SIEMENS

SIMATIC NET

S7-1200 - TeleControl SIMATIC CP 1243-1

Istruzioni operative

06/2022

C79000-G8972-C365-06

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
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANIA

C79000-G8972-C365-06
Ⓟ 05/2022 Con riserva di modifiche

Prefazione

Validità di questo manuale

In questo documento si trovano informazioni sul seguente prodotto Telecontrol:

- **CP 1243-1**
  Numero di articolo 6GK7 243-1BX30-0XE0
  Versione hardware 3
  Versione firmware V3.3

  Il CP 1243-1 è il processore di comunicazione per il collegamento di SIMATIC S7-1200 ad sistemi con stazioni di controllo tramite l'infrastruttura pubblica (ad es. DSL). Per i protocolli Telecontrol supportati vedere il capitolo Proprietà del CP (Pagina 13).

  Grazie alla tecnologia VPN e al firewall il CP consente l'accesso protetto a die S7-1200.

  Inoltre il CP può essere utilizzato come interfaccia Ethernet supplementare della CPU per la comunicazione S7.

Figura 1 CP 1243-1

Dietro allo sportellino superiore della custodia dell'unità è impressa come segnaposto una "X" a destra di fianco al numero di articolo della versione hardware. Se la scritta ad es. è "X 2 3 4", X è il segnaposto per la versione hardware 1.

La versione firmware del CP allo stato della fornitura si trova dietro allo sportellino superiore della custodia, a sinistra sotto al campo dei LED.

L'indirizzo MAC si trova dietro lo sportello inferiore della custodia.

Denominazioni del prodotto e abbreviazioni

- **CP / modulo / unità**

  Queste abbreviazioni vengono in seguito utilizzate al posto della denominazione completa del prodotto CP 1243-1.

- **TCSB**

  Questa abbreviazione viene di seguito utilizzata per il software "TeleControl Server Basic" nella versione V3.

- **STEP 7**

  Questa abbreviazione viene di seguiti utilizzata per lo strumento di progettazione STEP 7 Basic / Professional.

- **ES**

  PC con il progetto STEP 7

Scopo del manuale

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

Inoltre qui si trovano avvertenze per il funzionamento e le possibilità di diagnostica del dispositivo.

Progettazione

I passi di progettazione necessari vengono descritti come panoramica.

- **CP senza comunicazione Telecontrol**

  Nel presente manuale sono descritti passi di progettazione rilevanti per questi casi applicativi.

- **CP con comunicazione Telecontrol**

  Per questi casi applicativi nel rispettivo manuale di progettazione /4/ (Pagina 108) si trova una descrizione completa della progettazione e della diagnostica.

Osservare le indicazioni nella sezione "Struttura della documentazione".

Nuovo in questa edizione

- Versione hardware 3
- Versione firmware V3.3 con miglioramenti funzionali
- Nuove omologazioni (CCC / UKEX)

Limitazione:

Nel funzionamento Telecontrol con il protocollo IEC 60870-5 osservare quanto segue:

Se i valori dei due punti di accesso ai dati del valore di riferimento devono essere inviati quasi simultaneamente, l'invio del secondo valore di riferimento può essere ignorato. Tra l'invio dei valori di riferimento mantenere una distanza di almeno 70 millisecondi.

Versione di manuale sostituita

Edizione 12/2019

Edizione attuale del manuale in Internet

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

Link: (https://support.industry.siemens.com/cs/ww/it/ps/15922/man)

Struttura della documentazione

La documentazione del CP è costituita dai seguenti manuali e contenuti:

- **Istruzioni operative**
  - Applicazione e funzioni (senza Telecontrol)
  - Requisiti (CPU, software di progettazione ecc.)
  - Descrizione dell'hardware
  - Montaggio, collegamento, messa in servizio, funzionamento
  - Progettazione

    Il capitolo "Progettazione" descrive solo la progettazione delle funzioni che non dipendono da Telecontrol.

    Se si utilizzano le funzioni Telecontrol leggere il manuale di progettazione interessato.
  - Diagnostica, manutenzione
  - Dati tecnici, omologazioni, accessori
- **Manuale di progettazioneTeleControl Basic**

  Progettazione e diagnostica in STEP 7 Professional (TIA Portal)

  Valido per tutti i moduli di comunicazione SIMATIC NET che supportano il protocollo TeleControl Basic.

- **Manuale di progettazione DNP3**

  Progettazione e diagnostica in STEP 7 Professional (TIA Portal)

  Valido per tutti i moduli SIMATIC NET che supportano il protocollo DNP3.
- **Manuale di progettazione IEC 60870-5**

  Progettazione e diagnostica in STEP 7 Professional (TIA Portal)

  Valido per tutti i moduli SIMATIC NET che supportano il protocollo IEC 60870-5-101/104.

I link Internet dei manuali si trovano nell'appendice Bibliografia (Pagina 107).

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 S7-1200
- SIMATIC STEP 7 Basic / Professional

Avvertenze per il presente documento

Sigle del prodotto

- **CP / Modulo / Dispositivo / Unità**

  In questo documento queste denominazioni vengono utilizzate al posto della denominazione completa del prodotto CP 1243-1.

Riferimenti incrociati in PDF

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>.

Trova

Per visualizzare tutti i riscontri del termine cercato in un elenco, alcuni reader PDF supportano il comando <Ctrl>+<Maiusc>+<F>.

Condizioni di licenza

Nota
Open Source Software

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

Le condizioni di licenza di trovano sul supporto dati allegato:

- OSS_CP1243x_99.pdf

Firmware

Il firmware è contrassegnato e codificato. In questo modo viene assicurato che sul dispositivo possa essere caricato solo un firmware creato da Siemens.

Avvertenza sul supporto firmware/software

Tenersi regolarmente informati sulle ultime versioni di firmware/software oppure sugli aggiornamenti di sicurezza del firmware e applicarli. A partire dal rilascio di una nuova versione, le versioni precedenti non sono più supportate e non vengono più manutenute.

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 una componente imprescindibile di questo concetto.

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

Ulteriori informazioni relative alle possibili misure di sicurezza nell'ambito 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: (https://www.siemens.com/cert)

Dispositivo difettoso

In caso di guasto, inviare il dispositivo per la riparazione alla filiale SIEMENS locale. Una riparazione locale non è possibile.

Messa fuori servizio

Mettere fuori servizio il dispositivo per evitare che persone non autorizzate accedano a dati riservati nella memoria del dispositivo.

Resettare il dispositivo alle impostazioni di fabbrica.

Questi standard vengono raggiunti resettando la CPU tramite le funzioni online di STEP 7.

Riciclo e smaltimento

Il prodotto è a basso contenuto di sostanze nocive, è riciclabile e soddisfa i requisiti della direttiva WEEE 2012/19/UE "Rifiuti di apparecchiature elettriche ed elettroniche".

Non smaltire il prodotto nei siti di smaltimento pubblici. Per un riciclo compatibile con l'ambiente e lo smaltimento di vecchi dispositivi rivolgersi ad un'azienda di smaltimento per rifiuti elettronici o al partner di riferimento Siemens di competenza.

Osservare le disposizioni locali.

Le informazioni relative alla restituzione del prodotto si trovano nelle pagine Internet del Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/it/view/109479891).

Glossario SIMATIC NET

Il glossario SIMATIC NET descrive i termini specifici possibili utilizzati in questo documento.

Il glossario SIMATIC NET si trova nel Industry Online Support al seguente indirizzo:

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

Training, Service & Support

Le informazioni relative a Training, Service & Support si trovano nel documento multilingue "DC_support_99.pdf" sul supporto dati fornito in dotazione con la documentazione.

Indice del contenuto

Applicazione e funzioni

1

1.1 Proprietà del CP

Impiego

Il CP è previsto per il funzionamento in un sistema di automazione S7-1200.

Il CP consente il collegamento dell'S7–1200 a Industrial Ethernet o tramite Internet ai seguenti sistemi con stazioni di controllo:

- Server Telecontrol (applicazione server OPC TCSB V3)
- Centrale DNP3
- Centrale IEC

Inoltre il CP può essere impiegato come ampliamento di interfaccia della CPU. In questa funzione il CP serve come separazione di rete.

Grazie alla combinazione di diverse funzioni di sicurezza come firewall e protocolli per la codifica dei dati, il CP protegge la stazione o intere celle di automazione da accessi non autorizzati. Protegge la comunicazione tra la stazione e il partner di comunicazione da spionaggio e manipolazione.

1.2 Servizi di comunicazione

Comunicazione Telecontrol

Le seguenti applicazioni non sono supportate:

- **Comunicazione con una centrale master**

  Il CP è il processore di comunicazione di SIMATIC S7-1200 per il collegamento del sistema ai sistemi con stazioni di controllo indicati sopra. Il CP può comunicare con stazioni di controllo ridondanti.

  Per ciascun sistema con stazioni di controllo viene attivato il protocollo Telecontrol corrispondente nel CP ("Tipo di comunicazione"). I protocolli servono alla trasmissione dei dati basata su IP per applicazioni Telecontrol.

  Le funzioni Security utilizzabili si trovano nel capitolo Funzioni Security (Pagina 18).

- **Comunicazione trasversale**

  Comunicazione tra stazioni tramite centrale (TeleControl Basic)

  In questa applicazione il CP realizza un collegamento con il server Telecontrol tramite la rete mobile. Il server Telecontrol inoltra i telegrammi alla stazione di destinazione.

- **Comunicazione diretta**

  Nelle seguenti applicazioni è possibile la comunicazione diretta tra stazioni:

  – Open User Communication tramite blocchi di programma
  – Nei protocolli DNP3 e IEC, se nelle interfacce è attivata la "Funzione master".

Messaggi / e-mail

Per eventi particolari il CP può inviare messaggi sotto forma di e-mail.

La funzione viene progettata in STEP 7. Non è necessario l'impiego di blocchi di programma.

I requisiti e le funzioni si trovano nel capitolo Progettazione delle e-mail (Pagina 60).

Comunicazione tramite SINEMA Remote Connect

Supporto a partire dalla versione firmware V3.1. Vedere capitolo Comunicazione tramite SINEMA RC (Pagina 15).

Comunicazione S7 e comunicazione PG/OP

La lettura / scrittura di dati da una / in una CPU è consentita se nella progettazione del CP è attivata la comunicazione S7.

Il CP supporta le seguenti funzioni :

- **PUT/GET**

  Il CP supporta la funzione come client (blocchi di programma) e server per lo scambio di dati con stazioni remote (S7-300/400/1200/1500).

  Per maggiori dettagli sui blocchi di programma consultare il sistema di informazione di STEP 7.

- **Funzioni PG**
- **Funzioni di servizio e supervisione (HMI)**
- **Routing S7**

  A partire dal firmware del CP V2.1 con CPU ≥ V4.2

Per la comunicazione S7 il CP necessita di un indirizzo IP fisso.

Comunicazione tramite Open User Communication (OUC)

Tramite l'interfaccia Ethernet del CP e i blocchi di programma i blocchi di programma della Open User Communication nella CPU sono a disposizione del CP le seguenti possibilità di comunicazione:

- Comunicazione con stazioni SIMATIC
- Invio di e-mail

  A differenza del servizio corrispondente della comunicazione Telecontrol (vedere sopra) per la trasmissione di e-mail tramite OUC è necessario impiegare il blocco di programma TMAIL_C, vedere capitolo Blocchi di programma per OUC (Pagina 81).

1.3 Comunicazione tramite SINEMA RC

Comunicazione tramite SINEMA Remote Connect (SINEMA RC)

L'applicazione "SINEMA RC Server" offre una gestione del collegamento comune di reti ripartire su Internet, di cui fa parte anche l'accesso remoto sicuro alle stazioni subordinate. La comunicazione tra il SINEMA RC Server e i nodi remoti avviene tramite il tunnel VPN tenendo in considerazione i diritti di accesso memorizzati.

Per la codifica dei dati SINEMA RC utilizza OpenVPN. Il centro della comunicazione è il server SINEMA RC tramite il quale si svolge la comunicazione tra i nodi e che gestisce la configurazione del sistema di comunicazione.

I router SCALANCE M, che possono essere utilizzati per il collegamento, supportano anche OpenVPN e il collegamento a SINEMA Remote Connect.

Per la versione firmware del CP per la comunicazione tramite SINEMA RC vedere il capitolo Servizi di comunicazione (Pagina 13).

Gruppi di parametri

La progettazione della comunicazione tramite SINEMA RC e della comunicazione Telecontrol tramite SINEMA RC si esegue in due gruppi di parametri:

- Comunicazione tramite SINEMA RC:

  > "Security > VPN"

- Comunicazione Telecontrol tramite SINEMA RC:

  > "Tipi di comunicazione"

  Per la progettazione vedere i manuali di progettazione Telecontrol /4/ (Pagina 108).

Applicazioni

Dalla combinazione dei parametri per la comunicazione Telecontrol e SINEMA RC risultano le seguenti possibilità di applicazione:

Esempio applicativo:

- (1) Nessun Telecontrol e nessun SINEMA RC (CP solo per separazione della rete)
- (2) CP solo per manutenzione remota tramite SINEMA RC
- (3) CP solo per comunicazione Telecontrol
- (4) Il CP utilizza la comunicazione Telecontrol, SINEMA RC, ma solo per manutenzione remota.
- (5) Il CP utilizza SINEMA RC per la comunicazione Telecontrol e la manutenzione remota.

La tabella fornisce una panoramica sui casi di impiego con le rispettive impostazioni dei parametri.

- "ON" significa parametro attivato.
- "OFF" significa parametro disattivato.

Tabella 1- 1 Esempi applicativi e parametri da attivare

Esempio applicativo	Impostazioni di parametri (parametri abbreviati) *		
	SRC	**TC**	**TC-SRC**
(1)	Off	Off	Off
(2)	On	Off	Off
(3)	Off	On	Off
(4)	On	On	Off
(5)	On	On	On

***** Significato delle abbreviazioni dei parametri:

SRC - Security > VPN (attivato) > "Tipo di collegamento VPN":
"Configurazione OpenVPN automatica tramite SINEMA Remote Connect Server"

TC - Tipi di comunicazione > Comunicazione Telecontrol attivata

TC-SRC - Tipi di comunicazione >
"Attiva comunicazione Telecontrol tramite SINEMA Remote Connect"

1.4 Altri servizi e proprietà

Altri servizi e proprietà

- **Configurazione IP - IPv4 e IPv6**
  - IPv4 / IPv6

    Il CP supporta gli indirizzi IP secondo IPv4 e IPv6.

    Nelle reti IPv6 può essere utilizzato un indirizzo IPv6 in aggiunta a un indirizzo IPv4.
  - Assegnazione indirizzi

    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 rilevato da un server DHCP o in altro modo al di fuori della progettazione.
- **Sincronizzazione dell'ora**

  Il CP supporta diversi procedimenti della sincronizzazione dell'ora. Le informazioni si trovano nel capitolo "Sincronizzazione dell'ora (Pagina 47)".

- **Funzioni online**

  Dalla stazione di engineering è possibile accedere tramite il CP alla stazione con le funzioni online di STEP 7.

  Sono disponibili le seguenti funzioni online:

  – Caricamento di dati del progetto e di programmazione dal progetto STEP 7 alla stazione

  – Interrogazione di dati di diagnostica dalla stazione

  – Caricamento di file firmware nel CP

  Informazioni sulle funzioni online si trovano nel capitolo Possibilità di diagnostica (Pagina 87).

- **SNMP**

  Come SNMP Agent il CP supporta l'interrogazione dei dati tramite SNMP (Simple Network Management Protocol).

  Ulteriori informazioni si trovano nel capitolo SNMP (Pagina 92).

Altre proprietà nel funzionamento Telecontrol

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

  Grazie alla progettazione del punto di accesso ai dati in STEP 7 non è più necessaria la programmazione di blocchi di programma per la trasmissione dei dati di processo. I singoli punti di accesso ai dati vengono elaborati uno ad uno nel sistema di controllo.

- **Buffer di trasmissione**

  Il CP salva i valori dei punti di accesso ai dati progettati come evento nel buffer di trasmissione.

  I dati non vengono salvati nella memoria ritentiva. In caso di mancanza di tensione i dati vengono persi.

- **Trasmissione controllata dall'evento dei dati di processo**

  Il CP trasmette i dati singolarmente (spontaneamente) dal buffer di trasmissione o raggruppati al partner di comunicazione. La trasmissione può essere attivata da diversi trigger.

- **Preelaborazione del valore analogico**

  I valori analogici possono essere preelaborati nel CP secondo diversi metodi.

1.5 Funzioni Security

Industrial Ethernet Security

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 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.

Le funzioni Security possono essere utilizzate indipendentemente dalla comunicazione Telecontrol.

Funzioni Security dei protocolli Telecontrol

- **TeleControl Basic**
  - **Comunicazione Telecontrol codificata**

    Come funzione Security integrata (non progettabile) il protocollo codifica i dati durante la trasmissione.

    L'intervallo dello scambio di chiave tra CP e server Telecontrol si progetta in STEP 7 nel gruppo di parametri "Interfaccia Ethernet (X1) > Opzioni avanzate > Impostazioni di trasmissione".
  - **Password Telecontrol**

    Per l'autentificazione del CP nel server Telecontrol
- **DNP3**

  Possono essere utilizzate funzioni Security specifiche per DNP3.
- **IEC 60870-5**

  Per il protocollo IEC non sono disponibili funzioni Security specifiche per il protocollo.

