP-Verbindungen abgewickelt. Der Parameter identifiziert die genutzte Verbindung.
ConnectionType	BYTE	0	Verbindungstyp "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = aktiver Verbindungsaufbau
FTPCmd	BYTE	1	FTP-Kommando "CONNECT" FTP-Kommando, das beim Aufruf der Anweisung ausgeführt wird. Wertebereiche für die Kommandotypen finden Sie im Kapitel Eingangsparameter FTP_CMD (Seite 47). Hinweis: Das hier angegebene FTP-Kommando muss identisch im Eingangsparameter CMD angegeben werden.
CertIndex	BYTE	0 = FTP 1 = FTPS	Wählen Sie hier zwischen den Protokolltypen FTP oder FTPS. Hinweis für FTPS: Wenn der FTP-Server außerhalb des STEP 7-Projekts des FTP-Client konfiguriert wird, dann ist der Import des Zertifikats vom FTP-Server erforderlich.
UserName	STRING[32]	'benutzer'	Benutzername für das Login auf dem FTP-Server

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
Password	STRING[32]	'password'	Passwort für das Login auf dem FTP-Server
FTPserverIPAddr	IP_V4	ADDR(1) ... ADDR(4)	IP-Adresse des FTP-Servers als Array[1..4] of Byte, wobei jeweils 1 Byte einen Block der Adresse spezifiziert. Bsp.: ADDR(1) spezifizieren den ersten Adressblock (das erste Byte der Adresse).

Auftragsblock für FTP-Verbindungsaufbau mit IP-Adresse gemäß IPv6

Für den FTP-Verbindungsaufbau mit IP-Adresse gemäß IPv6 wird die folgende Datenstruktur verwendet.

Tabelle 4- 5 FTP_CONNECT_IPV6

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
InterfacelD	HW_ANY		Baugruppen-Anfangsadresse Beim Aufruf eine Anweisung übergeben Sie im Parameter LADDR die Baugruppen-Anfangsadresse des CP. Die Baugruppen-Anfangsadresse des CP können Sie in der Projektierung des CP entnehmen unter: "Eigenschaften>Adressen>Eingänge"
ID	CONN_OUC	1, 2...64	Die FTP-Aufträge werden über FTP-Verbindungen abgewickelt. Der Parameter identifiziert die genutzte Verbindung.
ConnectionType	BYTE	0	Verbindungstyp "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = aktiver Verbindungsaufbau
FTPCmd	BYTE	1	FTP-Kommando "CONNECT" FTP-Kommando, das beim Aufruf der Anweisung ausgeführt wird. Wertebereiche für die Kommandotypen finden Sie im Kapitel Eingangsparameter FTP_CMD (Seite 47). Hinweis: Das hier angegebene FTP-Kommando muss identisch im Eingangsparameter CMD angegeben werden.
CertIndex	BYTE	0 = FTP 1 = FTPS	Wählen Sie hier zwischen den Protokolltypen FTP oder FTPS. Hinweis für FTPS: Wenn der FTP-Server außerhalb des STEP 7-Projekts des FTP-Client konfiguriert wird, dann ist der Import des Zertifikats vom FTP-Server erforderlich.
UserName	STRING[32]	'benutzer'	Benutzername für das Login auf dem FTP-Server
Password	STRING[32]	'password'	Passwort für das Login auf dem FTP-Server
FTPserverIPAddr	IP_V6	ADDR(1) ... ADDR(16)	IP-Adresse des FTP-Servers als Array[1..16] of Byte, wobei jeweils 2 Byte einen Block der Adresse spezifizieren. Bsp.: ADDR(1) + ADDR(2) spezifizieren den ersten Adressblock.

Auftragsblock für FTP-Verbindungsaufbau mit Server-Name

Für den FTP-Verbindungsaufbau mit Angabe eines Server-Namens wird die folgende Datenstruktur verwendet. Der Server-Name wird über DNS einer IP-Adresse zugewiesen.

Tabelle 4- 6 FTP_CONNECT_NAME

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
InterfaceID	HW_ANY		Baugruppen-Anfangsadresse Beim Aufruf eine Anweisung übergeben Sie im Parameter LADDR die Baugruppen-Anfangsadresse des CP. Die Baugruppen-Anfangsadresse des CP können Sie in der Projektierung des CP entnehmen unter: "Eigenschaften>Adressen>Eingänge"
ID	CONN_OUC	1, 2...64	Die FTP-Aufträge werden über FTP-Verbindungen abgewickelt. Der Parameter identifiziert die genutzte Verbindung.
ConnectionType	BYTE	0	Verbindungstyp "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = aktiver Verbindungsaufbau
FTPcmd	BYTE	1	FTP-Kommando "CONNECT" FTP-Kommando, das beim Aufruf der Anweisung ausgeführt wird. Wertebereiche für die Kommandotypen finden Sie im Kapitel Eingangsparameter FTP_CMD (Seite 47). Hinweis: Das hier angegebene FTP-Kommando muss identisch im Eingangsparameter CMD angegeben werden.
CertIndex	BYTE	0 = FTP 1 = FTPS	Wählen Sie hier zwischen den Protokolltypen FTP oder FTPS. Hinweis für FTPS: Wenn der FTP-Server außerhalb des STEP 7-Projekts des FTP-Client konfiguriert wird, dann ist der Import des Zertifikats vom FTP-Server erforderlich.
UserName	STRING[32]	'benutzer'	Benutzername für das Login auf dem FTP-Server
Password	STRING[32]	'passwort'	Passwort für das Login auf dem FTP-Server
FTPserverName	STRING[254]		IP-Adresse des FTP-Servers

Auftragsblock für Schreib- und Lesezugriff sowie übrige FTP-Kommandos

Für die FTP-Kommandos store, retrieve, delete und append wird die folgende Datenstruktur verwendet.

