SIEMENS

SIMATIC NET

ET 200SP - Industrial Ethernet CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1

Istruzioni operative

01/2017

C79000-G8972-C426-03

Avvertenze di legge

Concetto di segnaletica di avvertimento

Questo manuale contiene delle norme di sicurezza che devono essere rispettate per salvaguardare l'incolumità personale e per evitare danni materiali. Le indicazioni da rispettare per garantire la sicurezza personale sono evidenziate da un simbolo a forma di triangolo mentre quelle per evitare danni materiali non sono precedute dal triangolo. Gli avvisi di pericolo sono rappresentati come segue e segnalano in ordine descrescente i diversi livelli di rischio.

⚠ PERICOLO
questo simbolo indica che la mancata osservanza delle opportune misure di sicurezza **provoca** la morte o gravi lesioni fisiche.

⚠ AVVERTENZA
il simbolo indica che la mancata osservanza delle relative misure di sicurezza **può causare** la morte o gravi lesioni fisiche.

⚠ CAUTELA
indica che la mancata osservanza delle relative misure di sicurezza può causare lesioni fisiche non gravi.

ATTENZIONE
indica che la mancata osservanza delle relative misure di sicurezza può causare danni materiali.

Nel caso in cui ci siano più livelli di rischio l'avviso di pericolo segnala sempre quello più elevato. Se in un avviso di pericolo si richiama l'attenzione con il triangolo sul rischio di lesioni alle persone, può anche essere contemporaneamente segnalato il rischio di possibili danni materiali.

Personale qualificato

Il prodotto/sistema oggetto di questa documentazione può essere adoperato solo da **personale qualificato** per il rispettivo compito assegnato nel rispetto della documentazione relativa al compito, specialmente delle avvertenze di sicurezza e delle precauzioni in essa contenute. Il personale qualificato, in virtù della sua formazione ed esperienza, è in grado di riconoscere i rischi legati all'impiego di questi prodotti/sistemi e di evitare possibili pericoli.

Uso conforme alle prescrizioni di prodotti Siemens

Si prega di tener presente quanto segue:

⚠ AVVERTENZA
I prodotti Siemens devono essere utilizzati solo per i casi d’impiego previsti nel catalogo e nella rispettiva documentazione tecnica. Qualora vengano impiegati prodotti o componenti di terzi, questi devono essere consigliati oppure approvati da Siemens. Il funzionamento corretto e sicuro dei prodotti presuppone un trasporto, un magazzinaggio, un’installazione, un montaggio, una messa in servizio, un utilizzo e una manutenzione appropriati e a regola d’arte. Devono essere rispettate le condizioni ambientali consentite. Devono essere osservate le avvertenze contenute nella rispettiva documentazione.

Marchio di prodotto

Tutti i nomi di prodotto contrassegnati con ® sono marchi registrati della Siemens AG. Gli altri nomi di prodotto citati in questo manuale possono essere dei marchi il cui utilizzo da parte di terzi per i propri scopi può violare i diritti dei proprietari.

Esclusione di responsabilità

Abbiamo controllato che il contenuto di questa documentazione corrisponda all'hardware e al software descritti. Non potendo comunque escludere eventuali differenze, non possiamo garantire una concordanza perfetta. Il contenuto di questa documentazione viene tuttavia verificato periodicamente e le eventuali correzioni o modifiche vengono inserite nelle successive edizioni.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANIA

C79000-G8972-C426-03
℗ 01/2017 Con riserva di modifiche

Copyright © Siemens AG 2017.
Tutti i diritti riservati

Prefazione

Validità di questo manuale

In questo documento si trovano informazioni sui seguenti moduli:

- **CP 1542SP-1**
  Numero di articolo **6GK7542-6UX00-0XE0**
  Versione hardware 1
  Versione firmware V1.0
  Processore di comunicazione per il collegamento di una CPU SIMATIC ET 200SP a Industrial Ethernet
- **CP 1542SP-1 IRC**
  Numero di articolo **6GK7542-6VX00-0XE0**
  Versione hardware 1
  Versione firmware V1.0
  Processore di comunicazione per il collegamento di una CPU SIMATIC ET 200SP tramite Industrial Ethernet ad una stazione di controllo (TCSB, DNP3, IEC 60870-5-104)
- **CP 1543SP-1**
  Numero di articolo **6GK7543-6WX00-0XE0**
  Versione hardware 1
  Versione firmware V1.0
  Processore di comunicazione per il collegamento di una CPU SIMATIC ET 200SP a Industrial Ethernet, Security

Figura 1 CP 1542SP-1 con BusAdapter inserito (in questo caso 2xRJ45)

Sul lato anteriore dell'unità è impressa come segnaposto una "X" a destra della versione hardware. Se la scritta ad es. è "X 2 3 4", X è il segnaposto per la versione hardware 1.

Subito sotto si trova l'indicazione della versione firmware del CP nello stato di fornitura.

L'indirizzo MAC è impresso sul lato anteriore a sinistra in basso, al di sopra dei collegamenti per l'alimentazione.

Denominazione di prodotto, termini e abbreviazioni

Di seguito sono riportati i termini e le abbreviazioni ricorrenti nel presente manuale.

- **CP**

  Se la proprietà descritta nel rispettivo contesto è valida per tutti e tre i tipi di CP o se il tipo di CP utilizzato si evince in modo chiaro dal contesto, l'abbreviazione "CP" viene utilizzata in sostituzione per tutte e tre le seguenti denominazioni di prodotto:

  – CP 1542SP-1

  – CP 1542SP-1 IRC

  – CP 1543SP-1

  Se le informazioni valgono solo per una determinata variante di prodotto, viene indicato il nome completo del modulo.

- **TCSB**

  Software della stazione di controllo "TeleControl Server Basic"

- **Server Telecontrol**

  PC con software "TeleControl Server Basic" installato

Scopo del manuale

Questo manuale descrive le proprietà dell'unità e fornisce un supporto durante il montaggio e la messa in servizio.

Le fasi di progettazione necessarie vengono descritte come panoramica e sono presenti le descrizioni della relazione tra le funzioni firmware e la progettazione.

Inoltre si trovano avvertenze sulle possibilità di diagnostica del dispositivo.

Conoscenze richieste

Per il montaggio, la messa in servizio e il funzionamento del CP sono richieste conoscenze dei seguenti settori:

- Tecnica di automazione
- Configurazione del sistema SIMATIC ET 200SP
- SIMATIC STEP 7 Professional

Nuovo in questa edizione

Elaborazione redazionale (omologazione MSIP)

Edizione sostituita

Uscita 11/2016

Edizione attuale del manuale in Internet

L'edizione attuale del presente manuale si trova anche nelle pagine Internet del Siemens Industry Online Support ai seguenti indirizzi:

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

Riferimenti incrociati

In questo manuale vengono frequentemente utilizzati riferimenti incrociati ad altri capitoli.

Per tornare alla pagina precedente dopo un salto ad un riferimento incrociato, alcuni PDF reader supportano il comando <Alt>+<freccia a sinistra>.

Ulteriore bibliografia

Nell'appendice di questo manuale si trova una panoramica di ulteriore documentazione.

Condizioni di licenza

Nota

Open Source Software

Prima di utilizzare il prodotto leggere attentamente le condizioni di licenza per l'Open Source Software.

Le condizioni di licenza si trovano nel seguente documento, contenuto nel supporto dati fornito:

- OSS_CP-ET200SP_86.pdf

Avvertenze di sicurezza

Siemens commercializza prodotti e soluzioni dotati di funzioni Industrial Security che contribuiscono al funzionamento sicuro di impianti, soluzioni, macchine e reti.

La protezione di impianti, sistemi, macchine e reti da minacce cibernetiche, richiede l'implementazione e la gestione continua di un concetto globale di Industrial Security che corrisponda allo stato attuale della tecnica. I prodotti e le soluzioni Siemens costituiscono soltanto una componente imprescindibile di questo concetto.

È responsabilità del cliente prevenire accessi non autorizzati ad impianti, sistemi, macchine e reti. Il collegamento di sistemi, macchine e componenti, se necessario, deve avvenire esclusivamente nell'ambito della rete aziendale o tramite Internet previa adozione di opportune misure (ad es. impiego di firewall e segmentazione della rete).

Attenersi inoltre alle raccomandazione Siemens concernenti misure di sicurezza adeguate. Ulteriori informazioni su Industrial Security sono disponibili al sito
Link: (http://www.siemens.com/industrialsecurity)

I prodotti e le soluzioni Siemens vengono costantemente perfezionati per incrementarne la sicurezza. Siemens raccomanda espressamente di eseguire gli aggiornamenti non appena sono disponibili i relativi update e di impiegare sempre le versioni aggiornate dei prodotti. L'uso di prodotti non più attuali o di versioni non più supportate incrementa il rischio di attacchi cibernetici.

Per essere costantemente aggiornati sugli update dei prodotti, abbonarsi a Siemens Industrial Security RSS Feed al sito
Link: (http://www.siemens.com/industrialsecurity)

Firmware

Il firmware è contrassegnato e codificato. Viene assicurato che nel dispositivo possa essere caricato solo un firmware creato da Siemens.

Glossario SIMATIC NET

Descrizione dei numerosi termini specifici, presenti nella documentazione che si trovano nel glossario SIMATIC NET.

Il glossario SIMATIC NET si trova:

- SIMATIC NET Manual Collection o DVD del prodotto

  Il DVD è allegato ad alcuni prodotti SIMATIC NET.

- In Internet al seguente indirizzo:

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

Training, Service & Support

Le informazioni relative al Training, Service & Support si trovano nel file multilingue "DC_support_99.pdf" nelle pagine Internet del Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/it/view/38652101)

Indice del contenuto

Applicazione e funzioni

1

1.1 Fornitura

I seguenti componenti fanno parte della fornitura del prodotto:

- CP 154xSP-1
- Connettore per la presa dell'alimentazione (DC 24 V) del CP
- DVD con documentazione e testi di licenza

Un BusAdapter per il collegamento Ethernet del CP non fa parte della fornitura.

1.2 Impiego

Impiego delle varianti CP

Il CP serve per il collegamento di ET 200SP a Industrial Ethernet tramite un cavo in rame o un cavo a fibre ottiche. Esso può essere utilizzato come interfaccia Ethernet supplementare della CPU per la comunicazione S7.

Per il collegamento Ethernet il CP necessita di un BusAdapter non compreso nella fornitura del CP.

Le tre varianti di CP sono previste per i seguenti compiti di comunicazione:

- **CP 1542SP-1**

  Il CP 1542SP-1 consente a ET 200SP un ulteriore collegamento Ethernet.

- **CP 1542SP-1 IRC**

  Il CP 1542SP-1 IRC supporta la comunicazione Telecontrol per il collegamento della CPU ET 200SP -CPU ad una stazione di controllo. I seguenti protocolli Telecontrol possono essere utilizzati in alternativa:

  – TeleControl Basic

    Per il collegamento di ET 200SP ad una centrale con server Telecontrol (TCSB V3 SP3)

  – DNP3

    Per il collegamento di ET 200SP ad una centrale con master DNP3

  – IEC 60870-5-104

    Per il collegamento di ET 200SP ad una centrale con master IEC

- **CP 1543SP-1**

  Il CP 1543SP-1 dispone di funzioni Security per la sicurezza della rete, quali ad es. firewall e VPN. In questo modo è possibile un accesso protetto a ET 200SP.

1.3 Servizi di comunicazione

Servizi di comunicazione

Vengono supportati i seguenti servizi di comunicazione:

- **Comunicazione S7 e comunicazione PG/OP con le seguenti funzioni:**
  - PUT/GET come client e server per lo scambio di dati con stazioni S7
  - Funzioni PG
  - Funzioni di servizio e supervisione (HMI)

  Per la comunicazione S7 il CP necessita di un indirizzo IP fisso.
- **Routing S7**
  - Routing di collegamenti S7 tramite il bus backplane e la CPU ad altre stazioni S7
- **Open User Communication (OUC)**

  OUC tramite blocchi di programma con i seguenti protocolli:
  - TCP/IP
  - ISO-on-TCP
  - UDP

  Il CP 1543SP-1 supporta Secure OUC.

  I blocchi di programma supportati dai tre tipi di CP si trovano nel capitolo Programmazione (OUC) (Pagina 97).
- **E-mail tramite blocchi di programma**
- **HTTP / HTTPS**

  Tramite HTTP / HTTPS è possibile accedere al Webserver della CPU.

Per la comunicazione Telecontrol del CP 1542SP-1 IRC vedere il capitolo Comunicazione Telecontrol del CP 1542SP-1 IRC (Pagina 13).

Per le funzioni Security del CP 1543SP-1 vedere il capitolo Funzioni Security (CP 1542SP-1 IRC, CP 1543SP-1) (Pagina 15).

1.4 Comunicazione Telecontrol del CP 1542SP-1 IRC

Protocolli Telecontrol

Oltre ai servizi di comunicazione indicati il CP 1542SP-1 IRC supporta i seguenti protocolli di telecontrollo per la comunicazione con una centrale:

- **TeleControl Basic**

  Questo è un protocollo di Siemens per applicazioni di telecontrollo. Il protocollo basato su IP serve a collegare il CP all'applicazione TCSB.

  TCSB è installato su un PC nella centrale, collegato al server Telecontrol. Tramite il server OPC DA o OPC UA del TCSB un client OPC può accedere ai dati di processo del CP.

  TCSB viene supportato a partire dalla seguente versione: V3.0 + SP3

  Per il manuale di TCSB vedere /3/ (Pagina 122).

- **DNP3**

  Il CP funge da stazione DNP3 (Outstation).

  La comunicazione si basa sulla DNP3 SPECIFICATION Version 2.11 (2007/2009).

  Una panoramica dettagliata degli attributi e delle proprietà specificati nel protocollo DNP3 e sopportati del CP si trova nel profilo del dispositivo DNP3, vedere Link: (https://support.industry.siemens.com/cs/ww/it/ps/22143/man).

  I gruppi degli oggetti e le variazioni si trovano nel capitolo Tipi di punti di accesso ai dati (Pagina 60).

  I partner di comunicazione (master DNP3) del CP possono essere:

  – SIMATIC PCS7 TeleControl
  – SIMATIC WinCC TeleControl
  – SIMATIC WinCC OA
  – Un'unità TIM con funzione DNP3 (TIM 3V IE DNP3 / TIM 4R IE DNP3)

    Per il manuale dell'unità TIM vedere /5/ (Pagina 122).
  – Sistemi di altri produttori che supportano la specifica DNP3 indicata.

- **IEC 60870-5-104**

  Il CP funge come sottostazione (slave).

  La comunicazione si basa sulla specifica IEC 60870-5, parte 104 (2006).

  Una panoramica dettagliata degli attributi e delle proprietà specificati nella specifica IEC e sopportati dal CP si trova nel profilo del dispositivo IEC, vedere Link: (https://support.industry.siemens.com/cs/ww/it/ps/22143/man).

  Le identificazioni di tipo IEC supportate si trovano nel capitolo Tipi di punti di accesso ai dati (Pagina 60).

  I partner di comunicazione (master IEC) del CP possono essere:

  – SIMATIC PCS7 TeleControl

- SIMATIC WinCC TeleControl
- SIMATIC WinCC OA
- Sistemi di altri produttori che supportano la specifica DNP3 indicata.

Proprietà del CP Telecontrol

- **Progettazione del punto di accesso ai dati**

  I valori di processo vengono progettati come punti di accesso ai dati per la comunicazione. I punti di accesso ai dati accedono alle variabili PLC nella CPU. I punti di accesso ai dati possono essere elaborati uno ad uno nel sistema di controllo.

- **Messaggi / e-mail**

  Per determinati eventi progettabili nell'immagine di processo della CPU, il CP 1542SP-1 IRC può inviare messaggi in forma di e-mail. I dati inviati per e-mail vengono progettati tramite variabili PLC.

- **Salvataggio di eventi**

  Il CP 1542SP-1 IRC può memorizzare eventi di diverse classi e trasferirli al partner di comunicazione in gruppi.

- **Preelaborazione del valore analogico**

  I valori analogici possono essere preelaborati nel CP 1542SP-1 IRC secondo diversi metodi.

1.5 Altri servizi e proprietà

Altri servizi e proprietà del CP

- **Configurazione IP**
  - Tipi di indirizzo

    Il CP supporta gli indirizzi IP secondo IPv4 e IPv6.
  - Indirizzamento

    L'indirizzo IP, la maschera di sottorete e l'indirizzo di un accoppiamento ad altra rete possono essere impostati manualmente durante la progettazione. In alternativa l'indirizzo IP può essere acquisito tramite un blocco di programma.
  - DHCP: In alternativa l'indirizzo IP può essere acquisito da un server DHCP.
  - Viene supportato DCP (Discovery and Configuration Protocol).

- **Sincronizzazione dell'ora**
  - NTP

    Sull'interfaccia Ethernet il CP può sincronizzare la sua ora tramite NTP.
  - Solo CP 1542SP-1 IRC

    Con la comunicazione Telecontrol attivata il CP rileva sempre l'ora locale come ora UTC dal partner di comunicazione. L'ora del CP può essere letta dalla CPU tramite una variabile PLC. Per il formato di data e ora dei telegrammi di dati vedere il capitolo Tipi di punti di accesso ai dati (Pagina 60).

    Con la comunicazione Telecontrol disattivata il CP può sincronizzare la sua ora tramite NTP.
  - Solo CP 1543SP-1

    Con le funzioni Security attivate può essere utilizzato il metodo protetto NTP (secure).

  Ulteriori informazioni si trovano nel capitolo Sincronizzazione dell'ora (Pagina 43).
- **SNMP**

  Come SNMP Agent il CP supporta interrogazioni tramite SNMPv1.

  Il CP 1543SP-1 supporta inoltre SNMPv3.

  Ulteriori informazioni si trovano nel capitolo SNMP (Pagina 45).

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

Le funzioni Security descritte di seguito vengono attivate nella progettazione per il rispettivo CP.

Per le funzioni Security della Open User Communication vedere il capitolo Programmazione (OUC) (Pagina 97).

Nota

Raccomandazioni per impianti a sicurezza critica

Osservare le avvertenze nel capitolo Raccomandazioni Security (Pagina 39).

Funzioni Security del CP 1542SP-1 IRC

- **E-mail**

  Per la trasmissione protetta di informazioni mediante e-mail codificate è possibile utilizzare in alternativa:
  - SSL/TLS
  - STARTTLS

  Per la progettazione vedere il capitolo Security > Progettazione delle e-mail (Pagina 87).

- **Certificati**

  Per l'autenticazione sicura dei partner di comunicazione vengono utilizzati certificati.

- **Comunicazione Telecontrol protetta**

  I protocolli Telecontrol offrono le seguenti funzioni Security:

  – TeleControl Basic

    Come funzione Security integrata il protocollo Telecontrol codifica i dati durante la trasmissione tra CP e server Telecontrol. L'intervallo dello scambio di codifica tra CP e il server Telecontrol è impostato su 1 ora.

    La password Telecontrol serve per l'autentificazione del CP nel server Telecontrol.

  – DNP3

    Il CP supporta i meccanismi Security elencati nella specifica.

Funzioni Security del CP 1543SP-1

Con Industrial Ethernet Security è possibile proteggere singoli apparecchi, celle di automazione o segmenti di rete di una rete Ethernet. La trasmissione di dati tramite il CP 1543SP-1 può essere protetta con la combinazione di diverse misure di sicurezza da:

- spionaggio dei dati
- manipolazione dei dati
- accessi non autorizzati

Tramite interfacce Ethernet/PROFINET supplementari della CPU possono essere utilizzate reti sicure subordinate.

Utilizzando il CP come modulo Security, per la stazione ET 200SP diventano accessibili le seguenti funzioni Security sull'interfaccia verso la rete Ethernet:

- **Firewall**

  Il firewall protegge il dispositivo tramite:

  – IP Firewall con Stateful Packet Inspection (layer 3 e 4)

  – Firewall anche per frame Ethernet "Non-IP" secondo IEEE 802.3 (layer 2)

  – Limitazione della velocità di trasmissione ("Limitazione di larghezza di banda")

- **Certificati**

  Per l'autenticazione sicura dei partner di comunicazione vengono utilizzati certificati.

- **Comunicazione protetta con IPsec Tunnel (VPN)**

  La comunicazione via tunnel VPN consente la realizzazione di un tunnel IPSec protetto per la comunicazione con uno o diversi moduli Security. Il CP può essere unito in un gruppo VPN con altre unità tramite progettazione. Tra tutti i moduli Security di un gruppo VPN vengono realizzati IPsec Tunnel (VPN).

- **Logging**

  Per la trasmissione è possibile salvare gli eventi in file Log, che possono essere letti con lo strumento di progettazione o inviati automaticamente ad un Syslog Server.

- **NTP (secure)**

  Per la trasmissione sicura con la sincronizzazione dell'ora

- **SNMPv3**

  Per la trasmissione continua sicura delle informazioni di analisi della rete

Avvertenze per la progettazione delle funzioni Security si trovano nel capitolo Progettazione Security (CP 1543SP-1) (Pagina 88).

Ulteriori informazioni per la funzionalità e la progettazione delle funzioni Security si trovano nel sistema di informazioni di STEP 7 e nel manuale /4/ (Pagina 122).

1.7 Limiti di configurazione e dati utili

Numero di CP per ogni stazione

Per ogni stazione ET 200SP si possono inserire e progettare fino a tre unità speciali di cui max. due CP 154xSP-1.

Per i dettagli relativi alle unità speciali e alle regole per i posti connettore vedere il capitolo Montaggio del CP (Pagina 32).

Risorse di collegamento

Numero complessivo di collegamenti tramite Industrial Ethernet max. 32,
di cui:

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

Inoltre:

- Collegamenti online della stazione di engineering (STEP 7): Max. 2
- Collegamenti TCP per HTTP

  Per gli accessi HTTP sono disponibili fino a 12 risorse di collegamento TCP che vengono utilizzate da uno o da più browser web per visualizzare i dati del CP.
- Collegamenti PG/OP (HMI): Complessivamente max. 16,
  di cui:
  - Risorse di collegamento per collegamenti PG: Max. 16
  - Risorse di collegamento per collegamenti OP: Max. 16

Memoria dei telegrammi (buffer di invio)

Solo CP 1542SP-1 IRC

Il CP dispone di una memoria di telegrammi (buffer di invio) per i valori dei punti di accesso ai dati progettati come evento.

Il volume del buffer di trasmissione si ripartisce in parti uguali tra tutti i partner di comunicazione progettati.

La dimensione del buffer di trasmissione è progettabile in STEP 7, vedere il capitolo Comunicazione con la CPU (Pagina 57).

La dimensione massima del buffer di trasmissione dipende dal protocollo di telecontrollo utilizzato ed è di:

- TeleControl Basic

  64000 eventi

- DNP3

  100000 eventi

- IEC 60870-5-104

  100000 eventi

I dettagli relativi alla funzione del buffer di trasmissione nonché al salvataggio di eventi e alle possibilità di trasmissione dei dati si trovano nel capitolo Immagine di processo, tipi di trasmissione, classi di evento, trigger (Pagina 64).

E-mail (tramite editor di messaggi)

Solo CP 1542SP-1 IRC

Con la comunicazione Telecontrol attivata in STEP 7 è possibile progettare fino a 10 messaggi. I messaggi vengono inviati come e-mail.

Collegamenti Telecontrol e punti di accesso ai dati

Solo CP 1542SP-1 IRC

- **Collegamenti Telecontrol**
  - TeleControl Basic

    Può essere realizzato un collegamento con un server Telecontrol con configurazione singola o ridondante.
  - DNP3

    Possono essere realizzati collegamenti con fino a quattro master.
  - IEC 60870-5-104

    Possono essere realizzati collegamenti con fino a quattro master.
- **Punti di accesso ai dati**

  I dati che devono essere trasferiti dal CP vengono assegnati a diversi punti di accesso nella progettazione di STEP 7. Le dimensioni dei dati utili per ogni punto di accesso ai

dati varia in funzione del tipo di dati di ciascun punto. I dettagli si trovano nel capitolo Tipi di punti di accesso ai dati (Pagina 60).

Il numero massimo di punti di accesso ai dati progettati è 500.

Nell'occupazione della memoria interna al CP per i punti di accesso ai dati viene inclusa anche la lunghezza dei nomi dei punti di accesso ai dati. Osservare a tal proposito le avvertenze nel capitolo Progettazione dei punti di accesso ai dati (Pagina 58).

Funzioni Security

Solo CP 1543SP-1

- **Tunnel VPN**

  Possono essere realizzati max. quattro tunnel VPN per la comunicazione protetta con altri moduli Security.

- **Regole firewall**

  Il numero massimo delle regole firewall in modalità firewall estesa è limitato a 256. Le regole firewall si suddividono nel modo seguente:

  – Max. 226 regole con indirizzi singoli

  – Max. 30 regole con aree di indirizzi o indirizzi di rete (ad es. 140.90.120.1 - 140.90.120.20 o 140.90.120.0/16)

  – Max. 128 regole con limitazione della velocità di trasmissione ("Limitazione di larghezza di banda")

1.8 Requisiti richiesti per l'impiego

1.8.1 Requisiti hardware

BusAdapter

Per il collegamento alla rete Ethernet il CP necessita di un BusAdapter. Un BusAdapter non fa parte della fornitura del CP.

Il CP supporta i seguenti BusAdapter:

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

Ulteriori dettagli sui BusAdapter sono riportati nel capitolo BusAdapter (Pagina 119) e nel manuale /2/ (Pagina 121).

CPU e altri componenti di ET 200SP

Il CP supporta il funzionamento in stazioni che contengono le seguenti CPU:

- CPU 1510SP-1 PN

  Numero di articolo: 6ES7510-1DJ01-0AB0
- CPU 1510SP F-1 PN

  Numero di articolo: 6ES7510-1SJ01-0AB0
- CPU 1512SP-1 PN

  Numero di articolo: 6ES7512-1DK01-0AB0
- CPU 1512SP F-1 PN

  Numero di articolo: 6ES7512-1SK01-0AB0

Ulteriori componenti e moduli supplementari, necessari per la configurazione della stazione ET 200SP, quali guide, moduli di periferia o cablaggio non vengono elencati nella presente descrizione. Vedere a riguardo /2/ (Pagina 121).

Componenti dei partner di comunicazione

I componenti necessari al partner di comunicazione del CP 1542SP-1 IRC non sono elencati nella presente descrizione. Rimandi alla documentazione di altri prodotti (ad es. TCSB) si trovano nella bibliografia nell'appendice del manuale.

1.8.2 Requisiti software

Software di progettazione

Per la progettazione del CP è necessario il seguente strumento di progettazione:

- STEP 7 Professional a partire dalla versione 14

Software per funzioni online

Per l'utilizzo delle funzioni online è necessario il seguente software:

- STEP 7 nella versione sopra indicata.