Ulteriori funzioni Security progettabili del CP

Utilizzando il CP come modulo Security, per la stazione S7-1200 diventano accessibili le seguenti funzioni Security sull'interfaccia verso la rete esterna:

- **Firewall**
  - 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 per la limitazione di attacchi Flooding e DoS ("Definisci regole filtro pacchetto IP")
  - Regole firewall globali

- **VPN**

  Possono essere utilizzate le seguenti alternative:

  – Comunicazione protetta con IPsec Tunnel

    La comunicazione 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.

  – Manutenzione remota tramite SINEMA Remote Connect

    Per la comunicazione tramite un server SINEMA RC non è necessario e possibile la creazione di un gruppo VPN. Il server SINEMA RC gestisce la comunicazione tra i nodi e i meccanismi Security (OpenVPN).

- **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.

- **STARTTLS / SMTPS**

  Per la trasmissione sicura di e-mail

- **NTP (secure)**

  Per la trasmissione sicura con la sincronizzazione dell'ora

- **SNMPv3**

  Per la trasmissione continua sicura delle informazioni di analisi della rete

- **Protezione per apparecchi e segmenti di rete**

  La protezione tramite firewall può estendersi da singoli apparecchi, più apparecchi, fino a interi segmenti di rete.

Nota

Impianti a sicurezza critica - Raccomandazione

Utilizzo delle seguenti possibilità:

- Negli impianti con elevate esigenze di sicurezza utilizzare i protocolli sicuri NTP (secure), HTTPS e SNMPv3.
- 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.

Vedere anche il capitolo Raccomandazioni Security (Pagina 41).

Per la progettazione delle funzioni Security vedere il capitolo Security (Pagina 56).

Ulteriori informazioni per la funzionalità e la progettazione delle funzioni Security si trovano nel sistema di informazioni di STEP 7.

1.6 Limiti di configurazione e dati utili

Numero di CM/CP per stazione

Per ogni stazione S7-1200 si possono inserire e progettare fino a tre CM/CP di cui max. tre CP 1243-1.

Risorse di collegamento

- **Collegamenti S7 e collegamenti TCP / UDP / ISO-on-TCP**

  Numero complessivo di collegamenti tramite Industrial Ethernet: Max. 14
  di cui:

  – S7: Max. 14 (inclusi collegamenti per routing S7)

  – TCP/IP: Max. 14

  – ISO-on-TCP: Max. 14

  – UDP: Max. 14

Inoltre:

- **Collegamenti Telecontrol**

  Il CP può realizzare collegamenti con diversi protocolli Telecontrol ai seguenti partner:

  TeleControl Basic

  – con un server Telecontrol (TCSB) con configurazione semplice o ridondante.

  – Inoltre Comunicazione trasversale

    La comunicazione trasversale tra i CP di due stazioni funziona sempre tramite il server Telecontrol. Viene progettata nel gruppo di parametri "Stazioni partner" > "Partner per la comunicazione trasversale".

    Struttura d'insieme per la comunicazione trasversale: Complessivamente max. 15, di cui:

    - Invio al partner: Max. 3 (parametro "Buffer di trasmissione" attivato)

    - Ricezione da partner: Max. 15 (parametro "Buffer di trasmissione" disattivato)

  DNP3 / IEC 60870-5

  – Comunicazione con massimo 4 partner

    Come partner vale un master con struttura semplice o ridondante o una stazione (Comunicazione diretta).

    La Comunicazione diretta tra stazioni viene progettata tramite collegamenti Telecontrol.

- **Collegamenti online**

  2 risorse per 1 collegamento online con una stazione di engineering (STEP 7)

- **Collegamenti PG e HMI (OP)**

  Complessivamente max. 4, di cui:

  – Risorse per collegamenti PG: Max. 1

  – Risorse per collegamenti HMI: Max. 3

Numero di punti di accesso ai dai per la progettazione dei punti di accesso ai dati

Numero massimo di punti di accesso ai dati progettabili

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

Dati utili

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 (vedere i tipi di punti di accesso ai dati).

Memoria dei telegrammi (buffer di trasmissione)

Il CP dispone di una memoria di telegrammi (buffer di invio) per i valori dei punti di accesso ai dati progettati come evento e che devono essere inviati al partner di comunicazione.

Il buffer di invio ha la seguente dimensione massima:

- TeleControl Basic: 64 000 eventi
- DNP3: 100 000 eventi
- IEC: 100 000 eventi

Il buffer di trasmissione si ripartisce in parti uguali tra tutti i partner di comunicazione progettati. La dimensione della memoria dei telegrammi è impostabile in STEP 7 (gruppo di parametri "Comunicazione con la CPU").

Messaggi (e-mail)

- L'invio di fino a 10 messaggi (e-mail) può essere progettato tramite l'editor dei messaggi.
- Invio di e-mail tramite il blocco di programma TMAIL_C.

Tunnel IPSec (VPN)

Con ulteriori moduli Security possono essere realizzati fino a 8 tunnel IPSec per la comunicazione protetta.

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")

1.7 Esempi di configurazione

Gli esempi di configurazione per le applicazioni Telecontrol si trovano nei manuali di progettazione /4/ (Pagina 108).

Configurazione con CP per la separazione protetta della rete

Il seguente esempio illustra una configurazione con il CP 1243-1 che protegge la stazione e le celle di automazione subordinate.

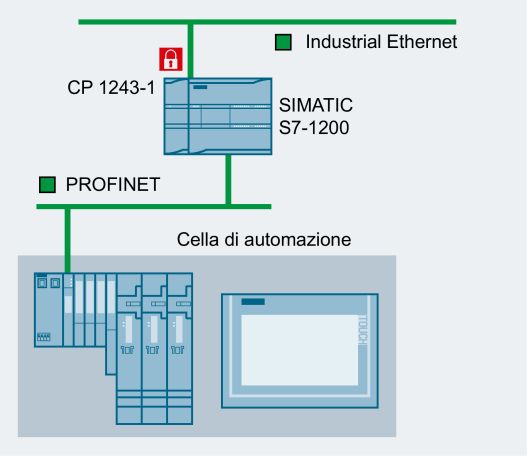


Figura 1-1 Comunicazione protetta con CP 1243-1

Configurazione con invio di e-mail

Il seguente esempio illustra una configurazione con invio di e-mail. La comunicazione Telecontrol del CP è disattivata.

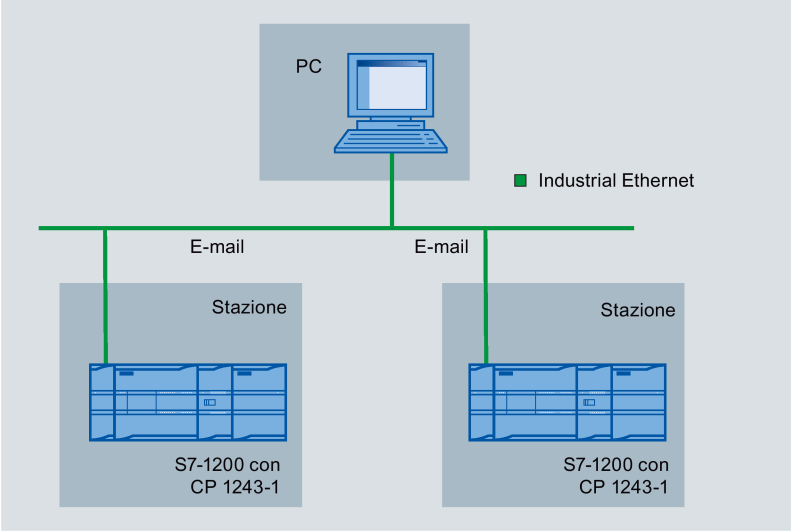


Figura 1-2 Invio di e-mail

Manutenzione remota con SINEMA RC

La seguente figura illustra il collegamento di diverse stazioni ad un CP Security ad una stazione di engineering tramite SINEMA Remote Connect - Server.

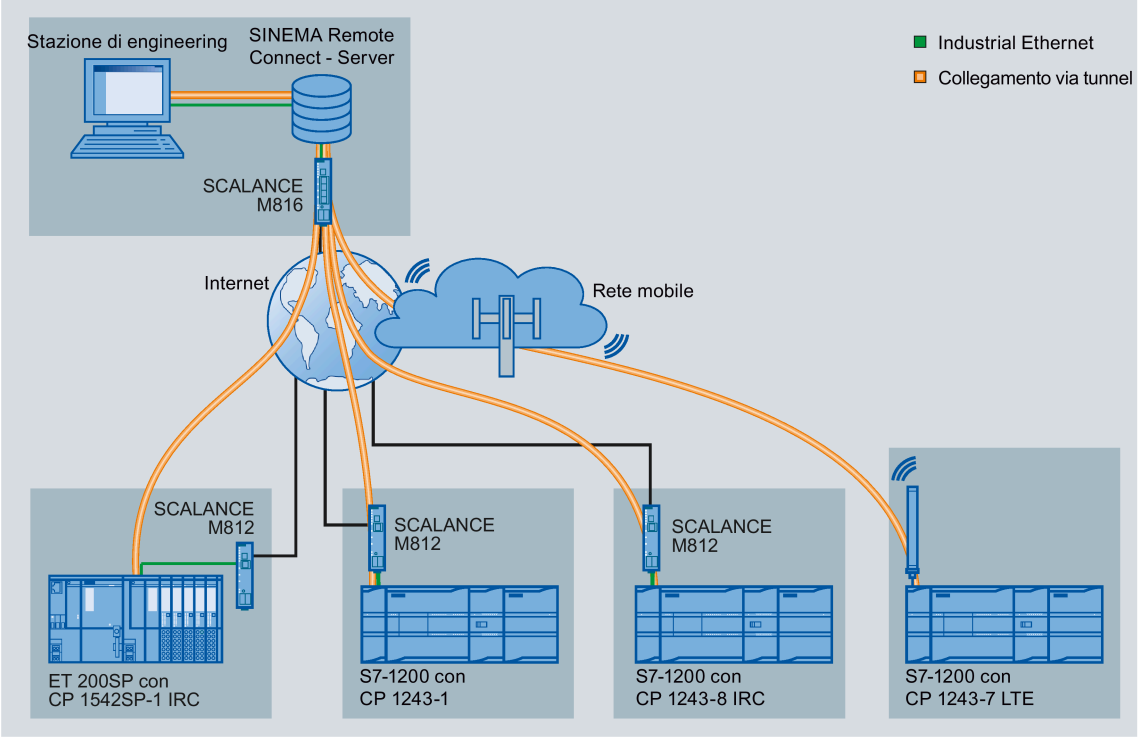


Figura 1-3 Collegamento di stazioni ad una stazione di engineering tramite SINEMA RC

1.8 Requisiti richiesti per l'impiego

1.8.1 Requisiti hardware

CPU 1200

Per l'utilizzo nella S7-1200 è necessario il seguente hardware:

- CP

  Il presupposto per la versione firmware V3.3 è un CP con versione hardware 2.

- CPU
  - Il CP fino alla versione firmware V2.1 (versione hardware 1) è compatibile con una CPU fino alla versione firmware V3.0.
  - Il CP dalla versione firmware V3.0 (versione hardware 2) è compatibile con una CPU dalla V4.1.
  - L'intera funzionalità del CP con la versione firmware V3.3 è disponibile solo con una CPU a partire da V4.4.

1.8.2 Requisiti software

Software per la progettazione e funzioni online

Per la progettazione dell'unità è necessario il seguente strumento di progettazione:

- Per il CP con versione firmware V3.2:

  STEP 7 Basic V16

- Per l'utilizzo dell'intera funzionalità della versione firmware V3.3:

  STEP 7 Basic V17

LED e collegamenti

2

2.1 Apertura degli sportelli del contenitore

Posizione degli elementi di indicazione e dei collegamenti elettrici

I LED per l'indicazione dettagliata degli stati dell'unità si trovano dietro lo sportello del contenitore dell'unità.

Il collegamento Ethernet si trova dietro lo sportello inferiore del contenitore dell'unità.

Apertura degli sportelli del contenitore

Aprire lo sportello superiore o inferiore ruotandolo verso il basso o verso l'alto come rappresentato dalle frecce nella figura. A tal proposito gli sportelli del contenitore sono provvisti di un'impugnatura.

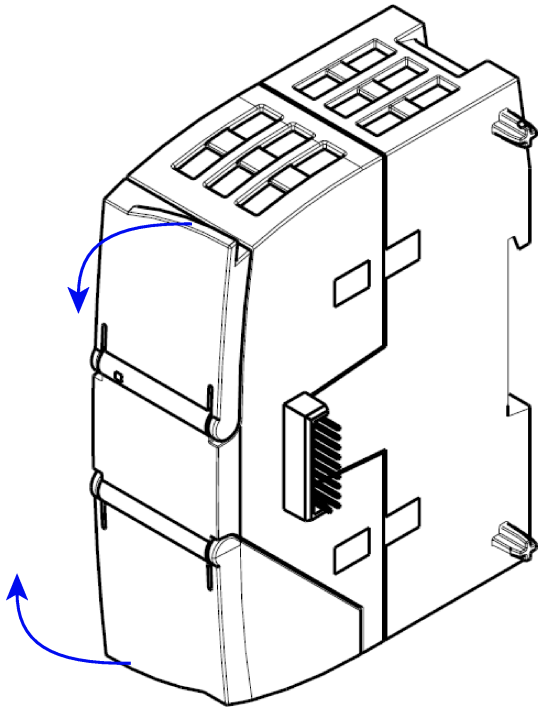


Figura 2-1 Apertura degli sportelli del contenitore

2.2 LED

LED dell'unità

L'unità dispone di diversi LED per l'indicazione dello stato:

- **LED sul frontalino**

  Il LED "DIAG" sempre visibile indica gli stati base dell'unità.

- **LED sotto lo sportello superiore del contenitore**

  I LED sotto lo sportello superiore del contenitore indicano altri dettagli sullo stato dell'unità.

Tabella 2- 1 LED sul frontalino

LED / colori	Denominazione	Significato
 (rosso / verde)	**DIAG**	Stato base dell'unità

Tabella 2- 2 LED sotto lo sportello superiore del contenitore

LED (colore)	Denominazione	Significato
 (verde)	**LINK**	Stato del collegamento con Industrial Ethernet
 (verde)	**CONNECT**	Stato dei collegamenti con il partner di comunicazione
 (verde)	**VPN**	Stato della progettazione VPN o SINEMA Remote Connect
 (verde)	**SERVICE**	Stato di un collegamento per funzioni online

Colori dei LED e rappresentazione degli stati dei LED

I simboli LED nella seguente tabella hanno il seguente significato:

Tabella 2- 3 Significato dei simboli LED

Simbolo				-
Stato del LED	OFF	ON (luce di riposo)	Lampeggiante	Irrilevante

Nota

Colori dei LED all'avvio dell'unità

All'avvio dell'unità per breve tempo si accendono tutti i LED. I LED a più colori indicano quindi un colore misto. In questo momento il colore dei LED non è univoco.

Indicazioni degli stati base del CP (LED "DIAG")

Tabella 2- 4 Indicazione degli stati base del CP

DIAG (rosso/verde)	**Significato (in più punti: significato alternativo)**
Stati base del CP	
○	• Tensione OFF • Avvio errato
● verde	In esecuzione (RUN) senza errori gravi
☼ verde lampeggiante	• Partner non collegato • Firmware caricato correttamente
☼ rosso lampeggiante	• In avvio • Errore unità • Dati di progetto STEP 7 non validi
◉ rosso-verde lampeggiante	Errore durante il caricamento del firmware

Indicazione degli stati di funzionamento e di comunicazione

In base al seguente schema i LED indicano lo stato di funzionamento e di comunicazione dell'unità:

Tabella 2- 5 Indicazione degli stati di funzionamento e di comunicazione

DIAG (rosso/verde)	-	**LINK** (verde)	**CONNECT** (verde)	**VPN** (verde)	**SERVICE** (verde)	**Significato (in più punti: significato alternativo)**
Avvio dell'unità (STOP → RUN) o stati di errore						
○		○	○	○	○	Tensione OFF
● rosso		●	●	●	●	Avvio - fase 1
☼ rosso lampeggiante		-	○	○	○	Avvio - fase 2
● verde		-	-	-	-	In esecuzione (RUN) senza errori gravi
○			●	●	●	Avvio errato
● rosso		-	☼	-	-	Dati di progetto STEP 7 non validi

DIAG (rosso/verde)	-	**LINK** (verde)	**CONNECT** (verde)	**VPN** (verde)	**SERVICE** (verde)	**Significato (in più punti: significato alternativo)**
rosso lampeggiante		-	○	-	-	Dati di progetto STEP 7 mancanti
rosso lampeggiante		●	☼	-	-	Errore bus back-plane
Collegamento con Industrial Ethernet						
-		●	-	-	-	Collegamento con Industrial Ethernet presente
verde		☼	-	-	-	• Creazione del collegamento con Industrial Ethernet in corso. • Acquisizione dell'indirizzo IP in corso.
-		○	-	-	-	Nessun collegamento con Industrial Ethernet
Collegamento ai partner di comunicazione						
verde		●	●	-	-	Collegamento realizzato con almeno un partner
verde		●	☼	-	-	Partner raggiungibile, CPU in STOP
verde lampeggiante		●	○	-	-	Partner non raggiungibile
Collegamento per funzioni online						
verde		●	-	-	●	Collegamento per funzioni online realizzato
verde		●	-	-	☼	Tentativo di realizzazione di un collegamento per funzioni online
verde		-	-	-	○	Nessun collegamento con la stazione di engineering
Collegamento VPN / SINEMA Remote Connect						
verde		●	-	●	-	Collegamento VPN / SINEMA Remote Connect realizzato
verde lampeggiante		●	-	verde lampeggiante	-	Tentativi di realizzazione di un collegamento VPN / SINEMA Remote Connect progettato
-		-	-	○	-	Nessun collegamento VPN / SINEMA Remote Connect progettato o momentaneamente realizzato nel CP

DIAG (rosso/verde)	-	**LINK** (verde)	**CONNECT** (verde)	**VPN** (verde)	**SERVICE** (verde)	**Significato** **(in più punti: significato alternativo)**
Caricamento del firmware						
						Il firmware viene caricato. Il LED DIAG lampeggia ad intermittenza con luce rossa e verde.
 verde lampeggiante						Il firmware è stato caricato con successo.
 rosso lampeggiante						Errore durante il caricamento del firmware

2.3 Collegamenti elettrici

2.3.1 Alimentazione

Alimentazione

L'alimentazione del CP viene fornita dal bus back-plane. Esso non necessita di un'alimentazione separata.