Tabelle 4- 7 FTP_FILENAME

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
InterfacelD	HW_ANY		Baugruppen-Anfangsadresse Beim Aufruf eine Anweisung übergeben Sie im Parameter LADDR die Baugruppen-Anfangsadresse des CP. Die Baugruppen-Anfangsadresse des CP können Sie in der Projektierung des CP entnehmen unter: "Eigenschaften>Adressen>Eingänge"
ID	CONN_OUC	1, 2...64	Die FTP-Aufträge werden über FTP-Verbindungen abgewickelt. Der Parameter identifiziert die genutzte Verbindung.
ConnectionType	BYTE	0	Verbindungstyp "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = aktiver Verbindungsaufbau
FTPcmd	BYTE	2, 3, 4, 6	FTP-Kommando "STORE / RETRIEVE / DELETE / APPEND" FTP-Kommando, das beim Aufruf der Anweisung ausgeführt wird. Wertebereiche für die Kommandotypen finden Sie im Kapitel Eingangsparameter FTP_CMD (Seite 47). Hinweis: Das hier angegebene FTP-Kommando muss identisch im Eingangsparameter CMD angegeben werden.
CertIndex	BYTE	0 = FTP 1 = FTPS	Wählen Sie hier zwischen den Protokolltypen FTP oder FTPS. Hinweis für FTPS: Wenn der FTP-Server außerhalb des STEP 7-Projekts des FTP-Client konfiguriert wird, dann ist der Import des Zertifikats vom FTP-Server erforderlich.
DataBlockNumber	UINT		Der hier angegebene Datenbaustein enthält den zu lesenden / zu schreibenden File-DB.
LenFilename	UINT	0...1000	Der Parameter "LenFilename" zur Angabe der Gesamtlänge des Dateinamens wird nicht ausgewertet. Stattdessen wird die Längenangabe im String des Parameters "Filename" ausgewertet.
Filename	ARRAY[0..3] OF STRING[254]		Dateiname der Ziel- bzw. Quelldatei. Die vier Strings für den Dateinamen werden verkettet und als Gesamt-String an den Server übertragen.

Auftragsblock für das FTP-Kommando RETR_PART

Für das FTP-Kommando RETR_PART wird die folgende Datenstruktur verwendet.

Tabelle 4- 8 FTP_FILENAME_PART

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
InterfaceID	HW_ANY		Baugruppen-Anfangsadresse Beim Aufruf eine Anweisung übergeben Sie im Parameter LADDR die Baugruppen-Anfangsadresse des CP. Die Baugruppen-Anfangsadresse des CP können Sie in der Projektierung des CP entnehmen unter: "Eigenschaften>Adressen>Eingänge"
ID	CONN_OUC	1, 2...64	Die FTP-Aufträge werden über FTP-Verbindungen abgewickelt. Der Parameter identifiziert die genutzte Verbindung.
ConnectionType	BYTE	0	Verbindungstyp "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = aktiver Verbindungsaufbau
FTPcmd	BYTE	7	FTP-Kommando "RETR_PART" FTP-Kommando, das beim Aufruf der Anweisung ausgeführt wird. Wertebereiche für die Kommandotypen finden Sie im Kapitel Eingangsparameter FTP_CMD (Seite 47). Das hier angegebene FTP-Kommando muss identisch im Eingangsparameter CMD angegeben werden.
CertIndex	BYTE	0 = FTP 1 = FTPS	Wählen Sie hier zwischen den Protokolltypen FTP oder FTPS. Hinweis für FTPS: Wenn der FTP-Server außerhalb des STEP 7-Projekts des FTP-Client konfiguriert wird, dann ist der Import des Zertifikats vom FTP-Server erforderlich.
Offset	DWORD		Offset in Byte, ab dem die Datei gelesen werden soll.
Length	DWORD		Teillänge in Byte, die ab dem in "OFFSET" angegebenen Wert gelesen werden. Besonderheiten: <ul style="list-style-type: none"> Bei Angabe von "DW#16#FFFFFFFF" wird der verfügbare Rest der Datei gelesen. Ergebnis OK (DONE = 1, STATUS = 0), falls kein sonstiger Fehler auftritt. Wenn OFFSET > Länge der Original-Datei: Länge der Ziel-Datei (ACT_LENGTH im File-DB): 0 Byte in der CPU. Ergebnis OK (DONE = 1, STATUS = 0), falls kein sonstiger Fehler auftritt. Wenn OFFSET + LEN > Länge der Original-Datei (und LEN ≠ 0xFFFFFFFF): Länge der Ziel-Datei (ACT_LENGTH im File-DB): Verfügbare Bytes ab "OFFSET". Ergebnis OK (DONE = 1, STATUS = 0), falls kein sonstiger Fehler auftritt.

Parameter	Typ	Wertebereich	Bedeutung / Bemerkung
DataBlockNumber	UINT		Der hier angegebene Datenbaustein enthält den zu lesenden / zu schreibenden File-DB.
LenFilename	UINT	0...1000	Der Parameter "LenFilename" zur Angabe der Gesamtlänge des Dateinamens wird nicht ausgewertet. Stattdessen wird die Längenangabe im String des Parameters "Filename" ausgewertet.
Filename	ARRAY[0..3] OF STRING[254]		Dateiname der Ziel- bzw. Quelldatei. Die vier Strings für den Dateinamen werden verkettet und als Gesamt-String an den Server übertragen.

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.

4.7.2.4 Ausgangsparameter und Statusinformationen FTP_CMD

Parameter BUSY, DONE und ERROR

Den Ausführungsstatus kontrollieren Sie über die Parameter BUSY, DONE, ERROR und STATUS. Der Parameter BUSY zeigt den Bearbeitungsstatus. Mit dem Parameter DONE kontrollieren Sie, ob ein Auftrag erfolgreich ausgeführt wurde. Der Parameter ERROR wird gesetzt, wenn Fehler während der Ausführung von "FTP_CMD" auftreten. Die Fehlerinformationen werden am Parameter STATUS ausgegeben.

Die folgende Tabelle zeigt den Zusammenhang zwischen den Parametern BUSY, DONE und ERROR:

BUSY	DONE	ERROR	Beschreibung
1	-	-	Der Auftrag wird bearbeitet.
0	1	0	Der Auftrag wurde erfolgreich durchgeführt.
0	0	1	Der Auftrag wurde mit einem Fehler beendet. Die Ursache des Fehlers wird im Parameter STATUS angegeben.
0	0	0	Kein neuer Auftrag wurde zugewiesen.

Statusanzeigen auswerten

Hinweis

Auswertung

- Auswertung bei BUSY = 0

Werten Sie die Statusanzeigen erst aus, wenn BUSY = 0.