Firmware CPU

Per l'impiego del CP è necessaria una CPU 151xSP con una versione firmware ≥ V2.0.

Protocolli di telecontrollo (CP 1542SP-1 IRC)

Le versioni dei protocolli di telecontrollo supportati dal CP si trovano nel capitolo Comunicazione Telecontrol del CP 1542SP-1 IRC (Pagina 13).

1.9 Esempi di configurazione

Di seguito sono riportati esempi di configurazione per l'impiego delle tre varianti di CP.

Separazione di reti CP 1542SP-1 -

Il CP viene impiego in ET 200SP per utilizzare separatamente reti sobordinate o per ottenere una separazione di reti sovraordinate.

ET 200SP può essere ampliata con altre interfacce Ethernet tramite il CP. Grazie alla separazione di reti è possibile la configurazione i macchine identiche con lo stesso indirizzo IP. Il CP assume la comunicazione e alleggerisce la CPU.

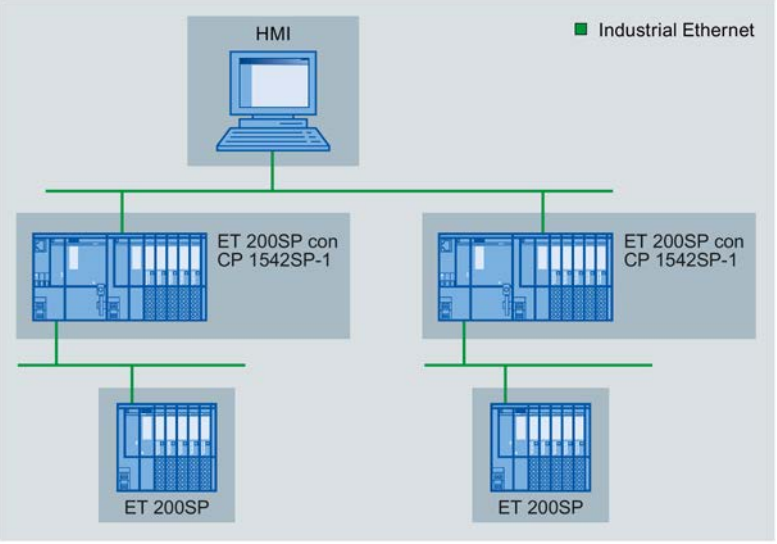


Figura 1-1 Esempio di configurazione di una ET 200SP con CP 1542SP-1

CP 1543SP-1 - Protezione delle celle mediante funzioni Security

Il CP comunica in modo codificato con i partner di comunicazione nella rete collegata. Il firewall sorveglia l'accesso a ET 200SP e protegge quindi le reti subordinate. In questo modo vengono ridotti la perdita di dati, i guasti della produzione e i danni alla macchina.

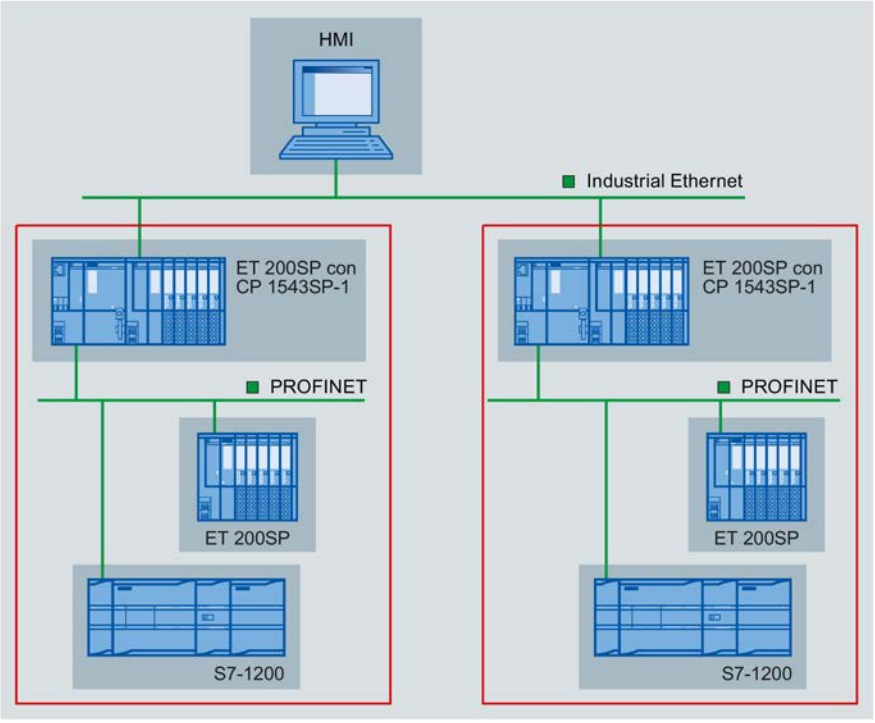


Figura 1-2 Esempio di configurazione di una ET 200SP con CP 1543SP-1

CP 1542SP-1 IRC - Collegamento alle centrali di controllo

Impiegando il CP è possibile impiegare ET 200SP come Remote Terminal Unit. Per la comunicazione possono essere impiegati i seguenti protocolli Telecontrol:

- TeleControl Basic

  Il protocollo di telecontrollo SIEMENS per il collegamento alle centrali con TCSB
- IEC 60870-5-104
- DNP3

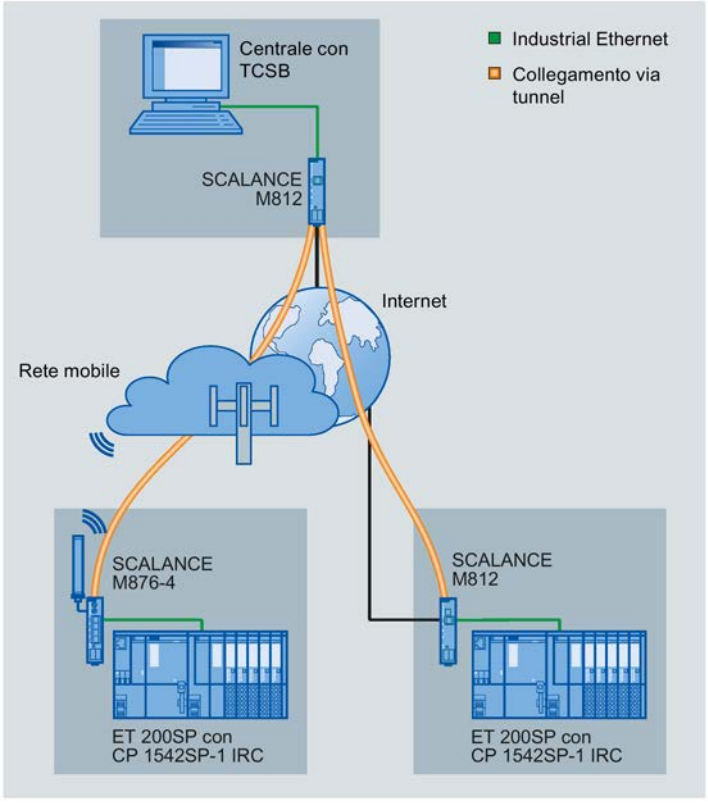


Figura 1-3 Esempio di configurazione di una ET 200SP con CP 1542SP-1 IRC; protocollo: TeleControl Basic

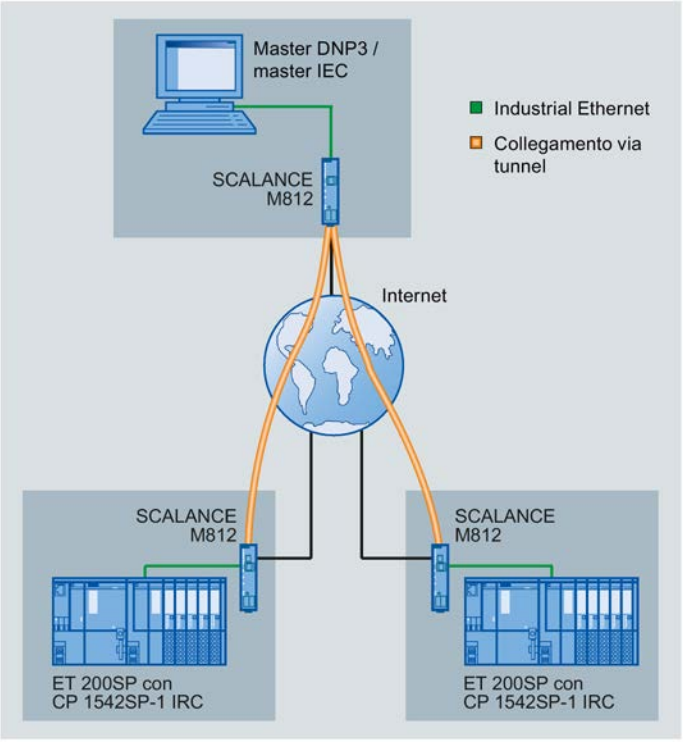


Figura 1-4 Esempio di configurazione di una ET 200SP con CP 1542SP-1 IRC; protocollo: DNP3 o IEC 60870-5-104

LED e collegamenti

2

2.1 LED

Significato degli indicatori LED del CP

Sulla parte anteriore il CP dispone dei seguenti diodi luminosi (LED):

Nome LED	Significato
PWR	Alimentazione
RN	Stato operativo
ER	Errore
MT	Manutenzione

Tabella 2- 1 Legenda delle seguenti tabelle

Simbolo				-
Significato / stato del LED	ON (LED acceso)	OFF	LED lampeggia	Qualsiasi

Tabella 2- 2 Significato degli indicatori LED del CP

PWR (verde)	RN (verde)	ER (rosso)	MT (giallo)	Significato
				Tensione di alimentazione del CP assente o insufficiente
				Avvio del CP
				CP nello stato operativo RUN
	-			Errore. Immagine LED con i seguenti eventi: • Indirizzo IP doppio • BusAdapter non inserito o estratto • Nessun collegamento Telecontrol (CP 1542SP-1 IRC)
				Errori: CP guasto
				Dati di progettazione assenti

PWR (verde)	RN (verde)	ER (rosso)	MT (giallo)	Significato
				Aggiornamento del firmware in corso.
				È presente una richiesta di manutenzione del CP. Esempio: • Fine dell'aggiornamento firmware

Indicatori LED del BusAdapter

Ciascuna porta di un BusAdapter dispone di un LED "LKx" che fornisce informazioni sullo stato del collegamento con Ethernet e sul traffico di telegrammi della porta.

Tabella 2- 3 Significato degli indicatori LED dei BusAdapter

LK (verde)	Significato
	Nessun collegamento Ethernet. Possibili cause: • Nessun collegamento fisico con la rete • Porta disattivata nella progettazione
	Test di lampeggio dei LED
	Esiste un collegamento Ethernet tra porta e partner di comunicazione.

2.2 Alimentazione

Alimentazione esterna necessaria

Il collegamento per l'alimentazione esterna di DC 24 V si trova sul lato anteriore del CP.

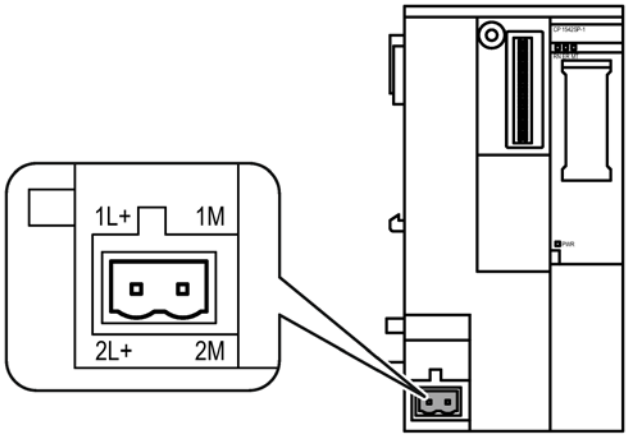


Figura 2-1 Alimentazione del CP

Il collegamento X80 è previsto per il collegamento ad un'alimentazione con configurazione singola o ridondante. L'alimentazione viene collegata alla morsettiera ad innesto fornita con il CP. La morsettiera viene inserita nella presa X80 del CP.

Le informazioni relative al montaggio e al collegamento si trovano nei capitoli Montaggio del CP (Pagina 32) e Collegamento del CP (Pagina 36).

Protezione da inversione polarità

La morsettiera ad innesto per il collegamento X80 è realizzata in modo da poter essere inserita solo in una posizione. Di conseguenza risulta una protezione da inversione polarità per la struttura.

Il collegamento X80 dispone inoltre di una protezione da inversione polarità elettronica.

Ulteriori dati relativi all'alimentazione si trovano nel capitolo Dati tecnici (Pagina 111).

2.3 Collegamento per il BusAdapter

Funzionamento del dispositivo solo con BusAdapter

Per il collegamento a Ethernet il CP necessita di un BusAdapter. Un BusAdapter non fa parte della fornitura del CP.

Il posto connettore si trova sul lato anteriore del dispositivo.

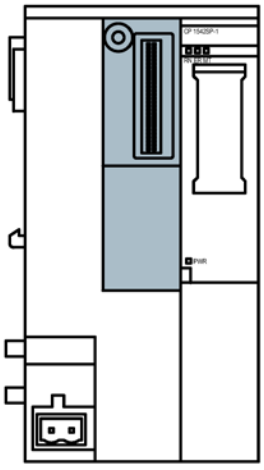


Figura 2-2 Lato frontale del CP, il posto connettore del BusAdapter è contrassegnato in grigio.

I BusAdapter supportati dal CP si trovano nel capitolo BusAdapter (Pagina 119).

Le informazioni relative al montaggio e al collegamento si trovano nei capitoli Montaggio del CP (Pagina 32) e Collegamento del CP (Pagina 36).

L'assegnazione dei pin dell'interfaccia Ethernet si trova nel capitolo Assegnazione dei pin dell'interfaccia Ethernet del BusAdapter (Pagina 120). Ulteriori dati tecnici del BusAdapter si trovano nel manuale /2/ (Pagina 121).

Montaggio e collegamento 3

3.1 Avvertenze importati per l'impiego del dispositivo

Avvertenze di sicurezza per l'impiego del prodotto

Osservare le seguenti avvertenze sulla sicurezza per l'installazione e il funzionamento del dispositivo e tutti i lavori connessi, come il montaggio e il collegamento o la sostituzione del dispositivo.

Protezione da sovratensione

ATTENZIONE
Protezione dell'alimentazione di tensione esterna Se l'unità o la stazione viene alimentata tramite cavi di alimentazione o reti particolarmente estesi, sono possibili interferenze di forti impulsi magnetici sui cavi di alimentazione, causati ad es. da fulmini o dall'attivazione di forti carichi. Il collegamento dell'alimentazione esterna non è protetto dagli impulsi elettromagnetici di forte intensità. A tal fine è necessario un modulo di protezione da sovratensioni esterno. I requisiti richiesti secondo EN61000-4-5, Surge controllo dei cavi di alimentazione, vengono soddisfatti solo in caso di impiego di elemento di protezione idoneo. È adatto per esempio il Dehn Blitzductor BVT AVD 24, numero di articolo 918 422 o un elemento di protezione di pari valore. Produttore: DEHN+SOEHNE GmbH+Co.KG, Hans-Dehn-Str.1, Postfach 1640, D-92306 Neumarkt

3.1.1 Avvertenze per l'impiego in zone Ex

⚠ AVVERTENZA
PERICOLO DI ESPLOSIONI NON APRIRE L'APPARECCHIO CON LA TENSIONE DI ALIMENTAZIONE INSERITA.

⚠ AVVERTENZA
Il dispositivo può essere utilizzato solo in un ambiente con grado di imbrattamento 1 o 2 (cfr. IEC60664-1).

⚠AVVERTENZA

L'apparecchio è progettato per il funzionamento con una tensione di sicurezza a basso voltaggio collegabile direttamente (Safety Extra Low Voltage, SELV) tramite un'alimentazione con potenza limitata (Limited Power Source, LPS).

Per questo motivo possono essere collegate solo tensioni di sicurezza a basso voltaggio (SELV) con potenza limitata (Limited Power Source, LPS) secondo IEC 60950-1 / EN 60950-1 / VDE 0805-1 con i collegamenti di alimentazione oppure la tensione di rete per l'alimentazione dell'apparecchio deve corrispondere a NEC Class 2 secondo il National Electrical Code (r) (ANSI / NFPA 70).

Se l'apparecchio viene collegato ad un'alimentazione ridondante (due alimentazioni separate), entrambe le alimentazioni devono soddisfare i requisiti richiesti.

⚠AVVERTENZA

PERICOLO DI ESPLOSIONI

In un ambiente facilmente infiammabile o incendiabile non devono essere collegati o scollegati cavi dal dispositivo.

⚠AVVERTENZA

PERICOLO DI ESPLOSIONI

La sostituzione di componenti può compromettere l'idoneità per Class I, Division 2 o Zone 2.

⚠AVVERTENZA

Per l'impiego in ambiente a pericolo di esplosioni secondo la Class I, Division 2 o Class I, Zone 2, l'apparecchio deve essere montato in un quadro elettrico o in una custodia.

⚠AVVERTENZA

Guida ad U

Nel campo applicativo di ATEX e IECEx per il montaggio dei moduli può essere utilizzata solo la guida ad U 6ES5 710-8MA11.

3.1.2 Avvertenze per l'impiego in zone Ex secondo ATEX / IECEx

⚠AVVERTENZA

Requisiti richiesti per il quadro elettrico

Per essere conforme alla direttiva UE 94/9 (ATEX 95), la custodia o il quadro elettrico deve soddisfare almeno i requisiti richiesti da IP54 secondo EN 60529.

⚠AVVERTENZA

Se sul cavo o sulla presa della custodia si verificano temperature superiori a 70 °C o se la temperatura sui punti di diramazione dei conduttori dei cavi è superiore 80 °C, è necessario adottare particolari misure. Se l'apparecchio viene utilizzato a temperature ambiente superiori 50 °C, vanno utilizzati cavi con una temperatura d'esercizio ammessa di almeno 80 °C.

⚠AVVERTENZA

Adottare misure per evitare sovratensioni transienti superiori al 40% della tensione nominale. Questo viene garantito se l'apparecchio viene utilizzato esclusivamente con SELV (tensione di sicurezza a basso voltaggio).

3.1.3 Avvertenze per l'impiego nell'area Ex secondo UL HazLoc

⚠AVVERTENZA

PERICOLO DI ESPLOSIONI

Non scollegare l'apparecchio dai cavi che conducono tensione fino a quando non si è sicuri che nell'ambiente non sia presente atmosfera a rischio di esplosione.

Questo apparecchio è adatto solo per l'impiego in aree secondo Class I, Division 2, Groups A, B, C e D e in aree non soggette a pericolo di esplosione.

Questo apparecchio è adatto solo per l'impiego in aree secondo Class I, Zone 2, Group IIC e in aree non soggette a pericolo di esplosione.

3.1.4 Avvertenze generali per l'impiego in zone Ex secondo FM

⚠ AVVERTENZA
PERICOLO DI ESPLOSIONI
I cavi che conducono tensione possono essere scollegati o collegati solo con l'alimentazione disinserita o se il dispositivo si trova in un'area senza concentrazioni di gas infiammabili.

Questo apparecchio è adatto solo per l'impiego in aree secondo Class I, Division 2, Groups A, B, C e D e in aree non soggette a pericolo di esplosione.

Questo apparecchio è adatto solo per l'impiego in aree secondo Class I, Zone 2, Group IIC e in aree non soggette a pericolo di esplosione.

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

3.2 Montaggio del CP

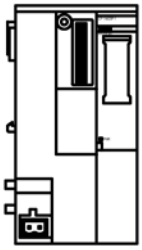
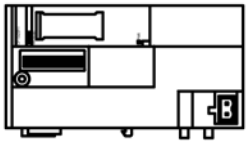
ATTENZIONE
Montaggio e smontaggio del CP solo in assenza di tensione!
Disinserire l'alimentazione di ET 200SP e del CP prima di montare o smontare i moduli. Il montaggio e lo smontaggio con l'alimentazione inserita può comportare il danneggiamento dei moduli e la perdita di dati.

Nota

Osservanza delle direttive di montaggio

Durante il montaggio e il collegamento del CP osservare le versioni nel manuale /2/ (Pagina 121).

ATTENZIONE
Posizione di montaggio - in funzione del campo di temperatura Il montaggio deve essere eseguito in modo che gli intagli di ventilazione superiori e inferiori del modulo non vengano coperti e che sia possibile un buon passaggio di aria. Sopra e sotto i moduli deve esserci uno spazio libero di 25 mm per la circolazione dell'aria per prevenire il surriscaldamento. Fare attenzione ai campi di temperatura ammessi in funzione della posizione di montaggio: • Per montaggio orizzontale del telaio di montaggio (guida ad U) si intende la posizione verticale del CP. • Per montaggio verticale del telaio di montaggio (guida ad U) si intende la posizione orizzontale del CP. I campi di temperatura ammessi si trovano nel capitolo Dati tecnici (Pagina 111).

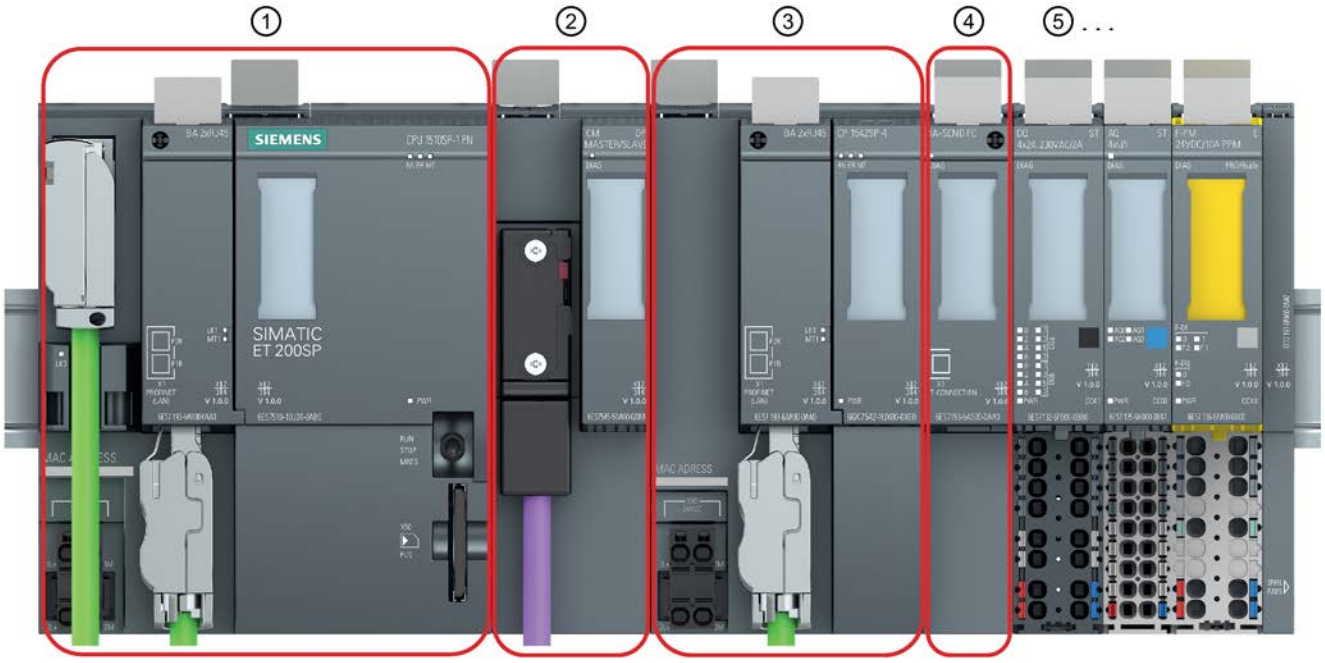
Struttura del telaio di montaggio	Posizione di montaggio del CP
Struttura orizzontale del telaio di montaggio	
Struttura verticale del telaio di montaggio	

Regole sui posti connettore

La CPU occupa sempre il posto connettore 1. In un'ET 200SP, sui posti connettore 2 .. 4 (cfr. figura) a destra di fianco alla CPU possono essere inseriti fino a tre dei seguenti moduli:

- CM
- CP
- BusAdapter Send

Di questi tre moduli possono essere inseriti fino a due CP 154xSP-1. Entrambi questi CP possono essere dello stesso tipo o essere diversi.



① Posto connettore 1 - ammesso solo per la CPU.

② Posto connettore 2 - per CM / CP / BusAdapter Send *****
Se si utilizza un PROFIBUS CM esso va inserito direttamente di fianco alla CPU nel posto connettore 1.

③ Posto connettore 3 - per CM / CP / BusAdapter Send *****

④ Posto connettore 4 - per CM / CP / BusAdapter Send *****

⑤ Posto connettore 5 ff - per periferia

***** Se si utilizza un BusAdapter Send, esso va inserito sul posto connettore direttamente di fianco ai moduli di periferia.

Figura 3-1 Posti connettore di ET 200SP

Montaggio su guida ad U

Nota

Elemento di bloccaggio dei moduli per impedire lo scivolamento sulla guida ad U

Se si montano i moduli in un'area con sollecitazione meccanica, per il bloccaggio dei moduli sulla guida ad U utilizzare dispositivi di serraggio adatti su entrambe le estremità del gruppo di dispositivi, ad es. la staffa terminale Siemens 8WA1808.

La staffa terminale impedisce che i moduli si separino in caso di sollecitazione meccanica.

In caso di impiego in settori ATEX o IECEx osservare l'avvertenza relativa alla guida ad U nel capitolo Avvertenze per l'impiego in zone Ex (Pagina 29).

Il sistema ET 200SP è adatto per il montaggio su una guida profilata secondo EN 60715 (35 × 7,5 mm o 35 × 15 mm)

1. Agganciare la CPU / il modulo di interfaccia nella guida profilata.
2. Ruotare indietro la CPU / il modulo di interfaccia fino a quando l'elemento di sbloccaggio della guida profilata scatta in posizione in modo udibile.
3. Agganciare il CP a destra di fianco alla CPU.
4. Ruotare indietro il CP fino a quando l'elemento di sbloccaggio della guida profilata scatta in posizione in modo udibile.
5. Spingere verso sinistra il CP fino a quando scatta in posizione in modo udibile nella CPU.
6. Montare le ulteriori BaseUnit e moduli di conseguenza.

   Vedere a riguardo il manuale /2/ (Pagina 121).

Inserimento del BusAdapter

ATTENZIONE
Contatto con i contatti ad innesto
Non toccare i contatti ad innesto se non è inserito nessun BusAdapter.

