SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Comunicazione

Manuale di guida alle funzioni

Introduzione 1

Avvertenze di sicurezza 2

Industrial Cybersecurity 3

Presentazione del prodotto 4

Servizi di comunicazione 5

Comunicazione PG 6

Comunicazione HMI 7

Open User Communication 8

Comunicazione S7 9

Accoppiamento punto a punto 10

Comunicazione OPC UA 11

Assegnazione di indirizzi tramite DHCP 12

Routing 13

Risorse di collegamento 14

Diagnostica ed eliminazione di guasti 15

Seguito alla pagina successiva

11/2024
A5E03735818-AM

Seguito

Comunicazione con il sistema ridondante S7-1500R/H 16

Industrial Ethernet Security con CP 1543-1 17

S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Comunicazione

Manuale di guida alle funzioni

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 Aktiengesellschaft. 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 Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANIA

A5E03735818-AM
Ⓟ 10/2024 Con riserva di modifiche

Copyright © Siemens 2013 - 2024.
Tutti i diritti riservati

Indice del contenuto

1 Introduzione ... 10

1.1 Guida alla documentazione: Manuali di guida alle funzioni ... 17
1.1.1 Classi di informazzione Manuali di guida alle funzioni ... 17
1.1.2 Utensili di base ... 19
1.1.3 S7 Port Configuration Tool (S7-PCT) ... 21
1.1.4 S7 Failsafe Configuration Tool (S7-FCT) ... 22
1.1.5 Multi Fieldbus Configuration Tool (MFCT) ... 22
1.1.6 Documentazione tecnica SIMATIC ... 23

2 Avvertenze di sicurezza ... 26

2.1 Avvertenze generali di sicurezza ... 26

3 Industrial Cybersecurity ... 27

3.1 Avvertenze di Cybersecurity ... 27

3.2 Informazioni rilevanti in materia di cybersecurity in questo manuale ... 28

4 Presentazione del prodotto ... 29

5 Servizi di comunicazione ... 35

5.1 Opzioni di comunicazione in sintesi ... 35

5.2 Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet ... 38

5.3 Panoramica delle risorse di collegamento ... 47

5.4 Configurazione di un collegamento ... 49

5.5 Coerenza dei dati ... 53

5.6 Comunicazione sicura ... 56
5.6.1 Nozioni di base sulla comunicazione sicura ... 56
5.6.1.1 Informazioni utili sulla comunicazione sicura ... 56
5.6.1.2 Caratteristiche di sicurezza che dipendono dal pannello operatore ... 59
5.6.1.3 Riservatezza grazie alla crittografia ... 61
5.6.1.4 Autenticità e integrità garantite da una firma ... 64
5.6.2 Gestione dei certificati ... 68
5.6.2.1 Informazioni utili sulla gestione dei certificati ... 68
5.6.2.2 Gestione dei certificati in TIA Portal ... 69
5.6.2.3 Esempi di gestione dei certificati ... 72
5.6.2.4 Come funziona la comunicazione con i certificati: HTTP over TLS ... 77
5.6.2.5 Suggerimento: Aggiornamento dei certificati caricati in RUN ... 80
5.6.3 Presupposti per la comunicazione sicura ... 81
5.6.3.1 Protezione dei dati di configurazione riservati ... 81
5.6.3.2 Informazioni importanti sulla protezione dei dati di configurazione PLC riservati ... 84
5.6.3.3 Modifica della password ... 85
5.6.3.4 Reset della password ... 87
5.6.3.5 Assegnazione della password tramite la SIMATIC Memory Card ... 89

5.6.3.6 Particolarità per il backup e il ripristino della CPU ... 91
5.6.3.7 Suggerimenti per evitare e gestire gli errori ... 92
5.6.3.8 Regole per la sostituzione ... 93
5.6.4 Secure Open User Communication ... 94
5.6.4.1 Configurazione di Secure OUC da una CPU S7-1500 come client TLS a un PLC di terzi (server TLS) ... 94
5.6.4.2 Secure OUC da una CPU S7-1500 come server TLS a un PLC di terzi (client TLS) ... 96
5.6.4.3 Secure OUC tra due CPU S7-1500 ... 99
5.6.4.4 Secure OUC tramite interfaccia CP ... 102
5.6.4.5 Secure OUC con Modbus TCP ... 108
5.6.4.6 Secure OUC via e-mail ... 109
5.6.5 Comunicazione PG/HMI sicura ... 112
5.6.5.1 Comunicazione PG/HMI basata su meccanismi di sicurezza standardizzati ... 112
5.6.5.2 Ulteriori impostazioni della comunicazione PG/HMI sicura ... 114
5.6.5.3 Suggerimento per la comunicazione basata su certificati tra PG e CPU ... 116
5.6.5.4 Comportamento della CPU dal caricamento allo stato "pronto al funzionamento" ... 118
5.6.5.5 Utilizzo della comunicazione HMI sicura ... 120
5.6.5.6 Utilizzo della comunicazione PG/PC legacy per TIA Portal ... 122
5.6.5.7 Informazioni sulla compatibilità ... 123

5.7 SNMP ... 125
5.7.1 Attivazione e disattivazione di SNMP ... 125
5.7.2 Attivazione / disattivazione di SNMP tramite trasferimento del set di dati: esempio di CPU 1516-3 PN/DP ... 128
5.7.3 Attivazione/disattivazione di SNMP nelle CPU S7-1500R/H tramite trasferimento del set di dati ... 130

6 Comunicazione PG ... 134

7 Comunicazione HMI ... 137

8 Open User Communication ... 140

8.1 Open User Communication in sintesi ... 140

8.2 Protocolli per Open User Communication ... 141

8.3 Istruzioni per Open User Communication ... 143

8.4 Open User Communication con indirizzamento tramite nome di dominio ... 147

8.5 Configurazione di Open User Communication tramite TCP, ISO on TCP, UDP e ISO ... 149

8.6 Configurazione della comunicazione tramite FDL ... 155

8.7 Configurazione della comunicazione tramiter Modbus TCP ... 158

8.8 Configurazione della comunicazione tramite e-mail ... 161

8.9 Configurazione della comunicazione tramite protocollo FTP ... 162

8.10 Creazione e interruzione di relazioni di comunicazione ... 165

9 Comunicazione S7 ... 166

10 Accoppiamento punto a punto ... 174

11 Comunicazione OPC UA ... 179

11.1 Informazioni utili su OPC UA ... 179

11.1.1 OPC UA e industria 4.0 ... 179
11.1.2 Proprietà generali di OPC UA ... 180
11.1.3 OPC UA nelle CPU S7-1200/S7-1500 ... 183
11.1.4 Accesso alle applicazioni OPC UA ... 185
11.1.5 Indirizzamento dei nodi ... 189
11.1.6 Vista generale dello spazio dei nomi per i server OPC UA delle CPU S7-1200/1500 ... 193
11.1.7 Informazioni utili sui client OPC UA ... 194

11.2 Security in OPC UA ... 197
11.2.1 Impostazioni di sicurezza ... 197
11.2.2 Certificati standard X.509 della ITU ... 199
11.2.3 Certificati in OPC UA ... 202
11.2.4 Creazione dei certificati autofirmati ... 203
11.2.5 Creazione autonoma di coppie di chiavi PKI e di certificati ... 204
11.2.6 Trasmissione sicura dei messaggi ... 207
11.2.7 Gestione certificato tramite Globale Discovery Server (GDS) ... 210
11.2.7.1 Gestione certificato automatizzata tramite GDS ... 210
11.2.7.2 Configurazione della funzione Push ... 213
11.2.7.3 Impostazione e caricamento dei parametri GDS ... 214
11.2.7.4 Messa in servizio GDS ... 216
11.2.7.5 Modello indirizzi per la gestione certificati Push ... 221
11.2.7.6 CertificateGroups nel modello indirizzi ... 226
11.2.8 Sicurezza basata sui ruoli in OPC UA ... 228
11.2.8.1 Nozioni utili su Security basata sui ruoli ... 228

11.3 Utilizzo della CPU S7-1500 come server OPC UA ... 232
11.3.1 Informazioni importanti sul server OPC UA delle CPU S7-1500 ... 232
11.3.1.1 Il server OPC UA delle CPU S7-1500 ... 232
11.3.1.2 Punti finali dei server OPC UA ... 234
11.3.1.3 Mappatura dei tipi di dati ... 236
11.3.1.4 Comportamento del server OPC UA durante il funzionamento ... 239
11.3.2 Modalità di accesso ai dati del server OPC UA ... 241
11.3.2.1 Accessi ai client e accessi locali al server OPC UA ... 241
11.3.2.2 Gestione dei diritti di scrittura e lettura ... 246
11.3.2.3 Gestione dei diritti di scrittura e lettura per l'intero DB ... 248
11.3.2.4 Coordinazione dei diritti di scrittura e lettura per le variabili della CPU ... 249
11.3.2.5 Coerenza delle variabili CPU ... 251
11.3.2.6 Accessi in scrittura alle variabili OPC UA di S7-1500 Motion Control ... 253
11.3.2.7 Modalità di accesso ai dati del server OPC UA ... 254
11.3.2.8 Attributo MinimumSamplingInterval ... 255
11.3.2.9 Esporta file XML OPC UA ... 255
11.3.3 Configurazione del server OPC UA ... 257
11.3.3.1 Attivazione del server OPC UA ... 257
11.3.3.2 Accesso al server OPC UA ... 259
11.3.3.3 Impostazioni generali del server OPC UA ... 261
11.3.3.4 Impostazioni del server per le sottoscrizioni ... 263
11.3.3.5 Utilizzo del servizio TransferSubscription ... 265
11.3.3.6 Handling dei certificati dei client e dei server ... 267
11.3.3.7 Generazione dei certificati server con STEP 7 ... 273
11.3.3.8 Autenticazione dell'utente ... 276
11.3.3.9 Gestione utenti e ruoli con diritti di accesso alle funzioni OPC UA ... 278
11.3.3.10 Impostazioni di diagnostica del server ... 280
11.3.3.11 Licenze per OPC UA ... 281

11.3.4 Progettazione dell'interfaccia del server OPC UA ... 282
11.3.4.1 Che cos'è un'interfaccia server? ... 282
11.3.4.2 Utilizzo delle specifiche Companion OPC UA ... 284
11.3.4.3 Creazione dell'interfaccia server per la specifica Companion ... 291
11.3.4.4 Creazione dell'interfaccia server personalizzata ... 296
11.3.4.5 Tipo di dati per le specifiche Companion ... 303
11.3.4.6 Tipi di dati LocalizedText e ByteString ... 304
11.3.4.7 Utilizzo di ulteriori tipi di dati OPC UA per le specifiche Companion ... 307
11.3.4.8 Array dinamici ... 309
11.3.4.9 Regole per i file XML OPC UA ... 313
11.3.4.10 Creazione dell'interfaccia server per lo spazio dei nomi d riferimento ... 314
11.3.4.11 Creazione di nodi OPC UA basandosi sulla mappatura dei dati locali dei tipi FB e UDT ... 317
11.3.4.12 Indicazioni sulle quantità di risorse consigliate per l'utilizzo delle interfacce server ... 321
11.3.5 Come mettere a disposizione i metodi del server OPC UA ... 321
11.3.5.1 Informazioni utili sui metodi server ... 321
11.3.5.2 Condizioni generali per l'impiego dei metodi server ... 324
11.3.6 Come rendere disponibili i messaggi sul server OPC UA ... 326
11.3.6.1 Informazioni utili sui messaggi ... 326
11.3.6.2 Eventi OPC UA ... 331
11.3.6.3 OPC UA Conditions e OPC UA Alarms ... 334
11.3.6.4 Attivazione di Alarms and Conditions ... 336
11.3.6.5 Acconsentire eventi di un server OPC UA ... 337
11.3.6.6 Modifica delle variabili nei messaggi ... 339
11.3.6.7 Ricezione simultanea di messaggi in più lingue ... 341
11.3.6.8 Metodi di OPC UA Alarms and Conditions ... 344
11.3.6.9 Gestione dei limiti di memoria per OPC UA Alarms and Conditions ... 348
11.3.7 Utilizzo delle possibilità di diagnostica ... 351
11.3.7.1 Diagnostica del server OPC UA ... 351
11.3.7.2 Diagnostica del server OPC UA nel programma ... 352
11.3.7.3 Diagnostica dei passaggi di stato del server ... 353
11.3.7.4 Diagnostica dei passaggi di stato della sessione ... 355
11.3.7.5 Controllo degli eventi Security ... 356
11.3.7.6 Richiesta di un client remoto non riuscita ... 356
11.3.7.7 Diagnostica di Subscription ... 358
11.3.7.8 Diagnostica cumulativa ... 361

11.4 Utilizzo della CPU S7-1500 come client OPC UA ... 364
11.4.1 Panoramica e presupposti ... 364
11.4.2 Informazioni importanti sulle istruzioni per i client ... 365
11.4.3 Numero di istruzioni per i client utilizzabili contemporaneamente ... 367
11.4.4 Configurazione di esempio per OPC UA ... 369
11.4.5 Creazione delle interfacce client ... 371
11.4.6 Rilevamento online dell'interfaccia server ... 379
11.4.7 Utilizzo di testi multilingue ... 383
11.4.8 Regole per l'accesso alle strutture ... 385
11.4.9 Utilizzo della parametrizzazione del collegamento ... 387
11.4.9.1 Creazione e parametrizzazione dei collegamenti ... 387
11.4.9.2 Handling dei certificati client della CPU S7-1500 ... 390
11.4.9.3 Autenticazione dell'utente ... 393
11.4.9.4 Utilizzo di un collegamento parametrizzato ... 394

11.5 Suggerimenti e raccomandazioni ... 400
11.5.1 Regole per Subscription ... 400
11.5.2 Regole per il programma utente ... 401
11.5.3 Copie master per la comunicazione OPC UA ... 402

12 Assegnazione di indirizzi tramite DHCP ... 404

12.1 Principio di assegnazione degli indirizzi con DHCP ... 407
12.2 DHCP con DNS ... 409
12.3 Disattivazione di DHCP ... 413
12.4 Configurazione dell'ID del client ... 414
12.5 Acquisizione degli indirizzi del server DNS tramite DHCP ... 416
12.6 Acquisizione degli indirizzi del server NTP tramite DHCP ... 416
12.7 Acquisizione del nome dell'host e del dominio tramite DHCP ... 417

13 Routing ... 418

13.1 Panoramica dei meccanismi di routing delle CPU S7-1500 ... 418
13.2 Routing S7 ... 419
13.3 IP Forwarding ... 423
13.4 Routing dei set di dati ... 430
13.5 Interfaccia virtuale per applicazioni basate su IP ... 432

14 Risorse di collegamento ... 436

14.1 Risorse di collegamento di una stazione ... 436
14.2 Occupazione delle risorse di collegamento ... 440
14.3 Visualizzazione delle risorse di collegamento ... 445

15 Diagnostica ed eliminazione di guasti ... 449

15.1 Diagnostica dei collegamenti ... 449
15.2 Indirizzo d'emergenza ... 452

16 Comunicazione con il sistema ridondante S7-1500R/H ... 454

16.1 Indirizzi IP di sistema nelle R/H-CPU ... 455
16.2 Indirizzi IP di sistema nei processori di comunicazione ... 461
16.3 Raggiungibilità ottimizzata tramite commutazione dell'indirizzo IP di sistema ... 466
16.4 Comportamento con Syncup ... 466
16.5 Comportamento in caso di commutazione principale/di backup ... 467
16.6 Risorse di collegamento del sistema ridondante S7-1500R/H ... 467
16.7 Comunicazione HMI con il sistema ridondante S7-1500R/H ... 469
16.7.1 Configurazione del collegamento HMI tramite l'indirizzo IP di sistema ... 469

16.8 Open User Communication con il sistema ridondante S7-1500R/H 471
16.8.1 Configurazione del collegamento tra Open User Communication e il sistema ridondante S7-1500R/H 472
16.8.2 Open User Communication con i processori di comunicazione CP 1543-1 477

16.9 Utilizzo di server OPC UA in un sistema S7-1500R/H 479
16.9.1 Informazioni importanti sul server OPC UA nel sistema S7-1500R/H 479
16.9.2 Transparent Mode (transparent Redundancy) 481
16.9.3 Non-transparent Mode (non-transparent Redundancy) 483
16.9.4 Modello di informazione in dettaglio 488
16.9.5 Istruzioni aggiornate per metodi Server 491

17 Industrial Ethernet Security con CP 1543-1 495

17.1 Firewall 496

17.2 Logging 497

17.3 Client NTP 497

17.4 SNMP 498

17.5 VPN 498

Glossario 499

Indice analitico 511

Introduzione 1

Scopo della documentazione

Il presente manuale di guida alle funzioni fornisce una panoramica delle possibilità di comunicazione offerte dalle CPU, dai moduli e dai processori di comunicazione così come dai sistemi PC dei sistemi SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro e SIMATIC Drive Controller. Nel presente manuale è descritta la comunicazione asincrona orientata alla connessione.

La documentazione tratta in particolare:

- Panoramica dei servizi di comunicazione
- Proprietà dei servizi di comunicazione
- Panoramica delle operazioni utente per la configurazione dei servizi di comunicazione

Nozioni di base necessarie

La comprensione del manuale di guida alle funzioni presuppone le seguenti conoscenze:

- Conoscenze generali nel campo della tecnica di automazione
- Conoscenze del sistema di automazione industriale SIMATIC
- Conoscenze sull'uso di STEP 7 (TIA Portal)

Campo di validità della documentazione

La presente documentazione è valida come base per tutti i prodotti dei sistemi SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL e ET 200pro. La documentazione dei singoli prodotti si basa su questa documentazione.

Novità del manuale di guida alle funzioni Comunicazione, edizione 11/2024 rispetto all'edizione 11/2023

Novità	Vantaggi per il cliente	Dove si trovano le informazioni?
Tabella dei protocolli di comunicazione e dei numeri di porta utilizzati nella comunicazione Ethernet dei moduli di interfaccia	Informazioni sui protocolli e sulle porte utilizzate dai moduli di interfaccia. L'utente può individuare le preimpostazioni a colpo d'occhio e adeguare in modo mirato soltanto le impostazioni di rilievo per il proprio caso applicativo.	Cap. Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet (Pagina 38)
OPC UA: maggiori risorse per le seguenti CPU S7-1500 dalla versione FW V4.0 in poi • CPU 151x(F)-3 PN • CPU 151xT(F)-3 PN	Le CPU S7-1500 151x(F)-3 PN e 151xT(F)-3 PN a partire dalla versione firmware V4.0 consentono di creare un maggior numero di nodi per le interfacce server e di metodi server. Inoltre è aumentata la performance per Read, Write e Subscription.	Manuale del prodotto della rispettiva CPU
OPC UA: ricezione simultanea di messaggi in più lingue	Per le CPU S7-1500, i client OPC UA con firmware V4.0 o superiore possono selezionare ad es. una delle lingue disponibili per i messaggi. Inoltre un client OPC UA può richiedere contemporaneamente i testi dei messaggi in tutte e 3 le lingue attive del progetto. I messaggi vengono così raccolti ad es. su un server centrale in modo che possano essere analizzati dagli utenti in lingue diverse.	Cap. Ricezione simultanea di messaggi in più lingue (Pagina 341)
OPC UA: Role based Security per CPU S7-1500 dalla versione FW V4.0	Grazie alla realizzazione del concetto di ruolo per le CPU S7-1500 dalla versione FW V4.0, il server OPC UA è in grado di gestire l'accesso di client OPC UA all'area indirizzi a un livello estremamente specifico.	Cap. Sicurezza basata sui ruoli in OPC UA (Pagina 228)
OPC UA: supporto della funzione "Transfer Subscription" per S7-1500	Per supportare le applicazioni di distribuzione del carico sui vari client OPC UA, per le CPU S7-1500 dalla versione V3.1.4 è disponibile la funzione "Transfer Subscription". Questa permette di trasferire una Subscription a un altro client OPC UA. Non è necessaria una configurazione specifica della funzione.	Cap. Utilizzo del servizio TransferSubscription (Pagina 265)

Novità del manuale di guida alle funzioni Comunicazione, edizione 11/2023 rispetto all'edizione 11/2022

Novità	Vantaggi per il cliente	Dove reperire le informazioni?
Capitolo "Industrial Cybersecurity"	Con la digitalizzazione e la crescente interconnessione delle macchine e degli impianti industriali è aumentato anche il rischio di attacchi informatici. È quindi diventato obbligatorio adottare adeguate misure di protezione, in particolare per le infrastrutture critiche.	Industrial Cybersecurity (Pagina 27)

Novità	Vantaggi per il cliente	Dove reperire le informazioni?
	Il capitolo contiene le seguenti informazioni: • Informazioni di base sull'Industrial Cybersecurity • Misure su come proteggere i singoli componenti e l'intero sistema dalla manipolazione e dagli accessi indesiderati.	
Aggiornamento delle tabelle dei protocolli di comunicazione e dei numeri di porta utilizzati nella comunicazione Ethernet	Informazioni aggiornate sui protocolli e sulle porte utilizzate. L'utente può individuare le preimpostazioni a colpo d'occhio e adeguare in modo mirato soltanto le impostazioni di rilievo per il proprio caso applicativo.	Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet (Pagina 38)
Informazioni aggiornate sulle risorse di collegamento delle CPU e dei dispositivi HMI.	Informazioni aggiornate sulle risorse di collegamento seguenti: • N° max. di risorse di collegamento supportate per alcuni tipi di CPU • N° max. di risorse di collegamento occupate per diversi dispositivi HMI	Risorse di collegamento (Pagina 436)
Ampliamento del sistema ridondante con processori di comunicazione	A partire da STEP 7 V19 è possibile ampliare un sistema ridondante S7-1500R/H dalla versione firmware V3.1 con i processori di comunicazione CP 1543-1.	Indirizzi IP di sistema nei processori di comunicazione (Pagina 461).
Secure Open User Communication con il sistema ridondante	A partire da STEP 7 V19 un sistema ridondante S7-1500R/H dalla versione firmware V3.1 supporta anche Secure Open User Communication.	Open User Communication con il sistema ridondante S7-1500R/H (Pagina 471)

Novità del manuale di guida alle funzioni Comunicazione, edizione 11/2022 rispetto all'edizione 05/2021

Novità	Vantaggi per il cliente	Dove reperire le informazioni
Aggiornamento delle tabelle dei protocolli di comunicazione e dei numeri di porta utilizzati nella comunicazione Ethernet	Informazioni aggiornate sui protocolli e sulle porte utilizzate. L'utente può individuare le preimpostazioni a colpo d'occhio e adeguare in modo mirato soltanto le impostazioni di rilievo per il proprio caso applicativo.	Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet (Pagina 38)
Attivazione / disattivazione di SNMP	A seconda della versione firmware delle CPU S7-1500, l'SNMP è attivato o disattivato nelle impostazioni predefinite. Le preimpostazioni possono essere modificate in base alle esigenze.	SNMP (Pagina 125)
Ottimizzazione dell'interfaccia virtuale per applicazioni basate su IP	Nei CP 1543-1 con versione firmware V3.0 o superiore, è disponibile il firewall interno al CP. Il firewall garantisce la sicurezza nel traffico dati tramite l'interfaccia virtuale.	Interfaccia virtuale per applicazioni basate su IP (Pagina 432)

Novità	Vantaggi per il cliente	Dove reperire le informazioni
Server OPC UA: Lettura dello stato di diagnostica della propria area di indirizzi	L'istruzione di lettura OPC UA ("OPC_UA_ReadList") consente di accedere al proprio spazio dei nomi per il server OPC UA. Ciò consente di leggere lo stato del proprio server OPC UA e dei collegamenti dei client OPC UA, della sessione e delle sottoscrizioni nonché di reagire a questi stati nel programma utente. Si possono ad esempio rilevare rapidamente i problemi di connessione e aumentare la disponibilità dell'impianto.	Diagnostica del server OPC UA nel programma (Pagina 352)
Server OPC UA: Registrazione di data e ora del source time dei nodi	L'istruzione di scrittura OPC UA ("OPC_UA_WriteList") consente di modificare sia il "SourceTimestamp" che il codice di stato di una variabile OPC UA (nodo). Pertanto, dalla versione V18, è possibile distinguere tra data e ora della "sorgente" e data e ora del "server".	Accessi ai client e accessi locali al server OPC UA (Pagina 241)
Meccanismo GDS OPC UA: Ora utilizzabile anche per i certificati Web server	Ora il certificato del Web server per la comunicazione HTTPS può essere gestito anche tramite il meccanismo OPC UA GDS, senza caricare separatamente la configurazione hardware.	Informazioni utili sulla gestione dei certificati (Pagina 68) Gestione certificato automatizzata tramite GDS (Pagina 210)

Novità del manuale di guida alle funzioni Comunicazione, edizione 05/2021 rispetto all'edizione 11/2019

Novità	Vantaggi per il cliente	Dove reperire le informazioni
Security ottimizzata per la comunicazione SIMATIC PG/HMI	• Consente l'identificazione univoca di ciascun PLC basato su certificati individuali • Offre una protezione di riservatezza supplementare mediante la comunicazione criptata • Protezione dei dati di configurazione tramite password individuali	Comunicazione PG/HMI sicura (Pagina 112)
Security Wizard per nuovi meccanismi PLC Security	• Configurazione rapida e semplice dei nuovi meccanismi Security del PLC in un passaggio • Informazioni di supporto per la selezione di impostazioni idonee per il proprio caso applicativo	Protezione dei dati di configurazione riservati (Pagina 81)
Gestione dei certificati tramite OPC UA (Global Discovery Server, GDS)	• Aggiornamento dei certificati durante il runtime • Supporto di CRL • Protezione dell'accesso per la gestione dei certificati	Gestione certificato tramite Globale Discovery Server (GDS) (Pagina 210)
Trasmissione di segnalazioni della CPU ai client OPC UA	• Con Subscription i client possono abbonare segnalazioni della CPU come "Alarms and Conditions" del server OPC UA della CPU • Le segnalazioni del programma, variabili comprese, vengono messi a disposizione dal server OPC UA	Come rendere disponibili i messaggi sul server OPC UA (Pagina 326)

Novità	Vantaggi per il cliente	Dove reperire le informazioni
	• Gli allarmi con obbligo di conferma possono essere confermati dal client OPC UA (disattivabile) • Una segnalazione in cascata viene visualizzata come "Overload" e con il metodo refresh i client possono caricare successivamente messaggi	
Assegnazione dinamica della configurazione della rete con DHCP	Impiego della CPU in rete con gestione IT tramite le seguenti funzioni: • Collegamento della CPU ad una rete disponibile senza configurazione manuale supplementare dell'interfaccia di rete • Richiesta di parametri di rete per la CPU secondo RFC 2131 da un server DHCPv4 (indirizzo IP e maschera di sottorete, indirizzo router IP predefinito e altri parametri di rete opzionali quali, ad es. indirizzi server DNS e NTP)	Assegnazione di indirizzi tramite DHCP (Pagina 404)
Indirizzamento basato sul nome con DNS	• Gli indirizzi server DNS possono essere rilevati dalla CPU tramite DHCP • La CPU può rilevare il nome host e di dominio da un server DHCP per le applicazioni realizzate con OPC UA o (Secure) OUC • La CPU può trasmettere i nomi host e di dominio configurati ai server DHCP accoppiati con i server DNS per la sincronizzazione dinamica (Dynamic DNS) • Il client NTP della CPU può interrogare server NTP con nome • I parametri della rete possono essere scritti con la nuova istruzione "CommConfig", ad es. parametri di indirizzo IP, DNS-Server, Host and Domain Name	DHCP con DNS (Pagina 409)

Novità del manuale di guida alle funzioni Comunicazione, edizione 11/2019 rispetto all'edizione 10/2018

Novità	Vantaggi per il cliente	Dove reperire le informazioni
IP Forwarding	Semplice accesso da livello gestione a livello di campo per la configurazione e la parametrizzazione di device, ad es. tramite PDM o Web browser.	IP Forwarding (Pagina 423)
Ampliamento del server OPC UA	Per le CPU S7-1500 a partire dal firmware V2.8 e dal TIA Portal Version 16 è possibile usufruire dei seguenti ampliamenti del server OPC UA integrato, se si è in possesso di un’adeguata licenza Runtime:	Cap. Comunicazione OPC UA (Pagina 179)

Novità	Vantaggi per il cliente	Dove reperire le informazioni
	• Diagnostica migliorata: Tramite messaggi nel buffer di diagnostica, una categoria OPC UA nell'area Online & Diagnostica in TIA Portal e anche una migliore visualizzazione delle risorse di collegamento, l'utente OPC UA riceve informazioni sullo stato del server OPC UA. • Stato del download: In stato di funzionamento RUN durante un download dal TIA Portal, il server OPC UA esegue un riavvio solo se i dati nuovamente caricati influiscono sulla gestione dei dati del server OPC UA. • Modellamento interfaccia del server: Ora le interfacce del server possono essere modellate anche nel TIA Portal oppure è possibile importare le specifiche Companion OPC UA e mapparle nella gestione dati PLC.	

Novità del manuale di guida alle funzioni Comunicazione, edizione 10/2018 rispetto all'edizione 12/2017

Novità	Vantaggi per il cliente	Dove reperire le informazioni
Descrizione della comunicazione con sistema ridondante S7-1500R/H	Fornisce informazioni sulle particolarità della comunicazione con sistema ridondante S7-1500R/H	Cap. Comunicazione con il sistema ridondante S7-1500R/H (Pagina 454)
Estensione del campo di validità del manuale di guida alle funzioni al sistema ridondante S7-1500R/H	Le funzioni già note del sistema di automazione SIMATIC S7-1500 sono state realizzate per il sistema ridondante S7-1500R/H	Manuale di sistema "Sistema ridondante S7-1500R/H" (https://support.industry.siemens.com/cs/ww/it/view/109754833)

Novità del manuale di guida alle funzioni Comunicazione, edizione 12/2017 rispetto all'edizione 09/2016

Novità	Vantaggi per il cliente	Dove reperire le informazioni
OPC UA Companion Specification	OPC UA Companion Specification consente di specificare metodi univoci e indipendenti dal produttore. Grazie ai metodi specifici è possibile integrare con facilità nel proprio impianto e nei processi produttivi dispositivi di produttori diversi.	Cap. Progettazione dell'interfaccia del server OPC UA (Pagina 282)
Collegamento protetto con un server e-mail tramite l'interfaccia della CPU	E' possibile creare un collegamento protetto con un server e-mail senza ulteriori hardware.	Cap. Secure OUC via e-mail (Pagina 109)
Comunicazione protetta tramite Modbus TCP	Consente la creazione di collegamenti TCP protetti tra un client Modbus TCP e un server Modbus TCP	Cap. Secure OUC con Modbus TCP (Pagina 108)

Novità del manuale di guida alle funzioni Comunicazione, edizione 09/2016 rispetto all'edizione 12/2014

Novità	Vantaggi per il cliente	Dove reperire le informazioni
Server OPC UA	OPC UA è un sistema standard omogeneo per lo scambio dati non legato all'impiego di determinate piattaforme di sistemi operativi. OPC UA utilizza meccanismi di sicurezza integrati su diversi sistemi di automazione, ad es. per lo scambio di dati, a livello di applicazione e per l'autenticazione dell'utente. Il server OPC UA mette a disposizione numerosi dati: • valori delle variabili PLC cui possono accedere i client • tipi di dati di queste variabili PLC • indicazioni per il server OPC UA stesso e per la CPU Ciò consente ai client di avere una visione d'insieme sulla gestione variabili e di leggere e scrivere valori.	Cap. Comunicazione OPC UA (Pagina 179)
Secure Open User Communication	Scambio di dati sicuro con altri dispositivi.	Cap. Secure Open User Communication (Pagina 94)
Utilizzo dei certificati in STEP 7	In STEP 7 si possono gestire certificati per le seguenti applicazioni: • Server OPC UA • Secure Open User Communication • Web server della CPU	Cap. Gestione dei certificati in TIA Portal (Pagina 69)
Disattivazione di SNMP per la CPU	Per la CPU è possibile disattivare SNMP. A determinate condizioni può essere utile, ad es. se le direttive di sicurezza della rete non ammettono SNMP.	Cap. SNMP (Pagina 125)

Convenzioni

STEP 7: per indicare il software di progettazione e programmazione, nella presente documentazione si utilizza la denominazione "STEP 7" come sinonimo di "STEP 7 a partire dalla versione V12 (TIA Portal)".

Per via delle funzioni Controller omogenee, la denominazione "CPU S7-1500" identifica anche le varianti di CPU S7-1500F, S7-1500T, S7-1500TF, S7-1500C, S7-1500R/H, S7-1500pro, ET200SP, S7-1500 Software Controller e SIMATIC Drive Controller. Per via ad es. della differente tecnica di installazione e delle diverse applicazioni, esistono delle differenze tra Advanced Controller, Distributed Controller e Software Controller.

La presente documentazione contiene illustrazioni dei dispositivi descritti. Le illustrazioni possono differire nei particolari dal dispositivo fornito.

Osservare inoltre le avvertenze contrassegnate nel modo seguente:

NOTA

Una nota contiene importanti informazioni sul prodotto descritto, sul relativo impiego o su una parte di documentazione alla quale occorre prestare particolare attenzione.

Industry Mall

L'Industry Mall è il catalogo prodotti e il sistema di ordinazione della Siemens AG per le soluzioni di automazione e azionamento sulla base di Totally Integrated Automation (TIA) e Totally Integrated Power (TIP).

I cataloghi per tutti i prodotti della tecnica di automazione e azionamento si trovano in Internet (https://mall.industry.siemens.com).

1.1 Guida alla documentazione: Manuali di guida alle funzioni

1.1.1 Classi di informazzione Manuali di guida alle funzioni

La documentazione per il sistema di automazione SIMATIC S7-1500 per le CPU 1513/1516pro-2 PN, SIMATIC Drive Controller per SIMATIC S7-1500 e i sistemi di periferia decentrata SIMATIC ET 200MP, ET 200SP, ET 200AL e ET 200eco PN è suddivisa in tre parti.

Questa suddivisione consente di accedere in maniera mirata ai contenuti di interesse.

La documentazione può essere scaricata gratuitamente da Internet. (https://support.industry.siemens.com/cs/ww/it/view/109742705)

Informazioni di base

I manuali di sistema e il Getting Started descrivono dettagliatamente la progettazione, il montaggio, il cablaggio e la messa in servizio dei sistemi SIMATIC S7-1500, SIMATIC Drive Controller, ET 200MP, ET 200SP, ET 200AL e ET 200eco PN. Per le CPU 1513/1516pro-2 PN utilizzare le istruzioni operative corrispondenti.

La Guida in linea di STEP 7 supporta l'utente nelle fasi di progettazione e programmazione.

Esempi:

- Getting Started S7-1500
- Manuali di sistema
- Istruzioni operative ET 200pro e CPU 1516pro-2 PN
- Guida in linea TIA Portal

Informazioni sul dispositivo

I manuali di prodotto contengono una descrizione compatta delle informazioni specifiche del modulo, come proprietà, schemi dei collegamenti, curve caratteristiche e dati tecnici.

Esempi:

- Manuali del prodotto delle CPU
- Manuali del prodotto dei moduli di interfaccia
- Manuali del prodotto dei moduli digitali
- Manuali del prodotto dei moduli analogici
- Manuali del prodotto dei moduli di comunicazione
- Manuale del prodotto dei moduli tecnologici
- Manuale del prodotto delle unità di alimentazione
- Manuale del prodotto delle BaseUnit

Informazioni generali

I manuali di guida alle funzioni contengono descrizioni dettagliate su argomenti generali inerenti a SIMATIC Drive Controller e al sistema di automazione S7-1500.

Esempi:

- Manuale di guida alle funzioni Diagnostica
- Manuale di guida alle funzioni Comunicazione
- Manuali di guida alle funzioni Motion Control
- Manuale di guida alle funzioni Server web
- Manuale di guida alle funzioni Tempi di ciclo e di reazione
- Manuale di guida alle funzioni PROFINET
- Manuale di guida alle funzioni PROFIBUS

Informazioni sul prodotto

Eventuali modifiche e integrazioni dei manuali vengono descritte in un file di informazioni sul prodotto. Le informazioni sul prodotto sono da considerarsi prioritarie rispetto a quelle contenute nel manuale del prodotto e nel manuale di sistema.

Le informazioni più aggiornate sul prodotto sono disponibili in Internet:

- S7-1500/ET 200MP (https://support.industry.siemens.com/cs/it/it/view/68052815)
- SIMATIC Drive Controller (https://support.industry.siemens.com/cs/de/it/view/109772684/it)
- Motion Control (https://support.industry.siemens.com/cs/de/it/view/109794046/it)
- ET 200SP (https://support.industry.siemens.com/cs/it/it/view/73021864)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/it/view/109765611)

Manual Collection

Le Manual Collection raggruppano in un unico file l'intera documentazione relativa ai diversi sistemi.

Le Manual Collection sono disponibili in Internet.

- S7-1500/ET 200MP/SIMATIC Drive Controller (https://support.industry.siemens.com/cs/ww/it/view/86140384)
- ET 200SP (https://support.industry.siemens.com/cs/ww/it/view/84133942)
- ET 200AL (https://support.industry.siemens.com/cs/ww/it/view/95242965)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/it/view/109781058)

1.1.2 Utensili di base

Strumenti

Gli strumenti descritti di seguito supportano durante tutte le fasi, dalla pianificazione e la messa in servizio all'analisi del sistema.

TIA Selection Tool

TIA Selection Tool supportano durante la selezione, la configurazione e l'ordinazione di dispositivi per Totally Integrated Automation (TIA).

Come successore del SIMATIC Selection Tools , il TIA Selection Tool raggruppa in un solo strumento i configuratori già noti per la tecnica di automazione.

TIA Selection Tool consente di generare un elenco di ordinazione completo dalla selezione del prodotto o dalla configurazione del prodotto.

TIA Selection Tool è disponibile in Internet.
(https://support.industry.siemens.com/cs/ww/it/view/109767888/en)

SIMATIC Automation Tool

Con SIMATIC Automation Tool è possibile eseguire operazioni di massa per interventi di service e di messa in servizio su diverse stazioni SIMATIC S7, indipendentemente da TIA Portal.

SIMATIC Automation Tool mette a disposizione numerose funzioni:

- Scansione di una rete di impianto PROFINET/Ethernet e identificazione di tutte le CPU collegate
- Assegnazione di indirizzi (IP, sottorete, Gateway) e nome del dispositivo (PROFINET Device) relativo ad una CPU
- Trasmissione della data e dell'ora del PG/PC convertita in formato UTC all'unità
- Download del programma sulla CPU
- Commutazione del modo di funzionamento RUN/STOP
- Localizzazione della CPU tramite lampeggio dei LED
- Lettura delle informazioni di errore della CPU

- Lettura del buffer di diagnostica della CPU
- Reset alle impostazioni di fabbrica
- Aggiornamento del firmware della CPU e dei moduli collegati

SIMATIC Automation Tool è disponibile in Internet.
(https://support.industry.siemens.com/cs/ww/it/view/98161300)

PRONETA

SIEMENS PRONETA (analisi della rete PROFINET) è uno strumento di messa in servizio e di diagnostica per reti PROFINET. PRONETA Basic dispone di 2 funzioni fondamentali:

- Nell'analisi della rete si ottiene una panoramica della topologia PROFINET. È possibile confrontare una configurazione reale con un impianto di riferimento o effettuare semplici modifiche di parametri, ad es. dei nomi e degli indirizzi IP dei dispositivi.
- Il "Test IO" consente un test semplice e rapido del cablaggio e della configurazione modulare di un impianto, inclusa una documentazione del risultato del test.

SIEMENS PRONETA Basic è disponibile in Internet:
(https://support.industry.siemens.com/cs/ww/it/view/67460624)

SIEMENS PRONETA Professional offre ulteriori funzioni come prodotto concesso in licenza. Consente il semplice Asset Management nelle reti PROFINET e supporta l'operatore di impianti di automazione nel rilevamento automatico dei dati dei componenti impiegati attraverso una vasta gamma di funzioni:

- L'interfaccia utente (API) offre un punto di accesso alla cella di automazione per automatizzare le funzioni di scansione tramite MQTT o una cella di comando.
- La diagnostica PROFIenergy consente di rilevare e in caso di necessità modificare molto rapidamente la modalità di pausa o la disponibilità al funzionamento per i dispositivi che supportano PROFIenergy.
- L'assistente per i set di dati consente allo sviluppatore PROFINET di leggere e scrivere in modo semplice e rapido i set di dati PROFINET aciclici, senza PLC ed engineering.

SIEMENS PRONETA Professional è disponibile in Internet: (https://www.siemens.com/proneta-professional)

SINETPLAN

SINETPLAN, il Siemens Network Planner, supporta l'utente nella pianificazione dei sistemi e nelle reti di automazione sulla base di PROFINET. Questo tool facilita il dimensionamento professionale e predittivo dell'installazione PROFINET già nella fase di pianificazione. Inoltre SINETPLAN fornisce all'utente strumenti utili per ottimizzare la rete, sfruttare al meglio le risorse di rete e pianificare le riserve. In questo modo, già prima dell'impiego pianificato si evitano problemi durante la messa in servizio e interruzioni nella fase produttiva. Questo aumenta la disponibilità dell'impianto produttivo e contribuisce a migliorare la sicurezza operativa.

I vantaggi in sintesi

- ottimizzazione della rete grazie al calcolo del carico di rete per le singole porte
- maggiore disponibilità della produzione grazie alla scansione online e alla verifica degli impianti esistenti
- trasparenza prima della messa in servizio mediante importazione e simulazione di progetti STEP 7 esistenti
- efficienza grazie alla protezione degli investimenti nel lungo periodo e allo sfruttamento ottimale delle risorse

SINETPLAN è disponibile in Internet.
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html)

1.1.3 S7 Port Configuration Tool (S7-PCT)

SIMATIC S7-PCT

Il Port Configuration Tool (PCT) è un software di parametrizzazione per PC per i moduli Siemens IO-Link Master e IO-Link Device di qualsiasi costruttore.

Gli IO-Link Device possono essere integrati tramite la descrizione del prodotto standardizzata "IODD", messa a disposizione dal rispettivo costruttore del dispositivo. S7-PCT supporta sia la versione 1.0 sia la versione V1.1 di IODD.

S7-PCT viene richiamato tramite la configurazione hardware dell' IO-Link Master da STEP 7. Se STEP 7 non viene impiegato o l'IO-Link Master non viene utilizzato in un controllore SIMATIC , è possibile anche un funzionamento "standalone".

Ulteriori informazioni su IO-Link sono disponibili in Internet.
(https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html)

1.1.4 S7 Failsafe Configuration Tool (S7-FCT)

SIMATIC S7-FCT

Il Failsafe Configuration Tool (FCT) consente di eseguire la progettazione GSD dei seguenti dispositivi nei sistemi di engineering di altri produttori:

- Periferia SIMATIC selezionata, con funzionamento fail-safe
- Interfacce SIRIUS ACT PROFINET selezionate, con funzionamento fail-safe

Il sistema di engineering deve soddisfare i seguenti requisiti:

- Supporto dell'integrazione di sistema CPD secondo "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO"
- Implementazione di TCI secondo Conformance Class C3

Ulteriori informazioni su S7-FCT si trovano in Internet.
(https://support.industry.siemens.com/cs/ww/it/view/109762827)

1.1.5 Multi Fieldbus Configuration Tool (MFCT)

MultiFieldbus Configuration Tool

MultiFieldbus Configuration Tool (MFCT) è un software basato su PC e assiste nella configurazione di dispositivi MultiFieldbus- e DALI-. MFCT offre inoltre comode opzioni per gli aggiornamenti di massa del firmware dei dispositivi ET 200 con supporto MultiFieldbus- e lettura dei dati del Service di molti altri dispositivi Siemens.

Funzioni di MFCT

- Configurazione di MultiFieldbus:
  Progettazione, configurazione e diagnostica di dispositivi MultiFieldbus-, approntamento dei file di progetto richiesti (file di progetto, UDT-, CSV- e EDS-), trasferimento/esportazione dei file sul dispositivo e/o memorizzazione dei dati.
- Configurazione DALI
  Selezione dispositivi e configurazione online di dispositivi DALI.
- TM FAST:
  Generazione e download di file FPGA-UPD- e FPGA-DB-.
- Manutenzione:
  Scansione della topologia della rete Ethernet, lettura dei dati del Service, assegnazione dei parametri e aggiornamento del firmware.
- Impostazioni:
  Commutazione tra le lingue tedesco e inglese, velocità dello scanner di rete, impostazione dell'adattatore di rete, installazione dei file GSDML- e EDS-.

Requisiti di installazione e di sistema per MFCT

L'MFCT viene eseguito in Microsoft Windows e non richiede né un'installazione né diritti di amministratore.

Per MFCT è necessario installare inoltre i seguenti software:

- Microsoft .NET Framework 4.8 (in Internet è disponibile un programma di installazione offline. (https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0))
- NPcap dalla cartella "Misc"
- PG/PC interface dalla cartella "Misc"
- Microsoft C++ Redistributable per sistemi x86- (i dati di installazione sono disponibili in Internet per il download. (https://aka.ms/vs/15/release/vc_redist.x86.exe))

Il download del tool, ulteriori informazioni nonché la documentazione sulle singole funzioni dell'MFCT sono disponibili in Internet.
(https://support.industry.siemens.com/cs/de/en/view/109773881)

1.1.6 Documentazione tecnica SIMATIC

Ulteriori documenti SIMATIC che integrano le informazioni. Questi documenti e la relativa utilità si trovano ai seguenti link e codici QR.

Industry Online Support completa le possibilità di ottenere informazioni su tutti gli argomenti. Gli esempi applicativi forniscono un supporto nella soluzione dei compiti di automazione.

Panoramica della documentazione tecnica SIMATIC

Qui si trova una panoramica della documentazione relativa a SIMATIC disponibile in Siemens Industry Online Support:

Industry Online Support International
(https://support.industry.siemens.com/cs/ww/it/view/109742705)

Un breve video illustra dove reperire la panoramica della documentazione direttamente in Siemens Industry Online Support e come utilizzare Siemens Industry Online Support su un dispositivo mobile:

Accesso rapido alla documentazione tecnica dei prodotti di automazione tramite video (https://support.industry.siemens.com/cs/it/it/view/109780491/)

Video YouTube: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Conservazione della documentazione

Conservare la documentazione per poterla utilizzare in seguito.

Documentazione allegata in formato digitale:

1. Scaricarle la documentazione pertinente dopo aver ricevuto il prodotto, al più tardi prima del primo montaggio/della prima messa in servizio. Per il download, utilizzare le seguenti opzioni:
   - Industry Online Support International: (https://support.industry.siemens.com)

     Il prodotto è abbinato alla documentazione in base al numero di articolo. Il numero di articolo si trova sul prodotto e sull'etichetta dell'imballo. Ai prodotti con nuove funzioni non compatibili viene assegnato un nuovo numero di articolo e una nuova documentazione.
   - ID Link:

     Se il prodotto è contrassegnato con un ID Link, questo è riconoscibile come codice QR con una cornice e angoli neri in basso a destra. L'ID Link collega alla targhetta identificativa digitale del prodotto. Scansionare il codice QR sul prodotto o sull'etichetta dell'imballo con la fotocamera dello smartphone, con un lettore di codici a barre o un'app di lettura. Richiamare l'ID Link.
2. Conservare questa versione della documentazione.

Aggiornamento della documentazione

La documentazione del prodotto viene aggiornata digitalmente. In particolare se si effettua un ampliamento delle funzioni vengono fornite nuove caratteristiche funzionali nella versione più aggiornata.

1. Scaricare la versione aggiornata come descritto più sopra tramite l'Industry Online Support o l'ID Link.
2. Conservare anche questa versione della documentazione.

mySupport

mySupport consente di sfruttare al meglio il servizio Industry Online Support.

Registrazione	Per poter usufruire della funzionalità completa di mySupport è necessaria una registrazione iniziale. Dopo la registrazione è possibile creare filtri, preferiti e schede nell'area di lavoro personale.
Richiesta di assistenza	I dati personali dell'utente sono già preimpostati nelle richieste di assistenza e l'utente ha modo di controllare in qualsiasi momento lo stato di elaborazione delle richieste che ha presentato.
Documentazione	Nell'area Documentazione è possibile raggruppare la biblioteca personale.

Preferiti	Utilizzare il pulsante "Aggiungi ai preferiti di mySupport" per inserire nei preferiti contenuti particolarmente interessanti o utilizzati di frequente. Al punto "Preferiti" si trova un elenco delle voci preimpostate.
Ultimi messaggi visualizzati	Le pagine richiamate per ultime nel mySupport si trovano in "Ultimi messaggi visualizzati".
Dati CAx	L'area dei dati CAx consente di accedere ai dati attuali del prodotto per il sistema CAx o CAe. Con pochi clic è possibile configurare il proprio pacchetto di download: • immagini del prodotto, disegni quotati in 2D, modelli in 3D, schemi elettrici dell'apparecchio, file macro EPLAN • manuali, curve caratteristiche, istruzioni operative, certificati • dati di base del prodotto

mySupport è disponibile in Internet. (https://support.industry.siemens.com/My/ww/it)

Esempi applicativi

Gli esempi applicativi forniscono diversi strumenti ed esempi utili nella soluzione dei problemi di automazione. In questa sezione vengono illustrate soluzioni che prevedono l'interazione di più componenti del sistema, senza soffermarsi sui singoli prodotti.

Gli esempi pratici sono disponibili in Internet.
(https://support.industry.siemens.com/cs/ww/it/ps/ae)

Avvertenze di sicurezza 2

2.1 Avvertenze generali di sicurezza

Osservare a questo proposito le avvertenze di sicurezza nel manuale di sistema corrispondente.

Avvertenze rilevanti in materia di cybersecurity si trovano al capitolo Industrial Cybersecurity (Pagina 27).

Industrial Cybersecurity 3

Con la digitalizzazione e la crescente interconnessione delle macchine e degli impianti industriali è aumentato anche il rischio di attacchi informatici. È quindi diventato obbligatorio adottare adeguate misure di protezione, in particolare per le infrastrutture critiche.

Le informazioni generali e le misure in materia di Industrial Cybersecurity sono disponibili nel Manuale di sistema e nella Guida alla sicurezza per pannelli operatore SIMATIC HMI (https://support.industry.siemens.com/cs/it/it/view/109481300).

Questo capitolo fornisce una panoramica delle informazioni rilevanti per la sicurezza che riguardano la comunicazione del sistema SIMATIC in uso.

NOTA

Le modifiche del software o dei dispositivi rilevanti per la sicurezza sono documentate nel capitolo Introduzione (Pagina 10).

3.1 Avvertenze di Cybersecurity

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

Al fine di proteggere impianti, sistemi, macchine e reti da minacce cibernetiche, è necessario implementare - e mantenere continuamente - un concetto di cybersecurity industriale globale ed all'avanguardia. I prodotti e le soluzioni Siemens costituiscono soltanto una componente di questo concetto.

È responsabilità dei clienti prevenire accessi non autorizzati ai propri impianti, sistemi, macchine e reti. Tali sistemi, macchine e componenti dovrebbero essere connessi unicamente a una rete aziendale o a Internet se e nella misura in cui detta connessione sia necessaria e solo quando siano attive appropriate misure di sicurezza (ad es. impiego di firewall e segmentazione della rete).

Per ulteriori informazioni inerenti alle misure di cybersecurity industriale che possono essere implementabili potete visitare il sito
https://www.siemens.com/cybersecurity-industry.

I prodotti e le soluzioni Siemens vengono costantemente perfezionati per incrementarne la sicurezza. Siemens raccomanda espressamente che gli aggiornamenti dei prodotti siano effettuati non appena disponibili e che siano utilizzate le versioni più aggiornate. L'utilizzo di versioni di prodotti non più supportate ed il mancato aggiornamento degli stessi incrementa il rischio di attacchi cibernetici.

Per essere informati riguardo agli aggiornamenti dei prodotti, potete iscrivervi a Siemens Industrial Cybersecurity RSS Feed al sito
https://www.siemens.com/cert.

3.2 Informazioni rilevanti in materia di cybersecurity in questo manuale

Osservare tutte le avvertenze rilevanti per la sicurezza contenute in questo manuale di comunicazione.

Avvertenze rilevanti per la sicurezza su...	**Capitolo**
Interfacce	Presentazione del prodotto (Pagina 29)
Porte e protocolli	Opzioni di comunicazione in sintesi (Pagina 35) Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet (Pagina 38)
Comunicazione sicura	Comunicazione sicura (Pagina 56)
Attivazione/disattivazione dei servizi	Attivazione e disattivazione di SNMP (Pagina 125) Assegnazione di indirizzi tramite DHCP (Pagina 404) IP Forwarding (Pagina 423)
Funzioni di sicurezza della comunicazione OPC UA (autenticazione, certificati, creazione di utenti e ruoli, trasmissione sicura dei messaggi)	Comunicazione OPC UA (Pagina 179)
Attivazione delle funzioni di sicurezza nei moduli di comunicazione	Interfaccia virtuale per applicazioni basate su IP (Pagina 432)
Comunicazione con il sistema ridondante S7-1500R/H	Comunicazione con il sistema ridondante S7-1500R/H (Pagina 454)
Protezione tramite Industrial Ethernet Security con CP 1543-1	Industrial Ethernet Security con CP 1543-1 (Pagina 495)
Comunicazione PG/HMI sicura	Comunicazione PG/HMI sicura (Pagina 112)
Protezione di dati riservati	Protezione dei dati di configurazione riservati (Pagina 81)

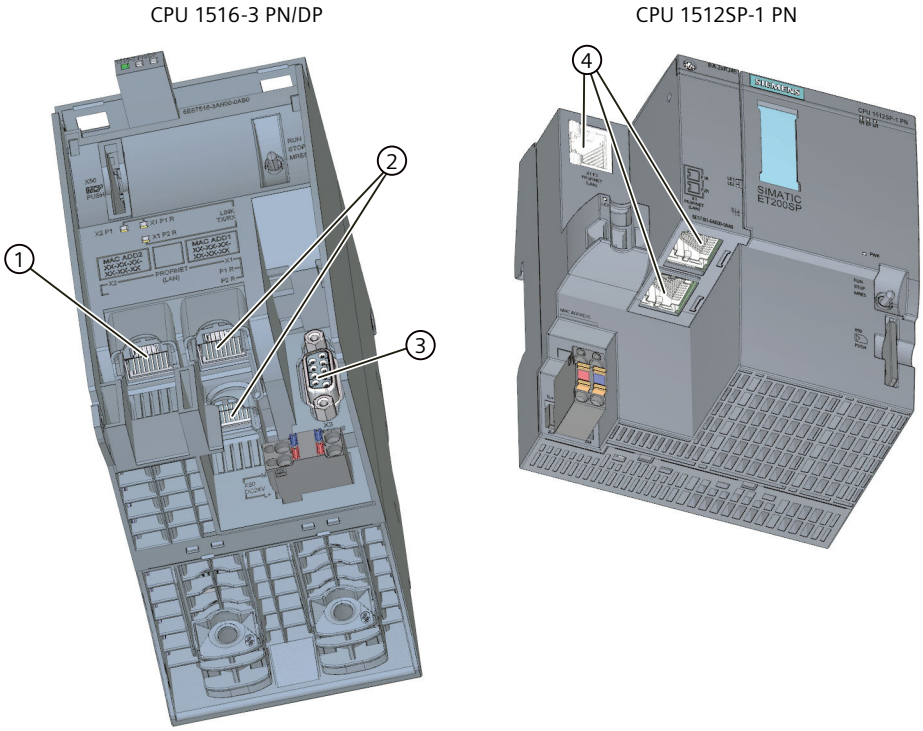
Presentazione del prodotto

4

Le CPU, i moduli e i processori di comunicazione così come i sistemi PC dei sistemi S7-1500, ET 200MP, ET 200SP, ET 200pro e ET 200AL mettono a disposizione diverse interfacce per la comunicazione tramite PROFINET, PROFIBUS e l'accoppiamento punto a punto.

CPU, moduli e processori di comunicazione

Le interfacce PROFINET e PROFIBUS DP sono integrate nelle CPU S7-1500. Ad esempio la CPU 1516-3 PN/DP dispone di 2 interfacce PROFINETe 1 interfaccia PROFIBUS DP. Ulteriori interfacce PROFINET e PROFIBUS DP sono disponibili tramite moduli di comunicazione (CM) e processori di comunicazione (CP).



① Interfaccia PROFINET (X2) con 1 porta

② Interfaccia PROFINET (X1) con switch a 2 porte

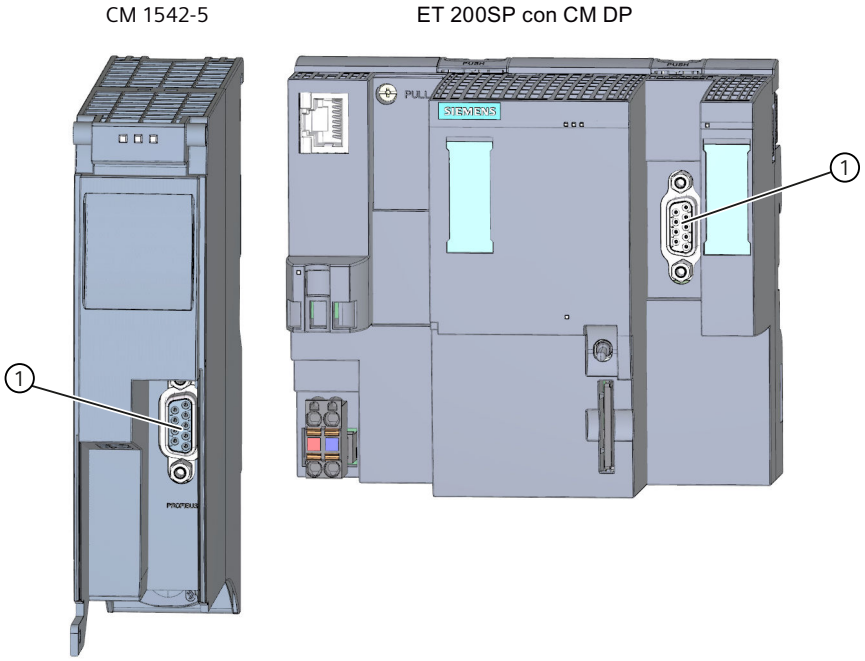
③ Interfaccia PROFIBUS DP (X3)

④ Interfaccia PROFINET (X1) con switch a 3 porte

Figura 4-1 Interfacce della CPU 1516-3 PN/DP e della CPU 1512SP-1 PN

Interfacce dei moduli di comunicazione

Le interfacce dei moduli di comunicazione (CM) ampliano le interfacce delle CPU (ad es. il modulo di comunicazione CM 1542-5 amplia il sistema di automazione S7-1500 con un'interfaccia PROFIBUS).



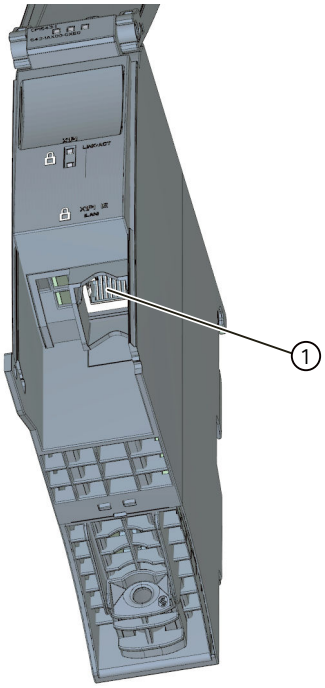
① Interfaccia PROFIBUS DP

Figura 4-2 Interfaccia PROFIBUS DP-del CM 1542-5 e del CM DP (in una CPU ET 200SP)

Interfacce dei processori di comunicazione

Le interfacce dei processori di comunicazione (CP) offrono funzionalità supplementari rispetto alle funzionalità delle interfacce integrate delle CPU. I CP coprono casi applicativi specifici, ad es. il CP 1543-1 offre, tramite la sua interfaccia Industrial Ethernet, funzioni di sicurezza per la protezione delle reti Industrial Ethernet.

CP 1543-1



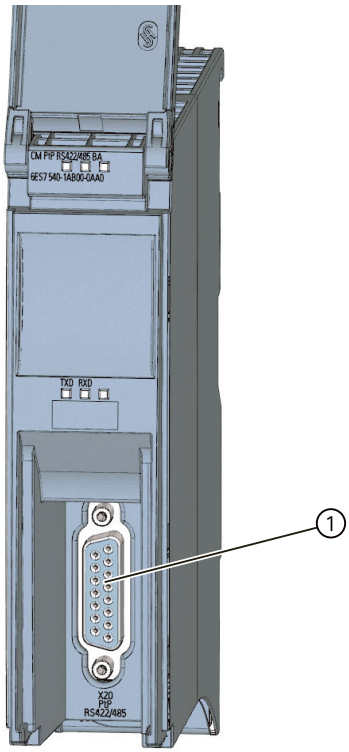
① Interfaccia Industrial Ethernet

Figura 4-3 Interfaccia Industrial Ethernet del CP 1543-1

Interfacce dei moduli di comunicazione per l'accoppiamento punto a punto

I moduli di comunicazione per l'accoppiamento punto a punto consentono la comunicazione attraverso le interfacce RS232, RS422 e RS485, come ad es. la comunicazione Freeport o Modbus.

CM PtP RS422/485 BA

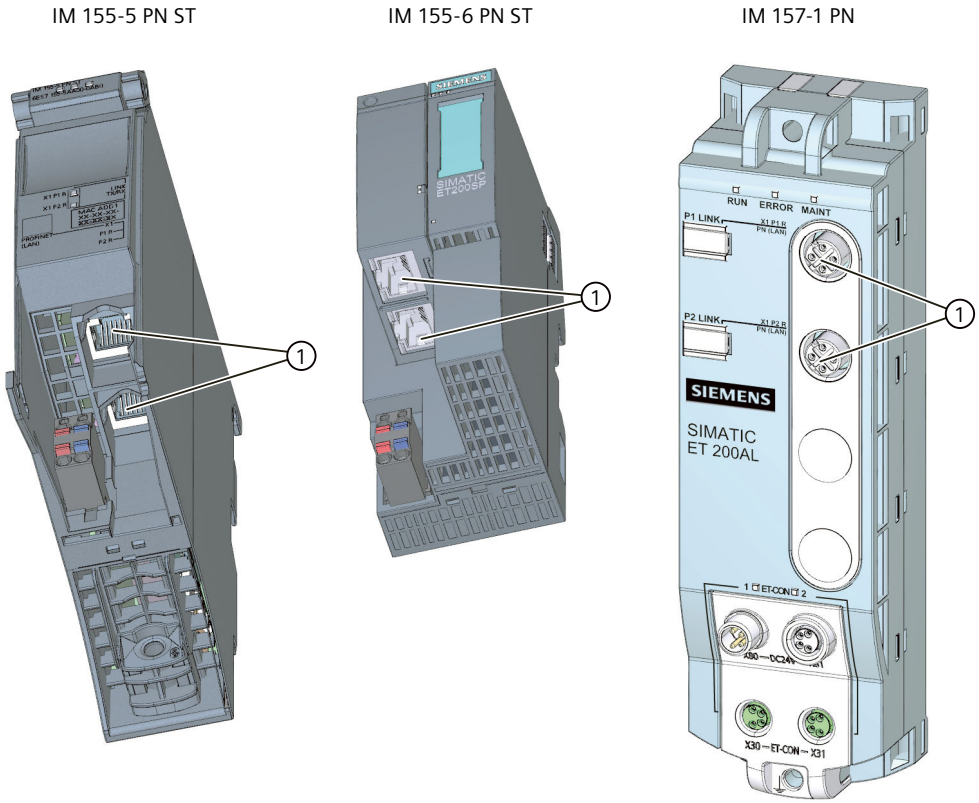


① Interfaccia per l'accoppiamento punto a punto

Figura 4-4 Esempio di interfaccia per l'accoppiamento punto a punto nel CM PtP RS422/485 BA

Interfacce dei moduli di interfaccia

Le interfacce PROFINET e PROFIBUS DP dei moduli di interfaccia (IM) su ET 200MP, ET 200SP e ET 200AL consentono di collegare la periferia decentrata ET 200MP, ET 200SP e ET 200AL a PROFINET o PROFIBUS dell'IO Controller o del master DP.



① Interfaccia PROFINET con switch a 2 porte

Figura 4-5 Interfacce PROFINET IM 155-5 PN ST (ET 200MP), IM 155-6 PN ST (ET 200SP) e IM 157-1 PN (ET 200AL)

Disattivazione della porta di un'interfaccia PROFINET

Le porte attivate rappresentano un rischio potenziale di accesso non autorizzato alla rete e ai programmi.
Per ridurre al minimo il rischio, disattivare tutte le porte inutilizzate.
Procedimento:

1. Selezionare la porta dell'interfaccia PROFINET nella vista dispositivi della CPU/IM di STEP7.
2. Nella finestra di ispezione spostarsi fino a "Opzioni avanzate > Porta [x]> Opzioni porta > Attiva.
3. Disattivare la casella di opzione "Attiva".

Almeno una porta della CPU/IM resta aperta.

Servizi di comunicazione

I servizi di comunicazione descritti nel seguito utilizzano le interfacce e i meccanismi di comunicazione offerti dal sistema tramite le CPU, i moduli e i processori di comunicazione.

Servizi di comunicazione 5

5.1 Opzioni di comunicazione in sintesi

Panoramica delle opzioni di comunicazione

Per la soluzione di compiti di automazione sono disponibili le seguenti opzioni di comunicazione.

Tabella 5-1 Opzioni di comunicazione

Opzioni di comunicazione	Funzionalità	Tramite l'interfaccia:		
		PN/IE[1]	DP	seriale
Comunicazione PG[2]	Per la messa in servizio, il test, la diagnostica	X	X	-
Comunicazione HMI[2]	Per il servizio e la supervisione	X	X	-
Comunicazione aperta tramite TCP/IP[2]	Scambio di dati tramite PROFINET/Industrial Ethernet con TCP/IP Istruzioni: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Comunicazione aperta tramite ISO-on-TCP[2]	Scambio di dati tramite PROFINET/Industrial Ethernet con ISO on TCP Istruzioni: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Comunicazione aperta tramite UDP[2]	Scambio di dati tramite PROFINET/Industrial Ethernet con UDP Istruzioni: • TSEND_C/TRCV_C • TUSEND/TURCV • TCON • T_DISCON	X	-	-
Comunicazione aperta tramite ISO (solo CP con interfaccia PROFINET/Industrial Ethernet)	Scambio di dati tramite PROFINET/Industrial Ethernet con protocollo ISO Istruzioni: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-

1 IE - Industrial Ethernet

2 Osservare le particolarità dell'S7-1500R/H

3 Solo tramite l'interfaccia PROFINET interna della CPU e l'interfaccia Ethernet CP 1543-1 con la funzione "Accesso al PLC tramite modulo di comunicazione" attivata

Opzioni di comunicazione	Funzionalità	Tramite l'interfaccia:		
		PN/IE[1]	DP	seriale
Comunicazione aperta tramite FDL (solo CM 1542-5 dalla versione firmware V2.0)	Scambio di dati tramite PROFIBUS con protocollo FDL Istruzioni: • TSEND_C/TRCV_C • TSEND/TRCV • TUSEND/TURCV • TCON • T_DISCON	-	X	-
Server OPC UA[3]	Scambio di dati con client OPC UA	X	-	-
Comunicazione tramite Modbus TCP	Scambio di dati tramite PROFINET con protocollo Modbus TCP Istruzioni: • MB_CLIENT • MB_SERVER	X	-	-
E-mail	Invio di segnalazioni di processo tramite e-mail Istruzione: • TMAIL_C	X	-	-
FTP (solo CP con interfaccia PROFINET/Industrial Ethernet)	Gestione file e accesso ai file tramite FTF (File Transfer Protocol); il CP può essere client FTP o server FTP Istruzione: • FTP_CMD	X	-	-
Fetch/Write (solo CP con interfaccia PROFINET/Industrial Ethernet)	Servizi server tramite TCP/IP, ISO on TCP e ISO Tramite istruzioni speciali per Fetch/Write	X	-	-
Comunicazione S7	Scambio dati con il protocollo S7 tramite PROFINET/PROFIBUS Istruzioni: • PUT/GET • BSEND/BRCV • USEND/URCV	X	X	-
Accoppiamento punto a punto seriale	Scambio di dati punto a punto con protocollo Freeport, 3964(R), USS o Modbus Tramite istruzioni speciali per PtP, USS o Modbus RTU	-	-	X
Web server	Scambio di dati tramite HTTP(S), ad es. per la diagnostica	X	-	-
SNMP (Simple Network Management Protocol)	Per il controllo e il rilevamento degli errori nelle reti IP; se necessario, parametrizzazione dei componenti IP tramite il protocollo standard SNMP	X	-	-
Sincronizzazione dell'ora	Tramite interfaccia PN/IE: La CPU è il client NTP (Network Time Protocol)	X	-	-
	Tramite interfaccia DP: La CPU/Il CM/CP è l'orologio master o l'orologio slave	-	X	-

1 IE - Industrial Ethernet

2 Osservare le particolarità dell'S7-1500R/H

3 Solo tramite l'interfaccia PROFINET interna della CPU e l'interfaccia Ethernet CP 1543-1 con la funzione "Accesso al PLC tramite modulo di comunicazione" attivata

Informazioni sull'S7-1500R/H

Informazioni sulle possibilità di comunicazione con il sistema ridondante S7-1500R/H sono disponibili nel capitolo Comunicazione con il sistema ridondante S7-1500R/H (Pagina 454).

Ulteriori informazioni

- Le modalità di configurazione della comunicazione PG/HMI basata su TLS e di protezione dei dati di configurazione riservati della CPU, sono illustrate in questo Esempio applicativo (https://support.industry.siemens.com/cs/ww/it/view/109798583).
- La comunicazione CPU-CPU con i SIMATIC Controller (compendio) in generale è illustrata in questo esempio applicativo (https://support.industry.siemens.com/cs/ww/it/view/20982954).
- La biblioteca TIA "LOpcUa" che rende disponibili i blocchi funzionali per l'implementazione di OPC UA PubSub per SIMATIC S7-1500, si trova in questo Esempio applicativo (https://support.industry.siemens.com/cs/ww/it/view/109782455).
- La configurazione della comunicazione Fetch/Write su S7-1500 attraverso un CP1543-1 è descritta in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/102420020).
- Per maggiori informazioni sui servizi Fetch/Write consultare la Guida in linea di STEP 7.
- Per informazioni sull'accoppiamento PtP consultare il manuale di guida alle funzioni CM PtP - Configurazioni di accoppiamenti punto a punto (https://support.industry.siemens.com/cs/it/it/view/59057093).
- La descrizione delle funzionalità del Web server è disponibile nel manuale di guida alle funzioni Web server (https://support.industry.siemens.com/cs/it/it/view/59193560).
- Per informazioni generali sul protocollo standard SNMP vedere le pagine Service & Support in Internet (https://support.industry.siemens.com/cs/it/it/view/15166742). In queste FAQ (https://support.industry.siemens.com/cs/at/it/view/79993228) si trovano domande e risposte sulle interrogazioni SNMP supportate dalle CPU S7-1500 e S7-1200.
- Maggiori informazioni sulla sincronizzazione dell'ora sono disponibili in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/86535497).

5.2 Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet

Questa sezione fornisce una panoramica dei protocolli supportati e dei numeri di porta utilizzati nella comunicazione tramite le interfacce PN/IE. Per ogni protocollo sono indicati i parametri dell'indirizzo, il livello di comunicazione interessato nonché il ruolo e la direzione della comunicazione.

Queste informazioni consentono all'utente di prendere le opportune misure di sicurezza sui protocolli utilizzati per proteggere il sistema di automazione (ad es. firewall). Poiché le misure di sicurezza sono limitate alle reti Ethernet e PROFINET, nelle tabelle non sono riportati i protocolli PROFIBUS.

NOTA

Numeri di porta utilizzati

I numeri di porta indicati sono quelli utilizzati per default dalle CPU S7-1500, dai moduli di comunicazione e dai moduli di interfaccia ET 200. Numerosi protocolli di comunicazione o implementazioni consentono l'utilizzo di altri numeri delle porte.

Le tabelle seguenti mostrano i vari livelli e protocolli utilizzati nelle CPU S7-1500, nei moduli di comunicazione S7-1500 e nei moduli di interfaccia ET 200.

Livelli e protocolli per S7-1500 CPU e Software Controller (tramite l'interfaccia PROFINET della CPU)

Nella tabella seguente sono elencati i protocolli supportati dalle CPU S7-1500, dalle CPU ET 200SP e dalle CPU 1513/1516pro-2 PN. I Software Controller S7-1500 supportano a loro volta i protocolli indicati nella tabella seguente per le interfacce Ethernet assegnate al Software Controller.

Tabella 5-2 Livelli e protocolli per le CPU S7-1500 e Software Controller (tramite l'interfaccia PROFINET della CPU)

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
Protocolli PROFINET				
DCP	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Discovery and Basic Configuration Protocol. DCP rileva i dispositivi PROFINET e abilita le impostazioni di base.	Preimpostazione: attivato fino alla versione FW V3.0, attivato con protezione in scrittura dalla versione FW V3.1. Nella modalità protetta in scrittura DCP non consente l'utilizzo di comandi DCP-Set esterni durante un rapporto di comunicazione attivo. La funzione può essere disattivata nelle proprietà della CPU tramite il Boundary "Fine della rilevazione dei nodi accessibili" dell'interfaccia.

[1] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[2] Non utilizzare per OUC porte già occupate da altri protocolli.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
DHCP Client	68	(4) UDP	Dynamic Host Configuration Protocol. Durante l'avvio dell'interfaccia PROFINET, IP Adress-Suite viene acquisito da un server DHCP.	Preimpostazione: disattivata. Modificabile nelle proprietà della CPU (dalla versione firmware 2.9).
LLDP	Non rilevante	(2) Ethertype 0x88CC (LLDP)	PROFINET Link Layer Discovery Protocol. LLDP rileva e gestisce le correlazioni con i dispositivi PROFINET vicini.	Preimpostazione: attivata. La funzione di trasmissione può essere disattivata tramite Boundary "Fine del riconoscimento topologia" nelle proprietà della CPU, la disponibilità alla ricezione rimane attiva. LLDP utilizza l'indirizzo MAC Multicast speciale: 01-80-C2-00-00-0E.
MRP	Non rilevante	(2) Ethertype 0x88E3 (IEC 62493-2-2010)	Media Redundancy Protocol. MRP permette di controllare i percorsi di trasmissione ridondanti in una topologia ad anello.	Preimpostazione: "Manager (auto)". Modificabile nelle proprietà della CPU. Quando si progetta la CPU e si collega l'interfaccia PN con una sottorete, la preimpostazione in TIA Portal è "non si tratta di un nodo dell'anello". MRP impiega indirizzi MAC Multicast conformi alla norma
PROFINET IO data	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Cyclic IO Data Transfer. I telegrammi PROFINET IO vengono utilizzati per il trasferimento ciclico dei dati IO tra il PROFINET IO Controller e gli IO Device via Ethernet.	Preimpostazione: disattivata. Il protocollo è attivato solo con il traffico dati PROFINET IO.
PROFINET Context Manager	34964	(4) UDP	Comunicazione PROFINET. Gestione dei rapporti di comunicazione e delle applicazioni tra IO Controller e IO Device.	Preimpostazione: Attivata (la porta UDP è aperta). Questa funzione non può essere disattivata.
PTCP	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Precision Transparent Clock Protocol, basato su IEEE 1588. PTCP consente la misurazione del ritardo temporale tra le porte RJ45 e quindi la sincronizzazione dell'ora e dell'intervallo di trasmissione.	Preimpostazione: disattivata. Attivabile con le seguenti progettazioni: • IRT con un dominio Sync. • Interconnessione di porte con una lunghezza specifica del cavo. La funzione può essere disattivata nelle proprietà della CPU tramite il Boundary "Fine del dominio Sync" dell'interfaccia. PTCP impiega indirizzi MAC Multicast conformi alla norma
Protocolli di comunicazione orientati alla connessione				
HTTP Server	80	(4) TCP	Hypertext Transfer Protocol. HTTP viene utilizzato per la comunicazione con il Web server interno alla CPU.	Preimpostazione: disattivata. Attivabile nelle proprietà della CPU. Presupposti: Web server attivabile nelle proprietà della CPU.

[1] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[2] Non utilizzare per OUC porte già occupate da altri protocolli.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
HTTPS Server	443	(4) TCP	Hypertext Transfer Protocol Secure. Il protocollo HTTP viene utilizzato per la comunicazione con il Web server interno alla CPU tramite Secure Socket Layer (SSL).	Preimpostazione: disattivata. Attivabile nelle proprietà della CPU. Presupposti: Web server attivabile nelle proprietà della CPU.
IGMPv2	Non rilevante	(3) Livello di rete	Internet Group Management Protocol. IGMPv2 è un protocollo di rete per l'organizzazione di circuiti multicast (solo UDP multicast).	IGMPv2 è una funzionalità dello stack IP. Questa funzione di sistema viene attivata tramite la funzione Multicast.
ISO-on-TCP Server	102	(4) TCP	ISO-on-TCP Protocol (secondo RFC 1006). Per la comunicazione PG/HMI con il sistema di Engineering (TIA Portal), il protocollo S7 utilizza ISO-on-TCP secondo RFC 1006.	Preimpostazione: attivata. Questa funzione non può essere disattivata.
MODBUS TCP Server / Client	502	(4) TCP	MODBUS Transmission Control Protocol. MODBUS/TCP viene utilizzato nel programma utente tramite le istruzioni MB_CLIENT/MB_SERVER.	Preimpostazione: disattivata. Attivabile nel programma utente utilizzando le istruzioni Modbus TCP.
NTP Client	123	(4) UDP	Network Time Protocol. NTP viene utilizzato per la sincronizzazione dell'ora del sistema della CPU con quella di un server NTP.	Preimpostazione: disattivata. Attivabile nelle proprietà della CPU.
OPC UA Server / Client	4840	(4) TCP	Open Platform Communications Unified Architecture (basata sul protocollo TCP/IP). Uno standard di comunicazione con portata dal livello aziendale fino al livello di campo.	Preimpostazione: disattivata. La funzione server e client è attivabile nelle proprietà della CPU. Possibilità di configurazione dell'accesso del client nel programma utente
OUC[1] Secure OUC Server / Client	1 ... 1999 utilizzabile limitatamente[2] 2000 ... 5000 consigliati	(4) TCP (4) UDP (4) ISO-on-TCP (porta: 102)	Open User Communication (TCP/UDP). Secure Open User Communication (TLS). Le istruzioni OUC consentono di attivare e disattivare il collegamento e di	Preimpostazione: disattivata. L'attivazione del protocollo specifico avviene con l'istruzione Open-User-Communication corrispondente nel programma utente oppure tramite la configurazione dei collegamenti nella vista di rete.

[1] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[2] Non utilizzare per OUC porte già occupate da altri protocolli.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
OUC[1] Secure OUC Server / Client	Dalla versione firmware V3.0, per i collegamenti programmati e configurati vale: 5001 ... 65535 utilizzabile limitatamente[2]	(4) TCP (4) UDP (4) ISO-on-TCP (porta: 102)	trasferire i dati tramite programma utente.	Per le versioni firmware inferiori alla V3.0, vale: • Collegamenti programmati: 5001 ... 49152 • Collegamenti configurati: 5001 ... 65535
SMTP Client	25	(4) TCP	Simple Mail Transfer Protocol. SMTP viene utilizzato per la trasmissione di e-mail	Preimpostazione: disattivato. Attivabile nel programma utente con l'istruzione TMAIL_C.
SMTPS (SMTP over TLS) Client	465	(4) TCP	Simple Mail Transfer Protocol Secure. SMTP viene utilizzato per la trasmissione di e-mail tramite un collegamento protetto.	Preimpostazione: disattivato. Attivabile nel programma utente con l'istruzione TMAIL_C.
SMTP con STARTTLS Client	25 587	(4) TCP	Simple Mail Transfer Protocol con il comando SMTP "STARTTLS". SMTP viene utilizzato per la trasmissione di e-mail	Preimpostazione: disattivato. Attivabile nel programma utente con l'istruzione TMAIL_C.
SNMP Agent	161 162 (trap)	(4) UDP	Simple Network Management Protocol. SNMP consente la lettura e impostazione dei dati di gestione della rete (SNMP managed Objects) utilizzando il manager SNMP.	Preimpostazione: fino alla versione FW V2.9 attivato, dalla versione FW V3.0 disattivato. Attivabile tramite set di dati nel programma utente. Dalla versione FW V3.0 attivabile nelle proprietà della CPU. Dalla versione FW V3.1 attivabile anche protetto in scrittura nelle proprietà della CPU.
Syslog (System Logging)	6514 514	(4) TCP (4) UDP	Syslog è un protocollo standard IETF (RFC 5424) per la trasmissione degli eventi rilevati da una CPU.	Preimpostazione: disattivato. Attivabile nelle proprietà della CPU. Nelle proprietà della CPU è possibile configurare la trasmissione delle segnalazioni syslog a un server syslog. Il rilevamento degli eventi System Logging in una CPU con versione firmware V3.1 o superiore non è disattivabile.

[1] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[2] Non utilizzare per OUC porte già occupate da altri protocolli.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
Reserved	49152 ... 65535	(4) TCP (4) UDP	Se un'applicazione non indirizza una porta locale, la CPU utilizza quest'area della porta per il punto di collegamento attivo.	-

[1] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[2] Non utilizzare per OUC porte già occupate da altri protocolli.

Livelli e protocolli per S7-1500 Software Controller (tramite l'interfaccia Ethernet della pagina Windows)

La tabella sottostante elenca i protocolli supportati dal software controller S7-1500 attraverso le interfacce Ethernet assegnate da Windows.

Tabella 5-3 Livelli e protocolli per S7-1500 Software Controller (tramite l'interfaccia Ethernet della pagina Windows)

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Avvertenze / Preimpostazione
Protocolli PROFINET				
DCP	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Discovery and Basic Configuration Protocol. DCP rileva i dispositivi PROFINET e abilita le impostazioni di base.	Preimpostazione: attivato fino alla versione V30.0. Dalla versione V30.1 attivato con protezione in scrittura. Nella modalità protetta in scrittura DCP non consente l'utilizzo di comandi DCP-Set esterni durante un rapporto di comunicazione attivo. La funzione può essere disattivata tramite Boundary "Fine della rilevazione dei nodi accessibili" nelle proprietà della CPU.
DHCP Client	68	(4) UDP	Dynamic Host Configuration Protocol. Durante l'avvio dell'interfaccia PROFINET, IP Adress-Suite viene acquisito da un server DHCP.	Preimpostazione: disattivata. Modificabile nelle proprietà della CPU (dalla versione firmware 2.9).
Protocolli di comunicazione orientati alla connessione				

[1] Preimpostazione nelle interfacce assegnate in Windows: 81

[2] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[3] Non utilizzare per OUC porte già occupate da altri protocolli.

[4] Non utilizzare per OUC porte già occupate da altre applicazioni Windows.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Avvertenze / Preimpostazione
HTTP Server	Impostabile [1]	(4) TCP	Hypertext Transfer Protocol. HTTP viene utilizzato per la comunicazione con il Web server interno alla CPU.	Preimpostazione: disattivata. Modificabile nelle proprietà della CPU. Per prevenire conflitti con altri Web server in ambiente Windows, adattare i numeri delle porte. Se si utilizza l'accesso al Web server del Software Controller S7-1500, è necessario abilitare la porta assegnata nel firewall di Windows.
IGMPv2	Non rilevante	(3) Livello di rete	Internet Group Management Protocol. IGMPv2 è un protocollo di rete per l'organizzazione di circuiti multicast (solo UDP multicast).	IGMPv2 è una funzionalità dello stack IP. Questa funzione di sistema viene attivata tramite la funzione Multicast.
ISO-on-TCP Server	102	(4) TCP	ISO-on-TCP Protocol (secondo RFC 1006). Per la comunicazione PG/HMI con il sistema di Engineering (TIA Portal), il protocollo S7 utilizza ISO-on-TCP secondo RFC 1006.	Preimpostazione: disattivata.
OUC[2] e Secure OUC	1 ... 1999 utilizzabile limitatamente[3,4]	(4) TCP (4) UDP (4) ISO-on-TCP (porta: 102)	Open User Communication (TCP/UDP). Secure Open User Communication (TLS). Le istruzioni OUC consentono di attivare e disattivare il collegamento e di trasferire i dati sulla base del Socket Layer.	Preimpostazione: disattivata. Attivabile tramite set di dati nel programma utente. Per l'utilizzo dell'OUC è necessario abilitare le porte nel firewall di Windows.
	2000 ... 5000 raccomandato[4]			
	5001 ... 49151 utilizzabile limitatamente[3,4]			

1 Preimpostazione nelle interfacce assegnate in Windows: 81

2 Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

3 Non utilizzare per OUC porte già occupate da altri protocolli.

4 Non utilizzare per OUC porte già occupate da altre applicazioni Windows.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Avvertenze / Preimpostazione
SMTP Client	25	(4) TCP	Simple Mail Transfer Protocol. SMTP viene utilizzato per la trasmissione di e-mail	Preimpostazione: disattivato. Attivabile tramite richiamo del blocco nel programma utente oppure dalla versione V3.0 tramite le impostazioni della CPU.
Syslog (System Logging)	6514 514	(4) TCP (4) UDP	Syslog è un protocollo standard IETF (RFC 5424) per la trasmissione degli eventi rilevati da una CPU.	Preimpostazione: disattivato. Attivabile nelle proprietà della CPU. Nelle proprietà della CPU è possibile configurare la trasmissione delle segnalazioni syslog a un server syslog. Il rilevamento degli eventi System Logging in una CPU con versione firmware V3.1 o superiore non è disattivabile.
Reserved	49152 ... 65535	(4) TCP (4) UDP	Quest'area dinamica della porta viene utilizzata dal punto finale attivo del collegamento, quando l'applicazione non determina il numero della porta locale.	Per l'utilizzo di questa comunicazione, è necessario abilitare le porte nel firewall di Windows.

[1] Preimpostazione nelle interfacce assegnate in Windows: 81

[2] Avvertenza: L'OUC (comunicazione aperta) consente un accesso diretto ai protocolli UDP e TCP. Tenere presenti le restrizioni e le definizioni della porta della IANA (Internet Assigned Numbers Authority).

[3] Non utilizzare per OUC porte già occupate da altri protocolli.

[4] Non utilizzare per OUC porte già occupate da altre applicazioni Windows.

Livelli e protocolli dei moduli di comunicazione S7-1500

Per accedere alla documentazione relativa ai protocolli dei moduli di comunicazione S7-1500 (ad es. CP 1543-1) fare clic qui (https://support.industry.siemens.com/cs/ww/it/view/67700710).

Livelli e protocolli dei moduli di interfaccia

La tabella seguente mostra i protocolli supportati dai moduli di interfaccia ET 200. I protocolli supportati da uno specifico modulo di interfaccia ET 200 sono riportati nei dati tecnici nel relativo manuale del prodotto.

Tabella 5-4 Livelli e protocolli dei moduli di interfaccia ET 200

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
Protocolli PROFINET				
DCP	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Discovery and Basic Configuration Protocol. DCP rileva i dispositivi PROFINET e abilita le impostazioni di base.	Preimpostazione nei moduli di interfaccia di supporto anche quando l'IO Controller sovraordinato supporta DCP: • Protezione in scrittura attivata Nella modalità protetta in scrittura DCP non consente l'utilizzo di comandi DCP-Set esterni durante un rapporto di comunicazione attivo. La funzione può essere disattivata nelle proprietà dell'interfaccia PROFINET.
LLDP	Non rilevante	(2) Ethertype 0x88CC (LLDP)	PROFINET Link Layer Discovery Protocol. LLDP rileva e gestisce le correlazioni con i dispositivi PROFINET vicini.	Preimpostazione: attivata. La funzione di trasmissione può essere disattivata tramite Boundary "Fine del riconoscimento topologia" nelle proprietà dell'interfaccia PROFINET, la disponibilità alla ricezione rimane attiva. LLDP utilizza l'indirizzo MAC Multicast speciale: 01-80-C2-00-00-0E.
MRP	Non rilevante	(2) Ethertype 0x88E3 (IEC 62493-2-2010)	Media Redundancy Protocol. MRP permette di controllare i percorsi di trasmissione ridondanti in una topologia ad anello.	Preimpostazione: "Non si tratta di un nodo dell'anello". Modificabile nelle proprietà dell'interfaccia PROFINET. Se si progetta il modulo di interfaccia e si intende attivare MRP, assegnare al modulo di interfaccia il ruolo della ridondanza del supporto di trasmissione "Client". MRP impiega indirizzi MAC Multicast conformi alla norma
PROFINET IO data	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Cyclic IO Data Transfer. I telegrammi PROFINET IO vengono utilizzati per il trasferimento ciclico via Ethernet dei dati IO tra il PROFINET IO Controller e gli IO Device.	Preimpostazione: disattivata. La funzione si attiva indirettamente non appena il modulo di interfaccia riceve una configurazione valida.
PROFINET Context Manager	34964	(4) UDP	Comunicazione PROFINET. Gestione dei rapporti di comunicazione e delle applicazioni tra IO Controller e IO Device.	Preimpostazione: Attivata (la porta UDP è aperta). Questa funzione non può essere disattivata.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
PTCP	Non rilevante	(2) Ethertype 0x8892 (PROFINET)	PROFINET Precision Transparent Clock Protocol, basato su IEEE 1588. Il PTCP consente le seguenti funzioni: • Misurazione del ritardo temporale tra 2 porte • Sincronizzazione tra intervallo di trasmissione e ora	Preimpostazione per la misurazione del ritardo temporale: attivata nei moduli di interfaccia di supporto. Nel caso della misurazione del ritardo temporale il PTCP non può essere disattivato. Preimpostazione per la sincronizzazione tra intervallo di trasmissione e ora: disattivata. Attivabile dall'IO Controller sovraordinato in funzione della progettazione. PTCP impiega indirizzi MAC Multicast conformi alla norma
Protocolli di comunicazione orientati alla connessione				
IGMPv2	Non rilevante	(3) Livello di rete	Internet Group Management Protocol. IGMPv2 è un protocollo di rete per l'organizzazione di circuiti multicast (solo UDP multicast).	IGMPv2 è una funzionalità dello stack IP. Questa funzione di sistema viene attivata tramite la funzione Multicast.
MODBUS TCP Slave	502	(4) TCP	MODBUS Transmission Control Protocol.	Preimpostazione: disattivata. Attivabile tramite MultiFieldbus Configuration Tool (MFCT).
SNMP Agent	161 162 (trap)	(4) UDP	Simple Network Management Protocol. SNMP consente la lettura e impostazione dei dati di gestione della rete (SNMP managed Objects) utilizzando il manager SNMP.	Preimpostazione nei modulo di interfaccia da supportare: • Sincronizzazione dei valori predefiniti dell'IO-Controller • Disattivato
EtherNet/IP CIP	44818 (TCP) 2222 (UDP)	(4) TCP (4) UDP	I protocolli EtherNet/IP e Common Industrial Protocol (CIP) consentono la comunicazione tra moduli di interfaccia e CPU. I protocolli EtherNet/IP utilizzano dispositivi MultiFieldbus per lo scambio di dati. Il CIP Implicit Messaging viene utilizzato per la trasmissione continua di dati in tempo reale in applicazioni con criticità temporali. Il CIP Explicit Messaging viene utilizzato per il richiamo o la trasmissione mirati di dati di configurazione e di diagnostica.	Preimpostazione: disattivato. Attivabile tramite MultiFieldbus Configuration Tool (MFCT).
TCP/IP	Non rilevante	(4) TCP	Transmission Control Protocol. Il TCP garantisce un collegamento affidabile tra 2 partner di comunicazione.	Preimpostazione: attivata. Questa funzione non può essere disattivata.

Protocollo / Ruoli	Numero della porta	(2) Livello Link Layer (4) Livello di trasporto	Descrizione / Funzione	Preimpostazioni / Avvertenze
UDP	Non rilevante	(4) UDP	User Datagram Protocol. UDP funziona senza collegamento e si basa sul protocollo Internet (IP) non protetto.	Preimpostazione: attivata. Questa funzione non può essere disattivata.
ARP	Non rilevante	(2) Ethertype 0x0806	Adress Resolution Protocol. Assegnazione degli indirizzi IP agli indirizzi MAC.	Preimpostazione: attivata. Questa funzione non può essere disattivata.
IPv4	Non rilevante	(3) Livello di rete	Internet Protocol Version 4. Identificazione di dispositivi con indirizzi IP. L'IPv4 consente ai pacchetti di dati di raggiungere la destinazione dal punto di partenza.	Preimpostazione: attivata. Questa funzione non può essere disattivata.
Reserved	49152 ... 65535	(4) TCP (4) UDP	Se un'applicazione non indirizza una porta locale, la CPU utilizza quest'area della porta per il punto di collegamento attivo.	-

5.3 Panoramica delle risorse di collegamento

Risorse di collegamento

Alcuni servizi di comunicazione necessitano di collegamenti. I collegamenti occupano delle risorse nelle CPU, CP e CM interessati (ad es. aree di memoria nel sistema operativo della CPU). Nella maggior parte dei casi ogni collegamento occupa una risorsa per ogni CPU/CP/CM. Nella comunicazione HMI ogni collegamento HMI richiede fino a 3 risorse.

Le risorse di collegamento disponibili dipendono dalla CPU, dai CP e CM utilizzati e non possono superare il limite superiore definito per il sistema di automazione.

Risorse di collegamento disponibili in una stazione

Il numero max. di risorse di una stazione è determinato dalla CPU.

Ogni CPU è dotata di risorse di collegamento riservate per la comunicazione PG, HMI e server web. Sono inoltre disponibili delle risorse per altri servizi di comunicazione che possono essere utilizzate ad es. per SNMP, collegamenti e-mail, comunicazione HMI e S7 e comunicazione aperta.

Quando vengono occupate le risorse di collegamento?

Il momento in cui vengono occupate le risorse di collegamento dipende dal tipo di configurazione del collegamento: se è automatica, programmata o progettata (vedere il capitolo Configurazione di un collegamento (Pagina 49)).

Ulteriori informazioni

Maggiori informazioni sull'occupazione e sulla visualizzazione delle risorse di collegamento in STEP 7 sono disponibili al capitolo Risorse di collegamento (Pagina 436).

5.4 Configurazione di un collegamento

Collegamento automatico

STEP 7 configura automaticamente un collegamento (ad es. un collegamento tramite PG o HMI), purché l'interfaccia PG/PC sia stata collegata fisicamente ad un'interfaccia della CPU e assegnata in STEP 7 nella finestra di dialogo "Collega online".

Configurazione programmata del collegamento

Il collegamento programmato viene configurato nell'editor di programma di STEP 7 all'interno di una CPU attraverso la parametrizzazione delle istruzioni di comunicazione, ad es. TSEND_C.

La semplice superficie operativa supporta l'utente nella definizione dei parametri di collegamento (nella finestra di ispezione, nelle proprietà dell'istruzione).

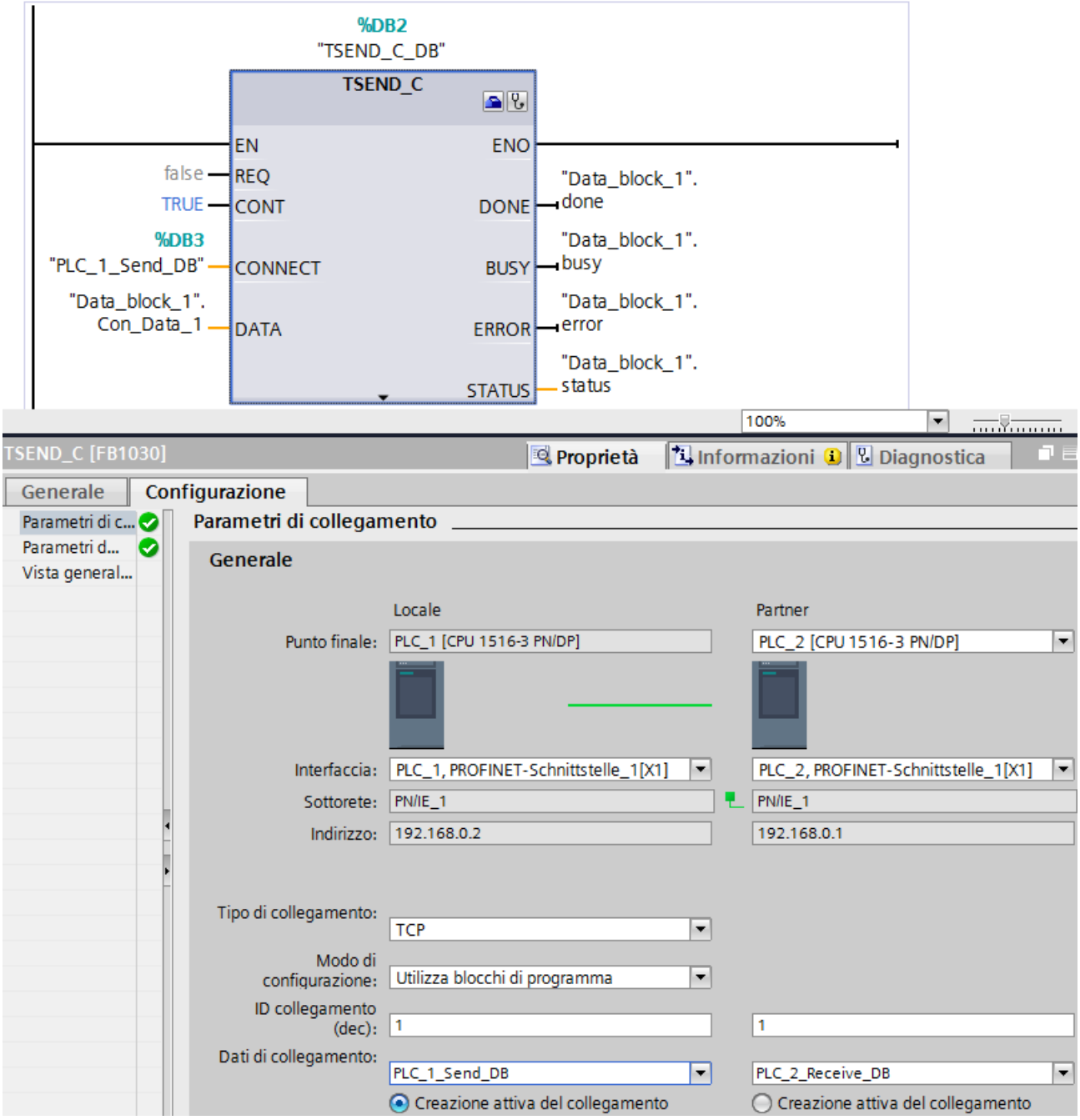


Figura 5-1 Configurazione programmata

Configurazione progettata del collegamento

Il collegamento progettato si configura nella vista di rete dell'editor hardware e di rete di STEP 7 all'interno di una CPU o di un software controller.

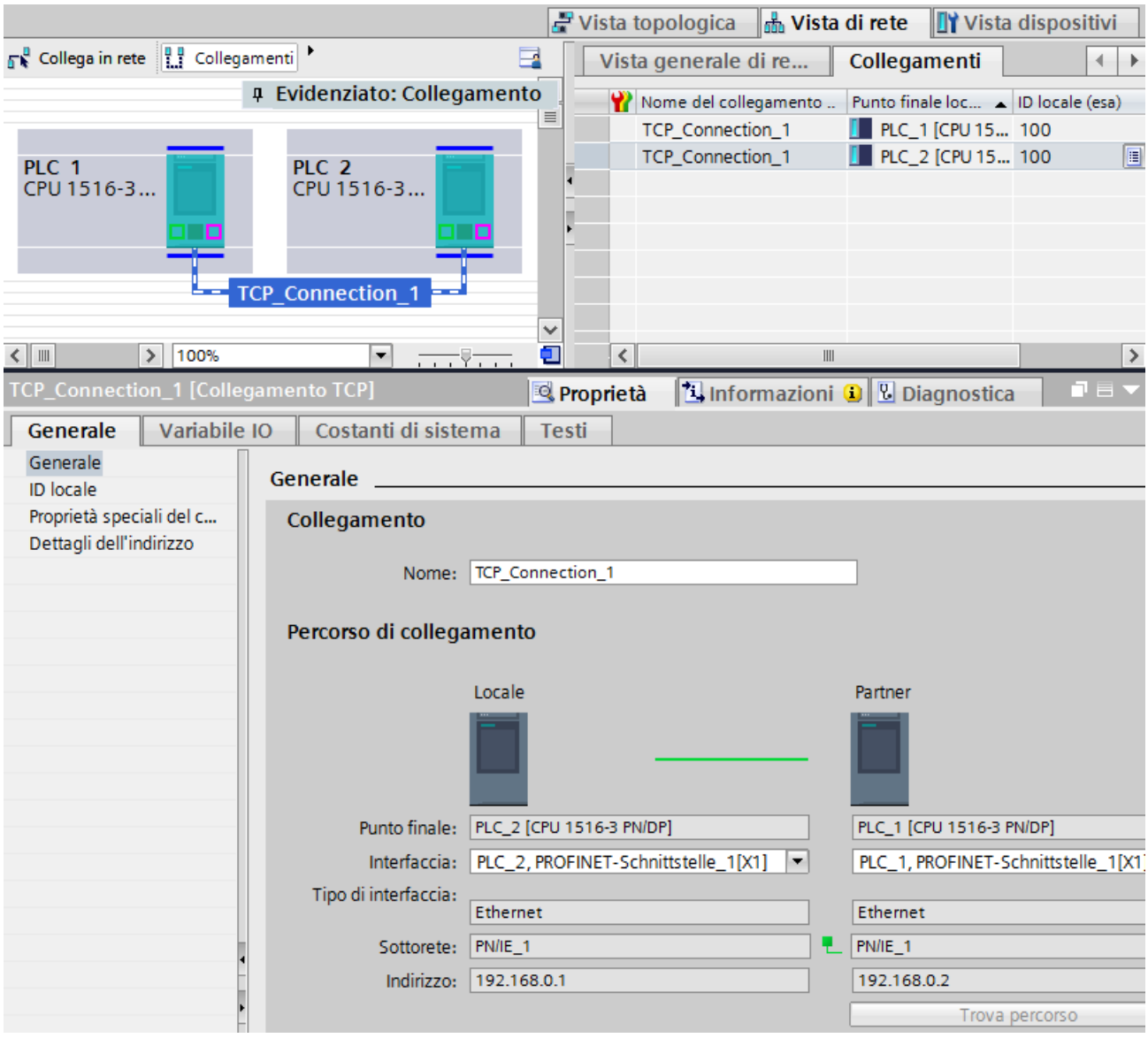


Figura 5-2 Configurazione progettata

Effetti sulle risorse di collegamento della CPU

Spesso si può scegliere tra un collegamento progettato o uno programmato. La configurazione programmata consente l'abilitazione delle risorse di collegamento dopo la trasmissione dei dati. Come i collegamenti instradati tramite router, i collegamenti programmati non sono garantiti, ovvero vengono creati solo se sono disponibili le risorse. Nella configurazione progettata la risorsa è disponibile dal termine del download della configurazione fino alla sua successiva modifica. Pertanto, per la creazione del collegamento con collegamenti progettati sono riservate le risorse necessarie. La tabella "Risorse di collegamento" nella finestra di ispezione della CPU mostra una panoramica delle risorse già occupate e di quelle ancora disponibili.

Come si possono configurare i vari tipi di collegamento?

Tabella 5-5 Configurazione del collegamento

Collegamento	Automatico	Configurazione programmata	Configurazione progettata
Collegamento PG	X	-	-
Collegamento HMI	X	-	X
Comunicazione web	X	-	-
Comunicazione server OPC UA	X	-	-
Comunicazione client OPC UA	-	X	-
Comunicazione aperta tramite collegamento TCP/IP	-	X	X
Comunicazione aperta tramite collegamento ISO-on-TCP	-	X	X
Comunicazione aperta tramite collegamento UDP	-	X	X
Comunicazione aperta tramite collegamento ISO	-	X	X
Comunicazione aperta tramite collegamento FDL	-	X	X
Comunicazione tramite collegamento Modbus TCP	-	X	-
Collegamento e-mail	-	X	-
Collegamento FTP	-	X	-
Collegamento S7*	-	-	X

* Tenere presente che nella CPU S7-1500 l'impiego della comunicazione PUT/GET deve essere abilitato nelle proprietà della CPU stessa. Maggiori informazioni sono disponibili nella Guida in linea a STEP 7.

Ulteriori informazioni

Maggiori informazioni sull'occupazione e sulla visualizzazione delle risorse di collegamento in STEP 7 sono disponibili al capitolo Risorse di collegamento (Pagina 436).

5.5 Coerenza dei dati

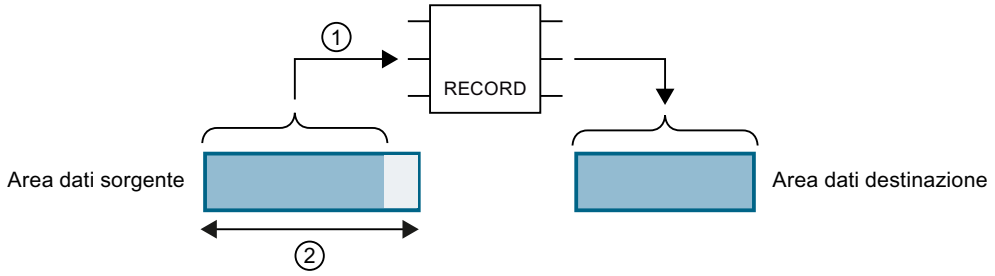
Definizione

Nel trasferimento dati la coerenza degli stessi è un aspetto importante da tenere in considerazione quando si progetta un compito di comunicazione. In caso contrario possono verificarsi malfunzionamenti.

Un’area dati che non può essere modificata da processi simultanei viene definita area di dati coerente. Ciò significa che un'area di dati correlati che abbia dimensioni maggiori dell'area dati coerente max. può essere costituita in uno stesso momento da dati in parte nuovi e in parte vecchi.

Si può verificare un'incoerenza quando un'istruzione di comunicazione viene interrotta ad es. da un OB di interrupt di processo con priorità maggiore. Di conseguenza si interrompe anche il trasferimento dell’area dati. Se ora il programma utente modifica in questo OB i dati che non sono ancora stati elaborati dall'istruzione di comunicazione, i dati trasferiti derivano da momenti diversi.

La figura seguente mostra un’area dati più piccola delle dimensioni max. dell’area dati coerente. In questo caso, al trasferimento dell’area dati viene garantito che il programma utente non provochi un’interruzione durante l’accesso ai dati e che i dati non vengano modificati.

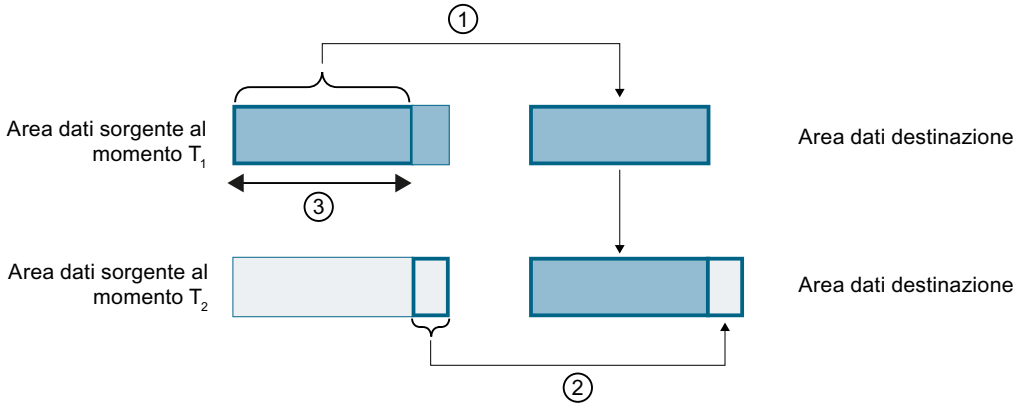


① L’area dati sorgente è minore delle dimensioni max. dell’area dati coerente (③). L’istruzione trasferisce i dati correlati nell’area dati di destinazione.

② Dimensioni max. dell’area di dati coerenti

Figura 5-3 Trasmissione coerente dei dati

La figura seguente mostra un'area dati che supera le dimensioni max. dell'area dati coerente. In questo caso i dati possono essere modificati durante un'interruzione del trasferimento. Si verifica un'interruzione anche se ad es. si deve trasferire l'area dati in diverse parti. Se i dati vengono modificati durante l'interruzione, i dati trasferiti provengono da momenti diversi.



① L'area dati sorgente è maggiore delle dimensioni max. dell'area dati coerente (③). Nel momento T1 l'istruzione trasferisce dall'area sorgente all'area di destinazione solo una quantità di dati che entra nell'area dati coerente.

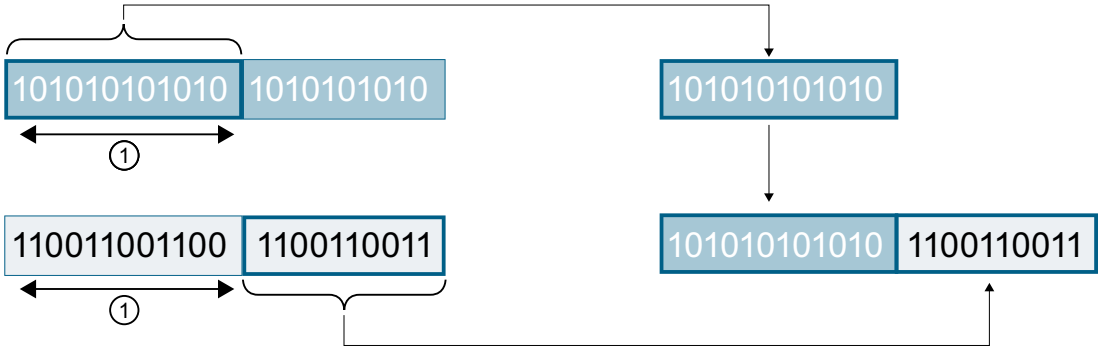
② Nel momento T2 l'istruzione trasferisce il resto dall'area dati sorgente all'area dati di destinazione. Dopo il trasferimento, nell'area dati di destinazione sono presenti dati di momenti diversi. Se i dati contenuti nell'area sorgente nel frattempo sono cambiati, può insorgere un'incoerenza.

③ Dimensioni max. dell'area di dati coerenti

Figura 5-4 Trasferimento di dati maggiori dell'area dati coerente max.

Esempio di incoerenza

La figura seguente mostra un esempio di modifica dei dati durante la trasmissione. Nell'area dati di destinazione sono presenti dati di momenti diversi.