2.3.2 Interfaccia Ethernet X1P1

Interfaccia Ethernet

Il collegamento Ethernet si trova dietro lo sportello inferiore del contenitore dell'unità. L'interfaccia è una presa RJ45 IEEE 802.3.

L'assegnazione dei pin e ulteriori dati dell'interfaccia Ethernet sono riportati nel capitolo Dati tecnici (Pagina 97).

Montaggio, collegamento, messa in servizio, smontaggio

3

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.

3.1 Avvertenze importati per l'impiego 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
Il dispositivo può essere utilizzato solo in un ambiente con classe di imbrattamento 1 o 2, come descritto in EN/IEC 60664-1, GB/T 16935.1.

⚠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.

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

⚠AVVERTENZA

Requisiti richiesti per il quadro elettrico

Per soddisfar la direttiva UE 2014/34 UE (ATEX 114), la regolamentazione UK SI 2016/1107 o le condizioni di IECEx o CCC-Ex, la custodia o il quadro di comando deve soddisfare almeno i requisiti richiesti da IP54 (secondo EN/IEC 60529, GB/T 4208) secondo EN IEC/IEC 60079-7, GB 3836.8.

⚠AVVERTENZA

Cavi idonei con elevate temperature in aree a rischio di esplosione

Ad una temperatura ambiente ≥ 60 °C impiegare cavi resistenti ad alte temperature, progettati per una temperatura ambiente di ameno 20 °C. I passacavi impiegati sul dispositivo devono essere conformi al grado di protezione IP richiesto secondo EN IEC / IEC 60079-0, GB 3836.1.

⚠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 il dispositivo viene utilizzato a temperature ambiente superiori 60 °C, vanno utilizzati cavi con una temperatura d'esercizio ammessa di almeno 80 °C.

⚠AVVERTENZA

Sovratensioni transienti

Adottare misure per evitare sovratensioni transienti superiori al 40% della tensione nominale (o più di 119 V). 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 e FM

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

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

Se il dispositivo viene montato in un quadro elettrico, la temperatura interna di questo corrisponde alla temperatura ambiente del dispositivo.

⚠ 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 °C higher than maximum ambient temperature.

3.2 Montaggio, smontaggio e riparazione nell'area Ex

⚠ AVVERTENZA

Accessori e ricambi non autorizzati

Pericolo di esplosione in aree a rischio di esplosione

- Utilizzare esclusivamente accessori e ricambi originali.
- Osservare tutte le istruzioni di installazione e di sicurezza rilevanti descritte nelle istruzioni del dispositivo o fornite insieme all'accessorio o al ricambio.

⚠AVVERTENZA

Cavo o connettore non adatto

Pericolo di esplosione in aree a rischio di esplosione

- Utilizzare esclusivamente connettori che soddisfino i requisiti della protezione antideflagrante rilevante.
- Serrare eventualmente i raccordi a spina, le viti di fissaggio del dispositivo, le viti di collegamento a terra o in base alle coppie indicate.
- Chiudere le apertura dei cavi non utilizzate per i collegamenti elettrici.
- Controllare che il cavo sia saldamente in sede dopo l'installazione.

⚠AVVERTENZA

Posa errata dei cavi schermati

A causa delle correnti di compensazioni tra l'area a rischio di esplosione e l'area non a rischio di esplosione sussiste il rischio di esplosione.

- Collegare a terra i cavi schermati che attraversano aree a rischio di esplosione solo su una estremità.
- In caso di collegamento a terra su entrambi i lati posare un conduttore equipotenziale.

⚠AVVERTENZA

Compensazione del potenziale mancante

In caso di mancata compensazione di potenziale in aree a rischio di esplosione sussiste pericolo di esplosione in seguito a corrente di compensazione o scintille.

- Assicurarsi che per il dispositivo esista compensazione di potenziale.

⚠AVVERTENZA

Estremità del cavo non protette

In caso di estremità del cavo non protette in aree a rischio di esplosione sussiste il rischio di esplosione.

- Proteggere le estremità dei cavi non utilizzate secondo IEC/EN 60079-14.

⚠AVVERTENZA

Separazione insufficiente di circuiti elettri con e senza protezione intrinseca

Pericolo di esplosione in aree a rischio di esplosione

- In caso di collegamento di circuiti elettrici con e senza protezione intrinseca, garantire che la separazione galvanica venga eseguita correttamente in osservanza delle direttive locali (ad es. IEC 60079-14).
- Osservare le omologazioni del dispositivo nazionali valide.

⚠AVVERTENZA

Riparazione non ammessa dei dispositivi nella versione protetta da esplosioni

Pericolo di esplosione in aree a rischio di esplosione

- I lavori di riparazione possono essere eseguiti solo da personale autorizzato da Siemens.

3.3 Montaggio, collegamento e messa in servizio

ATTENZIONE

Montaggio errato

In seguito ad un montaggio errato il dispositivo può essere danneggiato o ne può essere compromesso il funzionamento.

- Prima di ogni montaggio del dispositivo assicurarsi che questo non presenti danni visibili.
- Montare il dispositivo con un attrezzo adatto. Osservare le indicazioni riportate nel capitolo relativo al montaggio.

⚠AVVERTENZA

Risorse aperte

Per i dispositivi si tratta di "risorse aperte" (open equipment) secondo lo standard IEC 61010-2-201 o UL 61010-2-201 / CSA C22.2 No. 61010-2-201. Per garantire un funzionamento sicuro dal punto di vista della resistenza meccanica, della resistenza alla fiamma, della stabilità e della protezione da contatti, sono previste le seguenti alternative di montaggio:

- Montaggio in un quadro elettrico idoneo
- Montaggio in involucro idoneo
- Montaggio in un locale chiuso appositamente predisposto.

Prima del montaggio e della messa in servizio

⚠CAUTELA

Leggere il manuale di sistema "Sistema di automazione S7-1200"

Prima del montaggio leggere i passi relativi al collegamento e alla messa in servizio nel manuale di sistema "S7-1200 Sistema di automazione", vedere riferimento bibliografico nell'appendice.

Durante il montaggio e il collegamento procedere in base alle descrizioni riportate nel manuale di sistema "S7-1200 Sistema di automazione".

Estrazione/inserimento dell'unità

ATTENZIONE

Spegnimento della stazione durante l'estrazione/inserimento dell'unità

Prima dell'estrazione o dell'inserimento dell'unità disinserire sempre la tensione di alimentazione.

Dimensioni per il montaggio

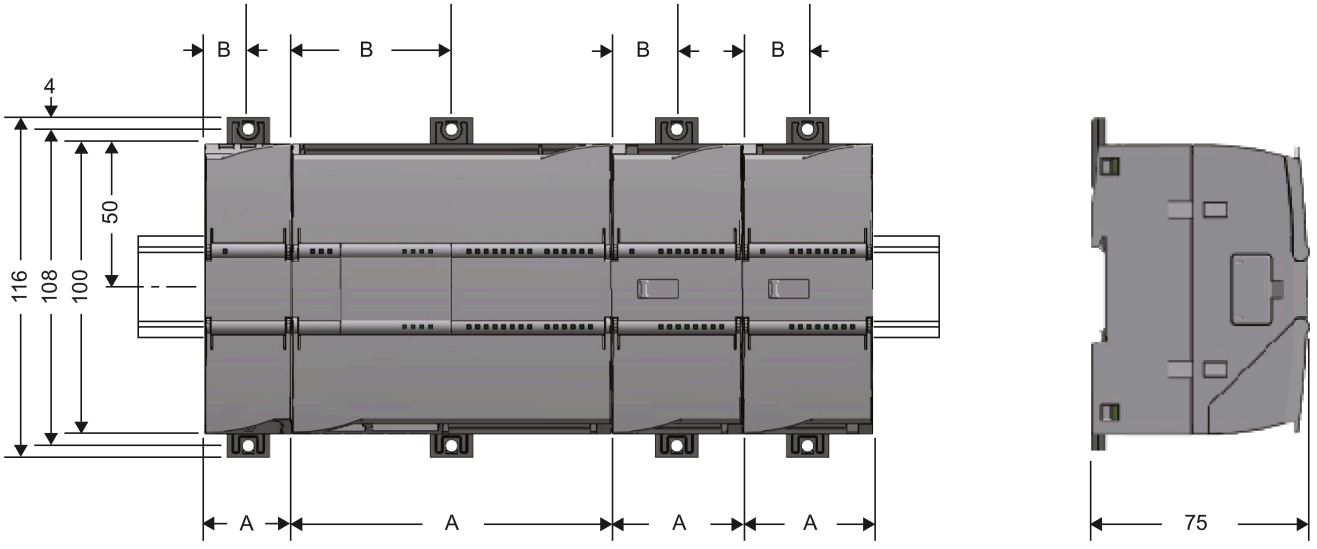


Figura 3-1 Dimensioni di montaggio dell'S7-1200

Tabella 3- 1 Dimensioni per il montaggio (mm)

Apparecchi S7-1200		**Larghezza A**	**Larghezza B ***
CPU (esempi)	CPU 1211C, CPU 1212C	90 mm	45 mm
	CPU 1214C	110 mm	55 mm

Apparecchi S7-1200		**Larghezza A**	**Larghezza B ***
Interfacce di comunicazione (esempi)	CM 1241, CM 1243-5, CM 1242-5	30 mm	15 mm
	CP 1242-7, CP 1243-1, CP 1243-7, CP 1243-8 IRC	30 mm	15 mm

* Larghezza B: Misura tra i bordo del contenitore e il centro del foro del morsetto guida ad U

Le dimensioni dettagliate si trovano nel capitolo Disegni quotati (Pagina 105).

Morsetti della guida, montaggio a incasso

Tutte le CPU, le SM, i CM e i CP possono essere montati su una guida standard DIN (35 mm) nel quadro elettrico. Per il fissaggio dell'apparecchio sulla guida ad U estraibile impiegare morsetti per guida ad U. Questi morsetti scattano anche in una posizione estratta per consentire il montaggio dell'apparecchio in un pannello di comando. La misura interna del foro per i morsetti della guida ad U è 4,3 mm.

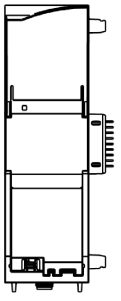
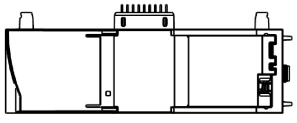
Posizione di montaggio

ATTENZIONE

Posizione di montaggio

Il montaggio deve essere eseguito in modo che gli intagli di ventilazione superiori e inferiori dell'unità non vengano coperti e che sia possibile un buon passaggio di aria. Sopra e sotto l'apparecchio deve esserci uno spazio libero di 25 mm per la circolazione dell'aria per prevenire il surriscaldamento dell'apparecchio.

Attenersi ai campi di temperatura ammessi in funzione della posizione di montaggio. I campi di temperatura ammessi si trovano nel capitolo Dati tecnici del CP 1243-1 (Pagina 97).

Posizione di montaggio / campo di temperatura ammesso	**Posizione di montaggio**
Struttura orizzontale del telaio di montaggio	
Struttura verticale del telaio di montaggio:	

⚠AVVERTENZA

Tensione di alimentazione

Il dispositivo 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).

Di conseguenza l'alimentazione deve soddisfare almeno una delle seguenti condizioni:

- Agli attacchi di alimentazione 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 o IEC 62368-1 / EN 62368-1 / VDE 62368-1.
- L'alimentatore per l'alimentazione del dispositivo deve essere conforme a NEC Class 2 secondo il National Electrical Code (r) (ANSI / NFPA 70).

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

Presupposto: Progettazione prima della messa in servizio

Il requisito per la messa in servizio completa dell'unità è l'integrità dei dati del progetto STEP 7 (vedere in basso, passo 5).

Montaggio, collegamento e messa in servizio dell'unità

Nota

Collegamento in assenza di tensione

Cablare l'S7-1200 solo in assenza di tensione.

Tabella 3- 2 Procedimento per il montaggio e il collegamento

Fase	Esecuzione	Avvertenze e descrizioni
1	Innestare il CP sulla guida ad U e collegarlo con l'unità adiacente alla sua destra.	Utilizzare una guida ad U DIN di 35 mm. Sono ammessi i posti connettore a sinistra di fianco alla CPU.
2	Fissare la guida ad U.	
3	Collegare il cavo Ethernet al CP.	L'assegnazione dei pin dell'interfaccia si trova nel capitolo Dati tecnici (Pagina 97).
4	Inserire l'alimentazione.	

Fase	Esecuzione	Avvertenze e descrizioni
5	L'ulteriore messa in servizio comprende il caricamento dei dati del progetto STEP 7.	I dati del progetto STEP 7 del CP vengono trasmessi durante il caricamento della stazione. Per caricare la stazione collegare la engineering station che si trova nei dati del progetto all'interfaccia Ethernet della CPU. Per ulteriori dettagli sul caricamento consultare i seguenti capitoli del sistema di informazione di STEP 7: • "Carica dati del progetto" • "Utilizza funzioni online e funzioni di diagnostica"

Impostazione manuale dell'ora durante la messa in servizio

Nota

Sincronizzazione dell'ora in caso di utilizzo di Security / SINEMA RC

In caso di utilizzo di funzioni Security, ad es SINEMA Remote Connect, il CP necessita dell'ora attuale per l'autenticazione nei partner o nel server SINEMA RC.

Il CP rileva l'ora dalla CPU o da un server NTP prima della prima realizzazione del collegamento.

Raccomandazione:

Durante la messa in servizio impostare almeno una volta manualmente l'ora della CPU tramite le funzioni online di STEP 7. Questo è necessario in particolare, se per la sincronizzazione dell'ora è stata progettata l'opzione "Ora del partner". In questo modo si garantisce che la CPU abbia un'ora valida durante l'avvio della stazione e che il CP possa scambiare i certificati necessari con il partner o il server SINEMA RC.

3.4 Avvertenza per il funzionamento

ATTENZIONE
Chiusura del frontalino Per garantire un funzionamento senza guasti tenere il frontalino dell'unità chiuso durante il funzionamento.

3.5 Smontaggio

⚠AVVERTENZA

Smontaggio errato

In caso di smontaggio errato in un'area a rischio di esplosione sussiste pericolo di esplosione.

Per uno smontaggio corretto osservare quanto segue:

- Prima dell'inizio dei lavori assicurarsi che l'elettricità sia disattivata.
- Proteggere i collegamenti restati in modo che in caso di avvio accidentale dell'impianto non possano verificarsi danni come conseguenza dello smontaggio.

Smontaggio

1. Estrarre il connettore del cavo di dati dal dispositivo, prima di disinserire l'alimentazione e staccare di conseguenza il collegamento di terra dei dispositivi.
2. Disinserire l'alimentazione della stazione.
3. Tirare verso il basso nella posizione estratta entrambe le clip inferiori della guida ad U sul lato posteriore dei dispositivi utilizzando un cacciavite ad intaglio.

   In questo modo si allenta il meccanismo di bloccaggio.
4. Ruotare in avanti i dispositivi per estrarli dal profilo della guida ad U.

Progettazione

4

4.1 Raccomandazioni Security

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

Con la comunicazione Telecontrol attivata osservare anche le avvertenze nel rispettivo manuale di progettazione.

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.
- Tenersi regolarmente informati sulle novità sulle pagine Internet Siemens.
  - Qui si trovano informazioni relative a Industrial Security:
    Link: (http://www.siemens.com/industrialsecurity)
  - In
    Link: (https://support.industry.siemens.com/cs/ww/it/view/92651441) si trova una selezione di documenti relativi all'argomento Sicurezza della rete
- Tenere aggiornato il firmware. Tenersi regolarmente informati sugli aggiornamenti di sicurezza del firmware e adottarli.

  Avvertenze sulle novità del prodotto e le nuove versione firmware si trovano al seguente indirizzo:
  Link: (https://support.industry.siemens.com/cs/ww/it/ps/21764/dl)

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.

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.