1. Collegare il relativo cavo al BusAdapter se si utilizza un BusAdapter con collegamento ottico o elettrico diretto (senza connettore).
2. Inserire il BusAdapter nel posto connettore del CP.

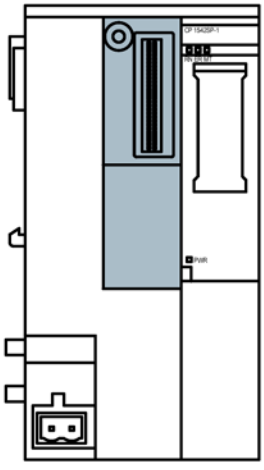


Figura 3-2 Lato anteriore del CP; il posto connettore del BusAdapter è contrassegnato in grigio.

3. Avvitare il BusAdapter con il CP.

   La vite di sicurezza di trova a sinistra in alto sul lato anteriore del BusAdapter.

   Utilizzare quindi un cacciavite con 3 ... 3,5 mm di larghezza della lama o un cacciavite Torx adatto (T15).

   La coppia di serraggio massima delle viti è di 0,25 Nm.

4. Inserire il connettore del cavo di collegamento nella presa del BusAdapter se si utilizza un BusAdapter con connettore.

Per inserire il BusAdapter e per confezionare i cavi vedere anche manuale /2/ (Pagina 121).

Smontaggio dalla guida ad U.

Eseguire le seguenti operazioni per smontare uno CP dalla guida ad U:

1. Disinserire l'alimentazione dell'intera stazione compresi il CP e la CPU.
2. Azionare l'elemento di sbloccaggio della guida profilata del modulo da spostare (CPU, CP) e spingerlo parallelamente a sinistra fino a quando si stacca dal restante insieme di moduli (spazio libero ca. 16 mm).

   Premere sempre verso il basso il cursore di bloccaggio contrassegnato con "PUSH" sul lato superiore di un modulo per poter spostare il modulo interessato sulla guida ad U.
3. Azionare l'elemento di sbloccaggio della guida profilata sul CP e spingerlo verso destra fino a quando si stacca dalla CPU (spazio libero ca. 8 mm).
4. Estrarre il CP con l'elemento di sbloccaggio della guida profilata sul CP dalla guida profilata.

3.3 Collegamento del CP

Sequenza dei lavori

ATTENZIONE
Collegamento solo in assenza di tensione
Collegare il CP solo in assenza di tensione. Osservare le indicazioni nel manuale di sistema, vedere /2/ (Pagina 121)

Il BusAdapter è già collegato al relativo cavo, vedere il capitolo Montaggio del CP (Pagina 32).

1. Collegare l'alimentazione esterna alla morsettiera del collegamento X80.

   Utilizzare la stessa alimentazione della CPU.
2. Inserire l'alimentazione solo dopo il cablaggio completo e il collegamento del CP.

Alimentazione sul collegamento X80

La posizione del collegamento X80 per l'alimentazione del CP si trova nel capitolo Alimentazione (Pagina 27). Qui si trovano anche le avvertenze per la protezione da inversione polarità.

La morsettiera innestabile a 2 poli per la presa X80 ha la seguente assegnazione:

Morsetto	Assegnazione
1L+ / 2L+	DC 24 V
1M / 2M	Massa

I due morsetti 1L+/L2+ nonché 1M/2M della morsettiera sono rispettivamente ponticellati internamente in modo da poter collegare un'alimentazione singola o un'alimentazione ridondante.

Sezioni del cavo collegabili:

- Senza capocorda: 0,2 .. 2,5 mm^2 / AWG 24 .. 13
- Con capocorda: 0,25 .. 1,5 mm^2 / AWG 24 .. 16
- Con capocorda TWIN: 0,5 .. 1,0 mm^2 / AWG 20 .. 17

Le indicazioni relative alla potenza assorbita e ad altri dettagli tecnici dei collegamenti si trovano nel capitolo Dati tecnici (Pagina 111).

Progettazione e funzionamento

4

4.1 Raccomandazioni Security

Osservare le seguenti raccomandazioni Security per impedire accessi non autorizzati al sistema.

Nota

Funzioni Security dei tipi di CP

Le seguenti avvertenze non valgono per ciascun tipo di CP descritto in questo manuale, a seconda della funzione supportata.

Generale

- Assicurarsi regolarmente che il dispositivo soddisfi queste raccomandazioni ed eventuali altre direttive Security interne.
- Valutare l'intero impianto in merito alla sicurezza. Utilizzare un concetto di protezione a cella con prodotti corrispondenti.
- Non collegare direttamente il dispositivo ad Internet. Utilizzare il dispositivo entro un'area di rete protetta.
- Tenere aggiornato il firmware. Tenersi regolarmente informati sugli aggiornamenti di sicurezza del firmware e adottarli.
- Tenersi regolarmente informati sulle novità sulle pagine Internet Siemens.
  - Qui si trovano informazioni relative alla sicurezza della rete:

    Link: (http://www.siemens.com/industrialsecurity)
  - Qui si trovano informazioni relative a Industrial Ethernet Security:

    Link: (http://w3.siemens.com/mcms/industrial-communication/it/ie/industrial-ethernet-security/Seiten/industrial-security.aspx)
  - Un'introduzione all'argomento Industrial Security si trova nella seguente documentazione:

    Link: (http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP02-0BA4_BR_Network_Security_en_112015.pdf)

Accesso fisico

Limitare l'accesso fisico al dispositivo a personale qualificato.

Collegamento alla rete

Non collegare il PC direttamente a Internet. Se è richiesto un collegamento del CP a Internet, attivare relativi dispositivi di protezione prima del CP, ad es uno SCALANCE S con firewall o utilizzare il CP 1543SP-1.

Funzioni Security del prodotto

Utilizzare le possibilità delle impostazioni Security nella progettazione del prodotto. Tra queste vi sono inoltre:

- Livelli di protezione

  Progettare un livello di protezione della CPU.

  Le avvertenze a riguardo si trovano nel sistema di informazione di STEP 7.

- Disattivazione delle porte BusAdapter

  Disattivare nella progettazione una porta non necessaria del BusAdapter utilizzato.

- Funzione Security della comunicazione
  - Attivare le funzioni Security del CP e configurare il firewall.

    In caso di collegamento a reti pubbliche è necessario utilizzare firewall. Definire i servizi con i quali si vuole consentire un accesso alla stazione tramite le reti pubbliche. Impiegando la "limitazione di larghezza di banda" del firewall si utilizza la possibilità di limitare attacchi flooding e DoS.
  - Utilizzare le varianti di protocollo sicure NTP (secure) e CP 1543SP-1.
  - Utilizzare le funzioni Security dei protocolli Telecontrol, o le opzioni DNP3 Security.
  - Utilizzare la Open User Communication sicura (Secure OUC) tramite i relativi blocchi di programma.
  - Lasciar disattivato l’accesso al Webserver della CPU (progettazione CPU) e al Webserver del CP.

- Protezione delle password per l'accesso ai blocchi di programma

  Proteggere da visione le password che vengono create per i blocchi di programma nei blocchi di dati. Avvertenze relative al procedimento si trovano nel sistema di informazione STEP 7 alla voce “Protezione del know-how".

- Funzione di logging

  Attivare la funzione tramite la progettazione Security e controllare regolarmente se vi sono accessi non autorizzati agli eventi inseriti nel protocollo.

Password

- Definire le regole per l'utilizzo dei dispositivi e l'assegnazione di password.
- Aggiornare regolarmente le password per aumentare la sicurezza.
- Utilizzare solo password con elevato livello di sicurezza. Evitare password con basso livello di sicurezza quali ad es. "password1", "123456789" o simili.

- Assicurarsi che tutte le password siano protette e non accessibili a personale non autorizzato.

  Vedere a riguardo anche la sezione precedente.
- Non utilizzare una password per diversi utenti e sistemi.

Protocolli

Protocolli sicuri e non sicuri

- Attivare solo i protocollo necessari per l'impiego del sistema.
- Utilizzare protocolli sicuri se l'accesso al dispositivo non è protetto da misure di protezione fisiche.

  Il protocollo NTP con NTP (secure) offre un'alternativa sicura.

Tabella: Significato del titolo della colonna e delle voci

La seguente tabella fornisce una panoramica sulle porte aperte in questo dispositivo.

- **Protocollo / Funzione**

  Protocolli supportati dal dispositivo.
- **Numero di porta (protocollo)**

  Numero di porta assegnato al protocollo.
- **Preimpostazione della porta**
  - Aperto

    All'inizio della progettazione la porta è aperta.
  - Chiuso

    All'inizio della progettazione la porta è chiusa.
- **Stato della porta**
  - Aperto

    La porta è sempre aperta e non può essere chiusa.
  - Aperta dopo la configurazione

    La porta è aperta se è stata configurata.
  - Aperta (login, se configurato)

    Come standard la porta è aperta. Dopo la configurazione della porta è necessario un login del partner di comunicazione.
  - Chiusa dopo la configurazione

    La porta è chiusa in quanto il CP è sempre il client per questo servizio.
- **Authentification**

  Indica se il protocollo autentica il partner di comunicazione durante l'accesso.

Protocollo / Funzione	Numero di porta (protocollo)	Preimpostazione della porta	Stato della porta	Autenticazione
DHCP	68 (UDP)	Chiusa	Aperta dopo la configurazione (mentre il CP rileva un nuovo indirizzo)	No
Collegamenti S7 e online	102 (TCP)	Aperta	Aperta dopo la configurazione	No
Diagnostica online (CP 1543SP-1)	8448 (TCP)	Chiusa	Aperta dopo la configurazione	No
Porta listener **DNP3**	20000 (TCP/UDP) impostabile	Chiusa	Aperta dopo la configurazione	Sì, se Security è attivata.
Porta listener IEC	2404 (TCP) impostabile	Chiusa	Aperta dopo la configurazione	No
SMTP	25 (TCP) impostabile	Chiusa	Chiusa dopo la configurazione	No
SSL/TLS	587 (TCP) impostabile	Chiusa	Chiusa dopo la configurazione	No
NTP	123 (TCP)	Chiusa	Chiusa dopo la configurazione	No
HTTP	80 (TCP)	Chiusa	Aperta dopo la configurazione	Sì
HTTPS	443 (TCP)	Chiusa	Aperta dopo la configurazione	Sì
SNMP	161 (UDP)	Aperto	Aperta dopo la configurazione	Sì (in SNMPv3)

4.2 Progettazione in STEP 7

Progettazione in STEP 7

La progettazione delle unità e delle reti si esegue in SIMATIC STEP 7. La versione necessaria si trova nel capitolo Requisiti software (Pagina 20). Per una ET 200SP è possibile progettare al massimo due CP 154xSP-1.

Per informazioni complete sulla progettazione consultare il sistema di informazione STEP 7 e i capitoli seguenti.

Panoramica della progettazione del CP

Per la progettazione procedere nel modo seguente:

1. Creare un progetto STEP 7.
2. Inserire le stazioni SIMATIC necessarie.
3. Inserire nelle stazioni i CP e le unità di ingresso e uscita necessarie.
4. Creare una rete Ethernet.
5. Collegare le stazioni con la sottorete Ethernet.

6. Progettare i CP inseriti.
7. Opzionalmente: Creare i blocchi di programma per la Open User Communication.
8. Salvataggio e compilazione del progetto.

Nei seguenti capitoli si trovano informazioni sui singoli gruppi di parametri. Informazioni relative ai parametri non descritti in questo manuale si trovano nel sistema di informazione di STEP 7.

I dettagli sui parametri della comunicazione Telecontrol del CP 1542SP-1 IRC si trovano nel capitolo Comunicazione Telecontrol (CP 1542SP-1 IRC) (Pagina 46).

I dettagli sui parametri delle funzioni Security si trovano nel capitolo Progettazione Security (CP 1543SP-1) (Pagina 88).

Caricamento e salvataggio dei dati di progettazione

Con il caricamento della stazione i dati del progetto della stazione vengono salvati sulla CPU insieme ai dati di progettazione del CP. Per informazioni sul caricamento della stazione consultare il sistema di informazione di STEP 7.

4.3 Interfaccia Ethernet

4.3.1 IPv6

Progettazione degli indirizzi Ethernet

Ulteriori informazioni relative alla progettazione si trovano nel sistema di informazione di STEP 7.

Nota

Comunicazione tramite IPv6

Se si vogliono utilizzare indirizzi IPv6 e collegare il CP a Internet, assicurarsi che anche il router collegato ad Internet e il provider sei servizi Internet utilizzati (ad es. e-mali) supportino gli indirizzi IPv6.

4.3.2 Sincronizzazione dell'ora

Procedimento della sincronizzazione dell'ora

Il gruppo di parametri per la sincronizzazione dell’ora si trova nell’interfaccia Ethernet.

Con le funzioni Security attive il gruppo di parametri viene visualizzato in "Security".

Nota

Raccomandazione per l'assegnazione dell'ora

La sincronizzazione con un orologio esterno viene raccomandata ad intervalli di ca. 10 secondi. In questo modo si ottiene uno scostamento possibilmente minimo dell'ora interna dall'ora assoluta.

Nota

Nessun inoltro dell'ora con NTP / NTP (secure)

CPU e CP possono entrambi sincronizzare l'ora tramite NTP. Se si attiva la sincronizzazione dell'ora in entrambi i moduli, si raccomanda di utilizzare lo stesso server NTP per concordare un'ora coerente all'interno della stazione.

In linea di principio il CP supporta il seguente procedimento di sincronizzazione dell'ora.

- **NTP**

  Si progettano gli indirizzo del o dei server NTP, l'intervallo di sincronizzazione e l'opzione "Accetta ora da server NTP non sincronizzati".

CP 1542SP-1 IRC

Con la comunicazione Telecontrol attivata (gruppo di parametri "Tipi di comunicazione") l'ora viene acquisita generalmente dal partner:

- **Ora del partner**

  Il CP imposta la sua ora utilizzando l'ora che rileva con i telegrammi del partner di comunicazione.

Il CP 1542SP-1 IRC offre alla CPU la possibilità di acquisire l'ora dal CP tramite una variabile PLC. Vedere a riguardo il capitolo Comunicazione con la CPU (Pagina 57).

Nota

Nessuna sincronizzazione dell'ora della CPU durante l'acquisizione dell'ora dal CP

Se la CPU acquisisce l'ora dal CP tramite una variabile PLC, disattivare la sincronizzazione dell'ora della CPU.

CP 1543SP-1

Nota

Garanzia dell'ora valida

Se si utilizzano le funzioni Security, un'ora valida è di estrema importanza. Si raccomanda di utilizzare il procedimento NTP (secure).

Il CP supporta i seguenti procedimento di sincronizzazione dell'ora:

- **NTP**
- **NTP (secure)**

  Il procedimento protetto NTP (secure) utilizza l'autenticazione tramite chiave simmetrica secondo l'algoritmo Hash MD5 o SHA-1.

  Nelle impostazioni globali è possibile creare e gestire server NTP supplementari, anche del tipo NTP (secure).

4.4 SNMP

Gruppo di parametri "SNMP"

- **Attiva SNMP**

  Abilita la funzione degli agenti SNMP nel CP.

Nota

Se nel CP 1543SP-1 sono attivate le funzioni Security, il gruppo di parametri "SNMP" si trova in "Security".

Fornitura dei CP

I CP supportano le seguenti versioni SNMP:

- **CP 1542SP-1, CP 1542SP-1 IRC**
  - SNMPv1
- **CP 1543SP-1**
  - SNMPv1
  - SNMPv3 (con le funzioni Security attivate)

I trap non sono supportati dal CP.

I dettagli sulle funzioni supportate sono riportati nel capitolo Diagnostica tramite SNMP (Pagina 102).

4.5 Comunicazione Telecontrol (CP 1542SP-1 IRC)

4.5.1 Progettazione

Punti di accesso ai dati per la comunicazione Telecontrol

Per il trasferimento di dati utili tra la stazione e il partner della comunicazione non è necessaria la programmazione di blocchi di programma per il CP 1542SP-1 IRC.

Le aree dati nella memoria della CPU previste per la comunicazione con il partner vengono progettate nel CP in riferimento al punto di accesso ai dati. Ogni punto di accesso ai dati è collegato con una variabile PLC o un elemento in un blocco dati nella CPU.

I singoli punti di accesso ai dati possono essere trasmessi individualmente al sistema di controllo e qui elaborati.

Per la trasmissione dei dati di processo e per alcune opzioni dei gruppi di parametri "Stazioni partner" e "Comunicazione con la CPU" sono necessari punti di accesso ai dati progettate.

Ulteriori informazioni si trovano nel capitolo Progettazione del punto di accesso ai dati (Pagina 58).

4.5.2 Tipi di comunicazione

In questo gruppo di parametri si attiva il tipo di comunicazione che si vuole utilizzare per il rispettivo CP.

Per ridurre al minimo il rischio di accessi non autorizzati alla stazione tramite Ethernet, è necessario attivare singolarmente i servizi di comunicazione che il CP deve eseguire.

La Open User Communication non esiste nel gruppo di parametri in quanto questi servizi di comunicazione non sono progettati, ma vengono programmati tramite blocchi di programma.

Il gruppo di parametri non è presente nel CP 1542SP-1 in quanto i servizi di comunicazione supportati da questo CP sono sempre attivati.

Gruppo di parametri "Tipi di comunicazione"

- **Attiva comunicazione Telecontrol**

  Solo nel CP 1542SP-1 IRC

  Abilita la comunicazione Telecontrol nel CP. I seguenti protocollo possono essere impiegati alternativamente:

  – **TeleControl Basic**

    Attiva la comunicazione con il server Telecontrol

  – **DNP3**

    Attiva la comunicazione con fino a quattro master DNP3

  – **IEC 60870-5-104**

    Attiva la comunicazione con fino a quattro master IEC

Nota

Intera funzionalità Telecontrol solo con funzioni Security attivate

Per le seguenti funzioni è necessario attivare le funzioni Security:

- Invio di messaggi (e-mail) tramite la funzionalità Telecontrol
- Utilizzo del protocollo "TeleControl Basic" (generale)
- Utilizzo delle funzioni DNP3 Security
- Utilizzo di certificati

Nota

Perdita dei dati di progettazioni in caso di cambio del protocollo Telecontrol

Se in un CP progettato si cambia il protocollo, i dati di progettazione specifici per il protocollo vengono persi, ad es. la progettazione del punto di accesso ai dati e del partner nonché i messaggi (e-mail).

- **Attiva le funzioni online**

  Abilita nel CP l'accesso alla CPU per le funzioni online (diagnostica, caricamento dei dati del progetto ecc.). Con la funzione attiva dalla stazione di engineering è possibile accedere alla CPU tramite il CP.

  Se l'opzione è disattivata, con le funzioni online non si ha accesso alla CPU tramite il CP. La diagnostica online della CPU con collegamento diretto all'interfaccia della CPU resta tuttavia possibile.

- **Attiva comunicazione S7**

  Abilita nel CP la comunicazione S7 con un SIMATIC S7 o il routing S7.

  Se si progettano collegamenti S7 con la stazione interessata, è necessario attivare questa opzione tramite il CP.

4.5.3 Informazioni di indirizzamento e di autenticazione

Informazioni di indirizzamento e di autenticazione per la comunicazione Telecontrol

A seconda del protocollo Telecontrol utilizzato i partner di comunicazione del CP necessitano le informazioni di indirizzamento e di autenticazione del CP progettate per il CP:

- **TeleControl Basic**

  Il server Telecontrol necessita di:

  – numero del progetto

  – numero di stazione

  – password (per l'autenticazione)

  Il parametro si trova nel gruppo di parametri "Identificazione CP" in "Security".

  – Indirizzo IP (nel gruppo di parametri "Interfaccia Ethernet”)

    Poiché il CP generalmente realizza il collegamento con il server Telecontrol, l’indirizzo IP del CP non deve essere progettato in TCSB.

- **DNP3**

  Il master necessita di:

  – numero di stazione (nel gruppo di parametri "Identificazione CP“)

  – Indirizzo IP (nel gruppo di parametri "Interfaccia Ethernet”)

  – Numero di porta del CP

- **IEC**

  Il master necessita di:

  – numero di stazione (nel gruppo di parametri "Identificazione CP“)

  – Indirizzo IP (nel gruppo di parametri "Interfaccia Ethernet”)

  – Numero di porta del CP

Informazioni di indirizzamento necessarie al CP

Informazioni relative alle informazioni di indirizzamento del partner di comunicazione necessarie al CP si trovano nel capitolo Stazioni partner (Pagina 52).

4.5.4 Interfaccia Ethernet (X1) > Opzioni avanzate

Progettare i parametri generali disponibili come per ogni altra interfaccia Ethernet:

- Dati generali (nome ecc.)
- Indirizzi ed event. router
- Impostazioni della porta
- Accesso al Webserver

Di seguito si trova solo la descrizione dei parametri specifici per la comunicazione Telecontrol.

Controllo del collegamento TCP

L'impostazione qui eseguita vale per globalmente per tutti i collegamenti TCP del CP. Osservare la possibilità di sovrascrivere il valore progettato per i singoli partner di comunicazione, vedere a seguito.

- **Tempo di controllo del collegamento TCP**

  se non vengono scambiati dati entro il tempo di sorveglianza del collegamento il CP invia un telegramma keep alive al partner della comunicazione.

  Campo consentito: 1 ... 65535 s. Preimpostazione: 180

  Il tempo di sorveglianza si progetta nell'interfaccia Ethernet come preimpostazione per tutti i collegamenti TCP. Il valore preimpostato si può adeguare a ogni singolo collegamento alla voce "Stazioni partner”, confronto capitolo Stazioni partner (Pagina 52). Solo nei partner la funzione può essere disattivata inserendo 0 (zero).

- **Tempo di controllo keep alive TCP**

  Dopo la trasmissione di un telegramma keep alive il CP attende una risposta dal partner della comunicazione entro il tempo di sorveglianza keep alive. Se il CP non riceve una risposta entro il tempo progettato, interrompe la comunicazione.

  Campo consentito: 1 ... 65535 s. Preimpostazione: 10

  Il tempo di sorveglianza si progetta nell'interfaccia Ethernet come preimpostazione per tutti i collegamenti TCP. Il valore preimpostato si può adeguare a ogni singolo collegamento alla voce "Stazioni partner". Solo nei partner la funzione può essere disattivata inserendo 0 (zero).

Impostazioni di trasmissione - TeleControl Basic

- **Ritardo di realizzazione del collegamento**

  Valore di base per il tempo di attesa fino al successivo tentativo di connessione dopo che un tentativo di collegamento è fallito. Dopo rispettivamente 3 tentativi il valore base viene raddoppiato fino a max. 900 s.

  Campo consentito: 10 ... 300. Preimpostazione: 10

  Es.: da un valore di base 20 risultano i seguenti tempi di attesa: 3 x 20 s, 3 x 40 s, 3 x 80 s ecc. fino a max. 3 x 900 s.

- **Tempo di sorveglianza trasmissione**

  Tempo (secondi) per la ricezione della conferma dal partner di comunicazione (server Telecontrol) dopo l'invio di telegrammi spontanei. Il tempo viene avviato dopo la trasmissione spontanea di un telegramma. Se al termine del tempo di controllo del collegamento non si riceve la conferma del partner il telegramma viene ripetuto tre volte. Dopo tre tentativi falliti il collegamento viene interrotto e riattivato.

  Campo consentito: 1 ... 65535. Preimpostazione: 5

- **Intervallo di scambio codifica**

  Qui si indica l'intervallo in ore dopo il cui termine viene scambiata di nuovo la chiave tra il CP e il partner di comunicazione (TCSB V3). La chiave è una funzione Security del protocollo Telecontrol utilizzato dal CP e dal TCSB V3.

  Campo consentito: 0 ... 65535. Preimpostazione: 8

  Con 0 (zero) la funzione è disattivata.

Impostazioni di trasmissione - DNP3

Ulteriori informazioni sulle funzioni, i campi ammessi e le preimpostazioni si trovano sui singoli passi si trovano nelle descrizioni comandi di STEP 7.

- **Bit di guasto**

  Il bit di guasto può essere utilizzato come bit 1.6 (IIN1.6) degli "Internal Indication Bytes“ per visualizzare se la CPU si trova nello stato STOP.

- **Tempo max. tra Select e Operate**
- **Ripetizioni telegramma**

- **Conferma del collegamento**
- **Tempo di controllo collegamento**
- **Modalità di trasmissione "Spontanea"**:
- **Numero max. di telegrammi spontanei**
- **Tempo di controllo per telegrammi spontanei**
- **Buffer per eventi di classe 1 / 2 / 3**

  Qui si definisce per ciascuna delle tre classi di evento il numero di evento a partire dal quale gli eventi salvati vengono inviati al partner di comunicazione.

  Campo consentito: 1 ... 255

- **Tempo di ritardo eventi della classe 1 / 2 / 3**

  Qui si definisce per ciascuna delle tre classi di evento in secondi il tempo massimo per il quale gli eventi devono essere salvati nel buffer di trasmissione prima di essere inviati al partner di comunicazione.

  Campo consentito: 0 ... 255

  Con 0 (zero) la funzione è disattivata.

I dettagli relativi alla funzione del buffer di trasmissione (salvataggio e invio di eventi) nonché alle possibilità di trasmissione di dati si trovano nel capitolo Immagine di processo, tipi di trasmissione, classi di evento, trigger (Pagina 64).

Impostazioni di trasmissione - IEC

Nota

Impostazioni nel master

Durante la progettazione dei tempi di controllo t_1 e t_2 osservare le impostazioni corrispondenti nel master in modo che non si verifichino messaggi di errore involontari o interruzioni del collegamento.

Ulteriori informazioni sulle funzioni, i campi ammessi e le preimpostazioni si trovano sui singoli passi si trovano nelle descrizioni comandi di STEP 7.

- **Tempo max. tra Select e Operate**
- **Tempo di controllo per creazione collegamento (t_0)**
- **Tempo di controllo telegramma (t_1)**

  Tempo di controllo per la conferma di telegrammi inviati dal CP da parte del partner della comunicazione. Il tempo di controllo vale per tutti i telegrammi in formato I, S e U inviati dal CP.

  Se il partner non invia una conferma entro il tempo di controllo, il CP interrompe il collegamento con il partner.

- **Tempo di controllo per telegrammi S e U (t_2)**

  Tempo di controllo per la conferma di telegrammi di dati del master attraverso il CP.

  Dopo la ricezione di dati dal master il CP conferma i dati ricevuti in alternativa:

  – Se il CP stesso invia dati al master entro t_2, con il telegrammi di dati inviato (formato I) esso invia i telegrammi di dati ricevuti dal master entro t_2.