① Dimensioni max. dell'area di dati coerenti

Figura 5-5 Esempio: modifica dei dati durante la trasmissione

Coerenza dei dati massima specifica del sistema per S7-1500:

Se si mantiene la dimensione massima specifica del sistema per i dati coerenti non si verifica alcuna incoerenza. Nell'S7-1500 i dati di comunicazione vengono copiati in modo coerente nella/dalla memoria utente in blocchi di max. 512 byte durante il ciclo del programma. Per tutte le aree dati di dimensioni maggiori la coerenza dei dati non è garantita. Se è necessaria una determinata coerenza dei dati, i dati di comunicazione nel programma utente della CPU non devono superare 512 byte. L'accesso coerente a queste aree di dati è possibile ad es. da un dispositivo HMI con funzione di lettura/scrittura delle variabili.

Se si devono trasmettere più dati coerenti di quanti previsti dalle dimensioni max. specifiche del sistema, è necessario garantire personalmente la coerenza dei dati con misure adeguate nel programma utente.

Garanzia della coerenza dati

Impiego di istruzioni per l'accesso ai dati comuni:

Se il programma utente contiene istruzioni per la comunicazione che accedono a dati comuni, ad es. TSEND/TRCV, si può coordinare direttamente l'accesso a questa area di dati ad es. con il parametro "DONE". La coerenza dei dati delle aree che vengono trasferite con un'istruzione di comunicazione può pertanto essere garantita nel programma utente.

NOTA

Misure nel programma utente

Per ottenere la coerenza dei dati è possibile copiare i dati da trasferire in un'area separata (ad es. un blocco dati globale). Mentre il programma continua a funzionare con i dati originali, è possibile trasferire in modo coerente i dati salvati nell’area dati separata con l’istruzione di comunicazione.

Per la copia utilizzare istruzioni che non si possono interrompere, ad es. UMOVE_BLK o UFILL_BLK. Queste istruzioni assicurano una coerenza dei dati fino a 16 KByte.

Impiego di istruzioni PUT/GET o scrittura/lettura tramite comunicazione HMI:

Nella comunicazione S7 con le istruzioni PUT/GET o la scrittura/lettura tramite comunicazione HMI occorre considerare le dimensioni delle aree di dati coerenti già durante la programmazione o la progettazione. Nel programma utente di un S7-1500 server non è disponibile un’istruzione che possa coordinare il trasferimento dei dati nel programma utente. S7-1500 aggiorna i dati scambiati attraverso le istruzioni PUT/GET durante l’esecuzione del programma utente. Non esiste all’interno dell’elaborazione del programma utente ciclico un momento in cui i dati vengono scambiati in modo coerente. La lunghezza dell'area dati da trasferire deve essere minore di 512 byte.

Maggiori informazioni

- Il numero massimo di dati coerenti è riportato anche nei dati tecnici sui manuali del prodotto dei moduli di comunicazione.
- Maggiori informazioni sulla coerenza dei dati sono disponibili nella descrizione delle istruzioni nella Guida in linea a STEP 7.

5.6 Comunicazione sicura

5.6.1 Nozioni di base sulla comunicazione sicura

5.6.1.1 Informazioni utili sulla comunicazione sicura

Per STEP 7 (TIA Portal) a partire dalla V14 e per le CPU S7-1500 a partire dal firmware V2.0, le opzioni per la comunicazione sicura (Secure Communication) sono state ampliate considerevolmente.

Con la denominazione "CPU S7-1500" si intendono anche le varianti di CPU S7-1500F, S7-1500T, S7-1500C e le CPU S7-1500pro e ET200SP.

Le seguenti versioni contengono ulteriori componenti che supportano la comunicazione sicura (ad es. Secure OUC), vedere il prossimo paragrafo.

Dalla versione firmware V4.4, anche le CPU S7-1200 supportano la comunicazione sicura.

Presupposti

- CPU che supportano il DB di descrizione del collegamento con la struttura dell'SDT TCON_IP_V4_SEC o SDT TCON_QDN_SEC. Si tratta delle seguenti CPU:
  - S7-1200 dalla versione firmware V4.4
  - S7-1500 dalla versione firmware V2.0
- Inoltre, in via opzionale, con le seguenti CPU:
  - CP 1243-1 dalla versione firmware V3.2
  - CP 1243-8 IRC dalla versione firmware V3.2
  - CP 1543-1 dalla versione firmware V2.0
  - CP 1545-1
  - CP 1543SP-1

  Secure Communication tramite CP 1242-7 GPRS V2 non è possibile.

Public Key Infrastructure (PKI)

L'attributo "secure" viene utilizzato per identificare i meccanismi di comunicazione basati sulla Public Key Infrastructure (PKI) (ad es. RFC 5280 per Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile). Per Public Key Infrastructure (PKI) si intende un sistema in grado di creare, distribuire e controllare certificati digitali. I certificati digitali vengono utilizzati all'interno della PKI per proteggere le comunicazioni elettroniche. Se una PKI si avvale della crittografia a chiave asimmetrica, i messaggi possono essere dotati di firma digitale e crittografati all'interno di una rete.

I componenti progettati in STEP 7 (TIA Portal) per la comunicazione sicura utilizzano la crittografia a chiave asimmetrica con chiave pubblica (Public Key) e privata (Private Key). Come protocollo di crittografia viene utilizzato il TLS (Transport Layer Security). TLS è la versione successiva del protocollo SSL (Secure Sockets Layer).

Obiettivi della comunicazione sicura

La comunicazione sicura viene utilizzata per raggiungere i seguenti obiettivi:

- Riservatezza:
  i dati rimangono segreti e illeggibili per chi si mettesse "in ascolto" senza autorizzazione.
- Integrità:
  il messaggio che arriva al destinatario è lo stesso, invariato, che ha trasmesso il mittente. Durante il trasporto il messaggio non è stato modificato.
- Autenticazione del punto finale:
  il partner della comunicazione come punto finale è esattamente quello che dive di essere e che deve essere raggiunto. L'identità del partner è verificata.

Se questi obiettivi in passato erano importanti per il mondo dell'IT e per i computer collegati in rete, oggi anche nel mondo dell'industria le macchine e i controllori sono collegati in rete e i dati da proteggere sono esposti allo stesso rischio, perciò anche qui è necessario uno scambio di dati che soddisfi requisiti di sicurezza molto elevati.

Come in passato, rimane e rimarrà in uso la protezione della cella di automazione con l'aiuto del concetto di protezione a livello di cella mediante firewall o collegamento VPN, ad es. con il modulo Security.

Tuttavia è in aumento la richiesta di comunicazione, anche con il trasferimento di dati a computer esterni in forma crittografata su Intranet o su reti pubbliche.

Principi comuni della comunicazione sicura

A prescindere dal contesto, la comunicazione sicura si basa sul concetto di Public Key Infrastructure (PKI) e comprende i seguenti componenti:

- Crittografia a chiave asimmetrica. Questo tipo di crittografia consente di:
  - Crittografare o decodificare i messaggi con l'aiuto di chiavi pubbliche o private;
  - Verificare le firme su messaggi e certificati.

    I messaggi/certificati vengono firmati con la chiave privata del mittente/proprietario del certificato. Il destinatario/revisore verifica la firma con la chiave pubblica del mittente/proprietario del certificato.
- Trasporto e salvataggio della chiave pubblica con l'aiuto di certificati X.509:
  - I certificati X.509 sono dati con firma digitale che consentono di verificare l'autenticità delle chiavi pubbliche e delle identità ad esse collegate.
  - I certificati X.509 possono contenere informazioni che caratterizzano o limitano con maggiore precisione l'utilizzo della chiave pubblica. Ad es. a partire da quando una chiave pubblica è valida in un certificato e da quando non è più valida.
  - I certificati X.509 contengono informazioni protette sull'emittente.

Le descrizioni che seguono forniscono una panoramica dei concetti di base necessari ad es. per l'utilizzo dei certificati in STEP 7 (TIA Portal) o per la programmazione delle istruzioni di comunicazione per la secure Open User Communication (sOUC).

Comunicazione sicura in STEP 7

Dalla V14 STEP 7 mette a disposizione la PKI di volta in volta necessaria per la progettazione e il funzionamento di una comunicazione sicura.

Esempi:

- Con il protocollo TLS (Transport Layer Security) l'Hypertext Transfer Protokoll (HTTP) diventa Hypertext Transfer Protokoll Secure (HTTPS). Poiché HTTPS è una combinazione di HTTP e TLS, nel corrispondente RFC viene definito "HTTP over TLS". L'utilizzo di HTTPS si riconosce nel browser dall'URL nella riga degli indirizzi che inizia con "https://" anziché "http://". La maggior parte dei browser, inoltre, evidenziano visivamente i collegamenti sicuri di questo tipo.
- Open User Communication diventa secure Open User Communication. Il protocollo di base è sempre il TLS.
- Anche i provider d posta elettronica offrono l'accesso tramite "Secure SMTP over TLS" per garantire la sicurezza della comunicazione via e-mail.

La figura seguente mostra il protocollo TLS all'interno dei livelli di comunicazione.

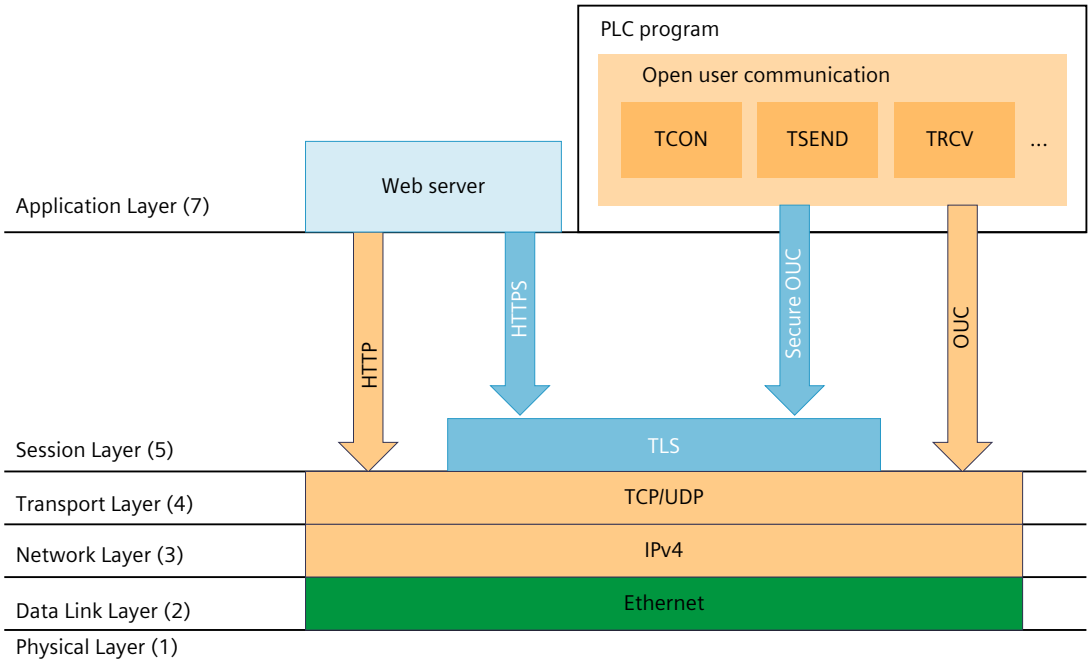


Figura 5-6 Protocollo TLS all'interno dei livelli di comunicazione

Comunicazione sicura su OPC UA

Nelle CPU S7-1500 con firmware V2.0 o superiore è implementato un server OPC UA. Anche OPC UA Security comprende l'autenticazione, la crittografia e l'integrità dei dati tramite certificati digitali X.509 e utilizza quindi a sua volta un'infrastruttura Public Key Infrastructure (PKI). A seconda dei requisiti dell'applicazione è possibile scegliere diversi livelli Security per la sicurezza del punto finale. Alla descrizione della funzionalità server OPC UA è dedicato un capitolo a parte.

Comunicazione sicura per la comunicazione PG/HMI

Con i componenti centrali di TIA Portal, STEP 7 e WinCC, a partire dalla versione V17 in combinazione con gli attuali controllori e dispositivi HMI viene implementata una nuova comunicazione PG/HMI standardizzata e sicura (secure), denominata in breve Comunicazione PG/HMI.

Ulteriori informazioni

Per ulteriori informazioni sull'OPC UA consultare il cap. Utilizzo della CPU S7-1500 come server OPC UA (Pagina 232).

Per maggiori informazioni sulla comunicazione PG/HMI sicura vedere il cap. Comunicazione PG/HMI sicura (Pagina 112).

5.6.1.2 Caratteristiche di sicurezza che dipendono dal pannello operatore

Transport Layer Security (TLS) è un protocollo di sicurezza ampiamente utilizzato che migliora la sicurezza dei dati per la comunicazione. Nel sistema di automazione S7-1500, TLS per la comunicazione sicura viene utilizzato per le seguenti applicazioni basate su certificati:

- Web server (variante di protocollo HTTPS)
- Secure Open User Communication (OUC) incl. Secure E-Mail (istruzione TMAIL_C)
- Comunicazione PG/HMI sicura

TLS garantisce l'autenticazione, la riservatezza e l'integrità della comunicazione tra client e server per le applicazioni indicate, ad esempio tra il Web server della CPU e i Web browser, per visualizzare una pagina web di diagnostica della CPU.

Le applicazioni server e client OPC UA non utilizzano direttamente TLS, ma metodi crittografici analoghi.

TLS è in continua evoluzione, il che significa che ne esistono diverse versioni che differiscono in termini di suite Cypher supportate (raccolta standardizzata di metodi crittografici) e prestazioni.

La descrizione del protocollo TLS è compito dell'Internet Engineering Task Force (IETF). Vale la seguente assegnazione:

- TLS 1.3 è definito nella RFC 8446
- TLS 1.2 è definito nella RFC 5246

Inoltre non sempre i dispositivi supportano tutti i metodi crittografici definiti nelle RFC; di conseguenza dopo la connessione il client e server negoziano un metodo supportato da entrambi (Handshake) e i parametri da utilizzare.

Versioni TLS supportate S7-1500

La seguente tabella mostra quali versioni di TLS sono supportate nelle diverse versioni del firmware della CPU.

Versione del firmware della CPU	Versione TLS supportata
V3.0	TLS 1.2, TLS 1.3
V2.9	TLS 1.2, TLS 1.3
V2.8 ... V2.0	TLS 1.2

Metodi e parametri di crittografia supportati per la creazione dei certificati

Per generare la chiave pubblica per un nuovo certificato si devono impostare il metodo e i parametri di crittografia in TIA Portal. Questi parametri del certificato dipendono dal dispositivo e dall'applicazione utilizzata.

Opzione possibile: Nelle proprietà della CPU, selezionare l'area "Protezione & Security > Gestione certificato" e creare un nuovo certificato del dispositivo. La finestra di dialogo "Crea certificato" dell'area "Parametri del certificato" contiene le impostazioni per il metodo e i parametri di crittografia.

Esempio: RSA 2048 corrisponde al metodo di crittografia asimmetrica RSA con lunghezza della chiave di 2048 bit.

La tabella sottostante indica i metodi e i parametri di crittografia supportati in funzione dei Service e dell'applicazione CPU.

Metodo/parametri di crittografia S7-1500 (firmware V3.0)	Web server (HTTPS) Comunicazione PG/HMI sicura Secure OUC	OPC UA
EC prime256v1	Sì	No
EC secp384r1	Sì	No
EC secp256k1	No	No
RFC 1024	Sì	Sì
RFC 2048	Sì	Sì
RFC 4096	Sì	Sì
RFC 8192	No	No

5.6.1.3 Riservatezza grazie alla crittografia

Un importante contributo alla sicurezza dei dati è dato dalla crittografia dei messaggi. Se i messaggi crittografati vengono intercettati da terzi durante il trasporto, il potenziale "intruso" non può utilizzarli in alcun modo.

Esiste tutta una serie di procedimenti matematici (algoritmi) per la crittografia dei messaggi.

Tutti gli algoritmi hanno in comune la capacità di elaborare un parametro "chiave" per cifrare o decifrare un messaggio.

- Algoritmo + chiave + messaggio => messaggio crittografato
- Messaggio crittografato + chiave + algoritmo => messaggio (decodificato)

Crittografia a chiave simmetrica

L'aspetto fondamentale della crittografia a chiave simmetrica è che entrambi i partner della comunicazione utilizzano la stessa chiave per crittografare e per decodificare i messaggi, come mostra la figura seguente. Bob utilizza la stessa chiave di crittografia che Alice usa per decodificare il messaggio. In generale si dice anche che entrambe le parti condividono come segreto la chiave segreta, con cui possono crittografare o decodificare un messaggio.

① Bob codifica il proprio messaggio con la chiave simmetrica

② Alice decodifica il messaggio crittografato con la chiave simmetrica

Figura 5-7 Crittografia a chiave simmetrica

Per rendere chiaro il procedimento è possibile paragonarlo a una ventiquattrore per la quale mittente e destinatario possiedono la stessa chiave.

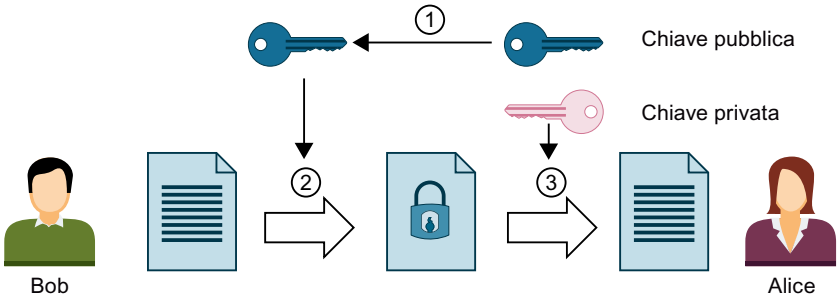
- Vantaggi: Gli algoritmi di crittografia simmetrica (ad es. AES, Advanced Encryption Algorithm) sono veloci.
- Svantaggi: Come far avere la chiave al destinatario senza che finisca nelle mani sbagliate? Questo è un problema di distribuzione delle chiavi. Inoltre, una volta intercettata, la chiave può essere indovinata in un numero sufficientemente elevato di casi, per cui diventa necessario concordare una nuova chiave piuttosto di frequente.

Se il numero dei partner della comunicazione è elevato, inoltre, sarà necessario distribuire anche un numero elevato di chiavi.

Crittografia a chiave asimmetrica

La crittografia a chiave asimmetrica funziona con una coppia di chiavi costituita da una chiave pubblica e una chiave privata. In combinazione con una PKI può essere definita anche crittografia a chiave pubblica o solo crittografia PKI. Un partner della comunicazione, nella figura in basso Alice, possiede una chiave privata e una chiave pubblica. La chiave pubblica viene messa a disposizione del pubblico, ovvero di ogni potenziale partner della comunicazione. Chiunque abbia la chiave pubblica può decodificare i messaggi per Alice. Nella figura in basso, Bob.

La chiave privata di Alice, che deve essere tenuta segreta, viene utilizzata da Alice per decodificare un messaggio crittografato a lei destinato.



① Alice mette a disposizione di Bob la propria chiave pubblica. In questo caso non sono necessarie particolari precauzioni, Perché chiunque può utilizzare la chiave pubblica per inviare messaggi ad Alice se è sicuro che è effettivamente la chiave pubblica di Alice.

② Bob codifica il proprio messaggio con la chiave pubblica di Alice.

③ Alice decodifica il messaggio crittografato di Bob con la propria chiave privata. Poiché solo Alice è in possesso della chiave privata e non la cede ad altri, è l'unica a poter decifrare questo messaggio. Con la chiave privata può decodificare qualsiasi messaggio che sia stato crittografato con la sua chiave pubblica - non solo quelli di Bob.

Figura 5-8 Crittografia a chiave asimmetrica

Per rendere comprensibile il procedimento è possibile paragonarlo a una cassetta delle lettere in cui chiunque può inserire una lettera ma soltanto chi è in possesso della chiave la può prelevare.

- Vantaggi: un messaggio crittografato con una chiave pubblica può essere decodificato solo da chi possiede la chiave privata. Poiché si deve utilizzare un'altra chiave (privata) per decodificare il messaggio, è anche molto più difficile individuare la chiave giusta in una moltitudine di messaggi crittografati. Le chiavi pubbliche non devono essere tenute strettamente segrete come nel caso delle chiavi simmetriche.

  Un ulteriore vantaggio è la semplicità con cui vengono distribuite le chiavi pubbliche. Con la crittografia a chiave asimmetrica non è necessario utilizzare un canale con una particolare protezione per trasmettere le chiavi pubbliche dal destinatario al mittente che codifica i messaggi. Per la gestione delle chiavi, quindi, sono necessarie meno operazioni che per la crittografia a chiave simmetrica.

- Svantaggi: algoritmo ad elevata intensità di calcolo (ad es. l'algoritmo RSA, che prende il nome dai tre matematici Rivest, Shamir e Adleman), perciò performance minore rispetto alla crittografia simmetrica.

La crittografia nella pratica

Nella pratica, come ad es. nel caso del server Web della CPU e della Secure Open User Communication, viene utilizzato il protocollo TLS sul rispettivo livello dell'applicazione. I livelli dell'applicazione sono ad es. HTTP o SMTP, come spiegato nella sezione precedente.

TLS (Transport Layer Security) utilizza una combinazione di crittografia a chiave asimmetrica e a chiave simmetrica (crittografia ibrida) per la trasmissione sicura dei dati, ad es. in Internet, e i seguenti protocolli secondari:

- TLS Handshake Protocol, cui compete l'autenticazione dei partner della comunicazione così come la negoziazione degli algoritmi e delle chiavi da utilizzare per la successiva trasmissione dei dati sulla base della crittografia asimmetrica.
- TLS Record Protocol, responsabile della crittografia dei dati utili per mezzo della crittografia e dello scambio di dati simmetrico.

Sia la crittografia asimmetrica che la crittografia simmetrica sono considerate sicure - non esistono differenze sostanziali tra i due metodi in termini di sicurezza. Il grado di sicurezza dipende dai parametri, come ad es. la lunghezza della chiave scelta.

Abuso della crittografia

In una chiave pubblica come sequenza di bit non è possibile determinare a quale identità essa sia assegnata. Un impostore potrebbe mettere a disposizione le proprie chiavi pubbliche sostenendo di essere tutt'altra persona. Se una terza persona utilizza questa chiave nella convinzione di aver indirizzato il partner della comunicazione giusto, informazioni confidenziali potrebbero arrivare all'impostore. L'impostore può decifrare con la propria chiave privata il messaggio che non era destinato a lui, per cui le informazioni confidenziali finiscono nelle mani sbagliate.

Per impedire questi abusi, è necessario creare le condizioni di attendibilità presso i partner di comunicazione in modo che siano sicuri di avere a che fare con il partner desiderato. Per creare questa attendibilità, in un'infrastruttura PKI si utilizzano certificati digitali.

5.6.1.4 Autenticità e integrità garantite da una firma

Gli attacchi da parte di programmi che intercettano la comunicazione tra server e client e agiscono come fossero essi stessi client o server vengono definiti attacchi "Man-in-the-Middle". Questi programmi, se non viene rilevata la loro falsa identità, possono ad es. ricevere informazioni importanti sul programma S7 o impostare valori nella CPU, e quindi attaccare una macchina o un impianto. Per impedire attacchi di questo genere si utilizzano certificati digitali.

La comunicazione sicura utilizza certificati digitali conformi allo standard X.509 della International Telecommunication Union (ITU). In questo modo è possibile verificare (autenticare) l'identità di un programma, un computer o un'organizzazione.

Come i certificati stabiliscono l'attendibilità

Il compito principale di un certificato X.509 è di collegare l'identità con i dati del proprietario di un certificato (ad es. indirizzo e-mail, nome del computer) alla chiave pubblica dell'identità. Le identità possono essere persone, computer o macchine.

I certificati vengono emessi dall'autorità di certificazione (Certificate Authority, CA) o dal proprietario stesso del certificato. I sistemi PKI stabiliscono in che modo gli utenti possono considerare attendibili le autorità di certificazione e i certificati emessi.

Come ottenere un certificato

1. Chi desidera ottenere un certificato, inoltra una richiesta attraverso un'autorità di registrazione collegata all'autorità di certificazione.
2. L'autorità di certificazione valuta la richiesta e il richiedente in base a criteri fissi.
3. Se riesce a verificare in modo univoco l'identità del richiedente, l'autorità di certificazione certifica questa identità con l'emissione di un certificato firmato. Il richiedente è ora diventato titolare del certificato.

Nella figura seguente è rappresentata la procedura in maniera semplificata. Non è indicato come Alice possa verificare la firma digitale.

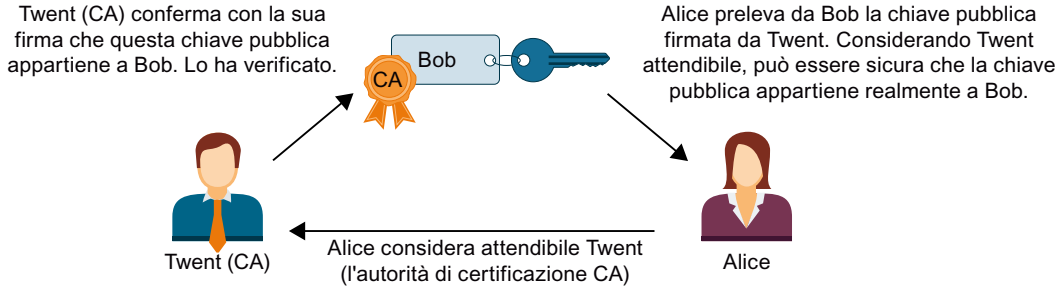


Figura 5-9 Firma di un certificato da parte di un'autorità di certificazione

Certificati autofirmati

I certificati autofirmati sono certificati la cui firma proviene dal proprietario e non da un'autorità di certificazione indipendente.

Esempi:

- È possibile emettere un certificato e firmarlo personalmente ad es. per crittografare i messaggi inviati a un partner di comunicazione. Nell'esempio precedente potrebbe essere Bob stesso (e non Twent) a firmare il proprio certificato con la sua chiave privata. Alice, con l'aiuto della chiave pubblica di Bob, può verificare che la firma e la chiave pubblica di Bob siano compatibili. Per crittografare una comunicazione semplice all'interno dell'impianto, ciò è sufficiente.
- Un certificato radice, ad es., è un certificato autofirmato dall'autorità di certificazione (emittente) di cui contiene la chiave pubblica.

Particolarità dei certificati autofirmati

Gli attributi "CN" (Common Name of Subject) per il titolare del certificato e "Issuer" (emittente) dei certificati autofirmati sono identici: infatti sono stati firmati dalla stessa persona. Il campo "CA" (Certificate Autority) dell'autorità di certificazione deve essere "False", perché il certificato autofirmato non deve essere utilizzato per firmare altri certificati.

I certificati autofirmati non sono inseriti in una gerarchia PKI.

Contenuto dei certificati

Un certificato conforme allo standard X.509 V3 - quello adottato anche da STEP 7 e dalle CPU S7-1500 - è costituito fondamentalmente dalle parti seguenti.

- Chiave pubblica
- Dati sul proprietario del certificato (ovvero il proprietario della chiave); si tratta ad es. del Common Name (CN) of Subject
- Attributi come numero di serie e periodo di validità
- Firma digitale (autenticazione) dell'autorità di certificazione (CA) che attesta l'autenticità dei dati.

Inoltre sono disponibili informazioni aggiuntive come ad es.:

- Indicazione dello scopo per il quale può essere utilizzata la chiave pubblica (Key Usage), ad es. per la firma o per la cifratura della chiave.
  Quando si crea un nuovo certificato con STEP 7, ad es. nel contesto Secure Open User Communication, selezionare dall'elenco delle possibili destinazioni d'uso la registrazione appropriata, ad es. "TLS".
- Indicazione di un "titolare alternativo del certificato" ("SAN", Subject Alternative Name) che, ad es. nel caso della comunicazione sicura con Web server (HTTP over TLS), viene utilizzato per dimostrare che il certificato appartiene anche al Web server indicato nell'URL nella barra dell'indirizzo del browser di rete.

Come creare e verificare le firme

I requisiti tecnici per poter verificare i certificati sono indicati nell'utilizzo della chiave asimmetrica. Prendiamo ad es. un certificato "MyCert" per spiegare le procedure di firma e di verifica della firma.

Creazione della firma

1. Dai dati del certificato, l'emittente del certificato "MyCert" crea un valore di hash con una determinata funzione hash (ad es. SHA-1, Secure Hash Algorithm).

   Il valore di hash è una sequenza di bit con lunghezza costante. La lunghezza costante del valore di hash ha il vantaggio che la firma richiede sempre lo stesso tempo.
2. Dal valore di hash così calcolato, l'emittente del certificato crea una firma digitale con l'aiuto della chiave privata. A questo scopo viene spesso utilizzato il sistema di firma RSA.
3. La firma digitale viene salvata nel certificato. Il certificato è così firmato.

Verifica della firma

1. Il revisore del certificato "MyCert" si procura il certificato dell'emittente e quindi la chiave pubblica.
2. Con lo stesso algoritmo di hash utilizzato per la firma (ad es. SHA-1) viene nuovamente calcolato un valore di hash dai dati del certificato.
3. Questo valore di hash viene confrontato con il valore di hash rilevato con l'aiuto della chiave pubblica dell'emittente e dell'algoritmo della firma per verificare la firma.
4. Se la verifica della firma è positiva, è provata sia l'identità del titolare che l'integrità, ovvero l'autenticità e l'originalità del contenuto del certificato. Chiunque sia in possesso della chiave pubblica, ovvero del certificato dell'autorità di certificazione, può verificare la firma e dimostrare che il certificato è stato effettivamente firmato dall'autorità.

L'esempio seguente mostra come Alice, con l'aiuto della chiave pubblica del certificato di Twent (che rappresenta l'autorità di certificazione CA), verifica la firma con la chiave pubblica di Bob. Il presupposto per la verifica è la disponibilità del certificato dell'autorità di certificazione al momento della verifica. La convalida in sé viene eseguita automaticamente nella sessione TLS.

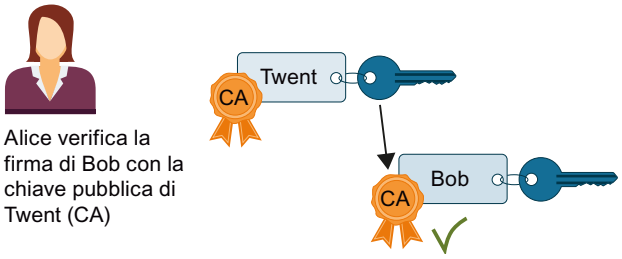


Figura 5-10 Verifica di un certificato tramite chiave pubblica del certificato di un'autorità di certificazione

Firma dei messaggi

Il metodo di firma e verifica dei certificati precedentemente descritto utilizza la sessione TLS anche per la firma e la verifica di messaggi:

Se si genera un valore di hash da un messaggio e si codifica questo valore di hash con la chiave privata del mittente allegandolo al messaggio originale, il destinatario del messaggio è in grado di rilevare l'integrità del messaggio. Il destinatario decodifica il valore di hash con la chiave pubblica del mittente, calcola a sua volta il valore di hash dal messaggio ricevuto e confronta entrambi i valori. Se i valori sono diversi significa che il messaggio o il valore di hash è stato alterato durante il trasporto.

Catena di certificati fino al certificato radice

I certificati di un'infrastruttura PKI sono organizzati in ordine gerarchico. In cima alla gerarchia si trovano i certificati radice, definiti anche certificati root o root certificate. Questi sono i certificati che non sono autenticati da un'autorità di certificazione di livello superiore. Titolare ed emittente dei certificati radice sono identici. I certificati radice godono di assoluta attendibilità, sono il "cardine" dell'attendibilità e pertanto devono essere noti al destinatario come certificati attendibili. Vengono salvati in un'area destinata ai certificati attendibili.

La funzione dei certificati radice può essere quella di firmare i certificati di autorità di certificazione subordinate, i cosiddetti certificati intermedi, in funzione della PKI. In questo modo l'affidabilità del certificato radice viene trasferita al certificato intermedio. Esattamente come il certificato radice, un certificato intermedio può a sua volta firmare un altro certificato, per cui entrambi vengono definiti anche "certificati CA".

Questa gerarchia può proseguire con diversi certificati intermedi fino al certificato dell'entità finale. Il certificato dell'entità finale è quello dell'utente che deve essere identificato.

Per la convalida, la gerarchia viene percorsa nella direzione opposta. Come descritto precedentemente viene determinato l'emittente del certificato, con la sua chiave pubblica viene verificata la firma, quindi viene determinato il certificato dell'emittente di livello superiore.... ripercorrendo tutta la catena di certificati fino alla radice.

In conclusione Il percorso dei certificati, ovvero la catena dei certificati intermedi fino al certificato radice, deve essere presente in ogni dispositivo che debba convalidare un certificato di entità finale del partner della comunicazione, indipendentemente dal tipo di comunicazione sicura progettata.

5.6.2 Gestione dei certificati

5.6.2.1 Informazioni utili sulla gestione dei certificati

Questa sezione mostra le possibilità di gestione dei certificati disponibili per una CPU S7-1500 a seconda del servizio (applicazione della CPU) utilizzato e delle versioni del TIA Portal / del firmware della CPU.

Panoramica delle possibilità di gestione dei certificati

Dalla versione V14 di TIA Portal e dalla versione V2.0 di CPU-FW, è possibile gestire i certificati per la comunicazione sicura per i vari servizi della CPU S7-1500 in TIA Portal e caricarli nella CPU.

Il TIA Portal dalla versione V17 e le CPU S7-1500 dalla versione FW V2.9 supportano un'altra possibilità di gestione dei certificati: È possibile utilizzare i metodi push di GDS per trasferire o rinnovare i certificati alla CPU in fase di esecuzione senza dover ricaricare la CPU.

È possibile utilizzare lo stesso metodo per trasmettere i certificati del Web server di una CPU S7-1500 (a partire dal firmware V3.0) da TIA Portal versione V18.

La tabella seguente fornisce una panoramica delle possibilità di gestione dei certificati a seconda del servizio utilizzato e della versione di TIA Portal o del firmware della CPU.

Service	Gestione dei certificati con TIA Portal (versione di TIA Portal / versione FW della CPU S7-1500)	Gestione del certificato con metodi push OPC UA GDS (versione di TIA Portal / versione FW della CPU S7-1500)
Web server	da V14 / da V2.0	da V18 / da V3.0
Comunicazione Secure OUC	da V14 / da V2.0	-
Server OPC UA	da V14 / da V2.0	da V17 / da V2.9
Client OPC UA	da V15.1 / da V2.6	-
Comunicazione sicura PG/HMI	da V17 / da V2.9	-

Ulteriori informazioni

La descrizione della gestione dei certificati con i metodi GDS-Push è disponibile qui: Gestione certificato tramite Globale Discovery Server (GDS) (Pagina 210).

Se non è necessario caricare nuovi certificati, ma è necessario rinnovare un certificato, ad es. perché il periodo di validità è scaduto, è possibile farlo anche nel RUN se sono soddisfatte alcune condizioni: Vedere Suggerimento: Aggiornamento dei certificati caricati in RUN (Pagina 80).

5.6.2.2 Gestione dei certificati in TIA Portal

STEP 7 dalla versione V14 in poi, insieme alle CPU S7-1500 dalla versione FW 2.0 in poi, supporta la PKI Internet (RFC 5280) in quanto una CPU S7-1500 è in grado di comunicare con dispositivi che a loro volta supportano la PKI Internet.

L'utilizzo di certificati X.509, ad es. per la verifica di certificati come descritto precedentemente, è una delle conseguenze.

STEP 7 dalla V14 supporta una PKI simile alla PKI Internet. Non sono supportate ad es. le Certificate Revocation List (CRL).

Creazione o assegnazione dei certificati in TIA Portal

Per i dispositivi con proprietà Security, come ad es. una CPU S7-1500 dal firmware V2.0, in STEP 7 si creano dei certificati per diverse applicazioni.

Le seguenti aree della finestra di ispezione della CPU consentono di creare o di selezionare i certificati.

- "Web server > Security" - per la generazione o l'assegnazione di certificati del Web server.
- "Protezione & Security > Meccanismi di collegamento" - per la generazione o l'assegnazione di certificati di comunicazione PLC (comunicazione sicura PG/HMI, da TIA Portal V17).
- "Protezione & Security > Gestione certificato" - per la generazione o l'assegnazione di certificati di tutti i tipi; per la creazione dei certificati sono preimpostati i certificati TLS per Secure Open User Communication.
- "OPC UA > Server > Security" - per la generazione o l'assegnazione dei certificati server OPC UA.

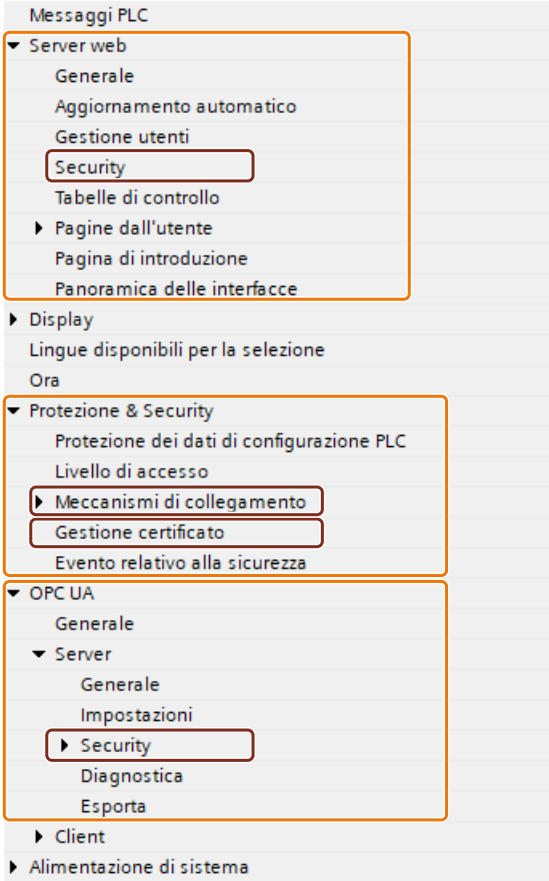


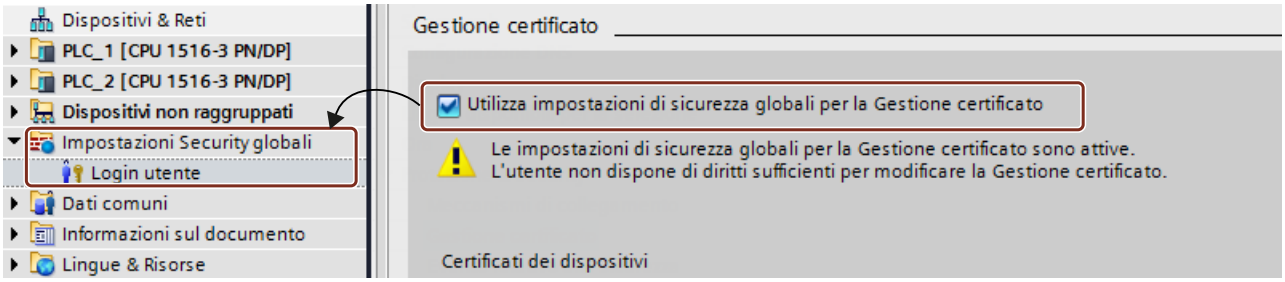
Figura 5-11 Impostazioni Security per una CPU S7-1500 in STEP 7

Particolarità dell'area "Protezione Security > Gestione certificato"

Solo in questa parte della finestra di ispezione è possibile commutare tra la gestione del certificato globale, ovvero per tutto il progetto, e quella locale, ovvero specifica del dispositivo (opzione "Utilizza impostazioni di sicurezza globali per la Gestione certificato"). Questa opzione decide se l'utente abbia accesso o meno a tutti i certificati del progetto.

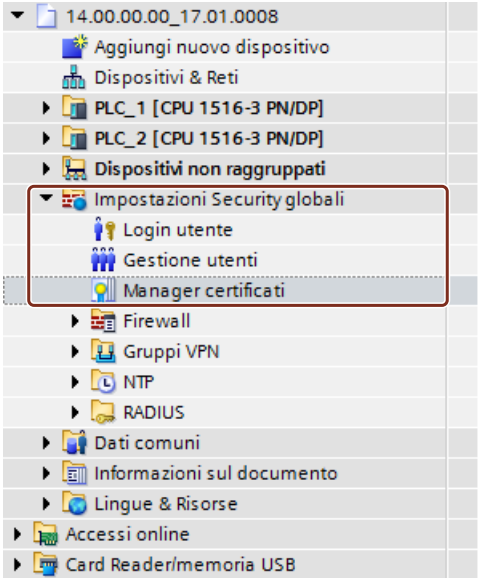
- Se **non** si utilizza la gestione del certificato nelle impostazioni di sicurezza globali, si avrà accesso solo alla memoria locale dei certificati della CPU. Non sarà possibile, ad es., accedere ai certificati importati o ai certificati radice. Senza questi certificati è disponibile solo una funzionalità limitata; è possibile, ad es., creare soltanto certificati autofirmati.
- Se si utilizza la gestione del certificato nelle impostazioni di sicurezza globali e si è connessi ad es. come amministratori, sarà possibile accedere alla memoria globale dei certificati per l'intero progetto. È possibile ad es. assegnare alla CPU dei certificati importati o creare certificati emessi e firmati dalla CA del progetto (autorità di certificazione del progetto).

La figura seguente mostra come, dopo aver attivato l'opzione "Utilizza impostazioni di sicurezza globali per la Gestione certificato" nella finestra di ispezione della CPU, le "Impostazioni Security globali" compaiono nella navigazione del progetto.



Se ci si connette facendo doppio clic su "Login utente" sotto le impostazioni di sicurezza globali nella navigazione del progetto, qui viene visualizzata anche una riga "Gestione certificato".

Con un doppio clic sulla riga "Gestione certificato" si ottiene l'accesso a tutti i certificati del progetto, suddivisi nelle schede "CA" (autorità di certificazione), "Certificati dei dispositivi" e "Certificati e autorità di certificazione accreditati".



Chiavi private

Al momento di generare i certificati dei dispositivi o i certificati dei server (certificati di entità finale), STEP 7 crea delle chiavi private. Una chiave privata viene crittografata e salvata in una memoria diversa a seconda dell'utilizzo delle impostazioni di sicurezza globali per la gestione certificato:

- Se si utilizzano le impostazioni di sicurezza globali, la chiave privata viene salvata nella memoria dei certificati globale (per tutto il progetto).
- Se non si utilizzano le impostazioni di sicurezza globali, la chiave privata viene crittografata e salvata nella memoria dei certificati locale (specifica della CPU).

La presenza della chiave privata, necessaria ad es. per decodificare i dati, è visualizzata nella colonna "Chiave privata" nella scheda "Certificati dei dispositivi" della gestione certificato nelle impostazioni di sicurezza globali.

Al momento di caricare la configurazione hardware, il certificato del dispositivo, la chiave pubblica e la chiave privata vengono caricati nella CPU.

ATTENZIONE

Attivazione dell'opzione "Utilizza impostazioni di sicurezza globali per la Gestione certificato" - Conseguenze

L'opzione "Utilizza impostazioni di sicurezza globali per la Gestione certificato" influisce sulla chiave privata utilizzata precedentemente: Se sono già stati creati dei certificati senza utilizzare la gestione certificato nelle impostazioni di sicurezza globali e si commuta l'opzione per l'utilizzo della gestione certificato, le chiavi private vanno perse e l'ID potrebbe essere modificato. In questo caso viene visualizzato un avviso. Stabilire pertanto all'inizio della progettazione quale opzione è necessaria per la gestione del certificato.

5.6.2.3 Esempi di gestione dei certificati

Come descritto in precedenza, i certificati sono necessari per qualsiasi tipo di comunicazione sicura. Qui di seguito sono riportati alcuni esempi di come gestire i certificati con STEP 7 in modo da creare i presupposti necessari per la Secure Open User Communication.

Inoltre è specificato di quali dispositivi si tratta per i vari partner della comunicazione. Sono descritti i diversi passi per fornire i certificati necessari ai partner della comunicazione. Si presuppone sempre l'uso di una CPU S7-1500 o di un S7-1500 Software Controller con versione firmware 2.0 o superiore.

In generale vale quanto segue:

Durante la creazione di un collegamento sicuro ("handshake"), normalmente i partner della comunicazione trasmettono solo i propri certificati di entità finale (certificati dei dispositivi).

Per questo motivo i certificati CA necessari per la verifica del certificato del dispositivo rilevato deve trovarsi nella memoria dei certificati del partner di comunicazione.

NOTA

Nella CPU deve essere impostata la data / l'ora aggiornata.

Se si utilizza la comunicazione sicura (ad es. HTTPS, Secure OUC, OPC UA) assicurarsi che le unità interessate dispongano dell'ora e della data attuale. In caso contrario le unità considerano i certificati non validi e la comunicazione protetta non funziona.

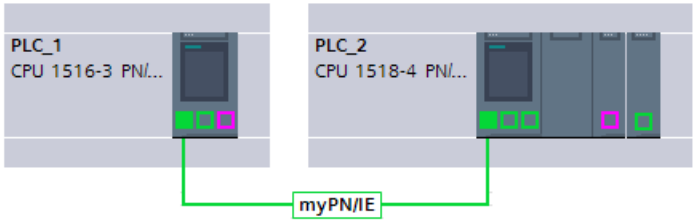
Secure Open User Communication tra 2 CPU S7-1500

Due CPU S7-1500 PLC_1 e PLC_2 devono scambiare dati tra loro attraverso la Secure Open User Communication.

I certificati dei dispositivi necessari vanno generati con STEP 7 e assegnati alle CPU come qui descritto.

Per firmare i certificati dei dispositivi vengono utilizzate le autorità di certificazione del progetto STEP 7 (CA del progetto).

I certificati devono essere referenziati nel programma utente (istruzione di comunicazione TCON in combinazione con il tipo di dati di sistema corrispondente, ad es. TCON_IPV4_SEC) dal rispettivo ID. L'ID del certificato viene assegnato automaticamente da STEP 7 al momento della generazione o della creazione dei certificati.



Procedimento

STEP 7 carica automaticamente i certificati CA necessari insieme alla configurazione hardware nelle CPU interessate, in modo da garantire i presupposti per la verifica dei certificati per entrambe le CPU. È sufficiente quindi generare i certificati di dispositivo per la rispettiva CPU, a tutto il resto provvede STEP 7.

1. Selezionare PLC_1 e attivare nell'area "Protezione Security" l'opzione "Utilizza impostazioni di sicurezza globali per la Gestione certificato".
2. Connettersi come utente nella navigazione del progetto nell'area "Impostazioni Security globali". Se il progetto è nuovo, per il primo login è previsto il ruolo "Amministratore".
3. Tornare al PLC-1 nell'area "Protezione Security". Nella tabella "Certificati dei dispositivi" fare clic su una riga vuota della colonna "Titolare del certificato" per creare un nuovo certificato.
4. Nella casella di riepilogo per la selezione di un certificato fare clic sul pulsante "Inserisci".

   Si apre la finestra di dialogo "Crea nuovo certificato".
5. Lasciare invariate le preimpostazioni nella finestra di dialogo, questi valori sono già adeguati alla Secure Open User Communication (utilizzo: TLS).

   Suggerimento: Completare il nome preimpostato del proprietario del certificato, in questo caso il nome della CPU. Per maggiore chiarezza lasciare invariato il nome preimpostato della CPU nel caso in cui si debbano gestire numerosi certificati dei dispositivi.

   Esempio: PLC_1/TLS diventa PLC_1-SecOUC-Chassis17FactoryState.
6. Compilare la configurazione.

   Il certificato del dispositivo e il certificato CA sono parte integrante della configurazione.
7. Ripetere i passi descritti anche per PLC_2.

Con il passo successivo si devono creare i programmi utente per lo scambio dei dati e caricare le configurazioni insieme al programma.

Utilizzo di certificati autofirmati invece di certificati CA

Quando si crea un certificato di dispositivo è possibile selezionare l'opzione "Autofirmato". I certificati autofirmati si possono creare senza essere connessi per le impostazioni di sicurezza globali. Questo procedimento è sconsigliato, perché i certificati così creati non sono disponibili nella memoria dei certificati globale e pertanto non possono essere assegnati direttamente a una CPU partner.

Come descritto precedentemente, occorre scegliere con attenzione il nome del titolare del certificato per poter assegnare con sicurezza il certificato giusto a un dispositivo.

Per i certificati autofirmati non è possibile eseguire una verifica con i certificati CA del progetto STEP 7. Per poter verificare i certificati autofirmati è necessario acquisire per ogni CPU il certificato autofirmato del partner della comunicazione nell'elenco dei dispositivi partner attendibili. Perciò è necessario aver attivato l'opzione "Utilizza impostazioni di sicurezza globali per la Gestione certificato" ed essere connessi come utenti nelle impostazioni di sicurezza globali.

Per aggiungere il certificato autofirmato dal partner della comunicazione nella CPU procedere nel modo seguente:

1. Selezionare PLC_1 e spostarsi fino alla tabella "Certificati dei dispositivi partner" nell'area "Protezione Security".
2. Fare clic in una riga vuota della colonna "Titolare del certificato" per aprire la casella di riepilogo e inserire o selezionare il certificato.
3. Selezionare dalla casella di riepilogo il certificato autofirmato del partner di comunicazione e confermare la selezione.

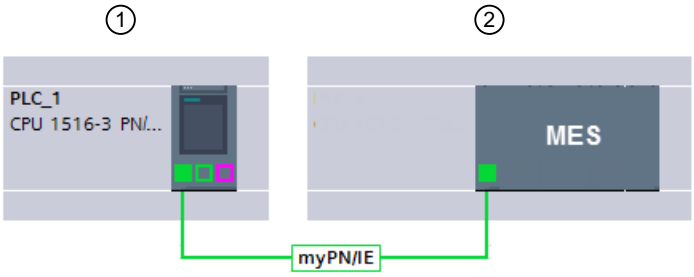
Con il passo successivo si devono creare i programmi utente per lo scambio dei dati e caricare le configurazioni insieme al programma.

Secure Open User Communication tra CPU S7-1500 come client TLS e dispositivo di terzi come server TLS

Due dispositivi devono scambiare dati tra loro attraverso un collegamento TLS o una sessione TLS, ad es. per lo scambio di ricette, dati sulla produzione o dati sulla qualità.

- Una CPU S7-1500 (PLC_1) come client TLS; la CPU utilizza la Secure Open User Communication
- Un dispositivo di terzi (ad es. un Manufacturing Execution System (MES)) come server TLS

La CPU S7-1500 in quanto client TLS crea il collegamento/la sessione TLS con il sistema MES.



① Client TLS

② Server TLS

Per l'autenticazione del server TLS la CPU S7-1500 ha bisogno dei certificati CA del sistema MES: Il certificato radice ed eventualmente i certificati intermedi per verificare il percorso del certificato.

Questi certificati vanno importati nella memoria dei certificati globale della CPU S7-1500.

Per importare i certificati del partner di comunicazione, procedere nel seguente modo:

1. Aprire la gestione certificato nelle impostazioni di sicurezza globali nella navigazione del progetto.
2. Selezionare la tabella adatta al certificato da importare (certificati attendibili e autorità di certificazione radice).
3. Aprire il menu di scelta rapida della tabella con un clic destro del mouse. Fare clic su "Importa" e importare il certificato o i certificati CA necessari.

   In seguito all'importazione, il certificato riceve un ID e può essere assegnato a un'unità con il passo successivo.
4. Selezionare PLC_1 e spostarsi fino alla tabella "Certificati dei dispositivi partner" nell'area "Protezione Security".
5. Fare clic in una riga vuota della colonna "Titolare del certificato" per inserire i certificati importati.
6. Selezionare dalla casella di riepilogo i certificati CA necessari del partner di comunicazione e confermare la selezione.

In via opzionale, il sistema MES può richiedere per l'autenticazione della CPU (ovvero del client TLS) anche un certificato di dispositivo della CPU. In questo caso è necessario mettere a disposizione del sistema MES i certificati CA della CPU. Per importare i certificati nel sistema MES è necessario aver prima esportato i certificati CA dal progetto STEP 7 della CPU. Procedere nel seguente modo:

1. Aprire la gestione certificato nelle impostazioni di sicurezza globali nella navigazione del progetto.
2. Selezionare la tabella adatta al certificato da esportare (certificati CA).
3. Selezionare il certificato e aprire il menu di scelta rapida con un clic destro del mouse.
4. Fare clic su "Esporta".
5. Selezionare il formato di esportazione del certificato.

Con il passo successivo si devono creare i programmi utente per lo scambio dei dati e caricare le configurazioni insieme al programma.

Secure Open User Communication tra CPU S7-1500 come server TLS e dispositivo di terzi come client TLS

Se la CPU S7-1500 agisce come server TLS e il dispositivo di terzi, ad es. un sistema ERP (Enterprise Resource Planning System), crea il collegamento/la sessione TLS, sono necessari i seguenti certificati.

- Per la CPU S7-1500 creare un certificato di dispositivo (certificato server) con chiave privata e caricarlo con la configurazione hardware nella CPU S7-1500. Per creare il certificato server utilizzare l'opzione "Firmato dall'autorità di certificazione".

  La chiave privata è necessaria per lo scambio delle chiavi, come mostra l'esempio "HTTP over TLS" nella figura.
- Per il sistema ERP è necessario esportare il certificato CA del progetto STEP 7 e importarlo/caricarlo nel sistema ERP. Con il certificato CA, il sistema ERP verifica il certificato server della S7-1500 che viene trasmesso dalla CPU al sistema ERP durante la creazione del collegamento/della sessione TLS.

① Server TLS

② Client TLS

Figura 5-12 Secure OUC tra una CPU S7-1500 e un sistema ERP

La descrizione dei passi necessari è riportata nelle sezioni precedenti.

Secure Open User Communication con un server e-mail (SMTP over TLS)

Una CPU S7-1500 può creare un collegamento sicuro con un server di posta elettronica con l'istruzione di comunicazione TMAIL-C.

I tipi di dati di sistema TMail_V4_SEC e TMail_QDN_SEC consentono di determinare la porta partner del server di posta elettronica e quindi di raggiungere quest'ultimo tramite "SMTP over TLS".

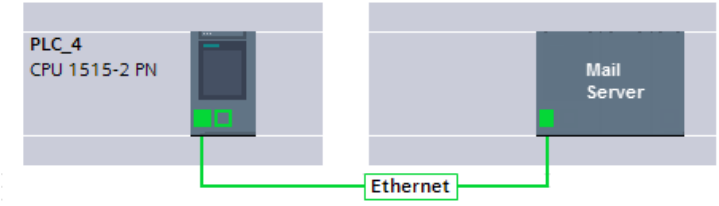


Figura 5-13 Secure OUC tra una CPU S7-1500 e un server e-mail

Presupposto necessario per poter stabilire un collegamento sicuro via e-mail è che il certificato radice e i certificati intermedi siano stati importati dal server e-mail (provider) nella

memoria dei certificati globale della CPU S7-1500. In base a questi certificati la CPU può verificare il certificato che il server e-mail le ha trasmesso quando è stato creato il collegamento/la sessione TLS.

Per importare i certificati del server e-mail procedere nel seguente modo:

1. Aprire la gestione certificato nelle impostazioni di sicurezza globali nella navigazione del progetto.
2. Selezionare la tabella adatta al certificato da importare (certificati attendibili e autorità di certificazione radice).
3. Aprire il menu di scelta rapida della tabella con un clic destro del mouse. Fare clic su "Importa" e importare il certificato o i certificati CA necessari.

   In seguito all'importazione, il certificato riceve un ID e può essere assegnato a un'unità con il passo successivo.
4. Selezionare PLC_1 e spostarsi fino alla tabella "Certificati dei dispositivi partner" nell'area "Protezione Security".
5. Fare clic in una riga vuota della colonna "Titolare del certificato" per inserire i certificati importati.
6. Selezionare dalla casella di riepilogo i certificati CA necessari del partner di comunicazione e confermare la selezione.

Con il passo successivo si devono creare i programmi utente per la funzione di client e-mail della CPU e caricare le configurazioni insieme al programma.

5.6.2.4 Come funziona la comunicazione con i certificati: HTTP over TLS

Qui di seguito mostriamo come utilizzare i meccanismi descritti per creare una comunicazione sicura tra un browser di rete e il Web server di una CPU S7-1500.

In primo luogo sono descritte le modifiche per l'opzione "Consenti accesso solo tramite HTTPS" in STEP 7. Da STEP 7 V14 è possibile influenzare il certificato del Web server di una CPU S7-1500 dal firmware V2.0: A partire da queste versioni, il certificato server viene generato con STEP 7.

Inoltre mostriamo quali processi vengono eseguiti quando si richiama una pagina web del Web server della CPU con un browser di rete di un PC attraverso un collegamento crittografato HTTPS.

Utilizzo dei certificati Web server per le CPU S7-1500 con FW V2.0 o superiore

Per le CPU S7-1500 con versione firmware precedente alla V2.0, per impostare le proprietà del Web server senza requisiti era possibile scegliere l'opzione "Consenti accesso solo tramite HTTPS".

Con queste CPU non è necessario occuparsi dell'utilizzo dei certificati perché i certificati necessari per il Web server vengono creati dalla CPU automaticamente.

Nel caso delle CPU S7-1500 con firmware V2.0 o superiore STEP 7 genera il certificato server (certificato dell'entità finale) per la CPU. Nelle proprietà della CPU (Web Server > Security) si assegna un certificato server al Web server.

Poiché è sempre preimpostato un nome di certificato server, nella progettazione semplice del Web server non cambia nulla: Attivare il Web server, l'opzione "Consenti accesso solo tramite

HTTPS" è preimpostata e, con la compilazione, STEP 7 genera un certificato server con il nome preimpostato.

Indipendentemente dall'uso o meno della gestione certificato nelle impostazioni di sicurezza globali, STEP 7 ha tutte le informazioni necessarie per poter generare il certificato server.

Inoltre esiste la possibilità di determinare le proprietà del certificato server, ad es. il nome o la durata di validità.

NOTA

Nella CPU deve essere impostata la data / l'ora aggiornata.

Se si utilizza la comunicazione sicura (ad es. HTTPS, Secure OUC, OPC UA) assicurarsi che le unità interessate dispongano dell'ora e della data attuali. In caso contrario le unità considerano i certificati non validi e la comunicazione protetta non funziona.

Caricamento del certificato del Web server

Con il caricamento della configurazione hardware nella CPU viene caricato automaticamente anche il certificato server generato da STEP 7.

- Se si utilizza la gestione certificato nelle impostazioni di sicurezza globali, l'autorità di certificazione del progetto (certificato CA) firma il certificato del Web server. Al momento del caricamento viene caricato automaticamente anche il certificato CA del progetto.
- Se non si utilizza la gestione certificato nelle impostazioni di sicurezza globali, STEP 7 genera il certificato server come certificato autofirmato.

Se si indirizza il Web server della CPU attraverso l'indirizzo IP della CPU, ogni volta che viene modificato l'indirizzo IP di un'interfaccia Ethernet della CPU è necessario creare e caricare un nuovo certificato server (certificato dell'entità finale). Il motivo è che con l'indirizzo IP cambia anche l'identità della CPU - che deve essere autenticata (firmata) secondo le regole della PKI.

A questo problema si può ovviare indirizzando la CPU con un nome di dominio anziché con l'indirizzo IP, ad es. "myconveyer-cpu.room13.myfactory.com". Allo scopo è necessario gestire i nomi di dominio delle CPU attraverso un server DNS.

Assegnazione del certificato CA del Web server al browser di rete

Sul browser di rete l'utente che accede tramite HTTPS alle pagine Web della CPU deve installare il certificato CA della CPU. Se il certificato non è stato installato, infatti, viene visualizzato un messaggio di avviso che consiglia di non utilizzare la pagina. Per poter visualizzare la pagina l'utente deve inserire esplicitamente un'eccezione.

L'utente può scaricare il certificato radice (Root Certificate) dalla pagina web "Introduzione" del Web server della CPU alla voce "Scarica certificato".

Un'altra possibilità è l'impiego di STEP 7: Esportare il certificato CA del progetto con la gestione certificato nelle impostazioni di sicurezza globali in STEP 7. Successivamente importare il certificato CA nel browser.

Meccanismo della comunicazione sicura

La figura seguente mostra in modo semplificato come si crea in generale la comunicazione ("handshake"), focalizzandosi sulla negoziazione delle chiavi utilizzate per lo scambio di dati (qui tramite HTTP over TLS).

In linea di principio comunque il procedimento è applicabile a tutte le opzioni di comunicazione che si basano sull'utilizzo di TLS, quindi anche per la Secure Open User Communication (vedere le nozioni di base della comunicazione sicura).

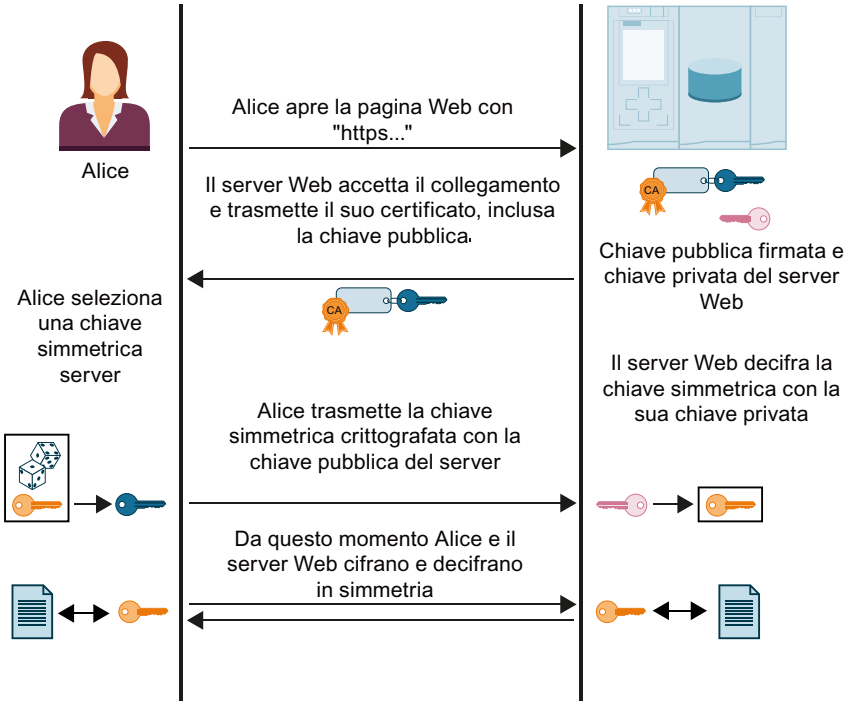


Figura 5-14 Handshake in https

Nella figura non sono rappresentate le azioni eseguite sul lato di Alice (browser) per verificare il certificato trasmesso dal Web server. Dall'esito positivo della verifica dipende il fatto che Alice possa ritenere attendibile il certificato trasmesso dal Web server e quindi l'identità del Web server, e partecipare allo scambio dei dati.

Questi i singoli passi per verificare l'autenticità del Web server:

1. Alice deve conoscere le chiavi pubbliche di tutte le autorità di certificazione coinvolte, ovvero Alice ha bisogno dell'intera catena di certificati per verificare il certificato del Web server (praticamente il certificato di entità finale del Web server).

   Normalmente Alice ha in archivio il certificato radice necessario. Con l'installazione di un browser di rete viene installata ad es. anche una serie di certificati radice attendibili. Se manca il certificato radice, deve scaricarlo dall'autorità di certificazione e installarlo nella memoria dei certificati del browser. L'autorità di certificazione può essere anche il dispositivo sul quale si trova il Web server.

Per ottenere i certificati intermedi esistono le seguenti possibilità:

– Il server stesso trasmette ad Alice i certificati intermedi necessari insieme al suo certificato di entità finale come messaggio firmato in modo che Alice possa verificare l'integrità della catena di certificati.
– Nei certificati si trovano spesso gli URL del rispettivo emittente. Attraverso questi URL Alice può caricare i certificati intermedi necessari.

Quando si utilizzano i certificati in STEP 7 si parte sempre dal presupposto che i certificati intermedi necessari e il certificato radice siano stati importati nel progetto e assegnati all'unità.

2. Con le chiavi pubbliche dei certificati Alice convalida le firme della catena dei certificati.
3. La chiave simmetrica deve essere stata creata e trasmessa al Web server.
4. Se il Web server viene indirizzato dal nome di dominio, Alice verifica secondo le regole PKI stabilite nella RFC 2818 l'identità del Web server. Questo è possibile perché l'URL del Web server, in questo caso il "Fully Qualified Domain Name" (FQDN), è salvato nel certificato dell'entità finale del Web server. Se la registrazione nel campo "Subject Alternative Name" del certificato corrisponde a quella nella riga dell'indirizzo del browser, è tutto in ordine.

Segue lo scambio di dati con la chiave simmetrica, come mostra la figura in alto.

5.6.2.5 Suggerimento: Aggiornamento dei certificati caricati in RUN

Da TIA Portal V19 e dalla versione firmware V3.1 delle CPU S7-1500 (incl. CPU R/H) è possibile aggiornare i certificati in runtime, ovvero con la CPU nello stato RUN.

Si tratta di certificati configurati e scaricati da TIA Portal.

In questo modo è possibile ad es. rinnovare o sostituire certificati scaduti senza interrompere il processo.

Requisiti

- La protezione del progetto è attivata.
- L'amministratore del progetto (amministrazione di engineering) è connesso con i diritti Security corrispondenti.
- Non vi sono altre modifiche della configurazione hardware. Queste modifiche richiederebbero uno STOP della CPU da caricare.

Regola

L'ID esistente del certificato aggiornato non deve essere modificato.

Procedura

1. In TIA Portal spostarsi (navigazione del progetto) sul manager dei certificati (impostazioni Security > Funzioni Security).
2. Selezionare la scheda "Autorità di certificazione (CA)" o la scheda "Certificati dei dispositivi" a seconda del certificato che si vuole aggiornare.
3. Selezionare il certificato aggiornato.
4. Selezionare il comando "Rinnova" o "Sostituisci" nel menu di scelta rapida, a seconda che si voglia sostituire il certificato esistente con un certificato del sistema di file, oppure ad es. aggiornare solo i dati di validità del certificato esistente.

   Nei certificati CA durale la sostituzione tutti i certificati derivati dei dispositivi vengono firmati automaticamente con il certificato CA rinnovato.
5. Caricare le modifiche nella CPU (caricare in Dispositivo > Configurazione hardware).

5.6.3 Presupposti per la comunicazione sicura

5.6.3.1 Protezione dei dati di configurazione riservati

Come descritto nelle nozioni di base sulla comunicazione sicura, per il corretto funzionamento dei protocolli basati su certificati sono necessarie chiavi private che devono essere protette nel miglior modo possibile.

A partire da STEP 7 V17 queste chiavi e altri dati importanti possono essere protetti con una password: la password per la protezione dei dati di configurazione riservati del PLC

L'assegnazione della password si rende superflua se sono state implementate altre misure volte ad impedire l'accesso non autorizzato al progetto TIA Portal e alla progettazione della CPU.

A prescindere che venga o meno assegnata una password: TIA Portal genera un'informazione chiave preposta alla protezione dei dati di configurazione PLC riservati. La password non ha alcuna influenza sul processo di comunicazione sicura. La complessità della password utilizzata per la protezione dei dati di configurazione PLC riservati determina, ad es. il grado di protezione delle chiavi private.

La disponibilità di un'informazione chiave costituisce un presupposto per la comunicazione sicura come ad es. la comunicazione PG/HMI sicura basata su TLS: La CPU, infatti, può gestire i certificati necessari per la comunicazione sicura solo se è disponibile quest'informazione.

La figura seguente illustra le correlazioni descritte.

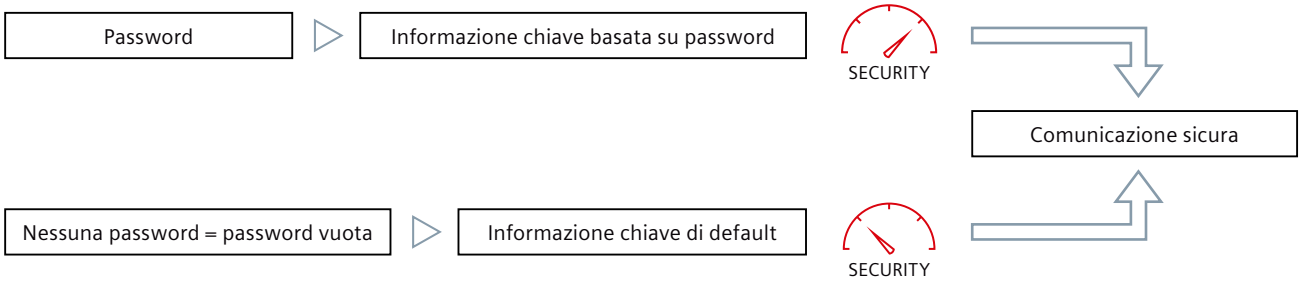


Figura 5-15 Correlazioni per la protezione dei dati di configurazione riservati

Assistente per le impostazioni Security

Quando si seleziona una CPU che supporta la comunicazione PG/HMI sicura nel catalogo hardware di TIA Portal e la si aggiunge a un progetto, si apre l'Assistente per le impostazioni Security della CPU.

L'assistente guida l'utente passo dopo passo mentre esegue le seguenti impostazioni della CPU:

- Password per la protezione dei dati di configurazione riservati del PLC
- Modalità di comunicazione HMI e PG/PC
- Livello di accesso

Ogni impostazione è descritta in dettaglio nell'Assistente. Alla fine le impostazioni vengono nuovamente riepilogate per chiarezza.

L'Assistente si avvia anche se si sostituisce un'unità nella vista di rete di TIA Portal e se la nuova CPU, diversamente da quella precedente, supporta la comunicazione PG/HMI sicura.

Tutte le impostazioni dell'Assistente vengono acquisite nella finestra di ispezione (proprietà della CPU).

L'Assistente può essere richiamato in qualsiasi momento con il pulsante di avvio disponibile nell'area "Protezione & Security" delle proprietà della CPU.

Presupposti

- TIA Portal versione V17 e successive
- La CPU supporta la comunicazione PG/HMI sicura (per CPU S7-1500 dalla versione firmware 2.9)
- La CPU non è ancora stata caricata o è stata resettata alle impostazione di fabbrica con l'opzione "Elimina password per la protezione dei dati di configurazione PLC riservati"

Procedimento

1. Aprire le proprietà della CPU nella vista di rete o nella vista dispositivi.
2. Spostarsi nella sezione "Protezione & Security > Protezione dei dati di configurazione PLC".

   Risultato: in un primo momento l'opzione "Proteggi dati di configurazione PLC riservati" è attivata e il campo vuoto per l'inserimento della password ha lo sfondo rosso.
3. Selezionando il pulsante "Definisci" configurare una password (metodo consigliato), oppure disattivare l'opzione "Proteggi dati di configurazione PLC riservati".
4. Completare la configurazione e creare il programma utente.
5. Caricare la CPU.
   Durante il caricamento della configurazione hardware viene chiesto una tantum di inserire nuovamente la password.
   Tenere presente che: La password configurata viene utilizzata in TIA Portal per generare l'informazione chiave per la protezione dei dati di configurazione riservati e proteggere questi dati. Tuttavia, per motivi di sicurezza né la password né l'informazione chiave vengono salvate nel progetto. Per consentire che l'informazione chiave venga ricevuta dalla CPU, durante il caricamento della configurazione hardware essa viene nuovamente

generata pertanto, durante questa fase, è richiesto anche un inserimento una tantum della password.

Comunicazione basata su certificati anche tra PG/HMI e CPU

Poiché da TIA Portal versione V17 e dalle versioni di firmware V2.9 (S7-1500) e V4.5 (S7-1200) della CPU anche la comunicazione PG/HMI si basa sull'uso di certificati, durante la messa in servizio viene chiesto di accettare il certificato server.

Suggerimenti e regole per la gestione delle password

- Gestire le password in una gestione password.
- Utilizzare le impostazioni di verifica dei criteri delle password in TIA Portal per controllare che le nuove password inserite corrispondano ai criteri ed evitare ad esempio password troppo semplici:
  - Spostarsi nella navigazione del progetto fino all'area "<Nome del progetto> > Impostazioni Security > Impostazioni" e selezionare l'area "Criteri password".
  - Specificare ad es. il numero minimo di caratteri o caratteri speciali che deve contenere la password.
- Non è necessario assegnare una password differente a ciascuna CPU di un impianto o di una macchina. A condizione che vengano soddisfatti alcuni presupposti, è possibile assegnare la stessa password ad un gruppo di CPU. Questa strategia offre alcuni vantaggi anche in caso di sostituzione delle CPU: Assegnando la password di gruppo alle CPU sostitutive si riduce il carico di lavoro durante la sostituzione della CPU.

  Tenere presente il rischio che in caso di compromissione della password di una di queste CPU, tutte le CPU con la stessa password sono vulnerabili.
- La configurazione delle password ha conseguenze anche sulla sostituzione dei componenti perché, oltre alla progettazione, deve essere trasferita nella nuova CPU (sostitutiva) la password per i dati di configurazione PLC riservati (vedere Regole per la sostituzione (Pagina 93)).
- Nel caso delle **CPU S7-1500R/H** la password per i dati di configurazione PLC riservati viene caricata solo in una delle due CPU. Perché il processo Sync-Up funzioni e anche la CPU del partner lavori correttamente si deve trasferire la password nella CPU del partner prima del Sync-Up mediante l'editor Online & Diagnostica:
  - Selezionare l'area "Definisci password per la protezione dei dati di configurazione sensibili del PLC" nella vista Online & Diagnostica.
  - Immettere la password e fare clic sul pulsante "Definisci".

    Se la password inserita è corretta, la CPU del partner può utilizzare i dati di configurazione PLC protetti e il processo Sync-Up può iniziare.

5.6.3.2 Informazioni importanti sulla protezione dei dati di configurazione PLC riservati

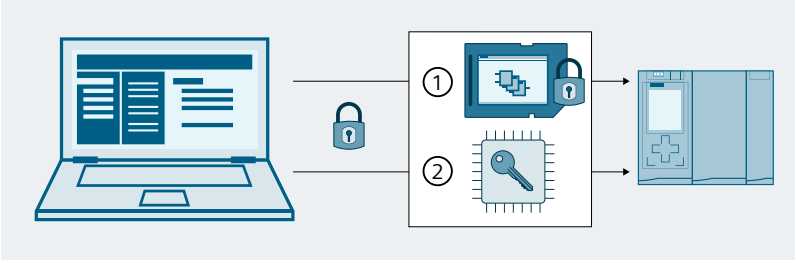
Il concetto di comunicazione sicura garantita da standard, comprende i seguenti componenti:

- Un'informazione chiave basata su password, impiegata per la protezione dei dati di configurazione riservati (ad es. chiave privata per certificati, password).
- Un protocollo standardizzato (TLS) che protegge la comunicazione tra i nodi (ad es. il dispositivo di programmazione e la CPU).

Principio di "protezione dei dati di configurazione riservati"

La seguente figura mostra in maniera semplificata come vengono protetti i dati di configurazione riservati ad es. di una CPU S7-1500 standard. Con il primo caricamento i due componenti "progetto" e "informazione chiave" vengono collocati in aree di memoria distinte: il progetto nella memoria di caricamento (Memory Card) e l'informazione chiave in un'area di memoria interna della CPU.

Negli altri sistemi di destinazione (ad es. CPU S7-1200, Software Controller) con sistemi di memorizzazione differenti, l'implementazione viene adattata al rispettivo sistema di memorizzazione, ma il principio è lo stesso.



① Progetto con dati di configurazione riservati protetti da password (qui: nella memoria di caricamento = Memory Card)

② Informazione chiave (generata dalla password) per poter utilizzare i dati di configurazione riservati protetti (qui: nell'area di memoria interna della CPU)

Figura 5-16 Principio per la protezione dei dati di configurazione riservati

Due aree di memoria per maggiore sicurezza

I componenti caricati possono essere considerati come due pezzi di un puzzle che si devono combaciare: il progetto è vincolato all'informazione chiave caricata, l'informazione chiave caricata è vincolata alla password assegnata durante la progettazione.

Progetto e informazione chiave devono essere compatibili, altrimenti la CPU non si avvia.

Il principio delle due aree di memoria separate vale anche per le varianti delle CPU S7-1200 e delle CPU S7-1500 senza Memory Card, come ad es. Software Controller o PLCSim/ PLCSim Advanced. Nelle varianti senza Memory Card vengono utilizzate due partizioni distinte per poter gestire entrambe le informazioni indipendentemente l'una dall'altra.

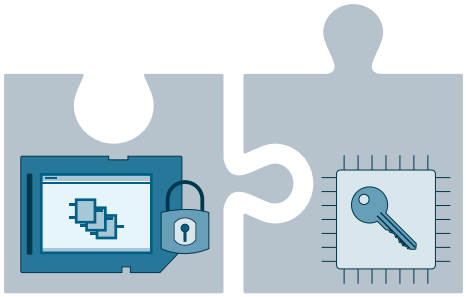


Figura 5-17 Principio delle aree della memoria separate

5.6.3.3 Modifica della password

Non fa alcuna differenza se la CPU è già stata caricata oppure no. Se la CPU è già stata caricata, essa dispone già dell'informazione chiave che permette di utilizzare i dati di configurazione PLC protetti da password.

Modifica della password - configurazione non ancora caricata

Fino a quando la configurazione non viene caricata nella CPU, è possibile modificare una password già inserita o annullare l'attivazione della protezione mediante password.

Presupposti

- La CPU non è ancora stata caricata

Procedimento

1. Aprire le proprietà della CPU nella vista di rete o nella vista dispositivi.
2. Spostarsi nella sezione "Protezione & Security > Protezione dei dati di configurazione PLC".
3. Fare clic sul pulsante "Modifica" oppure disattivare l'opzione "Proteggi dati di configurazione PLC riservati".
4. In questa finestra di dialogo inserire la password finora valida. Durante la modifica password, inserire la nuova password e confermarla nell'apposito campo.

Finché non si carica una configurazione nella CPU, quest'ultima è in una fase di distribuzione (vedere Comportamento della CPU dal caricamento allo stato "pronto al funzionamento" (Pagina 118)) ed è possibile caricare qualsiasi configurazione valida con la propria password configurata.

Modifica della password - configurazione già caricata

Se nella CPU è già stata caricata una configurazione protetta da una password per i dati di configurazione PLC riservati, è necessario resettare la CPU alle impostazioni di fabbrica, quindi cancellare la password per i dati di configurazione PLC riservati nella CPU, oppure cancellare la password direttamente online prima di reimpostarla.

Presupposti

- La CPU è accessibile in scrittura
- La CPU si trova nello stato di funzionamento STOP

Procedimento

1. Selezionare la CPU nella vista di rete.
2. Nel menu di scelta rapida selezionare il comando "Online & Diagnostica".
3. Se si intende modificare il progetto anche sulla Memory Card e successivamente ricaricare la configurazione:
   - Nella vista Online & Diagnostica aperta selezionare l'area "Resetta alle impostazioni di fabbrica".
   - Attivare l'opzione "Elimina password per la protezione dei dati di configurazione PLC riservati" Per evitare il riavvio della CPU, attivare anche l'opzione "Formatta Memory Card".
   - In seguito caricare il progetto con la configurazione modificata e con la password desiderata.
4. Se non è necessario modificare il progetto anche sulla Memory Card, ma è solo stata impostata una password errata:
   - Nella vista Online & Diagnostica selezionare l'area "Definisci password per la protezione dei dati di configurazione sensibili del PLC".
   - Fare clic sul pulsante "Elimina". Se il pulsante "Elimina" è disattivato, nella CPU la password non è ancora stata impostata.
   - Immettere la password e fare clic sul pulsante "Definisci".

   Se la password inserita è corretta, la CPU può utilizzare i dati di configurazione PLC riservati.

CPU non accessibile in scrittura

Se non si dispone dell'accesso in scrittura alla memoria di caricamento (livello di accesso in lettura), estrarre la Memory Card dalla CPU o cancellarla esternamente, ad es. nel computer, prima di ripristinare le impostazioni di fabbrica con l'opzione "Elimina password per la protezione dei dati di configurazione PLC riservati".

NOTA

Reset alle impostazioni di fabbrica con il selettore dei modi di funzionamento/i tasti dei modi di funzionamento della CPU

Se si resetta la CPU alle impostazioni di fabbrica con il selettore dei modi di funzionamento/i tasti dei modi di funzionamento si cancella anche l'indirizzo IP della CPU, ma non la password per la protezione dei dati di configurazione PLC riservati.

NOTA
Reset alle impostazioni di fabbrica tramite il display della CPU
Il ripristino delle impostazioni di fabbrica della CPU tramite il display cancella la password per la protezione dei dati di configurazione riservati del PLC.

Ulteriori informazioni

Per maggiori informazioni sui pezzi di ricambio consultare il cap. Regole per la sostituzione (Pagina 93).

5.6.3.4 Reset della password

La protezione dei dati di configurazione PLC può essere resettata. Ciò può rendersi necessario, ad esempio, se si intende modificare la password, ma non si ricorda più la password attuale.

Password dimenticata - configurazione non ancora caricata

Poiché al primo caricamento della CPU da TIA Portal è necessario immettere la password, la progettazione di questa CPU non può essere riutilizzata. Anche per modificare la password nelle proprietà della CPU è necessario immettere la password ancora valida. Se la password è stata dimenticata procedere nel seguente modo:

Presupposti

- La CPU non è ancora stata caricata

Procedimento

1. Aprire le proprietà della CPU nella vista di rete o nella vista dispositivi.
2. Spostarsi nella sezione "Protezione & Security > Protezione dei dati di configurazione PLC".
3. Fare clic sul pulsante "Resetta".

   Tenere presente che i certificati della CPU (ad es. certificati per il Web server, per il server OPC UA, per la comunicazione PG/PC e HMI) dopo il reset non possono più essere utilizzati e devono eventualmente essere ricreati e riassegnati.

   – Se si utilizzano le impostazioni Security globali per la gestione certificato è necessario assegnare di nuovo i certificati della gestione certificato.
   – Se non si utilizzano le impostazioni Security globali per la gestione certificato è necessario assegnare di nuovo i certificati.
4. Confermare il reset della password.

L'opzione per la protezione dei dati di configurazione PLC riservati è ancora abilitata.

Eliminazione della password - configurazione già caricata

Se nella CPU è già stata caricata una configurazione protetta da una password per i dati di configurazione PLC riservati, per il caricamento di un nuovo progetto è possibile cancellare questa password nella CPU, oppure direttamente online prima di reimpostarla.

Presupposti

- La CPU è accessibile in scrittura
- La CPU si trova nello stato di funzionamento STOP

Procedimento

1. Selezionare la CPU nella vista di rete.
2. Nel menu di scelta rapida selezionare il comando "Online & Diagnostica".
3. Nell'area "Definisci password per la protezione dei dati di configurazione sensibili del PLC", fare clic sul pulsante "Elimina".
   Se il pulsante "Elimina" è disattivato, nella CPU la password non è ancora stata impostata.

ATTENZIONE
Eliminazione della password per i dati di configurazione riservati Se la password viene cancellata e un progetto caricato necessita invece di quest'ultima, il progetto in questione potrebbe non funzionare più.

4. Se necessario inserire ora una nuova password selezionando il pulsante "Definisci".
5. Eseguire un nuovo avviamento della CPU.

NOTA

Password per la protezione dei dati di configurazione riservati dopo il ripristino delle impostazioni di fabbrica della CPU

- **Tramite il selettore/i pulsanti dei modi operativi (la SIMATIC Memory Card non è inserita):** La password per la protezione dei dati di configurazione riservati viene mantenuta.
- **Tramite display:** La password per la protezione dei dati di configurazione riservati viene eliminata.
- **Da STEP 7:** La password per la protezione dei dati di configurazione riservati viene mantenuta. La password viene cancellata solo se è attiva l'opzione "Cancella password per la protezione dei dati di configurazione PLC riservati".

Ulteriori informazioni

Per informazioni sulla modifica della password consultare il cap. Modifica della password (Pagina 85).

5.6.3.5 Assegnazione della password tramite la SIMATIC Memory Card

Per trasferire la password di protezione dei dati di configurazione PLC riservati ad una CPU senza l'impiego di TIA Portal, è possibile utilizzare per questa funzione anche una SIMATIC Memory Card.

L'utilizzo di una SIMATIC Memory Card si addice ai seguenti scopi:

- Preparazione di una nuova CPU

  Se viene reimpostata, la CPU deve essere configurata con una password per la protezione dei dati di configurazione PLC riservati. Una volta completata questa configurazione, è possibile utilizzare un'altra SIMATIC Memory Card con il progetto desiderato.

  (CPU S7-1200: per installare il programma sulla CPU è possibile anche utilizzare una "Transfer card" con ordine di trasferimento.)

- La CPU è dotata di una password per la protezione dei dati di configurazione PLC riservati, ma quest'ultima non è compatibile con il progetto.

  Se vi sono password diverse è possibile impostare nella CPU quella corretta utilizzando la Memory Card.

  (CPU S7-1200: dotata di una "Transfer card" SIMATIC oppure di una "Program card" SIMATIC).

- Reset della password per la protezione dei dati di configurazione PLC riservati nella CPU

  Come preparazione allo smaltimento della CPU oppure come preparazione di un nuovo progetto della CPU.

Presupposti

- TIA Portal versione V17 e successive

Procedimento di base

1. Creazione di una SIMATIC Memory Card con l'ordine "SET PASSWORD"

   Con quest'operazione viene creata, secondo uno schema specifico, la seguente struttura di cartelle e file e sulla SIMATIC Memory Card viene scritta, in un file speciale come solo testo, una password per la protezione dei dati di configurazione PLC riservati. Vedere la descrizione nel seguito.

2. Inserimento di una SIMATIC Memory Card preparata nella CPU e accensione di quest'ultima.

   Il PLC legge la password, la elabora e salva il risultato nella memoria interna. Un'eventuale registrazione preesistente viene sovrascritta.

3. Estrazione della SIMATIC Memory Card e riavvio della CPU.

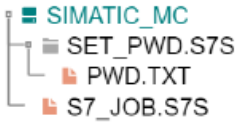
   Risultati (S7-1500): Durante la lettura della SIMATIC Memory Card da parte della CPU, il LED ha la stessa reazione che presenta quando viene aggiornato il firmware. Mentre la CPU imposta la password, il LED RUN/STOP lampeggia. Al termine dell'operazione, la luce gialla si accende sul LED RUN/STOP e lampeggia sul LED MAINT.

Il risultato dell'operazione viene visualizzato nel buffer di diagnostica come messaggio di errore o informazione sulla riuscita. Se la password non è stata impostata, il LED di errore lampeggia unitamente agli altri LED.

Creazione di una SIMATIC Memory Card con l'ordine "SET PASSWORD"

1. Nella directory radice creare una cartella con il nome "SET_PWD.S7S".
2. Creare un file di testo con il nome "PWD.TXT" indicando una password come solo testo nella cartella appena creata sulla Memory Card.
3. Nella directory radice della Memory Card creare un file di testo con il nome "S7_JOB.S7S" ed il contenuto "SET_PWD".

   Questo file è il "Job file" e consente l'assegnazione di una password per la protezione dei dati di configurazione riservati del PLC.
4. La struttura dei dati sulla SIMATIC Memory Card si presenta come segue:



NOTA

Conservazione sicura della SIMATIC Memory Card

Custodire la SIMATIC Memory Card in un luogo sicuro accessibile soltanto a personale autorizzato.

Regole e raccomandazioni

- L'impostazione della password deve avvenire in un ambiente sicuro.
- Il contenuto del file di testo "PWD.TXT" definisce la password per la protezione dei dati di configurazione PLC riservati e deve corrispondere alla password assegnata nella configurazione della CPU.
- Per consentire il reset della password del PLC, il file di testo "PWD.TXT" deve essere vuoto, ovvero avere dimensioni di 0 byte.
- La creazione del file di testo può avvenire in un editor di testo qualsiasi. Il formato di testo raccomandato è "UTF-8".
- Nei nomi di cartelle e file, non avviene alcuna distinzione tra caratteri maiuscoli e minuscoli. Nella password viene invece rilevata la differenza tra maiuscole e minuscole.
- Non inserire caratteri CR/LF alla fine della stringa (PWD.TXT o S7_JOB.S7S).

5.6.3.6 Particolarità per il backup e il ripristino della CPU

In TIA Portal è possibile fare il backup di una progettazione funzionante di una CPU per potervi accedere in un altro momento, il backup consente cioè di ripristinare la progettazione originale. In questo modo è possibile caricare una progettazione modificata, ad esempio per testare ampliamenti di funzioni, modificare programmi per la ricerca errori nell'impianto o per la sostituzione di componenti a scopo di test. Quindi è possibile ripristinare il backup della progettazione originale della CPU.

Backup della progettazione

Durante il backup della CPU (menu "Online", comando "Carica backup del dispositivo online" in TIA Portal), la password per la protezione dei dati di configurazione PLC riservati, non viene salvata nel backup.

Ripristino del backup

Con il ripristino del backup di una CPU (menu "Online", comando "Carica nel dispositivo" con backup selezionato in TIA Portal), quest'ultima può comunicare con un PG/PC o HMI, soltanto se sussiste la seguente condizione:

- Dopo il ripristino di una progettazione dotata di password per la protezione dei dati di configurazione PLC riservati, nella CPU deve essere presente esattamente quella password.

  Diversamente la CPU non può accedere ai dati di configurazione e quindi nemmeno eseguire il caricamento.

Rimedio

Se si verifica questo errore (cioè se la password per la protezione dei dati di configurazione PLC riservati non corrisponde al backup) cancellare la password nella CPU e impostare quella corretta. Dopo l'avvio della CPU il backup è funzionante.

5.6.3.7 Suggerimenti per evitare e gestire gli errori

Il testo che segue descrive alcuni casi applicativi che potrebbero causare messaggi di errore nella CPU.

Il buffer di diagnostica fornisce informazioni

La CPU rileva se la password per la protezione dei dati di configurazione riservati non è compatibile con la configurazione caricata. Un messaggio nel buffer di diagnostica indica le possibili cause e i rimedi e normalmente porta alla soluzione del problema.

Problemi tipici

Per evitare gli errori o per eliminarli tenere presente le seguenti situazioni:

- La configurazione è già stata caricata?
  A prescindere che i dati di configurazione riservati siano protetti da password o meno: finché la configurazione non è caricata, la CPU non esce dalla fase di distribuzione.
- Si tenta di caricare la CPU con una password configurata e la CPU ha già ricevuto un'altra password.
  Esempio: la CPU viene sostituita con un'altra CPU da magazzino, la CPU sostitutiva non è stata resettata completamente (reset alle impostazioni di fabbrica con l'opzione "Cancella password per la protezione dei dati di configurazione PLC riservati").
  Rimedio:
  - Preparare sempre le CPU sostitutive con l'opzione necessaria (password cancellata).
  - Per la configurazione da caricare utilizzare la stessa password utilizzata per la configurazione già caricata.
  - Il progetto / la configurazione della CPU caricati potrebbero essere errati. Controllare se è presente la configurazione della CPU compatibile.
  - Utilizzare la funzione online "Imposta password per la protezione dei dati di configurazione PLC riservati" per cancellare la password o impostare la stessa password della configurazione della CPU. Eseguire successivamente il riavvio.
- Un errore analogo si verifica se la configurazione della CPU non utilizza la password e se la configurazione già caricata richiede una password personalizzata.
  Rimedio:
  - Utilizzare la funzione online "Imposta password per la protezione dei dati di configurazione PLC riservati" per cancellare la password o impostare la stessa password della configurazione della CPU. Eseguire successivamente il riavvio.

5.6.3.8 Regole per la sostituzione

L'assegnazione di password per la protezione dei dati di configurazione PLC riservati si ripercuote anche sulla sostituzione dei componenti.

Regole per la sostituzione

In caso di sostituzione, attenersi alle regole seguenti:

Progettazione della CPU sostitutiva tramite TIA Portal

- Nella CPU destinata a sostituire una CPU esistente non deve essere presente alcuna progettazione né configurata alcuna password per la protezione dei dati di configurazione PLC riservati.
  Vantaggio: Il progetto può essere caricato nella CPU sostitutiva senza necessità di ulteriori operazioni, indipendentemente dal fatto che sia configurata una password o meno.
- Se la CPU sostitutiva è già progettata, la CPU deve essere resettata alle impostazioni di fabbrica impostando le opzioni seguenti:
  - "Elimina password per la protezione dei dati di configurazione PLC riservati"
  - "Formatta la Memory Card"

Caricamento dei dati di progettazione nella CPU sostitutiva tramite Memory Card

- Se nel progetto della CPU non è impostata **nessuna** password per la protezione dei dati di configurazione PLC riservati, è possibile inserire direttamente la Memory Card della CPU da sostituire in una CPU nuova e mai utilizzata.
  Se per la CPU sostitutiva è già stata progettata una password per la protezione dei dati di configurazione PLC riservati, occorre innanzitutto riportare la CPU alle impostazioni di fabbrica con l'opzione "Elimina password per la protezione dei dati di configurazione PLC riservati".
- Se ad un gruppo di CPU è stata assegnata la stessa password, è possibile assegnare la password di gruppo anche alla CPU sostitutiva tramite TIA Portal o tramite una scheda di memoria corrispondente (vedere Protezione dei dati di configurazione riservati (Pagina 81)).
  In questo caso è possibile ad es. inserire una Memory Card con il progetto attuale nella CPU ed effettuare la messa in servizio senza modificare la password.
- Se è stata assegnata una password diversa ad ogni CPU del progetto, in caso di impiego di una CPU sostitutiva è necessario innanzitutto impostare la password valida per ciascuna CPU nell'editor della vista Online & Diagnostica (area "Imposta password per la protezione dei dati di configurazione PLC riservati", vedere Modifica della password (Pagina 85)).

Ulteriori informazioni

Per informazioni sull'assegnazione della password per la protezione dei dati di configurazione riservati del PLC con l'ausilio della SIMATIC Memory Card, consultare il cap. Assegnazione della password tramite la SIMATIC Memory Card (Pagina 89).

5.6.4 Secure Open User Communication

5.6.4.1 Configurazione di Secure OUC da una CPU S7-1500 come client TLS a un PLC di terzi (server TLS)

Qui di seguito è descritta la configurazione della Secure Open User Communication tra una CPU S7-1500 come client TLS e un server TLS attraverso TCP.

Configurazione di un collegamento TCP protetto da una CPU S7-1500 come client TLS a un server TLS

Le CPU S7-1500 dalla versione firmware V2.0 in poi supportano la comunicazione sicura con indirizzamento attraverso un Domain Name System (DNS).

Per la comunicazione TCP protetta tramite nome del dominio è necessario creare e parametrizzare individualmente un blocco dati con il tipo di dati di sistema TCON_QDN_SEC e richiamarlo direttamente nell'istruzione TSEND_C, TRCV_C o TCON.

Presupposti:

- Nella CPU sono impostate data e ora attuali.
- Nella rete si trova almeno un server DNS.
- Per la CPU S7-1500 è stato configurato almeno un server DNS.
- Client TLS e server TLS sono in possesso di tutti i certificati necessari.

Per impostare un collegamento TCP protetto verso un server TLS, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire nel blocco dati globale una variabile del tipo di dati TCON_QDN_SEC.

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "DNS ConnectionSEC" del tipo di dati TCON_QDN_SEC.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	DNS Connection SEC	TCON_QDN_SEC		
3	ConnPara	TCON_QDN		parameter of the TCP connection
4	InterfaceId	HW_ANY	0	not relevant
5	ID	CONN_OUC	5	connection reference / identifier
6	ConnectionType	Byte	11	type of connection: 16#0B=11=TCP/IP, 16#13
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteQDN	String[254]	'plc_1.factory127.'	fully or partially qualified domain name of rem
9	RemotePort	UInt	4000	remote UDP / TCP port number
10	LocalPort	UInt	0	local UDP / TCP port number
11	ActivateSecureConn	Bool	true	activate the security functionality of that conn
12	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a
13	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 a
14	TLSServerCertRef	UDInt	7	for Server side: Reference to own X.509 V3 se
15	TLSClientCertRef	UDInt	0	for Client side: add id of own X.509 V3 client c

Figura 5-18 Tipo di dati TCON_QDN_SEC

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "RemoteQDN" il nome del dominio completo (FQDN) del server TLS.

4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio".
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "ExtTLSCapabilities": se si inserisce il valore 1, il client convalida subjectAlternateName nel certificato X.509-V3 del server per verificare l'identità del server. Questa convalida avviene nel contesto dell'istruzione.
   - "TLSServerCertRef": ID del certificato X.509-V3 (normalmente un certificato CA) che viene utilizzato dal client TLS per validare l'autenticazione del server TLS. Se questo parametro è 0, il client TLS, per validare l'autenticazione del server, utilizza tutti i certificati (CA) attualmente caricati nel Certificate Store del client.

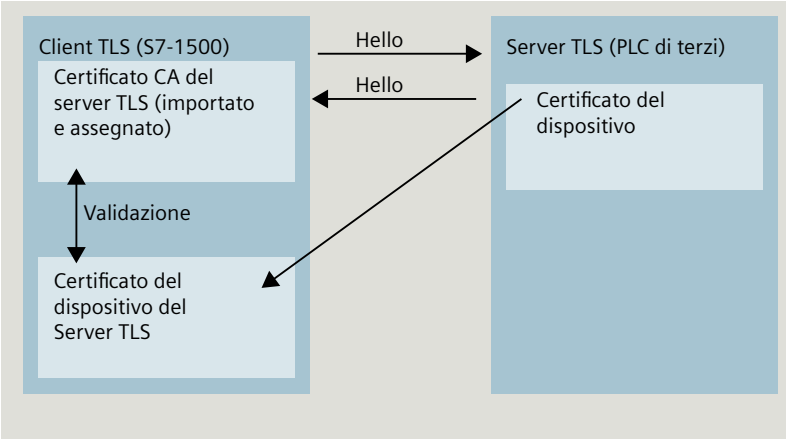


Figura 5-19 Utilizzo dei certificati dalla prospettiva della CPU S7-1500 come client TLS

   - "TLSClientCertRef": ID del proprio certificato X.509-V3.
5. Nell'editor di programma creare un'istruzione TSEND_C, TRCV_C o TCON.

6. Interconnettere il parametro CONNECT di una delle istruzioni TSEND_C, TRCV_C o TCON con la variabile del tipo di dati TCON_QDN_SEC.

   Nell'esempio seguente il parametro CONNECT dell'istruzione TCON è interconnesso con la variabile "DNS connectionSEC" (tipo di dati TCON_QDN_SEC).

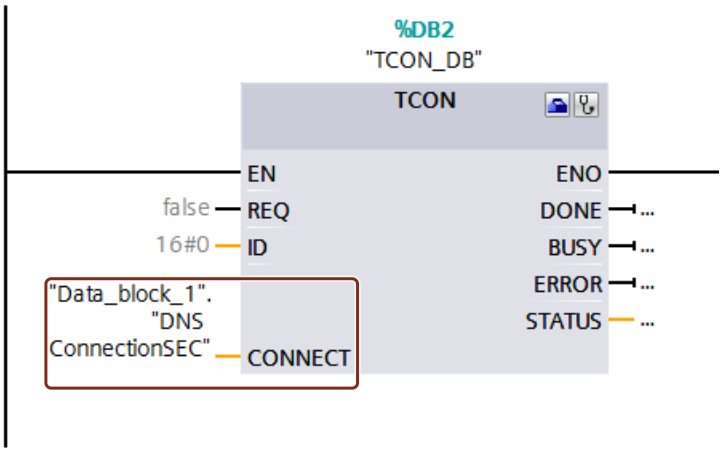


Figura 5-20 Istruzione TCON

Ulteriori informazioni

Maggiori informazioni sul tipo di dati di sistema TCON_QDN_SEC sono disponibili nella Guida in linea a STEP 7.

Per maggiori informazioni sulla comunicazione sicura vedere il capitolo Comunicazione sicura (Pagina 56).

5.6.4.2 Secure OUC da una CPU S7-1500 come server TLS a un PLC di terzi (client TLS)

Qui di seguito è descritta la configurazione della Secure Open User Communication tra una CPU S7-1500 come server TLS e un client TLS attraverso TCP.

Configurazione di un collegamento TCP protetto tramite nome del dominio del partner della comunicazione

Le CPU S7-1500 dalla versione firmware V2.0 in poi supportano la comunicazione sicura con indirizzamento attraverso un Domain Name System (DNS).

Per la comunicazione TCP protetta tramite nome del dominio è necessario creare e parametrizzare individualmente un blocco dati con il tipo di dati di sistema TCON_QDN_SEC e richiamarlo direttamente nell'istruzione TSEND_C, TRCV_C o TCON.

Presupposti:

- Nella CPU sono impostate data e ora attuali.
- Nella rete si trova almeno un server DNS.
- Per la CPU S7-1500 è stato configurato almeno un server DNS.
- Client TLS e server TLS sono in possesso di tutti i certificati necessari.

Per impostare un collegamento TCP protetto verso un client TLS, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire nel blocco dati globale una variabile del tipo di dati TCON_QDN_SEC.

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "DNS ConnectionSEC" del tipo di dati TCON_QDN_SEC.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	DNS Connection SEC2	TCON_QDN_SEC		
3	ConnPara	TCON_QDN		parameter of the TCP connection
4	InterfaceId	HW_ANY	0	not relevant
5	ID	CONN_OUC	8	connection reference / identifier
6	ConnectionType	Byte	11	type of connection: 16#0B=11=TCP/IP, 16#13
7	ActiveEstablished	Bool	false	active/passive connection establishment
8	RemoteQDN	String[254]	''	fully or partially qualified domain name of rem
9	RemotePort	UInt	0	remote UDP / TCP port number
10	LocalPort	UInt	2010	local UDP / TCP port number
11	ActivateSecureConn	Bool	true	activate the security functionality of that conn
12	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a
13	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 a
14	TLSServerCertRef	UDInt	5	for Server side: Reference to own X.509 V3 se
15	TLSClientCertRef	UDInt	0	for Client side: add id of own X.509 V3 client c

Figura 5-21 TCON_QDN_SEC_Server

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "ID" l'ID locale del collegamento TCP.
4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio".
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "TLSServerReqClientCert": richiesta di un certificato X.509-V3 dal client TLS.
   - "TLSServerCertRef": ID del proprio certificato X.509-V3.

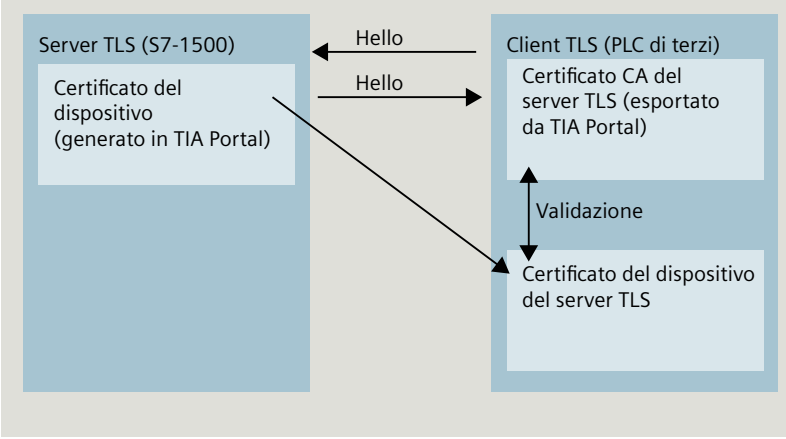


Figura 5-22 Utilizzo dei certificati dalla prospettiva della CPU S7-1500 come server TLS

– "TLSClientCertRef": ID del certificato X.509-V3 (o di un gruppo di certificati X.509-V3) che viene utilizzato dal server TLS per validare l'autenticazione del client TLS. Se questo parametro è 0, il server TLS, per validare l'autenticazione del client, utilizza tutti i certificati (CA) attualmente caricati nel Certificate Store del server.

5. Nell'editor di programma creare un'istruzione TSEND_C, TRCV_C o TCON.
6. Interconnettere il parametro CONNECT di una delle istruzioni TSEND_C, TRCV_C o TCON con la variabile del tipo di dati TCON_QDN_SEC.

   Nell'esempio seguente il parametro CONNECT dell'istruzione TCON è interconnesso con la variabile "DNS connectionSEC" (tipo di dati TCON_QDN_SEC).

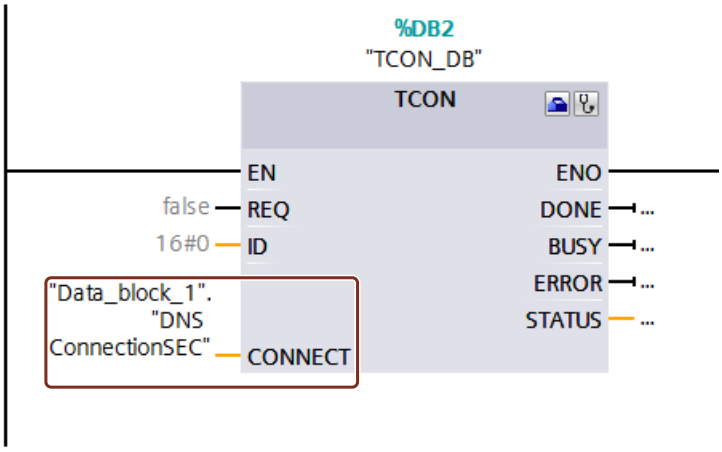


Figura 5-23 Istruzione TCON

Ulteriori informazioni

Maggiori informazioni sui tipi di dati di sistema TCON_QDN_SEC sono disponibili nella Guida in linea a STEP 7.

Per maggiori informazioni sulla comunicazione sicura vedere il capitolo Comunicazione sicura (Pagina 56).

5.6.4.3 Secure OUC tra due CPU S7-1500

Qui di seguito è descritta la configurazione della Secure Open User Communication tra due CPU S7-1500 attraverso TCP. Una CPU S7-1500 funge da client TLS (creazione del collegamento attiva) e l'altra CPU S7-1500 funge da server TLS (creazione del collegamento passiva).

Configurazione del collegamento TCP protetto tra due CPU S7-1500

Per la comunicazione TCP protetta tra due CPU S7-1500 è necessario creare e parametrizzare individualmente, per ogni CPU, un blocco dati con il tipo di dati di sistema TCON_IP_V4_SEC e richiamarlo direttamente nell'istruzione TSEND_C, TRCV_C o TCON.

Presupposti:

- Nella CPU sono impostate data e ora attuali.
- Entrambe le CPU S7-1500 hanno almeno la versione firmware V2.0
- Client TLS e server TLS sono in possesso di tutti i certificati necessari.

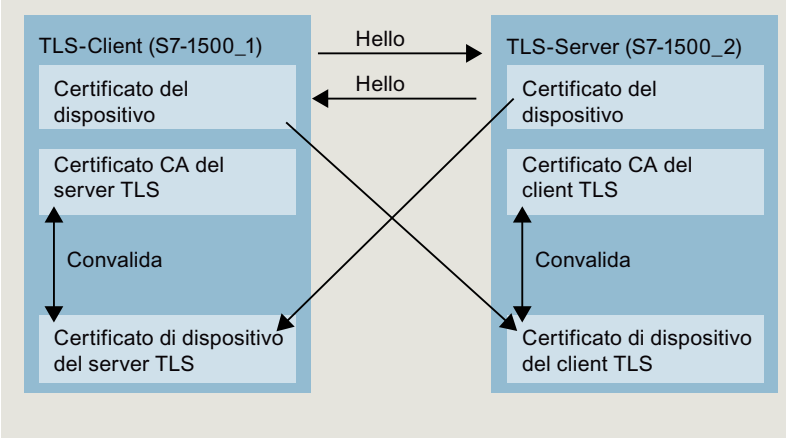


Figura 5-24 Utilizzo dei certificati per Secure OUC tra due CPU S7-1500

Impostazioni sul client TLS

Per impostare un collegamento TCP protetto sul client TLS, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire nel blocco dati globale una variabile del tipo di dati TCON_IP_V4_SEC.

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "SEC connection 1 TLS-Client" del tipo di dati TCON_IP_V4_SEC.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Client	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	72	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	100	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against th
19	TLSServerCertRef	UDInt	1	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	5	for Client side: add id of own X.509 V3 client certificate; for Serv

Figura 5-25 IP_V4_SEC_Client

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "RemoteAddress" l'indirizzo IPv4 del server TLS.

NOTA

Parametri di collegamento InterfaceId

Nel tipo di dati TCON_IP_V4_SEC è possibile specificare il valore "**0**" per l'InterfaceId. In questo caso è la CPU stessa a rilevare un'interfaccia locale adatta.

---

4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio".
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "TLSServerCertRef": Inserire il valore 2 (riferimento al certificato CA del progetto di TIA Portal (SHA256) o il valore 1 (riferimento al certificato CA del progetto di TIA Portal (SHA1)). Se si utilizza un altro certificato CA, inserire l'ID corrispondente della gestione certificato nelle impostazioni di sicurezza globali.
   - "TLSClientCertRef": ID del proprio certificato X.509-V3.

5. Nell'editor di programma creare un'istruzione TSEND_C, TRCV_C o TCON.
6. Interconnettere il parametro CONNECT di una delle istruzioni TSEND_C, TRCV_C o TCON con la variabile del tipo di dati TCON_IP_V4_SEC.

Impostazioni sul server TLS

Per impostare un collegamento TCP protetto sul server TLS, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire una variabile del tipo di dati TCON_IP_V4_SEC nel blocco dati globale.

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "SEC connection 1 TLS-Server" del tipo di dati TCON_IP_V4_SEC.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Server	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	120	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	false	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	10	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	true	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against the
19	TLSServerCertRef	UDInt	6	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	1	for Client side: add id of own X.509 V3 client certificate; for Serv

Figura 5-26 IP_V4_SEC_Server

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "RemoteAddress" l'indirizzo IPv4 del client TLS.
4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio".
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "TLSServerReqClientCert ": richiesta di un certificato X.509-V3 dal client TLS. Inserire il valore "true".
   - "TLSServerCertRef": ID del proprio certificato X.509-V3.
   - "TLSClientCertRef": Inserire il valore 2 (riferimento al certificato CA del progetto di TIA Portal (SHA256) o il valore 1 (riferimento al certificato CA del progetto di TIA Portal (SHA1)). Se si utilizza un altro certificato CA, inserire l'ID corrispondente della gestione certificato nelle impostazioni di sicurezza globali.

5. Nell'editor di programma creare un'istruzione TSEND_C, TRCV_C o TCON.
6. Interconnettere il parametro CONNECT di una delle istruzioni TSEND_C, TRCV_C o TCON con la variabile del tipo di dati TCON_IP_V4_SEC.

   Nell'esempio seguente il parametro CONNECT dell'istruzione TSEND_C è interconnesso con la variabile "SEC connection 1 TLS-Client" (tipo di dati TCON_IP_V4_SEC).