- Funzioni di sicurezza della comunicazione
  - Attivare le funzioni di sicurezza 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. Limitando la "velocità di trasmissione" nel firewall tramite le regole filtro pacchetto IP, si utilizza la possibilità di limitare attacchi flooding e DoS.
  - Utilizzare le varianti di protocollo sicure NTP (secure) e SNMPv3.
  - Utilizzare le funzioni Security dei protocolli Telecontrol.
  - Disattivare l'accesso al Web server della CPU.
- 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 di sicurezza 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 se non si utilizza la comunicazione Telecontrol.
  - Il protocollo HTTP con HTTPS offre un'alternativa sicura in caso di accesso al server web (progettazione nella CPU).

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**
  - Aperta

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

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

    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.
- **Autenticazione**

  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
DNP3	20000 (TCP/UDP) impostabile	Chiusa	Aperta dopo la configurazione	Sì, se Secure Authentication è attivata.
IEC	2404 (TCP) impostabile	Chiusa	Aperta	No
Collegamenti S7 e online	102 (TCP)	Chiusa	Aperta dopo la configurazione *	No
Diagnostica Security online (se supportata)	102 (TCP)	Aperta	Aperta dopo la configurazione *	No
Comunicazione tramite SINEMA RC (se supportata)	443 (TCP)	Chiusa	Aperta dopo la configurazione	Sì
HTTP	80 (TCP)	Chiusa	Aperta dopo la configurazione	Sì
HTTPS	443 (TCP)	Chiusa	Aperta dopo la configurazione	Sì
SNMP (se supportato)	161 (UDP)	Aperta	Aperta dopo la configurazione	Sì (in SNMPv3)
Syslog	514 (UDP)	Chiusa	Aperta dopo la configurazione	No

***** Alcuni provider del servizio contestano l'apertura della porta 102 come vulnerabilità. Per evitare l'apertura della porta 102 durante la diagnostica online vedere il capitolo Diagnostica Security online tramite porta 8448 (Pagina 91).

Porte dei partner di comunicazione e dei router

Fare attenzione ad abilitare le porte client necessarie nel firewall corrispondente nei partner di comunicazione e nei router intermedi.

Queste possono essere, se supportate o utilizzate:

- TeleControl Basic / 55097 (TCP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- SINEMA RC Autoconfigurazione / 443 (TCP) - impostabile
- SINEMA RC e OpenVPN / 1194 (UDP) - impostabile in SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)
- Syslog / 514 (UDP)

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 24).

Per ogni stazione è possibile progettare massimo tre CM/CP.

La seguente descrizione vale per casi applicativi senza comunicazione Telecontrol.

Progettazione della comunicazione Telecontrol

La descrizione relativa alla progettazione della comunicazione Telecontrol si trova nei manuali di progettazione /4/ (Pagina 108).

Panoramica dei passi di progettazione in STEP 7

Per la progettazione procedere nel modo seguente:

1. Creare un progetto STEP 7.
2. Creare le stazioni SIMATIC necessarie con i moduli e i CP necessari.
3. Creare una rete Ethernet.
4. Collegare le stazioni con la sottorete Ethernet.
5. Progettare i CP compresi i messaggi (e-mail).
6. Se richiesto, creare i blocchi di programma per la comunicazione S7 e la Open User Communication e parametrizzarli.
7. Salvataggio e compilazione del progetto.
8. Caricare i dati del progetto nelle stazioni

   Tramite la funzione "Carica nel dispositivo" i dati del progetto STEP 7 compresi i dati di progettazione dei PC vengono caricati nella rispettiva CPU.

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

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 Tipi di comunicazione

Gruppo di parametri "Tipi di comunicazione"

In questo gruppo di parametri si attivano i servizi di comunicazione del CP.

Per ridurre al minimo il rischio di accessi non autorizzati alla stazione, è necessario attivare singolarmente i servizi di comunicazione che il CP deve eseguire. Possono essere attivate tutte le opzioni, ma deve essere attivata almeno un'opzione.

- **Attiva comunicazione Telecontrol**

  Abilita la comunicazione Telecontrol nel CP.

  Selezionare il protocollo Telecontrol tramite la casella di riepilogo "Tipo di protocollo".

  – TeleControl Basic

  – DNP3

  – IEC 60870-5

  Osservare che in caso di una modifica successiva del protocollo Telecontrol vengono cancellati tutti i dati specifici del protocollo. Di questi fanno parte inoltre informazioni sul punto di accesso ai dati e sul partner.

  Ulteriori informazioni si trovano nei manuali di progettazione /4/ (Pagina 108).

- **Attiva comunicazione Telecontrol tramite SINEMA Remote Connect**

  Abilita nel CP la comunicazione tramite SINEMA RS.

  I casi applicativi di SINEMA Remote Connect e le avvertenze di progettazione per queste applicazioni si trovano nel capitolo SINEMA Remote Connect (Pagina 68).

  Ulteriori informazioni si trovano nei manuali di progettazione /4/ (Pagina 108).

  Per il manuale SINEMA Remote Connect - Server vedere /6/ (Pagina 108).

- **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 le funzioni della comunicazione S7 tra la stazione di engineering e la CPU della stazione nonché il routing S7.

  Se si progettano collegamenti S7 con questa stazione che devono funzionare tramite il modulo di comunicazione, questa opzione deve essere attivata nel modulo di comunicazione.

  Osservare:
  la disattivazione della funzione non richiede misure Security. Per la protezione della stazione utilizzare funzioni Security adatte quali Firewall, VPN o protezione password della CPU.

La Open User Communication non deve essere abilitata in quanto per questo deve essere creato in modo attivo il blocco di programma corrispondente. In questo modo non è possibile un accesso involontario al CP.

4.4 Sincronizzazione dell'ora

Nota

Sincronizzazione dell'ora in caso di utilizzo di SINEMA RC

Se il CP rileva l'ora dalla CPU, in caso di utilizzo di SINEMA Remote Connect impostare manualmente l'ora della CPU durante la messa in servizio, vedere l'avvertenza nel capitolo Montaggio, collegamento e messa in servizio (Pagina 35).

Nota

Sincronizzazione dell'ora del CP

Nelle applicazioni che richiedono una sincronizzazione dell'ora, l'ora del CP deve essere sincronizzata regolarmente. Se non si sincronizza regolarmente l'ora del CP, nell'indicazione dell'ora del CP possono verificarsi degli scostamenti di alcuni secondi al giorno.

Con le funzioni Security attivate è necessario attivare la sincronizzazione dell'ora.

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 UTC.

Sincronizzazione dell'ora nell'S7-1200

In caso di utilizzo di una sorgente dell'ora la stazione S7-1200 può rilevare l'ora attuale sia tramite la CPU sia tramite un CP.

Nota

Raccomandazione: Sincronizzazione dell'ora solo attraverso 1 modulo

Far sincronizzare l'ora della stazione da una sorgente dell'ora esterna solo attraverso un singolo modulo della stazione per mantenere un'ora coerente all'interno della stazione.

Se la CPU acquisisce l'ora dal CP disattivare la sincronizzazione dell'ora dalla CPU.

Un inoltro dell'ora dalla stazione alla sottorete non viene eseguito nell'S7-1200.

Gruppi di parametri per la sincronizzazione dell'ora

La sincronizzazione dell'ora si può progettare nei seguenti gruppi di parametri:

- **Interfaccia Ethernet**

  Eseguire qui la progettazione alle seguenti condizioni:

  – La comunicazione Telecontrol è disattivata.

  – Le funzioni Security sono disattivate.

- **Security**

  Qui si esegue la progettazione se sono attivate le funzioni Security.

Dipendenza del procedimento di sincronizzazione dall'utilizzo del CP

In base all'utilizzo della comunicazione Telecontrol o delle funzioni Security possono essere selezionati i seguenti procedimenti di sincronizzazione:

- **Comunicazione Telecontrol disattivata, Security disattivata**
  – NTP
  – Ora della CPU
- **Comunicazione Telecontrol disattivata, Security attivata**
  – NTP
  – NTP (secure)
  – Ora della CPU
- **Comunicazione Telecontrol e Security attivate**
  – Ora del partner
  – NTP
  – NTP (secure)
  – Ora della CPU

Metodo di sincronizzazione del CP

Il CP supporta i seguenti procedimenti della sincronizzazione dell'ora:

- **NTP**

  L'ora viene sincronizzata da un server NTP nella rete collegata.

  Il procedimento essere utilizzato anche se la comunicazione Telecontrol è attivata.

  Nei CP a partire dalla versione firmware V3 l'indirizzo del server NTP può essere inserito anche come URL, ad es. <ntp.server.com>. A riguardo è necessario un server DNS.

- **NTP (secure)**

  Con le funzioni Security attivate è disponibile anche il procedimento protetto NTP (secure). Il procedimento protetto utilizza l'autenticazione tramite chiave simmetrica. Per il controllo dell'integrità sono disponibili diversi algoritmi Hash.

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

  Definire nel CP i server utilizzati.

- **Ora della CPU**

  La CPU a partire da V4.2 può sincronizzare tutti i CM/CP della stazione in un ciclo di sincronizzazione di 10 secondi.

  Parametri della CPU:
  tramite l'opzione "CPU sincronizza i moduli del dispositivo" è possibile consentire che tutti i CP Telecontrol della stazione vengano sincronizzati con il firmware ≥ V2.1.77 in un ciclo di sincronizzazione di 10 secondi con l'ora della CPU.

- **Nessuna sincronizzazione dell'ora progettata**

  Se nel CP non è progettata una sincronizzazione dell'ora, l'ora del CP può essere sincronizzata alle seguenti condizioni:

  Se nella CPU in "Interfaccia PROFINET > Sincronizzazione dell'ora" è attivata l'opzione "CPU sincronizza i moduli del dispositivo" tutti i CM/CP della stazione vengano sincronizzati con l'ora della CPU.

- **Ora del partner**

  Solo con la comunicazione Telecontrol attivata: Il CP acquisisce l'ora dal partner di comunicazione.

  La descrizione si trova nel manuale di progettazione /4/ (Pagina 108).

Inoltro dell'ora dal CP alla CPU

Nota

Inoltro dell'ora alla CPU

In base alla versione firmware dei moduli interessati l'ora del CP viene inoltrata diversamente alla CPU:

- Inoltro dell'ora del CP alla CPU tramite una variabile PLC
- Inoltro dell'ora del CP alla CPU tramite il bus backplane

L'inoltro dell'ora del CP alla CPU dipende dalla versione firmware del CP e della CPU. Osservare il seguente comportamento.

- **Firmware CP < V3**

  Con questa versione di firmware l'ora del CP può essere messa a disposizione della CPU opzionalmente tramite una variabile PLC. Se la CPU legge ciclicamente questa variabile PLC, la CPU acquisisce l'ora del CP.

  Nel gruppo di parametri "Comunicazione con la CPU" è possibile impostare se l'ora attuale del CP della CPU deve essere messa a disposizione tramite una variabile PLC. Per le variabili PLC vedere il gruppo di parametri "Comunicazione con la CPU" del CP.

- **Firmware CP ≥ V3.0 e firmware CPU ≥ V4.2**

  Se entrambi i moduli in una stazione presentano una delle versioni di firmware indicate, l'ora del CP può essere inoltrata automaticamente alla CPU.

  La condizione è: Nella CPU in "Interfaccia PROFINET > Sincronizzazione dell'ora" è attivata l'opzione "CPU sincronizza i modulo del dispositivo".

  Successivamente tutti i moduli intelligenti della stazione vengono sincronizzati con questa ora della CPU.

  Poiché la CPU acquisisce automaticamente l'ora del CP, non è più necessaria l'opzione di inoltro tramite la variabile PLC.

4.5 Interfaccia Ethernet

4.5.1 Indirizzi Ethernet

Indirizzi Ethernet

Nei seguenti gruppi di parametri collegare in rete l'interfaccia Ethernet e progettare i parametri di indirizzo IP.

Osservare:
Per le seguenti applicazioni è necessario un indirizzo IP fisso (IPv4/IPv6):

- In caso di utilizzo della comunicazione S7
- In caso di ricezione di dati tramite Open User Communication
- In caso di utilizzo di VPN
- In caso di utilizzo di SINEMA Remote Connect

Nei gruppi di parametri in Opzioni avanzate > Porta [Xn P1] è possibile progettare le interconnessioni alla porta e le proprietà di trasmissione.

Ulteriori informazioni si trovano nel sistema di informazione STEP 7.

4.5.2 IPv6

Configurazione manuale di indirizzi IPv6

Se si progettano indirizzi IPv6 supplementari (opzione "Configurazione manuale"), assicurarsi che entrambi gli indirizzi IPv6 appartengano a sottoreti diverse.

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

Partner di comunicazione e IPv6

Nota

Comunicazione Internet 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.

Comunicazione OUC tramite IPv6

Se si utilizzano i blocchi della Open User Communication e si attiva IPv6, assicurarsi che anche i partner di comunicazione supportino IPv6. In caso di richieste al server DNS gli indirizzi restituiti utilizzano gli indirizzi IPv6 con priorità sugli indirizzi IPv4.

4.5.3 Identificazione CP

Il gruppo di parametri è disponibile solo con la comunicazione Telecontrol attivata. Ulteriori informazioni si trovano nei manuali di progettazione /4/ (Pagina 108).

4.5.4 Sincronizzazione dell'ora

Sincronizzazione dell'ora

Per la progettazione della sincronizzazione dell'ora leggere il capitolo riportato sopra Sincronizzazione dell'ora (Pagina 47).

4.5.5 Opzioni avanzate

Sorveglianza del collegamento TCP

Le impostazioni qui eseguite valgono globalmente per tutti i collegamenti TCP del CP.

- **Tempo di sorveglianza del collegamento TCP**

  Funzione: Se non vengono scambiati dati entro il Tempo di sorveglianza del collegamento TCP il modulo di comunicazione invia un telegramma keep alive al partner di comunicazione e attende la risposta da questo partner entro il Tempo di sorveglianza keep alive TCP.

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

- **Tempo di sorveglianza keep alive TCP**

  Dopo la trasmissione di un telegramma keep alive il modulo di comunicazione attende una risposta dal partner di comunicazione entro il tempo di sorveglianza keep alive. Se il modulo non riceve una risposta entro il tempo progettato, interrompe il collegamento e tenta di realizzarlo di nuovo.

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

Impostazioni di trasmissione

Le impostazioni di trasmissione specifiche per il protocollo sono visibili solo con la comunicazione Telecontrol attivata. Ulteriori informazioni si trovano nei manuali di progettazione /4/ (Pagina 108).

4.5.6 Accesso al Web server

Accesso al server web della CPU

Il Web server di una stazione S7-1200 si trova nella CPU. Tramite il CP si dispone dell'accesso al server web della CPU.

Da un PC è possibile accedere al server web della stazione tramite LAN.

Informazioni sul Web server si trovano nel manuale /1/ (Pagina 107).

Per particolarità dell'accesso al server web in caso di utilizzo del protocollo TeleControl Basic consultare il manuale di progettazione /4/ (Pagina 108).

Ulteriori informazioni sul Web server dell'S7-1200 si trovano nel manuale /1/ (Pagina 107).

4.6 Stazioni partner

Il gruppo di parametri viene visualizzato solo con la comunicazione Telecontrol attivata.

4.7 Configurazione DNS

DNS Server

Un server DNS può essere necessario se il modulo stesso, un partner di comunicazione o ad es. un server NTP o e-mail devono essere raggiungibili tramite un nome host (FQDN).

In caso di indirizzamento di un partner di comunicazione come FQDN è necessario progettare un server DNS. L'indirizzo IP (IPv4/IPv6) del partner di comunicazione viene rilevato tramite il server DNS progettato.

In caso di utilizzo di indirizzi IPv6 osservare la progettazione corrispondente del server DNS.

4.8 Comunicazione con la CPU

4.8.1 Comunicazione con la CPU

Comunicazione con la CPU

I primi 4 parametri sono rilevanti solo per la comunicazione Telecontrol.

Bit watchdog

- **Sorveglianza CP**

  Tramite il bit del watchdog il CP controlla il collegamento con la CPU.

  Il CP trasmette il bit ogni 5 secondi alla CPU e lo resetta nel successivo ciclo di campionamento della CPU. In caso di disturbi del collegamento il bit non viene trasmesso. In questo modo alla CPU viene segnalato il disturbo del collegamento.

  La variabile PLC del bit Watchdog deve essere valutata dal programma utente.

Ora CP

- **Ora CP alla CPU**

  La funzione consente alla CPU di leggere l'ora del CP. Tramite questo percorso il CP può sincronizzare l'ora della CPU.

  Procedura:

  – La CPU imposta l'ingresso "Variabile del trigger dell'ora" (BOOL) su 1 tramite il programma utente.

  – Il CP scrive di conseguenza la relativa ora nella "Variabile dell'ora del CP" (DTL) e imposta il valore della "Variabile del trigger dell'ora" di nuovo a 0.

  – Il programma utente legge la "Variabile dell'ora del CP" per l'impostazione dell'ora della CPU.

  Raccomandazione:
  Non impostare la "Variabile del trigger dell'ora" più di una volta al secondo per non caricare inutilmente il bus backplane con la comunicazione.

Nota

Osservare le avvertenze nel capitolo Sincronizzazione dell'ora (Pagina 47).

4.8.2 Diagnostica CP

Le funzioni sono supportate da un CP a partire dalla versione firmware V3.

Diagnostica CP

Nel gruppo di parametri "Diagnostica CP" esiste la possibilità di mettere a disposizione della CPU dati di diagnostica avanzati del CP tramite le variabili PLC.

Gli stati delle variabili PLC possono essere visualizzati tramite il server web della CPU.

