

SIEMENS

SIMATIC NET

TeleControl Projektierung - IEC 60870-5

Projektierungshandbuch

Vorwort

Funktionen und
Voraussetzungen **1**

Kommunikations-
Mechanismen **2**

Projektierung **3**

Inbetriebnahme **4**

Diagnose und
Instandhaltung **5**

OUC-Programmbausteine
(CP) **A**

SINEMA Remote Connect
(CP) **B**

WBM der TIM 1531 IRC **C**

Security **D**

Literaturverzeichnis **E**

Projektierung und Diagnose


02/2023


C79000-G8900-C509-04


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

Gültigkeit dieses Handbuchs

Das vorliegende Projektierungshandbuch ist gültig für folgende SIMATIC NET-Kommunikationsmodule, die das Protokoll IEC 60870-5 unterstützen:

- CP 1243-1
- CP 1243-7 LTE
- CP 1243-8 IRC
- CP 1542SP-1 IRC
- TIM 1531 IRC

Die Geräte-Versionen und die erforderlichen Produkte der Projektierungs-Software finden Sie im Kapitel Kommunikationsmodule (Seite 11).

Abkürzungen / Gerätebezeichnungen

In diesem Handbuch werden folgende Abkürzungen häufig verwendet:

- **Modul / Baugruppe / Gerät / CP / TIM**

Bezeichnungen für das jeweilige Kommunikationsmodul

- **Mobilfunk-CP**

CP 1243-7 LTE

- **STEP 7**

Diese Abkürzung wird nachfolgend für das Projektierungswerkzeug STEP 7 Basic / Professional verwendet.

- **WBM**

"WBM" ist die Abkürzung des "Web Based Management", der Seiten des Webserver der TIM für Projektierungs- und Diagnosedaten.

Neu in dieser Ausgabe

- TIM 1531 IRC V2.3 und CP 1542SP-1 IRC V2.2

Neue Firmware-Versionen mit folgenden neuen Funktionen:

- TLS-Erweiterung für das Protokoll DNP3
- TLS-Erweiterung für das Protokoll IEC 60870-5-104
- Secure Authentication für das Protokoll IEC 60870-5-101/104

- Neue Projektierungs-Software

STEP 7 Professional V18 mit folgenden für die Produkte relevanten Funktionen:

- Projektierbarkeit der oben genannten neuen Funktionen
- Geänderte Handhabung der Zertifikate

Abgelöste Handbuchausgabe

Ausgabe 05/2021

Aufbau der Dokumentation

Die Dokumentation der SIMATIC NET Telecontrol-Kommunikationsmodule besteht jeweils aus folgenden Handbüchern:

- Betriebsanleitung oder Gerätehandbuch
- Projektierungshandbücher (1 Projektierungshandbuch für jedes Telecontrol-Protokoll)

Die Internet-Links der Handbücher finden Sie im Literaturverzeichnis (Seite 225).

Für Module, die das Protokoll IEC 60870-5 unterstützen, besteht die Dokumentation aus folgenden Dokumenten:

CP-Baugruppen

- **Betriebsanleitung**

Gültig für den jeweiligen CP

- Anwendung, Funktionen, Voraussetzungen (CPUs, Software etc.)
- Hardware-Beschreibung
- Montage, Anschluss, Inbetriebnahme, Betrieb
- Projektierung (nur Telecontrol-unabhängige Funktionen)

Wenn Sie Telecontrol-Funktionen nutzen, dann lesen Sie das betreffende Projektierungshandbuch.

- Diagnose, Instandhaltung
- Technische Daten, Zulassungen, Zubehör

- **Projektierungshandbuch IEC 60870-5**

- Projektierung und Diagnose in STEP 7 Professional (TIA Portal)

TIM 1531 IRC

- **Gerätehandbuch**

- Anwendung und Funktionen
- Voraussetzungen (CPUs, Projektierungs-Software etc.)
- Hardware-Beschreibung
- Montage, Anschluss, Inbetriebnahme, Betrieb
- Diagnose, Instandhaltung
- Technische Daten, Zulassungen, Zubehör

- **Projektierungshandbuch IEC 60870-5**

- Projektierung und Diagnose in STEP 7 Professional (TIA Portal)

Aktuelle Handbuchausgabe im Internet

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

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/21764/man>)

Vorausgesetzte Kenntnisse

Für die Projektierung und Diagnose der Geräte werden Kenntnisse auf folgenden Gebieten vorausgesetzt:

- SIMATIC STEP 7 Professional
- Datenübertragung über WAN-Netze
- Aufbau industrieller Netze mit Security-Funktionen

Querverweise

In diesem Handbuch werden häufig Querverweise zu anderen Kapiteln verwendet.

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

Lizenzbedingungen

Hinweis

Open Source Software

Die Produkte enthalten Open Source Software. Lesen Sie die Lizenzbedingungen zur Open Source Software genau durch, bevor Sie die Produkte nutzen.

Hinweise zum Auffinden der Lizenzbedingungen finden Sie in der Betriebsanleitung des jeweiligen Produkts.

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: (<https://www.siemens.com/cert>)

Informieren Sie sich vor der Konfiguration und Inbetriebnahme der Baugruppen über deren Security-Funktionen:

Funktionen, Leistungsdaten und Mengengerüst (Seite 16)

Lesen Sie die Security-Empfehlungen im Anhang "Security":
Security (Seite 215)

SIMATIC NET-Glossar

Das SIMATIC NET-Glossar beschreibt Fachbegriffe, die möglicherweise in diesem Dokument verwendet werden.

Sie finden das SIMATIC NET-Glossar beim Siemens Industry Online Support unter folgender Adresse:

Link: (<http://support.automation.siemens.com/WW/view/de/50305045>)

Inhaltsverzeichnis

	Vorwort.....	3
1	Funktionen und Voraussetzungen	11
1.1	Kommunikationsmodule.....	11
1.2	Konfigurationsbeispiele.....	12
1.3	Einsetzbare CPUs	15
1.4	Software-Voraussetzungen	15
1.5	Funktionen, Leistungsdaten und Mengengerüst	16
1.5.1	CP 1243-1	16
1.5.2	CP 1243-7 LTE.....	18
1.5.3	CP 1243-8 IRC	20
1.5.4	CP 1542SP-1 IRC	21
1.5.5	TIM 1531 IRC	25
2	Kommunikations-Mechanismen.....	29
2.1	Kommunikationsmöglichkeiten.....	29
2.2	Adressierung	29
2.3	Verbindungsaufbau	31
2.4	Quittierung.....	32
3	Projektierung	33
3.1	Kommunikationsarten.....	33
3.2	Grundeinstellungen	34
3.3	Uhrzeitsynchronisation	37
3.4	Projektierung von Schnittstellen, Netzen und Netzknoten.....	45
3.4.1	WAN-Einstellungen der Schnittstellen.....	45
3.4.2	Vernetzen der Schnittstellen	46
3.5	Ethernet-Schnittstelle	48
3.5.1	Ethernet-Adressen	48
3.5.2	Erweiterte Optionen.....	49
3.5.2.1	TCP-Verbindungsüberwachung	49
3.5.2.2	Übertragungseinstellungen.....	50
3.5.3	Zugriff auf den Webserver.....	51
3.5.3.1	CP.....	51
3.5.3.2	TIM 1531 IRC	51
3.6	Serielle Schnittstelle.....	51
3.6.1	WAN-Parameter	51
3.6.2	Erweiterte Optionen.....	52
3.6.2.1	Standleitung	52
3.6.2.2	Wählnetz	54

3.6.2.3	Übertragungseinstellungen.....	55
3.7	IEC-Parameter der Schnittstellen	56
3.7.1	Übertragungseinstellungen - IEC 60870-5	56
3.7.2	Einstellungen IEC-Master	58
3.7.3	Einstellungen IEC-Station	59
3.8	WAN-Netze projektieren.....	60
3.9	Webserver (TIM 1531 IRC).....	63
3.10	Webdiagnose der TIM 1531 IRC.....	65
3.11	DNS-Konfiguration.....	65
3.12	Kommunikation mit der CPU	66
3.13	E-Mail-Projektierung	71
3.14	Teilnehmernummern.....	72
3.15	Gesicherte Kommunikation zwischen CPU und Modul.....	74
3.16	Log-Einstellungen.....	76
3.17	SNMP	76
3.18	Globaler Zertifikatsmanager.....	78
3.19	CP: Security und Zertifikate	78
3.19.1	Security-Benutzer.....	78
3.19.2	Log-Einstellungen - Filtern der System-Ereignisse	78
3.19.3	SYSLOG	79
3.19.4	VPN	79
3.19.4.1	VPN (Virtual Private Network).....	79
3.19.4.2	VPN-Tunnel für S7-Kommunikation zwischen Stationen anlegen	80
3.19.4.3	VPN-Kommunikation mit SOFTNET Security Client (Engineering-Station)	82
3.19.4.4	VPN-Tunnelkommunikation zwischen CP und SCALANCE M aufbauen.....	83
3.19.4.5	CP als passiver Teilnehmer von VPN-Verbindungen.....	83
3.19.5	Zertifikatsmanager.....	84
3.19.6	Handhabung von Zertifikaten.....	84
3.19.7	Gesicherte Kommunikation zwischen CPU und Kommunikationsmodul.....	87
3.19.8	CP 1542SP-1 IRC: Zertifikate zu Telecontrol-Verbindungen mit TLS.....	88
3.20	TIM 1531 IRC: Schutz und Zertifikate.....	89
3.20.1	Schutz.....	89
3.20.2	Zugriffsschutz projektieren	90
3.20.3	TIM 1531 IRC: Handhabung der Zertifikate für TLS.....	91
3.21	Telecontrol-Verbindungen	97
3.21.1	Telecontrol-Verbindungen	97
3.21.2	Der Editor "Netzwerkdaten".....	98
3.21.3	Verbindungswege festlegen.....	100
3.21.4	Verbindungstabelle.....	104
3.21.5	Parameter der IEC-Verbindungen	107
3.21.5.1	Allgemein.....	107
3.21.5.2	TCP-Verbindungsüberwachung	108
3.21.5.3	IEC 60870-5 Security-Optionen	109
3.21.5.4	Security-Statistik-Optionen (IEC 60870-5-104)	112
3.21.5.5	Abfrageoptionen	114

3.21.5.6	Fremdgerät-Parameter.....	115
3.22	Datenpunkte.....	115
3.22.1	Datenpunktprojektierung.....	115
3.22.2	Datenpunkttypen.....	123
3.22.3	Statuskennungen der Datenpunkte	125
3.22.4	Register "Allgemein".....	126
3.22.5	Master-Funktion der Datenpunkte.....	127
3.22.6	Datenpunktindex.....	128
3.22.7	Prozessabbild, Übertragungsart, Ereignisklassen.....	130
3.22.8	Lesezyklus	132
3.22.9	Register "Trigger".....	133
3.22.10	Schwellenwert-Trigger.....	136
3.22.11	Analogwert-Vorverarbeitung.....	138
3.22.12	Befehlsoptionen.....	146
3.22.13	Partnerstationen.....	149
3.23	Nachrichten.....	149
3.24	Zeichensatz für Benutzernamen, Passwörter und Nachrichten	155
4	Inbetriebnahme.....	157
4.1	CP in Betrieb nehmen.....	157
4.2	Uhrzeit bei Betrieb mit Security / SINEMA RC stellen.....	157
5	Diagnose und Instandhaltung	159
5.1	Diagnosemöglichkeiten.....	159
5.2	Webserver S7-1200: Verbindungsaufbau.....	161
5.3	Online-Security-Diagnose über Port 8448.....	162
5.4	Telegrammprotokoll-Diagnose	163
5.4.1	Telegrammprotokoll: Aufbau und Funktionen	163
5.4.2	Details	164
5.5	SNMP.....	165
5.6	Bearbeitungsstatus der Nachrichten (SMS, E-Mail).....	166
5.7	Instandhaltung	168
A	OUC-Programmbausteine (CP).....	169
A.1	Gültigkeit und Voraussetzungen.....	169
A.2	Programmbausteine für OUC.....	169
A.3	Änderung der IP-Adresse zur Laufzeit	173
A.4	SMS über OUC	174
A.5	TC_CONFIG zum Ändern der Projektierungsdaten des CP	177
A.6	IF_CONF_*: SDTs für Projektierungsdaten des CP.....	180
B	SINEMA Remote Connect (CP)	187
B.1	Gültigkeit und Voraussetzungen.....	187
B.2	Anbindung an SINEMA RC.....	187

B.3	Telecontrol über SINEMA RC.....	189
B.4	Security > VPN > SINEMA Remote Connect	189
C	WBM der TIM 1531 IRC	193
C.1	Unterstützte Webbrowser	193
C.2	Verbindung mit dem WBM der TIM aufbauen	193
C.3	Allgemeine Funktionen des WBM	194
C.4	Startseite.....	195
C.5	System	197
C.5.1	Geräte-Info	197
C.5.2	SD-Karte.....	197
C.5.3	Systemzeit.....	198
C.5.4	NTP	198
C.5.5	Webserver	198
C.5.6	DNS-Konfiguration.....	199
C.6	Instandhaltung	199
C.6.1	Firmware.....	199
C.6.2	Betriebszustand	201
C.7	Diagnose	202
C.7.1	Ereignisse.....	202
C.7.2	Nachrichten.....	203
C.8	LAN	204
C.8.1	Ethernet-Schnittstelle [Xn].....	204
C.9	Telecontrol	206
C.9.1	Partnerinformationen	206
C.9.1.1	Verbindungsübersicht.....	206
C.9.1.2	Sendepuffer.....	210
C.9.2	Datenpunkte.....	211
C.10	Logging.....	212
D	Security.....	215
D.1	Security-Empfehlungen.....	215
D.2	Syslog-Meldungen der TIM 1531 IRC.....	218
D.2.1	Aufbau der Syslog-Meldungen	218
D.2.2	Variablen in Syslog-Meldungen	219
D.2.3	Erläuterungen zu den Meldungen	221
D.2.4	Meldungen für TIM 1531 IRC.....	221
E	Literaturverzeichnis.....	225
	Index.....	229

Funktionen und Voraussetzungen

1.1 Kommunikationsmodule

Kommunikationsmodule für das Telecontrol-Protokoll IEC 60870-5

Die folgenden SIMATIC NET-Kommunikationsmodule sind für das Telecontrol-Protokoll IEC 60870-5 einsetzbar.

Bedeutung von Symbolen in der Tabelle:

- X = unterstützt
- - = nicht unterstützt

Tabelle 1- 1 Kommunikationsmodule für IEC 60870-5

Modul Artikelnummer	Anzahl Schnittstellen *			Stationstyp			STEP 7- Produkt	Erforderlic he Firmware
	IE IEC 60870- 5- 104	RS IEC 60870- 5- 101	M	Master	Knotenstati on	Station		
TIM 1531 IRC 6GK7 543-1MX00-0XE0	3	1 **	- ***	X	X	X	STEP 7 Professiona l	V2.3
CP 1542SP-1 IRC 6GK7 542-6VX00-0XE0	1	-	- ***	-	-	X	STEP 7 Professiona l	V2.2
CP 1243-8 IRC 6GK7 243-8RX30-0XE0	1	-	-	-	-	X	STEP 7 Basic **** / Professiona l	V3.3
CP 1243-1 6GK7 243-1BX30-0XE0 6AG1 243-1BX30-2AX0	1	-	-	-	-	X	STEP 7 Basic **** / Professiona l	V3.3
CP 1243-7 LTE 6GK7 243-7KX30-0XE0 6GK7 243-7SX30-0XE0	-	-	1	-	-	X	STEP 7 Basic **** / Professiona l	V3.3

* IE = Ethernet-Schnittstellen, RS = serielle Schnittstellen, M = Integrierte Mobilfunk-Schnittstelle

** Für den Anschluss an die serielle Schnittstelle werden keine GSM-Module unterstützt.

*** TIM-Baugruppen können über Modems an Mobilfunknetze angeschlossen werden.

**** STEP 7 Basic bei Anschluss des CP an einen Fremd-Master. Siehe Hinweis unten.

Hinweise zur Tabelle

Hinweise zu den Spalten:

- **Stationstyp "Knotenstation"**

Eine Knotenstation befindet sich in der Anlagenhierarchie zwischen der Zentrale (Master) und weiteren unterlagerten Stationen. Das Modul benötigt mindestens zwei Schnittstellen.

In der Projektierung wird der "Netzknotentyp" derjenigen Schnittstelle, die mit der Zentrale verbunden ist, als "Knotenstation" projektiert. Siehe hierzu Kapitel Vernetzen der Schnittstellen (Seite 46).

- **STEP 7-Produkt bei S7-1200-CPs**

CPs der S7-1200 können unter STEP 7 Basic für den Anschluss an einen Fremd-Master projektiert werden.

Für den Anschluss der CPs an SIMATIC NET-Master oder Knotenstationen, die in STEP 7 projektiert werden, benötigen Sie STEP 7 Professional.

- **Firmware**

Die erforderlichen Firmware-Versionen der Module beziehen sich auf die vollständige in diesem Handbuch beschriebene Projektierung. Die hierfür erforderliche STEP 7-Version finden Sie im Kapitel Software-Voraussetzungen (Seite 15).

Module mit kleineren Firmware-Versionen können auch in der aktuellen aktuellen STEP 7-Versionen mit einem abweichenden Funktionsumfang projektiert werden.

1.2 Konfigurationsbeispiele

Im Folgenden finden Sie einige Konfigurationsbeispiele mit den einsetzbaren Kommunikationsmodulen.

Kommunikation über Ethernet / Internet, Versenden von E-Mails

In der abgebildeten Beispielfunktion kommunizieren S7-Stationen mit Zentrale über die Ethernet-Schnittstellen der verschiedenen Module.

TIM-Baugruppen ermöglichen mit ihren Ethernet-Schnittstellen die Anbindung an eine redundante Zentrale.

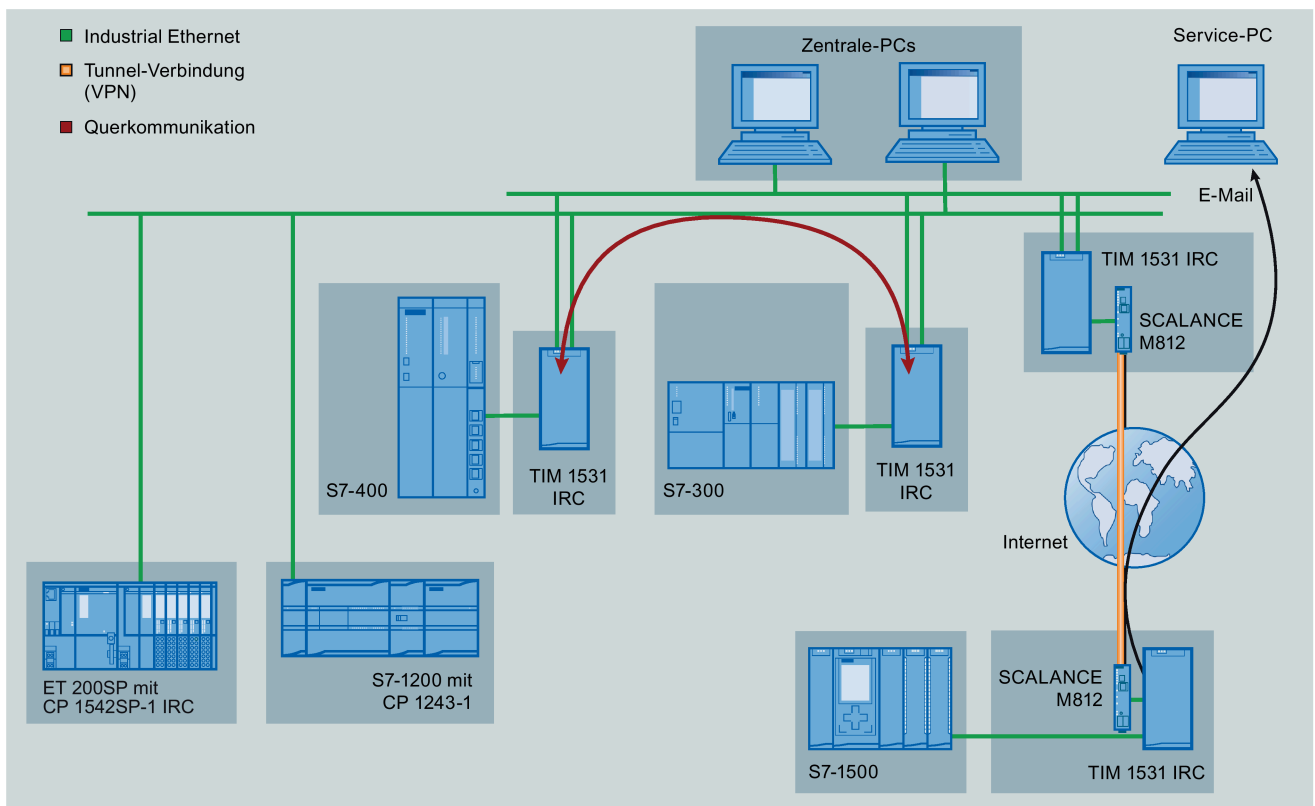


Bild 1-1 Kommunikation über Ethernet / Internet

E-Mails

Die Module können E-Mails versenden. Mögliche Empfänger sind:

- Für projektierte ereignisgesteuerte E-Mails:
 - PCs mit Internetanschluss
 - Mobiltelefone
- Für E-Mails über OUC-Bausteine:
 - SIMATIC-Stationen mit den entsprechenden Programmbausteinen

Direkte Kommunikation

Direkte Kommunikation zwischen S7-Stationen mit Kommunikationsmodul ist über IP-basierte Netze möglich. Die Telegramme laufen nicht über die Zentrale.

Direkte Kommunikation kann über folgende Mechanismen ermöglicht werden:

- Projektierte Telecontrol-Verbindungen
Zu den Voraussetzungen siehe Kommunikationsmöglichkeiten (Seite 29).
- Programmbausteine der Open User Communication
Siehe OUC-Programmbausteine (CP) (Seite 169)

Wegeredundanz unter Nutzung der seriellen Schnittstelle

Im nachfolgenden Beispiel werden bei der TIM 1531 IRC die Ethernet-Schnittstelle und die serielle Schnittstelle zum Aufbau redundanter Übertragungswege genutzt.

- Ethernet-Schnittstelle zur Kommunikation über Ethernet / Internet
- Serielle Schnittstelle zur Kommunikation über ein WAN-Netz (Standleitung bzw. Wählnetz)

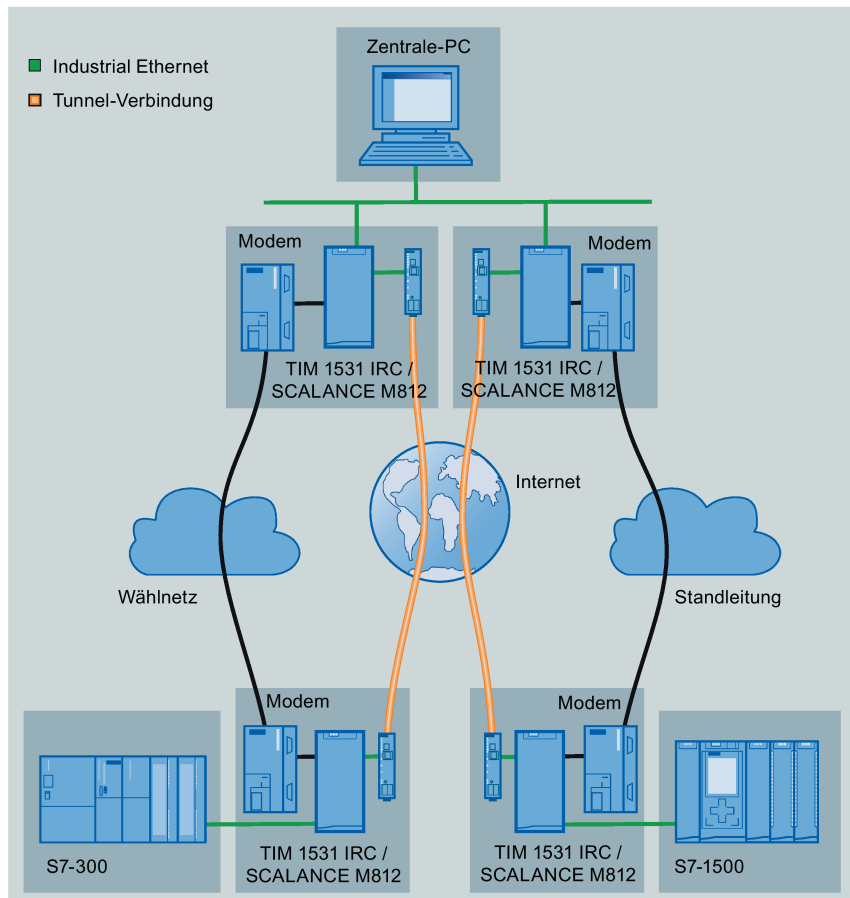


Bild 1-2 Kommunikation über redundante Wege

Wegeredundanz ist auch über zwei Ethernet-Netze möglich.

1.3 Einsetzbare CPUs

Kompatible CPUs

Als zugeordnete CPU der Kommunikationsmodule sind projektierbar:

- **TIM 1531 IRC ab V2.1**
 - S7-1500
 - Alle Standard-CPU's ab Firmware-Version V2.1
 - Alle redundanten CPU's (H-CPU, R-CPU) ab Firmware-Version V2.6
 - ET 200SP
 - Ab Firmware-Version V2.1 unterstützt die TIM 1531 IRC den Anschluss an:
Alle in STEP 7 projektierbaren CPU's ab Firmware-Version V2.5
 - S7-300
 - Alle CPU's mit PROFINET-Schnittstelle
 - S7-400
 - Alle in STEP 7 projektierbaren CPU's
- **CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC**
 - CPU ab Firmware-Version V4.2
 - Die volle Funktionalität des CP steht nur mit einer CPU ab V4.4 zur Verfügung.
- **CP 1542SP-1 IRC**
 - CPUs ab Firmware-Version V2.0:
 - CPU 1510SP-1 PN
 - CPU 1510SP F-1 PN
 - CPU 1512SP-1 PN
 - CPU 1512SP F-1 PN

Weitere Informationen zu den CPUs und den BusAdaptern finden Sie im Handbuch *I6I* (Seite 226).

1.4 Software-Voraussetzungen

Software für Projektierung und Online-Funktionen

Für die Projektierung des vollen in diesem Handbuch beschriebenen Funktionsumfangs der Module ist STEP 7 in der folgenden Version erforderlich:

- STEP 7 Basic / Professional V18

Zum jeweils benötigten STEP 7-Produkt siehe Kapitel Kommunikationsmodule (Seite 11).

1.5 Funktionen, Leistungsdaten und Mengengerüst

1.5.1 CP 1243-1

Anzahl CMs/CPs pro Station

Pro S7-1200-Station können bis zu drei CMs/CPs gesteckt und projektiert werden.

Zur Nutzung der Telecontrol-Kommunikation können pro Station drei CP 1243-1 gesteckt werden.

Verbindungs-Ressourcen

- **Telecontrol-Verbindungen inklusive Querkommunikation / Direkte Kommunikation**
Der CP kann Verbindungen mit bis zu 4 Kommunikationspartnern aufbauen.
Als Partner gilt ein einfach oder redundant aufgebauter Master oder eine Station (Direkte Kommunikation).
Zur Projektierung der direkten Kommunikation zwischen Stationen siehe Kapitel Kommunikationsmöglichkeiten (Seite 29).
- **S7-Verbindungen und TCP- / UDP- / ISO-on-TCP-Verbindungen**
Max. 14 Verbindungs-Ressourcen, beliebig aufteilbar für:
 - S7-Verbindungen (PUT/GET)
Inklusive Verbindungen für S7-Routing
 - Verbindungen über Programmbausteine (OUC) mit S7-Stationen
- **Online-Funktionen**
1 Verbindungs-Ressource ist für Online-Funktionen reserviert.
- **PG/OP-Verbindungen**
 - 1 Verbindungs-Ressource für PG-Verbindungen
 - 3 Verbindungs-Ressourcen für OP-Verbindungen

Anzahl der Datenpunkte für die Datenpunktprojektierung

Maximale Anzahl projektierbarer Datenpunkte pro CP

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

Telegrammspeicher (Sendepuffer)

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

Der Sendepuffer teilt sich auf alle projizierten Kommunikationspartner zu gleichen Teilen auf. Die Größe des Telegrammspeichers ist in STEP 7 einstellbar, siehe Kapitel Prozessabbild, Übertragungsart, Ereignisklassen (Seite 130).

Die maximale Größe des Sendepuffers beträgt:

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

Nachrichten (E-Mail)

- Versenden von bis zu 10 Nachrichten (E-Mails) mit Projektierung im Nachrichteneditor

IPSec-Tunnel (VPN)

Bis zu 8 IPSec-Tunnel können für die gesicherte Kommunikation mit weiteren Security-Modulen aufgebaut werden.

Firewall-Regeln

Die maximale Anzahl der Firewall-Regeln im erweiterten Firewall-Modus ist auf 256 begrenzt.

Die Firewall-Regeln teilen sich wie folgt auf:

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

1.5.2 CP 1243-7 LTE

Verbindungs-Ressourcen

- **Telecontrol-Verbindungen**
 - DNP3 / IEC
Der CP kann Verbindungen mit bis zu 4 Kommunikationspartnern aufbauen.
Als Partner gilt ein einfach oder redundant aufgebauter Master oder eine Station (Direkte Kommunikation).
 - TeleControl Basic
1 reservierte Verbindung für den Nutzdatenaustausch mit dem Telecontrol-Server
Zusätzlich Querkommunikation: Die Querkommunikation zwischen den CPs zweier Stationen läuft über den Telecontrol-Server. Sie wird in der Parametergruppe "Partnerstationen" > "Partner für Querkommunikation" projektiert.
Mengengerüst für Querkommunikation: Insgesamt max. 15, davon:
 - Senden an Partner: Max. 3 (Parameter "Sendepuffer" aktiviert)
 - Empfangen von Partnern: Max. 15 (Parameter "Sendepuffer" deaktiviert)
- **S7-Verbindungen und TCP- / UDP- / ISO-on-TCP-Verbindungen**

Max. 14 Verbindungs-Ressourcen, beliebig aufteilbar für:

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

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

Max. 1 Verbindung zu einem NTP-Server

Nutzdaten

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

Nutzdaten pro Telegramm bei den unterschiedlichen Verbindungstypen:

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

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

Anzahl der Datenpunkte für die Datenpunktprojektierung

Die maximale Anzahl der projektierbaren Datenpunkte unter den Telecontrolprotokollen beträgt:

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

Telegrammspeicher (Sendepuffer)

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

Der Sendepuffer hat folgende maximale Größe:

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

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

Nachrichten: E-Mail / SMS

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

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

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

IPSec-Tunnel (VPN)

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

Firewall-Regeln

Die maximale Anzahl der Firewall-Regeln im erweiterten Firewall-Modus ist auf 256 begrenzt.

Die Firewall-Regeln teilen sich wie folgt auf:

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

1.5.3 CP 1243-8 IRC

Anzahl CMs/CPs pro Station

Pro S7-1200-Station können bis zu drei CMs/CPs gesteckt und projektiert werden, davon maximal ein CP 1243-8 IRC.

Verbindungs-Ressourcen

- **Telecontrol-Verbindungen**
Der CP kann Verbindungen mit bis zu 4 Kommunikationspartnern aufbauen.
Die Partner können redundant angebunden sein.
- **TCP-/UDP-Verbindungen**
Der CP kann Verbindungen mit bis zu 4 Kommunikationspartnern (S7-Stationen) aufbauen.
- **Online-Funktionen**
1 Verbindungs-Ressource ist für Online-Funktionen reserviert.
- **S7-Verbindungen**
8 Verbindungs-Ressourcen für S7-Verbindungen (BSEND/BRCV)
- **S7-Routing**
Max. 4 Verbindungen gleichzeitig
- **PG/OP-Verbindungen**
 - 2 Verbindungs-Ressourcen für PG-Verbindungen
 - 1 Verbindungs-Ressource für OP-Verbindungen

Anzahl der Datenpunkte für die Datenpunktprojektierung

Maximale Anzahl projektierbarer Datenpunkte pro CP: 500

Telegrammspeicher (Sendepuffer)

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

Der Sendepuffer hat eine maximale Größe von 64000 Ereignissen. Die Größe des Telegrammspeichers teilt sich auf alle projizierten Kommunikationspartner zu gleichen Teilen auf. Sie ist in STEP 7 einstellbar, siehe Kapitel Kommunikation mit der CPU (Seite 66).

Details zur Funktion des Sendepuffers (Speichern und Senden von Ereignissen) sowie zu den Übertragungsmöglichkeiten von Daten finden Sie im Kapitel Prozessabbild, Übertragungsart, Ereignisklassen (Seite 130).

Nachrichten: E-Mail

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

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

IPSec-Tunnel (VPN)

Bis zu 8 IPSec-Tunnel können für die gesicherte Kommunikation mit weiteren Security-Modulen aufgebaut werden.

Firewall-Regeln

Die maximale Anzahl der Firewall-Regeln im erweiterten Firewall-Modus ist auf 256 begrenzt.

Die Firewall-Regeln teilen sich wie folgt auf:

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

1.5.4 CP 1542SP-1 IRC

Anzahl CPs pro Station

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

Zu Details der erlaubten Sonderbaugruppen und den Steckplatzregeln siehe Gerätehandbuch.

Verbindungs-Ressourcen

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

Siehe Betriebsanleitung des CP /6/ (Seite 226).

Zusätzlich:

- **Telecontrol-Verbindungen**

Der CP kann mit den unterschiedlichen Telecontrol-Protokollen Verbindungen mit folgenden Partnern aufbauen:

TeleControl Basic

- Mit einem einfachen oder redundant aufgebauten Telecontrol-Server (TCSB)
- Zusätzlich Querkommunikation

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

Mengengerüst für Querkommunikation: Insgesamt max. 15, davon:

- Senden an Partner: Max. 3 (Parameter "Sendepuffer" aktiviert)
- Empfangen von Partnern: Max. 15 (Parameter "Sendepuffer" deaktiviert)

DNP3 / IEC 60870-5

- Der CP kann Verbindungen mit bis zu 4 Kommunikationspartnern aufbauen.

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

Die Kommunikation zwischen den Stationen wird über die Telecontrol-Verbindungen projektiert.

SINAUT ST7

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

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

- **Online-Verbindungen**

2 Ressourcen für Online-Verbindungen mit einer Engineering-Station (STEP 7)

- **HTTP**
TCP-Verbindungen für HTTP-Zugriffe: Max. 12
HTTP-Verbindungen können von Webbrowsern genutzt werden, um Daten des Webservers der CPU anzuzeigen.
- **PG- und HMI-Verbindungen (OP)**
Insgesamt maximal 16, davon:
 - Ressourcen für PG-Verbindungen: Max. 16
 - Ressourcen für HMI-Verbindungen: Max. 16

Nachrichten (E-Mail)

- Das Versenden von bis zu 10 Nachrichten (E-Mails) kann über den Nachrichteneditor projektiert werden.
Maximale Anzahl an Zeichen, die pro E-Mail übertragen werden kann: 256 ASCII-Zeichen inklusive eines evtl. mitgeschickten Werts
- Versenden von E-Mails über den Programmbaustein TMAIL_C

Telegrammspeicher (Sendepuffer)

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

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

Die maximale Größe des Sendepuffers beträgt:

- TeleControl Basic: 64000 Telegramme
- ST7: 32000 Telegramme
- DNP3 / IEC: 100000 Ereignisse

Anzahl der Datenpunkte für die Datenpunktprojektierung

Maximale Anzahl projektierbarer Datenpunkte pro CP:

- ST7 / DNP3 / IEC: 1500
- TeleControl Basic: 500

Security-Funktionen

Der CP unterstützt folgende Security-Funktionen:

- **Verschlüsselte E-Mails**

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

- SSL/TLS
- STARTTLS

- **Zertifikate**

Für die sichere Authentifizierung der Kommunikationspartner werden Zertifikate genutzt.

- **Gesicherte Telecontrol-Kommunikation**

Die Telecontrol-Protokolle bieten folgende Security-Funktionen:

- **TeleControl Basic**

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

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

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

- **ST7**

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

- MSC

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

- MSCsec

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

- **DNP3**

Der CP unterstützt die Verwendung von TLS-Verbindungen sowie die gesicherte Authentifizierung gemäß IEEE 1815.

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

- **IEC 60870-5-104**

Der CP unterstützt die Verwendung von TLS-Verbindungen sowie die gesicherte Authentifizierung gemäß IEC 60870-5-7.

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

Zur Kommunikation über SINEMA Remote Connect siehe Anhang.

1.5.5 TIM 1531 IRC

Verbindungs-Ressourcen

- **Telecontrol-Verbindungen**

Die Anzahl der Verbindungen bzw. Kommunikationspartner ist für die beiden Schnittstellentypen und jede einzelne Schnittstelle begrenzt.

Beachten Sie, dass redundante Verbindungswege einer Verbindung zwischen zwei Partnern bei jedem Partner zwei Verbindungsressourcen benötigen.

- Max. Anzahl an Verbindungen: 128

Die Aufteilung auf die 4 Schnittstellen ist beliebig (max. 128 pro Schnittstelle).

- **E-Mail**

Zur Laufzeit kann eine Verbindung zum Senden von E-Mails aufgebaut werden.

- **S7-Verbindungen**

- Max. 4 Verbindungs-Ressourcen für PG/OP-Verbindungen (siehe unten)

- **PG/OP-Verbindungen**

4 Verbindungs-Ressourcen für Verbindungen mit der Engineering-Station oder HMI-Geräten

(enthalten im Mengengerüst der S7-Verbindungen, siehe oben)

- **PG-Routing**

Max. 4 Verbindungen gleichzeitig

- **Online-Funktionen**

Siehe PG/OP-Verbindungen

- **HTTP/HTTPS**

Max. 2 Verbindungen pro Ethernet-Schnittstelle

Anzahl der Datenpunkte für die Datenpunktprojektierung

Die maximale Anzahl der projektierbaren Datenpunkte beträgt 3000.

Telegrammspeicher: Sendepuffer / SD-Karte

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

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

Die maximale Größe des Sendepuffers beträgt:

- ST7: 250 000 Telegramme
- DNP3/IEC: 100 000 Ereignisse

Details zur Funktion des Sendepuffers (Speichern und Senden von Ereignissen) sowie zu den Übertragungsmöglichkeiten von Daten finden Sie im Kapitel Prozessabbild, Übertragungsart, Ereignisklassen (Seite 130).

Zum Speichern von Ereignissen auf einer optionalen SD-Karte siehe Kapitel Grundeinstellungen (Seite 34).

Nachrichten: E-Mail

Bis zu 10 Nachrichten, welche die TIM als E-Mail versenden kann, können in STEP 7 projiziert werden.

- Anzahl Zeichen pro E-Mail

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

Security-Funktionen der Übertragungsprotokolle

Die für die Telecontrol-Kommunikation verwendbaren Übertragungsprotokolle unterstützen folgende Security-Funktionen:

ST7

- **MSC**

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

- **MSCsec**

MSCsec unterstützt die Authentifizierung der Kommunikationspartner und die Daten-Verschlüsselung mit Benutzername und Passwort.

Zusätzlich wird der gemeinsame automatisch generierte Schlüssel in einem projektierbaren Schlüsselaustausch-Intervall zwischen den Kommunikationspartnern erneuert.

DNP3

- Die TIM unterstützt die Verwendung von TLS-Verbindungen sowie die gesicherte Authentifizierung gemäß IEEE 1815.

IEC 60870-5-101 / 104

- Die TIM unterstützt die Verwendung folgender Funktionen:
 - IEC 60870-5-101 / 104
Gesicherte Authentifizierung gemäß IEC 60870-5-7
 - IEC 60870-5-104
TLS-Verbindungen

Weitere Security-Funktionen der TIM

Weiterhin unterstützt die TIM die folgenden Security-Funktionen:

- **NTP (secure)**
Zur sicheren Übertragung bei der Uhrzeitsynchronisation
- **STARTTLS / SSL/TLS**
Zur sicheren Übertragung von E-Mails
- **HTTPS**
Für den sicheren Zugriff auf den Webserver der TIM
- **SNMPv3**
Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen

Hinweis

Sicherheitskritische Anlagen - Empfehlung

Nutzen Sie folgende Möglichkeiten:

- Verwenden Sie in Anlagen mit hohen Sicherheitsanforderungen sichere Protokolle wie bspw. HTTPS oder SNMPv3.
 - Beim Anschluss an öffentliche Netze sollten Sie Security-Module mit Firewall einsetzen. Mit Security-Modulen können einzelne Geräte, Automatisierungszellen oder Netzsegmente eines Ethernet-Netzwerks abgesichert werden. Hierfür eignen sich beispielsweise folgende Security-Module: SCALANCE S, SCALANCE M800
-

Formatierung der SD-Karte

Die SD-Karte der TIM 1531 IRC muss folgende Formatierung aufweisen, um Projektierungsdaten speichern zu können.

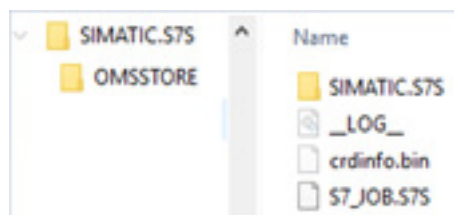


Bild 1-3 Formatierung der SD-Karte

Hinweise zur Formatierung der SD-Karte finden Sie im STEP 7 Informationssystem unter dem Suchbegriff "S7-1500-Memory Card formatieren".

Kommunikations-Mechanismen

2.1 Kommunikationsmöglichkeiten

Kommunikationswege

Bei der Telecontrol-Kommunikation sind folgende Wege bzw. Verbindungen möglich:

- **Verbindungen Master \leftrightarrow Station**
- **Redundante Verbindungen**

Wenn zwei Teilnehmer über unterschiedliche Netze erreichbar sind, können Sie zum Aufbau von Wegeredundanz maximal zwei Verbindungen zwischen den Teilnehmern anlegen.

- **Direkte Kommunikation (Station \leftrightarrow Station)**

Bei der direkten Kommunikation kommunizieren Stationen direkt miteinander, ohne dass die Telegramme von einer Zentrale vermittelt werden. Zwei Stationen können über einzelne Datenpunkte direkt miteinander kommunizieren.

Zur Projektierung siehe Kapitel Master-Funktion der Datenpunkte (Seite 127).

2.2 Adressierung

Für die Projektierung und die Inbetriebnahme des Kommunikationsmoduls sind folgende Informationen erforderlich:

Adressinformationen des Kommunikationsmoduls

Für die Adressierung müssen folgende Parameter für das Modul projektiert werden:

- ASDU-Adresse
 - Adresse des Informationsobjekts (Station) auf der Sicherungsschicht
 - Sie benötigen die ASDU-Adresse zur Identifikation des Masters und der Stationen im IEC-Netz.
- Indices der Datenpunkte (Datenpunktindex = Adresse des Informationsobjekts)
 - Zur Projektierung siehe Datenpunktindex (Seite 128).
- Adresse, je nach Netztyp und Modultyp:
 - IP-Adresse und Subnetzmaske; alternativ: IP-Adresse eines DHCP-Servers
 - Wenn Sie DNS einsetzen, dann muss ein DNS-Server (siehe unten) vorhanden und durch das Modul erreichbar sein.
 - Telefonnummer (für Wählnetz)
 - WAN-Adresse (für Standleitung)

- Listener-Port
 - Listener-Port der Station. Der Master benötigt die Portnummer für den Verbindungsaufbau.
 - Listener-Port eines Fremdgeräts mit der Funktion "Master"
- DNS-Server-Adresse(n)
 - Sie benötigen einen DNS-Server, wenn die Station Anfragen an Teilnehmer über deren FQDN stellt, beispielsweise NTP-Server.
 - Sie benötigen einen DNS-Server, wenn der Master Verbindungen mit den Stationen über deren FQDN aufbaut.

Eindeutigkeit der Adressen

Die Adressierung muss innerhalb eines Subnetzes und innerhalb des STEP 7-Projekts eindeutig sein.

Wenn Sie doppelte Teilnehmernummern / Stationsadressen in unterschiedlichen Subnetzen verwenden möchten, dann müssen Sie zwei STEP 7-Projekte anlegen.

Eindeutigkeit der ASDU-Adresse

Bei Modulen mit Telecontrol-Verbindungen, die über den Editor "Netzwerkdaten" projiziert sind, findet eine Konsistenzprüfung auf Eindeutigkeit der Adresse statt.

Bei CPs mit einer Firmware-Version $\leq V3.0$, deren Telecontrol-Verbindungen über die Parametergruppe "Partnerstationen" projiziert werden, ist eine Konsistenzprüfung auf Eindeutigkeit der Adresse nicht möglich. Achten Sie in diesen Fällen selbst auf Eindeutigkeit.

Adressinformationen des Masters

Folgende Informationen des Masters werden für die Projektierung des Moduls benötigt:

- ASDU-Adresse (Adresse des Informationsobjekts des Masters auf der Sicherungsschicht)
- Adresse des Masters, je nach Netztyp:
 - IP-Adresse / Subnetzmaske + Port-Nummer des Listener-Ports des Masters
 - oder
 - Durch DNS auflösbarer Name
(Sie benötigen die DNS-Server-Adresse; der DNS-Server muss durch das Modul erreichbar sein.)
 - Telefonnummer (für Wählnetz)
 - WAN-Adresse (für Standleitung)

Redundante IEC-Master

Beide Geräte eines redundanten Masters haben eine identische ASDU-Adresse.

Sie benötigen nur unterschiedliche IP-Adressen bzw. Host-Namen.

Konfigurationen mit Verbindungen über das Internet: VPN-Verbindungen

Bei Verbindungen, die über das Internet laufen, können dynamische IP-Adressen verwendet werden.

Um Kommunikation in beide Richtungen zu ermöglichen und damit die Daten geschützt übertragen werden, wird eine Verbindung mit VPN-Tunnel benötigt. Hierfür bieten sich Security-Baugruppen der Reihen SCALANCE S oder SCALANCE M an.

Berücksichtigen Sie bei der Projektierung folgende Punkte:

- Die Master-IP-Adresse projektieren Sie wie üblich.
- Bei der Projektierung der Schnittstelle des Moduls projektieren Sie die IP-Adresse des Routers.
- Die VPN-Projektierung mit SCALANCE S/SC/M nehmen Sie sowohl für die Stationsseite als auch für die Seite der Leitstelle in STEP 7 vor.