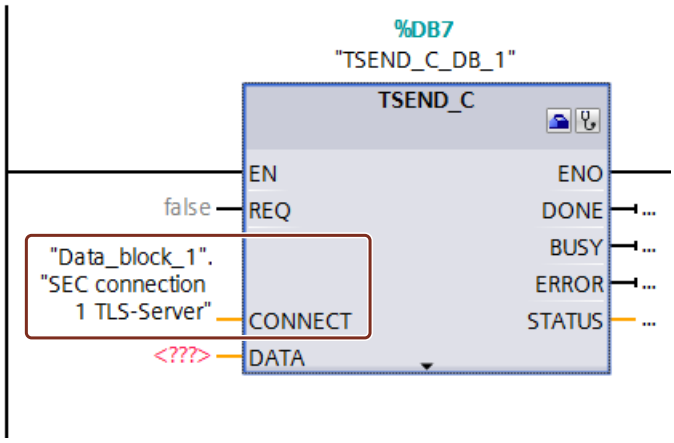


Figura 5-27 TSEND_C

Ulteriori informazioni

Maggiori informazioni sui tipi di dati di sistema TCON_IP_V4_SEC sono disponibili nella Guida in linea a STEP 7.

Per maggiori informazioni sulla comunicazione sicura vedere il capitolo Comunicazione sicura (Pagina 56).

5.6.4.4 Secure OUC tramite interfaccia CP

Di seguito sono descritte le particolarità da prendere in considerazione in caso di Secure Open User Communication tramite un'interfaccia CP. Almeno una stazione è una stazione S7-1500 con le seguenti unità:

- CPU S7-1500 dalla versione di firmware V2.0 (eccetto S7-1500 Software Controller)
- CP
  - CP 1543-1 dalla versione firmware V2.0
  - CP 1545-1 dalla versione firmware V1.0
  - CP 1543SP-1 dalla versione firmware V1.0

Il CP agisce in una stazione S7-1500 come client TLS (creazione attiva del collegamento) o come server TLS (creazione passiva del collegamento).

La procedura essenziale e il criterio per l'utilizzo della comunicazione sicura mediante un'interfaccia CP sono analoghi a quelli per la comunicazione sicura tramite le interfacce delle CPU S7-1500. Fondamentalmente è necessario assegnare i certificati al CP nel ruolo di server TLS o client TLS e non alla CPU. Pertanto sono valide altre regole e procedure descritte di seguito.

Gestione dei certificati per CP

In linea generale vale quanto segue: con la gestione del certificato è necessario essere registrati nelle impostazioni di sicurezza globali. Anche la creazione di certificati autofirmati non è possibile senza registrazione per le impostazioni di sicurezza globali. L'utente deve essere dotato di diritti sufficienti (amministratore o utente con il ruolo "standard" con il diritto "Configura sicurezza").

Il punto di partenza per la creazione o l'assegnazione di certificati nel caso del CP è l'area "Security > Proprietà Security". In quest'area è possibile registrarsi per le impostazioni di sicurezza globali.

Procedimento:

1. Nella Vista di rete di STEP 7 selezionare il CP e nella finestra di ispezione l'area "Security > Proprietà Security".
2. Fare clic sul pulsante "Login utente".
3. Registrarsi con nome utente e password.
4. Attivare l'opzione "Attiva funzioni Security".

   Vengono inizializzate le proprietà Security.
5. Fare clic nella prima riga della tabella "Certificati dei dispositivi" per creare un nuovo certificato o selezionare un certificato esistente.
6. Se il partner della comunicazione è anch'esso una stazione S7-1500 occorre assegnargli un certificato del dispositivo con STEP 7, come descritto qui o nella CPU S7-1500.

Esempio: configurazione del collegamento TCP protetto di due CPU S7-1500 tramite interfacce CP

Per la comunicazione TCP protetta tra due CP S7-1500 è necessario creare e parametrizzare individualmente un blocco dati con il tipo di dati di sistema TCON_IP_V4_SEC per ogni CPU e richiamarlo direttamente nell'istruzione.

Presupposti:

- Le due CPU S7-1500 hanno una delle versioni firmware sopra indicate.
- I CP hanno una delle versioni firmware sopra indicate.
- Client TLS e server TLS sono in possesso di tutti i certificati necessari.
  - Un certificato del dispositivo (certificato di entità finale) per il CP deve essere generato e trovarsi nella memoria dei certificati del CP. Se un partner della comunicazione è un dispositivo di terzi (ad es. un sistema MES o ERP), anche per questo dispositivo deve essere disponibile un certificato.
  - Il certificato radice (certificato CA), con il quale è firmato il certificato del dispositivo del partner della comunicazione, deve trovarsi nella memoria dei certificati del CP o in quella del dispositivo di terzi. Se si utilizzano dei certificati intermedi, occorre assicurarsi che l'intero percorso del certificato sia presente nel dispositivo che esegue la convalida. Questi certificati utilizzano un dispositivo per la convalida del certificato del dispositivo del partner della comunicazione.
- Il partner della comunicazione deve essere indirizzato generalmente tramite il suo indirizzo IPv4 e non tramite il suo nome di dominio.

La figura seguente riporta i diversi certificati nei dispositivi nel caso in cui i due partner della comunicazione comunichino attraverso un CP. Inoltre la figura mostra il trasferimento dei certificati del dispositivo alla creazione del collegamento ("Hello").

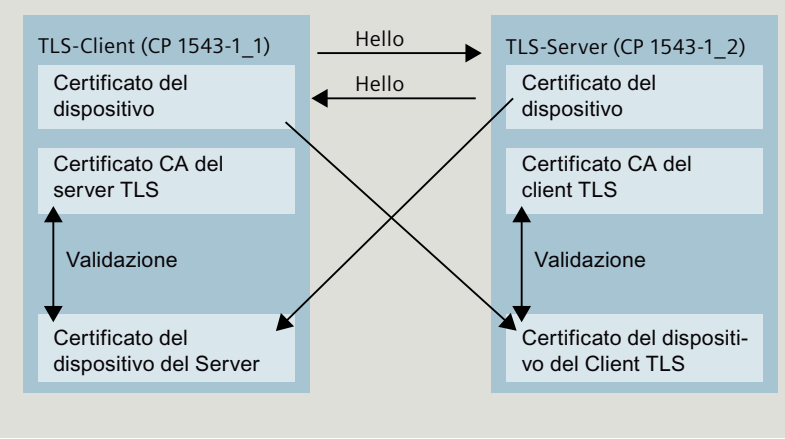


Figura 5-28 Utilizzo dei certificati per Secure OUC tra due CPU S7-1500 tramite interfacce CP

Impostazioni sul client TLS

Per impostare un collegamento TCP protetto sul client TLS, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire una variabile del tipo di dati TCON_IP_V4_SEC nel blocco dati globale. A questo scopo, nel campo “Tipo di dati” inserire la stringa di caratteri "TCON_IP_V4_SEC".

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "SEC connection 1 TLS-Client" del tipo di dati TCON_IP_V4_SEC.

   L’InterfaceId ha il valore dell’identificazione HW dell’interfaccia IE del CP locale (client TLS).

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Client	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	258	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	100	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against th
19	TLSServerCertRef	UDInt	1	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	5	for Client side: add id of own X.509 V3 client certificate; for Sen

Figura 5-29 IP_V4_SEC_Client

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in “RemoteAddress” l'indirizzo IPv4 del server TLS.
4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio".
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "TLSServerCertRef": Inserire il valore 2 (riferimento al certificato CA del progetto di TIA Portal (SHA256) o il valore 1 (riferimento al certificato CA del progetto di TIA Portal (SHA1)).
   - "TLSClientCertRef": ID del proprio certificato X.509-V3.
5. Nell'editor di programma creare un'istruzione TCON.
6. Interconnettere il parametro CONNECT dell'istruzione TCON con la variabile del tipo di dati TCON_IP_V4_SEC.

Impostazioni sul server TLS

Per impostare un collegamento TCP protetto sul server TLS, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire una variabile del tipo di dati TCON_IP_V4_SEC nel blocco dati globale.

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "SEC connection 1 TLS-Server" del tipo di dati TCON_IP_V4_SEC.

   L'InterfaceId ha il valore dell'identificazione HW dell'interfaccia IE del CP locale (server TLS).

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Server	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	260	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	false	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	10	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	true	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against the
19	TLSServerCertRef	UDInt	6	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	1	for Client side: add id of own X.509 V3 client certificate; for Serv

Figura 5-30 IP_V4_SEC_Server

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "RemoteAddress" l'indirizzo IPv4 del client TLS.
4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio".
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "TLSServerReqClientCert ": richiesta di un certificato X.509-V3 dal client TLS. Inserire il valore "true".
   - "TLSServerCertRef": ID del proprio certificato X.509-V3.
   - "TLSClientCertRef": Inserire il valore 2 (riferimento al certificato CA del progetto di TIA Portal (SHA256) o il valore 1 (riferimento al certificato CA del progetto di TIA Portal (SHA1)).

5. Nell'editor di programma creare un'istruzione TCON.
6. Interconnettere il parametro CONNECT dell'istruzione TCON con la variabile del tipo di dati TCON_IP_V4_SEC.

Caricamento del dispositivo come nuova stazione

Se una configurazione con certificati e Secure Open User Communication progettata viene caricata nel progetto STEP 7, i certificati del CP non vengono caricati, diversamente da quanto avviene per i certificati della CPU. Una volta caricato il dispositivo come nuova stazione, le tabelle corrispondenti dei CP non contengono più alcun certificato per i dispositivi.

Dopo il caricamento è necessario eseguire nuovamente la progettazione dei certificati. In caso contrario, un nuovo caricamento della configurazione determina la cancellazione dei certificati presenti originariamente nel CP e il mancato funzionamento della comunicazione sicura.

Collegamenti Secure OUC tramite interfacce CPU e CP - punti in comune

- Risorse di collegamento:
  Nessuna differenza tra OUC e Secure OUC. Un collegamento Secure OUC programmato richiede una risorsa di collegamento allo stesso modo di un collegamento OUC, indipendentemente dall'interfaccia IE/PROFINET con cui la stazione comunica.
- Diagnostica dei collegamenti:
  Nessuna differenza tra diagnostica dei collegamenti OUC e Secure OUC.
- Caricamento di progetti nella CPU con collegamenti Secure OUC:
  Possibile solo se la CPU è in stato di funzionamento STOP, qualora venissero caricati anche certificati. Per i requisiti per aggiornare i certificati caricato in RUN vedere Suggerimento: Aggiornamento dei certificati caricati in RUN (Pagina 80).
  Suggerimento: Carica nel dispositivo > Hardware e software. Motivo: Garantire la coerenza tra i programmi con Secure OUC, la configurazione hardware e i certificati.
  Il caricamento successivo di blocchi che utilizzano altri collegamenti Secure OUC è possibile nello stato di funzionamento RUN solo se i certificati necessari si trovano già sull'unità.

5.6.4.5 Secure OUC con Modbus TCP

Per garantire un collegamento Modbus TCP protetto verso un server di posta è necessario creare e parametrizzare individualmente un blocco dati con uno dei tipi di dati di sistema TCON_IP_V4_SEC o TCON_QDN_SEC e richiamarlo direttamente nell'istruzione MB_Server oppure MB_CLIENT.

Presupposti

- CPU S7-1500 dalla versione firmware V2.5
- Il client Modbus (client TLS) può accedere al server Modbus (server TLS) nella rete tramite comunicazione IP.
- Client TLS e server TLS sono provvisti di tutti i certificati necessari.

Esempio di configurazione del collegamento TCP Modbus al server Modbus TCP

Qui di seguito è descritta la configurazione, tramite Modbus TCP, di Secure Open User Communication tra un client Modbus TCP e un server Modbus TCP.

Per configurare un collegamento protetto da un client Modus TCP (client TLS) a un server Modus TCP (server TLS), procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire una variabile del tipo di dati TCON_IP_V4 SEC nel blocco dati globale.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC_ModbusTCP_1	TCON_IP_V4...		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	64	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	15	connection reference / identifier
6	ConnectionType	Byte	11	type of connection: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of B...		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	10	IPv4 address
13	ADDR[4]	Byte	100	IPv4 address
14	RemotePort	UInt	502	remote UDP/TCP port number
15	LocalPort	UInt	502	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	0	Bit 0: Just for client side: validate given IPv4 address against the subjectAlt
19	TLSServerCertRef	UDInt	2	for Server side: Reference to own X.509 V3 server certificate; for Client side:
20	TLSClientCertRef	UDInt	7	for Client side: add id of own X.509 V3 client certificate; for Server side: add

Figura 5-31 TCON_IP_V4_SEC

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "MailServerAdress" l'indirizzo IPv4 del server e-mail.

4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio". Inserire ad es. in "TLSServerCertRef" l'ID del certificato CA del partner di comunicazione.
   – "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso è possibile configurare un collegamento TCP non sicuro.
   – "TLSServerCertRef": Riferimento al certificato X.509 V3 (CA) del server Modbus TCP utilizzato dal client TLS per convalidare l'autenticazione di questo server.
5. Nell'editor di programma creare un'istruzione MB_Client.
6. Interconnettere il parametro CONNECT dell'istruzione MB_Client con la variabile del tipo di dati TCON_IP_V4_SEC.

5.6.4.6 Secure OUC via e-mail

Collegamento protetto con un server e-mail tramite l'interfaccia della CPU

Per garantire un collegamento protetto verso un server di posta è necessario creare e parametrizzare individualmente un blocco dati con uno dei tipi di dati di sistema TMAIL_V4_SEC, TMAIL_QDN_SEC e richiamarlo direttamente nell'istruzione TMAIL_C.

Presupposti

- Istruzione TMAIL_C dalla versione V5.0
- STEP 7 V15 o superiore
- CPU S7-1500 da V2.5
- Tutti i certificati CA del server e-mail (server TLS) sono stati assegnati alla CPU (client TLS) e la configurazione è stata caricata nella CPU.
- Nella CPU sono impostate data e ora attuali.

Procedura per la configurazione del collegamento protetto al server e-mail

Per la configurazione del collegamento protetto al server e-mail, è possibile optare per una delle seguenti procedure:

- SMTPS: Il client cerca subito di creare il collegamento TLS con il server e-mail (procedura "Handshake"). Se il server e-mail non supporta TLS, la comunicazione non viene creata.
- STARTTLS: Il client crea un collegamento TCP con il server e-mail. Mediante il collegamento TCP il client invia una richiesta di "Aggiornamento" del collegamento preesistente per realizzare una connessione TLS protetta. Supporta il server e-mail TLS, quindi invia al client il comando per la configurazione di un collegamento protetto. Il server e-mail utilizza il comando SMTP "STARTTLS". Il client crea un collegamento protetto con il server e-mail. Vantaggi: Se il server e-mail non supporta TLS, la comunicazione tra questo server e il client si svolge in modalità non sicura.

La selezione della procedura di comunicazione avviene nell'impostazione "Remote Port" nel tipo di dati nel parametro di bus "MAIL_ADDR_PARAM".

Tabella 5-6 Numeri delle porte per le procedure SMTPS e STARTTLS

Procedura	Porta
SMTPS	465[1]
STARTTLS	a scelta (≠465)[2]

[1] L'istruzione TMAIL_C utilizza SMTPS solo per la porta 465. Per tutte le altre porte viene utilizzato STARTTLS.

[2] secondo RFC i server e-mail impiegano le porte 25 e 587 per i collegamenti protetti con STARTTLS. L'utilizzo di altri numeri di porta SMTP non è conforme a RFC, la comunicazione con questo server e-mail non è garantita.

Esempio: Configurazione di un collegamento protetto con un server e-mail tramite IPv4

Qui di seguito viene descritta la modalità di configurazione di un collegamento protetto a un server e-mail IPv4 con l'istruzione di comunicazione TMAIL_C.

Per configurare un collegamento protetto attraverso l'indirizzo IPv4 del server e-mail, procedere nel modo seguente:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire nel blocco dati globale una variabile del tipo di dati TMAIL_V4_SEC.

   L'esempio seguente mostra il blocco dati globale "MailConnDB" nel quale è definita la variabile "MailConnectionSEC" del tipo di dati TMAIL_V4_SEC.

MailConnDB

Name	Datentyp	Startwert	Kommentar
Static			
MailConnectionSEC	TMail_V4_SEC		
InterfaceId	HW_ANY	"Local~CP_1543-1_1~Ethernet-Schnittstelle_1"	Use HW-identifier of the IE-interface to specify th
ID	CONN_OUC	100	connection reference / identifier
ConnectionType	Byte	16#20	type of connection 16#20=32=TMail_V4 or TMai
ActiveEstablished	Bool	true	active / passive connection establishment
WatchDogTime	Time	T#5000ms	watchdog time to monitor SMTP server associat
MailServerAddress	IP_V4		IPv4 address of mail server
ADDR	Array[1..4] of Byte		IPv4 address
ADDR[1]	Byte	144	IPv4 address
ADDR[2]	Byte	145	IPv4 address
ADDR[3]	Byte	2	IPv4 address
ADDR[4]	Byte	20	IPv4 address
UserName	String[254]	'myName'	user name which is necessary to login into the
PassWord	String[254]	'myPW'	user password which is necessary to login into
From	EMAIL_ADDR		source mail address
LocalPartPlusAt...	String[64]	'Mustermann@'	local part of e-mail address plus "@" sign
FullQualifiedD...	String[254]	'siemens.com'	full qualified domain name part of e-mail addre
RemotePort	UInt	587	remote TCP port number
ActivateSecureConn	Bool	TRUE	activate the security functionality of that conne
ExtTLSCapabilities	Byte	16#0	for further capability extensions of the TLS hand
TLSServerCertRef	UDInt	7	Reference to the X.509 V3 (CA-) certificate of the

Figura 5-32 Tipo di dati TMAIL_V4_SEC

3. Impostare i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "MailServerAdress" l'indirizzo IPv4 del server e-mail.

NOTA

Parametri di collegamento InterfaceId

Dalla versione V5.0 dell'istruzione TMAIL_C è possibile specificare nel tipo di dati TMAIL_V4_SEC il valore "**0**" per l'InterfaceId. In questo caso è la CPU stessa a rilevare un'interfaccia locale adatta.

---

4. Impostare i parametri per la comunicazione sicura nella colonna "Valore di avvio". Inserire ad es. in "TLSServerCertRef" l'ID del certificato CA del partner di comunicazione.
   - "ActivateSecureConn": Attivazione della comunicazione sicura per questo collegamento. Se questo parametro ha il valore FALSE, i parametri di sicurezza seguenti non sono rilevanti. In questo caso si può configurare un collegamento TCP o UDP non sicuro.
   - "TLSServerCertRef": Riferimento al certificato X.509 V3 (CA) del server e-mail utilizzato dal client TLS per convalidare l'autenticazione del server e-mail.
5. Creare un'istruzione TMAIL_C nell'editor di programma.
6. Interconnettere il parametro MAIL_ADDR_PARAM dell'istruzione TMAIL_C con la variabile del tipo di dati TMAIl_V4_SEC.

   Nell'esempio seguente il parametro Mail_ADDR_PARAM dell'istruzione TMAIL_C è interconnesso con la variabile "MailConnectionSEC" (tipo di dati TMAIL_V4_SEC).

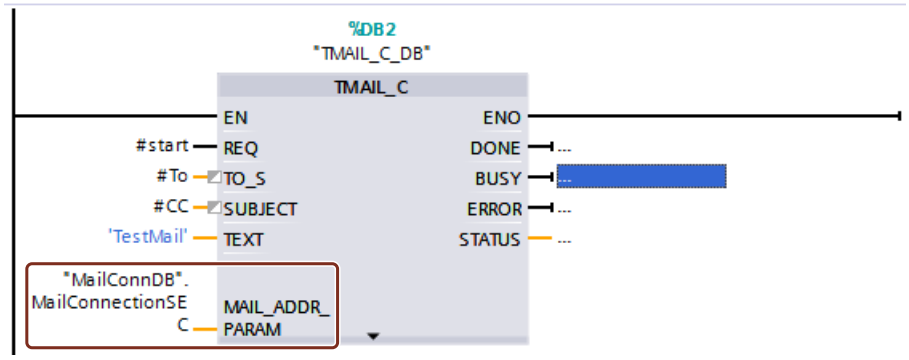


Figura 5-33 Istruzione TMAIL_C

Collegamento protetto con un server e-mail tramite l'interfaccia di un modulo di comunicazione

Per garantire un collegamento protetto verso un server e-mail tramite un modulo di comunicazione è necessario creare e parametrizzare individualmente un blocco dati con uno dei tipi di dati di sistema TMAIL_V4_SEC, TMAIL_QDN_SEC o TMAIL_V6_SEC (soltanto CP) e richiamarlo direttamente nell'istruzione TMAIL_C.

Presupposti:

- Istruzione TMAIL_C mcon versione **V4.0**
- CPU S7-1500 con versione firmware V2.0 o superiore e modulo di comunicazione CP 1543-1 dalla versione firmware V2.0

- CPU ET 200SP con versione firmware V2.0 o superiore e modulo di comunicazione CP 1542SP-1 (IRC) dalla versione firmware V1.0
- Tutti i certificati CA del server e-mail (server TLS) sono stati assegnati al CP (client TLS) e la configurazione è stata caricata nella CPU.
- Nella CPU sono impostate data e ora attuali.

Le modalità di configurazione del collegamento protetto con il server e-mail tramite l'interfaccia del modulo di comunicazione, sono descritte nella Guida in linea a STEP 7.

Esempio applicativo

Per informazioni su come impostare un collegamento protetto con un server e-mail tramite il CP di una stazione S7-1500 o S7-1200 e su come trasmettere dalla CPU S7 una e-mail con l'istruzione standard "TMAIL_C" vedere questo esempio applicativo (https://support.industry.siemens.com/cs/ww/it/view/46817803).

Ulteriori informazioni

Maggiori informazioni sui tipi di dati di sistema TMail_V4_SEC e TMAIL_QDN_SEC sono disponibili nella Guida in linea a STEP 7.

Per maggiori informazioni sulla comunicazione sicura vedere il capitolo Comunicazione sicura (Pagina 56).

5.6.5 Comunicazione PG/HMI sicura

5.6.5.1 Comunicazione PG/HMI basata su meccanismi di sicurezza standardizzati

Con i componenti centrali di TIA Portal, STEP 7 e WinCC, a partire dalla versione V17 in combinazione con gli attuali controllori e dispositivi HMI viene implementata una nuova comunicazione PG/HMI standardizzata e sicura (secure), denominata in breve Comunicazione PG/HMI.

In particolare si tratta delle seguenti famiglie di CPU:

- Famiglia di controllori S7-1500 a partire dalla versione firmware V2.9
- Famiglia di controllori S7-1200 a partire dalla versione firmware V4.5
- Software Controller a partire dalla versione firmware V21.9
- SIMATIC Drive Controller a partire dalla versione firmware V2.9
- PLCSim e PLCSim Advanced versione V4.0

Inoltre, per supportare la comunicazione sicura PG/HMI, sono stati aggiornati alcuni componenti HMI:

- Panel e PC progettati con WinCC Basic, Comfort e Advanced
- PC con WinCC RT Professional
- WinCC Unified PC e Comfort Panel

Allo stesso tempo vengono aggiornati SINAMICS RT SW dalla versione V6.1 in poi e STARTDRIVE dalla versione V17.

Proprietà della comunicazione PG/HMI

Un caratteristica della comunicazione PG e della comunicazione HMI è soprattutto la semplicità: creare un collegamento online tra un dispositivo di programmazione con TIA Portal e una CPU, ad esempio, è molto facile. Questo collegamento online, inoltre, soddisfa anche criteri come ad es. la riservatezza e l'integrità, basandosi su uno standard di comunicazione SIMATIC ormai collaudato.

Nell'ambito dell'integrazione di macchine e impianti in un ambiente IT aperto, tuttavia, è necessario preparare il terreno per una comunicazione tra dispositivo di programmazione/dispositivo HMI e CPU che non sia soltanto sicura perché garantisce la riservatezza e l'integrità dei dati sensibili, ma anche perché soddisfa standard comunemente riconosciuti ed è all'altezza delle sfide future.

Con TIA Portal versione V14 il metodo "Open User Communication" per la comunicazione basata su programma utente era già stato ampliato con la variante **"Secure** Open User Communication". Si sono affermati ulteriori meccanismi di comunicazione basati su certificato (HTTPS, Secure SMTP over TLS o OPC UA). A partire da TIA Portal versione V17 anche la comunicazione PG/HMI viene ottimizzata: anche qui viene introdotto il protocollo TLS (Transport Layer Security) per proteggere la comunicazione PG/HMI con meccanismi di sicurezza standardizzati.

Le modifiche

Password opzionale aggiuntiva per aumentare la sicurezza

La modifica più evidente nell'ambito della progettazione dei dispositivi sopra menzionati, consiste nella possibilità di assegnare una password per la protezione dei dati di configurazione riservati della rispettiva CPU. Con questo termine si intendono dati come ad es. chiavi private necessarie per il regolare funzionamento dei protocolli basati su certificati (Secure Communication). Da TIA Portal V17 è inclusa anche la comunicazione PG/HMI. Le password assegnate possono essere verificate già mentre vengono inserite in TIA Portal impostando delle regole, in modo da garantire il rispetto dei criteri per le password all'interno dell'azienda.

Se la macchina o l'impianto, esaminati globalmente sulla base del concetto di sicurezza industriale Siemens "Defense-in-Depth", non richiedono questa protezione, ad es. perché sussiste già una protezione analoga, si può decidere di non impostare la password. L'assegnazione della password si rende superflua se sono state implementate altre misure volte ad impedire l'accesso non autorizzato al progetto TIA Portal e alla progettazione della CPU.

⚠ **AVVERTENZA**
Senza password protezione bassa della chiave privata Tenere presente che senza una password per la protezione dei dati di configuazione riservati la protezione delle chiavi private per i certificati necessarie per la comunicazione sicura è bassa.

Comunicazione tra PG/HMI e CPU basata su certificati

Dato che la comunicazione PG/HMI si basa sull'uso di certificati, durante la messa in servizio viene chiesto di accettare il certificato server.

Altre opzioni di parametrizzazione consentono di determinare il comportamento della CPU durante il funzionamento: È possibile ad es. stabilire che la CPU debba consentire anche il collegamento ai dispositivi che non supportano la comunicazione PG/HMI sicura.

Manutenzione / sostituzione

Per evitare problemi in caso di sostituzione della CPU occorre osservare alcune regole (vedere Regole per la sostituzione (Pagina 93)).

Ulteriori informazioni

Una panoramica della protezione dei dati di configurazione riservati, si trova al cap. Protezione dei dati di configurazione riservati (Pagina 81).

5.6.5.2 Ulteriori impostazioni della comunicazione PG/HMI sicura

Oltre alla creazione di una password per la protezione dei dati di configurazione PLC riservati, sono disponibili altre impostazioni che permettono di influenzare il comportamento della CPU durante il funzionamento.

Modalità di comunicazione HMI e PG/PC

È possibile impostare in che modo la CPU dovrà comunicare con i dispositivi di programmazione e i dispositivi HMI:

- Solo tramite comunicazione PG/HMI sicura
- Sia tramite comunicazione sicura PG/HMI sia tramite la comunicazione PG/HMI utilizzata fino ad ora, abbreviata "Comunicazione PG/HMI legacy".

Procedimento

1. Navigare fino alla sezione "Protezione & Security > Meccanismi di collegamento".
2. Selezionare l'opzione desiderata.

Selezione o generazione del certificato

Se si seleziona il meccanismo di collegamento per la comunicazione PG/HMI, nello stesso contesto è possibile selezionare, o far generare da TIA Portal, un certificato di comunicazione PLC per la protezione del collegamento. Se è stata impostata una password e l'opzione per la protezione dei dati di configurazione PLC riservati è disattivata (oppure se non è impostata nessuna password), nell'area "Protezione & Security > Meccanismi di collegamento" è già preimpostato un certificato con le impostazioni necessarie e un nome predefinito valido.

Procedimento

Per fare generare un nuovo certificato da TIA Portal o selezionare un altro certificato già esistente:

1. Fare clic sui tre puntini del campo "Certificato di comunicazione PLC" per espanderlo.
2. Selezionare il certificato desiderato o fare clic sul pulsante "Aggiungi".
3. In questo caso si apre una finestra di dialogo con le possibilità di impostazione del certificato.
   Lo scopo di utilizzo è preimpostato su "TLS-Server", gli altri parametri (ad es. nome, algoritmo Hash, ...) possono essere modificati.

Valgono le regole generali per la gestione dei certificati; ciò significa che per generare un certificato CA occorre attivare l'opzione "Impostazioni globali per la Gestione certificato". Esiste anche la possibilità di generare un certificato PLC autofirmato.

Ulteriori informazioni

Informazioni di base sulla gestione dei certificati sono reperibili al cap. Gestione dei certificati in TIA Portal (Pagina 69).

5.6.5.3 Suggerimento per la comunicazione basata su certificati tra PG e CPU

La comunicazione PG/PC basata sui certificati (comunicazione sicura PG/PC) implica che il partner di comunicazione della CPU - il dispositivo di programmazione con TIA Portal installato - debba essere accreditato con il certificato del dispositivo della CPU per poter creare un collegamento.

Più semplicemente, per accreditare un dispositivo con il certificato di una CPU da TIA Portal esistono le seguenti possibilità:

- Il PG con TIA Portal dispone del certificato del dispositivo della CPU perché ad es. è stato generato o importato nel progetto. In questo caso la verifica del certificato avviene automaticamente e senza conferma.
- Il PG con TIA Portal non dispone del certificato del dispositivo della CPU; ad es. perché la CPU è stata rilevata tramite "Nodi accessibili" e non è nel progetto. In questo caso TIA Portal chiede all'utente di TIA Portal se il certificato è attendibile. Probabilmente è possibile solo con molte difficoltà in quanto la CPU non è ad es. nel campo visivo e di conseguenza l'autenticità non può essere verificata direttamente.
- Il PG con TIA Portal dispone del certificato CA (autorità di certificazione) e tutte le CPU accessibili nella rete da TIA Portal dispongono di certificati del dispositivo emessi da questo certificato CA.

  Vantaggio di questa soluzione: TIA Portal può verificare automaticamente certificati del dispositivo, anche se questi ultimi non sono accreditati con i partner di comunicazione in TIA Portal.

Di seguito è descritta dettagliatamente la soluzione con un certificato CA (autorità di certificazione).

Requisiti

Con l'autorità di certificazione di TIA Portal è possibile generare certificati del dispositivo per una CPU e utilizzare i certificati CA esistenti per firmare i certificati del dispositivo. Allo stesso modo è possibile importare e utilizzare un'altra autorità di certificazione in TIA Portal.

Il presupposto è l'attivazione delle impostazioni Security globali per la gestione certificato. Solo con questa impostazione è possibile generare certificati firmati da CA.

Vedere anche: Gestione dei certificati in TIA Portal (Pagina 69)

Esportazione del certificato CA per dispositii di programmazione

Per esportare il certificato CA corrispondente dopo la creazione e l'assegnazione di un certificato procedere nel modo seguente:

1. Aprire la gestione certificato nelle impostazioni di sicurezza globali nella navigazione del progetto.
2. Selezionare la tabella "Certificati CA" per il certificato da eportare.
3. Selezionare il certificato e aprire il menu di scelta rapida con un clic destro del mouse.
4. Fare clic su "Esporta".
5. Selezionare il formato di esportazione del certificato e la cartella di archiviazione.

Archiviazione del certificato CA in TIA Portal

Per rendere noto il certificato esportato ad un PG con TIA Portal e consentire di conseguenza la verifica automatica del certificato procedere nel modo seguente:

1. Copiare il certificato CA esportato nel passo precedente nella seguente direcotry:

   C:\ProgramData\Siemens\Automation\Certstore\Trusted

2. Avviare TIA Portal.

   Nella scheda "Informazioni" della finestra di ispezione per ciascun certificato CA compare un messaggio con l'informazione sull'avvenuta acquisizione del certificato CA nel CA Store di TIA Portal.

   Se l'acquisizione non riesce non vengono visualizzate cause dettagliate.

Acquisizione dei certificati dell'apparecchio nell'elenco di certificati revocati (CRL) in TIA Portal

È possibile aggiungere singoli certificati del dispositivo ad un elenco di certificati revocati (CRL), ad es. perché la rispettiva chiave non è più considerata sicura.

Se TIA Portal inizia un collegamento con una CPU il cui certificato del dispositivo si trova nell'elenco di certificati revocati, in TIA Portal compare una finestra di dialogo di attendibilità del certificato. In caso di rifiuto il collegamento non viene creato.

Per inserire il certificato dl dispositivo nell'elenco di certificati revocati procedere nel modo seguente:

1. Copiare il certificato del dispositivo nella seguente directory:

   C:\ProgramData\Siemens\Automation\Certstore\CRL

2. Avviare TIA Portal.

   Nella scheda "Informazioni" della finestra di ispezione per ciascun certificato compare un messaggio con l'informazione sull'avvenuta acquisizione del certificato nel CRL Store di TIA Portal.

   Se l'acquisizione non riesce non vengono visualizzate cause dettagliate.

5.6.5.4 Comportamento della CPU dal caricamento allo stato "pronto al funzionamento"

Per proteggere la comunicazione tra la CPU e un dispositivo di programmazione o un dispositivo HMI è necessario essere in possesso di un certificato. Il certificato per il funzionamento produttivo, tuttavia, le viene trasmesso solo con il caricamento del progetto nella CPU.

Per proteggere anche il caricamento iniziale, la CPU crea in un primo momento un certificato autofirmato. Il testo che segue spiega le varie fasi di creazione del collegamento.

Presupposti per la creazione del collegamento iniziale per il caricamento della CPU

- Nessuna password per i dati di configurazione PLC riservati nella CPU.

  Se la CPU è già stata caricata e ha già di una password per i dati di configurazione PLC riservati, è necessario che la password sia adatta al progetto da caricare.
- È presente un progetto con la configurazione della CPU (che include la password per i dati di configurazione PLC riservati) e il programma utente.
- La CPU deve trovarsi nello stato di funzionamento STOP.
- Il dispositivo di programmazione e la CPU sono collegati direttamente tra loro e si trovano in un ambiente protetto, ovvero è possibile identificare la CPU da caricare e controllare il collegamento tra la CPU e il dispositivo di programmazione.

Creazione del primo collegamento con la CPU - fase di distribuzione

Già la creazione del primo collegamento per il caricamento della CPU è protetto dal metodo TLS secondo i requisiti di una comunicazione PG/HMI sicura.

Per creare il collegamento la CPU utilizza tuttavia il certificato del costruttore (se disponibile) o un certificato autofirmato. In questa fase la CPU è utilizzabile limitatamente. In questa fase la CPU attende che venga messa a disposizione l'informazione chiave basata su password o più semplicemente: attende la password per i dati di configurazione PLC riservati. Da qui in poi questa fase viene definita fase di distribuzione. La CPU segnala di trovarsi in fase di distribuzione con un messaggio corrispondente nel buffer di diagnostica.

Quando viene caricato un progetto nella CPU, la CPU riceve i dati del progetto:

- Configurazione hardware comprensiva di certificati progettati per la comunicazione sicura (OPC UA, HTTPS, Secure OUC, comunicazione PG/HMI sicura)
- Programma utente

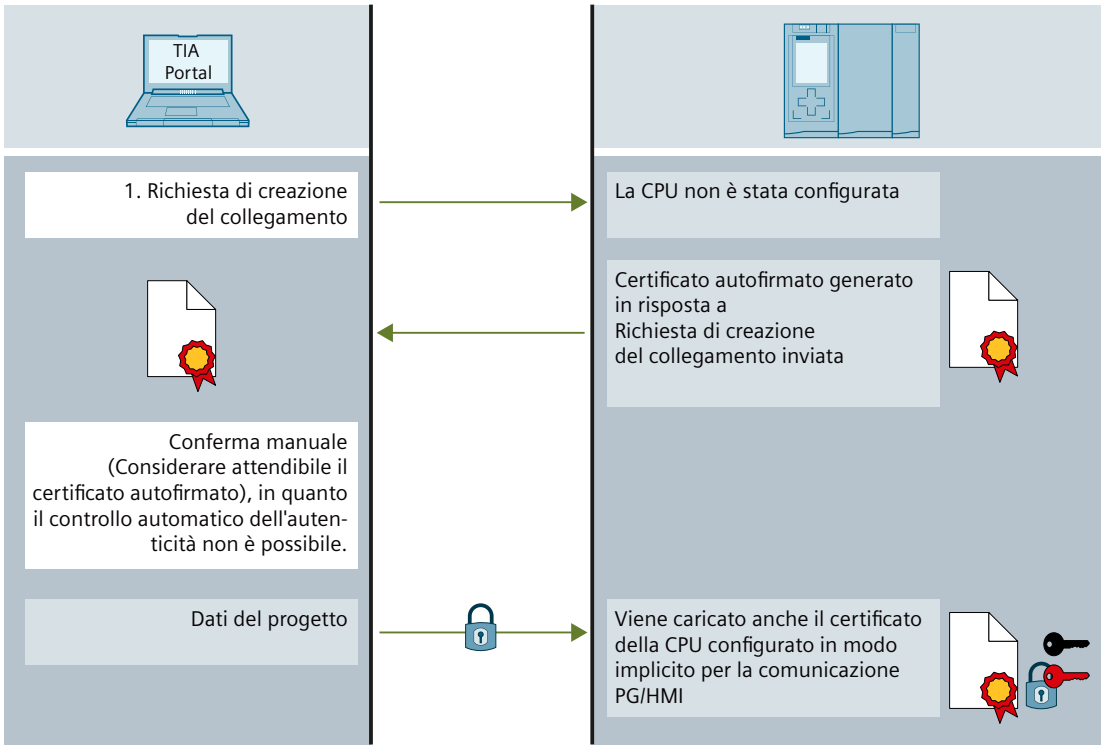


Figura 5-34 Creazione del collegamento con la fase di distribuzione

⚠ AVVERTENZA

Potenziali rischi per la sicurezza durante la messa in servizio

Durante la messa in funzione, la CPU fornisce un certificato del costruttore (se disponibile) o un certificato autofirmato che l'utente deve reputare attendibile per poter stabilire un collegamento. Attribuire attendibilità a questo certificato soltanto se il dispositivo di programmazione e la CPU si trovano in una rete protetta e sono direttamente collegati tra loro. In un ambiente non protetto, questi certificati possono essere manipolati e consentire a potenziali attaccanti l'accesso alla comunicazione tra il dispositivo di programmazione/HMI e la CPU (ad es. attraverso attacchi man-in-the-middle).

Conclusione della fase di distribuzione

TIA Portal non salva nel progetto la password per i dati di configurazione PLC riservati o l'informazione chiave generata dalla password.

Pertanto la password viene richiesta in modo interattivo e trasferita come informazione chiave nella CPU al primo caricamento o al caricamento di un nuovo progetto. Solo dopo questo passaggio la CPU è in grado di utilizzare i dati di configurazione PLC riservati. A questo punto la fase di distribuzione è conclusa e la CPU può entrare in funzione.

Se non si proteggono i dati di configurazione PLC riservati con una password, non è necessario inserire la password al primo caricamento. Questo non ha alcuna conseguenza sullo svolgimento della comunicazione PG/HMI, ma in questo caso si deve considerare che i dati di configurazione PLC riservati (ad es. chiave provata) sono meno protetti da accessi non autorizzati.

Avvio della comunicazione PG/HMI

Quando la CPU è stata caricata e ha ricevuto il certificato per la comunicazione PG/HMI sicura, il dispositivo di programmazione si ricollega, questa volta sulla base del certificato CPU caricato.

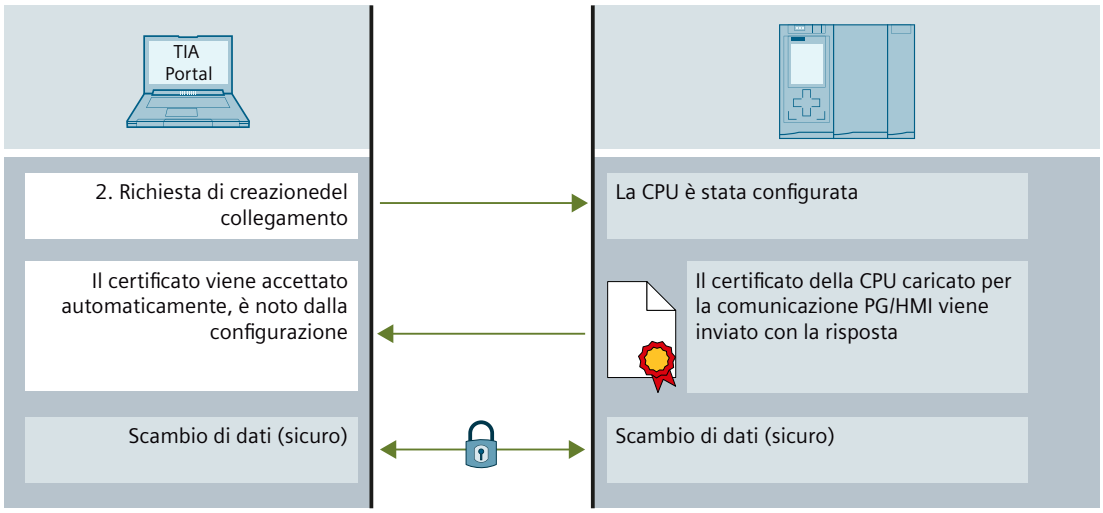


Figura 5-35 Avvio della comunicazione PG/HMI

5.6.5.5 Utilizzo della comunicazione HMI sicura

A partire dalla versione V17 di TIA Portal la CPU e il dispositivo HMI comunicano attraverso una comunicazione HMI sicura, purché entrambi i dispositivi soddisfino i requisiti necessari.

Per poter stabilire una comunicazione HMI sicura il dispositivo HMI deve poter verificare l'autenticità della CPU in base al certificato di comunicazione PLC che questa trasmette durante l'attivazione del collegamento e classificarlo come "attendibile". La comunicazione HMI sicura è possibile solo in questo caso.

Il presente capitolo descrive le operazioni che si devono eseguire per i diversi dispositivi HMI per contrassegnare manualmente come "attendibile" il certificato di comunicazione PLC.

Presupposti

- La CPU e il dispositivo HMI supportano la comunicazione HMI sicura.
- La CPU contiene un progetto aggiornato (> TIA Portal V17)

Progettazione della comunicazione HMI sicura

1. Progettare il dispositivo HMI con una vista segnalazioni.

   NOTA

   Senza la vista segnalazioni non è possibile rilevare gli errori in fase di attivazione del collegamento.

2. Progettare la CPU con le impostazioni Security necessarie. Selezionare un certificato di comunicazione PLC per proteggere il collegamento HMI o farlo generare da TIA Portal.
3. Progettare il collegamento HMI tra la CPU e il dispositivo HMI.
4. Caricare il progetto nella CPU e nel dispositivo HMI. Quando si trasferisce il progetto vengono trasferiti nella CPU e nel dispositivo HMI sia il certificato di comunicazione del PLC che l'eventuale certificato CA (autorità di certificazione).

   NOTA

   L'aggiornamento e il caricamento della progettazione della CPU richiedono il nuovo caricamento del dispositivo HMI.

   Se si modifica la progettazione CPU e questa modifica comporta una modifica del certificato di comunicazione PLC (ad es. in caso di modifica dell'indirizzo IP di un'interfaccia), è necessario caricare di nuovo anche il certificato di comunicazione PLC del dispositivo HMI collegato.

   In caso contrario non è possibile una comunicazione tra dispositivo HMI e CPU.

Impostazione dell'attendibilità del certificato di comunicazione del PLC

Quando si stabilisce il collegamento la CPU trasferisce nel dispositivo HMI il certificato di comunicazione PLC.

- Se il certificato di comunicazione PLC ha già lo stato "attendibile" nel dispositivo HMI, viene stabilita automaticamente una comunicazione HMI sicura tra la CPU e il dispositivo HMI.
- Se il certificato di comunicazione PLC non ha ancora lo stato "attendibile" nel dispositivo HMI, nella vista segnalazioni del dispositivo HMI compare con l'indicazione che la CPU non è attendibile e con un codice di errore.

  In questo caso si deve contrassegnare come "attendibile" il certificato di comunicazione del PLC nel dispositivo HMI.

A seconda del tipo di dispositivo HMI procedere come indicato di seguito.

Basic Panel 2nd Generation

1. Selezionare "Settings > Internet Settings > Certificate store" in Start Center.
2. Selezionare il certificato di comunicazione PLC nell'elenco "Available certificates in Device".
3. Premere il pulsante "Trust".
4. Riavviare il software di runtime dell'HMI.

Unified Comfort Panel

1. Aprire il Control Panel.
2. Selezionare "Security > Certificates".
3. Selezionare la voce "Other Certificates" nell'elenco a discesa "Certificate store".
4. Selezionare il certificato di comunicazione PLC nell'elenco "Other certificates".
5. Premere il pulsante "Trust".
6. Riavviare il software di runtime dell'HMI.

Comfort Panel, Mobile Panel 2nd Generation

1. Aprire il file manager dal desktop con l'icona di Windows CE "My Device".
2. Spostarsi nella directory "\flash\simatic\SystemRoot\OMS\Untrusted". Cercare il certificato di comunicazione PLC della CPU.
3. Copiare il certificato di comunicazione PLC della CPU nella directory "\flash\simatic\SystemRoot\OMS\Trusted".
4. Riavviare il software di runtime dell'HMI.

Se il certificato di comunicazione PLC ha già lo stato "attendibile" nel dispositivo HMI, è possibile stabilire la comunicazione HMI sicura. Per maggiori informazioni consultare le istruzioni operative del dispositivo HMI.

5.6.5.6 Utilizzo della comunicazione PG/PC legacy per TIA Portal

A partire dalla versione V17 di TIA Portal, TIA Portal e le CPU S7-1200/S7-1500 con versione di firmware V4.5/V2.9 o superiore comunicano automaticamente in modo "sicuro": i partner della comunicazione impostano automaticamente i loro meccanismi di collegamento sul massimo livello di sicurezza possibile.

Solo in condizioni particolari (vedere Informazioni sulla compatibilità (Pagina 123)) viene ripristinata la comunicazione PG/PC precedente, chiamata in breve "comunicazione PG/PC legacy".

Vi sono tuttavia casi specifici in cui la comunicazione sicura può non essere opportuna perché potrebbe ridurre la velocità di trasferimento nelle CPU che hanno prestazioni di comunicazione inferiori.

Presupposti

- Non devono essere attivi collegamenti online con le CPU.
- L'opzione "Consenti solo la comunicazione sicura PG/PC e HMI" (parametro della CPU nell'area "Meccanismi di collegamento") deve essere disattivata per le CPU che devono essere accessibili online.
- I partner di comunicazione si trovano in un ambiente protetto, ad es. durante la messa in servizio.

Impostazione della comunicazione PG/PC legacy

1. Selezionare il comando "Utilizza soltanto comunicazione PG/PC legacy" nel menu "Online".
2. Attivare la casella di opzione davanti al comando di menu.

Risultato: i collegamenti online vengono stabiliti come nelle versioni di TIA Portal < V17.

L'impostazione resta attivata durante la sessione. Quando si apre un progetto, l'opzione "Utilizza soltanto comunicazione PG/PC legacy" non è impostata.

Comportamento con l'opzione "Utilizza soltanto comunicazione PG/PC legacy" attivata

- La password per la protezione dei dati di configurazione PLC riservati non può essere né impostata online, né modificata, né cancellata per le CPU. Queste funzioni richiedono una disattivazione dell'opzione "Utilizza soltanto comunicazione PG/PC legacy"
- Le CPU impostate in modo da consentire solo la comunicazione PG/PC e HMI sicura non sono più accessibili online.

5.6.5.7 Informazioni sulla compatibilità

Il testo che segue fornisce informazioni sull'interazione tra diverse versioni di TIA Portal con le varie versioni firmware delle CPU e gli effetti sul tipo di collegamento PG/HMI.

Progetti creati con TIA Portal < V17

Se è stato creato un progetto ad es. con TIA Portal versione V16 per una CPU S7-1500 (ad es. versione V2.8), la configurazione può essere caricata con TIA Portal V17 anche in una CPU S7-1500 V2.9 (ad es. perché la CPU è stata sostituita), il progetto si comporterà come in una CPU S7-1500 V2.8.

Anche i progetti creati con TIA Portal < V17 e trasferiti su una Memory Card funzionano senza problemi in una CPU S7-1500 V2.9.

Se tuttavia si apre il progetto con TIA Portal ≥ V17, si aggiorna la versione firmware della CPU durante la sostituzione dei dispositivi e si salva una versione firmware della CPU ≥ V2.9, vale il concetto di protezione dei dati di configurazione PLC riservati (vedere Informazioni importanti sulla protezione dei dati di configurazione PLC riservati (Pagina 84)). Il progetto non può più essere modificato con le versioni precedenti di TIA Portal V17.

PG/HMI e CPU collegati in modo diverso

Come è stato spiegato nei capitoli precedenti, dalla V17 in poi il collegamento PG/HMI sicuro tra il dispositivo PG/HMI e la CPU (versione attuale) è caratterizzato dal sistema di comunicazione standardizzata TLS (Transport Layer Security).

È possibile collegare una CPU V2.9 con un dispositivo di programmazione attuale con TIA Portal V17 o superiore e inoltre, ad es., con un dispositivo HMI con una versione di runtime precedente: i dispositivi impostano automaticamente i meccanismi di collegamento adeguati. Per distinguere più facilmente i due meccanismi di collegamento, chiameremo la procedura precedente, basata su una variante della comunicazione S7, "procedura Legacy".

In breve ("PG" indica un dispositivo di programmazione con TIA Portal):

- PG/HMI e CPU hanno la versione V17 (o successiva): viene utilizzato il metodo TLS.
- Il PG/HMI proviene da una versione precedente (< V17): viene utilizzata la procedura Legacy, a condizione che l'opzione "Consenti solo la comunicazione sicura PG/PC e HMI" sia disattivata nelle proprietà della CPU.
- La CPU ha la versione V17 (o superiore), sono collegati vari PG/HMI sia con versione V17 (o superiore), sia con versioni precedenti: vengono utilizzate le procedure TLS+Legacy, a condizione che l'opzione "Consenti solo la comunicazione sicura PG/PC e HMI" sia disattivata nelle proprietà della CPU.

In caso di modifica dello stato della CPU

Il buffer di diagnostica segnala i cambi di stato dovuti ad eventi correlati alla comunicazione PG/HMI sicura.

Esempi:

- Il caricamento di una configurazione con password progettata è stato completato con successo e il buffer di diagnostica segnala che la CPU passa dalla fase di distribuzione alla modalità di sicurezza (procedura TLS).
- Un PG con TIA Portal V17 è stato collegato a una CPU V2.9. Viene impostata automaticamente la comunicazione PG/HMI sicura (procedura TLS), se "Utilizza soltanto comunicazione PG/PC legacy" è disattivata nel menu online.

Ulteriori informazioni

Le informazioni sulle caratteristiche specifiche dei dispositivi o dei firmware, quali ad es. la versione TLS utilizzata, sono riportate al cap. Caratteristiche di sicurezza che dipendono dal pannello operatore (Pagina 59).

5.7 SNMP

5.7.1 Attivazione e disattivazione di SNMP

Il protocollo di gestione della rete SNMP (Simple Network Management Protocol) viene utilizzato per la sorveglianza e la diagnostica della topologia di rete. SNMP utilizza il protocollo di trasporto UDP e riconosce due ruoli: l'SNMP Manager (client) e l'SNMP Agent (server).

- L'SNMP Manager controlla i nodi di rete.
- Gli Agent SNMP raccolgono nei singoli nodi di rete diverse informazioni specifiche della rete e le salvano in forma strutturata nel MIB (Management Information Base). Questi dati vengono utilizzati da diversi servizi e tool (con il ruolo di SNMP Manager) per effettuare una diagnostica dettagliata della rete.

SNMP viene utilizzato anche nei sistemi IO PROFINET per la gestione dell'infrastruttura di rete e degli IO Controller/IO Device.

NOTA

Se si disattiva SNMP per un dispositivo, alcune opzioni per la diagnostica della topologia di rete (ad es. il tool PRONETA) non sono più disponibili.

Esempio: Per il confronto della topologia online-offline, TIA Portal determina quali porte sono effettivamente collegate e utilizza SNMP per questa funzione.

Preimpostazioni in funzione della versione del firmware

Le CPU S7-1500 dispongono di un agente SNMP integrato. SNMP ha una preimpostazione diversa (SNMP attivato o disattivato) a seconda della versione del firmware.

Nelle CPU S7-1500 con versione firmware < V3.0, l'SNMP Agent è **attivato** per default e può essere disattivato solo tramite un set di dati nel programma utente.

A determinate condizioni può essere utile disattivare SNMP. Esempi:

- Le direttive di sicurezza della rete non consentono l'utilizzo di SNMP.
- Si utilizza una propria soluzione SNMP, ad es. con istruzioni di comunicazione proprie.

Nelle CPU S7-1500 con versioni firmware da V3.0, l'SNMP Agent è **disattivato** per default. La preimpostazione "disattivato" è attivata anche se non è stata caricata alcuna progettazione o se non è inserita alcuna Memory Card. Per la modifica delle impostazioni SNMP nelle CPU S7-1500 con versione firmware V3.0 o superiore, STEP 7 V18 offre le seguenti opzioni:

- Configurare SNMP nelle proprietà della CPU in TIA Portal.
- Attivare/disattivare SNMP nel programma utente trasferendo un set di dati ad un'interfaccia PROFINET.

NOTA

Sostituzione

Per motivi di compatibilità una CPU S7-1500 con versione firmware V3.0 o superiore sulla quale è caricato un progetto di una versione precedente (firmware della CPU < V3.0) si comporta come la CPU del progetto nella versione precedente:

SNMP è attivato e le stringhe Community "public" e "private" sono attive.

Configurazione di SNMP

A partire dalla versione firmware V3.0 della CPU e dalla versione V18 di TIA Portal è possibile modificare le seguenti impostazioni per SNMP nelle proprietà della CPU:

- Attiva SNMP (preimpostazione: disattivato)
- Stringa Community di sola lettura (preimpostazione: "public")
- Stringa Community di lettura-scrittura (preimpostazione: "private")

Le impostazioni sono riportate nell'area "Configurazione avanzata > SNMP".

A partire dalla versione firmware V3.1 della CPU e dalla versione V19 di TIA Portal è inoltre possibile attivare l'accesso con protezione dalla scrittura per SNMP quando questo è attivato.

Significato e proprietà delle stringhe Community

Una stringa Community SNMP, chiamata anche "nome Community", è simile a un ID o a una password che consente l'accesso alle informazioni/statistiche di un dispositivo, ad es. un router.
Per aumentare la sicurezza è quindi necessario modificare le stringhe Community preimpostate nelle proprietà della CPU. L'SNMP Manager si autentica presso l'SNMP Agent trasmettendo la stringa Community durante la richiesta.

Le stringhe Community vengono trasmesse come testo esteso.

- Le stringhe Community preimpostate per le operazioni SNMP di sola lettura (GET) sono "public".
- Le stringhe Community preimpostate per le operazioni SNMP di lettura-scrittura (SET) sono "private".

Numero di caratteri delle stringhe Community 1-240

Per le stringhe Community si possono utilizzare i seguenti caratteri:

- a-z
- A-Z
- 0-9
- -
- .

Attivazione/disattivazione dell'SNMP nel programma utente

Oltre alla configurazione nelle proprietà della CPU, è possibile attivare o disattivare SNMP anche nel programma utente. A tal fine, si deve trasmettere un set di dati 0xB071 ad un'interfaccia PROFINET della CPU. In questo set di dati è codificata l'informazione che stabilisce se SNMP debba essere attivato/disattivato. Indipendentemente dall'interfaccia PROFINET alla quale viene trasmesso il set di dati, esso è attivo in tutte le interfacce della CPU.

Una modalità di trasferimento del set di dati 0xB071: Definire la struttura del set di dati in un blocco dati e trasferire il blocco dati nell'OB del ciclo di programma (ad es. l'OB1) con l'istruzione "WRREC" (scrivi set di dati) ad un'interfaccia PROFINET della CPU.

Per eseguire quest'operazione procedere nel seguente modo:

1. Creare in STEP 7 un blocco dati che contenga la struttura del set di dati 0xB071.
   La seguente tabella mostra la struttura del set di dati 0xB071.

Byte	Elemento	Codifica	Spiegazione
0-1	BlockID	0xF003	Header La lunghezza dei set di dati viene contata a partire dal byte 4 “versione”.
2-3	BlockLength	8	
4	Versione	0x01	
5	Sottoversione	0x00	
6-7	Riservato	-	-
8-11	Controllo SNMP	0,1	0: Disattivazione di SNMP. 1: Attivazione di SNMP.

2. Trasferire nella CPU il set di dati 0xB071, ad es. all'interno dell'OB del ciclo di programma (OB1), utilizzando l'istruzione "WRREC" (scrivi set di dati). Come ID hardware utilizzare un'interfaccia PROFINET integrata della CPU.

Interazione tra la configurazione SNMP e il programma utente

- L'impostazione SNMP "attivato/disattivato" eseguita tramite programma utente non viene memorizzata in modo permanente nella CPU. Ad esempio, dopo ogni spegnimento / riaccensione, caricamento di una nuova configurazione hardware o ripristino alle impostazioni di fabbrica, è di nuovo attiva l'impostazione configurata.
- Quando si carica la configurazione dalla CPU ("Carica dispositivo come nuova stazione") viene acquisita l'impostazione SNMP configurata (attivato/disattivato). L'impostazione SNMP impostata tramite un set di dati nel programma applicativo viene invece ignorata.
- Le stringhe Community possono essere modificate solo nella configurazione e non possono essere impostate tramite set di dati nel programma utente.
  È tuttavia possibile attivare le stringhe Community progettate mediante un set di dati.
  Esempio:
  nella configurazione di una CPU S7-1500 è stato impostato che SNMP sia disattivato. Si modificano le stringhe Community preimpostate nelle proprietà della CPU e quindi si carica la configurazione nella CPU.
  Quindi si attiva SNMP trasmettendo il set di dati.
  Risultato: Le stringhe Community modificate sono attive.
- Nelle CPU S7-1500 con versione firmware < V3.0, con SNMP attivato, sono sempre attive le stringhe Community preimpostate ("public" e "private").

5.7.2 Attivazione / disattivazione di SNMP tramite trasferimento del set di dati: esempio di CPU 1516-3 PN/DP

Introduzione

Per la gestione dell'infrastruttura di rete, delle CPU e degli IO Device con SNMP, viene attivato SNMP per una CPU 1516-3 PN/DP. Nell'esempio che segue viene trasmesso a un'interfaccia PROFINET il set di dati 0xB071.

Presupposti

- CPU 1516-3 PN/DP dalla versione firmware V2.0
- STEP 7 dalla versione V14

Soluzione

Trasferire il set di dati 0xB071 ad un'interfaccia PROFINET della CPU. In questo modo viene attivato SNMP in tutte le interfacce PROFINET della CPU.

Il seguente esempio mostra come creare il set di dati in un blocco dati globale e trasferirlo nell'interfaccia PROFINET (Local~PROFINET_interface_1) all'interno di un OB del ciclo di programma (ad esempio l'OB1).

Per attivare SNMP per l'interfaccia PROFINET indirizzata della CPU 1516-3 PN/DP, procedere come segue:

1. Creare un blocco dati globale.
2. Assegnargli un nome, ad es. "ActivateSnmp".
3. Creare la struttura del set di dati 0xB071 in "Static" (nella figura: "snmpRecord") e altre variabili per la trasmissione del set di dati. La seguente figura rappresenta la struttura del blocco dati "ActivateSnmp".

ActivateSnmp

	Name	Data type	Start value	Re...	Ac...	Wr...	Vis...	Comment
1	Static							
2	snmpWrite	Bool	TRUE		✓	✓	✓	Start writing Data record 16#B071
3	snmpRecord	Struct			✓	✓	✓	Data record 16#B071
4	blockID	UInt	16#F003		✓	✓	✓	Data record ID
5	blockLength	UInt	8		✓	✓	✓	Length of block
6	version	USInt	1		✓	✓	✓	Byte 1 of blockversion
7	subversion	USInt	0		✓	✓	✓	Byte 2 of blockversion
8	reserved	UInt	0		✓	✓	✓	Reserverd for future usage
9	snmpControl	UDInt	1		✓	✓	✓	0: deactivate SNMP, 1: activate SNMP
10	snmpWrDone	Bool	false		✓	✓	✓	writing done
11	snmpWrError	Bool	false		✓	✓	✓	error while writing
12	snmpWrStatus	DWord	16#0		✓	✓	✓	status of writing

Figura 5-36 Struttura del blocco dati globale "ActivateSnmp"

4. Trasferire nella CPU 1516-3 PN/DP il set di dati 0xB071 all'interno di un OB del ciclo di programma (ad es. l'OB1) utilizzando l'istruzione "WRREC" (scrivi set di dati). Un esempio di programma è riportato nella prossima sezione.

Esempio di programmazione per il trasferimento dei set di dati nell'OB1

Nel seguente codice di programma il set di dati 0xB071 viene trasferito:

```
//-----------------------------------------
// Start writing SNMP settings
//-----------------------------------------
IF "ActivateSnmp".snmpWrite THEN
 IF (NOT "ActivateSnmp".snmpWriteDone)
 AND (NOT "ActivateSnmp".snmpWriteError) THEN
 "instWrrec_1"(REQ := "ActivateSnmp".snmpWrite,
 ID := "Local~PROFINET-Schnittstelle_1",
 INDEX := 16#B071,
 DONE => "ActivateSnmp".snmpWriteDone,
 ERROR => "ActivateSnmp".snmpWriteError,
 STATUS => "ActivateSnmp".snmpWriteStatus,
 RECORD := "ActivateSnmp".snmpRecord);
 END_IF;
 IF "ActivateSnmp".snmpWriteError THEN
```

```
 ; // add error handling
 END_IF;
 IF "ActivateSnmp".snmpWriteDone THEN
 "ActivateSnmp".snmpWrite := FALSE;
 END_IF;
END_IF;
```

Nuova disattivazione di SNMP

Con alcune piccole modifiche è possibile impiegare il codice di programma sopra utilizzato per disattivare SNMP. Assegnare alla variabile "ActivateSnmp".snmpRecord.snmpControl il valore "0" nel programma utente:

```
"ActivateSnmp".snmpRecord.snmpControl := 0;
```

Al successivo richiamo dell'istruzione "WRREC" SNMP viene nuovamente disattivato.

5.7.3 Attivazione/disattivazione di SNMP nelle CPU S7-1500R/H tramite trasferimento del set di dati

Nei sistemi S7-1500R/H, SNMP può essere attivato/disattivato nel programma utente come avviene nelle CPU standard. Tuttavia le interfacce PROFINET (X1, X2,...) di entrambe le CPU possiedono diversi ID hardware. L'interfaccia PROFINET X1 della CPU sinistra ad es. ha un ID hardware diverso dall'interfaccia PROFINET X1 della CPU destra. Il sistema S7-1500R/H non sincronizza automaticamente lo stato SNMP (attivato/disattivato) delle due CPU. Lo stato SNMP impostato con l'istruzione "WRREC" (attivato/disattivato) ha effetto solo sulla CPU la cui interfaccia PROFINET è indirizzata dall'istruzione "WRREC".

Esempio:

Il sistema S7-1500R/H ridondante si trova nello stato di sistema "RUN-redundant". Se ad es. con l'istruzione "WRREC" viene indirizzata un'interfaccia PROFINET della CPU sinistra, viene modificato lo stato SNMP della CPU sinistra. Lo stato SNMP della CPU sinistra resta invariato. Se la CPU sinistra si guasta o viene sostituita, lo stato SNMP rimane invariato dopo SYNCUP.

Rimedio:

Richiamare 2 volte l'istruzione "WRREC". Al primo richiamo di "WRREC", indirizzare l'ID hardware di un'interfaccia PROFINET della CPU sinistra. Eseguire un altro richiamo dell'istruzione "WRREC". Questa volta indirizzare l'ID hardware di un'interfaccia PROFINET della CPU destra.

ID hardware per l'interfaccia PROFINET X1:

- L'interfaccia PROFINET X1 della CPU sinistra ha l'ID hardware 65164 (nome preimpostato: Local1~PROFINET-interface_1).
- L'interfaccia PROFINET X1 della CPU destra ha l'ID hardware 65364 (nome preimpostato: Local2~PROFINET-interface_1).

L'indirizzamento tramite i relativi ID hardware dell'interfaccia PROFINET X1 viene utilizzato anche nel seguente esempio per il richiamo dell'istruzione "WRREC" per entrambe le CPU R/H.

NOTA

Trasferimento del set di dati alla CPU di backup

Trasferire il set di dati all'interfaccia PROFINET indirizzata della CPU di backup solo quando il sistema S7-1500R/H ha raggiunto lo stato di sistema "Run-REDUNDANT". In caso contrario, il set di dati non può essere trasmesso all'interfaccia PROFINET indirizzata della CPU di backup.

Quando il sistema S7-1500R/H raggiunge lo stato "Run-REDUNDANT" viene avviato l'OB di errore di ridondanza della CPU (OB72). Nella variabile "Fault_ID" dell'OB72 viene scritto il codice di errore "B#16#03" o "B#16#06".

Esempio: Richiami WRREC per entrambe le CPU R/H

Per attivare/disattivare SNMP per l'interfaccia PROFINET indirizzata di entrambe le CPU mediante il trasferimento di set di dati procedere come segue:

1. Creare un blocco dati globale.
2. Assegnargli un nome, ad es. "ActivateSnmp".
3. Creare la struttura del set di dati 0xB071 in "Static" (nella figura: "snmpRecord") e altre variabili per la trasmissione del set di dati. La seguente figura mostra la struttura del blocco dati "ActivateSnmp".

ActivateSnmp

	Name	Data type	Start value	Re...	Ac...	Wr..	Vis...	Comment
1	Static							
2	snmpWrite	Bool	TRUE		✓	✓	✓	Start writing Data record 16#B071
3	snmpRecord	Struct			✓	✓	✓	Data record 16#B071
4	blockID	UInt	16#F003		✓	✓	✓	Data record ID
5	blockLength	UInt	8		✓	✓	✓	Length of block
6	version	USInt	1		✓	✓	✓	Byte 1 of blockversion
7	subversion	USInt	0		✓	✓	✓	Byte 2 of blockversion
8	reserved	UInt	0		✓	✓	✓	Reserverd for future usage
9	snmpControl	UDInt	1		✓	✓	✓	0: deactivate SNMP, 1: activate SNMP
10	plcLeft	Struct			✓	✓	✓	Writing status of left plc
11	snmpWrDone	Bool	false		✓	✓	✓	writing done
12	snmpWrError	Bool	false		✓	✓	✓	error while writing
13	snmpWrStatus	DWord	16#0		✓	✓	✓	status of writing
14	plcRight	Struct			✓	✓	✓	Writing status of right plc
15	snmpWrDone	Bool	false		✓	✓	✓	writing done
16	snmpWrError	Bool	false		✓	✓	✓	error while writing
17	snmpWrStatus	DWord	16#0		✓	✓	✓	status of writing

Figura 5-37 Struttura del blocco dati globale "ActivateSnmp"

4. Aggiungere al programma utente il blocco organizzativo "CPU redundancy error" (OB72). Un esempio di programma per l'OB72 è riportato nella prossima sezione.

5. Aprire l'OB del ciclo di programma (OB1).
6. Nell'interfaccia OB1, eseguire due istruzioni "WRREC" per trasferire il set di dati nell'interfaccia PROFINET indirizzata di entrambe le CPU. Un esempio di programma per l'OB1 è riportato nella prossima sezione.

   Risultato: Il set di dati 0xB071 è stato trasferito all'interfaccia PROFINET indirizzata di entrambe le CPU.

Esempio di programmazione dei blocchi organizzativi OB72 e OB1

Aprire l'OB72 aggiunto. Con il seguente codice programma si può determinare se il sistema R/H ha assunto lo stato "Run-REDUNDANT" e impostare il comando di avvio per le istruzioni "WRREC":

```
//---------------------------------------------
// Check redundancy state and set "snmpWrite"
//---------------------------------------------
IF #Fault_ID = B#16#03 OR #Fault_ID = B#16#06 THEN
 "ActivateSnmp".snmpWrite := TRUE;
END_IF;
```

Aprire l'OB del ciclo di programma (OB1). Con il seguente codice di programma si eseguono 2 istruzioni "WRREC" per trasferire il set di dati nell'interfaccia PROFINET indirizzata di entrambe le CPU tramite:

```
//----------------------------------------
// Start writing SNMP settings
//----------------------------------------
IF "ActivateSnmp".snmpWrite THEN
 IF (NOT "ActivateSnmp".plcLeft.snmpWrDone)
 AND (NOT "ActivateSnmp".plcLeft.snmpWrError) THEN
 // write SNMP settings for the left PLC
 "instWrrec_1"(REQ := "ActivateSnmp".snmpWrite,
 ID := "Local1~PROFINET_interface_1",
 INDEX := 16#B071,
 DONE => "ActivateSnmp".plcLeft.snmpWrDone,
 ERROR => "ActivateSnmp".plcLeft.snmpWrError,
 STATUS => "ActivateSnmp".plcLeft.snmpWrStatus,
 RECORD := "ActivateSnmp".snmpRecord);
 END_IF;
 IF "ActivateSnmp".plcLeft.snmpWrError THEN
 ; // add error handling for left plc
 END_IF;
 IF (NOT "ActivateSnmp".plcRight.snmpWrDone)
 AND (NOT "ActivateSnmp".plcRight.snmpWrError) THEN
 // write SNMP settings for the right PLC
 "instWrrec_2"(REQ := "ActivateSnmp".snmpWrite,
 ID := "Local2~PROFINET_interface_1",
 INDEX := 16#B071,
 DONE => "ActivateSnmp".plcRight.snmpWrDone,
 ERROR => "ActivateSnmp".plcRight.snmpWrError,
 STATUS =>
 "ActivateSnmp".plcRight.snmpWrStatus,
 RECORD := "ActivateSnmp".snmpRecord);
 END_IF;
 IF "ActivateSnmp".plcRight.snmpWrError THEN
 ; // add error handling for right plc
```

```
 END_IF;
 IF "ActivateSnmp".plcLeft.snmpWrDone
 AND "ActivateSnmp".plcRight.snmpWrDone THEN
 "ActivateSnmp".snmpWrite := FALSE;
 END_IF;
END_IF;
```

Nuova disattivazione di SNMP

Con alcune piccole modifiche è possibile impiegare il codice di programma sopra utilizzato per disattivare SNMP. Assegnare alla variabile "ActivateSnmp".snmpRecord.snmpControl il valore "0" nel programma utente:

```
"ActivateSnmp".snmpRecord.snmpControl := 0;
```

Al successivo richiamo delle Istruzioni "WRREC", SNMP viene nuovamente disattivato.

Comunicazione PG

6

Proprietà

Attraverso la comunicazione PG la CPU o un altro modulo che supporta funzioni di comunicazione scambia dati con un'engineering station (ad es. PG, PC). Lo scambio di dati è possibile attraverso le sottoreti PROFIBUS e PROFINET. Viene supportato anche il routing tra sottoreti S7.

La comunicazione PG mette a disposizione funzioni necessarie per caricare programmi e dati di configurazione, per eseguire test e valutare le informazioni di diagnostica. Queste funzioni sono integrate nel sistema operativo del modulo che supporta funzioni di comunicazione.

NOTA

Da TIA Portal versione V17 viene supportato il protocollo TLS (Transport Layer Security) per la comunicazione PG/HMI per garantire lo scambio dati tra PG/PC e CPU tramite meccanismi Security standardizzati.

Per ulteriori informazioni consultare i seguenti capitoli:

- Presupposti per la comunicazione sicura (Pagina 81)
- Comunicazione PG/HMI sicura (Pagina 112)

Presupposti

- Il PG/PC è collegato fisicamente al modulo che supporta le funzioni di comunicazione.
- Per l'accesso tramite routing S7 al modulo che supporta le funzioni di comunicazione, caricare la configurazione hardware nelle stazioni interessate (router S7 e punto finale).

Procedura per il collegamento online

Per la comunicazione PG è necessario creare un collegamento online con la CPU:

1. Nella navigazione del progetto in STEP 7 selezionare la CPU.
2. Selezionare il comando di menu "Online > Collega online".
3. Nella finestra di dialogo "Collega online" definire le seguenti impostazioni per il collegamento online:
   - Nella casella di riepilogo "Tipo di interfaccia PG/PC" selezionare il tipo di interfaccia (ad es. PN/IE)
   - Nella casella di riepilogo "Interfaccia PG/PC" selezionare l'interfaccia PG/PC (ad es. scheda Ind. Ethernet) con la quale creare il collegamento online.

– Nella casella di riepilogo "Collegamento con l'interfaccia/la sottorete" selezionare l'interfaccia o la sottorete S7 con la quale il dispositivo di programmazione è collegato fisicamente.
– Se il modulo che supporta le funzioni di comunicazione è accessibile attraverso un router S7 (gateway), selezionare nella casella di riepilogo "1° gateway" il router S7 che collega tra loro le sottoreti interessate.

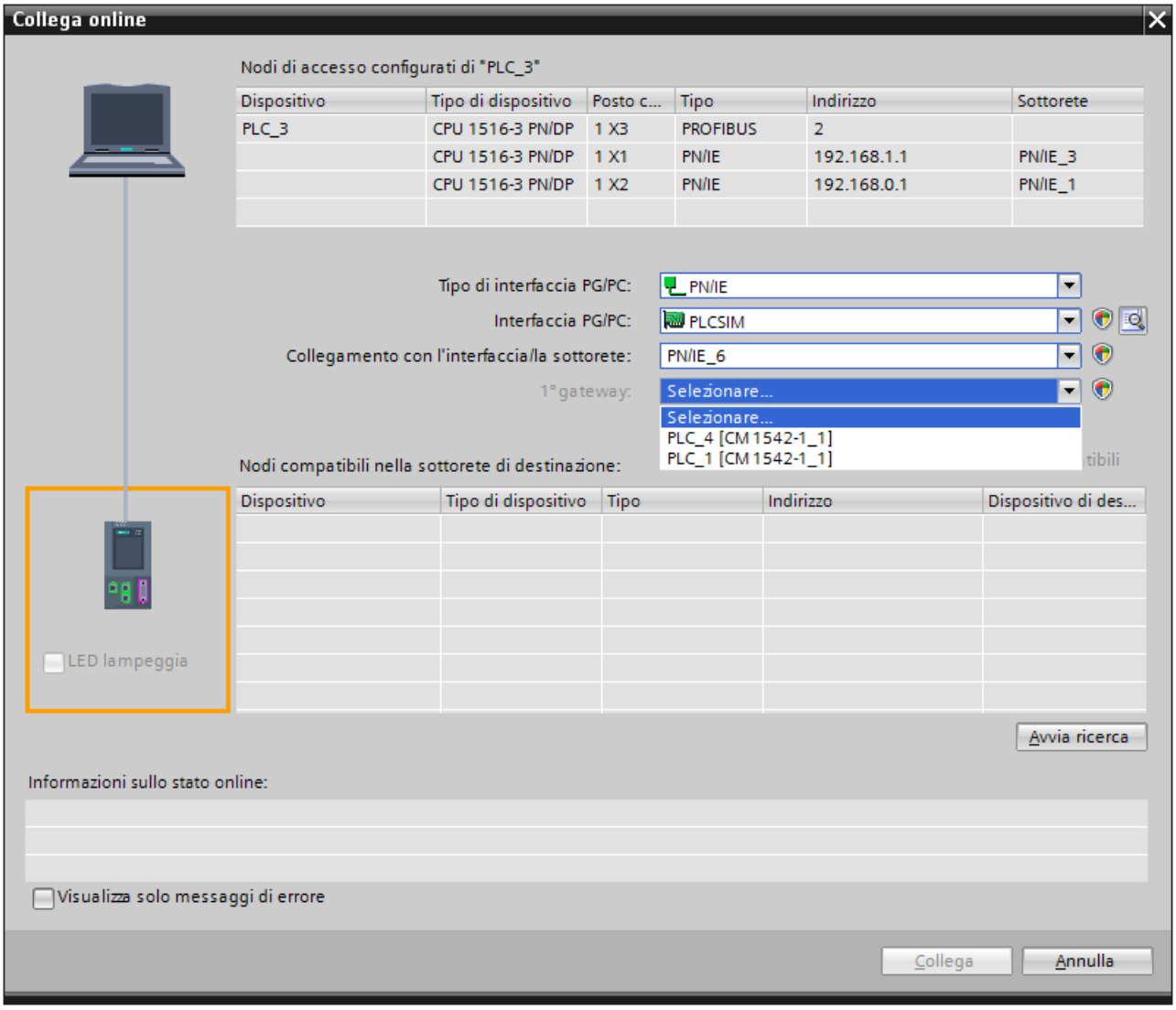


Figura 6-1 Configurazione della comunicazione PG

4. Fare clic su "Avvia ricerca".
   Dopo qualche istante nella tabella "Nodi compatibili nella sottorete di destinazione" vengono visualizzati tutti i dispositivi accessibili tramite comunicazione PG.
5. Nella tabella "Nodi compatibili nella sottorete di destinazione" selezionare la relativa CPU e confermare la selezione con "Collega".

Ulteriori informazioni

Maggiori informazioni sul comando "Collega online" sono disponibili nella Guida in linea a STEP 7.

Comunicazione HMI 7

Proprietà

Tramite la comunicazione HMI, uno o più dispositivi HMI (ad es. HMI Basic/Comfort/Mobile Panel) scambiano con una CPU i dati per il servizio e la supervisione attraverso l'interfaccia PROFINET o PROFIBUS DP. Lo scambio di dati avviene attraverso collegamenti HMI.

Per configurare più collegamenti HMI con una CPU, utilizzare ad es.:

- le interfacce PROFINET e PROFIBUS DP della CPU
- CP e CM con le rispettive interfacce

NOTA

Da TIA Portal versione V17 viene supportato il protocollo TLS (Transport Layer Security) per la comunicazione PG/HMI per garantire lo scambio dati tra PG/PC e CPU tramite meccanismi Security standardizzati.

Per ulteriori informazioni consultare i seguenti capitoli:

- Presupposti per la comunicazione sicura (Pagina 81)
- Comunicazione PG/HMI sicura (Pagina 112)

Procedura di configurazione della comunicazione HMI

Non appena si trascina una variabile in una pagina HMI o nella tabella delle variabili HMI, ad es. da un blocco dati globale, STEP 7 configura automaticamente un collegamento HMI. In alternativa è possibile anche configurare il collegamento HMI autonomamente.

Per configurare un collegamento HMI procedere nel seguente modo.

1. Nella vista di rete dell'editor hardware e di rete di STEP 7 progettare il dispositivo HMI in una configurazione esistente con la CPU.
2. Selezionare il pulsante "Collegamenti" e nell'elenco a discesa la voce "Collegamento HMI".
3. Con la funzione drag&drop tracciare una linea tra i punti finali del collegamento (dispositivo HMI e CPU). I punti finali sono evidenziati con un colore. Se non ancora presente, la sottorete S7 verrà creata automaticamente.

4. Nella scheda "Collegamenti" selezionare la riga del collegamento HMI.

   Nell'area "Generale", nella scheda "Proprietà" sono visualizzate le proprietà del collegamento HMI che si possono in parte modificare.

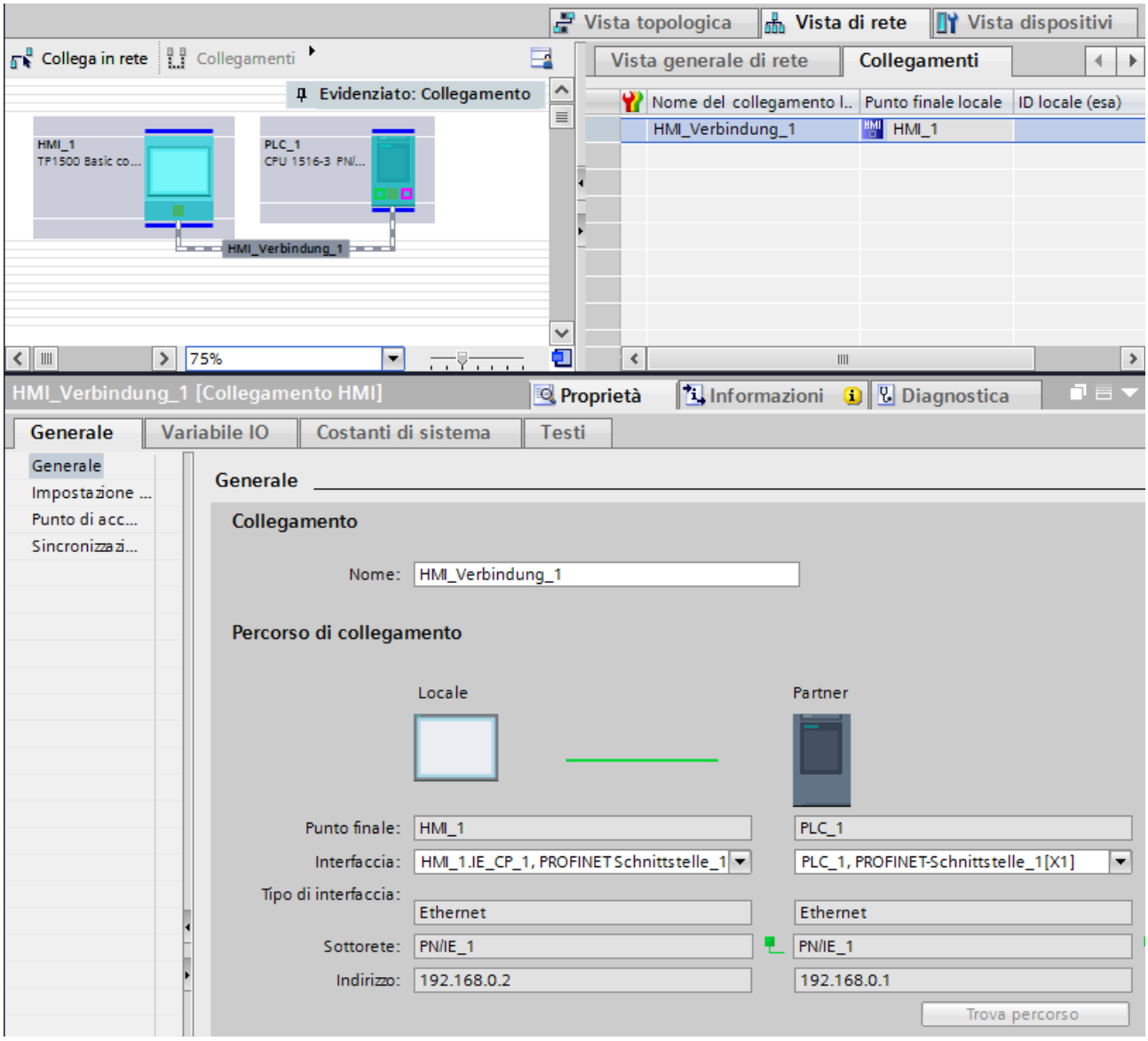


Figura 7-1 Configurazione della comunicazione HMI

5. Caricare la configurazione hardware nella CPU.
6. Caricare la configurazione hardware nel dispositivo HMI.

Ulteriori informazioni

Per informazioni sul routing S7 per i collegamenti HMI, consultare il capitolo Routing S7 (Pagina 419).

Maggiori informazioni sulla configurazione dei collegamenti HMI sono disponibili nella Guida in linea a STEP 7.

Open User Communication 8

8.1 Open User Communication in sintesi

Caratteristiche della Open User Communication

Attraverso la Open User Communication, definita anche "comunicazione aperta", la CPU scambia dati con un altro dispositivo capace di comunicare. La Open User Communication presenta le seguenti caratteristiche.

- Standard aperto (possono essere partner di comunicazione due CPU SIMATIC oppure una CPU SIMATIC e un dispositivo di terzi adeguato).
- Comunicazione tramite diversi protocolli (in STEP 7 denominati "Tipi di collegamento")
- Elevata flessibilità in considerazione delle struttura di dati da trasferire; consente lo scambio aperto dei dati con qualsiasi nodo di comunicazione purché supporti i tipi di collegamento disponibili
- Comunicazione sicura: Per la protezione del sistema di automazione, è possibile optare per lo scambio dati sicuro tramite Open User Communication. Nella modalità Open User Communication i dati trasferiti sono dotati di firma digitale e crittografati, vedere anche Secure Open User Communication (Pagina 94).
- La Open User Communication è possibile in diversi sistemi di automazione; consultare i dati tecnici nei rispettivi manuali del prodotto.
  Esempi:
  - Interfaccia PROFINET/Ind. Interfacce Ethernet delle CPU (S7-1500, CPU ET 200SP, S7-1500 Software Controller, CPU 1513/1516pro-2 PN)
  - Interfaccia PROFINET/Ind. Interfacce Ethernet dei moduli di comunicazione (ad es. CP 1543-1, CM 1542-1, CP 1543SP-1)

Per informazioni sulla Secure Open User Communication vedere il capitolo Comunicazione sicura (Pagina 56).

Informazioni sull’S7-1500R/H

Informazioni su Open User Communication con il sistema ridondante S7-1500R/H sono disponibili al capitolo Comunicazione con il sistema ridondante S7-1500R/H (Pagina 454).

8.2 Protocolli per Open User Communication

Protocolli per Open User Communication

Per la comunicazione aperta sono disponibili i seguenti protocolli:

Tabella 8-1 Protocolli di trasporto per la comunicazione aperta

Protocollo di trasporto	Tramite interfaccia
TCP secondo RFC 793	PROFINET/Industrial Ethernet
ISO-on-TCP secondo RFC 1006 (Class 4)	PROFINET/Industrial Ethernet
ISO secondo ISO/IEC 8073	Industrial Ethernet (solo CP 1543-1)
UDP secondo RFC 768	PROFINET/Industrial Ethernet
FDL	PROFIBUS

Tabella 8-2 Protocolli dell'applicazione per la comunicazione aperta

Protocollo dell'applicazione	Protocollo di trasporto impiegato
Modbus TCP	**TCP** secondo RFC 793
E-mail	**TCP** secondo RFC 793
FTP	**TCP** secondo RFC 793

TCP, ISO-on-TCP, ISO, UDP

Questi protocolli (tranne UDP) stabiliscono un collegamento di trasporto al partner di comunicazione prima della trasmissione dei dati. I protocolli orientati alla connessione vengono impiegati quando la sicurezza dei dati durante la trasmissione è particolarmente importante.

Con UDP è possibile:

- Unicast ad uno o Broadcast a tutti i nodi in PROFINET tramite l'interfaccia PROFINET della CPU o l'interfaccia Industrial Ethernet del CP 1543-1
- Multicast a tutti i destinatari di un gruppo multicast attraverso l'interfaccia PROFINET della CPU o attraverso l'interfaccia PROFINET/Industrial Ethernet del CP 1543-1

Numero massimo di gruppi multicast supportati e lunghezze massime dei dati utili: Vedere i dati tecnici riportati nei manuali dei rispettivi dispositivi.

Protocollo per la comunicazione via PROFIBUS: FDL

La trasmissione dei dati tramite un collegamento FDL (Fieldbus Data Link) è indicata per la trasmissione di blocchi di dati correlati a un partner di comunicazione in PROFIBUS che supporta l'invio e la ricezione conformi al servizio FDL SDA (Send Data with Acknowledge) secondo EN 50170, vol. 2.. Entrambi i partner hanno gli stessi diritti, vale a dire che ogni partner può avviare la procedura di invio e ricezione in funzione di un evento.

In conformità al servizio FDL SDN (Send Data with No Acknowledge) secondo EN 50170, vol. 2., con FDL sono possibili:

- Broadcast a tutti i nodi PROFIBUS attraverso l'interfaccia PROFIBUS del CM 1542-5
- Multicast a tutti i destinatari di un gruppo multicast attraverso l'interfaccia PROFIBUS del CM 1542-5

Modbus TCP

Il protocollo Modbus è un protocollo di comunicazione con topologia lineare sulla base di un'architettura master/slave. Nella modalità di trasmissione Modbus TCP (Transmission Control Protocol), i dati vengono trasmessi come pacchetti TCP/IP.

La comunicazione viene comandata esclusivamente tramite le relative istruzioni nel programma utente.

E-mail e FTP

Tramite e-mail è possibile ad es. inviare i contenuti dei blocchi dati (ad es. i dati di processo) come allegato.

Il collegamento FTP (FTP = funzioni di trasferimento file) trova impiego per il trasferimento di file da e verso i dispositivi S7.

Nel client la comunicazione viene comandata per mezzo delle istruzioni corrispondenti nel programma utente.

Esempio applicativo: MQTT Publisher per la CPU SIMATIC S7-1500

Il "Message Queue Telemetry Transport" (MQTT) è un protocollo semplice a livello TCP/IP. È adatto per scambiare messaggi tra dispositivi con funzionalità ridotta e per trasmettere dati su reti non affidabili.

L'esempio applicativo descrive un blocco funzionale utilizzabile per implementare il protocollo MQTT nella CPU SIMATIC S7-1500.

Gli esempi applicativi sono disponibili in Internet (https://support.industry.siemens.com/cs/ww/it/view/109772284).

Vedere anche

SYSLOG (https://support.industry.siemens.com/cs/ww/it/view/51929235)

8.3 Istruzioni per Open User Communication

Introduzione

Open User Communication si configura tramite il relativo collegamento (ad es. collegamento TCP) nel modo seguente:

- eseguendo la programmazione nei programmi utente dei partner di comunicazione oppure
- eseguendo la progettazione del collegamento in STEP 7 nell'editor hardware e di rete

A prescindere dalla configurazione del collegamento attraverso programmazione o progettazione, nei programmi utente dei due partner di comunicazione sono sempre necessarie le istruzioni per l'invio e la ricezione dei dati.

Configurazione del collegamento tramite il programma utente

Nella configurazione programmata il collegamento si stabilisce o si interrompe con le istruzioni nel programma utente.

In determinate aree applicative è utile configurare i collegamenti di comunicazione non in modo statico attraverso la progettazione nella configurazione hardware, bensì tramite il programma utente. I collegamenti possono essere configurati comandati da un programma tramite un'applicazione specifica e quindi nel momento in cui sono necessari. La configurazione programmata consente inoltre di abilitare le risorse di collegamento al termine della trasmissione dei dati.

Per ogni collegamento di comunicazione è necessaria una struttura di dati contenente i parametri per la creazione del collegamento (ad es. il tipo di dati di sistema "TCON_IP_v4" per TCP).

I tipi di dati di sistema (SDT) vengono forniti dal sistema e hanno una struttura predefinita che non può essere modificata.

I vari protocolli hanno rispettivamente strutture di dati proprie (vedere la tabella seguente). I parametri vengono salvati in un blocco dati ("DB di descrizione del collegamento") ad es. del tipo di dati di sistema TCON_IP_v4.

Esistono due possibilità di assegnare al DB una struttura di dati:

- Suggerimento: Far creare automaticamente il blocco dati durante la parametrizzazione del collegamento nelle proprietà nell'editor di programma con l'ausilio della parametrizzazione del collegamento con le istruzioni TSEND_C, TRCV_C e TCON
- Creare e parametrizzare manualmente il blocco dati e scriverlo direttamente nell'istruzione Necessario per:
  - Secure OUC
  - Collegamento tramite DNS
  - E-mail
  - FTP

Nel "DB di descrizione del collegamento" si possono modificare i parametri di collegamento.

La programmazione dell'istruzione TCON per configurare un collegamento tra due CPU S7-1500 per Open User Communication è descritta in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/58875807).

Protocolli, tipi di dati di sistema e istruzioni utilizzabili per la configurazione programmata

La seguente tabella elenca i protocolli della Open User Communication e i tipi di dati di sistema e le istruzioni con cui sono utilizzabili.

Tabella 8-3 Istruzioni per la configurazione programmata del collegamento

Protocollo	Tipo di dati di sistema	Istruzioni
TCP	• TCON_QDN • TCON_IP_v4	Creazione del collegamento e invio/ricezione dei dati tramite: • TSEND_C/TRCV_C oppure • TCON, TSEND/TRCV oppure • TCON, TUSEND/TURCV (interruzione del collegamento possibile con TDISCON)
ISO-on-TCP	• TCON_IP_RFC	
ISO secondo ISO/IEC 8073 (Class 4)	• TCON_ISOnative[1] • TCON_Configured	
UDP	• TCON_IP_v4 • TADDR_Param • TADDR_SEND_QDN • TADDR_RCV_IP	Creazione del collegamento e invio/ricezione dei dati tramite: • TSEND_C/TRCV_C • TUSEND/TURCV/TRCV (interruzione del collegamento possibile con TDISCON)
FDL[1]	• TCON_FDL	Creazione del collegamento e invio/ricezione dei dati tramite: • TSEND_C/TRCV_C oppure • TCON, TSEND/TRCV oppure • TCON, TUSEND/TURCV (interruzione del collegamento possibile con TDISCON)

[1] questo protocollo è utilizzabile solo con il CM 1542-5

[2] questo protocollo è utilizzabile solo con il CP 1543-1

[3] tipo di dati definito dall'utente

Protocollo	Tipo di dati di sistema	Istruzioni
Modbus TCP	• TCON_IP_v4 • TCON_QDN • TCON_Configured	• MB_CLIENT • MB_SERVER
E-mail	• TMAIL_v4 • TMAIL_v6 • TMAIL_FQDN	• TMAIL_C
FTP[2]	• FTP_CONNECT_IPV4[3] • FTP_CONNECT_IPV6[3] • FTP_CONNECT_NAME[3]	• FTP_CMD

[1] questo protocollo è utilizzabile solo con il CM 1542-5

[2] questo protocollo è utilizzabile solo con il CP 1543-1

[3] tipo di dati definito dall'utente

La seguente tabella elenca i diversi collegamenti della Open User Communication e i tipi di dati di sistema e le istruzioni con cui sono utilizzabili.

Collegamento Secure OUC	Tipo di dati di sistema	Istruzioni
Collegamento TCP protetto da una CPU S7-1500 come client TLS a un PLC di terzi (server TLS) Collegamento TCP protetto da una CPU S7-1500 come server TLS a un PLC di terzi (client TLS)	• TCON_QDN_SEC	• TSEND_C/TRCV_C • TCON, TSEND/TRCV
Collegamento TCP protetto tra due stazioni S7-1500	• TCON_IP_V4_SEC[1]	
Collegamento protetto con un server e-mail[2]	• TMAIL_V4_SEC • TMAIL_QDN_SEC	• TMAIL_C (dalla versione V5.0)
Collegamento Modbus TCP	• TCON_IP_V4_SEC[1] • TCON_QDN_SEC	• MB_CLIENT • MB_SERVER

[1] È possibile anche con il CP 1543-1

[2] Il collegamento protetto con un server e-mail è possibile anche con il CP1543-1 e TMAIL_C (V4.0)

Configurazione del collegamento tramite progettazione

Con la configurazione tramite progettazione del collegamento vengono definiti i parametri dell'indirizzo del collegamento nell'editor hardware e di rete di STEP 7.

Per inviare e ricevere i dati utilizzare le stesse istruzioni della configurazione programmata dei collegamenti:

Tabella 8-4 Istruzioni per l'invio/la ricezione nei collegamenti progettati

Protocollo	Invio/ricezione nei collegamenti progettati
Istruzioni utilizzabili:	
TCP	Invio/Ricezione dei dati tramite: • TSEND_C/TRCV_C oppure • TSEND/TRCV oppure • TUSEND/TURCV
ISO-on-TCP	
ISO secondo ISO/IEC 8073 (Class 4)	

Protocollo	Invio/ricezione nei collegamenti progettati
UDP	Invio/Ricezione dei dati tramite: • TSEND_C/TRCV_C oppure • TUSEND/TURCV
FDL	Invio/Ricezione dei dati tramite: • TSEND_C/TRCV_C oppure • TSEND/TRCV oppure • TUSEND/TURCV
Modbus TCP	Non supportato
E-mail	Non supportato
FTP	Non supportato

Ulteriori istruzioni per la comunicazione aperta

Le seguenti istruzioni possono essere impiegate sia per i collegamenti configurati nel programma utente sia per quelli progettati:

- T_RESET: interruzione e creazione del collegamento
- T_DIAG: verifica del collegamento

Esempi di base di Open User Communication

Il Siemens Online Support mette a disposizione blocchi funzionali (FB) che facilitano la gestione delle istruzioni della Open User Communication. I blocchi funzionali e i relativi esempi sono disponibili in Internet (https://support.industry.siemens.com/cs/ww/it/view/109747710).

Ulteriori informazioni

Nella Guida in linea a STEP 7 sono descritti:

- tipi di dati utente e di sistema
- istruzioni per la comunicazione aperta
- parametri del collegamento

Per maggiori informazioni sull'occupazione e l'abilitazione delle risorse di collegamento consultare il capitolo Occupazione delle risorse di collegamento (Pagina 440).

Per informazioni sulla Secure Open User Communication vedere il capitolo Secure Open User Communication (Pagina 94).

8.4 Open User Communication con indirizzamento tramite nome di dominio

Le CPU S7-1500, le CPU ET 200SP e le CPU 1513/1516pro-2 PN dalla versione firmware V2.0 supportano la Open User Communication con indirizzamento attraverso un Domain Name System (DNS). Nella CPU è integrato un client DNS. Nel caso della comunicazione tramite DNS, per indirizzare i partner di comunicazione si utilizzano i nomi dei domini come alias degli indirizzi IP. L'indirizzamento dei partner di comunicazione tramite nome di dominio è possibile per la comunicazione aperta attraverso TCP e UDP.

Il requisito necessario per la comunicazione tramite DNS è che sulla rete sia presente almeno un server DNS.

S7-1500 Software Controller supporta la comunicazione attraverso DNS per tutte le interfacce assegnate al software controller.

Configurazione della comunicazione tramite DNS

Per consentire a una CPU di creare un collegamento a un partner della comunicazione attraverso il suo nome di dominio, il client DNS della CPU deve conoscere l'indirizzo IPv4 di almeno un server DNS. La CPU supporta fino a 4 diversi server DNS.

Per configurare la comunicazione tramite nome di dominio per una CPU S7-1500, procedere come indicato nel seguito:

1. Selezionare la CPU nella vista di rete di STEP 7.
2. Nella finestra di ispezione selezionare "Proprietà" > "Generale" > "Configurazione avanzata" > "Configurazione DNS".
3. Immettere nella tabella "Elenco server", nella colonna "Indirizzi del server DNS", l'indirizzo IPv4 di un server DNS.
   È possibile immettere fino a 4 indirizzi IPv4 di server DNS.

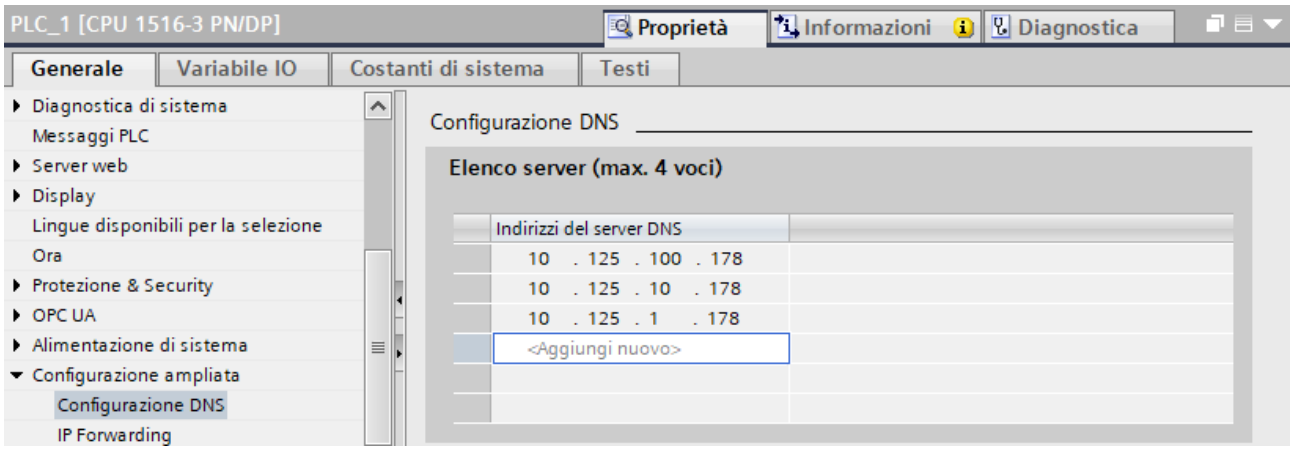


Figura 8-1 Esempio di inserimento degli indirizzi dei server DNS su CPU 1516-3 PN/DP

Configurazione di un collegamento TCP tramite nome del dominio del partner della comunicazione

Per la comunicazione TCP tramite nome del dominio è necessario creare e parametrizzare individualmente un blocco dati con il tipo di dati di sistema TCON_QDN e richiamarlo direttamente nell'istruzione. Le istruzioni TCON, TSEND_C e TRCV_C supportano il tipo di dati di sistema TCON_QDN:
per configurare un collegamento TCP mediante il nome del dominio del partner di comunicazione, procedere come segue:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire nel blocco dati globale una variabile del tipo di dati TCON_QDN.

   L'esempio seguente mostra il blocco dati globale "Data_block_1" nel quale è definita la variabile "DNS Connection1" del tipo di dati TCON_QDN.

Data_block_1

		Name	Datentyp	Startwert	Kommentar
1		Static			
2		DNS Connection1	TCON_QDN		
3		InterfaceId	HW_ANY	0	not relevant
4		ID	CONN_OUC	16#0	connection reference / identifier
5		ConnectionType	Byte	16#0B	type of connection: 16#0B=11=TCP/IP, 16#13=19=UDP
6		ActiveEstablished	Bool	false	active/passive connection establishment
7		RemoteQDN	String[254]	''	fully or partially qualified domain name of remote partner
8		RemotePort	UInt	0	remote UDP / TCP port number
9		LocalPort	UInt	0	local UDP / TCP port number

Figura 8-2 Tipo di dati TCON_QDN

3. Programmare i parametri del collegamento TCP - ad es. il nome del dominio completo (FQDN) - nella variabile del tipo di dati TCON_QDN.
4. Nell'editor di programma creare un'istruzione TCON.
5. Interconnettere il parametro CONNECT dell'istruzione TCON con la variabile del tipo di dati TCON_QDN.

   Nell'esempio seguente il parametro CONNECT dell'istruzione TCON è interconnesso con la variabile "DNS connection1" (tipo di dati TCON_QDN).

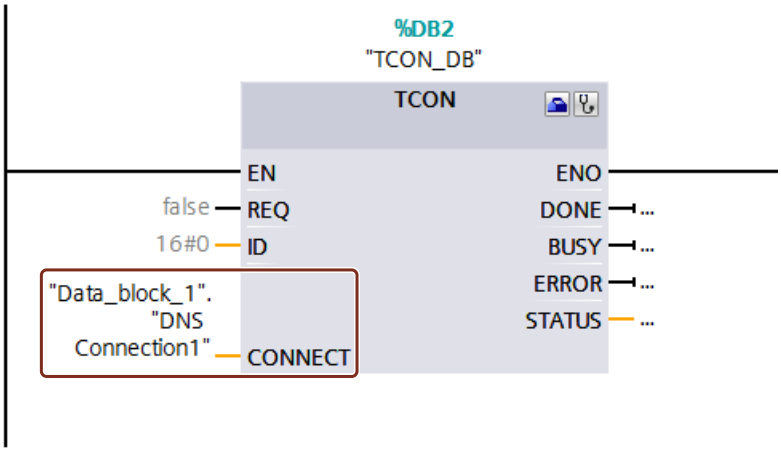


Figura 8-3 Istruzione TCON

Indirizzamento di un collegamento UDP tramite nome del dominio del partner della comunicazione

Durante la trasmissione dei dati tramite UDP, per le CPU S7-1500 a partire dalla versione firmware V2.0 è possibile indirizzare il ricevente con il relativo nome completo di dominio (FQDN). Con l'istruzione TUSEND nel parametro ADDR si punta ad una struttura del tipo TADDR_SEND_QDN.

Il ricevente può restituire un indirizzo IPv4 o un indirizzo IPv6. Con l'istruzione TURCV nel parametro ADDR puntare pertanto a una struttura del tipo TADDR_RCV_IP. Solo questa può accogliere entrambi i tipi di indirizzo IP.

NOTA

Carico di rete

Diversamente dal TCP, il protocollo UDP non ha un funzionamento orientato alla connessione. Ad ogni fronte nel parametro di blocco REQ l'istruzione TUSEND o TURCV interroga il server DNS. Questo può determinare un carico eccessivo sulla rete o sul server DNS.

Ulteriori informazioni

Maggiori informazioni sui tipi di dati di sistema TCON_QDN, TADDR_SEND_QDN e TADDR_RCV_IP sono disponibili nella Guida in linea a STEP 7.

La configurazione di un collegamento TCP sicuro tramite nome del dominio del partner della comunicazione è descritta nel capitolo Secure Open User Communication (Pagina 94).

8.5 Configurazione di Open User Communication tramite TCP, ISO on TCP, UDP e ISO

Parametrizzazione del collegamento per le istruzioni TSEND_C, TRCV_C o TCON

Presupposti: Nell'editor di programma è stata creata un'istruzione TSEND_C, TRCV_C o TCON.

1. Selezionare un blocco della Open User Communication TCON, TSEND_C o TRCV_C nell'editor di programma.
2. Nella finestra di ispezione aprire la scheda "Proprietà > Configurazione".
3. Selezionare il gruppo "Parametri di collegamento". Finché non si seleziona un partner di collegamento, per il punto finale del partner è attiva soltanto la casella di riepilogo vuota. Tutte le altre opzioni per l'inserimento dati sono disattivate.

   Vengono visualizzati i parametri di collegamento già noti:

   – Nome del punto finale locale
   – Interfaccia del punto finale locale

– Indirizzo IPv4 del punto finale locale

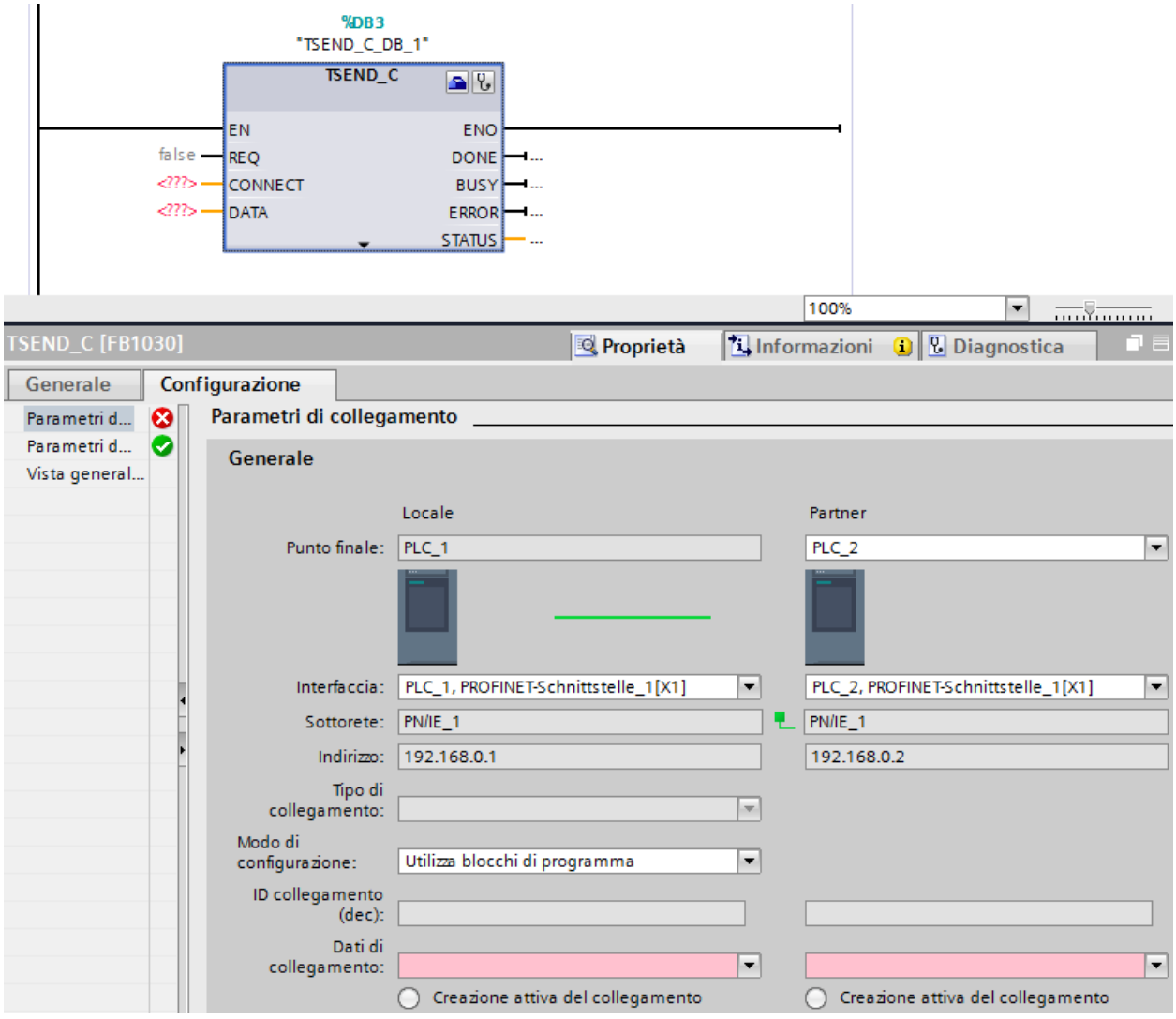


Figura 8-4 Parametrizzazione del collegamento per TSEND_C

4. Selezionare un partner di collegamento nella casella di riepilogo del punto finale del partner. Come partner di comunicazione si possono prendere in considerazione un dispositivo non specificato oppure una CPU disponibile nel progetto. In seguito, determinati partner di collegamento vengono inseriti automaticamente come preimpostazione.

   Vengono impostati i seguenti parametri:

   – Nome del punto finale del partner
   – Interfaccia del punto finale del partner
   – Indirizzo IPv4 del punto finale del partner

   Se i partner di collegamento sono collegati in rete, viene visualizzato il nome della sottorete.