- Status 8FxxH

Beachten Sie für die Einträge mit den Status 8FxxH auch die Angaben im Referenzhandbuch STEP 7 Standard und Systemfunktionen. Sie finden dort Hinweise im Kapitel "Fehlerauswertung mit dem Ausgangsparameter RET_VAL".

Tabelle 4- 9 FTP_CMD: Bedeutung des Parameters STATUS in Zusammenhang mit DONE und ERROR

DONE	ERROR	STATUS	Bedeutung
0	0	0000 _H	Es ist kein Auftrag in Bearbeitung.
1	0	0000 _H	Der Auftrag ist fertig ohne Fehler.
0	0	7001 _H	Der Auftrag wurde erstmalig angestoßen.
0	0	7002 _H	Der Auftrag läuft noch.
0	1	80C4 _H	Kommunikationsfehler (tritt temporär auf; daher ist Wiederholung im Anwenderprogramm sinnvoll.)
0	1	8183 _H	Die Projektierung entspricht nicht den Auftragsparametern.
0	1	8401 _H	Unbekannter Fehler Mögliche Ursachen: <ul style="list-style-type: none"> • Auf der Verbindung wurde ein Timeout erkannt. • Der FTP-Server hat die Verbindung abgebrochen. Abhilfe: QUIT und CONNECT-Kommandos erneut senden, um die Verbindung wieder einzurichten.
0	1	8402 _H	Verbindung befindet sich in fehlerhaftem Zustand. Das Timeout der Verbindung kann überschritten sein oder der FTP-Server kann die Verbindung abgebaut haben. Abhilfe: Senden Sie erneut die Kommandos QUIT und CONNECT, um die Verbindung wieder aufzubauen.
0	1	8403 _H	Login ist fehlgeschlagen.
0	1	8404 _H	FTP-Server ist nicht erreichbar.
0	1	8405 _H	Übertragung ist fehlgeschlagen.
0	1	8406 _H	Timeout bei aktuellem Vorgang
0	1	8407 _H	Datei im FTP-Server wurde nicht gefunden.
0	1	8408 _H	Übertragung nicht möglich.
0	1	8409 _H	Datei konnte nicht geholt werden.
0	1	8410 _H	Das Setzen des TCP Port für die Datenverbindung ist fehlgeschlagen.
0	1	8411 _H	Offset-Angabe passt nicht.
0	1	8412 _H	Fehler beim Wechsel der Verzeichnisangabe
0	1	8413 _H	Fehler beim Daten Empfangen

DONE	ERROR	STATUS	Bedeutung
0	1	8414 _H	Fehler beim Daten Senden.
0	1	8415 _H	CMD-Angabe (Kommandotyp) wurde vom Client abgewiesen.
0	1	8416 _H	Verbindung wurde vom FTP-Server geschlossen.
0	1	8418 _H	Fehler in den Nutzdaten. Mögliche Ursachen: <ul style="list-style-type: none"> • Dateiname ist leer. • Datenlänge ist "0". • usw.
0	1	8419 _H	Es ist keine Socket-Ressource zum Öffnen einer Datenverbindung vorhanden.
0	1	8420 _H	Es ist keine Socket-Ressource zum Öffnen einer Control-Verbindung vorhanden.
0	1	8421 _H	Fehler beim Öffnen des zu lesenden File-DB
0	1	8422 _H	Fehler beim Öffnen des zu beschreibenden File-DB
0	1	8423 _H	Der Verbindungsaufbau zum FTP Server ist fehlgeschlagen.
0	1	8424 _H	Interner Fehler
0	1	8425 _H	Formatfehler beim Domain-Namen
0	1	8426 _H	Es stehen zu viele DNS-Anfragen an.
0	1	8427 _H	Der angegebene DNS-Server konnte den spezifizierten Domain-Namen nicht zuordnen.
0	1	8428 _H	Es ist keine Verbindungs-Ressource verfügbar.
0	1	8429 _H	Unbekannte Kanal-ID
0	1	8430 _H	Der File-DB ist zu kurz.
0	1	8431 _H	Fehler beim Schreiben in den File-DB.
0	1	8432 _H	Fehler beim Lesen aus dem File-DB.
0	1	8433 _H	Fehler beim Zugriff auf den File-DB.
0	1	8434 _H	Aktion wurde abgebrochen.
0	1	8435 _H	Kanal wird zurückgesetzt.
0	1	8436 _H	Unerwartete Server Antwort
0	1	8437 _H	Zertifikat konnte nicht verifiziert werden.
0	1	8438 _H	Unbekannter Fehler aufgetreten.
0	1	8439 _H	Das FTP-Kommando führt zu einem Fehler. Die Ursache ist beim FTP-Server zu suchen (REST-Kommando).
0	1	8440 _H	Der FTP-Server unterstützt das geforderte SSL-Protokoll nicht.
0	1	8446 _H	Nachdem das FTP-Passwort an den FTP-Server gesendet wurde, wurde ein unerwarteter Code vom FTP-Server zurückgegeben.
0	1	8451 _H	Beim Versuch, den Übertragungsmodus von binär auf ASCII umzustellen, wurde ein Fehler gemeldet.
0	1	8455 _H	Eine Speicheranforderung im CM/CP ist fehlgeschlagen.
0	1	8460 _H	Bei der SSL/TLS-Abwicklung ist ein Problem aufgetreten.