2.3 Verbindungsaufbau

Verbindungsaufbau

Der Master baut die Verbindung auf (Aufrufbetrieb / Polling). Dies gilt auch für Stationen mit Datenpunkten, bei denen die Option "Master-Funktion" aktiviert ist.

Wenn eine aufgebaute Verbindung unterbrochen wird, dann versucht ein Master-Modul, die Verbindung wieder aufzubauen.

Hinweis

Verbindungsunterbrechung durch Mobilfunknetzbetreiber

Beachten Sie bei der Nutzung von Mobilfunkdiensten, dass bestehende Verbindungen von Mobilfunk-Netzbetreibern zu Wartungszwecken unterbrochen werden können.

Verbindungsaufbau bei Open User Communication und PG/OP-Kommunikation

Bei der Open User Communication ist in einer S7-Station die CPU der Verbindungspartner.

Verbindungen werden aufgebaut, sobald die entsprechenden Programmbausteine in der CPU aufgerufen werden.

Dies gilt auch für den Fall, dass eine andere S7-Station Daten sendet. In diesem Fall werden von der Empfängerstation die entsprechenden Empfangsbausteine aufgerufen.

2.4 Quittierung

Quittier-Mechanismen beim Protokoll IEC 60870-5-104

Projektierung: Schnittstelle des Moduls > "Erweiterte Optionen" > Übertragungseinstellungen - IEC 60870-5"

Das Modul schickt mit jedem gesendeten Daten-Telegramm eine fortlaufende Sendefolgennummer mit. Das Daten-Telegramm bleibt zunächst im Sendepuffer des Moduls gespeichert.

Beim Empfang schickt der Master die Sendefolgennummer aus diesem oder (bei Empfang mehrerer Daten-Telegramme) dem letzten Daten-Telegramm als Quittung an das Modul zurück. Das Modul speichert die vom Master zurückgeschickte Sendefolgennummer als Empfangsfolgennummer und verwendet sie als Quittung.

Daten-Telegramme, deren Sendefolgennummer gleich oder kleiner der aktuellen Empfangsfolgennummer ist, werden als erfolgreich übertragen gewertet und aus dem Sendepuffer des Moduls gelöscht.

Parameter:

- **k: Differenz Sendefolgennummer N(S) zu Empfangsfolgennummer N(R)**

Maximale Anzahl an unquittierten Daten-Telegrammen (I-APDUs) als maximale Differenz zwischen Sendefolgennummer N(S) und Empfangsfolgennummer N(R).

Wenn k erreicht ist und t_1 noch nicht abgelaufen ist, sendet das Modul solange keine Daten-Telegramme, bis alle gesendeten Daten-Telegramme vom Master quittiert sind.

Wenn k erreicht ist und t_1 abgelaufen ist, wird die TCP-Verbindung abgebaut.

- **w: Max. Anzahl unquittierter Datentelegramme**

Maximale Anzahl an empfangenen Daten-Telegrammen (I-APDUs), nach der das älteste vom Master empfangene Daten-Telegramm quittiert werden muss.

Zur Projektierung siehe Kapitel Übertragungseinstellungen - IEC 60870-5 (Seite 56).

Empfehlungen der Spezifikation:

- w sollte nicht größer sein als $2/3 k$.
- Empfohlener Wert für k: 12
- Empfohlener Wert für w: 8

Projektierung

3.1 Kommunikationsarten

"Kommunikationsarten"

In dieser Parametergruppe aktivieren Sie die Kommunikationsfähigkeit des Moduls.

Abhängig vom Modultyp können Sie das Telecontrol-Protokoll und weitere Kommunikationsarten festlegen.

- **Telecontrol-Kommunikation aktivieren**

Aktiviert die Telecontrol-Kommunikation mit den Kommunikationspartnern.

- **Protokolltyp**

- ST7
- DNP3
- IEC 60870-5

- **Online-Funktionen aktivieren**

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

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

S7-Routing wird von folgenden Modulen unterstützt:

- CP 1243-1, CP 124x-7, CP 1243-8
Ab CP-Firmware V2.1 mit CPU \geq V4.2
- CP 1542SP-1 IRC
Ab CP-Firmware V1.0 mit CPU \geq V2.0
- TIM 1531 IRC

Beachten Sie:

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

- **S7-Kommunikation aktivieren**

Gibt im Modul die Funktionen der S7-Kommunikation mit der Stations-CPU und das S7-Routing frei.

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

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

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

Projektierbar bei:

- CP 1243-1
- CP 1243-7 LTE
- CP 1243-8 IRC
- CP 1542SP-1 IRC

Zu weiteren Details siehe Anhang SINEMA Remote Connect (CP) (Seite 187).

3.2 Grundeinstellungen

IEC-Basiseinstellungen

Nicht alle Parameter werden bei jedem Modultyp angezeigt.

- **Listener-Port**

Eigener Listener-Port des Moduls. Der Master benötigt die Portnummer für den Verbindungsaufbau.

Die Portnummer gilt für alle Schnittstellen des Kommunikationsmoduls.

Wertebereich: 1024...65535

Vorbelegung: 2404

- **Telegrammspeichergöße**

Nur bei TIM 1531 IRC

Hier stellen Sie die Größe des Telegrammspeichers für Ereignisse (Sendepuffer) ein.

Die Kapazität des Telegrammspeichers teilt sich zu gleichen Teilen auf alle Kommunikationspartner auf. Zur Größe des Telegrammspeichers siehe "Leistungsdaten und Mengengerüst".

Details zur Funktion des Sendepuffers (Speichern und Senden von Ereignissen) sowie zu den Übertragungsmöglichkeiten von Daten finden Sie im Kapitel Prozessabbild, Übertragungsart, Ereignisklassen (Seite 130).

- **Max. Befehls-Lebensdauer**

Nur bei TIM 1531 IRC

Maximales Alter empfangener Befehle vom Typ Single/Double command with time tag (<58>/<59>)

Wenn der Zeitstempel zum Zeitpunkt des Empfangs älter ist als der hier projektierte Wert, wird der Befehl ohne Rückmeldung verworfen. Der Parameter wird von Stationenen und Knotenstationen ausgewertet.

Wertebereich: 1...65

Vorbelegung: 20

Private ASDUs

Nur bei TIM 1531 IRC

Über den projektierbaren Wert legen Sie die TYPE IDENTIFICATION des jeweiligen ASDU-Typs fest. Der 'Private Bereich' von 136...254 für die Typ-Identifikation ist reserviert für anwenderspezifische Anwendungen.

Die TIM prüft bei empfangenen privaten ASDUs die Typ-Identifikation und wertet den jeweils projektierten Wert aus.

Bei Projektierung von 0 (Null) wertet die TIM keine Typ-Identifikation aus.

- **ASDU-Typ für PG-Routing**

Typ-Identifikation für ASDUs zur Übertragung von S7-Telegrammen (PG-Routing)

Wertebereich: 136...254

Vorbelegung: 0

- **ASDU-Typ für Status-Distribution**

Typ-Identifikation für ASDUs zur Übertragung des Wegestatus der Verbindung

Wertebereich: 136...254

Vorbelegung: 0

- **ASDU-Typ für Verbindungstrennung**

Typ-Identifikation für ASDUs zur Ankündigung des Verbindungsabbaus bei temporären Verbindungen

Temporäre Verbindungen werden von der RTU3000C aufgebaut.

Wertebereich: 136...254

Vorbelegung: 0

Secure Communication-Optionen

Gültigkeit: TIM 1531 IRC, CP 1542SP-1 IRC

- **Secure Listener-Port**

Eigener Listener-Port für TLS-Kommunikation.

Die Portnummer gilt für alle Schnittstellen des Kommunikationsmoduls.

Wertebereich: 1024...65535

Vorbelegung: 19998

Remanentes Speichern von Ereignissen

Nur bei TIM 1531 IRC

Wenn Sie eine optionale SD-Karte in der TIM verwenden, stellen Sie in dieser Parametergruppe die Bedingungen für das Speichern der Werte von Telegrammen ein, deren Datenpunkte als Ereignis projektiert sind.

Das Verhalten stellen Sie über folgende Parameter ein:

- **Remanentes Speichern ermöglichen**

Aktiviert bei Verbindungsstörungen das remanente Speichern von Ereignissen auf der SD-Karte.

- **Anzahl Ereignisse vor Speichern**

Das Speichern der Ereignisse auf der SD-Karte setzt ein, wenn die hier projektierte Anzahl an Ereignissen im Sendepuffer erreicht ist.

- **Unterbrechungszeit vor Speichern**

Das Speichern der Ereignisse auf der SD-Karte setzt ein, wenn die hier projektierte Zeit der Verbindungsunterbrechung erreicht ist.

- **Max. Anzahl an Ereignissen in Archivdatei**

Maximale Anzahl an Ereignissen in der gespeicherten Archivdatei

Bei Überschreitung der Anzahl werden die ältesten Ereignisse überschrieben.

Zur maximale Anzahl an speicherbaren Ereignissen siehe Kapitel Funktionen, Leistungsdaten und Mengengerüst (Seite 16).

IP-Routing

Nur bei TIM 1531 IRC

Hinweis

Die Funktion ist nicht für große Datenmengen vorgesehen.

Beschränken Sie das Routing über die TIM auf ca. 1 Mbit/s, um den Produktivbetrieb der TIM nicht zu beeinträchtigen.

IP-Routing

- **IP-Routing ermöglichen**

Gibt das IP-Routing über die Schnittstellen des Moduls frei.

- **Routing-Weg**

Legt die Wege für das IP-Routing fest:

- Lokal: IP-Routing nur zwischen den Ethernet-Schnittstellen des Moduls
- Über Subnetze: IP-Routing über max. 10 projektierbare Router, die über die Schnittstellen des Moduls erreichbar sind.

Router-Adressen

- **Ethernet-Schnittstelle**

Ethernet-Schnittstelle des Moduls, über die IP-Routing projiziert werden soll. Die IP-Adressen der für IP-Routing verwendeten Schnittstellen müssen fest projiziert sein.

Eine Schnittstelle kann mehrfach für unterschiedliche Routen ausgewählt werden.

Hinweis

Konsistenz der Adressparameter

STEP 7 führt keine Prüfung der Konsistenz zwischen manuell projizierten Adressen und den Parametern der Ethernet-Schnittstellen des Moduls durch.

Achten Sie auf Konsistenz mit den Adressparametern der jeweiligen Schnittstelle.

- **Adresstyp**

Auswahl der IP-Version der nachfolgend projizierten Adressparameter (IPv4 / IPv6)

Bei Verwendung von IPv6-Adressen müssen Sie IPv6 für die jeweilige Schnittstelle freigeben.

- **Netzwerkadresse**

Netzwerkadresse des Routing-Ziels (IP-Adresse * Subnetzmaske)

- **Subnetzmaske / Präfix**

Subnetzmaske (IPv4) bzw. Präfix (IPv6) des Routing-Ziels

- **Router-Adresse**

3.3 Uhrzeitsynchronisation

Uhrzeitsynchronisation und Security

Wenn Sie bei Modulen mit Security die Security-Funktionen aktivieren, finden Sie die Parametergruppe unter "Security".

Bei aktivierten Security-Funktionen müssen Sie die Uhrzeit des Kommunikationsmoduls regelmäßig synchronisieren.

Grundsätzliches zur Uhrzeitsynchronisation

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

Das Kommunikationsmodul kann die Uhrzeit von extern beziehen (zu Verfahren siehe unten) und die Uhrzeit an die Station oder die angeschlossenen WAN-Netze weiterleiten.

Bei Verwendung einer externen Uhrzeitquelle kann die angeschlossene S7-Station die aktuelle Uhrzeit sowohl über die CPU als auch über ein Kommunikationsmodul (TIM, CP) beziehen.

Hinweis

Empfehlungen

- **Uhrzeitsynchronisation nur durch 1 Modul**

Lassen Sie die Uhrzeit der Station von einer externen Uhrzeitquelle nur durch ein einziges Modul der Station synchronisieren, um innerhalb der Station eine konsistente Uhrzeit vorzuhalten.

Wenn die CPU die Uhrzeit von einem Kommunikationsmodul übernimmt, dann deaktivieren Sie die Uhrzeitsynchronisation der CPU.

Wenn Sie die Uhrzeit sowohl beim Kommunikationsmodul als auch bei der CPU über NTP synchronisieren lassen, dann verwenden Sie möglichst dieselben NTP-Server, um innerhalb der Station eine konsistente Uhrzeit vorzuhalten.

- **Längere Synchronisationszyklen bei instabilen Netzen**

Wenn ein Netz öfters Verbindungsstörungen aufweisen, können Sie dessen Synchronisationszyklus vergrößern.

Damit vermeiden Sie, dass nach Verstreichen des vom Slave erwarteten Synchronisationszeitpunkts die Telegramme als "ungültig" markiert und verworfen werden.

Uhrzeit-Konzept

Treffen Sie vor der Projektierung der Uhrzeitsynchronisation folgende Festlegungen:

- Legen Sie die Uhrzeit-Quelle im Netz fest.
- Legen Sie den Uhrzeit-Master im Netz fest.
- Legen Sie das oder die Netze fest, über welche die Uhrzeit vom Uhrzeit-Master an die Uhrzeit-Slaves weitergeleitet werden soll.

Synchronisationsverfahren der Kommunikationsmodule

Die Module unterstützen folgenden Verfahren und Funktionen (Empfang / Weiterleitung) der Uhrzeitsynchronisation:

- **TIM 1531 IRC**
 - NTP
 - Von WAN
 - An lokale Station
 - An WAN

- **CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC**

Der CP kann für das angeschlossene Subnetz nur Uhrzeit-Slave sein.

- Uhrzeit vom Partner
- NTP
- Uhrzeit von CPU
- Uhrzeitweiterleitung an die CPU

- **CP 1542SP-1 IRC**

- NTP
- Von WAN

CPs unterstützen keine Weiterleitung der Uhrzeit an angeschlossene Subnetze.

Verfahren zum Empfangen der Uhrzeit

- **NTP / NTP (secure)**

Network Time Protocol

Uhrzeitsynchronisation nur über Ethernet

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

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

Empfehlung bei NTP:

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

Hinweis zur TIM 1531 IRC:

Bei Verwendung eines FQDN als Adresse des NTP-Servers können bis zu 240 Zeichen eingegeben werden.

- **Von WAN**

Die TIM übernimmt die Uhrzeit von einem oder mehreren Teilnehmern im angeschlossenen Netz.

Uhrzeit-Master können sein:

- Eine synchronisierte CPU
- Teilnehmer mit Uhrzeitempfänger
- Ein am Ethernet-Netz angeschlossener Zentrale-PC

- **Uhrzeit vom Partner (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC / CP 1542SP-1 IRC)**

Der CP übernimmt die Uhrzeit vom Kommunikationspartner in der Zentrale.

- **Uhrzeit von der CPU (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC)**

Die CPU 1200 ab V4.2 synchronisiert alle CMs/CPs der Station mit einem Synchronisationszyklus von 10 Sekunden.

Parameter der CPU:

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

- **Manuelles Setzen der Uhrzeit über das WBM (TIM 1531 IRC)**

Wenn Sie eine Uhrzeitquelle für die TIM projektiert haben, können Sie die Uhrzeit auch über das WBM setzen, siehe Kapitel Systemzeit (Seite 198).

Uhrzeit empfangen > Zeitzonen-Unterstützung

In dieser Parametergruppe finden Sie folgende Parameter:

- Zeitunterschied aktivieren

Die Option ist vorgesehen für Kommunikationsmodule vom Typ "Station", welche die Uhrzeit vom Master empfangen und ihre lokale Zeit an die Station (CPU mit UTC-Zeit) weiterleiten.

Bei aktivierter Option passt das Kommunikationsmodul seine lokale Uhrzeit, die es an CPU weiterleitet, an die Uhrzeit der CPU (UTC) an.

Das Kommunikationsmodul behält seine lokale Zeit, auch wenn es wiederum von der CPU synchronisiert wird.

- Zeitunterschied:

Wählen Sie die Zeitspanne (Minuten) aus, um den Unterschied zwischen der lokalen Zeit des Kommunikationsmoduls und der CPU-Zeit (UTC) auszugleichen.

Beispiel: Wenn das Kommunikationsmodul eine lokale Zeit von "UTC" hat und die CPU eine Zeit von "UTC - 1" hat, dann wählen Sie in der Klappliste "- 60" aus.

Uhrzeitweiterleitung durch einen CP 1200

- **Uhrzeitweiterleitung an die CPU (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC)**

Voraussetzung: CP-Firmware \geq V3.0 und CPU-Firmware \geq V4.2

Wenn beide Module in einer Station die genannte Firmware-Versionen aufweisen, wird die Uhrzeit des CP automatisch an die CPU weitergeleitet. Da die CPU automatisch die CP-Zeit übernimmt, benötigen Sie die Weiterleitungsoption über die PLC-Variable, wie bei CP-Firmware $<$ V3, nicht mehr.

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

Uhrzeitweiterleitung durch den CP 1542SP-1 IRC

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

Wenn Sie die Uhrzeit der Station über die CPU synchronisieren lassen möchten, dann deaktivieren Sie beim CP die Uhrzeitsynchronisation.

CPs: Uhrzeitweiterleitung durch PLC-Variable

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

Siehe hierzu Parametergruppe "Kommunikation mit der CPU".

Uhrzeitweiterleitung durch die TIM

Die TIM kann ihre Uhrzeit folgendermaßen weiterleiten:

- **An angeschlossene Netze**

Projektierung über "Uhrzeitsynchronisation" > "Uhrzeit senden" bzw. "Uhrzeit empfangen"

Die Vorgehensweise der Projektierung unterscheidet sich bei Ethernet und klassischen WAN-Netzen, siehe unten.

- **An die zugeordnete CPU**

- Projektierung über "Uhrzeitsynchronisation" > "Uhrzeit senden"

- Projektierung über "Kommunikation mit der CPU" > "Uhrzeit an CPU"

Bei dieser Methode wird der CPU die Uhrzeit über eine PLC-Variable zur Verfügung gestellt.

Entscheiden Sie sich bei der Weiterleitung an die CPU für eine der beiden Methoden und deaktivieren Sie die jeweils andere.

Uhrzeit-Projektierung bei der TIM 1531 IRC

Parametergruppen für die Uhrzeitsynchronisation

Für die Ethernet-basierte Uhrzeit-Synchronisation nehmen Sie die Einstellungen in den Parametergruppen "Uhrzeit empfangen" und "Uhrzeit senden" vor.

Bei der Uhrzeit-Synchronisation über klassische WAN-Netze übernehmen diese beiden Parametergruppen der seriellen Schnittstellen der TIM die Werte, die Sie direkt am angeschlossenen klassischen WAN-Netz projektiert haben (siehe unten).

- **Uhrzeit empfangen**

Hier legen Sie fest, über welches der angeschlossenen Netze die TIM die Uhrzeit empfangen soll. Diese Parametergruppe projektieren Sie bei TIM-Baugruppen mit dem Netznotentyp "Knotenstation" und "Station".

Hier projektieren Sie auch die NTP-Server, wenn die TIM direkt über NTP synchronisiert werden soll. Dies wird in der Regel nur eine TIM sein, die als Uhrzeit-Master im Netz fungiert.

Außerdem können Sie festlegen, über welche Schnittstelle der TIM die Uhrzeit über WAN empfangen wird und Einstellungen zum Synchronisationszyklus vornehmen.

- Sommerzeitumstellung aktivieren

Aktiviert die automatische Anpassung an Sommer- und Winterzeit (Sommerzeitschaltung).

Vom Master empfangene Uhrzeittelegramme mit Sommerzeit übernimmt das Modul, ohne die Uhrzeit zu korrigieren.

Knotenstationen reichen Uhrzeittelegramme mit Sommerzeit vom Master an die Stationen ohne Korrektur weiter.

- **Uhrzeit senden**

Hier legen Sie fest, auf welche Netze die TIM die Uhrzeit weiterleiten soll.

Diese Parametergruppe projektieren Sie bei TIM-Baugruppen mit dem Netzknotentyp "Zentrale-Station", das heißt bei derjenigen TIM, die als Uhrzeit-Master im Netz fungiert.

Projektierung an der Ethernet-Schnittstelle der TIM 1531 IRC

Uhrzeit-Master

1. Projektieren Sie in der Parametergruppe "Uhrzeit empfangen" derjenigen TIM, welche Uhrzeit-Master sein soll, die Uhrzeit-Quelle über eine der folgenden Optionen:
 - Von NTP-Server
 - Von lokaler Station
(Übernahme der Uhrzeit von der zugeordneten CPU)
 - Von WAN
(Übernahme der Uhrzeit aus einem Netz über einen bestimmten Verbindungspartner)
2. Projektieren Sie diejenige Schnittstelle der TIM, über welche die Uhrzeit-Telegramme weitergeleitet werden sollen, in der Parametergruppe "WAN-Einstellungen" als Netzknotentyp "Zentrale-Station".
3. Aktivieren Sie in der Parametergruppe "Uhrzeit senden" für die Schnittstelle aus Schritt 2 die Option "Uhrzeit an WAN senden über ... (Schnittstelle)".
Über die Schnittstelle werden die Uhrzeittelegramme in das angeschlossene Netz weitergeleitet.
Bei einer Ethernet-Schnittstelle mit der Einstellung "Netztyp" = "Neutral" ist die Aktivierung der Funktion wirkungslos, da es beim S7-Protokoll keine Uhrzeit-Master und Slaves gibt.
4. Aktivieren Sie bei Bedarf in der Parametergruppe "Uhrzeit senden" die Option "An lokale Station", wenn auch die zugeordnete CPU synchronisiert werden soll.

Uhrzeit-Slaves

1. Projektieren Sie die Schnittstellen der übrigen TIM-Baugruppen, welche Uhrzeit-Slave sein sollen, in der Parametergruppe "WAN-Einstellungen" als Netzknotentyp "Knotenstation" bzw. "Station".

Die Funktion wird für die Ethernet-Schnittstelle mit dem MSC-Protokoll und für die serielle Schnittstelle unterstützt, nicht für eine Ethernet-Schnittstelle mit der Einstellung "Netztyp" = "Neutral".

2. Vernetzen Sie die Schnittstellen der beteiligten TIM-Baugruppen untereinander und mit der Schnittstelle des Uhrzeit-Masters.
3. Stellen Sie bei den Stationen die Parameter der Uhrzeitsynchronisation in der Parametergruppe "Uhrzeit empfangen" ein.
4. Aktivieren Sie bei Bedarf in der Parametergruppe "Uhrzeit senden" die Option "An lokale Station", wenn auch die zugeordnete CPU synchronisiert werden soll.
5. Wenn die Uhrzeit von einer bestimmten Schnittstelle der TIM an das WAN-Netz weitergeleitet werden soll, aktivieren Sie diese in der Parametergruppe "Uhrzeit senden" > "An WAN". Für jede aktivierte Schnittstelle können Sie Einstellungen zum Synchronisationszyklus vornehmen.

Projektierung der Synchronisation über klassische WAN-Netze

Für die klassischen Netze projektieren Sie die "Uhrzeitsynchronisation" in der gleichnamigen Parametergruppe.

Die Einstellungen zur Synchronisation werden anschließend von allen seriellen Schnittstellen der angeschlossenen TIM-Baugruppen übernommen.

Die Senderichtung der Uhrzeittelegramme wird automatisch aus dem Netzknotentyp der angeschlossenen Schnittstellen abgeleitet:
Zentrale-Station ⇒ Knotenstation ⇒ Station

TIM-Baugruppen (Uhrzeit-Master und Slaves)

1. Klassisches WAN-Netz

Für die klassischen Netze wird die "Uhrzeitsynchronisation" in der gleichnamigen Parametergruppe aktiviert. Hier legen Sie auch den Synchronisationszyklus fest.

Die Einstellungen zur Synchronisation werden anschließend von allen angeschlossenen TIM-Baugruppen übernommen.

Die Senderichtung der Uhrzeittelegramme wird automatisch aus dem Netzknotentyp der angeschlossenen Schnittstellen abgeleitet:
Zentrale-Station ⇒ Knotenstation ⇒ Station

2. Projektieren Sie in der Parametergruppe "Uhrzeit empfangen" derjenigen TIM, welche Uhrzeit-Master sein soll, die Uhrzeit-Quelle über eine der folgenden Optionen:
 - Von NTP-Server
 - Von lokaler Station
(Übernahme der Uhrzeit von der zugeordneten CPU)
 - Von WAN
(Übernahme der Uhrzeit aus einem Netz)
3. Projektieren Sie die Schnittstelle der Master-TIM als Netzknotentyp "Zentrale-Station".
4. Projektieren Sie die Schnittstellen der übrigen TIM-Baugruppen (Uhrzeit-Slaves) als Netzknotentyp "Knotenstation" bzw. "Station".
5. Aktivieren Sie bei Bedarf in der Parametergruppe "Uhrzeit senden" der Stationen die Option "Uhrzeit an lokale Station senden", wenn auch die zugeordnete CPU synchronisiert werden soll.
6. Wenn die Uhrzeit von einer bestimmten Schnittstelle der TIM an das WAN-Netz weitergeleitet werden soll, aktivieren Sie diese in der Parametergruppe "Uhrzeit senden" > "An WAN". Für jede aktivierte Schnittstelle können Sie Einstellungen zum Synchronisationszyklus vornehmen.

WAN-Netz

1. Aktivieren Sie in der Parametergruppe "Uhrzeitsynchronisation" des Netzes die Option "Uhrzeitsynchronisation für WAN aktivieren".
2. Projektieren Sie den gewünschten Synchronisationszyklus.
3. Vernetzen Sie die Schnittstellen aller beteiligten TIM-Baugruppen mit dem WAN-Netz.
Die am WAN-Netz projektierten Einstellungen werden bei den angeschlossenen TIM-Baugruppen in folgenden Parametergruppen übernommen:
 - Beim Uhrzeit-Master (Zentrale-Station): Parametergruppe "Uhrzeit senden"
 - Bei den Uhrzeit-Slaves (Knotenstationen / Station): Parametergruppe "Uhrzeit empfangen"

Optional: Uhrzeit-Partner festlegen (TIM 1531 IRC)

Wenn mehrere Uhrzeit-Master am Netz angeschlossen sind, können Sie bei der TIM 1531 IRT einen spezifischen Teilnehmer als Uhrzeit-Master festlegen.

1. Projektieren Sie die Telecontrol-Verbindungen über die seriellen Schnittstellen der beiden Geräte.
2. Nach dem Anlegen der Telecontrol-Verbindungen können Sie beim Uhrzeit-Slave den über die Verbindung projektierten Partner auswählen.
Auswahl am Parameter "Uhrzeit empfangen > Uhrzeit vom Partner beziehen" der seriellen Schnittstelle

In der Einstellung "Kein Verbindungspartner" akzeptiert die TIM die Uhrzeit von allen angeschlossenen Uhrzeit-Mastern.

3.4 Projektierung von Schnittstellen, Netzen und Netzknoten

3.4.1 WAN-Einstellungen der Schnittstellen

WAN-Einstellungen

Die folgenden Parameter bestimmen die Eigenschaften der Schnittstellen und der angeschlossenen WAN-Netze.

Projektieren Sie zuerst die jeweilige Schnittstelle des Moduls. Das anschließend angeschlossene WAN-Netz übernimmt die wichtigsten Einstellungen.

- **WAN-Typ**

Auswahl des WAN-Typs der Schnittstelle:

- IP-basiert
Standardeinstellung der Ethernet-Schnittstelle
- Klassisches WAN
Standardeinstellung einer seriellen Schnittstelle

- **Netztyp**

Für IP-basiertes WAN:

- IEC 60870-5
- Neutral

Für klassisches WAN:

- Standleitung
- Wählnetz

Beachten Sie, dass klassische WAN-Netze nur für TIM-Baugruppen unterstützt werden.

- **Netzknotentyp**

Bestimmt den Netzknotentyp der Schnittstelle:

- Zentrale-Station
- Knotenstation

Bei Modulen, die als Knotenstation fungieren, werden die Schnittstelle folgendermaßen projektiert:

- Schnittstelle in Richtung Zentrale: "Knotenstation"
- Schnittstelle in Richtung unterlagertes Netz: "Zentrale"

- Station

Eine Abbildung finden Sie im Kapitel Vernetzen der Schnittstellen (Seite 46).

- **Modemtyp**

Der Modemtyp für den Anschluss an die serielle Schnittstelle muss für den Netztyp "Wählnetz" projektiert werden, bei den klassischen TIM-Baugruppen auch für den Netztyp "Standleitung".

Die Einträge haben folgende Bedeutung:

- MD2
Standleitungsmodem (Netztyp "Standleitung")
- MD3
Modem für analoge Wählnetze (Netztyp "Wählnetz")
- MD4
ISDN-Modem (Netztyp "Wählnetz")
- MD720
Das GSM-Modem MD720 wird nicht unterstützt, da es das Telegrammformat FT2 verwendet.
- Fremdmodem
Beliebiges kompatibles Modem für die Netztypen "Standleitung" oder "Wählnetz" (analog / ISDN / GSM)

3.4.2 Vernetzen der Schnittstellen

Schnittstellen der Module

Die Anordnung der Schnittstellen der Module im STEP 7-Gerätesymbol (Netzansicht) entspricht weitgehend dem Aufbau des jeweiligen Geräts.

Die Schnittstellen einer TIM 1531 IRC beispielsweise haben folgende Anordnung:

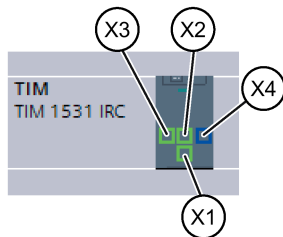


Bild 3-1 Gerätesymbol der TIM mit Schnittstellen-Nummern

Vernetzen von Schnittstellen

Um eine Schnittstelle zu vernetzen, haben Sie je nach Ausgangssituation unterschiedliche Möglichkeiten:

- Subnetz erstellen
- Zwei Zielgeräte über ein neues Subnetz verbinden

- Geräte mit bestehendem Subnetz verbinden
- Vorhandenes Subnetz aus Liste "Subnetz" auswählen

Die Beschreibung der einzelnen Methoden finden Sie im STEP 7-Informationssystem.

Vernetzen von WAN-Schnittstellen

Empfehlung für die Vernetzung:

Für die Vernetzung der Schnittstellen mit einem WAN-Netz empfiehlt sich folgende Vorgehensweise:

1. Vernetzen Sie die WAN-Netze in der Netzsicht von STEP 7.

In der grafischen Netzsicht behalten Sie die Übersicht über die Subnetze der gesamten Anlage im Projekt.

2. Projektieren Sie zuerst die Schnittstellen-Parameter, die im Kapitel WAN-Einstellungen der Schnittstellen (Seite 45) beschrieben sind:

- WAN-Typ
- Netztyp
- Netzknontentyp
- Modemtyp

3. Selektieren Sie die betreffende Schnittstelle, um ein neues WAN-Netz anzulegen. Alternativ:

In der Parametergruppe "Schnittstelle vernetzen mit" der Schnittstelle:

- Über die Schaltfläche "Neues Subnetz hinzufügen"

An der Schnittstelle im Gerätesymbol des Moduls:

- Über das Kontextmenü "Subnetz erstellen"
- Grafisch durch Ziehen (Mauszeiger gedrückt halten) auf das Schnittstellensymbol des Kommunikationspartners

Ein neues WAN-Netz wird angelegt, welches den Netztyp von der angeschlossenen Schnittstelle übernimmt.

Netzdarstellung eines klassischen WAN

Ein klassisches WAN-Netz wird blau dargestellt.

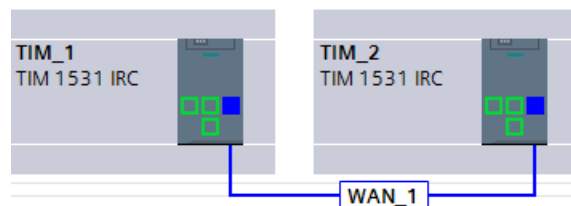


Bild 3-2 TIM-Baugruppen, serielle Schnittstellen über klassisches WAN vernetzt.

Netz mit Knotenstation

In der folgenden Abbildung ist die mittlere TIM eine Knotenstation. Der Parameter "Netzknotentyp" der Schnittstellen ist folgendermaßen projektiert:

- Schnittstelle in Richtung Zentrale: "Knotenstation"
- Schnittstelle in Richtung unterlagertes Netz: "Zentrale-Station"

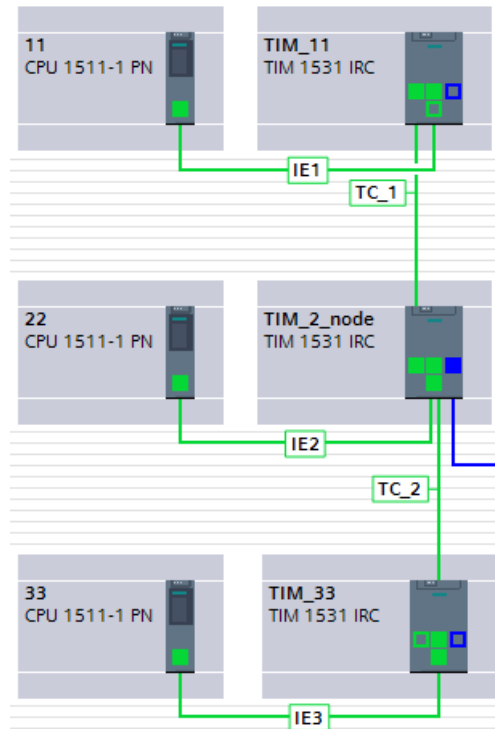


Bild 3-3 Netz mit Zentrale-Station (oben), Knotenstation (Mitte) und Station (unten)

3.5 Ethernet-Schnittstelle

3.5.1 Ethernet-Adressen

Die Ethernet-Schnittstelle

- **Ethernet-CPs**

Die Telecontrol-Kommunikation der Ethernet-CPs läuft über die Ethernet-Schnittstelle. Projektieren Sie die erforderlichen Parameter.

- **Mobilfunk-CPs**

Mobilfunk-CPs haben keine physische Ethernet-Schnittstelle.

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

Bei Nutzung von Security-Funktionen müssen Sie die Schnittstelle vernetzen.

Ethernet-Adressen

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

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

Beachten Sie:

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

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

IPv6-Protokoll verwenden

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

Optionen für Mobilfunk-CPs:

- **Dynamische IP-Adresse**

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

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

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

Ethernet-Schnittstelle > Port [Xn P1]

Informationen zur Projektierung finden Sie im STEP 7-Informationssystem.

Zur Projektierung der WAN-Einstellungen siehe Kapitel WAN-Einstellungen der Schnittstellen (Seite 45).

3.5.2 Erweiterte Optionen

3.5.2.1 TCP-Verbindungsüberwachung

Ethernet-Schnittstelle > Erweiterte Optionen > TCP-Verbindungsüberwachung

Die Einstellungen der beiden Parameter an der Ethernet-Schnittstelle gelten übergeordnet für TCP-Verbindungen über diese Schnittstelle.

Sie können die Parameter in den Eigenschaften der Telecontrol-Verbindungen für jeden Verbindungsabschnitt anpassen.

- **TCP-Verbindungs-Überwachungszeit**

Funktion: Wenn innerhalb der TCP-Verbindungs-Überwachungszeit kein Datenverkehr stattfindet, sendet das Modul ein Keep-alive-Telegramm an den Kommunikationspartner.

Bei 0 (Null) ist die Funktion deaktiviert.

Voreinstellung: 180 s

Zulässiger Bereich

- TIM 1531 IRC
1...65535 s
- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
- CP 1542SP-1 IRC
0...32767 s

- **TCP-Keep-alive-Überwachungszeit**

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

Bei 0 (Null) ist die Funktion deaktiviert.

Voreinstellung: 10 s

Zulässiger Bereich

- TIM 1531 IRC
1...65535 s
- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
- CP 1542SP-1 IRC
0...32767 s

3.5.2.2 Übertragungseinstellungen

Die spezifischen Parameter des Telecontrol-Protokolls finden Sie im Kapitel IEC-Parameter der Schnittstellen (Seite 56).

3.5.3 Zugriff auf den Webserver

3.5.3.1 CP

Zugang zum Webserver der CPU

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

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

Informationen zum Webserver der S7-1200 finden Sie im Handbuch /7/ (Seite 227).

Informationen zum Webserver der ET 200SP finden Sie im Handbuch /8/ (Seite 227).

3.5.3.2 TIM 1531 IRC

Zugriff auf den Webserver

Sie können den Zugriff auf den Webserver der TIM über HTTP/HTTPS für jede einzelne Ethernet-Schnittstelle aktivieren.

In der Voreinstellung ist der Zugriff deaktiviert. Beachten Sie hierzu die Ausführungen im Kapitel Security-Empfehlungen (Seite 215).

Die Aktivierung des Webserver und weitere Einstellungen nehmen Sie in der Parametergruppe "Webserver" vor, siehe Kapitel Webserver (TIM 1531 IRC) (Seite 63). Dort können Sie den Zugriff auch aktivieren bzw. deaktivieren.

Für den Zugriff auf den Webserver müssen Sie sowohl den Zugriff bei der Ethernet-Schnittstelle freigeben ("Zugriff auf den Webserver") und den Webserver selbst aktivieren (Parametergruppe "Webserver").

3.6 Serielle Schnittstelle

3.6.1 WAN-Parameter

Über die Klappliste "Subnetz" vernetzen Sie die Schnittstelle.

WAN-Adresse

Hier legen Sie die Länge des optionalen Adressfeldes (LADDR) für die Link-Layer-Adresse fest.

- **Adressformat (2-Byte-Adresse)**

Beachten Sie: Das Adressformat muss für alle Stationen des IEC-Netzes (60870-5-101) gleich sein.

- Bei deaktivierter Option wird die ASDU-Adresse in 1 Byte gespeichert (niederwertiges Byte des Worts).

Der Wertebereich für die Link-Layer-Adresse liegt bei 1...255.

- Bei aktivierter Option wird der Adressbereich der Link-Layer-Adresse (siehe unten) auf 1...65535 erhöht.

- **WAN-Adresse**

Optionale Link-Layer-Adresse der Schnittstelle

Standard-Wertebereich: 1...255

Erhöhter Wertebereich bei aktiviertem Parameter "2-Byte-Adresse": 1...65535

3.6.2 Erweiterte Optionen

3.6.2.1 Standleitung

Einstellungen Standleitung

Einstellungen serielle Schnittstelle

- **Schnittstellenstandard**

Standard der seriellen Schnittstelle: RS232 / RS485

Wählen Sie den folgenden Wert:

- RS232

Bei Anschluss eines Modems mit RS-232-Schnittstelle an die Schnittstelle der TIM

- RS485

Bei Anschluss eines Modems mit RS-485-Schnittstelle

Bei parallelem Anschluss mehrerer Modems an die Schnittstelle der TIM (sternförmiges Netz)

- **RS-485-Terminierung**

Aktivieren Sie die Option bei Zuschaltung eines Abschlusswiderstandes für den RS-485-Bus bei Anschluss eines sternförmigen Netzes.

Zeitoptionen

- **Sendeverzögerungszeit (nach RTS)**

Die Sendeverzögerungszeit (nach RTS) (ms) wird nach dem Setzen von RTS gestartet.

- Wert = 0

Das Modul wartet mit dem Senden von Daten solange, bis sie das CTS-Signal (Sendebereitschaft) vom Modem empfängt.

- Wert > 0

Das Modul wartet nicht auf das CTS-Signal des Modems, sondern sendet, sobald die projektierte Zeit abgelaufen ist.

Voreinstellung: 0. Zulässiger Bereich: 0...65535 ms

- **Sendeverzögerungszeit (nach CTS)**

Die Verzögerungszeit (ms) wird verwendet, wenn vom Modem das CTS-Signal (Sendebereitschaft) empfangen wird und wenn für die "Sendeverzögerungszeit (nach RTS)" 0 (Null) projektiert wurde.

- Wert = 0

Es wird nicht auf das CTS-Signal des Modems gewartet.

- Wert > 0

Sobald das CTS-Signal vom Modem empfangen wird, wird die Sendeverzögerungszeit gestartet. Nach Ablauf der Zeit wird mit dem Senden begonnen.

Voreinstellung: 0. Zulässiger Bereich: 0...65535 ms

- **RTS-Off-Verzögerung**

Nur projektierbar bei: TIM 1531 IRC

Die RTS-OFF-Verzögerung (ms) legt fest, wann das Modul nach dem Senden das RTS-Signal zurücknimmt.

- Wert = 0

Das Modul nimmt das RTS-Signal sofort nach dem Senden des letzten Zeichens zurück.

- Wert > 0

Nach dem Senden des letzten Zeichens läuft die RTS-OFF-Verzögerung ab, bevor das Modul das RTS-Signal zurücknimmt.

Voreinstellung: 0. Zulässiger Bereich: 0...65535 ms

3.6.2.2 Wählnetz

Einstellungen Wählnetz

Einstellungen serielle Schnittstelle

- **Schnittstellenstandard**

Standard der seriellen Schnittstelle: RS232 / RS485 - umschaltbar

Wählen Sie einen der folgenden Werte:

- RS232

Bei Anschluss eines Modems an die Schnittstelle der TIM

- RS485

Zuschaltung des internen Abschlusswiderstandes der TIM

Bei parallelem Anschluss mehrerer Modems an die Schnittstelle der TIM (sternförmiges Netz)

- **RS485-Terminierung**

Aktivieren Sie die Option bei Zuschaltung eines Abschlusswiderstandes für den RS485-Bus bei Anschluss eines sternförmigen Netzes.

Rufparameter

- **Wahlbefehl**

Wahlbefehl für das lokale Modem

Mögliche Werte:

- D (AT-Befehl)
- DP (AT-Befehl, Pulswahl)
- DT (AT-Befehl, Tonwahl)

Verwenden Sie möglichst den Wahlbefehl "D".

- **Wahl-Präfix**

Zugangsnummer (Amtsholung) für eine Nebenstellenanlage (typischer Eintrag 0 oder 9) oder für einen alternativen Telefondienstbetreiber.

Zulässiger Bereich: Max. 12 Ziffern

Bei direktem Anschluss an das Wählnetz und ohne alternativen Telefondienstbetreiber kann dieser Parameter leer bleiben.

- **Eigene Telefonnummer**

Eingabe der eigenen Telefonnummer des Netzknotens inklusive Ortsvorwahl

Zulässige Werte:

- Ziffern 0 - 9
- Pluszeichen (+) als Platzhalter für die nationalen Ausscheidungsziffern (meist 00 oder 09) vor der Ländervorwahl

Beispiel: +1230123456789

AT-Initialisierung

- **Benutzerdefiniert**

Bei aktivierter Option muss der AT-Initialisierungs-String für die Grundeinstellungen des Modems manuell vergeben werden.

Bei deaktivierter Option wird der AT-Initialisierungs-String Modem-spezifisch vorbelegt:

- MD3 : ATS45=3\N0F0&W
- MD4 : ATS45=83\$P1\N0&W

- **Initialisierungsstring**

Eingabefeld für den AT-Initialisierungs-String

Zeitoptionen

- **Wählprüfintervall**

Das Prüfintervall (min) wird gestartet, wenn vom Kommunikationsmodul nach Ablauf von 3 Wiederholungsversuchen keine Verbindung aufgebaut werden konnte. Nach Ablauf des Prüfintervalls unternimmt das Kommunikationsmodul einen erneuten Verbindungsaufbau.

Wenn der Verbindungsaufbau wieder nicht gelingt, wird das Prüfintervall erneut gestartet.

Wenn in einer Zentrale-TIM ein neues Telegramm während des Prüfintervalls zur Übertragung ansteht, versucht die TIM sofort, eine Verbindung aufzubauen.

Voreinstellung: 5. Zulässiger Bereich: 0...255

- **Max. Verbindungsdauer**

Nur für Schnittstellen mit dem Netzknotentyp "Zentrale".

Maximale Verbindungsdauer (s) für eine Wählverbindung. Nach Ablauf der Zeit wird die Verbindung abgebaut. Telegramme, die in der Station noch zur Übertragung anstehen, werden beim nächsten Verbindungsaufbau übertragen.

Bei 0 (Null) bleibt die Wählverbindung solange stehen, bis alle anstehenden Daten übertragen sind.

Voreinstellung: 5. Zulässiger Bereich: 0...65535

- **Wiederholfaktor**

Der Wiederholfaktor bestimmt, wie oft ein nicht positiv quittiertes Daten-Telegramm wiederholt wird.

Mobilfunkeinstellungen

Kommunikation über Mobilfunknetze wird nicht unterstützt.

3.6.2.3 Übertragungseinstellungen

Die spezifischen Parameter des Telecontrol-Protokolls finden Sie im Kapitel IEC-Parameter der Schnittstellen (Seite 56).

3.7 IEC-Parameter der Schnittstellen

3.7.1 Übertragungseinstellungen - IEC 60870-5

Übertragungseinstellungen - IEC 60870-5

- **ACTTERM**

Aktiviert das Versenden von Quittungen mit der Übertragungsursache ACTTERM (cause of transmission <10>).

Damit wird dem Partner das Ende der Befehlsbearbeitung signalisiert.

Bei direkter Kommunikation zwischen zwei Stationen muss ACTTERM für beide Partner identisch projektiert werden.

- **Max. Zeit zwischen Select und Operate**

Max. Zeitdauer (Sekunden) zwischen Select und Operate. Damit ein Select-Befehl an die CPU übertragen und damit wirksam wird, darf zwischen Select und Operate kein anderes Telegramm an die Station gesendet werden.

Zulässiger Bereich: 1..65535

Voreinstellung: 1

Den Modus der Befehlsverarbeitung legen Sie für jeden einzelnen Befehls-Datenpunkt fest, siehe Befehlsoptionen (Seite 146).

- **Überwachungszeit für Verbindungsaufbau (t_0)**

Überwachungszeit für den Verbindungsaufbau (t_0) in Sekunden. Wenn der Kommunikationspartner den Verbindungsaufbau innerhalb der Überwachungszeit nicht bestätigt, dann versucht das Modul, die Verbindung erneut aufzubauen.

Zulässiger Bereich: 1..255

Voreinstellung: 30

- **Telegramm-Überwachungszeit (t_1)**

Überwachungszeit in Sekunden für die Quittierung von Telegrammen, die das Modul gesendet hat, durch den Kommunikationspartner. Die Überwachungszeit gilt für alle vom Modul gesendeten Telegramme im I-, S- und U-Format.