5. Nella casella di riepilogo "Modo di configurazione" selezionare l'utilizzo di blocchi di programma o di collegamenti configurati.
6. Nella casella di riepilogo "Dati di collegamento" selezionare un DB di descrizione collegamento esistente oppure un collegamento disponibile nei collegamenti configurati alla voce "Nome del collegamento". È possibile anche creare un nuovo DB di descrizione collegamento o un nuovo collegamento configurato. È possibile selezionare successivamente anche altri DB di descrizione del collegamento o collegamenti configurati, oppure modificare il nome dei DB esistenti per creare nuovi blocchi dati:
   - Il blocco dati selezionato è visibile anche sul collegamento del parametro di ingresso CONNECT dell'istruzione selezionata TCON, TSEND_C o TRCV_C.
   - Se per il partner di collegamento è già stato indicato un DB di descrizione del collegamento attraverso il parametro CONNECT dell'istruzione TCON, TSEND_C o TRCV_C, è possibile utilizzare questo DB oppure crearne uno nuovo.
   - Se si modifica il nome del blocco dati visualizzato nella casella di riepilogo viene automaticamente generato e utilizzato per il collegamento un nuovo blocco dati con un altro nome ma con la medesima struttura e il medesimo contenuto.
   - I nomi modificati di un blocco dati devono essere univoci nel contesto del partner di comunicazione.
   - Un DB di descrizione del collegamento deve avere la struttura TCON_Param, TCON_IP_v4 o TCON_IP_RFC in funzione del tipo di CPU e del collegamento.
   - Non è possibile selezionare un blocco dati per un partner non specificato.

   Dopo la selezione o la creazione del DB di descrizione del collegamento o del collegamento configurato, vengono rilevati e registrati ulteriori valori.

   Per i partner di collegamento specificati vale quanto segue:
   - Tipo di collegamento ISO-on-TCP
   - ID del collegamento con il valore predefinito 1
   - Creazione attiva del collegamento dal partner locale
   - ID TSAP
     per S7-1200/1500: E0.01.49.53.4F.6F.6E.54.43.50.2D.31

   Per i partner di collegamento non specificati vale quanto segue:
   - Tipo di collegamento TCP
   - Porta partner 2000

   Per il collegamento configurato con un partner di collegamento specifico, vale quanto segue:
   - Tipo di collegamento TCP
   - ID del collegamento con il valore predefinito 257
   - Creazione attiva del collegamento dal partner locale
   - Porta partner 2000

   Per il collegamento configurato con un partner di collegamento non specificato, vale quanto segue:
   - Tipo di collegamento TCP
   - Porta locale 2000

7. Indicare se necessario un ID del collegamento per il partner. Non è possibile assegnare un ID di collegamento a un partner non specificato.

   NOTA

   Se il partner è noto si deve immettere un valore univoco per l'ID del collegamento. L'univocità dell'ID del collegamento non viene verificata dalla parametrizzazione del collegamento, e alla creazione di un nuovo collegamento non viene indicato alcun valore di default per l'ID del collegamento.

8. Selezionare il tipo di collegamento desiderato dalla corrispondente casella di riepilogo. Ai dettagli dell'indirizzo vengono preassegnati dei valori in funzione del tipo di collegamento. Esistono le seguenti opzioni:
   - TCP
   - ISO-on-TCP
   - UDP
   - ISO (soltanto nel modo di configurazione "Utilizza collegamento configurato")

   I dati nei campi di immissione nei dettagli dell'indirizzo possono essere modificati. In funzione del protocollo impostato è possibile modificare le porte (per TCP e UDP) oppure i TSAP (per ISO-on-TCP e ISO).
9. Nel caso di TCP, ISO e ISO-on-TCP impostare il comportamento per la creazione del collegamento nella casella "Creazione attiva del collegamento". È possibile selezionare quale partner di comunicazione debba creare il collegamento attivo.

La correttezza dei valori modificati viene immediatamente verificata dalla parametrizzazione del collegamento, quindi questi valori vengono inseriti nel blocco dati per la descrizione del collegamento.

NOTA

La modalità Open User Communication tra due partner di comunicazione è eseguibile soltanto dopo il caricamento nell'hardware della parte del programma per il punto finale del partner. Al fine di garantire il funzionamento della comunicazione, accertarsi che venga caricata nel dispositivo non solo la descrizione del collegamento della CPU locale bensì anche quella della CPU partner.

Progettazione dei collegamenti, ad es. per TSEND/TRCV

Per utilizzare le istruzioni per TSEND/TRCV ad es. per la comunicazione aperta, è necessario innanzitutto progettare un collegamento (ad es. un collegamento TCP).

Per progettare un collegamento TCP, procedere nel seguente modo:

1. Configurare i partner di comunicazione nella vista di rete dell'editor hardware e di rete di STEP 7.
2. Selezionare il pulsante "Collegamenti" e, nella casella di riepilogo, la voce "Collegamento TCP".
3. Collegare tra loro i partner di comunicazione con la funzione drag&drop (dall'interfaccia o dal punto finale locale). Se non ancora presente, la sottorete S7 verrà creata automaticamente.

   In alternativa è possibile configurare un collegamento a partner non specificati.
4. Nella vista di rete selezionare il collegamento creato.
5. Nell'area "Generale" della scheda "Proprietà" impostare all'occorrenza le proprietà del collegamento, ad es. il nome e le interfacce utilizzate dei partner di comunicazione.

   Per i collegamenti a un partner non specificato, impostare l'indirizzo del partner.
   L'ID locale è disponibile nell'area "ID locale" (riferimento al collegamento nel programma utente).
6. Nella navigazione del progetto selezionare per una delle due CPU la cartella "Blocchi di programma" in cui aprire l'OB 1 con un doppio clic. Si apre l'editor di programma.
7. Nella task card "Istruzioni", area "Comunicazione", "Open User Communication", selezionare l'istruzione desiderata, ad es. TSEND e trascinarla per drag&drop in un segmento dell'OB 1.
8. Nell'ID del parametro dell'istruzione assegnare l'ID locale del collegamento progettato che dovrà essere impiegato nella trasmissione dei dati.
9. Interconnettere il parametro "DATA" nell'istruzione TSEND con i dati utente, ad es. in un blocco dati.
10. Caricare la configurazione hardware e il programma utente nella CPU.

Configurare il collegamento nella CPU partner con l'istruzione TRCV per la ricezione seguendo il procedimento precedentemente descritto e caricarlo nella CPU.

Particolarità dei collegamenti ISO con CP 1543-1

Se si utilizza il tipo di collegamento "Collegamento ISO", è necessario attivare la casella di controllo "Utilizza protocollo ISO" nelle proprietà del CP per far funzionare l'indirizzamento tramite indirizzi MAC.

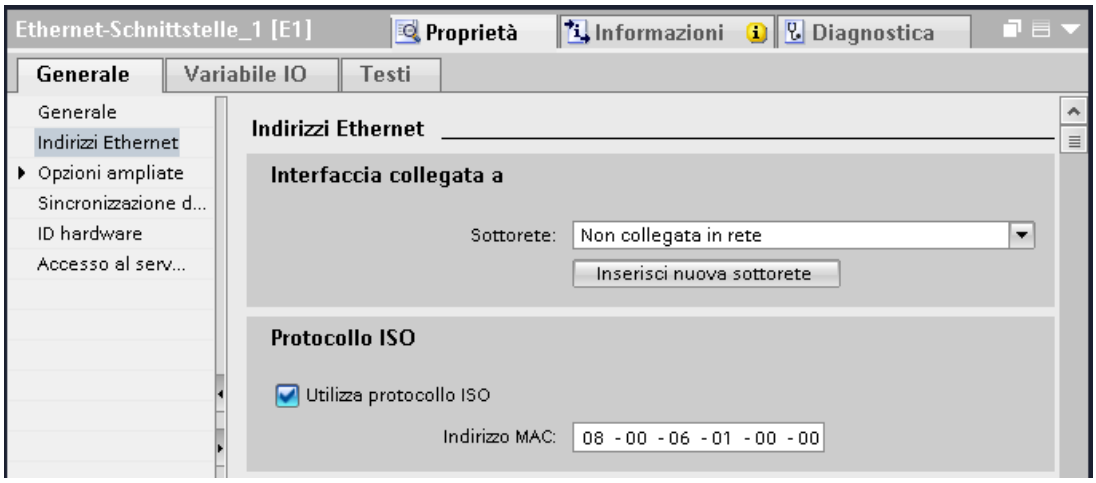


Figura 8-5 Selezione del protocollo ISO CP 1543-1

Ulteriori informazioni

Nella Guida in linea a STEP 7 sono descritti:

- istruzioni per la comunicazione aperta
- parametri del collegamento

Il comportamento delle istruzioni TSEND_C e TRCV_C su S7-1500 è descritto in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/109479564).

8.6 Configurazione della comunicazione tramite FDL

Presupposti

- Software di progettazione: STEP 7 Professional V14
- Punto finale del collegamento: CPU S7-1500 dalla versione firmware V2.0 con modulo di comunicazione CM 1542-5 con versione firmware V2.0

Impostazione di un collegamento FDL configurato

Per la configurazione di un collegamento FDL in STEP 7 procedere nel seguente modo:

1. Nell'editor di programma creare un'istruzione TSEND_C.
2. Selezionare l'istruzione TSEND_C quindi navigare su "Proprietà > Generale > Parametri di collegamento" nella finestra di ispezione.
3. Alla voce "Punto finale" selezionare il punto finale del partner. Utilizzare uno dei due punti finali del partner seguenti:
   - CPU S7-1500 con CM 1542-5
   - Non specificato
4. Alla voce "Modo di configurazione", selezionare la funzione "Utilizza collegamento configurato".
5. Alla voce "Tipo di collegamento" selezionare "FDL".
6. Alla voce Interfaccia, selezionare le seguenti interfacce:
   - Locale: Interfaccia PROFIBUS del CM 1542-5
   - Partner non specificato: Interfaccia PROFIBUS del CM 1542-5
7. Nei dati di collegamento selezionare l'impostazione <nuovo>.

La figura seguente mostra un collegamento FDL completamente configurato in STEP 7.

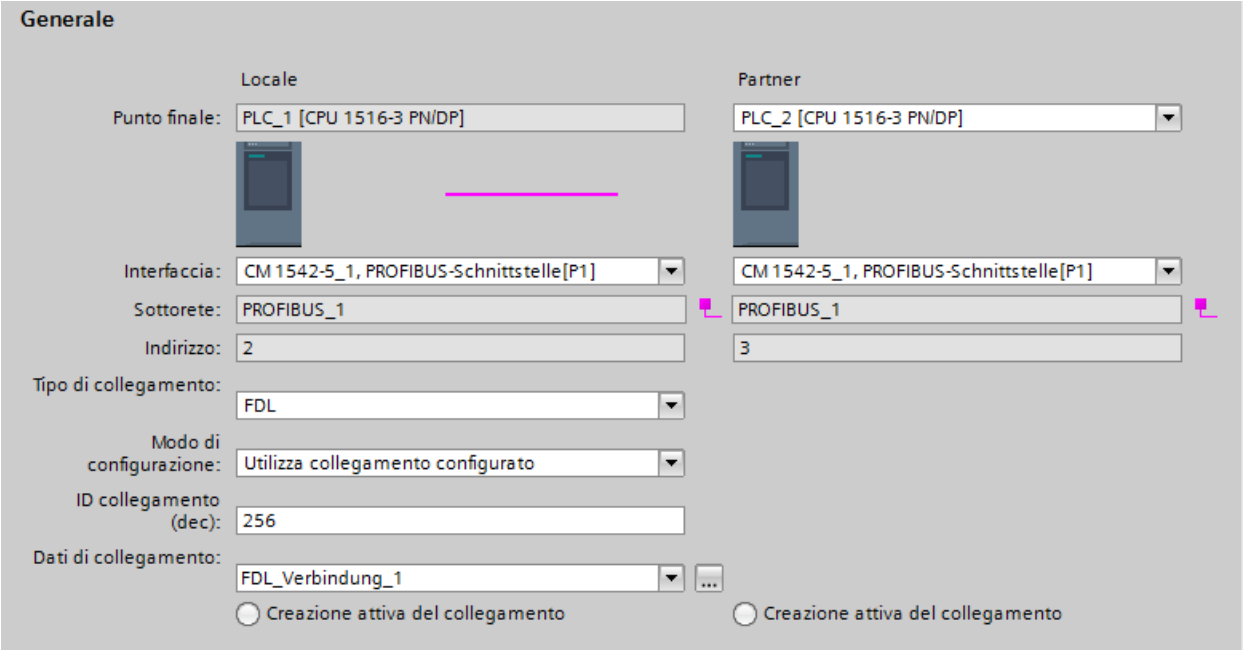


Figura 8-6 Configurazione del collegamento FDL

Configurazione di un collegamento FDL nel programma utente

Per la comunicazione tramite FDL è necessario creare e parametrizzare il rispettivo blocco dati del tipo di dati di sistema TCON_FDL e richiamarlo direttamente nell'istruzione. Procedere nel seguente modo:

1. Nella navigazione del progetto creare un blocco dati globale.
2. Definire una variabile del tipo di dati TCON_FDL nel blocco dati globale

   L'esempio seguente mostra il blocco dati globale "FDL_connection" nel quale è definita la variabile "FDL_connection" del tipo di dati TCON_FDL.

FDL_connection

		Nome	Tipo di dati	Valore ...	A...	A...	S...	V...	V...	Contr...	Commento
1		Static									
2		FDL_connection	TCON_FDL			☑	☑	☑			
3		InterfaceId	HW_ANY	0		☑	☑	☑			HW identifier of PB interface submodule
4		ID	CONN_OUC	16#0		☑	☑	☑			connection reference / identifier
5		ConnectionType	Byte	16#15		☑	☑	☑			type of connection: 21= FDL connection
6		ActiveEstablished	Bool	false		☑	☑	☑			active/passive connection establishment
7		ServiceId	Byte	16#0		☑	☑	☑			service id: 0 – default, 1 – SDA, 2 – SDN
8		RemotePBAddress	Byte	16#0		☑	☑	☑			remote ProfiBus partner address
9		LocalPBAddress	Byte	16#0		☑	☑	☑			local ProfiBus partner address
10		RemoteLSAP	Byte	16#0		☑	☑	☑			remote PB link-layer service access point
11		LocalLSAP	Byte	16#0		☑	☑	☑			local PB link-layer service access point

Figura 8-7 Programmazione del collegamento FDL

3. Programmare i parametri del collegamento FDL (ad es. gli indirizzi PROFIBUS) nella variabile del tipo di dati TCON_FDL.
4. Nell'editor di programma creare un'istruzione TCON.
5. Interconnettere il parametro CONNECT dell'istruzione TCON con la variabile del tipo di dati TCON_FDL.

   Nell'esempio seguente il parametro CONNECT dell'istruzione TCON è interconnesso con la variabile "FDL_Connection" (tipo di dati TCON_FDL).

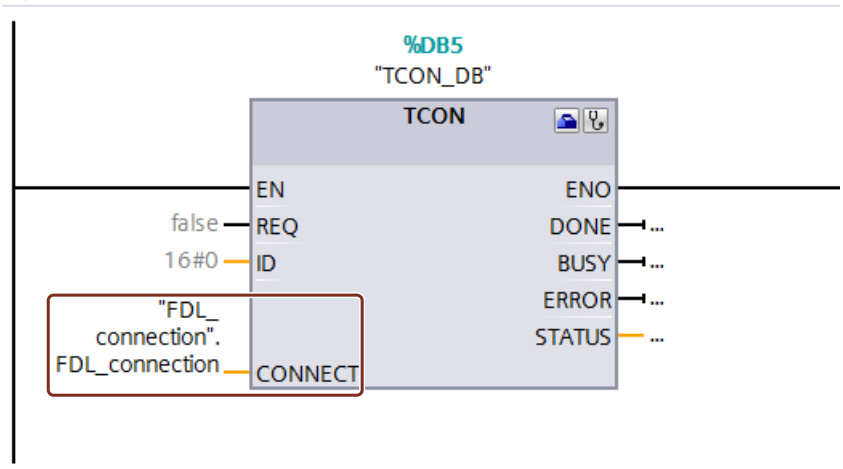


Figura 8-8 Esempio: Istruzione TCON per collegamento FDL

8.7 Configurazione della comunicazione tramiter Modbus TCP

Configurazione di un collegamento tramite il programma utente per Modbus TCP

La parametrizzazione viene eseguita nell'editor di programma nell'istruzione "MB_CLIENT" (MB_SERVER).

Procedimento di configurazione della comunicazione tramite Modbus TCP

L'istruzione "MB_CLIENT" comunica come client Modbus TCP tramite un collegamento TCP. L'istruzione consente di stabilire un collegamento tra client e server, di inviare richieste Modbus al server e ricevere le relative risposte Modbus. Permette inoltre di comandare la disattivazione del collegamento TCP.

L'istruzione MB_SERVER comunica come server Modbus TCP tramite un collegamento TCP. L'istruzione elabora le richieste di collegamento di un client Modbus, riceve ed elabora le richieste Modbus e invia messaggi di risposta. Permette inoltre di comandare la disattivazione del collegamento TCP.

Presupposti: il client può raggiungere il server nella rete attraverso la comunicazione IP.

1. Configurare un sistema di automazione S7-1500 con CPU nella vista di rete dell'editor hardware e di rete di STEP 7.
2. Nella navigazione del progetto selezionare per la CPU la cartella "Blocchi di programma" in cui aprire l'OB 1 con un doppio clic. Si apre l'editor di programma.
3. Nella task card "Istruzioni", area "Comunicazione", "Ulteriori", "MODBUS TCP" selezionare l'istruzione desiderata, ad es. MB_CLIENT e trascinarla per drag&drop in un segmento dell'OB 1.
4. Parametrizzare l'istruzione MB_CLIENT o MB_SERVER. Attenersi alle seguenti regole:

   Per ogni collegamento MB_CLIENT è necessario specificare un indirizzo IPv4 per il server.

   Ogni collegamento MB_CLIENT o MB_SERVER deve utilizzare un DB di istanza univoco con le strutture di dati TCON_IP_v4, TCON_QDN o TCON_Configured.

Ogni collegamento richiede un ID di collegamento univoco. L'ID di collegamento e il DB di istanza sono raggruppati rispettivamente in coppie e devono essere univoci per ogni collegamento.

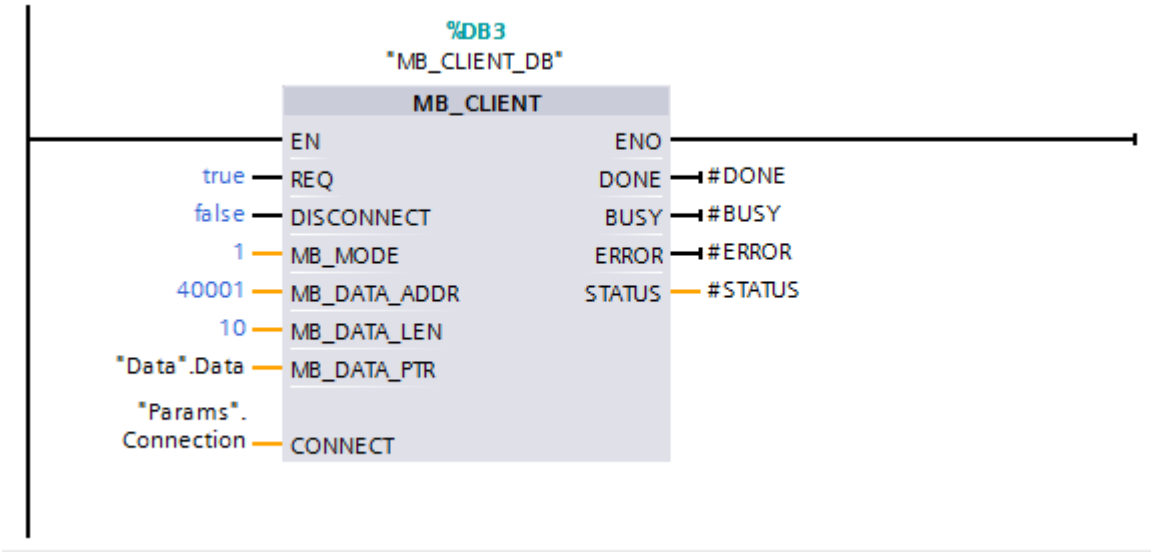


Figura 8-9 MB_CLIENT

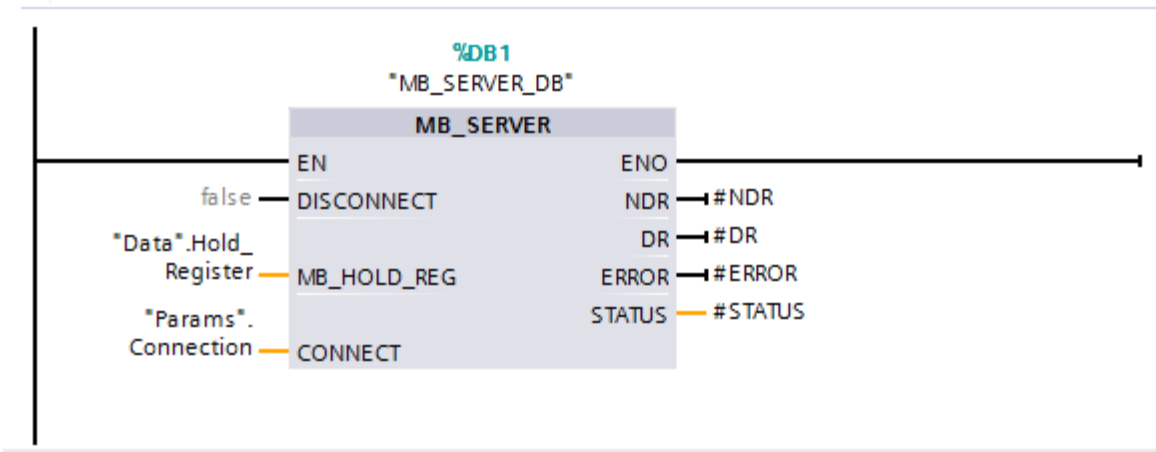


Figura 8-10 MB_SERVER

5. Caricare la configurazione hardware e il programma utente nella CPU.

Comunicazione ridondante tramite Modbus TCP

La comunicazione ridondante tramite Modbus TCP può essere parametrizzata con le istruzioni MB_RED_CLIENT o MB_RED_SERVER:

Istruzione MB_RED_CLIENT: L'istruzione "MB_RED_CLIENT" consente di stabilire un collegamento ridondante tra client e server, inviare richieste Modbus e ricevere risposte nonché di comandare la disattivazione del collegamento del client Modbus TCP.

Istruzione MB_RED_SERVER: L'istruzione "MB_RED_SERVER" elabora le richieste di collegamento di un client Modbus TCP, riceve ed elabora le richieste Modbus e invia messaggi di risposta. Le CPU sono in grado:

- di elaborare collegamenti multipli al server e
- di collegare contemporaneamente diversi client su una porta del server.

Per ulteriori informazioni sulle istruzioni MB_RED_CLIENT o MB_RED_SERVER consultare la guida in linea di STEP 7.

Server Modbus TCP come gateway verso un protocollo Modbus RTU

Se si utilizza un server Modbus TCP come gateway verso un protocollo Modbus RTU, indirizzare il dispositivo slave nella rete seriale tramite il parametro statico MB_UNIT_ID. Il parametro MB_UNIT_ID corrisponde al campo dell'indirizzo slave nel protocollo Modbus RTU. Il parametro MB_UNIT_ID in questo caso inoltrerebbe la richiesta all'indirizzo slave Modbus RTU corretto.

La funzione Gateway deve essere programmata dall'utente.

Il parametro MB_UNIT_ID si trova nel blocco dati di istanza dell'istruzione MB_CLIENT.

Maggiori informazioni sul parametro MB_UNIT_ID sono disponibili nella Guida in linea a STEP 7.

Riferimenti

- La programmazione e la parametrizzazione della comunicazione Modbus-TCP tra due CPU S7-1500 sono descritte in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/94766380).
- La programmazione e la parametrizzazione della comunicazione Modbus TCP tra una CPU S7-1500 e una CPU S7-1200 sono descritte in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/102020340).

8.8 Configurazione della comunicazione tramite e-mail

Configurazione di un collegamento tramite il programma utente per e-mail

Per la comunicazione tramite e-mail è necessario creare e parametrizzare il blocco dati del rispettivo tipo di dati di sistema e richiamarlo direttamente nell'istruzione. Il procedimento è rappresentato di seguito.

Procedimento di configurazione della comunicazione tramite e-mail

Le e-mail possono essere inviate da una CPU. Per l'invio di e-mail dal programma utente della CPU impostare l'istruzione TMAIL_C.

Presupposti: Il server SMTP è accessibile dalla rete IPv4.

1. Configurare un sistema di automazione S7-1500 con CPU nella vista di rete dell'editor hardware e di rete di STEP 7.
2. Parametrizzare l'istruzione TMAIL_C, ad es. specificando in Subject l'oggetto della mail.
3. Creare una variabile di tipo TMAIL_v4, TMAIL_v6 (solo CP 1543-1) o TMAIL_FQDN (solo CP 1543-1) in un blocco dati globale.
4. Impostare nella variabile i parametri del collegamento TCP nella colonna "Valore di avvio". Inserire ad es. in "MailServerAdress" l'indirizzo IPv4 del server e-mail (per TMAIL_v4)

   NOTA
   Parametri di collegamento InterfaceId
   Dalla versione V5.0 dell'istruzione TMAIL_C è possibile specificare nel tipo di dati TMAIL_V4_SEC il valore "**0**" per InterfaceId. In questo caso è la CPU stessa a rilevare un'interfaccia locale adatta.

   Collegare la variabile al parametro MAIL_ADDR_PARAM dell'istruzione TMAIL_C.
5. Caricare la configurazione hardware e il programma utente nella CPU.

Ulteriori informazioni

Nella Guida in linea a STEP 7 sono descritti:

- tipi di dati di sistema
- istruzioni per la comunicazione aperta
- parametri del collegamento

8.9 Configurazione della comunicazione tramite protocollo FTP

Configurazione di un collegamento tramite il programma utente per FTP

Per la comunicazione tramite FTP è necessario creare e parametrizzare il blocco dati del rispettivo tipo di dati di sistema e richiamarlo direttamente nell'istruzione. Il procedimento è rappresentato di seguito.

Funzionalità client e server FTP

I file possono essere inviati da una CPU a un server FTP e ricevuti da quest'ultimo. La comunicazione tramite FTP è possibile per l'S7-1500 solo con il CP 1543-1. Il CP può essere il server FTP, il client FTP o entrambi. I client FTP possono anche essere sistemi di terzi/PC.

Per la funzionalità come server FTP si deve progettare il CP in STEP 7.

La funzionalità come client FTP consente ad es. di creare e interrompere un collegamento FTP e di trasferire ed eliminare file sul server. Per la funzionalità come client FTP impostare l'istruzione FTP_CMD.

Procedimento di configurazione della funzionalità come server FTP

Presupposti: Il server FTP deve essere accessibile dalla rete IPv4.

1. Nella vista dispositivi dell'editor hardware e di rete di STEP 7 configurare un sistema di automazione S7-1500 con CPU e CP 1543-1.

   Allo stesso tempo attivare l'opzione "Consenti accesso tramite la comunicazione PUT/GET tramite partner remoti (PLC, HMI, OPC, ...)" nella sezione "Meccanismi di collegamento" della navigazione nell'area "Protezione" all'interno della configurazione hardware della CPU S7-1500.

2. Nelle proprietà del CP, in "Configurazione FTP", eseguire le seguenti impostazioni:
   - Selezionare la casella di scelta "Utilizza server FTP per dati CPU S7".
   - Assegnare la CPU, un blocco dati e un nome del file con il quale salvare il DB per FTP.

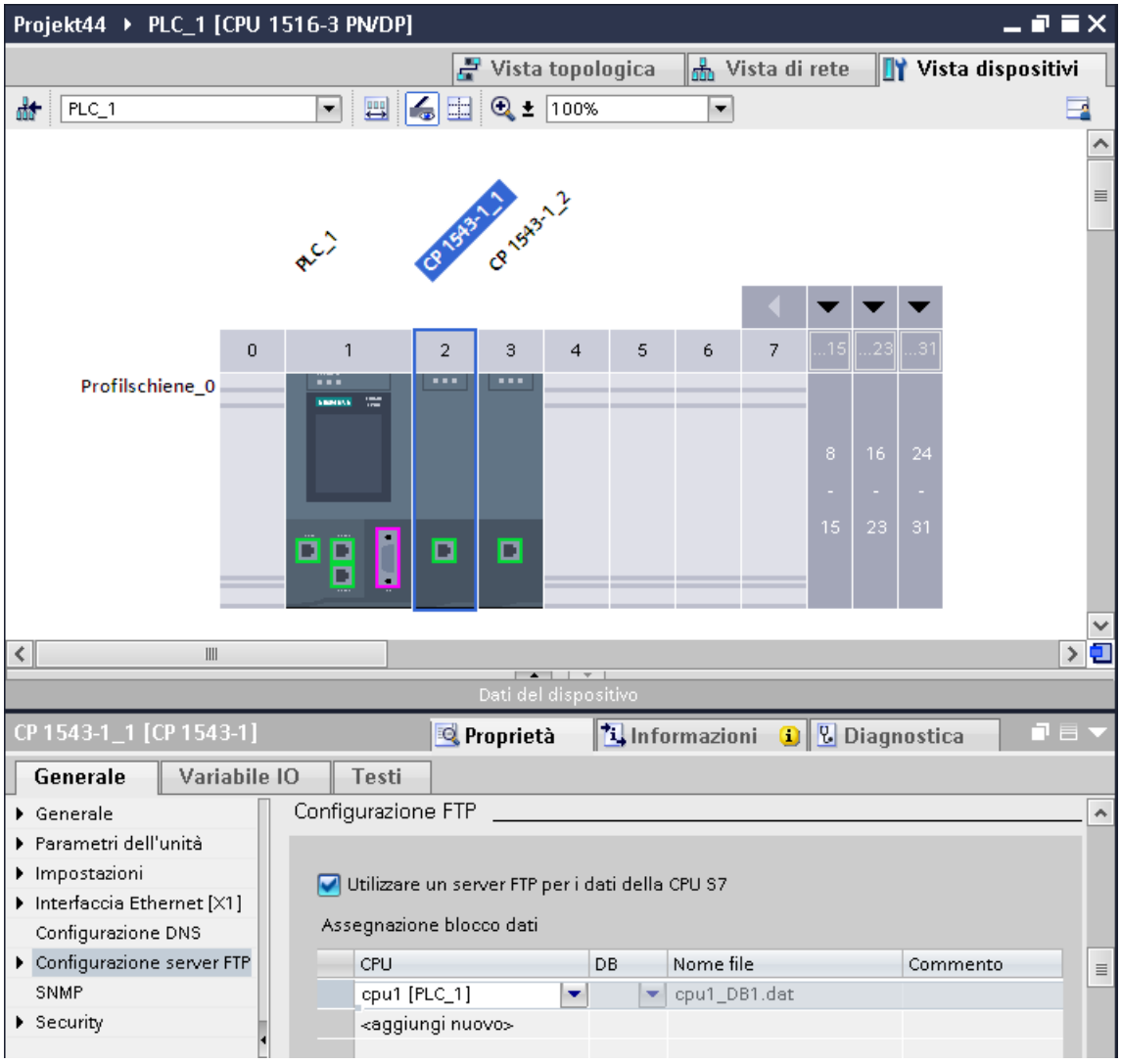


Figura 8-11 Impostazione della configurazione FTP

3. Caricare la configurazione hardware nella CPU.

Procedimento di configurazione della funzionalità come client FTP

Presupposti: Il server FTP deve essere accessibile dalla rete IPv4**.**

1. Nella vista dispositivi dell'editor hardware e di rete di STEP 7 configurare un sistema di automazione S7-1500 con CPU e CP 1543-1.

   Allo stesso tempo attivare la casella di scelta "Consenti accesso tramite la comunicazione PUT/GET tramite partner remoti (PLC, HMI, OPC, ...)" nella sezione "Meccanismi di collegamento" della navigazione nell'area "Protezione" all'interno della configurazione hardware della CPU S7-1500.
2. Richiamare l'istruzione FTP_CMD nel programma utente della CPU.
3. Parametrizzare nell'istruzione FTP_CMD i parametri del collegamento per il server FTP.
4. Creare un DB globale e al suo interno una variabile di tipo FTP_CONNECT_IPV4, FTP_CONNECT_IPV6 o FTP_CONNECT_NAME.
5. Nel blocco dati collegare la variabile con l'istruzione FTP_CMD.
6. Per il collegamento al server FTP indicare nel DB:
   – il nome utente, la password e l'indirizzo IP per l'accesso FTP nel relativo tipo di dati (FTP_CONNECT_IPV4, FTP_CONNECT_IPV6 o FTP_CONNECT_NAME)
7. Caricare la configurazione hardware e il programma utente nella CPU.

Esempi pratici

- Esempio applicativo: comunicazione FTP con S7-1500 e CP 1543-1
  L'esempio pratico è disponibile in Internet (https://support.industry.siemens.com/cs/ww/it/view/103550797).
- Esempio applicativo: Comunicazione client FTP con S7-1200/1500
  L'esempio pratico è disponibile in Internet (https://support.industry.siemens.com/cs/ww/it/view/81367009).

Ulteriori informazioni

Nella Guida in linea a STEP 7 sono descritti:

- tipi di dati di sistema
- istruzioni per la comunicazione aperta
- parametri del collegamento

8.10 Creazione e interruzione di relazioni di comunicazione

Creazione e interruzione di relazioni di comunicazione

La seguente tabella illustra la creazione e l'interruzione delle relazioni di comunicazione nell'ambito della comunicazione aperta.

Tabella 8-5 Creazione e interruzione di relazioni di comunicazione

Configurazione del collegamento	Creazione della relazione di comunicazione	Interruzione della relazione di comunicazione
Tramite programma utente	Dopo il caricamento del programma utente nelle CPU: Il partner di comunicazione passivo configura l'accesso locale al collegamento richiamando TSEND_C/TRCV_C o TCON. Il richiamo di TSEND_C/TRCV_C o TCON nel partner attivo avvia la creazione del collegamento. Se la creazione del collegamento è riuscita, si verifica una risposta positiva nelle istruzioni nel programma utente. Dopo avere interrotto un collegamento con l'istruzione T_RESET, il collegamento viene nuovamente creato. In caso di interruzione del collegamento il partner attivo tenta di ristabilire il collegamento configurato. Questo vale se prima è stato creato correttamente il collegamento con TCON.	• Tramite le istruzioni TSEND_C/TRCV_C, TDISCON e T_RESET • Se la CPU passa dallo stato di funzionamento RUN a STOP • In caso di rete OFF/ON in una CPU
Tramite progettazione del collegamento	Dopo il caricamento della progettazione del collegamento e del programma utente nelle CPU.	Cancellando la progettazione del collegamento in STEP 7 e caricando la progettazione modificata nella CPU.

Comunicazione S7

9

Caratteristiche della comunicazione S7

La comunicazione S7, quale comunicazione omogenea SIMATIC, è caratterizzata dalla comunicazione specifica del produttore tra CPU SIMATIC (nessuno standard aperto). La comunicazione S7 consente la migrazione e la connessione a sistemi esistenti (S7-300, S7-400).

Per il trasferimento dei dati tra due sistemi di automazione S7-1500 si consiglia di utilizzare la comunicazione aperta (vedere il capitolo Open User Communication (Pagina 140)).

Proprietà della comunicazione S7

Attraverso la comunicazione S7 la CPU scambia dati con un'altra CPU. Non appena l'utente ha ricevuto i dati sul lato destinatario, la ricezione dei dati viene confermata automaticamente nella CPU di trasmissione.

Lo scambio di dati avviene attraverso collegamenti S7 progettati. I collegamenti S7 possono essere progettati unilateralmente o bilateralmente.

Comunicazione S7 possibile tramite:

- Interfaccia integrata PROFINET o PROFIBUS DP di una CPU
- Interfacce di un CP/CM

Collegamenti S7 progettati unilateralmente

Nei collegamenti S7 progettati unilateralmente il collegamento viene progettato e caricato in un solo partner di comunicazione.

Un collegamento S7 unilaterale può essere progettato verso una CPU che funge soltanto da server di un collegamento S7 (ad es. CPU 315-2 DP). La CPU è stata progettata e i parametri degli indirizzi e le interfacce sono noti.

Inoltre è possibile progettare un collegamento S7 unilaterale verso un partner non presente nel progetto, i cui parametri degli indirizzi e la cui interfaccia non sono pertanto noti. L'indirizzo deve essere immesso dall'utente e non viene controllato da STEP 7. Inizialmente il partner non è specificato (al momento della creazione del collegamento S7 non è ancora stato immesso alcun indirizzo del partner). Non appena viene immesso, l'indirizzo è considerato "sconosciuto" (ovvero: è specificato ma non è noto al progetto).

In questo modo è possibile impiegare i collegamenti S7 oltre i limiti del progetto. Il partner di comunicazione è sconosciuto (non specificato) per il progetto locale e viene progettato in un altro progetto STEP 7 o in un progetto di terzi.

Collegamenti S7 progettati bilateralmente

Nei collegamenti S7 progettati bilateralmente i parametri di collegamento S7 vengono progettati e caricati in entrambi i partner della comunicazione.

Istruzioni per la comunicazione S7

Per la comunicazione S7 nell'S7-1500 si possono utilizzare le seguenti istruzioni:

- PUT/GET

  Con l'istruzione PUT è possibile scrivere dati in una CPU remota. L'istruzione GET consente di leggere dati da una CPU remota. Le istruzioni PUT e GET sono unilaterali, ovvero l'istruzione è necessaria soltanto in un partner di comunicazione. Le istruzioni PUT e GET si possono comodamente configurare con la parametrizzazione del collegamento.

  NOTA
  Blocchi dati per le istruzioni PUT/GET
  Con le istruzioni PUT/GET si possono utilizzare solo blocchi dati con indirizzamento assoluto. L'indirizzamento simbolico dei blocchi dati non è possibile.
  Inoltre questo servizio deve essere abilitato nell'area "Protezione" nella progettazione della CPU.

  La progettazione e programmazione di un collegamento S7 e delle istruzioni di comunicazione PUT e GET per lo scambio di dati tra due CPU S7-1500 sono descritte in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/82212115).

- BSEND/BRCV

  L'istruzione BSEND trasmette dati a un'istruzione partner remota di tipo BRCV. L'istruzione BRCV riceve i dati da un'istruzione partner remota del tipo BSEND. La comunicazione S7 attraverso la coppia di istruzioni BSEND/BRCV viene utilizzata per la trasmissione sicura dei dati.

- USEND/URCV

  L'istruzione USEND trasmette dati a un'istruzione partner remota di tipo URCV. L'istruzione URCV riceve dati da un'istruzione partner remota di tipo USEND. La comunicazione S7 attraverso la coppia di istruzioni USEND/URCV si utilizza per la trasmissione rapida e non protetta dei dati a prescindere dall'elaborazione temporale del partner di comunicazione, ad es. per le segnalazioni di servizio e di manutenzione.

Comunicazione S7 attraverso l'interfaccia PROFIBUS DP nel funzionamento slave

In STEP 7, nelle proprietà dell'interfaccia PROFIBUS DP dei moduli di comunicazione (ad es. CM 1542-5), si trova la casella di controllo "Test, messa in servizio e routing". Questa casella di controllo permette di impostare se l'interfaccia PROFIBUS DP dello slave DP è nodo attivo o passivo in PROFIBUS.

- Casella di controllo attivata: lo slave DP è nodo attivo in PROFIBUS.
- Casella di controllo disattivata: lo slave DP è nodo passivo in PROFIBUS. Per questo slave DP si possono configurare solo collegamenti S7 progettati unilateralmente.

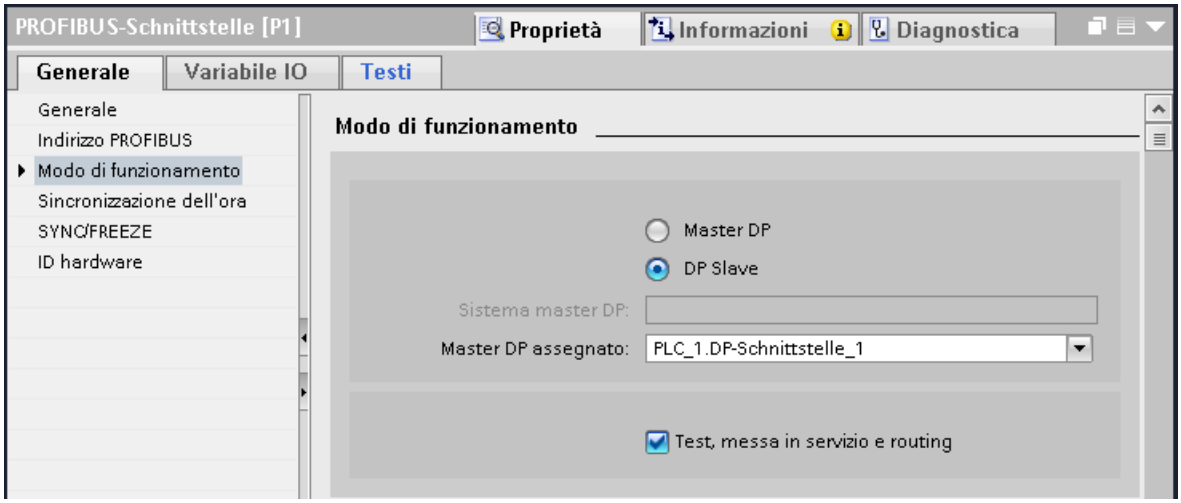


Figura 9-1 Casella di controllo "Test, messa in servizio e routing"

Parametrizzazione di collegamenti S7 per istruzioni PUT/GET

Con la parametrizzazione del collegamento delle istruzioni PUT/GET è possibile creare e parametrizzare collegamenti S7. La parametrizzazione dei collegamenti verifica direttamente che i valori modificati non siano errori di inserimento.

Presupposti: Nell'editor di programma è stata creata un'istruzione PUT o GET.

Per progettare un collegamento S7 con le istruzioni PUT/GET procedere nel seguente modo:

1. Selezionare nell'editor di programma il richiamo dell'istruzione PUT o GET.
2. Nella finestra di ispezione aprire la scheda "Proprietà > Configurazione".
3. Selezionare il gruppo "Parametri di collegamento". Finché non si seleziona un partner di collegamento, per il punto finale del partner è attiva soltanto la casella di riepilogo vuota. Tutte le altre opzioni per l'inserimento dati sono disattivate.

   Vengono visualizzati i parametri di collegamento già noti:

   – Nome del punto finale locale
   – Interfaccia del punto finale locale

– Indirizzo IPv4 del punto finale locale

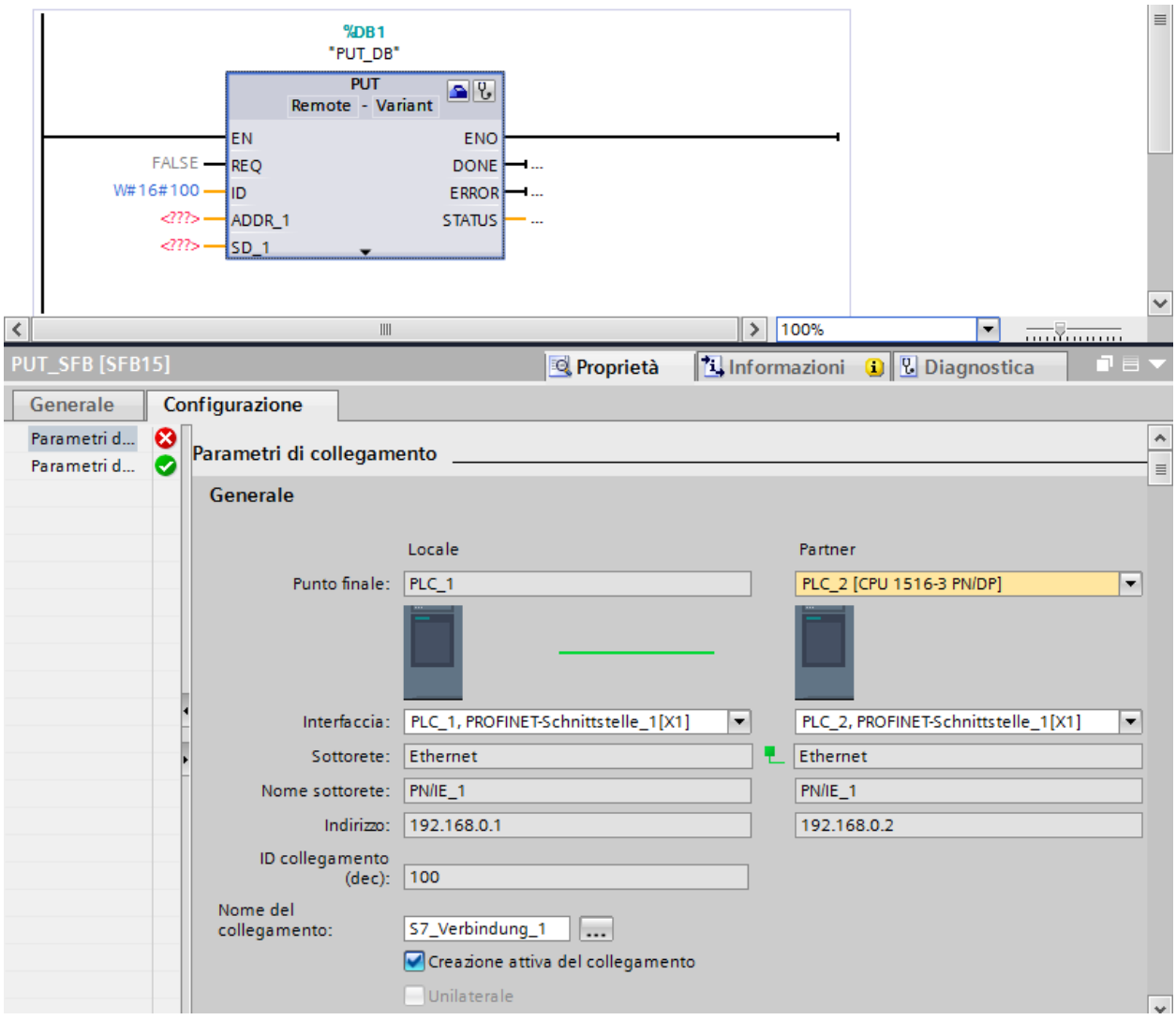


Figura 9-2 Parametrizzazione del collegamento per l'istruzione PUT

4. Selezionare un partner di collegamento nella casella di riepilogo del punto finale del partner. Come partner di comunicazione si possono prendere in considerazione un dispositivo non specificato oppure una CPU disponibile nel progetto.

   I seguenti parametri vengono immessi automaticamente non appena si seleziona il partner di collegamento:

   – Nome del punto finale del partner
   – Interfaccia del punto finale del partner. Se sono disponibili più interfacce, questa interfaccia può essere cambiata.
   – Tipo di interfaccia del punto finale del partner
   – Nome della sottorete di entrambi i punti finali
   – Indirizzo IPv4 del punto finale del partner
   – Nome del collegamento utilizzato per la comunicazione.

5. Se necessario, rinominare il collegamento nella casella di introduzione "Nome del collegamento". Facendo clic sul pulsante “Seleziona collegamento" a destra di fianco alla casella di introduzione per il nome del collegamento è possibile creare un nuovo collegamento oppure modificare un collegamento esistente.

NOTA

Le istruzioni PUT e GET tra due partner di comunicazione diventano eseguibili soltanto dopo il caricamento della configurazione hardware e della parte di programma per il punto finale del partner nell'hardware. Al fine di garantire il funzionamento della comunicazione, accertarsi che venga caricata nel dispositivo non solo la descrizione del collegamento della CPU locale bensì anche quella della CPU partner.

Progettazione dei collegamenti S7, ad es. per BSEND/BRCV

Per utilizzare le istruzioni per BSEND/BRCV ad es. per la comunicazione S7, è necessario innanzitutto progettare un collegamento S7.

Per progettare un collegamento S7, procedere nel seguente modo:

1. Configurare i partner di comunicazione nella vista di rete dell'editor hardware e di rete di STEP 7.
2. Selezionare il pulsante "Collegamenti" e nell'elenco a discesa la voce "Collegamenti S7".
3. Collegare tra loro i partner di comunicazione con la funzione drag&drop (dall'interfaccia o dal punto finale locale). Se non ancora presente, la sottorete S7 verrà creata automaticamente.

   In alternativa è possibile configurare un collegamento a partner non specificati.
4. Nella scheda "Collegamenti" selezionare la riga del collegamento S7.
5. Nell'area "Generale" della scheda "Proprietà" impostare all'occorrenza le proprietà del collegamento S7, ad es. il nome e le interfacce utilizzate dei partner di comunicazione.

   Per i collegamenti S7 a un partner non specificato, impostare l'indirizzo del partner. L'ID locale è disponibile nell'area "ID locale" (riferimento al collegamento S7 nel programma utente).
6. Nella navigazione del progetto selezionare per una delle due CPU la cartella "Blocchi di programma" in cui aprire l'OB 1 con un doppio clic. Si apre l'editor di programma.
7. Richiamare qui le istruzioni per la comunicazione S7 nel programma utente del partner di comunicazione (unilaterale) o nei programmi utente dei partner di comunicazione (bilaterale). Nella task card "Istruzioni", area "Comunicazione", selezionare ad es. le istruzioni BSEND e BRCV e trascinarle per drag&drop in un segmento dell'OB 1.
8. Nell'ID del parametro dell'istruzione assegnare l'ID locale del collegamento progettato che dovrà essere impiegato nella trasmissione dei dati.
9. Parametrizzare le istruzioni che scrivono o leggono dati.
10. Caricare la configurazione hardware e il programma utente nella/e CPU.

Comunicazione S7 tramite il CP 1543-1

Se si configura la comunicazione S7 tramite l'interfaccia Industrial Ethernet del CP 1543-1, nelle proprietà dell'interfaccia S7 alla voce "Generale" si può selezionare il protocollo di trasporto per la trasmissione dati:

- Casella di controllo "TCP/IP" attivata (per default): ISO-on-TCP (RFC 1006): per la comunicazione S7 tra CPU S7-1500
- Casella di controllo "TCP/IP" disattivata: Protocollo ISO (ISO/IEC 8073): indirizzamento tramite indirizzi MAC

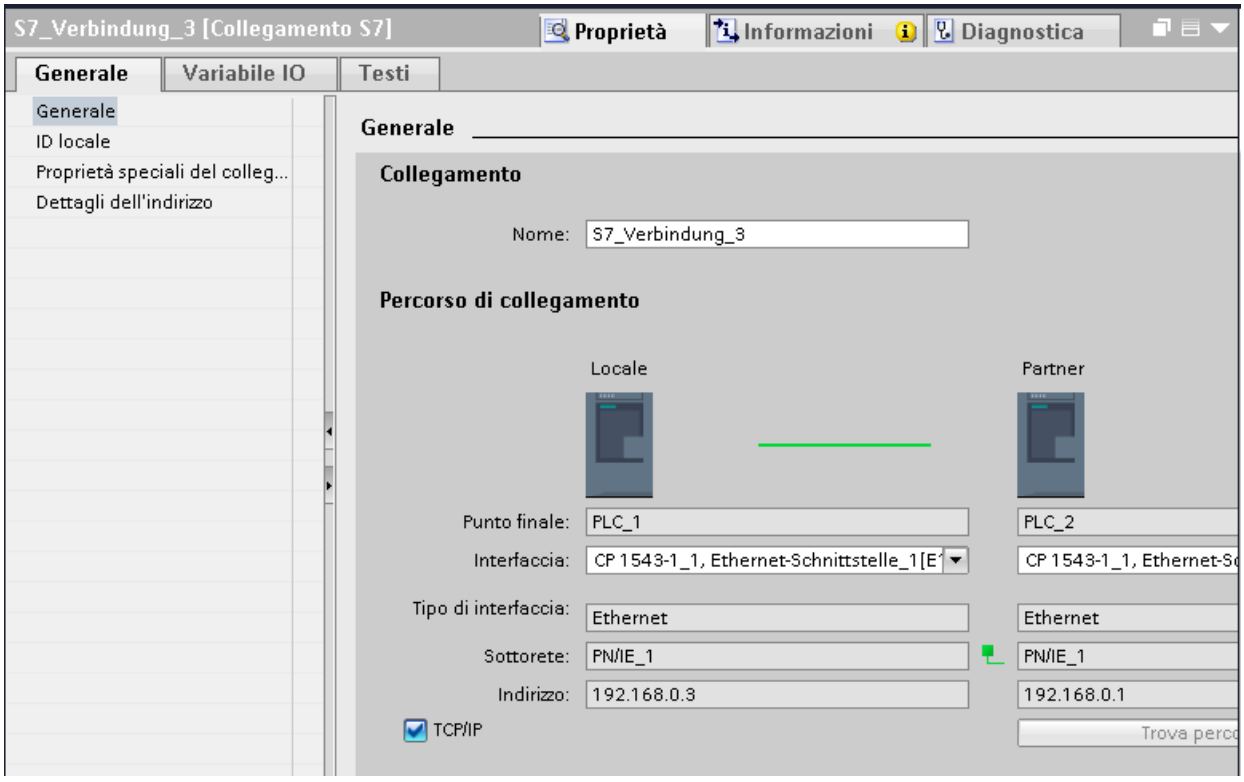


Figura 9-3 Selezione del protocollo di trasporto CP 1543-1

Procedimento di configurazione di un collegamento S7 tramite diverse sottoreti S7

Un collegamento S7 può essere utilizzato da più sottoreti S7 (PROFIBUS, PROFINET/Industrial Ethernet) (routing tramite S7 (Pagina 419)).

1. Configurare i partner di comunicazione nella vista di rete dell'editor hardware e di rete di STEP 7.
2. Selezionare il pulsante "Collega in rete".
3. Collegare con drag&drop le interfacce interessate con le rispettive sottoreti S7 (PROFIBUS o PROFINET / Industrial Ethernet).
4. Selezionare il pulsante "Collegamenti" e nell'elenco a discesa la voce "Collegamenti S7".

5. Collegare con la funzione drag&drop il PLC_1 nella sottorete S7 a sinistra (PROFIBUS) con il PLC_3 nella sottorete S7 a destra (PROFINET) nell'esempio.

   Il collegamento S7 dalla CPU 1 alla CPU 3 è configurato.

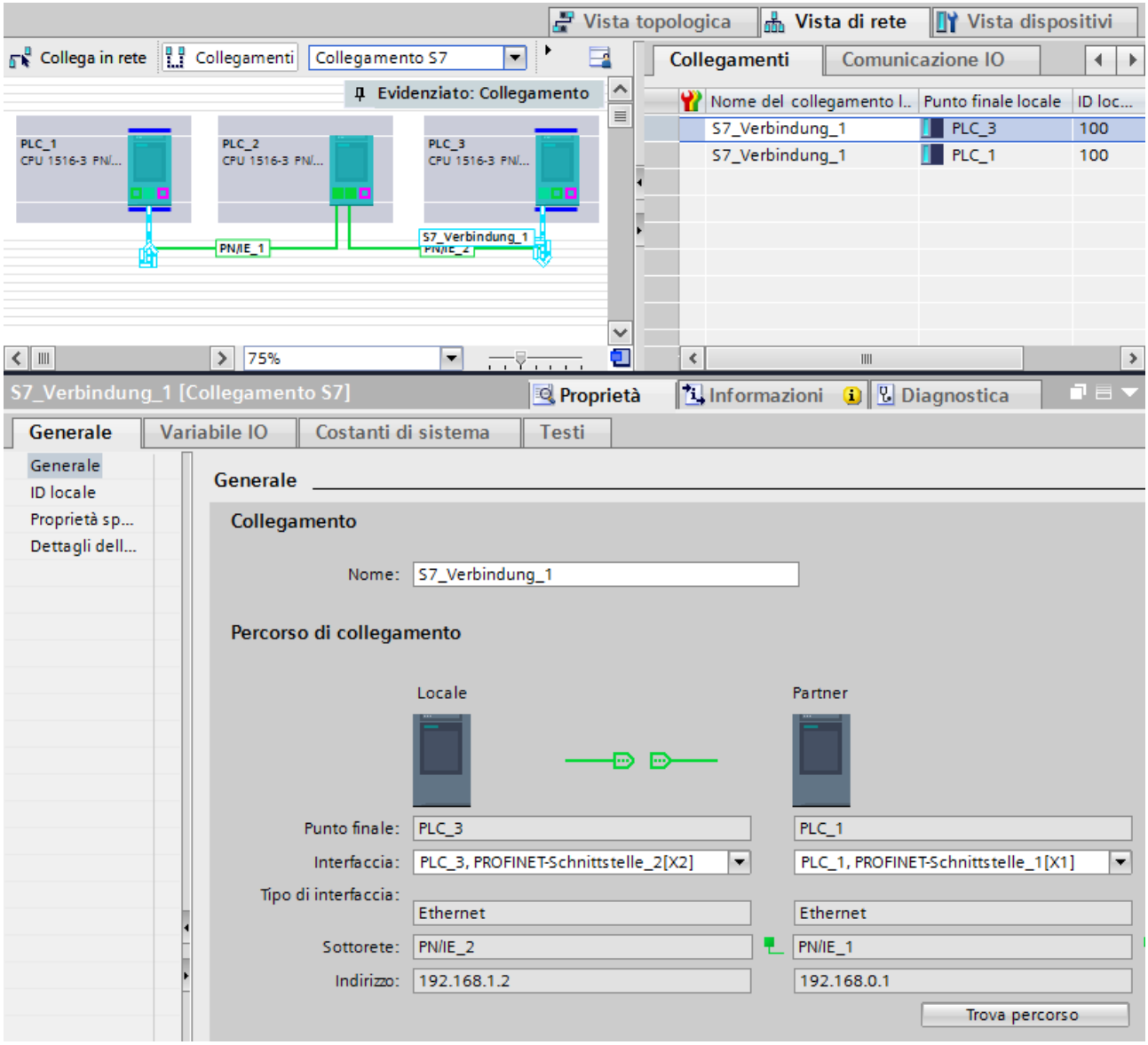


Figura 9-4 Collegamenti S7 tramite diverse sottoreti

ET 200SP Open Controller come router per collegamenti S7

Se si assegna l'interfaccia "PROFINET onboard [X2]" della CPU 1515SP PC (F) alla stazione SIMATIC PC, è possibile utilizzare la CPU 1515SP PC (F) come router per collegamenti S7. Se si utilizza l'interfaccia del CP per "Nessuna impostazione o un'altra impostazione Windows", non è possibile utilizzare l'Open Controller come router per i collegamenti S7 con routing.

Un collegamento S7 esistente con routing tramite CPU 1515SP PC (F) non è più valido se l'assegnazione dell'interfaccia della CPU 1515SP PC (F) viene modificata da "Stazione SIMATIC PC" a "Nessuna applicazione o un'altra applicazione Windows". Poiché il PLC non svolge più la funzione di router per questo collegamento, durante la compilazione della CPU 1515SP PC (F) non viene visualizzato alcun riferimento al collegamento non valido. Il collegamento S7 con routing non valido viene visualizzato solo con la compilazione dei punti finali del collegamento.

Le interfacce necessarie per i collegamenti S7 con routing devono rimanere assegnate esplicitamente nella CPU 1515SP PC (F) . È possibile modificare l'assegnazione dell'interfaccia della CPU 1515SP PC (F) nelle proprietà alla voce"PROFINET onboard [X2] > Assegnazione interfaccia".

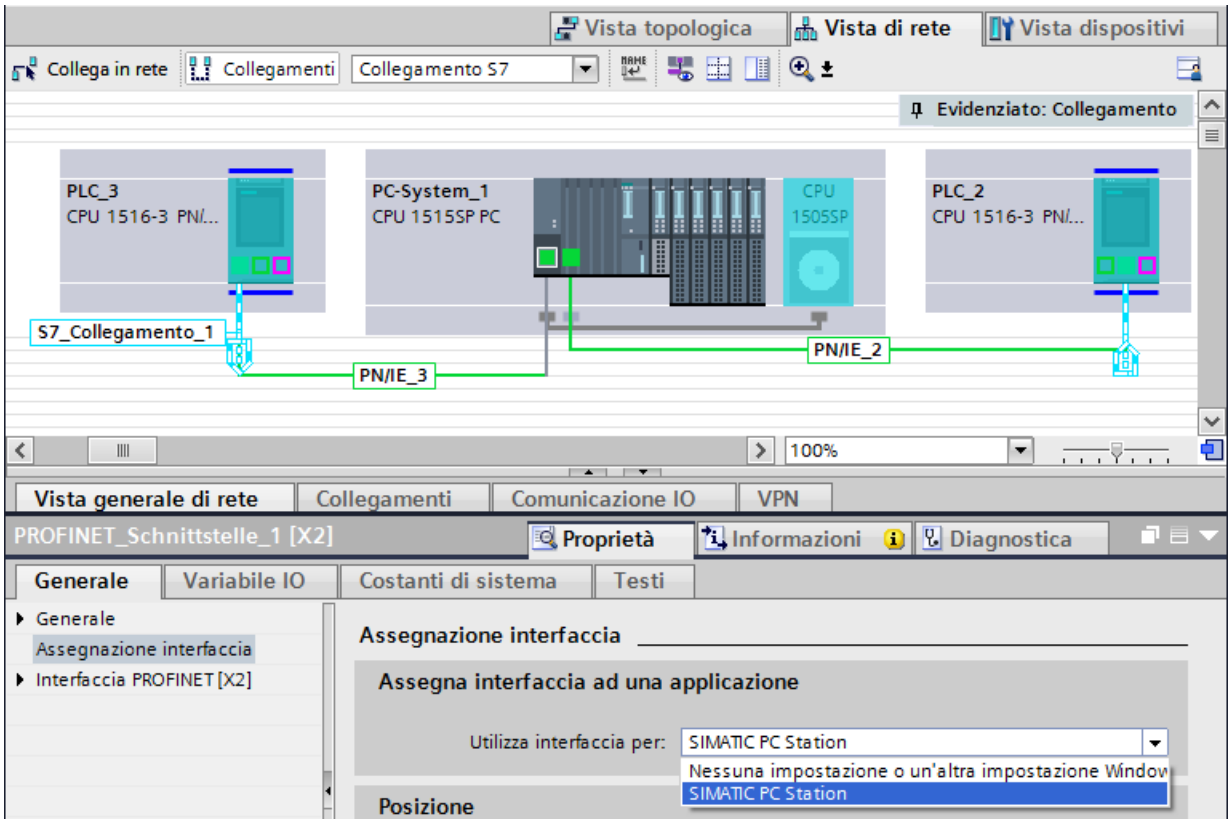


Figura 9-5 Routing S7 stazione PC

Ulteriori informazioni

Per informazioni più dettagliate sulla progettazione di collegamenti S7 e sull'utilizzo delle istruzioni per la comunicazione S7 nel programma utente consultare la Guida in linea di STEP 7.

Accoppiamento punto a punto 10

Funzionalità

La comunicazione tramite accoppiamento punto a punto nell'S7-1500, ET 200MP e ET 200SP avviene attraverso moduli di comunicazione (CM) con interfacce seriali (RS232, RS422 o RS485):

- S7-1500/ET 200MP:
  - CM PtP RS232 BA
  - CM PtP RS422/485 BA
  - CM PtP RS232 HF
  - CM PtP RS422/485 HF
- ET 200SP:
  - CM PtP

Lo scambio bidirezionale di dati tramite accoppiamento punto a punto funziona tra moduli di comunicazione o sistemi/dispositivi di terzi che supportano funzioni di comunicazione. Per la comunicazione sono necessari almeno 2 partner di comunicazione ("punto a punto"). Con RS422 e RS485 sono possibili più di due partner di comunicazione.

Protocolli per la comunicazione tramite accoppiamento punto a punto

- Protocollo Freeport (denominato anche protocollo ASCII)
- Procedura 3964(R)
- Protocollo Modbus nel formato RTU (RTU: Remote Terminal Unit)
- Protocollo USS (protocollo di interfaccia seriale universale)

I protocolli utilizzano diversi livelli secondo il modello di riferimento ISO/OSI:

- Freeport: utilizza il livello 1 (livello fisico)
- 3964 (R), USS e Modbus: utilizzano il livello 1 e 2 (livello fisico e livello di linea; quindi maggiore sicurezza nella trasmissione rispetto al Freeport). USS e Modbus utilizzano inoltre il livello 4.

Proprietà del protocollo Freeport

- Il destinatario riconosce la fine della trasmissione dei dati attraverso un criterio di fine parametrizzabile (ad es. decorso il tempo di ritardo caratteri, ricezione dei caratteri finali, ricezione di un numero fisso di dati).
- Il mittente non ha modo di vedere se i dati inviati sono arrivati correttamente al destinatario.

Proprietà della procedura 3964 (R)

- Durante l'invio vengono aggiunti ai dati dei caratteri di controllo (caratteri di inizio, fine e di controllo blocco) che però non sono disponibili come dati nel telegramma.
- Con questi caratteri si crea e interrompe un collegamento.
- In caso di errori di trasmissione la trasmissione dei dati viene automaticamente ripetuta.

Scambio di dati tramite comunicazione Freeport o 3964 (R)

I dati di invio vengono salvati nel programma utente della rispettiva CPU nei blocchi dati (buffer di invio). Per i dati di ricezione è disponibile, nel modulo di comunicazione, un buffer di ricezione. Controllare ed eventualmente adeguare le proprietà del buffer di ricezione. Nella CPU è necessario creare un blocco dati per la ricezione.

Nel programma utente della CPU le istruzioni "Send_P2P" e "Receive_P2P" comandano il trasferimento dei dati tra CPU e CM.

Procedura di configurazione della comunicazione Freeport o 3964 (R)

1. Nella vista dispositivi dell'editor hardware e di rete di STEP 7 progettare una configurazione per l'S7-1500 con CPU e CM.
2. Selezionare l'interfaccia del CM nella vista dispositivi di STEP 7.
3. Parametrizzare l'interfaccia (ad es. comunicazione finale, configurazione della trasmissione dei messaggi) nella finestra di ispezione di STEP 7 in "Proprietà > Generale".
4. Nella task card "Istruzioni" selezionare "Comunicazione > Processore di comunicazione" e le istruzioni "Send_P2P" e "Receive_P2P" e trascinarle con drag&drop nel programma utente (ad es. in un FB).
5. Parametrizzare le istruzioni in base alle preimpostazioni effettuate.
6. Caricare la configurazione hardware e il programma utente nella CPU.

Alternativa: parametrizzazione dinamica del modulo di comunicazione

In determinate aree di applicazione è utile configurare la comunicazione in modo dinamico, vale a dire comandata dal programma tramite un'applicazione specifica.

Casi applicativi tipici sono ad es. quelli dei costruttori di macchine in serie. Per offrire ai propri clienti superfici operative il più semplici possibile, questi costruttori adattano i servizi di comunicazione ai rispettivi input di comando.

Istruzioni per la comunicazione Freeport

Per la comunicazione Freeport sono disponibili 3 istruzioni per la progettazione dinamica nel programma utente. Per tutte e 3 queste istruzioni vale: i dati di configurazione finora validi vengono sovrascritti ma non salvati in modo permanente nel sistema di destinazione.

- L'istruzione "Port_Config" consente la configurazione comandata dal programma della rispettiva porta del modulo di comunicazione.
- L'istruzione "Send_Config" consente la progettazione dinamica ad es. di intervalli temporali e pause durante la trasmissione (parametri di trasmissione seriali) per la rispettiva porta.
- L'istruzione "Receive_Config" consente la progettazione dinamica ad es. di condizioni di inizio e fine di un messaggio da trasmettere (parametri di ricezione seriali) per la rispettiva porta.

Istruzioni per la comunicazione 3964 (R)

Per la comunicazione 3964(R) sono disponibili 2 istruzioni per la progettazione dinamica nel programma utente. Per le istruzioni vale quanto segue: i dati di configurazione finora validi vengono sovrascritti ma non salvati in modo permanente nel sistema di destinazione.

- L'istruzione "Port_Config" consente la configurazione comandata dal programma della rispettiva porta del modulo di comunicazione.
- L'istruzione "P3964_Config" consente la progettazione dinamica dei parametri di protocollo.

Proprietà del protocollo USS

- Semplice protocollo di trasmissione dati seriale con traffico di telegrammi ciclico nel funzionamento half duplex, creato per soddisfare le esigenze della tecnologia di azionamento.
- La trasmissione dei dati funziona secondo il principio master-slave.
  - Il master ha accesso alle funzioni dell'azionamento e può anche controllare l'azionamento, leggere i valori di stato e leggere o scrivere i parametri dell'azionamento.

Scambio di dati tramite la comunicazione USS

Il modulo di comunicazione è il master. Il master invia continuamente telegrammi ad un massimo di 16 azionamenti (telegrammi d'ordine) e attende un telegramma di risposta da ciascuno degli azionamenti indirizzati.

L'azionamento invia un telegramma di risposta nei seguenti casi:

- Se è stato ricevuto correttamente un telegramma
- Se in questo telegramma è stato indirizzato l'azionamento

Un azionamento non deve rispondere se queste condizioni non sono soddisfatte o se è stato indirizzato in broadcast.

Il master considera attivo il collegamento con un azionamento se dopo un determinato tempo di elaborazione (tempo di ritardo risposta) riceve un telegramma di risposta dall'azionamento.

Procedura di configurazione della comunicazione USS

1. Nella vista dispositivi dell'editor hardware e di rete di STEP 7 progettare una configurazione per l'S7-1500 con CPU e CM.
2. Nella navigazione del progetto selezionare per la CPU la cartella "Blocchi di programma" in cui aprire l'OB 1 con un doppio clic. Si apre l'editor di programma.
3. Nella task card "Istruzioni", area "Comunicazione", cartella "Processore di comunicazione" selezionare le istruzioni per la comunicazione USS in funzione del compito e trascinarle per drag&drop in un segmento dell'OB 1.
   - L'istruzione "USS_Port_Scan" consente la comunicazione attraverso la rete USS.
   - L'istruzione "USS_Drive_Control" predispone i dati di invio per l'azionamento e ne valuta i dati di risposta.
   - L'istruzione "USS_Read_Param" consente la lettura dei parametri dell'azionamento.
   - L'istruzione "USS_Write_Param" consente la modifica dei parametri dell'azionamento.
4. Parametrizzare le istruzioni in base alle preimpostazioni effettuate.
5. Caricare la configurazione hardware e il programma utente nella CPU.

Proprietà del protocollo Modbus (RTU)

- La comunicazione si svolge tramite trasmissioni asincrone seriali con una velocità di 115,2 kbit/s max., in funzionamento half duplex.
- La trasmissione dei dati funziona secondo il principio master-slave.
- Il master Modbus può inviare ordini allo slave Modbus per la lettura e scrittura di operandi:
  - Lettura di ingressi, temporizzatori, contatori, uscite, merker, blocchi dati
  - Scrittura di uscite, merker, blocchi dati
- Broadcast a tutti gli slave possibile.

Scambio di dati tramite comunicazione Modbus (RTU)

Il modulo di comunicazione può essere sia master Modbus che slave Modbus. Un master Modbus può comunicare con uno o più slave Modbus (il numero dipende dalla fisica dell'interfaccia). Solo lo slave Modbus indirizzato esplicitamente dal master Modbus può rinviare i dati al master Modbus. Lo slave riconosce la fine della trasmissione dei dati e la conferma. In caso di errore fornisce al master un codice di errore.

Procedura di configurazione della comunicazione Modbus (RTU)

1. Nella vista dispositivi dell'editor hardware e di rete di STEP 7 progettare una configurazione per l'S7-1500 con CPU e CM.
2. Nella navigazione del progetto selezionare per la CPU la cartella "Blocchi di programma" in cui aprire l'OB 1 con un doppio clic. Si apre l'editor di programma.
3. Nella task card "Istruzioni", area "Comunicazione", cartella "Processore di comunicazione" selezionare le istruzioni per la comunicazione Modbus in funzione del compito e trascinarle per drag&drop in un segmento dell'OB 1.
   - L'istruzione "Modbus_Comm_Load" consente di configurare la porta del CM per la comunicazione Modbus.
   - L'istruzione "Modbus_Master" viene utilizzata per la funzionalità del master Modbus.
   - L'istruzione "Modbus_Slave" viene utilizzata per la funzionalità dello slave Modbus.
4. Parametrizzare le istruzioni in base alle preimpostazioni effettuate.
5. Caricare la configurazione hardware e il programma utente nella CPU.

Ulteriori informazioni

- Per maggiori informazioni sulla comunicazione tramite accoppiamento punto a punto e le nozioni di base sulla trasmissione di dati seriale consultare il manuale di guida alle funzioni CM PtP - Configurazioni di accoppiamenti punto a punto (https://support.industry.siemens.com/cs/it/it/view/59057093).
- La descrizione delle modalità di utilizzo delle istruzioni citate per l'accoppiamento punto a punto nel programma utente è disponibile nella Guida in linea a STEP 7.
- Informazioni sui moduli di comunicazione con interfaccia seriale sono riportate nel rispettivo manuale del prodotto del modulo di comunicazione.

Comunicazione OPC UA 11

11.1 Informazioni utili su OPC UA

11.1.1 OPC UA e industria 4.0

Standard uniforme per lo scambio delle informazioni e dei dati

Industria 4.0 significa utilizzo intensivo, valutazione e analisi dei numerosi dati della produzione nei sistemi IT del livello aziendale. Con Industria 4.0 lo scambio dei dati tra il livello di produzione e il livello aziendale è destinato a subire un notevole incremento. Uno dei requisiti necessari per la sua riuscita è l'impiego di uno standard uniforme per lo scambio delle informazioni e dei dati.

OPC in versione classica è eseguibile solo sui sistemi operativi Windows. Per ovviare questa restrizione OPC Foundation ha sviluppato lo standard OPC UA (OPC Unified Architecture).

Lo standard OPC UA è particolarmente indicato per lo scambio di dati multilivello grazie alla possibilità di impiego in tutti i sistemi operativi, al procedimento di trasmissione sicuro e alla descrizione semantica dei dati. In questo modo è possibile trasmettere anche dati macchina (grandezze di regolazione, valori di misura o parametri).

La componente più importante di questo concetto è la possibilità di eseguire la comunicazione OPC UA parallelamente alla comunicazione realtime per la trasmissione dei dati a criticità di tempo in prossimità della macchina.

OPC UA presenta una funzione di scala molto elevata rendendo possibile uno scambio di informazioni continuo tra sensori, controllori e sistemi di misura o ERP.

OPC UA non mette a disposizione solo i dati, ma anche informazioni sui dati (ad es. tipi di dati, tipi di oggetti), rendendo possibile un accesso ai dati interpretabile dalle macchine.

Pagina degli argomenti OPC UA

Una panoramica dei contenuti di maggiore rilievo e dei link sull'argomento OPC UA si trovano nel Siemens Industry Online Support.

Pagina degli argomenti OPC UA
(https://support.industry.siemens.com/cs/ww/it/view/109770435)

11.1.2 Proprietà generali di OPC UA

OPC UA e PROFINET

OPC UA e PROFINET possono essere utilizzati insieme. Entrambi i protocollo utilizzano la stessa infrastruttura di rete.

Utilizzo in tutti i sistemi operativi

Lo standard OPC UA è indipendente dalla piattaforma e utilizza un protocollo binario ottimizzato basato su TCP per garantire applicazioni high-performance.

OPC UA può ad es. essere utilizzato in Windows, Linux, Mac OS X, un sistema realtime o un sistema operativo mobile (Android o iOS).

Indipendenza da un preciso livello di trasporto

OPC UA utilizza attualmente i seguenti meccanismi di trasporto e protocolli:

- Trasmissione di messaggi come corrente binaria direttamente attraverso TCP/IP.
- Trasmissione di messaggi con XML tramite TCP/IP e HTTP. Poiché consente una trasmissione piuttosto lenta, questo meccanismo viene utilizzato raramente e non è supportato dalle CPU S7-1500.

Tutte le applicazioni OPC UA supportano lo scambio binario dei dati (prescritto dalla specifica OPC UA).

Semplice principio client-server

Un server OPC UA mette a disposizione numerose informazioni all'interno di una rete, ad es. sulla CPU, sul server OPC UA stesso, sui dati e sui tipi di dati. Un client OPC UA richiama queste informazioni.

Realizzazione in diversi linguaggi di programmazione

La OPC Foundation ha implementato lo standard OPC UA in diversi linguaggi di programmazione: Sono disponibili stack per .NET, ANSI C e Java, anche se gli stack per ANSI C e Java non sono più sottoposti a manutenzione.

La OPC Foundation offre lo stack .NET e programmi di esempio come software open source. Vedere GitHub (https://github.com/opcfoundation).

Diverse aziende offrono Software Development Kits (SDK). Questi pacchetti di sviluppo contengono stack della OPC Foundation e altre funzioni che facilitano lo sviluppo di soluzioni.

Vantaggio degli SDK:

- Assistenza del fornitore
- Software testato
- Documentazione completa
- Condizioni di licenza chiare (è importante per poter rivendere le soluzioni)

Scalabilità

OPC UA può essere utilizzato in dispositivi di diverse classi di potenza:

- Sensori
- Sistemi integrati
- Controllori
- Sistemi PC
- Smartphone
- Server sul quale funzionano le applicazioni MES o ERP.

La classe di potenza dei dispositivi viene differenziata dai profili. Diversi profili offrono la possibilità di adattare OPC UA dai dispositivi più piccoli e semplici a quelli molto più potenti.

Un profilo OPC UA descrive funzioni e servizi che devono essere supportati dal server e dal client. Inoltre è possibile fornire opzionalmente ulteriori funzioni/servizi non richiesti dal profilo.

I profili OPC UA si differenziano dai profili PROFINET, questi ultimi definiscono i tipi di comportamento e le proprietà supplementari per dispositivi e sistemi estese a tutti i produttori con l'obiettivo di impiego di un'interfaccia software uguale per ogni costruttore.

Nano Embedded Device 2017 Server Profile

Per i dispositivi più piccoli con funzionalità molto limitata esiste il "Nano Embedded Device 2017 Server Profile" della OPC Foundation. La funzionalità di questo profilo corrisponde a Core Server Facette e definisce il protocollo OPC UA TCP come profilo di trasporto necessario. Il profilo consente collegamenti senza UA Security, nessuna Subscription e richiami di metodo. Il supporto degli oggetti e delle variabili di diagnostica è opzionale per questo profilo.

Ulteriori profili realizzano il "Nano Embedded Device 2017 Server Profile", richiedono più risorse e offrono più funzionalità.

Micro Embedded Device 2017 Server Profile

Questo profilo offre funzionalità limitata, richiede almeno due collegamenti paralleli, Subscription/monitoraggio dati supplementari, ma non UA Security e richiami di metodo.

- I Basic Controller S7-1200 supportano il "Micro Embedded Device 2017 Server Profile"; inoltre l'S7-1200 supporta l'UA Security.

Embedded 2017 UA Server Profile

Questo profilo è stato sviluppato per i dispositivi con più di 50 MB di memoria di lavoro e un processore potente. Questo profilo è basato sul profilo Micro Embedded Device Server. Inoltre richiede UA Security e richiami di metodo.

Inoltre i server devono rendere disponibile il modello di tipo utilizzato (tipi di dati, tipi di riferimenti, tipi di variabili, ...).

- Advanced Controller S7-1500 supportano "Embedded 2017 UA Server Profile".

Profili standard e Global Discovery

La "OPC UA Specification Part 7" definisce ulteriori profili:

- "Standard 2017 UA Server Profile", idoneo per i server OPC UA basati su PC
- 2 profili globali, "Global Discovery Server 2017 Profile" e "Global Discovery and Certificate Management 2017 Server Profile" che supportano i modelli service e di informazioni necessari di un server Global Discovery

Concetto tipo-istanza

OPC UA offre un modello di informazioni orientato all'oggetto integralmente collegato in rete (full-meshed-network) per spazi dei nomi, inclusi i metadati per la descrizione dell'oggetto. Tramite il riferimento delle istanze tra loro e i relativi tipi possono essere generate strutture di dati qualsiasi. Poiché il server rileva il sistema di istanze e di tipo, i client possono navigare tramite questa rete e ottenere tutte le informazioni necessarie. Sia le istanze che le definizioni del tipo corrispondente sono disponibili durante l'esecuzione.

Procedimenti o concetti su come gestire i riferimenti ai tipi saranno ottimizzati nel corso del tempo. Queste ottimizzazioni portano a nuove versioni della specifica OPC UA (es. V1.03 => V1.04).

Rappresentazione delle variabili PLC

Le informazioni del server OPC UA (ad es. le variabili PLC) sono strutturate come nodi (node) collegati tra loro mediante riferimenti. La semantica viene visualizzata dal server nell'area di indirizzi e può essere rilevata dai client (durante la navigazione). In questo modo è possibile spostarsi da un nodo all'altro con un client OPC UA e sapere quali contenuti si possono leggere, controllare o scrivere.

Meccanismi di sicurezza integrati

OPC UA utilizza meccanismi di sicurezza a diversi livelli:

- È possibile creare un collegamento sicuro tra un server OPC UA e un client OPC UA solo se entrambi i sistemi sono in grado di comunicare la propria identità mediante certificati X.509-v3 e di riconoscere i rispettivi certificati (sicurezza a livello dell'applicazione). Tra server e client sono possibili diverse Security Policy, anche un collegamento non sicuro (Security Policy: “None”).
- Per consentire l'accesso autorizzato (autenticazione) il server in linea generale può richiedere all'utente le seguenti informazioni:

  - un certificato utente (non progettabile in STEP 7)

  - il nome utente e la password

  - nessuna legittimazione dell'utente

I meccanismi di sicurezza sono opzionali e configurabili.

Ulteriori informazioni

Ulteriori informazioni sono disponibili nella pagina Internet della OPC Foundation (https://opcfoundation.org).

11.1.3 OPC UA nelle CPU S7-1200/S7-1500

In OPC UA un sistema funge da server e fornisce ad altri sistemi (i client) le informazioni disponibili.

I client OPC UA accedono ad es. in lettura e in scrittura ai dati del server OPC UA e richiamano dei metodi nel server OPC UA.

È possibile accedere online a questi dati con un client, anche ad es. a informazioni relative a rendimento e diagnostica. Normalmente in OPC UA questa funzione è denominata "Browsen". La funzione "Subscription" evita che una variabile venga letta regolarmente: il client viene informato dal server in merito alle variazioni del valore.

Un sistema può funzionare contemporaneamente come client e come server.

Server OPC UA della CPU S7-1500

A partire dal firmware 2.0 le CPU S7-1500 dispongono di un server OPC UA.

I capitoli che seguono spiegano come configurare il server OPC UA della CPU S7-1500 e predisporre i dati e i metodi per i client OPC UA, in modo che i client possano accedere in scrittura e in lettura alle variabili PLC e richiamare i metodi nel server.

I prossimi capitoli spiegano inoltre come integrare le specifiche Companion nell'area degli indirizzi del server OPC UA.

Server OPC UA della CPU S7-1200

A partire dal firmware V4.4 le CPU S7-1200 dispongono di un server OPC UA.

Sostanzialmente il server OPC UA è configurato come una CPU S7-1500, la gamma delle funzioni e le risorse sono limitate a seconda del profilo "Micro Embedded Device 2017 Server Profile" supportato. Diversamente dalla CPU S7-1500 le funzioni "Registered Read" e "Registered Write" **non** sono quindi disponibili.

A partire dal firmware V4.5 le CPU S7-1200 supportano sia i metodi server che i tipi di dati strutturati (strutture e array).

Maggiori informazioni sono disponibili nella Guida in linea a STEP 7.

Client OPC UA delle CPU S7-1500

Dal firmware V2.6 le CPU S7-1500 dispongono anche di un client OPC UA.

I prossimi capitoli spiegano come utilizzare le istruzioni standardizzate (blocchi funzionali PLCopen) per creare un programma utente che predisponga le seguenti funzioni come client OPC UA.

- Lettura di dati da un server OPC UA
- Scrittura di dati a un server OPC UA
- Richiamo di metodi di un server OPC UA

STEP 7 (TIA Portal) facilita la creazione dei programmi utente mettendo a disposizione un editor per interfacce client e funzioni per la configurazione dei collegamenti OPC UA.

Le istruzioni OPC UA per le CPU S7-1500 con funzione di client sono descritte in dettaglio nella Guida (Istruzioni > Comunicazione > OPC UA).

Client OPC UA a scopo di test

Per spiegare come si impiegano i client OPC UA la presente descrizione si serve di client diversi:

- "UaExpert" di Unified Automation. Un client completo che può essere utilizzato gratuitamente:
  Link al download di UaExpert (https://www.unified-automation.com/downloads/opc-ua-clients.html)
- "UA Sample Client" della OPC Foundation. Questo client è gratuito per gli utenti registrati alla OPC Foundation :
  link al download del client di esempio della OPC Foundation (https://opcfoundation.org)

Esempio applicativo nell'Industry Online Support

Siemens Industry Online Support mette a disposizione, per di diversi casi applicativi, un esempio gratuito con un'API client. La funzione di quest'interfaccia consente la creazione di client OPC UA personalizzati adeguati al proprio caso applicativo. Per facilitare l'uso dell'API, SIEMENS mette a disposizione una classe .NET helper sovraordinata.

L'API client si basa sullo stack .NET OPC UA della OPC Foundation.

L'esempio applicativo è gratuito e spiega come creare i collegamenti tra server e client e come leggere e scrivere le variabili PLC.

Link per il download: OPC UA .NET Client per SIMATIC S7-1500 OPC UA Server (https://support.industry.siemens.com/cs/it/it/view/109737901)

11.1.4 Accesso alle applicazioni OPC UA

Di seguito sono descritte le possibilità di accesso che ha una CPU S7-1500 con una applicazione OPC UA (client o server) tramite un PC nella stessa stazione. Inoltre viene mostrato come queste possibilità di accesso possono essere combinate con la funzione "IP Forwarding" per accedere tramite una stazione S7-1500 a dispositivi di un'altra sottorete IP.

Tutte le impostazioni si raggiungono tramite le proprietà della CPU, area "Configurazione avanzata" nella finestra di ispezione

L'opzione di raggiungere l'applicazione OPC UA nella CPU tramite un'interfaccia PC OA è legata ai seguenti presupposti:

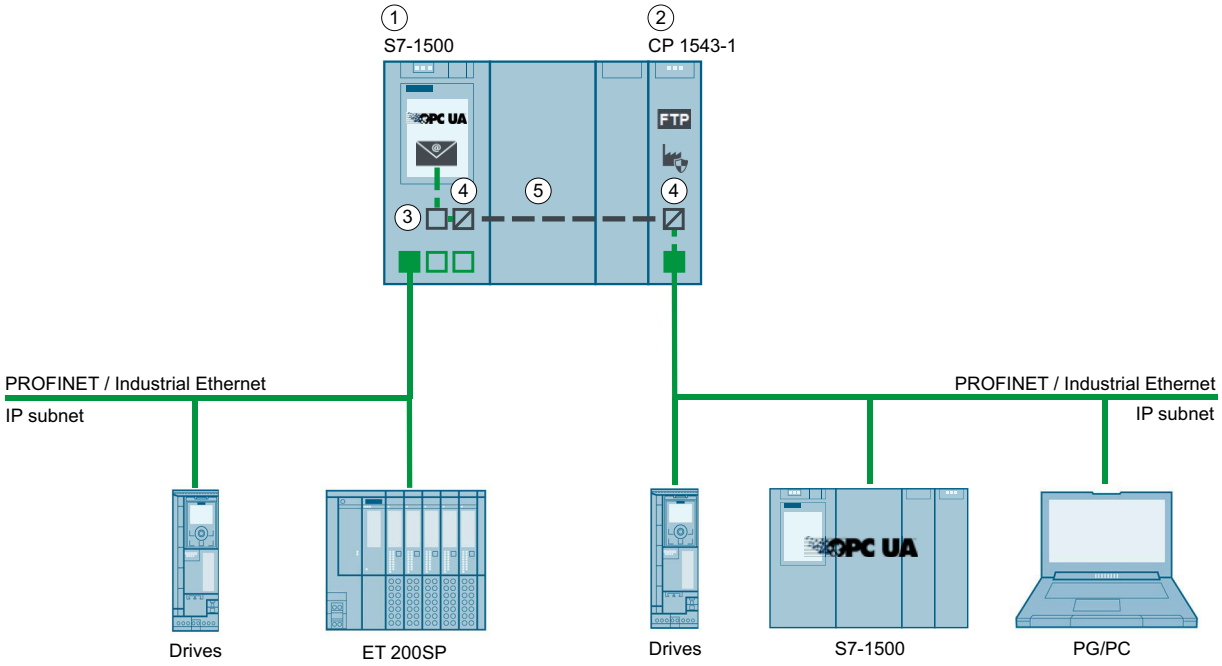
- CPU S7-1500 (Advanced Controller) dalla versione firmware V2.8, CPU S7-1500R/H dalla versione firmware V3.1
- CP 1543-1 dalla versione firmware V2.2

Suggerimento: Utilizzare un CP 1543-1 con firmware V3.0 o superiore. A partire da questa versione, le funzioni Security (firewall) sono disponibili anche per l'interfaccia virtuale (W1) rendendo superflua l'installazione di un firewall aggiuntivo tra la stazione e la rete non sicura.

Principio: interfaccia di accesso tramite modulo di comunicazione

Per accedere a un'applicazione CPU come OPC UA tramite un'interfaccia CP è necessario progettare un'interfaccia virtuale (W1). Tramite i parametri di indirizzo IP di questa interfaccia virtuale è possibile raggiungere applicazioni basate su IP.

Il principio è illustrato nella figura seguente:



① CPU S7-1500 versione firmare V2.8 o superiore (ad es. CPU 1515-2 PN)

② CP 1543-1 (versione firmare V2.2 o superiore)

③ Interfaccia virtuale (W1)

④ Conversione del protocollo PROFINET / Industrial Ethernet in bus backplane o del bus backplane in PROFINET / Industrial Ethernet

⑤ Bus backplane

Figura 11-1 Principio: Interfaccia di accesso tramite modulo di comunicazione

Esempio: Accesso da client OPC UA a server OPC UA della CPU

Per l'accesso di un client OPC UA al server OPC UA della CPU sono disponibili le seguenti interfacce della stazione S7-1500:

- Le interfacce locali PROFINET della CPU S7-1500
- L'interfaccia Ethernet di un CP 1543-1 (dalla versione firmware V2.2)

La seguente figura illustra un esempio delle configurazioni realizzabili. La CPU può anche svolgere il ruolo di client OPC UA e il dispositivo collegato alla sottorete del CP quello di server OPC UA.

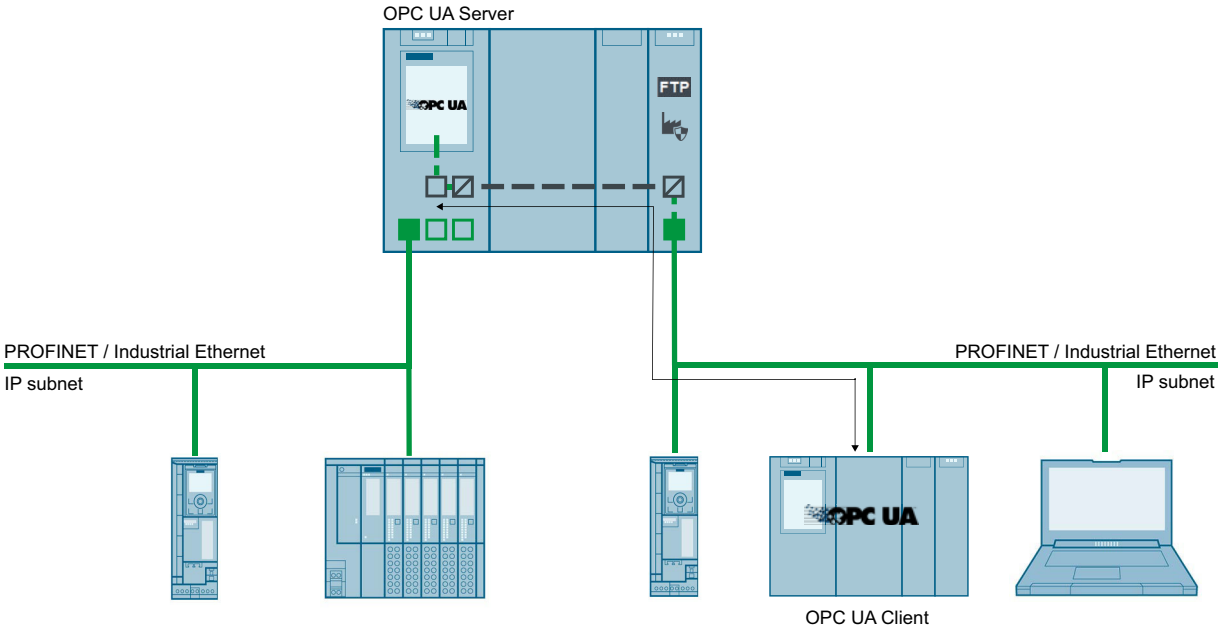


Figura 11-2 Esempio: Accesso da client OPC UA a server OPC UA della CPU

Esempio: Accesso di client OPC UA a server OPC UA tramite CPU S7-1500 con IP Forwarding attivato

Client OPC UA e server OPC UA possono anche essere collegati tra loro tramite una CPU S7-1500 dove la CPU S7-1500 funge da IP Forwarder. Questa possibilità di configurazione consente un ampliamento flessibile degli impianti esistenti.

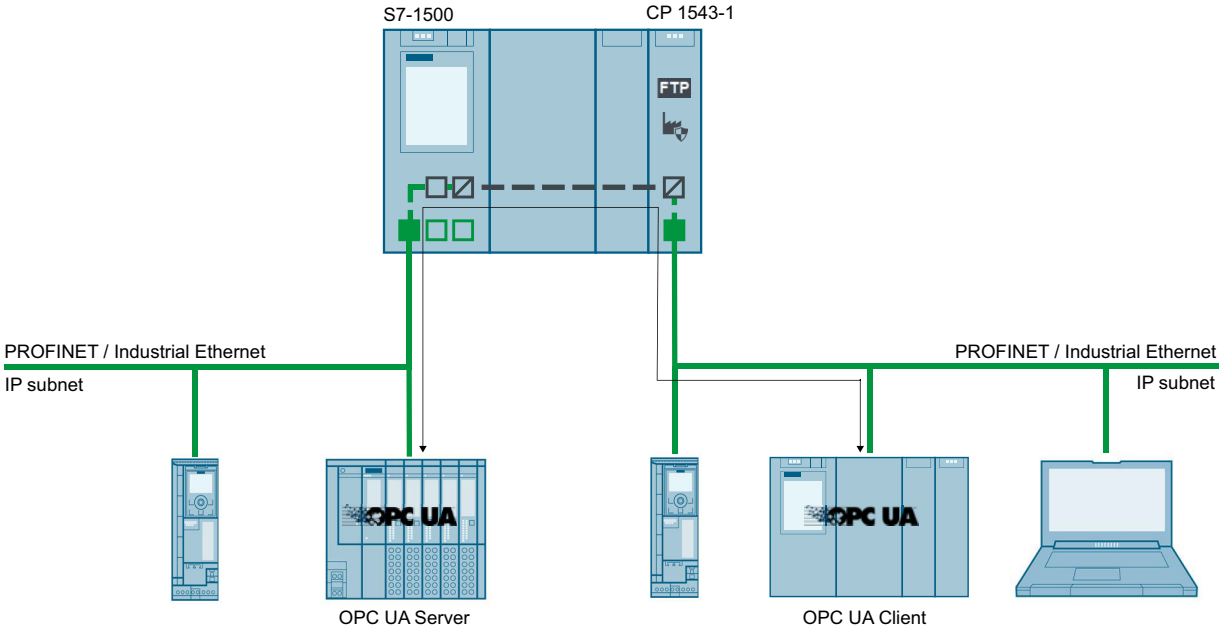


Figura 11-3 Esempio: Accesso di client OPC UA a server OPC UA tramite CPU S7-1500 con IP Forwarding attivato

Ulteriori informazioni

Ulteriori informazioni sulle modalità di accesso tramite l'interfaccia virtuale e IP Forwarding sono riportate nelle sezioni seguenti:

- IP Forwarding (Pagina 423)
- Interfaccia virtuale per applicazioni basate su IP (Pagina 432)

11.1.5 Indirizzamento dei nodi

I nodi (Nodes) costituiscono gli elementi di base di OPC UA, e sono equiparabili agli oggetti nella programmazione orientata agli oggetti. I nodi vengono utilizzati ad es. per i dati utili (variabili) o per altri metadati. Tramite nodi viene modellata un'area indirizzi OPC UA contenente anche un modello con definizioni del tipo.

ID del nodo (NodeId)

I nodi nell'area degli indirizzi OPC UA vengono definiti in modo univoco da un NodeId (Node Identifier).

Il NodeId è costituito dall'Identifier, dall'Identifier Type e dall'indice per lo spazio dei nomi. Gli spazi per i nomi vengono utilizzati per evitare conflitti tra i nomi.

La OPC Foundation ha definito una serie di nodi che forniscono informazioni sul rispettivo server OPC UA. Questi nodi si trovano nello spazio dei nomi della OPC Foundation e hanno l'indice 0.

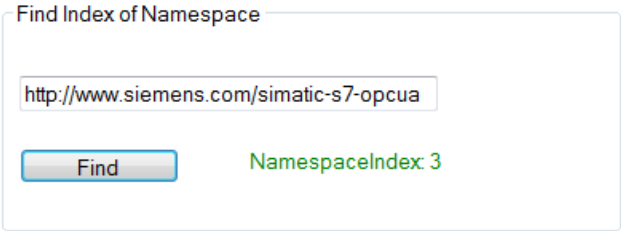
Inoltre la OPC Foundation ha definito tipi di dati e di variabili.

Spazio dei nomi (Namespace)

Oltre allo spazio dei nomi della OPC Foundation sopra descritto, merita interesse anche lo spazio dei nomi per l'accesso ai dati della CPU. Tutte le variabili e i metodi di un server S7-1500 OPC UA si trovano nello spazio dei nomi (Namespace) dell'interfaccia standard del server "http://www.siemens.com/simatic-s7-opcua".

Lo spazio dei nomi ha per default l'indice 3. Se sul server vengono inseriti ulteriori spazi per i nomi o se vengono cancellati spazi esistenti, l'indice può subire modifiche. È pertanto necessario che un Client OPC UA richieda al server l'indice aggiornato dello spazio del nome (ad es. "http://www.siemens.com/simatic-s7-opcua") prima di leggerne o scriverne i valori.

La seguente figura mostra un risultato esemplificativo di una tale richiesta.



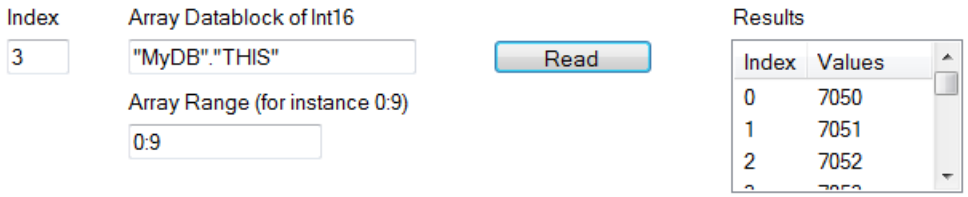
Identifier

L'Identifier corrisponde al nome delle variabili PLC tra virgolette. Le virgolette sono gli unici caratteri non consentiti per comporre i nomi in STEP 7. Le virgolette vengono utilizzate per evitare conflitti nei nomi.

L'esempio seguente legge il valore della variabile "StartTimer":

L'Identifier può essere formato da diversi componenti. I singoli componenti sono separati da un punto.

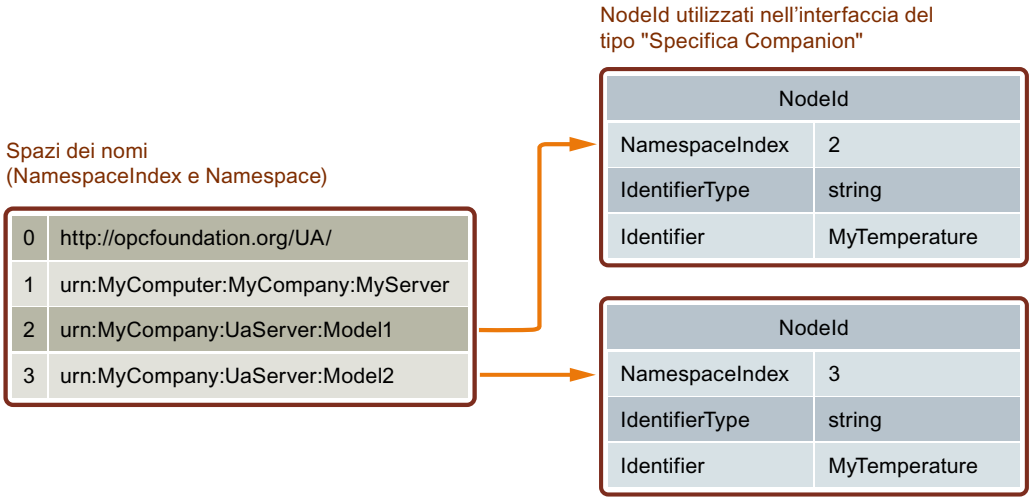
L'esempio seguente legge per intero il blocco dati array "MyDB". In questo blocco dati si trova un array con dieci valori integer. I dieci i valori devono essere letti tutti insieme. Perciò nell'array è inserito il range "0:9":



Esempio di NodeId, ID e spazi dei nomi

La seguente figura illustra la relazione tra NodeId, ID e spazi dei nomi: Non costituisce un problema se due nodi hanno lo stesso ID ma fanno parte di spazi dei nomi diversi.

STEP 7 (TIA Portal) prevede una procedura semplice per l'importazione di spazi dei nomi tramite un'interfaccia del server.



Variabili PLC nell'area di indirizzi del server OPC UA

La seguente figura mostra dove si trovano le variabili PLC dell'esempio nell'area di indirizzi del server OPC UA (dettaglio del client UA):

Il blocco dati "MyDB" è un blocco dati globale. Si trova quindi sotto il nodo "DataBlocksGlobal". "StartTimer" è una variabile merker e compare quindi sotto il nodo "Memory".

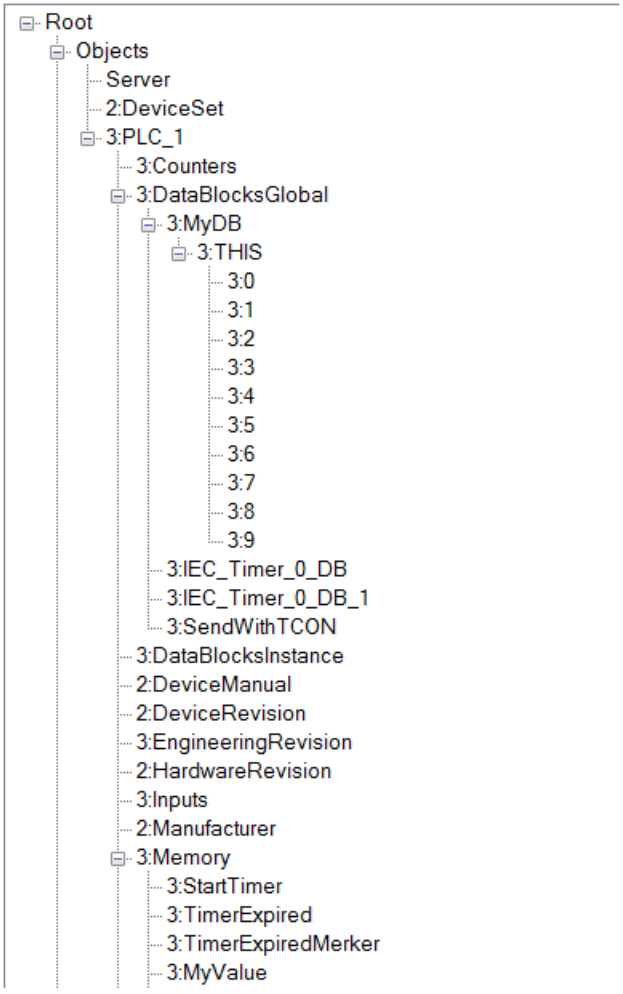


Figura 11-4 variabili PLC nell'area di indirizzi del server OPC UA

Metodi nell'area di indirizzi del server OPC UA

I metodi implementati con il programma utente vengono visualizzati nel seguente modo nell'area di indirizzi del server OPC UA

(vedere Come mettere a disposizione i metodi del server OPC UA (Pagina 321)):

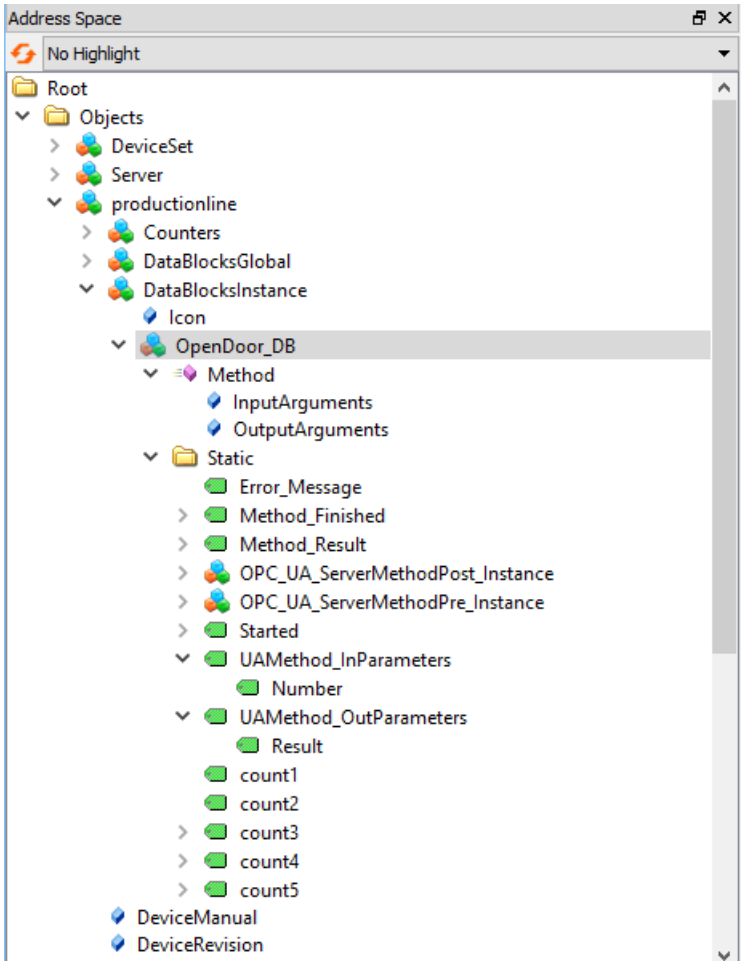


Figura 11-5 Metodi nell'area di indirizzi del server OPC UA

11.1.6 Vista generale dello spazio dei nomi per i server OPC UA delle CPU S7-1200/1500

Come già descritto all'argomento "Indirizzamento di nodi", l'indice dello spazio dei nomi fa parte degli ID dei nodi. Per garantire che l'ID di un nodo sia sempre univoco nello spazio degli indirizzi, OPC UA utilizza gli spazi dei nomi; il BrowseName come unico mezzo per identificare un nodo può essere ambiguo.

Gli spazi dei nomi sono definiti in OPC UA da diverse "Naming Authorities" che sviluppano modelli informativi OPC UA, ad es. un gruppo di lavoro, dalla Fondazione OPC o da organizzazioni che sviluppano modelli informativi standard.

Gli spazi dei nomi sono identificati da un URI dello spazio dei nomi; l'URI dello spazio dei nomi identifica la Naming Authority.

Per ottimizzare l'accesso ai nodi del server, al posto dell'URI dello spazio dei nomi viene utilizzato un indice dello spazio dei nomi. L'indice dello spazio dei nomi è un puntatore su un array dello spazio dei nomi che gestisce il server. Il client legge l'indice dello spazio dei nomi una volta dal server per accedere successivamente ai nodi del server con un semplice numero intero invece che con una stringa URI.

La tabella seguente contiene l'assegnazione tra gli URI degli spazi dei nomi e gli indici degli spazi dei nomi delle CPU S7-1500 e S7-1200.

Assegnazione tra URU dello spazio dei nomi e l'indice dello spazio dei nomi

Nelle CPU S7-1200 e S7-1500 gli indici degli spazi dei nomi sono assegnati in modo fisso per gli indici degli spazi dei nomi da 0 a 3. Attualmente non sono definiti altri indici di spazi dei nomi.

URI spazio dei nomi	Indice spazio dei nomi	Descrizione
http://opcfoundation.org/UA/	0	Namespace per i KnSoten-ID e i BrowseNames della specifica OPC UA (OPC 10000-3). **Esempio** 0:EngineeringUnits
Local Server URI ("urn:" + nome applicazione come progettato in TIA Portal (area "OPC UA > Generale" nelle proprietà CPU))	1	Spazi dei nomi per nodi definiti nel server locale (OPC 10000-5). **Esempio** urn:SIMATIC.S7-1500.OPC-UA.Application:PLC_1
http://opcfoundation.org/UA/DI/	2	Namespace per gli ID dei nodi e gli BrowseNames della specifica OPC UA per i device (OPC 10000-100). **Esempio** 2:DeviceRevision
http://www.siemens.com/simatic-s7-opcua	3	Namespace per gli ID dei nodi e i BrowsName definiti in base al prodotto per una CPU S7-1200/S7-1500. In questo spazio dei nomi sono definite tutte le istanze (CPU, variabili, DB ...) nonché i relativi tipi (UDT, LDT, FB ...). **Esempio**

URI spazio dei nomi	Indice spazio dei nomi	Descrizione
		3:DataBlocksGlobal
URI di spazi dei nomi supplementari per ulteriori istanze e tipi **Esempi** http://machinesupplier.org/implementedPackML http://opcfoundation.org/UA/PackML	> 3	Non definito Possono essere definiti ad es. con SiOME. **Esempi** 4:MyPackMLMachineInstance 5:PackMLBaseObjectType

11.1.7 Informazioni utili sui client OPC UA

Nozioni di base sui client OPC UA

I client OPC UA sono programmi che:

- Accesso alle informazioni da un server OPC UA (ad es. una CPU S7-1500): in lettura, in scrittura, subscription.
- fanno eseguire dei metodi dal server OPC UA.

I client OPC UA possono tuttavia accedere solo ai dati che sono stati abilitati per tali operazioni (vedere "Gestione dei diritti di scrittura e lettura (Pagina 246)").

Per creare un collegamento a un server OPC UA è necessario conoscere il punto finale del server (vedere "Punti finali dei server OPC UA (Pagina 234)").

Lettura di informazioni dal server OPC UA

Quando è attivo un collegamento a un punto finale del server è possibile utilizzare le funzioni di navigazione del client. Da un determinato punto di partenza (dal nodo radice "Root") è possibile navigare nell’area indirizzi del server.

In questo modo si ottengono tra l'altro le seguenti informazioni:

- Variabili PLC, blocchi dati e componenti dei blocchi dati abilitati
- Indice dello spazio dei nomi e identificatori di tali variabili PLC, blocchi dati e componenti dei DB
- Tipi di dati delle variabili PLC e dei componenti dei DB
- Numero di componenti negli array (necessario per la lettura e la scrittura degli array)

Inoltre si ricevono informazioni sul server OPC UA stesso e informazioni sull'S7-1500 basate sullo standard "OPC UA for Devices" della OPC Foundation, ad es. numero di serie, versione firmware.