  – Al più tardo allo scadere di t_2 il CP invia un telegramma di conferma (formato S) al master.

  Il valore di t_2 deve essere inferiore di quello di t_1.

- **Tempo di riposo per telegrammi di test (t_3)**

  Tempo di controllo nel quale il CP non riceve telegrammi dal master.

  Allo scadere di t_3 il CP invia un telegramma di test/di controllo (formato U) al master.

  Questo parametro serve per i tempi prolungati senza scambio di dati.

- **Differenza tra numero sequenza di trasmissione N(S) e numero di sequenza di ricezione N(R) (k)**

  Numero massimo di telegrammi di dati non confermati (I-APDU) come differenza massima tra numero sequenza di trasmissione N(S) e numero sequenza di ricezione N(TR).

  Se k è raggiunto e t_1 non è ancora trascorso, il CP non invia telegrammi fino a quando tutti i telegrammi inviati sono confermati dal master.

  Se k è raggiunto e t_1 è trascorso, viene interrotto il collegamento TCP.

- **Numero max. di telegrammi dati non confermati (w)**

  Numero massimo di telegrammi di dati ricevuti (I-APDU), dopo il quale il telegramma ricevuto meno recente dal master deve essere confermato.

Meccanismo di conferma con il protocollo IEC

Con ciascun telegramma di dati inviato il CP invia un numero progressivo di trasmissione. Il telegramma di dati resta dapprima salvato nel buffer di trasmissione.

Durante la ricezione il master restituisce come conferma al CP il numero sequenziale di trasmissione di questo telegramma o (in caso di ricezione di più telegrammi) dell'ultimo telegramma. Il CP salva i numeri sequenziali di trasmissione restituiti dal master come numero sequenziale di ricezione e li utilizza come conferma.

I telegrammi il cui numero sequenziale di trasmissione è uguale o inferiore del numero sequenziale di ricezione attuale vengono considerati inviati correttamente e vengono cancellati dal buffer di trasmissione del CP.

Raccomandazioni della specifica:

- w non deve essere maggiore di 2/3 del k.
- Valore raccomandato per k: 12
- Valore raccomandato per w: 8

Porta [X1 Px]

Se non si vogliono utilizzare le due porte del BusAdapter è possibile disattivare una delle due porte.

Per informazioni relative ad altri parametri consultare il sistema di informazione di STEP 7.

4.5.5 Stazioni partner

4.5.5.1 Progettazione del partner

Non è possibile e non è necessaria la progettazione STEP 7 dei partner di comunicazione del CP (server Telecontrol, master DNP3 o IEC) nonché dei collegamenti con i partner.

Informazioni di indirizzamento dei partner di comunicazione

Durante la progettazione del CP, per i partner di comunicazione del CP sono necessarie le seguenti informazioni:

- TeleControl Basic
  - Indirizzo IP partner

    Vedere a riguardo il capitolo Indirizzamento di partner di comunicazione semplici e ridondanti (Pagina 55).
  - Porta partner (Numero della porta listener del TCSB)
- DNP3 / IEC
  - Indirizzo stazione master

    Indirizzo della stazione definita nel master

    Nel protocollo IEC non viene analizzato l'Indirizzo della stazione master.
  - Indirizzo IP partner

    Indirizzo IP del master

    Per l'indirizzamento di partner ridondanti vedere il capitolo Indirizzamento di partner di comunicazione semplici e ridondanti (Pagina 55).
  - Porta partner

"Stazioni partner" (solo con DNP3 / IEC)

- **Porta listener**

  Porta listener propria del CP

"Server Telecontrol" / "Partner"

- **Attiva partner**

  Attivare l'opzione per poter utilizzare il partner progettato di seguito per la comunicazione.

  In "TeleControl Basic" il server Telecontrol è sempre attivato come partner.

- **Numero di partner**

  Il numero di partner viene sempre assegnato da STEP 7.

- **Indirizzo stazione / Indirizzo stazione master**

  Con la comunicazione Telecontrol attivata, l'indirizzo della stazione del server Telecontrol viene assegnato automaticamente dal sistema.

"Collegamento al partner"

Ulteriori informazioni sui campi ammessi e le preimpostazioni si trovano sui singoli passi si trovano nelle descrizioni comandi di STEP 7.

- **Indirizzo IP partner**

  Indirizzo IP o nome Host (FQDN) del server Telecontrol. Esso può essere ad es. anche il FQDN di un servizio DynDNS.

- **Sorveglianza del collegamento**

  Se si attiva questa funzione il collegamento con il partner di comunicazione viene sorvegliato con la trasmissione di telegrammi keep alive.

  Il tempo di controllo del collegamento TCP viene impostato per tutti i collegamenti TCP del CP nel gruppo di parametri dell'interfaccia Ethernet, cfr. capitolo Interfaccia Ethernet (X1) > Opzioni avanzate (Pagina 48). Questa impostazione vale per tutti i collegamenti TCP del CP.

  Nel gruppo di parametri "Stazioni partner", può quindi essere impostato separatamente il tempo di controllo impostato in modo globale per questo partner. Il valore qui impostato per questo partner sovrascrive il valore globale che è stato impostato nel gruppo di parametri "Interfaccia Ethernet (X1) > Opzioni avanzate > Sorveglianza del collegamento TCP".

- **Tempo di controllo del collegamento TCP**

  Solo per TCP: se non vengono scambiati dati entro il tempo di sorveglianza del collegamento il CP invia un telegramma keep alive al partner della comunicazione.

  Il tempo di sorveglianza si progetta nell'interfaccia Ethernet come preimpostazione per tutti i collegamenti TCP. Il valore preimpostato può essere adattato individualmente in "Stazioni partner" per ciascun collegamento e per questo partner sovrascrive il valore globale che è stato impostato in "Interfaccia Ethernet".

  Inserendo 0 (zero) è possibile disattivare la funzione per i singoli partner.

- **Tempo di controllo keep alive TCP**

  Solo per TCP: Dopo la trasmissione di un telegramma keep alive il CP attende una risposta dal partner della comunicazione entro il tempo di sorveglianza keep alive. Se il CP non riceve una risposta entro il tempo progettato, interrompe la comunicazione.

  Il tempo di sorveglianza si progetta nell'interfaccia Ethernet come preimpostazione per tutti i collegamenti TCP. Il valore preimpostato si può adeguare a ogni singolo collegamento alla voce "Stazioni partner".

  Inserendo 0 (zero) è possibile disattivare la funzione per i singoli partner.

- **Modalità di collegamento**

  In modalità "Permanente" sussiste un collegamento permanente con il partner di comunicazione.

- **Realizzazione del collegamento**

  Definisce il partner della comunicazione che crea il collegamento (sempre il CP).

- **Porta partner**

  Numero di porta del partner di comunicazione

"Collegamento al partner ridondante“ (solo con DNP3 / IEC)

- **Modo di ridondanza**

  Attivare l'opzione se il partner di comunicazione è un master ridondante.

Per ulteriori parametri vedere sopra.

"Impostazioni estese"

- **Tempo di controllo del partner (solo con DNP3 / IEC)**

  Se il CP non riceve il lifebeat entro il tempo progettato dal partner di comunicazione, il CP lo considera come un guasto del partner. Con 0 la funzione è disattivata.

- **Segnala stato del partner (collegamento al partner)**

  Durante l'attivazione della funzione il CP della CPU segnala segnala lo stato del collegamento al partner di comunicazione.

  – Il bit 0 delle "Variabili PLC per lo stato del partner" (tipo di dati WORD) viene impostato su 1 se il partner è raggiungibile.

  – Il bit 1 viene impostato a 1 se tutti i percorsi al partner remoto sono regolari (sensato in caso di percorsi ridondanti).

  – Bit 2-3 indica lo stato del buffer di trasmissione (memoria del telegramma). Sono possibili i seguenti valori:

    - 0: Buffer di invio OK

    - 1: Il buffer di trasmissione minaccia il superamento (80 % di grado di riempimento superato).

- 3: Il buffer di trasmissione è superato (100 % di grado di riempimento raggiunto).

  I bit 2 e 3 vengono azzerati di nuovo non appena viene superato il 50 % di grado di riempimento.

I bit 4 ... 15 delle variabili PLC non sono occupate e non devono essere analizzati dal programma.

Impostazioni specifiche per DNP3

- **DNP3 level**

  Livello di conformità DNP3 supportata dal partner.

- **Modalità di trasmissione eventi**

  Modalità con cui vengono trasmessi i telegrammi del buffer di trasmissione del CP (eventi):

  – Trasmissione cronologica dei singoli telegrammi

    oppure

  – Trasmissione a blocchi dei telegrammi di un punto di accesso ai dati

4.5.5.2 Indirizzamento di partner di comunicazione semplici e ridondanti

Indirizzamento del server Telecontrol

- **Indirizzamento di server Telecontrol con configurazione semplice**

  Progettare l'indirizzo IP del server Telecontrol o del router DSL nei collegamenti tramite Internet.

  In caso di utilizzo di un servizio DynDNS è possibile indicare il nome Host (FQDN).

- **Indirizzamento del gruppo di ridondanza TCSB attraverso le stazioni tramite un unico indirizzo IP**

  Nella LAN nella centrale alla quale sono collegati i PC server TCSB e il router DSL (ad es. SCALANCE M), ad entrambi i PC server viene assegnato un indirizzo IP virtuale comune attraverso la rete Load Balancing (NLB) del sistema operativo del computer.

  Questo indirizzo IP viene progettato in funzione della configurazione della rete:

  – Se è collegato un CP senza router DSL, nel CP deve essere progettato come indirizzo IP del server Telecontrol l'indirizzo virtuale assegnato mediante NLB.

  – In caso di utilizzo di un router DSL, per l'indirizzamento del server Telecontrol ridondante nelle stazioni viene progettato un unico indirizzo IP, l'indirizzo pubblico del router DSL.

    Nel router DSL impostare l'inoltro della porta (TCP) in modo che l'indirizzo IP pubblico (rete esterna) conduca all'indirizzi IP virtuale dei PC server TCSB (rete interna). Solo l'indirizzo IP pubblico è raggiungibile da Internet. La stazione non riceve quindi l'informazione relativa a quale dei due computer è collegato il gruppo di ridondanza.

Indirizzamento del master DNP3 ridondante o IEC

Indicare per ciascun master l'indirizzo di stazione master e l'indirizzo IP utilizzato.

4.5.5.3 Partner per la comunicazione trasversale

Solo in caso di utilizzo del protocollo "TeleControl Basic".

Comunicazione trasversale

In questa tabella si definiscono le stazioni S7 e i CP con i quali la stazione attuale può utilizzare la comunicazione trasversale. Per la comunicazione trasversale i collegamenti avvengono tramite il server Telecontrol.

Partner

Il numero del partner viene assegnato dal sistema. Esso è necessario nell'ambito della progettazione del punto di accesso ai dati per l'assegnazione dei punti di accesso ai dati nei partner di comunicazione.

L'indirizzamento del partner per la comunicazione trasversale viene eseguita tramite i parametri "Progetto", "Stazione" e "Posto connettore".

Progetto

Inserire qui il numero di progetto del CP nella stazione partner. (Gruppo di parametri "Security > Identificazione CP" nel partner)

Stazione

Inserire qui il numero di stazione del CP nella stazione partner. (Gruppo di parametri "Security > Identificazione CP" nel partner)

posto connettore

Inserire qui il numero di posto connettore del CP nella stazione partner tramite il quale viene realizzato il collegamento.

Memoria telegramma

In caso di attivazione e di disturbi del collegamento i telegrammi vengono salvati nel buffer di invio (memoria dei telegrammi) del CP. Osservare che la capacità della memoria dei telegrammi è ripartita su tutti i partner di comunicazione.

Con l'opzione disattivata i telegrammi degli eventi vengono salvati nella memoria di immagine del CP, ovvero in caso di disturbi del collegamento i valori precedenti vengono sovrascritti da nuovi valori.

ID di accesso

L'ID di accesso qui visualizzata viene generata dai valori esadecimali del numero del progetto, del numero di stazione e del posto connettore. Il parametro del tipo DWORD è assegnato nel modo seguente:

- Bit 0 - 7: posto connettore
- Bit 8 - 20: numero di stazione
- Bit 21 - 31: numero del progetto

4.5.6 Comunicazione con la CPU

Comunicazione con la CPU

Tramite i primi tre parametri definire l'accesso alla CPU tramite il CP nel ciclo di campionamento della CPU. La struttura del ciclo di campionamento della CPU è descritta nel capitolo Ciclo di lettura (Pagina 72).

Il quarto parametro "Dimensione di memorizzazione del telegramma" determina la grandezza del buffer di trasmissione nel CP per telegrammi di punti di accesso ai dati progettati come evento.

- **Tempo di pausa del ciclo**

  Tempo di attesa tra due cicli di campionamento dell'area di memoria della CPU

- **Numero massimo degli ordini di scrittura**

  Numero max. di ordini di scrittura nell'area di memoria della CPU nel corso di un ciclo di campionamento della CPU

- **Numero massimo degli ordini di lettura**

  Numero max. di ordini di lettura con bassa priorità dall'area di memoria della CPU nel corso di un ciclo di campionamento della CPU

- **Dimensione di memorizzazione del telegramma**

  Impostare qui la dimensione della memoria dei telegrammi (buffer di trasmissione) per l'evento.

  La capacità della memoria dei telegrammi si ripartisce in parti uguali su tutti i partner di comunicazione. La dimensione della memoria dei telegrammi si trova nel capitolo Limiti di configurazione e dati utili (Pagina 17).

  I dettagli relativi alla funzione del buffer di invio (salvataggio e invio di eventi) nonché alle possibilità di trasmissione di dati si trovano nel capitolo Immagine di processo, tipi di trasmissione, classi di evento, trigger (Pagina 64).

Bit watchdog

- **Sorveglianza CP**

  Tramite il bit Watchdog può essere comunicato alla CPU lo stato della comunicazione ad azione remota del CP.

Ora CP

- **Ora CP sulla CPU**

  Tramite questa funzione il CP può mettere a disposizione della CPU la sua ora.

  I dettagli si trovano nel sistema di informazione STEP 7.

4.5.7 Progettazione del punto di accesso ai dati

4.5.7.1 Progettazione dei punti di accesso ai dati

Creazione di punti di accesso ai dati e di messaggi

La progettazione dei punti di accesso ai dati e dei messaggi si esegue nell'editor per la configurazione dei punti di accesso ai dati e dei messaggi di STEP 7. Essa si trova nella navigazione del progetto:

Progetto > Catella della rispettiva stazione > Unità locali > CP

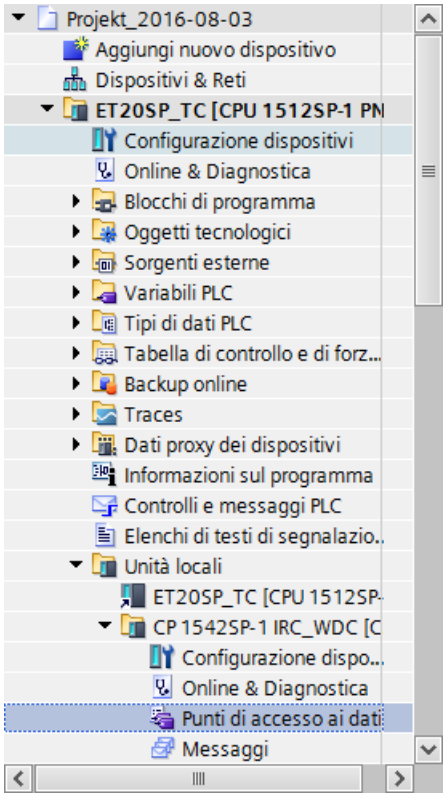


Figura 4-1 Apertura dell'editor dei punti di accesso ai dati e dei messaggi

Aprire l'editor dei punti di accesso ai dati e dei messaggi facendo doppio clic sulla voce "Punti di accesso ai dati" o "Messaggi".

Presupposto per i punti di accesso ai dati: Variabili PLC e/o blocchi dati (DB)

Per la progettazione dei punti di accesso ai dati è necessario aver già creato le variabili PLC o i DB corrispondenti nel programma della CPU.

Le variabili PLC per la progettazione dei punti di accesso ai dati possono essere create nella tabella delle variabili standard o in una tabella delle variabili definita dall'utente.

Attenersi al numero max. consentito delle variabili PLC utilizzabili per la progettazione dei punti di accesso ai dati nel capitolo Limiti di configurazione e dati utili (Pagina 17).

Accesso alle aree della memoria della CPU

I valori delle variabili PLC o dei DB referenziati nei punti di accesso ai dati vengono letti e trasmessi dal CP al partner della comunicazione. I dati ricevuti dal partner della comunicazione vengono scritti dal CP alla CPU tramite le variabili PLC o i DB.

Le aree di indirizzi, i formati e i tipi di dati S7 delle variabili PLC, compatibili con i tipi di punti di accesso ai dati del CP specifici per il protocollo, si trovano nel capitolo Tipi di punti di accesso ai dati (Pagina 60).

Proprietà dei punti di accesso ai dati

Tutte le variabili PLC che devono essere utilizzate per la progettazione dei punti di accesso ai dati devono avere l'attributo "Visibile in HMI".

Nota

Lunghezza dei nomi dei punti di accesso ai dati

Se si vuole utilizzare il numero massimo di punti di accesso ai dati progettabili, assegnare nomi di punti di accesso ai dati, nomi di CP e nomi di stazioni possibilmente brevi.

Set di caratteri per nomi dei punti di accesso ai dati

Durante la creazione di un punto di accesso ai dati viene acquisito un nome preassegnato "DataPoint_n". Nella tabella dei punti di accesso ai dati e nella scheda "Generale" del punto di accesso ai dati è possibile modificare il nome del punto di accesso ai dati.

Per l’assegnazione del nome possono essere utilizzati solo caratteri ASCII della banda 0x20 ... 0x7e con l’eccezione riportata di seguito.

I seguenti caratteri sono vietati poiché essi non sono conformi alle regole di sintassi di TCSB per gli item OPC:

Caratteri non ammessi: . ' [ ] / \ |
punto, apostrofo, parentesi quadre, barra, trattino, barra verticale (pipe)

4.5.7.2 Tipi di punti di accesso ai dati

Tipi di punti di accesso ai dati supportati del CP 1542SP-1 IRC

Quando si progettano i dati utili da trasferire dal CP 1542SP-1 IRC, ogni punto di accesso ai dati viene assegnato a un tipo di punto di accesso specifico del protocollo. I tipi di punti di accesso ai dati con i rispettivi tipi di dati S7 compatibili sono elencati qui di seguito. Sono raggruppati per formato (spazio di memoria necessario).

TeleControl Basic: Tipi di punti di accesso ai dati

Tabella 4- 1 Tipi di punti di accesso ai dati e tipi di dati S7 compatibili supportati

Formato (spazio di memoria necessario)	Tipo di punto di accesso ai dati	Tipi di dati S7	Area operandi
Bit	Ingresso digitale	Bool	I, Q, M, DB
	Uscita digitale	Bool	Q, M, DB
Byte	Ingresso digitale	Byte, USInt	I, Q, M, DB
	Uscita digitale	Byte, USInt	Q, M, DB
Numero intero con segno (16 bit)	Ingresso analogico	Int	I, Q, M, DB
	Uscita analogica	Int	Q, M, DB
Contatore (16 bit)	Ingresso contatore	Word, UInt	I, Q, M, DB
Numero intero con segno (32 bit)	Ingresso analogico	DInt	Q, M, DB
	Uscita analogica	DInt	Q, M, DB
Contatore (32 bit)	Ingresso contatore	UDInt, DWord	I, Q, M, DB
Numero in virgola mobile con segno (32 bit)	Ingresso analogico	Real	Q, M, DB
	Uscita analogica	Real	Q, M, DB
Numero in virgola mobile con segno (64 bit)	Ingresso analogico	LReal	Q, M, DB
	Uscita analogica	LReal	Q, M, DB
Blocco dati (1 .. 64 byte)	Dati	ARRAY [1]	DB
	Dati	ARRAY [1]	DB

[1] Per i formati possibili del tipo di dati ARRAY vedere la seguente sezione.

Blocco dati (ARRAY)

Con il tipo di dati ARRAY possono essere trasmesse aree di memoria attigue con una dimensione fino a 64 byte. I componenti compatibili di ARRAY sono i seguenti tipi di dati S7:

- Byte, USInt (complessivamente fino a 64 per ciascun blocco di dati)
- Int, UInt, Word (complessivamente fino a 32 per ciascun blocco di dati)
- DInt, UDInt, DWord (complessivamente fino a 16 per ciascun blocco di dati)

Data e ora in formato UTC

La data e l'ora vengono trasmesse in formato UTC (48 bit) e contengono la differenza di ora a parte da 01.01.1970 in millisecondi.

DNP3: Tipi di punti di accesso ai dati

Tabella 4- 2 Tipi di punti di accesso ai dati, gruppi di oggetti DNP3, varianti e tipi di dati S7 compatibili supportati

Formato (spazio di memoria necessario)	Tipo di punto di accesso ai dati	Gruppo di oggetti DNP3 [variations]	Direzione	Tipi di dati S7	Area operandi
Bit	Binary Input	**1** [1, 2]	in	Bool	I, Q, M, DB
	Binary Input Event	**2** [1, 2]	in	Bool	I, Q, M, DB
	Binary Output 1)	**10** [2]	out		
	Binary Output Event 1)	**11** [1, 2]	out		
	Binary Command	**12** [1]	out	Bool	Q, M, DB
Integer (16 bit)	Counter Static	**20** [2]	in	UInt, Word	I, Q, M, DB
	Frozen Counter 2)	**21** [2, 6]	in		
	Counter Event	**22** [2, 6]	in	UInt, Word	I, Q, M, DB
	Frozen Counter Event 3)	**23** [2, 6]	in		
	Analog Input	**30** [2]	in	Int	I, Q, M, DB
	Analog Input Event	**32** [2]	in	Int	I, Q, M, DB
	Analog Output Status 4)	**40** [2]	out		
	Analog Output	**41** [2]	out	Int	Q, M, DB
	Analog Output Event 4)	**42** [2, 4]	out		
Integer (32 bit)	Counter Static	**20** [1]	in	UDInt, DWord	I, Q, M, DB
	Frozen Counter 2)	**21** [1, 5]	in		
	Counter Event	**22** [1, 5]	in	UDInt, DWord	I, Q, M, DB
	Frozen Counter Event 3)	**23** [1, 5]	in		
	Analog Input	**30** [1]	in	DInt	Q, M, DB
	Analog Input Event	**32** [1]	in	DInt	Q, M, DB
	Analog Output Status 4)	**40** [1, 3]	out		
	Analog Output	**41** [1]	out	DInt	Q, M, DB
	Analog Output Event 4)	**42** [1]	out		
Numero in virgola mobile (32 bit)	Analog Input	**30** [5]	in	Real	Q, M, DB
	Analog Input Event	**32** [5, 7]	in	Real	Q, M, DB
	Analog Output Status 4)	**40** [3]	out		
	Analog Output	**41** [3]	out	Real	Q, M, DB
	Analog Output Event 4)	**42** [5, 7]	out		
Numero in virgola mobile (64 bit)	Analog Input	**30** [6]	in	LReal	Q, M, DB
	Analog Input Event	**32** [6, 8]	in	LReal	Q, M, DB
	Analog Output	**41** [4]	out	LReal	Q, M, DB
	Analog Output Event 4)	**42** [6, 8]	out		

Formato (spazio di memoria necessario)	Tipo di punto di accesso ai dati	Gruppo di oggetti DNP3 [variations]	Direzione	Tipi di dati S7	Area operandi
Blocco dati (1 ... 64 byte) [5]	Octet String / Octet String Output	**110** [-]	in, out	[5]	DB
	Octet String Event [5]	**111** [-]	in, out	[5]	DB

[1] Questo gruppo di oggetti è progettabile nell'editor del punti di accesso ai dati di STEP 7 tramite il gruppo di oggetti sostitutivo 12.

[2] Questo gruppo di oggetti è progettabile nell'editor del punti di accesso ai dati di STEP 7 tramite il gruppo di oggetti sostitutivo 20.

[3] Questo gruppo di oggetti è progettabile nell'editor del punti di accesso ai dati di STEP 7 tramite il gruppo di oggetti sostitutivo 22.

[4] Questo gruppo di oggetti è progettabile nell'editor del punti di accesso ai dati di STEP 7 tramite il gruppo di oggetti sostitutivo 41.

[5] Con questi tipi di punti di accesso ai dati possono essere trasmesse aree di memoria attigue con una dimensione fino a 64 byte. Sono compatibili tutti i tipi di dati S7 con una dimensione compresa tra 1 e 64 byte.

Per i piè di pagina della tabella [1], [2], [3], [4]: Progettazione dei punti di accesso ai dati tramite i gruppi di oggetti sostitutivi

I tipi di punti di accesso ai dati di uscita dei gruppi di oggetti sono progettabili tramite i gruppi di oggetti sostitutivi indicati:

- 10 [2]
- 11 [1, 2]
- 21 [1, 2, 5, 6]
- 23 [1, 2, 5, 6]
- 40 [1, 2, 3]
- 42 [1, 2, 4, 5, 6, 7, 8]

Per la progettazione nel CP DNP3 utilizzare il rispettivo gruppo di oggetti sostitutivo indicato.

Assegnare il rispettivo punto di accesso ai dati nel master tramite l'indice del punto di accesso ai dati progettabile in STEP 7. Il punto di accesso ai dati del CP DNP3 viene assegnato al relativo punto di accesso ai dati nel master.

Esempio per la progettazione del punto di accesso ai dati Binary Output (10 [2])
Il punto di accesso ai dati viene progettato nel modo seguente:
Nel CP DNP3 come Binary Command (12 [1])
Nel master come Binary Output (10 [2])

Nei tipi di punti di accesso ai dati Binary Output Event (11) e Analog Output Event (42) è necessario attivare il ripristino, vedere la seguente sezione.

Progettazione del ripristino negli Output Events (gruppi di oggetti 11 e 42)

Come descritto in precedenza, i tipi di punti di accesso ai dati Binary Output Event (gruppo di oggetti 11) e Analog Output Event (gruppo di oggetti 42) si creano dapprima come punti di accesso ai dati dei gruppi di oggetti 12 o 41.

È possibile controllare se i valori locali di entrambi questi gruppi di oggetti presentano modifiche e le modifiche vengono trasmesse al master. La modifica di un valore locale può ad es. essere causata da un comando manuale locale.

Per poter trasmettere al master il valore causato da eventi o interventi locali, il rispettivo punto di accesso ai dati necessita di un canale di ripristino. La funzione remirror viene attivata tramite l'opzione "Sorveglianza valore" nella progettazione del punto di accesso ai dati, scheda "Generale".