Wenn der Partner innerhalb der Überwachungszeit keine Quittung sendet, dann baut das Modul die Verbindung zum Partner ab.

Zulässiger Bereich: 1..255

Voreinstellung: 15

Hinweis

Einstellungen beim Master

Beachten Sie bei der Projektierung der Überwachungszeiten t_1 und t_2 die korrespondierenden Einstellungen beim Master, damit es nicht zu ungewollten Fehlermeldungen oder Verbindungsabbrüchen kommt.

- **Überwachungszeit für S- und U-Telegramme (t_2)**

Überwachungszeit in Sekunden für die Quittierung von Datentelegrammen des Masters durch das Modul.

Nach dem Empfang von Daten vom Master quittiert das Modul die empfangenen Daten alternativ:

- Wenn das Modul innerhalb von t_2 selbst Daten an den Master sendet, dann quittiert er mit dem gesendeten Datentelegramm (I-Format) gleichzeitig die innerhalb von t_2 vom Master empfangenen Datentelegramme.
- Das Modul sendet spätestens nach Ablauf von t_2 ein Quittungstelegramm (S-Format) an den Master.

Zulässiger Bereich: 1 ... 255

Voreinstellung: 10

Der Wert von t_2 sollte kleiner sein als der von t_1 sein.

- **Ruhezeit für Testtelegramme (t_3)**

Überwachungszeit in Sekunden, in welcher das Modul keine Telegramme vom Master bekommt.

Nach Ablauf von t_3 sendet das Modul ein Test-/Steuer-Telegramm (U-Format) an den Master.

Der Parameter ist vorgesehen für den Fall langer Ruhezustände, d. h. in Zeiten ohne Datenverkehr.

Zulässiger Bereich: 1 ... 255

Voreinstellung: 30

- **Diff. (k) Sendefolgennummer N(S) zu Empfangsfolgennummer N(R)**

Differenz zwischen Sendefolgennummer $N(s)$ und Empfangsfolgennummer $N(r)$ eines Telegramms.

Der Master schickt die Sendefolgennummer eines Telegramms vom Modul als Quittung zurück, welche das sendende Modul dann als Empfangsfolgennummer speichert. Telegramme, deren Sendefolgennummer kleiner der Empfangsfolgennummer zuzüglich der hier projizierten Differenz ist, werden als erfolgreich übertragen gewertet und aus dem Sendespeicher des Moduls gelöscht.

Zulässiger Bereich: 1 ... 64

Voreinstellung: 12

- **Max. Anzahl unquittierter Datentelegramme (w)**

w: Maximale Anzahl an empfangenen Datentelegrammen (I-APDUs), nach der das älteste vom Master empfangene Telegramm quittiert werden muss.

Zulässiger Bereich: 1..8

Voreinstellung: 8

Der Wert muss kleiner sein als der Wert von "Differenz Sendefolge- zu Empfangsfolgennummer" (k).

Quittierungsmechanismus beim IEC-Protokoll

Das Modul schickt mit jedem gesendeten Datentelegramm eine fortlaufende Sendefolgennummer mit. Das Datentelegramm bleibt zunächst im Sendepuffer gespeichert.

Beim Empfang schickt der Master die Sendefolgennummer aus diesem oder (bei Empfang mehrerer Telegrammen) dem letzten Telegramm als Quittung an das Modul zurück. Das Modul speichert die vom Master zurückgeschickte Sendefolgennummer als Empfangsfolgennummer und verwendet sie als Quittung.

Telegramme, deren Sendefolgennummer gleich oder kleiner der aktuellen Empfangsfolgennummer ist, werden als erfolgreich übertragen gewertet und aus dem Sendepuffer des Moduls gelöscht.

Empfehlungen der Spezifikation:

- w sollte nicht größer sein als $2/3$ von k .
- Empfohlener Wert für k : 12
- Empfohlener Wert für w : 8

3.7.2 Einstellungen IEC-Master

IEC-Master

Folgende Parameter finden Sie in der Parametergruppe "Einstellungen IEC-Master" der auf den Netztyp IEC und den Netzknotentyp "Zentrale-Station" eingestellten Schnittstellen des Kommunikationsmoduls.

- **Polling-Basisintervall**

Hier legen Sie das Basisintervall für Stationsaufrufe durch die Zentrale fest.

Wertebereich: 0 ... 65535 Sekunden

Vorbelegung: 30

Bei 0 (Null) ist die Funktion abgeschaltet. Es findet kein zyklisches Polling statt, auch nicht für die nachfolgend aufgeführten Parameter, deren Berechnung auf dem Polling-Basisintervall beruht.

Das Basisintervall wird für die Berechnung der folgenden Parameter in der Verbindungsprojektierung verwendet:

- Intervall für Generalabfrage
- Intervall für Zähler-Generalabfrage
- Intervall für Gruppenabfrage
- Intervall für Zähler-Gruppenabfrage

Zur Projektierung siehe Kapitel Abfrageoptionen (Seite 114).

- **Max. Anzahl Ereignisse pro Aufruf**

Maximale Anzahl an Ereignissen, die nach einem Aufruf durch die Zentrale im Antworttelegramm der Station gesendet werden dürfen.

Wertebereich: 0 ... 65535

Vorbelegung: 0

Bei 0 (Null) ist die Funktion abgeschaltet (keine Begrenzung).

Beachten Sie zum Parameter "Partnerüberwachungszeit" auch das Kapitel Einstellungen IEC-Station (Seite 59).

3.7.3 Einstellungen IEC-Station

Ereignis-Einstellungen

Voraussetzungen

- Der Netzknotentyp der Schnittstelle ist "Station" oder "Knotenstation".
- Die Datenpunkte sind vom gleichen Typ.
- Die Indices der Datenpunkte liegen lückenlos hintereinander.

Siehe Kapitel Datenpunktindex (Seite 128).

Funktion

Für die nachfolgend aufgelisteten Datenpunkttypen können Sie die Übertragungsform einstellen. Die Einstellungen gelten für Datenpunkte, die als Ereignis projiziert sind (getriggert).

Die Funktion entspricht dem Bit "SQ" des "VARIABLE STRUCTURE QUALIFIER field" gemäß IEC 60870-5-101.

- **Übertragungsverhalten**

- Einzelübertragung:

Die Objektheadresse wird einzeln übertragen.

SQ = 0

- Sequentielle Übertragung

Die Objektheadressen werden zusammenhängend angelegt, um bei der Übertragung Datenvolumen zu sparen.

SQ = 1

Einstellungen der unterstützten Datenpunkttypen

Bei Projektierung von Übertragungsverhalten = "Sequentielle Übertragung" gelten für die aufgelisteten Datenpunkttypen die folgende Parameter.

Die Übertragung der gepufferten Ereignisse wird ausgelöst, sobald eine der beiden folgenden Bedingungen erfüllt ist.

- **Anzahl der Ereignisse**

Übertragung, wenn die projektierte Anzahl an gepufferten Ereignissen erreicht ist.

- **Verzögerungszeit**

Übertragung, wenn die projektierte Verzögerungszeit (Sekunden) erreicht ist.

Bei Projektierung von 0 (null) ist die jeweilige Funktion deaktiviert.

Weitere Stations-relevante Parameter

Folgende Stations-relevanten Parameter werden bei der Projektierung der Verbindungen festgelegt:

- Spontan
- Polling-Modus

Zur Projektierung siehe Kapitel Verbindungstabelle (Seite 104).

Weitere Parameter finden Sie in den folgenden Parametergruppen:

- Antwort auf Generalabfrage / Zuordnung zu Gruppenabfrage (cause of transmission 20 - 41)
 - Die Zuordnung einzelner Datenpunkte zu einer Generalabfrage oder Gruppenabfrage projektieren Sie bei der Datenpunktprojektierung, siehe Kapitel Register "Allgemein" (Seite 126).
 - Die Intervalle der Abfragen projektieren Sie bei den Telecontrol-Verbindungen, siehe Kapitel Abfrageoptionen (Seite 114).

3.8 WAN-Netze projektieren

Parameter der klassischen WAN-Netze

Projektieren Sie zuerst die Parametergruppe "WAN-Einstellungen" der Schnittstellen des Kommunikationsmoduls, siehe Kapitel WAN-Einstellungen der Schnittstellen (Seite 45).

Beim Erzeugen eines neuen Netzes werden die wichtigsten Einstellungen der Schnittstelle vom angeschlossenen WAN-Netz übernommen.

Die klassischen WAN-Netze, in STEP 7 blau dargestellt, haben folgende Parametergruppen.

Allgemein

Hier projektieren Sie, wie für jedes andere Netz auch, den Namen und die S7-Subnetz-ID.

Netzeinstellungen

Netzwerk-Konfiguration

- **Protokolltyp**

Abhängig vom Modultyp können folgende Fernwirkprotokolle zur Auswahl stehen:

- ST7
- DNP3
- IEC 60870-5

- **Netztyp**

Der Netztyp wird von der angeschlossenen Schnittstelle übernommen:

- Standleitung
- Wählnetz

Zugriffsverfahren

Nur bei Standleitung

- **Zugriffsverfahren**

Das Zugriffsverfahren ist vorgelegt und nicht änderbar:

- Polling

Telegrammparameter

Die Parameter sind vorgelegt und nicht änderbar.

- **Telegrammformat**

- FT1.2

- **Quittungsart**

- Kurzquittung (1 Byte)

- **Wiederholfaktor**

Der Wiederholfaktor bestimmt, wie oft ein nicht positiv quittiertes Daten-Telegramm wiederholt wird:

- 3

- **Max. Telegrammlänge**

Maximale Größe eines Daten-Telegramms innerhalb des Netzes:

- 240

Netzeinstellungen

- **Richtungsabhängigkeit**

Richtungsabhängigkeit des Netzes

- Duplex
- Halbduplex

- **Übertragungsgeschwindigkeit**

Geschwindigkeit, mit der zwischen Kommunikationsmodul und Modem kommuniziert wird.

Wählen Sie aus der Klappliste einen Wert aus, der von allen angeschlossenen Modems unterstützt wird.

Uhrzeitsynchronisation

- Uhrzeitsynchronisation für WAN aktivieren

Mit aktiviertem Parameter legen Sie fest, ob die Uhrzeit für die Uhrzeitsynchronisation der angeschlossenen Stationen über das WAN-Netz übertragen werden soll.

Bei aktiviertem Parameter legen Sie den Synchronisationszyklus fest.

Hinweis

Übernahme der Einstellung durch Stationen

Die angeschlossenen TIM-Baugruppen übernehmen die hier am Netz vorgenommenen Einstellungen.

Zum Uhrzeitkonzept siehe Kapitel Uhrzeitsynchronisation (Seite 37).

Stationsliste

Hier finden Sie eine Übersichtstabelle der am Netz angeschlossenen Stationen mit ihren wichtigsten Parametern.

Die WAN-Adresse ist die Stationsadresse.

3.9 Webserver (TIM 1531 IRC)

Der Webserver der TIM

Die TIM stellt Ihnen für den Zugriff über einen Webbrowser die Funktion eines Webserver zur Verfügung. Über den Webserver stehen Ihnen folgende Funktionen zur Verfügung:

- Lesender Zugriff
 - Eine Auswahl an Diagnosedaten
 - Eine Auswahl an Projektierungsdaten
- Schreibender Zugriff
 - Uhrzeit stellen
 - Firmware-Aktualisierung
 - Neustart der Baugruppe
 - Rücksetzen auf Werkseinstellungen
 - Aufzeichnung von Statistikwerten der Ethernet-Schnittstellen

Die Beschreibung der Inhalte finden Sie im Kapitel WBM der TIM 1531 IRC (Seite 193).

Zugriffsberechtigung über "Globale Security-Einstellungen"

Die Rechte für den Zugriff auf den Webserver werden in STEP 7 in den Globalen Security-Einstellungen projektiert. Nur dort angelegte Benutzer können sich über HTTP/HTTPS am Webserver der TIM anmelden.

Für den Webserver-Zugriff sind folgende vorbelegten Rollen relevant:

- NET Standard
- NET Diagnose

Die erforderlichen Rechte für die Diagnose, den Zugriff auf den Webserver und das Lesen und Schreiben von Daten werden damit freigegeben.

Weitere Hilfe zu den Rollen und Rechten der Benutzer finden Sie im STEP 7-Informationssystem.

Zugriff auf den Webserver und Start der Webdiagnose

Um sich mit dem Webserver der TIM verbinden zu können, muss der Zugriff auf den Webserver für jede Ethernet-Schnittstelle aktiviert werden, vgl. Kapitel Zugriff auf den Webserver (Seite 51). In der Voreinstellung ist der Zugriff deaktiviert.

Zum Start der Webdiagnose siehe Kapitel Webdiagnose der TIM 1531 IRC (Seite 65).

Parametergruppe "Webserver"

Allgemein

- **Webserver auf dieser Baugruppe aktivieren**

Aktiviert die Datenverarbeitung im Webserver der TIM und ermöglicht den Zugriff auf diese Daten.

- **Zugriff nur über HTTPS zulassen**

Erlaubt den Zugriff auf den Webserver nur mit dem gesicherten Protokoll HTTPS.

Hinweis

Zugriff nur über HTTPS zulassen (aktivierte Security-Funktion)

Beachten Sie Folgendes, wenn die Option "Zugriff nur über HTTPS zulassen" in der Parametergruppe "Webserver" aktiviert ist:

- Die Daten werden verschlüsselt übertragen.

Voraussetzungen

- Dem Benutzer müssen die oben genannten Rollen mit den zugehörigen Rechten zugewiesen sein.
 - Bei aktivierter Firewall müssen die Protokolle HTTP/HTTPS freigegeben sein.
-

Automatische Aktualisierung

- **Automatische Aktualisierung aktivieren**

Aktiviert das automatische Aktualisieren der angezeigten Werte.

Bei deaktivierter Option werden nur die Werte zum Zeitpunkt des Verbindens mit dem Webserver angezeigt.

- **Aktualisierungsintervall**

Wählen Sie das Intervall, in dem Sie eine Aktualisierung der angezeigten Werte wünschen.

Voreinstellung: 30. Zulässiger Bereich: 5...999

Übersicht der Schnittstellen

Hier sehen Sie tabellarisch die Freischaltung des Zugriffs auf den Webserver über alle Ethernet-Schnittstellen der TIM.

Sie können den Zugriff auf den Webserver der TIM über HTTP/HTTPS für jede einzelne Ethernet-Schnittstelle aktivieren.

Die Einstellungen zur Aktivierung in den Parametergruppen "Zugriff auf den Webserver" und "Webserver" werden wechselseitig in die jeweils andere Parametergruppe übernommen.

3.10 Webdiagnose der TIM 1531 IRC

Voraussetzungen

- Der Webserver des Moduls ist in der Projektierung, Parametergruppe "Webserver", aktiviert und die Schnittstelle ist ausgewählt.
- Die Schnittstelle ist in der Projektierung, Parametergruppe "Ethernet-Schnittstelle > Zugriff auf Webserver", für den Zugriff auf den Webserver freigegeben.

Start der Webdiagnose

1. Stellen Sie eine physikalische Verbindung zwischen der Engineering-Station und der SIMATIC-Station her.
2. Stellen Sie die PC-Schnittstelle so ein, dass das Modul erreichbar ist.
Weitere Hilfe erhalten Sie unter der Funktion "PG/PC-Schnittstelle einstellen...".
3. Klicken Sie im STEP 7-Projekt unter der Parametergruppe "Webdiagnose" auf die Schaltfläche "Webdiagnose", um die Verbindung mit dem Webbrowser des Moduls herzustellen.

Die Inhalte werden vom integrierten Webserver des Moduls geliefert. Zur Bedienung und zu den Inhalten siehe Kapitel WBM der TIM 1531 IRC (Seite 193).

3.11 DNS-Konfiguration

DNS-Server

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

DNS-Server für E-Mail-Server-Adresse

Bei der E-Mail-Projektierung ist die Adresse des Mail-Servers anzugeben, über den die E-Mails geschickt werden sollen. Die Adresse des Mail-Servers kann als IP-Adresse oder als FQDN angegeben werden.

Bei der Angabe der Server-Adresse als FQDN müssen Sie einen DNS-Server projektieren. In diesem Fall wird die IP-Adresse des Mail-Servers über den projizierten DNS-Server ermittelt.

3.12 Kommunikation mit der CPU

Kommunikation mit der CPU

Über die ersten drei Parameter legen Sie den CPU-Zugriff durch die TIM im CPU-Abtastzyklus fest. Den Aufbau des CPU-Abtastzyklus finden Sie im Kapitel Lesezyklus (Seite 132).

- **Zykluspausenzeit**

Wartezeit zwischen zwei Abtastzyklen des CPU-Speicherbereichs

- **Max. Anzahl der Schreibaufträge**

Maximale Anzahl der Schreibaufträge an den CPU-Speicherbereich innerhalb eines CPU-Abtastzyklus

- **Max. Anzahl der Leseaufträge**

Maximale Anzahl der niederpriorigen Leseaufträge aus dem CPU-Speicherbereich innerhalb eines CPU-Abtastzyklus

Watchdog-Bit

- **TIM-Überwachung / CP-Überwachung**

Über das Watchdog-Bit kann der CPU der Zustand der Fernwirkkommunikation des Kommunikationsmoduls mitgeteilt werden.

CP-Uhrzeit

- **CP-Uhrzeit an CPU**

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

Ablauf:

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

Empfehlung:

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

CP-Diagnose

Über die Parametergruppe haben Sie die Möglichkeit, erweiterte Diagnosedaten über PLC-Variablen aus dem CP auszulesen.

- **Erweiterte CP-Diagnose aktivieren**

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

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

Die nachfolgenden PLC-Variablen für die einzelnen Diagnosedaten können selektiv aktiviert werden, abhängig von den vom CP unterstützten Funktionen.

- **Diagnose-Trigger-Variable**

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

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

Hinweis

Schnelles Setzen der Diagnose-Trigger-Variable

Trigger sollten nicht öfter als einmal pro Sekunde gesetzt werden.

- **Telegrammspeicher-Überlaufwarnung**

PLC-Variable (Datentyp Byte) für die Sendepuffer-Überlauf-Vorwarnung. Bit 0 wird auf 1 gesetzt, wenn 80 % Füllgrad des Sendepuffers erreicht sind.

- **Telegrammspeicher-Belegung**

PLC-Variable (Datentyp DWord) für die Belegung des Sendepuffers. Die Anzahl der gespeicherten Telegramme wird angegeben.

- **Aktuelle IP-Adresse**

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

- **VPN-IPsec-Status**

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

- 0 = Kein Tunnel aufgebaut
- 1 = Tunnel aufgebaut

- **Verbindung mit SINEMA Remote Connect**

Die PLC-Variable (BOOL) gibt an, ob eine Verbindung zum SINEMA RC-Server besteht:

- 0 = Keine Verbindung aufgebaut
- 1 = Verbindung aufgebaut

PLC-Variablen für Partnerstatus / Wegestatus

Über die hier projektierbare PLC-Variable können Sie folgende Informationen zur Erreichbarkeit der Kommunikationspartner überwachen:

- **Partnerstatus**
Erreichbarkeit des remoten Kommunikationspartners
- **Wegestatus**
Status des Verbindungswegs bzw. der redundanten Verbindungswege zum remoten Kommunikationspartner
Zur Kommunikation und die möglichen Verbindungswege siehe Kapitel Kommunikationsmöglichkeiten (Seite 29).

Für jeden projektierten Kommunikationspartner, zu dem eine einfache oder redundante Telecontrol-Verbindung angelegt ist, können Sie eine PLC-Variable vom Typ Word anlegen.

Belegung der PLC-Variable für Partnerstatus / Wegestatus

In den zwei Bytes der PLC-Variable vom Datentyp Word (DB, Merker, Ausgang) werden folgende Informationen ausgegeben:

- **Byte 0: Partnerstatus**
- **Byte 1: Wegestatus**

Byte 0 "Partnerstatus"

Byte 0 kodiert Informationen zur Erreichbarkeit des Kommunikationspartners, zu vorhandenen Verbindungen und Verbindungswegen und zum Zustand des Sendepuffers der TIM.

Tabelle 3- 1 Belegung von Byte 0: Bedeutung der Bit-Zustände

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Wegeredundanz	Verbindungsmodus	Temporäre Verbindung *	<i>(Reserviert)</i>	Telegrammspeicher **	Wegestatus	Partnerstatus	
0: Keine Redundanz 1: Redundanz vorhanden	0: Permanent 1: Temporär	0: Partner nicht erreichbar 1: Partner erreichbar *	-	0: Sendepuffer OK 1: Speicherbelegung > 80 % 3: Überlauf (Speicherbelegung 100 %)	0: Nicht alle Wege erreichbar 1: Alle Wege erreichbar	0: Partner nicht erreichbar 1: Partner erreichbar	

** Partner, die temporäre Verbindungen unterstützen, werden als "erreichbar" gesetzt, wenn der Partner selbst die Verbindung abbaut und keine Verbindung besteht.

** Status des Sendepuffers:

Wenn bei einem Sendepuffer-Überlauf bzw. der Vorwarnung Bit 2 bzw. Bit 2+3 gesetzt sind, werden die beiden Bits erst wieder zurückgesetzt, wenn die Speicherbelegung 50 % unterschreitet.

Zum Sendepuffer siehe Kapitel Prozessabbild, Übertragungsart, Ereignisklassen (Seite 130).

Byte 1 "Wegestatus"

Byte 1 zeigt aus Sicht der lokalen TIM den Status des Verbindungswegs (projektierte Verbindung) zum Partner an.

Maximal können 2 Wege (Haupt- und Ersatzweg) zu einem Partner projiziert werden, siehe Kapitel Kommunikationsmöglichkeiten (Seite 29).

Die beiden Verbindungswege müssen auf einer lokalen TIM beginnen oder enden.

Das Byte zeigt folgendes an:

- Die Wege, über die der Partner erreichbar ist.
- Der aktuell genutzte Weg
- Die TIM-Schnittstelle, über die der Hauptweg projiziert wurde.
- Die TIM-Schnittstelle, über die der Ersatzweg projiziert wurde.

Der Weg einer Verbindung wird angegeben als Kombination aus den benutzten Schnittstellen der TIM und dem Status des Wegs.

Byte-Belegung

Byte 1 ist folgendermaßen belegt:

- Zwei Bits für die Schnittstelle des Hauptwegs
- Zwei Bits für die Schnittstelle des Ersatzwegs
- Zwei Bits für den Wegestatus des Hauptwegs
- Zwei Bits für den Wegestatus des Ersatzwegs

Tabelle 3- 2 Belegung von Byte 1

Bit 6 + 7	Bit 4 + 5	Bit 2 + 3	Bit 0 + 1
Projektierte Schnittstelle		Wegestatus	
Kodierung für Ersatzweg	Kodierung für Hauptweg	Ersatzweg (2. Weg)	Hauptweg (1. Weg)

- **Projektierte Schnittstelle**

Die TIM-Schnittstellen "Ethernet 1" (IE1), "Ethernet 2" (IE2), "Ethernet 3" (IE3) und WAN1 sind von 0 .. 3 durchnummeriert (dezimal):

- 0 = Ethernet-Schnittstelle IE1 (X1)
- 1 = Ethernet-Schnittstelle IE2 (X2)
- 2 = Ethernet-Schnittstelle IE3 (X3)
- 3 = Serielle Schnittstelle WAN1 (X4)

Zustand Bit 5 (7)	Zustand Bit 4 (6)	Bedeutung
0	0	Kodierung für Ethernet-Schnittstelle X1 (dezimal: Nr. 0)
0	1	Kodierung für Ethernet-Schnittstelle X2 (dezimal: Nr. 1)
1	0	Kodierung für Ethernet-Schnittstelle X3 (dezimal: Nr. 2)
1	1	Kodierung für serielle Schnittstelle X4 (dezimal: Nr. 3)

- **Wegestatus**
 - Hauptweg = 1. Weg (Bit 0 + 1)
 - Ersatzweg = 2. Weg (Bit 2 + 3)

Zustand Bit 1 (3)	Zustand Bit 0 (2)	Bedeutung Bit 1	Bedeutung Bit 0
0	0	Bit 1: Weg nicht aktuell	Bit 0: Teilnehmer nicht erreichbar
0	1	Bit 1: Weg nicht aktuell	Bit 0: Teilnehmer erreichbar
1	0	Bit 1: Weg aktuell	Bit 0: Teilnehmer nicht erreichbar
1	1	Bit 1: Weg aktuell	Bit 0: Teilnehmer erreichbar

Kodierungsmöglichkeiten von Byte 1

Gleiche Kodierung der projektierten Schnittstelle für den Haupt- und den Ersatzweg bedeutet, dass keine Wegeredundanz vorliegt (nur eine Schnittstelle projektiert). Der Wegestatus wird dann über die Bits des Hauptwegs (1. Weg) ausgegeben.

Tabelle 3- 3 Kodierungsmöglichkeiten für den Wegestatus

Projektierte Schnittstelle		Wegestatus	
Kodierung für Ersatzweg	Kodierung für Hauptweg	Ersatzweg (2. Weg)	Hauptweg (1. Weg)
0 0	0 0 (Kodierung für IE1)	Irrelevant (nicht redundant)	Status IE1
0 0	0 1 (Kodierung für IE2)	Status IE1	Status IE2
0 0	1 0 (Kodierung für IE3)	Status IE1	Status IE3
0 0	1 1 (Kodierung für WAN1)	Status IE1	Status WAN1
0 1	0 0	Status IE2	Status IE1
0 1	0 1	Irrelevant (nicht redundant)	Status IE2
0 1	1 0	Status IE2	Status IE3
0 1	1 1	Status IE2	Status WAN1
1 0	0 0	Status IE3	Status IE1
1 0	0 1	Status IE3	Status IE2
1 0	1 0	Irrelevant (nicht redundant)	Status IE3
1 0	1 1	Status IE3	Status WAN1
1 1	0 0	Status WAN1	Status IE1
1 1	0 1	Status WAN1	Status IE2
1 1	1 0	Status WAN1	Status IE3
1 1	1 1	Irrelevant (nicht redundant)	Status WAN1

3.13 E-Mail-Projektierung

Projektierung von E-Mails

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

Im Nachrichteneditor (Eintrag "Nachrichten") projektieren Sie die einzelnen E-Mails, siehe Kapitel Nachrichten (Seite 149).

Voraussetzungen für E-Mail

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

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

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

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

E-Mail-Projektierung

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

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

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

- Port-Nr. 587

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

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

- Port-Nr. 465

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

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

Zur Projektierung der Passwörter siehe Zeichensatz für Benutzernamen, Passwörter und Nachrichten (Seite 155).

Zertifikat importieren bei verschlüsselter Übertragung

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

Verwenden Sie das Zertifikat über folgende Schritte:

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

Zur Vorgehensweise siehe Kapitel Zertifikatsmanager (Seite 84).

3.14 Teilnehmernummern

Teilnehmernummern

In diesem Verzeichnis projektieren Sie in Abhängigkeit des Kommunikationsmoduls die Stationsadresse und die Zuordnung der CPU:

- **CP**

- ASDU-Adresse

ASDU-Adresse der Station

Das Kommunikationsmodul und die Station (CPU) haben dieselbe ASDU-Adresse.

- Strukturierte ASDU-Adresse

Strukturierte ASDU-Adresse der Station

Die CPU ist dem Kommunikationsmodul automatisch über das Rack zugeordnet.

- **TIM**

- Zugeordnete CPU

In der Klappliste werden nur diejenigen CPUs angezeigt, die mit der TIM vernetzt sind.

- Passwort der zugeordneten CPU

Wenn die zugeordnete CPU mit "Kein Zugriff (kompletter Schutz)" geschützt ist, dann geben Sie hier das Passwort ein, das bei der CPU unter "Schutz & Security > Zugriffsstufe" projiziert ist.

- ASDU-Adresse

ASDU-Adresse der Station

Das Kommunikationsmodul und die Station (CPU) haben dieselbe ASDU-Adresse.

- ASDU-Adresse

Strukturierte ASDU-Adresse der Station

Beachten Sie die grundlegenden Adressierungs-Richtlinien im Kapitel Adressierung (Seite 29).

Zuordnung der CPU und Projektierung der Teilnehmer-Adressen

Für Module, die über Telecontrol-Verbindungen kommunizieren (Editor "Netzwerkdaten"), nehmen Sie die Zuordnung der CPU und die Projektierung der Moduladressen in der Parametergruppe "Teilnehmernummern" vor.

- **Zugeordnete CPU**

Bei folgenden Kommunikationsmodulen, die sich im gleichen Rack befinden wie die CPU, wird die lokale CPU automatisch dem Modul zugeordnet:

- CPs (S7-1200, ET 200SP)

Bei Kommunikationsmodulen, die sich nicht zusammen mit einer CPU im gleichen Rack befinden, müssen Sie das Modul einer CPU, mit der es vernetzt ist, über die Klappliste zuordnen. Dies betrifft:

- TIM 1531 IRC

Der TIM 1531 IRC können Sie eine CPU der folgenden SIMATIC-Familien zuordnen: S7-300, S7-400, S7-1500, ET 200SP

Wenn Sie die TIM 1531 IRC einer S7-1500R/H-CPU zuordnen, wird für die Kommunikation der TIM mit der CPU die System-IP-Adresse der S7-1500R/H-CPU verwendet.

Strukturierte Adressierung beim IEC-Protokoll

Die ASDU-Adresse kann in zwei Eingabefeldern mit unterschiedlichem Format projektiert werden:

- ASDU-Adresse

Hier wird die Adresse unstrukturiert als Ganzzahl projektiert.

Wertebereich: 0..65534

- Strukturierte ASDU-Adresse

Hier können Sie die Adresse gemäß IEC 60870-5-3 strukturiert projektieren. Über die strukturierte Adressierung wird eine anlagenorientierte Strukturierung der ASDU-Adresse ermöglicht.

Projektiertbar sind 2 Adress-Stufen (Oktette).

Wertebereich: 0.0..255.254

Die projektierten Werte der beiden Felder sind gekoppelt. Ein projektiertes Wert wird umgerechnet und im jeweils anderen Eingabefeld angezeigt.

Umrechnung der Werte:

Die Werte werden für die Umrechnung wie folgt bezeichnet:

- ASDU-Adresse
Bezeichnung des Ganzzahl-Werts: X
- Strukturierte ASDU-Adresse
Bezeichnung der Werte der 2 Oktette: A.B

Der projektierte Wert wird nach folgender Formel in das jeweils andere Feld übernommen:

$$X = A * 256 + B$$

3.15 Gesicherte Kommunikation zwischen CPU und Modul

Gesicherte Kommunikation mit Zertifikaten

Einem Kommunikationsmodul müssen Sie in folgenden Fällen das Zertifikat der CPU zuweisen.

Erforderlich bei:

- Kommunikationsmodul in separatem Rack (TIM 1531 IRC)
und
- CPU 1500 / CPU 1500 SP ab V2.9

Voraussetzungen:

- Unter "Teilnehmernummern" ist die CPU dem Modul zugeordnet.
- Sie sind mit der Rolle "NET Administrator" angemeldet.
- In der CPU wurde das Passwort zum Schutz der vertraulichen PLC-Konfigurationsdaten angelegt. Dadurch wird im Zertifikatsmanager der CPU das Kommunikationszertifikat mit der ID "1" und dem Zertifikatsinhaber "PLC-Name/Communication-1" angelegt.

Das Kommunikationszertifikat muss dem Modul, das der CPU zugeordnet ist, zugewiesen werden. Dafür gibt es folgende Vorgehensweisen.

Vorgehensweisen

Verwenden Sie alternativ eine der beiden folgenden Methoden.

Verwendung des globalen Zertifikatsmanagers für die CPU

Das lokale Kommunikationszertifikat der CPU wird in diesem Fall neu angelegt.

1. Selektieren Sie die CPU: "Schutz & Security > Zertifikatsmanager".
2. Aktivieren Sie das Optionskästchen "Globale Security-Einstellungen für den Zertifikatsmanager verwenden".
3. Nach Bestätigung des nachfolgenden Dialogs wird das Kommunikationszertifikat aus dem Zertifikatsmanager der CPU entfernt.

4. Zum Erstellen eines neues Kommunikationszertifikats wählen Sie in den allgemeinen Einstellungen das Menü "Schutz & Security > Verbindungsmechanismen".
5. Erstellen Sie unter "PLC-Kommunikationszertifikat" ein neues Kommunikationszertifikat. Klicken Sie dazu rechts auf "...".
6. Klicken Sie im folgenden Fenster auf "Hinzufügen".
7. Bestätigen Sie die Einstellungen im Fenster "Zertifikat erstellen" mit "OK".

Ergebnis: Das Zertifikat ist im Zertifikatsmanager der CPU und im globalen Zertifikatsmanager verfügbar.

Zertifikat dem Modul zuzuordnen:

1. Öffnen Sie in der Projektnavigation "Security-Einstellungen" > "Security-Funktionen" > "Zertifikatsmanager".
 2. Wählen Sie das Register "Gerätezertifikate".
 3. Klicken Sie mit der rechten Maustaste auf das Kommunikationszertifikat und wählen Sie "Zuordnen".
 4. Klicken Sie bei dem Modul, welchem das Zertifikat zugewiesen werden soll, auf die Option "Zugewiesen".
 5. Wechseln Sie bei "Verwendung" von "Gerätezertifikat" auf "Vertrauenswürdige Zertifikat".
- Sie können das Zertifikat auch über den lokalen Zertifikatsmanager des Moduls zuordnen.

Verwendung des lokalen Zertifikatsmanagers der CPU

Das lokale Kommunikationszertifikat der CPU wird in diesem Fall direkt verwendet, muss aber über Export und Import dem Kommunikationsmodul zugewiesen werden.

1. Selektieren Sie die CPU und wählen Sie in den allgemeinen Einstellungen das Menü "Schutz & Security > Zertifikatsmanager".
2. Klicken Sie mit der rechten Maustaste auf das Kommunikationszertifikat und wählen Sie "Exportieren".
3. Speichern Sie das Zertifikat.

Zertifikat dem Modul zuzuordnen:

1. Öffnen Sie in der Projektnavigation "Security-Einstellungen" > "Security-Funktionen" > "Zertifikatsmanager".
 2. Wählen Sie das Register "Gerätezertifikate".
 3. Importieren Sie das Kommunikationszertifikat.
 4. Klicken Sie mit der rechten Maustaste auf das Kommunikationszertifikat und wählen Sie "Zuordnen".
 5. Klicken Sie bei dem Modul, welchem das Zertifikat zugewiesen werden soll, auf die Option "Zugewiesen".
 6. Wechseln Sie bei "Verwendung" von "Gerätezertifikat" auf "Vertrauenswürdige Zertifikat".
- Sie können das Zertifikat auch über den lokalen Zertifikatsmanager des Moduls zuordnen.

3.16 Log-Einstellungen

Log-Einstellungen

Gültigkeit: TIM 1531 IRC

Zur Überwachung lassen sich Ereignisse in Log-Dateien aufzeichnen. Sie können einstellen, wie die Ereignisse aufgezeichnet werden:

- Lokales Logging

Meldungen zu internen Ereignissen und Fehlern werden im Diagnosepuffer der TIM gespeichert.

Aufgezeichnet werden könne die folgenden Ereignisse:

- Audit-Log: Audit-Ereignisse
- System-Log: System-Ereignisse

- Netzwerk-Syslog

Die Meldungen zu den Ereignissen werden im UDP-Format nach RFC 5424 bzw. RFC 5426 an einen Syslog-Server versendet. Details zum Aufbau der Syslog-Telegramme und den unterstützten Ereignispuffer-Einträgen entnehmen Sie dem Kapitel Security (Seite 215).

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

3.17 SNMP

SNMP

Den Leistungsumfang der Module finden Sie im jeweiligen Gerätehandbuch.

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

SNMP

- **"SNMP aktivieren"**

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

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

- **"SNMPv1 verwenden"**

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

- **"SNMPv3 verwenden"**

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

SNMPv1

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

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

- **"Community String lesend"**

Der String ist für den lesenden Zugriff erforderlich.

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

- **"Erlaube schreibenden Zugriff"**

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

- **"Community String schreibend"**

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

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

Hinweis

Sicherheit des Zugriffs

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

SNMPv3

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

- **"Authentifizierungsalgorithmus"**

Selektieren Sie in der Klappliste das zu verwendende Authentifizierungsverfahren.

- **"Verschlüsselungsalgorithmus"**

Selektieren Sie in der Klappliste das zu verwendende Verschlüsselungsverfahren.

Benutzerverwaltung

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

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

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

3.18 Globaler Zertifikatsmanager

Zertifikate von SIMATIC NET-Geräten

SIMATIC NET-Kommunikationsmodule verwenden grundsätzlich den globalen Zertifikatsmanager. Diesen finden Sie in der Projektnavigation unter "Security-Einstellungen > Security-Funktionen".

Alle lokalen Zertifikate von SIMATIC NET-Kommunikationsmodulen finden Sie auch im globalen Zertifikatsmanager.

3.19 CP: Security und Zertifikate

3.19.1 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.

3.19.2 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.

3.19.3 SYSLOG

Nutzung von SYSLOG nur bei 1 VPN-Verbindung

Wenn Sie SYSLOG mit Stufe 7 (debug) über VPN-Verbindungen nutzen möchten, dann ist dies nur mit einer einzigen projektierten VPN-Verbindung möglich.

3.19.4 VPN

3.19.4.1 VPN (Virtual Private Network)

VPN - IPsec

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

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

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

Eigenschaften

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

Anwendungsgebiete/Einsatzgebiete

- Lokale Netze können über das Internet auf sichere Art miteinander verbunden werden (Site-to-Site-Verbindung).
- Gesicherter Zugriff auf ein Firmennetz (End-to-Site-Verbindung)
- Gesicherter Zugriff auf einen Server (End-to-End-Verbindung)

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

Zellenschutzkonzept

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

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

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

- Datenspionage
- Datenmanipulation
- Unerwünschte Zugriffe

3.19.4.2 VPN-Tunnel für S7-Kommunikation zwischen Stationen anlegen

Voraussetzungen

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

- Die zwei Stationen sind projektiert.
- Die CPs in beiden Stationen müssen die Security-Funktionen unterstützen.
- Die Ethernet-Schnittstellen der beiden Stationen befinden sich im gleichen Subnetz.

Hinweis

Kommunikation auch über einen IP-Router möglich

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

Vorgehensweise

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

1. Security-Benutzer anlegen

Wenn der Security-Benutzer schon angelegt ist: Melden Sie sich als dieser Benutzer an.

2. Option "Aktiviere Security-Funktionen" aktivieren

3. VPN-Gruppe anlegen und Security-Module zuweisen

4. Eigenschaften der VPN-Gruppe projektieren

5. Lokale VPN-Eigenschaften der beiden CPs projektieren

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

"Aktiviere Security-Funktionen" anwählen

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

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

VPN-Gruppe anlegen und Security-Module zuweisen

1. Wählen Sie in den globalen Security-Einstellungen den Eintrag "Firewall" > "VPN-Gruppen" > "Neue VPN-Gruppe hinzufügen".

2. Doppelklicken Sie auf den Eintrag "Neue VPN-Gruppe hinzufügen", um eine VPN-Gruppe anzulegen.

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

3. Doppelklicken Sie in den globalen Security-Einstellungen auf den Eintrag "VPN-Gruppen" > "Modul einer VPN-Gruppe zuweisen".

4. Ordnen Sie der VPN-Gruppe die Security-Module zu, zwischen denen VPN-Tunnel aufgebaut werden sollen.

Hinweis

Aktuelles Datum und aktuelle Uhrzeit im CP für VPN-Verbindungen

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

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

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

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

Eigenschaften der VPN-Gruppe projektieren

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

Hinweis

VPN-Eigenschaften der CPs festlegen

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

Ergebnis

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

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

3.19.4.3 VPN-Kommunikation mit SOFTNET Security Client (Engineering-Station)

Das Anlegen der VPN-Tunnelkommunikation zwischen SOFTNET Security Client und dem CP nehmen Sie entsprechend Kapitel VPN-Tunnel für S7-Kommunikation zwischen Stationen anlegen (Seite 80) vor.

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 gelingt.

3.19.4.4 VPN-Tunnelkommunikation zwischen CP und SCALANCE M aufbauen

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

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

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

3.19.4.5 CP als passiver Teilnehmer von VPN-Verbindungen

Erlaubnis zum VPN-Verbindungsaufbau bei passivem Teilnehmer einstellen

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

Dies ist der Fall bei folgender typischer Konfiguration:

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

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

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

3.19.5 Zertifikatsmanager

Zuordnung von Zertifikaten

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

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

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

Die Beschreibung der Vorgehensweise finden Sie im Kapitel Handhabung von Zertifikaten (Seite 84).

Weitere Informationen finden Sie im STEP 7-Informationssystem.

3.19.6 Handhabung von Zertifikaten

Zertifikate für die Authentifizierung

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

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

Für die gesicherte Übertragung von E-Mails über SSL/TLS wird für die Baugruppe ein SSL-Zertifikat erstellt. Es wird in STEP 7 unter "Globale Security-Einstellungen > Zertifikatsmanager > Gerätezertifikate" sichtbar.

In der Tabelle "Gerätezertifikate" werden Aussteller, Gültigkeit, Verwendung eines Zertifikats (Dienst/Applikation) und die Verwendung eines Schlüssels angezeigt. Weitere Informationen eines Zertifikats können Sie aufrufen, wenn Sie das Zertifikat in der Tabelle selektieren und das Kontextmenü "Anzeigen" wählen.

In der Tabelle sehen Sie auch alle weiteren von STEP 7 erzeugten sowie alle importierten Zertifikate.

Wenn die Baugruppe bei aktivierten Security-Funktionen mit Nicht-Siemens-Partnern kommuniziert, dann müssen die entsprechenden Zertifikate der Kommunikationspartner ausgetauscht werden. Hierzu müssen Sie folgendermaßen vorgehen:

1. Fremdzertifikate von Kommunikationspartnern importieren
⇒ Globale Security-Einstellungen des Projekts (Zertifikatsmanager)
2. Zertifikate lokal zuordnen
⇒ Lokale Security-Einstellungen der Baugruppe (Tabelle "Zertifikatsmanager")

Diese zwei Schritte sind in den nächsten beiden Abschnitten beschrieben.

Fremdzertifikate von Kommunikationspartnern importieren

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

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

Zertifikate lokal zuordnen

Um ein importiertes Zertifikat für die TIM nutzen zu können, müssen Sie es in der Parametergruppe "Security" der TIM angeben. Gehen Sie hierzu folgendermaßen vor:

1. Selektieren Sie im STEP 7-Projekt die Baugruppe.
2. Navigieren Sie zur Parametergruppe "Security > Zertifikatsmanager".

3. Doppelklicken Sie in der Tabelle auf die Zelle mit dem Eintrag "<Neu hinzufügen>".
Die Tabelle "Zertifikatsmanager" der Globalen Security-Einstellungen wird angezeigt.
4. Selektieren Sie in der Tabelle das gewünschte Fremdzertifikat und klicken Sie zur Übernahme auf das grüne Häkchen unter der Tabelle.
Das ausgewählte Zertifikat wird in der lokalen Tabelle der Baugruppe angezeigt.
Erst jetzt wird das Fremdzertifikat für die Baugruppe verwendet.

Zertifikate für Applikationen von Drittherstellern exportieren

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

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

1. Öffnen Sie im STEP 7-Projekt den globalen Zertifikatsmanager:
Globale Security-Einstellungen > Zertifikatsmanager
2. Öffnen Sie das Register "Gerätezertifikate".
3. Selektieren Sie in der Tabelle die Zeile mit dem gewünschten Zertifikat und wählen Sie das Kontextmenü "Exportieren".
4. Speichern Sie das Zertifikat im Dateisystem des PC der angeschlossenen Engineering-Station.

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

Zertifikat ändern: Alternativer Name des Zertifikatsinhabers

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

Sie können diesen Parameter eines Zertifikats im Zertifikatsmanager der Globalen Security-Einstellungen ändern. Selektieren Sie hierzu in der Tabelle der Gerätezertifikate ein Zertifikat und rufen Sie das Kontextmenü "Erneuern" auf. In STEP 7 geänderte Eigenschaften des Parameters "Alternativer Name des Zertifikatsinhabers" werden nicht vom STEP 7-Projekt übernommen.

3.19.7 Gesicherte Kommunikation zwischen CPU und Kommunikationsmodul

Vorgehensweise

Voraussetzungen:

- Unter "Teilnehmernummern" ist die CPU dem Modul zugeordnet.
- Sie sind mit der Rolle "NET Administrator" angemeldet.
- Besonderheit bei ST7:
 - Bei Verwendung von TD7onCPU ist die nachfolgend beschriebene Vorgehensweise nicht erforderlich.

Das Kommunikationszertifikat muss dem Modul, das der CPU zugeordnet ist, zugewiesen werden. Dafür gibt es unterschiedliche Vorgehensweisen:

Verwendung des globalen Zertifikatsmanagers für die CPU

Dabei wird das lokale Kommunikationszertifikat der CPU neu angelegt.

1. Selektieren Sie die CPU: "Schutz & Security > Zertifikatsmanager".
2. Aktivieren Sie das Optionskästchen "Globale Security-Einstellungen für den Zertifikatsmanager verwenden".
3. Nach Bestätigung des nachfolgenden Dialogs wird das Kommunikationszertifikat aus dem Zertifikatsmanager der CPU entfernt.
4. Zum Erstellen eines neuen Kommunikationszertifikats wählen Sie in den allgemeinen Einstellungen das Menü "Schutz & Security > Verbindungsmechanismen".
5. Erstellen Sie unter "PLC-Kommunikationszertifikat" ein neues Kommunikationszertifikat. Klicken Sie dazu rechts auf "...".
6. Klicken Sie im folgenden Fenster auf "Hinzufügen".
7. Bestätigen Sie die Einstellungen im Fenster "Zertifikat erstellen" mit "OK".

Ergebnis: Das Zertifikat ist im Zertifikatsmanager der CPU und im globalen Zertifikatsmanager verfügbar.

Um das Zertifikat dem Modul zuzuordnen:

1. Öffnen Sie in der Projektnavigation "Security-Einstellungen" > "Security-Funktionen" > "Zertifikatsmanager".
2. Wählen Sie das Register "Gerätezertifikate".
3. Klicken Sie mit der rechten Maustaste auf das Kommunikationszertifikat und wählen Sie "Zuordnen".
4. Klicken Sie bei dem Modul, welchem das Zertifikat zugewiesen werden soll, auf das Optionskästchen "Zugewiesen".
5. Wechseln Sie bei "Verwendung" von "Gerätezertifikat" auf "Vertrauenswürdigen Zertifikat".