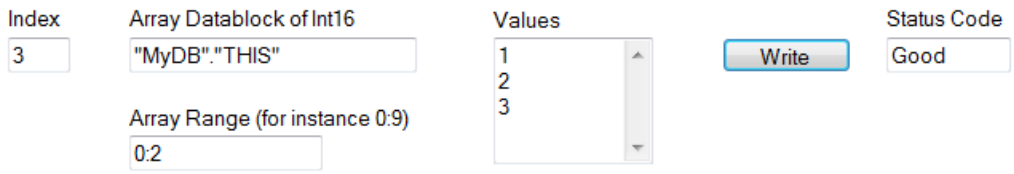
Lettura dei dati dal server e scrittura dei dati sul server

A questo punto si conoscono l'indice dello spazio dei nomi, l'identificatore e il tipo di dati delle variabili PLC. Ciò consente di leggere singolarmente le variabili PLC e i componenti dei DB o anche interi array e strutture.

Per degli esempi di lettura delle variabili booleane e dei blocchi dati array consultare Indirizzamento dei nodi (Pagina 189).

Le regole per l'accesso alle strutture sono descritte qui (Pagina 385).

Con le informazioni acquisite navigando nell'area indirizzi del server (indice, identificatore e tipo di dati) è possibile anche trasferire valori all'S7-1500 con il client OPC UA. Il seguente esempio sovrascrive i primi tre valori nel blocco dati array "MyDB".



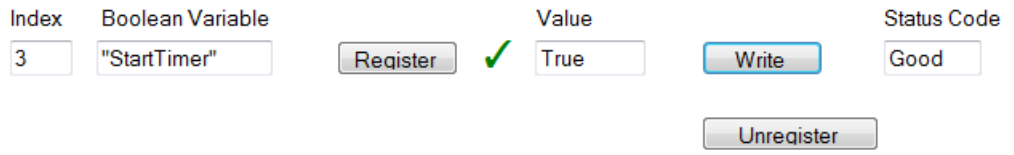
In "Array Range" si deve specificare quali componenti dell'array si vogliono sovrascrivere. Dal codice di stato "Good" è possibile vedere che i valori sono stati trasferiti correttamente. Tuttavia è possibile scrivere nell'S7-1500 solo i valori e non la relativa registrazione di data e ora. La data e l'ora possono essere solo lette.

Accesso rapido tramite registrazione

Registered Read/Write è disponibile per l'accesso ripetuto, ottimizzato ai dati, con le massime prestazioni. In caso di registrazione di nodi di variabili il server OPC UA crea un Identifier numerico (NodeId numerico) che rimanda direttamente al nodo registrato. In caso di ordini di lettura o di scrittura del client su questo Identifier numerico, il server non deve annullare alcuna stringa di caratteri come Identifier e può accedere in modo ottimizzato alla variabile richiesta.

Questo Identifier è valido esclusivamente per la sessione corrente e deve essere richiesto nuovamente in caso di interruzione/perdita della sessione.

Nell'esempio seguente è stata inizialmente registrata sul server solo la variabile "StartTimer". Successivamente, per l'impostazione del valore viene utilizzata la funzione veloce "RegisteredWrite".



Seguendo lo stesso schema è possibile utilizzare anche la funzione "RegisteredRead", utile in particolare se si devono leggere i dati in maniera ricorrente. Tuttavia tenere presente che, a seconda dell'applicazione, può essere utile utilizzare una Subscription.

Consiglio: inserire le registrazioni preferibilmente nel programma di avvio del client OPC UA, perché richiedono del tempo.

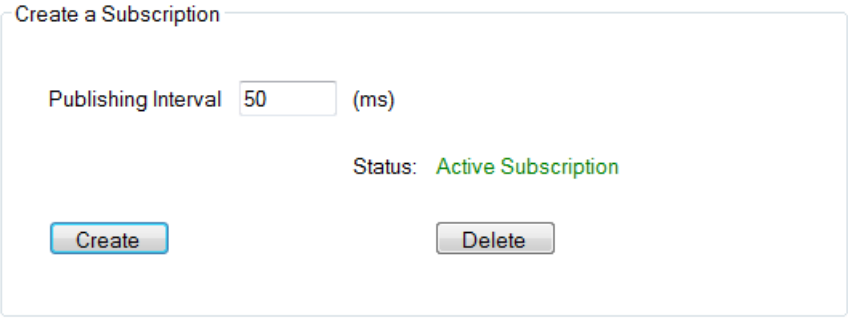
Nelle proprietà della CPU S7-1500 è possibile specificare il numero massimo di nodi registrati e i client devono tener conto del numero impostato, vedere Impostazioni generali del server OPC UA (Pagina 261).

Subscription

Con "Subscription" si definisce una funzione con la quale vengono trasmesse solamente le variabili per le quali un client OPC UA si è registrato nel server OPC UA. Per queste variabili registrate (elementi monitorati = monitored Items) il server OPC UA trasmette un messaggio al client OPC UA solo nel caso di una variazione di un valore. Controllando queste variabili si evitare che vengano interrogate di continuo dal client OPC UA (Polling) e si riduce il carico della rete.

Per utilizzare questa funzione è necessario creare una Subscription. Specificare l'intervallo di trasmissione ("Publishing Interval") in UaClient e fare clic sul pulsante "Create". L'intervallo di trasmissione è l'intervallo di tempo nel quale il server invia al client nuovi valori in un messaggio (data change notification).

Nell'esempio seguente è stata creata una sottoscrizione: Ogni 50 millisecondi il client riceve un messaggio con i nuovi valori (intervallo di trasmissione 50 ms).



Protezione del server dal sovraccarico

Il server OPC UA della CPU S7-1500 si può impostare con il parametro "Intervallo di trasmissione più breve" in modo che possa comandare gli intervalli di trasmissione desiderati dal client che non siano troppo corti; vedere Impostazioni del server per le sottoscrizioni (Pagina 263).

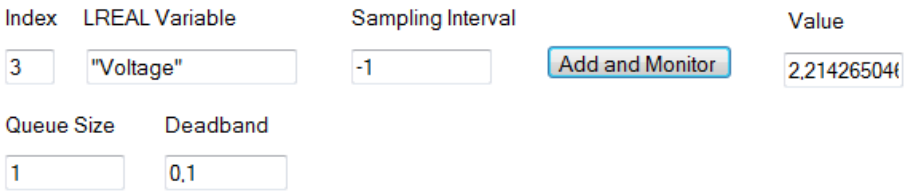
Esempio: Un client vuole ricevere i dati dal server a intervalli di 50 ms. Un intervallo di trasmissione così breve determinerebbe tuttavia un carico eccessivo sulla rete e sul server. L'utente imposta quindi per il server un "Intervallo di trasmissione più breve" pari a 1000 ms. I client che nella loro subscription richiedono intervalli più brevi vengono "rallentati" a 1000 ms in modo da proteggere il server dal sovraccarico.

Campionamento e Invio (Sampling & Publishing) nell'ambito di una subscription sono processi di comunicazione che, come altri processi di comunicazione (TCP/UDP/comunicazione con il web server ...) sono elaborati con priorità 15 dalla CPU. Gli OB con priorità superiore interrompono la comunicazione. Se si impostano intervalli di campionamento e invio troppo brevi, questa impostazione causa un notevole carico di comunicazione. Selezionare possibilmente grandi intervalli, sufficienti per l'applicazione.

Per informazioni sulla coerenza delle variabili, consultare la seguente sezione Coerenza delle variabili CPU (Pagina 251).

Controllo di variabili PLC

Dopo aver creato una Subscription è necessario comunicare al server quali variabili deve controllare. Nell'esempio seguente è stata aggiunta alla sottoscrizione (Subscription) la variabile "Voltage".



La variabile "Voltage" contiene ad es. il valore di una grandezza di tensione che viene rilevata da una CPU S7-1500.

L'intervallo di campionamento ("Sampling Interval") contiene un valore negativo (-1). Questo fa sì che venga utilizzata per l'intervallo di campionamento l'impostazione di default del server OPC UA. L'impostazione di default è determinata mediante l'intervallo di trasmissione ("Publishing Interval") della subscription. Per impostare l'intervallo di campionamento più piccolo possibile selezionare il valore "0".

In questo esempio la lunghezza della coda di attesa è impostata a "1": Un valore viene sempre letto dalla CPU e successivamente trasmesso al client OPC UA a intervalli di 50 millisecondi solo se è cambiato.

Il parametro "Deadband" (banda morta) nell'esempio è "0,1": le variazioni del valore devono essere di almeno 0,1 volt, solo allora il server trasmette il nuovo valore al client. Il server non trasmette variazioni del valore inferiori. Questo parametro consente ad es. di eliminare i rumori: variazioni minime di una grandezza di processo che non hanno un reale importanza.

11.2 Security in OPC UA

11.2.1 Impostazioni di sicurezza

Affrontare i rischi

OPC UA consente lo scambio di dati tra sistemi diversi, sia all'interno del livello di processo e di produzione sia con sistemi del livello di controllo e di gestione.

Questa opzione comporta anche rischi per la sicurezza. Per questo motivo OPC UA utilizza tutta una serie di meccanismi di sicurezza:

- Verifica dell'identità dei server e dei client OPC UA
- Verifica dell'identità degli utenti
- Scambio di dati firmati/crittografati tra server e client OPC UA.

Le impostazioni di security si devono bypassare solo in casi speciali ben precisi:

- durante la messa in servizio,
- nel caso di progetti isolati senza collegamento Ethernet verso l'esterno.

Se per "UA Sample Client" della OPC Foundation si sceglie ad es. il punto finale "None", il programma invia un avviso molto chiaro:

Warning: Selected Endpoint has no security.

Durante la compilazione del progetto STEP 7 controlla inoltre se sono state prese in considerazione le impostazioni di protezione e emette un'avvertenza in caso di rischio. In tali misure rientra anche una OPC UA Security Policy con l'impostazione "None"(senza sicurezza), che corrisponde al punto finale "None".

NOTA

Disattivazione delle Security Policy non necessarie

Se nelle impostazioni del Secure Channel del server OPC UA S7-1500 si sono attivate tutte le Security Policy e quindi anche il punto finale "None" (Senza sicurezza), il traffico dati tra il server e il client può avvenire anche in modo non sicuro (senza firma e crittografia). Il server OPC UA della CPU S7-1500 trasmette il proprio certificato pubblico al client anche se è stato selezionato "None" (nessuna sicurezza). E alcuni client controllano questo certificato. Tuttavia il client non è obbligato a trasmettere un certificato al server. L'identità del client rimane sconosciuta. Qualsiasi client OPC UA può collegarsi al server, indipendentemente dalle altre eventuali impostazioni di security effettuate successivamente.

Quando si progetta il server OPC UA è importante verificare che siano attive solo le Security Policy compatibili con il concetto di sicurezza della propria macchina o impianto. Tutte le altre Security Policy devono essere disattivate.

Consiglio: Utilizzare l'impostazione "Basic256Sha256 - Firma e crittografia" con la quale il server accetta solo certificati Sha256. Le Security Policy "Basic128Rsa15" e "Basic256" sono disattivate per default e non devono essere utilizzate come punto finale. Selezionare punti finali con una Security Policy superiore.

Altre regole di sicurezza

- Utilizzare il punto finale "None" solo in casi eccezionali.
- Utilizzare l'"autenticazione ospite" dell'utente solo in casi eccezionali.
- Consentire l'accesso alle variabili PLC e ai componenti dei DB da OPC UA solo se effettivamente necessario.
- Utilizzare gli elenchi dei client affidabili specificati nelle impostazioni del client OPC UA S7-1500 per consentire l'accesso solo a client particolari.

11.2.2 Certificati standard X.509 della ITU

In OPC UA sono integrati diversi meccanismi si sicurezza a diversi livelli. I certificati digitali hanno un ruolo importante. Un client OPC UA, ad es., può creare un collegamento sicuro con un server OPC UA solo se il server accetta il certificato digitale del client e lo considera attendibile.

Vedere il capitolo Handling dei certificati dei client e dei server (Pagina 267).

Inoltre anche il client deve verificare il certificato del server e considerarlo attendibile. Server e client devono dimostrare di essere chi sostengono di essere. Devono dimostrare la propria identità. L'autenticazione reciproca di client e server impedisce ad es. gli attacchi di tipo "Man in the Middle".

Attacchi da parte di un "Man in the Middle"

Tra server e client potrebbe trovarsi un "Man in the middle", un programma che intercetta la comunicazione tra server e client e che, sostenendo di essere esso stesso client o server, ottiene informazioni importanti sul programma S7, imposta valori nella CPU e può quindi attaccare una macchina o un impianto.

OPC UA utilizza certificati digitali conformi allo standard X.509 della International Telecommunication Union (ITU).

In questo modo è possibile dimostrare (autenticare) l'identità di un programma, un computer o un'organizzazione.

Certificati X.509

Un certificato X.509 contiene tra l'altro le informazioni seguenti:

- Numero di versione del certificato
- Numero di serie del certificato
- Informazioni sull'algoritmo utilizzato dall'autorità di certificazione per firmare il certificato.
- Nome dell'autorità di certificazione
- Inizio e fine della validità del certificato
- Nome del programma, della persona o dell'organizzazione per cui il certificato è stato firmato dall'autorità di certificazione.
- Chiave pubblica del programma, della persona o dell'organizzazione.

Un certificato X509 collega un'identità (nome di un programma, di una persona o di un'organizzazione) alla chiave pubblica del programma, della persona o dell'organizzazione.

Verifica durante la creazione del collegamento

Quando si crea un collegamento tra il client e il server, i nodi verificano tutte le informazioni del certificato che consentono di valutarne l'integrità, ad es. la firma, il periodo di validità, il nome dell'applicazione (URN) e nella versione firmware V2.5 (solo in questa versione) anche gli indirizzi IP del client nel certificato client.

NOTA

Inoltre nella realizzazione del collegamento viene controllato il periodo di validità impostato nel certificato. È quindi necessario impostare l'orologio della CPU e la data/ora devono essere comprese entro il periodo di validità, altrimenti la comunicazione non avviene.

Firma e crittografia

Per poter verificare se un certificato è stato manipolato, i certificati vengono firmati.

Si può procedere in vari modi:

- In TIA Portal è possibile creare e firmare i certificati. Se il progetto è protetto e ci si collega come utente con il diritto di effettuare impostazioni di security, si possono utilizzare anche le impostazioni di security globali, Che consentono di accedere alla Gestione certificato e quindi anche all'autorità di certificazione (CA) di TIA Portal.
- Per creare e firmare i certificati sono disponibili anche ulteriori possibilità. Nel TIA Portal si possono importare i certificati in Gestione certificato globale.
  - Rivolgersi a un'autorità di certificazione (CA) per farsi firmare il certificato.

    In questo caso l'autorità di certificazione verifica l'identità dell'utente e firma il suo certificato con la propria chiave privata. Trasmettere una CSR (Certificate Signing Request) all'autorità di certificazione.
  - Creare autonomamente un certificato e firmarlo.

    Utilizzare ad es. il programma "Opc.Ua.CertificateGenerator" della OPC Foundation. Oppure utilizzare OpenSSL.
    Per maggiori informazioni vedere Creazione autonoma di coppie di chiavi PKI e di certificati (Pagina 204).

Informazioni sui tipi di certificato

- Certificato autofirmato:

  ogni nodo genera un proprio certificato e lo firma. Esempio di applicazione: configurazione statica con numero limitato di nodi di comunicazione.

  I certificati autofirmati non sono utilizzabili per creare altri certificati. I certificati autofirmati dei dispositivi partner devono essere caricati nella CPU (che deve essere in STOP).

- Certificato CA:

  i certificati vengono firmati da un'autorità di certificazione. Esempio di applicazione: impianti che si sviluppano dinamicamente.

  Si deve caricare nella CPU solo il certificato dell'autorità di certificazione. L'autorità di certificazione può generare nuovi certificati (si possono aggiungere dispositivi partner senza portare la CPU in STOP).

Firma

In base alla firma è possibile dimostrare l'integrità e l'origine di un messaggio come spiegato di seguito.

Con la firma, il mittente genera in primo luogo un valore di hash dal testo in chiaro (messaggio in chiaro). Quindi codifica il valore di hash con la sua chiave privata e infine trasmette al destinatario il testo in chiaro insieme al valore di hash crittografato Per verificare la firma, il destinatario deve conoscere la chiave pubblica del mittente (contenuta nel certificato X509 del mittente). Con la chiave pubblica del mittente, il destinatario decifra il valore di hash. Lo stesso destinatario calcolerà poi a sua volta il valore di hash dal testo in chiaro ricevuto (il metodo hash è contenuto nel certificato del mittente). Successivamente il destinatario mette a confronto i due valori di hash.

- Se i due valori di hash sono uguali significa che il messaggio in chiaro è arrivato integro al destinatario e non è stato manipolato.
- Se i due valori di hash non sono uguali significa che il messaggio in chiaro non è arrivato integro al destinatario: il messaggio in chiaro è stato manipolato o falsificato durante la trasmissione.

Crittografia

Crittografando i dati si evita che persone non autorizzate possano venire a conoscenza del loro contenuto. I certificati X509 non vengono crittografati perché sono pubblici e possono essere visionati da tutti.

Con la crittografia, il mittente cifra il messaggio in chiaro con la chiave pubblica del destinatario. Il mittente, perciò, deve avere il certificato X509 del destinatario, perché contiene la chiave pubblica del destinatario. Il destinatario decifra il messaggio con la propria chiave privata. Solo il destinatario può decifrare il messaggio. È l'unico a possedere la chiave privata. Perciò la chiave privata non deve mai essere comunicata ad altri.

Secure Channel

OPC UA utilizza la chiave pubblica e privata del client e del server per creare un collegamento sicuro: il canale sicuro. Stabilito il collegamento sicuro, client e server creano un'ulteriore chiave interna, nota soltanto a loro, che utilizzano per firmare e crittografare i messaggi. Questo metodo simmetrico (una chiave comune) è molto più veloce del metodo asimmetrico (chiave privata e pubblica).

Ulteriori informazioni

Per un esempio applicativo di utilizzo di certificati con TIA Portal, fare clic qui: Utilizzo di certificati con TIA Portal (https://support.industry.siemens.com/cs/ww/it/view/109769068).

11.2.3 Certificati in OPC UA

Utilizzo di certificati X.509 in OPC UA

Per creare un collegamento dal client al server, OPC UA utilizza tre tipi diversi di certificati X.509:

- Certificati dell'applicazione OPC UA

  Questi certificati X.509 identificano l'istanza software, la specifica installazione di un software client o server. Nell'attributo "Organisation Name" va inserito il nome dell'azienda che utilizza il software.

  NOTA

  Il server OPC UA dell'S7-1500 utilizza certificati dell'applicazione anche se l'impostazione di sicurezza è "None" (nessuna sicurezza). Questo garantisce la compatibilità con OPC UA V1.1 e con le versioni precedenti.

- Certificati software OPC UA

  Questo certificato X.509 identifica una versione concreta del software client o server. Questi certificati contengono attributi che descrivono quali test ha superato questa versione software per la certificazione da parte della OPC Foundation (ovvero test di laboratorio riconosciuti). Nell'attributo "Organisation Name" va inserito il nome dell'azienda che ha sviluppato il software o che lo commercializza.

  NOTA

  STEP 7 non supporta i certificati software.

- Certificati utente OPC UA

  Questo certificato X.509 identifica l'utente reale che ad es. richiama i dati di processo da un server OPC UA. Questo certificato non è necessario se l'utente dimostra la propria autorizzazione inserendo la password o se è configurato un accesso anonimo.

  NOTA

  STEP 7 non supporta i certificati utente.

I certificati descritti sono certificati di entità finale: identificano ad es. una persona, un'organizzazione, un'azienda, un'istanza (installazione) di un software.

11.2.4 Creazione dei certificati autofirmati

Utilizzo del generatore di certificati del client

Numerose applicazioni OPC UA client o SDK sono integrati in un'applicazione di esempio che può essere utilizzata come base per creare certificati per il client.

La descrizione della creazione certificato è riportata nel contesto relativo alla descrizione dell'applicazione OPC UA client.

Esempio di client dell'Online Support

Il client OPC UA .NET per il SIMATIC S7-1500 server OPC UA (https://support.industry.siemens.com/cs/ww/it/view/109737901) crea durante il primo avvio del programma un certificato software autofirmato per l'applicazione client, nel Certificate Store. La documentazione relativa all'esempio descrive il procedimento per la gestione di questi certificati.

Utilizzo del Generatore certificati di TIA Portal

Se si utilizza un client OPC UA che non crea certificati client, si possono creare certificati autofirmati con STEP 7.

Per eseguire questa operazione, procedere nel modo seguente:

1. Nelle proprietà della CPU in "Protezione & Security > Gestione certificato > Certificati dei dispositivi" fare due volte clic su "<Aggiungi nuovo>".
2. Fare clic su "Aggiungi".
3. Nella finestra di dialogo "Crea nuovo certificato" selezionare in "Destinazione d'uso" l'opzione "Client OPC UA".
4. Fare clic su "OK".

Nel campo "Nome alternativo del richiedente" (Subject Alternative Name) STEP 7 immette automaticamente l'URI del certificato creato. Se si crea il certificato nel programma con Stack .Net della OPC Foundation il campo si chiama ad es. "ApplicationUri", in altri tool per la creazione di certificati può però avere un altro nome.

Ulteriori informazioni

Per ulteriori informazioni sulla gestione dei certificati client consultare il capitolo Handling dei certificati client della CPU S7-1500 (Pagina 390).

11.2.5 Creazione autonoma di coppie di chiavi PKI e di certificati

Questo capitolo è rilevante solo se si vuole utilizzare un client OPC UA che non può generare autonomamente una coppia di chiavi PKI e un certificato client. In questo caso si utilizza OpenSSL per creare una chiave privata e una chiave pubblica, generare un certificato X.509 e firmarlo autonomamente.

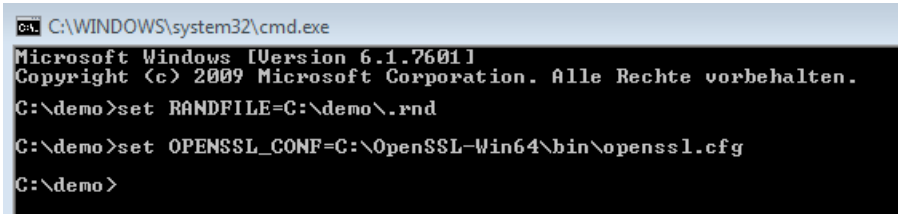
Utilizzo di OpenSSL

OpenSSL è un tool per Transport Layer Security, utilizzabile per generare certificati. Si possono usare anche altri tool, ad es. XCA, un software di gestione chiavi con interfaccia grafica che consente una migliore visualizzazione dei certificati emessi.

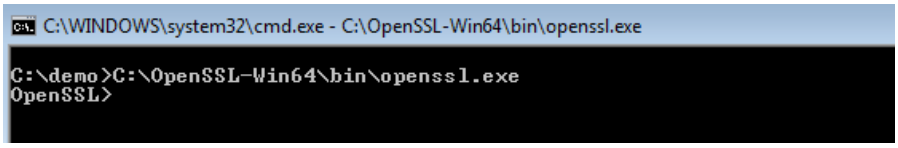
Per utilizzare OpenSSL su Windows, procedere nel seguente modo:

1. Installare OpenSSL su Windows. Se si utilizza una versione del sistema operativo a 64 bit, installare OpenSSL ad es. nella directory "C:\OpenSSL-Win64". OpenSSL-Win64 è disponibile come download presso diversi fornitori di software open source.
2. Creare una directory, ad es. "C:\demo".
3. Aprire la riga di comando (prompt). Per questa operazione fare clic su "Start" e inserire "cmd"o "Prompt" nel campo di ricerca. Nell'elenco dei risultati fare clic con il tasto destro del mouse su "cmd.exe" o "Prompt" ed eseguire il programma come amministratore: Windows apre il prompt.
4. Passare alla directory "C:\demo". Per questa operazione inserire il comando: "cd C:\demo".
5. Impostare le seguenti variabili di ambiente:
   - set RANDFILE=c:\demo\.rnd
   - set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg

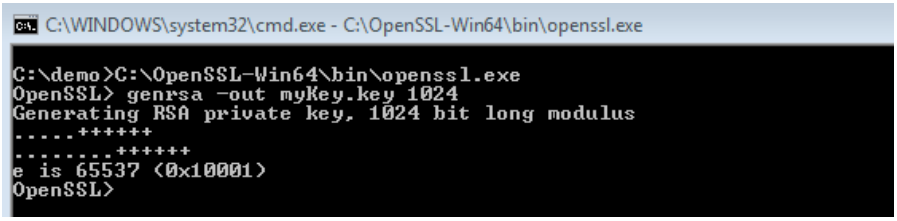
   La seguente figura mostra la riga di comando con i comandi:



6. Avviare OpenSSL. Se OpenSSL è stato installato nella directory C:\OpenSSL-Win64 inserire: C:\OpenSSL-Win64\bin\openssl.exe. La seguente figura mostra la riga di comando con il comando:



7. Generare una chiave privata. Salvare la chiave nel file "myKey.key". In questo esempio la chiave ha una lunghezza di 1024 bit; per aumentare la sicurezza dell'RSA si consiglia di utilizzare chiavi di 2048 bit. Immettere il comando: "genrsa -out myKey.key 2048" (nell'esempio "genrsa -out myKey.key 1024"). La seguente figura mostra la riga di comando con il comando e l'output di OpenSSL:



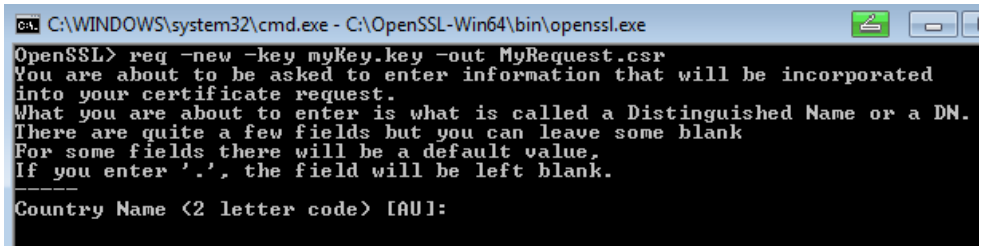
8. Generare una CSR (Certificate Signing Request), una richiesta di firmare un certificato. Per questa operazione inserire il comando: "req -new -key myKey.key -out myRequest.csr". Durante l'esecuzione di questo comando, OpenSSL chiede alcuni dati sul certificato:
   - Country Name: ad esempio "DE", per Germania, "IT" per Italia
   - State or Province Name: ad es. "Lombardia"
   - Location Name: ad es. "Milano"
   - Organisation Name: inserire il nome della propria azienda.
   - Organisational Unit Name: ad es. "IT"
   - Common Name: ad es. "OPC UA Client della macchina A"
   - Email Address:

NOTA

Avvertenza per CPU S7-1500 come server con versione firmware V2.5

Il campo "Nome alternativo del richiedente" (Subject Alternative Name) del certificato creato deve contenere, nella CPU S7-1500 V2.5, l'indirizzo IP del programma del client, in caso contrario la CPU non accetta il certificato.

I dati vengono inseriti nel certificato. La seguente figura mostra la riga di comando con il comando e l'output di OpenSSL:



Il comando crea nella directory C:\demo un file che contiene la Certificate Signing Request (CSR), nell'esempio "myRequest.csr".

Utilizzo del CSR

Una CSR si può utilizzare in due modi:

- È possibile trasmettere la CSR a un'autorità di certificazione (CA). A questo proposito attenersi alle indicazioni dell'autorità specifica. L'autorità di certificazione (CA) verifica i dati e l'identità (autenticazione) e firma il certificato con la chiave privata dell'autorità di certificazione. Chi ha creato il certificato X.509 lo riceve firmato e può utilizzarlo ad es. per OPC UA, HTTPS o Secure OUC (secure open user communication). I partner della comunicazione verificano attraverso la chiave pubblica dell'autorità di certificazione se il certificato è stato realmente emesso e firmato da questa autorità (ovvero se tale autorità ha confermato i dati contenuti nel certificato).
- È possibile firmare la CSR autonomamente. In questo caso occorre utilizzare la propria chiave privata. Questa opzione è spiegata nel prossimo passo.

Firma autonoma dei certificati

Per poter creare e firmare autonomamente un certificato (certificato autofirmato) inserire il comando: "x509 -req -days 365 -in myRequest.csr -signkey myKey.key -out myCertificate.crt".

La seguente figura mostra la riga di comando con il comando e l'output di OpenSSL:

Questo comando genera un certificato X.509 con gli attributi trasmessi con la CSR (nell'esempio "myRequest.csr”), ad es. con un periodo di validità di un anno (-days 365). Inoltre questo comando firma il certificato con la chiave privata di chi lo ha creato (nell'esempio "myKey.key"). Attraverso la chiave pubblica (contenuta nel certificato) i partner della comunicazione si accertano che l'utente disponga della chiave privata corrispondente. In questo modo si esclude che la chiave pubblica possa essere utilizzata impropriamente da un utente malintenzionato.

Nel caso dei certificati autofirmati si conferma personalmente che i dati in essi indicati sono corretti. Non esistono autorità di certificazione che verifichino tali dati.

Ulteriori informazioni

Per informazioni sulla gestione dei certificati client della CPU S7-1500 consultare il capitolo Handling dei certificati client della CPU S7-1500 (Pagina 390).

11.2.6 Trasmissione sicura dei messaggi

Creazione di collegamenti sicuri in OPC UA

OPC UA utilizza collegamenti sicuri tra client e server. OPC UA controlla l'identità dei partner della comunicazione. Per l'autenticazione di client e server, OPC UA utilizza certificati conformi allo standard X.509-V3 ITU (International Telecommunication Union). Eccezione: con la Security Policy “None” non viene creato un collegamento sicuro.

Message Security Modus

OPC UA utilizza le seguenti Security Policy per proteggere i messaggi:

- None

  I messaggi non sono sicuri. Per utilizzare questa Security Policy si crea un collegamento a un punto finale None di un server.

- Firma

  Tutti i messaggi vengono firmati. Ciò consente di verificare l'integrità dei messaggi ricevuti. Le manipolazioni vengono riconosciute. Per utilizzare questa Security Policy si crea un collegamento a un punto finale Sign di un server.

- Firma e crittografia

  Tutti i messaggi vengono firmati e crittografati. Ciò consente di verificare l'integrità dei messaggi ricevuti. Le manipolazioni vengono riconosciute. Inoltre il contenuto del messaggio non è leggibile da eventuali pirati informatici (protezione della riservatezza). Per utilizzare questa Security Policy si crea un collegamento a un punto finale “Firma e crittografia” di un server.

Le Security Policy vengono denominate anche in base agli algoritmi utilizzati. Esempio: "Basic256Sha256 - Firma e crittografia" significa: Punto finale sicuro, supporta una serie di algoritmi di hashing a 256 bit e la crittografia a 256 bit.

Livelli necessari

Nella seguente figura sono riportati i tre livelli "Transport", "Secure Channel" e "Session", che sono sempre necessari per creare un collegamento.

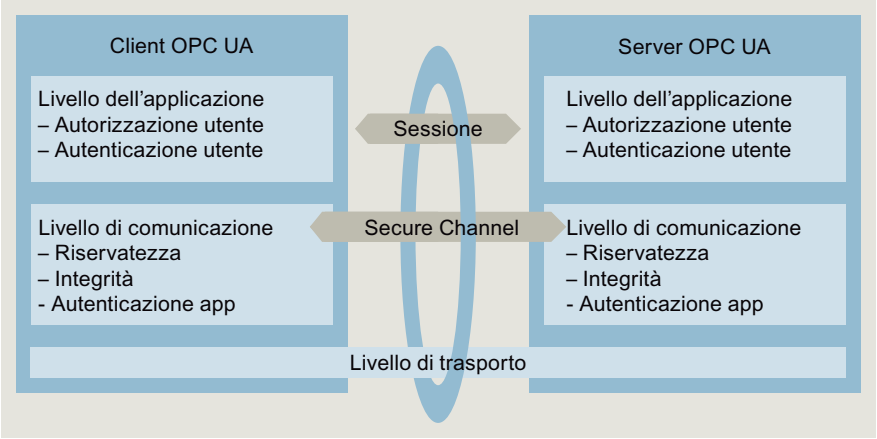


Figura 11-6 Livelli necessari "Transport", "Secure Channel" e "Session"

- Livello di trasporto

  Questo livello trasmette e riceve messaggi. OPC UA utilizza in questo caso un protocollo binario ottimizzato basato su TCP. Il livello di trasporto è la base per il successivo livello "Secure Channel".

- Secure Channel

  Secure Channel riceve i dati ricevuti dal livello di trasporto e li inoltra al livello "Session". Secure Channel inoltra al livello di trasporto i dati della sessione che devono essere trasmessi.

  Con la modalità di sicurezza “Firma” Secure Channel firma i dati (messaggi) che vengono trasmessi. All'arrivo di messaggi, Secure Channel verifica la firma per rilevare eventuali manipolazioni

  Con la Security Policy “Firma e crittografia” Secure Channel firma e cifra i dati da trasmettere. I dati ricevuti vengono decodificati da Secure Channel. Quindi il Secure Channel verifica la firma.

  Con la Security Policy “None” i pacchetti di messaggi attraversano il Secure Channel invariati (i messaggi vengono trasmessi e ricevuti con testo in chiaro).

- Session

  La sessione inoltra i messaggi dal canale di sicurezza all'applicazione e riceve dall'applicazione i messaggi da trasmettere. L'applicazione utilizza i valori di processo o mette a disposizione i valori.

Creazione del canale sicuro

Il Secure Channel viene creato nel modo seguente:

1. Il server inizia a configurare il canale di sicurezza quando riceve una richiesta dal client. Questa richiesta può essere firmata, firmata e crittografata oppure il messaggio viene trasmesso con testo in chiaro (modalità di sicurezza del punto finale del server selezionato). Con “Firma” e “Firma e crittografia” il client trasmette un "segreto" (un numero casuale) assieme alla richiesta.
2. Il server convalida il certificato del client (contenuto nella richiesta e non crittografato) e verifica l'identità del client. Se il server considera attendibile il certificato del client
   - decodifica il messaggio e verifica la firma (“Firma e crittografia”),
   - oppure verifica solo la firma (“Firma”)
   - o lascia il messaggio invariato (“None”).
3. In seguito il server invia una risposta al client (ugualmente sicura come la richiesta). La risposta contiene il segreto del server. Il client e il server ricavano dal segreto una chiave simmetrica. Così è configurato il canale di sicurezza.

La chiave simmetrica viene ora utilizzata per firmare e crittografare i messaggi (al posto della chiave privata e della chiave pubblica del client e del server).

Creazione della sessione

La sessione viene creata nel modo seguente:

1. Il client avvia la sessione inviando al server una CreateSessionRequest. Questo messaggio contiene un Nonce, un numero casuale che viene utilizzato una volta sola. Il server deve firmare il numero casuale (Nonce) per dimostrare che è il proprietario della chiave privata. La chiave privata appartiene al certificato utilizzato dal server per creare il Secure Channel. Questo messaggio (come tutti quelli successivi) è protetto in base alle impostazioni di sicurezza del punto finale del server scelto (Security Policyselezionate).
2. Il server risponde con la CreateSession Response. Questo messaggio contiene la chiave pubblica del server e il Nonce firmato. Il client verifica il Nonce firmato.
3. Se il server ha superato il test, il client invia al server una SessionActivateRequest. Il messaggio contiene i dati necessari per l'autenticazione dell'utente:
   - nome utente e password
   - o il certificato X.509 dell'utente (non supportato in STEP 7)
   - o nessun dato (se è configurato un accesso anonimo).
4. Se l'utente dispone dei diritti necessari, il server invia al client un messaggio di risposta (ActivateSessionResponse) e la sessione viene attivata.

Il collegamento sicuro tra client e server OPC UA è attivo.

Creazione di un collegamento con i blocchi funzionali PLCopen

La specifica PLCopen ha definito una serie di blocchi funzionali IEC 61131 per i client OPC UA. L'istruzione UA_Connect avvia un Secure Channel e una Session in base allo schema descritto più sopra.

11.2.7 Gestione certificato tramite Globale Discovery Server (GDS)

11.2.7.1 Gestione certificato automatizzata tramite GDS

A partire da TIA Portal V17 e dalle CPU S7-1500 con versione firmware V2.9 è possibile utilizzare i servizi di gestione dei certificati del server OPC UA per la trasmissione dei certificati del server OPC UA in runtime.

Le funzioni di GDS Push Management consentono l'aggiornamento automatico dei certificati OPC UA; degli elenchi di affidabilità e delle revoche certificati (CRL) per un server OPC UA della CPU S7-1500. La gestione automatizzata dei certificati evita l'incombenza di una nuova progettazione manuale della CPU, ad es. alla scadenza della durata di validità di un certificato, e di un nuovo caricamento della CPU. Inoltre, tramite le funzioni di GDS Push Management è possibile trasferire certificati ed elenchi aggiornati con la CPU in STOP e in RUN.

Il modello informativo sulla Gestione certificati è descritto nella Specifica OPC UA Parte 12 (OPC 10000-12: OPC Unified Architecture, Part 12: Discovery and Global Services).

A partire da TIA Portal versione V18 e dalle CPU S7-1500 con versione firmware V3.0 è possibile utilizzare le funzioni di GDS Push Management anche per i certificati del Web server. L'aggiornamento dei certificati tramite le funzioni di GDS Push Management, ad es. è sostanzialmente identico all'aggiornamento dei certificati del server OPC UA. In luogo dei certificati del server OPC UA, vengono trasferiti alla CPU i certificati del Web server in runtime o durante il funzionamento. Differenze e limitazioni vengono spiegate nei punti specifici nella seguente descrizione.

Le seguenti sezioni forniscono una panoramica di Global Discovery Service in generale nonché delle funzioni di aggiornamento automatico dei certificati supportate dalla versione V17 di TIA Portal / dalla versione V2.9. del firmware della CPU.

Discovery Server

Per collegarsi al server OPC UA, un client OPC UA necessita di informazioni sul relativo punto finale quali ad es. il punto finale URL e la Security Policy. In presenza di un gran numero di possibili server nella rete, un Discovery Server può farsi carico della ricerca e della gestione di queste informazioni.

- I server OPC UA si registrano al Discovery Server.
- I Client OPC UA richiedono al Discovery Server un elenco dei server accessibili e successivamente si collegano al server OPC UA desiderato.

Global Discovery Server (GDS)

Il concetto GDS OPC UA da un lato consente la configurazione di servizi Discovery per tutte le sottoreti, dall'altro fornisce interfacce per la gestione centrale dei certificati.

Un Global Discovery Server (GDS) mette a disposizione meccanismi per la gestione centrale dei seguenti componenti:

- Certificati firmati CA e certificati autofirmati
- Elenchi attendibili (Trusted Lists) e elenchi di revoche certificati (Certificate Revocation Lists, CRL)

Un GDS fornisce un punto di accesso alla Gestione certificato centrale - svolgendo in tal modo il compito di server security all'interno di una rete di comunicazione OPC UA.

L'impiego principale di GDS concerne la gestione dei certificati firmati da CA con i CRL corrispondenti, nello specifico si tratta dei seguenti compiti:

- Impostazione iniziale di un certificato dell'applicazione OPC UA, ad es. per il server OPC UA o per il web server
- Aggiornamento a intervalli regolari dell'elenco attendibile (Trust List) e dei CRL
- Rinnovo di un certificato dell'applicazione

Gestione certificato

La Gestione certificato ha il compito di gestire e distribuire automaticamente i certificati e gli elenchi attendibili per diversi servizi e applicazioni UA.

In questo contesto si distinguono i seguenti ruoli:

- Gestione certificato - un'applicazione OPC UA che rende disponibili funzioni di gestione dei certificati
- Destinatario del certificato - un'applicazione OPC UA che riceve i certificati, gli elenchi attendibili e del CRL del manager dei certificati.

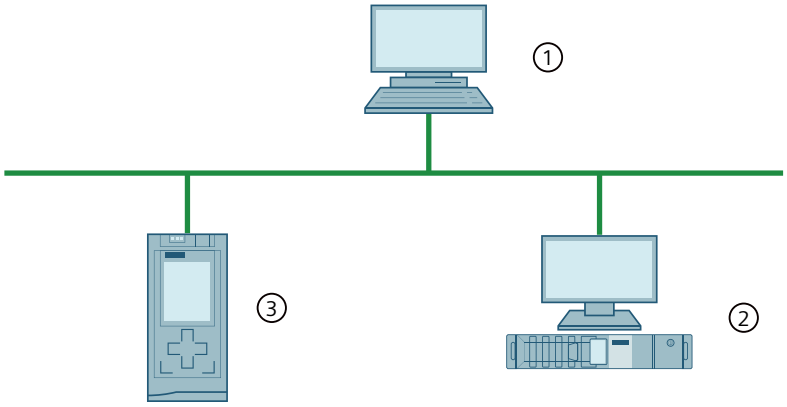
Sono disponibili due modelli di gestione certificato: Gestione Pull and Push

- Con la gestione Pull l'applicazione OPC UA opera come un client del server GDS e utilizza i metodi di gestione dei certificati per richiedere gli aggiornamenti di certificati e elenchi attendibili.
- Con la gestione Push l'applicazione OPC UA funziona come un server e rende disponibili i metodi per un OPC UA GDS operante come client OPC UA. Nel ruolo di Gestione certificato il GDS utilizza questi metodi per la trasmissione di certificati e aggiornamenti di elenchi attendibili ("pushen"), vedere la spiegazione del concetto di aggiornamento automatico dei certificati riportata nel seguito.

Dalla versione firmware V2.9 la CPU S7-1500 supporta inizialmente soltanto la gestione Push per il server OPC UA della CPU.

Configurazione d'impianto con GDS

La figura sottostante riporta un esempio dei compiti svolti dai dispositivi interessati in combinazione con un GDS che fornisce funzioni di gestione certificati.



① Root CA - dispositivo che emette certificati per gli impianti (la trasmissione di questi certificati può avvenire anche in altro modo, ad es per e-mail)

② GDS OPC UA con manager dei certificati: crea o firma i certificati del dispositivo, gestisce gli elenchi attendibili e gli elenchi di certificati revocati (Certificate Revocation Lists, (CRL)), scrive i certificati e gli elenchi nei dispositivi (funzione Push). Per la funzione Push questo dispositivo deve svolgere la funzione di client OPC UA.

③ Dispositivo con applicazione OPC UA: riceve certificati ed elenchi in modalità "push"

Criterio di aggiornamento automatico dei certificati per STEP 7 versione V17

GDS e Gestione certificato vengono combinati normalmente in un'applicazione - nella figura in basso tuttavia sono due componenti separati.

Per la Gestione certificati si addicono anche dispositivi come i "normali" client OPC UA, questi devono tuttavia supportare il tipo di dati ByteString indispensabile per la trasmissione dei certificati, come ad es. una CPU S7-1500 dalla versione firmware V2.9 come client OPC UA, oppure il tool UA Expert (Unified Automation) con Plugin GDS.

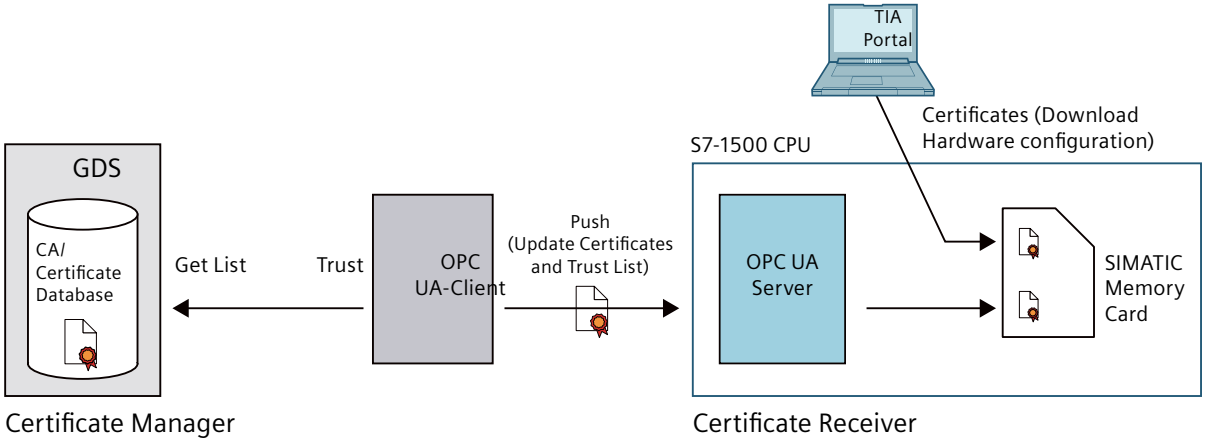
Il server OPC UA della CPU S7-1500 con il ruolo di destinatario del certificato fornisce i metodi e gli attributi standardizzati necessari, tramite i quali gli OPC UA Client possono scrivere e leggere certificati, elenchi attendibili e CRL.

Nel contesto del server OPC UA della CPU S7-1500 l'attenzione particolare è rivolta alla descrizione della funzione Push in contrapposizione al metodo già noto per trasferire i certificati nella CPU: tramite caricamento della configurazione hardware.

La figura sottostante illustra le modalità di trasferimento dei certificati e degli elenchi per OPC UA in una CPU S7-1500 a partire dalla versione firmware V2.9:e

- Tramite caricamento della configurazione hardware (event. con la CPU in STOP; i certificati costituiscono parte della configurazione hardware e possono essere caricati in RUN solo con determinati requisiti, vedere Suggerimento: Aggiornamento dei certificati caricati in RUN (Pagina 80))
- Oppure tramite metodi GDS Push con la CPU in RUN o in STOP.

Non è possibile l'impiego simultaneo di entrambi i metodi di trasmissione. Se si sceglie di trasferire ad es. i certificati del server OPC UA con funzioni GDS Push in runtime, è necessario trasferire alla CPU anche tutti gli altri tipi di certificati nello stesso modo.



Ulteriori informazioni

Per ulteriori informazioni sui certificati in OPC UA consultare il capitolo Certificati in OPC UA (Pagina 202).

11.2.7.2 Configurazione della funzione Push

Numero di certificati per la funzione Push

Per quanto concerne la funzione Push OPC UA, una CPU S7-1500 con versione firmware V2.9 o superiore presenta, indipendentemente dal tipo, una configurazione di 62 voci attendibili.

- Ogni servizio attivato basato su certificati (applicazione CPU) "occupa" rispettivamente una voce per il certificato e una voce per la chiave privata.
- Una voce nella lista della revoca certificati (CRL) ha lo stesso valore di una voce nell'elenco dei certificati considerati attendibili.
- Un certificato utilizzato da diversi servizi (applicazioni CPU) è considerato come un'unica voce nell'elenco dei certificati attendibili.

Dimensioni degli elementi per la funzione Push (ad es. certificati)

Max. 4096 byte.

Esempio

Si intende consentire l'accesso al server OPC UA ad un max di 62 client OPC UA e compilare di conseguenza l'elenco dei certificati attendibili.

Dopo che una voce della lista dei certificati revocati è stata inserita nell'elenco dei certificati attendibili, è possibile dichiarare attendibili soltanto max 61certificati del client.

I certificati aggiuntivi per OPC UA **non** possono essere trasferiti nella CPU caricando la configurazione hardware.

Suggerimento

Per contenere il numero di certificati necessari, si raccomanda di far firmare possibilmente dalla stessa CA i certificati client OPC UA.

La CPU operante come server OPC UA necessita in questo caso soltanto del certificato CA corrispondente e di CRL. Con questi elementi il server OPC UA può verificare tutti i certificati client firmati CA. Non è quindi necessario aggiungere i singoli certificati client agli elenchi attendibili.

11.2.7.3 Impostazione e caricamento dei parametri GDS

Nel seguito sono descritte le impostazioni necessarie per l'aggiornamento dei certificati.

Presupposti

- A seconda del certificato dell'applicazione è necessaria la versione compatibile di STEP 7/TIA Portal e del firmware della CPU S7-1500.

  Vedere anche: Informazioni utili sulla gestione dei certificati (Pagina 68)

  – Per i certificati del server OPC UA, ad es., TIA Portal dalla V17, versione firmware della CPU V2.9

  – Per i certificati del Web server, ad es., TIA Portal dalla V18, versione firmware della CPU V3.0

- Ora/data della CPU impostata (vale in generale per la comunicazione basata su certificati)
- Il server OPC UA è attivato
- Il service che utilizza GDS Push Management deve essere già attivato. Ad es. deve essere attivato il Web server per il trasferimento dei certificati del Web server.
- Deve essere stato progettato almeno un punto finale con la Security Policy "Firma e crittografia" per il server OPC UA, il partner deve utilizzare questo punto finale

- L’utente autenticato con sufficienti diritti di accesso alle funzioni è parametrizzato
  L’utente deve avere un ruolo con il **diritto di accesso alla funzione "Gestione certificati"**.

  Questo diritto di accesso alle funzioni richiede a sua volta i seguenti presupposti:

  – Nella navigazione del progetto deve essere **attivata la protezione del progetto** : Navigazione del progetto: "Impostazioni Security > Impostazioni > Protezione del progetto".

  – L'utente con un ruolo con diritto di accesso alla funzione "Gestione certificati" è configurato nella navigazione del progetto "Impostazioni di sicurezza > Utenti e ruoli". TIA Portal < V19: Nelle impostazioni della CPU nell’area "OPC UA > Generale" deve essere attivata la seguente impostazione per la gestione utenti generale: "Attiva Gestione utenti supplementare tramite le impostazioni di security del progetto".

Nella sezione Gestione utenti e ruoli con diritti di accesso alle funzioni OPC UA (Pagina 278) viene descritto come impostare i diritti di accesso alle funzioni.

Attivazione di GDS

Se i presupposti summenzionati sono soddisfatti, deve ancora essere attivato GDS.

1. Nella finestra di ispezione (Parametri CPU) navigare nell'area "OPC UA > Server > Generale".
2. Attivare l’opzione "Attiva Global Discovery Services (Push)"

Definizione dell'archivio dei certificati

I certificati gestiti tramite GDS si trovano in un’area di memoria separata rispetto ai certificati scaricati da TIA Portal (STEP 7).

Quando è attivata la gestione certificati GDS Push, i servizi (applicazioni) della CPU devono attingere anche dalla memoria che contiene i certificati gestiti durante il runtime.

1. Navigare nelle impostazioni della CPU fino alla sezione "Protezione & Security > Gestione certificato".
2. Selezionare l'opzione "Utilizza i certificati forniti dalla gestione certificati durante il runtime".

   L'altra opzione (utilizza certificati configurati e scaricati tramite TIA Portal) utilizza i certificati che vengono caricati da TIA Portal con la configurazione o le modifiche della configurazione nella CPU. In questo archivio di certificati non è possibile aggiornare certificati o elenchi attendibili in fase di esecuzione e i certificati possono essere aggiornati solo in presenza di particolari condizioni generali (vedere Suggerimento: Aggiornamento dei certificati caricati in RUN (Pagina 80)).

Attivazione della diagnostica per la scadenza dei certificati

Se si desidera essere informati in anticipo sulla scadenza di un certificato, selezionare l'opzione "Attiva evento di diagnostica di sistema per la scadenza del certificato" nella sezione "Protezione & Security > Gestione certificato".

Inserire un valore percentuale nel campo di immissione "Visualizza evento alla durata residua del certificato ...".

Effetto di queste impostazioni:

- Non appena un certificato raggiunge questo valore, viene visualizzato un messaggio di diagnostica di sistema fino alla scadenza o all'aggiornamento del certificato.
- Raggiunta la fine del periodo di validità di un certificato, la CPU genera un corrispondente messaggio di diagnostica di sistema e una voce nel buffer di diagnostica, mentre il LED della manutenzione si accende.

Esempio:
Il certificato trasmesso tramite GDS il 1.6.22 è valido dal 1.6.22 al 30.6.22 (30 giorni). Per l'evento di diagnostica, l'utente ha inserito il valore percentuale 10. Il 27.6.22, trascorso il 90% del periodo di validità, un messaggio segnala che il certificato trasmesso scadrà il 30.06.2022.
Indipendentemente dal valore percentuale parametrizzato, allo scadere del periodo di validità di un certificato viene comunque visualizzato un messaggio corrispondente, viene creata una voce nel buffer di diagnostica, e il LED della manutenzione si accende.

Caricamento della CPU

Quando si carica la configurazione nella CPU è possibile cancellare prima i certificati gestiti tramite GDS. Confermando la cancellazione, dopo il caricamento segue una fase di distribuzione (consultare la sezione sulla messa in servizio).

Quando si carica la Memory Card esternamente alla CPU (Card Reader), quest'archivio dei certificati viene sempre cancellato.

Se Global Discovery Services (Push) è attivato e non sono presenti certificati push, per il server OPC UA non è presente né un proprio certificato né un elenco di certificati e nemmeno un CRL.

11.2.7.4 Messa in servizio GDS

Nella specifica OPC UA Parte 12, nella gestione dei certificati si distingue tra una fase di distribuzione (provisioning phase) e una fase di runtime (run time phase).

Durante la fase di distribuzione un GDS o un client OPC UA fornisce al server OPC UA della CPU elenchi attendibili iniziali e CRL. In questa fase il server OPC UA della CPU accetta tutti i certificati e gli elenchi che gli vengono forniti come avviene con l'impostazione "Client affidabili" per il server OPC UA che prevede l'accettazione di tutti i certificati del client in runtime. Solo così è possibile creare un collegamento con i client che il server non conosce, vale a dire che non può autenticare tramite certificati o elenchi di certificati esistenti fino a quando non ha ricevuto il certificato del client o gli elenchi di certificati corrispondenti.

La fase di distribuzione è caratterizzata da una scarsa sicurezza (livello di sicurezza più basso); pertanto questa fase viene segnalata dal LED Maintenance lampeggiante e da una voce corrispondente nel buffer di diagnostica (Maintenance demanded).

Durate la fase di runtime vengono aggiornati ad es. i CRL esistenti e vengono rinnovati i certificati e gli elenchi attendibili. In questa fase la comunicazione è sicura (secure).

Presupposti

Soltanto gli utenti con sufficienti diritti di accesso alle funzioni possono creare un collegamento nella fase di distribuzione. Gli utenti devono avere un ruolo con il diritto di accesso alla funzione "Gestione certificati".

Vedere anche Impostazione e caricamento dei parametri GDS (Pagina 214).

Regole per la fase di distribuzione

Durante la fase di distribuzione, il server OPC UA della CPU non è in grado di autenticare i client OPC UA che inizializzano la creazione del collegamento. Devono quindi essere rispettate le seguenti regole:

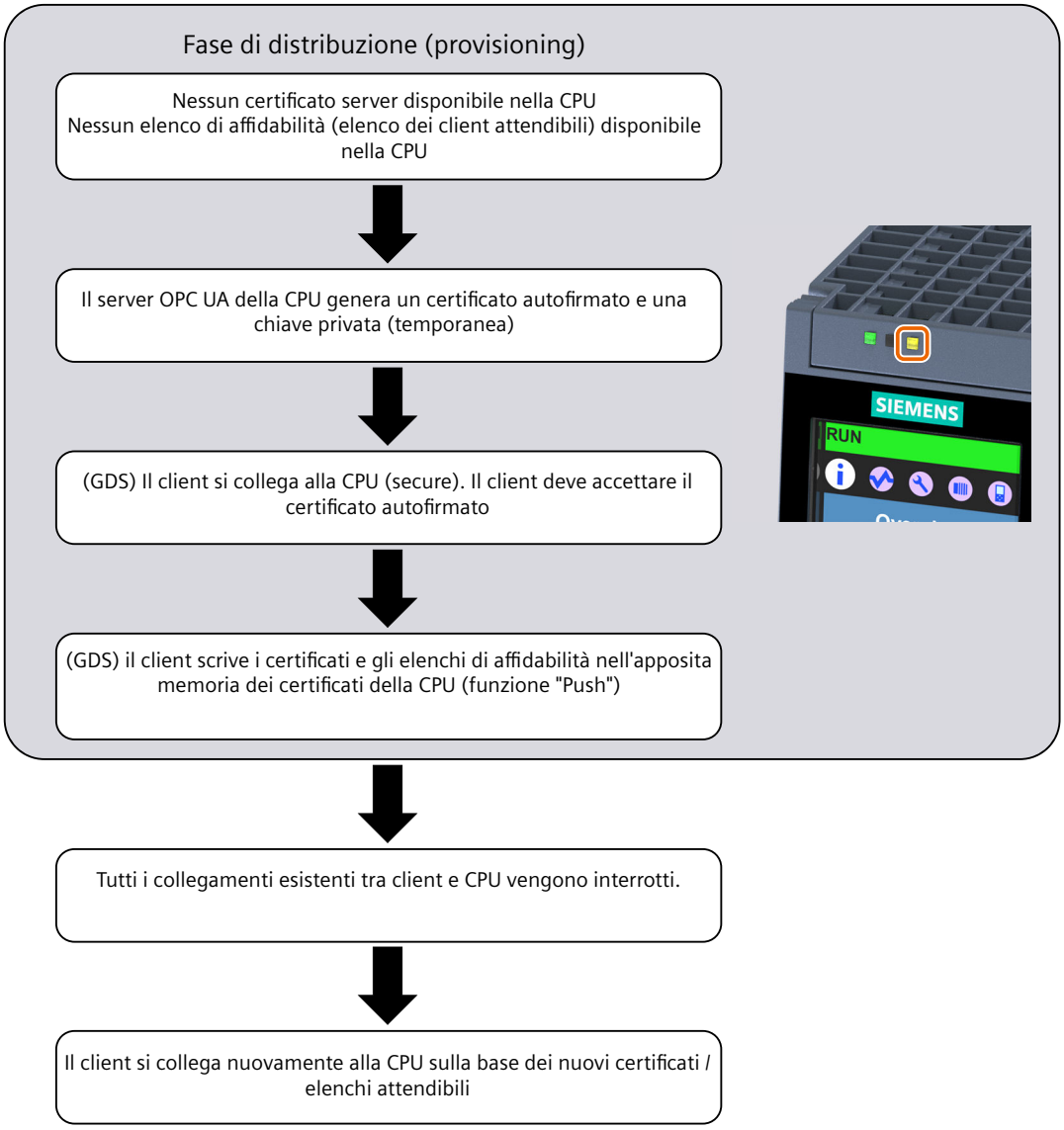
- Garantire un ambiente sicuro, ad es. consentire l'accesso alla CPU soltanto al responsabile per la messa in servizio. Controllare che la comunicazione si svolga tra i dispositivi richiesti.
- Limitare la durata di questa fase.

La CPU segnala che si trova in fase di distribuzione con il LED Maintenance lampeggiante e alla voce corrispondente nel buffer di diagnostica (Maintenance demanded).

Svolgimento della fase di distribuzione

Di seguito è descritta brevemente l'esecuzione della fase di distribuzione per i certificati del server OPC UA e per gli
elenchi attendibili.

Nei certificati del Web server la fase di distribuzione si svolge nello stesso modo. A differenza di OPC UA, il Client GDS inserisce nell'archivio dei certificati soltanto i certificati del Web server e non
gli elenchi attendibili.



Avvio della fase di distribuzione

Dopo l'avviamento del server OPC UA, la CPU si trova automaticamente nella fase di distribuzione se è soddisfatta una delle seguenti condizioni:

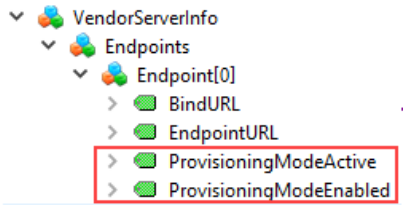
- Il certificato del server OPC UA è il certificato iniziale generato e autofirmato dalla CPU e non è ancora stato sostituito da un certificato del server valido.
- L'elenco attendibile (elenco dei client affidabili) è vuoto.

Il certificato del server OPC UA generato dalla CPU contiene i parametri più importanti di questo server e viene rigenerato, includendo la chiave privata, dopo ogni avvio del server OPC UA dopo un RETE ON, fino a quando non è disponibile il certificato del server valido. Pertanto l'avvio del server OPC UA dopo un RETE ON può richiedere tempi più lunghi.

A seconda delle impostazioni, dopo il caricamento della configurazione hardware, l'archivio dei certificati che possono essere aggiornati in runtime viene eliminato oppure i certificati vengono mantenuti. Ovvero, se GDS è attivato e l'archivio certificati è stato eliminato, dopo il caricamento della configurazione hardware la CPU si trova nella fase di distribuzione.

Diagnostica della fase di distribuzione

Oltre al LED Maintenance acceso, il modello di indirizzi GDS dispone di due nodi che indicano se il server OPC UA della CPU è in fase di distribuzione:



Soltanto quando i requisiti GDS sono soddisfatti (sicurezza del punto finale firmata e crittografata nonché disponibilità dei diritti di accesso alle funzioni di amministratore), è possibile l'impiego dei due nodi per la diagnostica come evidenziato nella figura.

ProvisioningModeEnabled: Indica che la fase di distribuzione viene supportata.

ProvisioningModeActive: Indica che il server OPC UA della CPU si trova nella fase di distribuzione.

Fine della fase di distribuzione

La CPU termina automaticamente la fase di distribuzione, se sono soddisfatte le seguenti condizioni:

- Il certificato generato e autofirmato dalla CPU per la fase di distribuzione è stato sostituito da un certificato valido del server. Questo certificato server valido può essere un certificato autofirmato o firmato CA.
- L'elenco attendibile nella CPU non è vuoto. I certificati client dei client OPC UA attendibili, o i certificati CA per il controllo dei certificati dei client, sono disponibili.

Se il client OPC UA trasmette un certificato firmato CA aggiungendolo anche all'elenco dei certificati attendibili, il server OPC UA della CPU può accettare automaticamente tutti gli altri certificati dei client OPC UA che sono stati firmati dalla medesima CA.

Richiesta di un certificato server valido

A partire da TIA Portal versione V18 / dalle CPU S7-1500 versione V3.0, oltre ai certificati del server OPC UA è possibile trasferire alla CPU anche certificati per altri servizi, ad es. per il Web server.

Il servizio interessato, ad es. il server OPC UA della CPU, riceve un certificato valido nelle fasi seguenti:

1. Un client GDS (client OPC UA) richiama il metodo "CreateSigningRequest" per richiedere un certificato del server con un Certificate Signing Request (CSR).
2. Questo CSR deve essere firmato da una Certificate Authority (CA).
3. Il CSR firmato deve essere poi ritrasferito come certificato al server OPC UA della CPU.

Il server OPC UA della CPU fornisce questo metodo a condizione che il client disponga del necessario diritto di accesso alla funzione "Gestione certificati".

Il metodo "CreateSigningRequest" consente le seguenti varianti:

- Aggiornamento del certificato senza creazione di una nuova coppia di chiavi (vengono utilizzate le chiavi interne già disponibili della CPU)
- Aggiornamento del certificato con creazione di una nuova coppia di chiavi (internamente alla CPU)

Esiste inoltre la possibilità di creare certificati con coppie di chiavi generate esternamente.

ATTENZIONE
Procedimento consigliato durante la generazione del certificato Evitare possibilmente il trasporto di chiavi private; le chiavi private non dovrebbero lasciare il dispositivo. Per questo motivo si consiglia la generazione del certificato senza creazione di una nuova coppia di chiavi ovvero con la creazione di una coppia di chiavi all’interno della CPU.

Generazione del certificato senza coppia di chiavi

- Il metodo "CreateSigningRequest" restituisce una Certificate Signing Request (CSR), ovvero un file (*.csr) con informazioni specifiche sul server o sul service, come ad es. il nome dell'applicazione e l'URL.
- Questo CSR deve essere validato al di fuori della CPU da una Certificate Authority (CA), firmato e restituito come certificato.
- Il certificato deve essere quindi trasferito (con modalità "push") alla CPU con il metodo "UpdateCertificate".

Con questa procedura la chiave non lascia la CPU.

Generazione del certificato con coppia di chiavi creata internamente

La procedura è simile a quella prevista per il metodo illustrato nel paragrafo precedente, con la sola differenza che oltre al CSR viene creata anche una coppia di chiavi. Nel parametro "reateSigningRequest" del metodo specificare che quest'ultimo deve creare una coppia di chiavi.

Anche con questa procedura la chiave privata non lascia la CPU.

La generazione di una nuova coppia di chiavi comporta un carico notevole sulla CPU. L'elaborazione di quest'ordine da parte della CPU si estende su un intervallo di tempo più

lungo, con priorità minore, nell'area riservata per il carico di comunicazione. La durata di quest'intervallo di tempo dipende dalle prestazioni della CPU.

Poiché durante la generazione della chiave, la percentuale del carico di comunicazione impostato viene utilizzata completamente per un tempo piuttosto lungo, impostare la percentuale del "Carico del ciclo dovuto alla comunicazione" in modo da consentire una disponibilità sufficiente di riserve e al contempo evitare che il tempo di ciclo massimo venga superato. Per questo scopo consultare ad es. la pagina del Web server "Diagnostica > Informazioni sul tempo di esecuzione" della CPU. Questa pagina fornisce informazioni sul carico attuale del programma e della comunicazione e sul tempo di ciclo del programma utente. Un regolatore fornisce informazioni sulle ripercussioni che un carico di comunicazione modificato ha sul tempo di ciclo.

Generazione del certificato con coppia di chiavi creata esternamente

Questo tipo di generazione del certificato funziona con l'ausilio di tool in grado di creare chiavi supplementari.

Certificato e chiave vengono trasferiti nella CPU tramite il metodo "UpdateCertificate".

A causa della sua scarsa sicurezza, questa procedura è sconsigliabile.

ATTENZIONE
Chiavi diverse per i diversi sistemi di destinazione Per un sistema di produzione utilizzare sempre chiavi di nuova generazione. Se il progetto viene simulato e testato sul PC ad es. con PLCSIM Advanced, non impiegare mai per un sistema produttivo le chiavi utilizzate per questa simulazione. Limitare l'accesso ai controllori basati su PC configurando le autorizzazioni corrispondenti.

11.2.7.5 Modello indirizzi per la gestione certificati Push

La parte 12 della specifica OPC UA (OPC 10000-12: Discovery, Global Services) definisce metodi e attributi ad es. per il server OPC UA, per consentire a GDS o ai client OPC UA di aggiornare certificati ed elenchi attendibili nel server ("Gestione certificato Push"). Tali metodi e attributi si ritrovano anche nel modello indirizzi del server OPC UA.

Di seguito è spiegata la sezione pertinente nel modello indirizzi del server OPC UA della S7-1500.

Presupposti

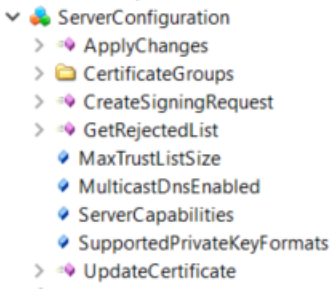
Affinché i metodi e gli attributi rilevanti per la funzionalità GDS Push siano visibili, devono sussistere i seguenti presupposti:

- GDS è attivato.
- La Security Policy impostata supporta l'integrità e la riservatezza dei dati attraverso la firma e la crittografia (Sign & Encrypt)
- Accesso con diritto di funzione runtime "Gestione certificati".

Modello indirizzi per la funzionalità GDS Push

Il modello indirizzi per la funzionalità GDS Push corrisponde al "Information Model for Push Certificate Management" della specifica OPC UA OPC 10000-12: Discovery, Global Services.

Nel nodo "ServerConfiguration" è presente la seguente struttura:



Metodi e attributi per l'accesso al modello indirizzi

Di seguito sono spiegati brevemente i metodi e gli attributi con specificità e limitazioni del modello indirizzi concreto della CPU S7-1500. Suddetta specifica OPC UA contiene la descrizione generale.

Di seguito alla tabella riepilogativa è presente la descrizione dettagliata dei singoli metodi.

Metodo / Attributo (variabile)	Descrizione
CreateSigningRequest	Metodo per la creazione di una Certificate Request con codifica PKCS#10 firmata con la chiave privata del servizio (ad es. server OPC UA).
UpdateCertificate	Metodo per aggiornare il certificato server, ad es. per il server OPC UA.
ApplyChanges	Metodo per applicare una modifica rilevante per la sicurezza, nel caso in cui durante l'esecuzione di uno dei metodi precedentemente descritti sia stato impostato l'attributo "ApplyChangesRequired". **Nota** La modifica di un certificato con la funzione "ApplyChanges", comporta l'interruzione da parte della CPU dei collegamenti/delle sessioni protette da questo certificato. Tenere presente che: La base per i collegamenti sicuri, ovvero il certificato, non è più valida.
GetRejectedList	Metodo che restituisce un elenco di certificati che sono stati rifiutati dal server OPC UA. I certificati rifiutati non vengono attualmente salvati dal server OPC UA delle CPU S7-1500. Il metodo restituisce un array vuoto (RejectedList).
ServerCapabilities	Il server OPC UA della CPU S7-1500 non supporta questa variabile.
SupportedPrivateKeyFormats	Variabile che indica i formati ammessi per le chiavi private. Per CPU S7-1500 solo "PEM" (String Array)

Metodo / Attributo (variabile)	Descrizione
MaxTrustListSize	Variabile che indica le dimensioni massime dell'elenco attendibile.
MulticastDnsEnabled	Variabile che indica se Multicast DNS è supportato. Per le CPU S7-1500 il valore è "False".
CertificateGroups	Oggetto (cartella) che organizza tutti i gruppi di certificati supportati dal server OPC UA. Nei gruppi di certificati si trovano gli oggetti che possono essere aggiornati in modo dinamico durante il runtime: Ad es. un elenco attendibile e uno o più certificati che sono assegnati a un servizio (ad es. applicazione OPC UA). I dettagli sulla struttura dell'oggetto CertificateGroups e su metodi e attributi disponibili, sono spiegati nel prossimo capitolo.

CreateSigningRequest

Il metodo ha i seguenti parametri:

Parametro	Tipo di dati	Descrizione
[in] certificateGroupId	NodeId	NodeId dell'oggetto CertificateGroup.
[in] certificateTypeId	NodeId	Tipo di certificato richiesto. L'elenco dei tipi di certificati ammessi è specificato dalla variabile "CertificateTypes" del gruppo certificati. Per il server OPC UA ad es. il tipo di certificato "RsaSha256ApplicationCertificateType", per il Web server il tipo di certificato "HttpsCertificateType"
[in] subjectName	String	Subject Name, che viene richiesto nella Certificate Request. Se non specificato, viene utilizzato l'attuale Subject Name del certificato.
[in] regeneratePrivateKey	Boolean	True: Il server genera una nuova chiave privata. La chiave resta memorizzata fino a quando viene richiamato il metodo UpdateCertificate con gli appropriati certificati firmati. False: il server utilizza la chiave privata disponibile.
[in] nonce	ByteString	Nonce supplementare per la creazione di una nuova chiave privata (vedere regeneratePrivateKey). Dove avere una lunghezza di almeno 32 byte.
[out] certificateRequest	ByteString	PKCS #10 - Certificate Request con codifica.

Method Result Codes

Result Code	Descrizione
Bad_InvalidArgument	certificateTypeId, certificateGroupId o subjectName non valido.
Bad_UserAccessDenied	L'utente corrente non dispone dei necessari diritti di accesso alle funzioni.

UpdateCertificate

Casi applicativi:

- Generazione di certificati con CreateSigningRequest. Nessuna chiave privata fornita.
- La nuova chiave privata e il nuovo certificato sono stati creati esternamente al server. Entrambi saranno aggiornati con UpdateCertificate.
- Certificato creato e firmato con la chiave privata del certificato esistente. Nessuna chiave privata fornita.

Parametro	Tipo di dati	Descrizione
[in] certificateGroupId	NodeId	NodeId dell'oggetto CertificateGroup.
[in] certificateTypeId	NodeId	Tipo di certificato richiesto. L'elenco dei tipi di certificati ammessi è specificato dalla variabile "CertificateTypes" del gruppo certificati.
[in] certificate	ByteString	Certificato con codifica DER che sostituisce il certificato esistente.
[in] issuerCertificates	ByteString	Certificati emittenti
[in] privateKeyFormat	String	Formato della chiave privata. Al momento supporta solo PEM. Se la privateKey non è specificata: zero o stringa vuota.
[in] privateKey	ByteString	Chiave privata codificata come indicato in privateKeyFormat.
[out] applyChangesRequired	Boolean	Indica che deve essere richiamato il metodo "ApplyChanges" prima di utilizzare un nuovo certificato.

Method Result Codes

Result Code	Descrizione
Bad_InvalidArgument	certificateTypeId o certificateGroupId non valido.
Bad_CertificateInvalid	Il certificato non è valido o il formato non è supportato.

Result Code	Descrizione
Bad_NotSupported	La chiave privata non è valida o il formato non è supportato.
Bad_UserAccessDenied	L'utente corrente non dispone dei necessari diritti di accesso alle funzioni.
Bad_SecurityChecksFailed	Si è verificato un errore durante la verifica dell'integrità del certificato.

Apply Changes

Il metodo non ha nessun parametro.

Method Result Codes

Result Code	Descrizione
Bad_UserAccessDenied	L'utente corrente non dispone dei necessari diritti di accesso alle funzioni.

GetRejectedList

Il metodo ha i seguenti parametri:

Parametro	Tipo di dati	Descrizione
[out] certificates	ByteStrings	Elenco con codifica DER dei certificati rifiutati. Attualmente il metodo restituisce un elenco vuoto (array vuoti) in quanto i certificati rifiutati non vengono salvati.

Method Result Codes

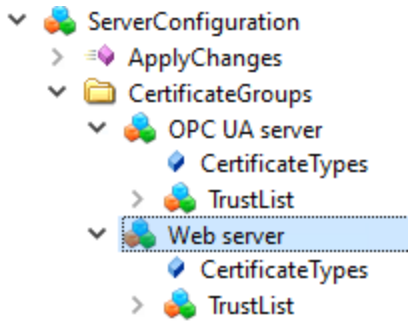
Result Code	Descrizione
Bad_UserAccessDenied	L'utente corrente non dispone dei necessari diritti di accesso alle funzioni.

11.2.7.6 CertificateGroups nel modello indirizzi

I certificati e gli elenchi attendibili per i servizi e le applicazioni della CPU (ad es. server OPC UA) che possono essere aggiornati durante il runtime si trovano nel modello indirizzi nell'oggetto "CertificateGroups"; per i diversi servizi della CPU S7-1500 è disponibile un gruppo di certificati ciascuno. Per il certificato del server OPC UA il gruppo di certificati ha il nome "OPC UA server".

CertificateGroup nel modello indirizzi

La figura seguente mostra la struttura dell'oggetto "CertificateGroups" all'interno del nodo "ServerConfiguration".



Il Display Name del CertificateGroups (ad es. "OPC UA server" può essere modificato in STEP 7 (TIA Portal):

1. Navigare nella finestra di ispezione (Proprietà della CPU) fino alla sezione "Protezione & Security > Gestione certificato".
2. Attivare l'opzione "Utilizza i certificati forniti dalla gestione certificati durante il runtime".
3. Modificare il nome (DisplayName) del gruppo di certificati nella tabella sottostante. Sono consentiti da 1 a 64 caratteri in formato ASCII 7 bit.
   Nella prima colonna è indicato il servizio attivato per il quale possono essere trasferiti i certificati in runtime, mentre nella colonna "ID" è riportato un identificatore numerico fisso utilizzato internamente dalla CPU per referenziare i certificati.

Esempio di visualizzazione nell'area "Gestione certificato":

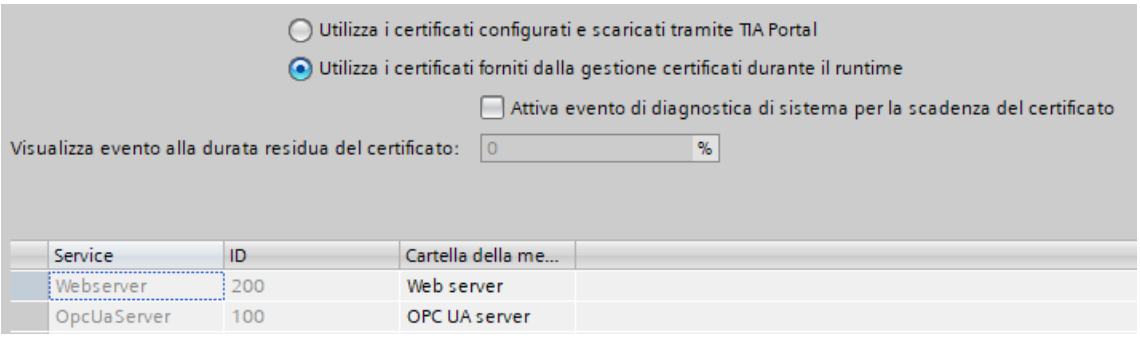


Figura 11-7 Impostazioni nella Gestione certificato

Nodo "CertificateTypes"

La variabile "CertificateTypes" specifica i NodeId dei tipi di certificati che sono assegnati all'applicazione server.

Per il servizio server OPC UA, ad es. è supportato il CertificateType "RsaSha256ApplicationCertificateType" e per il servizio Web server il CertificateType "HttpsCertificateType".

Nodo "TrustList"

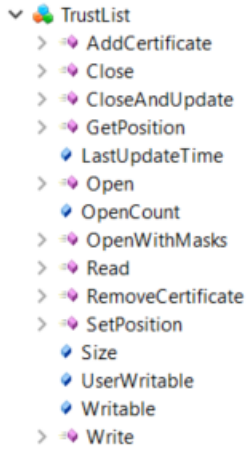
Il nodo per l'oggetto elenchi attendibili (file TrustList) definisce un tipo di file OPC UA (Binary encoded stream) che contiene l'informazione su quali certificati e CRL possono essere letti e aggiornati nella cartella "pki store\trusted\issuer" della Memory Card. Questo nodo fornisce metodi e attributi che rendono possibile la lettura e l'aggiornamento.

Il nodo è un'istanza del tipo di dati OPC UA "TrustListDataType" con la seguente struttura:

Parametro	Tipo di dati	Descrizione
specifiedLists	TrustListsMasks	Maschera di bit che indica quali elenchi contengono informazioni.
trustedCertificates	ByteStrings	Elenco dei certificati dell'applicazione e dei certificati CA considerato attendibile.
trustedCrls	ByteStrings	CRL per i certificati nell'elenco "trustedCertificates".
issuerCertificates	ByteStrings	Elenco dei certificati CA necessari per la convalida dei certificati CA firmati.
issuerCrls	ByteStrings	CRL dei certificati CA nell'elenco "issuerCertificates".

Struttura del nodo "TrustList"

Il nodo "TrustList" ha la seguente struttura:



Metodi e attributi per il nodo "TrustList"

Nel seguito si trova, alla voce "TrustList", una descrizione dei nodi che integrano i metodi di Object Type "FileType". Il TrustList Type deriva da FileType (vedere OPC 10000-5: OPC Unified Architecture, Part 5: Information Model).

Metodo / Attributo (variabile)	Descrizione
LastUpdateTime	Variabile che indica la data e l'ora dell'ultimo aggiornamento.
OpenWithMasks	Metodo che consente a un client di leggere solo una parte della TrustList.
CloseAndUpdate	Metodo per chiudere il file TrustList e applicare le modifiche.
AddCertificate	Metodo per aggiungere un singolo certificato alla TrustList.
RemoveCertificate	Metodo per rimuovere un singolo certificato dalla TrustList.

Descrizione dei metodi

La descrizione dei metodi con i relativi Result Codes, Attributi e Tipi dell'oggetto TrustList è disponibile nella specifica OPC UA Parte 12, Discovery and Global Services.

11.2.8 Sicurezza basata sui ruoli in OPC UA

11.2.8.1 Nozioni utili su Security basata sui ruoli

In OPC UA, il concetto di sicurezza basata sui ruoli è definito nella Parte 18 delle specifiche OPC UA (OPC 10000-18: UA Part 18: Role-Based Security). Sono rilevanti anche le parti 3 e 5 delle specifiche OPC UA, che contengono singoli aspetti della definizione dei ruoli, ad es. quali ruoli un server deve supportare con quali autorizzazioni e quali oggetti con quali attributi o proprietà sono definiti nell'area degli indirizzi.

Grazie alla realizzazione del concetto di ruolo per le CPU S7-1500 a partire dalla versione firmware V4.0, il server OPC UA è in grado di gestire l'accesso dei client all'area indirizzi a un livello estremamente specifico.

Diritti di accesso OPC UA individuali ai nodi nell'area indirizzi

Grazie alla sicurezza basata sui ruoli in OPC UA è possibile configurare attraverso le interfacce server OPC UA/le specifiche Companion quali ruoli determinano le opzioni di accesso ai nodi nei namespace preesistenti e con quali autorizzazioni.

Le opzioni di configurazione dei ruoli e delle autorizzazioni consentono, insieme alla gestione utenti di TIA Portal (utenti e ruoli), di limitare efficacemente l'accesso.

Correlazione tra ruoli/autorizzazioni per OPC UA e tra ruoli/diritti di accesso alle funzioni per utenti e ruoli

Gli utenti definiti nelle impostazioni Security del progetto, nell'ambito della gestione utenti centrale o locale (utenti e ruoli), vengono inclusi nel controllo degli accessi al server OPC UA nel seguente modo: possono accedere al server OPC UA soltanto gli utenti che dispongono del diritto di accesso alla funzione "Accesso al server OPC UA".

- La gestione utenti locale o centrale della CPU è responsabile dell'autenticazione degli utenti (client OPC UA) che accedono al server OPC UA.
- La responsabilità legata ai controlli dell'autorizzazione degli utenti (client OPC UA), ovvero di appurare se un utente sia autorizzato ad eseguire l'azione richiesta (ad es. di lettura e scrittura su un nodo), è in capo al server OPC UA della CPU.

  La configurazione del controllo dell'accesso per il server OPC UA avviene nell'interfaccia server OPC UA specifica. All'editor delle interfacce del server OPC UA è stata aggiunta l'area "Controllo dell'accesso". In questo campo sono possibili le seguenti impostazioni:

  – Assegnazione di ruoli esistenti ai ruoli OPC UA (dalle Impostazioni Security del progetto > Utenti e ruoli).
  – Assegnazione di autorizzazioni standard per il namespace dell'interfaccia del server. Inoltre è possibile definire per i namespace ad es. che una data azione sia consentita ad un ruolo solo a determinate condizioni, ad es. a condizione che i messaggi siano firmati e crittografati.
  – Adattamento delle autorizzazioni standard per i singoli nodi dell'interfaccia del server/della specifica Companion: Nella scheda separata "Gestione degli accessi" dell'editor dell'interfaccia del server è possibile adeguare le autorizzazioni per ciascun ruolo a livello di nodi (nella CPU: variabili).

Nel funzionamento questo fa sì che alla sessione di un utente connesso vengono assegnati uno o più ruoli. I ruoli assegnati rendono possibile l'accesso ai nodi nell'area indirizzi solo se le autorizzazioni OPC UA dei ruoli relative a questo nodo e le limitazioni di accesso impostate lo consentono (ad es. Read o Write).

Ruoli utente nel server OPC UA

Per le specifiche Companion importate con i dati della gestione utenti è disponibile una vista dell'interfaccia server, che oltre ai ruoli della gestione utenti (utenti e ruoli) visualizza anche i ruoli OPC UA importati. In questa vista è possibile una mappatura tra i ruoli OPC UA e i ruoli nel progetto. Per ogni ruolo viene visualizzato anche il namespace in cui il ruolo è definito.

Per alcuni ruoli OPC UA predefiniti nel namespace 0, sono stati definiti ruoli quali ad es. "AuthenticatedUser", per i quali non esiste un corrispondente diretto in "Utenti e ruoli". Ad ogni utente che si autentica con il proprio nome utente/password al momento dell'accesso alla CPU vengono assegnati i diritti di accesso del ruolo "AuthenticatedUser".

Ruoli e autorizzazioni per OPC UA

Nell'editor per gli utenti e i ruoli è possibile creare un ruolo, disponibile per l'ulteriore configurazione delle interfacce del server.

I ruoli e le autorizzazioni OPC UA possono essere assegnati per elementi delle interfacce del server (variabili, metodi) e per interi namespace (ovvero per tutti i nodi del namespace).

È possibile assegnare le seguenti autorizzazioni OPC UA a un ruolo:

- Browse - Un client con questa autorizzazione può vedere i riferimenti a/da questo nodo, ovvero anche per tutti gli attributi ad eccezione degli attributi Value e RolePermissions.
- Read - Un client con questa autorizzazione può leggere l'attributo value.
- Write - Un client con questa autorizzazione può scrivere l'attributo value.
- Call - Un client con questa autorizzazione può richiamare il metodo corrispondente, valido per gli oggetti, i tipi di oggetti o i metodi.
- Receive events - Un client con questa autorizzazione può ricevere messaggi (eventi) (Alarms and Conditions).
- Read Role Permissions - Un client con questa autorizzazione può leggere l'attributo RolePermission.

È possibile attivare ulteriori limitazioni di accesso per i namenspace e anche per i singoli nodi:

- Signing Required - Un client ha accesso ai nodi solo se viene utilizzato un SecureChannel che firma digitalmente i messaggi. Vedere anche la descrizione della restrizione "Apply Restrictions to Browse".
- Encryption Required - Un client ha accesso ai nodi solo se viene utilizzato un SecureChannel che cripta i messaggi. Vedere anche la descrizione della restrizione "Apply Restrictions to Browse".
- Apply Restrictions to Browse - Se questa limitazione di accesso è attivata, i requisiti descritti per "Signing Required" e "Encryption Required" si applicano anche all'autorizzazione di browse.

Requisiti

- S7-1500 CPU con firmware da V4.0
- TIA Portal da V20

Regole

- Per l'assegnazione di ruoli a utenti o gruppi di utenti utilizzare l'editor per utenti e ruoli (impostazioni Security > Utenti e ruoli nella navigazione del progetto).

  Anche il server OPC UA utilizza questi utenti e gruppi di utenti; il servizio di autenticazione durante il login è gestito dalla CPU o da un server UMC.
- L'utente collegato deve avere il diritto di accesso alla funzione "Accesso al server OPC UA".
- L'inserimento di ruoli aggiuntivi durante il runtime non è possibile, tutti i ruoli e le relative autorizzazioni OPC UA per l'area indirizzi devono essere configurati e caricati nella CPU prima della messa in servizio.

  Per una maggiore flessibilità per quanto concerne gli utenti, utilizzare un server UMC per la gestione utenti centrale e riunire in gruppi i singoli utenti.
- OPC UA prevede diversi criteri per autorizzare l'accesso al server, nel gergo di OPC UA si tratta di "Mapping Rules", ad es.:
  - User Identity: L'accesso dipende dall'identità dell'utente
  - Application Identity: L'accesso dipende dall'ApplicationUri specificata nel certificato del client.
  - Endpoint: L'accesso dipende dall'URL utilizzato per accedere al server.

  Il server OPC UA della CPU S7-1500 convalida l'autorizzazione solo tramite User Identity.
- Il server OPC UA della CPU S7-1500 supporta i "Well-Known Role" definiti nell'OPC 10000-3: UA Part 3: Address Space Model. I ruoli "SecurityKeyServer..." sono definiti nell'OPC 10000-14: UA Part 14 PubSub, capitolo 8.8.

Well-Known Roles

La OPC Foundation dispone di ruoli predefiniti nel namespace 0 (http://opcfoundation.org/UA/); questi ruoli sono disponibili senza una definizione di ruolo separata per ogni server OPC UA che supporta la sicurezza basata sui ruoli.

Esempi di "Well-Known Roles":

Anonymous, AuthenticatedUser, Observer, Operator, Engineer, Supervisor, ConfigureAdmin, SecurityAdmin e Security Key Service Roles.

Questi ruoli possono essere facilmente generati in TIA Portal come ruoli OPC UA standard.

Ulteriori informazioni

Per avere informazioni aggiornate sulla configurazione della Security basata sui ruoli per le CPU S7-1500 consultare le Informazioni sul prodotto (https://support.industry.siemens.com/cs/ww/it/view/68052815).

11.3 Utilizzo della CPU S7-1500 come server OPC UA

11.3.1 Informazioni importanti sul server OPC UA delle CPU S7-1500

11.3.1.1 Il server OPC UA delle CPU S7-1500

Le CPU S7-1500 dal firmware V2.0 dispongono di un server OPC UA. Oltre alle CPU S7-1500 standard il server OPC UA è presente nelle varianti S7-1500F, S7-1500T, S7-1500C, CPU S7-1500pro, CPU ET 200SP, SIMATIC S7-1500 SW Controller e PLCSIM Advanced.

Convenzione: Con la denominazione "CPU S7-1500" si intendono anche le varianti sopra indicate.

Nozioni di base sul server OPC UA della CPU S7-1500

L'accesso al server OPC UA della CPU è possibile da tutte le interfacce Ethernet integrate della CPU S7-1500.

Alle seguenti condizioni via CP non è possibile accedere direttamente al server OPC UA della CPU tramite tramite il bus backplane del sistema di automazione.

- Progettazione con TIA Portal Version dalla V16
- CPU S7-1500 dalla versione firmware 2.8 e CP 1543-1 dalla versione firmware V2.2

Per la progettazione vedere Accesso alle applicazioni OPC UA (Pagina 185).

Non è possibile accedere direttamente al server OPC UA della CPU da un CM tramite il bus backplane del sistema di automazione.

Per l'accesso dai client, il server salva le variabili PLC abilitate e altre informazioni in forma di nodi (vedere Modalità di accesso ai dati del server OPC UA (Pagina 241)). Questi nodi sono collegati tra loro e formano una rete. OPC UA definisce punti di ingresso a questa rete (Well-known Nodes) che consentono di spostarsi verso i nodi subordinati.

Con un client OPC UA è possibile leggere, controllare o scrivere le variabili di un programma PLC, oltre a richiamare i metodi messi a disposizione dal server. Dalla versione 2.5 del firmware è possibile implementare dei metodi, vedere Informazioni utili sui metodi server (Pagina 321).

Classi di nodi

I server OPC UA mettono a disposizione le informazioni sotto forma di nodi (nodes). Un nodo può essere costituito ad es. da un oggetto, una variabile, un metodo o una proprietà.

L'esempio seguente mostra l'area indirizzi del server OPC UA di una CPU S7-1500 (dettaglio del client OPC UA "UaExpert" di Unified Automation).

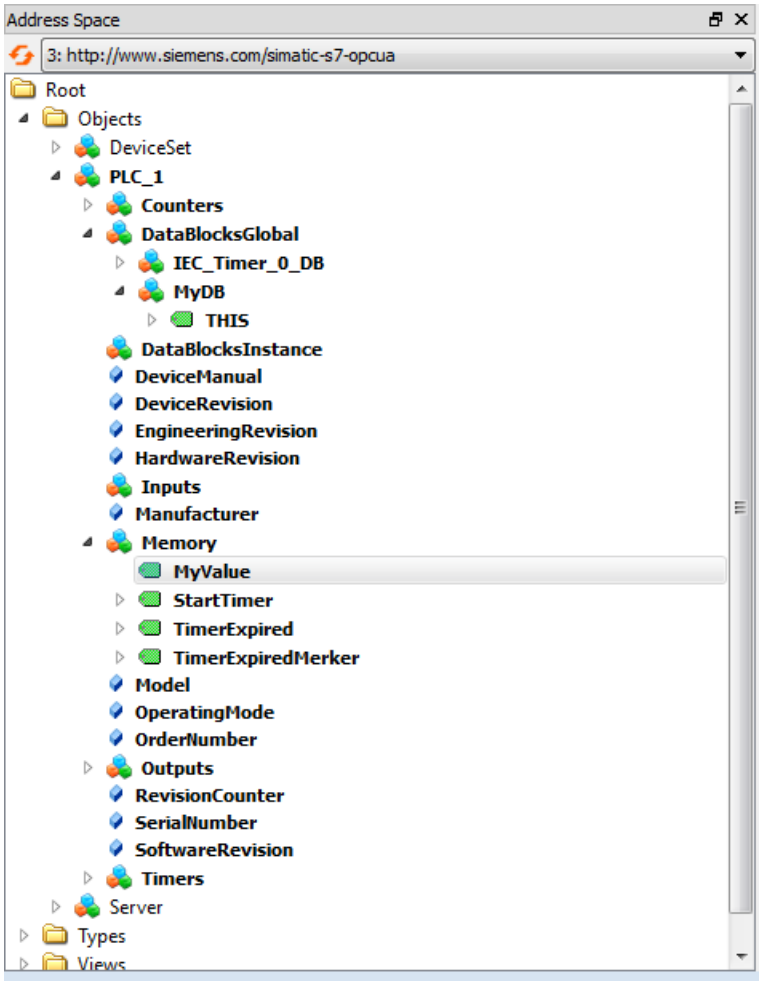


Figura 11-8 Esempio di area di indirizzi del server OPC UA di una CPU S7-1500

Nella figura precedente la variabile "MyValue" è selezionata (evidenziata in grigio).

La variabile si trova sotto il nodo "Memory" che appartiene alla classe "Object".

Anche "Memory" si trova sotto il nodo ""PLC_1" (anch'esso un Object).

Area di indirizzi

I nodi sono collegati tra loro attraverso dei riferimenti, ad es. il riferimento "HasComponent" che rappresenta una relazione gerarchica tra un nodo e i nodi che gli sono subordinati. Attraverso i riferimenti i nodi creano una rete che può avere ad es. una struttura ad albero.

Una rete di nodi viene definita anche area di indirizzi. Partendo dalla radice, tutti i nodi dell'area di indirizzi sono accessibili.

11.3.1.2 Punti finali dei server OPC UA

I punti finali dei server OPC UA definiscono il livello di sicurezza per un collegamento. In funzione dello scopo d'impiego o del livello di sicurezza desiderato, occorre eseguire le impostazioni corrispondenti per il collegamento nel punto finale.

Diverse impostazioni di security

Prima di creare un collegamento sicuro i client OPC UA chiedono al server con quali impostazioni di security è possibile creare i collegamenti. Il server restituisce un elenco con tutte le impostazioni di security (punti finali) che mette a disposizione.

Struttura dei punti finali

I punti finali sono costituiti dai seguenti componenti:

- Identificazione per OPC: "opc.tcp"
- Indirizzo IP: 192.168.178.151 (nell'esempio)
- Numero di porta per OPC UA: 4840 (porta standard)

  Il numero di porta è configurabile.
- Impostazioni di sicurezza per i messaggi (Message Security Modus): None, Sign, SignAndEncrypt.
- Metodo di codifica e hash (Security Policy): Nessuno, Basic128Rsa15, Basic256, Basic256Sha256 (nell'esempio)

Nella figura più avanti si vede il programma "UA Sample Client" della OPC Foundation.

Il client ha creato un collegamento sicuro con il server OPC UA di una CPU S7-1500, con il punto finale "opc.tcp://192.168.178.151:4840 - [SignAndEncrypt: Basic256Sha256:Binary]". Le impostazioni di sicurezza "SignAndEncrypt:Basic256Sha256" sono contenute nel punto finale.

NOTA

Selezione del punto finale con la massima Security Policy possibile per il server

- Attivare solo i punti finali più sicuri del server OPC UA ancora supportati dal client.
- Nel server OPC UA disattivare la Security Policy con il livello di sicurezza più basso.

Creazione di un collegamento con il server (lato client)

- Per creare un collegamento con il server scegliere la Security Policy adatta all'applicazione.
- Per i punti finali attivati del server OPC UA della CPU sono necessari certificati corrispondenti (ad es. un certificato Sha256 per Basic256Sha256).

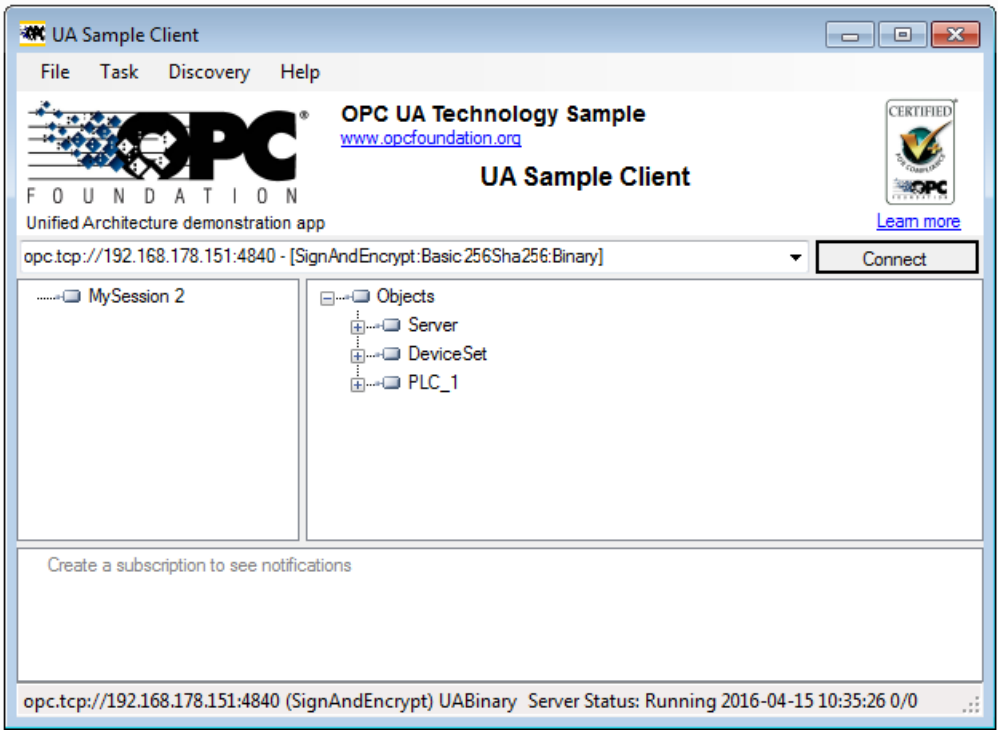


Figura 11-9 Programma "UA Sample Client" della OPC Foundation

Il collegamento con un punto finale del server si può stabilire solo se il client OPC UA soddisfa le impostazioni di security di questo punto finale.

Informazioni messe a disposizione dal server OPC UA

I server OPC UA mettono a disposizione numerose informazioni:

- I valori delle variabili PLC e dei componenti DB ai quali possono accedere i client.
- I tipi di dati di queste variabili PLC e di questi componenti DB.
- Dati sul server OPC UA stesso e sulla CPU.

I client possono così avere una panoramica generale e leggere informazioni mirate. Non è necessario conoscere già il programma PLC e la gestione dati della CPU. Non è necessario chiedere a chi ha sviluppato il programma PLC quando devono essere lette le variabili PLC. Tutti i dati necessari (ad es. i tipi di dati delle variabili PLC) sono memorizzati sul server stesso.

Visualizzazione delle informazioni del server OPC UA

Esistono le seguenti possibilità:

- Online: visualizzare tutte le informazioni disponibili durante l'esecuzione del server OPC UA. Allo scopo si naviga nell'area di indirizzi del server.
- Offline: esportare un file XML basato sugli schemi XML della OPC Foundation.

  Dalla versione V15.1 di STEP 7 vengono esportati anche i metodi server creati dall'utente (istanze FB richiamabili da un client OPC UA), vedere Come mettere a disposizione i metodi del server OPC UA (Pagina 321).
- Offline con l'API Openness: l'API (Application Programming Interface) di TIA Portal può essere utilizzata nel programma per richiamare la funzione che consente di esportare tutte le variabili PLC leggibili da OPC UA (è necessario .NET Framework 4.0, vedere TIA Portal Openness, Automazione dei progetti SIMATIC tramite script (https://support.industry.siemens.com/cs/ww/it/view/109477163)).
- Se si conosce già la sintassi e il programma PLC è possibile accedere al server OPC UA senza ricerche preliminari.

11.3.1.3 Mappatura dei tipi di dati

Tipi di dati SIMATIC e OPC UA

I tipi di dati SIMATIC non corrispondono sempre ai tipi di dati OPC UA.

Le CPU S7-1500 forniscono al proprio server OPC UA le variabili SIMATIC (con tipi di dati SIMATIC) sotto forma di tipi di dati OPC UA, in modo che i client OPC UA possano accedere a queste variabili con tipi di dati OPC UA tramite l'interfaccia del server.

Un client può leggere l'attributo "DataType" di una tale variabile e ricostruire il tipo di dati originale in SIMATIC.

Esempio

Una variabile ha il tipo di dati SIMATIC "COUNTER". L'utente vede nella tabella che COUNTER → UInt16. Ora sa che non deve ricodificare la variabile perché il valore COUNTER viene trasmesso come tipo di dati UInt16.

Dall'attributo "DataType" il client capisce che la variabile è di tipo SIMATIC “COUNTER”. e utilizza questa informazione per ricostruire il tipo di dati.

Tabella 11-1 Tipi di dati SIMATIC e OPC UA

Tipo di dati SIMATIC	Tipo di dati OPC UA
BOOL	Boolean
BYTE	BYTE → Byte
WORD	WORD → UInt16
DWORD	DWORD → UInt32
LWORD	LWORD → UInt64
SINT	SByte

Tipo di dati SIMATIC	Tipo di dati OPC UA
INT	Int16
DINT	Int32
LINT	Int64
USINT	Byte
UINT	UInt16
UDINT	UInt32
ULINT	UInt64
REAL	Float
LREAL	Double
S5TIME	S5TIME → UInt16
TIME	TIME → Int32
LTIME	LTIME → Int64
DATE	DATE → UInt16
TIME_OF_DAY (TOD)	TOD → UInt32
LTIME_OF_DAY (LTOD)	LTOD → UInt64
DATE_AND_TIME (DT)	DT → Byte[8]
LDT	DateTime
DTL Particolarità: la struttura può essere scritta solo per intero con un client OPC UA. In lettura è invece possibile accedere ai singoli elementi che la compongono (ad es. a "YEAR")	Mappato come struttura
CHAR	CHAR → Byte
WCHAR	WCHAR → UInt16
STRING (Codepage 1252 o Windows 1252)	STRING → String
WSTRING (UCS-2; Universal Coded Character Set)	String
TIMER	TIMER → UInt16
COUNTER	COUNTER → UInt16

Array

Un ordine di lettura o di scrittura in OPC UA è sempre un accesso a un array, ovvero fondamentalmente dispone di un indice e una lunghezza. Una variabile singola è una variante eccezionale di un array (indice 0 e lunghezza 1). Il tipo di dati viene semplicemente trasmesso più volte in sequenza. Nella variabile l'attributo "DataType" punta al tipo di dati di base. Dagli attributi "ValueRank" e "ArrayDimensions" si capisce se si tratta di un array e quanto è grande.

Tipi di dati basati su array

Si hanno tipi di dati SIMATIC per i quali viene rappresentato un valore OPC UA su un array di byte. Un array di questi tipi di dati viene rappresentato con un array bidimensionale.

Esempio: Il tipo di dati SIMATIC DATE_AND_TIME (DT) viene sottoposto a mapping su un array di 8 byte (Byte[8]), consultare la tabella riportata precedentemente. Se si definisce un array del tipo di dati SIMATIC DATE_AND_TIME (DT), risulta come array bidimensionale.

Questo influisce ad es. sull’utilizzo di tipi di dati di sistema come OPC_UA_NodeAdditionalInfo e OPC_UA_NodeAdditionalInfoExt:

Per i tipi di dati sopra descritti si deve utilizzare il tipo di dati di sistema OPC_UA_NodeAdditionalInfoExt per array pluridimensionali invece di OPC_UA_NodeAdditionalInfo.

Strutture

Le strutture vengono trasmesse come ExtensionObject. Il server dell'S7-1500 utilizza la rappresentazione binaria per trasmettere gli ExtensionObjects, disponendo i singoli elementi della struttura uno dopo l'altro. Davanti si trova il NodeId del tipo di dati con cui il client rileva la configurazione della struttura.

In OPC UA <= V1.03 il client deve leggere, decodificare e interpretare il DataTypeDictionary completo (sempre che non lo abbia già rilevato offline da un file XML importato).

Da OPC UA V1.04 in poi è disponibile l'attributo DataTypeDefinition che può essere letto e interpretato in modo più semplice e rapido. Il client rileva la configurazione della struttura una sola volta, sia prima che durante il primo accesso e si serve delle informazioni rilevate durante la sessione.

Tipi di dati Simatic specifici

Il client OPC UA non supporta tipi di dati Simatic che non sono presenti nella precedente tabella né che possono essere definiti come elementi di una struttura di un tipo di dati PLC.

Si tratta ad es. del puntatore "ANY" o "POINTER", del blocco funzionale "Block_FB", funzione "Block_FC" o tipo di dati hardware "REMOTE".

La selezione di un tipo di dati non supportato comporta una segnalazione di errore.

Ulteriori informazioni

Per maggiori informazioni sul mapping dei tipi di dati di base, degli array e delle strutture consultare la parte 6 "Mappings" della specifica OPC UA (in particolare il paragrafo "OPC UA BINARY").

Che cosa è necessario osservare negli array e nei tipi di dati DTL e LDT nel server OPC UA di un SIMATIC S7-1500? FAQ (https://support.industry.siemens.com/cs/ww/it/view/109766726)

11.3.1.4 Comportamento del server OPC UA durante il funzionamento

Il server OPC UA è in funzione

Il server OPC UA della CPU S7-1500 si avvia quando l'utente lo attiva e carica il progetto nella CPU.

La procedura per l'attivazione del server OPC UA è descritta qui.

Comportamento nello stato di funzionamento STOP della CPU

Il server OPC UA resta in funzione anche se la CPU passa nello stato di funzionamento "STOP" e continua a rispondere alle interrogazioni dei client OPC UA.

Il comportamento del server in dettaglio:

- Se si interrogano i valori delle variabili PLC si ottengono i valori che erano validi prima che la CPU entrasse o venisse portata in "STOP".
- Se si scrivono valori nel server OPC UA il server li acquisisce.

  Tuttavia la CPU non li elabora perché nello stato di funzionamento "STOP" il programma utente non viene eseguito.

  I client OPC UA possono comunque leggere i valori scritti in STOP dal server OPC UA della CPU.

  Quando viene riavviata la CPU sovrascrive i valori scritti in STOP con i valori iniziali delle variabili PLC.
- Se si richiama un metodo server viene visualizzato il messaggio di errore 16#00AF_0000 (BadInvalidState), perché il metodo (programma utente) non viene eseguito.
- I collegamenti con il server OPC UA vengono conservati in caso di passaggio ad un altro stato di funzionamento (STOP > RUN oppure RUN > STOP). Eccezione: Vengono caricati i dati rilevanti per OPC UA, vedere la sezione seguente.

Il caricamento della CPU può influire sul server OPC UA

Se si carica una CPU con il server OPC UA in funzione, in funzione degli oggetti caricati può essere necessario arrestare e riavviare il server. In questo caso i collegamenti attivi vengono interrotti e devono essere realizzati di nuovo dopo il riavvio del server.

La durata del riavvio dipende principalmente dai seguenti parametri:

- Dalla dimensione della struttura di dati
- Dal numero delle variabili visibili nello spazio di indirizzi OPC UA
- Dall'impostazione della definizione del tipo di dati compatibile con la versione precedente in base alla specifica OPC UA fino a V1.03 (TypeDictionary attivato)
- Dalle impostazioni del carico di comunicazione e del tempo di ciclo minimo, trovate maggiori informazioni qui. (Pagina 400)

Nelle versioni FW della CPU inferiori a V2.8 il server OPC UA viene arrestato e successivamente riavviato ad ogni caricamento nella CPU.

Dalla versione FW V2.8 il comportamento del server OPC UA è stato ottimizzato nel modo seguente:

- Durante il caricamento degli oggetti con la CPU in STOP il server OPC UA si arresta sempre e successivamente si riavvia. In questo caso STEP 7 visualizza un avviso.
- Durante il caricamento di oggetti con la CPU in RUN, il server OPC UA si arresta quando gli oggetti caricati sono rilevanti per OPC UA o potrebbero essere rilevanti per OPC UA. Dopo una reinizializzazione a causa di dati OPC UA modificati, il server OPC UA si riavvia.

  Prima che gli oggetti rilevanti per OPC UA vengano caricati nella CPU e il server OPC UA si arresti, STEP 7 visualizza un avviso nella finestra di dialogo di anteprima del caricamento. Successivamente è possibile decidere se può essere eseguito un riavvio del server per il processo in corso o se il caricamento deve essere interrotto. Questi avvisi vengono visualizzati solo con il server OPC UA in funzione. Se il server OPC UA non è attivato, i dati OPC UA modificati non influiscono sul caricamento.

Esempi

- Si vuole aggiungere solo un ulteriore blocco di codice.
  Non vengono interessati né i blocchi dati né gli ingressi, le uscite, i merker, i tempi o i contatori.
  Reazione durante il caricamento: Un server OPC UA in funzionamento non viene interrotto.
- Si vuole caricare un nuovo blocco dati e il blocco dati è stato contrassegnato come non rilevante per OPC UA.
  Reazione durante il caricamento: Un server OPC UA in funzione non viene interrotto.
- Si vuole sovrascrivere un blocco dati.
  Reazione durante il caricamento: Compare un avviso che il server viene riavviato.
  Motivazione: STEP 7 non può determinare se le modifiche si riferiscono a dati rilevanti per OPC UA o meno.

Lettura dello stato di funzionamento della CPU dal server OPC UA

Come si vede nella seguente figura, il server OPC UA consente di leggere lo stato di funzionamento della CPU:

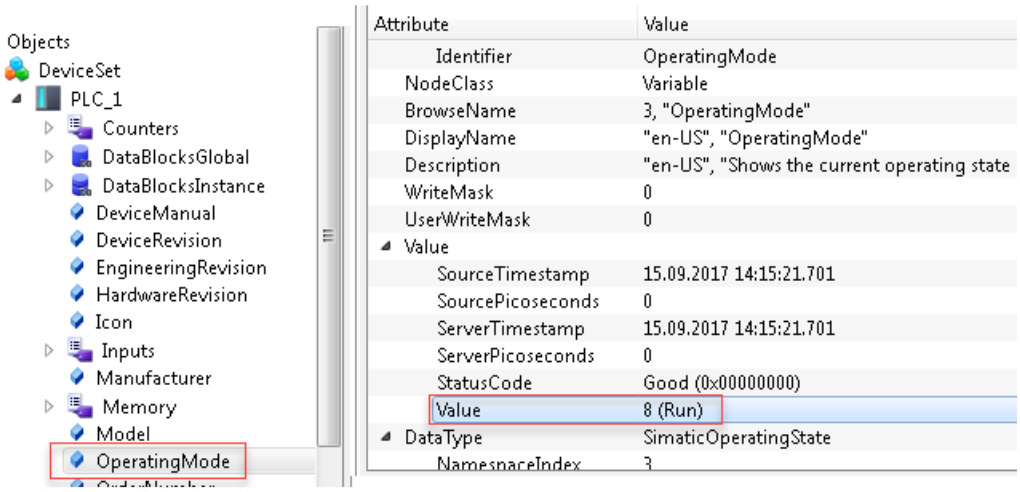


Figura 11-10 Lettura dello stato di funzionamento della CPU dal server OPC UA

Oltre allo stato di funzionamento della CPU è possibile leggere ad es. anche informazioni sul manuale (DeviceManual) o la versione di firmware (HardwareRevision).