Osservare che per la funzione remirror i valori locali nel controllo devono essere ordinati in base alla variabile PLC corrispondente del punto di accesso ai dati.

Data e ora nel CP DNP3 in formato UTC

La data e l'ora vengono trasmesse in formato UTC (48 bit) e contengono millisecondi a parte da 01.01.1970.

IEC: Tipi di punti di accesso ai dati

Tabella 4- 3 Tipi di punti di accesso ai dati, tipi di IEC e tipi di dati S7 compatibili supportati

Formato (spazio di memoria necessario)	Tipo di punto di accesso ai dati	Tipo di IEC	Direzione	Tipi di dati S7	Area operandi
Bit	Single point information	<1>	in	Bool	I, Q, M, DB
	Single point information with time tag [1)]	<30>	in	Bool	I, Q, M, DB
	Single command	<45>	out	Bool	Q, M, DB
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag [1)]	<32>	in	Byte, USInt	I, Q, M, DB
Integer (16 bit)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag [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 [1)]	<35>	in	Int	I, Q, M, DB
	Set point command, normalised value	<48>	out	Int	Q, M, DB
	Set point command, scaled value	<49>	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>	out	UDInt, DWord	Q, M, DB
Numero in virgola mobile (32 bit)	Measured value, short floating point number	<13>	in	Real	Q, M, DB

Formato (spazio di memoria necessario)	Tipo di punto di accesso ai dati	Tipo di IEC	Direzione	Tipi di dati S7	Area operandi
	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>	out	Real	Q, M, DB
Blocco dati (1...2 Bit) [2]	Double-point information	<3>	in	[2]	DB
	Double-point information with time tag CP56Time2a [1]	<31>	in	[2]	DB
	Double command	<46>	out	[2]	DB
	Regulating step command	<47>	out	[2]	DB
Blocco dati (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>	out	[3]	DB

[1] Per il formato di data e ora vedere la seguente sezione.

[2] Creare per questi tipi di punti di accesso ai dati un blocco dati con un array di esattamente 2 bool.

[3] Con questi tipi di punti di accesso ai dati possono essere trasmesse aree di memoria attigue con una dimensione fino a 32 bit. È compatibile solo il tipo di dati S7 Bool.

Data e ora nel CP IEC

Nel CP IEC data e ora vengono trasmesse in formato "CP56Time2a" conformemente alla specifica IEC. Osservare che nei telegrammi vengono trasmessi solo i primi 3 byte per millisecondi e minuti.

4.5.7.3 Immagine di processo, tipi di trasmissione, classi di evento, trigger

Salvataggio dei valori del punto di accesso ai dati

Generalmente i valori vengono salvati dai punti di accesso ai dati nella memoria di immagine del CP e trasmessi solo dopo l'interrogazione da parte del partner di comunicazione.

Gli eventi vengono inoltre salvati nel buffer di invio e possono essere trasmessi spontaneamente.

Tramite il parametro "Tipo di trasmissione" (vedere in basso) vengono progettati i punti di accesso ai dati come valore statico o come evento:

- **Valore statico (nessun evento)**

  I valori statici vengono inseriti nella memoria di immagine (immagine di processo del CP).

  I valori statici corrispondono alle seguenti classi:

  – DNP3: Class 0

  – IEC: Classe 2

- **Evento**

  Anche i valori dei punti di accesso ai dati progettati come evento vengono inseriti nella memori ad immagine del CP. Il valore dell'evento viene inviato spontaneamente al partner di comunicazione se esso è abilitato dal master.

  Inoltre i valori degli eventi vengono inseriti nel buffer di invio del CP.

  Gli eventi corrispondono alle seguenti classi:

  – DNP3: Class 1 / 2 / 3

  – IEC: Classe 1

La memoria immagini, l'immagine di processo del CP

Nella memoria di immagine vengono salvati tutti i valori attuali dei punti di accesso ai dati progettati. I nuovi valori di un punto di accesso ai dati sovrascrivono il valore salvato per ultimo nella memoria di immagine.

I valori vengono inviati dopo l'interrogazione del partner di comunicazione. Vedere "Trasmissione dopo il richiamo" nella sezione "Tipi di trasmissione" in basso.

Il buffer di invio

Il buffer di trasmissione del CP è la memoria per i singoli valori dei punti di accesso ai dati progettati come evento. Il numero massimo si ripartisce in parti uguali tra tutti i partner di comunicazione progettati e attivati. La dimensione del buffer di trasmissione si progetta tramite il parametro "Dimensione di memorizzazione del telegramma", vedere capitolo Comunicazione con la CPU (Pagina 57).

Se il collegamento con un partner di comunicazione è interrotto, i singoli valori degli eventi vengono mantenuti dalla bufferizzazione. Al ritorno del collegamento vengono inviati i valori bufferizzati. La memoria dei telegrammi funziona in modo cronologico, ovvero vengono inviati dapprima i telegrammi meno recenti (principio FIFO).

Se un telegramma è stato trasmesso al partner di comunicazione, il valore trasmesso dal buffer di trasmissione viene cancellato.

Se non è possibile inviare telegrammi per un intervallo prolungato e il buffer di trasmissione rischia un overflow, a seconda del protocollo utilizzato vale il seguente comportamento:

- TeleControl Basic

  Il metodo di salvataggio forzato dell'immagine di processo

  Raggiunto un grado di riempimento dell'80% del buffer di trasmissione, il CP commuta al metodo di salvataggio forzato dell'immagine di processo. I nuovi valori dei punti di accesso ai dati progettati come evento non vengono più aggiunti al buffer di trasmissione ma sovrascrivono i valori esistenti meno recenti nella memoria immagini.

  Quando viene ripristinato il collegamento con il partner della comunicazione, il CP commuta nuovamente al metodo di salvataggio del buffer di trasmissione se il grado di riempimento del buffer scende al di sotto del 50%.

- DNP3 / IEC

  Raggiunto il grado di riempimento del 100% del buffer di trasmissione i valori meno recenti vengono sovrascritti.

  In caso di utilizzo del protocollo DNP3 possono essere definite ulteriori condizioni per l'invio degli eventi:

  – Un numero massimo di eventi nel buffer di invio, progettabile per ciascuna classe di evento.

  – Una durata di salvataggio massima progettabile di eventi nel buffer di invio.

Tipo di trasmissione

Sono possibili i seguenti tipi di trasmissione:

- **Trasmissione dopo il richiamo (class 0)**

  Il valore rispettivamente attuale del punti di accesso ai dati viene inserito nella memoria di immagine del CP. I nuovi valori di un punto di accesso ai dati sovrascrivono il valore salvato per ultimo nella memoria di immagine.

  Dopo il richiamo da parte del partner di comunicazione viene trasmesso il valore attuale in questo momento.

- **Attivato (eventi)**

  I valori dei punti di accesso ai dati progettati come evento vengono inseriti nella memoria immagini e inoltre nel buffer di trasmissione del CP.

  I valori di eventi vengono salvati nei seguenti casi:

  – Le condizioni di trigger rispettivamente progettate sono soddisfatte (progettazione del punto di accesso ai dati > scheda "Trigger", vedere in basso)

  – Il valore di un bit di stato dell'identificazione di stato del punto di accesso ai dati viene modificato, cfr. capitolo Identificazioni di stato dei punti di accesso ai dati (Pagina 69).

Classi di evento nel tipo di trasmissione “Attivato"

In funzione del protocollo utilizzato sono disponibili le seguenti classi di evento:

- **TeleControl Basic**
  - **Ogni valore attivato**

    Ciascuna modifica del valore viene inserita in sequenza cronologica nel buffer di invio.
  - **Valore attuale attivato**

    Nel buffer di trasmissione solo il rispettivo ultimo valore attuale. Esso sovrascrive il valore precedentemente salvato nel buffer di trasmissione.
- **DNP3**

  L'analisi della seguente classificazione deve essere eseguita dal master.
  - **Classe di evento 1**

    Classe in base al protocollo DNP3: Class 1

    Ciascuna modifica del valore viene inserita in sequenza cronologica nel buffer di invio.
  - **Classe di evento 2**

    Classe in base al protocollo DNP3: Class 2

    Ciascuna modifica del valore viene inserita in sequenza cronologica nel buffer di invio.
  - **Classe di evento 3**

    Classe in base al protocollo DNP3: Class 3

    Nel buffer di invio viene inserito solo il rispettivo valore attuale nel momento in cui viene soddisfatta la condizione trigger, sovrascrivendo il valore precedentemente salvato.
- **IEC**

  Entrambe le seguenti classe di evento corrispondono alla classe di dati utente 1 del protocollo IEC
  - **Ogni valore attivato**

    Ciascuna modifica del valore viene inserita in sequenza cronologica nel buffer di invio.
  - **Valore attuale attivato**

    Nel buffer di invio viene inserito solo il rispettivo valore attuale nel momento in cui viene soddisfatta la condizione trigger, sovrascrivendo il valore precedentemente salvato.

Trigger

Tipi di attivazione

Per la trasmissione controllata dell'evento sono disponibili diversi tipi di attivazione:

- **Trigger valore di soglia**

  Il valore del punto di accesso ai dati viene trasmesso se esso raggiunge una determinata soglia. La soglia viene calcolata come differenza dall'ultimo valore salvato, vedere capitolo Trigger valore di soglia (Pagina 74).

- **Trigger temporizzato**

  Il valore del punto di accesso ai dati viene trasmesso ad una scadenza progettabile o ad una determinata ora.

- **Trigger evento**

  Il valore del punto di accesso ai dati viene trasmesso se viene attivato un segnale di attivazione progettabile. Come segnale di attivazione viene analizzato il cambio di fronte (0 → 1) di un bit di attivazione, impostato dal programma utente. In caso di necessità, per ciascun punto di accesso ai dati può essere progettato un bit di attivazione separato.

  Reset delle variabili di attivazione nell'area di merker / DB:

  Se l'area di memoria delle variabili di attivazione si trova nell'area merker o in un blocco dati, la variabile di attivazione viene azzerata con la trasmissione del punto di accesso ai dati.

Ora di trasmissione del telegramma

Se il valore di un punto di accesso ai dati dopo l'attivazione del trigger viene trasmesso direttamente o con ritardo al partner di comunicazione dipende dal protocollo utilizzato e dalle impostazioni.

- **TeleControl Basic**

  L'ora di trasmissione si definisce con il parametro "Modalità di trasmissione" nella scheda "Trigger" del punto di accesso ai dati:

  – **Spontaneamente**

    Il valore viene trasmesso direttamente.

  – **Spontanea condizionata**

    Il valore viene trasmesso solo se una delle seguenti condizioni è soddisfatta:

    - Il server Telecontrol interroga la stazione.

    - Il valore di un altro evento con Modalità di trasmissione viene trasmesso "Spontaneamente".

    - Il grado di riempimento del buffer di trasmissione ha raggiunto l'80 % della sua capacità massima.

- **DNP3 / IEC**

  Con questo protocollo la trasmissione spontanea dipende dalla possibilità di invio spontaneo o dalla comunicazione asimmetrica nella rete.

4.5.7.4 Identificazioni di stato dei punti di accesso ai dati

Identificazione di stato dei punti di accesso ai dati

Le identificazioni di stato dei punti di accesso ai dati elencate di seguito vengono trasmesse per ciascun punto di accesso ai dati con ciascun telegramma. Esse si differenziano minimamente nei tre tipi di protocollo.

Per il significato dei bit di stato vedere di seguito. Il “significato” (seconda riga della tabella) si riferisce al rispettivo “Stato di bit” (terza riga della tabella).

Creazione dell'evento in caso di modifica dello stato del punto di accesso ai dati

Nei punti di accesso ai dati progettati come evento, la modifica del bit di stato dell'identificazione di stato descritta in seguito comporta anch'essa la generazione di un evento.

Esempio: Se il valore dello stato "RESTART" di un punto di accesso ai dati progettato come evento si modifica durante l'avvio della stazione da 1 (valore non ancora aggiornato) a 0 (valore aggiornato), avviene la generazione di un evento.

Identificazioni di stato - TeleControl Basic

I bit di stato vengono convertiti da TCSB nell’OPC quality code nel modo seguente.

- Quality = BAD, se:

  NON_EXISTENT o OVER_RANGE = 1
- Quality = UNCERTAIN, se:

  RESTART o CARRY o SB = 1
- Quality = GOOD, se:

  Bit 1, 2, 3, 5 e 6 = 0

Tabella 4- 4 Assegnazione dei bit del byte di stato 0

Bit	7	6	5	4	3	2	1	0
Nome flag	-	NON_ EXISTENT	SB	LOCAL_ FORCED	CARRY	OVER_ RANGE	RESTART	ONLINE
Significato	-	Punto di accesso ai dati inesistente o indirizzo S7 non raggiungibile	Valore sostitutivo	*(il bit non viene impostato.)*	Superamento del valore numerico prima della lettura del valore	Valore limite della preelaborazione del valore analogico superato / non raggiunto	Valore non ancora aggiornato dopo l'avvio	Il valore è valido, CPU in RUN.
Stato bit	*(sempre 0)*	1	1	*(irrilevante)*	1	1	1	1

Identificazioni di stato - DNP3

Le identificazioni di stato possono essere valutate dal master. Esse corrispondono ai seguenti elementi della specifica:

OBJECT FLAGS - DNP3 Specification, Volume 6, Data Object Library - Part 1

Tabella 4- 5 Assegnazione dei bit del byte di stato

Bit	7	6	5	4	3	2	1	0
Nome flag	-	-	-	LOCAL_ FORCED	DISCONTI NUITY	OVER_ RANGE	RESTART	ONLINE
Significato	-	-	-	Comando locale	Superamento del valore numerico prima della lettura del valore	Valore limite della pre-elaborazione del valore analogico superato / non raggiunto	Valore non ancora ag-giornato dopo l'avvio	Il valore è valido
Stato bit	*(sempre 0)*	*(sempre 0)*	*(sempre 0)*	1	1	1	1	1

Identificazioni di stato - IEC

Le identificazioni di stato possono essere valutate dal master. Esse corrispondono ai seguenti elementi della specifica:

Quality descriptor - IEC 60870 Part 5-101

Tabella 4- 6 Assegnazione dei bit del byte di stato

Bit	7	6	5	4	3	2	1	0
Nome flag	-	-	SB substituted	-	CY carry	OV overflow	NT not topical	IV invalid
Significato	-	-	Valore sosti-tutivo	-	Superamento del valore numerico prima della lettura del valore	Campo di valori supera-to, valore analogico	Valore non aggiornato	Il valore è valido
Stato bit	*(sempre 0)*	*(sempre 0)*	1	*(sempre 0)*	1	1	1	0

4.5.7.5 Regole per la progettazione dell'indice punto di accesso ai dati

Progettazione dell'indice punto di accesso ai dati

Di seguito si trovano le regole di progettazione per l’indice del punto di accesso ai dati in funzione del protocollo utilizzato.

TeleControl Basic

All'interno di un CP gli indici delle classi dei punti di accesso ai dati devono rispettare le regole seguenti:

- Ingresso

  L'indice di un punto di accesso ai dati del tipo ingresso deve essere univoco per tutti i tipi di punti di accesso ai dati (ingressi digitali, ingressi analogici ecc.).

- Uscita
  - Un punto di accesso ai dati del tipo uscita può avere lo stesso indice di un punto di accesso ai dati del tipo ingresso.
  - Diversi punti di accesso ai dati del tipo uscita possono avere lo stesso indice.

Nota

Punti di accesso ai dati per la comunicazione trasversale con un CP in un'altra stazione S7

Osservare che nella comunicazione trasversale gli indici di entrambi i punti di accesso ai dati corrispondenti (coppie di punti di accesso ai dati) devono essere identici nei CP che inviano e che ricevono.

DNP3

In un CP gli indici dei punti di accesso ai dati devono essere univoci all'interno di ognuno dei seguenti gruppi di oggetti:

- Binary Input / Binary Input Event
- Binary Output / Binary Command
- Counter / Counter Event
- Analog Input / Analog Input Event
- Analog Output
- Octet String / Octet String Event

Gli indici di due punti di accesso ai dati possono essere identici in diversi gruppi di oggetti.

IEC

In un CP gli indici dei punti di accesso ai dati devono essere univoci.

Gli indici dei punti di accesso ai dati assegnati doppi vengono segnalati come errori al momento della verifica della coerenza e impediscono di salvare il progetto.

4.5.7.6 Ciclo di lettura

Priorità dei punti di accesso ai dati

La lettura ciclica dei valori dei punti di accesso ai dati di ingresso dalle variabili PLC assegnate nella CPU può essere priorizzato.

I punti di accesso ai dati di ingresso di minore rilevanza non devono essere letti in ciascun ciclo di campionamento della CPU. I punti di accesso ai dati di ingresso rilevanti invece possono essere priorizzati per un aggiornamento in ciascun ciclo di campionamento della CPU.

Eseguire la definizione di priorità in STEP 7, nella progettazione del punto di accesso ai dati, scheda "Generale" con il parametro "Ciclo di lettura". Qui si definiscono le due seguenti opzioni per i punti di accesso ai dati di ingresso:

- Ciclo più rapido
- Ciclo normale

I punti di accesso ai dati vengono letti in base al comportamento descritto di seguito.

Struttura del ciclo di campionamento della CPU

Il ciclo (compresa la pausa) con cui il CP scansiona l'area di memoria della CPU è costituito dalle fasi seguenti.

- **Job di lettura ad alta priorità**

  I valori dei punti di accesso ai dati di ingresso con la priorità di campionamento "Priorità maggiore" vengono letti ad ogni ciclo di campionamento.

- **Job di lettura di priorità minore**

  I valori dei punti di accesso ai dati di ingresso con la priorità di campionamento "Priorità minore" vengono letti in percentuale ad ogni ciclo di campionamento.

  Il numero dei valori che vengono letti in ogni ciclo viene definito per il CP nel gruppo di parametri "Comunicazione con la CPU" con il parametro "Numero massimo di ordini di lettura". I valori che superano questo valore e quindi non vengono letti in un ciclo vengono letti nel ciclo successivo o in uno dei cicli seguenti.

- **Job di scrittura**

  In ogni ciclo vengono scritti nella CPU i valori di un determinato numero di ordini di scrittura spontanei. Il numero dei valori che vengono scritti in ogni ciclo viene definito per il CP nel gruppo di parametri "Comunicazione con la CPU" con il parametro "Numero massimo di ordini di scrittura". I valori il cui numero supera questo valore vengono scritti nel ciclo successivo o in uno dei cicli successivi.

- **Tempo di pausa del ciclo**

  Esso è il tempo di atteso tra due cicli di campionamento. Esso è necessario per riservare tempo sufficiente ad altri processi che accedono alla CPU tramite il bus back-plane della stazione.

Durata del ciclo di campionamento della CPU

Non essendo possibile progettare un tempo di ciclo fisso e poiché alle singole fasi non è assegnato un numero fisso di oggetti, la durata del ciclo di campionamento è variabile e può cambiare dinamicamente.

4.5.7.7 Scheda "Trigger"

Trigger

I punti di accesso ai dati vengono progettati tramite il parametro "Tipo di trasmissione" come valore statico o come evento:

Salvataggio del valore di un punto di accesso ai dati progettato come evento

Il salvataggio del valore di un punto di accesso ai dati progettato come evento nel buffer di trasmissione (memoria telegrammi) può essere attivato tramite diversi tipi di trigger:

- **Trigger valore di soglia**

  Il valore del punto di accesso ai dati viene salvato se esso raggiunge una determinata soglia. La soglia viene calcolata come differenza dall'ultimo valore salvato, vedere capitolo Trigger valore di soglia (Pagina 74).

- **Trigger temporizzato**

  Il valore del punto di accesso ai dati viene salvato ad una scadenza progettabile o ad una determinata ora.

- **Trigger evento (Variabile trigger)**

  Il valore del punto di accesso ai dati viene salvato se viene attivato un segnale di attivazione progettabile. Come segnale di trigger viene analizzato il cambio di fronte (0 → 1) di una variabile di attivazione impostato dal programma utente. In caso di necessità, per ciascun punto di accesso ai dati può essere progettato una variabile di attivazione separata.

  Reset delle variabili di attivazione nell'area di merker / DB:

  Se l'area di memoria di una variabile di trigger si trova nell'area merker o in un blocco dati, il CP stesso resetta la variabile trigger su 0 (zero) non appena il valore del punto di accesso ai dati è trasmesso. Questa operazione può durare fino a 500 millisecondi.

Nota

Impostazione rapida di trigger

I trigger non possono essere impostati più velocemente di un intervallo minimo di 500 secondi. Lo stesso vale per il trigger hardware (campo di inserimento).

Nota

Trigger hardware

Il trigger hardware deve essere resettato tramite il programma utente.

Trasmissione del valore di un punto di accesso ai dati progettato come evento

Definire con il parametro "Modalità di trasmissione" se il valore di un punto di accesso ai dati dopo l'attivazione del trigger viene trasmesso direttamente o con ritardo al partner di comunicazione.

Modalità di trasmissione

La Modalità di trasmissione di un telegramma viene impostata nella scheda "Trigger" del punto di accesso ai dati. Con l'opzione si definisce se i telegrammi di eventi vengono inviati direttamente o con ritardo:

- Trasmissione diretta - Spontanea

  Il valore viene trasmesso direttamente.

- Trasmissione bufferizzata - Spontanea condizionata

  Il valore viene trasmesso solo se una delle seguenti condizioni è soddisfatta:

  – Il partner di comunicazione interroga la stazione.

  – Il valore di un altro evento con Modalità di trasmissione viene trasmesso "Spontaneamente".

4.5.7.8 Trigger valore di soglia

Nota

Trigger valore di soglia: Calcolo solo dopo la Pre-elaborazione del valore analogico

Fare attenzione che la Pre-elaborazione del valore analogico viene eseguita prima del controllo di un valore di soglia progettato e prima del calcolo del valore di soglia.

Questo incide sul valore che viene progettato nel Trigger valore soglia.

Nota

Nessun Trigger valore soglia con Formazione valore medio progettata

Con la Formazione valore medio per l'evento del valore analogico interessato non può essere progettato nessun Trigger valore soglia.

Per lo svolgimento temporale della pre-elaborazione del valore analogico vedere il capitolo Pre-elaborazione del valore analogico (Pagina 76).

Trigger valore di soglia

Funzione

Il valore di processo viene salvato quando la divergenza è pari all'importo del valore di soglia

Il calcolo della divergenza del valore di soglia può essere eseguito in due modi:

- **Procedimento assoluto**

  Con i valori binari e numerici nonché con i analogici con formazione del valore medio progettata, il calcolo della divergenza del valore di soglia prevede il procedimento assoluto.

- **Procedimento integrativo**

  Con i valori analogici senza formazione del valore medio progettata, il calcolo della divergenza del valore di soglia prevede il procedimento integrativo.

  Nel calcolo integrato del valore di soglia non viene analizzata la somma assoluta dello scostamento del valore del processo dall'ultimo valore salvato, ma lo scostamento integrato.

Procedimento assoluto

Ogni valore binario viene testato per verificare se il valore attuale (eventualmente livellato) si trova al di fuori della banda del valore di soglia. La banda del valore di soglia di volta in volta attuale è costituita dall'ultimo valore salvato e dall'importo del valore di soglia progettato.

- Limite superiore della banda del valore di soglia: Ultimo valore salvato + valore di soglia
- Limite inferiore della banda del valore di soglia: Ultimo valore salvato - valore di soglia

Non appena il valore di processo raggiunge il limite superiore o inferiore della banda del valore di soglia, questo valore viene salvato. Il nuovo valore salvato costituisce la base per il calcolo della nuova banda del valore di soglia.

Procedimento integrativo

Il calcolo integrato del valore di soglia funziona con un confronto ciclico del valore attuale integrato con l'ultimo valore salvato. Il ciclo di calcolo nel quale vengono confrontali entrambi i valori è di 500 millisecondi.
(Osservazione: Il ciclo di calcolo non va scambiato con il ciclo di campionamento delle aree della memoria della CPU).

Gli scostamenti del valore attuale di processo vengono sommati in ciascun ciclo di calcolo. Il trigger viene impostato e un nuovo valore di processo viene registrato nel buffer di diagnosi solo quando il valore sommato ha raggiunto il valore progettato del trigger valore di soglia.

Il procedimento viene spiegato con il seguente esempio, nel quale è progettato un valore di soglia di 2,0.

Tabella 4- 7 Esempio per il calcolo integrato di un valore di soglia progettato con 2,0

Tempo [s] (Ciclo di calcolo)	Valore di processo salvato nel buffer di invio	Valore di processo attuale	Scostamento assoluto dal valore salvato	Scostamento integrato
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

Tempo [s] (Ciclo di calcolo)	Valore di processo salvato nel buffer di invio	Valore di processo attuale	Scostamento assoluto dal valore salvato	Scostamento integrato
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**

Nello svolgimento dei valore di processo illustrato nell'esempio il trigger valore di soglia progettato con 2,0 viene attivato due volte:

- A 3,5 s: La somma dello scostamento integrato è di 2,0. Il nuovo valore di processo salvato nel buffer di invio è 20,5.
- A 6,0 s: La somma dello scostamento integrato è di 2,1. Il nuovo valore di processo salvato nel buffer di invio è 19,9.

Se in questo esempio uno scostamento del valore di processo di ca. 0,5 deve consentire l'attivazione del trigger, nel comportamento illustrato del valore di processo deve essere progettato un valore di soglia di ca. 1,5 ... 2,5.

4.5.7.9 Pre-elaborazione del valore analogico

I CP con progettazione dei punti di accesso ai dati supportano la pre-elaborazione del valore analogico. Per i punti di accesso ai dati del valore analogico possono essere progettate alcune o con tutte le funzioni qui descritte.

Presupposti e restrizioni

I presupposti per la progettazione delle opzioni di pre-elaborazione e le relative restrizioni sono riportati nella sezione delle rispettive funzioni.

Nota

Restrizioni dovute ai trigger progettati

Se per il punto di accesso ai dati interessato non è stato progettato il trigger del valore di soglia, le operazioni di pre-elaborazione del valore analogico "Tempo di soppressione errore", “Calcolo valore limite" e “Livellamento" non vengono eseguite. In questi casi il valore di processo letto del punto di accesso ai dati viene inserito nella memoria di backup del CP e inoltrato in modo trasparente prima della conclusione del ciclo di pre-elaborazione del calcolo del valore di soglia (500 ms).