Das Zuordnen kann auch über den lokalen Zertifikatsmanager des Moduls erfolgen.

Verwendung des lokalen Zertifikatsmanagers der CPU

Das lokale Kommunikationszertifikat der CPU wird direkt verwendet, muss aber über Export und Import dem Kommunikationsmodul zugewiesen werden.

1. Selektieren Sie die CPU und wählen Sie in den allgemeinen Einstellungen das Menü "Schutz & Security > Zertifikatsmanager".
2. Klicken Sie mit der rechten Maustaste auf das Kommunikationszertifikat und wählen Sie "Exportieren".
3. Speichern Sie das Zertifikat.

Um das Zertifikat dem Modul zuzuordnen:

1. Öffnen Sie in der Projektnavigation "Security-Einstellungen" > "Security-Funktionen" > "Zertifikatsmanager".
2. Wählen Sie das Register "Gerätezertifikate".
3. Importieren Sie das Kommunikationszertifikat.
4. Klicken Sie mit der rechten Maustaste auf das Kommunikationszertifikat und wählen Sie "Zuordnen".
5. Klicken Sie bei dem Modul, welchem das Zertifikat zugewiesen werden soll, auf das Optionskästchen "Zugewiesen".
6. Wechseln Sie bei "Verwendung" von "Gerätezertifikat" auf "Vertrauenswürdiges Zertifikat".

Das Zuordnen kann auch über den lokalen Zertifikatsmanager des Moduls erfolgen.

3.19.8 CP 1542SP-1 IRC: Zertifikate zu Telecontrol-Verbindungen mit TLS

Zur Handhabung von Zertifikaten für die Nutzung von TLS für die Telecontrol-Verbindungen siehe Kapitel TIM 1531 IRC: Handhabung der Zertifikate für TLS (Seite 91).

3.20 TIM 1531 IRC: Schutz und Zertifikate

3.20.1 Schutz

Schutzfunktionen

Die Baugruppe bietet verschiedene Zugriffsstufen, um den Zugang zu bestimmten Funktionen einzuschränken.

ACHTUNG

Projektierung einer Zugriffsstufe ersetzt nicht den Know-how-Schutz

Die Projektierung von Zugriffsstufen verhindert unrechtmäßige Änderungen an der Baugruppe, indem die Rechte zum Download eingeschränkt werden.

Bausteine auf einer Speicherkarte sind dadurch aber nicht schreib- oder lesegeschützt. Verwenden Sie den Know-how-Schutz zum Schutz des Codes von Bausteinen auf der Speicherkarte.

Die Tabelle der Zugriffsstufen

Die Projektierung der Zugriffsstufen nehmen Sie in der Tabelle vor. Die grünen Haken in den Spalten rechts der jeweiligen Zugriffsstufe geben an, welche Operationen maximal möglich sind, ohne das Passwort dieser Zugriffsstufe zu kennen.

Voreingestellt ist die Zugriffsstufe "Vollzugriff (kein Schutz)". Jeder Nutzer kann die Konfiguration lesen und verändern. Ein Passwort ist nicht projektiert und wird auch für den Online-Zugriff nicht benötigt.

Sie können folgende Zugriffsstufen projektieren:

- **Vollzugriff (kein Schutz)**

Die Konfiguration und die Bausteine können von jedem gelesen und verändert werden.

- **Lesezugriff**

Mit dieser Zugriffsstufe ist ohne Angabe des Passwortes nur lesender Zugriff auf die Hardware-Konfiguration und die Bausteine möglich, d. h. Sie können ohne Eingabe des Passwortes keine Bausteine und Hardware-Konfiguration in die TIM laden. Außerdem sind ohne Passwort schreibende Testfunktionen und Firmware-Updates nicht möglich.

- **Kein Zugriff (kompletter Schutz)**

Wenn die Baugruppe komplett geschützt ist, dann ist weder lesender noch schreibender Zugriff auf die Hardware-Konfiguration und die Bausteine möglich.

Wenn Sie die Funktionen nicht markierter Zugriffsstufen nutzen möchten, dann ist die Eingabe eines Passwortes notwendig.

Durch die Legitimation mit dem Passwort erhalten Sie wieder Vollzugriff auf die Baugruppe.

Verhalten einer Passwort-geschützten Baugruppe im Betrieb

Der Schutz der Baugruppe ist wirksam, nachdem die Einstellungen in die Baugruppe geladen wurden.

Vor der Ausführung einer Online-Funktion wird die Zulässigkeit geprüft. Im Falle eines Passwortschutzes werden Sie zur Passworteingabe aufgefordert.

Beispiel:

Die Baugruppe wurde mit Lesezugriff projektiert und Sie wollen die Funktion "Variable steuern" ausführen. Da es sich um einen schreibenden Zugriff handelt, muss zur Ausführung der Funktion das projektierte Passwort eingegeben werden.

Die durch Passwort geschützten Funktionen können zu einem Zeitpunkt nur von einem PG/PC ausgeführt werden. Ein weiteres PG/PC kann sich nicht anmelden.

Die Zugangsberechtigung zu den geschützten Daten gilt für die Dauer der Online-Verbindung oder bis die Zugangsberechtigung manuell über "Online > Zugriffsrechte löschen" wieder aufgehoben wird.

Jede Zugriffsstufe lässt auch ohne Eingabe eines Passwortes den uneingeschränkten Zugriff auf bestimmte Funktionen zu, z. B. Identifikation über die Funktion "Erreichbare Teilnehmer".

3.20.2 Zugriffsschutz projektieren

Projektierung

Sie können mehrere Passwörter eingeben und damit unterschiedliche Zugriffsrechte für verschiedene Nutzergruppen einrichten.

Die Passwörter werden in einer Tabelle eingegeben, so dass jedem Passwort genau eine Zugriffsstufe zugeordnet ist.

Wie das Passwort wirkt, steht in der Spalte "Zugriffsstufe".

Beispiel:

Sie wählen die Zugriffsstufe "Kein Zugriff (kompletter Schutz)" für die Baugruppe und geben für jede der in der Tabelle darüber liegenden Zugriffsstufen ein eigenes Passwort ein.

Für Nutzer, die keines der Passwörter kennen, ist die Baugruppe komplett geschützt.

Für Nutzer, die eines der parametrisierten Passwörter kennen, hängt die Wirkung ab von der Tabellenzeile, in der das Passwort steht:

- Das Passwort in Zeile 1 "Vollzugriff (kein Schutz)" wirkt, als wäre die Baugruppe ungeschützt. Nutzer, die dieses Passwort kennen, haben uneingeschränkten Zugriff auf die Baugruppe.
- Das Passwort in Zeile 2 "Lesezugriff" wirkt, als wäre die Baugruppe schreibgeschützt. Trotz Passwort-Kenntnis haben Nutzer, die dieses Passwort kennen, nur lesenden Zugriff auf die Baugruppe.
- Das Passwort in Zeile 3 "Kein Zugriff (kompletter Schutz)" wirkt, als wäre die Baugruppe schreib- und lesegeschützt. Nutzer, die dieses Passwort kennen, haben nur lesenden Zugriff auf die Baugruppe.

Vorgehen

Gehen Sie folgendermaßen vor, um die Zugriffsstufen für die Baugruppe zu parametrieren:

1. Öffnen Sie die Eigenschaften der Baugruppe im Inspektorfenster.
2. Öffnen Sie in der Bereichsnavigation den Eintrag "Schutz".
Eine Tabelle mit den möglichen Zugriffsstufen wird im Inspektorfenster angezeigt.
3. Wählen Sie die gewünschte Zugriffsstufe in der ersten Spalte der Tabelle. Die grünen Haken in den Spalten rechts der jeweiligen Schutzstufe zeigen Ihnen, welche Operationen noch möglich sind, ohne das Passwort einzugeben.
4. Wenn Sie eine andere Zugriffsstufe als "Vollzugriff" gewählt haben:
 - Vergeben Sie in der Spalte "Passwort" in der ersten Zeile (Vollzugriff) ein Passwort für den Vollzugriff.
 - Wiederholen Sie zum Schutz vor Fehleingaben das gewählte Passwort in der Spalte "Passwort bestätigen".
 - Achten Sie darauf, dass das Passwort ausreichend sicher ist, d. h. dass es kein durch eine Maschine erkennbares Muster besitzt!
 - Die Eingabe eines Passwortes in der ersten Zeile "Vollzugriff (kein Schutz)" ist obligatorisch und ermöglicht dem Passwort-Kenner uneingeschränkten Zugriff auf die Baugruppe, unabhängig von der gewählten Schutzstufe.
5. Weisen Sie weiteren Zugriffsstufen nach Bedarf weitere Passwörter zu, falls die gewählte Zugriffsstufe das erlaubt.
6. Laden Sie die Hardware-Konfiguration, damit die Zugriffsstufe wirksam wird.

Ergebnis

Die Hardware-Konfiguration und die Bausteine sind entsprechend der eingestellten Zugriffsstufe vor unberechtigtem Online-Zugriff geschützt. Wenn eine Operation aufgrund der parametrierten Zugriffsstufe nicht ohne Passwort ausgeführt werden kann, wird ein Dialog zur Eingabe eines Passwortes aufgeblendet.

3.20.3 TIM 1531 IRC: Handhabung der Zertifikate für TLS

Secure Communication bei Telecontrol-Modulen

Die unten beschriebene Kommunikation über TLS wird von folgenden Modulen unterstützt:

- TIM 1531 IRC V2.3 ab Firmware-Version V2.3
zusammen mit CPU 1500 ab Firmware-Version V2.9
Einsetzbare Telecontrol-Protokolle: DNP3 und IEC 60870-5-104
- CP 1542SP-1 IRC ab Firmware-Version V2.2
zusammen mit ET 200SP CPU ab Firmware-Version V2.9
Einsetzbare Telecontrol-Protokolle: DNP3 und IEC 60870-5

Die Kommunikationsmodule verwenden TLS 1.2, die Kommunikation entspricht IEC/TS 62351-3.

Kommunikation zwischen CPU und Telecontrol-Modul

CP: Kommunikation über Rückwandbus

Wenn sich CPU und Telecontrol-CP im gleichen Rack befinden, läuft die Kommunikation zwischen ihnen über den Rückwandbus. Die CPU ist dem Telecontrol-CP automatisch zugeordnet.

TIM 1531 IRC: TLS-Kommunikation mit der CPU über Ethernet

Die TIM 1531 IRC wird nicht im Rack der CPU gesteckt, sondern in einem separaten Rack. Die Verbindung zur CPU läuft über Ethernet und verwendet bei allen einsetzbaren Telecontrol-Protokollen Secure Communication über TLS.

Für die Kommunikation über TLS müssen Sie ein neu erstelltes Zertifikat der CPU verwenden und dieses bei der TIM in der Parametergruppe "Teilnehmernummern" angeben. Wenn Sie ein Zertifikat für die CPU erstellen und die TIM der CPU zuweisen, wird das Zertifikat automatisch eingetragen.

Erzeugen des CPU-Zertifikats und Zuordnen der CPU (TIM 1531 IRC)

Voraussetzungen

Zum Erzeugen und Zuweisen von Zertifikaten müssen folgende Voraussetzung erfüllt sein:

- Als STEP 7-Projektbenutzer besitzen Sie mindestens das Recht der Rolle "NET Administrator".
Siehe hierzu "Security-Einstellungen > Benutzer und Rollen > Zugewiesene Rollen".
- Die Geräte haben die erforderliche Mindest-Firmware-Version, siehe oben.
- Die Konfigurationsdaten der CPU sind geschützt.
Siehe hierzu "Schutz & Security > Schutz vertraulicher PLC-Konfigurationsdaten"

Um der TIM 1531 IRC ihre lokale CPU zuordnen zu können, müssen folgende Voraussetzung erfüllt sein:

- CPU und TIM 1531 IRC sind vernetzt.
- Für die TIM ist unter "Kommunikationsarten" das gewünschte Telecontrol-Protokoll aktiviert.

Zertifikat der CPU erzeugen

Zunächst müssen Sie für die CPU ein vom System (Globaler Zertifikatsmanager des STEP 7-Projekts) erzeugtes Zertifikat erstellen. Das lokal erzeugte Zertifikat der CPU kann für die Kommunikation nicht verwendet werden.

Die ID des neu erstellten CPU-Zertifikats wird beim Zuweisen der CPU zur TIM (siehe unten) automatisch an folgenden Stellen eingetragen:

- Im Dialog "Teilnehmernummern" der TIM
- Im Zertifikatsmanager der TIM als Partnerzertifikat

Gehen Sie zum Erzeugen des CPU-Zertifikats folgendermaßen vor:

1. Selektieren Sie bei der CPU die Parametergruppe "Schutz & Security > Zertifikatsmanager > Globale Security-Einstellungen".
2. Aktivieren Sie die Option "Globale Security-Einstellungen für den Zertifikatsmanager verwenden".

Beachten Sie:

Mit der Aktivierung der Option werden vorhandene lokale Zertifikate der CPU gelöscht.

3. Wechseln Sie zu "Schutz & Security > Verbindungsmechanismen > Kommunikation nach TIA Portal und HMI".
4. Klicken Sie in der Zeile "PLC-Kommunikationszertifikat" rechts auf das Symbol für die Auswahlliste.
5. Klicken Sie unterhalb der geöffneten Auswahlliste auf die Schaltfläche "Hinzufügen".

Der Dialog "Zertifikat erstellen" öffnet sich, unter anderem folgenden Optionen:

- Verwendungszweck: TLS Client / Server
- Zertifizierungsstelle (CA): Von Zertifizierungsstelle signiert
- Zertifikatsinhaber: Name der selektierten CPU
- Verschlüsselungsverfahren: EC
- Hash-Algorithmus: sha256

Bei Bedarf können Sie unter "Alternativer Name des Zertifikatsinhabers (SAN)" einen weiteren Adresstyp für die CPU ergänzen.

6. Behalten Sie die Einstellungen bei und klicken Sie auf "OK".

Das neu erstellte TLS-Zertifikat wird bei der CPU in der Tabelle der Gerätezertifikate mit dem Dienst "TlsServer" angezeigt.

7. Öffnen Sie in der Projektnavigation den Globalen Zertifikatsmanager:
Security-Einstellungen > Security-Funktionen > Zertifikatsmanager > Gerätezertifikate"
8. Selektieren Sie das neu erstellte Zertifikat der CPU (ID siehe oben) und öffnen Sie das Kontextmenü "Zuweisen".
9. Selektieren Sie in der Liste diejenige TIM, welcher die CPU zugeordnet werden soll.
10. Klicken Sie in der Spalte "Verwendet als" in die Zelle ("Nicht zugewiesen"), wählen Sie die Option "Vertrauenswürdige Zertifikat" und klicken Sie auf das grüne Häkchen.
11. Schließen Sie den Dialog mit OK.

CPU der TIM 1531 IRC zuweisen

1. Öffnen Sie bei der TIM, die mit der CPU kommunizieren soll, die Parametergruppe "Teilnehmernummern".
2. Klicken Sie in der Zeile "Zugeordnete CPU" rechts auf das Symbol für die Auswahlliste.
Die Liste mit den vernetzten CPUs wird geöffnet.
3. Selektieren Sie die CPU, die der TIM zugeordnet werden soll, und klicken Sie unten auf das grüne Häkchen.
In der Zeile "Zugeordnete CPU" wird der Name der CPU angezeigt.
Gleichzeitig wird in der Zeile "Kommunikationszertifikat" automatisch die ID des zuvor für die CPU erzeugten Zertifikats angezeigt.

Weitere Projektierung

Projektieren Sie anschließend die weiteren Stationen als Kommunikationspartner und die entsprechenden Telecontrol-Verbindungen.

TLS für Telecontrol-Verbindungen

TLS für projektinterne Telecontrol-Verbindungen

Secure Communication über TLS können Sie für Telecontrol-Verbindungen von Kommunikationsmodulen projektieren, die eines der folgenden Protokolle verwenden:

- IEC 60870-5-104
- DNP3

Sie projektieren Secure Communication bei den Telecontrol-Verbindungen (Task Card "TeleControl").

1. Legen Sie zunächst die Telecontrol-Verbindungen an.
2. Selektieren Sie die Hauptverbindung und dort die Parametergruppe "Secure Communication (TLS)".
3. Aktivieren Sie die Option "Secure Communication aktivieren".

Wenn alle Zertifikate der Verbindungspartner vorhanden sind, werden bei Siemens-Geräten die Eigene Zertifikats-ID und die Partner-Zertifikats-ID automatisch in die gesamte Verbindung inklusive der Teilverbindungen übernommen.

TLS für Telecontrol-Verbindungen mit Fremdgeräten

Wenn Sie Secure Communication über TLS für Telecontrol-Verbindungen mit Fremdgeräten verwenden möchten, müssen Sie einige weitere Schritte durchführen.

Sie müssen ein Zertifikat für das Fremdgerät erzeugen, die ID in die Verbindungsparameter übernehmen, das Zertifikat sowie das zugehörige CA-Zertifikat exportieren und in das Fremdgerät importieren.

Legen Sie zunächst die Verbindung wie oben beschrieben an und aktivieren Sie die Option "Secure Communication aktivieren". Gehen Sie im Weiteren wie folgt vor.

Fremdgerät-Zertifikat importieren oder erstellen und zuweisen

Das Fremdgerät-Zertifikat können Sie dem STEP 7-Projekt alternativ zur Verfügung stellen:

- Importieren

Falls vorhanden, können Sie das Zertifikat des Fremdgeräts im Dateisystem der Engineering-Station speichern und importieren.

Zum Importieren öffnen Sie im Globalen Zertifikatsmanager das Register "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen", klicken in eine freie Zeile und öffnen das Kontextmenü "Importieren".

Anschließend müssen Sie das importierte Zertifikat der TIM zuweisen (siehe unten).

- Erstellen

Alternativ können Sie ein Zertifikat für das Fremdgerät in STEP 7 erstellen und in das Fremdgerät importieren.

Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie in der Projektnavigation den Globalen Zertifikatsmanager:

"Security-Einstellungen > Security-Funktionen > Zertifikatsmanager > Gerätezertifikate"

2. Klicken Sie in einer freien Zeile auf das Kontextmenü "Erstellen".

Der Dialog "Zertifikat erstellen" öffnet sich.

3. Wählen Sie für das Zertifikat des Fremdgeräts folgende Optionen:

- Verwendungszweck: TLS Client / Server
- Zertifizierungsstelle (CA): Selbstsigniert
- Zertifikatsinhaber: Geben Sie den Namen des Fremdgeräts ein.

Passen Sie die übrigen Parameter an die Funktionalität des Fremdgeräts an.

Möglich sind beispielsweise:

- Verschlüsselungsverfahren: RSA
- Schlüssellänge: 2048
- Hash-Algorithmus: sha256

4. Schließen Sie den Dialog mit "OK".

Das Zertifikat erscheint in der Tabelle.

Die ID des Zertifikats benötigen Sie für die Zuweisung und die Telecontrol-Verbindung.

5. Selektieren Sie das neu erstellte Zertifikat und öffnen Sie das Kontextmenü "Zuweisen".

6. Selektieren Sie in der Liste diejenige TIM, mit der das Fremdgerät über die Telecontrol-Verbindung kommunizieren soll.

7. Klicken Sie in der Spalte "Verwendet als" in die Zelle ("Nicht zugewiesen"), wählen Sie die Option "Vertrauenswürdige Zertifikat" und klicken Sie auf das grüne Häkchen.

8. Schließen Sie den Dialog mit OK.

Die ID des Zertifikats benötigen Sie für die Telecontrol-Verbindung.

Zertifikate für Fremdgerät exportieren und dort importieren

Wenn Sie das Gerätezertifikat des Fremdgeräts importiert haben, müssen Sie nur das Gerätezertifikat der TIM und das zugehörige CA-Zertifikat exportieren.

Wenn Sie das Gerätezertifikat des Fremdgeräts in STEP 7 erstellt haben, müssen Sie auch dieses exportieren.

Gehen Sie folgendermaßen vor:

1. In STEP 7 erstelltes Gerätezertifikat für das Fremdgerät
 - Öffnen Sie im Globalen Zertifikatsmanager das Register "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen".
 - Selektieren Sie das Gerätezertifikat für das Fremdgerät und klicken Sie auf das Kontextmenü "Zertifikat exportieren".
 - Speichern Sie das Zertifikat im Dateisystem der Engineering-Station.
Das vorgelegte Dateiformat "*.der" können Sie ändern.
Eine Beschreibung der Funktionen der Zertifikats-Dateiformate finden im Hilfesystem im Kapitel "Zertifikate exportieren".
2. Gerätezertifikat der TIM
 - Wechseln Sie im Globalen Zertifikatsmanager in das Register "Gerätezertifikate".
 - Selektieren Sie das Gerätezertifikat der TIM als Partnerzertifikat für das Fremdgerät.
 - Machen Sie die Spalte "Aussteller" völlig sichtbar.
Den Namen des Ausstellers benötigen Sie für den Export des ausstellenden CA-Zertifikats.
 - Exportieren Sie das selektierte Gerätezertifikat der TIM über das Kontextmenü "Zertifikat exportieren".
3. Ausstellendes CA-Zertifikat
 - Wechseln Sie in das Register "Zertifizierungsstelle (CA)".
 - Selektieren Sie das CA-Zertifikat, welches Aussteller für das Gerätezertifikat der TIM ist.
Wenn Sie das CA-Zertifikat aufklappen, werden unterhalb alle abgeleiteten Gerätezertifikate angezeigt, unter anderem auch das der TIM.
 - Exportieren Sie das selektierte CA-Zertifikat über das Kontextmenü "Zertifikat exportieren".
4. Importieren Sie für die Kommunikation zur Laufzeit alle gespeicherten Zertifikate in das Fremdgerät bzw. dessen Projektierungswerkzeug.

Zertifikats-ID in die Telecontrol-Verbindung eintragen

1. Wechseln Sie wieder zur angelegten Telecontrol-Verbindung, Parametergruppe "Secure Communication (TLS)".
2. Tragen Sie bei der Verbindung mit einem Fremdgerät folgende Werte manuell ein:
 - Partner-Zertifikats-ID: ID des importierten oder manuell erstellten Zertifikats für das Fremdgerät
 - Eigene Zertifikats-ID: ID des Zertifikats der TIM

Fahren Sie mit der Projektierung der übrigen Parameter fort.

3.21 Telecontrol-Verbindungen

3.21.1 Telecontrol-Verbindungen

Telecontrol-Verbindungen

Für die Fernwirk-Kommunikation werden Telecontrol-Beziehungen zwischen den beteiligten Kommunikationsmodulen benötigt. Abhängig vom Modultyp und der Firmware-Version nehmen Sie die Projektierung in folgenden Parametergruppen vor:

- Parametergruppe "Partnerstationen"
oder
- Editor "Netzwerkdaten"

Projektierung in der Parametergruppe "Partnerstationen"

Für folgende CPs, die nur als Station fungieren, werden die Beziehungen zur Zentrale-Station bzw. zum Master in der Parametergruppe "Partnerstationen" projektiert:

- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC bis Firmware V3.0
- CP 1542SP-1 IRC bis Firmware V1.0

Alle weiteren Einstellungen, die für die Kommunikation mit der Zentrale-Station benötigt werden, werden aus den weiteren Projektierungsdaten der CPs herangezogen und müssen für die Verbindungen nicht extra projektiert werden.

Projektierung im Editor "Netzwerkdaten"

Für folgende Module projektieren Sie Telecontrol-Verbindungen im Editor "Netzwerkdaten":

- CP 1243-1 / CP 1243-8 IRC ab Firmware V3.1
- CP 1243-7 LTE ab Firmware V3.3
- CP 1542SP-1 IRC ab Firmware V2.0
- TIM 1531 IRC ab Firmware V2.0

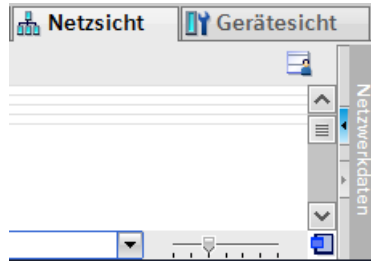
3.21.2 Der Editor "Netzwerkdaten"

Öffnen des Editors "Netzwerkdaten" > Register "TeleControl"

Gehen Sie zum Öffnen des Editors folgendermaßen vor:

1. Öffnen Sie die Netzsicht des Projekts.

Rechts finden Sie den eingeklappten Editor "Netzwerkdaten".



2. Öffnen Sie den Editor "Netzwerkdaten" über das Pfeilsymbol.

Der Editor wird mit mehreren Registern eingeblendet, links das Register "Netzübersicht".

3. Ziehen Sie den Editor soweit heraus, bis das Register "TeleControl" erscheint.

Dieses Register ist weiter unterteilt in folgende Register:

- ST7
- DNP3
- IEC 60870

Wählen Sie je nach genutztem Protokoll das entsprechende Register, um die Telecontrol-Verbindungen zu projektieren.

Anzeigen und Ein-/Ausblenden von Spalten

	Verbindung	Startpunkt	Start-Teiln..	Start-Schnittstelle	Endpunkt	End-...	Partnerliste	End-Schnittstelle/Adresse
	*	*	*		*	*		
	Section_1	1	1	TIM_1 - Ethernet-S.	2	2	2,3	TIM_2 - TIM_2 - Ethernet-S
	Section_2	2	2	TIM_2 - Ethernet-S.	1	1	2,3	TIM_1 - TIM_1 - Ethernet-S
	Section_3	TIM_2	2	TIM_2 - Serial Inter.	3	3	1	TIM_3 - TIM_3 - Serial Inte
	Section_4	3	3	TIM_3 - Serial Inter.	1	1	1	TIM_2 - TIM_2 - Serial Inte
	Section_5	TIM_2	2	TIM_2 - Ethernet-S.	1	1	3, 12	TIM_1 - TIM_1 - Ethernet-S
	Section_6	2	2	TIM_2 - Serial Inter.	3	3	3	TIM_3 - TIM_3 - Serial Inte
	Section_7	3	3	TIM_3 - Serial Inter.	2	2	2	TIM_2 - TIM_2 - Serial Inte
	Section_99	1	1	TIM_1 - Ethernet-S.	Fremdgerät	99	99	192.168.2.99
	Section_8	1	1	TIM_1 - Ethernet-S.	1200	12	12	TIM_2 - TIM_2 - Ethernet-S
	Section_9	TIM_2	2	TIM_2 - Ethernet-S.	1200	12	1	S7-1200-Station_1 - CP 1..
	Section_10	1200	12	CP 1243-8 IRC - Et..	1	1	1	TIM_2 - TIM_2 - Ethernet-S

Bild 3-4 Editor "Netzwerkdaten", Register "Telecontrol > ..."

In der Tabelle "Telecontrol-Verbindungen" können Sie die Spalten anzeigen oder ausblenden, anordnen und die Spaltenbreite optimieren. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um zu dem Kontextmenü zu gelangen.

- Spalten anordnen
Wenn Sie auf einen Spaltenkopf klicken, können Sie die Spalte mit gedrückter linker Maustaste innerhalb der Tabelle verschieben.
- Anzeigen/Verbergen
Über diese Funktion des Kontextmenüs können Sie einzelne Spalten ein- oder ausblenden. Damit lässt sich die Übersichtlichkeit der Tabelle erhöhen.
- Alle Spalten anzeigen
Blendet alle Spalten der Tabelle ein.
- Breite optimieren / Breite aller Spalten optimieren
Über diese Kontextmenüs optimieren Sie die Breite der selektierten Spalte bzw. aller Spalten der Tabelle.
Die Spaltenbreite passt sich an den breitesten Eintrag in dieser Spalte an.

Manche Felder der Tabelle sind editierbar, in anderen projektieren Sie den Parameter über eine Klappliste.

Felder mit fehlender oder fehlerhafter Projektierung werden rot hinterlegt.

Namen der Verbindungen

Sie können die vorbelegten Namen der Verbindungen anpassen.

Erlaubt sind max. 129 Zeichen aus folgenden ASCII-Zeichensätzen (Nummern dezimal):

- **Nr. 32..126**
Leerzeichen , ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~
- **Nr. 128, 130..140, 142, 145..156, 158..159, 161..172**
€ , f „ … † ‡ ^ % ¢ Š ‹ Œ Ž ‘ ’ ’ ’ ’ • — — ~ ™ š › œ ž Ÿ ĳ € £ ¤ ¥ ¦ § ¨ © ª « ¬
- **Nr. 174..255**
® ¯ ° ± ² ³ ´ μ , ¹ º » ¼ ½ ¾ ¿ À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

Fehleranzeigen

Fehlerhafte Verbindungspunkte, Netze oder Parameter werden in den Tabellen rot hinterlegt.

Ursachen für fehlerhafte Verbindungen sind beispielsweise:

- Startpunkt und Endpunkt sind identisch.
- Die Verbindung läuft über ein unzulässiges Netz.
- Die Verbindung läuft über einen unzulässigen Teilnehmer.

Löschen ungültiger oder redundanter Verbindungen

Im Fall von unzulässigen oder unerwünschten redundanten Verbindungen müssen Sie einen Verbindungsweg löschen:

1. Selektieren Sie in der Tabelle "Projektierte Verbindungswege" den nicht erwünschten Verbindungsweg.
2. Klicken Sie auf das Kontextmenü "Löschen".

3.21.3 Verbindungswege festlegen

Regeln für die Verbindungsprojektierung

Beachten Sie folgende Regeln für die Verbindungsprojektierung:

- Verbindungen sind für folgende Netze projektierbar:
 - Verbindungen in Ethernet-Netzen zwischen TIM-Modulen und CPs
 - Verbindungen in klassischen WAN-Netzen (Standleitung / Wählnetz) - nur zwischen TIM-Modulen
- Sie können Verbindungen zwischen Endpunkten (Teilnehmern) anlegen, die im STEP 7-Projekt projiziert sind.

Für die Adressdaten und Schnittstellen-Parameter beider Endpunkte stehen Felder in der Verbindungstabelle zur Verfügung.

- Sie können Verbindungen anlegen zwischen einem Endpunkt des STEP 7-Projekts und einem "Fremdgerät", das nicht in STEP 7 projiziert ist. Das Fremdgerät liegt in einem anderen IP-Subnetz und ist über einen Netzübergang erreichbar.

In diesem Fall projektieren Sie den Netzübergang als Endpunkt der Verbindung.

- Endpunkt einer Verbindung ist immer die CPU oder eine PC-Applikation, nicht das Kommunikationsmodul.

Ausnahme: Fremdgerät

- Für jede Verbindung muss jeweils ein Verbindungs-Abschnitt für den Hinweg und den Rückweg angelegt sein.

Beispiel für eine Verbindung zwischen Partner 1 und 2:

- Verbindungs-Abschnitt 1 \Rightarrow 2
- Verbindungs-Abschnitt 2 \Rightarrow 1

- Sie können einfache und redundante Verbindungen zwischen zwei Teilnehmern projektieren.
- Zwei Verbindungen zu einem Partner über die selbe Schnittstelle eines Moduls sind nicht erlaubt.
- Eine Verbindung über ein inkonsistentes Netz ist ungültig.

Beispiele für inkonsistente Netze:

- Ein Teilnehmer eines Verbindungs-Abschnitts ist mit einem anderen Telecontrol-Protokoll projektiert.
Verbindungen über Knoten, die nicht als Knotenstation projektiert sind.
Teilnehmer mit inkompatiblen Modems
Inkompatible Einstellungen von zwei Modems in einer Verbindung
Inkompatible Einstellungen zwischen Modem- und Netz-Parametern

Schnittstellen-spezifische Projektierung der Verbindungs-Abschnitte

Verbindungen zwischen zwei Endpunkten können über mehrere Teilnehmer laufen.

Ein Verbindungsabschnitt zwischen zwei Teilnehmern kann für mehrere Verbindungen genutzt werden.

Für einzelne Verbindungs-Abschnitte und den beteiligten Schnittstellen der Module können individuelle Einstellungen projektiert werden. Daher werden in der Verbindungstabelle die einzelnen Verbindungs-Abschnitte zwischen den Schnittstellen zweier Teilnehmer in separaten Zeilen angezeigt.

	Verbindung	Startpunkt	Start-Teiln..	Start-Schnittstelle	Endpunkt	End-...	Partnerliste	End-Schnittstelle/Adresse
	*	*	*		*	*		
	Section_1	1	1	TIM_1 - Ethernet-S.	2	2	2,3	TIM_2 - TIM_2 - Ethernet-S
	Section_2	2	2	TIM_2 - Ethernet-S.	1	1	2,3	TIM_1 - TIM_1 - Ethernet-S
	Section_3	TIM_2	2	TIM_2 - Serial Inter.	3	3	1	TIM_3 - TIM_3 - Serial Inte
	Section_4	3	3	TIM_3 - Serial Inter.	1	1	1	TIM_2 - TIM_2 - Serial Inte
	Section_5	TIM_2	2	TIM_2 - Ethernet-S.	1	1	3, 12	TIM_1 - TIM_1 - Ethernet-S
	Section_6	2	2	TIM_2 - Serial Inter.	3	3	3	TIM_3 - TIM_3 - Serial Inte
	Section_7	3	3	TIM_3 - Serial Inter.	2	2	2	TIM_2 - TIM_2 - Serial Inte
	Section_99	1	1	TIM_1 - Ethernet-S.	Fremdgerät	99	99	192.168.2.99
	Section_8	1	1	TIM_1 - Ethernet-S.	1200	12	12	TIM_2 - TIM_2 - Ethernet-S
	Section_9	TIM_2	2	TIM_2 - Ethernet-S.	1200	12	1	S7-1200-Station_1 - CP 1..
	Section_10	1200	12	CP1243-8 IRC - Et..	1	1	1	TIM_2 - TIM_2 - Ethernet-S

Bild 3-5 Editor "Netzwerkdaten", Register "Telecontrol > ...

Anlegen von Verbindungen und Suche der Verbindungswege

Gehen Sie zum Anlegen von Verbindungen folgendermaßen vor:

1. Klicken Sie in der nächsten freien Zeile auf das Feld "Startpunkt".

Eine Klappliste mit den verfügbaren Endpunkten wird aufgeblendet.

Die erste Zeile unterhalb des Tabellenkopfs ist zur Eingabe von Filtern reserviert, siehe Kapitel Verbindungstabelle (Seite 104).

2. Wählen Sie aus der Tabelle den Startpunkt (CPU) per Doppelklick aus.

3. Klicken Sie in der gleichen Zeile auf das Feld "Endpunkt".

Wählen Sie aus der Tabelle den Endpunkt (CPU oder PC-Applikation) per Doppelklick aus.

- Sonderfall "Fremdgerät":

Wenn Sie statt eines Endpunkts aus dem STEP 7-Projekt ein Fremdgerät als Endpunkt anlegen möchten, dann lassen Sie den voreingestellten Eintrag "Fremdgerät" in der Zelle stehen.

Projektieren die Schnittstelle des Startpunkts sowie die Adresdaten und weiteren Parameter des Fremdgeräts durch Eingabe in die entsprechenden Felder.

Bei einem Fremdgerät als Endpunkt ist die nachfolgend beschriebene Verbindungssuche über den Dialog deaktiviert.

Nach Auswahl eines Endpunkts aus dem STEP 7-Projekt werden der Startpunkt und Endpunkt in der Tabellenzeile angezeigt. Die übrigen Felder sind in der Regel leer und rot hinterlegt.

Nach dem Anlegen einer Verbindung steht noch nicht in jedem Fall der tatsächliche Verbindungsverlauf fest. Insbesondere bei größeren Netzen sind häufig mehrere Verbindungswege möglich.

Für eine erleichterte Suche des Verbindungswegs steht die Suchfunktion über das Symbol "Neuen Verbindungsweg hinzufügen" zur Verfügung:



4. Lassen Sie die Tabellenzeile mit dem ausgewählten Start- und Endpunkt selektiert und klicken Sie auf das Symbol "Neuen Verbindungsweg hinzufügen".

Der Dialog zum Festlegen der Verbindungswege öffnet sich:

Dialog "Verbindungswege hinzufügen"

Die möglichen Verbindungswege werden automatisch gesucht, erkennbar am Laufbalken unten im Dialog.







- Status und Ergebnis der Suche werden unten im Feld "Informationen" ausgegeben.
- Die gefundenen Verbindungswege werden in der oberen Tabelle "Selektieren Sie einen Verbindungsweg..." angezeigt.
- Zu einem selektierten Verbindungsweg werden Details in der Tabelle "Verbindungsweg" eingeblendet.
- Bei Selektion eines Verbindungswegs wird in der Tabelle "Vorschau" angezeigt, welche Verbindungspunkte des selektierten Verbindungswegs in den Verbindungseditor übernommen werden, wenn Sie auf "Hinzufügen" klicken.

5. Selektieren Sie den bzw. die gewünschten Verbindungswege.
- Wenn ein oder mehrere Verbindungswege in der oberen Tabelle angezeigt werden, dann selektieren Sie den gewünschten Verbindungsweg und klicken auf "Hinzufügen".
Unter "Informationen" wird angezeigt, ob der Verbindungsweg hinzugefügt wurde oder ob er bereits projektiert ist.
 - Wenn Sie eine redundante Verbindung nutzen möchten, dann selektieren Sie einen zweiten Weg und klicken auf "Hinzufügen".
Schließen Sie den Dialog über die Schaltfläche "Schließen", wenn die hinzugefügten Verbindungswege den Projektvorgaben entsprechen.
 - Wenn keine Verbindung in der Tabelle angezeigt wird, liegt ein Projektierungsfehler in den zugehörigen Stationen oder Netzen vor.
Schließen Sie in diesem Fall den Dialog über die Schaltfläche "Schließen" und vervollständigen Sie die Projektierung.

Bei der Prüfung der Verbindungswege unterstützt Sie die Tabelle "Verbindungsweg". Für jede projektierte Verbindung wird hier der detaillierte Verbindungsweg angezeigt.

In der Spalte "Position" wird ein Stationssymbol mit einer Kennung für den Verbindungspunkt angezeigt. Die Farbe der Kennung kennzeichnet die Gültigkeit des Verbindungspunkts:

- Blau: Gültiger Verbindungspunkt
- Rot: Ungültiger Verbindungspunkt

Symbol	Bedeutung
	Startpunkt
	Knoten-Eingang
	Knoten-Ausgang
	Endpunkt
 	Beispiele für ungültige Verbindungspunkte

Parameter der Verbindungstabelle

Projektieren Sie die Parameter der Verbindungstabelle für jeden Verbindungs-Abschnitt. Die Beschreibung der Parameter finden Sie im Kapitel Verbindungstabelle (Seite 104).

Unterhalb der Verbindungstabelle finden Sie im Inspektorfenster das Register "Eigenschaften", welches zu jedem Verbindungs-Abschnitt weitere Parameter anzeigt.

Register "Eigenschaften" der Verbindungen

In den Parametergruppen können Sie jeden Verbindungs-Abschnitt prüfen, ggf. korrigieren und weitere Eigenschaften projektieren.

Die Beschreibung der Parametergruppen finden Sie im Kapitel Parameter der IEC-Verbindungen (Seite 107).

3.21.4 Verbindungstabelle

Filter

Die erste Zeile unter dem Tabellenkopf enthält eine Filterfunktion, mit der Sie die Auswahl der projektierbaren Teilnehmer und Verbindungsmöglichkeiten einschränken können. Dadurch werden die Kombinationsmöglichkeiten verringert und die Übersichtlichkeit erhöht.

Wenn Sie einige Verbindungsabschnitte angelegt haben, aktivieren Sie den Filter, indem Sie einen sich wiederholenden Namen oder Teilnamen in die Filterzelle eintippen. Die Zelle wird farbig hinterlegt, siehe Abbildung.






	Verbindung	Startpunkt	Start-Teiln..	Start-Schnittstelle	Endpunkt	End-...	Partnerliste
	*	1	*		*	*	
	Section_1	1	1	TIM_1 - Ethernet-Schnitts.	2	2	2,3
	Section_99	1	1	TIM_1 - Ethernet-Schnitts.	Fremdgerät	99	99
	Section_8	1	1	TIM_1 - Ethernet-Schnitts.	1200	12	12
	Section_10	1200	12	CP1243-8 IRC - Ether..	1	1	1

Bild 3-6 Verbindungstabelle

In der Spalte "Startpunkt" ist der Filter "1" gesetzt.


Beispiel:

Sie haben Verbindungen mit den Startpunkten "1200", "1" und "2" angelegt.

Bei Eingabe von "1" in die Filterzelle werden in der Tabelle nur die Abschnitte eingeblendet, deren Startpunkte mit diesem Teil-String beginnen: "1" und "1200"

Gesetzte Filter in mehreren Spalten multiplizieren sich.

Die Auswahl "*" blendet alle vorhandenen Verbindungsabschnitte ein.

Das Filtersymbol links in der ersten Zeile () blendet einen vorhandenen Filter ein bzw. wieder aus.

Der Filter ist anwendbar auf alle Spalten, deren erste Zelle einen Stern (*) enthält.

Beachten Sie:

Wenn Sie Verbindungen angelegt haben und einen Filter setzen, können Sie keine neuen Verbindungen anlegen. Zum Anlegen neuer Verbindungen müssen Sie den Filter zuerst zurücksetzen.

Parameter

Soweit Parameter bereits durch die Projektierung belegt sind, werden die Werte in die jeweiligen Spalten übernommen.

- **Name**

Sie können den vorgelegten Namen des Verbindungsabschnitts zwischen zwei Teilnehmern anpassen.

Siehe hierzu Kapitel Der Editor "Netzwerkdaten" (Seite 98).

- **Startpunkt**

Wählen Sie aus der Klappliste den gewünschten Startpunkt der Verbindung aus.

- Startpunkt einer Verbindung ist jeweils eine CPU.

- **Start-Teilnehmer**
Stationsadresse des Startpunkts
 - **Start-Schnittstelle**
Schnittstelle des Startpunkt-Moduls, über welche die Verbindung läuft.
 - **Endpunkt**
Wählen Sie den Endpunkt der Verbindung aus.
Endpunkte einer Verbindung können sein:
 - Eine CPU
 - Ein FremdgerätDen Netzknotentyp von Fremdgeräten projektieren Sie im Eigenschaftendialog der Verbindung, siehe Kapitel Fremdgerät-Parameter (Seite 115).
-

Hinweis**Ändern des Endpunkts**

Wenn Sie den Endpunkt einer Verbindung nachträglich ändern, dann werden bei der Suche des Verbindungswegs die neuen Verbindungsabschnitte hinzugefügt.

Beachten Sie, dass die Abschnitte der vorherigen Verbindung bestehen bleiben. Löschen Sie diese selbst.

- **End-Teilnehmer**
Stationsadresse des Endpunkts
 - **Partnerliste**
Bei Auswahl eines Partners (Endpunkts), der im STEP 7-Projekt liegt, wird dessen Stationsadresse bei der Verbindungssuche automatisch gefunden und in die Partnerliste eingetragen.
In Verbindungs-Abschnitte, die für mehrere Verbindungen genutzt werden, wird die Stationsadressen von allen Zielteilnehmern eingetragen.
-

Hinweis**Manuelle Eintragung bei Fremdgerät**

Bei einem Fremdgerät, das nicht im STEP 7-Projekt projektiert ist, müssen Sie die Stationsadresse manuell eintragen.

Die Stationsadressen werden Komma-separiert eingetragen.

- **End-Schnittstelle/Adresse**
Schnittstelle des Endpunkt-Moduls, über welche die Verbindung läuft.
Bei einem Fremdgerät, das nicht im STEP 7-Projekt projektiert ist, müssen Sie die IP-Adresse (Ethernet) oder Telefonnummer (Wählnetz) des Partners manuell eintragen.

- **End-Port**

Relevant für Fremdgerät (Master / Station)

Nummer des Listener-Ports des Partners

Bei Modulen des STEP 7-Projekts wird der Wert aus der Projektierung übernommen. Er ist änderbar.

Bei Fremdgeräten müssen Sie die Portnummer eintragen.

Wertebereich: 0 ... 65535

Vorbelegung: 2404

- **Partnerüberwachungszeit**

Relevant für alle Teilnehmertypen

Wenn das Stations-Modul innerhalb der projektierten Zeit kein Lebenszeichen vom Master auf Applikationsebene empfängt, stuft es die Verbindung als gestört ein und baut die Verbindung ab.

Das Master-Modul erwartet nach dem Senden von Daten innerhalb der projektierten Zeit eine Antwort von der Station.

Hinweis

Redundante Verbindungswege

Wenn Sie redundante Verbindungswege zwischen zwei Partnern projektieren, dann projektieren Sie für beide Wege die gleiche Zeit.

Wertebereich: 0 ... 65535

Bei 0 (Null) ist die Funktion abgeschaltet.

- **Spontan**

Der Parameter für den Übertragungsmodus legt fest, ob ASDUs (Ereignisse) der Station spontan über diesen Verbindungsabschnitt gesendet werden dürfen.

Wertebereich:

- Ja

Das Modul darf spontane ASDUs senden (cause of transmission <3>).

- Nein

Das Modul sendet keine spontanen ASDUs.

Vorbelegung: Ja

Hinweis

Kollisionen bei Vollduplex-Standleitungen

Bei Anschluss einer seriellen Schnittstelle an eine Standleitung mit der Verbindungsart "halbduplex" müssen Sie Spontane Übertragung deaktivieren.

Zur Vermeidung von Kollisionen sollten Sie Spontane Übertragung auch bei Anschluss an Vollduplex-Multidrop-Standleitungen deaktivieren.

- **Polling-Modus**

Relevant für Master, Fremdgerät (Master)

Hier legen Sie den Modus fest, nach dem die Zentrale die Station aufruft.

Der bei der Station projektierte Wert wird an die Zentrale übermittelt und dort gespeichert.

Wertebereiche:

- Zyklisch

Die Station wird zyklisch aufgerufen. Die Zeitdauer des Polling-Zyklus wird aus dem Parameter "Klasse-0-Polling-Intervall" berechnet, siehe oben.

- Nach Anlauf

Die Station wird nur nach dem ersten Anlaufen und nach einem Neustart aufgerufen.

Wenn für eine Station keine spontane Übertragung aktiviert ist, werden bei Auswahl dieser Option keine Daten im laufenden Betrieb übertragen.

- **Temporär**

Partner mit aktivierter Option "Temporär" werden als "erreichbar" eingestuft, wenn sie selbst die Verbindung abbauen (bspw. RTU3000C).