- **Attiva diagnostica CP avanzata**

  Attivare l'opzione per utilizzare la diagnostica CP avanzata.

  Con l'opzione attivata deve essere progettata almeno la "Variabile di trigger della diagnostica".

  Le seguenti variabili PLC per i singoli dati di diagnostica possono essere attivate in modo selettivo.

- **Variabile di trigger della diagnostica**

  Se dal programma utente della CPU la variabile PLC (BOOL) viene impostata su 1, il CP aggiorna i valori delle variabili PLC successive per la diagnostica avanzata.

  Dopo la scrittura dei valori attuali nelle seguenti variabili PLC successive, il CP imposta la "Variabile di trigger della diagnostica" su 0 e segnala quindi alla CPU che i valori aggiornati possono essere letti dalle variabili PLC.

  Nota

  Impostazione rapida della variabile di attivazione della diagnostica

  È consigliabile non impostare i trigger più di una volta al secondo.

A seconda del tipo di CP e delle funzioni supportate, possono essere progettate variabili PLC per i seguenti dati di diagnostica:

- **Avviso di superamento della memoria dei telegrammi**

  - Rilevante solo per la comunicazione Telecontrol -

- **Assegnazione della memoria dei telegrammi**

  - Rilevante solo per la comunicazione Telecontrol -

- **Indirizzo IP corrente**

  Variabile PLC (tipo di dati stringa) per l'indirizzo IP attuale dell'interfaccia del CP

- **Data longin riuscito nel TCSB**

  - Rilevante solo per la comunicazione Telecontrol -

- **Data longin non riuscito nel TCSB**

  - Rilevante solo per la comunicazione Telecontrol -

- **Stato TeleService**

  - Rilevante solo per la comunicazione Telecontrol -

- **Stato VPN-IPsec**

  La variabile PLC (BOOL) indica se è realizzato un tunnel VPN-IPsec:

  – 0 = nessun tunnel realizzato

  – 1 = tunnel realizzato

- **Collegamento con SINEMA Remote Connect**

  La variabile PLC (BOOL) indica se è realizzato un tunnel OpenVPN verso SINEMA RC:

  – 0 = nessun tunnel realizzato

  – 1 = tunnel realizzato

4.9 SNMP

Il CP supporta le seguenti versioni SNMP:

- **SNMPv1**

  Disponibile con funzioni Security attivate e disattivate.

  Osservare che in questo modo è possibile l'accesso in lettura e in scrittura alle unità. In questo caso non sono possibili altre impostazioni.

  La progettazione delle stringhe Community è possibile solo con le funzioni Security attivate.

  Nella preimpostazione il CP utilizza le seguenti stringhe Community per l'autenticazione dell'accesso tramite SNMPv1 sui relativi SNMP Agent:

Accesso a SNMP Agent nel CP	Stringa Community per l'autenticazione con SNMPv1 *)
Accesso per lettura	public
Accesso per lettura e per scrittura	private

*) Osservare il tipo di scrittura con lettere minuscole!

Nota

Sicurezza dell'accesso

Per motivi di sicurezza modificare le stringe preimpostate e generali note "public" e "private".

Con funzioni Security attivate sono progettabili le stringe Community.

- **SNMPv3**

  Disponibile solo con attivazione delle funzioni Security

  Per la progettazione di SNMPv3 vedere il capitolo SNMP (Pagina 62).

Progettazione

- **"Attiva SNMP"**

  Con l'opzione attivata, nel CP viene abilitata la comunicazione tramite SNMPv1.

  Con l'opzione disattivata alle richieste dei client SNMP il CP non risponde né tramite SNMPv1 né tramite SNMPv3.

4.10 Security

La possibilità di progettazione delle singole opzioni dipende dal protocollo Telecontrol utilizzato.

Una panoramica dell'ambito e dell'applicazione delle funzioni Security del CP si trova nel capitolo Funzioni Security (Pagina 18).

Per la struttura d'insieme delle funzioni Security vedere il capitolo Limiti di configurazione e dati utili (Pagina 20).

Per attivare le funzioni Security è necessario creare un utente Security, vedere capitolo Utente Security (Pagina 57).

4.10.1 Utente Security

Creazione di un utente Security

Per poter progettare le funzioni Security sono necessari i diritti di progettazione corrispondenti. Per questa operazione è necessario creare almeno un utente Security con i diritti corrispondenti.

Navigare alle impostazioni Security globali > "Utenti e ruoli" > scheda "Utenti".

1. Creare un utente e progettare i parametri.
2. Assegnare a questo utente nell'area sottostante "Ruoli assegnati" i ruoli "NET Standard" o "NET Administrator".

Dopo il login nel progetto STEP 7 questo utente può eseguire le impostazioni necessarie.

Eseguire anche in futuro il login ai parametri Security come utente di questo tipo.

4.10.2 Panoramica dei parametri

Gruppi di parametri

Nelle funzioni Security attivate del CP si trovano i seguenti gruppi di parametri per la progettazione del CP:

- **Identificazione CP**

  Solo nel protocollo TeleControl Basic

  Qui si progettano i parametri per l'autenticazione del CP sul server Telecontrol: I dettagli relativi ai parametri si trovano di seguito.

- **Opzioni Security DNP3**

  Solo nel protocollo DNP3

  Qui si progettano le funzioni Security specifiche per il protocollo. I dettagli relativi ai parametri si trovano di seguito.

- **Firewall**

  Vedere il capitolo Firewall (Pagina 58).

- **Sincronizzazione dell'ora**

  Per la progettazione della sincronizzazione dell'ora leggere il capitolo riportato sopra Sincronizzazione dell'ora (Pagina 47).

- **Progettazione delle e-mail**

  Vedere il capitolo Progettazione delle e-mail (Pagina 60).

- **Impostazioni Log**

  Qui si eseguono le impostazioni per il protocollo di eventi rilevanti per Security.

  Vedere il capitolo Impostazioni Log - Filtraggio degli eventi di sistema (Pagina 61).

- **SNMP**

  Qui si eseguono le impostazioni per le impostazioni di il protocollo di SNMP Agent nel CP.

  Vedere il capitolo SNMP (Pagina 62).

- **Manager dei certificati**

  Vedere il capitolo Manager dei certificati (Pagina 71).

Nelle impostazioni Security globali di STEP 7 si trovano inoltre i seguenti gruppi di parametri:

- **Gruppi VPN**

  Qui si esegue la progettazione della comunicazione VPN, vedere il capitolo VPN (Pagina 63).

- **Gestione utenti**

  Qui si esegue la progettazione di utenti, ruoli e diritti.

4.10.3 Firewall

4.10.3.1 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.

4.10.3.2 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.

4.10.3.3 Impostazioni firewall per collegamenti progettati via tunnel VPN

Regole IP in modalità firewall estesa

Se si configurano collegamenti progettati 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*".

Vedere a riguardo il capitolo Impostazioni per la diagnostica Security online e caricamento nella stazione con il firewall attivato (Pagina 59).

4.10.3.4 Impostazioni per la diagnostica Security online e caricamento nella stazione con il firewall attivato

Impostare il firewall per le funzioni online

Con le funzioni Security attivate procedere nel modo seguente.

Funzioni Security globali:

1. Selezionare 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".

Funzioni Security locali del CP:

Selezionare quindi il CP nella stazione S7.

1. Attivare la modalità firewall estesa nelle impostazioni locali Security del CP nel gruppo di parametri "Security > Firewall".
2. Aprire il gruppo di parametri "Regole IP".
3. Inserire nella tabella rispettivamente una nuova regola IP per i servizi precedentemente creati in modo globale nel modo seguente:
   - Azione: Accept; Da: Esterno; A: Stazione; servizio > Servizio ICMPv4/6 > Echo Request (del servizio globale precedentemente creato)
   - Azione: Accept; Da: Stazione; A: Esterno; servizio > Servizio ICMPv4/6 > Echo Reply (del servizio globale precedentemente creato)
4. Inserire per la regola IP relativa al servizio "Echo Request" "Indirizzo IP della stazione di engineering in "Indirizzo IP sorgente".

Con queste regole il CP può essere raggiunto dalla stazione di engineering solo con pacchetti ICMP (ping) tramite il firewall.

Nota

Ulteriori servizi per la diagnostica Security online e caricamento

Se si vogliono utilizzare le funzioni "Diagnostica Security online" o "Carica nel dispositivo", è necessario creare regole supplementari o disattivare i servizi "Echo Request" / "Echo Reply".

4.10.4 Progettazione delle e-mail

Progettazione di e-mail in STEP 7

Per eventi particolari, ad es. STOP CPU, il CP può inviare e-mail. Questo avviene indipendentemente dall'utilizzo della comunicazione Telecontrol.

In caso di utilizzo della comunicazione Telecontrol, gli eventi supplementari progettabili nell'immagine di processo della CPU possono attivare l'invio di e-mail. Insieme alla e-mail possono essere inviati dati di processo.

Le singole e-mail devono essere progettate nell'editor dei messaggi (voce "Messaggi"), vedere capitolo Messaggi (Pagina 74).

Requisiti per e-mail

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

- le funzioni Security sono attivate.
- l'ora del CP è sincronizzata.

Per la progettazione sono necessari i dati del server SMTP e dell'account utente:

- Indirizzo server, numero di porta, nome utente, password, indirizzo e-mail del mittente (CP)
- In caso di trasmissione criptata: Certificato server

Progettazione delle e-mail

Nell'impostazione standard della porta SMTP 25 l'unità trasmette e-mail non codificate.

Se il provider del servizio e-mail supporta solo la trasmissione codificata, utilizzare una delle seguenti opzioni:

- N. porta 587

  Utilizzando STARTTLS l'unità invia e-mail codificate al server SMTP del proprio provider del servizio e-mail.

  Raccomandazione: Se il provider di e-mail offre entrambe le possibilità (STARTTLS / SSL/TLS) è necessario utilizzare STARTTLS con la porta 587.

- N. porta 465

  Utilizzando SSL/TLS (SMTPS) l'unità invia e-mail codificate al server SMTP del proprio provider del servizio e-mail.

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

Importazione del certificato con trasmissione codificata

Per poter utilizzare una trasmissione codificata è necessario caricare il certificato del proprio account e-mail nel manager dei certificati di STEP 7. Il certificato si riceve dal proprio provider del servizio e-mail.

Utilizzare il certificato tramite i seguenti passi:

1. Salvare il certificato del proprio provider del servizio e-mail nel sistema di file della stazione di engineering.
2. Importare il certificato nel progetto STEP 7 tramite "Impostazioni Security globali > Manager dei certificati".
3. Impiegare il certificato importato in ciascuna unità che utilizza e-mail codificate, tramite la tabella "Manager dei certificati" nel gruppo di parametri locali "Security".

Per il procedimento vedere il capitolo Utilizzo di certificati (Pagina 71).

4.10.5 Impostazioni Log - 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.

4.10.6 SNMP

SNMP

La potenzialità del CP con SNMP si trovano nel capitolo SNMP (Pagina 92).

Con le funzioni Security attivate esistono le seguenti possibilità di selezione e di impostazione.

SNMP

- **"Attiva SNMP"**

  Con l'opzione attivata, nel dispositivo viene abilitata la comunicazione tramite SNMP. Nella preimpostazione è attivato SNMPv1.

  Con l'opzione disattivata alle richieste del client SNMP non perviene risposta né tramite SNMPv1 né tramite SNMPv3.

- **"Utilizza SNMPv1"**

  Attiva l'utilizzo di SNMPv1 per il CP. Per la progettazione delle stringhe Community necessarie vedere in basso (SNMPv1).

- **"Utilizza SNMPv3"**

  Attiva l'utilizzo di SNMPv3 per il CP. Per la progettazione degli algoritmi necessari vedere in basso (SNMPv3).

SNMPv1

In caso di richieste al CP è necessario inviare insieme le stringhe Community tramite SNMPv1.

- **"Stringa Community in lettura"**

  La stringa è necessaria per l'accesso in lettura.

  Lasciare invariata la stringa preimpostata "public" oppure progettare una stringa.

- **"Consenti accesso in scrittura"**

  Attivando l'opzione viene abilitato l'accesso in scrittura al CP e la rispettiva stringa Community diventa editabile.

- **"Stringa Community in scrittura"**

  La stringa è necessaria per l'accesso in scrittura e può essere utilizzata anche per l'accesso in lettura.

  Lasciare invariata la stringa preimpostata "private" oppure progettare una stringa.

Osservare il tipo di scrittura delle stringhe Community preimpostate con lettere minuscole!

Nota

Sicurezza dell'accesso

Per motivi di sicurezza modificare le stringe generalmente note "public" e "private".

SNMPv3

Per l'accesso codificato al CP gli algoritmi devono essere protettati tramite SNMPv3.

- **"Algoritmo di autenticazione"**

  Selezionare nella casella di riepilogo il metodo di autenticazione da utilizzare.

- **"Algoritmo di codifica"**

  Selezionare nella casella di riepilogo il metodo di codifica da utilizzare.

  Osservare le esecuzioni per la sicurezza degli algoritmi possibili nella guida in linea.

Gestione utenti

Nella gestione utenti, che si trova nelle impostazioni Security globali, si assegnano ai diversi utenti i relativi ruoli.

Nelle proprietà dei ruoli si trova l'elenco dei diritti dei rispettivi ruoli, ad esempio i diversi tipi di accesso tramite SNMP. Per i nuovi ruoli è possibile progettare liberamente i singoli diritti.

Per informazioni relative agli utenti, ai ruoli e alle direttive password consultare il sistema di informazione di STEP 7.

4.10.7 VPN

4.10.7.1 VPN (Virtual Private Network)

VPN - IPsec

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 IPsec) tra due sistemi IT o reti sicuri nonostante una rete non sicura.

Il tunnel IPsec inoltra tutti dati, anche di protocolli di livelli superiori (HTTP, FTP, ecc.).

Il traffico di dati di due componenti di rete viene trasportato 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

4.10.7.2 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 di questo tipo.
2. Attivare l'opzione "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.

Selezionare "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.

La realizzazione di un collegamento VPN con una stazione di engineering, che è simultaneamente server Telecontrol (TCSB installato), si svolge insieme alla sincronizzazione dell'ora del CP:

Si vuole realizzare un collegamento VPN alla stazione di engineering (con TCSB) tramite il CP. Il collegamento VPN viene realizzato anche se il CP non dispone ancora dell'ora attuale. I certificati utilizzati vengono valutati validi e la comunicazione protetta funziona.

Dopo la realizzazione del collegamento il CP sincronizza la propria ora con il PC, in quanto con la comunicazione Telecontrol attivata il server è il master dell'ora.

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.

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

Eseguire la creazione della comunicazione via tunnel VPN tra SOFTNET Security Client e il CP in base al capitolo Creazione di tunnel VPN per la comunicazione S7 tra stazioni (Pagina 64).

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 riesce.

4.10.7.4 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.

4.10.7.5 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".

4.10.7.6 SYSLOG

Utilizzo di SYSLOG solo con 1 collegamento VPN

Se si vuole utilizzare SYSLOG con livello 7 (debug) tramite collegamenti VPN, questo è possibile solo con un singolo collegamento VPN progettato.

4.10.7.7 SINEMA Remote Connect

Manutenzione remota con SINEMA Remote Connect (SINEMA RC)

L'applicazione "SINEMA Remote Connect" (SINEMA RC) è disponibile solo per la manutenzione remota.

Per la codifica dei dati SINEMA RC utilizza OpenVPN. Il centro della comunicazione è il server SINEMA RC tramite il quale si svolge la comunicazione tra i nodi e che gestisce la configurazione del sistema di comunicazione.

Passi preliminari

Eseguire i seguenti passi prima di iniziare la progettazione del collegamento SINEMA RCdel modulo in STEP 7. Questi passi sono il requisito necessario per un progetto STEP 7 coerente.

- Progettazione di SINEMA Remote Connect Server

  Eseguire la progettazione necessaria di SINEMA RC Server (non in STEP 7). Il modulo di comunicazione e i relativi partner di comunicazione devono essere progettati nel server SINEMA RC.

- Esportazione del certificato CA (opzionale)

  Se come metodo di autenticazione del modulo di comunicazione per la realizzazione del collegamento si vuole utilizzare il certificato del server, esportare il certificato CA dal SINEMA RC Server.

  Importare successivamente il certificato CA dal SINEMA RC Server nella stazione di engineering.

  In alternativa, come metodo di autenticazione del modulo di comunicazione è necessario utilizzare l'impronta digitale del certificato del server. La durata di validità dell'impronta digitale può essere più breve di quella del certificato.

  Osservare che l'importazione del certificato deve essere ripetuta in caso di sostituzione dell'unità.

Progettazione di SINEMA Remote Connect

Importazione del proprio certificato

1. Navigare nel CP al gruppo di parametri "Security > Manager dei certificati > Certificati dei dispositivi partner".
2. Aprire la finestra di dialogo per la selezione del certificato facendo doppio clic sulla prima riga libera della tabella.
3. Selezionare il certificato CA da SINEMA RC Server.

Navigare successivamente al gruppo di parametri "Security > VPN".

VPN > Generale

1. Attivare VPN
2. Come "Tipo di collegamento VPN" selezionare l'opzione "Configurazione OpenVPN automatica tramite SINEMA Remote Connect Server" se non si vuole utilizzare la comunicazione tramite SINEMA Remote Connect.

SINEMA Remote Connect Server

Inserire l'indirizzo e il numero di porta del server.