Svolgimento delle operazioni di pre-elaborazione del valore analogico

I valori degli ingressi analogici progettati come evento, vengono elaborati nel CP secondo il seguente schema:

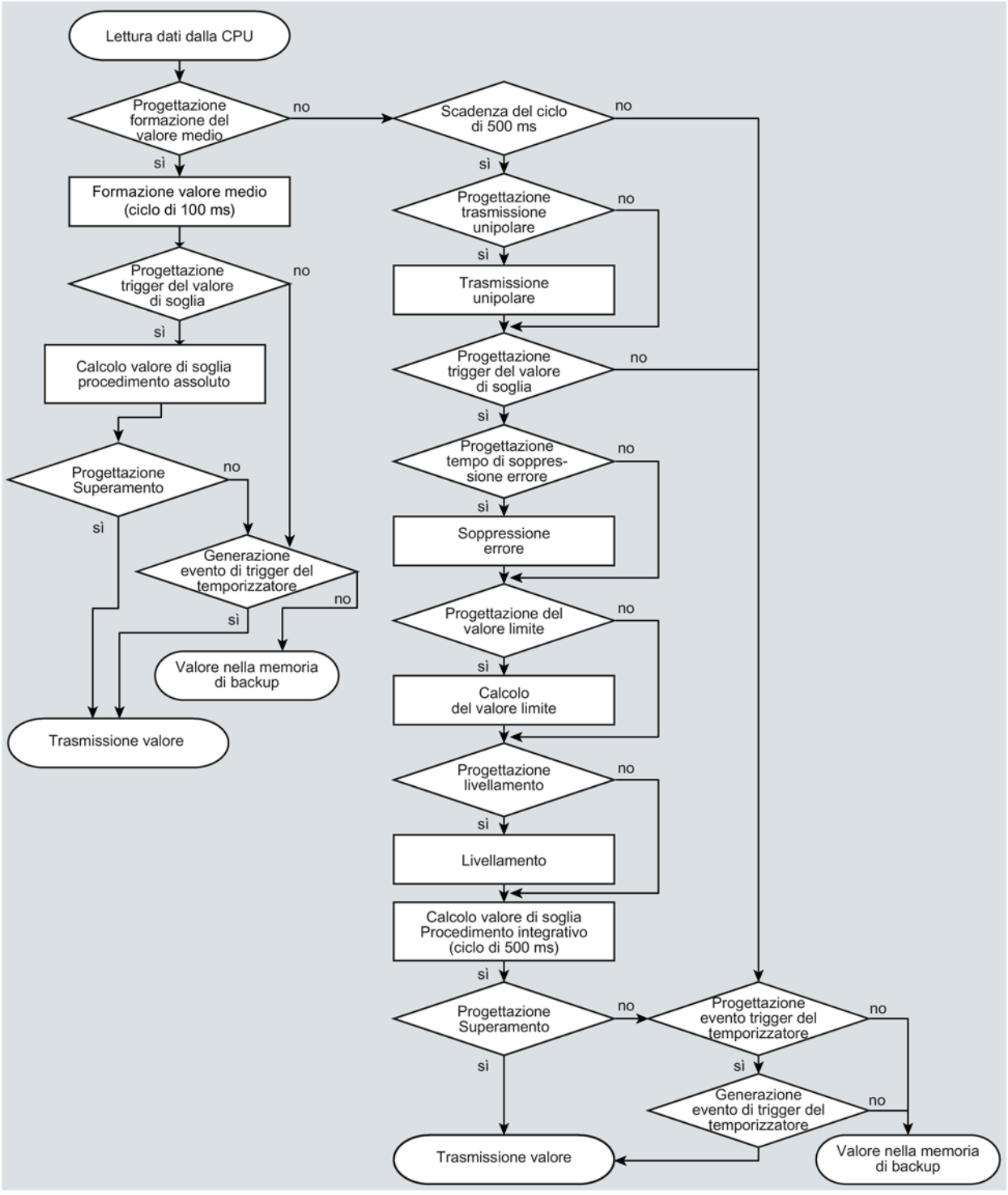


Figura 4-2 Svolgimento delle operazioni di pre-elaborazione del valore analogico

Il ciclo di 500 millisecondi viene applicato come risultato del calcolo integrativo del valore di soglia. In questo ciclo i valori vengono salvati anche se sono attivate le seguenti opzioni di pre-elaborazione:

- Trasmissione unipolare
- Tempo di soppressione errore
- Calcolo valore limite
- Livellamento

Formazione valore medio

Nota

Opzioni di pre-elaborazione limitate nella Formazione valore medio progettata

Se per un evento del valore analogico si progetta la Formazione valore medio, non sono disponibili le seguenti opzioni di pre-elaborazione:

- Trasmissione unipolare
- Durata di soppressione dell'errore
- Livellamento

Funzione

Con questo parametro i valori analogici acquisiti vengono trasferiti come valori medi.

Con la formazione del valore medio attivata, può rivelarsi utile la progettazione di un trigger del temporizzatore.

I valori attualmente presenti di un punto di accesso ai dati di un valore analogico vengono letti e sommati in cicli di 100 millisecondi. Il numero dei valori letti per unità di tempo dipende dal ciclo di lettura della CPU e dal ciclo di campionamento della CPU del CP.

Dai valori sommati viene calcolato il valore medio non appena viene avviata la trasmissione attraverso un trigger del temporizzatore. Successivamente l'addizione viene riavviata per la formazione del prossimo valore medio.

Il valore medio viene calcolato anche quando la trasmissione del telegramma del valore analogico viene attivata da un'interrogazione del partner della comunicazione. La durata del periodo di formazione del valore medio è il tempo che trascorre tra l'ultima trasmissione (ad es. attivata dal trigger) e l'interrogazione. Anche dopo questa trasmissione viene riavviata l'addizione per formare il valore medio successivo.

Unità di ingresso: Campo di overflow/underflow

Non appena viene rilevato un valore nel campo di overflow e underflow, la formazione del valore medio viene immediatamente interrotta. Per il periodo di formazione del valore medio in corso il valore 32767 / $7FFF_h$ o -32768 / 8000_h viene salvato come valore medio non valido e trasmesso con il telegramma successivo.

Successivamente viene avviata una nuova formazione del valore medio. Se il valore analogico si trova ancora nel campo di overflow o underflow, uno dei due valori interessati viene salvato come valore medio non valido e trasmesso con la successiva attivazione del telegramma.

Nota

Tempo di soppressione errore > 0 progettato

Se è stato progettato un tempo di soppressione errore e successivamente si attiva la formazione del valore medio, il valore del tempo di soppressione viene visualizzato in grigio, ma non viene più utilizzato. Con la formazione del valore medio attiva, il tempo di soppressione dell'errore viene impostato internamente a 0 (zero).

Trasmissione unipolare

Restrizioni

La trasmissione unipolare non può essere progettata contemporaneamente alla formazione del valore medio. L'attivazione del trasferimento unipolare viene annullata con l'attivazione della formazione del valore medio.

Funzione

Con la trasmissione unipolare i valori negativi vengono corretti con zero. Questo potrebbe essere opportuno se non devono essere trasmessi come valori di misura reali i valori del campo di sottocomando.

Eccezione: Nei dati di processo delle unità di ingresso, viene trasmesso il valore -32768 / 8000_h della rottura cavo di un ingresso life zero.

In un ingresso software invece vengono corretti a zero tutti i valore inferiori a zero.

Tempo di soppressione errore

Presupposti della funzione

Progettazione del trigger del valore soglia per questo punto di accesso ai dati

Restrizioni

Il tempo di soppressione errore non può essere progettato contemporaneamente alla formazione del valore medio. Un valore progettato viene annullato con l'attivazione della formazione del valore medio.

Funzione

Il tipico caso di applicazione di questo parametro è la soppressione di valori di picco della corrente all'avviamento di motori con potenza elevata, che altrimenti verrebbero segnalati come guasto alla stazione di controllo centrale.

Il trasferimento di un valore analogico in overflow ($7FFF_h$) o in underflow (8000_h) viene soppresso per la durata dell'intervallo indicato. Il valore di $7FFF_h$ o 8000_h - se viene trasferito, ancora presente, solo al termine della soppressione degli errori.

Il valore attuale viene trasmesso se rientra nel campo nominale prima dello scadere del tempo di soppressione errori.

Unità di ingresso

La soppressione è adeguata a valori analogici che vengono acquisiti direttamente come valori grezzi dalle unità di ingressi analogici S7. Queste unità forniscono i valori menzionati per il campo di overflow/underflow per tutti i campi di ingresso, anche per i life zero.

Per la durata della soppressione degli errori un valore analogico che si trovi nel campo di overflow (32767 / $7FFF_h$) o di underflow (-32768 / 8000_h) non viene trasmesso. Lo stesso vale per gli ingressi life zero. Il valore nel campo di overflow/underflow - se ancora presente - viene trasferito solo al termine della soppressione degli errori.

Raccomandazione per i valori pre-elaborati dalla CPU:

Se i valori pre-elaborati dalla CPU vengono messi a disposizione in un'area merker o in un blocco dati, una soppressione è possibile o opportuna solo se anch'essi assumono i valori menzionati di 32767 / $7FFF_h$ o -32768 / 8000_h nel campo di overflow o di underflow. In caso contrario non dovrebbe essere progettato il parametro per i valori preelaborati.

Per i valori già preelaborati nella CPU, i limiti per overflow e underflow possono essere definiti liberamente.

Fattore di livellamento

Presupposti della funzione

Progettazione del trigger del valore soglia per questo punto di accesso ai dati

Restrizioni

Il fattore di livellamento non può essere progettato contemporaneamente alla formazione del valore medio. Un valore progettato viene annullato con l'attivazione della formazione del valore medio.

Funzione

I valori analogici che subiscono rapide variazione possono essere stabilizzati con l'aiuto della funzione di livellamento.

I fattori di livellamento nelle unità di ingressi analogici S7 vengono calcolati secondo la formula seguente.

$$y_n = \frac{x_n + (k-1)y_{n-1}}{k}$$

dove
y_n = valore livellato nel ciclo attuale n
x_n = valore acquisito nel ciclo attuale n
k = fattore di livellamento

Come fattore di livellamento per l'unità si possono progettare i seguenti valori.

- 1 = nessun livellamento
- 4 = livellamento debole

- 32 = livellamento medio
- 64 = livellamento forte

Imposta valore limite 'basso' / / Imposta valore limite 'alto'

Requisiti richiesti per la funzione

- Progettazione del trigger del valore soglia per questo punto di accesso ai dati
- Variabile PLC nell'area operandi merker o area dati

  Il punto di accesso ai dati del valore analogico deve essere collegato a una variabile PLC nell'area merker o dati (blocco dati). Per le unità hardware (area operandi ingresso) non è possibile progettare un valore limite.

La progettazione di valori limite non è appropriata per i valori di misura già preelaborati nella CPU.

Funzione

In questi due campi di immissione è possibile impostare rispettivamente un valore limite in direzione 'inizio campo di misura' o in direzione 'fine campo di misura'. I valori limite si possono analizzare ad es. anche come inizio o come fine del campo di misura.

Identificazioni di stato "OVER_RANGE"

Al superamento negativo o positivo di un valore limite viene impostata l'identificazione di stato "OVER_RANGE" del punto di accesso ai dati. Le identificazioni di stato sono descritte al capitolo Identificazioni di stato dei punti di accesso ai dati (Pagina 69).

Con la trasmissione del valore analogico il bit "OVER_RANGE" dell'identificazione di stato del punto di accesso ai dati viene impostato nel modo seguente:

- Valore limite 'alto':
  - Al superamento del valore limite: OVER_RANGE = 1
  - Al superamento del valore limite: OVER_RANGE = 0
- Valore limite 'basso':
  - Al superamento negativo del valore limite: OVER_RANGE = 1
  - Al successivo superamento del valore limite: OVER_RANGE = 0

Progettazione del valore limite

Il valore limite viene progettato come numero decimale intero. Il campo valori si allinea a quello del valore grezzo delle unità di ingressi analogici.

Campo	Valore grezzo (16 bit) delle variabili PLC PLC-Variablen		Uscita dell'unità [mA]			Campo di misura [%]
	Decimale	Esadecimale	0 .. 20 (unipolare)	-20 .. +20 (bipolare)	4 .. 20 (life zero)	
Overflow	32767	7FFF	> 23,515	> 23,515	> 22,810	> 117,593
Campo di sovracomando	32511 ... 27649	7EFF ... 6C01	23,515 ... 20,001	23,515 ... 20,001	22,810 ... 20,001	117,593 ... 100,004
Campo nominale (unipolare / life zero)	27648 ... 0	6C00 ... 0000	20 ... 0		20 ... 4	100 ... 0
Campo nominale (bipolare)	27648 ... 0 ... -27648	6C00 ... 0000 9400		20 ... 0 ... -20		100 ... 0 ... -100
Campo di sottocomando (unipolare / life zero)	-1 ... -4864	FFFF ... ED00	-0,001 ... -3,518		3,999 ... 1,185	-0,004 ... -17,59
Campo di sottocomando (bipolare)	-27649 ... -32512	93FF ... 8100		-20,001 ... -23,516		-100,004 ... -117,593
Underflow / rottura conduttore	-32768	8000	< -3,518		< 1,185	< -17,593

Nota

Analisi del valore anche con opzione disattivata

Se si attivano una o entrambe le opzioni, si progetta un valore e successivamente si disattiva di nuovo l'opzione, il valore visualizzato in grigio viene analizzato ugualmente.

Per disattivare entrambe le opzioni cancellare dai campi di immissione i valori limite precedentemente progettati e disattivare solo allora la rispettiva opzione.

Raccomandazione per valori analogici che subiscono rapide variazioni:

Se il valore analogico subisce forti variazioni e sono progettati i valori limite può essere opportuno livellare prima il valore analogico.

4.5.8 Progettazione dei messaggi

Progettazione di e-mail

Negli eventi rilevati il CP può inviare e-mail ad un partner di comunicazione.

La progettazione delle e-mail si esegue nell'editor per la configurazione dei punti di accesso ai dati e dei messaggi di STEP 7. Essa si trova nella navigazione del progetto:

Progetto > Catella della rispettiva stazione > Unità locali > CP

Per la visualizzazione in STEP 7 vedere capitolo Progettazione dei punti di accesso ai dati (Pagina 58).

Presupposti e informazioni necessari

Osservare i seguenti presupposti nella progettazione del CP per la trasmissione di e-mail:

- Attivazione della comunicazione Telecontrol (gruppo di parametri "Tipi di comunicazione")
- Progettazione del gruppo di parametri "Progettazione e-mail“ (vedere gruppo di parametri "Security")

  A tal fine sono necessarie le seguenti informazioni:

  – Dati di accesso del server SMTP: Indirizzo, numero di porta, nome utente, password
  – Indirizzo e-mail del destinatario.

Trigger: Attivazione della trasmissione di e-mail

Tramite il gruppo di parametri "Trigger" nella tabella nei messaggi progettare tramite quale dei seguenti eventi viene attivato l’invio di e-mail:

- La CPU passa in STOP.
- La CPU passa in RUN.
- Il collegamento al partner è interrotto.
- Il collegamento al partner viene realizzato (viene ripristinato).
- Viene attivato un segnale trigger.

  Come segnale di trigger per l'invio di e-mail viene analizzato il cambio di fronte (0 → 1) di un bit di attivazione, impostato dal programma utente. In caso di necessità, per ciascuna e-mail può essere progettato un bit di attivazione separato.

  Se l'area della memoria del bit di attivazione si trova nell'area merker o in un blocco dati, il bit di attivazione viene azzerato all'invio della e-mail.

Nel protocollo "TeleControl Basic" sono progettabili ulteriori eventi che attivano una e-mail:

- La realizzazione del collegamento al partner è fallita.
- Una sessione TeleService è stata iniziata.
- Una sessione TeleService è stata chiusa.

Invia valore: Trasmissione del valore di una variabile PLC con un messaggio

Se nel gruppo di parametri “Trigger“ si attiva l'opzione "Invia valore", il CP invia un valore nel messaggio per il segnaposto $$ dall'area della memoria della CPU. Inserire quindi nel testo del messaggio "$$" come segnaposto per il valore da inviare insieme.

Selezionare una variabile PLC il cui valore viene integrato nel messaggio. Il valore viene visualizzato nel testo del messaggio al posto del segnaposto $$.

$$ può essere il segnaposto per i tipi di punto di accesso ai dati con tipo di dati singolo con una dimensione fino a 32 bit.

Attiva identificazione per stato di modifica

Se questa opzione in STEP 7 è attivata, nel CP viene emesso uno stato che fornisce informazioni sullo stato di elaborazione del messaggio. Lo stato viene scritto in una variabile PLC del tipo DWORD. Selezionare questa variabile tramite la casella "Variabili PLC per stato di modifica".

In caso di problemi con il recapito di messaggi è possibile definire lo stato, ad es. tramite il Webserver della CPU, visualizzando qui il valore della variabile PLC.

Per il significato dei singoli stati vedere il capitolo Stato di elaborazione delle e-mail Telecontrol (Pagina 106).

4.5.9 Security >Identificazione CP

Identificazione CP

Valido solo per CP con utilizzo del protocollo "TeleControl Basic".

- Numero del progetto

  Il numero di un progetto in STEP 7 è identico per tutti i CP Telecontrol. TCSB analizza i numeri di progetto di 1 ... 2000. Se si modifica il numero di progetto, questo parametro viene modificato per tutti i CP nel progetto STEP 7.

- Numero di stazione

  Per ciascuna stazione nel CP Telecontrol viene progettato un numero di stazione individuale. TCSB analizza i numeri di stazione di 1 ... 8000.

- Password Telecontrol

  Password per l'autenticazione del CP sul server Telecontrol. 8 ... 29 caratteri del set ASCII 0x20...0x7e. La password può essere uguale per tutti i CP del progetto STEP 7.

  La stessa password viene progettata nell'applicazione "TCSB" per questa stazione.

4.5.10 Security > Opzioni Security DNP3

Autenticazione e scambio di chiave nel protocollo DNP3

Con le funzioni Security attivate il master e la stazione (CP) si autenticano con una chiave comune, la pre-shared key.

Grazie alla pre-shared key comune, dopo la prima realizzazione del collegamento tra master e CP viene concordata una chiave di sessione che viene successivamente rinnovata ciclicamente. L'iniziativa per il rinnovo della chiave di sessione parte normalmente dal master. I criteri per il rinnovo della chiave vengono definiti nei seguenti parametri.

- Richieste di autenticazione prima dello scambio di codifica
- Intervallo di scambio codifica

Non appena una di queste due condizioni è soddisfatta, la chiave di sessione viene rinnovata.

Opzioni Security DNP3

- **Attiva opzioni Security DNP3**

  Metodo con cui il CP si autentica presso il master.

  – Disattivato

    Autenticazione non protetta: In caso di selezione di questa opzione il CP si connette solo con il proprio indirizzo della stazione.

  – Attivato

    Autenticazione protetta: In caso di selezione di questa opzione il CP e il master utilizzano i meccanismi DNP3 Security. I parametri vengono progettati di seguito.

- **Modalità IKE**

  Selezione della modalità per lo scambio di codifica (IKE).

  – Main Mode è la modalità standard.

  – Aggressive Mode è leggermente più veloce ma trasmette l'identità non criptata.

- **Statistica Security**

  Indica se la statistica degli eventi Security viene trasmessa al master. Gli eventi Security sono le richieste di autenticazione per il CP. Se si attiva questa opzione tutte le richieste di autenticazione vengono salvate nel CP con data, ora e risultato e trasmesse al master per un'ulteriore valutazione.

- **Blocco SHA-1**

  Specifica se il CP è autorizzato a utilizzare l'algoritmo Secure Hash SHA-1 se è stato progettato “SHA-256" come Secure Hash Algorithm ma il master non supporta SHA-256. Significato delle opzioni:

  – SHA-1 ammesso

    Il CP può utilizzare l'algoritmo SHA-1 se il master non supporta SHA-256.

  – SHA-1 non ammesso

    Il CP non può utilizzare SHA-1.

    Osservare quanto segue: Se il master non supporta SHA-256 il collegamento non viene creato con la selezione di questa opzione.

- **Secure Hash Algorithm**

  Selezione del Secure Hash Algorithm (SHA). Possibili selezioni:

  – SHA-1

  – SHA-256

- **Algoritmo Key Wrap**

  Selezione del Advanced Encryption Standard (AES). Possibili selezioni:

  – AES-128

  – AES-256

- **Lunghezza chiave**

  Lunghezza della pre-shared key in byte.

  In funzione dell’Algoritmo Key-Wrap vengono utilizzate le seguenti lunghezze:

  – Per AES-128: 16 byte

  – Per AES-256: 32 byte

- Numero massimo di richieste di scambio di chiavi

  La funzione è disattivata.

- **Richieste di autenticazione prima dello scambio di chiavi**

  Numero max. di richieste di autenticazione del CP al master prima che il la chiave di sessione venga rinnovata.

  Inserendo 0 (zero) la funzione è disattivata e la chiave di sessione viene rinnovata in funzione dell’intervallo dello scambio di chiave.

  Raccomandazione: Impostare il numero nel CP doppio rispetto al master.

- **Intervallo di scambio di chiavi**

  Intervallo dopo il quale viene scambiata di nuovo la chiave di sessione tra il CP e il master.

  Inserendo 0 (zero) la funzione è disattivata e la chiave non viene mai rinnovata.

  L'intervallo deve essere adeguato tra entrambi i partner della comunicazione.

- **Tempo di controllo autenticazione**

  Tempo di attesa max. (secondi) per la risposta del master a una richiesta di autenticazione del CP.

  Il superamento del tempo di attesa viene valutato dal CP come errore. Il CP genera in questo caso un evento Security e lo invia al master.

  Campo dei valori: 1 ... 65535

- **Pre-shared key**

  La chiave pre-shared key del CP deve essere identica alla pre-shared key utilizzata dal master.

  La chiave deve corrispondere alla "Lunghezza chiave" progettata sopra (2 caratteri per ogni byte).

  La pre-shared key può essere progettata in due modi:

  – Progettazione manuale

    Inserire manualmente la pre-shared key come valore esadecimale.

  – Importazione come file

    Importare la pre-shared key dal sistema di file della stazione di engineering se la pre-shared key è stata generata dal master o da un altro sistema.

4.5.11 Security > Progettazione delle e-mail

Progettazione delle e-mail

- **Nessuna configurazione**

  Nella preimpostazione l'invio di e-mail è disattivato.

- **Attiva SMTP**

  Attivare questa opzione se si vuole utilizzare l'invio di e-mail tramite la porta SMTP 25.

- **Attiva SSL/TLS**

  Se il provider del servizio e-mail supporta solo la trasmissione codificata, attivare questa opzione: Tramite il numero di porta selezionare il protocollo:

  – N. porta 587

    se si utilizza STARTTLS il CP invia e-mail crittografate.

  – N. porta 465

    se si utilizza SSL/TLS (SMTPS) il CP invia e-mail crittografate.

  Chiedere al proprio gestore del servizio e-mail quale opzione viene supportata.

  Se si vuole utilizzare una connessione Internet con infrastruttura IPv6 osservare l'avvertenza nel capitolo IPv6 (Pagina 43).

4.6 Progettazione Security (CP 1543SP-1)

4.6.1 VPN

4.6.1.1 VPN (Virtual Private Network)

VPN Tunnel

Virtual Private Network (VPN) è una tecnologia per il trasporto sicuro di dati riservati su reti IP pubbliche, ad es. Internet Con VPN viene configurato e utilizzato un collegamento sicuro (tunnel) tra due sistemi IT o reti sicuri nonostante una rete non sicura.

Il tunnel VPN si distingue per l'inoltro di tutti i telegrammi, anche di protocolli di livelli superiori (HTTP, FTP, ecc.).

Il traffico di dati di due componenti di rete viene trasportato praticamente senza limiti attraverso un'altra rete. In questo modo è possibile collegare tra loro reti complete oltre una rete adiacente o interconnessa.

Proprietà

- VPN forma una rete parziale logica che si incorpora in una rete (assegnata) adiacente. VPN utilizza gli usuali meccanismi di indirizzamento della rete assegnata, tuttavia trasporta i propri telegrammi con la tecnologia di dati e funziona staccata dal resto di questa rete.
- VPN consente la comunicazione dei partner VPN compresi con la rete assegnata.
- VPN basata su una tecnica tunnel e configurabile individualmente.
- La comunicazione a prova di intercettazioni e manipolazioni tra i partner VPN viene garantita dall'utilizzo di password, chiavi pubbliche o da un certificato digitale (autenticazione).

Settori applicativi/settori d'impiego

- Le reti locali possono essere collegate tra loro in modo sicuro tramite Internet (collegamento "Site-to-Site").
- Accesso protetto ad una rete industriale (collegamento "End-to-Site")
- Accesso protetto ad un server (collegamento "End-to-End")
- Comunicazione tra due server senza che la comunicazione venga vista da terzi (collegamento End-to-End o Host-to-Host)
- Garanzia per la sicurezza di informazione in impianti collegati in rete della tecnica di automazione

- Protezione di sistemi computerizzati compresa la relativa comunicazione dei dati all'interno di una rete di automazione o l'accesso remoto sicuro tramite Internet
- Accessi remoti protetti di PC/dispositivo di programmazione dispositivi di automazione o reti protetti da moduli Security, possibili oltre le reti pubbliche.

Principio di protezione delle celle

Con Industrial Ethernet Security è possibile proteggere singoli apparecchi o segmenti di rete di una rete Ethernet protetta:

- È consentito l'accesso a singoli dispositivi e segmenti di rete protetti da moduli Security.
- Sono consentiti collegamenti protetti tramite strutture di rete non protette.

Grazie alla combinazione di diverse misure di sicurezza quali il firewall, i router NAT/NAPT e la VPN tramite il tunnel IPsec, i moduli Security proteggono da:

- spionaggio dei dati
- manipolazione dei dati
- Accessi indesiderati

4.6.1.2 Creazione di tunnel VPN per la comunicazione S7 tra stazioni

Requisiti richiesti

Per creare un tunnel VPN per la comunicazione S7 tra due stazioni S7 o tra una stazione S7 e una stazione di engineering con CP Security (ad es. CP 1628), è necessario soddisfare i seguenti requisiti:

- Sono progettate le due stazioni.
- I CP in entrambe le stazioni devono supportare le funzioni Security.
- Le interfacce Ethernet di entrambe le stazioni si trovano nella stessa sottorete.

Nota

La comunicazione è possibile anche tramite un router IP

La comunicazione tra le due stazioni è possibile anche tramite un router IP. Per questo percorso di comunicazione è tuttavia necessario eseguire altre impostazioni.