Parameter für redundante Verbindungswege

Im Fall, dass redundante Verbindungswege projektiert sind, werden diese ebenso projektiert wie die Hauptwege.

Die Parameter der redundanten Verbindungswege sind ausgezeichnet durch den folgenden Suffix:

- *** (red)**

Die Parameter der redundanten Verbindungswege haben die entsprechenden Funktionen wie diejenigen für den Hauptweg. Zur Bedeutung siehe oben.

Beispiele:

- **Start-Schnittstelle (red.)**

Schnittstelle des Startpunkt-Moduls, über welche die redundante Verbindung läuft.

- **End-Schnittstelle (red.)**

Schnittstelle des Endpunkt-Moduls, über welche die redundante Verbindung läuft.

3.21.5 Parameter der IEC-Verbindungen

3.21.5.1 Allgemein

Wenn Sie in der Tabelle "Telecontrol-Verbindungen" im Editor "Netzwerkdaten" eine Verbindung selektieren, werden im Register "Eigenschaften" des Inspektorfensters weitere Parametergruppen zu dieser Verbindung angezeigt.

In den Parametergruppen können Sie die Verbindung prüfen, ggf. korrigieren und weitere Eigenschaften projektieren.

Allgemein

- **Verbindung**
Zeigt den Namen der Verbindung und das Protokoll an.
Den Verbindungsnamen können Sie auch hier verändern.
- **Verbindungsendpunkte**
Zeigt die wichtigsten Parameter der Verbindung an.
Die Stationsadresse eines Fremdgeräts können Sie auch hier verändern.

3.21.5.2 TCP-Verbindungsüberwachung

Ethernet-Schnittstelle > Erweiterte Optionen > TCP-Verbindungsüberwachung

Die Einstellungen der beiden Parameter an der Ethernet-Schnittstelle gelten übergeordnet für TCP-Verbindungen über diese Schnittstelle.

Sie können die Parameter in den Eigenschaften der Telecontrol-Verbindungen für jeden Verbindungsabschnitt anpassen.

- **TCP-Verbindungs-Überwachungszeit**

Funktion: Wenn innerhalb der TCP-Verbindungs-Überwachungszeit kein Datenverkehr stattfindet, sendet das Modul ein Keep-alive-Telegramm an den Kommunikationspartner.

Bei 0 (Null) ist die Funktion deaktiviert.

Voreinstellung: 180 s

Zulässiger Bereich

- TIM 1531 IRC
1...65535 s
- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
- CP 1542SP-1 IRC
0...32767 s

- **TCP-Keep-alive-Überwachungszeit**

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

Bei 0 (Null) ist die Funktion deaktiviert.

Voreinstellung: 10 s

Zulässiger Bereich

- TIM 1531 IRC
1...65535 s
- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
- CP 1542SP-1 IRC
0...32767 s

Wenn Sie eine redundante Verbindung zu einem Partner projektiert haben, sind die Parameter für beide Verbindungswege separat einstellbar.

3.21.5.3 IEC 60870-5 Security-Optionen

Secure Authentication

Bei aktivierter Security-Funktion authentifizieren sich IEC-Master und Station durch einen geheimen Schlüssel, dem Pre-shared Key.

Mithilfe des gemeinsamen Pre-shared Key werden nach dem ersten Verbindungsaufbau zwischen Master und Station Sitzungsschlüssel vereinbart, die danach zyklisch erneuert werden. Die Initiative für die Erneuerung der Sitzungsschlüssel geht vom Master aus. Die Kriterien für die Schlüsselerneuerung werden in folgenden Parametern festgelegt.

- Schlüsselaustauschintervall
- Authentifizierungsanfragen vor Schlüsselaustausch

Sobald eine dieser beiden Bedingungen erfüllt ist, wird der Sitzungsschlüssel erneuert.

Parameter

- **IEC-Security-Optionen aktivieren**

Aktivieren Sie die Option, wenn Sie Secure Authentication nutzen möchten.

Hinweis:

Achten Sie darauf, dass Sie die Option bei allen Verbindungen des Moduls, die diese Funktion verwenden sollen, aktivieren.

- **Security-Statistik**

Gibt an, ob die Statistik von Security-Ereignissen an den Master gesendet werden. Security-Ereignisse sind Authentifizierungsanfragen des Masters an das Stations-Modul. Bei Aktivierung der Option werden alle Authentifizierungsanfragen mit Datum, Zeit und

Ergebnis im Stations-Modul gespeichert und zur weiteren Auswertung an den Master gesendet.

Security-Statistik-Ereignisse werden nur ausgegeben, wenn ein SCADA-System an den Master angeschlossen ist.

Wertebereich:

- Keine Security-Statistik senden
- Security-Statistik senden

Bei aktivierter Option werden die auswählbaren Statistik-Parameter unterhalb der Tabelle zur Projektierung freigegeben.

Voreinstellung: Keine Security-Statistik senden

- **Secure Hash-Algorithmus (SHA)**

Auswahl des Secure Hash Algorithm (SHA)

Wertebereich:

- SHA-256

- **Schlüssellänge**

Angabe der Länge des Pre-shared Key in Byte.

In Abhängigkeit des Key-Wrap-Algorithmus werden folgende Längen verwendet:

- 32 Byte

- **Max. Anzahl an Schlüsselstatus-Anfragen**

Wenn die hier projektierte Anzahl an Schlüsselstatus-Anfragen eines Masters innerhalb des Schlüsselaustauschintervalls überschritten wird, alarmiert das Modul alle anderen verbundenen Master-Stationen. Diejenige Master-Station, von der die Anfragen gestellt wurde, wird nicht alarmiert."

trägt das Modul eine Meldung in den Diagnosepuffer der CPU ein.

Wertebereich: 2...255. Voreinstellung: 5

- **Authentifizierungsanfragen vor Schlüsselaustausch**

Maximale Anzahl an Authentifizierungsanfragen des Moduls beim Master. Wenn diese Anzahl erreicht ist, wird der Sitzungsschlüssel erneuert.

Wertebereich: 1...10000. Voreinstellung: 1000

Empfehlung: Stellen Sie die Anzahl beim Stations-Modul doppelt so hoch ein wie beim Master.

- **Schlüsselaustauschintervall**

Zeitraum, nach dem der Schlüssel zwischen Stations-Modul und Master neu ausgetauscht wird. Das Intervall muss bei beiden Kommunikationspartnern aufeinander abgestimmt sein.

Wertebereich: 0...65535 min. Bei 0 (Null) wird der Schlüssel nie getauscht (Funktion abgeschaltet). Voreinstellung: 15 min.

Empfehlung: Stellen Sie das Schlüsselaustauschintervall beim Stations-Modul doppelt so hoch ein wie beim Master.

- **Authentifizierungs-Timeouts**

Maximale Wartezeit des Moduls nach einer Authentifizierungsanfrage beim Master. Bei Überschreitung der Wartezeit auf die Antwort des Masters generiert das Modul ein Security-Ereignis und sendet dieses an den Master.

Wertebereich: 1... 65535 s. Voreinstellung: 5
- **Authentifizierung und Datenlänge für Schlüsselstatus-Challenge**

Datenlänge (CLN) einer Authentifizierungs-Challenge oder Sitzungsschlüssel-Status-Challenge

Wertebereich: 1... 65535 s. Voreinstellung: 4
- **Max. Anzahl an Authentifizierungsfehlern**

Maximale Anzahl an Authentifizierungsfehlern, bevor der Challenger eine Fehlermeldung sendet und der Sitzungsschlüssel geändert wird.

Wertebereich: 1... 65535 s. Voreinstellung: 25
- **Max. Anzahl gesendeter Fehlertelegramme**

Maximale Anzahl gesendeter Fehlermeldungen. Bei Erreichen der projektierten Anzahl stellt die Station das Senden von Fehlermeldungen ein.

Wertebereich: 1... 65535 s. Voreinstellung: 100
- **Max. Anzahl an Schlüssel-Änderungen**

Maximale Anzahl an Sitzungsschlüssel-Änderungen wegen Authentifizierungsfehlern. Bei Erreichen der projektierten Anzahl werden Sitzungsschlüssel-Änderungen wegen Authentifizierungsfehlern solange eingestellt, bis der Sitzungsschlüssel aus einem anderen Grund geändert wird.

Wertebereich: 1... 65535 s. Voreinstellung: 50
- **Max. Anzahl an Antwort-Timeouts**

Beim Master: Maximale Anzahl an Antwort-Timeouts

Bei Erreichen des projektierten Werts bricht der Master die aktuelle Aktion ab.

Wertebereich: 1... 65535 s. Voreinstellung: 20
- **Max. Anzahl Schlüssel-Änderungen wegen Neustart**

Beim Master: Maximale Anzahl an Schlüsselaustauschen wegen Neustart der Station

Bei Erreichen des projektierten Werts sendet der Master bis zum nächsten Schlüsseländerungs-Timeout keine Sitzungsschlüssel mehr an die Station.

Wertebereich: 1... 65535 s. Voreinstellung: 20

- **Pre-shared Key**

Der Pre-shared Key kann auf zwei Wegen projektiert werden:

- Manuelle Projektierung

Geben Sie den Pre-shared Key in STEP 7 manuell als Hexadezimalwert ein.

- Import als Datei

Importieren Sie den Pre-shared Key aus dem Dateisystem der Engineering-Station, wenn der Pre-shared Key vom Master oder einem anderen System erzeugt worden ist.

Der Pre-shared Key des Stations-Moduls muss identisch sein mit dem Pre-shared Key des Masters.

Siehe auch

Security-Statistik-Optionen (IEC 60870-5-104) (Seite 112)

3.21.5.4 Security-Statistik-Optionen (IEC 60870-5-104)

Security-Statistik (IEC 60870-5-104)

Die Statistik-Parameter werden zur Projektierung freigegeben, wenn die Option "Security-Statistik senden" der Security-Basis-Optionen aktiviert ist.

Die nachfolgende Tabelle enthält diejenigen Security-Statistik-Optionen gemäß IEC/TS 60870-5-7 und IEC/TS 62351-5, die Sie für die einzelnen Telecontrol-Verbindungsabschnitte projektieren können.

Bei aktivierten Optionen sendet Kommunikationsmodul als Station Security-Statistik-Ereignisse an den Master. Dort stehen Sie zur weiteren Auswertung zur Verfügung. Anhand der Häufigkeit dieser Ereignisse können Sie Rückschlüsse auf eventuelle Angriffe oder Schwachstellen Ihres Systems ziehen.

Die Security-Statistik-Ereignisse werden nur ausgegeben, wenn ein SCADA-System an den Master angeschlossen ist.

Security-Statistik-Optionen

Eine Station führt bei Verwendung von Secure Authentication für verschiedene Werte eine Statistik.

Die Ereignisse werden über den ASDU-Typ "Information 41" (integrated total for the statistic) übertragen.

Die nachfolgende Tabelle listet die vom Modul unterstützten Statistik-Parameter gemäß IEC/TS 62351-5 auf.

- **Schwellenwert**
Für jeden Statistikwert kann ein Schwellenwert projektiert werden, bei dessen Überschreitung eine Übertragung als Ereignis zum Partner ausgelöst wird.
Der Wertebereich liegt jeweils bei 0...65535.
Bei 0 (Null) ist die Funktion abgeschaltet, für den jeweiligen Wert werden keine Statistikdaten übertragen.
- **IOA**
Jedem Wert in der Statistik müssen Sie eine IOA-Adresse (IOA - Information object address) über die Projektierung zuweisen.
Der Wertebereich liegt jeweils bei 0...16777215.

Für die kritischen Telegramme können Sie unterhalb der Tabelle projektieren, welche ASDU-Typen als kritisch eingestuft werden sollen.

Parameter	Vorbelegung
Schwellenwert Unerwartete Telegramme	3
Unerwartete Telegramme (IOA)	0
Schwellenwert Autorisierungsfehler	5
Autorisierungsfehler (IOA)	0
Autorisierungsfehler (IOA)	5
Authentifizierungsfehler (IOA)	0
Schwellenwert Antwort-Timeouts	3
Antwort-Timeouts (IOA)	0
Schwellenwert Schlüssel-Änderungen wegen Authentifizierungsfehler	3
Schlüssel-Änderungen wegen Authentifizierungsfehler (IOA)	0
Schwellenwert Gesendete Telegramme (gesamt)	100
Gesamtanzahl gesendeter Telegramme (IOA)	0
Schwellenwert Empfangene Telegramme (gesamt)	100
Gesamtanzahl empfangener Telegramme (IOA)	0
Schwellenwert Gesendete kritische Telegramme	100
Gesendete kritische Telegramme (IOA)	0
Schwellenwert Empfangene kritische Telegramme	100
Empfangene kritische Telegramme (IOA)	0
Schwellenwert Verworfen Telegramme	10
Verworfen Telegramme (IOA)	0
Schwellenwert Gesendete Fehlertelegramme	10
Gesendete Fehlertelegramme (IOA)	0
Schwellenwert Empfangene Fehlertelegramme	10
Empfangene Fehlertelegramme (IOA)	0
Schwellenwert Erfolgreiche Authentifizierungen	100
Schwellenwert Erfolgreiche Authentifizierungen	0
Schwellenwert Sitzungsschlüssel-Änderungen	10
Sitzungsschlüssel-Änderungen (IOA)	0
Schwellenwert Fehlgeschlagene Sitzungsschlüssel-Änderungen	5
Fehlgeschlagene Sitzungsschlüssel-Änderungen (IOA)	0

Optionale kritische Funktionen

Die Zeile "Kritische Funktionen" listet die Nummern aller ASDU-Typen auf, die als kritisch eingestuft werden. Sie werden für die Statistik der folgenden Parameter verwendet:

- Empfangene kritische Telegramme
- Gesendete kritische Telegramme

Über die Klappliste der Zeile "Kritische Funktionen" können Sie die einzelnen ASDU-Typen für die Einstufung als 'kritisch' aktivieren bzw. deaktivieren.

3.21.5.5 Abfrageoptionen

Die folgenden Parameter finden Sie in den Parametergruppen "Optionen 1. Weg" / "Optionen 2. Weg" der IEC-Verbindungen.

Aufruf-Intervalle

Die nachfolgenden Parameter legen für die Station die Intervalle von speziellen Aufrufen des Masters fest (cause of transmission 20 - 41).

Alle Parameter werden als Vielfaches des "Polling-Basisintervalls" projiziert, siehe Kapitel Einstellungen IEC-Master (Seite 58).

- **Intervall für Generalabfrage**
Legt das Intervall fest, mit dem Generalabfragen des Masters beantwortet werden.
- **Intervall für Gruppenabfrage**
Legt das Intervall fest, mit dem die jeweilige Gruppenabfrage des Masters beantwortet werden.
- **Intervall für Zähler-Generalabfrage**
Legt das Intervall fest, mit dem Zähler-Generalabfragen des Masters beantwortet werden.
- **Intervall für Zähler-Gruppenabfrage**
Legt das Intervall fest, mit dem die jeweilige Zähler-Gruppenabfrage des Masters beantwortet werden.

Die Einstellung, ob auf eine Generalabfrage geantwortet wird, und die Zuordnung zu einer Gruppenabfrage legen Sie für jeden einzelnen Datenpunkt in der Datenpunktprojektierung fest.

3.21.5.6 Fremdgerät-Parameter

Fremdgerät-Parameter

Nur gültig für Partner, die nicht im STEP 7-Projekt projiziert werden.

- **Partner-Stationsadresse / Stationsadresse (red.)**

Stationsadresse (ASDU-Adresse) des Fremdgeräts, das über eine Verbindung bzw. über einen redundanten Verbindungsweg erreichbar ist.

- **Netzknotentyp Fremdgerät / Netzknotentyp Fremdgerät (red.)**

Legen Sie den Netzknotentyp des Fremdgeräts, das über eine Verbindung bzw. über einen redundanten Verbindungsweg erreichbar ist, fest:

- Zentrale-Station
(Master)

- Knotenstation

Bei Modulen, die als Knotenstation fungieren, gilt:

Die Schnittstelle in Richtung Zentrale wird als "Knotenstation" projiziert.

Die Schnittstelle in Richtung unterlagertes Netz wird als "Zentrale" projiziert.

- Station

3.22 Datenpunkte

3.22.1 Datenpunktprojektierung

Datenpunkt-bezogene Kommunikation mit der CPU

Zur Übertragung von Nutzdaten zwischen Station und Kommunikationspartner ist bei Telecontrol-Modulen mit Datenpunktprojektierung kein Anlegen von Programmbausteinen erforderlich.

Die Datenbereiche im Speicher der CPU, welche für die Kommunikation mit dem Kommunikationspartner vorgesehen sind, werden Datenpunkt-bezogen im Modul projiziert. Dabei ist jeder Datenpunkt mit einer PLC-Variable oder der Variable eines Datenbausteins verknüpft.

Voraussetzung: Angelegte PLC-Variablen und/oder Datenbausteine (DBs)

Voraussetzung für die Projektierung der Datenpunkte sind die entsprechend angelegten PLC-Variablen bzw. DBs in der CPU.

 **WARNUNG**

Schreiben von Werten in Ausgänge

- PLC-Variablen

Beachten Sie bei Referenzierung auf PLC-Variablen, dass bei schreibenden Zugriff die Werte sofort in die Ausgänge der CPU geschrieben werden, ohne zuvor vom Anwenderprogramm bearbeitet zu werden.

Das Schreiben von Werten hat unmittelbaren Einfluss auf den Prozess.

- DB-Variablen

Bei Referenzierung auf DB-Variablen werden geschriebene Werte erst bei Bearbeitung durch das Anwenderprogramm verwendet.

Die PLC-Variablen für die Datenpunktprojektierung können in der Standard-Variablen-tabelle oder in einer benutzerdefinierten Variablen-tabelle angelegt werden. Alle PLC-Variablen, welche für die Datenpunktprojektierung verwendet werden sollen, müssen mit dem Attribut "Sichtbar in HMI" ausgezeichnet sein.

Adressbereiche der PLC-Variablen sind Eingangs-, Ausgangs- oder Merkerbereiche in der CPU.

Hinweis

Anzahl der PLC-Variablen

Beachten Sie die maximal mögliche Anzahl der für die Datenpunktprojektierung verwendbaren PLC-Variablen.

Die Formate und S7-Datentypen der PLC-Variablen, welche mit den Datenpunkttypen der Module kompatibel sind, finden Sie im Kapitel Datenpunkttypen (Seite 123).

Zugriff auf die Speicherbereiche der CPU

Die Werte der von den Datenpunkten referenzierten PLC-Variablen bzw. DBs werden gelesen und durch das Modul an den Kommunikationspartner übertragen.

Vom Kommunikationspartner empfangene Daten werden durch das Modul über die PLC-Variablen bzw. DBs in die CPU geschrieben.

Projektierung der Datenpunkte und Nachrichten in STEP 7

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

- Selektion der Kommunikationsbaugruppe
Kontextmenü "Datenpunkt- und Nachrichten-Editor öffnen"
- Über die Projektnavigation:
Projekt > Verzeichnis der jeweiligen Station > Lokale Baugruppen > gewünschte Kommunikationsbaugruppe
Durch Doppelklick auf den Eintrag öffnet sich der Datenpunkt- bzw. Nachrichten-Editor.

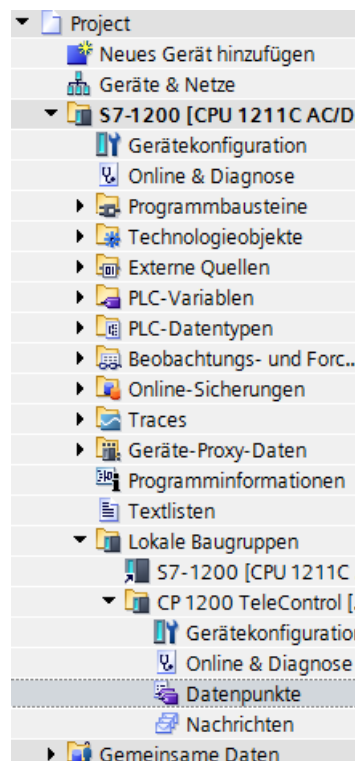


Bild 3-7 Projektierung der Datenpunkte und Nachrichten

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



Bild 3-8 Umschaltung zwischen den zwei Editoren

Anlegen von Objekten

Bei geöffnetem Datenpunkt- bzw. Nachrichten-Editor legen Sie ein neues Objekt (Datenpunkt / Nachricht) an, indem Sie in die erste Tabellenzeile mit dem grauierten Eintrag "<Objekt hinzufügen>" doppelklicken.

Ein vorgelegter Name wird in die Zelle geschrieben. Den Namen können Sie nach Ihren Bedürfnissen anpassen, er muss aber innerhalb des Moduls eindeutig sein.

	Name	PLC-Variablen
1	DataPoint	"Tag_1-BI"
2	DataPoint_1	"Tag_2-BQ"
3	DataPoint_2	"Tag_1-BI"



Bild 3-9 Datenpunkt-Tabelle

Die weiteren Eigenschaften eines jeden Objekts projektieren Sie über die Klapplisten der weiteren Tabellenspalten und über die unten eingeblendeten Parameterfelder.

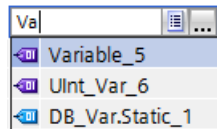
Datenpunkte ihrer Datenquelle zuordnen

Einen neuen Datenpunkt ordnen Sie anschließend seiner Datenquelle zu. Je nach Datentyp des Datenpunkts kommt als Datenquelle eine PLC-Variablen in Betracht.

Für die Zuordnung haben Sie folgende Möglichkeiten:

- Klicken Sie auf das Tabellensymbol  in der Zelle der Spalte "PLC-Tag".
Alle projektieren PLC-Variablen und die Variablen der angelegten Datenbausteine werden eingeblendet. Wählen Sie mit der Maus oder der Tastatur die gewünschte Datenquelle aus.
- Klicken Sie auf das Symbol .
Eine Auswahlliste der projektieren PLC-Tags und der Bausteine wird aufgeblendet. Wählen Sie aus der entsprechenden Tabelle die gewünschte Datenquelle aus.
- Geben Sie in dem Namensfeld der PLC-Variablen einen Teil des Namens der gewünschten Datenquelle ein.

Alle projektieren PLC-Variablen und Variablen der Datenbausteine, deren Namen die eingegebenen Buchstaben enthalten, werden eingeblendet.



Wählen Sie die gewünschte Datenquelle aus.

Hinweis

Zuordnung von Parameterwerten zu PLC-Variablen

Die hier beschriebenen Mechanismen gelten auch, wenn Sie den Wert eines Parameters einer PLC-Variablen zuordnen müssen. Die Eingabefelder für die PLC-Variablen (Bsp.: PLC-Variablen für Partnerstatus, unterstützen die hier beschriebenen Funktionen zur Auswahl der PLC-Variablen.

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

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

- Spalten anordnen

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

- Objekte sortieren

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

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

- Spaltenbreite anpassen

Diese Funktion erreichen Sie über folgende Aktionen:

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

"Breite optimieren", "Breite aller Spalten optimieren"

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



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

- Spalten ein-/ausblenden

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

Datenpunkte und Nachrichten kopieren

Wie bei vielen anderen Programmen können Sie auch im Datenpunkt- bzw. Nachrichten-Editor Objekte kopieren und einfügen.

Wenn Sie mit der rechten Maustaste in die Zeile eines Objekts in der Tabelle klicken, erreichen Sie die genannten Funktionen über das Kontextmenü:

- Ausschneiden
- Kopieren
- Einfügen

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

Sie können ausgeschnittene oder kopierte Objekte auch in Tabellen anderer Kommunikationsmodule vom gleichen Typ und mit gleichem Telecontrol-Protokoll einfügen.

- Löschen

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

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

Datenpunkte exportieren und importieren

Um das Engineering größerer Anlagen zu erleichtern, können Sie die Datenpunkte eines projektierten Moduls exportieren und in weitere Module im Projekt importieren. Dies bietet Vorteile vor allem bei Projekten mit vielen gleichen oder ähnlichen Stationen bzw. Datenpunkt-Modulen.

Kommunikationsmodule mit gleichem Telecontrol-Protokoll sind untereinander kompatibel. Datenpunkte können zwischen kompatiblen Modulen importiert und exportiert werden.

Die Export-/Import-Funktion erreichen Sie, wenn Sie das Modul bspw. in der Netz- oder Geräte-Sicht selektieren und das entsprechende Kontextmenü anwählen.

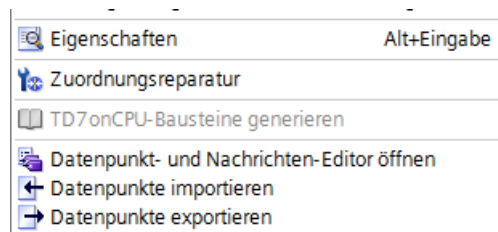


Bild 3-10 Kontextmenü des Moduls

Die Datenpunktinformationen eines Moduls werden beim Export in eine CSV-Datei geschrieben.

Der Import von Datenpunkten eines älteren Projekts in ein Projekt, das in STEP 7 V15.1 angelegt wurde, ist nicht möglich, da der Parameterumfang einiger Datenpunkttypen nicht identisch ist. Der Import funktioniert jedoch, wenn fehlende Parameter (siehe nachfolgende Parameterbeschreibungen) in der CSV-Datei ergänzt werden.

Export

Beim Aufruf der Exportfunktion öffnet sich der Exportdialog. Hier selektieren Sie den oder die Module des Projekts, deren Datenpunktinformationen exportiert werden sollen. Bei Bedarf können Sie die Datenpunkte aller Module des Projekts zusammen exportieren.

Im Exportdialog können Sie den Speicherort im Dateiverzeichnis auswählen. Wenn Sie die Daten eines Moduls exportieren, können Sie auch den vorbelegten Dateinamen ändern.

Beim Export aus mehreren Modulen werden die Dateien mit vorbelegten Namen aus Stationsname und Modul-Name gebildet.

Die Datei selbst enthält neben den Datenpunktinformationen folgende Angaben:

- Modul-Name
- Modul-Typ
- CPU-Name
- CPU-Typ

Editieren der Export-Dateien

Sie können die Datenpunktinformationen in einer exportierten CSV-Datei editieren. Dadurch können Sie diese Datei als Projektierungsvorlage für viele andere Stationen verwenden.

Wenn Sie ein Projekt mit vielen gleichartigen Stationen haben, dann können Sie die CSV-Datei mit den Datenpunkten einer fertig projektierten Baugruppe für weitere, noch nicht projektierte Stationen kopieren und einzelne Parameter an die jeweilige Station anpassen. Damit ersparen Sie sich die Projektierung der Datenpunkte für jede Baugruppe in STEP 7. Stattdessen importieren Sie einfach die kopierte und angepasste CSV-Datei in die anderen, gleichartigen Baugruppen. Die geänderten Parameterwerte der CSV-Datei werden beim Import dieser Datei in eine andere Baugruppe in die Datenpunkt-Projektierung dieses Moduls übernommen.

Die Zeilen der CSV-Datei haben folgende Inhalte:

- Zeile 1: ,Name,Type,
Diese Zeile darf nicht geändert werden.
- Zeile 2: PLC,<CPU-Name>,<CPU-Typ>,
Bedeutung: PLC (Bezeichnung der Stationsklasse), CPU-Name, CPU-Typ
Nur die Elemente <CPU-Name> und <CPU-Typ> dürfen geändert werden.
Der CPU-Typ muss exakt dem Namen der CPU im Katalog entsprechen.
- Zeile 3: Module,<Baugruppen-Name>,<Baugruppen-Typ>,
Bedeutung: Module (Bezeichnung der Modulkategorie), Baugruppen-Typ, Baugruppen-Name
Nur die Elemente <Baugruppen-Name> und <Baugruppen-Typ> dürfen geändert werden.
Seien Sie sorgfältig beim Ändern der Baugruppen-Namen, wenn Sie Datenpunkte in mehrere Baugruppen importieren möchten (siehe unten).
Der Baugruppen-Typ muss exakt dem Namen der Baugruppe im Katalog entsprechen.
- Zeile 4: Parameternamen (englisch) der Datenpunkte
Diese Zeile darf nicht geändert werden.
- Zeilen 5..n: Werte der Parameter gemäß Zeile 4 der einzelnen Datenpunkte
Die Parameterwerte dürfen Sie für die jeweilige Station ändern.

Import in ein Modul

Stellen Sie vor dem Importieren der Datenpunkte sicher, dass die entsprechend benötigten PLC-Variablen für die Datenpunkte angelegt sind.

Beachten Sie, dass beim Import einer CSV-Datei alle im Modul vorhandenen Datenpunkte gelöscht und durch die importierten Datenpunkte ersetzt werden.

Selektieren Sie ein Modul und wählen Sie die Importfunktion aus dem Kontextmenü des Moduls. Es öffnet sich der Importdialog, in dem Sie die gewünschte CSV-Datei im Dateiverzeichnis auswählen.

Wenn die Informationen zur Zuordnung der einzelnen Datenpunkte zu ihrer jeweiligen PLC-Variablen mit der Zuordnung im ursprünglichen Modul entsprechen, werden die Datenpunkte den jeweiligen PLC-Variablen zugeordnet.

Wenn Sie Datenpunkte in ein Modul importieren, aber einige benötigte PLC-Variablen in der CPU noch nicht angelegt sind, dann können die entsprechenden Datenpunktinformationen nicht zugeordnet werden. In diesem Fall können Sie fehlende PLC-Variablen nachträglich anlegen und diesen danach die importierten Datenpunktinformationen zuordnen. Hierfür steht die Funktion "Zuordnungsreparatur" zur Verfügung (siehe unten).

Wenn sich die Namen der PLC-Variablen in dem Modul, in welches importiert wird, von demjenigen Modul, welches exportiert hat, unterscheiden, dann können die entsprechenden Datenpunkte nicht ihren PLC-Variablen zugeordnet werden.

Import in mehrere Module

Sie können die Datenpunkte von mehreren Modulen in die Module eines anderen Projekts importieren. Selektieren Sie hierzu im Importdialog über die Steuerungstaste alle benötigten CSV-Dateien.

Stellen Sie vor dem Importieren der Datenpunkte sicher, dass sowohl die entsprechenden Stationen mit gleichnamigen CPUs, gleichnamigen Modulen und die gleichnamigen PLC-Variablen angelegt sind.

Beim Import werden anhand der Modulnamen in den CSV-Dateien die entsprechenden Stationen des Projekts gesucht. Wenn eine Zielstation nicht im Projekt vorhanden ist oder das Modul einen unterschiedlichen Namen hat, wird der Import der entsprechenden CSV-Datei ignoriert.

Beschränkungen des Imports von Datenpunkten

In folgenden Fällen wird der Import von Datenpunkten abgebrochen:

- Ein vom Modul benötigtes Attribut fehlt in der zu importierenden CSV-Datei.
Beispiel: Wenn ein zu importierender Datenpunkt einen Uhrzeit-Trigger verwendet, dann wird der Import abgebrochen, wenn für das Modul keine Uhrzeitsynchronisation projektiert wurde.
- Das vom Modul verwendete Telecontrol-Protokoll unterscheidet sich vom ursprünglichen Modul.


Module mit gleichem Telecontrol-Protokoll sind untereinander kompatibel:

Nur beim Import in mehrere Module:

- Der Import wird abgebrochen, wenn sich ein Modul- oder CPU-Name von den Daten der CSV-Datei unterscheidet.

Zuordnungsreparatur

Wenn Sie in einer Station, in die Sie importieren wollen, die PLC-Variablen anders benannt haben als in derjenigen Station, aus der die CSV-Datei exportiert wurde, dann geht die Zuordnung zwischen Datenpunkt und PLC-Variable beim Import verloren.

Sie haben dann die Möglichkeit, entweder vorhandene PLC-Variablen passend umzubenennen oder fehlende PLC-Variablen hinzuzufügen. Anschließend können Sie die Zuordnung zwischen nicht zugeordneten Datenpunkten und PLC-Variablen reparieren. Die Funktion erreichen Sie entweder über das Kontextmenü des Moduls (siehe oben) oder über das folgende Symbol links oben im Datenpunkteditor: 

Wenn von der Reparaturfunktion zu einem Datenpunkt eine PLC-Variable mit passendem Namen gefunden wird, wird die Zuordnung wieder hergestellt. Dabei wird jedoch nicht der Datentyp der Variable geprüft.

Prüfen Sie nach der Zuordnungsreparatur auf jeden Fall, ob die neu zugeordneten PLC-Variablen richtig sind.

3.22.2 Datenpunkttypen

Bei der Projektierung der zu übertragenden Nutzdaten wird jeder Datenpunkt einem Datenpunkttyp zugeordnet.

Nachfolgend werden die protokollspezifischen Datenpunkttypen mit den jeweils kompatiblen S7-Datentypen aufgelistet.

Die Spalte "Richtung" gibt die Übertragungsrichtung an:

- "in": Beobachtungsrichtung
- "out": Steuerungsrichtung

Bei ST7-Protokoll ist die Übertragungsrichtung aus dem Objektnamen ablesbar.

Hinweis

Auswirkung der Änderung von Arrays für Datenpunkte

Bei der nachträglichen Änderung eines Arrays muss der Datenpunkt neu angelegt werden.

Datenpunkttypen des Protokolls "IEC 60870-5"

Tabelle 3- 4 Datenpunkttypen, IEC-Typen und kompatible S7-Datentypen

Format (Speicherbedarf)	Datenpunkttyp	IEC-Typ	Richtung	S7-Datentypen	Operandenbereich
Bit	Single-point information	<1>	in	Bool	I, Q, M, DB
	Single-point information with time tag CP56Time2a ¹⁾	<30>	in	Bool	I, Q, M, DB
	Single command	<45> ⁴⁾	out	Bool	Q, M, DB
	Single command with time tag CP56Time2a ¹⁾	<58> ^{5) 6)}	out	Bool	Q, M, DB
	Double command with time tag CP56Time2a ¹⁾	<59>	out	Bool	DB ²⁾
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag CP56Time2a ¹⁾	<32>	in	Byte, USInt	I, Q, M, DB
	Regulating step command with time tag CP56Time2a ¹⁾	<60>	out	Byte, USInt	DB ²⁾
Integer (16 Bit)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag CP56Time2a ¹⁾	<34>	in	Int	I, Q, M, DB
	Measured value, scaled value	<11>	in	Int	I, Q, M, DB
	Measured value, scaled value with time tag CP56Time2a ¹⁾	<35>	in	Int	I, Q, M, DB
	Set point command, normalized value	<48> ⁴⁾	out	Int	Q, M, DB

Format (Speicherbedarf)	Datenpunkttyp	IEC-Typ	Richtung	S7-Datentypen	Operandenbereich
	Set point command, scaled value	<49> ⁴⁾	out	Int	Q, M, DB
	Set point command, normalized value with time tag CP56Time2a ¹⁾	<61> ⁵⁾	out	Int	Q, M, DB
	Set point command, scaled value with time tag CP56Time2a ¹⁾	<62> ⁵⁾	out	Int	Q, M, DB
Integer (32 Bit)	Bitstring of 32 bits	<7>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a ¹⁾	<33>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals	<15>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals with time tag CP56Time2a ¹⁾	<37>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits	<51> ⁴⁾	out	UDInt, DWord	Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a - control direction ¹⁾	<64> ⁵⁾	out	UDInt, DWord	Q, M, DB
Gleitpunktzahl (32 Bit)	Measured value, short floating point number	<13>	in	Real	Q, M, DB
	Measured value, short floating point number with time tag CP56Time2a ¹⁾	<36>	in	Real	Q, M, DB
	Set point command, short floating point number	<50> ⁴⁾	out	Real	Q, M, DB
	Set point command, short floating point with time tag CP56Time2a ¹⁾	<63> ⁵⁾	out	Real	Q, M, DB
Datenblock (1...2 Bit) ²⁾	Double-point information	<3>	in	ARRAY [0...1] of Bool	DB
	Double-point information with time tag CP56Time2a ¹⁾	<31>	in	ARRAY [0...1] of Bool	DB
	Double command	<46> ⁴⁾	out	ARRAY [0...1] of Bool	DB
	Regulating step command	<47> ⁴⁾	out	ARRAY [0...1] of Bool	DB
	Double command with time tag CP56Time2a ¹⁾	<59> ^{5) 6)}	out	ARRAY [0...1] of Bool	DB
	Regulating step command with time tag CP56Time2a ¹⁾	<60> ^{5) 6)}	out	ARRAY [0...1] of Bool	DB
Datenblock (1...32 Bit) ³⁾	Bitstring of 32 bits ³⁾	<7>	in	³⁾	DB
	Bitstring of 32 bits with time tag CP56Time2a ^{1) 3)}	<33>	in	³⁾	DB
	Bitstring of 32 bits ³⁾	<51> ⁴⁾	out	³⁾	DB
	Bitstring of 32 bits with time tag CP56Time2a - control direction ^{1) 3)}	<64> ⁵⁾	out	³⁾	DB

¹⁾ Zum Format der Zeitstempel siehe nachfolgender Abschnitt.

²⁾ Legen Sie für diese Datenpunkttypen einen Datenbaustein mit einem Array von genau 2 Bool an.

³⁾ Mit diesen Datenpunkttypen können zusammenhängende Speicherbereiche bis zu einer Größe von 32 Bit übertragen werden. Kompatibel ist nur der S7-Datentyp Bool.

⁴⁾ Für IEC 60870-5-104 dürfen diese IEC-Typen alternativ zu denen mit Fußnote ⁵⁾ projektiert werden, aber nicht beide IEC-Typen gemischt.

⁵⁾ Diese IEC-Typen werden nur durch IEC 60870-5-104 unterstützt.

⁶⁾ Die "Max. Befehls-Lebensdauer" der Befehle projektieren Sie in der Parametergruppe "Grundeinstellungen" der Module.

Rückspiegelung bei Single Command

Bei folgenden Befehlen können Sie die Rückspiegelung des aktuellen Werts in der Station an den Master aktivieren:

- Single Command <45>

Der lokale Wert dieses Datenpunkts kann auf Änderungen überwacht werden und bei Änderung an den Master übertragen werden. Die Änderung eines lokalen Werts kann bspw. durch eine Handbedienung vor Ort verursacht werden.

Damit der Wert, der durch lokale Ereignisse oder Eingriffe verursacht wird, an den Master übertragen werden kann, benötigt der jeweilige Datenpunkt einen Rückspiegelungskanal. Hierfür wird ein zweiter Datenpunkt "Single-point information <1>" benötigt. Gehen Sie zur Projektierung der Rückspiegelungsfunktion folgendermaßen vor.

Legen Sie die Datenpunkte an:

- Im Master-Modul
 - Single Command <45>
 - Single-point information <1>

Den zurückgespiegelten Wert müssen Sie beim Master in eine Variable schreiben. Ordnen Sie daher beim Master-Modul beide Datenpunkte unterschiedlichen Variablen zu.

Vergeben Sie für beide Datenpunkte denselben Index.

- Im Stations-Modul
 - Single Command <45>
 - Single-point information <1>

Ordnen Sie im Stations-Modul beide Datenpunkte derselben Variable zu.

Vergeben Sie für beide Datenpunkte denselben Index.

Der von der Station zurückgespiegelte Wert wird beim Master in den Datenpunkttyp "Single-point information <1>" geschrieben.

Zeitstempel der Daten beim IEC-Protokoll

Zeitstempel werden gemäß der IEC-Spezifikation im Format "CP56Time2a" übertragen.

Beachten Sie, dass nur die ersten 3 Bytes für Millisekunden und Minuten übertragen werden.

3.22.3 Statuskennungen der Datenpunkte

Statuskennungen

Die in den nachfolgenden Tabellen aufgelisteten Statuskennungen der Datenpunkte werden zusammen mit dem Wert in jedem Daten-Telegramm an den Kommunikationspartner übertragen. Sie können vom Kommunikationspartner ausgewertet werden.

Die Einträge der Tabellenzeile "Bedeutung" beziehen sich auf den jeweiligen Eintrag in der Tabellenzeile "Bit-Zustand".

Quality descriptor - IEC 60870-5

Die Statuskennungen entsprechen folgenden Elementen der Spezifikation:

Quality descriptor - IEC 60870 Part 5-101

Tabelle 3- 5 Bit-Belegung des Status-Byte

Bit	7	6	5	4	3	2	1	0
Flag-Name	-	-	SB substituted	-	CY carry	OV overflow	NT not topical	IV invalid
Bedeutung	-	-	Ersatzwert	-	Zählwert-überlauf vor Lesen des Werts	Wertebereich über- oder unterschritten, Analogwert	Wert nicht aktualisiert	Wert ist ungültig
Bit-Zustand	(immer 0)	(immer 0)	1	(immer 0)	1	1	1	1

3.22.4 Register "Allgemein"

Datenpunkt-Tabelle

Die wichtigsten Parameter im ersten Register des Datenpunkteditors finden Sie in der Standardeinstellung der Datenpunkt-Tabelle.

Wenn Sie mit der Maus auf die Titelleiste der Datenpunkt-Tabelle gehen, können Sie über das Kontextmenü alle Parameter der Datenpunkt-Projektierung einblenden.

Allgemein

Parameter:

- **Name**
Eindeutiger Name des Datenpunkts
- **PLC-Variable**
Zur Zuordnung siehe Kapitel Datenpunktprojektierung (Seite 115).
- **Datenpunkttyp**
Siehe Kapitel Datenpunkttypen (Seite 123)
- **Datenpunktindex**
Siehe Kapitel Datenpunktindex (Seite 128)
- **Master-Funktion**
Aktiviert die Master-Funktion des Datenpunkts.
Zur Bedeutung siehe Kapitel Master-Funktion der Datenpunkte (Seite 127).

- **Übertragungsart**
Zur Übertragungsart siehe Kapitel Prozessabbild, Übertragungsart, Ereignisklassen (Seite 130).
- **Lesezyklus**
Nur bei Eingängen
Zum Lesezyklus siehe Kapitel Lesezyklus (Seite 132).
- **Antwort auf Generalabfrage**
Aktiviert den Datenpunkt für die Antwort auf eine Generalabfrage. Bei deaktivierter Funktion wird der Wert des Datenpunkts nach einer Generalabfrage nicht an den Kommunikationspartner gesendet.
- **Zuordnung zu Gruppenabfrage**
Ordnet den Datenpunkt einer Gruppenabfrage zu.
Bei Gruppenabfragen des Masters auf die betreffende Gruppe wird der Wert des Datenpunkts an den Master gesendet.

3.22.5 Master-Funktion der Datenpunkte

Die Master-Funktion zur direkten Kommunikation

Direkte Kommunikation zwischen zwei Telecontrol-Stationen, bei welcher die Telegramme nicht von einer Zentrale vermittelt werden, wird durch Aktivierung der Master-Funktion der Datenpunkte ermöglicht.

Voraussetzungen

Voraussetzungen für die Projektierung der direkten Kommunikation zwischen zwei Datenpunkten zweier Partner sind:

- Zwischen den zwei Partnern muss eine Telecontrol-Verbindung angelegt sein.
- In der Telecontrol-Verbindung ist die Option "Spontan" aktiviert.
- Der Datenpunkt muss einem Partner zugeordnet sein.

Projektierung in der Spalte "Partner des Datenpunkts" der Datenpunkt-Tabelle.

Bedeutung der Master-Funktion

- **"Master-Funktion" aktiviert**

Die Werte des Datenpunkts werden wie bei einem Master behandelt:

- **Eingangs-Datenpunkte (Richtung "in")**

Eingangs-Datenpunkte werden entsprechend der beim Partner eingestellten Parameter vom Partner empfangen.

Die Übertragungsart "Übertragung nach Aufruf" ist fest gesetzt.

Die Optionen zur "Analogwert-Vorverarbeitung" sind deaktiviert.

- **Ausgangs-Datenpunkte (Richtung "out")**

Ausgangs-Datenpunkte werden entsprechend der Trigger-Projektierung an den Partner gesendet.

Die Übertragungsart "Jeder Wert getriggert" ist fest gesetzt.

Zur Aktivierung der Option siehe Kapitel Register "Allgemein" (Seite 126).

- **"Master-Funktion" deaktiviert**

- **Eingangs-Datenpunkte (Richtung "in")**

Eingangs-Datenpunkte werden entsprechend der Projektierung behandelt.

Die Übertragungsart und die Optionen zur "Analogwert-Vorverarbeitung" können frei projektiert werden.

- **Ausgangs-Datenpunkte (Richtung "out")**

Ausgangs-Datenpunkte werden entsprechend der Projektierung behandelt.

Die Übertragungsart "Übertragung nach Aufruf" ist automatisch ausgewählt und nicht veränderbar.

3.22.6 Datenpunktindex

Der Index eines Datenpunkts ist die Adresse des Informationsobjekts.

Programmseitig werden die Indices beim Anlegen der Datenpunkte aufsteigend vorbelegt. Sie können die Indices entsprechend Ihren Anforderungen und den folgenden Regeln projektieren.

Projektierung des Datenpunktindex

Strukturierte Adressierung

Der Index kann in zwei Eingabefeldern mit unterschiedlichem Format projektiert werden:

- Datenpunktindex

Hier wird der Index unstrukturiert als Ganzzahl projektiert.

Wertebereich: 1..16777215

- **Strukturierter Index**

Hier können Sie den Index gemäß IEC 60870-5-3 strukturiert projektieren. Über die strukturierte Adressierung wird eine anlagenorientierte Strukturierung der Datenpunkte ermöglicht.

Projektierbar sind 3 Adress-Stufen (Oktette).

Wertebereich: 0.0.1..255.255.255

Die projektierten Werte der beiden Felder sind gekoppelt. Ein projektiertes Wert wird umgerechnet und im jeweils anderen Eingabefeld angezeigt.

Umrechnung der projektierten Werte

Die Werte werden für die Umrechnung wie folgt bezeichnet:

- **Datenpunktindex**

Bezeichnung des Ganzzahl-Werts: X

- **Strukturierter Index**

Bezeichnung der Werte der 3 Oktette: A.B.C

Der projektierte Wert wird nach folgender Formel in das jeweils andere Feld übernommen:

$$X = A * 256 * 256 + B * 256 + C$$

Projektierungsregeln

Folgende Regeln gelten für die Projektierung des Datenpunktindex.

- In einem Modul müssen die Indices pro Kommunikationspartner eindeutig sein.

Doppelt vergebene Indices werden bei der Konsistenzprüfung als Fehler gemeldet und verhindern das Übersetzen des Projekts.

- Die Indices zweier Datenpunkte können identisch sein, wenn die zwei Datenpunkte für unterschiedliche Partner projektiert sind.