DONE	ERROR	STATUS	Bedeutung
0	1	8469 _H	Schnittstellen-Fehler Die angegebene Ausgangs-Schnittstelle konnte nicht genutzt werden. Abhilfe: Stellen Sie ein, welche Schnittstelle für ausgehende Verbindungen genutzt werden soll.
0	1	8475 _H	Das SSL-Zertifikat oder der SSH md5 fingerprint wurde als nicht vertrauenswürdig erachtet.
0	1	8476 _H	Vom FTP-Server wurde nichts empfangen. Im aktuellen Zustand muss von einem fehlerhaften Verhalten ausgegangen werden.
0	1	8477 _H	Die angegebene "Crypto engine" (kryptografisches Modul) wurde nicht gefunden.
0	1	8478 _H	Der Vorgang schlug fehl, die gewählte SSL-"Crypto engine" (kryptografisches Modul) als Standard zu setzen.
0	1	8480 _H	Es ist ein Problem mit dem Zertifikat des FTP-Client aufgetreten.
0	1	8481 _H	Die angegebene Ziffer konnte nicht verwendet werden.
0	1	8482 _H	Der FTP-Server verwendet eine Kodierung, die nicht unterstützt wird.
0	1	8484 _H	Die maximale Dateigröße wurde überschritten.
0	1	8485 _H	Der File-DB wurde während der Sendebearbeitung verändert oder der File-DB ist nicht korrekt aufgebaut.
0	1	8489 _H	Daten konnten nicht gesendet werden. Es ist nicht genügend Speicherkapazität für den Vorgang auf dem FTP-Server verfügbar.
0	1	8492 _H	Die Datei existiert bereits. Die Datei wird nicht überschrieben.
0	1	8496 _H	Beim Lesen des SSL CA-Zertifikats ist ein Problem aufgetreten.
0	1	8497 _H	Ein unerwarteter Fehler ist bei der SSH-Sitzung aufgetreten.
0	1	8498 _H	Es war nicht möglich, die SSL-Verbindung abzubauen.
0	1	8499 _H	Der Socket ist nicht bereit zum Senden/Empfangen. Warten Sie, bis die Bereitschaft besteht, und versuchen Sie es erneut.
0	1	8501 _H	Die Überprüfung des SSL-Zertifikats des FTP-Servers ist fehlgeschlagen.
0	1	8507 _H	Während der aktiven FTP-Sitzung ist im Rahmen des Verbindungsaufbaus beim Warten auf den FTP-Server ein Timeout aufgetreten.
0	1	8F54 _H	Das Bit "EXIST" im File-DB-Header ist nicht gesetzt.
0	1	8F55 _H	Header-Status-Bit: Locked
0	1	8F56 _H	Das NEW-Bit im File-DB-Header wurde nicht zurückgesetzt
0	1	8F6B _H	Mögliche Ursachen: <ul style="list-style-type: none"> Falscher Wert für den Parameter CMD Werte von 0 bis 15 sind zugelassen. Ein Kommando des FB 40 wird nicht unterstützt. Mögliche Ursache: Falsche Firmware des CP Abhilfe: Firmware-Update (bei älteren CPs statt des FB 40 die Funktionen FC 40...FC 44 benutzen.)
0	1	8F7F _H	Interner Fehler, beispielsweise unzulässige ANY-Referenz.

4.7.2.5 Aufbau des Datenbausteins (File-DB) für den FTP-Client-Betrieb

Funktionsweise

Für die Übertragung von Daten mittels FTP legen Sie in der CPU Ihrer S7-Station Datenbausteine (File-DBs) an. Diese Datenbausteine müssen einer bestimmten Struktur genügen, damit sie von den FTP-Diensten als übertragbare Dateien hantiert werden können. Sie bestehen aus folgenden Abschnitten:

- Abschnitt 1: File-DB-Header (besitzt feste Struktur mit einer Länge von 20 Byte)
- Abschnitt 2: Nutzdaten als "Array [...] of Byte" oder "Array [...] of Char" (besitzt variable Länge und Struktur)

Datenkonsistenz

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

Anlegen eines File-DB

1. Legen Sie in STEP 7 einen neuen Datenbaustein an.
2. Öffnen Sie den Bausteineditor.
3. Selektieren Sie im Bausteineditor des DB die Zeile, die Sie als Startzeile für den File-DB verwenden werden.
4. Geben Sie in der Spalte "Datentyp" den Typ "FILE_DB_HEADER" über die Tastatur ein. Es wird eine Datenstruktur mit der für den File-DB benötigte Header-Struktur angelegt.
5. Setzen Sie den Parameter "WRITEACCESS" auf "true", um den Zugriff zu ermöglichen.
6. Geben Sie einen Wert für die Länge der Nutzdaten am Parameter "MAX_LENGTH" ein.
7. Legen Sie darunter für die zu übertragenden Nutzdaten ein Datenfeld vom Typ "Array [...] of Byte" oder "Array [...] of Char" an.

Die Größe des Feldes muss der Angabe von "MAX_LENGTH" im Header entsprechen.

File-DB-Header für FTP-Client-Betrieb

Der hier beschriebene File-DB Header ist identisch zu dem für den Server-Betrieb beschriebenen File-DB-Header.

Parameter	Typ	Wert / Bedeutung	Versorgung
EXIST	BOOL	<p>Das EXIST-Bit zeigt an, ob der Nutzdatenbereich gültige Daten enthält.</p> <p>Das FTP-Kommando retrieve bearbeitet den Auftrag nur, wenn EXIST=1.</p> <ul style="list-style-type: none"> 0: Der File-DB enthält keine gültigen Nutzdaten (Datei existiert nicht). 1: Der File-DB enthält gültige Nutzdaten (Datei existiert). 	<p>Das FTP-Kommando "DELETE" setzt EXIST=0.</p> <p>Das FTP-Kommando "STORE" setzt EXIST=1.</p>
LOCKED	BOOL	<p>Das LOCKED-Bit dient zum Zugriffsschutz für den File-DB.</p> <ul style="list-style-type: none"> 0: Auf den File-DB kann zugegriffen werden. 1: Der File-DB ist gesperrt. 	<p>Die FTP-Kommandos "STORE" und "RETRIEVE" setzen während der Bearbeitung LOCKED=1, wenn das Bit zuvor auf 0 stand.</p> <p>Das Anwenderprogramm in der S7-CPU kann zur Konsistenzsicherung während eines Schreibzugriffes ebenfalls LOCKED setzen bzw. zurücksetzen.</p> <p>Dadurch wird zur Konsistenzsicherung eine gegenseitige Verriegelung zwischen Anwenderprogramm und FTP-Abwicklung bewirkt.</p> <p>Empfehlung zur Vorgehensweise im Anwenderprogramm:</p> <ol style="list-style-type: none"> 1. LOCKED-Bit prüfen (wenn = 0) 2. WRITEACCESS-Bit=0 setzen 3. LOCKED-Bit prüfen (wenn = 0) 4. LOCKED-Bit=1 setzen 5. Daten schreiben 6. LOCKED-Bit=0 setzen
NEW	BOOL	<p>Das NEW-Bit informiert, ob Daten seit dem letzten Lesevorgang verändert wurden.</p> <ul style="list-style-type: none"> 0: Inhalt des File-DB ist unverändert seit letztem Schreibvorgang. Das Anwenderprogramm der S7-CPU hat die letzte Änderung registriert. 1: Das Anwenderprogramm der S7-CPU hat den letzten Schreibvorgang noch nicht registriert. 	<p>Das FTP-Kommando "RETRIEVE" setzt nach der Bearbeitung NEW=1.</p> <p>Das Anwenderprogramm in der S7-CPU muss nach dem Lesen der Daten NEW=0 setzen, um ein erneutes Kommando "RETRIEVE" zu ermöglichen.</p>