11.3.2 Modalità di accesso ai dati del server OPC UA

11.3.2.1 Accessi ai client e accessi locali al server OPC UA

Il server OPC UA fornisce molte informazioni ai client OPC UA all'interno della rete. Di seguito vengono descritte le modalità con cui le variabili CPU (variabili PLC ed elementi DB) vengono messe a disposizione nell'area indirizzi del server OPC UA.

Messa a disposizione delle variabili CPU tramite interfacce server nell'area di indirizzi OPC UA

Il modo più semplice per trasferire automaticamente le variabili della CPU nell'area indirizzi del server OPC UA è il seguente:

- Attivare l'interfaccia server SIMATIC standard nelle proprietà OPC UA della CPU.

  A questo punto tutte le variabili CPU abilitate per OPC UA sono automaticamente disponibili anche nell'area indirizzi OPC UA sotto il nome della CPU.

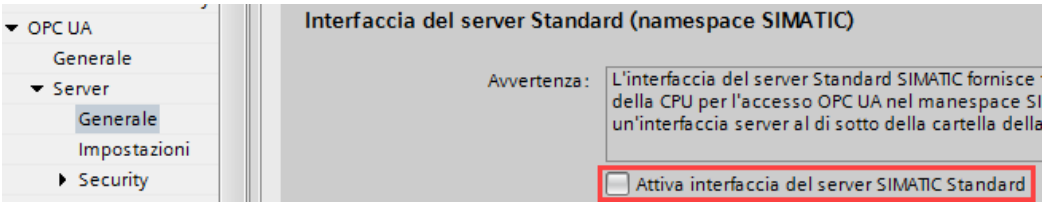


Figura 11-11 Interfaccia server SIMATIC Standard del server OPC UA

L'uso delle interfacce server OPC UA è più flessibile e chiaro; le interfacce server possono essere progettate nella navigazione del progetto (sotto la CPU, nella cartella "Comunicazione OPC UA"). Le interfacce server OPC UA definite dall'utente consentono di assegnare ("mapping") facilmente le variabili OPC UA alle variabili CPU (dati locali).

Interfaccia server OPC UA

Browse Name	Tipo di nodo	Livello di acce...	Dati locali
myServerInterface	Interface	---	
myOPC_UA_Variable	BOOL	RD	"myDataBlock"."myVarBool"
myOPC_UA_Variable2	Word	RD/WR	"myDataBlock"."myVarWord"

Figura 11-12 Interfaccia server personalizzata con variabili CPU mappate

Lo scambio dei dati tra il client OPC UA e il server OPC UA è illustrato nel seguente esempio che riguarda due CPU S7-1500.

Una CPU S7-1500 funge da client e scrive i valori in una variabile OPC UA del server OPC UA. Effettuando la mappatura tra la variabile CPU e la variabile OPC UA, è come se il client OPC UA scrivesse un valore direttamente nella variabile CPU. Per le CPU client S7-1500 utilizzare l'istruzione "OPC_UA_WriteList" insieme ad altre istruzioni necessarie per lo scambio di dati.

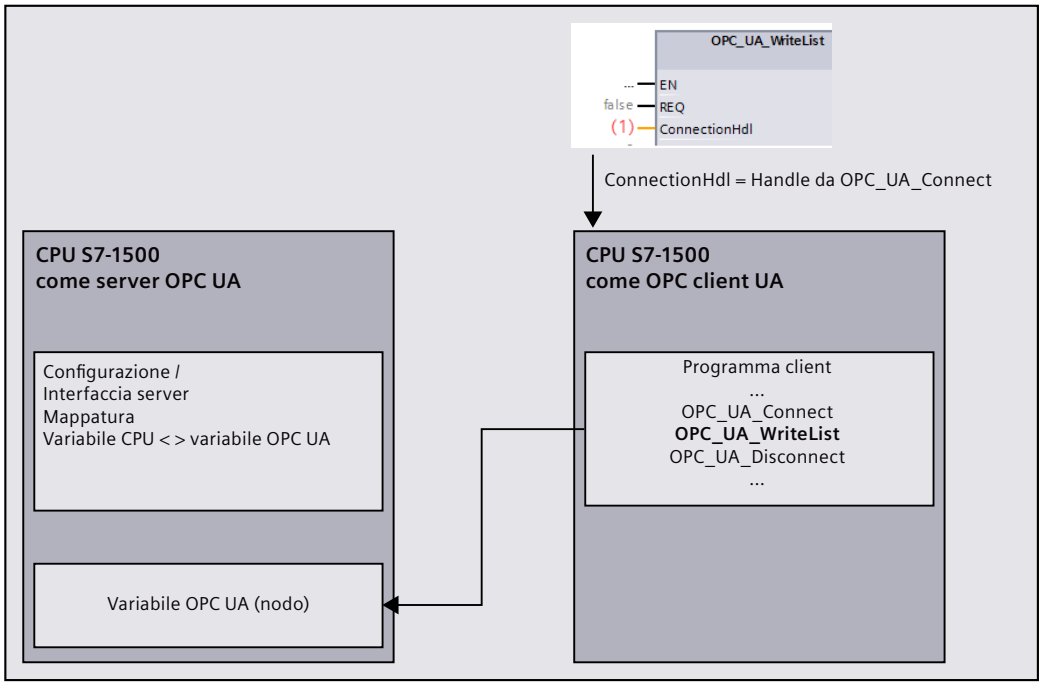


Figura 11-13 Accesso del client alla variabile OPC UA del server

Scrivere i valori delle variabili CPU direttamente nella variabile OPC UA (impostare OPC UA-DataValue)

A partire dalla versione firmware V3.0, oltre alla mappatura delle variabili le CPU S7-1500 offrono anche la possibilità di scrivere i valori direttamente nei nodi di variabile OPC UA locali del server tramite l'istruzione "OPC_UA_WriteList". Generalmente l'istruzione "OPC_UA_WriteList" viene utilizzata nel programma client della CPU per scrivere valori nelle variabili OPC UA di un server OPC UA remoto.

Vantaggio dell'utilizzo di "OPC_UA_WriteList" nel server: Oltre al valore (Value), è possibile fornire al nodo delle variabili OPC UA le seguenti informazioni aggiuntive:

- SourceTimestamp
- StatusCode

OPC UA mette a disposizione il tipo di dati built-in "DataValue". DataValue è una struttura che registra sia il valore (Value) che, come informazioni aggiuntive, il SourceTimestamp e lo StatusCode. La struttura DataValue viene utilizzata solo dai servizi OPC UA, non è possibile scrivere sui suoi elementi direttamente nel programma della CPU. L'accesso in scrittura è possibile solo tramite un uso speciale dell'istruzione "OPC_UA_WriteList".

Possibilità di impiego

Le variabili CPU non possono includere il timestamp che indica l'ultima volta in cui il valore è stato scritto nella variabile CPU. Pertanto, quando si mappano le variabili CPU con le variabili OPC UA sulle interfacce server, il server OPC UA non imposta il SourceTimestamp sulla data/ora in cui la variabile CPU è cambiata, ma sulla data/ora in cui il valore è stato "rilevato" nel server, ad es. da un servizio Read o durante una scansione nell'ambito di una subscription.

Se si scrive DataValue direttamente in un nodo di variabile OPC UA utilizzando "OPC_UA_WriteList", si può specificare come SourceTimestamp per il valore (Value) ad es. un timestamp determinato nel programma.

Principio di funzionamento dell'istruzione "OPC_UA_WriteList" per l'impostazione dei DataValues

È possibile ad es. configurare la struttura DataValue come UDT e trasferire all'istruzione "OPC_UA_WriteList" una variabile di questo tipo di dati. L'istruzione trasferisce quindi gli elementi della variabile in modo coerente al nodo delle variabili OPC UA.

Con il valore del parametro applicativo "ConnectionHdl" si definisce il funzionamento dell'istruzione "OPC_UA_WriteList": istruzione client "normale" o istruzione per la scrittura su nodi di variabili OPC UA locali. In quest'ultimo caso, i client OPC UA possono leggere il valore con informazioni aggiuntive e valutarlo di conseguenza.

Il principio è illustrato nelle seguenti figure, utilizzando come client OPC UA in un caso un client qualsiasi e nell'altro una CPU S7-1500. Nel caso del client della CPU S7-1500 viene rappresentata l'assegnazione degli elementi DataValue ai rispettivi parametri dell'istruzione "OPC_UA_ReadList". L'utente ha pieno accesso a tutti gli elementi della struttura DataValue.

Il valore di "Read" (-42) dell'istruzione "OPC_UA_WriteList" fa sì che nel server venga effettuata una scrittura nei nodi delle variabili OPC UA locali.

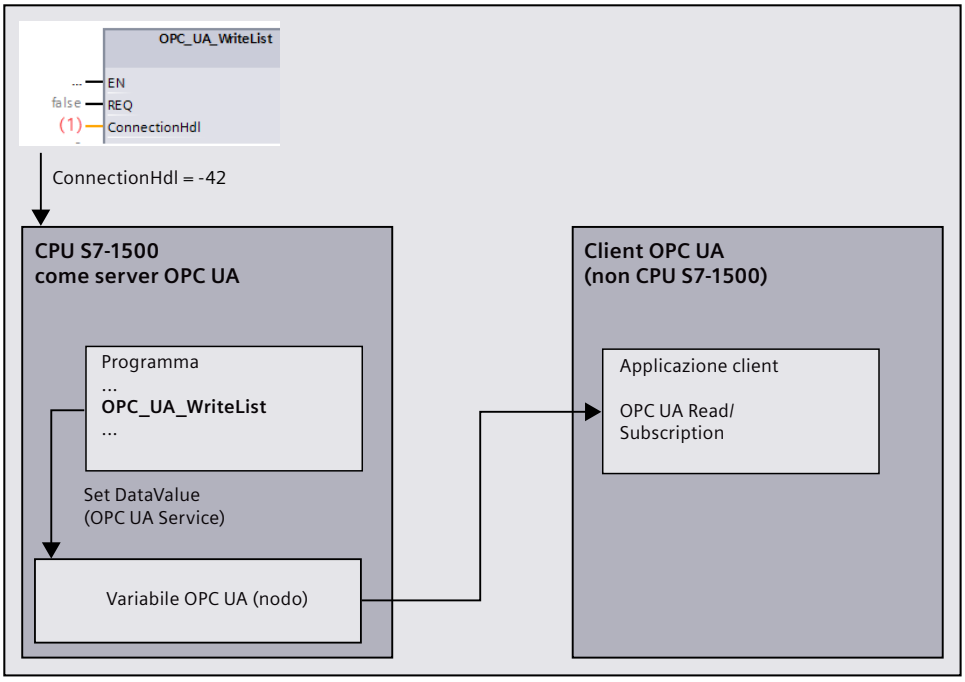


Figura 11-14 Set Data Value nella variabile OPC UA del server

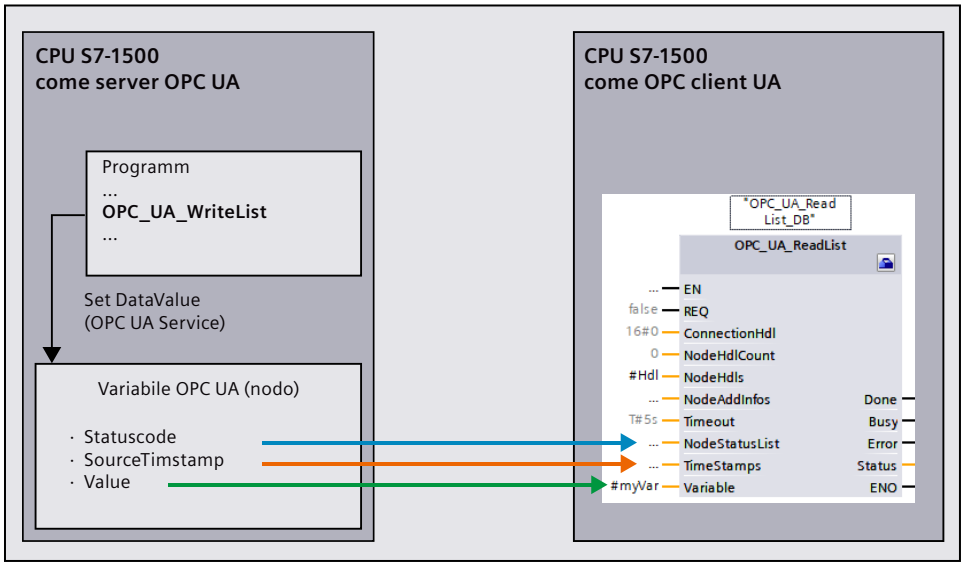


Figura 11-15 Il client legge Data Value (variabile OPC UA del server della CPU S7-1500)

Ulteriori possibilità di impiego

Se i client OPC UA si collegano a una CPU S7-1500 per modificare valori nell'ambito di una subscription (Monitored Items) e l'utente fornisce al DataValue corrispondente sia il valore (Value) che le informazioni aggiuntive sopra descritte, anche le modifiche apportate alle informazioni aggiuntive possono attivare una notifica (Notification).

Esempio: Un valore binario cambia così rapidamente che riprende il suo valore originale entro l'intervallo di campionamento (variazione rapida TRUE > FALSE > TRUE). La variazione del valore non viene rilevata. Viene invece rilevata la variazione del timestamp. Analogamente, la modifica dello StatusCode può causare l'attivazione di una notifica anche senza che il valore cambi.

Condizioni generali

- I client OPC UA possono solo leggere la variabile OPC UA; l'attributo "AccessLevel" per i diritti di scrittura/lettura deve essere impostato di conseguenza per la variabile OPC UA.
- Solo le variabili OPC UA delle interfacce server definite dall'utente possono essere impostate localmente.
- Nell'interfaccia server definita dall'utente non si può effettuare una mappatura sulle variabili CPU per le variabili OPC UA che vengono scritte direttamente.

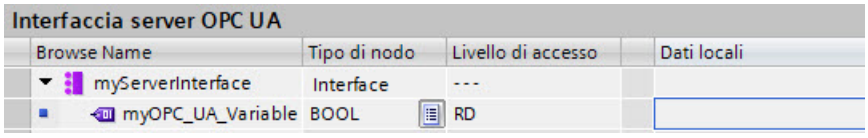


Figura 11-16 Interfaccia server personalizzata:

Per informazioni dettagliate sull'utilizzo dell'istruzione "OPC_UA_WriteList" nel contesto "Impostazione di OPC UA-DataValue" consultare il paragrafo corrispondente della Guida alle istruzioni di comunicazione.

Impostazione degli attributi OPC UA-DataValue per gli array e le strutture

Quando si impostano le variabili OPC UA del tipo Structure o Array tramite "OPC_UA_WriteList" per definire gli attributi OPC UA-DataValue, l'array o la struttura vengono popolati con tutti gli elementi.

I singoli elementi delle strutture o degli array non devono essere modellati come variabili OPC UA secondarie.
Motivo: Se si modellano singoli elementi di array o strutture anche come nodo separato nello spazio degli indirizzi del server come nodo secondario, questi nodi **non** vengono inseriti automaticamente. Per il server OPC UA questi nodi separati sono indipendenti dalla variabile OPC UA sovraordinata di tipo Structure o array, perché non sono mappati su variabili CPU.

Per popolare questi nodi modellati separatamente è necessario creare nel programma i singoli elementi come strutture DataValue separate.

Suggerimento: Per fare in modo che, in questo caso, i client OPC UA vengano informati contemporaneamente delle modifiche apportate ai nodi interessati, impostare i valori di tutte le variabili OPC UA interessate nello stesso richiamo "OPC_UA_WriteList".

Ulteriori informazioni

Un esempio applicativo (https://support.industry.siemens.com/cs/it/it/view/109820694) fornisce supporto per quanto concerne la funzione "Imposta attributi OPC UA-DataValue".

Per informazioni sul coordinamento dei diritti di scrittura e lettura per le variabili della CPU, consultare il capitolo Coordinamento dei diritti di scrittura e lettura per le variabili della CPU (Pagina 249).

Per informazioni su come creare un'interfaccia server definita dall'utente consultare il capitolo Creazione di un'interfaccia server definita dall'utente (Pagina 296).

11.3.2.2 Gestione dei diritti di scrittura e lettura

Abilitazione delle variabili PLC e DB per OPC UA

I client OPC UA possono accedere in lettura e in scrittura alle variabili PLC e DB se queste sono abilitate per OPC UA (preimpostazione). Per le variabili abilitate è attivata la casella di scelta "Accessibile da HMI/OPC UA".

La preimpostazione può essere modificata nelle impostazioni del TIA Portal. Comando "Impostazioni > Programmazione PLC > Generale" nel menu "Strumenti". Nell'area "Interfaccia del blocco/Elementi di blocchi dati" si trovano le relative opzioni.

L'esempio seguente mostra un blocco dati Array.

MyDB

Nome	Tipo di dati	Accessibile da HMI/OPC UA	Scrivibile da HMI/OPC UA	Visibile in HMI Engineering
MyDB	Arr...	☑	☑	☑
MyDB[0]	Int	☑	☑	☑
MyDB[1]	Int	☑	☑	☑
MyDB[2]	Int	☑	☑	☑
MyDB[3]	Int	☑	☑	☑
MyDB[4]	Int	☑	☑	☑
MyDB[5]	Int	☑	☑	☑
MyDB[6]	Int	☑	☑	☑
MyDB[7]	Int	☑	☑	☑
MyDB[8]	Int	☑	☑	☑
MyDB[9]	Int	☑	☑	☑

Figura 11-17 Abilitazione delle variabili PLC e DB per OPC UA

L'array può essere letto per intero in un'unica soluzione dai client OPC UA (vedere Indirizzamento dei nodi (Pagina 189)). In tutti i componenti dell'array sono attivate le caselle di scelta "Accessibile da HMI/OPC UA" e "In scrittura da HMI/OPC UA".

Conseguenza: i client OPC UA possono sia leggere che scrivere questi componenti.

Annullamento dei diritti di scrittura

Se si vuole proteggere una variabile dall'accesso in scrittura si deve disattivare l'opzione "In scrittura da HMI/OPC UA" per quella variabile specifica. In questo modo si annulla il diritto di scrittura del client OPC UA e dei dispositivi HMI.

Conseguenza: Sono consentiti soltanto accessi in lettura dai client OPC UA e dai dispositivi HMI. I client OPC UA non possono assegnare valori a questa variabile e quindi nemmeno influenzare l'esecuzione del programma S7.

Annullamento dei diritti di scrittura e lettura

Per proteggere una variabile dall'accesso in lettura e scrittura si deve disattivare l'opzione "Accessibile da HMI/OPC UA" (segno di spunta non impostato) per quella variabile specifica. Il server OPC UA rimuoverà questa variabile dalla sua area indirizzi. I client OPC UA non vedono più questa variabile della CPU.

Conseguenza: i client OPC UA e i dispositivi HMI non possono né leggerla né scriverla.

Diritti di scrittura e di lettura delle strutture

Se si annulla il diritto di lettura o scrittura di un componente di una struttura, la struttura e il blocco dati non saranno più scrivibili o leggibili in blocco.

Se si annullano i diritti di lettura e di scrittura di singoli componenti di un tipo di dati PLC (UDT), i diritti vengono annullati anche nei blocchi dati che si basano sull'UDT.

Visibile in HMI Engineering

L'opzione "Visibile in HMI Engineering" si riferisce ai tool di engineering Siemens. Se si attiva l'opzione "Visibile in HMI Engineering" (segno di spunta non impostato) non è più possibile progettare la variabile in WinCC TIA Portal.

Questa opzione non ha nessuna conseguenza per OPC UA.

Regole

- Consentire gli accessi in lettura alle variabili PLC e alle variabili dei blocchi dati in STEP 7 solo se necessario per la comunicazione con altri sistemi (controllori, sistemi integrati, MES).

  Non abilitare altre variabili PLC.
- Consentire l'accesso in scrittura da OPC UA solo se sono effettivamente necessari diritti di scrittura per particolari variabili PLC e variabili dei blocchi dati.
- Se è stata resettata l’opzione “Accessibile da HMI/OPC UA” per tutti gli elementi di un blocco dati, quest’ultimo non è più visibile per i client OPC UA nell’area indirizzi del server OPC UA della CPU S7-1500.
- È possibile impedire l'accesso a un intero blocco dati (vedere Gestione dei diritti di scrittura e lettura per l’intero DB (Pagina 248)) anche centralmente. Questa impostazione diventa prioritaria rispetto alle impostazioni dei componenti nell'editor DB.

Ulteriori informazioni

Per informazioni sulla coordinazione dei diritti di scrittura e lettura per le variabili della CPU, consultare il capitolo Coordinazione dei diritti di scrittura e lettura per le variabili della CPU (Pagina 249).

11.3.2.3 Gestione dei diritti di scrittura e lettura per l'intero DB

Disattivazione della visualizzazione dei DB o dei contenuti dei DB per i client OPC UA

E' possibile impedire facilmente l'accesso a un blocco dati completo da parte di un client OPC UA.

Così facendo i dati del DB, compresi i DB di istanza dei blocchi funzionali, non vengono visualizzati per i client OPC UA.

Per default i client OPC UA possono accedere in lettura e in scrittura ai blocchi dati. Questa preimpostazione può essere modificata nelle impostazioni del TIA Portal: Comando "Impostazioni > Programmazione PLC > Generale" nel menu "Strumenti". Nell'area "Preimpostazione per nuovi blocchi" si trova le relativa opzione.

Procedimento

Per fare in modo che un blocco dati non sia visibile ai client OPC UA o per proteggere un blocco dati dall'accesso in scrittura dei client OPC UA procedere nel seguente modo:

1. Selezionare nella navigazione del progetto il blocco dati da proteggere.
2. Selezionare il menu di scelta rapida "Proprietà".
3. Selezionare l'area "Attributi".
4. Attivare/disattivare secondo le proprie esigenze la casella di opzione "DB accessibile da OPC UA".

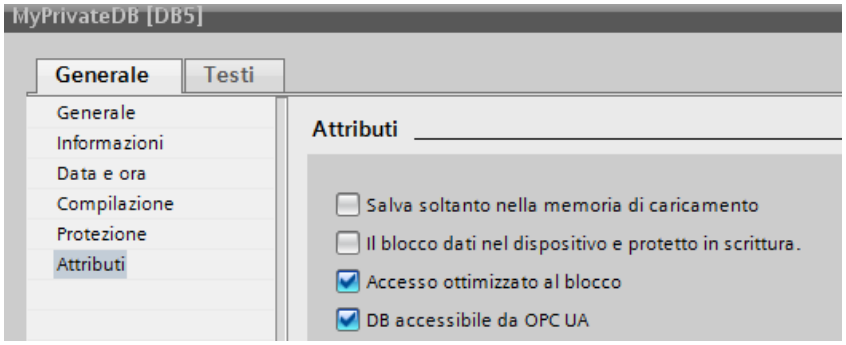


Figura 11-18 Disattivazione della visualizzazione dei DB o dei contenuti dei DB per i client OPC UA

NOTA

Effetto sulle impostazioni nell'editor DB

Se si disattiva la visualizzazione di un DB con l'attributo DB ora descritto, le impostazioni dei componenti dell'editor DB non sono più rilevanti; non è più possibile accedere ai singoli componenti né scrivervi.

Suggerimento: utilizzo della panoramica di tutti i blocchi di programma

Se si utilizzano più blocchi è possibile utilizzare la rappresentazione generale della cartella "Blocchi di programma" per una attivazione e disattivazione mirata della raggiungibilità OPC UA.

Procedere nel modo seguente:

1. Nella navigazione di progetto selezionare la cartella "Blocchi di programma".
2. Attivare il comando "Panoramica" nel menu "Vista".
3. Selezionare la scheda "Dettagli".

   Viene visualizzata una rappresentazione generale dei blocchi con i relativi attributi.
4. Assicurarsi che la colonna "Blocco dati raggiungibile tramite OPC UA" sia attivata.
5. Attivare solo i blocchi dati che devono essere raggiungibili tramite l'OPC UA.

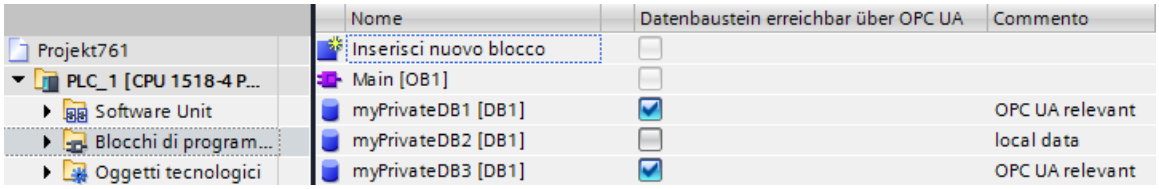


Figura 11-19 Panoramica dei componenti

11.3.2.4 Coordinazione dei diritti di scrittura e lettura per le variabili della CPU

Definizione dei diritti di scrittura e lettura nel modello di informazioni (XML OPC UA)

Nel modello di informazioni OPC UA l'accesso alle variabili è regolato dall'attributo "AccessLevel".

AccessLevel è definito da bit:

bit 0 = CurrentRead e bit 1 = CurrentWrite. Le combinazioni dei bit hanno il seguente significato:

- AccessLevel = 0: nessun accesso
- AccessLevel = 1: read only
- AccessLevel = 2: write only
- AccessLevel = 3: read+write

Esempio di assegnazione dei diritti di scrittura e lettura (read+write)

```
<UAVariable NodeId="ns=3;s=&quot;Data_block_2&quot;.&quot;Static_1&quot;"
BrowseName="3:Static_1"
ParentNodeId="ns=3;s=&quot;Data_block_2&quot;"
DataType="INT"
AccessLevel="3">
    <DisplayName>Static_1</DisplayName>
```

Definizione dei diritti di scrittura e lettura in STEP 7

Quando si definiscono le variabili si stabiliscono i diritti di accesso con le proprietà "Accessibile da HMI/OPC UA" e "In scrittura da HMI/OPC UA".

Esempio di assegnazione dei diritti di scrittura e lettura

Name	Data type	Accessible from HMI/OPC UA	Writable from HMI/OPC UA
Static_1	Int	☑	☑
<Add new>		☑	☑

Figura 11-20 Esempio di assegnazione dei diritti di scrittura e lettura

Interazione dei diritti di scrittura e lettura

Se è stata importata un'interfaccia server OPC UA e nel file XML OPC UA sono impostati attributi AccessLevel, i diritti di scrittura e di lettura vengono definiti in base alla seguente regola: sono attivi i diritti di accesso più bassi di entrambe le impostazioni.

Esempio

- AccessLevel = 1 (read only) nell'interfaccia server OPC UA
- Sia "Accessibile da HMI/OPC UA" che "In scrittura da HMI/OPC UA" è stata attivata nella tabella delle variabili PLC

Risultato: La variabile può solo essere letta.

Regole

Se sono necessari diritti di scrittura:

- AccessLevel = 2 o 3
- "In scrittura da HMI/OPC UA" è attivo

Se sono necessari diritti di lettura:

- AccessLevel = 1 (è possibile anche l'AccessLevel 3 ma è ambiguo. L'impostazione fa pensare che un client OPC UA abbia diritti di scrittura e di lettura)
- "Accessibile da HMI/OPC UA" è attivo, "In scrittura da HMI/OPC UA" è disattivato

Se non si vogliono concedere diritti di lettura e di scrittura (nessun accesso):

- AccessLevel = 0
- "Accessibile da HMI/OPC UA" è disattivato

  Per bloccare qualsiasi tipo di accesso deve essere soddisfatta solo una delle due condizioni. In questo caso è bene valutare con attenzione se la variabile dell'interfaccia server OPC UA sia effettivamente necessaria o meno.

Tabella per l'accesso

"Accessibile da HMI/OPC UA" deve essere impostato perché sia possibile accedere tramite OPC UA. "In scrittura da HMI/OPC UA" deve essere impostato perché un client OPC UA possa scrivere in una variabile/un elemento DB.

I dati riportati nella tabella consentono di dedurre il diritto di accesso.

Tabella 11-2 Tabella per l'accesso

XML OPC UA	STEP 7 (TIA Portal) ad es. tabella delle variabili		
AccessLevel	**Accessibile da HMI/OPC UA**	**In scrittura da HMI/OPC UA**	**Diritto di accesso risultante**
0	x	x	Nessun accesso
x	0	x	Nessun accesso
1	Attivato	x	Read only
2	Attivato	Disattivato	Nessun accesso
3	Attivato	Disattivato	Read only
2	Attivato	Attivato	Write only
3	Attivato	Attivato	Read+write

(x = don't care)

11.3.2.5 Coerenza delle variabili CPU

L'attributo "AccessLevelEx" amplia le proprietà di accesso

Dalla versione firmware V2.6 il server OPC UA della CPU S7-1500 supporta, oltre all'attributo "AccessLevel" (vedere Coordinazione dei diritti di scrittura e lettura per le variabili della CPU (Pagina 249)), anche l'attributo "AccessLevelEx" che, in aggiunta ai bit descritti più sopra per l'accesso in lettura e in scrittura, fornisce informazioni sulla coerenza delle variabili OPC UA. Questo nuovo attributo è stato introdotto con la versione V1.04 della specifica OPC UA (parte 3, Address Space Model).

Lettura delle proprietà che definiscono la coerenza

Nel modello di informazioni OPC UA del server OPC UA l'accesso alle variabili è definito dall'attributo "AccessLevelEx".

AccessLevelEx è definito da bit, quelli di interesse nel nostro caso sono i seguenti:

- Bit 0 = CurrentRead
- Bit 1 = CurrentWrite
- I bit da 2 a 7 non sono rilevanti per il server OPC UA delle CPU S7-1500

Il significato delle combinazioni dei bit è spiegato nel capitolo relativo ai diritti di lettura e di scrittura.

Sono stati aggiunti anche i seguenti bit per le proprietà della coerenza:

- Bit 8 = NonatomicRead; viene impostato se la variabile non viene letta in modo coerente. Se la lettura della variabile è coerente il bit 8=0.
- Bit 9 = NonatomicWrite; viene impostato se la variabile non viene scritta in modo coerente. Se la scrittura della variabile è coerente o se non è possibile accedervi in scrittura, il bit 9=0.

Esempi

La variabile OPC UA (struttura) può essere letta e scritta ma è incoerente per l'accesso in lettura e in scrittura.

Di conseguenza: i bit 0, 1, 8 e 9 sono impostati: AccessLevelEx = "771" (1+2+256+512).

Un'altra struttura è di sola lettura.

Di conseguenza: i bit 0 e 8, 1 sono impostati e i bit 1 e 9 non lo sono: AccessLevelEx = "257" (1+0+256+0).

Gestione dell'attributo nel server

L'attributo "AccessLevelEx" è disponibile solo nel server OPC UA, ma non è contenuto nei file Nodeset (file di esportazione XML).

Tuttavia l’attributo "AccessLevel" che viene esportato riporta l’informazione di “AccessLevelEx”, vedere la prossima sezione.

Esportazione

Durante l'esportazione dell'interfaccia del server SIMATIC standard in un file XML il server imposta l'attributo "AccessLevel" (che diversamente dalla specifica V1.03, nella V1.04 è stato ampliato a 32 bit) sul valore dell'attributo "AccessLevelEx".

Importazione

Durante l'importazione del file Nodeset (ad es. da un file di esportazione di un'interfaccia server) la CPU S7-1500 imposta l'attributo "AccessLevelEx" in base alle informazioni di cui dispone sulla coerenza del tipo di dati importato (vedere il prossimo paragrafo). Il valore importato viene ignorato.

Coerenza dei tipi di dati nell'interfaccia server

La coerenza delle variabili (nel linguaggio di OPC UA: "atomicity") all'interno di un ciclo di programma di una CPU S7-1500 è garantita nei nodi dell'interfaccia server per i seguenti tipi di dati:

- BOOL, BYTE, WORD, DWORD, LWORD
- SINT, INT, LINT, DINT, USINT, UINT, ULINT, UDINT
- REAL, LREAL
- DATE, LDT, TIME, LTIME, TIME_OF_DAY, LTIME_OF_DAY, S5TIME
- CHAR, WCHAR
- Sono coerenti anche i tipi di dati di sistema, ovvero i tipi di dati hardware, che si basano su questi tipi di dati.

  Esempio: HW_ANY, derivato da UINT (UInt16).

Suggerimento: se ci si sposta nell'area di indirizzi della CPU S7-1500 (ad es. con OPC UA Client UaExpert) si trovano i tipi di dati coerenti in Types > BaseDataType > Enumeration/Number/String.

Le variabili dei seguenti tipi di dati **non** sono coerenti (nel linguaggio di OPC UA sono "nonatomic"):

- Generalmente le strutture SIMATIC non sono coerenti. Più precisamente non sono coerenti le variabili che hanno ad es. strutture senza nome o il tipo di dati UDT.
- I tipi di dati di sistema come DTL, IEC_Counter, IEC_TIMER ecc. sono tipi di dati derivati da strutture.
- Le stringhe (Array of Char) non sono coerenti.

Suggerimento: se ci si sposta nell'area di indirizzi della CPU S7-1500 (ad es. con OPC UA Client UaExpert) si trovano i tipi di dati basati sulle strutture in Types > BaseDataType > Structure.

11.3.2.6 Accessi in scrittura alle variabili OPC UA di S7-1500 Motion Control

Oltre alla coerenza dei tipi di dati, la CPU verifica la plausibilità e la validità delle variabili degli oggetti tecnologici.

Se un client OPC UA scrive un valore non valido o non plausibile in una variabile, nella variabile dell'oggetto tecnologico viene mantenuto il valore originale.

Nonostante l'accesso in scrittura non riuscito, viene emesso lo stato "Good".

Esempio 1

Tipo di interpolazione della camma elettronica

La variabile "Cam_1".InterpolationSettings.InterpolationMode deve essere di tipo INT, e può assumere soltanto i valori 1..2.

Se si modifica questa variabile tramite OPC UA con un valore non valido, ad es. 3, viene emesso il codice di stato "Good", ma la variabile non viene modificata.

Esempio 2

Posizionamento dei finecorsa software con un asse di posizionamento

Il valore della posizione del finecorsa HW positivo deve essere maggiore di quello della posizione del finecorsa SW negativo.

"PosAxis_1".PositionLimits_SW.MaxPosition > "PosAxis_1".PositionLimits_SW.MinPosition

Se si modifica una variabile tramite OPC UA con un valore che non soddisfa questa condizione, viene emesso il codice di stato "Good", ma la variabile non viene modificata.

Per conoscere i valori validi per le variabili degli oggetti tecnologici, consultare la Documentazione degli oggetti tecnologici (https://support.industry.siemens.com/cs/ww/it/view/109751049).

11.3.2.7 Modalità di accesso ai dati del server OPC UA

High performance in funzione del caso applicativo

OPC UA è configurato per consentire la trasmissione di numerosi dati in breve tempo. È possibile incrementare notevolmente la potenza leggendo e scrivendo gli array e le strutture per intero anziché accedere alle singole variabili PLC.

Il più veloce è l'accesso agli array. È quindi preferibile raggruppare i dati per i client OPC UA negli array.

Suggerimenti per accedere al server OPC UA dal client OPC UA

- Per accedere ai dati una sola volta o raramente utilizzare il normale accesso Read/Write.
- Per accedere ciclicamente (al massimo ogni 5 secondi circa) a quantità ridotte di dati utilizzare le Subscription.

  Ottimizzare sul server OPC UA le impostazioni per l'intervallo di trasmissione e l'intervallo di campionamento più brevi.
- Per accedere regolarmente (in modo ricorrente) a determinate variabili utilizzare le funzioni "RegisteredRead" e "RegisteredWrite".

Assegnare alla CPU un maggior carico di comunicazione cambiando il valore di "Carico del ciclo a causa della comunicazione". Accertarsi che l'applicazione funzioni correttamente anche con le impostazioni modificate.

Creazione di un DB Array

Gli array possono essere creati ad es. nei blocchi dati globali, nel blocco dati di istanza di un blocco funzionale o come DB Array. Il paragrafo che segue spiega come creare un DB Array.

Per creare un blocco dati con un array (blocco dati array) procedere nel seguente modo:

1. Nella navigazione del progetto selezionare la CPU con il server OPC UA.
2. Fare doppio clic su "Blocchi di programma".
3. Fare doppio clic su "Inserisci nuovo blocco".
4. Fare clic sul pulsante "Blocco dati".
5. Selezionare un nome univoco per il blocco dati o acquisire il nome già inserito.
6. Selezionare nella casella di riepilogo "Tipo" la voce "DB ARRAY".

7. Selezionare nella casella di riepilogo "Tipo di dati ARRAY" il tipo di dati per i singoli componenti dell'array.
8. Immettere il limite superiore dell'array in "Limite dell'Array".
9. Fare clic sul pulsante "OK".

11.3.2.8 Attributo MinimumSamplingInterval

Attributo MinimumSamplingInterval di variabili

Oltre a "Value", "DataType" e "AccessLevel", nel file XML che rappresenta l'area di indirizzi del server è possibile impostare anche l'attributo "MinimumSamplingInterval" per una variabile.

L'attributo indica la velocità con la quale il server può campionare il valore della variabile.

Il server OPC UA della CPU S7-1500 CPU gestisce i valori di MinimumSamplingInterval nel seguente modo:

- I valori negativi e i valori superiori a 4294967 sono impostati a -1; ciò significa: La velocità di scansione minima è indeterminata, il server non indica con quale velocità il valore variabile può essere scansionato.
- I numeri decimali vengono arrotondati a tre cifre dopo la virgola.

11.3.2.9 Esporta file XML OPC UA

Creazione di un file di esportazione OPC UA

La OPC Foundation ha specificato un formato standard, basato su XML, per descrivere i modelli di informazione. In questo modo è possibile mettere anticipatamente a disposizione di un client il modello di informazione di un server OPC UA oppure è possibile caricare modelli di informazione in un server OPC UA. Un file in questo formato viene denominato file Nodeset, perché descrive un modello di informazione come quantità (set) di nodi (node).

STEP 7 (TIA Portal) consente di esportare facilmente il modello di informazione SIMATIC standard della CPU S7-1500 come server in un file OPC UA XML (file Nodeset), comprese le variabili PLC e i metodi abilitati dall'utente per OPC UA:

- Variabili CPU (variabili PLC ed elementi DB)
- Blocchi funzionali con i rispettivi ingressi/uscite

Gli elementi presenti nella CPU, ma non utilizzati nel programma non compaiono nel file OPC UA-XML dopo l'esportazione. Questi elementi non utilizzati possono essere ad esempio:

- UDT non assegnati ad un blocco dati
- Blocchi funzionali con ingressi/uscite senza assegnazione degli ingressi/delle uscite alle variabili CPU

Il file OPC UA XML viene utilizzato per la progettazione offline di un client OPC UA; questo file è configurato secondo le specifiche OPC UA e funge da interfaccia server SIMATIC standard.

Per creare ed esportare il file OPC UA-XML, procedere come indicato nel seguito:

1. Selezionare la CPU. Fare clic sull'icona della CPU (ad es. nella vista di rete).
2. Nelle proprietà della CPU fare clic su "Generale > OPC UA > Server > Esporta".
3. Fare clic sul pulsante "Esporta file XML OPC UA".
4. Selezionare la directory in cui salvare il file di esportazione.
5. Scegliere un nuovo nome per il file. Oppure mantenere il nome già registrato.
6. Fare clic su "Salva".

NOTA

Dalla versione V15.1 di STEP 7 (TIA Portal) i metodi server sono contenuti nel file di esportazione OPC UA (file Nodeset) unitamente ai rispettivi parametri di ingresso e di uscita.

Esportazione separata di tutti gli elementi di un array

Se nelle proprietà della CPU "OPC UA > Server > Esporta" è attivata l'opzione "Esporta tutti gli elementi dell'array come nodi separati", il file XML OPC UA contiene gli elementi degli array sotto forma di singoli elementi XML. Inoltre nel file XML ogni array è a sua volta descritto in un elemento XML.

Se un array contiene molti elementi il file XML può assumere dimensioni notevoli.

Suggerimento

Nella seguente FAQ è descritto un convertitore che consente di convertire il file di esportazione in formato CSV. In questo modo si ottiene un elenco delle variabili della CPU accessibili per OPC UA.

La FAQ è disponibile in Internet (https://support.industry.siemens.com/cs/ww/it/view/109742903).

11.3.3 Configurazione del server OPC UA

11.3.3.1 Attivazione del server OPC UA

Presupposti

- Se si utilizzano **certificati** per la comunicazione protetta (ad es. HTTPS, Secure OUC, OPC UA) assicurarsi che **la data e l'ora** delle unità interessate siano aggiornate. In caso contrario le unità considerano i certificati non validi e la comunicazione protetta non funziona.
- È stata acquisita una licenza di runtime per il funzionamento delle funzioni OPC UA, vedere Licenze per OPC UA (Pagina 281).
- Se è attivata la gestione accessi e si utilizza la gestione utenti (locale o centrale): Gli utenti devono avere il diritto di accesso alle funzioni "Accesso al server OPC UA". Informazioni sull'assegnazione del diritto di accesso alla funzione "Accesso al server OPC UA" sono disponibili nel Siemens Industry Online Support con l'ID dell'articolo: ID articolo SIOS 109954947 (https://support.industry.siemens.com/cs/it/it/view/109954947)

Messa in servizio del server OPC UA

Per ragioni di sicurezza il server OPC UA della CPU non è abilitato nell'impostazione di base. I client OPC UA non possono accedere alla CPU S7-1500 né in lettura né in scrittura.

Per attivare il server OPC UA della CPU, procedere nel modo seguente:

1. Selezionare la CPU. Fare clic sull'icona della CPU (ad es. nella vista di rete).
2. Nelle proprietà della CPU fare clic su "OPC UA > Server".
3. Attivare il server OPC UA della CPU.
4. Confermare le avvertenze di sicurezza.
5. Selezionare l'area "Licenze di runtime" nelle proprietà della CPU e impostare la licenza acquistata per il server OPC UA.
6. Compilare il progetto.
7. Caricare il progetto nella CPU.

   Il server OPC UA della CPU viene quindi avviato.

Le impostazioni vengono mantenute in memoria

Se il server era già attivo ed erano state effettuate delle impostazioni, queste ultime non vanno perse anche se si disattiva il server. Le impostazioni vengono mantenute in memoria e sono disponibili quando si riattiva il server.

Nome dell'applicazione

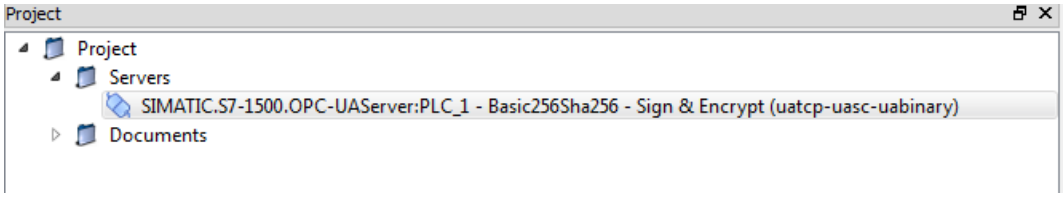
Il nome dell'applicazione è il nome dell'applicazione OPC UA ed è valida per il server e per il client, e viene visualizzato in "OPC UA > Generale":

- La preimpostazione per il nome dell'applicazione è: "SIMATIC.S7-1500.OPC-UA.Application:PLC_1".
- Il nome preimpostato è formato da "SIMATIC.S7-1500.OPC-UA.Application:" e dal nome della CPU selezionato in "Generale > Informazione sul prodotto > Nome", qui "PLC_1).
- Questo nome dell'applicazione consente di identificare il server OPC UA per il partner di comunicazione (client OPC UA), ad es. se un client OPC UA usa il servizio Discovery per rilevare i server accessibili.
- Il nome dell'applicazione visualizzato viene usato dal client OPC UA della CPU per stabilire la comunicazione con un server OPC UA. Più precisamente la CPU inserisce automaticamente questo nome "ApplicationName" nell'istruzione "OPC_UA_Connect" (variabile di tipo "OPC_UA_SessionConnectInfo" nel parametro "SessionConnectInfo" dell'istruzione "OPC_UA_Connect").

  Quando si programma l'istruzione "OPC_UA_Connect" si deve quindi inserire in "ApplicationName" una riga vuota. Il nome dell'applicazione consente ad es. di identificare il client e le sue sessioni (SessionNames).

Se il server è stato attivato, è possibile anche utilizzare un altro nome che sia significativo all'interno del progetto e che soddisfi i requisiti impostati per il progetto, come ad es. l'univocità a livello mondiale.

L'esempio seguente proviene da UaExpert:



Modifica del nome dell'applicazione

Per modificare il nome dell'applicazione procedere nel seguente modo:

1. Selezionare la CPU. Fare clic sull'icona della CPU (ad es. nella vista di rete).
2. Nelle proprietà della CPU fare clic su "OPC UA > Generale".
3. Immettere un nome significativo.

Poiché il nome dell'applicazione è specificato anche nel certificato (Subject Alternative Name), se lo si modifica può essere necessario riemettere il certificato.

11.3.3.2 Accesso al server OPC UA

Indirizzi del server

L'accesso al server OPC UA della CPU S7-1500 è possibile da tutte le interfacce PROFINET integrate della CPU (dalla versione firmware V2.0)

Alle seguenti condizioni via CP non è possibile accedere direttamente al server OPC UA della CPU tramite tramite il bus backplane del sistema di automazione.

- Progettazione in TIA Portal con la CPU S7-1500 V16, dalla versione di firmware 2.8 e CP 1543-1 dalla versione di firmware V2.2

  Per la progettazione vedere Accesso alle applicazioni OPC UA (Pagina 185).

Non è possibile accedere direttamente al server OPC UA della CPU da un CM tramite il bus backplane del sistema di automazione.

Nei SIMATIC S7 1500 SW Controller l'accesso al server OPC UA può essere effettuato tramite le interfacce PROFINET assegnate al PLC software.

Ulteriori opzioni di accesso per i controllori SW sono descritte nel seguente esempio applicativo: Collegamento OPC-UA interno ed esterno tramite interfaccia Ethernet virtuale del Software Controller dalla versione V2.5 (https://support.industry.siemens.com/cs/ww/it/view/109760541).

Esempio di URL (Uniform Resource Locator) con cui è possibile stabilire collegamenti al server OPC UA della CPU:

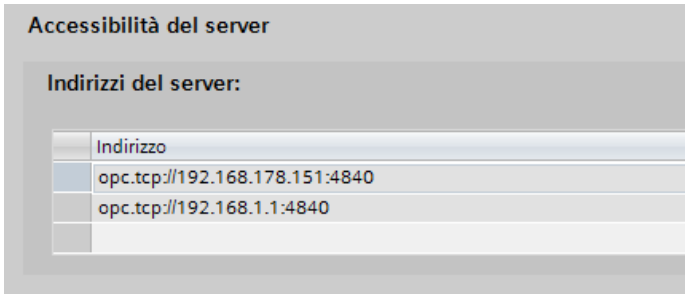


Figura 11-21 Visualizzazione degli indirizzi del server

Gli URL sono composti nel modo seguente:

- ID del protocollo "opc.tcp://"
- Indirizzo IP
  - 192.168.178.151

    Indirizzo IP attraverso il quale il server OPC UA è accessibile dalla sottorete Ethernet 192.168.178.
  - 192.168.1.1

    Indirizzo IP attraverso il quale il server OPC UA è accessibile dalla sottorete Ethernet 192.168.1.
- Numero della porta TCP
  - Preimpostazione: 4840 (porta standard)

    Il numero della porta può essere modificato in "OPC UA > Server > Impostazioni > Porta".

Indirizzi IP dinamici

Nell'esempio seguente l'indirizzo IP dell'interfaccia PROFINET [X2] non è ancora definito.

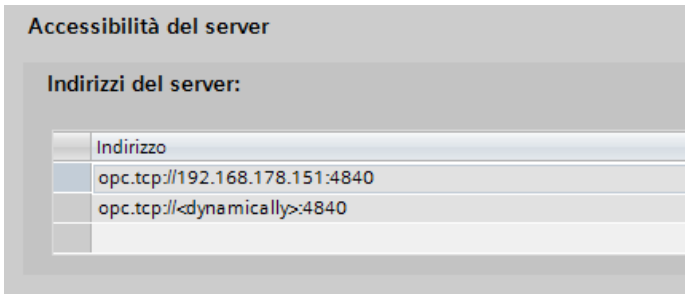


Figura 11-22 Visualizzazione degli indirizzi del server con indirizzo IP dinamico

Nella tabella compare il segnaposto "<dynamically>".

L'indirizzo IP di questa interfaccia PROFINET viene impostato in un secondo momento nel dispositivo, ad es. tramite il display della CPU.

Attivazione dell'interfaccia del server SIMATIC standard

Se è attivata l'opzione "Attiva interfaccia del server SIMATIC Standard", il server OPC UA della CPU mette a disposizione dei client le variabili PLC e i metodi server abilitati, come stabilito da SIEMENS nel namespace definito autonomamente.

Quest'opzione è attivata per default.

Mantenere l'opzione attivata per permettere ai client OPC UA di collegarsi automaticamente al server OPC UA della CPU e di scambiare i dati.

Se non si attiva questa opzione si deve aggiungere l'interfaccia del server con la voce per la "Comunicazione OPC UA" della navigazione del progetto. L'interfaccia verrà quindi utilizzata come interfaccia del server OPC UA, vedere Progettazione dell'interfaccia del server OPC UA (Pagina 282).

NOTA

Informazioni generali sul dispositivo leggibili anche con l'interfaccia del server SIMATIC Standard disattivata

Anche se l'interfaccia del server SIMATIC Standard viene disattivata, i client OPC UA possono leggere le informazioni generali sul dispositivo tramite il server OPC UA della CPU.

Esempi di informazioni generali sul dispositivo: DeviceManual, DeviceRevision, OrderNumber. In questo caso tuttavia alcuni oggetti del programma utente non sono visibili per i client.

Per evitare che queste informazioni sul dispositivo restino nascoste occorre disattivare il server OPC UA della CPU.

11.3.3.3 Impostazioni generali del server OPC UA

Porta TCP per OPC UA

Per default OPC UA utilizza la porta TCP 4840. Tuttavia è possibile anche scegliere una porta diversa. Sono possibili inserimenti da 1024 a 49151. È comunque necessario assicurarsi che non insorgano conflitti con altre applicazioni. I client OPC UA devono utilizzare la porta selezionata per creare i collegamenti.

Nell'esempio seguente è stata scelta la porta 48400:

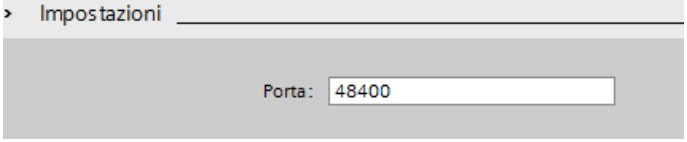


Figura 11-23 Porta TCP per OPC UA

Il capitolo Protocolli di comunicazione e numeri di porta utilizzati nella comunicazione Ethernet (Pagina 38) fornisce una panoramica dei protocolli supportati e dei numeri di porta utilizzati delle CPU S7-1500.

Impostazioni per le sessioni

- Timeout massimo della sessione

  In questo campo si definisce il tempo massimo che può trascorrere prima che il server OPC UA interrompa una sessione senza comunicazione.

  I valori possibili vanno da 1 a 600000 secondi.

- Numero massimo di sessioni OPC UA

  In questo campo si definisce il numero massimo di sessioni che possono essere create e gestite contemporaneamente dal server OPC UA della CPU.

  Il numero massimo delle sessioni dipende dalle prestazioni della CPU. Ogni sessione occupa delle risorse.

Numero massimo di nodi registrati

In questo campo si definisce il numero massimo di nodi (node) registrati dal server OPC UA.

Il numero massimo di nodi registrati dipende dalle prestazioni della CPU e viene visualizzato quando si definisce il contenuto del campo (inserendo nel campo il puntatore del mouse). Ogni registrazione occupa delle risorse.

NOTA

Il tentativo di registrare un numero di nodi superiore al numero massimo impostato non viene segnalato da un messaggio di errore

Se durante il runtime un client vuole registrare un numero di nodi superiore al numero massimo progettato, il server della CPU S7-1500 registra solo il numero massimo progettato. Dopo tale numero il server restituisce invariato al client gli String Node ID regolari; di conseguenza il vantaggio in termini di velocità viene meno a causa della registrazione di questi nodi. Il client non riceve messaggi di errore.

Durante la progettazione è fondamentale prevedere una riserva sufficiente; tenere conto a tal riguardo del numero massimo di nodi registrabili (ad es. nei dati tecnici della CPU).

Ulteriori informazioni

Per sapere quali porte vengono utilizzate dai diversi servizi per la trasmissione dei dati tramite TCP e UDP e di cosa si deve tener conto quando si impiegano router e firewall consultare la FAQ (https://support.industry.siemens.com/cs/ww/it/view/8970169).

Definizioni del tipo di dati compatibili con le versioni precedenti secondo la specifica OPC UA ≤ V1.03

La specifica OPC UA (<= V1.03) definisce i meccanismi necessari per poter leggere da un server le definizioni dei tipi di dati mediante TypeDictionaries, ad es. per le strutture definite dall'utente (UDT).

Nelle proprietà del server OPC UA della CPU si può definire se la CPU creerà o meno queste definizioni dei tipi di dati compatibili con le versioni precedenti secondo la specifica OPC UA ≤ V1.03 per l'interfaccia del server SIMATIC standard.

Poiché i TypeDictionary sono complessi e generano file XML OPC UA (interfacce server) molto grandi, che devono essere interpretati dal client, nella specifica OPC UA V1.04 è stata prevista una soluzione più semplice (attributo "DataTypeDefinition" sul nodo DataType). Se il client supporta la specifica OPC UA dalla versione V1.04, disattivare l'opzione.

Vantaggi offerti dalle definizioni del tipo di dati secondo alla specifica OPC UA dalla versione V1.04:

- Il server si avvia più velocemente
- La memoria viene utilizzata in modo più efficiente
- La funzione "Browse" reagisce più rapidamente

11.3.3.4 Impostazioni del server per le sottoscrizioni

Subscription anziché interrogazione ciclica

Un'alternativa all'interrogazione ciclica di una variabile PLC (polling) è il controllo di questo valore. Utilizzare una Subscription (abbonamento): Quando il valore delle variabili PLC cambia il server informa il client.

Un server sorveglia per lo più numerosi valori PLC. Perciò il server trasmette a intervalli regolari messaggi (notifiche) al client che contengono i nuovi valori delle variabili PLC.

Vantaggio delle subscription:

- il server parte più velocemente
- la memoria viene utilizzata in modo più efficiente

Con quale frequenza il server trasmette messaggi?

Se si crea una Subscription il client OPC UA stabilisce a quali intervalli vuole ricevere i nuovi valori quando questi subiscono una variazione. Per limitare il carico di comunicazione determinato da OPC UA è possibile stabilire l'intervallo di trasmissione minimo fra i messaggi. A questo scopo utilizzare i parametri per l'intervallo di trasmissione e l'intervallo di campionamento più brevi.

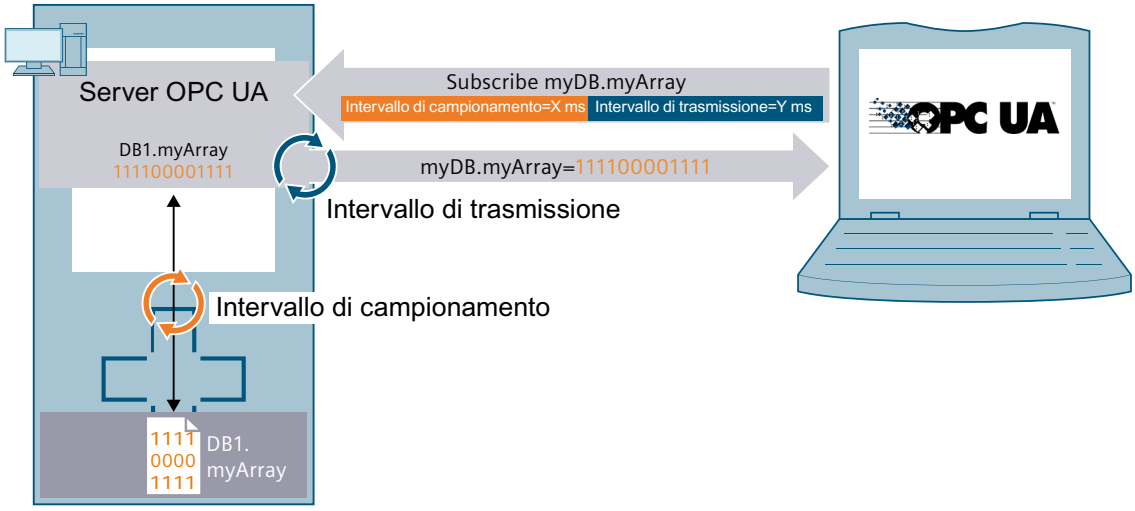


Figura 11-24 Principio di una subscription

Intervallo di trasmissione più breve

Con "Intervallo di trasmissione più breve" si impostano gli intervalli ai quali il server trasmette al client un messaggio contenente il nuovo valore in caso di variazione.

Nella seguente figura viene utilizzato come “Intervallo di campionamento più breve” il valore 250 ms. Come "Intervallo di trasmissione più breve" è inserito il valore 200 ms.

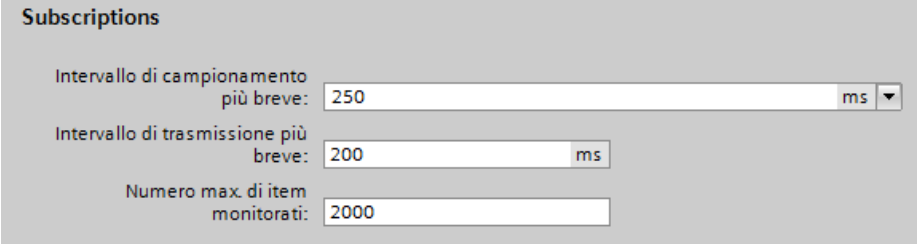


Figura 11-25 Impostazioni delle subscription

Nell'esempio, se il client OPC UA richiede un aggiornamento, quando il valore cambia il server OPC UA invia un nuovo messaggio ogni 200 ms.

Se il client OPC UA richiede un aggiornamento ogni 1000 ms, anche il server OPC UA trasmette una sola volta ogni 1000 ms (un secondo) un messaggio con i nuovi valori.

Se il client OPC UA richiede un aggiornamento ogni 100 ms, il server trasmette comunque solo ogni 200 ms (intervallo di trasmissione più breve).

Intervallo di campionamento più breve

Con "Intervallo di campionamento più breve" si impostano gli intervalli ai quali il server OPC UA rileva il valore di una variabile della CPU e lo confronta con il valore precedente per verificare eventuali variazioni.

Se l'intervallo di campionamento selezionato è inferiore all'intervallo di trasmissione e un client OPC UA richiede una frequenza di campionamento elevata per determinate variabili PLC, si potrebbero avere due o più valori per ogni intervallo di trasmissione.

In questo caso il server OPC UA scrive le modifiche dei valori nella coda d'attesa e al termine dell’intervallo di trasmissione invia tutte le modifiche dei valori al client. Se, durante l'intervallo di trasmissione, si verificano più modifiche dei valori di quante la coda d'attesa ne possa contenere, il server OPC UA sovrascrive i valori meno recenti (in funzione della "Discard Policy" impostata dei dati del client abbonato, in questo caso l'opzione "Discard Oldest" deve essere attiva). I valori più recenti vengono trasmessi al client.

Numero massimo di elementi controllati (Monitored Items)

In questo campo si definisce il numero massimo di elementi che il server OPC UA della CPU controlla contemporaneamente per rilevare le variazioni dei valori.

Il controllo occupa delle risorse. Il numero massimo di elementi controllati dipende dalla CPU utilizzata.

Ulteriori informazioni

Per maggiori informazioni sui limiti di sistema del server OPC UA delle CPU S7-1500 (firmware V2.0 e V2.1) riguardo alle subscription, gli intervalli di campionamento e gli intervalli di trasmissione, consultare questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/109755846).

Quando si utilizzano le subscription, se si verificano errori sono disponibili codici di stato che forniscono informazioni sull'errore specifico. Quando compare un codice di errore, per avere informazioni sulle cause e le soluzioni nel client OPC UA consultare l'elenco dei codici nella Guida in linea di STEP 7 (TIA Portal) o in questa FAQ (https://support.industry.siemens.com/cs/it/de/view/109755860).

Le regole per le subscription sono disponibili nel capitolo Regole per Subscription (Pagina 400).

Per informazioni sulla diagnostica delle subscription consultare il capitolo Diagnostica di Subscription (Pagina 358).

11.3.3.5 Utilizzo del servizio TransferSubscription

Nozioni utili sul trasferimento di Subscription

Le specifiche OPC UA stabiliscono che i client OPC UA possono trasferire una Subscription con i relativi elementi sorvegliati (Monitored Items) da una sessione a un'altra sessione (vedere OPC 10000-4: UA Part 4: Services - in particolare la sezione "TransferSubscriptions").

Il server OPC UA di una CPU S7-1500 supporta il trasferimento di Subscription dalla versione firmware V3.1.4.

Esempi pratici:

- Interruzione/timeout di una sessione attiva; ad es. a causa di un disturbo di comunicazione: Trasferimento della Subscription da una sessione interrotta ad una sessione attiva per evitare la perdita di dati.
- Un client deve essere arrestato; un atro client svolge la Subscription.
- Ripartizione del carico: Trasferimento della Subscription da una sessione attiva ad un'altra sessione attiva o ad una nuova sessione.

Vantaggio di un trasferimento Subscription:

- L'acquisizione di una Subscription evita la perdita di dati (guasto di un client, interruzione del collegamento, sovraccarico).

  Il servizio Transfer Subscription consente di trasferire i dati sottoscritti. Con questo servizio, è possibile risolvere il problema dell'interruzione del collegamento che si verifica nel modo seguente:

  Se il collegamento tra il client che rileva la Subscription e il server è creato, non è necessario ricreare la Subscription con tutti i Monitored Item. Le notifiche accumulate, ovvero non inviate, possono essere ripubblicate dopo il trasferimento della Subscription (Republish). Vedere anche OPC 10000-4: UA Part 4: Services, sezione "Re-establishing connections".

- Acquisendo una Subscription, ai client OPC UA viene risparmiato il processo di creazione di una Subscription, che richiede molto tempo e risorse.

  Quando si crea una Subscription con numerosi elementi sorvegliati, si genera un elevato carico della CPU.

Presupposto

Non è necessaria una configurazione per il server S7-1500 OPC UA; il servizio "TransferSubscription" è fornito su richiesta di un client OPC UA.

Tutte le CPU S7-1500 dal firmware V3.1.4 supportano il trasferimento di Subscription.

Ulteriori presupposti:

- L'utente (client) deve avere un ruolo che gli conferisca l'autorizzazione alla lettura (Read permission).
- Se si vuole trasferire una Subscription di una sessione già chiusa, il processo deve essere completato entro il timeout della Subscription.
- Le Subscription possono essere trasferite sia tra le sessioni di un utente autenticato sia tra le sessioni di utenti anonimi.
  - Per gli utenti autenticati, entrambe le sessioni devono essere assegnate allo stesso utente.
  - Per gli utenti anonimi, anche il collegamento deve essere criptato e le sessioni devono essere state create da client con URI di applicazione identici.

11.3.3.6 Handling dei certificati dei client e dei server

Un collegamento sicuro tra server OPC UA e client OPC UA è possibile solo se il server è in grado di dimostrare la propria identità al client. È a questo che serve il certificato del server.

Certificato del server OPC UA

Se è stato attivato il server OPC UA e le avvertenze per la sicurezza sono state confermate, STEP 7 genera automaticamente il certificato per il server e lo salva nella directory locale dei certificati della CPU. Questa directory può essere visualizzata e gestita (esportazione o cancellazione dei certificati) con la gestione certificato locale della CPU.

La seguente figura mostra la gestione certificato locale della CPU con il certificato generato automaticamente per il server OPC UA:

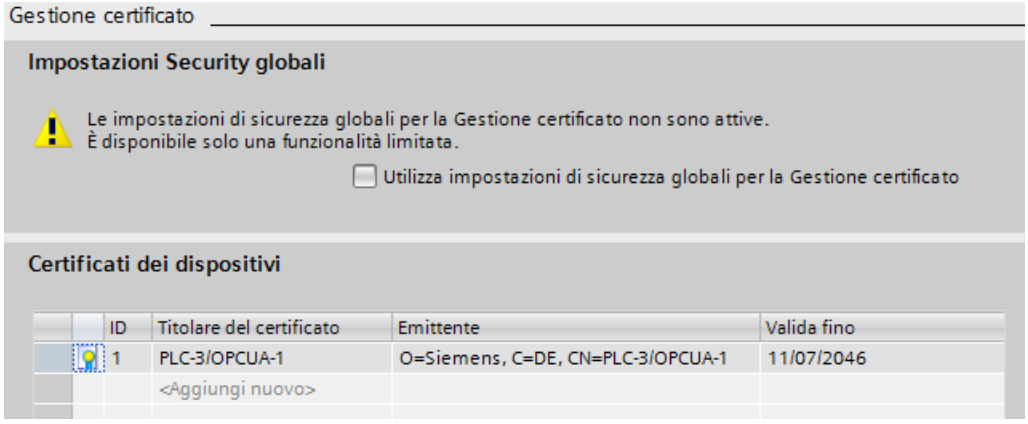


Figura 11-26 Gestione certificato locale della CPU

In alternativa è possibile anche generare individualmente un certificato server.

Il certificato del server viene trasferito dal server al client mentre viene stabilito il collegamento; il client verifica il certificato.

L'utente client decide se considerare attendibile il certificato del server

Sul lato del client, l'utente deve decidere se considerare attendibile il certificato server. Se l'utente considera attendibile il certificato server, il client salva il certificato del server nella sua directory contenente i certificati server attendibili.

L'esempio seguente mostra una finestra di dialogo del client "UA Sample Client". Se l'utente fa clic sul pulsante "Sì" il client considera attendibile il certificato server:

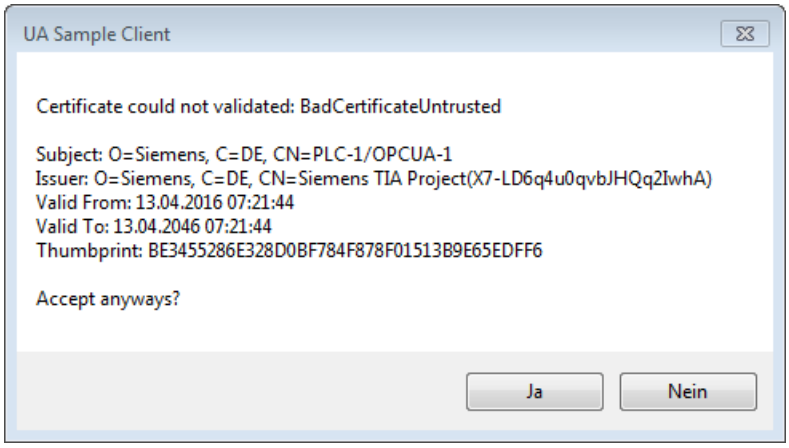


Figura 11-27 Finestra di dialogo del client "UA Sample Client".

Da dove proviene il certificato del client?

Client dell'S7-1500

Se si utilizza il client OPC UA di una CPU S7-1500 (client OPC UA attivato), è possibile creare certificati per questi client con STEP 7 V15 o successiva.

1. Nell'area "Navigazione del progetto" selezionare la CPU che funge da client.
2. Fare doppio clic su "Configurazione del dispositivo".
3. Fare clic su "Protezione & Security > Gestione certificato" nelle proprietà della CPU.
4. Fare doppio clic su "<Aggiungi nuovo>" nella tabella "Certificati dei dispositivi".

   STEP 7 apre una finestra di dialogo.
5. Fare clic sul pulsante "Aggiungi".
6. Selezionare dall'elenco "Destinazione d'uso" la voce "Client OPC UA".

   Attenzione:

   Alla voce "Titolare alternativo del certificato (SAN)" devono essere indicati gli indirizzi IP con i quali la CPU è raggiungibile nell'impianto.

   Prima di creare il certificato client è quindi necessario configurare le interfacce IP della CPU.
7. Fare clic su "OK".

   STEP 7 visualizza il certificato client nella tabella "Certificati dei dispositivi".

8. Fare clic con il tasto destro del mouse sulla riga corrispondente e selezionare la voce "Esporta certificato" nel menu di scelta rapida.
9. Selezionare la directory di destinazione in cui salvare il certificato client.

Client di altri costruttori

Se si utilizzano client UA di altri produttori o della OPC Foundation, al momento dell'installazione o del primo richiamo del programma viene generato automaticamente un certificato client. Questi certificati devono essere importati in STEP 7 dalla gestione certificato ed essere utilizzati per la CPU corrispondente (come mostrato in precedenza).

Se si programma autonomamente un client OPC UA, è possibile creare i certificati nel programma, vedere "Certificato di istanza per il client". In alternativa è possibile creare i certificati con altri tool come OpenSSL o con il generatore di certificati OPC Foundation:

- Il procedimento da adottare in OpenSSL è descritto in "Creazione autonoma di coppie di chiavi PKI e di certificati".
- Il procedimento nel caso del generatore di certificati OPC Foundation è descritto in "Creazione dei certificati autofirmati".

Comunicazione dei certificati client al server

Per poter stabilire un collegamento sicuro è necessario fornire al server i certificati dei client.

Per eseguire questa operazione procedere nel seguente modo:

1. Attivare l'opzione "Utilizza impostazioni di security globali per la Gestione certificato" nella Gestione certificato locale del server. In questo modo diventa disponibile la Gestione certificato globale.

   Questa opzione si trova in “Protezione & Security > Gestione certificato", nelle proprietà della CPU utilizzata come server.

   Se il progetto non è ancora protetto selezionare la voce "Impostazioni Security > Impostazioni" nella navigazione nel progetto di STEP 7, fare clic sul pulsante "Proteggi questo progetto" ed effettuare il login.

   In "Impostazioni Security" di "Navigazione del progetto" di STEP 7 ora compare la voce "Impostazioni Security globali".
2. Fare doppio clic su "Impostazioni Security globali".
3. Fare doppio clic su "Gestione certificato".

   STEP 7 apre la Gestione certificato globale.
4. Fare clic sulla scheda “Certificati affidabili”.
5. Fare clic con il tasto destro del mouse su una superficie libera nella scheda (non su un certificato).
6. Selezionare il comando "Importa" dal menu di scelta rapida.

   Si apre la finestra di dialogo per l'importazione dei certificati.
7. Selezionare il certificato client attendibile per il server.
8. Fare clic sul pulsante "Apri" per importare il certificato.

   Il certificato del client è ora contenuto nella gestione certificato globale.

   Prendere nota dell'ID del certificato client appena importato.

9. Fare clic sulla scheda "Generale" nelle proprietà della CPU utilizzata come server.
10. Fare clic sull'area "OPC UA > Server > Security > Secure Channel".
11. Far scorrere verso il basso la finestra di dialogo "Secure Channel" fino alla sezione "Client affidabili".
12. Fare doppio clic sulla riga vuota della tabella con "<Aggiungi nuovo>". Nella riga viene visualizzato un pulsante con tre puntini.
13. Fare clic su questo pulsante.
14. Selezionare il certificato client importato.
15. Selezionare il pulsante con il segno di spunta verde.
16. Compilare il progetto.
17. Caricare la configurazione nella CPU S7-1500.

Risultato:

Il server ora considera il client attendibile. Inoltre, se il certificato server è considerato attendibile, il server e il client possono stabilire un collegamento sicuro.

Accettazione automatica di tutti i certificati dei client

Se si attiva l'opzione "Accetta automaticamente qualsiasi certificato client durante il tempo di esecuzione" (sotto l'elenco "Client affidabili"), il server accetta tutti i certificati dei client.

ATTENZIONE
Impostazione al termine della messa in servizio Per evitare rischi per la sicurezza, disattivare nuovamente l'opzione "Accetta automaticamente qualsiasi certificato client durante il tempo di esecuzione" al termine della messa in servizio.

Configurazione delle impostazioni di security del server

La seguente figura mostra le impostazioni "Security" disponibili del server per firmare e crittografare i messaggi.

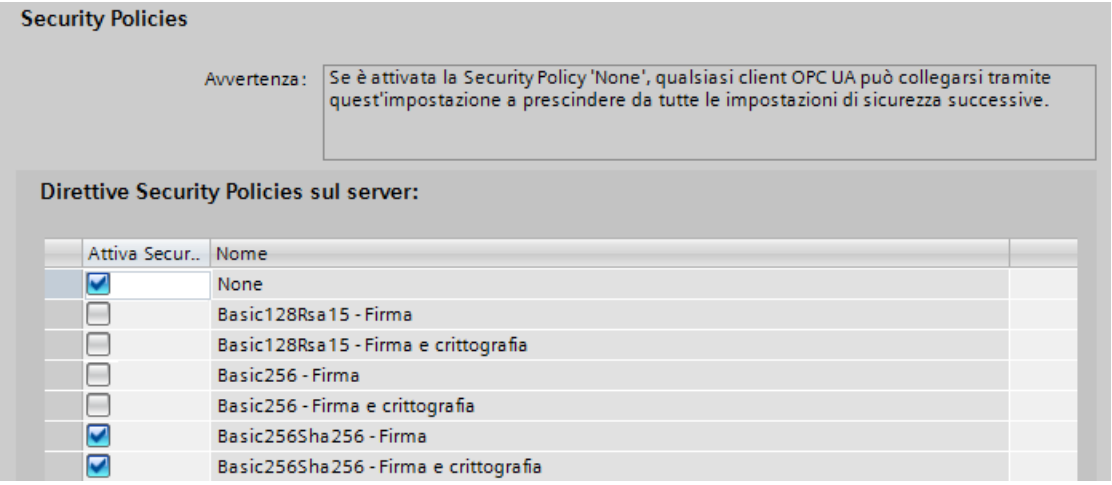


Figura 11-28 Configurazione delle impostazioni di security del server

Per default viene creato un certificato server che utilizza la firma SHA256. Sono abilitate le seguenti Security Policy:

- Nessuna
  Punto finale non sicuro

  NOTA
  Disattivazione delle Security Policy non necessarie
  Se nelle impostazioni del Secure Channel del server OPC UA S7-1500 si selezionano tutte le Security Policy (default) e quindi anche il punto finale "None", il traffico dati tra il server e il client può avvenire anche in modo non sicuro (senza firma e crittografia). Se è impostato "None" l'identità del client rimane sconosciuta. Qualsiasi client OPC UA può collegarsi al server, indipendentemente dalle altre eventuali impostazioni di security effettuate successivamente.
  Quando si progetta il server OPC UA è importante verificare che siano attive solo le Security Policy compatibili con il concetto di sicurezza della propria macchina o impianto. Tutte le altre Security Policy devono essere disattivate.
  Suggerimento: se possibile utilizzare l'impostazione "Basic256Sha256".

- Basic128Rsa15 - Firma
  Punto finale sicuro, supporta una serie di algoritmi che utilizzano l'algoritmo hash RSA15 e la crittografia a 128 bit.
  Questo punto finale garantisce l'integrità dei dati attraverso la firma.
- Basic128Rsa15 - Firma e crittografia
  Punto finale sicuro, supporta una serie di algoritmi che utilizzano l'algoritmo hash RSA15 e la crittografia a 128 bit.
  Questo punto finale garantisce l'integrità e l'attendibilità dei dati attraverso la firma e la crittografia.

- Basic256Rsa15 - Firma
  Punto finale sicuro, supporta una serie di algoritmi che utilizzano l'algoritmo hash RSA15 e la crittografia a 256 bit.
  Questo punto finale garantisce l'integrità dei dati attraverso la firma.
- Basic256Rsa15 - Firma e crittografia
  Punto finale sicuro, supporta una serie di algoritmi che utilizzano l'algoritmo hash RSA15 e la crittografia a 256 bit.
  Questo punto finale garantisce l'integrità e l'attendibilità dei dati attraverso la firma e la crittografia.
- Basic256Sha256 - Firma
  Punto finale sicuro, supporta una serie di algoritmi di hashing a 256 bit e la crittografia a 256 bit.
  Questo punto finale garantisce l'integrità dei dati attraverso la firma.
- Basic256Sha256 - Firma e crittografia
  Punto finale sicuro, supporta una serie di algoritmi di hashing a 256 bit e la crittografia a 256 bit.
  Questo punto finale garantisce l'integrità e l'attendibilità dei dati attraverso la firma e la crittografia.
- Aes256_Sha256_RsaPss - Firma

  Punto finale sicuro, supporta una serie di algoritmi per la crittografia a 256 bit e lo hashing a 256 bit. Tutti i certificati devono utilizzare almeno le firme Sha256. Questo punto finale garantisce l'integrità dei dati attraverso la firma.
  Per requisiti di sicurezza elevati. Infrastruttura PKI necessaria.
- Aes256_Sha256_RsaPss - Firma e crittografia

  Punto finale sicuro, supporta una serie di algoritmi per la crittografia a 256 bit e lo hashing a 256 bit. Tutti i certificati devono utilizzare almeno le firme Sha256. Questo punto finale garantisce l’integrità e la riservatezza dei dati attraverso la firma e la crittografia.
  Per requisiti di sicurezza elevati. Infrastruttura PKI necessaria.

Per abilitare un'impostazione di sicurezza, spuntare la casella nella riga corrispondente.

NOTA

Se si utilizzano le impostazioni "Basic256Sha256 -Firma" e "Basic256Sha256 - Firma e crittografia", il server OPC UA e i client OPC UA devono utilizzare certificati firmati "SHA256".

Con le impostazioni "Basic256Sha256 - Firma" e "Basic256Sha256 - Firma e crittografia" l'autorità di certificazione di STEP 7 firma i certificati automaticamente con "SHA256".

Security Policy “None” e autenticazione tramite nome utente e password

Si possono impostare le seguenti combinazioni:

Security Policy =“None” e autenticazione tramite nome utente e password.

- Il server OPC UA delle CPU S7-1500 supporta questa combinazione. I client OPC UA possono collegarsi e codificare o meno i dati di autenticazione.
- Anche il client OPC UA della CPU S7-1500 supporta questa combinazione: durante il runtime si collega tuttavia solo se può trasmettere i dati di autenticazione codificati.

11.3.3.7 Generazione dei certificati server con STEP 7

La seguente descrizione spiega come creare nuovi certificati con STEP 7 e vale in linea di principio per i diversi utilizzi dei certificati. A seconda dell'area delle proprietà della CPU dalla quale si avvia la seguente finestra di dialogo, STEP 7 mette a disposizione l'utilizzo adatto - in questo caso "OPC UA-Client & -Server".

Consiglio: per usufruire della funzionalità completa per la sicurezza del server OPC UA è consigliabile utilizzare le impostazioni di security globali.

Le impostazioni di security globali possono essere attivate nell'area "Protezione Security > Gestione certificato" delle proprietà della CPU.

Adattamento individuale dei certificati server

STEP 7 genera automaticamente un certificato per il server OPC UA dell'S7-1500 quando si attiva il server (vedere "Attivazione del server OPC UA (Pagina 257)"). Per i parametri del certificato, STEP 7 utilizza valori preimpostati. Per modificare i parametri, procedere nel seguente modo:

1. Nelle proprietà della CPU fare clic su "Generale > OPC UA > Server > Security > Secure Channel > Certificato server" e quindi sul pulsante con i tre puntini. Si apre una finestra di dialogo con i certificati locali disponibili.
2. Fare clic sul pulsante "Aggiungi".

3. Si apre la finestra di dialogo per la creazione di nuovi certificati (seguente figura). I valori per un esempio sono già inseriti.

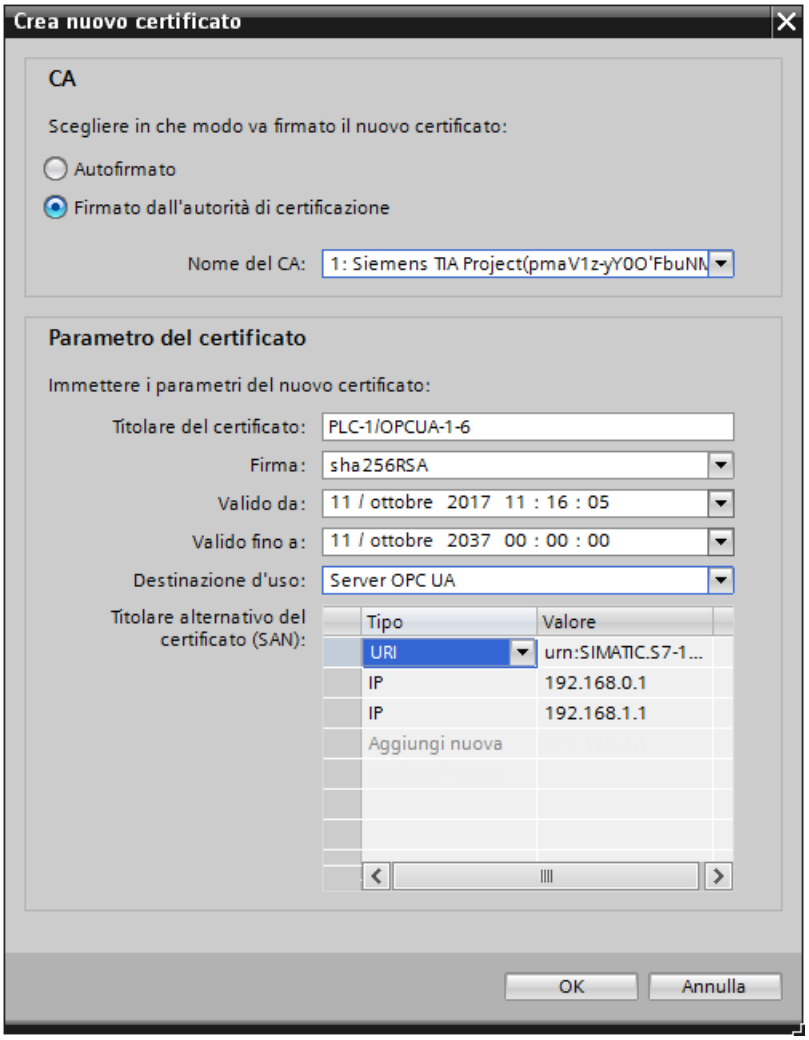


Figura 11-29 Adattamento individuale dei certificati del server

4. Utilizzare altri parametri se le direttive di sicurezza dell'azienda o del committente lo richiedono.

Descrizione dei campi per la generazione dei certificati

- CA

  Scegliere se il certificato debba essere autofirmato o firmato da uno dei certificati CA di TIA Portal. I certificati sono descritti in "Certificati in OPC UA". Per poter creare un certificato che deve essere firmato da uno dei certificati CA di TIA Portal è necessario proteggere il progetto e connettersi con i necessari diritti di accesso alle funzioni. Per ulteriori informazioni vedere "Nozioni di base sulla gestione utenti in TIA Portal".

- Titolare del certificato

  Il nome preimpostato è composto dal nome del progetto e da "\OPCUA-1". Nell'esempio il nome del progetto è "PLC1". Nelle proprietà della CPU selezionare "Generale > Informazione sul progetto > Nome" e impostare il nome del progetto. Mantenere la preimpostazione o immettere nel campo "Titolare del certificato" un nome per il server OPC UA che sia più significativo nel progetto.

- Firma

  Selezionare qui il metodo hash o la crittografia da utilizzare per la firma del certificato server. Sono disponibili le registrazioni seguenti:

  – "sha1RSA",
  – "sha256RSA".

- Valido da

  Immettere qui la data e l'ora in cui inizia la validità del certificato server.

- Valido fino

  Immettere qui la data e l'ora in cui scade la validità del certificato server. Assicurarsi che il certificato non sia valido solo uno o per pochi anni. Nell'esempio il certificato ha una validità di 30 anni. Per motivi di sicurezza, tuttavia, è necessario rinnovare il certificato a intervalli molto più brevi. Un periodo di validità lungo comunque lascia la possibilità di decidere quando è il momento giusto ad es. per la manutenzione dell'impianto.

- Destinazione d'uso

  Per default è impostato "Client e server OPC UA". Mantenere questa preimpostazione per il server OPC UA. La finestra di dialogo "Crea nuovo certificato" può essere richiamata da diversi punti in STEP 7. Se ad es. si richiama questa finestra di dialogo per il server Web della CPU, nella "Destinazione d'uso" viene registrato "Server Web". Nella casella di riepilogo per la destinazione d'uso compaiono le voci seguenti:

  – "Client OPC UA"
  – "Client e server OPC UA"
  – "Server OPC UA"
  – "TLS"
  – "Webserver"

- Titolare alternativo del certificato (SAN)

  Nell'esempio in alto è inserito:
  "URI:urn:SIMATIC.S7-1500.OPC-UAServer:PLC1,IP:192.168.178.151,IP:192.168.1.1".
  Questo URI deve essere inserito correttamente perché viene verificato rispetto alla descrizione dell'applicazione trasmessa.

Sarebbe valida anche la registrazione seguente: "IP: 192.168.178.151, IP: 192.168.1.1". L'importante è che qui siano riportati gli indirizzi IP attraverso i quali il server OPC UA della CPU è accessibile.

Vedere "Accesso al server OPC UA (Pagina 259)".

I client OPC UA possono così verificare se devono effettivamente stabilire un collegamento con il server OPC UA dell'S7-1500 o se invece un pirata informatico sta tentando di trasmettere al client OPC UA valori manipolati da un altro PC.

11.3.3.8 Autenticazione dell'utente

Tipi di autenticazione utente

Nel server OPC UA dell'S7-1500 è possibile impostare come si deve autenticare un utente del client OPC UA se vuole accedere al server.

Esistono le possibilità seguenti:

- **Autenticazione ospite**

  L'utente non deve dimostrare di essere autorizzato (accesso anonimo). Il server OPC UA non verifica l'autorizzazione dell'utente client.

  Per le CPU fino alla versione firmware V3.0: Se si vuole utilizzare questo tipo di autenticazione utente, alla voce "OPC UA > Server > Security > Autenticazione utente" selezionare l'opzione "Attiva autenticazione ospite".

  Per le CPU dalla versione firmware V3.1: Utilizzare la gestione utenti locale per realizzare l'autenticazione degli ospiti tramite l'utente "Anonimo"

  NOTA

  Per aumentare il livello di sicurezza è consigliabile consentire l'accesso al server OPC UA solo agli utenti autenticati.

- **Autenticazione tramite nome utente e password**

  L'utente deve dimostrare di essere autorizzato (nessun accesso anonimo). Il server OPC UA verifica se l'utente client è autorizzato ad accedere al server. Come prova vale il nome utente con la password corretta.

  Per le CPU fino alla versione firmware V3.0: Per utilizzare questo tipo di autenticazione utente procedere nel modo seguente:

  – Selezionare l'opzione "Attiva autenticazione con nome utente e password" alla voce "OPC UA > Server > Security > Autenticazione utente".
  – Disattivare l'autenticazione ospite.
  – Inserire gli utenti nella tabella "Gestione utenti".

    Fare clic sulla voce "<Aggiungi nuovo utente>". Viene creato un nuovo utente con un nome assegnato automaticamente. È possibile modificare il nome utente e immettere la password corrispondente. È possibile aggiungere al massimo 21 utenti.

- **Gestione utenti supplementare tramite le impostazioni di security del progetto**

  Per le CPU fino alla versione firmware V3.0 è disponibile l'opzione "Gestione utenti supplementare tramite le impostazioni di security del progetto". Questa impostazione si trova sotto le impostazioni OPC UA generali (Proprietà della CPU: OPC UA > Generale). Se si attiva questa opzione la gestione utenti del progetto aperto viene utilizzata anche per l'autenticazione dell'utente del server OPC UA: In OPC UA sono quindi validi gli stessi nome utente e password del progetto attuale.

  Per attivare la gestione utenti del progetto procedere nel seguente modo:

  – Fare clic su "Impostazioni Security > Impostazioni" nella navigazione del progetto.
  – Fare clic sul pulsante "Proteggi questo progetto".
  – Inserire nome utente e relativa password.
  – In "Impostazioni Security > Utenti e ruoli" inserire ulteriori utenti.

  Se si configura un ulteriore server OPC UA, attivare nel progetto anche l'opzione "Attiva Gestione utenti supplementare tramite le impostazioni di security del progetto". In questo modo non è necessario inserire nuovamente nomi utente e password.

Trasmissione dell'autenticazione utente tramite il Secure Channel

In OPC UA i dati identificativi per l'autenticazione dell'utente, come il nome utente e la password, vengono trasmessi con una Security Policy specifica. La Security Policy è denominata "UserTokenPolicy".

Quando viene richiesta l'autenticazione utente durante la connessione, il client OPC UA seleziona una "UserTokenPolicy" adatta alle sue esigenze indipendentemente dalle Security Policy impostate per il Secure Channel. La UserTokenPolicy garantisce che lo UserIdentityToken (ad es. il nome utente e la password) venga sempre trasmesso con le impostazioni di security adeguate.

Il client OPC UA ha quindi la possibilità di trasmettere il nome utente e la password in modo crittografato anche se, a causa della Security Policy impostata, viene applicata al Secure Channel la policy "No Security". Per informazioni sulla connessione sicura in OPC UA vedere Trasmissione sicura dei messaggi (Pagina 207).

11.3.3.9 Gestione utenti e ruoli con diritti di accesso alle funzioni OPC UA

Le opzioni di autenticazione utente descritte di seguito fanno riferimento alle impostazioni centrali degli utenti del progetto.

- Server:

  parametrizzazione delle proprietà della CPU (OPC UA > Server > Security > Autenticazione utente). Qui è disponibile l'opzione "Gestione utenti supplementare tramite le impostazioni di security del progetto".

- Client:

  configurazione dell'interfaccia del client (scheda "Configurazione", area "Security"). Qui è disponibile l'opzione "Utente (TIA Portal - Impostazioni Security)".

Presupposti

Per poter modificare le impostazioni di security è necessario che il progetto sia protetto e che l'utente connesso disponga di diritti sufficienti, ad es. diritti di amministratore.

Impostazioni nella navigazione del progetto > "Impostazioni Security"

Le impostazioni utente e i ruoli centrali sono indicati nell'area "Impostazioni Security" nella navigazione del progetto protetto. In questa area si definiscono centralmente gli utenti specificandone il nome, la password e i diritti di accesso alle funzioni. Queste impostazioni possono essere riutilizzate facilmente in un altro punto.

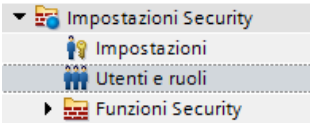


Figura 11-30 Impostazione utenti e ruoli

Riutilizzo delle impostazioni di security centrali

Le impostazioni di security possono essere riutilizzate ad esempio nei seguenti punti:

- Selezione utente per l'autenticazione utente nel server OPC UA

  Con questa impostazione si comunica al server quale client (utente) ha accesso al server, con quale nome e quale password.

- Selezione utente per l'autenticazione del client OPC UA

  Con questa impostazione si comunicano al client il nome e la password con cui può autenticarsi sul server.

Le impostazioni per il client e il server devono coincidere: il nome utente e la password utilizzati dal client per connettersi devono essere impostati anche nel server e avere gli stessi diritti.

Diritti di accesso alle funzioni per il server e il client

Per gli utenti della funzionalità client e quelli della funzionalità server di una CPU S7-1500 è necessario attivare per il client e il server anche i corrispondenti diritti di accesso alle funzioni. Non è sufficiente impostare centralmente solo il nome utente e la password.

Un esempio spiega questo tipo di gestione dei diritti utente.

1. Aprire la scheda "Ruoli" in "Impostazioni Security > Utenti e ruoli" e definire un nuovo ruolo, ad es. con il nome "PLC-opcua-role-all-inclusive".
   Suggerimento: la scheda potrebbe essere coperta da una finestra di informazione ("Lo stato attuale non è ancora stato verificato..."). In questo caso chiudere innanzitutto la finestra.
2. Aprire "Diritti di runtime" e poi "Diritti di funzione CPU" nell'area "Categorie di diritti di accesso alle funzioni", quindi selezionare la CPU di cui si vogliono impostare i diritti di accesso alle funzioni.
3. Nell'area "Diritti di accesso alle funzioni" sono disponibili i seguenti diritti:
   - **Accesso al server OPC UA**

     Questo diritto vale per il server OPC UA della CPU S7-1500. Soltanto se quest'opzione è selezionata l'utente con il ruolo "PLC-opcua-role-all-inclusive" può trasferire nella CPU certificati, CRL o elenchi attendibili in runtime (funzione Push). Questo diritto di accesso alla funzione è richiesto per un handling automatizzato del certificato, ad es. nell'ambito di GDS (Global Discovery Service).
   - **Gestione dei certificati**

     Questo diritto vale per il server OPC UA della CPU S7-1500. Soltanto se quest'opzione è attivata l'utente con il ruolo "PLC-opcua-role-all-inclusive" può trasferire nella CPU certificati, CRL o elenchi attendibili in runtime (funzione Push). Questo diritto di accesso alla funzione è richiesto per un handling automatizzato del certificato, ad es. nell'ambito di GDS (Global Discovery Service).
   - **Autenticazione utente del client OPC UA**

     Questo diritto di accesso vale per il client OPC UA della CPU S7-1500 (per le istruzioni del client). Soltanto se quest'opzione è selezionata l'utente a cui è assegnato il ruolo "PLC-opcua-role-all-inclusive" può utilizzare il nome utente e la password corrispondenti per autenticarsi e creare una sessione con un server.

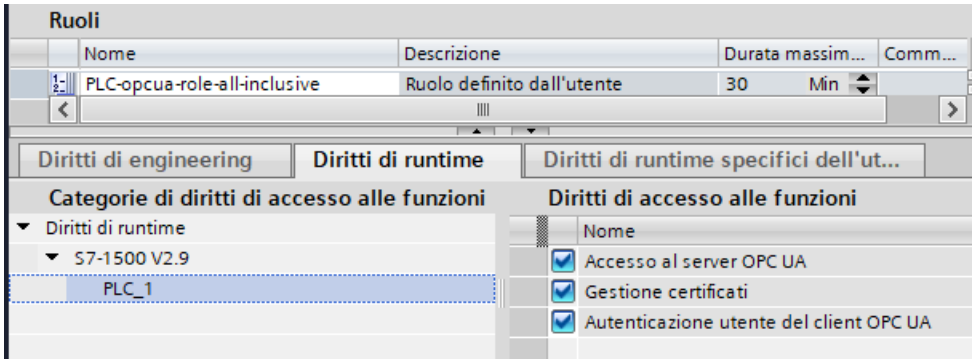


Figura 11-31 Impostazione dei diritti di accesso alle funzioni

4. Si deve inoltre assegnare agli utenti il ruolo "PLC-opcua-role-all-inclusive" (scheda "Utente" nell'area "Impostazioni Security" nella navigazione del progetto).

NOTA

"Runtime-Timeout" per utenti con diritti di accesso alle funzioni OPC UA

I valori nella colonna "Runtime-Timeout" (durata max. della sessione) nella tabella per la configurazione degli utenti non vengono rilevati dalla CPU come diritti di runtime OPC UA.

Un utente non viene quindi disconnesso automaticamente decorso un determinato intervallo. Per questo scopo utilizzare meccanismi OPC UA specifici quali ad es. il parametro "Max. Session Timeout" (area OPC UA > Server > Impostazioni).

11.3.3.10 Impostazioni di diagnostica del server

Diagnostica

L'estensione della diagnostica del server OPC UA si può definire nelle impostazioni della CPU.

Per modificare l'estensione della diagnostica navigare all'area "OPC UA > Server > Diagnostica".

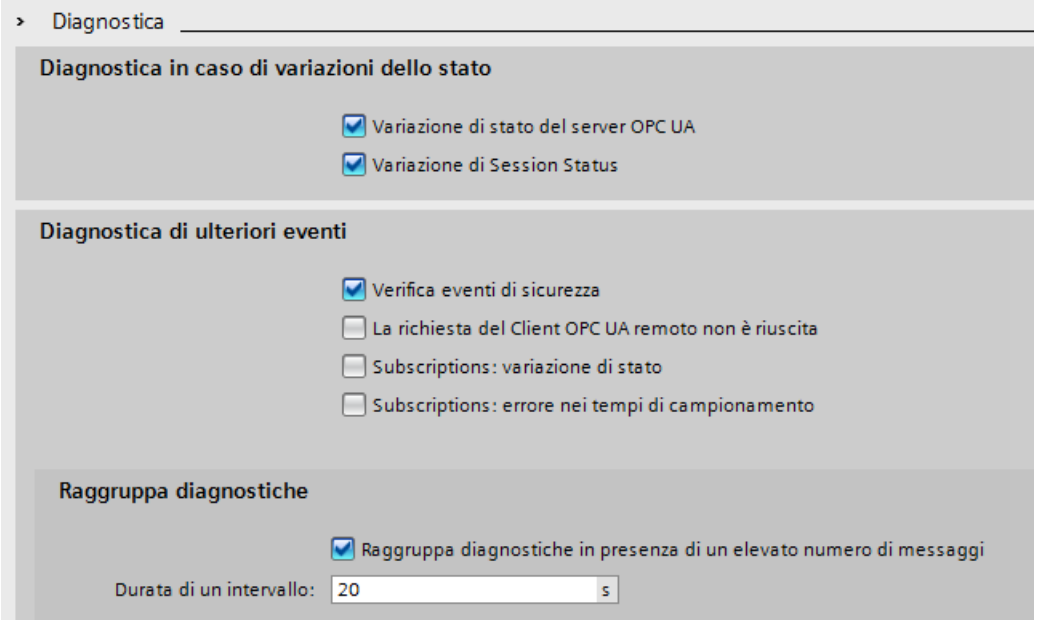


Figura 11-32 Impostazioni di diagnostica del server OPC UA

Preimpostazione

Per default è impostato un comportamento di diagnostica che consente le attività di diagnostica principali senza aumentare il carico di comunicazione in modo rilevante.

Le attività di diagnostica si attivano quando il server OPC UA comanda anche subscription, eventualmente solo nella fase di messa in servizio.

Motivo: Molte diagnostiche comportano un elevato carico di comunicazione nella CPU e possono eventualmente scalzare altri messaggi importanti. Oppure in caso di un elevato traffico di messaggi di diagnostica, può accadere che messaggi importanti non vengano considerati perché mescolati ai tanti altri.

Ulteriori informazioni

Qui (Pagina 351) si trovano ulteriori informazioni sul significato e l'effetto delle impostazioni mostrate in precedenza.

11.3.3.11 Licenze per OPC UA

Licenze di runtime

Per il funzionamento del server OPC UA della CPU S7-1500 è necessaria una licenza. Il tipo di licenza necessaria dipende dalla potenza della CPU corrispondente. Le licenze si suddividono nei seguenti tipi:

- SIMATIC OPC UA S7-1500 small (necessaria per CPU 1511, CPU 1512, CPU 1513, ET 200SP CPU, CPU 1515SP PC)
- SIMATIC OPC UA S7-1500 medium (necessaria per CPU 1515, CPU 1516, software controller CPU 1507, CPU 1516pro-2PN)
- SIMATIC OPC UA S7-1500 large (necessaria per CPU 1517, CPU 1518)

Il tipo di licenza necessario è visualizzato in "Proprietà > Generale > Licenze di runtime > OPC-UA > Tipo di licenza richiesta":

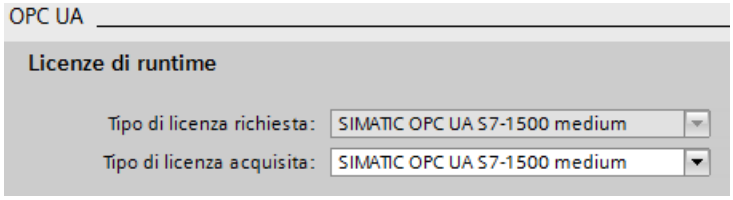


Figura 11-33 Licenze di runtime del server OPC UA

Per confermare l'acquisto della licenza necessaria, procedere nel seguente modo:

1. Nelle proprietà della CPU fare clic su "Licenze di runtime > OPC UA".
2. Selezionare la licenza necessaria nella casella di riepilogo "Tipo di licenza acquisita".

11.3.4 Progettazione dell'interfaccia del server OPC UA

11.3.4.1 Che cos'è un'interfaccia server?

Definizione

Un'interfaccia server raggruppa i nodi di un'area indirizzi OPC UA di una CPU che condividono particolari caratteristiche, in modo da mettere a disposizione dei client OPC UA una vista specifica sulla CPU.

Ogni interfaccia server definisce uno o più spazi dei nomi sul server OPC UA della CPU.

STEP 7 (TIA Portal) distingue i seguenti tipi di interfacce server:

- Specifica Companion

  Per questo tipo di un’interfaccia server utilizzare ad es. una specifica Companion che ha creato un gruppo di lavoro.

  Il gruppo di lavoro è composto normalmente da membri della OPC Foundation e da un’altra organizzazione industriale che hanno specificato in comune un modello di informazione OPC UA per un determinato scopo (ad esempio per lo scambio di dati con dispositivi RFID o con macchine a iniezione).

  Questo modello di informazione viene realizzato sotto forma di nodi OPC UA nell’area di indirizzi di un server OPC UA. A questi nodi OPC UA possono accedere client OPC UA.

  Il tipo di interfaccia server "Specifica Companion" si può utilizzare, ad es., anche per caricare dei modelli di informazione creati internamente a un’azienda, ad es. in SiOME.

  Se nel progetto si modifica una determinata specifica Companion, acquisire i dati di questa specifica Companion nel progetto come interfaccia server.

  Per interfacce server del tipo specifiche Companion è possibile importare più spazi dei nomi che utilizza la specifica Companion.

  Informazioni approfondite sulle specifiche Companion sono disponibili qui (Pagina 284).

  Informazioni approfondite su SiOME sono disponibili qui (https://support.industry.siemens.com/cs/ww/it/view/109755133).

  – Se le specifiche Companion ricorrono a definizioni del tipo in specifiche dipendenti, utilizzare namespace di riferimento. L'importazione dei namespace di riferimento avviene esattamente come previsto per le specifiche Companion.

    Vedere Creazione dell’interfaccia server per la specifica Companion (Pagina 291).

  – Per rendere accessibili ai client OPC UA i dati di istanza di FB o UDT della CPU, da TIA Portal versione V17 è possibile predisporre automaticamente le assegnazioni di questi dati. Per questo scopo è sufficiente mappare i tipi di FB o gli UDT in base ai tipi di dati OPC UA adatti di un namespace di riferimento importato. Per rendere possibile questa mappatura, nella finestra di dialogo per la creazione dell'interfaccia del server OPC UA di tipo Specifica Companion/namespace di riferimento, attivare l'opzione "Genera nodi OPC UA basati sulla mappatura dei dati locali".

    Vedere Creazione di nodi OPC UA basandosi sulla mappatura dei dati locali dei tipi FB e UDT (Pagina 317)

- Interfaccia server personalizzata:

  Per questo tipo di interfaccia server raggruppare in un’unità i nodi OPC UA di un server OPC UA.

  CI si attiene ai dati per il progetto o alle esigenze della macchina o dell’impianto.

  Maggiori informazioni sull'interfaccia server personalizzata sono disponibili qui (Pagina 296).

Macchina ad iniezione come esempio della specifica Companion

In questo esempio un'interfaccia server contiene i seguenti elementi:

- nodi OPC UA, che possono essere letti con un client OPC UA per ottenere informazioni sulla macchina a iniezione (dalle variabili PLC leggibili),
- nodi OPC UA, che possono essere scritti con un client OPC UA per trasferire valori nella macchina a iniezione (nelle variabili PLC scrivibili),
- nodi OPC UA, che possono essere richiamati con un client OPC UA per avviare delle funzioni nella macchina a iniezione (con i metodi server).

Questa interfaccia server consente la vista standardizzata su una CPU che può essere utilizzata per controllare una macchina a iniezione.

Per le macchine a iniezione le specifiche Companion "OPC UA specifications for plastics and rubber machines" (precedente "Euromap") definiscono un’intera serie di nodi OPC UA che possono essere acquisiti come interfaccia server.

In questa interfaccia server non sono compresi altri nodi nodi OPC UA della CPU. In questo modo si ottiene una visione più chiara.

Esempio di un'interfaccia server personalizzata

Una CPU deve controllare la realizzazione di pezzi. Quando viene ricevuto un ordine di produzione dal sistema di controllo sovraordinato, la produzione ha inizio.

Gli ordini di produzione vengono inoltrati tramite un metodo server: Un sistema di controllo inoltra informazioni ad un pezzo richiamando il metodo server nella CPU. Inoltre questo metodo server avvia anche la produzione.

Il sistema di controllo, ovvero il client OPC UA collegato deve vedere soltanto questo metodo server. Per questo motivo, nella CPU creare un’interfaccia server personalizzata e assegnarle il metodo server. Abilitare soltanto quest'interfaccia server per i client OPC UA e limitare quindi a quest'unica funzione la vista della CPU.

11.3.4.2 Utilizzo delle specifiche Companion OPC UA

Introduzione

OPC UA è utilizzabile universalmente: questo standard non dà indicazioni ad es. su come denominare le variabili PLC. Il singolo utente (lo sviluppatore dell'applicazione) ha anche facoltà di decidere come programmare e denominare i metodi server richiamabili mediante OPC UA.

Information modeling e standardizzazione per dispositivi e settori

Grazie alla sua modularità OPC UA offre la possibilità di standardizzare l'interfaccia dei dispositivi e delle macchine per le applicazioni dello stesso tipo.

La standardizzazione è stata sostenuta da numerosi organismi e gruppi di lavoro che hanno elaborato diverse specifiche Companion.

Le specifiche stabiliscono quanto segue:

- quali oggetti, metodi e variabili si utilizzano per descrivere un dispositivo o un macchina tipica,
- Namespace previsti per gli oggetti indicati.

Le macchine vengono strutturate tipicamente in unità funzionali e tecnologiche che vengono standardizzate.

La specifiche Companion offrono ai gestori di macchine e impianti il vantaggio di disporre di un'interfaccia unica. Così ad esempio tutti i lettori RFID che rispettano la specifica AutoID sono integrabili nello stesso modo. Più precisamente tutti i lettori RFID conformi alla specifica AutoID possono essere interrogati nello stesso modo dai client OPC UA, indipendentemente dal loro produttore.

Un altro esempio di specifica Companion nel settore delle macchine di stampaggio ad iniezione è la Euromap 77.

Il prossimo capitolo prende come esempio la Euromap 77 per spiegare come si acquisisce una specifica in STEP 7 (TIA Portal) e si creano le necessarie variabili PLC.

NOTA

EUROMAP e OPC Foundation hanno affermato il Joint Working Group "OPC UA Plastics and Rubber Machinery".

Le raccomandazioni EUROMAP 77 preesistenti (data exchange between injection moulding machines and MES), 82.1 (temperature control devices) e 83 (general definitions) sono state pubblicate sotto l'ombrello neutrale della OPC Foundation come OPC 40077, 40082-1 and 40083.

Una modifica di particolare rilievo è costituita dalla modifica del namespace ad es. per EUROMAP 77: Attualmente all'indirizzo "http://opcfoundation.org/UA/PlasticsRubber/IMM2MES/".

Gli esempi riportati nel seguito utilizzano le denominazioni e i riferimenti finora validi.

Esempio Euromap 77 (attualmente: OPC 40077)

La Euromap 77 e lo standard seguente OPC 40077 standardizza lo scambio dati tra le macchine di stampaggio ad iniezione e il MES (Manufacturing Execution System). In questo modo il MES può collegarsi direttamente a tutte le macchine di stampaggio ad iniezione subordinate.

La disponibilità di un'interfaccia unica facilita l'integrazione delle macchine nell'impianto.

Utilizzo della specifica Companion: Panoramica

La Euromap 77 è descritta nel file XML OPC UA "Opc_Ua.EUROMAP77.NodeSet2.xml".

NOTA

Euromap 77, Euromap 83 e OPC UA for Devices (DI)

Con la release Candidate 2 una parte delle definizioni della Euromap 77 sono state trasferite nella Euromap 83 (attualmente OPC 40083). È quindi necessario importare anche l'interfaccia del server OPC UA della Euromap 83.

"OPC UA for Devices" è un modello di informazioni generale per la configurazione dei componenti hardware e software. Poiché serve anche come base per altri standard Companion viene anch'esso importato.

I file XML OPC UA sono scaricabili da questi link:

Euromap77 (https://www.euromap.org/euromap77)

Euromap83 (https://www.euromap.org/euromap83)

OPC UA for Devices (https://opcfoundation.org/UA/schemas/DI/)

Questi file XML definiscono un'interfaccia OPC UA di una macchina ad iniezione conforme allo standard Euromap 77.

Utilizzo di Euromap 77: Panoramica

Per utilizzare Euromap 77, procedere nel modo seguente:

1. Con il programma SiOME creare un file XML in cui inserire un'istanza del tipo "IMM_MES_InterfaceType".

   La procedura è illustrato in seguito al "Passo 1: Creazione di istanze in SiOME".

2. Creare in STEP 7 (TIA Portal) variabili PLC e metodi server che corrispondono all’istanza del tipo "IMM_MES_InterfaceType" (creata nel passo 1).

   Il procedimento è illustrato in seguito al “Passo 2: Creazione di variabili PLC in STEP 7".

   Un esempio dei nodi OPC UA e delle variabili PLC corrispondenti è descritto nel capitolo "Creazione dell’interfaccia server per la specifica Companion (Pagina 291)".

3. Inserire in STEP 7 (TIA Portal) una nuova interfaccia server del tipo specifica Companion e importare il file XML creato al passo 1.

   Il procedimento è illustrato nel capitolo "Creazione dell'interfaccia server per la specifica Companion (Pagina 291)".

4. Assegnare le variabili PLC corrispondenti ai nodi OPC UA della nuova interfaccia server, create al passo 2.

   Il procedimento è illustrato a sua volta nel capitolo "Creazione dell'interfaccia server per la specifica Companion (Pagina 291)".

Passo 1: Creazione di istanze in SiOME

Il presente paragrafo spiega come utilizzare il programma gratuito "SiOME" (Siemens OPC UA Modeling Editor).

SiOME consente di creare un file XML OPC UA che descrive un'interfaccia server (un modello di informazioni).