Beispiel:

- Datenpunkt 1, Index 1, Partner 1
- Datenpunkt 2, Index 1, Partner 2
- Datenpunkt 3, Index 2, Partner 1
- Datenpunkt 4, Index 2, Partner 7

- Die korrespondierenden Partner-Indizes müssen auf Sende- und Empfangsseite identisch sein.

Index und "Sequenzielle Übertragung"

Gültigkeit:

- Module
 - CP 1243-7 LTE
 - TIM 1531 IRC
- Netzknotentyp der Schnittstelle für Telecontrol-Kommunikation: Station oder Knotenstation
- Parametergruppe: Schnittstelle > Erweiterte Optionen > Einstellungen IEC-Station > Ereignis-Einstellungen > Übertragungsverhalten

Die gemeinsame Übertragung von Ereignis-Telegrammen in einer Sequenz kann für Datenpunkte ohne Uhrzeitstempel projektiert werden.

Folgende Voraussetzungen müssen für die sequenzielle Übertragung erfüllt sein:

- Die Datenpunkte sind vom gleichen Typ.
- Die Indices der Datenpunkte liegen lückenlos hintereinander.

3.22.7 Prozessabbild, Übertragungsart, Ereignisklassen

Speicherung von Werten

Generell werden die Werte von allen Datenpunkten im Abbildspeicher der Baugruppe gespeichert. Werte im Abbildspeicher werden erst nach Aufruf durch die Zentrale-TIM übertragen.

Ereignisse werden zusätzlich im Sendepuffer gespeichert und können spontan übertragen werden.

Der Abbildspeicher, das Prozessabbild des Moduls

Der Abbildspeicher ist das Prozessabbild der TIM. Im Abbildspeicher werden alle aktuellen Werte der projektierten Datenpunkte gespeichert. Neue Werte eines Datenpunkts überschreiben den zuletzt gespeicherten Wert im Abbildspeicher.

Die Werte werden erst nach Abfrage des Kommunikationspartners gesendet, siehe "Übertragung nach Aufruf" im Abschnitt "Übertragungsarten" unten, oder zusammen mit einem Telegramm aus dem Sendepuffer, das sofort übertragen werden muss.

Der Sendepuffer

Der Sendepuffer der TIM ist der Speicher für die einzelnen Werte von Datenpunkten, die als Ereignis projektiert sind. Die Größe des Sendepuffers entnehmen Sie dem Handbuch der jeweiligen Baugruppe.

Die Kapazität des Sendepuffers wird für alle aktivierten Partner gleichmäßig aufgeteilt.

Wenn die Verbindung mit einem Kommunikationspartner unterbrochen ist, bleiben die einzelnen Werte der Ereignisse durch die Pufferung erhalten. Bei wiederkehrender Verbindung werden die gepufferten Werte gesendet. Der Telegrammspeicher arbeitet chronologisch, das heißt, die ältesten Telegramme werden zuerst gesendet (FIFO-Prinzip).

Wenn ein Telegramm an den Kommunikationspartner übertragen wurde, dann wird der übertragene Wert aus dem Sendepuffer gelöscht.

Wenn Telegramme für längere Zeit nicht übertragen werden können und der Sendepuffer droht überzulaufen, gilt das folgende Verhalten:

- Bei Erreichen von 80 % Füllgrad des Sendepuffers wird eine Warnmeldung ausgegeben.
- Bei Erreichen von 100 % Füllgrad des Sendepuffers werden keine weiteren Werte mehr gespeichert, bis der Füllgrad wieder unter 100 % sinkt.

Speicherung der Datenpunktwerte

Generell werden die Werte von Datenpunkten im Abbildspeicher der Baugruppe gespeichert und erst nach Abfrage durch den Kommunikationspartner übertragen.

Ereignisse werden zusätzlich im Sendepuffer gespeichert und können spontan übertragen werden.

Über den Parameter "Übertragungsart" (siehe unten) werden Datenpunkte als statischer Wert oder als Ereignis projiziert:

- **Statischer Wert (kein Ereignis)**

Statische Werte werden in den Abbildspeicher (Prozessabbild) eingetragen.

Statische Werte entsprechen der folgenden Übertragungsart "Übertragung nach Aufruf (class 0)".

- **Ereignis**

Die Werte von Datenpunkten, welche als Ereignis projiziert sind (getriggerte Übertragungsart), werden ebenfalls in den Abbildspeicher des Moduls eingetragen. Zusätzlich werden die Werte in den Sendepuffer eingetragen.

Übertragungsarten und Ereignisklassen

Folgende Übertragungsarten sind möglich:

- **Übertragung nach Aufruf (class 0)**

Der jeweils aktuelle Wert des Datenpunkts wird in den Abbildspeicher eingetragen. Neue Werte eines Datenpunkts überschreiben den zuletzt gespeicherten Wert im Abbildspeicher.

Nach Aufruf durch den Kommunikationspartner wird der zu diesem Zeitpunkt aktuelle Wert übertragen.

Bei Ausgangs-Datenpunkten ist diese Option vorbelegt und nicht änderbar.

- **Getriggert**

Über eine getriggerte Übertragungsart werden Datenpunkte als Ereignis projiziert. Die Werte dieser Datenpunkte werden in den Abbildspeicher und zusätzlich in den Sendepuffer eingetragen.

Die Werte eines Ereignisses werden gespeichert, sobald die projizierten Triggerbedingungen erfüllt sind.

Folgende Ereignisklassen stehen zur Verfügung:

- **Jeder Wert getriggert**

Jede Wertänderung wird in chronologischer Reihenfolge in den Sendepuffer eingetragen.

- **Aktueller Wert getriggert**

Nur der jeweils letzte, aktuelle Wert wird in den Sendepuffer eingetragen. Er überschreibt den dort zuvor gespeicherten Wert.

Zu den verschiedenen Trigger-Typen siehe Kapitel Register "Trigger" (Seite 133).

3.22.8 Lesezyklus

Eingangs-Datenpunkte werden dem Lesezyklus der CPU in der Datenpunktprojektierung im Register "Allgemein > Lesezyklus" zugeordnet.

Aufbau des CPU-Abtastzyklus

Der Zyklus, mit dem die Übertragungs-Baugruppe (TIM) den Speicherbereich der CPU abtastet, ist aus den folgenden Phasen aufgebaut:

- **Hochpriorie Leseaufträge**

- (Schneller Zyklus)

Für alle Datenpunkte mit der Zuordnung "Schneller Zyklus" werden die PLC-Variablen in jedem Abtastzyklus gelesen.

In der Regel ist es ausreichend, nur schnell zu erfassende Daten wie Alarmer und Wischermeldungen sowie Befehls-, Sollwert- und Parameter-Objekte für die 1-aus-n-Prüfung dem schnellen Zyklus zuzuordnen.

Zur 1-aus-n-Prüfung siehe Glossar.

- **Schreibaufträge**

In jedem Zyklus werden die Werte einer bestimmten Anzahl spontaner Schreibaufträge in die CPU geschrieben.

Die Anzahl der Variablen, die pro Zyklus geschrieben werden, wird für die Übertragungs-Baugruppe in der Parametergruppe "Kommunikation mit der CPU" mit dem Parameter "Max. Anzahl der Schreibaufträge" festgelegt. Diejenigen Variablen, deren Anzahl diesen Wert übersteigt, werden dann im nächsten oder einem der folgenden Zyklen geschrieben.

- **Niederpriore Leseaufträge - anteilig**

(Normaler Zyklus)

Für Datenpunkte mit der Zuordnung "Normaler Zyklus" werden die Werte ihrer PLC-Variablen anteilig in jedem Abtastzyklus gelesen.

Die Anzahl der Variablen, die pro Zyklus gelesen werden, wird für die Übertragungs-Baugruppe in der Parametergruppe "Kommunikation mit der CPU" mit dem Parameter "Max. Anzahl der Leseaufträge" festgelegt. Die Variablen, die diesen Wert übersteigen und somit in einem Zyklus nicht gelesen werden, werden dann im nächsten oder einem der folgenden Zyklen gelesen.

- **Zykluspausenzeit**

Diese Wartezeit zwischen zwei Abtastzyklen dient dazu, anderen Prozessen, die auf die CPU zugreifen, genügend Zeit zu reservieren.

3.22.9 Register "Trigger"

Trigger

Datenpunkte werden über den Parameter "Übertragungsart" als statischer Wert oder als Ereignis projiziert:

Speichern des Werts eines als Ereignis projizierten Datenpunkts

Das Speichern des Werts eines als Ereignis projizierten Datenpunkts im Sendepuffer (Telegrammspeicher) kann über verschiedene Trigger-Typen ausgelöst werden:

- **Schwellenwert-Trigger**

Der Wert des Datenpunkts wird gespeichert, wenn dieser eine bestimmte Schwelle erreicht. Die Schwelle wird als Differenz zu dem zuletzt gespeicherten Wert berechnet, siehe Kapitel Schwellenwert-Trigger (Seite 136).

- **Zeit-Trigger**

Der Wert des Datenpunkts wird in einem projizierbaren Zeitraster oder zu einer bestimmten Uhrzeit gespeichert.

- **Ereignis-Trigger (Trigger-Variable)**

Der Wert des Datenpunkts wird gespeichert, wenn ein projektierbares Trigger-Signal ausgelöst wird. Als Trigger-Signal wird der Flankenwechsel (0 → 1) einer Trigger-Variablen ausgewertet, die vom Anwenderprogramm gesetzt wird. Für jeden Datenpunkt kann bei Bedarf eine separate Trigger-Variable projektiert werden.

Rücksetzen der Trigger-Variablen im Merkerbereich / DB:

Wenn der Speicherbereich einer Trigger-Variablen im Merkerbereich oder in einem Datenbaustein liegt, dann setzt das Modul die Trigger-Variable selbst auf 0 (Null) zurück, sobald der Wert des Datenpunkts übertragen ist. Dies kann bis zu 500 Millisekunden dauern.

Hinweis

Schnelles Setzen von Triggern

Trigger dürfen nicht schneller als in einem Mindestabstand von 500 Millisekunden gesetzt werden. Dies gilt auch für Hardware-Trigger (Eingabebereich).

Hinweis

Hardware-Trigger

Hardware-Trigger müssen Sie über das Anwenderprogramm zurücksetzen.

Übertragungszeitpunkt

Ob der Wert eines Ereignisses nach Auslösen des Triggers sofort oder zeitversetzt an den Kommunikationspartner übertragen wird, hängt davon ab, ob spontanes Senden bzw. asymmetrische Kommunikation im Netz möglich ist.

Die spontane Übertragung von Ereignissen stellen Sie im Editor "Netzwerkdaten" der Telecontrol-Verbindungen für jeden Verbindungsabschnitt über den Parameter "Spontan" ein.

Archivierung aktivieren

Nur projektierbar bei: TIM 1531 IRC

Die Option ermöglicht bei Verbindungsstörungen, die Werte von Ereignissen außer im Sendepuffer zusätzlich remanent auf der SD-Karte zu speichern.

Die Funktion wird für Datenpunkte in Beobachtungsrichtung der folgenden Informationsobjekt-Klassen unterstützt:

- Single-point information
- Double-point information
- Step position information
- Measured value
- Integrated totals
- Bitstring

Zum Aktivieren und zu den Optionen des remanenten Speicherns siehe Kapitel Grundeinstellungen (Seite 34).

Die Archivierung ist möglich bei folgenden Datenpunkttypen:

- ST7
 - Bin04B_S / Bin08X_S
 - Ana04W_S / Ana04R_S
 - Mean04W_S
 - Cnt01D_S / Cnt04D_S
 - Dat12D_S / Dat12x1D_S
 - Cmd01B_S / Cmd08X_S
 - Set01W_S
 - Par12D_S / Par12x1D_S
- DNP3
 - Binary Input Event (2)
 - Counter Input Event (22)
 - Analog Input Event (32)
 - Octet String Event (111)
- IEC 60870-5
 - Information objects <1/5/30/32>
 - Measured value <9/11/13/34/35/36>
 - Integrated totals <15/37>
 - Bitstring <7/33>

Stationszustands-Ereignisse

Nur projektierbar bei TIM 1531 IRC und Datenpunkttyp "Single-point information" <1/30>

- **Stationszustands-Ereignistyp**

Wählen Sie aus, bei welchem Ereignis die Station Telegramme an den festgelegten Partner sendet. Das Telegramm wird zusammen mit der Objektnummer übertragen.

 - Kein Stationszustands-Ereignis
 - Status der lokalen CPU (True = RUN, False = STOP)
 - Verbindungsstatus zur lokalen CPU
(True = Verbindung OK, False = Verbindung nicht OK)
 - Verbindungsstatus zur Unterstation
 - Fehler SD-Karte (True = SD-Karte fehlerhaft, False = SD-Karte OK)
- **Adresse Unterstation**

Bei Auswahl der Option "Verbindungsstatus zur Unterstation geändert" geben Sie hier die Stationsadresse der Unterstation ein, deren Verbindungsstatus sich geändert hat.

3.22.10 Schwellenwert-Trigger

Hinweis

Schwellenwert-Trigger: Berechnung erst nach Analogwert-Vorverarbeitung

Beachten Sie, dass die Analogwert-Vorverarbeitung vor der Prüfung auf einen projektierten Schwellenwert und vor der Berechnung des Schwellenwerts durchgeführt wird.

Glättungsfaktoren und ein eventuell projektiertes Integrations-Intervall werden bei der Berechnung berücksichtigt.

Dies hat Auswirkungen auf den Wert, der beim Schwellenwert-Trigger projiziert wird.

Hinweis

Schwellenwert-Trigger bei projektiierter Mittelwertbildung

Bei aktivierter Mittelwertbildung wird für Analogwerte beim Schwellenwert-Trigger das absolute Verfahren für die Berechnung der Schwellenwert-Abweichung verwendet.

Zum zeitlichen Ablauf der Analogwert-Vorverarbeitung siehe Kapitel Analogwert-Vorverarbeitung (Seite 138).

Schwellenwert-Trigger

Funktion

Bei Abweichung des Prozesswerts um den Betrag des Schwellenwerts wird der Prozesswert gespeichert.

Für die Berechnung der Schwellenwert-Abweichung werden zwei Verfahren angewendet:

- **Absolutes Verfahren**

Bei Binär- und Zählwerten sowie bei Analogwerten mit projektiierter Mittelwertbildung wird für die Berechnung der Schwellenwert-Abweichung das absolute Verfahren angewendet.

- **Integratives Verfahren**

Bei Analogwerten ohne projektierte Mittelwertbildung wird für die Berechnung der Schwellenwert-Abweichung das integrierende Verfahren angewendet.

Bei der integrierenden Schwellenwertberechnung wird nicht der absolute Betrag der Abweichung des Prozesswerts vom zuletzt gespeicherten Wert ausgewertet, sondern die integrierte Abweichung.

Über das "Integrations-Intervall" (Analogwert-Vorverarbeitung) ist die Anwendung des integrativen Verfahrens auf Analogwerte abschaltbar.

Absolutes Verfahren

Für jeden Binärwert wird geprüft, ob der aktuelle (eventuell geglättete) Wert außerhalb des Schwellenwertbandes liegt. Das jeweils aktuelle Schwellenwertband ergibt sich aus dem zuletzt gespeicherten Wert und dem Betrag des projizierten Schwellenwerts:

- Obergrenze des Schwellenwertbandes: Letzter gespeicherter Wert + Schwellenwert
- Untergrenze des Schwellenwertbandes: Letzter gespeicherter Wert - Schwellenwert

Sobald der Prozesswert die Ober- oder Untergrenze des Schwellenwertbandes erreicht, wird der Wert gespeichert. Der neue gespeicherte Wert dient als Basis für die Berechnung des neuen Schwellenwertbandes.

Integratives Verfahren

Die integrierende Schwellenwertberechnung arbeitet mit einem zyklischen Vergleich des integrierten aktuellen Werts mit dem zuletzt gespeicherten Wert. Der Berechnungszyklus, in dem die beiden Werte verglichen werden, kann eingestellt werden, siehe Abschnitt "Integrations-Intervall" im Kapitel Analogwert-Vorverarbeitung (Seite 138).

(Anmerkung: Der Berechnungszyklus ist nicht zu verwechseln mit dem Abtastzyklus der CPU-Speicherbereiche).

Die Abweichungen des aktuellen Prozesswerts werden in jedem Berechnungszyklus aufaddiert. Erst wenn der aufsummierte Wert den projizierten Wert des Schwellenwert-Triggers erreicht, wird der Trigger gesetzt und ein neuer Prozesswert in den Sendepuffer eingetragen.

Das Verfahren wird am folgenden Beispiel erläutert, bei dem ein Schwellenwert von 2,0 projiziert ist.

Tabelle 3- 6 Beispiel für die integrierende Berechnung eines mit 2,0 projizierten Schwellenwerts

Zeit [s] (Berechnungs- Zyklus)	Im Sendepuffer gespeicherter Prozesswert	Aktueller Prozesswert	Absolute Abweichung vom gespeicherten Wert	Integrierte Abweichung
0	20,0	20,0	0	0
0,5		20,3	+0,3	0,3
1,0		19,8	-0,2	0,1
1,5		20,2	+0,2	0,3
2,0		20,5	+0,5	0,8
2,5		20,3	+0,3	1,1
3,0		20,4	+0,4	1,5
3,5	20,5	20,5	+0,5	2,0
4,0		20,4	-0,1	-0,1
4,5		20,1	-0,4	-0,5
5,0		19,9	-0,6	-1,1
5,5		20,1	-0,4	-1,5
6,0	19,9	19,9	-0,6	-2,1

Bei dem im Beispiel dargestellten Verlauf des Prozesswerts wird der mit 2,0 projizierte Schwellenwert-Trigger zweimal ausgelöst:

- Zum Zeitpunkt 3,5 s: Der Betrag der integrierten Abweichung liegt bei 2,0. Der neue im Sendepuffer gespeicherte Prozesswert beträgt 20,5.
- Zum Zeitpunkt 6,0 s: Der Betrag der integrierten Abweichung liegt bei 2,1. Der neue im Sendepuffer gespeicherte Prozesswert beträgt 19,9.

Wenn in diesem Beispiel eine Abweichung des Prozesswerts von ca. 0,5 das Auslösen des Triggers veranlassen sollte, dann müsste bei dem dargestellten Verhalten des Prozesswerts ein Schwellenwert von ca. 1,5 ... 2,5 projiziert werden.

3.22.11 Analogwert-Vorverarbeitung

Die TIM unterstützt die Analogwert-Vorverarbeitung. Für Analogwert-Datenpunkte können einige oder alle der nachfolgend beschriebenen Funktionen projiziert werden.

Voraussetzungen und Restriktionen

Voraussetzungen für die Projektierung der Vorverarbeitungsoptionen und gegenseitige Restriktionen finden Sie im Abschnitt der jeweiligen Funktion.

Hinweis

Restriktionen aufgrund von projizierten Triggern

Die Analogwert-Vorverarbeitungsoptionen "Fehlerunterdrückungszeit", "Grenzwertberechnung" und "Glättung" werden nicht durchgeführt, wenn kein Schwellenwert-Trigger für den betreffenden Datenpunkt projiziert ist. In diesen Fällen wird der gelesene Prozesswert des Datenpunkts vor Ablauf des Vorverarbeitungszyklus der Schwellenwert-Berechnung (500 ms) in den Abbildspeicher eingetragen und transparent übertragen.

Ablauf der Analogwert-Vorverarbeitungsoptionen

Die Werte von Analogeingängen, die als Ereignis projiziert sind, werden in der TIM nach folgendem Schema bearbeitet:

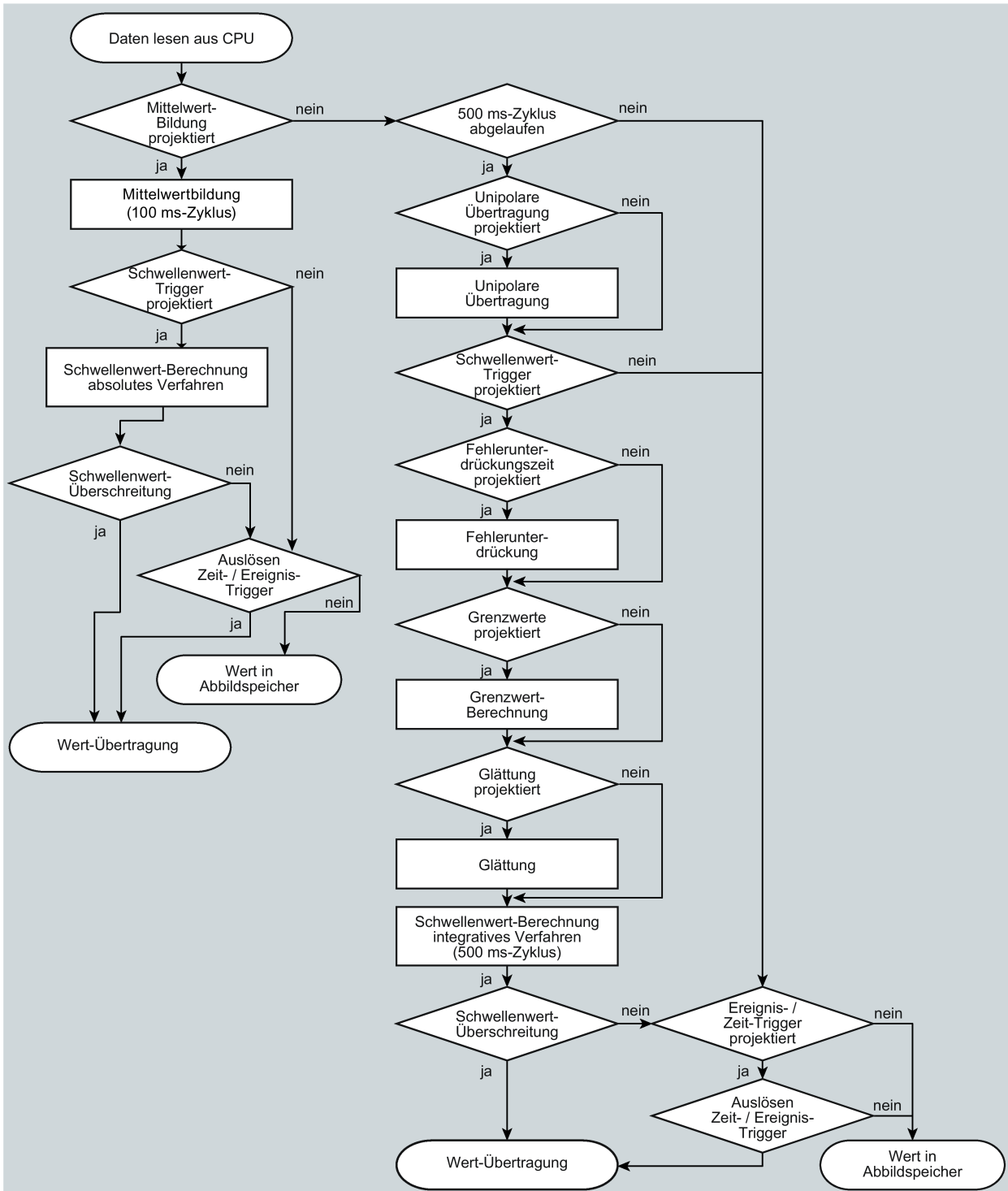


Bild 3-11 Ablauf der Analogwert-Vorverarbeitung

Der 500-Millisekunden-Zyklus wird durch die integrative Schwellenwert-Berechnung aufgesetzt. In diesem Zyklus werden die Werte auch bei Aktivierung der folgenden Vorverarbeitungsoptionen gespeichert:

- Unipolare Übertragung
- Fehlerunterdrückungszeit
- Grenzwertberechnung
- Glättung

Mittelwertbildung

Mit diesem Parameter werden erfasste Analogwerte als Mittelwerte übertragen.

Bei den folgenden Protokollen wird die Mittelwertbildung nur für Ganzzahlen vom Typ "Int" unterstützt:

- TeleControl Basic
- DNP3
- IEC 60870-5

Hinweis

Eingeschränkte Vorverarbeitungsoptionen bei projektierter Mittelwertbildung

Wenn Sie für ein Analogwertereignis die Mittelwertbildung projektieren, dann stehen folgende Vorverarbeitungsoptionen nicht zur Verfügung:

- Unipolare Übertragung
 - Fehlerunterdrückungszeit
 - Glättung
 - Schwellenwert-Berechnung nur mit dem absoluten Verfahren
-

Funktion

Bei aktivierter Mittelwertbildung ist die Projektierung eines Zeit-Triggers sinnvoll.

Die aktuell anstehenden Werte eines Analogwert-Datenpunkts werden im 100-Millisekunden-Zyklus gelesen und aufsummiert. Die Anzahl der gelesenen Werte pro Zeiteinheit ist abhängig vom Lesezyklus der CPU und vom CPU-Abtastzyklus des CP.

Aus den aufsummierten Werten wird der Mittelwert gebildet, sobald die Übertragung über einen Trigger ausgelöst wird. Danach wird die Aufsummierung zur Bildung des nächsten Mittelwerts neu gestartet.

Der Mittelwert wird auch dann gebildet, wenn die Übertragung des Analogwerttelegramms durch eine Abfrage vom Kommunikationspartner ausgelöst wird. Die Dauer der Mittelungsperiode ist dann die Zeit von der letzten Übertragung (z. B. über den Trigger ausgelöst) bis zum Zeitpunkt der Abfrage. Auch nach dieser Übertragung wird die Aufsummierung zur Bildung des nächsten Mittelwertes neu gestartet.

Eingabebaugruppen: Überlaufbereich / Unterlaufbereich

Sobald ein Wert im Überlauf- bzw. Unterlaufbereich erfasst wird, wird die Mittelwertbildung abgebrochen. Für die laufende Mittelungsperiode wird der Wert 32767 / 7FFF_h bzw. -32768 / 8000_h als ungültiger Mittelwert gespeichert und im nächsten Telegramm übertragen.

Danach wird eine neue Mittelwertbildung gestartet. Wenn der Analogwert dann immer noch im Überlauf- oder Unterlaufbereich liegt, wird wieder einer der beiden genannten Werte als ungültiger Mittelwert gespeichert und bei der nächsten Telegrammauslösung übertragen.

Hinweis

Fehlerunterdrückungszeit > 0 projiziert

Wenn Sie eine Fehlerunterdrückungszeit projiziert haben und danach die Mittelwertbildung aktivieren, dann wird der Wert der Fehlerunterdrückungszeit ausgegraut aber nicht mehr angewendet. Die Fehlerunterdrückungszeit wird bei aktivierter Mittelwertbildung intern auf 0 (null) gesetzt.

Unipolare Übertragung

Restriktionen

Unipolare Übertragung kann nicht gleichzeitig mit der Mittelwertbildung projiziert werden. Die Aktivierung der unipolaren Übertragung wird bei Aktivierung der Mittelwertbildung unwirksam.

Funktion

Bei der unipolaren Übertragung werden negative Werte auf Null korrigiert. Dies kann gewünscht sein, wenn Werte aus dem Untersteuerungsbereich nicht als reale Messwerte übertragen werden sollen.

Ausnahme: Bei Prozessdaten von Eingabebaugruppen wird der Wert -32768 / 8000_h für Drahtbruch eines Life-Zero-Eingangs übertragen.

Bei einem Software-Eingang dagegen werden alle Werte kleiner Null auf Null korrigiert.

Fehlerunterdrückungszeit

Voraussetzungen für die Funktion

Projektierung des Schwellenwert-Triggers für diesen Datenpunkt

Restriktionen

Die Fehlerunterdrückungszeit kann nicht gleichzeitig mit der Mittelwertbildung projiziert werden. Ein projizierter Wert wird bei Aktivierung der Mittelwertbildung unwirksam.

Funktion

Typischer Anwendungsfall für diesen Parameter ist die Unterdrückung von Spitzenstromwerten beim Anlauf leistungsstarker Motoren, die sonst als Störung an die Leitstelle gemeldet würden.

Die Übertragung eines Analogwerts im Überlauf (7FFF_h) oder Unterlauf (8000_h) wird für die Dauer der angegebenen Zeitspanne unterdrückt. Erst nach Ablauf der Fehlerunterdrückungszeit wird der Wert von 7FFF_h bzw. 8000_h übertragen, falls er noch ansteht.

Wenn der Wert vor Ablauf der Fehlerunterdrückungszeit in den Bemessungsbereich zurückfällt, wird der aktuelle Wert übertragen.

Eingabebaugruppen

Die Unterdrückung ist abgestimmt auf Analogwerte, die als Rohwerte direkt von S7-Analog-Eingabebaugruppen erfasst werden. Diese Baugruppen liefern für alle Eingangsbereiche die genannten Werte für den Überlauf- bzw. Unterlaufbereich, auch für Life-Zero-Eingänge.

Ein Analogwert im Überlaufbereich (32767 / 7FFF_h) oder Unterlaufbereich (-32768 / 8000_h) wird für die Dauer der Fehlerunterdrückungszeit nicht übertragen. Dies gilt auch für Life-Zero-Eingänge. Erst nach Ablauf der Fehlerunterdrückungszeit wird der Wert im Über- bzw. Unterlaufbereich übertragen, falls er noch ansteht.

Empfehlung zu Fertigwerten, die von der CPU vorverarbeitet wurden:

Wenn von der CPU vorverarbeitete Fertigwerte im Merkerbereich oder in einem Datenbaustein bereitgestellt werden, dann ist eine Unterdrückung nur möglich bzw. sinnvoll, wenn die Fertigwerte im Überlauf bzw. Unterlauf ebenfalls die genannten Werte von 32767 / 7FFF_h bzw. -32768 / 8000_h annehmen. Wenn dies nicht der Fall ist, dann sollte der Parameter für vorverarbeitete Werte nicht projiziert werden.

Für bereits in der CPU vorverarbeitete Fertigwerte können die Grenzen für den Überlauf/Unterlauf frei vergeben werden.

Integrations-Intervall

Das Integrations-Intervall wird für die Schwellenwertbearbeitung von Analogwerten nach dem Integrationsprinzip verwendet. Der Schwellenwert wird für den Schwellenwert-Trigger verwendet, vergleiche Kapitel Schwellenwert-Trigger (Seite 136).

Der eingegebene Wert bestimmt das zeitliche Intervall, in dem Analogwerte integriert werden.

Bei 0 (null) wird der Schwellenwert ohne Integration berechnet. Dies bedeutet ein geringeres Datenaufkommen. In diesem Fall wird das Absolute Verfahren angewendet.

Glättungsfaktor

Voraussetzungen für die Funktion

Projektierung des Schwellenwert-Triggers für diesen Datenpunkt

Restriktionen

Der Glättungsfaktor kann nicht gleichzeitig mit der Mittelwertbildung projiziert werden. Ein projizierter Wert wird bei Aktivierung der Mittelwertbildung unwirksam.

Funktion

Schnell schwankende Analogwerte können mit Hilfe der Glättungsfunktion beruhigt werden.

Die Glättungsfaktoren werden wie bei S7-Analogeingabebaugruppen nach folgender Formel berechnet.

$$y_n = \frac{x_n + (k - 1) y_{n-1}}{k}$$

mit

y_n = Geglätteter Wert im aktuellen Zyklus n

y_{n-1} = Geglätteter Wert im vorhergehenden Zyklus n-1

x_n = Erfasster Wert im aktuellen Zyklus n

k = Glättungsfaktor

Als Glättungsfaktor sind folgende Werte für die Baugruppe projektierbar.

- 1 = Keine Glättung
- 4 = Schwache Glättung
- 32 = Mittlere Glättung
- 64 = Starke Glättung

Grenzwert 'tief' setzen / Grenzwert 'hoch' setzen

Voraussetzungen für die Funktion

- Projektierung des Schwellenwert-Triggers für diesen Datenpunkt
- Unterstützte Variablentypen der CPU

Der Analogwert-Datenpunkt muss alternativ mit einer der folgenden Variablen verknüpft sein:

- PLC-Variable im Merkerbereich
- DB-Variable (Variable in Datenbaustein)

Für PLC-Variablen, die auf Hardware-Baugruppen (Operandenbereich Eingang/Ausgang) zugreifen, ist die Grenzwertprojektierung nicht möglich.

Für Messwerte, die bereits in der CPU vorverarbeitet wurden, ist die Projektierung von Grenzwerten nicht sinnvoll.

Funktion

In diesen beiden Eingabefeldern können Sie jeweils einen Grenzwert in Richtung Messbereichsanfang bzw. in Richtung Messbereichsende setzen.

Die Grenzwerte können Sie bspw. auch als Messbereichsanfang bzw. Messbereichsende auswerten.

Empfehlung für schnell schwankende Analogwerte:

Wenn der Analogwert schnell schwankt, kann es bei projektierten Grenzwerten sinnvoll sein, den Analogwert zuvor zu glätten.

Statuskennung "OVER_RANGE" / "overflow"

Bei Protokollen, die Statuskennungen unterstützen, wird bei Unter- bzw. Überschreitung des Grenzwerts die Statuskennung des Datenpunkts für Messbereichsüberschreitung gesetzt, nachfolgend als Kennung "OV" bezeichnet. Die Statuskennungen sind im Kapitel Statuskennungen der Datenpunkte (Seite 125) beschrieben.

Das Bit "OV" der Statuskennung des Datenpunkts wird bei der Übertragung des betreffenden Analogwerts wie folgt gesetzt:

- Grenzwert 'hoch':
 - Bei Überschreitung des Grenzwerts: OV = 1
 - Bei anschließender Unterschreitung des Grenzwerts: OV = 0
- Grenzwert 'tief':
 - Bei Unterschreitung des Grenzwerts: OV = 1
 - Bei anschließender Überschreitung des Grenzwerts: OV = 0

Projektierung des Grenzwerts

Ein Grenzwert wird je nach Datentyp als ganze Dezimalzahl oder als Gleitpunktzahl projektiert.

Tabelle 3- 7 Wertebereiche der Grenzwerte

Datentyp	Wertebereich
Int	-32768 ... 32767
DInt	-2147483648 ... 2147483647
Real	1.175495E-38 ... 3.402823E+38
LReal	2.225073E-308 ... 1.797693E+308

Hinweis**Grenzwert 0 (null)**

- Bei den meisten Modulen wird die Eingabe des Werts 0 als deaktivierter Grenzwert interpretiert.
Ausnahmen:
- Bei folgenden Modulen ist auch 0 als Grenzwert möglich:
 - CP 1243-7 LTE V3.3
 - TIM 1531 IRC V2.2

Die folgende Tabelle gibt die Bereiche einer 32-Bit-Zahl an in Bezug auf den Bereiche des Rohwerts einer analogen Eingabe- bzw. Ausgabebaugruppe.

Bereich	Wert der 16 Bit-PLC-Variable *		Baugruppenausgang [mA]			Messbereich [%]
	Dezimal	Hexadezimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
Überlauf	32767	7FFF	> 23,515	> 23,515	> 22,810	> 117,593
Übersteuerungs-Bereich	32511	7EFF	23,515	23,515	22,810	117,593
	... 27649	... 6C01	... 20,001	... 20,001	... 20,001	... 100,004
Nennbereich (unipolar / life zero)	27648	6C00	20		20	100
	... 0	... 0000	... 0		... 4	... 0
Nennbereich (bipolar)	27648 ...	6C00 ...		20 ...		100 ...
	0	0000		0		0
	... -27648	... 9400		... -20		... -100
Untersteuerungs-Bereich (unipolar / life zero)	-1	FFFF	-0,001		3,999	-0,004
	... -4864	... ED00	... -3,518		... 1,185	... -17,59
Untersteuerungs-Bereich (bipolar)	-27649	93FF		-20,001		-100,004
	... -32512	... 8100		... -23,516		... -117,593
Unterlauf / Drahtbruch	-32768	8000	< -3,518		< 1,185	< -17,593

* Die Wertebereiche (Unterlauf / Überlauf) bei PLC-Variablen mit verschiedenen Datentypen liegen wie folgt:

- Int
 - -32768
 - 32767
- DInt
 - -2147483648
 - 2147483647
- Real
 - -3.4000E+038
 - 3.4000E+038
- LReal
 - -1.7000E+308
 - 1.7000E+308

Hinweis

Auswertung des Werts auch bei deaktivierter Option

Wenn Sie eine oder beide Optionen aktivieren und einen Wert projektieren und danach die Option wieder deaktivieren, dann wird der ausgegraute Wert trotzdem ausgewertet.

Löschen Sie zur Deaktivierung der beiden Optionen die zuvor projizierten Grenzwerte aus den Eingabefeldern und deaktivieren Sie erst dann die jeweilige Option.

3.22.12 Befehlsoptionen

Ausgabeoptionen

Die Ausgabeoptionen entsprechen der Spezifikation IEC 60870-5-101 - Qualifier of command.

Parameter

Die beiden Ausgabeoptionen unter "Control Code" können alternativ aktiviert werden:

- **LATCH_ON/OFF**

- Qualifier of command - QU (Type 1.1) <1> persistent output

Die Funktion verriegelt einen Befehlsausgang dauerhaft auf den Wert 0 oder 1.

Beachten Sie:

Der verriegelte Wert wird erst durch einen neuen Befehl aufgehoben. Alternativ kann der Befehl vom Anwenderprogramm zurückgesetzt werden.

- **PULSE_ON**

Qualifier of command - QU (Type 1.1)

Die Funktion wertet Anzahl und Länge der Signale (Pulse) von Befehlsausgängen der Zentrale aus.

Kodierung:

- <1> short pulse duration

Korrespondierender Parameter beim Modul: "Kurze Pulsdauer"

- <2> long pulse duration

Korrespondierender Parameter beim Modul: "Lange Pulsdauer"

Die Ausgabeoption "Befehlsmodus" kann unabhängig aktiviert werden:

- **Befehlsmodus**

Qualifier of command / Qualifier of set-point command - S/E (Type 6)

Kodierung:

- <0> execute

- <1> select

Die Funktion legt fest, ob ein Befehl direkt an die CPU übertragen wird (direct command transmission) oder ob nach der Anwahl (select) eine Ausführungsbestätigung (execute) erwartet wird, bevor der Befehl weitergeleitet wird.

Das Stationsmodul quittiert den Empfang der Anwahl-ASDU mit dem Qualifier <1> select.

Der Master sendet nach Empfang der Quittung die Ausführungs-ASDU mit dem Qualifier <0> execute".

Verarbeitung

- LATCH_ON/OFF
Die Funktion verriegelt den Wert eines Befehls wie oben beschrieben.
- PULSE_ON/OFF
Die Funktion wird vom Master über einen "Qualifier of command" kodiert. Folgende Kodierungen werden vom Kommunikationsmodul in der Station ausgewertet:
 - QU (Type 1.1) <0> no additional definition
Korrespondierender Parameter beim Modul: "Puls-Steuerung"
 - QU (Type 1.1) <1> short pulse duration
Korrespondierender Parameter beim Modul: "Kurze Pulsdauer"
 - QU (Type 1.1) <2> long pulse duration
Korrespondierender Parameter beim Modul: "Lange Pulsdauer"
 - S/E (Type 6) <0> execute
Korrespondierender Parameter beim Modul: "Befehlsmodus"
 - S/E (Type 6) <1> select
Korrespondierender Parameter beim Modul: "Befehlsmodus"

Datenpunkttypen

Die Ausgabeoptionen sind für folgende Datenpunkttypen projektierbar:

- Control Code (LATCH_ON/OFF / PULSE_ON)
 - Single command ... <45>, <58>
 - Double command ... <46>, <59>
 - Regulating step command ... <47>, <60>
- Befehlsmodus
 - Single command ... <45>, <58>
 - Double command ... <46>, <59>
 - Regulating step command ... <47>, <60>
 - Set-point command ... <48>, <49>, <61>, <62>

Parameter

Name: **Control Code**
Wertebereich:

- PULSE_ON
- LATCH_ON/OFF

Erläuterung: Ausgabeoption des Befehlsausgangs. Zur Bedeutung siehe oben.

Name: **Puls-Anzahl / Max. Pulsanzahl**
Vorbelegung: 1
Erläuterung: Anzahl der Pulse, die der Datenpunkt des Masters an den korrespondierenden Datenpunkt der Station überträgt.
Bei der Station überwacht der Parameter die vom Master gesendete Anzahl der Pulse. Wenn die vom Master empfangene Pulsanzahl den vorgegebenen Wert übersteigt, wird der Befehl verworfen.

Name: **Puls-Steuerung**
(nur "Double command")
Wertebereich:

- Kurze Pulsdauer
- Lange Pulsdauer

Erläuterung:

- Kurze Pulsdauer
Kurze Pulse sind für zeitkritische Vorgänge vorgesehen, beispielsweise zur Steuerung von Leistungsschaltern.
- Lange Pulsdauer
Lange Pulse sind für zeitunkritische Vorgänge vorgesehen.

Name: **Kurze Pulsdauer (s)**
Wertebereich: 0 ... 65535
Vorbelegung: 0
Erläuterung: Befehle vom Master mit dem Qualifier of command = <1> (short pulse duration) werden vom Kommunikationsmodul für die hier projektierte Zeitdauer ausgegeben.
Wenn "Kurze Pulsdauer" mit 0 (null) projektiert ist, werden Befehle mit dem Qualifier of command von <1> vom Modul verworfen.

Name: **Lange Pulsdauer (s)**
Wertebereich: 0 ... 65535
Vorbelegung: 0
Erläuterung: Befehle vom Master mit dem Qualifier of command = <2> (long pulse duration) werden vom Kommunikationsmodul für die hier projektierte Zeitdauer ausgegeben.
Wenn "Lange Pulsdauer" mit 0 (null) projektiert ist, werden Befehle mit dem Qualifier of command von <2> vom Modul verworfen.

Name: **Befehlsmodus**
Wertebereich:

- Direkte Ausführung
- Anwahl und Ausführung

Vorbelegung: Direkte Ausführung

- Erläuterung:
- Direkte Ausführung
"direct command transmission"
Der Befehl wird sofort an die CPU der Station zur Ausführung übertragen.
 - Anwahl und Ausführung
"select / execute"
Ablauf:
 - Auslösen des Befehls im Master-Modul
Das "Anwahl"-Telegramm wird von der Zentrale an das Kommunikationsmodul der Station übertragen.
 - Die Station quittiert den Empfang.
 - Der Master-Datenpunkt sendet das Ausführungs-Telegramm nach Empfang der Quittung der Station.
 - Die Station leitet den Befehl erst dann an die CPU weiter, wenn sie innerhalb der projektierten "Max. Zeit zwischen Select und Operate" das "Ausführungs"-Telegramm des Masters empfängt.
Die Station darf zwischen Anwahl und Ausführung kein anderes Daten-Telegramm empfangen.
- Hinweis: "Max. Zeit zwischen Select und Operate" wird in den Übertragungseinstellungen der jeweiligen Schnittstelle projektiert.

3.22.13 Partnerstationen

Aktivierung der Partner des Datenpunkts

In der Tabelle werden diejenigen Stationen als Partner angezeigt, mit denen eine Telecontrol-Verbindung projektiert wurde.

Aktivieren Sie den oder diejenigen Partner, mit denen der selektierte Datenpunkt Daten austauschen soll, über das Optionskästchen:

3.23 Nachrichten

Projektierung der Nachrichten

Bei wichtigen Ereignissen kann das Kommunikationsmodul projektierte Nachrichten absetzen. Für die Projektierung müssen keine Programmbausteine eingesetzt werden.

Für die Übertragung von Nachrichten muss die Telecontrol-Kommunikation (Parametergruppe "Kommunikationsarten") nicht mehr aktiviert werden.

Projektierbar sind:

- E-Mails
Empfänger kann ein PC mit Internetanschluss oder eine S7-Station sein.
- SMS (nur Mobilfunk-CPs oder TIM-Baugruppen)
Empfänger kann ein Mobiltelefon oder eine S7-Station sein.

Pro Modul können bis zu 10 Nachrichten (E-Mail oder SMS) projiziert werden.

Die Nachrichten projizieren Sie im Nachrichteneditor des Moduls. Diesen finden Sie alternativ über:

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

Zur Ansicht in STEP 7 siehe Kapitel Datenpunktprojektierung (Seite 115).

Auslösen der Nachrichtenübertragung

Das Versenden der Nachricht wird über ein Ereignis ausgelöst, das im Register "Trigger" projiziert wird (siehe unten).

Voraussetzungen, benötigte Informationen und Vorgehensweise

E-Mails

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

- Aktivierung der Telecontrol-Kommunikation (Parametergruppe "Kommunikationsarten")
- Aktivierung der Security-Funktionen
- Projektierung der Parametergruppe "E-Mail-Projektierung"

Benötigte Informationen:

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

Die Zugangsdaten zum Mobilfunknetz und zu einem APN für die Übertragung von E-Mails erhalten Sie von Ihrem Netzbetreiber. Diese projizieren Sie in der Parametergruppe "Mobilfunk-Kommunikationseinstellungen".

Die Projektierung nehmen Sie in folgenden Parametergruppen vor:

- Aktivierung der Security-Funktionen
Für die Nutzung von E-Mails müssen Sie die Security-Funktionen des CP aktivieren, Parametergruppe "Security".
- Projektierung des Dienstes / Protokolls:
"E-Mail-Projektierung"
- Bei Nutzung von STARTTLS oder SSL/TLS:
 - Import des Zertifikats des E-Mail-Dienst-Betreibers:
"Globale Security-Einstellungen"
 - Verwendung des importierten Zertifikats für das Modul:
Parametergruppe "Security" > "Zertifikatsmanager"

SMS (Mobilfunk-CPs oder TIM)

Benötigte Informationen:

- Nummer des SMSC

Die Projektierung nehmen Sie in folgenden Parametergruppen vor:

- Aktivierung der SMS-Funktion:
"Kommunikationsarten" > "SMS aktivieren"
- Projektierung des SMSC
"Mobilfunk-Kommunikationseinstellungen"
- Projektierung der SMS
Nachrichteneditor

"Nachrichtenparameter"

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

Text: Anzahl Zeichen

Maximale Anzahl an Zeichen, die im Nachrichtentext übertragen werden können:

- SMS: Max. 160 ASCII-Zeichen inklusive eines evtl. mitgeschickten Werts
- E-Mail: 256 ASCII-Zeichen inklusive eines evtl. mitgeschickten Werts

Zum Wert siehe unten, Parameter "Wert mitschicken".