Parameter	Typ	Wert / Bedeutung	Versorgung
WRITEACCESS	BOOL	<ul style="list-style-type: none"> 0: Das Anwenderprogramm hat Schreibrecht für die File-DBs in der S7-CPU. 1: Das Anwenderprogramm hat kein Schreibrecht für die File-DBs in der S7-CPU. 	<p>Das Bit wird bei der DB-Projektierung auf einen Initialisierungswert gesetzt.</p> <p>Empfehlung: Das Bit sollte nach Möglichkeit unverändert bleiben! In besonderen Fällen ist eine Anpassung im laufenden Betrieb möglich.</p>
ACT_LENGTH	DINT	<p>Aktuelle Länge des Nutzdatenbereiches.</p> <p>Der Inhalt dieses Feldes ist nur dann gültig, wenn EXIST = 1.</p>	<p>Die aktuelle Länge wird nach einem Schreibvorgang aktualisiert.</p>
MAX_LENGTH	DINT	<p>Maximale Länge des Nutzdatenbereichs (Länge des gesamten DB abzüglich 20 Byte Header).</p>	<p>Die maximale Länge sollte bei der DB-Projektierung festgelegt werden.</p> <p>Der Wert kann auch im laufenden Betrieb vom Anwenderprogramm geändert werden.</p>
FTP_REPLY_CODE	INT	<p>Vorzeichenlose Zahl (16 Bit), die den letzten Reply-Code von FTP als Binärwert enthält.</p> <p>Der Inhalt dieses Feldes ist nur dann gültig, wenn EXIST = 1.</p>	<p>Wird vom FTP-Protokoll-Abwickler bei der FTP-Kommandobearbeitung des Servers aktualisiert.</p>
DATE_TIME	DATE_AND_TIME	<p>Datum und Zeit der letzten Änderung des Files.</p> <p>Der Inhalt dieses Feldes ist nur dann gültig, wenn EXIST = 1.</p>	<p>Das aktuelle Datum wird nach einem Schreibvorgang aktualisiert.</p> <p>Wenn die Funktion "Uhrzeitweiterleitung" genutzt wird, dann entspricht der Eintrag der weitergeleiteten Zeit.</p> <p>Wenn die Funktion "Uhrzeitweiterleitung" nicht genutzt wird, dann wird eine relative Zeit eingetragen. Bezug ist der Anlaufzeitpunkt des CP (Initialisierungswert: 01.01.1994 00:00h).</p>

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.

4.8 Security

Eine Übersicht über Umfang und Anwendung der Security-Funktionen des CP finden Sie im Kapitel Industrial Ethernet Security (Seite 14).

Zum Mengengerüst der Security-Funktionen siehe Kapitel Kenndaten Security (Seite 18).

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

4.8.1 Security-Benutzer

Security-Benutzer anlegen

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

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

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

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

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

4.8.2 VPN

Die Parametergruppe "VPN" des Moduls wird erst eingeblendet, wenn Sie das Modul in den globalen Security-Funktionen einer VPN-Gruppe zuweisen.

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

4.8.2.1 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.
- Beteiligte CP 1543-1 sind mit einer Firmware-Version \geq 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.

Option "Aktiviere Security-Funktionen" aktiviert

- Nach dem Anmelden müssen Sie bei beiden CPs die Option "Aktiviere Security-Funktionen" aktivieren.
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.
Damit legen Sie die Basis-Eigenschaften der VPN-Gruppe fest.

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: Die Option "Firewall aktivieren" wird beim Anlegen einer VPN-Gruppe standardmäßig aktiviert. Sie können die Option nicht deaktivieren.

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

4.8.2.2 VPN-Tunnelkommunikation zwischen CP und SCALANCE M aufbauen

Das Anlegen der VPN-Tunnelkommunikation zwischen CP und SCALANCE M erfolgt entsprechend der beschriebenen Vorgehensweise bei S7-1500-Stationen (Seite 63).

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

Wenn die Option deaktiviert ist, lehnt der CP den Verbindungsaufbau ab.

4.8.2.3 VPN-Tunnelkommunikation mit SOFTNET Security Client

Das Anlegen der VPN-Tunnelkommunikation zwischen SOFTNET Security Client und dem CP erfolgt entsprechend der beschriebenen Vorgehensweise bei S7-1500-Stationen (Seite 63).

VPN-Tunnelkommunikation gelingt nur bei deaktiviertem internem Teilnehmer

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

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

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

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

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

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

Der unterlagerte Teilnehmer verschwindet vorerst aus der Tunnelliste.

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

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

Der unterlagerte Teilnehmer erscheint vorübergehend wieder in der Tunnelliste.

4. Selektieren Sie in der Tunnelliste den unterlagerten Teilnehmer.

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

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

4.8.2.4 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".

4.8.3 Firewall

4.8.3.1 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.

Siehe auch

Programmierte Verbindungen: Einschränkung der Firewall-Regeln (Seite 40)

Die virtuelle Schnittstelle der CPU (Seite 37)

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

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

- Trennen Sie die beiden IP-Adressen nur durch einen Bindestrich.

Richtig: 192.168.10.0-192.168.10.255

- Geben Sie keine weiteren Zeichen zwischen die beiden IP-Adressen ein.

Falsch: 192.168.10.0 - 192.168.10.255

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

4.8.3.3 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.

4.8.3.4 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 Einstellung "Accept" aus.

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

Dies gilt für Verbindungen zwischen einem CP 154x-1 und beispielsweise einem CP 343-1 Advanced, CP 443-1 Advanced, CP 1628 oder CP 1243-1.

Siehe auch

Einstellungen für Online-Security-Diagnose und Laden in Station bei aktivierter Firewall (Seite 67)

4.8.4 Online-Funktionen

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

Firewall für Online-Funktionen einstellen

Gehen Sie bei aktivierten Security-Funktionen wie folgt vor:

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 Engineering-Station ein. So sorgen Sie dafür, dass ICMP-Telegramme (Ping) nur von Ihrer Engineering-Station aus die Firewall passieren können.