Controllo server

Selezionare il metodo di autenticazione del modulo di comunicazione per la realizzazione del collegamento.

- Certificato CA

  Selezionare in "Certificato CA" il certificato CA precedentemente importato e assegnato nel manager locale dei certificati da SINEMA RC Server.

  Il modulo controlla sostanzialmente il certificato CA del server e il relativo periodo di validità. Entrambe le opzioni non possono essere modificate.

- Impronta digitale

  Se si seleziona questo metodo di autenticazione, inserire l'impronta digitale del certificato del server di SINEMA RC Server.

Autenticazione

- ID dispositivo

  Inserire l'ID dispositivo per il modulo generata in SINEMA RC.

- Password dispositivo

  Inserire la password dispositivo per il modulo progettata in SINEMA RC.

  Numero massimo di caratteri: 127

Impostazioni opzionali

La realizzazione del collegamento viene progettata nel gruppo di parametri "Security > VPN > Impostazioni opzionali" tramite il parametro "Tipo di collegamento".

- **Intervallo di aggiornamento**

  Tramite il parametro si imposta l'intervallo nel quale il CP richiede la configurazione al server SINEMA RC.

  Con l'impostazione 0 (zero) osservare che le modifiche della configurazione del server SINEMA RC possono comportare l'impossibilità di realizzare un collegamento al server SINEMA RC dal CP.

- **"Tipo di collegamento"**

  Entrambe le opzioni del parametro hanno il seguente effetto sulla realizzazione del collegamento:

  – Auto

    Il modulo realizza un collegamento al server SINEMA RC. Il collegamento OpenVPN rimane attivo finché i parametri del collegamento non vengono modificati dal server SINEMA Remote Connect. In caso di interruzione del collegamento il CP realizza di nuovo il collegamento automaticamente.

    In caso di modifica dei parametri del collegamento mediante il server SINEMA Remote Connect il CP interroga i nuovi dati del collegamento allo scadere dell'Intervallo di aggiornamento progettato in alto.

  – Trigger PLC

    L'opzione è prevista per la comunicazione sporadica del modulo tramite il server SINEMA RC.

    Questa opzione può essere utilizzata se si vogliono realizzare collegamenti temporanei tra il modulo e un PC. I collegamenti temporanei vengono realizzati tramite una variabile PLC e possono ad es. essere utilizzati per casi di service.

Nota

Interruzione del collegamento

In caso di STOP della CPU, ad esempio in seguito ad un aggiornamento del firmware o della funzione "Carica nel dispositivo", il collegamento OpenVPN viene interrotto.

Queste funzioni possono essere utilizzate solo in caso di attivazione dell'opzione "Auto".

- **Variabile PCL per la realizzazione del collegamento**

  Il modulo realizza un collegamento con l'opzione "Trigger PLC" se la variabile PLC (Bool) accetta il valore 1. Durante il funzionamento la variabile PLC può essere utilizzata in caso di necessità, ad es. tramite un pannello HMI.

  In caso di reset della variabile PLC a 0 il collegamento viene interrotto di nuovo.

4.10.8 Manager dei certificati

Assegnazione di certificati

Se per l'unità si utilizza la comunicazione con autenticazione, ad esempio SSL/TLS per la trasmissione protetta di e-mail, sono necessari certificati. È necessario importare i certificati di partner di comunicazione non Siemens nel progetto STEP 7 e caricarli nell'unità con i dati di progettazione:

1. Importare i certificati del partner di comunicazione nelle impostazioni Security globali tramite il manager dei certificati.
2. Successivamente assegnare all'unità i certificati importati, a scelta:
   - Tramite la tabella "Certificati e autorità di certificazione accreditati" le impostazioni Security globali
   - Tramite la tabella "Certificati dei dispositivi partner" nel manager dei certificati dell'unità (Security):

     Inserire in questa tabella anche i certificati di partner di comunicazione i cui certificati sono stati generati nello stesso progetto STEP 7.

Per la descrizione dei procedimenti consultare il capitolo Utilizzo di certificati (Pagina 71).

Ulteriori informazioni si trovano nel sistema di informazione STEP 7.

4.10.9 Utilizzo di certificati

Certificati per l'autenticazione

Se per il modulo di comunicazione è stata progettata la comunicazione con autocertificazione, per la realizzazione della comunicazione sono necessari i propri certificati e i certificati del partner di comunicazione.

A tutti i nodi di un progetto STEP 7 con funzioni Security attivate vengono forniti certificati. Il progetto STEP 7 è l'autorità di certificazione.

Nota

Nessun certificato con le funzioni Security disattivate

Se nel progetto STEP 7 le funzioni Security del CP sono disattivate, non viene generato nessun certificato nemmeno per il CP.

Per la trasmissione protetta di e-mail tramite SSL/TLS viene creato un certificato SSL per il CP. Questo certificato viene visualizzato in STEP 7 in "Impostazioni Security globali > Manager dei certificati > Certificati del dispositivo". Nella tabella "Certificati del dispositivo" vengono visualizzati l'emittente, la validità, l'utilizzo di un certificato (servizio/applicazione) e l'utilizzo di una chiave. È possibile richiamare ulteriori informazioni di un certificato selezionando il certificato nella tabella e selezionato il menu di scelta rapida "Visualizza". Nella tabella si trovano anche tutti i certificati creati da STEP 7 e tutti i certificati importati.

Per consentire che il modulo comunichi con partner non Siemens con le funzioni Security attivate, è necessario sostituire i certificati corrispondenti dei partner nella comunicazione. Per impostare nel modulo i certificati di altri produttori, procedere nel modo seguente:

1. Importare i certificati non Siemens dai partner di comunicazione

   ⇒ Impostazioni Security globali del progetto (manager dei certificati)

2. Assegnazione dei certificati, in alternativa:
   - Impostazioni Security globali > Manager dei certificati > "Certificati e autorità di certificazione attendibili"
   - Impostazioni Security locali del modulo > Manager dei certificati > "Certificati dei dispositivi partner"

I seguenti passi sono descritti nelle seguenti sezioni.

Importare i certificati non Siemens dai partner di comunicazione

Importare i certificati dei partner di comunicazione di terzi tramite il manager dei certificati nelle impostazioni Security globali del progetto STEP 7. A tal proposito procedere nel modo seguente:

1. Salvare il certificato non Siemens nel sistema di file del PG della stazione di engineering collegata.
2. Aprire nel progetto STEP 7 il Manager dei certificati globale:

   Impostazioni Security globali > Manager dei certificati
3. Aprire la scheda "Certificati e autorità di certificazione accreditati".
4. Fare clic in una riga della tabella e selezionare il menu di scelta rapida "Importa".
5. Dalla finestra di dialogo aperta importare il certificato dal sistema di file della stazione di engineering nel progetto STEP 7.

Assegnazione di certificati nelle impostazioni Security globali

Importare il certificato partner tramite: Impostazioni Security globali > Manager dei certificati > Certificati affidabili > tasto destro del mouse. Assegnare il certificato al CP (selezionare il certificato > tasto desto del mouse).

1. Aprire la scheda "Certificati e autorità di certificazione accreditati".
2. Selezionare il certificato desiderato.
3. Selezionare il menu contestuale "Assegna" (tasto destro del mouse).
4. Selezionare nella finestra di dialogo successiva l'unità desiderata.

   Dopo l'assegnazione il certificato compare nel manager dei certificati locale dell'unità nella tabella "Certificati dei dispositivi partner".

Assegnare localmente i certificati

Per poter utilizzare un certificato importato per il modulo, il certificato deve essere visualizzato nel gruppo di parametri "Security" del modulo. A tal proposito procedere nel modo seguente:

1. Selezionare il modulo nel progetto STEP 7.
2. Navigare al gruppo di parametri "Security > Manager dei certificati".
3. Nella tabella fare doppio clic sulla riga con la voce "<Aggiungi nuovo>".

   Viene visualizzata la tabella "Manager dei certificati" delle Impostazioni Security globali.
4. Selezionare nella tabella il certificato non Siemens desiderato e fare clic sul segno di spunta verde sotto la tabella per applicare il certificato.

   Il certificato selezionato viene visualizzato nella tabella locale del modulo.

A partire da questo momento per il modulo viene utilizzato il certificato non Siemens.

Inserire in questa tabella anche i certificati di partner di comunicazione i cui certificati sono stati generati nello stesso progetto STEP 7.

Esportazione dei certificati per applicazioni di terzi (ad es. server Logging)

Per la comunicazione con applicazioni di terzi, normalmente anche le applicazioni non Siemens necessitano del certificato del modulo.

Eseguire l'esportazione del certificato del modulo per partner di comunicazione di terzi come l'importazione (cfr. in alto). A tal proposito procedere nel modo seguente:

1. Aprire nel progetto STEP 7 il Manager dei certificati globale:

   Impostazioni Security globali > Manager dei certificati
2. Aprire la scheda "Certificati del dispositivo".
3. Nella tabella selezionare la riga con il certificato desiderato e successivamente il menu di scelta rapida "Esporta".
4. Salvare il certificato nel sistema di file del PC della stazione di engineering collegata.

A questo punto è possibile trasferire il certificato esportato del modulo nel sistema di terzi.

Certificato per server Logging

Se si utilizza un server Logging nel proprio impianto, per l'autenticazione del modulo esportare nel server il certificato SSL.

Modifica del certificato: Nome alternativo del proprietario del certificato

STEP 7 acquisisce le proprietà "Nome DNS", "Indirizzo IP" e "URI" del parametro "Nome alternativo del proprietario del certificato" (Windows: "Nome alternativo del richiedente") dai dati di progettazione STEP 7.

Questo parametro di un certificato può essere modificato nel manager dei certificati delle impostazioni Security globali. Nella tabella dei certificati del dispositivo selezionare quindi un certificato e richiamare il menu di scelta rapida "Rinnova". Le impostazioni del parametro "Nome alternativo del proprietario del certificato" modificato in STEP 7 non vengono acquisite dal progetto STEP 7.

4.11 Punti di accesso ai dati

La descrizione dei parametri specifici di Telecontrol si trova nei manuali di progettazione, vedere /4/ (Pagina 108).

4.12 Messaggi

Progettazione di e-mail

In caso di eventi rilevanti il CP può inviare messaggi. Sono progettabili e-mail. Il destinatario può essere un PC con connessione Internet o una stazione S7.

I messaggi si progettano nell'editor dei messaggi del CP. Essi si trovano in alternativa tramite:

- Il menu contestuale del CP (con modulo selezionato)
- Tramite navigazione del progetto: Catella della stazione > Moduli locali > CP

I caratteri ammessi per i testi dei messaggi e altri parametri si trovano nel capitolo Set di caratteri per nome utente, password o messaggi (Pagina 79).

Panoramica della progettazione e informazioni necessarie

Per la trasmissione dei messaggi non deve più essere attivata la comunicazione Telecontrol (gruppo di parametri "Tipi di comunicazione"). Con il CP è possibile inviare messaggi, senza utilizzare la comunicazione Telecontrol.

Informazioni necessarie per l'utilizzo di e-mail:

- Dati di accesso del server SMTP: Indirizzo, numero di porta, nome utente, password
- In caso di utilizzo di STARTTLS o SSL/TLS: Certificato del provider del servizio e-mail
- Indirizzi e-mail del destinatario

Eseguire la progettazione nei seguenti gruppi di parametri:

- Attivazione della funzione Security

  Per l'utilizzo di e-mail è necessario attivare le funzioni Security del CP, gruppo di parametri "Security".

- Progettazione del servizio / del protocollo

  "Progettazione di e-mail", vedere il capitolo Progettazione delle e-mail (Pagina 60).

- In caso di utilizzo di STARTTLS o SSL/TLS:
  - Importazione del certificato del provider del servizio e-mail

    "Impostazioni Security globali"
  - Utilizzo del certificato importato per il CP:

    Gruppo di parametri "Security" > "Manager dei certificati"

Progettazione dell'editor dei messaggi

La progettazione dei messaggi si esegue nell'editor dei punti di accesso ai dati e dei messaggi di STEP 7. In alternativa aprire gli editor tramite:

- Selezione dell'unità di comunicazione

  Menu di scelta rapida "Apri editor dei punti di accesso ai dati e dei messaggi"

- Tramite navigazione del progetto:

  Progetto > Catella della rispettiva stazione > Unità locali > Unità di comunicazione desiderata

  Facendo doppio clic sulla voce si apre l'editor del punto di accesso ai dati e delle segnalazioni.

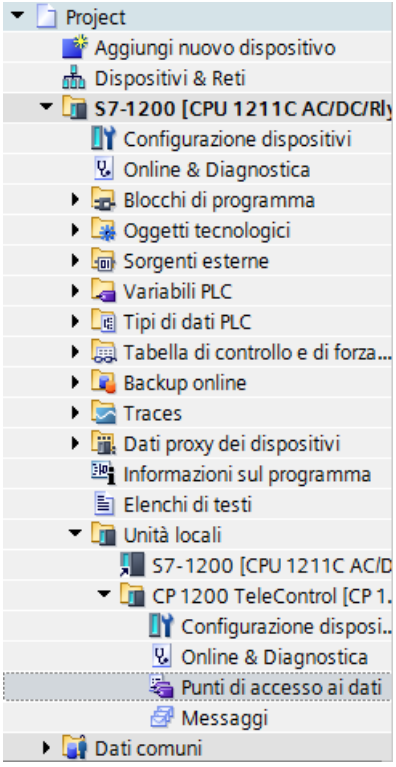


Figura 4-1 Apertura dell'editor dei messaggi tramite la navigazione del progetto

Dopo l'apertura dell'editor è possibile commutare tra editor del punto di accesso ai dati ed editor dei messaggi tramite le due voci a destra in alto sopra la tabella.

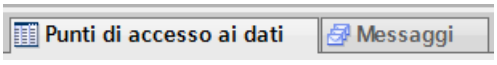


Figura 4-2 Commutazione tra i due editor

L'editor dei punti di accesso ai dati è rilevante per la comunicazione Telecontrol.

Creazione di oggetti

Creare un nuovo oggetto (messaggio) facendo doppio clic nella prima riga della tabella con la voce grigia "<Aggiunti oggetto>".

Il nome preassegnato può essere adattato a secondo delle necessità. Esso deve essere tuttavia univoco all'interno del modulo.

Disposizione delle colonne e delle righe, visualizzazione/soppressione di colonne

Come in molti altri programmi, è possibile disporre le colonne e ordinare le tabelle in base alle proprie esigenze:

- Disposizione delle colonne

  Tendo premuto il tasto sinistro del mouse su un'intestazione colonna è possibile spostare la colonna.

- Ordinamento degli oggetti

  Facendo un breve clic con il tasto sinistro del mouse su un'intestazione colonna è possibile ordinare gli oggetti della tabella in ordine crescente o decrescente in base alle voci di questa colonna. L'ordinamento viene visualizzato nell'intestazione della colonna tramite una freccia.

  L'ordinamento decrescente di una colonna può essere disattivato di nuovo facendo di nuovo clic sull'intestazione colonna.

- Adattamento della larghezza della colonna

  Questa funzione si ottiene con le seguenti azioni:

  – tramite il menu contestuale che viene aperto facendo clic con il tasto destro del mouse su un'intestazione colonna.

    "Ottimizza larghezza", "Ottimizza la larghezza di tutte le colonne"

  – Se si sposta il cursore in prossimità della limitazione destra di un'intestazione della colonna, compare la seguente icona:

    A questo punto fare doppio clic sull'intestazione della colonna. La larghezza della colonna si adatta alla voce più estesa in questa colonna.

- Visualizza/nascondi colonne

  A questa funzione si accede tramite il menu contestuale che viene aperta facendo clic con il tasto destro del mouse su un'intestazione colonna.

Copia messaggi

I messaggi possono essere copiati e inseriti Facendo clic con il tasto destro del mouse nella riga di un oggetto nella tabella, si accede alle funzioni indicate tramite il menu contestuale:

- Taglia
- Copia

- Inserisci

  Gli oggetti tagliati o copiati possono essere inseriti al di sopra della tabella o nella prima riga libera sotto la tabella.

  Gli oggetti tagliati o copiati possono essere inseriti anche in tabelle di altri moduli di comunicazione dello stesso tipo e con lo stesso protocollo.

- Cancella

Con il tasto <Ctrl> premuto è possibile selezionare più righe non attigue.

Con il tasto <Maiusc> premuto è possibile selezionare l'inizio e la fine dell'area attigua.

Scheda per la progettazione dei messaggi

Selezionare un messaggio nella tabella "Messaggi". I parametro di questo messaggio selezionato vengono progettati nelle schede sotto la tabella.

"Parametri del messaggio"

Progettare qui il numero telefonico o il destinatario, l'oggetto (e-mail) e il testo del messaggio.

"Trigger":

Tramite il gruppo di parametri "Trigger" progettare l'attivazione del mittente del messaggio nonché altri parametri.

- **Trigger e-mail**

  Definisce l'evento nel quale viene attivato l'invio del messaggio:

  – **Utilizza variabile PLC**

    Come segnale di trigger per l'invio di e-mail viene analizzato il cambio di fronte (0 → 1) del bit di attivazione "Variabile PLC per trigger", impostato dal programma utente. In caso di necessità, per ciascun messaggio può essere progettato un bit di attivazione separato. Per il bit di attivazione vedere in basso.

    Reset del bit di attivazione:
    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 del messaggio.
    In tutti gli altri casi il bit di attivazione deve essere resettato tramite il programma utente.