Zeichensatz für Nachrichtentexte

Angabe der nachfolgenden zugelassenen Zeichen als ASCII-Zeichensätze (Hexadezimalwert und Zeichenname):

- 0x20
Leerzeichen
- 0x21 ... 0x5F
!"#\$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN OPQRS
TUVWXYZ[\]^_
- 0x61 ... 0x7E
abcdefghijklmnopqrstuvwxy z{|}~
- 0x7C, 0x7E
|~
- Manueller Zeilenumbruch (↵)
In Nachrichtentexten können Sie einen Zeilenumbruch über <Shift>+<Enter> einfügen.

"Trigger"

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

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

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

- **PLC-Variable verwenden**

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

Rücksetzen des Trigger-Bits:

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

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

Hinweis

Schnelles Setzen der Diagnose-Trigger-Variable

Trigger sollten nicht öfter als einmal pro Sekunde gesetzt werden.

Häufiges Senden von SMS

Das Versenden einer SMS kann abhängig von der Systemumgebung bis zu 2 Minuten dauern. Um bei Mobilfunkmodulen eine sichere Übertragung von SMS zu gewährleisten, wird empfohlen, für das Auslösen von SMS einen Mindestabstand von 10 Sekunden einzuhalten.

- **CPU geht in STOP**

- **CPU geht in RUN**
- **Verbindung zu einem Partner unterbrochen**

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

Zur Festlegung des Partners siehe unten, Parameter "Partner für Trigger".
- **Verbindung zu einem Partner aufgebaut**

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

Zur Festlegung des Partners siehe unten, Parameter "Partner für Trigger".
- **Verbindungsaufbau zu einem Partner fehlgeschlagen**

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

(Mobilfunk-CPs)

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

(Mobilfunk-CPs)

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

(Nur SMS)

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

(CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

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

(CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

Löst das Senden der Nachricht aus, wenn die VPN-Verbindung unterbrochen wird.
- **SINEMA RC-Verbindung aufgebaut**

(CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

Löst das Senden der Nachricht aus, wenn die VPN- bzw. OpenVPN-Verbindung aufgebaut wird oder wiederkehrt.
- **SINEMA RC-Verbindung abgebaut**

(CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

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

- **Partner für Trigger**

Hier wählen Sie aus den projektierten Partnern des Geräts denjenigen aus, dessen Verbindung in den Trigger-Optionen "Verbindung zu einem Partner aufgebaut" bzw. "Verbindung zu einem Partner unterbrochen" betroffen ist.

- **PLC-Variable für Trigger**

PLC-Variable für den Trigger "PLC-Variable verwenden"

- **Kennung für Bearbeitungsstatus aktivieren**

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

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

Zur Bedeutung der hexadezimal ausgegebenen Status siehe Kapitel Bearbeitungsstatus der Nachrichten (SMS, E-Mail) (Seite 166).

- **PLC-Variable für Bearbeitungsstatus**

PLC-Variable vom Typ DWORD für den Bearbeitungsstatus

- **Wert mitschicken**

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

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

\$\$ als Platzhalter für den Wert einer PLC-Variable unterstützt folgende Datentypen:

- Bool, Byte, Char, USInt, Int, UInt, Word, DWord, UInt, DInt, Real, String
- Arrays dieser Datentypen

- **PLC-Variable für Wert**

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

Fehlermeldungen

Wenn beim Übersetzen der Station eine Fehlermeldung zum Trigger-Typ angezeigt wird, dann prüfen Sie die Projektierung.

Haben Sie als Trigger-Typ für die Nachricht eine der folgenden Optionen projektiert:

- VPN / IPSec / SINEMA RC
- Prüfen Sie Folgendes:
 - Sind die Security-Funktionen aktiviert?
 - Ist VPN aktiviert?
 - Sind weitergehende Optionen richtig eingestellt?

3.24 Zeichensatz für Benutzernamen, Passwörter und Nachrichten

Zeichensatz für Benutzernamen, Passwörter und Nachrichtentexte

Die nachfolgenden zugelassenen Zeichen gelten für:

- E-Mail-Server:
 - Benutzername und Passwort
- Nachrichten im Nachrichteneditor:
 - Nachrichtentexte

Angabe als ASCII-Zeichensätze (Hexadezimalwert und Zeichenname):

- 0x20
Leerzeichen
- 0x21 ... 0x5F
! " # \$ % & ' () * + , - . / 0 1 2 3 4 5 6 7 8 9 ; : < = > ? @ A B C D E F G H I J K L M N O P Q R S
T U V W X Y Z [\] ^ _
- 0x61 ... 0x7E
a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
- 0x7C, 0x7E
| ~

Zusätzlich für Nachrichtentexte:

- Manueller Zeilenumbruch (↵)

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

Inbetriebnahme

4.1 CP in Betrieb nehmen

Voraussetzung: Projektierung vor Inbetriebnahme

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

Baugruppe in Betrieb nehmen

Die weitere Inbetriebnahme umfasst folgende Schritte:

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

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 CPU an.

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

4.2 Uhrzeit bei Betrieb mit Security / SINEMA RC stellen

Uhrzeit bei der Inbetriebnahme manuell stellen

Hinweis

Uhrzeitsynchronisation bei Nutzung von Security / SINEMA RC

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

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

Empfehlung:

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

Diagnose und Instandhaltung

5.1 Diagnosemöglichkeiten

Die folgenden Diagnosemöglichkeiten stehen bei den meisten Modulen zur Verfügung. Einige Funktionen sind auf bestimmte Gerätetypen bzw. Protokolle beschränkt.

LEDs der Baugruppe

Informationen zu den LED-Anzeigen finden Sie im Gerätehandbuch des jeweiligen Moduls.

STEP 7: Das Register "Diagnose" im Inspektorfenster

Wenn Ihre Engineering-Station über Ethernet mit einem Modul verbunden ist, erhalten Sie hier folgende Informationen zur selektierten Baugruppe:

- Verbindungszustand der Engineering-Station mit dem Modul

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

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

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

Online-Zugänge

Hier stellen Sie die Online-Verbindung zur Baugruppe her.

Zur Vorgehensweise siehe STEP 7-Informationssystem.

Diagnose

Hier erhalten Sie folgende statische Informationen zur selektierten Baugruppe:

- **Allgemein**
Allgemeine Angaben zur Baugruppe
- **Diagnosestatus > Gerätespezifische Ereignisse**
Hier finden Sie die Diagnosepuffereinträge des Moduls und eine Übersicht der gesendeten Nachrichten (SMS / E-Mails).
- **Diagnosepuffer**
Hier finden Sie die Einträge in den Diagnosepuffer der TIM.
- **Ethernet-Schnittstelle[X1/2/3]**
Adress- und statistische Angaben

- **Industrial Remote Communication**

Hier erhalten Sie WAN-spezifische Informationen zur TIM-Baugruppe:

- **Partner**

Hier finden Sie Adress- und Projektierungsdaten der Partner, eine Verbindungsstatistik und weitere Diagnoseinformationen. Klicken Sie auf einen Teilnehmer zur Anzeige weiterer Informationen.

Informationen zu den Partnern finden auch im WBM, siehe unten.

- **Datenpunktliste**

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

- **Telegrammprotokoll-Diagnose**

Mit dieser Funktion können Sie die Protokollierung von Telegrammen des Moduls aktivieren, auswerten und anzeigen.

Zur Beschreibung siehe Kapitel Telegrammprotokoll-Diagnose (Seite 163).

- **Ethernet-Diagnose**

Mit der Funktion des Logging können Sie zu Diagnosezwecken den Datenverkehr der TIM über PCAP-Funktionalität protokollieren.

Im Fehlerfall oder bei unerwünschtem Verhalten der TIM kann das Kommunikationsverhalten der TIM aufgezeichnet werden. Über einen definierten Zeitraum oder für eine projektierbare Anzahl an Telegrammen wird der Telegrammverkehr der TIM aufgezeichnet.

Die Log-Dateien wird als PCAP-Datei auf dem angeschlossenen PC gespeichert und kann beispielsweise mit dem Programm Wireshark ausgewertet werden.

- **Uhrzeit**

Angabe der aktuellen Uhrzeit im Modul und der Uhrzeitquelle. Möglichkeit, die Uhrzeit im Modul zu stellen.

Funktionen

Hier können Sie folgende Funktionen ausführen:

- **Firmware-Aktualisierung**
- **IP-Adresse zuweisen**
- **PROFINET-Gerätenamen vergeben**
- **Rücksetzen auf Werkseinstellungen**

Zu den Funktionen siehe Kapitel Instandhaltung (Seite 168).

Webserver (WBM) der TIM 1531 IRC

Von einem PC aus können Sie über HTTP/HTTPS auf die Webseiten (WBM) der TIM zugreifen. Das WBM liefert diverse Informationen.

Zum Zugriff und den Inhalten siehe Kapitel WBM der TIM 1531 IRC (Seite 193).

Partnerstatus und Verbindungszustände im WBM

Sie sehen die projektierten Partner und den Zustand der Verbindungen zu den lokalen und remoten Kommunikationspartnern der TIM auf der Seite "Telecontrol" > "Partnerinformationen" des WBM. Zu Details siehe Kapitel Partnerinformationen (Seite 206).

Partner- und Verbindungs-Informationen an die CPU

Die TIM kann ihrer lokalen CPU den Zustand der Verbindung und der Verbindungswege zum Kommunikationspartner über eine PLC-Variable signalisieren. Zur Projektierung siehe Kapitel Kommunikation mit der CPU (Seite 66).

SNMP

Zu den Funktionen siehe Kapitel SNMP (Seite 165).

5.2 Webserver S7-1200: Verbindungsaufbau

Verbindung mit dem Webserver der CPU aufbauen

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

Voraussetzungen in der Projektierung der CPU

1. Öffnen Sie an der Engineering-Station das entsprechende Projekt.
2. Selektieren Sie in STEP 7 die CPU der betreffenden Station.
3. Selektieren Sie den Eintrag "Webserver".
4. Aktivieren Sie in der Parametergruppe "Allgemein" die Option "Webserver auf dieser Baugruppe aktivieren".
5. Legen Sie bei einer CPU ab Version V4.0 in der Benutzerverwaltung einen Benutzer mit den erforderlichen Rechten an.

Abhängig davon, ob Sie in der Parametergruppe "Allgemein" die Option "Zugriff nur über HTTPS zulassen" aktiviert oder deaktiviert haben, unterscheidet sich die Vorgehensweise zum Verbindungsaufbau mit dem Webserver:

- **Verbindungsaufbau über HTTP**

Vorgehensweise bei deaktivierter Option "Zugriff nur über HTTPS zulassen"

- **Verbindungsaufbau über HTTPS**

Vorgehensweise bei aktivierter Option "Zugriff nur über HTTPS zulassen"

Die beiden Varianten sind in den folgenden Abschnitten beschrieben.

Die Voraussetzungen für den Zugriff auf den Webserver der CPU (zugelassene Webbrowser) und die Beschreibung der Vorgehensweise finden Sie im STEP 7-Informationssystem unter dem Stichwort "Wissenswertes zum Webserver".

Verbindungsaufbau über HTTP

1. Verbinden Sie den PC über die Ethernet-Schnittstelle mit der CPU.
2. Geben Sie die Adresse der CPU in das Adressfeld Ihres Webbrowsers ein: `http://<IP-Adresse>`
3. Drücken Sie die Eingabetaste <Enter>.
Die Startseite des Webserver öffnet sich.
4. Klicken Sie auf den Eintrag "Download-Zertifikat" rechts oben im Fenster.
Das Dialogfeld "Zertifikat" öffnet sich.
5. Laden Sie das Zertifikat auf Ihren PC, indem Sie auf die Schaltfläche "Zertifikat installieren ..." klicken.
Das Zertifikat wird auf Ihren PC geladen.
Informationen zum Laden eines Zertifikats finden Sie in der Hilfe Ihres Webbrowsers und im STEP 7-Informationssystem unter den Stichworten "HTTPS" bzw. "Zugriff für HTTPS (S7-1200)".
6. Wenn die Verbindung in den sicheren Modus HTTPS gewechselt ist ("`https://<IP-Adresse>/...`" im Adressfeld des Webserver), dann können Sie fortfahren, wie im nachfolgenden Abschnitt beschrieben.
Wenn Sie die Verbindung zum Webserver trennen, dann können Sie sich das nächste Mal ohne das Laden des Zertifikats über HTTP am Webserver anmelden.

Verbindungsaufbau über HTTPS

1. Verbinden Sie den PC über die Ethernet-Schnittstelle mit der CPU.
2. Geben Sie die Adresse der CPU in das Adressfeld Ihres Webbrowsers ein: `https://<IP-Adresse>`
3. Drücken Sie die Eingabetaste <Enter>.
Die Startseite des Webserver öffnet sich.
4. Melden Sie sich auf der Startseite des Webserver als Benutzer mit den erforderlichen Rechten an.
Verwenden Sie die in der Benutzerverwaltung des Webserver der CPU projizierten Benutzerdaten.
5. Wählen Sie nach der Anmeldung in der Navigation des Webserver den Eintrag "Baugruppenzustand".
6. Selektieren Sie in der Baugruppenliste den CP.
Die CP-spezifischen Inhalte werden angezeigt.

5.3 Online-Security-Diagnose über Port 8448

Security-Diagnose über Port 8448

Voraussetzungen:

- Bei aktivierter Firewall muss der Zugang freigegeben sein.

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

1. Selektieren Sie in STEP 7 den CP.
 2. Öffnen Sie das Kontextmenü "Online & Diagnose".
 3. Klicken Sie in der Parametergruppe "Security" auf die Schaltfläche "Online verbinden".
- Über diesen Weg führen Sie die Security-Diagnose über Port 8448 aus.

5.4 Telegrammprotokoll-Diagnose

Die SINAUT-Spezial-Diagnose steht für folgende Module zur Verfügung:

- S7-1200-Telecontrol-CPs
- TIM 1531 IRC

5.4.1 Telegrammprotokoll: Aufbau und Funktionen

Die Diagnosefunktion "Telegrammprotokoll" dient der Aufzeichnung von übertragenen Telegrammen.

Zur Aktivierung der Funktion siehe Absatz "Bedienung" unten.

Aufbau des Dialogs "Telegrammprotokoll"

Nach Aktivierung zeigen die Spalten folgende Daten:

- Nr.
 - Symbol für ein- bzw. ausgehende Telegramme
 - Telegramm-Nummer, fortlaufend nummeriert.
- Block
Länge des Telegrammblocks, in dem das Telegramm übertragen wurde.
- Header-Felder
Hexadezimale Darstellung einiger Header-Daten
Zur Bedeutung siehe Kapitel Details (Seite 164).
- Teilnehmer (Quelle / Ziel)
Teilnehmernummern des sendenden (Quelle) und empfangenden Teilnehmers (Ziel)
- Objekt (Quelle / Ziel)
Objektnummer des Datenobjekts im Telegramm beim Quell- und Ziel-Teilnehmer
- Index
Adressparameter für Nettodaten bei Datentelegrammen (Kanalnummer)

- Datum, Zeit und Status
Zeitstempel des Telegramms und Zeit-Status vom Zeitpunkt der Übertragung
Zur Darstellung siehe Kapitel Details (Seite 164).
- Nettodaten
Hexadezimale Darstellung der Nettodaten des Telegramms
Zur Bedeutung siehe Kapitel Details (Seite 164).

Bedienung

Sie bedienen die Funktion über die drei Schaltflächen unterhalb des oben beschriebenen Dialogs.

- Telegrammprotokoll-Diagnose aktivieren
Durch Klicken auf die Schaltfläche wird die Protokollierung der übertragenen Telegramme gestartet.
Pro Aufzeichnungszyklus werden 400 Telegramme aufgezeichnet. Maximal können 10000 Telegramme in einem Ringpuffer gespeichert werden.
- Aktualisieren
Aktualisiert die Aufzeichnung; ein neuer Aufzeichnungszyklus wird gestartet.
- Speichern
Speichert die aufgezeichneten Telegramme in einer Binärdatei. Über die Schaltfläche legen Sie den Speicherort fest.
- Gespeichert anzeigen
Zeigt die aufgezeichneten und gespeicherten Telegramme an.

5.4.2 Details

Detailinformationen

Header-Felder

Die 5 hexadezimal ausgegebenen Felder haben folgende Bedeutung:

- 1. Feld: Telegrammzähler
0...7
- 2. Feld: Kontroll-Code
- 3. Feld: Funktionsauswahl
 - 0: Bearbeitung in TIM
 - 1: Bearbeitung in CPU

- 4. Feld: Adresserweiterung
 - 0: ST1-Telegramm ohne Adresserweiterung
 - 1: ST1-Telegramm mit Adresserweiterung
 - 2: ST7-Telegramm
- 5. Feld: Richtungsbit
 - 0: Überwachungsrichtung
 - 1: Steuerungsrichtung

Nettodaten

Die Spalte zeigt die Nettodaten des Telegramms.

Die Werte werden hexadezimal angezeigt.

Datum, Zeit und Status

Die Spalte zeigt in den Zeitstempel des Telegramms in folgendem Format:

Jahr/Monat/Tag_Stunde:Minute:Sekunde_Zeit-Status

Belegung des Zeit-Status:

- 2^0
 - 0: Zeit ist ungültig
 - 1: Zeit ist gültig
- 2^1
 - 0: Winterzeit (Normalzeit)
 - 1: Sommerzeit
- 2^2

Nicht belegt
- 2^3
 - 0: Keine Bedeutung
 - 1: Ankündigungszeit für Sommer-Winterzeit-Umschaltung

Nur im Zeitsynchronisations-Telegramm

5.5 SNMP

SNMP (Simple Network Management Protocol)

SNMP ist ein Protokoll für die Verwaltung und Diagnose 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.

Leistungsumfang der Module als SNMP-Agent

Nicht alle der nachfolgend beschriebenen Funktionen stehen für jedes Modul zur Verfügung. Informieren Sie sich im Gerätehandbuch des jeweiligen Moduls über den Funktionsumfang.

Die Kommunikationsmodule unterstützen die Datenabfrage in folgenden SNMP-Versionen:

- SNMPv1 (Standard)
- SNMPv3 (Security)

Sie liefern dabei die Inhalte von MIB-Objekten der Standard-MIB II gemäß RFC1213.

- **MIB II**

Die MIB unterstützt folgende Gruppen von MIB-Objekten:

- System
- Interfaces

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

- IP
- ICMP
- TCP
- UDP
- SNMP

Die folgenden Gruppen der Standard-MIB II werden nicht unterstützt:

- Adress Translation (AT)
- EGP
- Transmission

Traps werden von den Modulen nicht unterstützt.

Weitere Informationen über die MIB-Dateien und SNMP finden Sie im Handbuch /9/ (Seite 227).

Projektierung

Zur Projektierung siehe Kapitel SNMP (Seite 76).

5.6 Bearbeitungsstatus der Nachrichten (SMS, E-Mail)

Bearbeitungsstatus von Nachrichten

Wenn im Register "Trigger" der Nachrichtenprojektierung von STEP 7 diese Option "Kennung für Bearbeitungsstatus aktivieren" gesetzt ist, gibt das Modul einen Status aus.

Der Bearbeitungsstatus gibt Auskunft über den Bearbeitungszustand der gesendeten Nachricht. Der Status wird in eine PLC-Variable vom Typ DWORD geschrieben. Wählen Sie diese Variable über das Feld "PLC-Variable für Bearbeitungsstatus" aus.

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

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

Die gelieferten Status haben folgende Bedeutung:

Bearbeitungsstatus der Telecontrol-Nachrichten

Tabelle 5- 1 SMS: Bedeutung der hexadezimal ausgegebenen Statuskennung

Status	Bedeutung
0000	Übertragung fehlerfrei abgeschlossen
0001	Fehler bei der Übertragung; mögliche Ursachen: <ul style="list-style-type: none"> • SIM-Karte nicht gültig • Kein Netz • Falsche Zielrufnummer (Nummer nicht erreichbar)

Tabelle 5- 2 E-Mail: Bedeutung der hexadezimal ausgegebenen Statuskennung

Status	Bedeutung
0000	Übertragung fehlerfrei abgeschlossen
82xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht die Meldung der dreistelligen Fehlernummer des Protokolls SMTP.
8401	Kein Kanal verfügbar. Mögliche Ursache: Es besteht bereits eine E-Mail-Verbindung über das Modul. Eine zweite Verbindung kann nicht parallel eingerichtet werden.
8403	Es konnte keine TCP/IP-Verbindung zum SMTP-Server aufgebaut werden.
8405	Der SMTP-Server hat die Login-Anfrage verweigert.
8406	Ein interner SSL-Fehler oder ein Problem mit der Struktur des Zertifikats wurde durch den SMTP-Client festgestellt.
8407	Anfrage zur Verwendung von SSL wurde verweigert.
8408	Der Client konnte kein Socket zur Erstellung einer TCP/IP-Verbindung zum Mail-Server ermitteln.
8409	Über die Verbindung kann nicht geschrieben werden. Mögliche Ursache: Durch den Kommunikationspartner wurde ein Reset der Verbindung durchgeführt oder die Verbindung wurde abgebrochen.
8410	Über die Verbindung kann nicht gelesen werden. Mögliche Ursache: Durch den Kommunikationspartner wurde die Verbindung abgebaut oder die Verbindung wurde abgebrochen.
8411	Senden der E-Mail fehlgeschlagen. Ursache: Speicherplatz war nicht ausreichend, um den Sendevorgang durchzuführen.
8412	Konfigurierter DNS-Server konnte den angegebenen Domain-Namen nicht auflösen.
8413	Aufgrund eines internen Fehlers im DNS-Subsystem konnte der Domain-Name nicht aufgelöst werden.
8414	Als Domain-Name wurde eine leere Zeichenkette angegeben.
8415	Ein interner Fehler ist im Curl-Modul aufgetreten. Ausführung wurde abgebrochen.
8416	Ein interner Fehler ist im SMTP-Modul aufgetreten. Ausführung wurde abgebrochen.
8417	Anfrage an SMTP auf bereits verwendetem Kanal oder ungültige Kanal-ID. Ausführung wurde abgebrochen.

Status	Bedeutung
8418	Senden der E-Mail wurde abgebrochen. Mögliche Ursache: Überschreitung der Ausführungszeit.
8419	Der Kanal wurde unterbrochen und kann nicht verwendet werden, bevor die Verbindung abgebaut wird.
8420	Zertifikatskette vom Server konnte nicht mit dem Root-Zertifikat des Moduls verifiziert werden.
8421	Interner Fehler aufgetreten. Ausführung wurde gestoppt.
8450	Aktion nicht ausgeführt: Mailbox nicht verfügbar / nicht erreichbar. Versuchen Sie es später noch einmal.
84xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht die Meldung der dreistelligen Fehlernummer des Protokolls SMTP.
8500	Syntax-Fehler: Kommando unbekannt. Das schließt auch den Fehler einer zu langen Befehlskette ein. Ursache kann sein, dass der E-Mail-Server das Authentifizierungsverfahren LOGIN nicht unterstützt. Versuchen Sie, E-Mails ohne Authentifizierung zu versenden (kein Benutzername).
8501	Syntax-Fehler. Überprüfen Sie die folgenden Projektierungsdaten: Meldungskonfiguration > E-Mail-Daten (Content): <ul style="list-style-type: none"> • Empfängeradresse ("An" bzw. "Cc").
8502	Syntax-Fehler. Überprüfen Sie die folgenden Projektierungsdaten: Meldungskonfiguration > E-Mail-Daten (Content): <ul style="list-style-type: none"> • E-Mail-Adresse (Absender)
8535	SMTP-Authentifizierung unvollständig. Überprüfen Sie in der Projektierung die Parameter "Benutzername" und "Passwort".
8550	SMTP-Server kann nicht erreicht werden. Sie haben keine Zugriffsrechte. Überprüfen Sie die folgenden Projektierungsdaten: <ul style="list-style-type: none"> • Baugruppen-Projektierung > E-Mail-Projektierung: <ul style="list-style-type: none"> – Benutzername – Passwort – E-Mail-Adresse (Absender) • Meldungskonfiguration > E-Mail-Daten (Content): <ul style="list-style-type: none"> – Empfängeradresse ("An" bzw. "Cc").
8554	Übertragung fehlgeschlagen
85xx	Sonstige Fehlermeldung vom E-Mail-Server Bis auf die führende "8" entspricht die Meldung der dreistelligen Fehlernummer des Protokolls SMTP.

5.7 Instandhaltung

Instandhaltungsfunktionen

Die Beschreibung der folgenden Instandhaltungsfunktionen finden Sie im Gerätehandbuch bzw. in der Betriebsanleitung des jeweiligen Moduls, siehe Literaturverzeichnis (Seite 225).

- Firmware-Aktualisierung
- Rücksetzen
- Baugruppentausch

OUC-Programmbausteine (CP)

A.1 Gültigkeit und Voraussetzungen

Gültigkeit

Die nachfolgend beschriebenen Funktionen werden von folgenden Modulen unterstützt:

- CP 1243-1
 - Ab Firmware \geq V3.1
- CP 1243-7 LTE
 - Ab Firmware \geq V3.1
- CP 1243-8 IRC
 - Ab Firmware \geq V3.1
- CP 1542SP-1 IRC
 - Ab Firmware \geq V2.0

Beachten Sie die Abweichungen der Firmware-Versionen für die gesicherte Kommunikation (Secure OUC), siehe unten.

A.2 Programmbausteine für OUC

Verwendung der Programmbausteine für die Open User Communication (OUC)

Die unten aufgeführten Anweisungen (Programmbausteine) können Sie für die direkte Kommunikation zwischen S7-Stationen nutzen.

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

Hinweis

Keine unterschiedlichen Programmbaustein-Versionen

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

Voraussetzungen für Secure OUC

Voraussetzungen für die Nutzung der gesicherten Übertragung über Secure OUC:

- STEP 7: Ab V16
- CPU-Firmware
 - CPU-1200: Ab V4.4
 - CPU 151xSP: Ab V2.0
- CP-Firmware
 - CP 1200: Ab V3.2
 - CP 1542SP-1 IRC: Ab V2.1

Unterstützte Programmbausteine für OUC

Folgende Anweisungen in der angegebenen Mindestversion stehen für die Parametrierung der Open User Communication zur Verfügung:

- **TSEND_C V3.0 / TRCV_C V3.0**

Kompakte Bausteine für:

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

Verwenden Sie alternativ:

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

Verbindungsaufbau / Verbindungsabbau

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

Senden bzw. Empfangen von Daten über UDP

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

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

- **TMAIL_C V4.0**

Senden von E-Mails

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

Zum Ändern der Projektierungsdaten des Moduls zur Laufzeit:

- **T_CONFIG V1.0**

Programmgesteuerte Konfiguration der IP-Parameter

Beachten Sie die Hinweise zu T_CONFIG und zu den SDTs "IF_CONF_..." im Kapitel Änderung der IP-Adresse zur Laufzeit (Seite 173).

Hinweis

Keine Rückmeldung des CP

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

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

- **TC_CONFIG**

Programmgesteuerte Änderung der Projektierungsdaten von Mobilfunk-CPs

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

Verbindungsbeschreibungen in Systemdatentypen (SDTs)

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

Die Verbindungsbeschreibung wird in einem Datenbaustein abgelegt, dessen Struktur durch einen Systemdatentyp (SDT) festgelegt wird.

Anlegen eines SDT für die Datenbausteine

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

Der SDT-Typ wird erzeugt, indem Sie in der Deklarationstabelle des Bausteins nicht einen Eintrag aus der Klappliste "Datentyp" wählen, sondern in das Feld "Datentyp" manuell den Namen eingeben, beispielsweise "TCON_IP_V4".

Der entsprechende SDT wird dann mit seinen Parametern angelegt.

Verwendbare SDTs

- **TCON_IP_V4**

Für die Übertragung von Telegrammen über TCP oder UDP

- **TCON_QDN**

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

- **TCON_IP_RFC**

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

- **TADDR_Param**
Für die Übertragung von Telegrammen über UDP
- **TMail_V4**
Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv4-Adresse
Empfehlung Für Mobilfunk-Anwendungen:
Setzen Sie den Parameter "WatchdogTime" von "MAIL_ADDR_PARAM" auf einen Wert größer 3 Minuten.
- **TMail_V6**
Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv6-Adresse
- **TMail_FQDN**
Für die Übertragung von E-Mails mit Adressierung des E-Mail-Servers über dessen Namen (FQDN)
- **IF_CONF**
Für die Änderung der Projektierungsdaten von Mobilfunk-CPs mithilfe des TC_CONFIG
- **TCON_IP_V4_SEC**
Nur CP 1200
Für die gesicherte Übertragung von Daten über TCP
- **TCON_QDN_SEC**
Nur CP 1200
Für die gesicherte Übertragung von Daten über den Host-Namen
- **TMail_V4_SEC**
Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv4-Adresse
- **TMail_V6_SEC**
Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über eine IPv6-Adresse
- **TMail_QDN_SEC**
Für die gesicherte Übertragung von E-Mails mit Adressierung des E-Mail-Servers über den Host-Namen

Hinweis zu TMail_Vx_SEC / TMail_QDN_SEC:

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

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

Verbindungs-Auf- und Abbau

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

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

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

Hinweis

Verbindungsabbruch

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

A.3 Änderung der IP-Adresse zur Laufzeit

Änderung der IP-Adresse zur Laufzeit

Sie können folgende Adressparameter des CP zur Laufzeit programmgesteuert ändern:

- IP-Adresse
- Subnetzmaske
- Router-Adresse

Außer den Adress-Parametern des CP können mit T_CONFIG auch die Adress-Parameter von DNS-Servern (IF_CONF_DNS) und NTP-Servern (IF_CONF_NTP) programmgesteuert geändert werden.

Hinweis

Änderung der IP-Parameter bei dynamischer IP-Adresse

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

Voraussetzungen - Projektierung

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

Voraussetzungen - STEP 7-Version

- STEP 7 \geq V14

Voraussetzungen - Firmware-Versionen

- **CP 1243-1 / CP 1243-8 IRC**
 - CP-Firmware \geq V2.1.7x
 - CPU-Firmware \geq V4.2
- **CP 1542SP-1 IRC**
 - CP-Firmware \geq V1
 - CPU-Firmware \geq V2.0 (CPU 151xSP)

Programmbausteine

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

Folgende Programmbausteine und Systemdatentypen können verwendet werden:

- **T_CONFIG**

Zusammen mit:

 - IF_CONF_V4
 - IF_CONF_NTP
 - IF_CONF_V6
 - IF_CONF_DNS

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

Hinweis

Keine Rückmeldung des CP

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

Detaillierte Informationen zur Parametrierung der Bausteine und SDTs finden Sie im STEP 7-Informationssystem.

A.4 SMS über OUC

Verschicken von E-Mails / SMS über OUC

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

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

Hinweis**Häufiges Senden von SMS**

Das Versenden einer SMS kann abhängig von der Systemumgebung bis zu 2 Minuten dauern.

Um eine sichere Übertragung von SMS zu gewährleisten, wird empfohlen, für das Auslösen von SMS einen Mindestabstand von 10 Sekunden einzuhalten.

Dies können Sie beispielsweise über das Setzen des Parameters "REC" bei den Bausteinen TCON und TSEND_C steuern.

SMS über Programmbausteine**SMS an einen Partner senden**

Legen Sie hierzu alternativ folgende Bausteine bzw. Systemdatentypen an:

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

SMS von einem Partner empfangen

Legen Sie hierzu alternativ folgende Bausteine bzw. Systemdatentypen an:

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

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

SMS von mehreren Partnern empfangen

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

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

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

Zu sendender Nachrichtentext am Parameter "DATA"

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

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

Auslesen des Nachrichtentextes am Parameter "DATA"

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

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

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

- DTL
12 Byte für den Zeitstempel der empfangenen SMS (Zeitstempel vom Netz)
- String[22]
String von 22 Byte für den Rufnummer des Absenders (+ 2 Byte String-Header)
- String[160]
String von 160 Byte für den Nachrichtentext (+ 2 Byte String-Header)
Der SMS-Text darf max. 160 Zeichen enthalten.

Die Struktur benötigt pro SMS einen Speicherplatz von 198 Byte.

Speichern der letzten 10 empfangenen SMS

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

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

- Empfangsdaten SMS 1 (DTL, String[22], String[160], Byte)
- Empfangsdaten SMS 2 (DTL, String[22], String[160], Byte)
... bis
- Empfangsdaten SMS 10 (DTL, String[22], String[160], Byte)

Die Empfangsdaten jeder SMS haben folgenden Aufbau:

- DTL
12 Byte für den Zeitstempel der empfangenen SMS (Zeitstempel vom Netz)
- String[22]
String von 22 Byte für den Rufnummer des Absenders (+ 2 Byte String-Header)
- String[160]
String von 160 Byte für den Nachrichtentext (+ 2 Byte String-Header)

- Byte
Status der SMS
Wenn mehr als eine SMS empfangen wird, dann wird für jede SMS der Status in diesem Status-Byte gespeichert:
 - 0 = Ungültig
 - 1 = Ungelesen
 - 2 = Gelesen

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

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

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

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

Zeichensatz für den SMS-Text

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

- 0x0A
LF (Zeilenvorschub)
- 0x0D
CR (Carriage Return)
- 0x20
Leerzeichen
- 0x21 ... 0x5A
!"#\$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPS
TUVWXYZ
- 0x61 ... 0x7A
abcdefghijklmnopqrstuvwxyz

A.5 TC_CONFIG zum Ändern der Projektierungsdaten des CP

Bedeutung

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

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

Der Parameter CONFIG zeigt auf den Speicherbereich mit den Projektierungsdaten. Die Projektierungsdaten werden in einem Datenbaustein (DB) gespeichert. Der DB kann nicht mit optimiertem Bausteinzugriff angelegt werden. Die Struktur des DB wird durch den Systemdatentyp (SDT) IF_CONF_v4 vorgegeben.

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

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

Details zur Parametrierung des SDT IF_CONF_v4 enthält der Abschnitt IF_CONF_*: SDTs für Projektierungsdaten des CP (Seite 180).

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

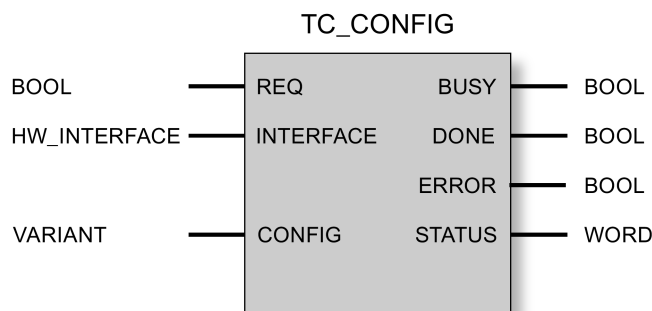
Voraussetzungen

- Um die Funktion nutzen zu können, müssen in der STEP 7-Basisprojektierung des CP bereits projektierte Werte vorhanden sein.
- Für die Nutzung des Parameter-Blocks "IF_CONF_PrefProvider" (bevorzugte Mobilfunknetze) des SDT "IF_CONF_v4":

Das zu nutzende Mobilfunknetz muss in der Projektierung des CP wie folgt gesetzt sein:

"Mobilfunk-Kommunikationseinstellungen > Liste der bevorzugten Netzwerke":
 "Bevorzugte Mobilfunknetze" = "Vertragsnetz und alternative Netze"

Aufrufschnittstelle in FUP-Darstellung



Erläuterung der Formalparameter

Die folgende Tabelle erläutert die Formalparameter der Anweisung TC_CONFIG

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

Die Anzeigen BUSY, DONE und ERROR

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

BUSY	DONE	ERROR	Bedeutung
0	0	0	Kein Auftrag in Bearbeitung

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

Die Anzeigen DONE, ERROR und STATUS

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

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

A.6 IF_CONF_*: SDTs für Projektierungsdaten des CP

Aufbau des IF_CONF-DB für den Programmbaustein TC_CONFIG

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

Um die Funktion nutzen zu können, müssen in der STEP 7-Basisprojektierung des CP bereits projektierte Werte vorhanden sein.

Der IF_CONF-DB setzt sich aus einem Header und nachfolgenden Blöcken zusammen, die den Parametern in der Projektierung des CP entsprechen.

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

Anlegen des DB und der IF_CONF-Strukturen

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

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

Gehen Sie zum Anlegen des IF_CONF.DB folgendermaßen vor:

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

Den Name können Sie frei festlegen.

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

Der Header der Struktur mit seinen drei Parametern (siehe unten) wird angelegt.

4. Legen Sie eine weitere Struktur für den ersten zu ändernden Parameter an, indem Sie den gewünschten Datentyp (bspw. "IF_CONF_APN") in die Zelle des Datentyps eintippen.

5. Wiederholen Sie den letzten Schritt für all diejenigen Parameter, die Sie mithilfe von TC_CONFIG im CP ändern wollen.

6. Aktualisieren Sie abschließend im Header die Blockanzahl im Parameter "subfieldCnt".

Header von IF_CONF

Tabelle A- 1 IF_CONF_Header

Byte	Parameter	Datentyp	Anfangswert	Beschreibung
0 ... 1	fieldType	UINT		Blocktyp: Muss immer 0 sein.
2 ... 3	fieldId	UINT		Block-ID: Muss immer 0 sein.
4 ... 5	subfieldCnt	UINT		Gesamtanzahl der im DB enthaltenen Blöcke (Strukturen) für die zu ändernden Parameter

Allgemeine Parameter der Parameterblöcke

Jeder Block enthält folgende allgemeine Parameter:

- Id
Dieser Parameter kennzeichnet den jeweiligen Block und darf nicht verändert werden.
- Length
Dieser Parameter gibt die Länge des Blocks an. Der Wert dient nur Informationszwecken. Blöcke mit Strings und / oder Arrays haben eine variable Länge. Durch versteckte Bytes kann die tatsächliche Länge von Blöcken größer als die Summe der angezeigten Parameter sein.
- Mode
Für diesen Parameter sind die folgenden Werte zulässig:

Tabelle A- 2 Werte von "Mode"

Wert	Bedeutung
1	Permanente Gültigkeit der Projektierungsdaten Nicht relevant beim CP
2	Temporäre Gültigkeit der Projektierungsdaten einschließlich Löschen vorhandener permanenter Projektierungsdaten Die permanenten Projektierungsdaten werden durch die im Baustein parametrisierten Strukturen ersetzt.

"APN-Einstellungen"

Korrespondierende Parametergruppe in der Projektierung:
"Mobilfunk-Kommunikationseinstellungen > APN-Einstellungen"

Tabelle A- 3 IF_CONF_APN

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

"CP-Identifikation"

Korrespondierende Parametergruppe in der Projektierung:
"Security > CP-Identifikation"

Tabelle A- 4 IF_CONF_Login

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	5	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 54
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
ModemName	STRING [22]		Zugangs-ID Der Wert ist nicht parametrierbar.
ModemPassword	STRING [22]		Telecontrol-Passwort Das Passwort ist beim CP 1242-7 (6GK7 242-7KX30-0XE0) nicht über den SDT änderbar.

"Telecontrol-Server" (DNS)

Korrespondierende Parametergruppe in der Projektierung:
"Partnerstationen > Telecontrol-Server"

Dieser Block ist nur zu verwenden, wenn der Telecontrol-Server mit einem über DNS auflösbaren Namen adressiert wird. Wenn der Telecontrol-Server mit seiner IP-Adresse adressiert wird, dann wird der Block "IF_CONF_TCS_IP_V4" verwendet.

Bei mehreren Telecontrol-Servern verwenden Sie den Block je einmal pro Server.

Tabelle A- 5 IF_CONF_TCS_Name

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

"SMSC"

Korrespondierende Parametergruppe in der Projektierung:
"Mobilfunk-Kommunikationseinstellungen > Mobilfunk-Einstellungen"

Tabelle A- 6 IF_CONF_SMS_Provider

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

"PIN"

Korrespondierende Parametergruppe in der Projektierung:
"Mobilfunk-Kommunikationseinstellungen > Mobilfunk-Einstellungen"

Tabelle A- 7 IF_CONF_PIN

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

"Autorisierte Rufnummer"

Korrespondierende Parametergruppe in der Projektierung:
 "Security > Autorisierte Rufnummern"

Tabelle A- 8 IF_CONF_WakeupList

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

"Bevorzugte Mobilfunknetze"

Korrespondierende Parametergruppe in der Projektierung:
 "Mobilfunk-Kommunikationseinstellungen > Liste der bevorzugten Netzwerke"

Voraussetzung:

Das zu nutzende Mobilfunknetz muss in der Projektierung des CP wie folgt gesetzt sein:

"Mobilfunk-Kommunikationseinstellungen > Liste der bevorzugten Netzwerke":
 "Bevorzugte Mobilfunknetze" = "Vertragsnetz und alternative Netze"

Tabelle A- 9 IF_CONF_PrefProvider

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	14	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 46
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
Provider [1...5]	ARRAY [1...5] of STRING [6]		Parameter "Vertragsnetz und alternative Netze" 1. bis 5. bevorzugtes Mobilfunknetz, in das sich der CP außer dem Vertragsnetz einwählt. Nr. 1 mit höchster Priorität, Nr. 5 mit niedrigster Priorität. Eingabe des Public Land Mobile Network (PLMN) des Netzbetreibers, bestehend aus Mobile Country Code (MCC) und Mobile Network Code (MNC). Beispiel (Testnetz der Siemens AG): 26276

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

Korrespondierende Parametergruppe in der Projektierung:
 "Mobilfunk-Kommunikationseinstellungen > "TeleService-Einstellungen"

Zugangsdaten des TeleService-Servers (Vermittlerstation). Bei zwei TeleService-Servern verwenden Sie den Block je einmal pro Server.

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

Tabelle A- 10 IF_CONF_TS_Name

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	20	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 266
Mode	UINT		Gültigkeit (1, 2) - siehe oben (Allgemeine Parameter)
ts_name	String [254]		Durch DNS auflösbarer Name des TeleService-Servers oder IP-Adresse als String
RemotePort	UINT		Port der Engineering-Station
Rank	UINT		Priorität des Servers [1] oder [2]: <ul style="list-style-type: none"> • 1 = Server 1 • 2 = Server 2 (nicht relevant)

TeleService-Zugang (IP-Adresse des Servers)

IP-Adresse des TeleService-Servers. Nicht mehr verwendbar ab Firmware-Version V2.1 des CP.

Bei zwei TeleService-Servern verwenden Sie den Block je einmal pro Server.

Tabelle A- 11 IF_CONF_TS_IF_V4

Parameter	Datentyp	Anfangswert	Beschreibung
Id	UINT	21	Kennung des Parameterblocks
Length	UINT		Länge des Parameterblocks in Byte: 14
Mode	UINT		Gültigkeit (1: permanent, 2: temporär)
RemoteAddress	IP_V4		IP-Adresse des TeleService-Servers
RemotePort	UINT		Port des TeleService-Servers
Rank	UINT		Priorität des Servers [1] oder [2] 1 = Server 1, 2 = Server 2

SINEMA Remote Connect (CP)

B.1 Gültigkeit und Voraussetzungen

Gültigkeit

Die Kommunikation über SINEMA Remote Connect wird von folgenden Modulen unterstützt:

- CP 1243-1
 - Ab Firmware V3.1
- CP 1243-7 LTE
 - Ab Firmware V3.1
- CP 1243-8 IRC
 - Ab Firmware V3.1
 - Unter ST7 als MSC-Station ab Firmware V3.2
- CP 1542SP-1 IRC
 - Ab Firmware V2.0
 - Unter ST7 als MSC-Station ab Firmware V2.1

Die Funktionen werden von folgenden Software-Versionen unterstützt:

- SINEMA Remote Connect
 - Ab Software-Version V1.3

B.2 Anbindung an SINEMA RC

Kommunikation über SINEMA Remote Connect (SINEMA RC)

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

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

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

Der CP kann auch die Telecontrol-Kommunikation über den SINEMA RC-Server abwickeln.

Parametergruppen

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

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

Zu den unterstützten Protokollen und zur Projektierung siehe Kapitel Telecontrol über SINEMA RC (Seite 189).

Anwendungen

Aus der Kombination der Parameter für Telecontrol-Kommunikation und SINEMA RC ergeben sich folgende Anwendungsmöglichkeiten des CP:

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

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

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

Tabelle B- 1 Anwendungsfälle und zu aktivierende Parameter

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

* Bedeutung der Parameter-Abkürzungen:

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

"Automatische OpenVPN-Konfiguration über SINEMA Remote Connect Server"

TC - Kommunikationsarten > Telecontrol-Kommunikation aktiviert

TC-SRC - Kommunikationsarten >

"Telecontrol-Kommunikation über SINEMA Remote Connect aktivieren"

B.3 Telecontrol über SINEMA RC

Zu den Anwendungsmöglichkeiten der Kommunikation über SINEMA Remote Connect siehe Kapitel Anbindung an SINEMA RC (Seite 187).

Voraussetzungen

Nehmen Sie vor der Projektierung des CP in STEP 7 die erforderliche Projektierung von SINEMA Remote Connect - Server vor (nicht in STEP 7). Der CP und der Kommunikationspartner des CP müssen im SINEMA RC-Server projektiert werden.

Projektierung der Telecontrol-Kommunikation über SINEMA Remote Connect

Gehen Sie bei der Projektierung des Moduls für die Nutzung der Telecontrol-Kommunikation über SINEMA RC folgendermaßen vor:

1. Aktivieren Sie in der Parametergruppe "Kommunikationsarten" die Telecontrol-Kommunikation und wählen Sie das Protokoll aus.
Die Option zur Kommunikation über SINEMA RC ist noch nicht sichtbar.
2. Wechseln Sie in die Parametergruppe "Security" und aktivieren Sie die Security-Funktionen.
(In der Parametergruppe "Kommunikationsarten" erscheint die SINEMA RC-Option deaktiviert und graut.)
3. Öffnen Sie die Parametergruppe "Security > VPN" und aktivieren Sie VPN.
4. Wählen Sie beim Parameter "VPN-Verbindungstyp" die Option "Automatische OpenVPN-Konfiguration über SINEMA Remote Connect Server" aus, wenn diese noch nicht vorbelegt ist.
(In der Parametergruppe "Kommunikationsarten" wird die SINEMA RC-Option bedienbar.)
5. Wechseln Sie in die Parametergruppe "Kommunikationsarten" und aktivieren Sie die Option "Telecontrol-Kommunikation über SINEMA Remote Connect aktivieren".
6. Nehmen Sie die weitere Projektierung der SINEMA RC-Anbindung des CP unter "Security > VPN" vor.

Zur Projektierung siehe Kapitel Security > VPN > SINEMA Remote Connect (Seite 189).