4.8.4.2 Online-Security-Diagnose über Port 8448

Security-Diagnose über Port 8448

Voraussetzung: Zugriff auf den Webserver des CP über HTTPS ist aktiviert.

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

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

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

4.8.5 Log-Einstellungen - Filtern der System-Ereignisse

Kommunikationsprobleme bei zu hoch eingestelltem Wert für System-Ereignisse

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

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

4.9 Programmbausteine für OUC

Programmierung der Open User Communication (OUC)

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

- ISO-Transport
- TCP (IPv4 / IPv6)
- 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.

- **TCON_Configured**
Für die Übertragung von Telegrammen über TCP
- **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 (IPv4 / IPv6)
- **TCON_QDN_SEC**
Für die gesicherte Übertragung von Telegrammen über TCP (IPv4 / IPv6)
- **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.

Diagnose und Instandhaltung

5.1 Diagnosemöglichkeiten

Für die Baugruppe stehen Ihnen folgende Diagnosemöglichkeiten zur Verfügung:

LEDs der Baugruppe

Informationen zu den LED-Anzeigen finden Sie im Kapitel LEDs (Seite 21).

STEP 7: Das Register "Diagnose" im Inspektorfenster

Wenn Ihre Engineering-Station über Ethernet mit der Baugruppe verbunden ist, erhalten Sie hier Informationen zum Verbindungszustand der ES mit der Baugruppe.

STEP 7: Diagnosefunktionen über das Kontextmenü "Online & Diagnose"

Über die Online-Funktionen können Sie von einer Engineering-Station, auf welcher das STEP 7-Projekt gespeichert ist, verschiedene Diagnoseinformationen aus der Baugruppe lesen und Instandhaltungsfunktionen ausführen.

Weitergehende Informationen zu den Diagnosefunktionen von STEP 7 erhalten Sie im STEP 7-Informationssystem.

Diagnose

Hier erhalten Sie folgende statische Informationen zur selektierten Baugruppe:

- Allgemein
Allgemeine Angaben zur Baugruppe
- Diagnosestatus
Angaben zum Diagnosestatus
- Ethernet-Schnittstelle
Adress- und statistische Angaben
- Uhrzeit
Angabe der aktuellen Uhrzeit im Modul und der Uhrzeitquelle
- Security
Zustandsangaben und Log-Einträge

Funktionen

Hier können Sie folgende Funktionen ausführen:

- Firmware-Aktualisierung
Zur Beschreibung siehe Kapitel Firmware aktualisieren (Seite 77).
- IP-Adresse zuweisen
- PROFINET-Gerätenamen vergeben
- Servicedaten speichern

STEP 7: Online-Verbindung

Über das Kontextmenü "Online verbinden" stellen Sie eine Online-Verbindung zur Baugruppe her.

Zur Vorgehensweise siehe Kapitel Online verbinden (Seite 74).

Webserver

Von einem PC aus können Sie über HTTP/HTTPS auf die Webseiten der CPU zugreifen. Diese liefern diverse Informationen.

Zum Zugriff und den Inhalten siehe Wegweiser Dokumentation (Seite 9).

SNMP

Details zu den unterstützten Funktionen finden Sie im Kapitel Diagnose über SNMP (Seite 75).

5.2 Online verbinden

Online-Funktionen

Der CP bietet zusammen mit STEP 7 an der Engineering-Station (ES) verschiedene Diagnose- und Instandhaltungsfunktionen. Voraussetzung ist, dass die ES und der CP im gleichen Subnetz liegen.

Aufbau einer Online-Verbindung über Ethernet

Vorgehensweise:

1. Verbinden Sie die ES mit dem Netz.
2. Öffnen Sie auf der ES das betreffende STEP 7-Projekt.
3. Selektieren Sie den CP.
4. Aktivieren Sie die Online-Funktionen über das Symbol "Online verbinden".

5. Selektieren Sie im Dialog "Online verbinden" in der Klappliste "Typ der PG/PC-Schnittstelle" den Eintrag "PN/IE".
6. Selektieren Sie in der Klappliste "PG/PC-Schnittstelle" die Schnittstelle der ES.
Über das Symbol  rechts neben der Klappliste können Sie die Einstellungen der Schnittstelle prüfen.
7. Selektieren Sie in der Klappliste "Verbinden mit Schnittstelle/Subnetz" die Schnittstelle der Station.
8. Klicken Sie auf "Suche starten".
Bei einer möglichen Verbindung wird die Station angezeigt.
9. Selektieren Sie in der Tabelle der Zielgeräte die Station.
Der Weg ist sowohl über den CP als auch über die CPU ist möglich.
10. Klicken Sie auf "Verbinden".

Online-Verbindung abbauen

Bauen Sie die Online-Verbindung nach Abschluss der Sitzung über die Schaltfläche "Trennen" wieder ab.

Siehe auch

Online-Funktionen (Seite 67)

5.3 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
- IP (IPv4/IPv6)
- ICMP
- TCP
- UDP
- SNMP

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

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!

Hinweis

Sicherheit des Zugriffs

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

5.4 Firmware aktualisieren

Neue Firmware-Versionen des CP

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

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

Firmware-Dateien haben das Dateiformat *.upd.

Speichern Sie die Firmware-Datei auf Ihrem PC.

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

- Online-Funktionen von STEP 7 über Ethernet
- Laden der Firmware-Datei von einer SD-Karte in der CPU

Hinweis

SD-Karte nur für Firmware-Datei

Für die Firmware-Datei benötigen Sie eine SIMATIC SD-Speicherkarte, beispielsweise (Artikelnummern):

- 6AV6671-8XB10-0AX1
- 6AV2181-8XP00-0AX0
- 6AV2181-8AQ10-0AX0

Die Karte für die Firmware-Aktualisierung darf keine anderen Dateien enthalten. Eine SD-Karte mit Projektierungsdaten können Sie nicht verwenden.

Hinweis

Dauer der Firmware-Aktualisierung

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

Warten Sie immer so lange, bis der Abschluss der Firmware-Aktualisierung an den LEDs erkennbar ist (siehe unten).