Da qui (https://support.industry.siemens.com/cs/ww/it/view/109755133) è possibile richiamare la pagina con il link per il download e informazioni su SiOME.

Procedura in STEP 7

Per utilizzare la nuova interfaccia server, provvedere alla relativa importazione nel progetto STEP 7 come descritto al capitolo "Creazione dell'interfaccia server per la specifica Companion (Pagina 291)"

Una volta caricato il progetto nella CPU, la nuova interfaccia server è a disposizione del client OPC UA.

Procedura in SiOME 1.7.3

NOTA

La seguente descrizione illustra le operazioni in SiOME 1.7.3.

Le versioni successive di SiOME semplificano ad es. la creazione di DB, strutture, variabili o metodi corrispondenti nel programma utente. Tramite Drag&Drop è possibile ad es. trasferire dati di SiOME in TIA Portal (programma utente). Le variabili ecc. sono quindi già mappate correttamente e, nel caso dei metodi, vengono generati correttamente nel programma utente anche gli elementi FB corrispondenti.

Dal link sopraindicato scaricare l'ultima versione di SiOME, quindi seguire le istruzioni riportate nella documentazione fornita.

La seguente descrizione illustra le operazioni in SiOME 1.7.3.

Per utilizzare Euromap 77 creare un file XML con un'istanza di "IMM_MES_InterfaceType".

Soltanto con la definizione di istanze del tipo di oggetto viene generata la serie (il modello di informazione) della macchina vera e propria nell'area indirizzi del server OPC A.

Il tipo di oggetto "IMM_MES_InterfaceType" è il tipo di oggetto root di Euromap 77. "IMM" sta per "Injection Moulding Machine".

Procedere nel modo seguente:

1. Caricare i file "Opc_Ua.EUROMAP77.NodeSet2.xml" e "Opc_Ua_EUROMAP83_NodeSet2.xml" dalla pagina web della Euromap (vedere più sopra).
2. Caricare il file "Opc.Ua.Di.NodeSet2.xml" dalla pagina web della OPC Foundation.

   Nel file "Opc.Ua.Di.NodeSet2.xml" si trovano le definizioni di tipo utilizzate da Euromap 77 .
3. Avviare SiOME.
4. Importare innanzitutto lo spazio dei nomi "http://opcfoundation.org/UA/DI/".

   Per importarlo fare clic sul pulsante "Import XML" nell'area "Information model".

   Figura 11-34 Pulsante "Import XML" in SiOME

   SiOME visualizza la finestra di dialogo per aprire i file.
5. Selezionare il file "Opc.Ua.Di.NodeSet2.xml" quindi fare clic sul pulsante "Apri" per procedere alla relativa importazione.
   Risultato: SiOME importa il file XML e visualizza lo spazio dei nomi "http://opcfoundation.org/UA/DI/" in "Namespaces".

   Lo spazio dei nomi standard "http://opfoundation.org/UA/" è presente per default in SiOME e non deve essere importato.
6. Importare lo spazio dei nomi "http://www.euromap.org/euromap83/".

   Per la relativa importazione fare nuovamente clic sul pulsante ""Import XML" nell'area "Information model".

   Selezionare il file "Opc_Ua.EUROMAP83.NodeSet2.xml".

   Risultato: SiOME importa il file XML e visualizza in "Namespaces" anche lo spazio dei nomi "http://www.euromap.org/euromap83/".
7. Importare lo spazio dei nomi "http://www.euromap.org/euromap77/"

   Per importarlo fare nuovamente clic sul pulsante "Import XML" nell'area "Information model".

   Selezionare il file "Opc_Ua.EUROMAP77.NodeSet2.xml".
8. Creare uno spazio dei nomi dedicato per il progetto.

   Nel campo "Namespaces" fare clic con il tasto destro del mouse su "OPC UA Modelling Editor Project" o su "Namespaces" e selezionare "Add Namespace".

   SiOME apre la finestra di dialogo "Add Namespace".

9. Inserire il nome di uno spazio dei nomi.

   Nell'esempio è impostato lo spazio del nome "YourCompany.org".

   A questo punto SiOME visualizza anche il nuovo spazio dei nomi:

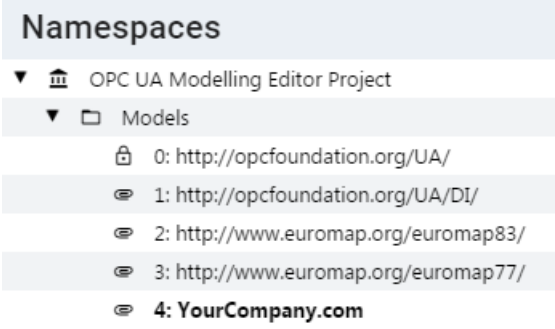


   Figura 11-35 Visualizzazione del namespace in SiOME

10. Creare una nuova istanza del tipo di oggetto root IMM_MES_InterfaceType della specifica Companion Euromap 77.
    Nel campo "Information model" fare clic con il tasto destro del mouse sulla directory "DeviceSet" e selezionare "Add Instance".

    SiOME visualizza la finestra di dialogo "Add Instance".

11. In "Name" inserire un nome esplicito per la nuova istanza.

    Per l'esempio impostare il nome "IMM_Manufacturer_01234".

    Selezionare "IMM_MES_InterfaceType" in "TypeDefinition".

    Questo tipo di oggetto è il tipo di oggetto root di Euromap 77: Se si forma un’istanza di questo tipo di oggetto, utilizzare Euromap 77 una volta nell’area di indirizzi del server OPC UA.

12. Fare clic su "OK".

    SiOME visualizza la nuova istanza "IMM_Manufacturer_01234" nel campo "Information model" in "DeviceSet" :

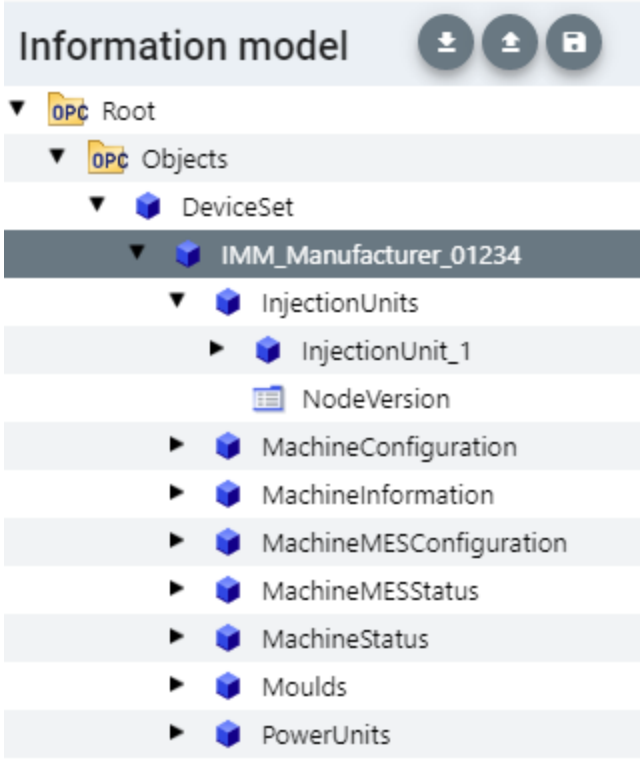


Figura 11-36 Visualizzazione dell'"information model"

13. Creare questa istanza del tipo di oggetto "InjectionUnitType".

    Nel campo "Information model" fare clic con il tasto destro del mouse sulla directory "InjectionUnits" e selezionare "Add Instance".

    SiOME visualizza la finestra di dialogo "Add Instance".

    In "Name" inserire un nome esplicito per l'istanza.

    Per l'esempio impostare "InjectionUnit_1".

    Selezionare "InjectionUnitType" in "TypeDefinition".

    Fare clic su "OK".

14. Creare nella directory "Moulds" una nuova istanza "Mould_1" del tipo do oggetto "MouldType".

15. Nella directory "PowerUnits" creare una nuova istanza "PowerUnit_1" del tipo do oggetto "PowerUnitType".

16. Salvare il file XML.

    Per importarlo fare clic sul pulsante Quick save" nell'area "Information model":

Figura 11-37 Pulsante "Quick save" in SiOME

17. Esportare il file XML.

    Per importarlo fare clic sul pulsante "Export XML" nell'area "Information model".

Figura 11-38 Pulsante "Export XML" in SiOME

SiOME apre la finestra di dialogo "Export XML".

18. Lasciare tutti gli spazi dei nomi attivati e fare clic su "OK".

    SiOME visualizza la finestra di dialogo “Salva con nome".

19. Scegliere un nome esplicito e salvare il file esportato.

    Nell’esempio indicare il file XML "IMM_Manufacturer_01234".

Risultato:

È stato creato un file XML che utilizza una volta la specifica Companion Euromap 77 (con una istanza).

Passo 2: Creazione in STEP 7 delle variabili PLC per l'istanza Euromap 77

Per Euromap 77 è necessario mettere a disposizioni nel programma utente variabili PLC e metodi server e assegnarli all’istanza di tipo "IMM_MES_InterfaceType".

Procedere nel modo seguente per creare variabili PLC per l'istanza del tipo "IMM_MES_InterfaceType".

1. Creare un tipo di dati personalizzato (UDT).

   La seguente figura illustra, a titolo di esempio, l’inizio del tipo di dati personalizzato "InjectionUnit".

   Questo tipo di dati dispone della stessa struttura di "InjectionUnit" nel tipo "IMM_MES_InterfaceType".

   Fare attenzione a utilizzare tipi di dati SIMATIC compatibili con i tipi di dati OPC UA (vedere in "Mapping dei tipi di dati").

InjectionUnit

	Name	Data type	Default value	Accessible from HMI/OPC UA	Writable from HMI/OPC UA
	BarrelId	String	''	☑	☑
	Index	UDInt	0	☑	☑
	InProduction	Bool	false	☑	☑
	IsPresent	Bool	false	☑	☑

Figura 11-39 Creazione UDT in STEP 7

2. Inserire nel progetto STEP 7 un nuovo blocco dati globale.

   Nell’esempio indicare il blocco dati "IMM_Manufacturer_01234“ in modo che ci sia un riferimento alla macchina ad iniezione del rispettivo produttore e del numero di serie.

3. Creare in questo blocco dati un nuovo elemento.

   Nell’esempio indicare questo elemento "InjectionUnit_1"

4. Assegnare a questo elemento il nuovo tipo di dati personalizzato "InjectionUnit".

Risultato

Nel blocco dati "IMM_Manufacturer_01234" del progetto STEP 7 è stata creata una variabile per Euromap 77 .

11.3.4.3 Creazione dell’interfaccia server per la specifica Companion

Per informazioni approfondite sulle specifiche Companion consultare il capitolo "Utilizzo delle specifiche Companion OPC UA (Pagina 284)". Questo capitolo tratta in modo esaustivo anche l'utilità della specifica Euromap 77 che fornisce un modello per macchine a iniezione.

Con l'ausilio di questa specifica Companion standard, la CPU S7-1500 può ad es. controllare una macchina a iniezione e fornire ad un Client OPC UA, ad es ad un sistema MES sovraordianto, un'interfaccia per l'accesso alle funzioni e alle variabili della macchina a iniezione.

L'interfaccia server OPC UA di tipo "Companion Standard" limita l'accesso dei client esattamente alle funzioni e variabili necessarie ad es. ai sistemi sovraordinati (sistemi MES).

La seguente descrizione illustra come creare in STEP 7 (TIA Portal) un’interfaccia server che contenga solo la specifica Companion Euromap 77.

Per consentire ai Client OPC UA l'accesso a ulteriori variabili e metodi oltre a quelli richiesti per la gestione di una macchina a iniezione, è sufficiente creare un'altra interfaccia server OPC UA. In questo modo è possibile disporre con chiarezza le funzionalità della CPU come server OPC UA.

Creazione dell’interfaccia server per una specifica Companion

Per creare in STEP 7 (TIA Portal) un’interfaccia server per una specifica Companion, procedere nel modo seguente:

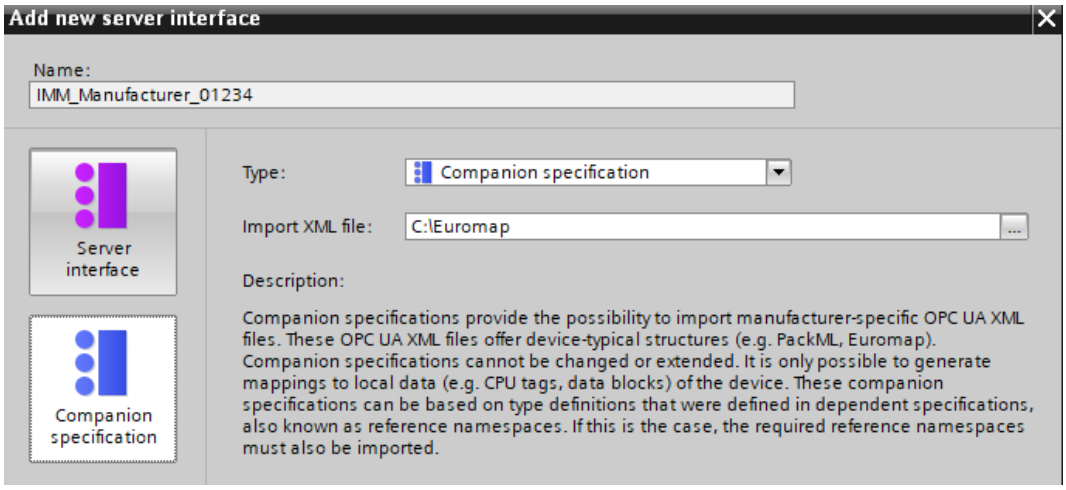
1. Selezionare la CPU da utilizzare come server OPC UA.
2. Fare clic su "Comunicazione OPC UA > Interfacce server" nella navigazione del progetto.
3. Fare doppio clic su "Aggiungi nuova interfaccia server".
4. Fare clic sul pulsante “Specifica Companion” per selezionare questo tipo di un’interfaccia server.

   Nella finestra di dialogo è inserito un nome generale per la nuova interfaccia server, ad esempio "Interfaccia server_1".

5. Modificare il nome della nuova interfaccia server in modo da renderlo significativo all'interno del progetto.

   Il nome deve presentare la seguente struttura in base a Euromap 77: “IMM_<Produttore>_<Numero di serie>".

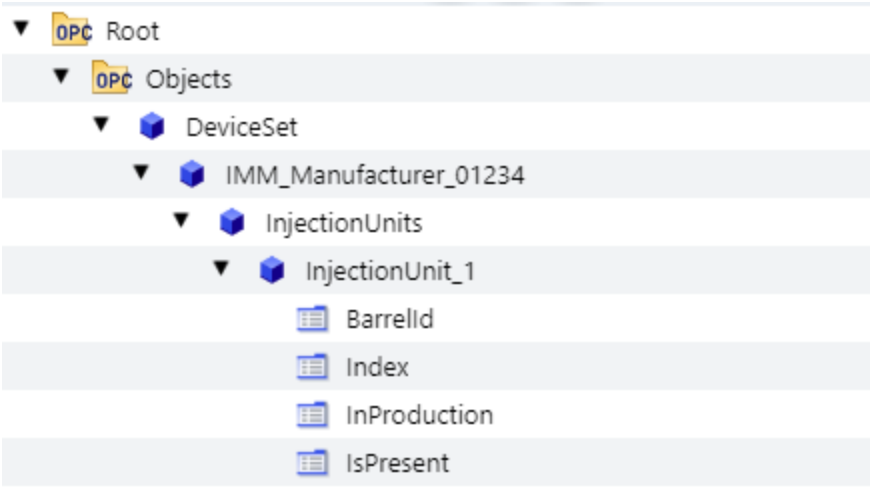
   L’esempio utilizza il nome "IMM_Manufacturer_01234".



6. Nella casella "Importazione del file XML", selezionare un file XML descritto nel modello di informazione.

   Per informazioni sulle modalità di creazione del file XML con il tool SiOME consultare il capitolo "Utilizzo delle specifiche Companion OPC UA (Pagina 284)".

   La figura seguente mostra una sezione del modello di informazione: "IMM_MANUFACTURER_0123456" un'istanza (utilizzo) del tipo "IMM_MES_InterfaceType", definito da Euromap 77 . "InjectionUnit_1" è un'istanza del tipo "InjectionUnitType" di Euromap 77.



7. Fare clic sul pulsante "OK".

   STEP 7 (TIA Portal) importa il modello di informazione descritto nel file XML selezionato.

   Si verifica un errore se nel file XML importato vengono utilizzate definizioni di tipo ancora inesistenti in STEP 7 (TIA Portal) e ancora non contenute nel file XML importato.

Nell'esempio viene importato un file XML che utilizza le definizioni di tipo definite nei seguenti spazi dei nomi (Namespaces):

– http://opcfoundation.org/UA/DI/
– http://www.euromap.org/euromap83/
– http://www.euromap.org/euromap77/

Suggerimento: Gli spazi dei nomi mancanti vengono visualizzati in STEP 7 nella sezione inferiore dell'editor dell'interfaccia OPC UA (scheda "Proprietà").

Selezionare l'interfaccia server nella navigazione del progetto (qui: IMM_Manufacturer_01234) quindi selezionare l'area "Spazio dei nomi" nella finestra di ispezione. Gli spazi dei nomi mancante sono evidenziati.

Se nel progetto STEP 7 manca uno o più spazi dei nomi, per ciascuno spazio dei nomi creare una nuova interfaccia server del tipo "Namespace di riferimento".

Il procedimento da seguire è descritto nel capitolo "Creazione dell'interfaccia server per lo spazio dei nomi d riferimento (Pagina 314)".

Se sono presenti tutti gli spazi dei nomi di riferimento, STEP 7 visualizza la tabella senza errori:

DeviceSet	Object
IMM_Manufacturer_01234	Object
InjectionUnits	Object
InjectionUnit_1	Object
TemperatureZones	Object
BarrelId	String
Index	UInt32
InProduction	Boolean
IsPresent	Boolean

8. Con Drag&Drop trascinare gli elementi OPC UA dalla sezione destra alla sezione sinistra della tabella (interfaccia server OPC UA), in modo che ogni elemento OPC UA (variabili PLC locali) sia assegnato al rispettivo nodo OPC UA di Euromap 77.

   La seguente figura illustra un dettaglio dell'assegnazione dei dati locali (variabili PLC) ai nodi OPC UA di Euromap 77:

OPC UA-Server-Schnittstelle

Name	Node type	Local data	Data type
DeviceSet	Object		
IMM_Manufacturer_01234	Object		
InjectionUnits	Object		
InjectionUnit_1	Object		
TemperatureZones	Object		
NodeVersion	String		
BarrelId	String	"IMM_Manufacturer_01234"."InjectionUnit_1"."BarrelId"	String
Index	UInt32	"IMM_Manufacturer_01234"."InjectionUnit_1"."Index"	UDInt
InProduction	Boolean	"IMM_Manufacturer_01234"."InjectionUnit_1"."InProduction"	Bool
IsPresent	Boolean	"IMM_Manufacturer_01234"."InjectionUnit_1"."IsPresent"	Bool

ATTENZIONE
Controllare la mappatura dei dati locali della CPU sui nodi dell'interfaccia server OPC UA Eventuali assegnazioni non valide (mapping) sull'interfaccia del server possono essere causa di errori di lettura e scrittura. Controllare le assegnazioni ed eseguire una verifica della coerenza.

Informazioni sull'interfaccia server

L'editor per la progettazione dell'Interfaccia server OPC UA è strutturato come tabella e mette a disposizione le seguenti informazioni:

- **Nome**

  Il primo nodo in alto (nodo root) inserisce nell’esempio il nome "IMM_Manufacturer_01234". Se un Client naviga nell'area indirizzi del server, questo nodo diventa la cartella di tutti i nodi subordinati. BrowseName e il DisplayName di questo nodo dipendono dal nome assegnato dall'utente all'interfaccia server.

  Qui ad es. questo nome si riferisce alla macchina a iniezione nel suo complesso. e corrisponde al nome dell'istanza della specifica Companion Euromap 77. La specifica Companion stabilisce che il nome dell'istanza cominci per "IMM", sia seguito dal nome del costruttore e termini con il numero di serie della macchina. Questo consente di identificare la macchina in modo univoco.

  I nomi degli altri nodi (subordinati) sono definiti dalla specifica (nell'esempio qui sopra da Euromap 77) La modifica di questi nomi dei nodi non è consentita. Questo garantisce una rappresentazione uniforme di tutte le macchine a iniezione definite secondo la specifica.

- **Tipo di nodo**

  Tipo del nodo OPC UA. Il tipo è definito dalla specifica Companion utilizzata.

  Nei seguenti casi STEP 7 evidenzia con un colore il tipo di nodo nella tabella:

  – se il file XML importato non contiene una definizione o

  – se lo spazio dei nomi nella quale è stata eseguita la definizione di tipo non esiste in STEP 7.

  In questo caso creare rispettivamente un’interfaccia server di tipo "Namespace di riferimento" per lo spazio o gli spazi dei nomi mancanti.

  Gli spazi dei nomi mancanti si trovano nelle proprietà dell’interfaccia server alla voce "Namespace".

- **Dati locali**

  STEP 7 visualizza il blocco dati assegnato al nodo OPC UA. La CPU legge da questo blocco dati i valori dei nodi OPC UA.

  Se un blocco dati è evidenziato con un colore (ad es. dopo la verifica coerenza), significa che non è disponibile nella CPU.

  In questo caso si deve creare il blocco dati mancante nella CPU (nel programma utente) e assegnargli i valori.

- **Tipo di dati**

  Il tipo di dati SIMATIC della variabile PLC (ad es. elemento di un blocco di dati) nella CPU dal quale viene letto il valore di un nodo OPC UA (del tipo UAVariable) o al quale viene assegnato un valore.

Aggiorna interfaccia

L'interfaccia del server può essere aggiornata per le specifiche Companion.

Esempio: Dopo l'importazione delle specifiche Companion e la successiva importazione dei namespace di riferimento da cui queste specifiche dipendono, le definizioni dei tipi degli spazi dei nomi di riferimento non sono ancora attive.

Facendo clic sul pulsante "Aggiorna interfaccia", le definizioni mancanti dei tipi delle specifiche Companion vengono risolte.

Pulsante "Aggiorna interfaccia":

Generazione di dati locali

Per tutti i nodi dell'interfaccia server o per quelli selezionati che non siano già assegnati ai dati locali della CPU ("mappati") è possibile generare dati locali. I nuovi dati locali generati vengono mappati automaticamente.

La generazione automatica dei dati locali si avvia facendo clic sul pulsante "Genera dati locali" (tutti i nodi non ancora mappati) o selezionando singoli nodi e successivamente il menu contestuale "Genera dati locali".

Pulsante "Genera dati locali":

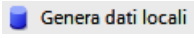


Figura 11-40 Pulsante "Genera dati locali":

È possibile generare solo nodi rappresentabili sui dati locali, e non oggetti, cartelle, metodi o argomenti input/output di metodi.

Dopo aver selezionato con un clic il pulsante o il menu contestuale è necessario selezionare nella finestra di dialogo successiva se i dati locali devono essere visualizzati in un nuovo DB oppure in un DB esistente.

Verifica coerenza

Questa opzione consente di verificare la coerenza dell'interfaccia server.

STEP 7 (TIA Portal) controlla se ai nodi OPC UA dell'interfaccia server sono state assegnate variabili PLC (blocchi dati) con tipi di dati SIMATIC compatibili.

Per controllare la coerenza dell'interfaccia server fare clic sulla seguente icona sulla barra degli strumenti dell'editor dell'interfaccia server OPC UA:

Figura 11-41 Pulsante "Verifica coerenza"

Esporta interfaccia

Sussiste la possibilità di esportare come file XML l'interfaccia del server OPC UA. Questo file XML contiene tutte le definizioni dei tipi di dati che indirizzano l'interfaccia del server.

Per esportare l'interfaccia server OPC UA, fare clic sulla seguente icona sulla barra degli strumenti dell'editor dell'interfaccia server OPC UA:

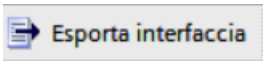


Figura 11-42 Pulsante "Esporta interfaccia"

11.3.4.4 Creazione dell'interfaccia server personalizzata

Introduzione

La descrizione si basa sul seguente esempio:

Un recinto di protezione circonda la cella di produzione "Cell_1". Il recinto ha la porta "Gate_1".

Una CPU S7-1500 comanda l'intera cella di produzione e controlla anche l'accesso tramite Gate_1.

Un robot nella cella di produzione confeziona un farmaco in cartoni, quindi impila i cartoni sui pallet.

Dei carrelli elevatori semoventi trasportano i pallet nel magazzino centrale passando per il Gate_1.

La CPU pubblica un'interfaccia server tramite la quale i sistemi di trasporto senza conducente comandano l'apertura del Gate_1.

L'interfaccia server contiene il metodo server "smOpenGate" per l'apertura della porta e la variabile "Gate_1_State" che visualizza lo stato della porta (aperto o chiuso).

Creazione dell'interfaccia server personalizzata

Per creare un'interfaccia server procedere nel seguente modo:

1. Selezionare la CPU da utilizzare come server OPC UA e opportunamente configurata.
2. Fare clic su "Comunicazione OPC UA > Interfacce server".
3. Fare doppio clic su "Aggiungi nuova interfaccia server".

   STEP 7 visualizza la seguente finestra di dialogo:

Figura 11-43 Aggiunta dell'interfaccia del server

4. Modificare il nome della nuova interfaccia server in modo da renderlo significativo all'interno del progetto.

   Nell'esempio modificare il nome "Interfaccia server_1", proposto da STEP 7, in "Cell_1".
5. Fare clic sul pulsante "Interfaccia server " e successivamente su "OK".
6. Fare clic sul triangolo prima di "Blocchi di programma" nel campo "Elementi OPC UA" per aprire la cartella "Blocchi di programma".

   STEP 7 visualizza le seguente tabelle per l'editazione:

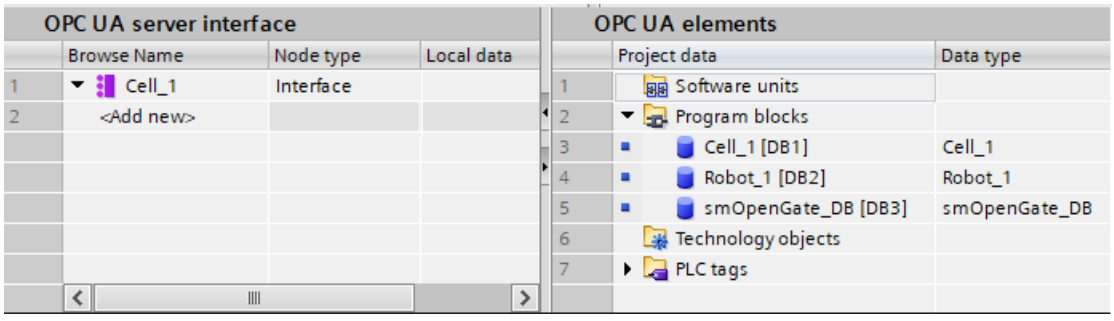


Figura 11-44 Modifica dell'interfaccia server

Questo editor è suddiviso in due campi:

– **Interfaccia server OPC UA**

  Sul lato sinistro si trova il nodo radice dell'interfaccia server "Cell_1".

  Questa interfaccia è attualmente ancora vuota: All'interfaccia server non è ancora stato aggiunto alcun elemento OPC UA.

– **Elementi OPC UA**

  Sul lato destro si trovano gli elementi creati nell'OPC UA.

  Gli elementi OPC UA sono oggetti creati finora nel progetto STEP 7 e che hanno la proprietà "Accessibile da HMI/OPC UA".

  Questi elementi OPC UA possono essere aggiunti alla nuova interfaccia server "Cell_1".

7. Tramite Drag&Drop trascinare gli elementi OPC UA sulla cella "<Aggiungi nuovo>" della nuova interfaccia server.

NOTA

In linea generale vale quanto segue: Con la memorizzazione di blocchi dati o anche di oggetti tecnologici nella sezione sinistra della tabella, STEP 7 (TIA Portal) genera un oggetto nell'interfaccia server. Al di sotto sono disposti elementi dei blocchi dati come nodi propri.

Con la memorizzazione di strutture nella sezione sinistra della tabella, STEP 7 crea un nodo per la struttura nel suo complesso e nodi per ogni singolo elemento della stessa.

Lo stesso comportamento si ha con gli array: Anche in questo caso STEP 7 crea un nodo per l'array nel suo complesso e nodi per ogni singolo elemento dello stesso.

Con la memorizzazione di un metodo nella sezione sinistra della tabella, STEP 7 crea un singolo nodo, gli argomenti del metodo inserito vengono visualizzati come informazione.

Nell'esempio trascinare la variabile "Gate_1_State" dall'area a destra in quella a sinistra su "<Aggiungi nuovo>".

Quindi trascinare il metodo server nell'area di sinistra.

Questo metodo server si trova all'interno del blocco dati "smOpenGate_DB [DB3]" nell'area di destra.

STEP 7 (TIA Portal) visualizza la finestra di dialogo nel modo seguente:

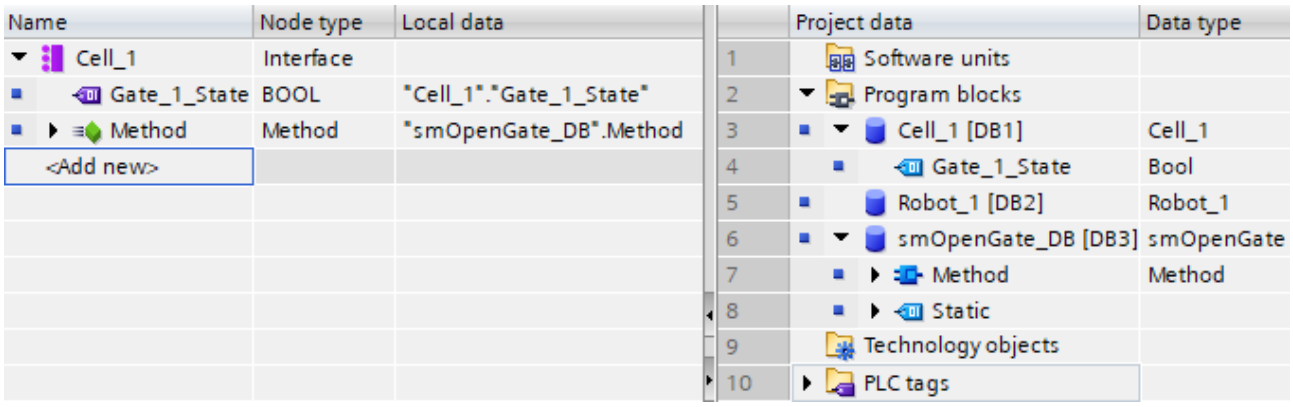


Figura 11-45 Aggiunta di elementi OPC UA dell'interfaccia del server

ATTENZIONE
Controllare la mappatura dei dati locali della CPU sui nodi dell'interfaccia server OPC UA Eventuali assegnazioni non valide (mapping) sull'interfaccia del server possono essere causa di errori di lettura e scrittura. Controllare le assegnazioni ed eseguire una verifica della coerenza. Il fatto che, in caso di assegnazioni non valide, TIA Portal generi solo avvisi e non errori consente di procedere per gradi: Si può ad esempio iniziare modificando il programma/i dati locali in modo che il programma funzioni correttamente. Quindi si può trascinare l'interfaccia del server OPC UA ed eliminare le incongruenze. Nei punti in cui TIA Portal genera degli avvisi l'interfaccia server OPC UA non funziona durante il runtime; il server OPC UA genera errori di runtime.

Limita la visuale al server OPC UA

Selezionando gli elementi OPC UA è possibile limitare la visuale al server OPC UA e le possibilità dei client OPC UA.

Nell’interfaccia server dell’esempio manca il blocco dati "Robot_1" perché i carrelli elevatori non hanno bisogno di accedere ai metodi server e alle variabili del robot.

In questo caso è opportuno disattivare l'interfaccia del server standard (SIMATIC namespace) nelle proprietà OPC UA della CPU S7-1500 in modo che i nodi filtrati non siano accessibili in altro modo.

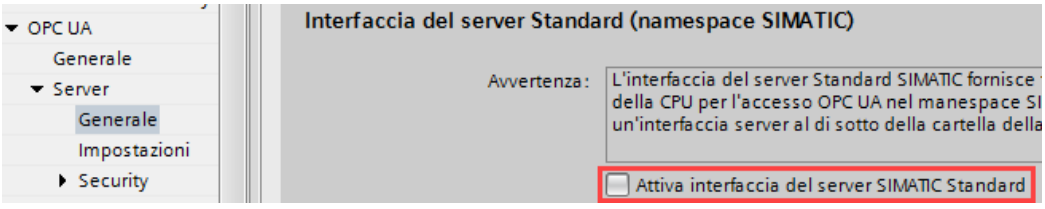


Figura 11-46 Disattivazione dell'interfaccia standard del server

È possibile disattivare la visibilità delle singole interfacce server OPC UA parametrizzate nelle rispettive proprietà, impedendo così che vengano utilizzate nel funzionamento dei client.

- Selezionare l'interfaccia del server, quindi fare clic con il tasto destro del mouse sul comando "Proprietà".

Questa opzione consente ad es. di definire più interfacce server a livello centrale e di attivare e caricare solo quella necessaria.

Una volta definita un'interfaccia server la si può copiare in un'altra CPU trascinandola con drag&drop nella navigazione del progetto.

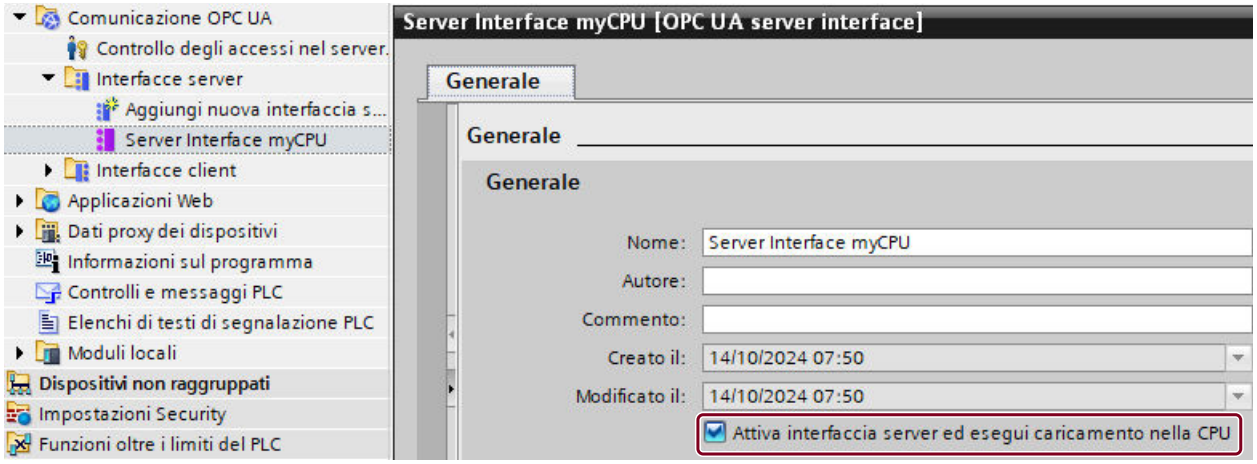


Figura 11-47 Disattivazione della visibilità dell'interfaccia standard del server

Informazioni sull'interfaccia server

L'editor per l'elaborazione dell'Interfaccia server OPC UA è strutturato come tabella e mette a disposizione le seguenti informazioni:

Osservare che inizialmente non vengono visualizzate tutte le caselle. Facendo clic con il testo destro del mouse sulla riga di intestazione della tabella, l'utente può stabilire quali caselle visualizzare.

Se è selezionata un riga, è possibile visualizzare gli attributi OPC UA del nodo nella finestra di ispezione (area "Attributi OPC UA"), ad es. ID del nodo, classe del nodo, tipo di nodo e descrizione.

- **BrowseName**

  Sul lato superiore è riportato il nome, uguale per tutte le lingue, dell'interfaccia server personalizzata (BrowseName). Questo nome può essere scelto liberamente.

  Sotto il nome dell'interfaccia sono riportati i nomi (BrowseNames) dei singoli nodi OPC UA che vengono aggiunti all'interfaccia server.

  Il nome di un nodo OPC UA non può essere modificato in questa finestra di dialogo. I nomi provengono dal progetto STEP 7.

  Un nodo OPC UA può essere eliminato dalla tabella. In questo modo il nodo non fa più parte dell'interfaccia server e non è più visibile per i client OPC UA.

- **DisplayName**

  Come BrowseName; se disponibile, il nome può essere ovviamente tradotto nella rispettiva lingua.

- **ID del nodo**

  NodeId del nodo OPC UA, ad es. http://Server-Node_1; i=1

- **Tipo di nodo**

  Tipo del nodo OPC UA, ad es. BOOL, BYTE, INT, ecc.

  Questi tipi di nodi sono stati definiti da Siemens e non dalla OPC Foundation. La OPC Foundation utilizza ad es. il tipo di nodo booleano per BOOL. BOOL deriva direttamente da booleano.

  Il tipo di nodo indicato non è modificabile in questa finestra di dialogo: Se si vuole utilizzare un altro tipo di nodo, è necessario modificare il tipo delle rispettive variabili PLC nel progetto STEP 7.

- **Tipo di dati**

  È indicato il tipo di dati SIMATIC che viene utilizzato nel progetto STEP 7, ad es. bool, byte, int, ecc.

- **Livello di accesso**

  – Se un nodo OPC UA è una variabile (tipo UAVariable), il nodo può essere solo leggibile (RD) o leggibile e scrivibile (RD/WR).

  – Se un nodo OPC UA è un metodo (tipo UAMethod), questo nodo è già richiamabile.

- **Dati locali**

  Il tipo di dati SIMATIC del blocco di dati nella CPU dal quale viene letto il valore di un nodo OPC UA (del tipo UAVariable) o dal quale viene scritto un valore.

Generazione di dati locali

Per tutti i nodi dell'interfaccia server o per quelli selezionati che non siano già assegnati ai dati locali della CPU ("mappati") è possibile generare dati locali. I nuovi dati locali generati vengono mappati automaticamente.

La generazione automatica dei dati locali si avvia facendo clic sul pulsante "Genera dati locali" (tutti i nodi non ancora mappati) o selezionando singoli nodi e successivamente il menu contestuale "Genera dati locali".

Pulsante "Genera dati locali":

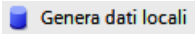


Figura 11-48 Pulsante "Genera dati locali":

È possibile generare solo nodi rappresentabili sui dati locali, e non oggetti, cartelle, metodi o argomenti input/output di metodi.

Dopo aver selezionato con un clic il pulsante o il menu contestuale è necessario selezionare nella finestra di dialogo successiva se i dati locali devono essere visualizzati in un nuovo DB oppure in un DB esistente.

Verifica coerenza

Questa opzione consente di verificare la coerenza dell'interfaccia server.

In caso di verifica della coerenza, STEP 7 controlla se i nodi OPC UA dell'interfaccia server sono stati assegnati rispettivamente ad un elemento OPC UA adatto (tipo di dati uguale) oppure se l'elemento utilizzato è ancora esistente nella CPU.

Per controllare la coerenza dell'interfaccia server fare clic sulla seguente icona sulla barra degli strumenti dell'editor dell'interfaccia server OPC UA:

Figura 11-49 Pulsante "Verifica coerenza"

Esporta interfaccia

Sussiste la possibilità di esportare come file XML l'interfaccia del server OPC UA. Questo file XML contiene tutte le definizioni dei tipi di dati che indirizzano l'interfaccia del server.

Per esportare l'interfaccia server OPC UA, fare clic sulla seguente icona sulla barra degli strumenti dell'editor dell'interfaccia server OPC UA:

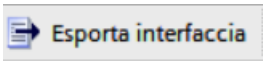


Figura 11-50 Pulsante "Esporta interfaccia"

Ulteriori informazioni

Per informazioni sulle copie master per la comunicazione OPC UA consultare il capitolo Copie master per la comunicazione OPC UA (Pagina 402).

Vedere anche

Accessi ai client e accessi locali al server OPC UA (Pagina 241)

11.3.4.5 Tipo di dati per le specifiche Companion

Mappatura del tipo di dati

La seguente tabella elenca i tipi di dati SIMATIC compatibili con i diversi tipi di dati OPC UA.

Assegnare i tipi di dati come indicato qui di seguito (tipo di dati SIMATIC - tipo di dati OPC UA). Altre assegnazioni non sono consentite. STEP 7 non verifica che questa regola venga rispettata e non impedisce un'assegnazione scorretta. È compito dell'utente scegliere e assegnare i tipi di dati in base alla regola.

I tipi di dati nell'elenco possono essere utilizzati anche ad es. come elementi di strutture/UDT per i parametri di ingresso e di uscita di metodi server creati individualmente (UAMethod_InParameters e UAMethod_OutParameters).

Tabella 11-3 Mappatura del tipo di dati

Tipo di dati SIMATIC	Tipo di dati OPC UA
BOOL	Boolean
SINT	SByte
INT	Int16
DINT	Int32
LINT	Int64
USINT	Byte
UINT	UInt16
UDINT	UInt32
ULINT	UInt64
REAL	Float
LREAL	Double
LDT	DateTime
WSTRING	String
DINT	Enumeration (Encoding Int32) e tutti i tipi di dati da esso derivati
È necessario il tipo di dati definito dall'utente (UDT, user-defined data type) Il tipo di dati definito dall'utente deve avere il prefisso "Union_", ad es. "Union_MyDatatype", vedere l'esempio dopo la tabella. Il primo elemento (Selector) di questo UDT deve avere il tipo di dati "UDINT".	UNION e tutti i tipi di dati da esso derivati
Vedere Tipi di dati LocalizedText e ByteString (Pagina 304)	LocalizedText ByteString

Tipo di dati definito dall'utente necessario per UNION

Nella seguente figura si vede la variabile "MyVariable" che ha il tipo di dati "Union_MyDatatype".

Questo tipo di dati SIMATIC corrisponde a una variabile OPC UA con tipo di dati UNION.

La seguente figura mostra un esempio di dichiarazione: Se Selector = 1, Union è una ByteArray, se Selector = 2 è una WString.

Nome	Tipo di dati
Static	
Selector	UDInt
ByteArray	Array[0..1] of Byte
WString	WString[42]

11.3.4.6 Tipi di dati LocalizedText e ByteString

A partire da TIA Portal versione V17 e CPU S7-1500 con versione firmware V2.9 sono disponibili i due tipi di dati built-in OPC UA "LocalizedText" e "ByteString" per la mappatura sulle corrispondenti strutture di dati SIMATIC. Per la definizione di questi tipi di dati OPC UA vedere anche OPC 10000-3 DataType Definitions.

Questi tipi di dati vengono utilizzati ad es. nelle specifiche Companion e sono facili da utilizzare per il programma utente con l'editor di interfaccia OPC UA.

LocalizedText

Struttura contenente una sequenza di caratteri (String) con identificatore delle impostazioni locali (locale identifier, ad es. 'en-US').

La struttura ha 3 elementi disposti secondo una sequenza prestabilita e in SIMATIC è formata nel modo seguente:

- **Encoding** (tipo di dati OPC_UA_LocalizedTextEncodingMask): indica nel bit 0 se il campo "Locale" ha un contenuto e nel bit 1 se il campo "Text" ha un contenuto. Poiché entrambi i campi dovrebbero avere un contenuto, si consiglia di impostare a 2#00000011 il valore di "Encoding" per SIMATIC.
- **Locale** (tipo di dati WString): identificatore delle impostazioni locali, ad es. 'en-US'.
- **Text** (tipo di dati WString): casella di testo, ad es. 'Text'.

ByteString

Sequenza di ottetti.

La struttura è organizzata nel seguente modo:

- **ActualLength** (tipo di dati "OPC_UA_ByteStringActualLength"): lunghezza dell'array ByteString riempito
- **ByteString** (tipo di dati "Array of Byte"): array byte

Presupposti

È stata creata un'interfaccia server OPC UA.

Impiego

È possibile importare una specifica Companion o uno spazio dei nomi di riferimento che contengano le definizioni del tipo "LocalizedText" o "ByteString".

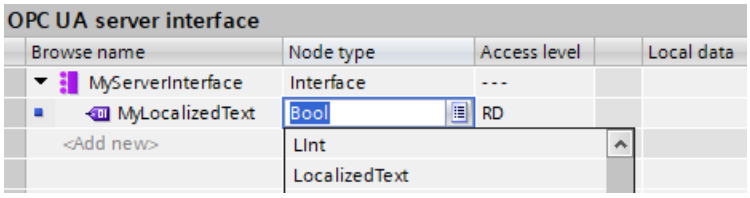
Allo stesso modo è possibile creare un'interfaccia server e definire individualmente un modello di indirizzo con i tipi di dati "LocalizedText" e "ByteString". La procedura è descritta nella sezione seguente.

Procedimento

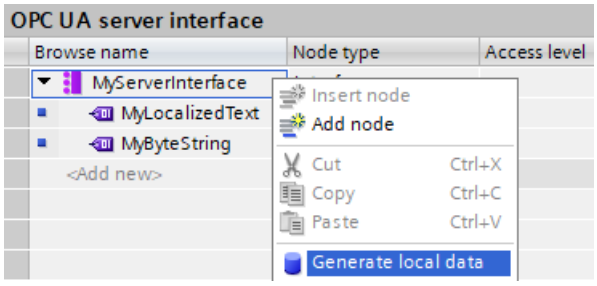
Qui di seguito è descritto come creare un nodo del tipo "LocalizedText" o "ByteString" con l'editor di interfaccia e come far generare automaticamente una struttura di dati SIMATIC per questo nodo.

Per definire i nodi OPC UA del tipo "Localized Text"/"ByteString" in un'interfaccia server, procedere nel seguente modo:

1. Creare nell'area "Interfaccia server OPC UA" dei nodi del tipo "LocalizedText" o "ByteString". Questi tipi di nodi sono contenuti nell'elenco dei tipi di nodi selezionabili.



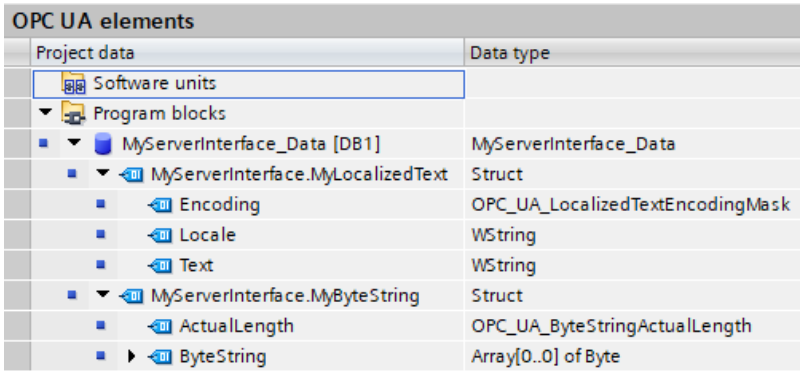
2. Selezionare nel menu di scelta rapida il comando "Genera dati locali". Per la generazione dei dati locali selezionare un blocco dati come ad es. un nuovo DB con il nome "MyServerInterface_Data".



Risultato: STEP 7 crea la struttura adeguata per la mappatura, nella quale si devono adattare la lunghezza del testo (Text) necessaria per "LocalizedText" e l'identificatore delle impostazioni locali (Locale).

Per "ByteString" vale lo stesso; qui devono essere adeguati la lunghezza e l'array.

La verifica della coerenza genera un avviso per segnalare le modifiche necessarie.



Regole

- Per i tipi di nodi "LocalizedText" e "ByteString" è possibile anche creare UDT con la struttura opportuna come descritto precedentemente e utilizzarli per elementi DB.
- I tipi di nodi "LocalizedText" e "ByteString" possono essere utilizzati in altre strutture (annidamento).
- Le strutture SIMATIC per "LocalizedText" e "ByteString" devono essere utilizzate solo per intero; non è previsto un tipo di dati isolato come ad es. "OPC_UA_LocalizedTextEncodingMask" per altri scopi.
- I parametri di ingresso e di uscita dei metodi possono anche avere il tipo di dati/nodo "LocalizedText" o "ByteString".

11.3.4.7 Utilizzo di ulteriori tipi di dati OPC UA per le specifiche Companion

Oltre ai tipi di dati OPC UA elencati nella sezione "Mapping dei tipi di dati" e i tipi di dati SIMATIC corrispondenti, sono disponibili anche i seguenti tipi di dati di base OPC UA:

- OpcUa_NodeId
- OpcUa_QualifiedName
- OpcUa_Guid
- OpcUa_XmlElement
- OpcUa_ByteString (Pagina 304)
- OpcUa_LocalizedText (Pagina 304)

Requisiti per poter utilizzare questi tipi di dati di base nel programma utente: devono essere tipi di dati di base complessi, strutturati esattamente come i tipi di dati di base OPC UA corrispondenti.

- OpcUa_NodeId e OpcUa_QualifiedName sono tipi di dati di sistema e sono quindi utilizzabili per le singole variabili, ma anche come elementi di una struttura.
- Per i tipi di dati di base o i tipi di dati Built-in GUID e XmlElement si deve creare un tipo di dati PLC secondo la specifica OPC UA e utilizzarlo come elemento in una struttura, in modo che i tipi di dati degli elementi possano essere risolti. Qui di seguito viene spiegato come strutturare il tipo di dati PLC per ogni tipo di dati di base.
- Per OpcUa_ByteString e OpcUa_LocalizedText in TIA Portal V17 sono stati soddisfatti i requisiti per utilizzare semplicemente questi tipi di dati nell'interfaccia server del tipo "Specifica Companion":
  - Si genera nell'interfaccia server il tipo di nodo corrispondente (ad es. OpcUa_LocalizedText)
  - Si fa clic su "Genera dati locali"

  Successivamente STEP 7 genera automaticamente le strutture di dati adatte in un DB.
- Per OpcUa_Guid questi requisiti sono stati creati in TIA Portal V19. Procedere come descritto nella vista precedente.

Tipo di dati di sistema "OPC_UA_NodeId"

La seguente tabella spiega il significato dei parametri per il tipo di dati di base OPC UA "OPC_UA_NodeId". OPC_UA_NodeId viene utilizzato per identificare un nodo nel server OPC UA.

Parametri	Tipo di dati S7	Significato
NamespaceIndex	UINT	Indice dello spazio dei nomi del nodo nel server OPC UA. Un nodo può essere ad es. una variabile.
Identifier	WSTRING[254]	Il nome del nodo (oggetto o variabile) dipende dal tipo di Identifier: • Identifier numerico: il nodo viene definito con un numero, ad es. "12345678". • String Identifier: il nodo viene definito con un nome, ad es. "LaMiaVariabile". Si distingue tra lettere maiuscole e minuscole.

Parametri	Tipo di dati S7	Significato
IdentifierType	UDINT	Tipo di Identifier • 0: Identifier numerico: • 1: String Identifier • 2: GUID • 3: Opaque

Tipo di dati di sistema "OPC_UA_QualifiedName"

La seguente tabella descrive la struttura del tipo di dati di sistema "OPC_UA_QualifiedName":

Nome	Tipo di dati S7	Significato
NamespaceIndex	UINT	Namespaceindex del nome.
Name	WSTRING[64]	Nome del nodo o della variabile.

Tipo di dati di sistema "GUID"

Il tipo di dati "Guid" è disponibile come tipo di nodo a partire da TIA Portal V19. Per la definizione di questo tipo di dati OPC UA vedere anche OPC 10000-6 Mapping.

La figura mostra l'assegnazione del tipo di dati "Guid" per un nodo di variabili in un'interfaccia server.

la seguente figura mostra il blocco dati con gli elementi GUID creato automaticamente con "Genera dati locali".

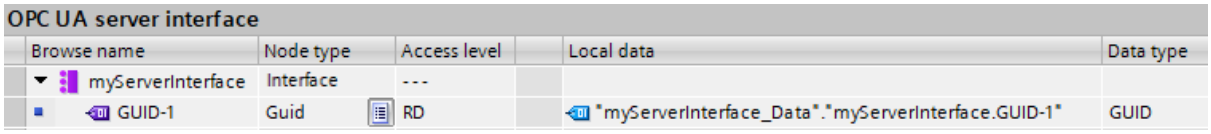


Figura 11-51 Nodi GUID nell'interfaccia server:

la seguente figura mostra il blocco dati con gli elementi GUID creato automaticamente con "Genera dati locali".

Name	Data type	Start value
Static		
myServerInterface.GUID-1	GUID	
Data1	UDInt	16#C4965784
Data2	UInt	16#0DFE
Data3	UInt	16#4B8F
Data4	Array[0..7] of Byte	
Data4[0]	Byte	16#87
Data4[1]	Byte	16#0A
Data4[2]	Byte	16#74
Data4[3]	Byte	16#52
Data4[4]	Byte	16#38
Data4[5]	Byte	16#C6
Data4[6]	Byte	16#AE
Data4[7]	Byte	16#AE

Figura 11-52 Blocco dati con l'SDT GUID

UDT per il tipo di dati di base XmlElement

Un XmlElement è un frammento XML serializzato (UTF-8 string).

Per il tipo di dati di base "XmlElement" creare il seguente tipo di dati PLC:

XmlElement

	Name	Data type	Default value
1	XmlElement	WString	WSTRING#''

11.3.4.8 Array dinamici

Nozioni utili sugli array dinamici

A partire da TIA Portal V19 e dalla versione firmware della CPU S7-1500 V3.1 è possibile utilizzare i cosiddetti "array dinamici" per le interfacce del server OPC UA e del client OPC UA. La seguente descrizione illustra il principio ed il funzionamento sulla base dell'interfaccia del server. La configurazione della struttura/dell'UDT di un array dinamico è identica per le applicazioni client e server.

Con gli array dinamici è possibile definire strutture di dati il cui numero di elementi sul lato dell'interfaccia del server può essere modificato in runtime. Sul lato CPU, l'array dinamico viene riprodotto su una struttura di dimensioni fisse.

Esempio: I dati di processo per il controllo qualità, provenienti dalla produzione, vengono trasmessi a un sistema di gestione di livello superiore. Il numero dei dati di processo è diverso a seconda del tipo di prodotto. Se il tipo di prodotto viene modificato durante il runtime, anche il numero dei dati di processo necessari verrà modificato.

In STEP 7 (TIA Portal), un array è un tipo di dati che può essere assegnato a una variabile. Un array rappresenta una struttura di dati composta da un numero fisso di componenti con lo stesso tipo di dati. Per i componenti sono consentiti tutti i tipi di dati ad eccezione di ARRAY.

Al contrario, OPC UA non definisce un array come tipo di dati. Ogni valore della variabile (Value) può essere un array. La conformazione di una variabile rispetto alla sua "geometria" come array è definita in OPC UA dai seguenti attributi e proprietà del Variable NodeClass (estratto da https://reference.opcfoundation.org/Core/Part3/v104/docs/5.6):

Attribut / Property	Tipo di dati	Valori possibili, significato
ValueRank (Mandatory)	Int32	• n > 1: Value è un array con dimensione n. • 1: Value è un array con una dimensione • 0: Value è un array con una o più dimensioni • -1: Value è una scala (non un array) • -2: Value è uno scalare o un array con un numero qualsiasi di dimensioni • -3: Value può essere uno scalare o un array unidimensionale
ArrayDimensions (Optional)	UInt32[]	Lunghezza massima supportata per dimensione. 0 o vuoto: lunghezza sconosciuta.
MaxArrayLength (Optional)	UInt32	Per DataVariables con attributo ValueRank non scalare: Lunghezza massima dell'array. Esempio: Un array tridimensionale con le lunghezze 2x3x10 ha lunghezza 60.

In questo contesto si ricorre alla denominazione "Array dinamico" per attribuire un equivalente sotto il profilo del tipo di dati SIMATIC, alla dinamica della geometria delle variabili definita in OPC UA, in modo da consentire la mappatura dei dati dell'array. Durante il runtime è possibile modificare la geometria di un array mappato tramite il programma STEP 7. Sul lato OPC UA, si definisce un nodo nell'interfaccia del server OPC UA attraverso il quale un client può accedere ai dati mappati della CPU (all'array dinamico).

Principio

Per consentire la mappatura delle variabili OPC UA sulla base delle variabili CPU di tipo array, utilizzare una struttura o un UDT con il nuovo tipo di dati di sistema "OPC_UA_ArrayBoundaries".

La struttura o l'UDT ha i seguenti elementi ed è impostata come segue:

- Il primo elemento della struttura (dimensione dell'array) è a sua volta un array e definisce le dimensioni attuali dell'array dinamico. Il tipo di dati di sistema "OPC_UA_ArrayBoundaries" definisce per ogni dimensione il campo degli indici proposto nell'interfaccia del server (ciascuno con gli elementi limite inferiore e superiore).
- Il secondo elemento della struttura (dati dell'array) contiene tutti gli elementi dell'array con un tipo di dati selezionabile consentito per OPC UA.

STEP 7 (TIA Portal) assicura automaticamente che, ad es. indici negativi sul lato SIMATIC siano convertiti in indici non negativi (a partire da "0") sul lato OPC UA (interfaccia server).

Esempio di array unidimensionale

L'esempio seguente illustra la struttura di un semplice array unidimensionale con un massimo di 10 elementi. Le dimensioni attuali dell'array sono impostate su 3 elementi [0..2].

Nome	Tipo di dati	Possibili valori / Descrizione
1-Dim-Struct	Struct (UDT)	
- **ArraySizeAct**	Array [0..0] of OPC_UA_ArrayBoundaries	**Dimensioni attuali dell'array**
- - ArraySizeAct[0]	OPC_UA_Boundaries	Unidimensionale
- - - Lower	DInt	**0** (indice in basso)
- - - Upper	DInt	2 (possibili valori superiori dell'indice: 0..9)
- **MyDataArray**	Array[**0**..9] of Byte	**Dati dell'array (tutti gli elementi dell'array)**
- - MyDataArray[0]	Byte	Primo elemento
...	...	...
- - MyDataArray[9]	Byte	Ultimo elemento

Esempio di array bidimensionale

L'esempio seguente illustra la struttura di un array bidimensionale con 10x6 = 60 elementi. Gli indici inferiori di entrambe le dimensioni non sono "0". Le dimensioni attuali dell'array sono impostate su 2x6 = 12 elementi.

Nome	Tipo di dati	Possibili valori / Descrizione
2-Dim-Struct	Struct (UDT)	
- **ArraySizeAct**	Array [0..1] of OPC_UA_ArrayBoundaries	**Dimensioni attuali dell'array**
- - ArraySizeAct[0]	OPC_UA_Boundaries	Prima dimesnione
- - - Lower	DInt	**-9** (indice in basso)
- - - Upper	DInt	-8 (possibili valori superiori dell'indice: -9...0)
- - ArraySizeAct[1]	OPC_UA_Boundaries	Seconda dimesnione
- - - Lower	DInt	**5** (indice in basso)
- - - Upper	DInt	10 (possibili valori superiori dell'indice: 5..10)
- **MyDataArray**	Array[-**9**..0, **5**..10] of Byte	**Dati dell'array (tutti gli elementi dell'array)**
- - MyDataArray[-9,5]	Byte	Primo elemento
- - MyDataArray[-9,6]	Byte	Secondo elemento
...	...	...
- - MyDataArray[0,9]	Byte	Penultimo elemento
- - MyDataArray[0,10]	Byte	Ultimo elemento

Ripercussioni sull'interfaccia server

Aspetto nell'interfaccia server: Se nell'editor dell'interfaccia server si trascina e si rilascia un array dinamico (ad es. 2-Dim-Struct) su questa interfaccia, STEP 7 (TIA Portal) crea un nodo con lo stesso nome senza gli elementi subordinati. Nella colonna "Tipo di nodo" il nodo visualizza il tipo "ARRAY" con le lunghezze massime possibili dell'array.

Navigazione: L'array dinamico è disponibile come nodo nell'area degli indirizzi OPC UA. A differenza degli array statici, gli elementi subordinati dell'array non sono visibili come nodi subordinati.

Lettura: L'array dinamico è leggibile tramite il servizio di lettura. Il client può specificare se la lettura concerne l'intero array o solo alcune parti di esso (IndexRange). Solo le parti lette che rientrano nei limiti del campo dell'array attuale restituiscono lo stato "Good". Se le dimensioni dell'array sono, in ogni singola dimensione, pari a "0", viene restituito un array vuoto con lo stato "Good".
Se un array di dimensioni "0" viene letto in una dimensione, viene restituito un array vuoto con lo stato "Good".

Scrittura: se il campo da scrivere è minore o uguale alle dimensioni massime dell'array, tutti gli elementi vengono scritti (stato "Good"). Se il campo da scrivere supera le dimensioni massime dell'array, non viene scritto nulla e viene restituito lo stato 8074_0000 (OpcUa_BadTypeMismatch). Lo stesso vale per la scrittura di un array parziale (IndexRange): L'area dell'array da scrivere deve rientrare completamente in tutte le dimensioni all'interno delle dimensioni massime dell'array. Solo a questo punto i dati vengono scritti e viene confermato lo stato "Good".
Se un array di dimensioni "0" viene scritto in almeno una dimensione, questo valore viene impostato correttamente nei dati della CPU. Gli elementi "Lower" e "Upper" nella struttura OPC_UA_ArrayBoundary corrispondente, vengono opportunamente adeguati ("Upper" = "Lower-1").

Regole e particolarità

- Gli array dinamici possono essere utilizzati anche per i parametri di ingresso e di uscita nei metodi.
- Evitare le incoerenze modificando le dimensioni attuali dell'array mentre un client accede all'array. In questo caso il risultato dell'accesso è indefinito.
  Per modificare le dimensioni attuali dell'array, utilizzare l'istruzione non interrompibile UMOVE_BLK.
- A differenza dell'array del tipo di dati SIMATIC, l'OPC UA dispone anche di array "vuoti". La definizione di un array con 0 elementi in una dimensione avviene con OPC_UA_ArrayBoundaries, impostando il valore più alto dell'indice (Upper) sul valore più basso dell'indice stesso (Lower), ad es. con i seguenti valori: Upper = Lower-1.

  Se si definisce un array multidimensionale nell'interfaccia del server (o nell'interfaccia del client) e almeno una dimensione è "0" (vuota), si tratta per definizione di un array vuoto (tutte le dimensioni sono 0).

- I valori delle dimensioni attuali dell'array e i valori dei dati dell'array devono essere coerenti, diversamente verrà emesso il codice di errore 803A_0000 (OpcUa_BadNotReadable).
  - I valori che per una dimensione vengono impostati come "Lower" nelle dimensioni attuali dell'array, devono essere impostati come valore inferiore dell'indice anche nel campo dati dell'array nella dimensione corrispondente.
  - I valori impostati come "Upper" per una dimensione nelle dimensioni attuali dell'array, devono rientrare nel campo dati dell'array per questa dimensione.
- Un client OPC UA che scrive in un array dinamico sul server, deve scrivere un array delle stesse dimensioni (ValueRank). Diversamente viene restituito lo stato 8074_0000 (OpcUa_BadTypeMismatch).

11.3.4.9 Regole per i file XML OPC UA

Importazione dei file XML OPC UA esportati in una CPU S7-1500

Quando si importano interfacce server che sono state create esportando il file XML OPC UA di una S7-1500 è importante tener conto della seguente avvertenza.

NOTA

Blocco dell'importazione per lo spazio dei nomi "http://www.siemens.com/simatic-s7-opcua"

Non è possibile importare interfacce server con lo spazio dei nomi "http://www.siemens.com/simatic-s7-opcua" in una CPU S7-1500 perché si tratta di uno spazio riservato alle CPU S7-1500 (interfaccia server SIMATIC standard) e l'importazione è bloccata.

Per poter importare un'interfaccia server con lo spazio dei nomi "http://www.siemens.com/simatic-s7-opcua" la si deve aprire (file XML OPC UA) e si deve modificare lo spazio dei nomi nei punti corrispondenti. Così modificato il file può essere importato.

Integrità dei file XML OPC UA

I file XML OPC UA rappresentano lo spazio degli indirizzi del server. Questi file vengono adattati all'applicazione e importati dall'utente come interfaccia server, caricati nella CPU S7-1500 e quindi testati, ad es. nel contesto delle specifiche OPC UA Companion.

⚠ AVVERTENZA

Nessuna verifica dei file XML OPC UA importati

Proteggere questi file XML OPC UA dalle manipolazioni non autorizzate, perché STEP 7 non ne verifica l'integrità.

Raccomandazione

Per ridurre al minimo i rischi nel caso di un'estensione o di un adattamento dello spazio di indirizzi del server procedere nel modo seguente:

1. Proteggere il progetto (navigazione nel progetto: Impostazioni Security > Impostazioni).
2. Prima di procedere all'estensione o all'adattamento esportare l'interfaccia server corrispondente.
3. Modificare il file XML OPC UA.
4. Importare nuovamente il file come interfaccia server.

11.3.4.10 Creazione dell’interfaccia server per lo spazio dei nomi d riferimento

Specifiche Companion e spazi dei nomi utilizzati

In una specifica Companion sono definiti una serie di tipi di oggetto OPC UA (nonché altre definizioni) Questi tipi di oggetto sono stati definiti rispettivamente negli spazi dei nomi per far sì che i nomi dei tipo di oggetto (definizioni di tipo) siano univoci

Per utilizzare una specifica Companion nel progetto, creare istanze dei tipi di oggetto di questa specifica Companion.

Le definizioni dell’oggetto devono trovarsi nel progetto STEP 7. In caso contrario è necessario importare le definizioni dell’oggetto. Per importare tutte le definizioni di uno spazio dei nomi, creare in STEP 7 un’interfaccia server del tipo “Spazio dei nomi di riferimento" in ciascun spazio dei nomi.

NOTA

EUROMAP e OPC Foundation hanno affermato il Joint Working Group "OPC UA Plastics and Rubber Machinery".

Le raccomandazioni EUROMAP 77 preesistenti (data exchange between injection moulding machines and MES), 82.1 (temperature control devices) e 83 (general definitions) sono state pubblicate sotto l'ombrello neutrale della OPC Foundation come OPC 40077, 40082-1 and 40083. Gli esempi riportati nel seguito utilizzano tuttavia le denominazioni e i riferimenti finora validi.

Esempio Euromap 77 (attualmente OPC 40077)

Per la specifica Companion Euromap 77 (attualmente OPC 40077) è stata aggiunta un'interfaccia server.

L'interfaccia server utilizza tipi di oggetto definiti in OPC UA DI e in Euromap 83 e Euromap 77 nei relativi spazi dei nomi.

In STEP 7 creare pertanto, oltre all'interfaccia del server Euromap 77 di tipo "Specifica Companion", ulteriori interfacce server di tipo "Namespace di riferimento", rispettivamente per i seguenti spazi dei nomi:

- http://opcfoundation.org/UA/DI/
- http://www.euromap.org/euromap83/
- http://www.euromap.org/euromap77/

La seguente descrizione mostra il procedimento.

Creazione dell'interfaccia server per uno spazio dei nomi d riferimento

Per creare un'interfaccia server per uno spazio dei nomi procedere nel modo seguente:

1. Selezionare la CPU da utilizzare come server OPC UA.
2. Fare clic su "Comunicazione OPC UA > Interfacce server".
3. Fare doppio clic su "Aggiungi nuova interfaccia server".

   STEP 7 (TIA Portal) visualizza la finestra di dialogo "Aggiungi nuova interfaccia server".

   Nella finestra di dialogo è inserito un nome generale per la nuova interfaccia server, ad esempio "Interfaccia server_1".
4. Assegnare un nome significativo alla nuova interfaccia server.

   Nell'esempio selezionare il nome "Opc.Ua.Di" o un nome simile che rimandi in modo univoco allo spazio dei nomi "http://opcfoundation.org/UA/D/I/".

   Questo spazio dei nomi deve essere importato per primo. Contiene definizioni di base (ad esempio UAObjectType "DeviceType").
5. Fare clic sul pulsante "Specifica Companion" e selezionare il tipo "Namespace di riferimento".
6. Fare clic sui 3 punti di fianco al campo "Importa file XML".
7. Selezionare un file XML che contenga le definizioni dello spazio dei nomi "http://opcfoundation.org/UA/DI/".

   Nell'esempio selezionare il file "Opc.Ua.Di.NodeSet2.xml". Questo file può essere caricato qui:

   Opc.Ua.Di.NodeSet2.xml (https://opcfoundation.org/UA/schemas/DI/)

   Avvertenza: Se il file non può essere importato, è possibile che la versione del modello OPC UA ("CORE") presente in TIA Portal non corrisponda alla versione del modello OPC UA for Devices ("DI"). In questo caso selezionare un'altra versione del modello DI (ad es. una versione precedente).

La seguente figura illustra la finestra di dialogo con le voci:

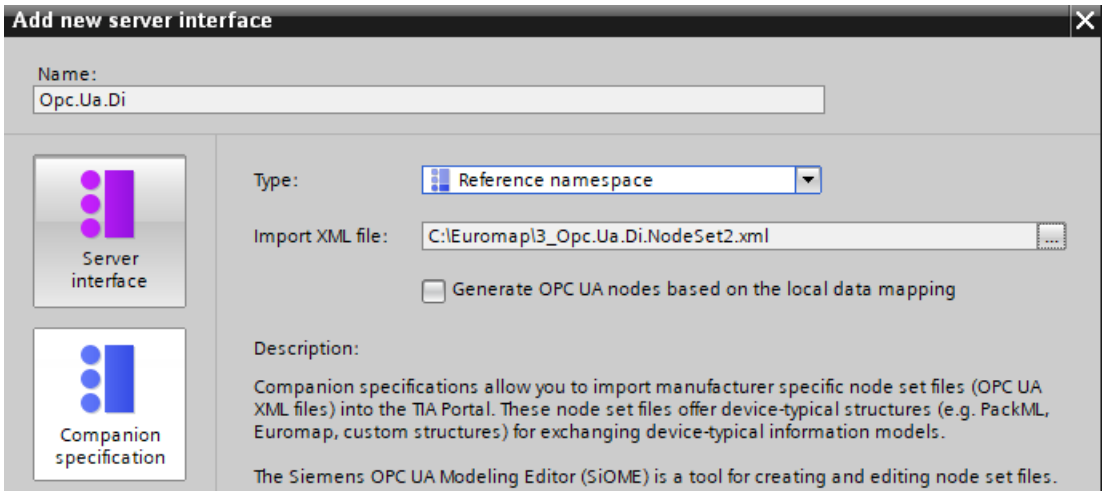


Figura 11-53 Inserimento del namespace di riferimento

8. Fare clic sul pulsante "OK".

   STEP 7 (TIA) genera quindi la nuova interfaccia server.

L'interfaccia server si trova nella navigazione del progetto di STEP 7 (TIA Portal), in "Comunicazione OPC UA > Interfaccia server > Namespace di riferimento".

Se una specifica Companion utilizza altri spazi dei nomi, aggiungere rispettivamente una nuova interfaccia server per ciascuno spazio dei nomi.

Aggiunta di ulteriori interfacce server per Euromap77

Per Euromap 77 sono necessari i seguenti spazi dei nomi:

- http://www.euromap.org/euromap83/
- http://www.euromap.org/euromap77/

Aggiungere dapprima un'interfaccia server per lo spazio dei nomi "http://www.euromap.org/euromap83/".

Questo spazio dei nomi contiene definizioni di base per Euromap 77, per questo è necessario per primo. Tutte le definizioni di questo spazio dei nomi sono contenute nel file XML "Opc_Ua.EUROMAP83.NodeSet2.xml" che può essere caricato dalla pagina web di Euromap (https://www.euromap.org/en/euromap83).

Aggiungere quindi un'interfaccia server per lo spazio dei nomi "http://www.euromap.org/euromap77". Tutte le definizioni di questo spazio dei nomi sono contenute nel file XML "Opc_Ua.EUROMAP77.NodeSet2.xml" che può essere caricato dalla pagina web di Euromap (https://www.euromap.org/en/euromap77)

11.3.4.11 Creazione di nodi OPC UA basandosi sulla mappatura dei dati locali dei tipi FB e UDT

Per rendere accessibili ai client OPC UA i dati di istanza di FB o UDT della CPU, da TIA Portal versione V17 è possibile predisporre automaticamente le assegnazioni di questi dati.

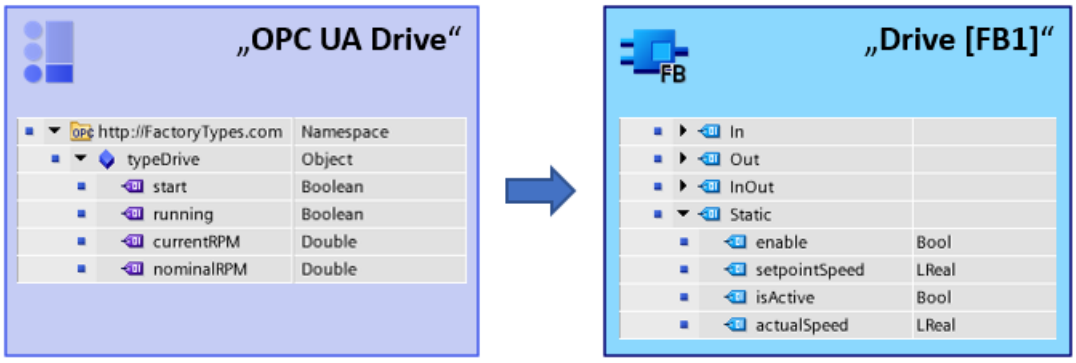
Per questo scopo è sufficiente mappare i tipi di FB o gli UDT in base ai tipi di dati OPC UA adatti dei namespace di riferimento importati. Basandosi su questa mappatura, durante la compilazione STEP 7 (TIA Portal) genera nell'interfaccia del server i nodi necessari per ogni istanza FB o per ogni utilizzo di UDT.

In caso di ampliamento del programma e inserimento di ulteriori istanze FB, o di utilizzi UDT, oppure di eliminazione di istanze esistenti, l'adeguamento dell'interfaccia del server si rende superfluo: STEP 7 adegua l'interfaccia del server automaticamente durante la compilazione.

Esempio

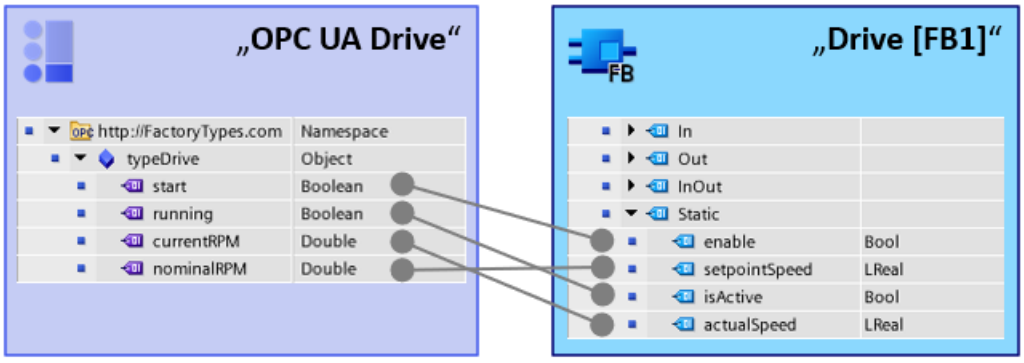
- Creare un blocco funzionale (FB) nel programma utente della CPU, e nell'area "Static" dell'interfaccia di questo blocco, definire i parametri che ne formano la "memoria". Le istanze (valori) di questi parametri devono essere accessibili ai client OPC UA.
- Creare un tipo di dati OPC UA (ad es. con SiOME) con elementi corrispondenti al tipo di dati dei parametri nell'area Static dell'interfaccia del blocco funzionale. La sequenza degli elementi è irrilevante. Importare quindi il file nodeset di riferimento come namespace di riferimento.

La figura seguente mostra l'assegnazione degli elementi come confronto tra la vista del namespace di riferimento (interfaccia server) e la vista degli elementi OPC UA (programma).



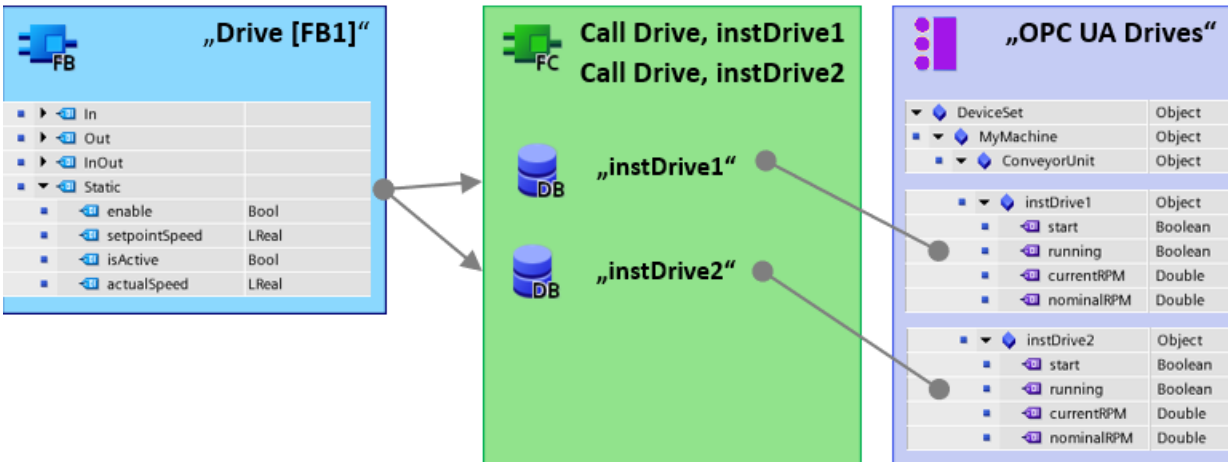
Mappatura dei tipi di dati (interfaccia FB o interfaccia OPC UA): Principio

La figura seguente mostra l'assegnazione degli elementi del programma utente della CPU agli elementi dell'interfaccia server OPC UA. La sequenza degli elementi non deve necessariamente corrispondere.

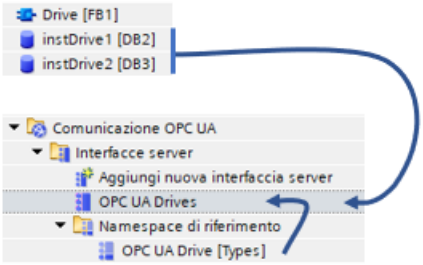


Creazione automatica delle istanze del server OPC UA nell'interfaccia del server: Principio

La figura seguente mostra il risultato della compilazione del progetto: Le istanze del programma utente vengono create anche nell'interfaccia del server.



Tramite la mappatura tra le informazioni di tipo FB / UDT e le informazioni di tipo OPC UA, STEP 7 è in grado di generare tutte le istanze presenti nel programma come nodi nell'interfaccia del server.



Regole

- Soltanto gli elementi FB nell'area "Static" di un'interfaccia FB possono essere mappati sulla base delle descrizioni del tipo OPC UA.
- Durante la mappatura dei tipi di dati, per un oggetto devono sempre essere selezionati gli elementi OPC UA della stessa interfaccia FB o dello stesso UDT. Non è consentito eseguire la mappatura da FB o UDT diversi su un oggetto.

Presupposti

- I tipi di FB utilizzati, definiti nell'area "Static" di un FB, devono essere progettati come "Accessibile per OPC UA"
- I tipi di UDT utilizzati, devono essere progettati come "Accessibile per OPC UA"
- Deve essere disponibile un file nodeset (file XML) con le definizioni del tipo di dati OPC UA adatte ai (mappabili sui) tipi FB o agli UDT definiti nel programma utente.
  Utilizzare il tool "SiOME" per la generazione del file nodeset (Siemens Industry Online Support).
- Deve essere inoltre disponibile il programma utente con le istanze FB e gli utilizzi UDT.

Procedimento

Per la mappatura del tipo di dati di un namespace di riferimento sulla base di un tipo di FB o di un tipo di dati UDT, procedere come indicato nel seguito:

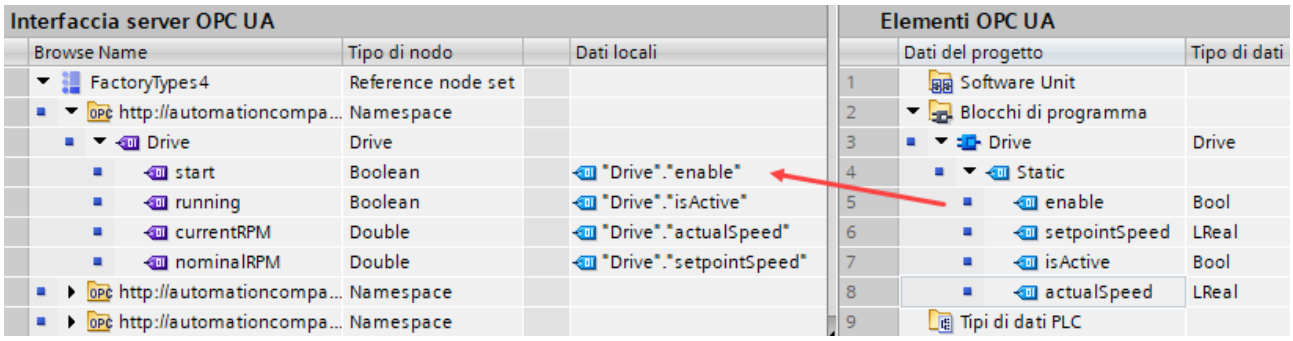
1. Selezionare la CPU da utilizzare come server OPC UA.
2. Come nuova interfaccia del server importare il file nodeset preparato (file XML) con le definizioni del tipo come namespace di riferimento
   - Nella finestra di dialogo "Aggiungi nuova interfaccia server", attivare l'opzione "Genera nodi OPC UA basati sulla mappatura dei dati locali".

     Soltanto se quest'opzione è attivata i tipi FB o UDT possono essere mappati tramite Drag&Drop sulle descrizioni dei tipi OPC UA.
3. Fare clic sull'icona dell'interfaccia del server di tipo "Namespace di riferimento" appena creata.

   Si apre l'editor per la mappatura tra l'interfaccia del server OPC UA e gli elementi OPC UA. Nell'area delle proprietà dell'editor, alla voce "Mappatura dei dati locali", è attivata l'opzione "Genera nodi OPC UA basati sulla mappatura dei dati locali". Diversamente attivare quest'opzione.

   Nel campo "Nome interfaccia" adeguare il nome dell'interfaccia server da creare. Durante la compilazione, viene creata una nuova interfaccia server di tipo "Specifiche Companion" con questo nome.

4. Assegnare i tipi di FB o gli UDT preesistenti ai nodi dell'interfaccia server (namespace di riferimento) trascinando l'elemento OPC UA (sezione destra dell'editor) sul nodo corrispondente dell'interfaccia server (namespace di riferimento, colonna "Dati locali").



5. Compilare il progetto.

   Dopo la compilazione i nodi delle istanze appena creati si trovano nell'interfaccia del server generata di tipo "Specifica Companion". STEP 7 crea un oggetto per ogni istanza DB. Gli elementi generati si trovano sotto ciascuno di questi oggetti.

   Analogamente STEP 7 genera a sua volta un oggetto per ogni DB globale creato durante l'assegnazione di istanze ad un UDT.

   L'interfaccia di specifica Companion così generata non è modificabile (operazioni non più possibili: Genera dati locali, Importa specifica Companion). Questa misura protegge dalla perdita di dati nel caso in cui l'interfaccia del server sia stata ampliata manualmente e, di conseguenza, sovrascritta durante una nuova compilazione. È possibile modificare solo il nome dell'interfaccia di specifica Companion generata.

   Inoltre le cartelle di gruppo create per strutturare i dati nella navigazione del progetto TIA possono essere acquisite come "cartella" (tipo di nodo) nell'interfaccia di specifica Companion generata.

Creazione del programma utente con tipi di FB o UDT

In questa sede la creazione di FB e UDT non viene illustrata nei dettagli, leggere quindi la descrizione sulla creazione di un programma utente, ad es. la dichiarazione dell'interfaccia dei blocchi e la dichiarazione dei tipi di dati PLC (UDT).

Verifica coerenza

La verifica coerenza (pulsante "Verifica coerenza" dell'editor) controlla anche la mappatura dei tipi di dati e aggiorna la visualizzazione di questi tipi dati nella colonna corrispondente dell'editor.

11.3.4.12 Indicazioni sulle quantità di risorse consigliate per l'utilizzo delle interfacce server

Quando si utilizzano le interfacce server OPC UA si devono considerare i limiti massimi consentiti per i seguenti oggetti in funzione della classe di prestazione della CPU S7-1500:

- Numero delle interfacce server
- Numero di nodi OPC UA (Nodes)
- quantità di dati degli oggetti di caricamento
- Se sono stati implementati dei metodi: numero di metodi server o di istanze dei metodi server

Quantità di risorse consigliate per le interfacce server OPC UA e metodi

Le strutture quantitative delle interfacce server OPC UA e i metodi sono riportati nei dati tecnici dei manuali del prodotto delle rispettive CPU. I dati tecnici più recenti delle CPU sono disponibili in Internet (https://support.industry.siemens.com/cs/ww/it/ps/td).

Se non si rispettano le quantità consigliate compare un messaggio di errore.

11.3.5 Come mettere a disposizione i metodi del server OPC UA

11.3.5.1 Informazioni utili sui metodi server

Come mettere a disposizione il programma utente per i metodi server

Nel server OPC UA delle CPU S7-1500 (dal firmware V2.5) è possibile mettere a disposizione dei metodi mediante il programma utente. Tali metodi sono utilizzabili dai client OPC UA che li possono richiamare ad es. per avviare un ordine di produzione dalla CPU S7-1500.

I metodi OPC UA, un'implementazione dei "Remote Procedure Call", sono un meccanismo efficiente di interazione tra i diversi partner della comunicazione. Il meccanismo fornisce sia la conferma dell'ordine sia valori di ritorno, evitando così la necessità di programmare meccanismi di handshaking.

Con i metodi OPC UA è ad es. possibile trasferire i dati in modo coerente senza bit di trigger/handshaking e senza eseguire particolari operazioni nel controllore.

Come funziona un metodo OPC UA?

In linea di massima un metodo OPC UA funziona come un blocco funzionale con protezione del know-how che viene richiamato da un client OPC UA esterno durante il runtime.

Il client OPC UA "vede" solo gli ingressi e le uscite definite. L'interno del blocco funzionale, il metodo o l'algoritmo, restano invisibili al client OPC UA. Il client OPC UA riceve una risposta di "esecuzione conclusa correttamente" e valori di ritorno forniti dal blocco funzionale (metodo). Se l'esecuzione non si conclude correttamente riceve invece un messaggio di errore.

Il programmatore ha il completo controllo sul contesto del programma in cui viene eseguito il metodo OPC UA e ne è pienamente responsabile.

Regole per la programmazione dei metodi e del comportamento durante il runtime

- Garantire che i valori di ritorno forniti dal metodo OPC UA siano coerenti con i valori di ingresso forniti dal client OPC UA.
- Tener conto delle regole per l'assegnazione dei nomi e la definizione dei parametri e dei tipi di dati utilizzabili (vedere la descrizione delle istruzioni per il server OPC UA).
- Comportamento durante il runtime: il server OPC UA accetta **un unico** richiamo per istanza del metodo. L'istanza potrà essere richiamata nuovamente per altri client OPC UA solo dopo che il programma utente ha concluso il richiamo in corso o se nel frattempo si verifica un timeout.

Qui di seguito viene descritta la procedura generale che consente di implementare un programma utente come metodo server.

Implementazione di un metodo server

I programmi (blocchi funzionali) per l'implementazione dei metodi server hanno la seguente struttura:

1. **Richiamo del metodo server con OPC_UA_ServerMethodPre**

   Richiamare innanzitutto l'istruzione "OPC_UA_ServerMethodPre" nel programma utente (ovvero nel metodo server).

   Questa istruzione ha i seguenti compiti:

   – Con essa si verifica nel server OPC UA della CPU se il metodo server è stato richiamato da un client OPC UA.
   – Se il metodo è stato richiamato e dispone di parametri di ingresso, questi ultimi gli vengono quindi assegnati.

     I parametri di ingresso del metodo server provengono dal client OPC UA che l'ha richiamato.

2. **Elaborazione del metodo server**

   In questa sezione del metodo server si predispone il programma utente vero e proprio.

   Qui sono disponibili le stesse opzioni degli altri programmi utente (ad es. la possibilità di accedere ad altri blocchi funzionali o a blocchi dati globali).

   Se il metodo server utilizza parametri di ingresso, sono inoltre disponibili i parametri di ingresso del metodo server.

   Questa sezione del metodo server dovrebbe essere eseguita solo se un client OPC UA ha richiamato il metodo server.

   Una volta eseguito correttamente il metodo impostarne i parametri di uscita (se disponibili).

3. **Risposta al metodo server con OPC_UA_ServerMethodPost**

   Concludere il metodo server richiamando l'istruzione "OPC_UA_ServerMethodPost".

   Utilizzando gli appositi parametri specificare nell'istruzione "OPC_UA_ServerMethodPost" se il programma utente è stato eseguito o meno.

   Se l'esecuzione si è conclusa correttamente il server OPC UA viene informato dai corrispondenti parametri e trasmette al client OPC UA i parametri di uscita del metodo.

Richiamare le istruzioni "OPC_UA_ServerMethodPre" e "OPC_UA_ServerMethodPost" sempre insieme, sia che il programma utente venga eseguito completamente fra un'istruzione e l'altra, sia che l'esecuzione prosegua nel ciclo successivo.

Un esempio di implementazione di un metodo server è descritto nella Guida in linea di STEP 7.

Integrazione del metodo server

La seguente grafica illustra in che modo un client OPC UA (A) richiama il metodo server "Cool".

La CPU esegue l'istanza "Cool1" del metodo server "Cool" ⑥ nel programma utente ciclico.

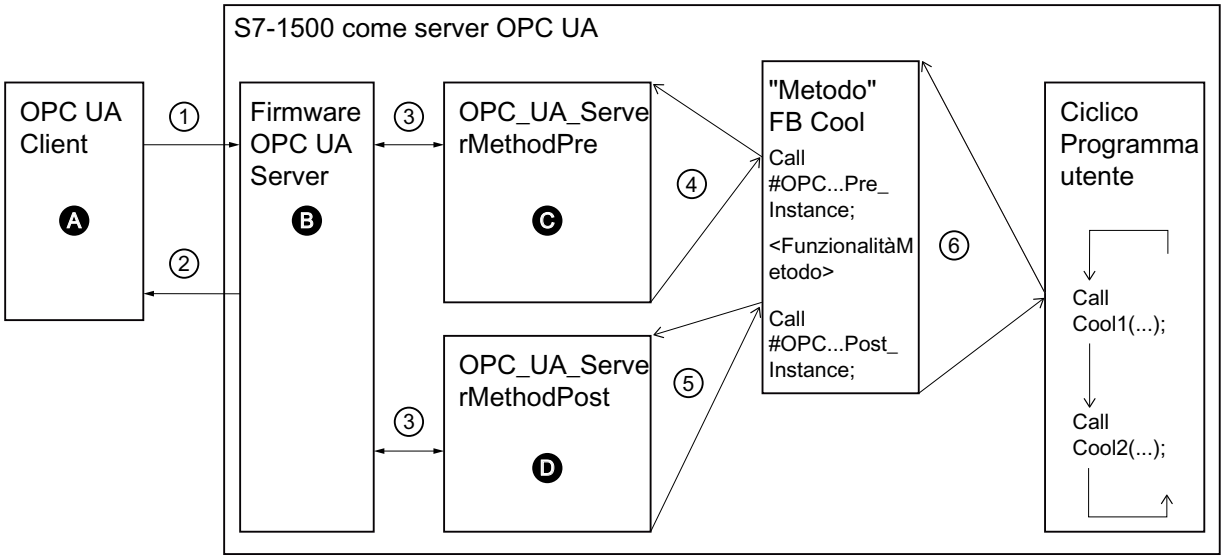
La CPU esegue innanzitutto l'istruzione "OPC_UA_ServerMethodPre" ④ per chiedere se un client OPC UA ha richiamato il metodo server "Cool" ①.

- Se il metodo server non è stato richiamato il programma utente riprende direttamente l'esecuzione ciclica tramite ④ e ⑥. Dopo "Cool1" la CPU continua ad eseguire il programma utente ciclico.
- Se il metodo server è stato richiamato, questa informazione viene restituita al metodo server Cool tramite ④. Nel metodo server Cool viene eseguita la funzione vera e propria, vedere "<funzionalità del metodo>" nella grafica.

  Quindi il metodo server utilizza l'istruzione "OPC_UA_ServerMethodPost" ⑤ per comunicare al firmware (B) che l'istruzione è stata eseguita ③.

  Il firmware restituisce l'informazione al client OPC UA richiamante (A) tramite ②.

  Dopo "Cool1" la CPU continua ad eseguire il programma utente ciclico.



A Richiamo del metodo server e gestione dell'informazione "Done" (metodo concluso).

① Richiamo asincrono del metodo server.

② Informazione "Done" asincrona del metodo richiamato (metodo concluso).

B Attesa dei richiami del client OPC UA, gestione dei richiami nella coda di attesa, inoltro dell'informazione "Done" dal programma utente ciclico al client OPC UA.

③ Trasferimento dei dati dal server OPC UA all'istanza del metodo del programma utente e viceversa.

C Verifica se il metodo è stato richiamato.
In caso affermativo inoltrare i dati di ingresso del server OPC UA all'istanza del metodo del programma utente e segnalare all'istanza che il metodo è stato richiamato ("called").

④ Richiamo sincrono dell'istruzione OPC_UA_ServerMethodPre come multiistanza con indicazione dell'area di memoria per i dati di ingresso del server OPC UA.
Il Return Value indica se il metodo è stato richiamato dal client OPC UA.

⑤ Verifica se il metodo è terminato o è ancora attivo ("busy").

D Verifica se il metodo è terminato.
In caso affermativo i dati di uscita dell'istanza del metodo vengono inoltrati al server OPC UA e viene segnalato all'istanza che il metodo è terminato. L'informazione viene inoltrata al server OPC UA.

⑥ Richiamo dell'FB del metodo (in questo caso: FB Cool) con l'istanza desiderata e i parametri del processo.

Figura 11-54 Esempio: Richiamo del metodo del server "Cool"

Informazioni sulle istruzioni per il server

Le istruzioni "OPC_UA_ServerMethodPre" e "OPC_UA_ServerMethodPost" sono descritte in dettaglio nella Guida sulle Istruzioni > Comunicazione > OPC UA > Server OPC UA.

11.3.5.2 Condizioni generali per l'impiego dei metodi server

Tipi di dati ammessi

Se si definiscono dei metodi server attenersi alle seguenti regole.

- Assegnare i tipi di dati come indicato qui di seguito (tipo di dati SIMATIC - tipo di dati OPC UA). Altre assegnazioni non sono consentite.

STEP 7 non verifica che questa regola venga rispettata e non impedisce un'assegnazione scorretta. È compito dell'utente scegliere e assegnare i tipi di dati in base alla regola.

I tipi di dati nell'elenco possono essere utilizzati anche ad es. come elementi di strutture/array/UDT per i parametri di ingresso e di uscita di metodi server creati individualmente (UAMethod_InParameters e UAMethod_OutParameters).

Tipo di dati SIMATIC	Tipo di dati OPC UA
BOOL	Boolean
SINT	SByte
INT	Int16
DINT	Int32
LINT	Int64
USINT	Byte
UINT	UInt16
UDINT	UInt32
ULINT	UInt64
REAL	Float
LREAL	Double

Tipo di dati SIMATIC	Tipo di dati OPC UA
LDT	DateTime
WSTRING	String
DINT	Enumeration (Encoding Int32) e tutti i tipi di dati da esso derivati
È necessario il tipo di dati definito dall'utente (UDT, user-defined data type) Il tipo di dati definito dall'utente deve avere il prefisso "Union_", ad es. "Union_MyDatatype". Il primo elemento (Selector) di questo UDT deve avere il tipo di dati "UDINT".	UNION e tutti i tipi di dati da esso derivati
Vedere Tipi di dati LocalizedText e ByteString (Pagina 304)	LocalizedText ByteString
GUID Vedere Utilizzo di ulteriori tipi di dati OPC UA per le specifiche Companion (Pagina 307)	GUID

Numero di metodi server implementabili e numero di argomenti

Se si implementato i metodi server tramite il programma utente, il numero di metodi utilizzabili è limitato in base al tipo di CPU. Queste informazioni sono disponibili nei manuali del prodotto delle CPU o nell'ultimo aggiornamento dei dati tecnici delle CPU in Internet (https://support.industry.siemens.com/cs/ww/it/ps/td).

Messaggio di errore in caso di superamento verso l'alto

Se viene superato il numero massimo di metodi server, le istruzioni OPC_UA_ServerMethodPre o OPC_UA_ServerMethodPost segnalano il codice errore 0xB080_B000 (TooManyMethods).

Quantità di dati che possono essere trasferiti su una CPU S7-1500 con il metodo server

Max. 2097152 byte (= 2,1 megabyte MaxMessageSize).

Assegnazione di tipi di dati strutturati con array annidati

Se un tipo di dati strutturato (Struct/UDT) contiene un array, il server OPC UA non mette a disposizione informazioni sulla lunghezza di questo array.

Se si utilizza una struttura di questo tipo, ad es. come parametro di ingresso o di uscita di un metodo server, è necessario fare in modo la lunghezza che viene assegnata all'array annidato al richiamo del metodo sia corretta.

Se non si rispetta questa regola il metodo non funziona e compare il codice errore "BadInvalidArgument".

11.3.6 Come rendere disponibili i messaggi sul server OPC UA

11.3.6.1 Informazioni utili sui messaggi

I messaggi permettono all'utente di rilevare rapidamente gli errori durante l'elaborazione dei processi nei sistemi di automazione, di localizzarli con precisione e infine di eliminarli, riducendo così notevolmente i tempi di inattività dell'impianto. Con il modello informativo OPC UA "Alarms & Conditions" si realizza un modo standardizzato e indipendente dalla piattaforma per l'elaborazione dei messaggi.

A partire dal firmware V2.9 il server OPC UA di una CPU S7-1500 supporta il modello informativo OPC UA "Alarms and Conditions". Il server OPC UA offre così accesso alle segnalazioni del controllore.

Le sezioni seguenti indicano quali tipi di messaggi disponibili in SIMATIC vengono supportati sull'interfaccia OPC UA del server OPC UA.

Nei capitoli che seguono si illustrano le modalità di configurazione del server OPC UA della CPU S7-1500 per Alarms and Condition, la struttura di base del modello Alarms and Conditions in OPC UA e le particolarità da osservare nella gestione dei messaggi nell'area di indirizzi del server OPC UA rispetto alla gestione delle segnalazioni del controllore SIMATIC del sistema di segnalazione della CPU.

Base per l'applicazione dei messaggi secondo OPC UA Alarms & Conditions

Il modello di informazione Alarms and Conditions è descritto nella specifica "OPC 10000-9: OPC Unified Architecture Part 9: Alarms & Conditions".

Segnalazioni del controllore in SIMATIC

Il server OPC UA della CPU S7-1500 supporta le segnalazioni del controllore sotto elencate disponibili per le CPU S7-1500. La progettazione e la programmazione di questi messaggi avvengono come di consueto, senza richiedere l'osservanza di ulteriori regole per il loro utilizzo da parte dei client OPC UA.

L'ulteriore vantaggio di OPC UA Alarms and Conditions risiede nel fatto che questi tipi di messaggi possono essere visualizzati non soltanto da dispositivi HMI, browser web, display delle CPU o TIA Portal, ma anche da tutti i client OPC UA che supportano OPC UA Alarms and Conditions.

- Messaggi di controllo PLC con ProDiag
  Poche operazioni di progettazione sono già sufficienti per l'integrazione nel programma di semplici controlli, senza che sia necessaria la modifica del codice di programma. La progettazione dei controlli è indipendente dai linguaggi di programmazione del TIA Portal in quanto il controllo concerne soltanto singoli operandi rendendo superflue ulteriori sezioni di progettazione.
- Messaggi di diagnostica di sistema
  Gli eventi delle unità dipendenti dalla configurazione sono noti alla CPU per effetto della configurazione hardware e possono essere analizzati tramite i dispositivi di visualizzazione collegati. Nell'editor dei messaggi questi eventi possono essere visualizzati ma non modificati.

- Messaggi di programma (istruzione Program_Alarm)
  Vengono utilizzati per segnalare eventi sincroni al programma e sono assegnati rispettivamente a un blocco. Vengono creati nell'editor di programmazione ed elaborati nell'editor di messaggi (TIA Portal).
- Messaggi GRAPH
  Anche per i blocchi funzionali GRAPH possono essere attivati messaggi. ad es. per interblocchi, supervisioni e avvisi GRAPH (controllo del tempo del passo).

Informazioni importanti sui tipi di messaggi

Essenziali per le differenze nel comportamento dei messaggi sono le seguenti caratteristiche:

- Se i messaggi sono provvisti di indicazione di stato (ad es. in entrata, in uscita, con i relativi timbri di data e ora)?
- Si tratta di messaggi con obbligo di conferma?

Se nessuna di queste condizioni si è verificata, ovvero se sono privi di stato e non necessitano di conferma, i messaggi informano soltanto su un evento che si è verificato ("Fire and Forget"). Sarà poi il dispositivo che riceve il messaggio a provvedere o meno alla sua memorizzare temporanea per un ulteriore utilizzo o anche soltanto per la visualizzazione.

La classe di segnalazione determina il comportamento di conferma

La presente sezione tratta le opzioni di impostazione dei messaggi di programma. Anche il comportamento dei messaggi di diagnostica di sistema e dei messaggi di controllo PLC, può essere a sua volta impostato (ad es. impostazioni di controllo ProDiag). Per maggiori dettagli fare clic sul link delle informazioni.

Le opzioni di impostazione dei messaggi del programma si trovano nell'editor dei messaggi (fare doppio clic su "Controlli e messaggi PLC" nella navigazione del progetto, quindi selezionare la scheda "Messaggi").

Per le CPU S7-1500 stabilire qui, tramite la classe di segnalazione, se un messaggio debba essere o meno confermato. Al momento della creazione di una nuova classe di segnalazione, oltre al comportamento di conferma, l'utente definisce anche la priorità di default del messaggio di questa classe di segnalazione.

Con l'opzione "Solo informazioni" ad es. nel tipo di messaggio, è possibile determinare se un messaggio è legato o meno allo stato, questo consente di ottenere un comportamento "fire-and-forget".

Nel seguito si riporta un esempio di impostazioni nell'editor dei messaggi con diverse classi di segnalazione ("Controlli e messaggi PLC" nella navigazione del progetto):

- Seconda riga "Program_Alarm": senza obbligo di conferma, soltanto informazioni ("Fire and Forget").
- Seconda riga "Program_Alarm_1": con obbligo di conferma e legato allo stato, in altri termini con il messaggio viene indicato se si tratta di un messaggio in entrata o in uscita.
- Terza riga "Program_Alarm_2": senza obbligo di conferma e legato allo stato, in altri termini con il messaggio viene indicato se si tratta di un messaggio in entrata o in uscita.

Tipi di messaggi

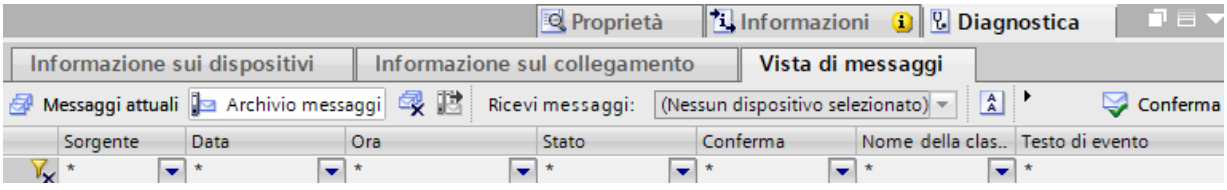
Nome	Tipo	ID	Luogo	Testo di messaggio	Testo info...	Classe di messaggio	Con conferma	Solo informaz
Program_Alarm	Messaggio PLC		AlarmType	myText	myINFO	No Acknowledgement	☐	☑
Program_Alarm_1	Messaggio PLC		AlarmType			Acknowledgement	☑	☐
Program_Alarm_2	PLC Alarm		AlarmType			No Acknowledgement	☐	☐

Visualizzazione di messaggi in TIA Portal

In runtime è inoltre possibile visualizzare i messaggi in TIA Portal: La vista messaggi si trova direttamente sotto l'editor dei messaggi (scheda "Diagnostica" > scheda "Vista messaggi").

Per quanto concerne il comportamento di conferma e di stato, vale quanto segue:

- Facendo clic sul pulsante "Messaggi attuali", vengono visualizzati i messaggi attualmente in entrata, in uscita e confermati. Soltanto i messaggi legati allo stato e quelli con obbligo di conferma vengono visualizzati qui. Un messaggio con obbligo di conferma (carattere blu) può essere confermato a sua volta in questa vista utilizzando il menu di scelta rapida oppure selezionando il pulsante "Conferma".
- Per osservare la sequenza cronologica (ad es. messaggio entrante, confermato e in uscita), fare clic sul pulsante "Archivio delle segnalazioni". Soltanto in questa vista sono elencati in sequenza i tre eventi appartenenti a questo messaggio. Nella vista "Messaggi attuali" si trova soltanto lo stato attuale di ciascun messaggio.
- I report informativi (messaggi con la proprietà "Solo informazioni") vengono visualizzati nella vista "Archivio delle segnalazioni". Poiché questi messaggi vengono attivati una sola volta e non vengono memorizzati negli Appunti, non appaiono nella vista "Messaggi attuali".
- I controlli PLC vengono a loro volta visualizzati nella vista messaggi.
- I messaggi di sistema appartengono generalmente alla classe di segnalazione "No Acknowledgement" con l'opzione "Solo informazioni". Questi messaggi vengono registrati nel buffer di diagnostica della CPU e consentono un'analisi della sequenza dei messaggi di sistema per un periodo di tempo limitato. Variazioni degli stati di funzionamento, registrate anche nel buffer di diagnostica, sono invece legate allo stato, ed indicano ad es. quando una CPU è entrata nello stato di funzionamento STOP, e se e quando ha abbandonato questo stato portandosi nello stato di funzionamento RUN. Queste informazioni vengono visualizzate negli stati "in entrata/in uscita".



Segnalazioni del controllore messe a disposizione dal server OPC UA

Per ricevere i messaggi della CPU S7-1500, un client OPC UA deve abbonarsi agli eventi OPC UA (MonitoredEventItems).

Per questo scopo, nell'area di indirizzi del server OPC UA della CPU S7-1500 si trovano i nodi corrispondenti, ovvero "Event-Notifier", questi nodi creano una Subscription per i client OPC UA per rendere possibile la ricezione di messaggi.

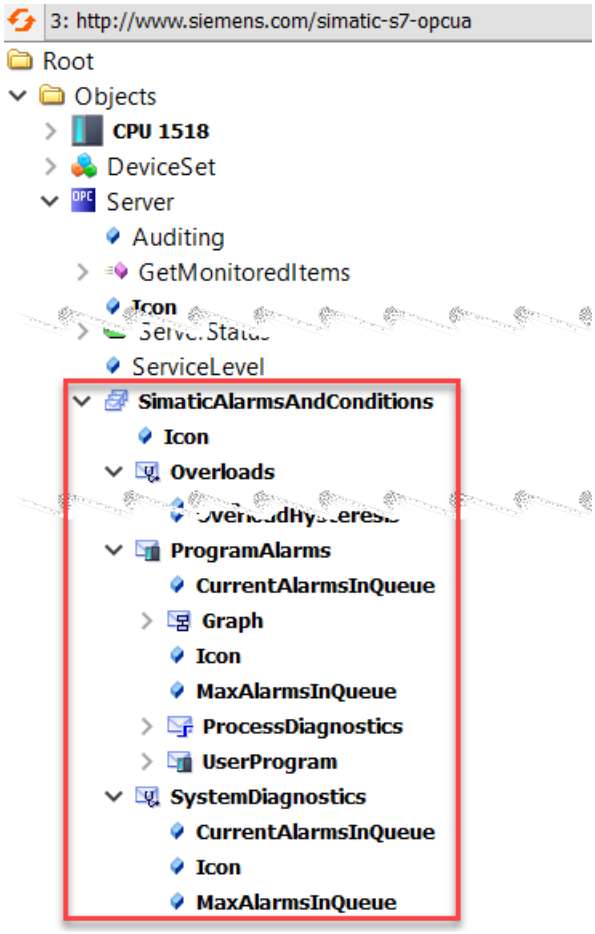
Per completezza va menzionato che per questo scopo, alla voce "Tipi" nell'area di indirizzi del server, sono inserite come nodi altre definizioni dei tipi. Le definizioni del tipo in "BaseEventType" e "ConditionType" garantiscono che i campi utilizzati dai messaggi SIMATIC vengano messi a disposizione anche sul server OPC UA.

L'area di indirizzi OPC UA della CPU S7-1500 rispecchia quindi, dopo l'attivazione di OPC UA Alarms and Conditions (proprietà della CPU nella configurazione hardware), i diversi tipi di messaggi (segnalazioni del controllore) come sopra descritto:

- ProcessDiagnostics
  Corrisponde ai messaggi di controllo del PLC con ProDiag
- SystemDiagnostics
  Corrisponde ai messaggi di diagnostica di sistema
- UserProgram
  Corrisponde ai messaggi di programma
- Graph
  Corrisponde ai messaggi GRAPH

Con la selezione del nodo per la Subscription, l'utente determina i tipi di messaggi che riceverà il client OPC UA. Il nodo "Server" ad es. consente la ricezione di tutti i messaggi, il nodo "UserProgram" invece, soltanto la ricezione di messaggi di programma.

Informazioni dettagliate sul modello OPC UA per Alarms & Conditions sono disponibili nel prossimo capitolo, in particolare, ulteriori informazioni sui nodi "Overloads" sono disponibili qui: Gestione dei limiti di memoria per OPC UA Alarms and Conditions (Pagina 348).



Ulteriori informazioni sui tipi di messaggi

I concetti e le possibilità di progettazione per le segnalazioni del controllore non vengono ulteriormente illustrati in questa sede. Nella guida in linea di STEP 7 sono disponibili informazioni sulla progettazione dei messaggi, sulla vista messaggi e sulle relative istruzioni, ad es. "Progam_Alarm".

11.3.6.2 Eventi OPC UA

Nel seguito si approfondiscono i concetti di base per l'elaborazione dei messaggio in OPC UA. Viene preso in esame il concetto di base degli "Events". In questo contesto sono state mantenute le denominazioni inglesi utilizzate nelle varie parti della specifica OPC UA.

Proprietà di Events

Nel modello di indirizzi del server OPC UA, a partire dalla versione firmware V2.9 della CPU, è possibile non soltanto accedere alle variabili PLC tramite nodi (lettura, scrittura) e utilizzare i metodi, ma anche ricevere eventi e messaggi dai nodi. Nel gergo di OPC UA si tratta di eventi.