Procedimento

Per creare un tunnel VPN è necessario eseguire i seguenti passi:

1. Creazione di un utente Security

   Se l'utente Security è già creato: Eseguire la connessione come utente.
2. Selezionare la casella di controllo "Attiva funzioni Security"
3. Creazione di gruppi VPN e assegnazione dei moduli Security

4. Progettare le proprietà del gruppo VPN
5. Progettare le proprietà VPN locali di entrambi i CP

La descrizione esatta dei singoli passi si trova nelle seguenti sezioni di questo capitolo.

Creazione di un utente Security

Per creare un tunnel VPN sono necessari relativi diritti di progettazione. Per attivare le funzioni Security è necessario creare almeno un utente Security.

1. Nelle impostazioni Security locali del CP fare clic sul pulsante "Login utente".

   Risultato: Si apre una nuova finestra.
2. Inserire il nome utente, la password e la conferma della password.
3. Fare clic sul pulsante "Registrazione".

   È stato creato un nuovo utente Security. Sono disponibili le funzioni Security.

Connettersi come utente per tutte le altre applicazioni.

Selezionare la casella di controllo "Attiva funzioni Security"

Dopo il login è necessario attivare in entrambi i CP la casella di controllo "Attiva funzioni Security".

Per entrambi i CP sono ora disponibili le funzioni Security.

Creazione di gruppi VPN e assegnazione dei moduli Security

1. Selezionare nelle impostazioni Security globali la voce "Firewall" > "Gruppi VPN" > "Aggiungi nuovo gruppo VPN".
2. Fare doppio clic sulla voce "Aggiungi nuovo gruppo VPN" per aggiungere un nuovo gruppo VPN.

   Risultato: Un nuovo gruppo VPN viene visualizzato sotto la voce selezionata.
3. Nelle impostazioni Security fare doppio clic sulla voce "Gruppi VPN" > "Assegna modulo ad un gruppo VPN"".
4. Assegnare al gruppo VPN i moduli Security tra i quali deve essere realizzato il tunnel VPN.

Nota

Data attuale e ora attuale nel CP per collegamenti VPN

Normalmente per la realizzazione di un collegamento VPN e il relativo riconoscimento dei certificati da scambiare sono presupposte la data e l'ora attuali in entrambe le stazioni.

Progettare le proprietà del gruppo VPN

1. Fare doppio clic sul nuovo gruppo VPN creato.

   Risultato: Le proprietà del gruppo VPN vengono visualizzate in "Autenticazione".

2. Inserire un nome del gruppo VPN. Progettare nelle proprietà le impostazioni del gruppo VPN.

   Queste proprietà definiscono le impostazioni standard del gruppo VPN che possono essere modificate in qualsiasi momento.

Nota

Definizione delle proprietà VPN dei CP

Le proprietà VPN dei CP si definiscono nel gruppo di parametri "Security" > "Firewall" > "VPN" della rispettiva unità.

Risultato

È stato creato un tunnel VPN. Il firewall dei CP viene attivato automaticamente: La casella di controllo "Attiva firewall" viene attivata automaticamente durane la creazione di un gruppo VPN. La casella non può essere disattivata.

Caricare la configurazione in tutti i moduli che appartengono al gruppo VPN.

4.6.1.3 Comunicazione VPN con il SOFTNET Security Client (stazione di engineering)

La comunicazione via tunnel VPN riesce solo con il nodo interno disattivato

A determinate condizioni la realizzazione di una comunicazione via tunnel VPN tra SOFTNET Security Client e il CP non riesce.

Il client SOFTNET Security Client tenta inoltre di realizzare una comunicazione via tunnel VPN con un nodo interno subordinato. La realizzazione della comunicazione con un nodo non esistente impedisce la realizzazione di comunicazione desiderata con il CP.

Per realizzare una comunicazione via tunnel VPN corretta con un CP è necessario disattivare il nodo interno.

Il seguente procedimento di disattivazione del nodo deve essere utilizzato solo se sussiste il problema descritto.

Disattivare il nodo nel client SOFTNET Security - Panoramica tunnel:

1. Rimuovere il segno di spunta nella casella di controllo "enable active learning".

   Il nodo subordinate scompare dapprima dall'elenco del tunnel.

2. Selezionare nell'elenco del tunnel il collegamento desiderato con il CP.

3. Selezionare con nel menu di scelta rapida con il tasto destro del mouse "Enable all Members".

   Il nodo subordinate ricompare temporaneamente nell'elenco del tunnel.

4. Selezionare il nodo subordinato nell'elenco del tunnel.
5. Selezionare con nel menu di scelta rapida con il tasto destro del mouse "Delete Entry".

Risultato: Il nodo subordinato è disattivato in modo univoco. La realizzazione di una comunicazione via tunnel VPN con CP riesce.

4.6.1.4 Realizzazione della comunicazione via tunnel VPN tra CP e SCALANCE M

Creare un tunnel VPN tra il CP e un router SCALANCE M in base al procedimento descritto nelle stazioni.

Se nelle impostazioni Security globali del gruppo VPN creato ("Gruppi VPN > Autenticazione") è stata selezionata la casella di controllo "Perfect Forward Secrecy", viene realizzata una comunicazione via tunnel VPN.

Se la casella di controllo non è selezionata, il CP rifiuta la realizzazione del collegamento.

4.6.1.5 CP come nodo passivo di collegamenti VPN

Impostazione del consenso per la realizzazione del collegamento VPN con nodi passivi

Se il CP è collegato ad un altro nodo VPN tramite un gateway e il CP è un nodo passivo, il consenso per la realizzazione del collegamento VPN deve essere impostato su "Responder".

Questo si verifica con la seguente configurazione caratteristica:

nodo VPN (attivo) ⇔ gateway (indirizzo IP dinamico) ⇔ Internet ⇔ gateway (indirizzo IPf fisso) ⇔ CP (passivo)

Progettare per il CP come nodo passivo il consenso per la realizzazione del collegamento VPN nel modo seguente:

1. Da STEP 7 passare alla visualizzazione del dispositivo e della rete.
2. Selezionare il CP.
3. Aprire nelle impostazioni Security locali il gruppo di parametri "VPN".
4. Per ciascun collegamento VPN con il CP come nodo VPN passivo modificare l'impostazione standard "Initiator/Responder" in impostazione "Responder".

4.6.2 Firewall

4.6.2.1 Controllo precedente di telegrammi attraverso il firewall

Ciascun telegramma in ingresso o in uscita attraversa dapprima il firewall MAC (layer 2). Se il telegramma viene già respinto su questo livello, non viene controllato in aggiunta attraverso il firewall IP (layer 3). In questo modo, grazie a relative regole firewall MAC la comunicazione può essere limitata o bloccata.

4.6.2.2 Diagnostica online e caricamento nella stazione con il firewall attivato

Impostazione del firewall - Procedimento

Con la funzione Security attivata procedere nel modo seguente:

1. Selezionare nelle impostazioni Security globali (vedere la navigazione del progetto) la voce Firewall > Servizi > Definisci servizi per regole IP".
2. Selezionare la scheda "ICMP".
3. Inserire rispettivamente una nuova voce del tipo "Echo Reply" e "Echo Request".
4. Selezionare quindi il CP nella stazione ET 200SP.
5. Attivare la modalità firewall estesa nelle impostazioni locali Security del CP nel gruppo di parametri "Security > Firewall".
6. Aprire il gruppo di parametri "Regole IP".
7. Inserire nella tabella rispettivamente una nuova regola IP per i servizi precedentemente creati in modo globale nel modo seguente:
   - Azione: Consenti; "Dall'esterno -> verso la stazione" con il servizio creato globalmente "Echo Request"
   - Azione: Consenti; "Dalla stazione -> verso l'esterno" con il servizio creato globalmente "Echo Reply"
8. Inserire per la regola IP relativa a Echo Request in "Indirizzo IP di destinazione" l'indirizzo IP del PG/PC. In questo modo si ottiene che i telegrammi PING possano attraversare il firewall solo dal proprio PG/PC.

4.6.2.3 Tipo di scrittura dell'indirizzo IP sorgente (modalità firewall estesa)

Se nelle impostazioni firewall estese del CP nell'indirizzi IP di destinazione si indica un'area di indirizzi, osservare il seguente tipo di scrittura:

- Separare i due indirizzi IP solo con un trattino.

  Corretto: 192.168.10.0-192.168.10.255

- Non inserire nessun altro carattere tra i due indirizzi IP.

  Errato: 192.168.10.0 - 192.168.10.255

Se si inserisce l'area errata, la regola firewall non viene utilizzata.

4.6.2.4 Impostazioni firewall per collegamento S7 via tunnel VPN

Regole IP in modalità firewall estesa

Se si configurano collegamenti progettati (S7, OUC) con tunnel VPN tra il CP e un partner di comunicazione, le impostazioni locale del firewall del CP devono essere adattate:

Per entrambi i collegamenti in modalità firewall estesa ("Security > Firewall > Regole IP") per entrambe le direzioni di comunicazione del tunnel VPN selezionare l'azione "Allow*".

4.6.3 Filtraggio degli eventi di sistema

Problemi di comunicazione con un valore impostato troppo alto per eventi di sistema

In caso di un valore troppo alto impostato per il filtraggio degli eventi di sistema non è eventualmente possibile utilizzare la potenzialità massima della comunicazione. L'elevato numero di messaggi di errore emessi può ritardare o impedire l'elaborazione dei collegamenti di comunicazione.

Impostare il parametro "Livello:" in "Security > Impostazioni Log > Configura eventi di sistema" sul valore "3 (errore)" per garantire la realizzazione sicura dei collegamenti di comunicazione.

4.7 Tabella “Manager dei certificati“(CP 1542SP-1 IRC, CP 1543SP-1)

Con le funzioni Security attivate, nel progetto STEP 7 vengono sempre creati automaticamente i certificati necessari per poter comunicare ad es. tramite collegamenti VPN per tutti i moduli Security interessati.

I certificati generati da STEP 7, quali i certificati SSL o i certificati dei gruppi VPN vengono assegnati automaticamente ai relativi moduli e non devono essere assegnati tramite le impostazioni Security locali.

Il Manager dei certificati locale

I certificati importati tramite il manager dei certificati nelle impostazioni Security globali non vengono assegnate automaticamente ai relativi moduli. I certificati importati devono essere registrati manualmente nell’elenco dei certificati del partner accreditati tramite la voce “Manager dei certificati" nelle impostazioni Security locali. Durante l’assegnazione di un certificato CA, al modulo vengono assegnati anche i certificati derivati.

Gruppo di parametri “Security“ > tabella “Manager dei certificati“

Tramite il Manager dei certificati locale assegnare al CP certificati per determinati servizi (ad es. invio protetto di e-mail).

1. Fare quindi clic nella riga della tabella "Aggiungi nuovo".
2. Fare clic sul pulsante bianco “...“.
3. Nell’elenco dei certificati aperto inserire un nuovo certificato tramite il pulsante “Aggiungi” o selezionare un certificato esistente del progetto tramite il simbolo di spunta.

   Il tipo e le proprietà dei certificati visualizzati possono essere riconosciuti nel manager dei certificati globale.

Certificati per il CP 1542SP-1 IRC

Presupposti nelle impostazioni Security globali

Per l’invio protetto di e-mail importare il certificato del provider di e-mail nel manager dei certificati.

Assegnazione del certificato nella progettazione del CP

Selezionare il seguente certificato nella progettazione del CP:

- Tabella "Certificati client accreditati":

  Il certificato del provider di e-mail

Certificati per il CP 1543SP-1

Prima che i certificati possano essere referenziati nei blocchi di programma per Secure Communication , questi certificati devono essere assegnati al modulo Security come certificati del dispositivo tramite il Manager dei certificati locale.

Presupposti nelle impostazioni Security globali

Per poter assegnare al CP certificati di un partner di comunicazione è necessario dapprima importare i certificati del partner nel Manager dei certificati globale (Impostazioni Security globali).

Per rendere noto al modulo partner il certificato assegnato, dopo l’importazione questo certificato deve essere registrato nell’elenco dei certificati del partner accreditati.

Assegnazione dei certificati nella progettazione del CP

Selezionare i seguenti certificati nella progettazione del CP:

- Tabella “Certificati del dispositivo”:

  Il certificato del dispositivo del CP creato dal progetto STEP 7

- Tabella “Certificati dei dispositivi partner”:

  Il certificato importato del partner

Programmazione (OUC) 5

5.1 Blocchi di programma per OUC

Utilizzo dei blocchi di programma per la comunicazione Open User Communication (OUC)

I collegamenti della Open User Communication non vengono progettati.

Per la comunicazione TCP-/UDP-/ISO-on-TCP tramite Ethernet vengono impiegati i blocchi elencati di seguito della Open User Communication (OUC). Creare quindi i relativi blocchi di programma. Per maggiori dettagli sui blocchi di programma consultare il sistema di informazione di STEP 7.

Nota

Versioni differenti dei blocchi di programma

Osservare che in STEP 7 in una stazione non possono essere utilizzate versioni differenti di un blocco di programma.

Blocchi di programma supportati per OUC

Blocchi di programma per tutti e tre i tipi di CP

Le seguenti istruzioni nella versione minima indicata sono disponibili per la programmazione della Open User Communication per tutti e tre i tipi di CP:

- **TSEND_C V3.0 / TRCV_C V3.1**

  Blocchi compatti per la realizzazione/l'interruzione del collegamento nonché invio e ricezione di dati

  e

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

  Realizzazione del collegamento / interruzione del collegamento

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

  Invio o ricezione di dati tramite UDP

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

  Invio e ricezione di dati tramite il TCP o ISO-on-TCP

- **TMAIL_C V4.0**

  Invio di e-mail

I blocchi di programma si trovano in STEP 7 nella finestra "Istruzioni > Comunicazione > Open User Communication".

Descrizioni del collegamento nei tipi di dati di sistema (SDT)

Per la relativa descrizione del collegamento i blocchi indicati sopra utilizzano il parametro CONNECT (o MAIL_ADDR_PARAM in TMAIL_C). La descrizione del collegamento viene trasferito in un blocco dati la cui struttura viene definita da un tipo di dati di sistema (SDT).

Creazione di un SDT per il blocchi dati

Creare l'SDT necessario per ciascuna descrizione del collegamento come blocco dati. Il tipo SDT viene generato non selezionando in STEP 7 nella tabella della dichiarazione del blocco una voce dalla casella di riepilogo "Tipo di dati", ma inserendo manualmente il nome nella casella "Tipo di dati", (ad es. "TCON_Param"). Il SDT corrispondente viene quindi creato con i relativi parametri.

In base alle funzioni Security supportate i tre tipi di CP supportano i seguenti SDT:

SDT per tutti e tre i tipi di CP

I seguenti SDT possono essere utilizzati da tutti e tre i tipi di CP:

- **TCON_Param**

  Per la trasmissione di telegrammi tramite TCP

- **TADDR_Param**

  Per la trasmissione di telegrammi tramite UDP

- **TCON_IP_RFC**

  Per la trasmissione di telegrammi tramite ISO-on-TCP

- **TMail_V4**

  Per la trasmissione di e-mail con indirizzamento del server e-mail tramite un indirizzo IPv4

- **TMail_V6**

  Per la trasmissione di e-mail con indirizzamento del server e-mail tramite un indirizzo IPv6

- **TMail_FQDN**

  Per la trasmissione di e-mail con indirizzamento del server e-mail tramite il nome Host

La descrizione degli SDT con i relativi parametri si trovano nel sistema di informazione STEP 7 al rispettivo nome dell'SDT.

SDT per CP 1542SP-1 IRC e CP 1543SP-1

Questi due tipi di CP possono utilizzare il seguente SDT per collegamento e-mail con funzione Security:

- **TMail_V4_SEC**

  Per la trasmissione protetta di e-mail con indirizzamento del server e-mail tramite un indirizzo IPv4

- **TMail_QDN_SEC**

  Per la trasmissione protetta di e-mail con indirizzamento del server e-mail tramite il nome Host

SDT solo per CP 1543SP-1

Il CP CP 1543SP-1 può utilizzare il seguente SDT per la trasmissione dei dati con funzione Security:

- **TCON_IP_V4_SEC**

  Per la trasmissione protetta di dati tramite TCP

Realizzazione e interruzione del collegamento

Con il blocco di programma TCON vengono realizzati collegamenti. Fare attenzione che per ciascun collegamento deve essere richiamato un proprio blocco di programma TCON.

Per ciascun partner di comunicazione deve essere realizzato un collegamento proprio, anche se vengono inviati blocchi di dati identici.

Alla conclusione della trasmissione dei dati un collegamento può essere interrotto. Un collegamento viene interrotto richiamando TDISCON.

Nota

Interruzione del collegamento

Se un collegamento in atto viene interrotto dal partner di comunicazione o da guasti della rete, il collegamento deve essere interrotto anche dal richiamo di TDISCON. Tenerne conto durante la parametrizzazione.

Diagnostica e manutenzione

6

6.1 Possibilità di diagnostica

Sono disponibili le seguenti possibilità di diagnostica.

LED dell'unità

Informazioni sugli indicatori LED si trovano nel capitolo LED (Pagina 25).

STEP 7: La scheda "Diagnostica" nella finestra di ispezione

Qui si ottengono le seguenti informazioni sull'unità selezionata:

- Registrazioni nel buffer di diagnostica della CPU
- Informazioni sullo stato online dell'unità

STEP 7: Funzioni di diagnostica nel menu "Online > Online e diagnostica"

Attraverso le funzioni online è possibile leggere da una stazione di engineering sulla quale è salvato il progetto con il CP le informazioni di diagnostica dal CP. Si ottengono le seguenti informazioni statiche sull'unità selezionata:

- Informazioni generali sull'unità
- Stato della diagnostica
- Informazioni sulle interfacce dell’unità

  Informazioni su ulteriori funzioni dell’unità

Se si vuole utilizzare la diagnostica online con la stazione tramite il CP, come presupposto è necessario attivare le funzioni online nel gruppo di parametri “Tipi di comunicazione, vedere il capitolo Tipi di comunicazione (Pagina 46).

Maggiori informazioni sulle funzioni di diagnostica di STEP 7 sono riportate nel sistema di informazione di STEP 7.

Il Webserver della CPU

Tramite il CP è possibile accedere al Webserver della CPU e alle relative informazioni disponibili. Per l’accesso vedere il capitolo Il Webserver della CPU (Pagina 104).

SNMP

Per le funzioni vedere il capitolo Diagnostica tramite SNMP (Pagina 102).

6.2 Diagnostica tramite SNMP

Presupposto

Il presupposto per l'utilizzo di SNMP è l'attivazione della funzione nella progettazione, vedere il capitolo SNMP (Pagina 45).

SNMP (Simple Network Management Protocol)

SNMP è un protocollo per la diagnostica e la gestione di reti e di nodi nella rete. Per la trasmissione dei dati l'SNMP utilizza il protocollo senza collegamento UDP.

Le informazioni sulle proprietà dei dispositivi con funzione SNMP si trovano nei file MIB (MIB = Management Information Base).

Informazioni dettagliate relative a SNMP e Siemens Automation MIB si trovano nel manuale /6/ (Pagina 122).

Fornitura dei CP

I CP supportano le seguenti versioni SNMP:

- **CP 1542SP-1, CP 1542SP-1 IRC**
  - SNMPv1
- **CP 1543SP-1**
  - SNMPv1
  - SNMPv3 (con le funzioni Security attivate)

I trap non sono supportati dal CP.

MIB supportati in SNMPv1

I CP supportano i seguenti MIB:

- **MIB II (secondo RFC1213)**

  Il CP supporta i seguenti gruppi di oggetti MIB:
  - System
  - Interfaces
  - IP
  - ICMP
  - TCP
  - UDP
  - SNMP
- **LLDP MIB**
- **Siemens Automation MIB**

  Osservare le aree di scrittura negli oggetti MIB, vedi sezione successiva (SNMPv3).

Oggetti MIB supportati in SNMPv3

Con SNMPv3 attivo il CP fornisce i seguenti oggetti MIB:

- **MIB II (secondo RFC1213)**

  Il CP supporta i seguenti gruppi di oggetti MIB:

  – System

  – Interfaces

    L'oggetto MIB "Interfaces" fornisce informazioni sullo stato tramite le interfacce del CP.

  – IP (IPv4/IPv6)

  – ICMP

  – TCP

  – UDP

  – SNMP

  I seguenti gruppi dei MIB II standard non vengono supportati:

  – Adress Translation (AT)

  – EGP

  – Transmission

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

  Osservare che gli accessi per scrittura sono ammessi solo per i seguenti oggetti MIB del gruppo "System":

  – sysContact

  – sysLocation

  – sysName

    Il sysName impostato come nome Host tramite l'opzione- DHCP 12 viene inviato al server DHCP per la registrazione in un server DNS.

  Per motivi di sicurezza, per tutti gli altri oggetti MIB e gruppi è possibile solo l'accesso per lettura.

Autorizzazioni di accesso tramite nomi Community (SNMPv1)

Per il controllo dei diritti per l'accesso agenti SNMP, il CP utilizza le seguenti stringe Community:

Tabella 6- 1 Autorizzazioni di accesso negli agenti SNMP

Tipo di accesso	Stringa Community *)
Accesso per lettura	public
Accesso per lettura e per scrittura	private

*) Osservare il tipo di scrittura con lettere minuscole!

6.3 Il Webserver della CPU

Il Webserver della CPU

La CPU ha un Webserver al quale è possibile accedere da una stazione di engineering mediante HTTP/HTTPS tramite il CP.

Il Webserver della CPU offre numerose funzioni per la diagnostica e per scopi di service, ad esempio il caricamento di file firmware. Per informazioni dettagliate consultare il manuale di sistema /2/ (Pagina 121) e il sistema di informazione di STEP 7 alla voce “Webserver”.

Presupposti per l’accesso al Webserver

Webbrowser ammesso

I Webserver sulla stazione di engineering per l’accesso al Webserver della CPU si trovano nel sistema di informazione STEP 7 alla voce "Webserver".

Presupposti nella progettazione della CPU

1. Aprire il progetto corrispondente nella stazione di engineering.
2. Selezionare la CPU della stazione interessata in STEP 7.
3. Selezionare la voce "Web server".
4. Attivare nel gruppo di parametri "Generale" l'opzione "Attiva Web server su questa unità".
5. In una CPU creare un utente con i relativi diritti nella gestione utenti.

   Per caricare il firmware, a questi utenti è necessario assegnare il diritto di eseguire l'aggiornamento firmware nel livello di accesso.

   Il nome utente e la password sono necessari in un secondo momento per l’accesso.
6. Progettazione dell’opzione “Consenti accesso solo tramite HTTPS"“ nel gruppo di parametri “Generale“

   A seconda del tipo di accesso al Webserver che si vuole eseguire tramite HTTP o HTTPS si distingue la progettazione del parametro:

   – "Consenti accesso solo tramite HTTPS“ attivato

     La realizzazione del collegamento è possibile solo tramite HTTPS.

   – "Consenti accesso solo tramite HTTPS“ disattivato

     La realizzazione del collegamento è possibile tramite HTTP e HTTPS.

Presupposti supplementari nella progettazione del CP 1543SP-1

Attivare il firewall nel gruppo di parametri "Security".

A seconda del protocollo utilizzato è necessario eseguire ulteriori impostazioni nel gruppo di parametri del firewall "Dall'esterno alla stazione".

- In caso di realizzazione del collegamento tramite HTTP
  - Attivare l'opzione "Consenti HTTP".
  - Attivare l'opzione "Consenti HTTPS"
    Motivo: la commutazione su HTTPS avviene dopo l'autentificazione nel server web.
- In caso di realizzazione del collegamento tramite HTTPS
  - Disattivare l'opzione "Consenti HTTP".
  - Attivare l'opzione "Consenti HTTPS".

Realizzazione del collegamento con il Webserver

Procedere nel modo seguente per collegarsi dalla stazione di engineering con il Webserver della CPU.

I seguenti procedimento sono descritti nelle seguenti sezioni.

Realizzazione del collegamento tramite HTTP

1. Collegare il PC sul quale si trova il nuovo file del firmware tramite l'interfaccia Ethernet con il CP.
2. Inserire l'indirizzo del CP nella casella di indirizzo del proprio Web browser:
   http://<indirizzo IP>
3. Premere il tasto di inserimento <Invio>.

   La pagina iniziale del Web server si apre.
4. Fare clic sulla voce "Download certificato" a destra in alto nella finestra.

   Si apre la finestra di dialogo "Certificato".
5. Caricare il certificato sul PC facendo clic sul pulsante "Installa certificato ...".

   Il certificato viene caricato sul PC.

   Le informazioni relative al caricamento di un certificato si trovano nella guida del proprio Web browser e nel sistema di informazione STEP 7 alla voce “Certificati per Webserver".

Se il collegamento è passato in modalità protetta HTTPS ("https://<Indirizzo IP>/..." nella casella di indirizzo del Webserver), è possibile comandare il Webserver, ad es. caricare il file del firmware (vedi sezione seguente).

Se si interrompe il collegamento al Web server, la volta successiva è possibile connettersi al Web server senza caricare il certificato tramite HTTP.

Realizzazione del collegamento tramite HTTPS

1. Collegare il PC sul quale si trova il nuovo file del firmware tramite l'interfaccia Ethernet con il CP o la CPU.
2. Inserire l'indirizzo del CP nella casella di indirizzo del proprio Web browser: https://<indirizzo IP>
3. Premere il tasto di inserimento <Invio>.

   La pagina iniziale del Web server si apre.

Il Webserver può essere comandato.

Caricamento dei file del firmware tramite il Webserver della CPU

Presupposto: Il nuovo file del firmware è salvato nella stazione di engineering.

1. Connettersi alla pagina iniziale del Webserver.
2. Dopo la connessione nella navigazione del Web server selezionare la voce "Stato dell'unità".
3. Selezionare il CP nell'elenco delle unità.
4. Selezionare nella parte inferiore della finestra la scheda "Firewall".
5. Cercare il file del firmware nel PC con il pulsante "Sfoglia..." e caricare il file tramite il pulsante "Esegui aggiornamento" nella stazione.

Osservare le avvertenze relative alla durata dell'aggiornamento del firmware nel capitolo Caricamento del firmware (Pagina 108).

6.4 Stato di elaborazione delle e-mail Telecontrol

Progettazione dello stato di elaborazione di e-mail Telecontrol (CP 1542SP-1 IRC)

Le seguenti identificazioni di stato valgono per e-mail progettate tramite l'editor dei messaggi del CP 1542SP-1 IRC, cfr. capitolo Progettazione dei messaggi (Pagina 83).

Le e--mail che devono essere inviate tramite i blocchi di programma della Open User Communication restituiscono un altro stato tramite il blocco (vedi guide al blocco).