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

Voraussetzungen:

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

Vorgehensweise:

1. Selektieren Sie die Station, die Sie mit einer neuen Firmware aktualisieren wollen.
2. Aktivieren Sie die Online-Funktionen über das Symbol "Online verbinden".
3. Selektieren Sie im Dialog "Online verbinden" in der Auswahlliste "Typ der PG/PC-Schnittstelle" die Ethernet-Schnittstelle.
4. Selektieren Sie die CPU der Station.
5. Klicken Sie auf "Suche starten", um das Modul im Netz zu suchen und den Verbindungsweg festzulegen.

Wenn das Modul gefunden wurde, wird es in der Tabelle angezeigt.

6. Verbinden Sie sich über die Schaltfläche "Verbinden".
Der Assistent "Online verbinden" führt Sie durch die weiteren Schritte.
 7. Selektieren Sie in der Netzsicht die CPU und wählen Sie das Kontextmenü "Online & Diagnose" (rechte Maustaste).
 8. Wählen Sie in der Navigation der Online & Diagnose-Sicht den Eintrag "Funktionen > Firmware-Update".
 9. Suchen Sie über die Schaltfläche "Durchsuchen" (Parametergruppe "Firmware-Lader") die neue Firmware-Datei im Dateisystem der Engineering-Station.
 10. Starten Sie das Laden der Firmware über die Schaltfläche "Starte Aktualisierung", wenn im Ausgabefeld "Status" die richtige Version der signierten Firmware angezeigt wird.
- Weitere Hilfe zu den Online-Funktionen bietet Ihnen das STEP 7-Informationssystem.

Laden der Firmware über die SD-Karte

Detaillierte Informationen zum Umgang mit einer SD-Karte finden Sie im Systemhandbuch der S7-1500, siehe Wegweiser Dokumentation (Seite 9).

Voraussetzungen:

- Sie haben die neue Firmware-Datei von Ihrem PC über einen geeigneten Kartenleser auf die SD-Karte kopiert.
- Optional: Sie haben eine Sicherungsdatei der derzeitigen Firmware-Datei gespeichert.

Vorgehensweise:

1. Setzen Sie den Betriebsartenschalter der CPU nach STOP.
Stellen Sie sicher, dass im Zustand STOP keine schreibenden Funktionen (bspw. Online- oder Test-Funktionen) aktiv sind.
2. Nehmen Sie die SIMATIC Memory Card mit den Projektierungsdaten aus dem Schacht der CPU.
3. Stecken Sie die SD-Karte mit der Firmware-Datei in den Kartenschacht der CPU.
Kurze Zeit nach dem Stecken der Karte beginnt das Firmware-Update. Das Display zeigt Folgendes an: "STOP - FW UPDATE"
Bei eventuell auftretenden Fehlern werden entsprechende Meldungen angezeigt.
Nach dem Beenden des Firmware-Updates zeigt das Display eine Ergebnisseite an.
Ein erfolgreiches Firmware-Update erkennen Sie an folgendem LED-Bild der CPU:
 - RUN leuchtet gelb.
 - MAINT blinkt gelb.
4. Entnehmen Sie die SD-Karte und stecken Sie wieder die SIMATIC Memory Card.
5. Setzen Sie den Betriebsartenschalter der CPU nach RUN.
Der CP verwendet beim Anlauf die neue Firmware.
Zum LED-Bild des CP während des Anlaufs siehe Kapitel LEDs (Seite 21).

5.5 Baugruppentausch ohne PG

Projektierungsdaten beim Baugruppentausch

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 bei Adress-Bezug über DHCP (IPv4)

Eine Option bei der IP-Konfiguration des CP ist der Bezug der IP-Adresse von einem DHCP-Server.

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 dem DHCP-Server die werkseitig eingestellte MAC-Adresse der neuen Baugruppe übermittelt wird, liefert der DHCP-Server 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, dass der CP nach einem Baugruppetausch immer die gleiche IP-Adresse vom DHCP-Server erhält.

Wenn Sie statt der werkseitig eingestellten MAC-Adresse eine neue MAC-Adresse projiziert 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

6.1 Technische Daten des CP

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.

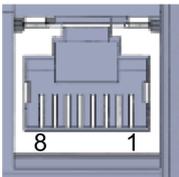
Technische Daten - CP 1543-1	
Produktbezeichnung	CP 1543-1
Artikelnummer	6GK7 543-1AX00-0XE0
Anschluss an Industrial Ethernet	
• Anzahl	1 x Ethernet (Gigabit)-Schnittstelle
• Ausführung	RJ45-Buchse
• Übertragungsgeschwindigkeit	10 / 100 / 1000 Mbit/s
Elektrische Daten	
Spannungsversorgung	
• über S7-1500 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)	35 x 142 x 129 mm
Montagemöglichkeiten	Montage im S7-1500 Rack
Produktfunktionen *	

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

6.2 Belegung der Ethernet-Schnittstelle

Belegung der Gigabit-Ethernet-Schnittstellen

Die folgende Tabelle zeigt die Anschlussbelegung der Schnittstelle X1.

Ansicht der RJ45-Buchse	Pin	Signalname	Belegung
	1	D1+	D1+ bidirektional
	2	D1-	D1- bidirektional
	3	D2+	D2+ bidirektional
	4	D3+	D3+ bidirektional
	5	D3-	D3- bidirektional
	6	D2-	D2- bidirektional
	7	D4+	D4+ bidirektional
	8	D4-	D4- bidirektional

6.3 Zulässige Leitungslängen - Ethernet

Zulässige Leitungslängen - Ethernet	Alternative Kombinationen pro Längenbereich
0 ... 55 m	<ul style="list-style-type: none"> 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
0 ... 85 m	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

Siehe auch Siemens Mall: (<https://mall.industry.siemens.com>)

6.4 Zulässige Leitungslängen - Gigabit-Ethernet

Zulässige Leitungslängen - Gigabit-Ethernet	Alternative Kombinationen
0 ... 60 m	<ul style="list-style-type: none"> Max. 60 m IE FC TP Flexible Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 über IE FC RJ45 Modular Outlet Insert 1GE
0 ... 100 m	<ul style="list-style-type: none"> Max. 90 m IE FC TP Standard Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 über IE FC RJ45 Modular Outlet Insert 1GE

Siehe auch Siemens Mall: (<https://mall.industry.siemens.com>)