    Nota

    Impostazione rapida della variabile di attivazione della diagnostica

    È consigliabile non impostare i trigger più di una volta al secondo.

  – **La CPU entra in STOP**.

  – **La CPU entra in RUN**

- **Collegamento con un partner interrotto**

  Attiva l'invio del messaggio se il collegamento Telecontrol con un partner viene interrotto.

- **Collegamento con un partner creato**

  Attiva l'invio del messaggio se il collegamento Telecontrol viene ripristinato.

- **Creazione del collegamento con un partner non riuscita**

  Attiva l'invio del messaggio se il collegamento con un server Telecontrol non ha potuto essere realizzato.

- **Sessione TeleService iniziata**

  Attiva l'invio del messaggio se il Tipo di comunicazione TeleControl Basic è stato attivato ed è realizzato un TeleService.

- **Sessione TeleService terminata**

  Attiva l'invio del messaggio se il Tipo di comunicazione TeleControl Basic è stato attivato e un collegamento TeleService è stato chiuso.

- **Collegamento VPN realizzato**

  Attiva l'invio del messaggio se il collegamento VPN viene realizzato o ripristinato.

- **Collegamento VPN interrotto**

  Attiva l'invio del messaggio se il collegamento VPN viene interrotto.

- **Collegamento SINEMA RC realizzato**

  Attiva l'invio del messaggio se il collegamento OpenVPN viene realizzato o ripristinato.

- **Collegamento SINEMA RC interrotto**

  Attiva l'invio del messaggio se il collegamento OpenVPN viene interrotto.

- **Variabile PLC per trigger**

  Variabile PLC per il trigger "Utilizza variabile PLC"

- **Attiva identificazione per stato di modifica**

  Attivando l'opzione, dopo ogni tentativo di invio viene restituito lo stato che fornisce informazioni sullo stato di elaborazione del messaggio.

  Lo stato viene scritto nella "Variabili PLC per stato di modifica". In caso di problemi con il recapito di messaggi è possibile definire lo stato, tramite il server web della CPU, visualizzando qui il valore della variabile PLC.

  Per il significato dello stato visualizzato in caratteri esadecimale vedere il capitolo Stato di modifica delle e-mail (Pagina 93).

- **Variabili PLC per stato di modifica**

  Variabile PLC del tipo DWORD per lo stato di modifica

- **Invia valore**

  Con l'opzione attivata 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 $$.

  $$ come segnaposto per i valori dei punti di accesso ai dati, supporta i seguenti tipi di dati:

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

  – Array dei tipi di dati indicati

- **Variabile PCL per il valore**

  Variabile PLC nella quale è scritto il valore da inviare.

4.13 Set di caratteri per nome utente, password o messaggi

Set di caratteri per nome utente, password o testi dei messaggi

I seguenti caratteri ammessi valgono per:

- Server e-mail:
  – Nome utente e password
- Messaggi nell'editor dei messaggi:
  – Testi dei messaggi

Indicazione come set di caratteri ASCII (valore esadecimale e nome carattere):

- 0x20

  Carattere spazio

- 0x21 ... 0x5F

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

- 0x61 ... 0x7E

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

- 0x7C, 0x7E

  | ~

Inoltre per i testi dei messaggi:

- Interruzione di riga manuale (↵)

  Nei testi dei messaggi è possibile inserire un'interruzione di riga tramite <Maius>+<Invio>.

Blocchi di programma (OUC) 5

5.1 Blocchi di programma per OUC

Utilizzo dei blocchi di programma per la comunicazione Open User Communication (OUC)

Le istruzioni riportate sotto (blocchi di programma) possono essere utilizzate per la comunicazione diretta tra stazioni S7.

A differenza degli altri tipi di comunicazione la Open User Communication non deve essere attivata nella progettazione del CP in quanto per questo devono essere creati attivamente i blocchi di programma corrispondenti. 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.

Requisiti per Secure OUC

Presupposti per l'utilizzo della trasmissione protetta tramite Secure OUC:

- STEP 7: A partire da V16
- Firmware CPU: A partire da V4.4
- Firmware CP: A partire da V3.2

Blocchi di programma supportati per OUC

Le seguenti istruzioni nella versione minima indicata sono disponibili per la programmazione della Open User Communication:

- **TSEND_C V3.0 / TRCV_C V3.0**

  Blocchi compatti per:

  – Realizzazione/interruzione del collegamento e invio di dati.

  – Realizzazione/interruzione del collegamento e ricezione di dati.

In alternativa utilizzare:

- **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

  Per la trasmissione di e-mail codificate con questo blocco è necessaria l'ora esatta nel CP. Progettare la sincronizzazione dell'ora.

Per la modifica dei dati di progettazione del CP durante il tempo di esecuzione:

- **T_CONFIG V1.0**

  Configurazione controllata dal programma dei parametri IP

  Osservare le avvertenze relative a T_CONFIG e agli SDT "IF_CONF_..." nel capitolo Modifica dell'indirizzo IP durante il tempo di esecuzione (Pagina 84).

Nota

Nessuna risposta del CP

"T_CONFIG" non supporta la risposta del CP alla CPU. Gli errori nel richiamo del blocco o durante l'impostazione del parametro di indirizzi non vengono segnalati. Il blocco emette "BUSY" o "DONE", indipendentemente dall'impostazione dei parametri di indirizzi.

I blocchi di programma si trovano in STEP 7 nella task card "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. TMAIL_C utilizza il parametro MAIL_ADDR_PARAM.

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 (DB globale).

Il tipo SDT viene generato non selezionando 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_IP_V4".

Il SDT corrispondente viene quindi creato con i relativi parametri.

SDT utilizzabili

- **TCON_IP_V4**

  Per la trasmissione di telegrammi tramite TCP o UDP

- **TCON_QDN**

  Per la comunicazione TCP o UDP tramite il nome di dominio completamente qualificato (FQDN) (IPv4 / IPv6)

- **TCON_IP_RFC**

  Per la trasmissione di telegrammi tramite ISO-on-TCP (comunicazione diretta tra due stazioni S7)

- **TADDR_Param**

  Per la trasmissione di telegrammi tramite UDP

- **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 relativo nome (FQDN)

- **TCON_IP_V4_SEC**

  Per la trasmissione protetta di dati tramite TCP

- **TCON_QDN_SEC**

  Per la trasmissione protetta di dati tramite il nome host

- **TMail_V4_SEC**

  Per la trasmissione protetta di e-mail con indirizzamento del server e-mail tramite un indirizzo IPv4

- **TMail_V6_SEC**

  Per la trasmissione protetta di e-mail con indirizzamento del server e-mail tramite un indirizzo IPv6

- **TMail_QDN_SEC**

  Per la trasmissione protetta di e-mail con indirizzamento del server e-mail tramite il nome Host

Avvertenza relativa a TMail_Vx_SEC / TMail_QDN_SEC:
In questi SDT viene controllato il certificato del server mail, mentre l'ID del certificato "TLSServerCertRef" (riferimento interno di STEP 7) non viene controllato.

La descrizione degli SDT con i relativi parametri si trovano nel sistema di informazione STEP 7 al rispettivo nome.

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.

5.2 Modifica dell'indirizzo IP durante il tempo di esecuzione

Modifica dei parametri di indirizzi durante il tempo di esecuzione tramite T_CONFIG

Utilizzando il blocco T_CONFIG è possibile modificare con il programma i seguenti parametri durante il tempo di esecuzione:

- Indirizzo IP del CP
- Maschera della sotto-rete del CP
- Indirizzo router del CP
- Parametri di indirizzi dei server DNS (IF_CONF_DNS)
- Parametri di indirizzi dei server NTP (IF_CONF_NTP)

Presupposti nella progettazione CP

Per poter modificare i parametri IP in modo controllato dal programma, nella progettazione dell'indirizzo IP dell'interfaccia del CP è necessario attivare l'opzione "Consenti l'adattamento dell'indirizzo IP direttamente sul dispositivo".

Nota

Modifica dei parametri IP con indirizzo IP dinamico

Osservare gli effetti delle modifiche controllate dal programma dei parametri IP nel caso in cui il CP rilevi un indirizzo IP dinamico dal router collegato: In questo caso il CP non è più raggiungibile dal partner di comunicazione.

Blocchi di programma / versioni STEP 7

I presupposti per la modifica controllata dal programma dei parametri IP è supportata dal blocco di programma T_CONFIG. Questo blocco accede ai dati di indirizzi memorizzati in un tipo di dati si sistema adatto (SDT).

T_CONFIG può essere utilizzato con i seguenti tipi di dati di sistema (SDT):

- IF_CONF_V4
- IF_CONF_V6

- IF_CONF_DNS
- IF_CONF_NTP

I parametri di indirizzamento possono essere configurati in un CP solo con validità temporanea.

Nel rispettivo SDT "IF_CONF_..." deve essere impostato il parametro "Mode" = 2.

Nota

Nessuna risposta del CP

"T_CONFIG" non supporta la risposta del CP alla CPU. Gli errori nel richiamo del blocco o durante l'impostazione del parametro di indirizzi non vengono segnalati. Il blocco emette "BUSY" o "DONE", indipendentemente dall'impostazione dei parametri di indirizzi.

Le informazioni dettagliate relative alla parametrizzazione dei blocchi e degli SDT si trovano nel sistema di informazione STEP 7.

Presupposti

Versione STEP 7

È possibile utilizzare T_CONFIG da STEP 7 Basic V14.

Indirizzi IP progettati

Per poter modificare i parametri IP in modo controllato dal programma, nella progettazione dell'indirizzo IP dell'interfaccia del CP è necessario attivare l'opzione "Consenti l'adattamento dell'indirizzo IP direttamente sul dispositivo".

Versione firmware

I presupposti per la modifica controllata dal programma dei parametri IP sono:

- Firmware CP ≥ V2.1.7x

  e

- Firmware CPU ≥ V4.2

Diagnostica e manutenzione

6

⚠ AVVERTENZA

Pulizia del contenitore

- **Nell'area a rischio di esplosione**
  Pulire i componenti esterni del contenitore solo con un panno umido.
- **Nell'area non-Ex**
  Pulire i componenti esterni del contenitore solo con un panno asciutto.

Non utilizzare liquidi o solventi.

⚠ CAUTELA

Superfici calde

Pericolo di incendio durante gli interventi di manutenzione su componenti che presentano temperature della superficie superiori a 70 °C (158 °F).

- Adottare misure di protezione corrispondenti, ad es. indossare guanti di protezione.
- Dopo gli interventi di manutenzione ripristinare le misure di protezione da contatto.

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 26).

STEP 7: La scheda "Diagnostica" nella finestra di ispezione

Qui si ottengono le seguenti informazioni sullo stato online dell'unità selezionata.

STEP 7 Basic: Funzioni di diagnostica tramite il menu "Online" > "Online & 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.

Se si vuole utilizzare la diagnostica online con la stazione tramite il CP, come presupposto è necessario attivare il tipo di comunicazione "Attiva funzioni online", vedere capitolo Tipi di comunicazione (Pagina 46).

Gruppo "Diagnostica"

Le pagine di diagnostica sono suddivise nei seguenti gruppi:

- **Generale**

  Questo gruppo mostra le Indicazioni generali sull'unità.

- **Stato della diagnostica**

  Questo gruppo indica informazioni di stato del modulo dal lato della CPU.

  – Eventi specifici per il dispositivo

    Qui vengono visualizzate le indicazioni sugli eventi interni al modulo.

- **Interfaccia Ethernet**

  Indicazioni dell'indirizzo e statistiche

- **Industrial Remote Communication**

  Il gruppo ha le seguenti pagine di diagnostica:

  – Partner

    Informazioni relative alle indicazioni di indirizzo del partner, alla statistica del collegamento, ai dati di progettazione del partner e ad altre informazioni di diagnostica

  – Elenco dei punto di accesso ai dati

    Diverse informazioni sui punti di accesso ai dati quali i dati di progettazione, il valore, lo stato del collegamento ecc.

  – Diagnostica del protocollo

    Tramite il pulsante "Attiva traccia protocollo" vengono scritti insieme anche i telegrammi che vengono ricevuti e inviati dall'unità.

    Tramite "Disattiva traccia protocollo" i protocolli vengono arrestati e i dati vengono scritti in un file di protocollo.

    Tramite "Salva" è possibile salvare e successivamente analizzare il file di protocollo in una stazione di engineering.

- **Ora**

  Indicazioni sull'ora nel dispositivo

- **Security**

  Il gruppo ha le seguenti pagine di diagnostica:

  – Stato

    Questa pagina di diagnostica indica le impostazioni Security più rilevanti, l'ora e i dati per la configurazione.

  – Log di sistema

    Con un collegamento in atto con un modulo SCALANCE S in questa pagina di diagnostica è possibile avviare la compilazione del protocollo delle registrazioni di sistema. Le registrazioni possono essere salvate.

– Audit Log

  In questa pagina di diagnostica è possibile avviare la compilazione del protocollo dei dati Log del modulo. Le registrazioni possono essere salvate.

– Stato della comunicazione

  Questa pagina di diagnostica indica gli stati dei moduli Security noti del gruppo VPN, del relativi punti terminale e delle proprietà del tunnel.

– SINEMA RC - Configurazione VPN automatica

  Questa pagina di diagnostica mostra lo stato della configurazione OpenVPN automatica e dei collegamenti OpenVPN.

Gruppo "Funzioni"

- **Update del firmware**

  Per la descrizione vedere il capitolo Caricamento del firmware (Pagina 95).

- **Assegna indirizzo IP**
- **Assegna nome di apparecchio PROFINET**
- **Salva dati di service**

  La funzione serve per il protocollo di processi interni dell'unità nelle situazioni nelle quale è impossibile eliminare autonomamente comportamenti inattesi e indesiderati dell'unità.

  Con il pulsante "Salva dati di service" viene creato il file di protocollo. I dati vengono salvati in un file con formato "*.dmp", che può essere valutati dalla hotline Siemens.

E-mail di diagnostica

Il CP può inviare una e-mail di diagnostica con eventi progettabili ad es. in caso di STOP della CPU. Per la progettazione vedere "Messaggi".

Stato del partner

In caso di utilizzo della comunicazione Telecontrol il CP della CPU può segnalare lo stato del collegamento con il partner di comunicazione tramite una variabile. Lo stato della variabile può essere visualizzato tramite il server web della CPU. La variabile può essere progettata nel seguente gruppo di parametri:

- TeleControl Basic: "Stazioni partner"
- DNP3 / IEC: "Comunicazione con la CPU"

Diagnostica CP

Il CP può memorizzare dati di diagnostica estesi nelle variabili PLC. Gli stati delle variabili PLC possono essere visualizzati tramite il Web server della CPU.

Per la progettazione vedere il capitolo Diagnostica CP (Pagina 54).

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 Accesso al Web server (Pagina 52).

SNMP

Per le funzioni vedere il capitolo SNMP (Pagina 92).

6.2 Server web S7-1200: Realizzazione del collegamento

Realizzazione del collegamento con il server web server della CPU

Procedere nel modo seguente per collegarsi da un PC con il server Web della CPU.

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 "Server web".
4. Attivare nel gruppo di parametri "Generale" l'opzione "Attiva server web su questa unità".
5. In una CPU a partire della versione V4.0 creare un utente con i diritti necessari nella gestione utenti.

In funzione dell'attivazione o della disattivazione dell'opzione "Consenti accesso solo tramite HTTPS" nel gruppo di parametri "Generale", il procedimento per la realizzazione del collegamento con il server web è diverso:

- **Realizzazione del collegamento tramite HTTP**

  Procedimento con l'opzione "Consenti accesso solo tramite HTTPS" disattivata

- **Realizzazione del collegamento tramite HTTPS**

  Procedimento con l'opzione "Consenti accesso solo tramite HTTPS" attivata

I seguenti procedimento sono descritti nelle seguenti sezioni.

I presupposti per l'accesso al server web della CPU (Web browser ammesso) e la descrizione del procedimento si trovano nel sistema di informazione STEP 7 alla voce "Informazioni relative al server web".

Realizzazione del collegamento tramite HTTP

1. Collegare il PC alla CPU tramite l'interfaccia Ethernet.
2. Inserire l'indirizzo della CPU nella casella di indirizzo del proprio Web browser: http://<Indirizzo IP>
3. Premere il tasto di inserimento <Invio>.

   La pagina iniziale del server web 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 alle voci "HTTPS" o "Accesso per HTTPS (S7-1200)".

6. Se il collegamento è passato in modalità protetta HTTPS ("https://<Indirizzo IP>/..." nella casella di indirizzo del server web), è possibile procedere come descritto nella seguente sezione.

   Se si interrompe il collegamento al server web, la volta successiva è possibile connettersi al Web server senza caricare il certificato tramite HTTP.

Realizzazione del collegamento tramite HTTPS

1. Collegare il PC alla CPU tramite l'interfaccia Ethernet.
2. Inserire l'indirizzo della CPU nella casella di indirizzo del proprio Web browser: https://<Indirizzo IP>
3. Premere il tasto di inserimento <Invio>.

   La pagina iniziale del server web si apre.

4. Connettersi alla pagina iniziale del server web come utente con i diritti necessari.

   Utilizzare i dati utente progettati nella gestione utenti del server web della CPU.

5. Dopo la connessione nella navigazione del server web selezionare la voce "Stato dell'unità".
6. Selezionare il CP nell'elenco delle unità.

   Vengono visualizzati i contenuti specifici del CP.