Stato di elaborazione delle e-mail Telecontrol

Gli stati forniti dalla "Variabili PLC per stato di modifica" hanno i seguenti significati:

Tabella 6- 2 Significato dell'identificazione di stato esadecimale emessa

Stato	Significato
0000	Trasmissione conclusa senza errori
82xx	Altri messaggi di errore dal server e-mail Ad eccezione dell'"8" iniziale, il messaggio corrisponde al numero di errore a tre posizioni del protocollo SMTP.
8401	Nessun canale disponibile. Causa possibile: È già in atto un collegamento e-mail tramite il CP. Non è possibile configurare parallelamente un secondo collegamento.
8403	Non è stato possibile realizzare un collegamento TCP/IP al server SMTP.
8405	Il server SMTP ha negato la richiesta di login.
8406	Un errore SSL interno o un problema con la struttura del certificato è stato determinato con il client SMTP.
8407	La richiesta per l'utilizzo dell'SSL è stata negata.
8408	Il client non ha potuto rilevare un socket per la realizzazione di un collegamento TCP/IP al server mail.
8409	Non è possibile scrivere sul collegamento. Causa possibile: Il partner di comunicazione ha eseguito un reset del collegamento o il collegamento è stato interrotto.
8410	Non è possibile leggere sul collegamento. Causa possibile: Il partner di comunicazione ha disconnesso il collegamento o il collegamento è stato interrotto.
8411	Invio di e-mail non riuscito. Causa: Lo spazio di memoria non era sufficiente per eseguire l'operazione di invio.
8412	Il server DNS configurato non ha potuto attivare il nome di dominio specificato.
8413	A causa di un errore interno nel sottosistema DNS il nome di dominio non ha potuto essere attivato.
8414	Come nome di dominio è stata indicata una stringa di caratteri vuota.
8415	Nel modulo Curl è subentrato un errore interno. L'esecuzione è stata interrotta.
8416	Nel modulo SMTP è subentrato un errore interno. L'esecuzione è stata interrotta.
8417	Richiesta a SMTP su un canale già utilizzato o un'ID di canale valida. L'esecuzione è stata interrotta.
8418	L'invio di e-mail è stato interrotto. Causa possibile: Superamento del tempo di esecuzione.
8419	Il canale è stato interrotto e non può essere utilizzato prima che il collegamento venga interrotto.
8420	La stringa del certificato del server non ha potuto essere verificata con il certificati Root del CP.
8421	Si è verificato un errore interno. L'esecuzione è stata arrestata.
8450	Azione non eseguita: Mailbox non disponibile / non accessibile. Ripetere il tentativo più tardi.
84xx	Altri messaggi di errore dal server e-mail Ad eccezione dell'"8" iniziale, il messaggio corrisponde al numero di errore a tre posizioni del protocollo SMTP.

Stato	Significato
8500	Errore di sintassi: Comando sconosciuto. Include anche l'errore di una stringa di comando troppo lunga. La causa può essere il server e-mail che non supporta il metodo di autenticazione LOGIN. Tentare di inviare e.mail senza autenticazione (nessun nome utente).
8501	Errore di sintassi. Controllare i seguenti dati di progettazione: Configurazione del messaggio > Dati e-mail (Content): • Indirizzo del destinatario ("A" o "Cc").
8502	Errore di sintassi. Controllare i seguenti dati di progettazione: Configurazione del messaggio > Dati e-mail (Content): • Indirizzo e-mail (mittente)
8535	Autenticazione SMTP incompleta. Controllare nella progettazione del CP i parametri "Nome utente" e "Password".
8550	Non è possibile accedere al server SMTP. Non si hanno diritti di accesso. Controllare i seguenti dati di progettazione: • Progettazione del CP > Progettazione e-mail: – Nome utente – Password – Indirizzo e-mail (mittente) • Configurazione del messaggio > Dati e-mail (Content): – Indirizzo del destinatario ("A" o "Cc").
8554	Trasmissione non riuscita
85xx	Altri messaggi di errore dal server e-mail Ad eccezione dell'"8" iniziale, il messaggio corrisponde al numero di errore a tre posizioni del protocollo SMTP.

6.5 Caricamento del firmware

Nuove versioni firmware del CP

Se per il CP è disponibile una nuova versione firmware, essa si trova nelle pagine Internet del Siemens Industry Online Support:

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

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

Per caricare un nuovo file del firmware nel CP sono disponibili tre modi:

- Salvataggio del file firmware nella Memory Card della CPU

  Una descrizione del procedimento per il caricamento nella Memory Card della CPU si trova nelle pagine Internet indicate dell'Industry Online Support.

- Caricamento del firmware con le funzione online di STEP 7 tramite Ethernet / Internet

  La descrizione di questi metodi è riportata di seguito.

- Caricamento del firmware tramite il Web server della CPU

  La descrizione di questi metodi è riportata nel capitolo Il Webserver della CPU (Pagina 104).

Nota

Durata dell'aggiornamento firmware

Il caricamento di un nuovo file del firmware può durare alcuni minuti.

Osservare che la durata dell'aggiornamento dipende dalla dimensione della configurazione della stazione con i moduli della periferia.

Attendere sempre che la conclusione dell'aggiornamento del firmware sia riconoscibile dai LED (immagine LED "Richiesta di manutenzione" - fine dell'aggiornamento del firmware).

Caricamento del firmware con le funzione online di STEP 7 tramite Ethernet / Internet

Presupposti:

- Il CP o la CPU è raggiungibile tramite l'indirizzo IP.
- La stazione di engineering e il CP si trovano nella stessa sotto-rete.
- Il nuovo file del firmware è salvato nella stazione di engineering.
- Collegare la stazione di engineering alla rete.
- Nella stazione di engineering è aperto il progetto STEP 7 interessato.

Procedimento:

1. Selezionare il CP o la CPU della stazione il cui CP si vuole aggiornare alla nuova versione firmware.
2. Attivare le funzioni online tramite il simbolo "Collega online".
3. Selezionare l'interfaccia Ethernet nella finestra di dialogo "Collega online" nell'elenco di selezione "Tipo dell'interfaccia PG/PC".
4. Selezionare il posto connettore del CP o della CPU.

   Sono possibili entrambi i modi.

5. Fare clic su "Avvia ricerca " per trovare il modulo nella rete e definire il percorso del collegamento.

   Se il modulo è stato trovato, viene visualizzato nella tabella.

6. Eseguire il collegamento tramite il pulsante "Collega".

   L'assistente "Collega online" conduce ai passi successivi.

7. Selezionare il CP nella vista della rete e quindi il menu di scelta rapida “Online & diagnostica” (tasto destro del mouse).
8. Selezionare nella navigazione della vista Online & diagnostica la voce "Funzioni > Aggiornamento firmware".
9. Cercare tramite il pulsante “Sfoglia" (gruppo di parametri "Programma di aggiornamento firmware") il nuovo file del firmware nel sistema di file della stazione di engineering.
10. Avviare il caricamento del firmware tramite il pulsante “Avvia aggiornamento", se nella casella di selezione “Stato" viene visualizzata la versione corretta del firmware firmato.

Il sistema di informazioni STEP 7 fornice una guida ulteriore alle funzioni online.

6.6 Sostituzione delle unità

⚠ CAUTELA

Leggere il manuale di sistema "SIMATIC ET 200SP Sistema di periferia decentrata"

Prima del montaggio leggere i passi relativi al collegamento e alla messa in servizio nel manuale di sistema "SIMATIC ET 200SP Sistema di periferia decentrata” (vedere rimando bibliografico nell’appendice).

Durante il montaggio e il collegamento procedere in base alle descrizioni riportate nel manuale di sistema "SIMATIC ET 200SP Sistema di periferia decentrata".

Assicurarsi che durante il montaggio/lo smontaggio dell'apparecchio l'alimentazione sia disinserita.

Sostituzione delle unità

I dati di progettazione STEP-7 del CP vengono salvati sulla relativa CPU locale. In caso di sostituzione questo consente una semplice sostituzione del CP, senza dover ricaricare i dati del progetto nella stazione.

Durante il riavvio della stazione il nuovo CP legge i dati del progetto dalla CPU.

Dati tecnici

7

Dati tecnici		
Numeri articolo	CP 1542SP-1	6GK7542-6UX00-0XE0
	CP 1542SP-1 IRC	6GK7542-6VX00-0XE0
	CP 1543SP-1	6GK7543-6WX00-0XE0
Collegamento a Industrial Ethernet		
Quantità	1	
Esecuzione	Posto connettore per BusAdapter	
Proprietà	100BASE-TX, IEEE 802.3-2005, half duplex/full duplex, autocrossover, autonegotiation, separazione galvanica	
Velocità di trasmissione	10 / 100 Mbit/s	
Lunghezze ammesse dei cavi Ethernet, rame, con 100 Mbit/s *		
Tipo di cavo - rame	Lunghezze max.	
TP Torsion Cable	• Max. 55 m TP Torsion Cable con IE FC RJ45 Plug 180 • Max. 45 m TP Torsion Cable con IE FC RJ45 + 10 m TP Cord tramite IE FC RJ45 Outlet	
TP FC Marine Cable, TP FC Trailing Cable, TP FC Flexible Cable, TP FC FRNC Cable, TP FC Festoon Cable, TP FC Food Cable	• Max. 85 m TP FC Marine/Trailing/Flexible/FRNC/Festoon/Food Cable con IE FC RJ45 Plug 180 • Max. 75 m TP FC Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord tramite IE FC RJ45 Outlet	
TP FC Standard Cable	• Max. 100 m TP FC Standard Cable con IE FC RJ45 Plug 180 • Max. 90 m TP FC Standard Cable + 10 m TP Cord tramite IE FC RJ45 Outlet	
Lunghezze ammesse dei cavi Ethernet, fibra ottica (FO), con 100 Mbit/s *		
Tipo di cavo - FO di vetro (Multimode):	Lunghezze max.	
• FO FRNC Cable GP, FO Standard Cable GP, FO Ground Cable, FO Trailing Cable, FO Trailing Cable GP, FO Robust Cable GP	• Max. 2000 m	
• INDOOR FO cavo per interno, cavo standard FO, cavo da trascinamento FO flessibile	• Max. 750 m	
• FO Robust Cable GP	• Max. 2000 m	
Tipo di cavo - FO di PCF e plastica	Lunghezze max.	
• POF Standard Cable GP 980/1000, POF Trailing Cable 980/1000	• Max. 50 m	

Dati tecnici		
• PCF Standard Cable GP, PCF Trailing Cable, PCF Trailing Cable GP	• Max. 100 m	
Dati elettrici		
Alimentazione esterna (X80), versione	Presa Morsettiera per presa	A due poli con protezione da inversione polarità 2 x a due poli per alimentazione semplice o ridondante
Tensione di alimentazione (esterna)	• Tipo di tensione • Limite inferiore ammesso • Limite superiore ammesso	• DC 24 V • 19,2 V • 28,8 V
Corrente assorbita	• Dai DC 24 V (esterni) • Dal bus backplane (3,3 V)	• 250 mA (tip.) • 4 mA (tip.)
Corrente di inserzione massima	(Valore nominale)	12 A
Potenza attiva dissipata	(tipica)	6 W
Categoria di sovratensione conforme a IEC / EN 60664-1	Categoria I	
Condizioni ambientali ammesse		
Temperatura ambiente	Durante il funzionamento in caso di struttura orizzontale del telaio di montaggio	0 .. + 60 °C
	Durante il funzionamento in caso di struttura verticale del telaio di montaggio	0 .. + 50 °C
	Durante il magazzinaggio	-40 .. +70 °C
	Durante il trasporto	-40 .. +70 °C
Umidità relativa	Durante il funzionamento	≤ 95 % a 25 °C, senza condensa
Forma costruttiva, dimensioni e peso		
Formato dell'unità	Unità compatta ET 200SP	
Grado di protezione	IP20	
Peso		
• Senza BusAdapter	• 180 g	
• Con BusAdapter 2xRJ45	• 230 g	
Dimensioni (L x A x P)	60 x 117 x 74 mm	
Possibilità di montaggio	Guida a U DIN (35 mm)	
Mean Time Between Failures (MTBF)		
• Con + 40 °C	• 56,87 anni	
• Con + 60 °C	• 24,78 anni	
Funzioni del prodotto **		

***** Per i dettagli relativi alle lunghezze dei cavi vedere ET 200SP Manuale di sistema, /2/ (Pagina 121).

****** Ulteriori proprietà e dati potenziali si trovano nel capitolo Applicazione e funzioni (Pagina 11).

Omologazione

A

Omologazioni assegnate

Nota

Omologazioni riportate sulla targhetta identificativa dell'apparecchio

Le omologazioni indicate valgono solo se sul prodotto è stata applicata una relativa contrassegnatura. Dalle sigle riportate sulla targhetta è possibile riconoscere quale delle seguenti omologazioni è stata assegnata al proprio prodotto.

Campo di validità delle omologazioni

Le omologazioni riportate di seguito sono valide per il CP.

I controlli necessari per le omologazioni sono stati eseguiti con il BusAdapter inserito.

I BusAdapter dispongono di proprie omologazioni e non sono riportati nella presente descrizione.

Dichiarazione di conformità UE

CE

Il CP soddisfa i requisiti e gli obiettivi di sicurezza stabiliti dalle direttive CE sotto indicate ed è conforme alle norme europee armonizzate (EN) sui controllori a logica programmabile pubblicate nelle Gazzette Ufficiali della Comunità Europea.

- **2014/34/UE (direttiva ATEX)**

  Direttiva del Parlamento Europeo e del consiglio del 26 febbraio 2014 per l'adeguamento delle legislazioni degli stati membri per dispositivi e sistemi di protezione per l'impiego conforme alle direttive in aree a rischio di esplosione; Gazzetta Ufficiale della Comunità Europea L96, 29/03/2014, v. 309-356.

- **2014/30/UE (EMC)**

  Direttiva EMC UE del Parlamento Europeo e del consiglio del 26 febbraio 2014 per l'adeguamento delle legislazioni degli stati membri sulla compatibilità elettromagnetica; Gazzetta Ufficiale della Comunità Europea L96, 29/03/2014, v. 79-106

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

  Direttiva del Parlamento Europeo e del consiglio dell'8 giungo 2011 per la limitazione dell'utilizzo di materiale particolarmente pericoloso in dispositivi elettrici ed elettronici; Gazzetta Ufficiale della Comunità Europea L174, 01/07/2011, v. 88-110.

La dichiarazione di conformità UE è archiviata e tenuta a disposizione delle autorità competenti presso:

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

La dichiarazione di conformità CE si trova anche in Internet al seguente indirizzo:

Link: (https://support.industry.siemens.com/cs/ww/it/ps/)

> Tipo di articolo: “Certificati”, tipo di certificato: "Dichiarazione di conformità UE"

IECEx

I CP soddisfano i requisiti richiesti riguardanti la protezione contro le esplosioni secondo IECEx.

Certificato IECEx: IECEx DEK 14.0025X

Il CP soddisfa i requisiti stabiliti dalle seguenti norme:

- IEC 60079-0

  Aree a rischio di esplosione - Parte 0: Equipaggiamento - Requisiti generali

- EN 60079-15

  Atmosfere esplosive - Parte 15: Protezione del dispositivo attraverso classe di protezione antideflagrante 'n'

La stesura attuale delle norme può essere consultata nel certificato IECEx, che si trova in Internet al seguente indirizzo:

Link: (https://support.industry.siemens.com/cs/ww/it/ps/)

Le condizioni per l'impiego sicuro del CP devono essere rispettate conformemente al capitolo Avvertenze per l'impiego in zone Ex secondo ATEX / IECEx (Pagina 31).

Osservare anche le indicazioni nel documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", che si trova in Internet al seguente indirizzo:

Link: (https://support.industry.siemens.com/cs/ww/it/view/78381013)

ATEX

Il CP soddisfa i requisiti richiesti dalla norma UE 2014/34/UE "Apparecchi e sistemi di protezione per l'utilizzo conforme in aree con pericolo di esplosione".

Norme applicate:

- EN 60079-0

  Aree a rischio di esplosione - Parte 0: Equipaggiamento - Requisiti generali

- EN 60079-15

  Atmosfere esplosive - Parte 15: Protezione del dispositivo attraverso classe di protezione antideflagrante 'n'

La stesura attuale delle norme può essere consultata nella dichiarazione di conformità UE, vedere sopra.

Omologazione ATEX: II 3 G Ex nA IIC T4 Gc

Numero di controllo: KEMA 07ATEX0145 X

Le condizioni per l'impiego sicuro del CP devono essere rispettate conformemente al capitolo Avvertenze per l'impiego in zone Ex secondo ATEX / IECEx (Pagina 31).

Osservare anche le indicazioni nel documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", che si trova in Internet al seguente indirizzo:

Link: (https://support.industry.siemens.com/cs/ww/it/view/78381013)

EMC

Il CP soddisfa i requisiti richiesti dalla direttiva UE 2014/30/UE “Compatibilità elettromagnetica EMC).

Norme applicate:

- EN 61000-6-4

  Compatibilità elettromagnetica (EMC) - Parte 6-4: Norme generiche - Emissioni per gli ambienti industriali

- EN 61000-6-2

  Compatibilità elettromagnetica (EMC) - Parte 6-2: Norme generiche - Immunità per gli ambienti industriali

RoHS

Il CP soddisfa i requisiti della direttiva UE 2011/65/UE per la limitazione dell'utilizzo di materiale particolarmente pericoloso in dispositivi elettrici ed elettronici.

Norma applicata:

- EN 50581:2012

c(UL)us

Norme applicate:

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

Report / UL file: E85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

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

Norme applicate:

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

APPROVED for Use in:

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

Ta: Vedere la classe di temperatura sulla targhetta identificativa del CP

Report / UL file: E223122 (NRAG, NRAG7)

Osservare le condizioni per l'impiego sicuro del CP conformemente al capitolo Avvertenze per l'impiego nell'area Ex secondo UL HazLoc (Pagina 31).

FM

Factory Mutual Approval Standard Class Number 3600, 3611, 3810

Class I, Division 2, Group A, B, C, D, T4 or Class I, Zone 2, Group IIC, T4

Ta: Vedere la classe di temperatura sulla targhetta identificativa del CP

Le condizioni per l'impiego sicuro del CP devono essere rispettate conformemente al capitolo Avvertenze generali per l'impiego in zone Ex secondo FM (Pagina 32).

Australia - RCM

Il CP soddisfa i requisiti stabiliti dalle norme AS/NZS 2064 (classe A).

Marchio per l'unione doganale euroasiatica

EAC (Eurasian Conformity)

Unione doganale euroasiatica per Russia, Bielorussia e Kazakistan

Dichiarazione di conformità secondo le prescrizioni tecniche dell'unione doganale (TR CU)

MSIP 요구사항 - For Korea only

Registration Number: MSIP REI S7M ET200SP

A급 기기(업무용 방송통신기자재)

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

Omologazioni attuali

I prodotti SIMATIC NET vengono periodicamente verificati da enti competenti e autorità di certificazione che ne certificano la conformità alle norme rispetto alle esigenze di particolari settori di mercato e applicazioni.

L'elenco aggiornato dei prodotti e delle relative certificazioni può essere richiesto al proprio rappresentante Siemens, oppure consultare le pagine Internet del Siemens Industry Online Support:

Link: (http://support.automation.siemens.com/WW/view/it/45605894)

Disegni quotati

B

Tutte le misure indicate nei disegni quotati sono in millimetri.

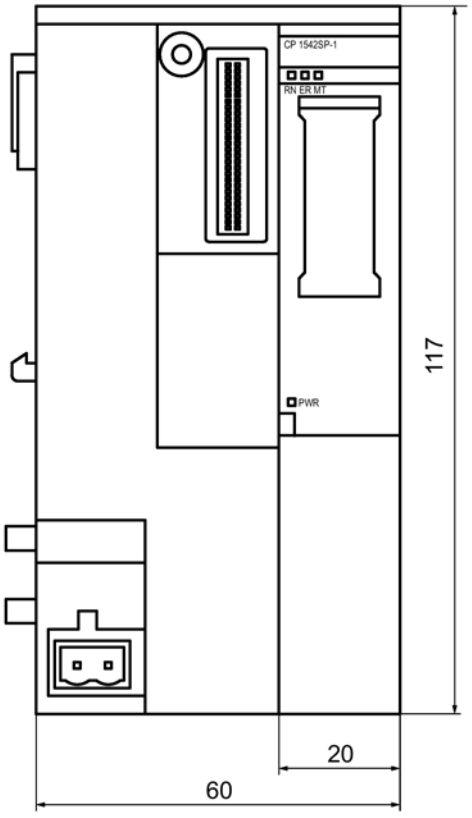


Figura B-1 Vista anteriore del CP

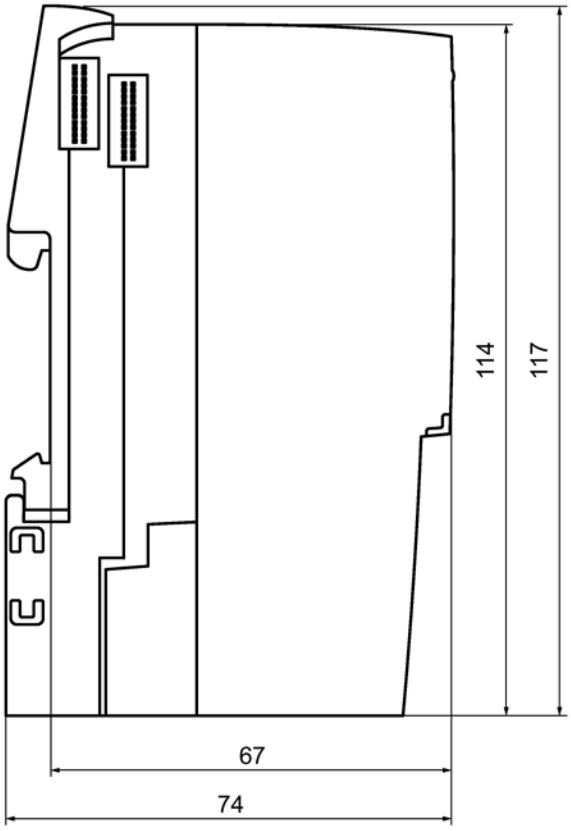


Figura B-2 Vista laterale (sinistra) del CP

Accessori

C

C.1 BusAdapter

BusAdapter

Per il collegamento alla rete Ethernet il CP necessita di un BusAdapter. Un BusAdapter non fa parte della fornitura del CP.

Figura C-1 Esempio di un BusAdapter, in questo caso: BA SCRJ/RJ45

Il CP supporta i seguenti BusAdapter:

- BA 2×RJ45

  PROFINET BusAdapter con i seguenti collegamenti:

  – 2 x prese Ethernet RJ45

  Numero di articolo: 6ES7193-6AR00-0AA0

- BA 2xFC

  PROFINET BusAdapter con i seguenti collegamenti:

  – 2 x collegamenti diretti del cavo di bus (FastConnect)

  Numero di articolo: 6ES7193-6AF00-0AA0

- BA 2xSCRJ

  PROFINET BusAdapter con i seguenti collegamenti:

  – 2 x cavi a fibra ottica POF/PCF

  Numero di articolo: 6ES7193-6AP00-0AA0

- BA SCRJ/RJ45

  PROFINET BusAdapter, convertitore supporto mediale FO - rame, con i seguenti collegamenti:

  – 1 x cavo a fibra ottica POF/PCF

  – 1 x presa Ethernet RJ45

  Numero di articolo: 6ES7193-6AP20-0AA0

- BA SCRJ/FC

  PROFINET BusAdapter, convertitore supporto mediale FO - rame, con i seguenti collegamenti:

  – 1 x cavo a fibra ottica POF/PCF

  – 1 x collegamento diretto del cavo di bus (FastConnect)

  Numero di articolo: 6ES7193-6AP40-0AA0

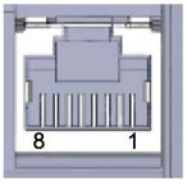
Ulteriori dettagli si trovano nel manuale /2/ (Pagina 121) e in Siemens Industry Mall in Link: (https://mall.industry.siemens.com).

C.2 Assegnazione dei pin dell'interfaccia Ethernet del BusAdapter

Assegnazione dei pin dell'interfaccia Ethernet

La tabella seguente mostra l'assegnazione dei collegamenti dell'interfaccia Ethernet. L'assegnazione corrisponde allo standard Ethernet 802.3-2005 in versione 100BASE-TX.

Tabella C- 1 Assegnazione del collegamento dell'interfaccia Ethernet

Vista della presa RJ45	Pin	Nome del segnale	Assegnazione
	1	TD	Transmit Data +
	2	TD_N	Transmit Data -
	3	RD	Receive Data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive Data -
	7	GND	Ground
	8	GND	Ground

Bibliografia

D

Come trovare la documentazione Siemens

- Numeri articolo

  I numeri di articolo per i prodotti Siemens qui rilevanti si trovano nei seguenti cataloghi:

  – SIMATIC NET - Comunicazione industriale / identificazione industriale, Catalogo IK PI

  – SIMATIC - Prodotti per Totally Integrated Automation e Micro Automation, Catalogo ST 70

  I cataloghi nonché informazioni supplementari possono essere richiesti presso la consulenza Siemens locale. Le informazioni sul prodotto si trovano anche in Siemens Industry Mall al seguente indirizzo:

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

- Manuali in Internet

  I manuali SIMATIC NET si trovano nelle pagine Internet del Siemens Industry Online Support:

  Link: (https://support.industry.siemens.com/cs/ww/it/ps/15247/man)

  Navigare al prodotto desiderato nella struttura ad albero del prodotto ed eseguire le seguenti impostazioni:

  Tipo di articolo "Manuali"

- Manuali su supporti dati

  I manuali dei prodotti SIMATIC NET si trovano anche nel supporto dati allegato ai vari prodotti SIMATIC NET.

/1/

SIMATIC
CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1
Istruzioni operative
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/22144/man)
Link: (https://support.industry.siemens.com/cs/ww/it/ps/22143/man)

/2/

SIMATIC
ET 200SP - Sistema di periferia decentrata
Manuale di sistema
Siemens AG
Link: (http://support.automation.siemens.com/WW/view/it/58649293)

/3/

SIMATIC NET
TeleControl Server Basic (Versione V3)
Istruzioni operative
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15918/man)

/4/

SIMATIC NET
Industrial Ethernet Security
Nozioni di base e applicazione
Manuale di progettazione
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15326/man)

/5/

SIMATIC NET
TIM DNP3
Manuale di sistema
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15940/man)

/6/

SIMATIC NET
Diagnostica e progettazione con SNMP
Manuale di diagnostica
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15392/man)

/7/

SIMATIC NET
Industrial Ethernet / PROFINET
Manuale di sistema
Siemens AG

- Industrial Ethernet
  Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465)
- Componenti di rete passivi
  Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

Indice analitico

S

T

V