Zulassungen

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



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
 Digital Industries
 Postfach 48 48
 90026 Nuernberg
 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

Zertifikat: IECEX DEK 14.0089X

Angewandte Normen:

- EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-15 - Explosionsfähige Atmosphäre - Teil 15: Geräteschutz durch Zündschutzart 'n'

- Ex ec IIC T4 Gc

Zertifikat: IECEX DEK 18.0019X

Angewandte Normen:

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

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

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

ATEX-Zulassung:

- II 3 G Ex nA IIC T4 Gc

Type Examination Certificate: DEKRA 12 ATEX 0240X

Angewandte Normen:

- EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-15 - Explosionsfähige Atmosphäre - Teil 15: Geräteschutz durch Zündschutzart 'n'

- II 3 G Ex ec IIC T4 Gc

Type Examination Certificate: DEKRA 18 ATEX 0027X

Angewandte Normen:

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

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

Die Bedingungen für den sicheren Einsatz des Produkts gemäß Kapitel Hinweise für den Einsatz im Ex-Bereich gemäß ATEX / IECEx (Seite 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-DVD 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 die Anforderungen der EU-Richtlinie 2014/30/EU "Elektromagnetische Verträglichkeit" (EMV-Richtlinie).

Angewandte Normen:

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

RoHS

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

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.

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 사용하는 것을 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, 35
- Anweisung
 - FTP_CMD, 20
 - T_CONFIG, 20
 - TCON, TSEND/TRCV, 19
 - TDISCON, 19
 - TMAIL_C, 19
 - TSEND_C/TRCV_C, 19
 - TUSEND/TURCV, 19
- Anzahl
 - betreibbarer CPs, 18
- Autocrossing-Mechanismus, 35
- Autosensing, 35

B

- Besondere Hinweise
 - Anschluss eines Switch, 35
 - Empfehlung für die Zeitvorgabe, 41
 - Gültige Uhrzeit sicherstellen, 41
- Betriebszustand der CPU, 30

D

- Datenhaltung - Projektierungsdaten, 80
- DHCP, 80
- Doppeladressierung im Netzwerk, 36
- Downloads, 10

E

- E-Mail, 11
- E-Mail-Verbindung, 15
- EMV - Elektromagnetische Verträglichkeit, 83
- Entsorgung, 6
- Ethernet-Schnittstelle, 3, 23
 - Konfiguration über T_CONFIG, 20
- Ethernnet-Schnittstelle
 - Anschlussbelegung, 29

F

- FETCH/WRITE, 12, 35
 - S5-/S7-Adressierungsmodus, 14
- FETCH/WRITE-Verbindungen, 15
- Firewall, 14
- Firmware-Version, 3
- FTP, 35
 - Verhalten bei fehlendem Verweis auf den FTP-Auftragsblock, 54
- FTP (FTP-Client), 15
- FTP_CMD, 45
 - Baustein-Laufzeit, 17
- FTP-Client
 - Mengengerüst, 17
- FTPS, 14
- FTPS - Security, 42
- FTP-Server
 - Mengengerüst, 17

G

- Gateway (VPN), 66
- gekreuztes Kabel, 35
- Gesamtmengengerüst, 18
- Gigabit-Spezifikation, 23
- Glossar, 6

H

- Hardware-Erzeugnisstand, 3
- HMI-Kommunikation, 11

I

- Inbetriebnahme
 - Vollständigkeit der STEP 7-Projektdateien, 28
- IP-Adresse
 - IPv6, 13
 - über DHCP, 36
- IP-Konfiguration
 - IPv4 / IPv6, 13
- IP-Routing, 36
- IPSec-Tunnel
 - Anzahl, 18

ISO-on-TCP (gemäß RFC 1006), 11
ISO-on-TCP-Verbindungen, 15
ISO-Transport (gemäß RFC 8073), 11
ISO-Transportverbindungen, 15

L

Laden der Projektdaten, 29
LED-Anzeige, 21
Logging, 14

M

MAC-Adresse, 3, 12
Manual Collection, 10
MIB, 75
Montage und Inbetriebnahme, 28
 Vorgehensweise, 28
Multicast
 über UDP, 11

N

NTP (secure), 14, 41
NTP-Server, 41
NTP-Verfahren, 12

O

Online-Diagnose, 73
Online-Funktionen, 74
Online-Hilfe von STEP 7, 29
Open User Communication (OUC), 11
OP-Verbindungen
 Anzahl, 17
OUC (Open User Communication), 68

P

Passiver VPN-Verbindungsaufbau, 66
PG-Kommunikation, 11
PG-Verbindungen
 Anzahl, 17
Port 8448, 68
Programmbausteine - max. Datenlänge, 16
Programmierte Kommunikationsverbindung, 40
Programmierte Verbindungen
 Anzahl, 17
Projektierung, 28
Projektierung und Laden der Projektierungsdaten, 19

PUT/GET, 35

R

Recycling, 6
RUN → STOP, 30

S

S5-/S7-Adressierungsmodus, 14
S7-Kommunikation, 11
S7-Verbindungen, 11, 15
 Anzahl frei nutzbarer, 17
Security-Diagnose, 68
Sicherheitshinweise, 25
SIMATIC NET, 10
SIMATIC NET-Glossar, 6
SMTPS, 15
SNMP, 75
SNMP-Agent, 12
SNMPv3, 15
STEP 7, 5, 19
Stromversorgungsmodule
 zusätzliche, 18
Systemdatentyp
 FTP_..., 20
 TCON_..., 19
 TMail_..., 19
Systemdatentypen (SDTs), 70

T

TCP (gemäß RFC 793), 11
TCP-Verbindungen, 15
TCP-Verbindungen für FTP, 17

U

UDP
 Einschränkungen, 16
UDP (gemäß RFC 768), 11
UDP-Telegramm-Pufferung, 16
UDP-Verbindungen, 15
Uhrzeitsynchronisierung, 12

V

Verbindungen für Web
 Anzahl, 17
Verbindungsressourcen der CPU, 15

Versionshistorie, 10
Virtual Private Network
 Definition, 61
VPN, (Virtual Private Network)
 Anwendungsgebiete, 62
 Zellenschutzkonzept, 62

W

Webserver, 13

Z

Zellenschutzkonzept
 VPN, 62