B.4 Security > VPN > SINEMA Remote Connect

Fernwartung mit SINEMA Remote Connect (SINEMA RC)

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

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

Vorbereitende Schritte

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

- Projektierung von SINEMA Remote Connect Server

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

- Exportieren des CA-Zertifikats (optional)

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

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

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

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

Projektierung von SINEMA Remote Connect

Importieren des eigenen Zertifikats

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

Navigieren Sie anschließend zur Parametergruppe "Security > VPN".

VPN > Allgemein

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

SINEMA Remote Connect Server

Tragen Sie die Adresse und Portnummer des Servers ein.

Serverüberprüfung

Hier wählen Sie die Authentifizierungsmethode des Kommunikationsmoduls beim Verbindungsaufbau aus.

- CA-Zertifikat

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

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

- Fingerabdruck

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

Authentifizierung

- Geräte-ID

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

- Gerätepasswort

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

Max. Anzahl an Zeichen: 127

Optionale Einstellungen

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

- **Aktualisierungsintervall**

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

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

- **"Verbindungsart"**

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

- Auto

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

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

- PLC-Trigger

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

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

Hinweis

Verbindungsabbruch

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

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

- **PLC-Variable für Verbindungsaufbau**

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

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

WBM der TIM 1531 IRC

C.1 Unterstützte Webbrowser

Webbrowser

Für den Zugriff auf den Webserver der TIM sind folgende Webbrowser geeignet:

- Internet Explorer (Version 11)
- Google Chrome (Version 68)
- Firefox (Version 62)

Die genannten Webbrowser sowie Hinweise und ggf. erforderliche Programmzusätze finden Sie im Internet.

C.2 Verbindung mit dem WBM der TIM aufbauen

Verbindungsmöglichkeiten

Sie können eine Verbindung zwischen einem PC und der TIM über das Protokoll HTTP/HTTPS aufbauen:

- LAN-Verbindung

Bei lokaler Anschaltung des PC an die TIM können Sie sich direkt verbinden.

- Verbindung über WAN (Internet/Mobilfunk)

Die TIM muss über eine feste IP-Adresse erreichbar sein.

Bei Verbindungen über das Internet / Mobilfunknetz müssen Sie das gesicherte Protokoll "HTTPS" nutzen.

Voraussetzungen

Voraussetzung für den Zugriff auf die TIM sind:

- Die TIM muss über eine IPv4-Adresse erreichbar sein.
- Der PC muss im selben Subnetz wie die TIM liegen.
- Die TIM muss erreichbar sein.

Verbindung mit dem Webserver der TIM

Gehen Sie folgendermaßen vor, um sich von dem PC mit dem Webserver der TIM zu verbinden:

1. Öffnen Sie den Webbrowser.
2. Geben Sie die Adresse (IP-Adresse / Host-Name) der TIM (bzw. des Routers) in die Adresszeile des Webbrowsers ein, alternativ über das Protokoll HTTP oder HTTPS:
 - http://<Adresse>
 - https://<Adresse>

Achten Sie bei der Auswahl des Protokolls darauf, dass dieses in der Projektierung der TIM freigegeben ist (Register "Webserver").

Bei HTTPS-Verbindungen über das Internet kann beim ersten Anmelden eine Warnmeldung erscheinen, dass die Webseite unsicher ist oder das Zertifikat nicht vertrauenswürdig. Wenn Sie sicher sind, dass Sie die richtige Adresse eingegeben haben, dann ignorieren Sie die Meldung. Fügen Sie die Verbindung gegebenenfalls zu den Ausnahmen hinzu (abhängig vom Webbrowser).

Das Anmeldefenster der TIM öffnet sich.

3. Geben Sie im Eingabefeld "Benutzername" den in STEP 7 projektierten Namen eines Benutzers oder Administrators ein.

Es gelten die in "Globale Security-Einstellungen" des STEP 7-Projekts zugewiesenen Rechte.

4. Geben Sie im Eingabefeld "Passwort" das dazugehörige Passwort ein.
5. Klicken Sie auf die Schaltfläche "Anmelden".

Der Webserver öffnet sich mit der Startseite:

C.3 Allgemeine Funktionen des WBM

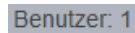

Die WBM-Sprache stellen Sie über die Einstellung des genutzten Browsers ein.




Folgende Sprachen werden unterstützt:

- Deutsch
- Englisch

Anzeigen und Symbole der Titelleiste

Die Anzeigen und Symbole in der Titelleiste des WBM haben folgende Funktion:

Symbol	Funktion
	Name des aktuell angemeldeten Benutzers
	Abmelden des Benutzers

Symbol	Funktion
Anzahl aktiver Sitzungen: 1	Anzahl der Verbindungen mit einem PC
2015-01-28 14:30:37	Datum und Zeitpunkt der letzten Seitenaktualisierung des WBM in lokaler Zeit der TIM (yyyy-mm-dd hh:mm:ss)
	Die automatische Aktualisierung der WBM-Anzeige ist aktiviert. Die Daten werden im dem Intervall abgerufen, das unter "System > Webserver" projiziert ist.
	Die automatische Aktualisierung der WBM-Anzeige ist deaktiviert.
Einschalten	Schaltet die automatische Aktualisierung der WBM-Anzeige ein.
Ausschalten	Schaltet die automatische Aktualisierung der WBM-Anzeige aus.
	Ausdrucken der aktuellen WBM-Seite

C.4 Startseite

Nach der Anmeldung am WBM erscheint die Startseite.

Links finden Sie den Navigationsbereich mit den Hauptebenen des WBM.

Navigation im WBM

Öffnen Sie links im Navigationsbereich durch Klick auf einen Eintrag diejenige WBM-Seite, zu der Sie weitere Informationen erhalten wollen oder auf der Sie projektieren oder programmieren wollen.

Das WBM öffnet jeweils das erste Register des Eintrags.

Wechseln Sie auf anderen Seiten mit mehreren Registern durch Anklicken des Registernamens in das jeweilige Register.

Startseite



Bild C-1 Startseite des WBM

Die Seite zeigt allgemeine Daten der Baugruppe.

Allgemein

- **Stationsname**
In STEP 7 projektierter Parameter
- **Baugruppenname**
In STEP 7 projektierter Parameter
- **Baugruppentyp**
- **Artikelnummer**

Status

- **Betriebszustand**
Aktueller Betriebszustand der TIM
- **Status**
Zustand des Firmware-Anlaufs der TIM:
 - TIM fehlerfrei angelaufen
 - Anlauf mit Fehler abgebrochen
- **Firmware-Datum**
Generierungsdatum der aktuell verwendeten Firmware-Datei
Format: MMM DD YYYY, hh:mm:ss

C.5 System

C.5.1 Geräte-Info

Modul

- Kurzbezeichnung
In STEP 7 projektierter Parameter
- Artikelnummer
- Hardware-Erzeugnisstand
- Firmware-Version
- Baugruppenträger
- Steckplatz

Baugruppeninformation

- Baugruppenname
In STEP 7 projektierter Parameter

Herstellerinformation

- Hersteller
- Seriennummer
Seriennummer des Geräts

C.5.2 SD-Karte

SD-Karte

SD-Karte

- **SD-Karte gesteckt**
ja / nein
- **Speicherplatz frei / gesamt**
Anzeige des freien noch verfügbaren Speicherplatzes und der gesamten nutzbaren Speicherkapazität
- **Inhalt**
Anzeige der auf der SD-Karte gespeicherten Telegramme und Dateien

C.5.3 Systemzeit

Systemzeit

Die aktuelle Systemzeit der TIM wird in der Titelleiste des WBM angezeigt.

- **Eingabefeld für Uhrzeit**

Format: YYYY-MM-DD hh:mm:ss

Über das Eingabefeld können Sie die Uhrzeit manuell eingeben und an die TIM übertragen.

Gehen Sie bei der Eingabe entsprechend dem vorgegebenen Format vor.

Monat, Tag und Stunde können auch einstellig eingegeben werden. Bsp.: März wird als "03" oder als "3" akzeptiert.

- **Uhrzeit übernehmen**

Durch Klicken auf die Schaltfläche übertragen Sie die oben eingegebene Uhrzeit an die TIM.

- **PC-Zeit übernehmen**

Durch Klicken auf die Schaltfläche übernimmt die TIM die Uhrzeit vom verbundenen PC.

C.5.4 NTP

NTP

- **NTP-Server-Liste**

Zeigt die Adressen der projizierten NTP-Server an.

C.5.5 Webserver

Webserver

- **Webserver deaktivieren**

Deaktiviert den Webserver der TIM. Die Einstellung wird in die Projektierungsdaten der TIM übernommen.

Hinweis

Keine HTTP/HTTPS-Verbindung zur TIM

Wenn Sie den Webserver der TIM deaktivieren, verlieren Sie die Möglichkeit, über HTTP/HTTPS auf die TIM zuzugreifen.

Ein Zugriff ist erst wieder nach dem Laden der Projektierungsdaten (mit aktiviertem Webserver-Zugriff) möglich.

- **Automatische Aktualisierung**
Aktivieren Sie die Option, wenn die Inhalte der Webseiten automatisch aktualisiert werden sollen.
Bei deaktivierter Option werden die Seiten in dem Intervall aktualisiert, das Sie in STEP 7 projiziert haben.
- **Aktualisierungsintervall (s)**
Hier wird das in STEP 7 projizierte Aktualisierungsintervall in Sekunden angezeigt.
Bei aktivierter Option (oben) können Sie das gewünschte Aktualisierungsintervall manuell eingeben.
- **Speichern**
Übernimmt das manuell eingegebene Aktualisierungsintervall.

C.5.6 DNS-Konfiguration

DNS-Server-Liste

- **Liste der projizierten DNS-Server**
In STEP 7 projizierte Server

C.6 Instandhaltung

C.6.1 Firmware

Firmware

Auf dieser Seite werden die wichtigsten Versionsdaten der aktuell verwendeten Firmware angezeigt.

Wenn für die TIM 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/21764/dl>)

Wenn eine neue Firmware-Version zur Verfügung steht, dann können Sie die Firmware-Datei über diese WBM-Seite vom PC in die TIM laden.

Hinweis

Digital signierte und verschlüsselte Firmware verhindert Manipulationen Dritter

Um die Authentizität der Firmware prüfen zu können, wird die Firmware von Siemens digital signiert. Damit sollen Manipulationen Dritter festgestellt und verhindert werden.

Hinweis

Keine Eingriffe während der Aktualisierung

Während des Aktualisierens der Firmware bis zum Neustart der TIM ist das WBM nicht gesperrt.

Nehmen Sie in dieser Zeitspanne keine Eingriffe vor (bspw. kein Neustart).

Hinweis

Kein Ausschalten der Spannungsversorgung

Schalten Sie die Spannungsversorgung während des Aktivierungsvorgangs der Firmware nicht aus. Sie vermeiden damit das Auftreten inkonsistenter Zustände.

Firmware

Folgende Informationen werden angezeigt:

- **Firmware-Version**
Version der aktuell von der TIM verwendeten Firmware
- **Datum**
Generierungsdatum der Firmware

Firmware-Aktualisierung

Laden Sie die Firmware-Datei in das Dateisystem Ihres angeschlossenen PC.

- **Datei**
Nach Auswahl einer auf dem PC gespeicherten Firmware-Datei über die Schaltfläche "Durchsuchen" wird hier der Dateiname angezeigt.
- **Durchsuchen**
Durchsucht das Dateisystem des PC nach einer dort gespeicherten Firmware-Datei, welche in die TIM geladen werden soll.
- **Laden in Gerät**
Durch Klicken auf die Schaltfläche laden Sie die selektierte Firmware-Datei in die TIM.
Beachten Sie, dass das Aktualisieren der Firmware eine Weile dauern kann. Den aktuellen Zustand des Firmware-Ladens erkennen Sie am LED-Bild.

Nach der Aktualisierung der Firmware läuft die TIM automatisch wieder an.

C.6.2 Betriebszustand

Betriebszustände

Außer über diese WBM-Seite können Sie die nachfolgend beschriebenen Funktionen auch über den Schalter der TIM ausführen.

Die Schaltflächen haben folgende Funktionen:

- **Neustart ausführen**

Beim Neustart werden bestehende Telecontrol-Verbindungen und die zyklische Bearbeitung abgebrochen. Die TIM läuft neu an.

- **Rücksetzen auf Werkseinstellungen**

Hinweis

Datenverlust: Auswirkungen des Rücksetzens beachten

Beachten Sie vor dem Rücksetzen die Auswirkungen.

Setzt die TIM auf Werkseinstellungen zurück. Dabei werden alle Parameter in den Auslieferungszustand zurückgesetzt und die TIM führt einen Neustart durch.

Wenn Sie eine SD-Karte verwenden und Sie möchten die TIM auf Werkseinstellungen zurücksetzen, dann müssen Sie vor dem Rücksetzen die SD-Karte ziehen (im spannungslosen Zustand). Bei gesteckter SD-Karte läuft die TIM wieder mit den Projektierungsdaten auf der SD-Karte an.

Rücksetzen auf Werkseinstellungen: Auswirkung

Hinweis

Projektierungsdaten werden gelöscht

Durch das Rücksetzen auf Werkseinstellungen werden alle Projektierungsdaten in der TIM gelöscht!

- **Gelöschte Daten**

Folgende Daten werden durch das Rücksetzen auf Werkseinstellungen gelöscht:

- Projektierte IP-Adressen der LAN-Schnittstellen X1, X2 und X3
- Alle weiteren Projektierungsdaten im Arbeitsspeicher der TIM

- **Nicht gelöschte Daten**

Folgende Daten werden durch das Rücksetzen auf Werkseinstellungen nicht gelöscht:

- MAC-Adressen der LAN-Schnittstellen

C.7 Diagnose

C.7.1 Ereignisse

Diagnosemeldungen

Tabelle

Die Tabelle listet die letzten in der TIM aufgetretenen Diagnoseereignisse mit folgenden Angaben auf:

- **Nummer**

Laufende Nummer

- **Zeit**

Zeit des Diagnoseereignisses

- **Datum**

Datum des Diagnoseereignisses

- **Ereignistyp**

Die Diagnosemeldungen sind folgendermaßen klassifiziert:

- INFO

Information über ein besonderes Ereignis

- WARNING

Warnung zu einem möglicherweise unerwünschten Ereignis

- ERROR

Interner Fehler. Die TIM läuft weiter.

- FATAL

Schwerwiegender Fehler, der den Betrieb der TIM beeinträchtigt oder unterbricht.

- **Ereignis**

Klartext des Diagnoseereignisses

Kopie des Diagnosepuffers

Über die Schaltfläche speichern Sie den Inhalt des Diagnosepuffers auf dem PC

Der Diagnosepuffer

Der Diagnosepuffer enthält Diagnosemeldungen zu internen Ereignissen und Fehlern. Er umfasst maximal 200 Einträge. Bei Überschreitung der maximalen Anzahl werden die ältesten Einträge überschrieben.

Die Einträge im Diagnosepuffer enthalten eine fortlaufende Nummer, eine Klassifizierung, einen Zeitstempel und den Meldungstext.

Nachfolgend finden Sie einige Beispiele für Ereignisse, die in den Diagnosepuffer eingetragen werden:

- Anlauf der TIM
- Änderung der Konfiguration
- Aufbau/Abbruch einer Kommunikationsverbindung
- Uhrzeitsynchronisation
- Spannungsausfall

C.7.2 Nachrichten

Nachrichten

Tabelle

Die Tabelle listet die letzten Nachrichten der TIM mit folgenden Angaben auf:

- **Nummer**
Laufende Nummer
- **Uhrzeit**
Uhrzeit des Versendens
- **Trigger**
Trigger, welcher das Erzeugen der Nachricht ausgelöst hat.
- **Empfänger**
Projektierter Empfänger der Nachricht
- **Nachricht**
Nachrichtentext
- **Bearbeitungsstatus**
Status des Versands der Nachricht
Eine Übersicht der möglichen Status finden Sie im Kapitel Bearbeitungsstatus der Nachrichten (SMS, E-Mail) (Seite 166).
- **Typ**
Typ der Nachricht

C.8 LAN

C.8.1 Ethernet-Schnittstelle [Xn]

- Die drei Ethernet-Schnittstellen der TIM werden über die obere Registerreihe selektiert:
 - X1 ... X3
- Die Parameter der selektierten Schnittstelle werden über die untere Registerreihe angezeigt:
 - IPv4-Parameter
 - IPv6-Parameter
 - Statistik

IPv4-Parameter

Netzanschluss

- **MAC-Adresse**

IP-Parameter

- **IP-Adresse**

Aktuelle IP-Adresse

- **Subnetzmaske**

Voreingestellte bzw. zuletzt projektierte Subnetzmaske

- **Default-Router**

Projektierter Default-Router

- **Adresszuweisung**

Zeigt an, wie der Bezug der IP-Adresse in STEP 7 projektiert ist:

- IP-Adresse im Projekt einstellen
- IP-Adresse von DHCP-Server
- IP-Adresse am Gerät einstellen

Bezug der IP-Adresse durch andere Dienste außerhalb der Projektierung

Ports

- **Portnummer**

Port der Schnittstelle

- **Verbindungsstatus**

- OK: Bestehende Verbindung zum Netz
- Nicht OK: Keine Verbindung

- **Einstellungen**
Verfahren der Netzeinstellung
 - Automatisch
 - Manuelle Einstellung zur Übertragungsgeschwindigkeit und Richtungsabhängigkeit
- **Modus**
Verwendete Übertragungsgeschwindigkeit und Richtungsabhängigkeit (duplex/halbduplex)
- **Verbindungsmedium**
Angeschlossenes Medium (Kupfer / optisch)

IPv6-Parameter

- **IPv6-Adresse**
Aktuell genutzte IPv6-Adresse
- **Gateway**
Anzeige der IPv6-Adressen von bis zu zwei Gateways

Statistik

Statistik

Folgende Statistikdaten der Schnittstelle seit dem letzten Anlauf der TIM werden angezeigt:

- **Bytes empfangen**
- **Empfangs-Telegramme verworfen**
Anzahl der Telegramme, die aufgrund von Adress-, Protokoll- oder Datenfehlern beim Empfang verworfen wurden.
- **Fehler beim Empfang**
Anzahl der internen Fehler beim Empfang
- **Telegramme mit unbekanntem Protokoll**
Anzahl der Telegramme mit falschem Protokoll
- **Bytes gesendet**
- **Gesendete Unicast-Telegramme**
- **Verworfenen Sende-Telegramme**
Anzahl der Telegramme, die aufgrund von Fehlern beim Senden verworfen wurden.
- **Fehler beim Senden**
Anzahl der internen Fehler beim Senden
- **Telegramme im Sendefach**
Anzahl der noch nicht gesendeten Telegramme, die zur Übertragung anstehen.

C.9 Telecontrol

C.9.1 Partnerinformationen

C.9.1.1 Verbindungsübersicht

Das Register gibt Ihnen Informationen zu den Kommunikationspartnern und dem Verbindungszustand der TIM.

Tabelle

Die Spaltenköpfe haben folgende Bedeutung:

- **Verbindungszustand**

Der Zustand der Verbindungen zur zugeordneten CPU und zu den remoten Partnern wird wie folgt angezeigt:

- **Grün: Verbunden**

Alle Verbindungen sind aufgebaut.

- **Gelb: Verbunden**

Die möglichen Verbindungen sind teilweise aufgebaut.

- **Rot: Getrennt**

Keine der möglichen Verbindungen ist aufgebaut.

- **Partner**

Mögliche Partnertypen:

- Lokale CPU

CPU, welche der TIM in der Projektierung zugeordnet wurde.

- Applikation

(bspw. WinCC)

- TIM

TIM der fernen Station

- Partner-CPU

CPU der fernen Station

- CP ...

CP der fernen Station (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC / CP 1542SP-1 IRC)

- **Teilnehmernummer**

Teilnehmernummer des Partners

Durch Klicken auf das Symbol '±' in einer Tabellenzeile werden die jeweiligen Parameter eingeblendet.

Zu jedem Teilnehmer stehen folgende Informationen zur Verfügung:

- Informationen zum Teilnehmer
- Informationen zum Übertragungsweg

Informationen zum Teilnehmer

Lokale CPU

- **Status**
Betriebszustand der lokalen CPU
- **Anzahl der Verbindungen**
Anzahl der Verbindungen zwischen TIM und lokaler CPU

Ferner Partner

- **Partnertyp**
 - Applikation (bspw. WinCC)
 - CPU
CPU der fernen Station
 - TIM
 - CP ...
- **Teilnehmernummer**
Teilnehmernummer des Partners
- **Uhrzeitmaster**
Anzeige der beim Partner projektierten Option:
Ja / Nein
- **Security-Optionen**
Anzeige der aktiven Zugriffsstufe (Schutz):
EIN / AUS
- **Verbindungszustand**
 - Verbunden
 - Nicht verbundenZur Bedeutung der Farben siehe oben (Verbindungsübersicht).

- **Telegrammspeicher-Zustand**

Zustand des Sendepuffers, nur relevant bei einem Kommunikationsmodul:

- **Normalbetrieb**

Der Sendepuffer arbeitet normal. Die Speicherplatzbelegung liegt zwischen 10 und 80 %.

- **80%-Grenze erreicht**

Bei Verwendung des Protokolls ST7 schaltet die TIM bei 80 % Speicherbelegung des Sendepuffers in das Zwangsabbildverfahren.

- **Überlauf**

100 % Speicherbelegung des Sendepuffers

Übertragungsweg

Informationen zum Übertragungsweg

Lokale CPU

- **Schnittstellen-ID**

Ethernet-Schnittstelle der TIM für die Verbindung mit der lokalen CPU

X1 (ETH1) / X2 (ETH2) / X3 (ETH3)

- **CPU-Typ**

Typ der lokalen CPU

- **Verbindungszustand**

- Verbunden

- Nicht verbunden

- **CFB-Referenz**

Lokale ID (dezimal) der S7-Verbindung

- **Lokaler TSAP**

Lokaler TSAP der S7-Verbindung

- **Ferner TSAP**

Ferner TSAP der S7-Verbindung

- **IP-Adresse**

IP-Adresse der CPU

Ferner Partner**• Adresse**

IP-Adresse oder WAN-Adresse der Schnittstelle der TIM

• Schnittstelle

Ethernet-Schnittstelle der TIM für die Verbindung mit dem fernen Partner

X1 (ETH1) / X2 (ETH2) / X3 (ETH3)

• CFB-Referenz

Lokale ID (dezimal) der S7-Verbindung

• Verbindungstyp

Anzeige von mehreren der folgenden Verbindungseigenschaften:

– PBK

Projektierte S7-Verbindung

– ST7

ST7-Verbindung über ein klassisches WAN-Netz

– DNP3

DNP3-Verbindung über ein klassisches WAN-Netz

– IEC

IEC 60870-5-101-Verbindung über ein klassisches WAN-Netz

– MSC-Verbindung

Nur ST7: Verbindung des Protokolls MSC, für die keine S7-Verbindung benötigt wird.

– CR-Verbindung

Read-/Write-Verbindung mit der lokalen CPU, die keine S7-Verbindung benötigt.

– X-Verbindung

Nicht-projektierte S7-Verbindung, welche die SFCs "X_SEND" und "X_RCV" verwendet.

– Permanent / Temporär

Permanente oder temporäre Telecontrol-Verbindung

– GPRS / no GPRS

GPRS-Verbindung bzw. keine GPRS-Verbindung

– local / remote

Verbindung zu einem lokalen oder fernen Partner

• Verbindungszustand**– Verbunden****– Getrennt**

C.9.1.2 Sendepuffer

Das Register gibt Ihnen Informationen zum Sendepuffer (Telegrammspeicher) der lokalen bzw. der fernen TIM.

Informationen zum Sendepuffer

Informationen zum Sendepuffer der TIM:

- **Größe (Speicherplätze)**
Projektierte Größe des Sendepuffers als Anzahl der Speicherplätze
Pro Telegramm wird ein Speicherplatz reserviert.
- **Frei (Speicherplätze)**
Aktuell freier Speicherplatz als Anzahl der Speicherplätze
- **Frei (%)**
Aktuell freier Speicherplatz in Prozent
In Klammern: Anzahl projektierter Ereignisse / Max. Anzahl an Ereignissen

Tabelle

Die Spaltenköpfe haben folgende Bedeutung:

- **Quell-Teilnehmer**
Teilnehmernummer des Quell-Teilnehmers, von dem aus die Verbindung aufgebaut wird.
- **Ziel-Teilnehmer**
Teilnehmernummer des Ziel-Teilnehmers, zu dem die Verbindung aufgebaut wird.
- **Anzahl Ereignisse**
Anzahl der projizierten Ereignisse des Quell-Teilnehmers

Parameter

Durch Klicken auf das Symbol '±' in einer Tabellenzeile werden die jeweiligen Parameter eingeblendet.

- **Unbedingt spontan**
Anzahl der gespeicherten Telegramme, die unbedingt spontan gesendet werden (nur in Wählnetzen relevant).
- **Priorisiert**
Anzahl der gespeicherten Telegramme, die hochprior gesendet werden.

- **Kennzeichnung**
Hexadezimaler Wert, der die nachstehenden Informationen kodiert.
 - Unbedingt spontan (9)
Anzahl der Telegramme mit Übertragungsmodus "Spontan (unmittelbare Übertragung)"
 - XGA (10)
Nur ST7: Ausstehende Generalabfrage
 - Überlaufwarnung (11)
Sendepuffer-Überlauf-Vorwarnung
 - Übertragungs-Stop (12)
Das Versenden von Daten an den fernen Partner ist vorübergehend gesperrt, weil der Partner nicht erreichbar ist oder weil bei ihm ein Speicherengpass aufgetreten ist.
 - Zwangsabbildspeicherverfahren (14)
Nur ST7: Ab 80 % Speicherplatzbelegung des Sendepuffers schaltet die TIM in das Zwangsabbildverfahren.
Zur Vermeidung eines Sendepuffer-Überlaufs werden alle Datentelegramme wie Abbild-Telegramme behandelt. Auch Sendepuffer-Telegramme werden wie Abbild-Telegramme behandelt, die Daten werden von neueren Daten überschrieben.
 - Gesperrt (15)
Der Sendepuffer ist gesperrt.

C.9.2 Datenpunkte

Das Register gibt Ihnen Informationen zu den projizierten Datenpunkten der TIM.

Datenpunkte

- **Datenpunktnummer**
Laufende Nummer
- **Name & Typ**
Name und Typ des Datenpunkts
Wenn Sie den Mauszeiger über die Spalteneinträge halten, werden in Tooltips weitere Eigenschaften der Datenpunkte angezeigt.
- **Typkennung**
Typ des Datenpunkts
- **Objektnummer**
Objektnummer des ST7-Datenpunkts

- **Objektgruppe**
Objektgruppe (DNP3 / IEC 60870-5; bei DNP3 werden die statischen Varianten angezeigt)
- **Datenpunktindex**
Index des DNP3-/IEC-Datenpunkts
- **Zustand**
Anlass der Übertragung / Zustand der TIM
- **Aktueller Wert**
Aktuell gespeicherter Wert
- **Historischer Wert**
Letzter gesendeter Wert
- **Zeitstempel**
Zeitstempel der letzten Wertänderung

C.10 Logging

Funktionen der Protokollierung

Über diese Seite können Sie zu Diagnosezwecken den Datenverkehr der TIM über PCAP-Funktionalität protokollieren.

Im Fehlerfall oder bei unerwünschtem Verhalten der TIM kann das Kommunikationsverhalten der TIM aufgezeichnet werden. Über einen definierten Zeitraum oder für eine projektierbare Anzahl an Telegrammen wird der Telegrammverkehr der TIM aufgezeichnet.

Die Log-Dateien werden als PCAP-Datei auf dem angeschlossenen PC gespeichert und kann beispielsweise mit dem Programm Wireshark ausgewertet werden.

Optionen:

- **Ethernet Interface X1 / X2 / X3**
Aktivieren Sie die Schnittstellen, für die Sie die Daten aufzeichnen möchten.
- **Datenvolumen (kB)**
Über das Eingabefeld legen Sie die Gesamtgröße der Protokollierungsdatei fest.
Max. Dateigröße: 10000 kB
- **Aufzeichnung nach Zeit**
Bei aktivierter Option wird die Aufzeichnung für einen projektierbaren Zeitraum durchgeführt.
Über das Eingabefeld legen Sie die Aufzeichnungsdauer in Sekunden fest.
Max. Aufzeichnungsdauer: 600 s

- **Aufzeichnung nach Telegrammen**

Bei aktivierter Option wird die Aufzeichnung für eine projektierbare Anzahl an Telegrammen durchgeführt.

Über das Eingabefeld legen Sie die Anzahl der Telegramme fest.

Max. Anzahl an Telegrammen: 500 s

- **Start**

Über diese Schaltfläche starten Sie die Protokollierung.

- **Stop**

Über diese Schaltfläche halten Sie die Protokollierung an.

D.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>)
 - 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/21764/dl>)

Physikalischer Zugang

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

Netzanschluss

Schließen Sie das Modul nicht direkt an das Internet an. Wenn ein Anschluss des Moduls an das Internet gewünscht ist, dann nutzen Sie die Security-Varianten der Telecontrol-Protokolle oder schalten Sie Schutzvorrichtungen vor das Modul. Schutzvorrichtungen sind bspw. ein Router SCALANCE M oder eine Security-Baugruppe 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 und Security-Funktionen der CPU
Projektieren Sie bei der CPU den Zugriff unter "Schutz und Security".
Nutzen Sie die weiteren Security-Funktionen der CPU, um nicht-autorisierte Zugriffe auf die Station zu verhindern.
Hinweise hierzu finden Sie im Informationssystem von STEP 7.
- Security-Funktion der Kommunikation
 - Nutzen Sie die Security-Funktionen der Telecontrol-Protokolle.
 - Verwenden Sie die sicheren Protokollvarianten, bspw. NTP (secure) oder SNMPv3.
 - Lassen Sie den Zugriff auf den Webserver deaktiviert.

Passwörter

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

Protokolle

Sichere und unsichere Protokolle

- Aktivieren Sie nur Protokolle, die Sie für den Einsatz des Systems benötigen.
- Nutzen Sie sichere Protokolle, wenn der Zugriff auf das Gerät nicht durch physikalische Schutzvorkehrungen gesichert ist.
 - Das Protokoll NTP bietet mit NTP (secure) eine sichere Alternative.
 - Das Protokoll HTTP bietet mit HTTPS eine sichere Alternative beim Zugriff auf den Webserver.
- 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.

- Geschlossen nach Konfiguration

Der Port ist geschlossen, da das Modul immer Client für diesen Dienst ist.

- **Authentifizierung**

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

Folgende Ports sind relevant. Nicht alle Protokolle werden von jedem Gerätetyp unterstützt.

Tabelle D- 1 Server-Ports

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
IEC 60870-5-104	2404 (TCP) einstellbar	Geschlossen	Offen nach Konfiguration	Nein
IEC 60870-5-104 mit TLS	19998 (TCP) einstellbar	Geschlossen	Offen nach Konfiguration	Ja, wenn Secure Communication aktiviert ist.
S7- und Online-Verbindungen	102 (TCP)	Offen	Offen nach Konfiguration	Nein
Online-Security-Diagnose (Security-Geräte)	102 (TCP)	Offen	Offen nach Konfiguration *	Ja

Protokoll / Funktion	Portnummer (Protokoll)	Voreinstellung des Ports	Portzustand	Authentifizierung
Kommunikation über SINEMA RC	443 (TCP), 5243 (UDP)	Geschlossen	Offen nach Konfiguration	Ja
HTTP	80 (TCP)	Geschlossen	Offen nach Konfiguration	Nein
HTTPS	443 (TCP)	Geschlossen	Offen nach Konfiguration	Ja
SNMP	161 (UDP)	Geschlossen	Offen nach Konfiguration	Nein (SNMPv1) Ja (SNMPv3)
IPsec (Security-Geräte)	500 (UDP)	Geschlossen	Offen nach Konfiguration	Ja

* Manche Dienstbetreiber beanstanden das Öffnen von Port 102 als Sicherheitslücke. Zur Vermeidung des Öffnens von Port 102 bei der Online-Diagnose siehe Kapitel Online-Security-Diagnose über Port 8448 (Seite 162).

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:

- NTP / NTP (secure) / 123 (UDP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- SINEMA RC Autokonfiguration / 443 (TCP) - einstellbar
- SINEMA RC und OpenVPN / 1194 (UDP) - einstellbar in SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)
- OpenVPN / 1194 (UDP)
- Syslog / 514 (UDP)

D.2 Syslog-Meldungen der TIM 1531 IRC

D.2.1 Aufbau der Syslog-Meldungen

Der Syslog-Server sammelt Log-Informationen der Geräte über bestimmte Ereignisse. Die Syslog-Meldungen werden vom Syslog-Server über den eingestellten UDP-Port (Standard: 514) empfangen und gemäß RFC 5424 bzw. RFC 5426 ausgegeben. Das Syslog-Protokoll schreibt eine festgelegte Reihenfolge und Struktur der möglichen Parameter vor.

Syslog-Meldungen sind gemäß RFC 5424 folgendermaßen aufgebaut:

Teil / Parameter	Erläuterung
HEADER	
PRI	Innerhalb PRI steht codiert die Priorität der Syslog-Meldung, aufgeteilt in Severity (Schweregrad der Nachricht) und Facility (Herkunft der Nachricht).
VERSION	Versionsnummer der Syslog-Spezifikation.
TIMESTAMP	Das Gerät versendet den Zeitstempel im Format "2010-01-01T02:03:15.0003+02:00" als lokale Zeit inklusive Zeitzone und ggf. Korrektur für Sommer-/Winterzeit.
HOSTNAME	Referenziert den Quell-Rechner mit seinem Namen oder der IP-Adresse. IPv4-Adresse nach RFC1035: Bytes in dezimaler Darstellung: XXX.XXX.XXX.XXX IPv6-Adresse nach RFC4291 Section 2.2 Bei fehlenden Angaben wird "-" ausgegeben. Beispiel im Produkt: Der im Register "System" projektierte Stationsname für die RTU.
APP-NAME	Gerät oder Anwendung, von dem die Meldung stammt. Bei fehlenden Angaben wird "-" ausgegeben.
PROCID	Die Prozess-ID dient z. B. bei der Analyse und Fehlersuche dazu, die einzelnen Prozesse eindeutig zu identifizieren. Bei fehlenden Angaben wird "-" ausgegeben.
MSGID	ID zur Identifizierung der Nachricht. Bei fehlenden Angaben wird "-" ausgegeben.
STRUCTURED-DATA	
timeQuality	Das strukturierte Datenelement "timeQuality" liefert Informationen zur Systemzeit. Beispiel: [timeQuality tzKnown="0" isSynced="0"] Der Parameter "tzKnown" gibt an, ob der Sender seine Zeitzone kennt (Wert "1" = bekannt; Wert "0" = unbekannt). Der Parameter "isSynced" gibt an, ob der Sender mit einer zuverlässigen externen Zeitquelle synchronisiert ist, z. B. über NTP (Wert "1" = synchronisiert; Wert "0" = nicht synchronisiert).
sysUpTime	Der Parameter "sysUpTime" ist eine Metainformation über die Meldung. Er gibt die Zeit (in Hundertstelsekunden) seit der letzten Neuinitialisierung des Netzwerkverwaltungsteils des Systems an.
MSG	
MESSAGE	Meldung als ASCII-String (Englisch)

Hinweis

Weiterführende Informationen

Weiterführende Informationen zum Aufbau der Syslog-Meldungen und zur Bedeutung der Parameter können Sie in den RFCs nachlesen:

<https://tools.ietf.org/html/rfc5424>

<https://tools.ietf.org/html/rfc5426>

D.2.2 Variablen in Syslog-Meldungen

Die Variablen werden im Kapitel "Syslog-Meldungen" im Feld "Meldungstext" mit geschweiften Klammern {variable} dargestellt.

Die ausgegebenen Meldungen können folgende Variablen enthalten:

Variable	Beschreibung	Format	Mögliche Werte oder Beispiel
{Ip address}	IPv4-Adresse nach RFC1035 IPv6-Adresse nach RFC4291 Abschnitt 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{FQHN}	Fully Qualified Host Name: Vollständig angegebener Host-Name; Angabe als Domain (FQDN) oder als IPAdresse.	FQDN: host1.com IPv4: %d.%d.%d.%d	server1 192.168.1.105
{Src port} {Dest port}	Portnummer (dezimal)	%d	0 ... 65535
{Client mac} {Dest mac} {Src mac}	MAC-Adresse	%02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	Verwendetes Layer-4-Protokoll oder Dienst, der das Ereignis generiert hat.	%s	UDP TCP WBM Telnet SSH Console TFTP SFTP
{Group}	Name zur Identifikation der Gruppe (Zeichenkette)	%s	it-service
{User name}	Zeichenkette (ohne Leerzeichen), die den authentifizierten Benutzer anhand seines Namens identifiziert.	%s	<name>
{Local interface}	Symbolischer Name der lokalen Schnittstelle	%s	Console
{Action user name} oder {Destination user name}	Identifiziert den Benutzer anhand seines Namens. Dies ist nicht der authentifizierte Benutzer.	%s	<Vorname>.<Name>
{Role}	Symbolischer Name der Gruppenrolle	%s	Administrator
{Time minute} {Timeout}	Anzahl Minuten	%d	44
{Time second}	Anzahl Sekunden	%d	44
{Failed login count}	Anzahl fehlgeschlagener Anmeldeversuche	%d	10
{Max sessions}	Maximale Anzahl der Sitzungen	%d	10
{Vap}	Symbolischer Name der virtuellen Access Point-Schnittstelle	(%s) oder (%s %s)	VAP1.1
{Status} {Reason}	Zusätzliche Statusinformation (Nummer oder Text)	muss mit "(" beginnen und mit mit ")" enden	(Invalid group cipher) (Unknown peer)
{Wlan interface}	Symbolischer Name der WLAN-Schnittstelle	%s	WLAN1
{Ssid}	SSID in ASCII-Darstellung; beliebig viele Leerzeichen.	%s	MyWLAN
{ssid_Hex}	SSID in Hex-Darstellung	%02x%02x%02x%02x%02x%02x	050E081234
{Channel}	Bezeichnung des Kanals	%s	12
{Signal strength}	Signalstärke	%d	12
{Version}	Bezeichnung der Version (ohne Leerzeichen)	%s	V1.0.3SP1

Variable	Beschreibung	Format	Mögliche Werte oder Beispiel
{Resource}	Durch das Schutzstufenkonzept geschützter Ressourcename (ohne Leerzeichen)	%s	FullReadAccess
{Trigger condition}	Zeichenkette (ohne Leerzeichen) für eine Auslösebedingung, mit der die betreffende Funktion aktiviert wird.	%s	E/A-Pin FB-88
{Trigger pin}	Zeichenkette (ohne Leerzeichen) für einen IO-Pin, der das Ereignis ausgelöst hat.	%s	DI1
{Firewall rule}	Zeichenkette (mit Leerzeichen) für einen Firewall-Regelsatz	%s	Rule1
{Subject}	Zeichenkette (mit Leerzeichen) für den Betreff im Zertifikat. Wird verwendet als Teil der zertifikatbasierten Authentifizierung und muss Unicode-Zeichen enthalten.	%s bei UTF8-Code: %S	(Peter Maier)
{Config detail}	Zeichenkette (mit Leerzeichen) für die Konfiguration	%s	OpenVPN
{Connection name}	Name einer VPN-Verbindung		to_Baugruppe1
{Firewall accept}	Firewall-Aktion ausgeführt (akzeptiertes Paket)		ACCEPT
{Firewall action reject}	Firewall-Aktion ausgeführt (abgelehntes Paket)		REJECT DROP
{Length}	Länge des Netzwerkpakets (in Bytes)	%d	52
{Network interface}	Symbolischer Name einer Netzwerkschnittstelle	%s	vlan 1

D.2.3 Erläuterungen zu den Meldungen

In diesem Kapitel werden die Syslog-Meldungen beschrieben. Der Aufbau der Meldungen orientiert sich an der IEC 62443-3-3.

D.2.4 Meldungen für TIM 1531 IRC

Benutzer-Identifikation und Authentifizierung

Meldungstext	{Protocol}: User {User name} logged in from {IP address}.
Beispiel	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.0.1.
Erläuterung	Gültige Anmeldeinformationen, die bei der Anmeldung angegeben wurden.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

Meldungstext	{Protocol}: User {User name} failed to log in from {IP address}.
Beispiel	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.

Erläuterung	Falscher Benutzername oder falsches Passwort bei der Anmeldung angegeben.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

Meldungstext	{protocol}: User {user name} logged out from {ip address}.
Beispiel	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
Erläuterung	Benutzersitzung beendet - Abmeldung erfolgt.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

Sitzungssperrung

Meldungstext	{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.
Beispiel	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The session of user admin was closed after 60 seconds of inactivity.
Erläuterung	Die aktuelle Sitzung wurde aufgrund der Inaktivität beendet.
Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.5

Begrenzung der Anzahl gleichzeitiger Sitzungen

Meldungstext	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Beispiel	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The maximum number of 10 concurrent login sessions exceeded.
Erläuterung	Die maximale Anzahl gleichzeitiger Sitzungen ist überschritten.
Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.7

Non-repudiation

{Protocol}: User {User name} has changed {Config detail} configuration.

Beispiel	SSH: User admin has changed VLAN configuration.
Erläuterung	Ein Benutzer hat bestimmte Konfigurationswerte geändert. In dem Beispiel hat der Benutzer "admin" die VLAN-Konfiguration geändert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

Beispiel	SSH: User admin has initiated a reset to factory defaults.
Erläuterung	Ein Benutzer hat ein Zurücksetzen auf Default-Einstellungen initiiert. In dem Beispiel hat der Benutzer "admin" ein Zurücksetzen auf Default-Einstellungen initiiert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

Software- und Informationsintegrität

Meldungstext	Integrity violations in configuration data detected
Beispiel	Integrity violations in configuration data detected
Erläuterung	Bei der Überprüfung der Konfigurationsintegrität wurde ein Integritätsfehler festgestellt.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 3.4

Wiederherstellung des Automatisierungssystems

{Protocol}: Firmware {Version} was activated.

Beispiel	WBM: Firmware v2.0 was activated.
Erläuterung	Eine Firmware-Version wurde erfolgreich aktiviert. In dem Beispiel wurde die Firmware-Version "v2.0" erfolgreich aktiviert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Firmware activation failed.

Beispiel	WBM: Firmware activation failed.
Erläuterung	Die Aktivierung der Firmware ist fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

Auffinden der Siemens-Literatur

- Artikelnummern

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

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

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

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

- Handbücher im Internet

Die SIMATIC NET-Handbücher finden Sie auf den Internet-Seiten des Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/15247/man>)

Navigieren Sie dort im Produktbaum zum gewünschten Produkt und nehmen Sie folgende Einstellungen vor:

Beitragstyp "Handbücher"

- Handbücher auf Datenträger

Handbücher von SIMATIC NET-Produkten finden Sie auch auf dem Datenträger, der vielen SIMATIC NET-Produkten beiliegt.

Weitere Literaturquellen finden Sie im Literaturverzeichnis der einzelnen Gerätehandbücher.

/1/

SIMATIC NET - TeleControl

Siemens AG

Projektierungshandbücher für die Protokolle:

- TeleControl Basic

- SINAUT ST7

- DNP3

- IEC 60870-5

Link: (<https://support.industry.siemens.com/cs/ww/de/ps/21764/man>)

12/

12/

SIMATIC NET
TIM 1531 IRC
Betriebsanleitung
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/24710/man>)

13/

SIMATIC NET
CP 1243-1
Betriebsanleitung
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/de/view/103948898>)

14/

SIMATIC NET
CP 1243-8 IRC
Betriebsanleitung
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/21162/man>)

15/

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

16/

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

/7/

SIMATIC
S7-1200 Automatisierungssystem
Systemhandbuch
Siemens AG
Link: (<http://support.automation.siemens.com/WW/view/de/34612486>)

/8/

SIMATIC
ET 200SP - Dezentrales Peripheriesystem
Systemhandbuch
Siemens AG
Link: (<http://support.automation.siemens.com/WW/view/de/58649293>)

/9/

SIMATIC NET
Diagnose und Projektierung mit SNMP
Diagnosehandbuch
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/de/ps/15392/man>)

/10/

SIMATIC NET
Industrial Ethernet
Systemhandbuch
Siemens AG

- Band 1: Industrial Ethernet
Link: (<https://support.industry.siemens.com/cs/ww/de/view/27069465>)
- Band 2: Passive Netzkomponenten
Link: (<https://support.industry.siemens.com/cs/ww/de/view/84922825>)

Index

A

Abbildspeicher, 130
Abkürzungen, 3
IPSec-Tunnel
Authentifizierung, 26

D

Datenpufferung, 19, 25
Datenpunkte - Projektierung, 115
Diagnosemeldungen, 202
Direkte Kommunikation, 13
 Projektierung, 127
Dokumentation - Aufbau, 4

E

E-Mail
 Anzahl Nachrichten, 19, 26

G

Gateway (VPN), 83
Glossar, 6

I

Internet-Verbindungen, 31
IP-Adresse - feste, 49
IPsec, 79

K

Klassisches WAN, 47
Knotenstation, 12
Konsistenter Datenbereich, 18

M

MIB, 166
MSC, 26
MSCsec, 26

N

NTP (secure), 39
Nutzdaten, 18

O

Online-Diagnose, 33
Online-Funktionen, 160
OUC (Open User Communication), 169

P

Partnerstatus - Diagnose, 161
Passiver VPN-Verbindungsaufbau, 83
Port 8448, 162

Q

Querverweise (PDF), 5

R

RS-485
 Projektierung, 52, 54
Rückspiegelung, 125

S

S7-Verbindungen
 freigeben, 33
SD-Karte, 25, 35
Security
 Protokolle, 26
Security-Diagnose, 162
Security-Funktionen, 24
Sendepuffer, 19, 25, 130
SIMATIC NET-Glossar, 6
SMS
 Anzahl Nachrichten, 19
SMTPS, 71
SNMP, 165
SNMPv3, 27, 76
Spontan, 134

SSL/TLS, 71
STARTTLS, 71
STEP 7 - Version, 15
SYSLOG, 79

T

Telegrammspeicher, 19, 25
Trigger-Variable - Rücksetzen, 133, 150

V

Verbindungs-Ressourcen, 25
Verbindungsunterbrechung, 31
Verbindungszustand - Diagnose, 161
Verschlüsselung, 26
VPN, 19, 31, 79

W

WAN - Netz anlegen, 47
Webserver, 51

Z

Zeitstempel, 18
Zertifikat importieren - E-Mail, 72
Zwangsabbildspeicherverfahren, 130