6.3 Diagnostica Security online tramite porta 8448

Diagnostica Security tramite porta 8448

Presupposti:

- Con il firewall attivato l'accesso deve essere abilitato.

Se si vuole eseguire una diagnostica Security in STEP 7 Professional, procedere nel modo seguente:

1. Selezionare il CP in STEP 7.
2. Aprire il menu di scelta rapida "Online & diagnostica".
3. Fare clic sul pulsante "Collega online" nel gruppo dei parametri "Security"

In questo modo eseguire la diagnostica Security tramite la porta 8448.

Osservare a tal proposito il capitolo Impostazioni per la diagnostica Security online e caricamento nella stazione con il firewall attivato (Pagina 59).

6.4 SNMP

SNMP (Simple Network Management Protocol)

SNMP è un protocollo per la gestione e la diagnostica 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).

Potenzialità del CP come SNMP Agent

Il CP supporta l'interrogazione dei dati nelle seguenti versioni SNMP:

- SNMPv1 (standard)
- SNMPv3 (Security)

Fornisce i contenuti di oggetti MIB del MIB II standard secondo RFC1213.

- **MIB II**

  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
  – ICMP
  – TCP
  – UDP
  – SNMP

  I seguenti gruppi dei MIB II standard non vengono supportati:

  – Adress Translation (AT)
  – EGP
  – Transmission

- **LLDP MIB**

I trap non sono supportati dal CP.

Ulteriori informazioni sui dati MIB e su SNMP si trovano nel manuale /5/ (Pagina 108).

Progettazione

Per la progettazione vedere:

- Con funzioni Security disattivate: (SNMPv1): SNMP (Pagina 56)
- Con funzioni Security attivate (SNMPv1 / SNMPv3): SNMP (Pagina 62)

6.5 Stato di modifica delle e-mail

Progettazione dello stato di modifica di e-mail

Le seguenti identificazioni di stato valgono per e-mail progettate tramite l'editor dei messaggi del CP. L'emissione dell'indicazione di stato viene abilitata con l'opzione "Attiva identificazione per stato di modifica". L'identificazione di stato viene scritta nella CPU nella "Variabile PLC per stato di modifica".

Per la progettazione vedere il capitolo Progettazione delle e-mail (Pagina 60).

Emissione dello stato di modifica di e-mail

Lo stato di modifica viene restituito dopo la trasmissione di un messaggio da inviare dal CP stesso o dal server del servizio.

In caso di problemi con il recapito di messaggi è possibile definire lo stato tramite il Web server della CPU.

Stato di modifica delle e-mail

Le identificazioni di stato fornite dalla "Variabili PLC per stato di modifica" hanno i seguenti significati:

Tabella 6- 1 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.

Stato	Significato
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.
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.

6.6 Caricamento del firmware

Nuove versioni firmware del CP

Se per l'unità è disponibile una nuova versione firmware, essa si trova nelle pagine Internet del Siemens Industry Online Support al seguente indirizzo:
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15922/dl)

Osservare che le versioni firmware a partire da V3 non possono essere caricate su CP con versione hardware 1.

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 del Siemens Industry Online Support.
- Caricamento del firmware con le funzione online di STEP 7 tramite WAN

Nota

Effetti sul salvataggio ritentivo della CPU

- Se per l'installazione del file firmware si utilizza una SIMATIC Memory Card, viene mantenuta la memoria ritentiva.
- Se per l'installazione del file firmware si utilizzano le funzioni online, la memoria ritentiva viene persa.

L'operazione di caricamento del firmware si riconosce dal lampeggio dei LED del CP, vedere LED (Pagina 26).

Caricamento del firmware con le funzione online di STEP 7 tramite WAN

Presupposti:

- Il CP è raggiungibile tramite il proprio 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.

Procedimento:

1. Collegare la stazione di engineering alla rete.
2. Aprire il progetto STEP 7 interessato nella stazione di engineering.
3. Selezionare il CP o la CPU della stazione il cui CP si vuole aggiornare alla nuova versione firmware.
4. Attivare le funzioni online tramite il simbolo "Collega online".
5. Selezionare l'interfaccia Ethernet "PN/IE" nella finestra di dialogo "Collega online" nell'elenco di selezione "Tipo dell'interfaccia PG/PC".

6. Selezionare il posto connettore del CP o della CPU.

   Sono possibili entrambi i modi.

7. Eseguire il collegamento tramite il pulsante "Collega".

L'assistente "Collega online" conduce ai passi successivi.

Il sistema di informazioni STEP 7 fornice una guida ulteriore alle funzioni online.

6.7 Sostituzione delle unità

Sostituzione delle unità

⚠CAUTELA

Leggere il manuale di sistema "Sistema di automazione S7-1200"

Prima del montaggio leggere i passi relativi al collegamento e alla messa in servizio nel manuale di sistema "S7-1200 Sistema di automazione" (vedere riferimento bibliografico nell'appendice).

Durante il montaggio e il collegamento procedere in base alle descrizioni riportate nel manuale di sistema "S7-1200 Sistema di automazione".

Assicurarsi che durante il montaggio/lo smontaggio dell'apparecchio l'alimentazione sia disinserita.

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.

Eccezione:
i dati della progettazione SINEMA RC e il certificato del server SINEMA RC sono salvati nel CP. Non possono essere letti dalla CPU.

Dati tecnici

7

7.1 Dati tecnici del CP 1243-1

Tabella 7- 1 Dati tecnici del CP 1243-1

Dati tecnici		
Numero articolo	6GK7 243-1BX30-0XE0	
Collegamento a Industrial Ethernet		
Quantità	1	
Esecuzione	Presa RJ45	
Proprietà	100BASE-TX, IEEE 802.3-2005, half duplex/full duplex, autocrossover, autonegotiation, separazione galvanica	
Velocità di trasmissione	10 / 100 Mbit/s	
Lunghezze dei cavi ammesse (Ethernet)	**(Combinazioni alternative per ciascun campo di lunghezza) ***	
0 ... 55 m	• Max. 55 m IE TP Torsion Cable con IE FC RJ45 Plug 180 • Max. 45 m IE TP Torsion Cable con IE FC RJ45 + 10 m TP Cord tramite IE FC RJ45 Outlet	
0 ... 85 m	• Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable con IE FC RJ45 Plug 180 • Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord tramite IE FC RJ45 Outlet	
0 ... 100 m	• Max. 100 m IE FC TP Standard Cable con IE FC RJ45 Plug 180 • Max. 90 m IE FC TP Standard Cable + 10 m TP Cord tramite IE FC RJ45 Outlet	
Dati elettrici		
Alimentazione	dal bus back-plane S7-1200	DC 5 V
Corrente assorbita (caratteristica)	dal bus back-plane S7-1200	250 mA
Potenza attiva dissipata (caratteristica)	dal bus back-plane S7-1200	1,25 W
Condizioni ambientali ammesse		
Temperatura ambiente	Durante il funzionamento in caso di struttura orizzontale del telaio di montaggio	-20 °C ... +70 °C
	Durante il funzionamento in caso di struttura verticale del telaio di montaggio	-20 °C ... +60 °C
	Durante il magazzinaggio	-40 °C ... +70 °C
	Durante il trasporto	-40 °C ... +70 °C
Umidità relativa	Durante il funzionamento	≤ 95 % a 25 °C, senza condensa
Forma costruttiva, dimensioni e peso		
Formato dell'unità	Unità compatta S7-1200, larghezza singola	
Grado di protezione	IP20	

Dati tecnici	
Peso	122 g
Dimensioni (L x A x P)	30 x 110 x 75 mm
Possibilità di montaggio	Guida ad U standard Quadro di comando
Funzioni del prodotto **	

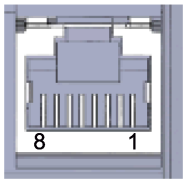
***** Per maggiori dettagli vedere il catalogo IK PI, tecnica di cablaggio
****** Ulteriori caratteristiche e dati utili sono riportati nel capitolo Applicazione e funzioni (Pagina 13).

7.2 Assegnazione dei pin dell'interfaccia Ethernet

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 7- 2 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

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.

Documenti in Internet

Le dichiarazioni di conformità e i certificati del prodotto riportati di seguito si trovano in Internet al seguente indirizzo:
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15922/cert)

Le norme osservate possono essere consultate nel rispettivo certificato che si trova in Internet all'indirizzo indicato:

Indirizzo per le dichiarazioni di conformità

Le dichiarazioni di conformità EU e UK sono archiviate e tenute a disposizione delle autorità competenti presso:

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 Nürnberg
Deutschland

Dichiarazione di conformità UE

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.

CE

- **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.

Dichiarazione di conformità UE

Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

Il prodotto soddisfa i requisiti delle seguenti direttive:

- UKEX Regulations

  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.

- EMC Regulations

  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

- RoHS Regulations

  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX / IECEx / UKEX / CCC-Ex

Osservare le indicazioni nel documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", che si trova:

- Nel DVD della documentazione allegato al prodotto in:
  "Tutti i documenti" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- I documenti si trovano in Internet al seguente indirizzo:
  Link: (https://support.industry.siemens.com/cs/ww/it/view/78381013)

Le condizioni per l'impiego sicuro del prodotto essere rispettate conformemente al capitolo Avvertenze per l'impiego in zone Ex secondo ATEX / UKEX / IECEx / CCC-Ex (Pagina 32).

Il prodotto soddisfa i seguenti requisiti riguardanti la protezione da esplosione.

⚠AVVERTENZA

Osservanza delle direttive di montaggio

Il prodotto soddisfa i requisiti necessari se installato e utilizzato osservando quanto segue:

- le avvertenze nel capitolo Avvertenze importati per l'impiego del dispositivo (Pagina 31)
- le direttive di montaggio nel documento /1/ (Pagina 107)

IECEx

Classificazione: Ex ec IIC T4 Gc, n. di certificato: IECEx DEK 18.0019X

Il prodotto soddisfa i requisiti delle norme:

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

ATEX

Classificazione: II 3 G Ex ec IIC T4 Gc, n. di certificato:DEKRA 18ATEX0027 X

Il prodotto soddisfa i requisiti delle norme:

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

UKEX

Classificazione: II 3 G Ex ec IIC T4 Gc, n. di certificato:DEKRA 21UKEX0003 X

Il prodotto soddisfa i requisiti delle norme:

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

Importer UK: Siemens plc (vedere sopra)

CCC-Ex

Classificazione:Ex na IIC T4 Gc (non sulla targhetta identificativa), n. di certificato:2020322310002625

Il prodotto soddisfa i requisiti delle seguenti norme

- GB 3836.1

  Aree a rischio di esplosione - Parte 0: Equipaggiamento - Requisiti generali

- GB 3836.8

  Atmosfere esplosive - Parte 15: Protezione del dispositivo attraverso classe di protezione antideflagrante 'n'

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 stabiliti dalle seguenti direttive:

- Direttiva UE 2011/65/UE per la limitazione dell'utilizzo di materiale particolarmente pericoloso in dispositivi elettrici ed elettronici.
- SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

Norma applicata:

- EN IEC 63000

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)

File Number: E223122

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: cULus 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 T4A; Ta = -20 °C...60 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...60 °C

Report / UL file: E223122 (NRAG.E223122)

Osservare le condizioni per l'impiego sicuro del CP conformemente al capitolo Avvertenze per l'impiego nell'area Ex secondo UL HazLoc e FM (Pagina 33).

FM

Factory Mutual Approval Standard Class Number 3600, 3611, 3810, ANSI/ISA-61010-1

Equipment rating:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C
(Ta reduced to 50 °C when mounted vertically)

Report Number: 3040919

Osservare le condizioni per l'impiego sicuro del CP conformemente al capitolo Avvertenze per l'impiego nell'area Ex secondo UL HazLoc e FM (Pagina 33).

Australia - RCM

Il CP soddisfa i requisiti stabiliti dalle norme AS/NZS 2064 (classe A).

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

A급 기기(업무용 방송통신기자재)

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

Osservare che riguardo all'emissione di radiodisturbi questo dispositivo corrisponde alla classe di valori limite A. Questo dispositivo può essere impiegato in tutte le aree, tranne il settore civile.

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: (https://support.industry.siemens.com/cs/ww/it/ps/15922/cert)

Disegni quotati

B

Nota

Tutte le misure indicate nei disegni del sono in millimetri.

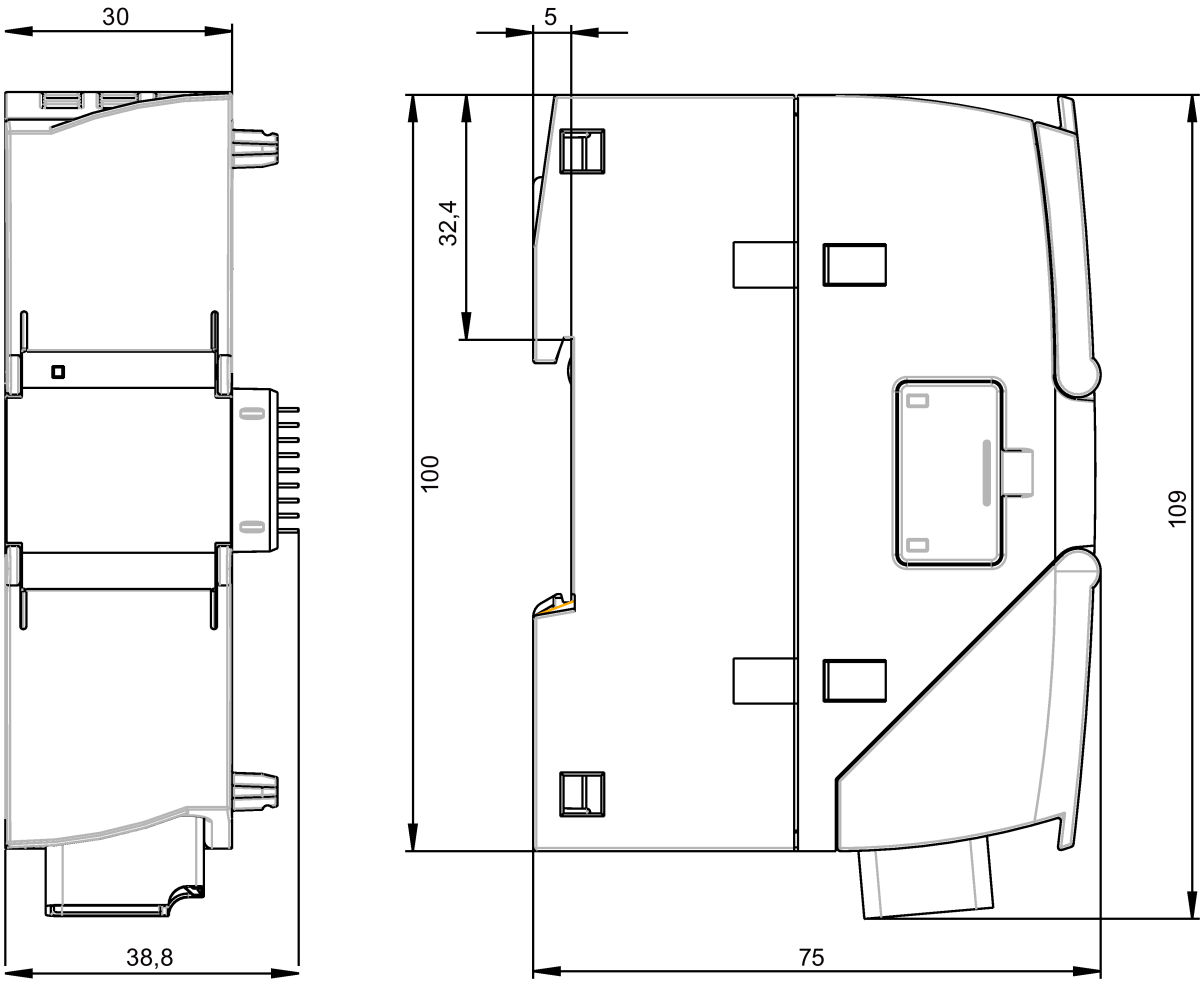


Figura B-1 Vista anteriore e laterale sinistra

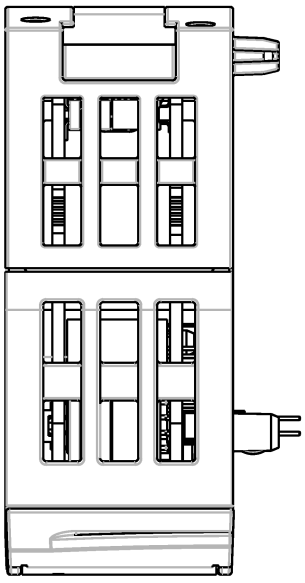


Figura B-2 Vista dall'alto

Bibliografia

C

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
S7-1200 Sistema di automazione
Manuale di sistema
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/13683/man)

/2/

SIMATIC NET
CP 1243-1
Istruzioni operative
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/view/103948898)

/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 - TeleControl
Siemens AG
Manuali di progettazione per i protocolli:
- TeleControl Basic
- SINAUT ST7
- DNP3
- IEC 60870-5
Link: (https://support.industry.siemens.com/cs/ww/it/ps/21764/man)

/5/

SIMATIC NET
Diagnostica e progettazione con SNMP
Manuale di diagnostica
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/15392/man)

/6/

SIMATIC NET
SINEMA Remote Connect - Server
Istruzioni operative
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/it/ps/21816/man)

Indice analitico

S

T

V

W