Un evento contiene, tra l'altro, il testo dell'evento (Message), il timbro di data e ora (Time) e la sorgente dell'evento (SourceNode).

Le informazioni fornite da un evento del server dipendono dal tipo di evento. Nella Parte 5 della Specifica (Information Model), OPC UA definisce un BaseEventType.

Ulteriori tipi di eventi che mettono a disposizione un altro sistema di segnalazione, sono derivati da BaseEventType. Queste informazioni del tipo dei diversi tipi di evento sono visibili nell'area indirizzi di un server OPC UA (cartella "Types"). Ciò vale ad es. anche per i tipi di eventi di "Conditions" e "Alarms" che verranno trattati nel prossimo capitolo.

Quali proprietà (campi) di un evento siano obbligatorie (mandatory) e quali eventi siano opzionali, è fissato nella specifica OPC UA per il BaseEventType e per gli EventType derivati.

La figura seguente mostra la struttura gerarchica di BaseEventType.

Le sezioni seguenti mostrano come dalla radice della gerarchia di derivazione, ovvero dai BaseEventType, siano stati ricavati EventTypes specializzati. Le derivazioni specifiche di SIMATIC garantiscono che un client OPC UA possa abbonarsi alle informazioni fornite con un messaggio in SIMATIC e visualizzate ad es. su un dispositivo HMI, anche nell'area di indirizzi del server OPC UA.

L'evento stesso non è disponibile come nodo nell'area di indirizzi. Gli eventi vengono generati soltanto da nodi o oggetti dotati della proprietà "Event-Notifier". Questi nodi vengono spesso denominati anche oggetti dei messaggi di evento. Soltanto i nodi con questa proprietà possono essere indicati in una Subscription come EventMonitoredItem per la ricezione nel client dei rispettivi eventi.

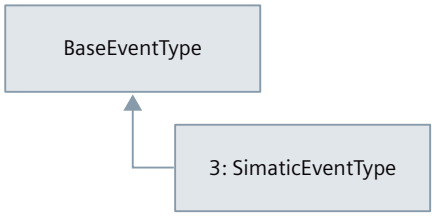
I nodi che possono generare eventi in una CPU S7-1500, sono oggetti come "Server", tra cui l'oggetto "SimaticAlarmsAndConditions" e i tre oggetti subordinati ProcessDiagnostics, SystemDiagnostics e UserProgram. In questi oggetti nell'area di indirizzi del server OPC UA della CPU è impostato l'attributo "EventNotifier".

Definizione di SimaticEventType

Dalla figura seguente è possibile vedere come il tipo "SimaticEventType" sia direttamente derivato da BaseEventType.

BaseEventType è la definizione di base del tipo di eventi in OPC UA.

Partendo da BaseEventType vengono definiti, direttamente o indirettamente, tutti i tipi di eventi per OPC UA.



Il tipo "SimaticEventType" è definito nel namespace SIMATIC(http://www.siemens.com/simatic-s7-opcua).

SimaticEventType è dotato di tutte le proprietà di BaseEventType, nonché delle proprietà specifiche che riproducono la struttura del campo dei messaggi di SIMATIC.

Descrizione dei campi degli eventi per SimaticEventType

La tabella seguente contiene informazioni sui campi di SimaticEventType per messaggi di tipo "Solo informazioni". I campi considerati opzionali da OPC UA e non utilizzati dal server OPC UA della CPU sono stati omessi. Una descrizione generale dei campi si trova inoltra nella specifica OPC 10000-5: OPC Unified Architecture, Part 5: Information Model, Release 1.04.

BrowsePath	DataType	Spiegazioni
EventId	ByteString	ID evento univoco
EventType	NodeId	ID del nodo di tipo di evento
Time	UtcTime	Data e ora dell'evento (Event occurrence)
ReceiveTime	UtcTime	Timbro di data e ora aggiornato in cui l'evento OPC UA è stato generato.
Message	LocalizedText	Testo dell'evento
Severity	UInt16	Priorità del messaggio di SIMATIC (0..16) esteso in un campo compreso tra 1..1000 in OPC UA, vedere la tabella seguente. La priorità definisce il grado di urgenza con cui è necessario reagire all'evento.
3:AdditionalText_01	LocalizedText	Testo supplementare opzionale 1
...	...	...
3:AdditionalText_09	LocalizedText	Testo supplementare opzionale 9
3:AssociatedValue_01	3:SimaticAssociatedAlarmValue	Variabile opzionale 1 (non per diagnostica di sistema)
...	...	...
3:AssociatedValue_10	3:SimaticAssociatedAlarmValue	Variabile opzionale 10 (non per diagnostica di sistema)
3:InfoText	LocalizedText	Testo informativo

BrowsePath	DataType	Spiegazioni
3:ID	UInt16	Numero del messaggio per tutta la CPU, assegnato dal sistema e che ha la funzione di identificare un messaggio.
3:DisplayClass	UInt16	Classe di segnalazione (utilizzata dai dispositivi HMI. Definisce quali eventi debbano essere visualizzati su un determinato dispositivo HMI.
3:GroupID	UInt8	Gruppo al quale appartengono i messaggi da confermare insieme.

Assegnazione priorità (SIMATIC) - Severity (OPC UA)

La seguente tabella mostra come le 17 priorità assegnabili ai messaggi in ambiente SIMATIC, vengano mappate sul livello 1000 Severity nel server OPC UA della CPU S7-1500.

Quest'assegnazione è specifica del produttore. E' possibile che per altri dispositivi valgano assegnazioni diverse.

OPC Range	Priorità 0..16 (SIMATIC)	Severity 1..1000 (OPC UA)
HIGH (667 – 1 000)	16	1000
	15	930
	14	860
	13	790
	12	720
MEDIUM (334 – 666)	11	650
	10	600
	9	550
	8	500
	7	450
	6	400
	5	350
LOW (1 – 333)	4	300
	3	225
	2	150
	1	75
	0	1

11.3.6.3 OPC UA Conditions e OPC UA Alarms

Nel seguito, basandosi sulle spiegazioni degli eventi riportate nei paragrafi precedenti, si approfondiscono i concetti di base di OPC UA Conditions e di OPC UA Alarms . In questo contesto sono state mantenute le denominazioni inglesi utilizzate nelle varie parti della specifica OPC UA.

Proprietà di Conditions

Presupposto per la comprensione è il concetto di "Events" in OPC UA.

Quando un oggetto del messaggio di evento, oltre alla sua proprietà di emettere Events, fornisce informazioni di stato, in OPC UA si parla di Conditions. Conditions rappresentano uno stato del sistema oppure uno dei suoi componenti. Sono stati di base "enabled" e "disabled", altre definizioni di stato sono comunque possibili.

Le variazioni di stato vengono a loro volta comunicate ai client OPC UA interessati tramite eventi (Condition Events).

Costituisce un esempio di Condition ad es. un'informazione di stato indicante che un dispositivo necessita di manutenzione.

Proprietà di Alarms

Le proprietà di ConditionType non sono tuttavia sufficienti a riprodurre completamente nel server OPC UA le caratteristiche dei messaggi SIMATIC.

Da ConditionType, derivato da BaseEventType, OPC UA definisce ulteriori tipi di eventi derivati, quali AcknowledgeableConditionType e AlarmConditionType.

AcknowledgeableConditionType integra le proprietà di ConditionType con la caratteristica "Confermabile" (AckedState).

AlarmConditionType integra le proprietà di ConditionType e AcknowledgeableConditionType con la capacità di assumere un "ActiveState". Nel gergo di SIMATIC questo è un messaggio in entrata. ActiveState segnala che la situazione che rappresenta Condition, attualmente esiste o si è verificata.

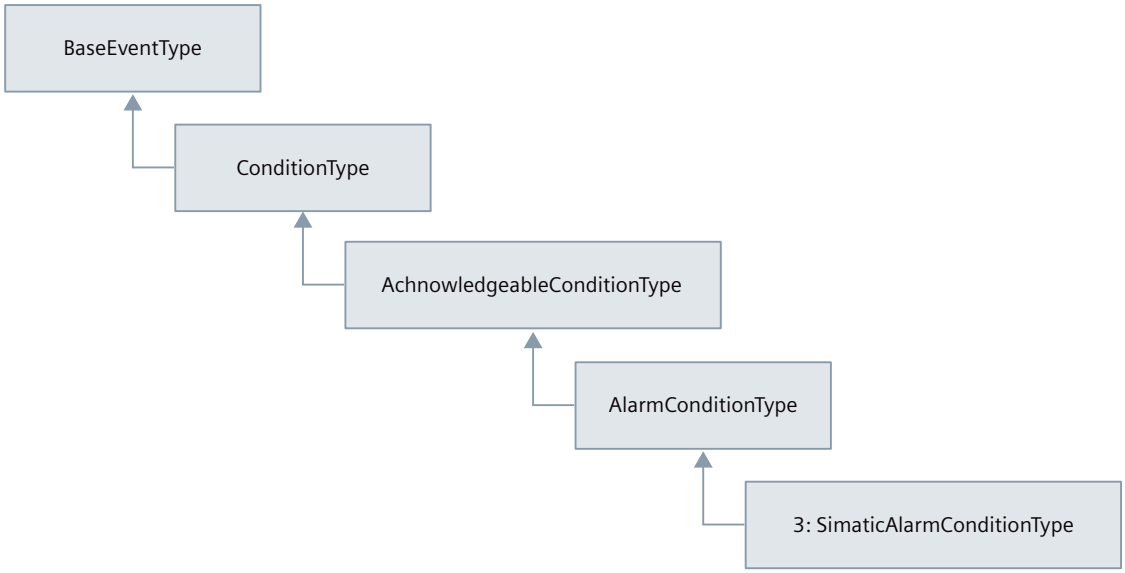
Esempio: La temperatura ha superato un valore limite. Se "ActiveState" non è impostato, la situazione rappresentata dalla condizione non esiste più. Generalmente in questo caso si parla di "Stato normale". Nel gergo SIMATIC questo corrisponde ad un messaggio in uscita.

In OPC UA vengono definiti ulteriori stati quali ad es. SilenceState o ShelvingState, che in questa sede non vengono tuttavia illustrati in quanto non svolgono alcun ruolo nella mappatura del sistema di segnalazioni SIMATIC.

AlarmConditionType deriva da SimaticAlarmConditionType che contiene tutti i campi degli eventi che consentono di riprodurre lo stato e le informazioni di conferma dei messaggi di SIMATIC.

Definizione di SimaticAlarmConditionType

La figura seguente illustra come gli eventi di tipo "SimaticAlarmConditionType" siano definiti da una serie di estensioni di OPC UA "BaseEventType";



Descrizione dei campi degli eventi per SimaticAlarmConditionType

La tabella seguente contiene informazioni sui campi di SimaticAlarmConditionType per messaggi legati allo stato e confermabili che vanno ad aggiungersi ai campi degli eventi come in SimaticEventType. I campi considerati opzionali da OPC UA e non utilizzati dal server OPC UA della CPU sono stati omessi. Una descrizione dei campi si trova inoltra nella specifica OPC 10000-9: OPC Unified Architecture, Part 9: Alarms & Conditions, Release 1.04.

BrowsePath	DataType	Spiegazioni
ConditionClassId	NodeId	Sono possibili ID dei nodi per SystemConditionClassType, ProcessConditionClassType o BaseConditionClassType
ConditionClassName	LocalizedText	DisplayName di ConditionClassId
Retain	Boolean	Indica che il messaggio è ancora rilevante per i client OPC UA (impostato se il messaggio è ancora presente e non è stato confermato).
Comment	LocalizedText	• Il commento più recente inserito con il metodo "AddComment" oppure "Acknowledge". • ZERO in caso di riavvio del server e quanto non è stato inserito alcun commento.
Comment.SourceTimestamp	UtcTime	Timbro di data e ora dell'ultima modifica al campo del commento
AckedState	LocalizedText	"Acknowledged" or "Unacknowledged"
AckedState.Id	Boolean	Impostato, se è stato confermato

BrowsePath	DataType	Spiegazioni
AckedState.TransitionTime	UtcTime	Momento in cui il messaggio è stato confermato. ZERO se non confermato o non confermabile.
ActiveState	LocalizedText	"Active" o "Inactive"
ActiveState.Id	Boolean	Impostato se "Attivo"

11.3.6.4 Attivazione di Alarms and Conditions

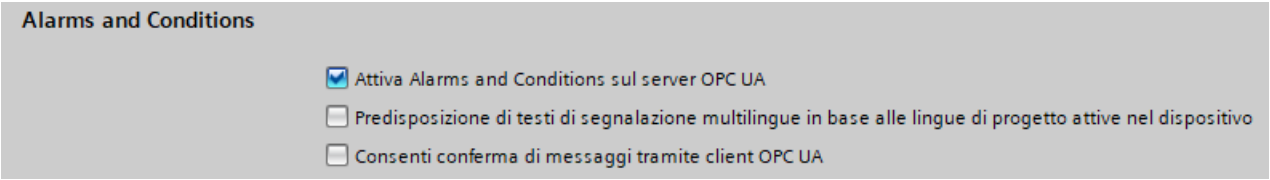
Presupposti

- CPU S7-1500 dalla versione firmware V2.9
- Licenza Runtime per OPC UA acquisita secondo le specifiche di licenza e impostate nelle proprietà della CPU.
- Il parametro "Gestione centrale dei messaggi nel PLC" è attivato (area "Messaggi PLC" nelle proprietà della CPU).

Procedimento

Per attivare i messaggi tramite OPC UA Alarms and Conditions, procedere nel modo seguente:

1. Nelle proprietà della CPU navigare fino all'area "OPC UA > Server > Generale".
2. Attivare l'opzione "Attiva Alarms and Conditions sul server OPC UA".
   Soltanto dopo che l'opzione è stata attivata, i relativi tipi e oggetti in grado di generare eventi, diventano visibili nell'area di indirizzi.
3. Se necessario, attivare anche l'opzione "Consenti conferma di messaggi tramite client OPC UA".
   In questo caso, tutti i client OPC UA collegati possono confermare un messaggio con obbligo di conferma utilizzando il metodo "Acknowledge".



Suggerimento: Attivazione della diagnostica "La richiesta del client OPC UA remoto non è riuscita"

Se il server OPC UA non può allocare una memoria sufficiente, in questo stato non è possibile generare allarmi OPC UA; è possibile una perdita dei messaggi per i client OPC UA.

Di conseguenza è necessario attivare la diagnostica "La richiesta del client OPC UA remoto non è riuscita" per poter diagnosticare questo stato (proprietà della CPU > OPC UA > Server > Diagnostica).

Inoltre è necessario attivare anche l'opzione "Raggruppa diagnostiche in presenza di un elevato numero di messaggi".

Non appena è d nuovo disponibile memoria sufficiente, i client OPC UA devono richiamare il metodo ConditionRefresh per ottenere lo stato attuale del sistema di allarme.

Ulteriori informazioni

Per informazioni sui metodi di OPC UA Alarms and Conditions consultare il capitolo Metodi di OPC UA Alarms and Conditions (Pagina 344).

Per informazioni sulle richieste fallite di un client rimosso consultare il capitolo Richiesta di un client remoto non riuscita (Pagina 356).

11.3.6.5 Acconsentire eventi di un server OPC UA

Abbonamento a tutti gli eventi dal nodo "Server"

I server OPC UA mettono a disposizione eventi tramite nodi "Server" e nodi subordinati. Abbonandosi al nodo "Server", i client OPC UA ricevono tutti gli eventi e i messaggi del server OPC UA.

Il nodo "Server" si trova nella cartella "Objects", sotto "Root".

I server OPC UA informano i relativi client sui tipi di eventi utilizzati (in "Root > Types > EventTypes" nell’area indirizzi).

Opzioni di filtraggio degli eventi

I client OPC UA possono effettuare una selezione e abbonarsi soltanto a determinati nodi al di sotto del nodo "Server" e pertanto a determinati tipi di evento, ad es. solo al nodo "UserProgram". In questo modo il numero di eventi dal server OPC UA si riduce ai messaggi del programma.

Un'altra modalità di filtraggio consiste nella selezione dei campi degli eventi, definiti "Select Clause" nel linguaggio OPC UA.

In altri termini, nella Subscription il client UA OPC specifica, oltre all'oggetto del messaggio di evento (ad es. il nodo "UserProgram"), anche una selezione dei campi degli eventi. La selezione dei campi degli eventi avviene dal Browse Name del campo corrispondente.

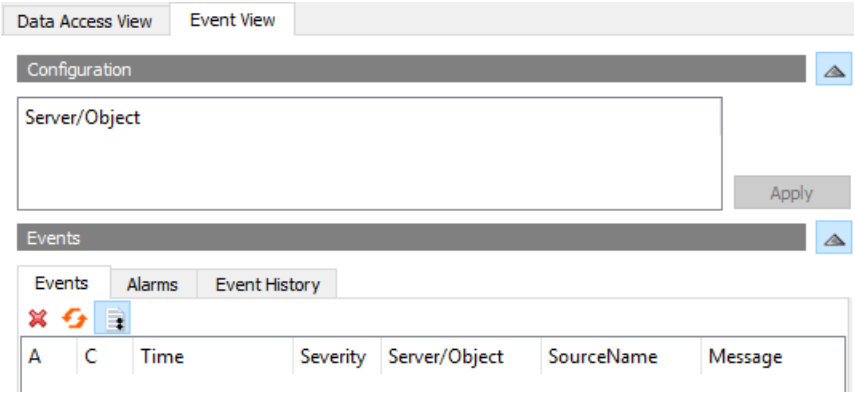
L'OPC UA definisce inoltre le cosiddette "Where Clauses". L'impiego di una Where Clause in un filtro di eventi avviene per limitare ulteriormente il numero di eventi forniti dal server OPC UA per l'oggetto selezionato, ad es. tramite un filtro in un'area di sicurezza.

Esempio di Client UaExpert

Sull'esempio del client OPC UA UaExpert, è possibile dimostrare come gli eventi di un server OPC UA possano essere ricevuti tramite una Subscription. Il seguito riporta le informazioni più importanti sugli eventi e sui messaggi visualizzati:

- Event View è una vista propria degli eventi oltre ad Access View.
- Nel campo "Configuration" si trova l'oggetto del messaggio di evento selezionato con i campi di Select Clause. La configurazione di Where-Clauses in UaExpert non è attualmente possibile.
- Nel campo "Events", nella scheda "Events": Corrisponde alla vista nella Vista messaggi TIA con il pulsante "Archivio delle segnalazioni" attivato; qui sono visibili anche eventi della categoria "Solo informazioni" e i messaggi usciti, in quanto UaExpert li salva in background nella memoria temporanea per la visualizzazione. Nella scheda "Alarms" questi eventi non sono visibili.
- Nel campo"Events", nella scheda "Alarms": Corrisponde alla vista nella Vista messaggi TIA con il pulsante "Messaggi attivi" selezionato; qui sono visibili i messaggi con il relativo stato, ad es. "active" (corrisponde a "in entrata") che possono essere anche confermati dal menu di scelta rapida. I messaggi in uscita non sono più visibili in questa vista.

Le colonne dei report degli eventi offrono una selezione dei campi degli eventi, ad es. il testo dell'evento (Message) e l'indicazione se il messaggio è stato o meno confermato (A=Acknowledged).



Particolarità della vista messaggi nel server OPC UA della CPU

Ne seguito si riepilogano ancora una volta le particolarità della visualizzazione dei messaggi tramite OPC UA Alams and Conditions per lo stato attuale.

Argomento	Spiegazione
Commento (Comment)	Con il metodo "AddComment" oppure con il metodo "Acknowledge" in OPC UA, è possibile aggiungere un commento al messaggio. Al riavvio del server il commento non è più disponibile.
I messaggi in attesa non vanno perduti dopo il riavvio del server	Il server OPC UA supporta il metodo "ConditionRefresh" che utilizza per fornire al client OPC UA lo stato attuale del sistema, ad es. dopo aver caricato un nuovo blocco dati (richiede un riavvio del server e una nuova creazione del collegamento).

11.3.6.6 Modifica delle variabili nei messaggi

Per i messaggi di SIMATIC è possibile specificare dei segnaposto. I segnaposto permettono di integrare nel testo del messaggio fino a 10 variabili (da SD_1 a SD_10). I segnaposto possono anche essere voci di elenchi di testi specifici.

Per utilizzare i messaggi con segnaposto valgono le regole seguenti:

- I segnaposto che rappresentano valori all'interno di un messaggio vengono inseriti automaticamente solo nel caso delle segnalazioni di diagnostica del sistema o delle segnalazioni di eventi di sicurezza. Per altre categorie di segnalazioni (ad es. i messaggi di programma) i segnaposto che corrispondono a valori non vengono risolti. Queste risoluzioni devono essere eseguite dai client OPC UA.
- I segnaposto che fanno riferimento a elenchi di testi vengono risolti dalla CPU (ad es. il formato: %t#<Nome elenco di testi>).

Esempio di assegnazione di valori e segnaposto tramite UaExpert

1. Assicurarsi che nella configurazione UaExpert siano attivati tutti i campi necessari.

   Tenere presente che ogni campo non necessario genera un carico di comunicazione. Evitare pertanto di selezionare tutte le voci, come mostra l'esempio seguente per semplificare.

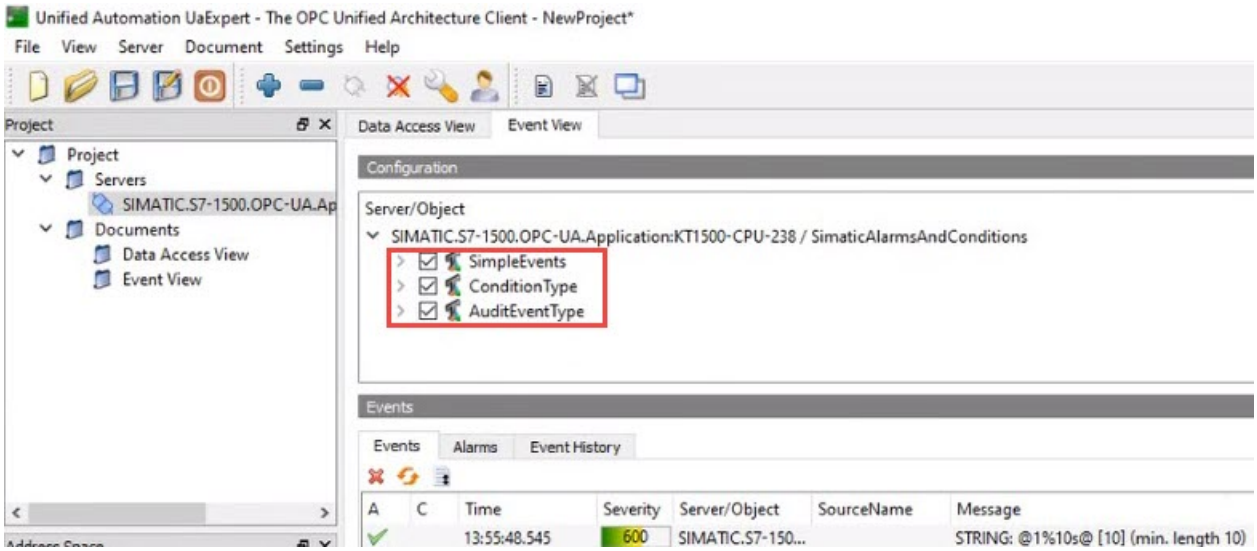


Figura 11-55 ServerObjekct-Configuration_neutral120

2. Nella scheda "Events" di UaExpert selezionare il messaggio con le variabili integrate.
   Nel campo "Details" del messaggio si trova il valore da integrare nel messaggio.
   Esempio: "AssociatedValue_01" viene assegnato a SD_1 (formato @1% ...@).
   Una spiegazione dei formati delle variabili si trova nel sistema di informazione di TIA Portal (ad es. cercando "Esempio di variabili").

Supporto di tipi di dati semplici come variabili

Il tipo campo da "AssociatedValue_01" a ..._10 è Union ed è limitato ad alcuni tipi semplici. Il tipo di dati OPC UA è SimaticAssociatedAlarmValue. Sono supportati i seguenti tipi di dati semplici:

3:AssociatedValue_01	SimaticAssociatedAlarmValue
Switch Field	2
Boolean	True
3:AssociatedValue_02	SimaticAssociatedAlarmValue
Switch Field	6
SByte	123
3:AssociatedValue_03	SimaticAssociatedAlarmValue
Switch Field	3
Int16	1234
3:AssociatedValue_04	SimaticAssociatedAlarmValue
Switch Field	4
Int32	12345
3:AssociatedValue_05	SimaticAssociatedAlarmValue
Switch Field	7
Byte	123
3:AssociatedValue_06	SimaticAssociatedAlarmValue
Switch Field	8
UInt16	1234
3:AssociatedValue_07	SimaticAssociatedAlarmValue
Switch Field	11
Float	1
3:AssociatedValue_08	SimaticAssociatedAlarmValue
Switch Field	12
Double	2
3:AssociatedValue_09	SimaticAssociatedAlarmValue
Switch Field	9
UInt32	12345
3:AssociatedValue_10	SimaticAssociatedAlarmValue
Switch Field	13
String	HelloWorld

Figura 11-56 UnionDataTypes_neutral120

Mappatura sui tipi di dati SIMATIC

Vale la seguente assegnazione dei tipi di dati SIMATIC => tipi di dati OPC UA:

Tipi di dati per supportati per SD_1 ... SD_10	Mappatura in OPC UA
BOOL	Boolean
BBOOL	Boolean
BYTE	Byte
CHAR	Byte
SINT	SByte
USINT	Byte
WORD	UInt16
WChar	UInt16
INT	Int16
UINT	UInt16

Tipi di dati per supportati per SD_1 ... SD_10	Mappatura in OPC UA
DWORD	UInt32
DINT	Int32
UDINT	UInt32
REAL	Float
LREAL	Double
String	String
WString	String

11.3.6.7 Ricezione simultanea di messaggi in più lingue

I messaggi vengono trasmessi dal server OPC UA al client OPC UA nella lingua predefinita o di riferimento. Nel campo "Lingue disponibili per la selezione" dei parametri della CPU è possibile impostare in quale lingua di progetto tra quelle caricate debbano essere trasmessi i messaggi.

Dalla versione V4.0 delle CPU S7-1500, è possibile selezionare le lingue dei client OPC UA collegati:

- All'apertura della sessione, un client può richiedere testi di segnalazione in una o più lingue di progetto attive utilizzando il parametro "LocaleIds []", vedere OPC 10000-4: Services, ActivateSession Service Parameters.

  Solo i testi di segnalazione possono essere richiesti al server OPC UA della CPU in questo modo; questo parametro non ha alcun effetto su altri testi localizzati nell'area indirizzi.

  Presupposti: l'opzione "Predisposizione di testi di segnalazione multilingue in base alle lingue di progetto attive nel dispositivo" è attivata.
- Un client può richiedere contemporaneamente i testi di segnalazione in tutte e 3 le lingue attive del progetto, ad es. per raggruppare i messaggi su un server centrale in modo che possano essere analizzati da persone in lingue diverse.

Presupposti

- CPU S7-1500 dalla versione firmware V 4.0
- Il client OPC UA supportata i LocaleIds "mul" e "qst" per i testi multilingue.
- L'opzione "Predisposizione di testi di segnalazione multilingue in base alle lingue di progetto attive nel dispositivo" è attivata (campo "Alarms and Conditions" nelle proprietà della CPU).

Azione di LocaleId "mul" e "qst"

La specifica OPC UA (OPC 10000-3: UA Part 3: Address Space Model) descrive il tipo di dati Built-in "LocalizedText" che viene utilizzato per i testi in diverse lingue.

Gli elementi della struttura per il tipo di dati LocalizedText sono definiti come indicato nel seguito:

Nome	Tipo	Descrizione
LocalizedText	Struttura	
Locale	LocaleId	Identificativo della lingua (abbreviazione della lingua) <lingua>-<paese/regione>, ad esempio "it-IT" Specificato tramite IETF RFC 5646
Testo	String	Testo localizzato (traduzione nella lingua richiesta)

LocaleId = "mul"

Un client OPC UA che richiede un LocalizedText con il LocalId "mul", riceve i testi di segnalazione in tutte le lingue di progetto caricate nella CPU come elemento di testo JSON costituito da un array formato da Locale/coppie di testo.

L'esempio seguente riporta testi in 2 lingue. Gli spazi e le interruzioni non vengono trasferiti, qui sono stati aggiunti per facilitare la leggibilità:

```
{
 "t": [
 ["de-DE","mein Text"],
 ["en-US","my text"]
 ]
}
```

Testo che ne risulta:

```
de-DE: "mein Text"
en-US: "my text"
```

LocaleId = "qst"

"qst" non è un'abbreviazione, ma semplicemente una stringa di caratteri definita per un parametro LocaleId che, come in "mul", oltre ai contenuti comprende anche testi sostitutivi.

Un client OPC UA che richiede un LocalizedText con il LocaleId "qst", riceve i testi di segnalazione in tutte le lingue di progetto caricate nella CPU. Oltre all'array di LocaleId, l'elemento di testo JSON ha anche una sezione con la definizione dei testi sostitutivi (sezione Replacement). Il client deve inserire nel testo del messaggio i testi sostitutivi forniti.

Testi di esempio in 2 lingue; "t" sta ad indicare "text", "r" indica invece "replacement":

```
{
 "t": [
 ["de-DE","mein Text @1@ /2/"],
 ["en-US","my text @1@ /2/"]
 ],
 "r": [
["@1@", "myCompany"]
```

["/2/", 1.2345]
]
}

Testo che ne risulta:

```
de-DE: "mein Text myCompany 1,2345"
en-US: "my text myCompany 1.2345"
```

Non essendo formattato come stringa nel campo Replacement, il numero decimale 1.2345 può essere scritto correttamente nelle diverse lingue (con una virgola in tedesco, con un punto in inglese americano) a condizione che questa funzione sia implementata nel client.

Regole

I testi di segnalazione vengono generati dal server secondo le regole seguenti e messi a disposizione del client:

- Per semplificare la gestione dei testi dei messaggi multilingue, per il server dell'S7-1500 è ammesso solo il LocaleId "qst".

  Se si richiedono testi di messaggi multilingue con "qst" e nel testo sono presenti segnaposto (variabili), questi verranno forniti nella sezione Replacement. Se nel testo non sono disponibili segnaposto, il testo viene restituito come LocaleId "mul" senza sezione Replacement.

  Se viene restituita una sola lingua (ad es. perché è l'unica lingua attiva, oppure perché il confronto con le lingue richieste restituisce una sola lingua), e nel testo non esistono segnaposto, il testo di segnalazione non viene restituito come JSON, bensì direttamente come testo localizzato nella lingua corrispondente.
- Un client può richiamare i messaggi in tutte le lingue fornite dal server oppure soltanto una selezione. Il client determina la selezione tramite un array di LocaleIds che segue il LocaleId "qst". Se nessun altro LocaleId segue il LocaleId "qst", tutte le lingue presenti vengono rese disponibili dal server.
- I testi sostitutivi multilingue non vengono restituiti nella sezione Replacement. I testi sostitutivi multilingue vengono creati utilizzando elenchi di testi, vedere AUTOHOTSPOT.

Lettura delle lingue supportate

Il server OPC UA pubblica le lingue supportate sotto il nodo "ServerCapabilities > LocaleIdArray".

11.3.6.8 Metodi di OPC UA Alarms and Conditions

La parte 9 della specifica OPC UA (OPC 10000-9: Alarms & Conditions) definisce i metodi per il server OPC UA, per consentire ai client OPC UA di reagire ad es. a variazioni di stato.

Di seguito sono descritti i metodi supportati con le loro specificità dal server OPC UA della CPU S7-1500.

Presupposti

Affinché i metodi rilevanti per la funzionalità Alarms and Conditions siano utilizzabili, devono sussistere i seguenti presupposti:

- Alarms and Conditions deve essere attivato
- Per il metodo "Acknowledge" il server deve consentire ai client OPC UA la conferma dei messaggi.

Metodi di OPC UA Alarms and Conditions

Di seguito sono spiegati brevemente i metodi con specificità e limitazioni derivanti dall'impiego del server OPC UA della CPU S7-1500.

Questi metodi sono visibili nell'area dei tipi.

Suddetta specifica OPC UA contiene la descrizione generale.

Di seguito alla tabella riepilogativa è presente la descrizione dettagliata dei singoli metodi.

Metodo	Descrizione
Acknowledge	Metodo di conferma di un oggetto di allarme contrassegnato in modo univoco da un EventId.
ConditionRefresh	Metodo di richiesta di aggiornamento di tutti gli oggetti di allarme (nel gergo di SIMATIC: aggiornamento di tutti i messaggi presenti). Tutti gli elementi controllati (Monitored Items) della Subscription vengono aggiornati. La sincronizzazione di oggetti di allarme presenti del server OPC UA della CPU viene ad es. visualizzata nelle seguenti situazioni: • Primo collegamento o ripristino del collegamento (dopo un'interruzione della comunicazione) • Commutazione della pagina sulla schermata di un dispositivo HMI
AddComment	Metodo di inserimento dei commenti agli oggetti di allarme.

Richiamo dei metodi "Acknowledge" e "AddComment"

I richiami dei metodi in OPC UA utilizzano MethodId und ObjectId.

Nel caso di un oggetto di allarme, ObjectId è l'ID del nodo per l'istanza di quest'oggetto.

Poiché il modello indirizzi Alarms and Conditions di Simatic non fornisce istanze per gli oggetti di allarme, la specifica OPC UA prevede che in questo caso il client OPC UA utilizzi il ConditionId come ObjectId.

Informazioni sulla rilevazione di ConditionId tramite SimpleAttributeOperands nella SelectClause del filtro di eventi, sono a loro volta disponibili nella parte 9 della specifica OPC UA (OPC 10000-9: Alarms & Conditions):

Name	Type	Description
SimpleAttributeOperand		
typeId	NodeId	*NodeId* of the *ConditionType Node*
browsePath[]	QualifiedName	empty
attributeId	IntegerId	Id of the *NodeId Attribute*

Acknowledge

Il metodo Acknowledge (MethodId: i=9111) ha i seguenti parametri:

Parametro	Tipo di dati	Descrizione
[in] EventId	ByteString	EventId identifica una determinata Event Notification. Soltanto gli eventi il cui campo AckedState.Id ha il valore "False", possono essere confermati con il metodo "Acknowledge".
[in] comment	LocalizedText	Testo del commento di una conferma, ad es. da parte dell'operatore. Vedere anche la descrizione integrativa del metodo "AddComment".

Method Result Codes

Result Code	Descrizione
Good	Il metodo è stato eseguito correttamente.
BadNotSupported	Il metodo non può essere richiamato perché nelle proprietà della CPU per OPC UA è disattivata l'opzione di conferma per Alarms and Conditions da parte dei client OPC UA.
BadConditionBranchAlreadyAcked	La conferma è già avvenuta.
BadNodeIdUnknown	Il richiamo del metodo è avvenuto con un ConditionId errato (vedere le note relative a ObjekctId).
BadEventIdUnknown	Il richiamo del metodo è avvenuto con un EventId errato.

ConditionRefresh

Il metodo ConditionRefresh (MethodId: i=3875) ha i seguenti parametri:

Parametro	Tipo di dati	Descrizione
[in] SubscriptionId	Uint32	SubscriptionId della Subscription da aggiornare.

Method Result Codes

Result Code	Descrizione
Bad_SubscriptionIdInvalid	SubscriptinId non è valido.
Bad_RefreshInProgress	Il metodo "ConditionRefresh" è attualmente in esecuzione.
Bad_UserAccessDenied	Il metodo "ConditionRefresh" è in esecuzione nel contesto di una sessione errata. In altri termini la Subscription fa parte di un'altra sessione.

NOTA

Metodo ConditionRefresh2

Il server OPC UA della CPU S7-1500 non supporta il metodo ConditionRefresh2, in grado di sincronizzare in modo mirato un elemento controllato (MonitoredItem) in una Subscription. In questo caso il server OPC UA restituisce Result Code "Bad_MethodInvalid". In questo caso impiegare il metodo "ConditionRefresh".

AddComment

L'utente può aggiungere un commento agli oggetti Alarms-di tipo SimaticAlarmConditionType in quanto il supporto dei commenti per OPC UA Alarms and Conditions è obbligatorio.

Un commento viene salvato nel campo degli eventi "Comment".

I seguenti campi degli eventi con timbro di data e ora appartengono al commento:

- "Comment.SourceTimestamp" per data e ora di acquisizione del commento nella CPU
- "Time" per data e ora della modifica all'oggetto Alarms

Con il richiamo del metodo "AddComment", "Time" e "Comment.SourceTimestamp" sono identici.

Particolarità dei commenti Alarm and Conditions per il server OPC UA della CPU

Il metodo Acknowledge (MethodId: i=9029) ha i seguenti parametri:

Parametro	Tipo di dati	Descrizione
[in] EventId	ByteString	EventId identifica Event Notification per la quale è stato segnalato uno stato.
[in] comment	LocalizedText	Testo del commento dell'oggetto Alarms specificato.

Method Result Codes

Result Code	Descrizione
Good	Il metodo è stato eseguito correttamente.
BadNodeIdUnknown	Il richiamo del metodo è avvenuto con un ConditionId errato (vedere le note sul richiamo dei metodi "Acknowlege" e "AddComment").
BadEventIdUnknown	Il richiamo del metodo è avvenuto con un EventId errato.

Particolarità dei commenti Alarm and Conditions per il server OPC UA della CPU

Utilizzando il metodo AddComment l'utente può aggiungere commenti agli oggetti di allarme di tipo "SimaticAlarmConditionType". Anche durante il richiamo del metodo Acknowledge viene impostato un commento. Il metodo "AddComment" può essere richiamato più volte.

- Un commento viene salvato nel campo degli eventi "Comment".
  "Comment.SourceTimestamp" identifica la data e l'ora dell'ultimo **commento**.
- Il timbro di data e ora "Time" identifica **data e ora dell'ultima modifica all'oggetto di allarme**.

Con il richiamo del metodo "AddComment", "Time" e "Comment.SourceTimestamp" sono identici.

Se viene richiamato il metodo "Acknowledge", può accadere che i due timbri di data e ora differiscano tra loro, in quanto la conferma avviene in modo asincrono.

Per OPC UA Alarms and Conditions il supporto dei commenti è obbligatorio. Il sistema di segnalazione SIMATIC non conosce commenti corrispondenti per i messaggi. Per questo occorre osservare alcune particolarità:

- È disponibile un solo commento:
  per un oggetto di allarme esiste soltanto un commento, ciò consente che in presenza di più richiami consecutivi dei metodi, un commento preesistente venga sempre sovrascritto.
- Durata e timbro di data e ora:
  i commenti vengono salvati soltanto nell'oggetto di allarme attuale. Se l'oggetto di allarme non è più disponibile, ad es. dopo un riavvio del server, anche il commento non sarà più disponibile. I rispettivi campi degli eventi "Comment" e "Comment.SourceTimestamp" sono resettati (zero).
  Il campo degli eventi "Time"è impostato come se il richiamo del metodo "AddComment" non fosse avvenuto. Esempio: Commentando un oggetto Alarms non confermato, il campo degli eventi "Time" riceve la data e l'ora di questa modifica al commento. Dopo un riavvio del server, il campo degli eventi "Time" non visualizza il momento in cui il commento è stato impostato, bensì il momento di entrata del relativo Event.

11.3.6.9 Gestione dei limiti di memoria per OPC UA Alarms and Conditions

Il server OPC UA della CPU S7-1500 dispone, per la funzione "Alarms and Conditions", di una capacità di memoria ridotta specifica del prodotto (vedere i dati tecnici delle CPU).

Per le diverse categorie di messaggi sono disponibili due pool di memoria:

- Pool di memoria destinato soltanto a ProgramAlarms (corrisponde ai generatori dei messaggi riferiti al programma (Producer) quali ad es. i messaggi di programma tramite Program_Alarm, ProDiag, Graph)
- Pool di memoria destinato soltanto a SystemDiagnostics (corrisponde ai messaggi di diagnostica di sistema)

In presenza di condizioni sfavorevoli (ad es. un picco di messaggi), la CPU non è in grado di fornire al sistema OPC UA Alarms and Conditions, tutti i messaggi in coda (ProgramAlarms o SystemDiagnostics) dell'area allarmi SIMATIC. In questo caso i messaggi non vanno comunque perduti.

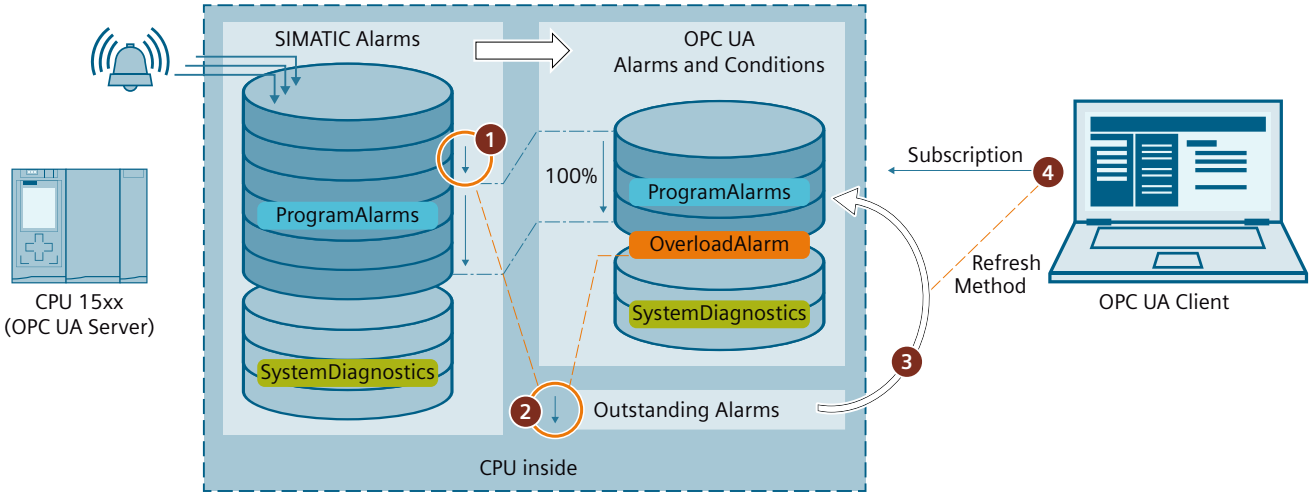
È possibile reagire a questo evento di sovraccarico nel programma utente. A seconda dell'applicazione, utilizzando il metodo "ConditionRefresh" è possibile rendere nuovamente disponibili al sistema OPC UA Alarms and Conditons, i messaggi che non sono per così dire "confluiti nel sistema OPC UA Alarms-and-Conditons".

Presupposti

- Alarms and Conditions deve essere attivato
- Le Subscriptions agli eventi sono configurate nel client OPC UA

Principio

La figura sottostante illustra in modo semplificato il processo di bufferizzazione dei messaggi ProgramAlarms per renderli nuovamente disponibili a OPC UA Alarms and Condition System in un secondo momento. I nodi menzionati nella legenda dei simboli sono visibili nella pagina successiva del modello indirizzi.



① Il numero di messaggi attivi è troppo elevato per rendere accessibili tutti i messaggi tramite OPC UA Alarms and Conditions.

② Viene generato l'allarme Overloads (messaggio di sovraccarico). Questo messaggio di sovraccarico rimane attivo fino al verificarsi della seguente situazione:
- Non sono più presenti allarmi per il sistema OPC UA Alarms and Conditions (OutstandingProgramAlarms = 0) e
- Il numero di allarmi nel sistema OPC UA Alarms and Conditions < Valore massimo corretto dall'isteresi per gli allarmi OPC UA (= MaxAlarmsInQueue - OverloadHysteresis)

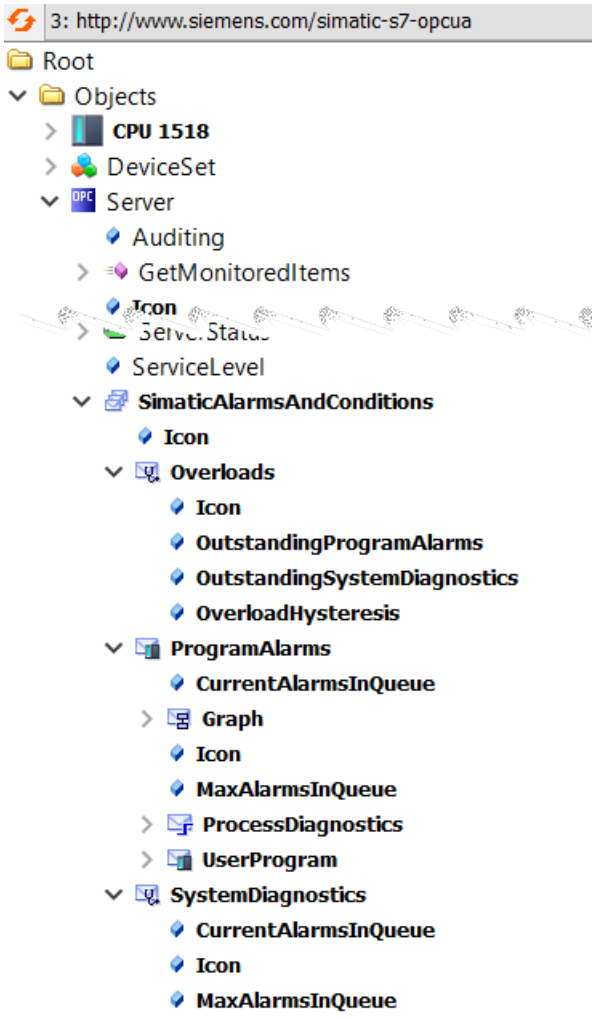
I messaggi che a causa della situazione di sovraccarico non sono disponibili nel sistema OPC UA Alarms and Conditions, vengono memorizzati negli Appunti dalla CPU come "OutstandingAlarms"

③ Se un client OPC UA esegue il metodo ConditionRefresh, non vengono sincronizzati soltanto tutti gli oggetti di allarme della Subscription interessata, ma anche i messaggi in coda (OutstandingAlarms) di OPC UA Alarms and Conditions vengono trasferiti nell'area di memoria Alarms and Condition fino al raggiungimento del numero massimo di allarmi. Gli allarmi "più datati" vengono trasferiti per primi. In questo modo ogni Subscription a questi allarmi riceve gli allarmi trasferiti e non soltanto il client OPC UA che ha richiamato il metodo ConditionRefresh.

④ Il client OPC UA comanda, tramite le informazioni dei nodi Overloads, la gestione dei messaggi in cosa.

Modello indirizzi per Alarms and Conditions

La figura seguente mostra il nodo del modello indirizzi di OPC UA Alarms and Conditions.



Particolarità

- Allarmi in uscita o confermati non confluiscono più nell'area di sistema OCP UA Alarms-and-Condition tramite il metodo ConditionRefresh. Per OPC UA Alarms and Conditions e conseguentemente per i client OPC UA collegati, questi allarmi non sono più visibili. Ciò influenza ad es. le analisi statistiche nell'andamento dei messaggi.
- Per evitare all'allarme Overload un'elevata frequenza di allarmi, quando il volume dei messaggi oscilla intorno al valore massimo, il limite per la generazione di un allarme è maggiore del limite per il relativo annullamento: Il valore di questa differenza viene visualizzato nel nodo "OverloadHysteresis".
  Esempio: Numero massimo di messaggi: 200, OverloadHysteresis: 3.
  Overloads Alarm viene attivato a partire da 200 messaggi e annullato quando il numero di messaggi è inferiore a 197. Con l'incremento del volume, e a partire dal 200 messaggi, quest'allarme viene nuovamente attivato.

11.3.7 Utilizzo delle possibilità di diagnostica

11.3.7.1 Diagnostica del server OPC UA

Diagnostica online del server OPC UA

La diagnostica online del server OPC UA della CPU S7-1500 può essere effettuata con i normali client OPC UA, ad es. UaExpert.

Le informazioni di diagnostica sono suddivise nei seguenti tipi:

- Server Diagnostics
- Sessions Diagnostics
- Subscriptions Diagnostics

Nell'area indirizzi del server sono ad es. disponibili i seguenti nodi con informazioni diagnostiche:

- **ServerDiagnosticsSummary**: Sintesi della diagnostica server
  - CurrentSessionCount: Numero di sessioni attive
  - SecurityRejectedSessionCount: numero delle sessioni rifiutate per impostazioni non compatibili di security del punto finale tra client e server
- **SessionsDiagnosticsSummary**: Sintesi della diagnostica sessione
  - ActualSessionTimeout: Il timeout di permanenza di una sessione ad es. in caso di interruzione del collegamento
- **SubscriptionsDiagnosticsArray**: Array con un elemento per ciascuna subscription per la relativa sessione

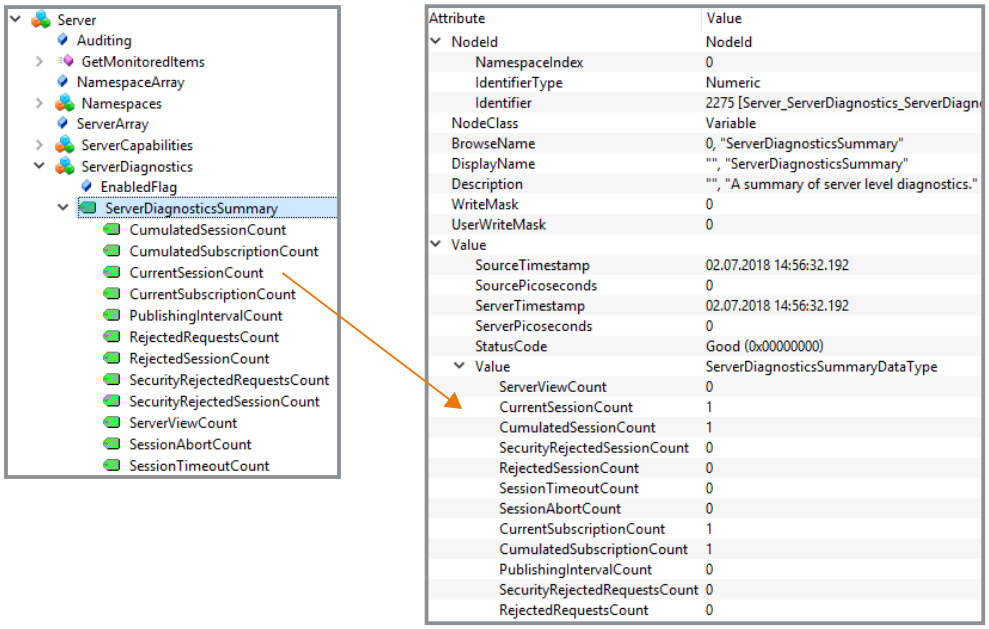


Figura 11-57 Server Diagnostics

Il nodo SessionsDiagnosticsSummary indica anche le caratteristiche dell'applicazione client che accede al server nell'ambito della sessione.

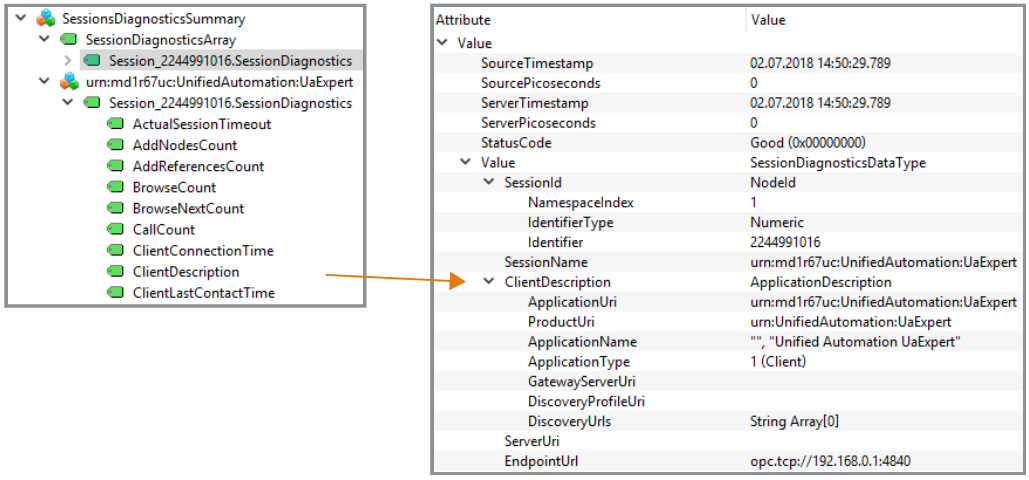


Figura 11-58 Sessions Diagnostics con le proprietà dell'applicazione client

Diagnostica del collegamento tra client e server

Per la diagnostica dello stato del collegamento durante il runtime del programma sul client, usare la seguente istruzione:

OPC_UA_ConnectionGetStatus: Leggi stato del collegamento.

11.3.7.2 Diagnostica del server OPC UA nel programma

A partire da STEP 7 (TIA Portal) V18, è possibile accedere ai nodi dell'area indirizzi OPC UA di una CPU S7-1500 (dalla versione firmware V3.0) per analizzare il contenuto nel programma a scopi di diagnostica.

Modalità di funzionamento

Nell'area di indirizzi locale della CPU sono presenti numerosi nodi nei quali il server OPC UA della CPU memorizza dati e stati. Utilizzando l'istruzione "OPC_UA_ReadList" è possibile accedere a queste informazioni e analizzarle nel programma utente.

Esempio: "ServerState" è un nodo nell'area indirizzi della CPU contenente i valori per lo stato del server o per le transizioni di stato (Running, Shutdown, Failed, ...).

L'istruzione non viene utilizzata come istruzione Client bensì come istruzione per la lettura di nodi nella propria area di indirizzi OPC UA locale. Per questo caso applicativo valgono pertanto regole e presupposti speciali.

Ulteriori informazioni

Ulteriori informazioni per il richiamo dell'istruzione "OPC_UA_ReadList" per scopi di diagnostica sono disponibili nella Guida a TIA Portal, alla sezione "Diagnostica del server OPC UA con OPC_UA_ReadList".

11.3.7.3 Diagnostica dei passaggi di stato del server

Informazioni sullo stato del server

Dalla versione firmware V2.8 le CPU S7-1500 sono in grado di generare una registrazione nel buffer di diagnostica in caso di modifiche dello stato del server OPC UA.

Il buffer di diagnostica visualizza il nuovo stato.

Inoltre viene visualizzata la causa della modifica di stato, ad es. caricamento nella CPU, passaggio OFF di rete - ON di rete, istruzione del programma utente o richiesta di service da parte di un partner (client).

Presupposti

Nelle proprietà OPC UA della CPU è attivata l'opzione "Modifica dello stato del server OPC UA" (OPC UA > Server > Diagnostica).

NOTA

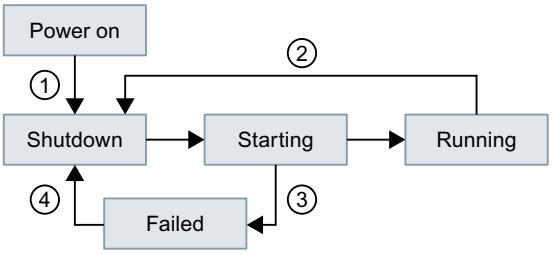
Se questa opzione è attivata, la CPU inserisce automaticamente la Security Policy più bassa impostata nel buffer di diagnostica dopo l'avvio.

Esempi

Se in seguito ad un caricamento il server OPC UA della CPU si arresta e successivamente si riavvia con una nuova configurazione valida, il buffer di diagnostica visualizza rispettivamente un nuovo stato del server, ad es. Shutdown => Starting => Running.

Se in seguito ad un caricamento il server OPC UA si arresta e non si può riavviare a causa di un Typedictionary troppo voluminoso, il buffer di diagnostica visualizza l'ultimo stato "Failed" (Shutdown => Starting => Failed).

Stati del server e passaggi di stato



①, ④ RETE ON o caricamento in RUN, se possono essere interessati dati rilevanti per OPC UA.

② Caricamento della configurazione hardware con server OPC UA disattivato Il server resta in shutdown.
Caricamento della configurazione hardware con server OPC UA attivato e dati OPC UA errati (ad es. strutture eccessive con conseguenza che il Typedictionary diventi troppo grande). In questo caso il server non può avviarsi (vedere ③).

③ Il server OPC UA non può avviarsi, ad es. a causa di dati errati.

Figura 11-59 Stati del server e passaggi di stato

Descrizione degli stati del server

Di seguito sono descritti i singoli stati che possono essere acquisiti dal server OPC UA.

Stati del server	Spiegazione
Shutdown	Stato iniziale • dopo RETE ON • dopo il caricamento della configurazione hardware con server OPC UA attivato o disattivato • dopo il caricamento di dati rilevanti per OPC UA
Starting	L'area di indirizzi OPC UA nel server viene inizializzata.
Running	Il server OPC UA è in funzione (stato produttivo normale del server OPC UA).
Failed	Stato di errore. Il server OPC UA non può avviarsi, ad es. a causa di dati errati.

11.3.7.4 Diagnostica dei passaggi di stato della sessione

Informazioni sullo stato del server

Dalla versione firmware V2.8 le CPU S7-1500 sono in grado di generare una registrazione nel buffer di diagnostica in caso di modifiche dello stato del server OPC UA.

Il buffer di diagnostica visualizza il nuovo stato. Viene visualizzato anche un Session ID corrispondente.

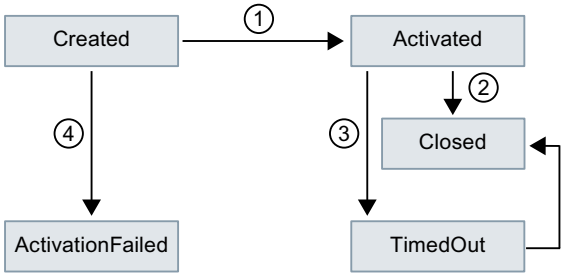
Presupposti

Nelle proprietà OPC UA della CPU è attivata l'opzione "Modifica dello stato della sessione OPC UA" (OPC UA > Server > Diagnostica).

Esempio

Un client trasferisce dati di autenticazione errati durante la creazione del collegamento (ad es. password errata). Nel buffer di diagnostica viene inserito il nuovo stato della sessione "ActivationFailed" con il Session ID corrispondente.

Stati della sessione e passaggi di stato



① Il client si collega al server, login con dati di autenticazione corretti (credenziali corrette).

② Il client chiude il collegamento correttamente.

③ Il client non invia più messaggi, la sessione viene chiusa con timeout.

④ Il client si collega al server, login con dati di autenticazione errati.

Figura 11-60 Stati della sessione e passaggi di stato

11.3.7.5 Controllo degli eventi Security

Se la CPU nell'ambito della comunicazione OPC UA diagnostica un evento Security, lo può inserire nel buffer di diagnostica.

Presupposti

- CPU S7-1500 a partire dalla versione FW 2.8
- L'opzione "Verifica eventi di sicurezza" è attivata (Proprietà della CPU > OPC UA > Server > Diagnostica)

Eventi Security diagnosticati

Le CPU S7-1500 diagnosticano i seguenti eventi Security di rilievo per OPC UA:

- Il certificato client non è valido (ad es. per sintassi o semantica errata, firma errata, la data attuale non è nel periodo di validità)
- La connessione con nome utente/password non è riuscita (è disattivata o contiene dati errati)
- Client vuole utilizzare una determinata Security Policy o un determinato Message Security Mode; il server non supporta la Security Policy o il Security Mode richiesto
- Il client non crea un collegamento conforme alla specifica (OPC UA Spec) (ad es. SecureChannelID/SessionID/Client Nonce inatteso)

Esempio

Eventuali tentativi di intercettare la comunicazione (ad es mediante session hijacking, attacchi man-in-the-middle ecc.) vengono individuati dal server sulla base di una verifica.

11.3.7.6 Richiesta di un client remoto non riuscita

Dalla versione firmware V2.8 le CPU S7-1500 sono in grado di generare una registrazione nel buffer di diagnostica in caso dei seguenti eventi.

- Richiesta client errata (errato utilizzo)
- si è verificato un errore server
- I limiti specifici per la CPU del server OPC UA sono stati superati

Esempio di richieste client errate

Una richiesta errata è presente ad es. se un client indirizza un nodo (variabile) inesistente o se viene richiesta una risorsa inesistente.

In questo caso viene inserito il servizio corrispondente che ha causato un errore e inoltre il Session ID corrispondente.

Errore di servizio

Se l'errore è da attribuirsi al servizio, il server segnale un errore dello stesso (ServiceFault). In questo caso la CPU inserisce il codice di stato (bad...) e l'ID della sessione corrispondente nel buffer di diagnostica.

Esempio di superamento dei limiti

Se una richiesta di servizio supera i limiti specifici della CPU, ad es. il numero di sessioni, il numero di elementi sorvegliati (Monitored Items), o il numero di subscription, il relativo messaggio viene inserito nel buffer di diagnostica. Oltre al messaggio, viene indicato anche quale limite sia stato superato.

Eccezione: Se i messaggi di diagnostica sono cumulativi e il messaggio viene generato ripetutamente, il limite causa dell'errore non viene inserito. Viene visualizzata un'avvertenza generale indicante che la quantità di risorse supportate è stata superata.

Inserimenti possibili per un servizio che causa l’errore

A seconda dell’applicazione client utilizzata le richieste al server possono essere attivate in modo diverso da parte dell’utente, ad es. mediante un tool online con interfaccia utente grafica o istruzioni nel programma di un client.

OPC UA con architettura basata sul servizio segue ad un paradigma Request-Response, di conseguenza la rispettiva applicazione client commuta le richieste in Service Request definite in OPC UA.

I nomi di questi servizi sono definiti e raggruppati in base al loro utilizzo, vedere anche opcfoundation.org.

In caso di utilizzo errato, nel buffer di diagnostica si trova esattamente questo nome dei servizi insieme al Session ID corrispondente come servizio che ha causato l’errore.

Di seguito sono elencati i servizi possibili con OPC UA.

Discovery Service Set

FindServers

GetEndpoints

Session Service Set

CreateSession

ActivateSession

CloseSession

Cancel

View Service Set

Browse

BrowseNext

TranslateBrowsePathsToNodeIds

RegisterNodes

UnregisterNodes

Attribute Service Set
Write
Read

Method Service Set
Call

Monitored Item Service Set
CreateMonitoredItems
ModifyMonitoredItems
DeleteMonitoredItems
SetMonitoringMode
SetTriggering

Subscription Service Set
CreateSubscription
ModifySubscription
DeleteSubscriptions
TransferSubscriptions
Publish
Republish
SetPublishingMode

11.3.7.7 Diagnostica di Subscription

Informazioni relative ad una Subscription

Dalla versione firmware V2.8 le CPU S7-1500 sono in grado di generare una registrazione nel buffer di diagnostica in caso di modifiche di una Subscription.

Il buffer di diagnostica visualizza il nuovo stato; eccezione: "KeepAlive".

Presupposti

Nelle proprietà OPC UA della CPU è attivata l'opzione "Subscription: Modifica dello stato" (OPC UA > Server > Diagnostica).

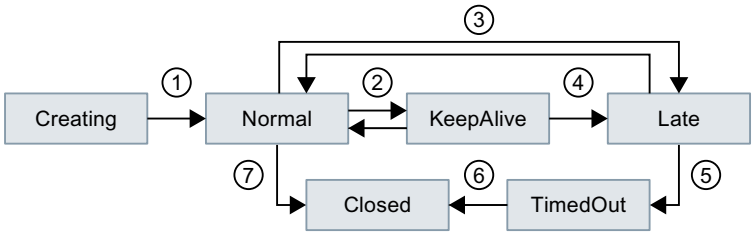
Esempio

Un client OPC UA è legato a una CPU S7-1500 come server OPC UA e genera una Subscription nel server.

Le opzioni di diagnostica per Subscription sono attivate nelle proprietà OPC UA della CPU.

Nel buffer di diagnostica vengono inseriti in successione gli stati "Creating" e "Normal" con il Subscription ID corrispondente.

Stati della Subscription e passaggi di stato



① Viene generata una Subscription che è successivamente attiva.

② Il passaggi di stato non viene inserito nel buffer di diagnostica poiché a seconda dei dati in ingresso si verificano troppe registrazioni nel buffer di diagnostica.

③ Vedere le spiegazioni nella tabella relative a "Late"; ad es. nessuna richiesta di invio da parte del client.

④ Valore massimo KeepAlive raggiunto.

⑤ Vedere le spiegazioni nella tabella relative a "TimedOut".

⑥ Lifetime massimo della Subscription raggiunto.

⑦ Il client ha cancellato la Subscription.

Figura 11-61 Stati della subscription e passaggi di stato

Descrizione degli stati della Subscription

Una Subscription nel server OPC UA può assumere i seguenti stati:

Stato	Significato
Creating	Il client ha richiesto una Subscription nel server; il server genera la Subscription.
Normal	La Subscription è creata e attiva nel server.
Closed	Il client ha cancellato la Subscription.
KeepAlive	Stato se per un tempo prolungato non si modificano gli elementi controllati (monitored items). Questi passaggi di stato non vengono registrati nel buffer di diagnostica.
Late	Il client ha generato una Subscription con intervalli di campionamento e di invio. La quantità di elemento controllati non viene trasmessa al client in questo periodo. Il client non trasmette più richieste di invio (ad es. a causa di un guasto).
TimedOut	Il client ha richiesto una Subscription. Il server può gestire l'abbonamento (Send Publish Response) solo se sono presenti sufficienti richieste di invio (Publish Requests) da parte del client. Se il client smette di inviare richieste di invio, dopo un certo periodo di tempo l'abbonamento entra nello stato "TimedOut" .

Subscription: Errore nei tempi di campionamento

Dal firmware V2.5 della CPU SIMATIC S7-1500 il server OPC UA può trasmettere il codice di stato "GoodOverload" in caso di utilizzo di Subscription, se con sampling degli Item si verifica un sovraccarico della CPU.

Dal firmware V2.8 della CPU SIMATIC S7-1500 il server OPC UA può inserire questo evento anche nel buffer di diagnostica.

Presupposti

Nelle proprietà OPC UA della CPU è attivata l'opzione "Subscription: Errore nei tempo di campionamento" (OPC UA > Server > Diagnostica).

Subscription corretta

In caso di una OPC UA su diversi elementi (Item, ad es. variabili) il server OPC UA di SIMATIC S7-1500 deve controllare la modifica dei valori degli elementi negli intervalli indicati (intervallo di campionamento). Questo controllo, il cosiddetto "Sampling", necessita di un certo tempo, in funzione del numero e del tipo di dati. Dopo la conclusione del Sampling e quando è presente un ordine di invio (Publishing Request), il server invia gli elementi al client.

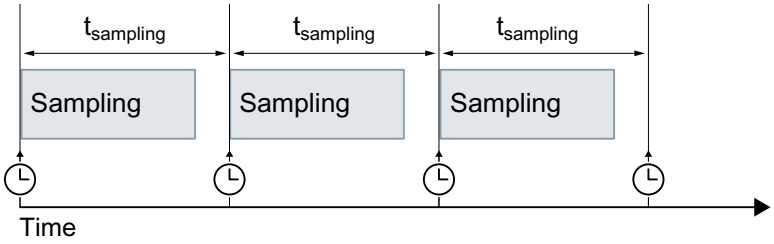
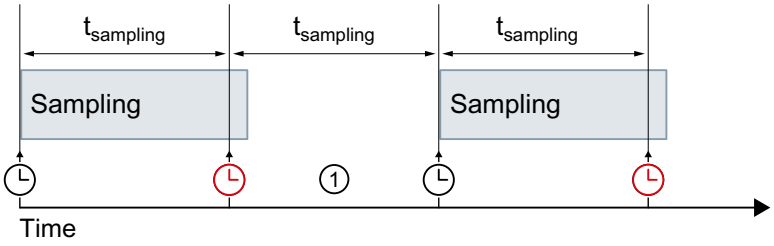


Figura 11-62 Subscription corretta

Subscription con errori

Se in coda (Queue) si trovato troppi elementi, può verificarsi un sovraccarico dello stack di comunicazione, un cosiddetto "Overload". La CPU non può quindi controllare tutti gli elementi nell'intervallo sampling indicato e deve perciò saltare il successivo ordine sampling.

In questo caso la CPU invia il codice di stato "GoodOverload" (0x002F0000) per ciascun elemento nonostante gli elementi non siano stati controllati. Il significato del codice di stato secondo IEC 61131-3 è: "Sampling has slowed down due to resource limitations".



① L'ordine sampling viene saltato

Figura 11-63 Subscription con errori

Vedere anche FAQ 109763090 (https://support.industry.siemens.com/cs/ww/it/view/109763090).

Ulteriori informazioni

Per informazioni sulle impostazioni server per le subscription consultare il capitolo Impostazioni del server per le sottoscrizioni (Pagina 263).

11.3.7.8 Diagnostica cumulativa

Per evitare che il buffer di diagnostica venga "sommerso" da molti messaggi di diagnostica OPC UA identici, a partire da STEP 7 V16 è possibile stabilire che questi messaggi vengano registrati nel buffer di diagnostica come segnalazione cumulativa. Per ogni intervallo (periodo di controllo) la CPU creerà soltanto una segnalazione cumulativa per ogni tipo di diagnostica UA OPC.

Le modalità con cui la CPU seleziona e raggruppa i messaggi di diagnostica e lo svolgimento del processo in presenza di un numero elevato di messaggi sono descritti nelle sezioni che seguono.

Presupposti

Nelle proprietà OPC UA della CPU è attivata l'opzione "Raggruppa diagnostiche in presenza di un elevato numero di messaggi" (OPC UA > Server > Diagnostica, alla voce "Raggruppa diagnostiche").

Esempio

Un client OPC UA "sovraccarica" una CPU S7-1500 come server OPC UA ripetutamente con una frequenza di campionamento che il server non è in grado di sostenere.

L'impostazione "Raggruppa diagnostiche in presenza di un elevato numero di messaggi" è attivata.

Nel buffer di diagnostica viene visualizzato il messaggio indicante che la frequenza di campionamento non è stata raggiunta seguito dal numero di questi eventi nell'intervallo progettato.

Messaggi di diagnostica OPC UA che possono far parte di messaggi cumulativi.

I messaggi di diagnostica elencati nel seguito formano gruppi propri (tipo). L'impostazione "Raggruppa diagnostiche in presenza di un elevato numero di messaggi" consente di raggruppare messaggi di diagnostica dello stesso gruppo:

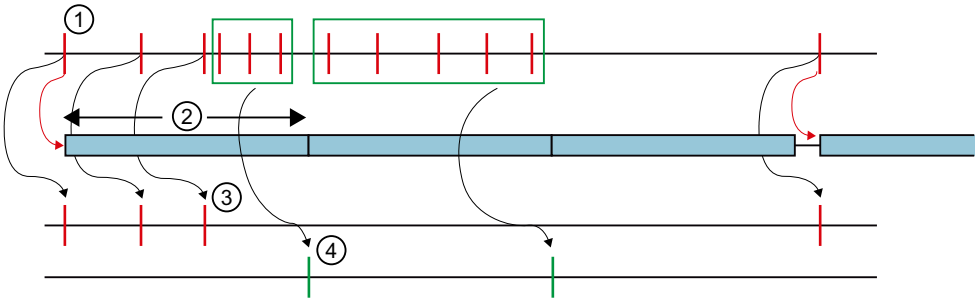
- Errato utilizzo di un servizio OPC UA
- Errore di servizio OPC UA
- Lo stato della subscription è cambiato
- Non è stato possibile raggiungere la frequenza di campionamento (subscription, sovraccarico)
- Controllo della sicurezza OPC UA non riuscito
- Superamento della quantità di risorse del server OPC UA

Modalità di funzionamento

La CPU registra immediatamente i primi tre messaggi di diagnostica di un gruppo nel buffer di diagnostica. e ignora tutti i messaggi di diagnostica successivi di questo gruppo.

Al termine del periodo di controllo (intervallo) la CPU crea una segnalazione cumulativa nella quale registra il messaggio di diagnostica e la relativa frequenza durante l'intervallo trascorso. Se questi messaggi di diagnostica vengono generati anche negli intervalli seguenti, la CPU genera solo una segnalazione cumulativa per ogni intervallo successivo.

Un sovraccarico di messaggi nel buffer di diagnostica lascia il seguente modello: tre segnalazioni singole seguite da una serie di segnalazioni cumulative. Questa serie può essere composta da due, tre o più segnalazioni cumulative a seconda del tempo di controllo selezionato e della durata del sovraccarico di messaggi.



① Messaggi di diagnostica di un gruppo (di un tipo), ad esempio "Non è stato possibile raggiungere la frequenza di campionamento"

② Intervallo (periodo di controllo): Se si verifica per la prima volta un evento di diagnostica (o si ripete), viene avviato (o riavviato) il tempo di controllo.

③ Segnalazioni singole: I primi tre messaggi di diagnostica di un gruppo vengono registrati immediatamente nel buffer di diagnostica. Dal quarto messaggio di diagnostica, la CPU genera soltanto segnalazioni cumulative. Se dopo una pausa di almeno un intervallo viene emesso nuovamente un messaggio di diagnostica di questo gruppo, la CPU registra nel buffer di diagnostica una segnalazione singola e riavvia il periodo di controllo.

④ Segnalazioni cumulative: Dopo tre messaggi di diagnostica la CPU genera ancora soltanto una segnalazione cumulativa che raggruppa tutti gli altri messaggi generati in quest'intervallo. Se questi messaggi di diagnostica vengono generati anche negli intervalli seguenti, la CPU genera soltanto una segnalazione cumulativa per ogni intervallo successivo.

Figura 11-64 Sintesi della diagnostica

11.4 Utilizzo della CPU S7-1500 come client OPC UA

11.4.1 Panoramica e presupposti

Con STEP 7 (TIA Portal) a partire dalla versione V15.1 sono possibili la progettazione e la programmazione di un client OPC UA in grado di leggere le variabili PLC in un server OPC UA. Inoltre è possibile trasferire a un server OPC UA nuovi valori per le variabili PLC. Nel programma utente si possono inoltre richiamare metodi messi a disposizione da un server OPC UA. Per farlo, utilizzare nel programma utente le nuove istruzioni per i client OPC UA.

Le istruzioni del client OPC UA si rifanno allo standard "PLCopen OPC-UA Client for IEC61131-3".

Specifica PLCopen

Queste istruzioni standardizzate consentono di utilizzare nel programma utente funzioni client OPC UA eseguibili in una CPU S7-1500.

Inoltre, con adattamenti minimi, è possibile eseguire questo programma utente anche in controllori di altri produttori, se anche questi ultimi utilizzano la specifica OPC UA "PLCopen OPC-UA Client for IEC61131-3".

Pratici editor in STEP 7

Per la parametrizzazione delle istruzioni per i client OPC UA è disponibile nel TIA Portal un pratico editor, la parametrizzazione del collegamento (Pagina 257).

STEP 7 dalla versione 15.1 dispone inoltre di un editor per le interfacce client (Pagina 371).

Questo capitolo descrive le modalità di utilizzo di questi editor.

Innanzitutto viene illustrato come creare e configurare una nuova interfaccia con l'editor per le interfacce poiché questa interfaccia sarà necessaria per la successiva parametrizzazione del collegamento.

Per facilitare la comprensione, la spiegazione ricorre a un esempio, vedere Descrizione dell'esempio (Pagina 369).

Presupposti

- Si dispone della licenza di runtime necessaria per l'OPC UA ed è stata progettata la licenza in STEP 7 (proprietà della CPU > Licenze di runtime).
- Il client della CPU S7-1500 è attivato.

Per poter utilizzare il client della CPU S7-1500 è necessario abilitarlo:

1. Selezionare nelle proprietà della CPU il campo "OPC UA > Client".
2. Attivare l'opzione "Attiva client OPC UA".

Se non si attiva il client non ha luogo nessuna creazione del collegamento. Viene visualizzato un messaggio di errore nelle istruzioni. come ad es. "OPC_UA_Connect".

Informazioni sul nome dell'applicazione, anche per il server e il client, sono riportate qui (Pagina 257).

Panoramica

Per utilizzare l'editor e la parametrizzazione del collegamento, procedere nel modo seguente:

1. Creare innanzitutto un'interfaccia client e inserirvi le variabili e i metodi PLC da utilizzare ("Primo passo (Pagina 371)").
2. Parametrizzare quindi il collegamento al server OPC UA (Secondo passo (Pagina 387)).
3. Infine utilizzare il collegamento parametrizzato nelle istruzioni client OPC UA (Terzo passo (Pagina 394)).

11.4.2 Informazioni importanti sulle istruzioni per i client

Con le istruzioni client OPC UA la CPU S7-1500 come client OPC UA consente di comandare la comunicazione per l'esecuzione dei seguenti compiti:

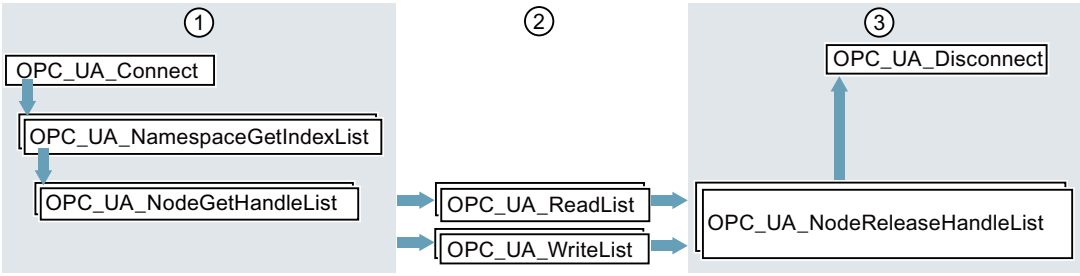
- Lettura/scrittura di variabili del server OPC UA
- Richiamo di metodi nel server OPC UA

Le istruzioni opzionali consentono di rilevare le seguenti informazioni:

- Lo stato del collegamento tra client OPC UA e server OPC UA
- NodeId di nodi con una gerarchia nota nell'area di indirizzi

Esecuzione standardizzata della comunicazione OPC UA

L'esecuzione della comunicazione e quindi la sequenza delle istruzioni si basa su un modello che è illustrato di seguito.

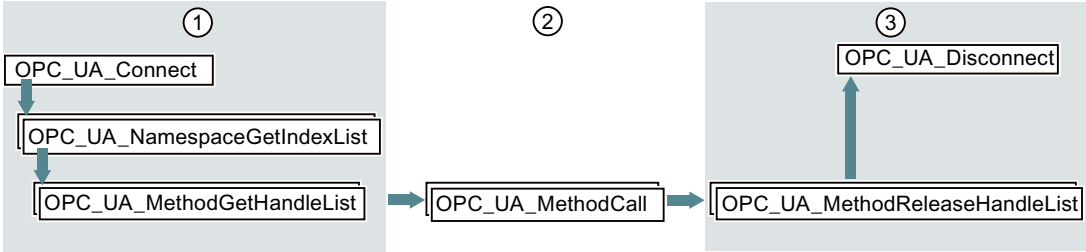


① Istruzioni per le operazioni preliminari di scrittura e lettura

② Istruzioni di lettura e scrittura

③ Istruzioni per il "clean up" al termine delle operazioni di lettura o scrittura

Figura 11-65 Sequenza di esecuzione per la lettura o la scrittura



① Istruzioni per le operazioni preliminari di richiamo del metodo

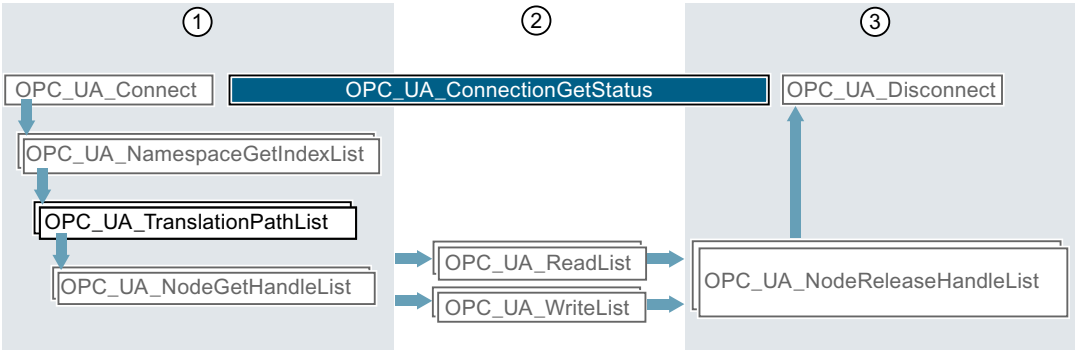
② Richiami dei metodi

③ Istruzioni per il "clean up" al termine dei richiami dei metodi

Figura 11-66 Sequenza di esecuzione per il richiamo del metodo nel server OPC UA

Istruzioni opzionali (lettura dello stato di un collegamento / lettura di NodeId di nodi con una gerarchia nota dell'area di indirizzi)

- OPC_UA_ConnectionGetStatus
- OPC_UA_TranslatePathList



① Istruzioni per le operazioni preliminari di lettura e scrittura con istruzione inserita per richiedere ad es. i NodeId dei nodi del server OPC UA.

② Analogamente ad altre istruzioni è possibile rilevare lo stato del collegamento tra la creazione e l'interruzione dello stesso

③ Istruzioni per il "clean up"

Figura 11-67 Sequenza di esecuzione delle istruzioni opzionali

Pratici editor in STEP 7

Le istruzioni per il client OPC UA sono descritte dettagliatamente nella sezione di riferimento (sistema di informazione STEP 7). Per la parametrizzazione delle istruzioni è disponibile nel TIA Portal un pratico editor, la parametrizzazione del collegamento (Pagina 387).

Per la prima bozza di programma si consiglia di iniziare con la parametrizzazione del collegamento e all'occorrenza di utilizzare altre istruzioni e di ottimizzare manualmente il programma.

Informazioni sulle istruzioni per i client

Le istruzioni per i client sono descritte in dettaglio nell'argomento della Guida alle istruzioni > Comunicazione > OPC UA > Client OPC UA.

Esempio applicativo nell'Online Support

In questo esempio applicativo (https://support.industry.siemens.com/cs/ww/it/view/109762770) è disponibile un blocco utente S7 "OpcUaClient" che raggruppa le principali funzioni delle istruzioni OPC UA, velocizza l'implementazione per l'utente e semplifica la programmazione. Nell'esempio un controllore S7-1500 funge da server OPC UA con un semplice programma di simulazione per i valori di processo.

Il blocco utente S7 svolge le seguenti funzioni:

- creazione e interruzione del collegamento con il server
- diagnostica del collegamento e ricollegamento automatico in caso disconnessione
- Registered Read
- Registered Write
- Registered Method Call

11.4.3 Numero di istruzioni per i client utilizzabili contemporaneamente

Istruzioni per i client utilizzabili contemporaneamente

Riguardo all'uso simultaneo delle istruzioni per i client OPC UA sono previsti i seguenti limiti (i dati tecnici aggiornati delle CPU sono consultabili in Internet (https://support.industry.siemens.com/cs/ww/it/ps/td)):

Tabella 11-4 Quantità massime di istruzioni per i client OPC UA

Istruzione OPC UA	Numero max. per CPU 1510SP (F) CPU 1511 (C/F/T/TF) CPU 1512C CPU 1512SP (F) CPU 1513 (F)	Numero max. per CPU 1505 (S/SP/SP F/SP T/SP TF) CPU 1515 (F/T/TF) CPU 1515 SP PC (F/T/TF) CPU 1516 (F/T/TF)	Numero max. per CPU 1507S (F) CPU 1517 (F/T/TF) CPU 1518 (F)
OPC_UA_Connect	4	10	40
OPC_UA_NamespaceGetIndexList	4*	10*	40*
OPC_UA_NodeGetHandleList	4*	10*	40*
OPC_UA_MethodGetHandleList	4*	10*	40*
OPC_UA_TranslatePathList	4*	10*	40*
OPC_UA_ReadList	20 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)	50 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)	200 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)

* max. 1 per collegamento porta

Istruzione OPC UA	Numero max. per CPU 1510SP (F) CPU 1511 (C/F/T/TF) CPU 1512C CPU 1512SP (F) CPU 1513 (F)	Numero max. per CPU 1505 (S/SP/SP F/SP T/SP TF) CPU 1515 (F/T/TF) CPU 1515 SP PC (F/T/TF) CPU 1516 (F/T/TF)	Numero max. per CPU 1507S (F) CPU 1517 (F/T/TF) CPU 1518 (F)
OPC_UA_WriteList	20 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)	50 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)	200 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)
OPC_UA_MethodCall	20 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)	50 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)	200 in totale (max. 5 per collegamento, vedere OPC_UA_Connect)
OPC_UA_NodeReleaseHandleList	4*	10*	40*
OPC_UA_MethodReleaseHandleList	4*	10*	40*
OPC_UA_Disconnect	4*	10*	40*
OPC_UA_ConnectionGetStatus	4*	10*	40*

* max. 1 per collegamento porta

Numero massimo di interfacce client OPC UA utilizzabili

Se si creano interfacce client OPC UA nella parametrizzazione del collegamento, il numero massimo di interfacce client è di 40.

Per creare le interfacce client OPC UA fare due volte clic sul simbolo "Aggiungi nuova interfaccia client" nell'area "Comunicazione OPC UA" della navigazione del progetto.

Se si utilizza la CPU anche come server OPC UA il numero massimo di interfacce client OPC UA non cambia.

11.4.4 Configurazione di esempio per OPC UA

I seguenti capitoli spiegano come utilizzare l'editor per le interfacce client e la parametrizzazione del collegamento.

La descrizione si basa su un esempio concreto: Nell'impianto sono in funzione due CPU S7-1500: Una CPU funziona come client OPC UA e l'altra come server OPC UA.

Naturalmente si possono utilizzare come client o server OPC UA anche controllori, sensori o sistemi IT di altri produttori. Proprio la comunicazione tra diversi sistemi (interoperabilità) rappresenta un grande vantaggio di OPC UA.

Parametrizzazione del collegamento sulla base di un esempio:

L'impianto produce pezzi grezzi in una linea di produzione.

Vengono impiegati i seguenti controllori:

1. Come controllore della linea di produzione viene utilizzata una CPU S7-1511.

   Nell'esempio il controllore è denominato "**Productionline**".

   Il server OPC UA del controllore è attivato.

   Nell'esempio la CPU ha l'indirizzo IP 192.168.1.1.

   Tramite il server OPC UA questa CPU pubblica i valori delle seguenti variabili:

   – **NewProduct**

     Questa variabile ha il tipo di dati "Bool".

     Se la variabile ha il valore TRUE, la linea di produzione ha lavorato un pezzo grezzo.

     Il pezzo grezzo è pronto per essere ritirato.

   – **ProductNumber**

     Questa variabile contiene il numero di identificazione del pezzo grezzo.

     Questa variabile ha il tipo di dati "Int".

   – **Temperatura**

     Questa variabile contiene i valori di temperatura rilevati durante la produzione del pezzo grezzo.

     È un array con elementi di tipo di dati "Real".

   Inoltre questa CPU mette a disposizione la seguente variabile da scrivere:

   – **ProductionEnabled**

     La variabile viene impostata dal client OPC UA.

     Questa variabile ha il tipo di dati "Bool".

     Se il valore è impostato su TRUE, la linea di produzione è abilitata e può produrre pezzi grezzi.

   Inoltre questa CPU mette a disposizione il seguente metodo attraverso il server OPC UA:

   – **OpenDoor**

     Con questo metodo i client OPC UA possono fare in modo che si apra una porta d'accesso alla linea di produzione.

2. Una CPU S7-1516 controlla l'interazione con altre linee di produzione.

   Nell'esempio questa CPU è denominata "**Supervisor**".

   Il client OPC UA di questa CPU è attivato.

   Attraverso OPC UA la CPU può leggere le variabili NewProduct e ProductNumber, impostare la variabile ProductionEnabled e richiamare il metodo OpenDoor.

   Nell'esempio la CPU ha l'indirizzo IP 192.168.1.2.

La seguente figura mostra l'esempio nella vista di rete del TIA Portal:

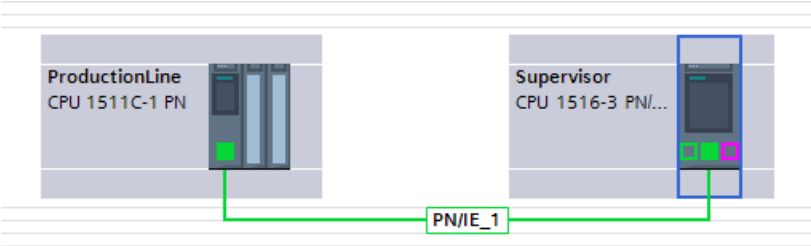


Figura 11-68 Esempio della parametrizzazione del collegamento nella vista di rete

11.4.5 Creazione delle interfacce client

Dalla versione V15.1 TIA Portal dispone di un editor per le interfacce client.

In un'interfaccia client vengono raggruppate tutte le variabili PLC che si intendono leggere o scrivere da/in un server OPC UA.

L'interfaccia client contiene inoltre tutti i metodi che il server OPC UA mette a disposizione e che vengono richiamati dal programma utente, che funziona come client OPC UA.

Quando si crea un'interfaccia client, STEP 7 crea anche i blocchi dati per la parametrizzazione del collegamento al server OPC UA dal quale/nel quale si intendono leggere/scrivere i dati.

Numero max. di interfacce client

Si possono creare al massimo 40 interfacce client.

Editor per le interfacce client

Per creare un'interfaccia client, procedere nel modo seguente:

1. Selezionare la vista del progetto in TIA Portal.
2. Nell'area "Dispositivi" selezionare la CPU da utilizzare come client OPC UA.
3. Fare clic su "Comunicazione OPC UA > Interfacce client".
4. Fare doppio clic su "Aggiungi nuova interfaccia client".

   STEP 7 genera una nuova interfaccia client e la visualizza nell'editor:

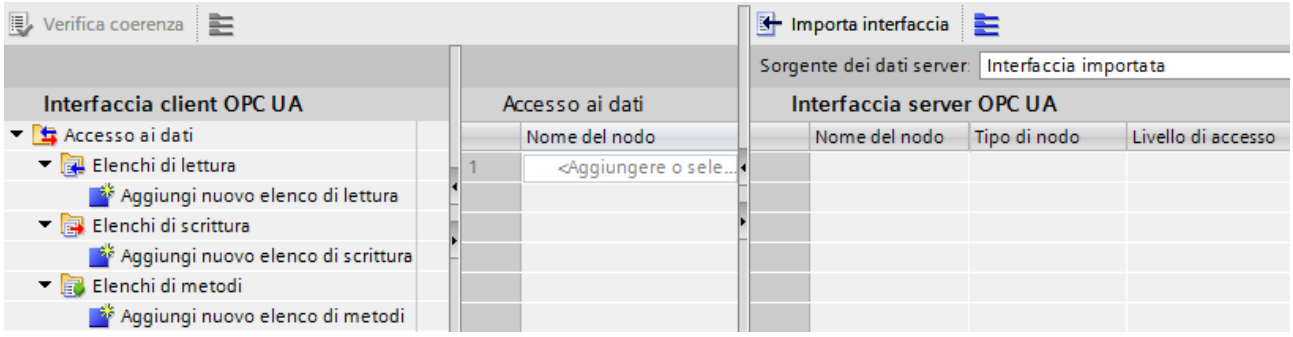


Figura 11-69 Aggiunta di una nuova interfaccia del client OPC UA

STEP 7 attribuisce alla nuova interfaccia il nome "Interfaccia client_1". Se esiste già un'interfaccia "Interfaccia client_1" modifica il nome in "Interfaccia client_2" ecc.

Inoltre STEP 7 genera i seguenti blocchi dati:

– Interfaccia client_1_Configuration

  Il blocco dati contiene già tutti i tipi di dati di sistema necessari per le istruzioni del client OPC UA.

  Viene compilato quando si parametrizza il collegamento con il server OPC UA.

  Il collegamento si parametrizza nelle proprietà dell'interfaccia client, vedere: Configurazione di esempio per OPC UA (Pagina 369).

– Interfaccia client_1_Data

  Un blocco dati per le variabili PLC da leggere o scrivere dal server OPC UA, nonché per i metodi che si intende richiamare nel server OPC UA.

  Questo blocco dati viene utilizzato nel programma utente.

  Al momento questo blocco dati è ancora vuoto.

5. Utilizzare un nome significativo per la nuova interfaccia client.

   Nell’esempio selezionare "Productionline".

   Così facendo viene modificato anche il nome dei rispettivi blocchi dati:

   – Productionline_Data

   – Productionline_Configuration

6. Per importare un'interfaccia server OPC UA fare clic sul pulsante “Importa interfaccia” in alto a destra nell’editor.

   Questo comando consente di importare un file XML che contiene la descrizione di un'interfaccia server OPC UA.

   Alternativa: rilevare l'interfaccia server online di un server OPC UA collegato, vedere: Rilevamento online dell'interfaccia server (Pagina 379).

7. STEP 7 visualizza una finestra di dialogo che consente di selezionare un file XML.

   Il file XML descrive l’area di indirizzi di un server OPC UA.

   L’area di indirizzi di un server OPC UA contiene tutte le variabili PLC e i metodi server che vengono pubblicati da un server OPC UA.

   A questa area di indirizzi possono accedere client OPC UA:

   - leggere le variabili PLC

   - scrivere nelle variabili PLC

   - richiamare i metodi server

   L’area di indirizzi di un server OPC UA può essere suddivisa in una o più interfacce server.

   Per creare interfacce serve vedere: Creazione dell’interfaccia server per la specifica Companion (Pagina 291).

8. Creare un **elenco di lettura** in questa interfaccia client.

   Per eseguire questa operazione procedere nel seguente modo:

   – Fare clic nella sezione sinistra dell'editor su "Aggiungi nuovo elenco di lettura".

     STEP 7 aggiunge un nuovo elenco con il nome "Elenco di lettura_1".

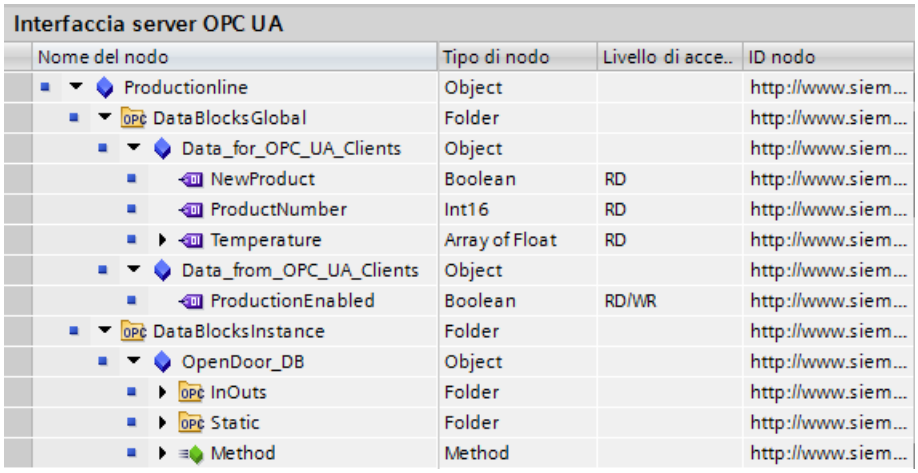
     Per questo esempio modificare il nome in "ReadListProduct"

   – Aggiungere al nuovo elenco di lettura le variabili PLC dell'interfaccia server che vogliono leggere dal server OPC UA.

     Nell'esempio vengono aggiunte all'elenco "ReadListProduct" le variabili "NewProduct" e "ProductNumber".

     Selezionare la variabile "NewProduct" nell'area destra dell'editor ("Interfaccia server OPC UA"). Trascinare la variabile "NewProduct" nell'elenco di lettura "ReadProduct", nel campo al centro dell'editor. Procedere allo stesso modo per la variabile "ProductNumber".

   La seguente figura rappresenta l'area destra dell'editor.



Interfaccia server OPC UA

Nome del nodo	Tipo di nodo	Livello di acce..	ID nodo
Productionline	Object		http://www.siem...
DataBlocksGlobal	Folder		http://www.siem...
Data_for_OPC_UA_Clients	Object		http://www.siem...
NewProduct	Boolean	RD	http://www.siem...
ProductNumber	Int16	RD	http://www.siem...
Temperature	Array of Float	RD	http://www.siem...
Data_from_OPC_UA_Clients	Object		http://www.siem...
ProductionEnabled	Boolean	RD/WR	http://www.siem...
DataBlocksInstance	Folder		http://www.siem...
OpenDoor_DB	Object		http://www.siem...
InOuts	Folder		http://www.siem...
Static	Folder		http://www.siem...
Method	Method		http://www.siem...

Figura 11-70 Elenco di lettura nell'interfaccia del server OPC UA

Alternativa:

Si può creare un nuovo elenco di lettura anche selezionando un nodo di tipo Object o Folder nell'area destra dell'editor ("Interfaccia server OPC UA") e trascinandolo in "Aggiungi nuovo elenco di lettura" nell'area sinistra. Il nuovo elenco di lettura conterrà le variabili PLC del nodo inserito.

Nell'esempio selezionare l'oggetto "Data_for_OPC_UA_Clients" che contiene le variabili "NewProduct" e "ProductNumber". STEP 7 crea il nuovo elenco di lettura "Data_for_OPC_UA_Clients". Viene inoltre aggiunta all'oggetto anche la variabile "Temperature". Eliminare la variabile "Temperature" dall'elenco di lettura, poiché non deve essere letta nell'esempio.

Modificare il nome dell'elenco di lettura in "ReadListProduct".

La seguente figura rappresenta il contenuto dell'elenco di lettura:

ReadListProduct

Nome del nodo	Tipo di nodo	Livello di accesso	ID nodo
NewProduct	BOOL	RD	http://www.siemen...
ProductNumber	INT	RD	http://www.siemen...

Figura 11-71 Elenco di lettura

NOTA

Gli elenchi di lettura e scrittura non supportano tutti i tipi di nodi

Il client OPC UA della CPU S7-1500 CPU non supporta tutti i tipi di dati OPC UA (tipi di nodo) che possono essere messi a disposizione tramite un'interfaccia server OPC UA. Se ad es. in un elenco di lettura o di scrittura si posiziona un tipo di nodo non supportato, compare una segnalazione di errore corrispondente. In questo caso non è possibile acquisire i nodi corrispondenti nell'elenco di lettura o di scrittura.

Qui vengono descritti i tipi supportati: Mappatura dei tipi di dati (Pagina 236)

9. Se si desidera assegnare nuovi valori alle variabili PLC creare un **elenco di scrittura** in questa interfaccia client.

   Per eseguire questa operazione procedere nel seguente modo:

   – Fare clic su "Aggiungi nuovo elenco di scrittura" nell'area sinistra dell'editor.

     STEP 7 aggiunge un nuovo elenco con il nome "Elenco di scrittura_1".

     Per questo esempio modificare il nome in "WriteListStatus".

   – Aggiungere al nuovo elenco di scrittura tutte le variabili del server OPC UA a cui si vogliono assegnare nuovi valori.

     Nell'esempio inserire nell'elenco "WriteListStatus" la variabile "ProductionEnabled".

     Selezionare la variabile nell'area destra dell'editor ("Interfaccia server OPC UA"). Trascinare la variabile nell'elenco di scrittura, nel campo al centro dell'editor.

   Alternativa:

   Si può creare un nuovo elenco di scrittura anche selezionando un nodo di tipo Object o Folder nell'area destra dell'editor ("Interfaccia server OPC UA") e trascinandolo in "Aggiungi nuovo elenco di lettura" nell'area sinistra.

   Il nuovo elenco di scrittura conterrà le variabili del nodo inserito.

   Nell'esempio selezionare l'oggetto "Data_from_OPC_UA_Clients" che contiene la variabile "ProductionEnabled". STEP 7 crea il nuovo elenco di scrittura "Data_from_OPC_UA_Clients". Modificare il nome in "WriteListStatus".

   La seguente figura rappresenta il contenuto dell'elenco di scrittura:

WriteListStatus

Nome del nodo	Tipo di nodo	Livello di accesso	ID nodo
ProductionEnabled	BOOL	RD/WR	http://www.siemen...

Figura 11-72 Elenco di scrittura

10. Se si desidera richiamare un metodo di questo server OPC UA creare un nuovo elenco di metodi.

    Per eseguire questa operazione procedere nel seguente modo:

    – Fare clic su “Aggiungi nuovo elenco di metodi” nell'area sinistra dell’editor.

      STEP 7 aggiunge un nuovo elenco con il nome “Elenco di metodi_1”.

      Per questo esempio modificare il nome in "MethodListOpenDoor".

    – Aggiungere al nuovo elenco di metodi tutte le variabili del server OPC UA.

      In questo esempio viene aggiunto il metodo "OpenDoor" all'elenco "MethodListOpenDoor" .

      Selezionare il metodo nell'area destra dell'editor ("Interfaccia server OPC UA"). Trascinare il metodo nell'elenco dei metodi, nel campo al centro dell'editor.

    Alternativa:

    Si può creare un nuovo elenco di metodi anche selezionando un metodo (nodo di tipo Object) o nell'area destra dell'editor ("Interfaccia server OPC UA") e trascinandolo in "Aggiungi nuovo elenco di metodi" nell'area sinistra. Il nuovo elenco di metodi conterrà il metodo del nodo inserito.

    La seguente figura rappresenta il contenuto dell'elenco di metodi:

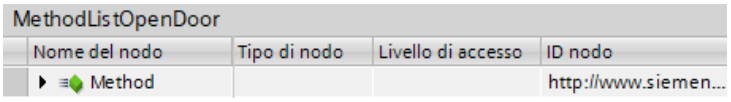


Figura 11-73 Elenco di metodi

    Vedere anche: Informazioni utili sui metodi server (Pagina 321).

11. Compilare il progetto.

    Per farlo, selezionare il progetto e fare clic nella barra degli strumenti sull’icona seguente:

STEP 7 compila il progetto e aggiorna i blocchi dati appartenenti all’interfaccia client "ProductionLine".

NOTA

STEP 7 sovrascrive in fase di traduzione tutti i dati nei blocchi di dati che appartengono all’interfaccia client. Per tale motivo non si devono inserire estensioni o correggere manualmente tali blocchi dati.

NOTA

Modifica del nome dei nodi (DisplayNames)

Negli elenchi di lettura, di scrittura e dei metodi è possibile modificare i nomi dei nodi dal menu di scelta rapida. Nel linguaggio di OPC UA si parla di "DisplayName".

Se si modifica il nome del nodo di un elenco di metodi e il nodo è già utilizzato in un blocco programmato per il richiamo "OPC_UA_MethodCall", quando si compila il progetto si verificano errori di coerenza: Durante la compilazione gli UDT del metodo vengono ricreati con il nome modificato. Di conseguenza i riferimenti al metodo utilizzati nel programma non corrispondono più.

Gli errori possono essere eliminati annullando la modifica del nome del metodo nell'interfaccia client oppure spostandosi sul richiamo del metodo e riassegnando i parametri in "Proprietà > Parametri del blocco" (scheda "Configurazione").

Blocchi dati dell’interfaccia client

I seguenti blocchi dati appartengono all’interfaccia client “Productionline”:

- **Productionline_Configuration**

  Un blocco dati per la configurazione.

  Nell’esempio questo blocco dati si chiama "Productionline_Configuration".

  Il blocco dati contiene già tutti i tipi di dati di sistema necessari per le istruzioni del client OPC UA.

  Contiene inoltre valori predefiniti generali per la parametrizzazione del collegamento a un server OPC UA.

  Quando si esegue la parametrizzazione del collegamento, questo blocco dati viene compilato.

- **Produktionline_Data**

  Un blocco dati per le variabili PLC che è stato inserito nell'editor per le interfacce client.

  Nell'esempio questo blocco dati si chiama "Productionline_Data".

  La seguente figura rappresenta il blocco dati.

Static	
ReadListProduct	Struct
Variable	"Productionline.ReadListProduct"
NewProduct	Bool
ProductNumber	Int
NodeStatusList	Array[0..1] of DWord
NodeStatusList[0]	DWord
NodeStatusList[1]	DWord
TimeStamps	Array[0..1] of LDT
TimeStamps[0]	LDT
TimeStamps[1]	LDT
WriteListStatus	Struct
Variable	"Productionline.WriteListStatus"
ProductionEnabled	Bool
NodeStatusList	Array[0..0] of DWord
NodeStatusList[0]	DWord
MethodListOpenDoor	Struct
MethodStatusList	Array[0..0] of DWord
MethodStatusList[0]	DWord
MethodResultList	Array[0..0] of DWord
MethodResultList[0]	DWord
Method	Struct
Inputs	"Productionline.MethodListOpendoor.Method.Inputs"
Number	Int
Outputs	"Productionline.MethodListOpendoor.Method.Outputs"
Result	Int

Figura 11-74 Blocco dati "Productionline_Data"

Il blocco dati "Productionline_Data" viene utilizzato nel programma utente per accedere ai valori letti delle variabili PLC "NewProduct" e "ProductNumber". Nel paragrafo seguente questa procedura è illustrata sulla base di un esempio.

Lettura e scrittura di variabili PLC dell'interfaccia client

Esempio: Lettura del valore "ProductNumber"

In un programma SCL scrivere ad esempio:

```
#MyLocalVariable :=
"Productionline_Data".ReadListProduct.Variable.ProductNumber;
```

In questo modo si assegna ad es. alla variabile locale "#MyLocalVariable" il numero del pezzo grezzo che è appena stato prodotto nella linea di produzione.

Presupposti:

- È attivo un collegamento al server OPC UA della CPU che controlla la linea di produzione.
- Il client OPC UA ha letto i valori attuali

Verificare quindi se un valore letto è valido (valide):

- Verificare se il valore in "Productionline_Data".ReadListProduct.NodeStatusList[1] è uguale a 0
- Opzione: Verificare quando questo valore è stato letto dal server OPC UA. Il valore si trova in "Productionline_Data".ReadProduct.TimeStamps[1]. Se non sono necessarie la data e l'ora, il carico di comunicazione si riduce.

Esempio: Scrittura del valore “ProductEnabled”

Con il blocco dati si trasferiscono al server OPC UA nuovi valori per le variabili PLC, nell’esempio per la variabile "ProductionEnabled".

L’assegnazione seguente abilita la linea di produzione nell’impianto di esempio:

```
"Productionline_Data".WriteListStatus.Variable.ProductionEnabled :=
TRUE;
```

L’abilitazione è possibile solo se sono soddisfatti i seguenti presupposti:

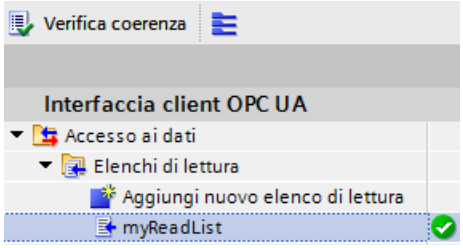
- È attivo un collegamento al server OPC UA della CPU che controlla la linea di produzione.
- Il client OPC UA scrive i valori attuali.

Verifica coerenza

Infine verificare la coerenza dell'elenco di lettura, di scrittura e dei metodi.

1. Selezionare l'elenco da verificare.
2. Fare clic sul pulsante "Verifica coerenza" sopra l'area "Interfaccia client OPC UA".

Se le variabili o i metodi sono assegnati correttamente agli elementi corrispondenti dell'interfaccia server, compare un segno di spunta verde.



Si può essere certi che lo scambio di dati tra il client e il server e i richiami dei metodi funzionino correttamente.

In caso di errore la finestra di ispezione visualizza un elenco che consente di passare al punto in cui si è verificato ciascun errore.

Durante la verifica della coerenza STEP 7 controlla:

- se tutti gli elementi utilizzati in un elenco sono presenti anche nel server,
- se i tipi di dati utilizzati corrispondono.
- Nel caso dei metodi: STEP 7 verifica se il numero, il nome, l'ordine e i tipi di dati degli argomenti corrispondono.

11.4.6 Rilevamento online dell'interfaccia server

STEP 7 (TIA Portal) consente di rilevare online l'interfaccia di un server OPC UA. In questo modo si capisce quali variabili di un server OPC UA collegato possono essere lette o impostate (scritte) con i client OPC UA e quali metodi il server OPC UA mette a disposizione dei client OPC UA.

Se si lavora offline si può creare l'interfaccia del server OPC UA con un file XML OPC UA. Il file descrive l'area degli indirizzi del server, vedere: Esporta file XML OPC UA (Pagina 255).

Rilevamento online delle interfacce server

Per rilevare online un'interfaccia server procedere nel seguente modo:

1. Nella navigazione del progetto di STEP 7 selezionare la CPU progettata come client OPC UA viene utilizzato (nell'esempio Supervisor).
2. Selezionare l'interfaccia client (nell'esempio Comunicazione OPC UA > Interfacce client > Productionline).

   Se non è ancora stata creata un'interfaccia client fare doppio clic su "Aggiungi nuova interfaccia client".
3. Fare doppio clic sull'interfaccia client selezionata.

   Compare l'editor per le interfacce client:

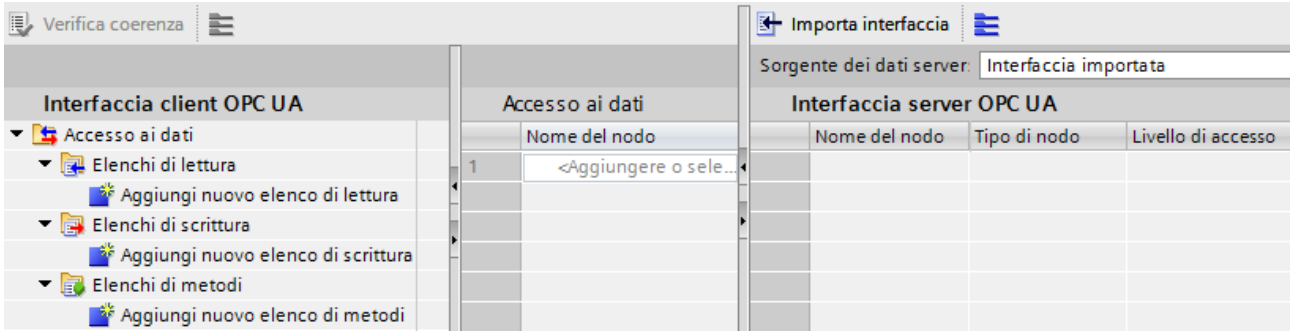


Figura 11-75 Editor per l'interfaccia client

4. Fare clic su "Aggiungi nuovo elenco di lettura", "Aggiungi nuovo elenco di scrittura" o "Aggiungi nuovo elenco di metodi" nell'area sinistra dell'editor.
5. Selezionare la sorgente di dati "Online[]" in "Sorgente dei dati server" nell'area destra dell'editor:

6. Fare clic sul pulsante "Accessi online".

   STEP 7 visualizza la finestra di dialogo "Collegamento con il server OPC UA":

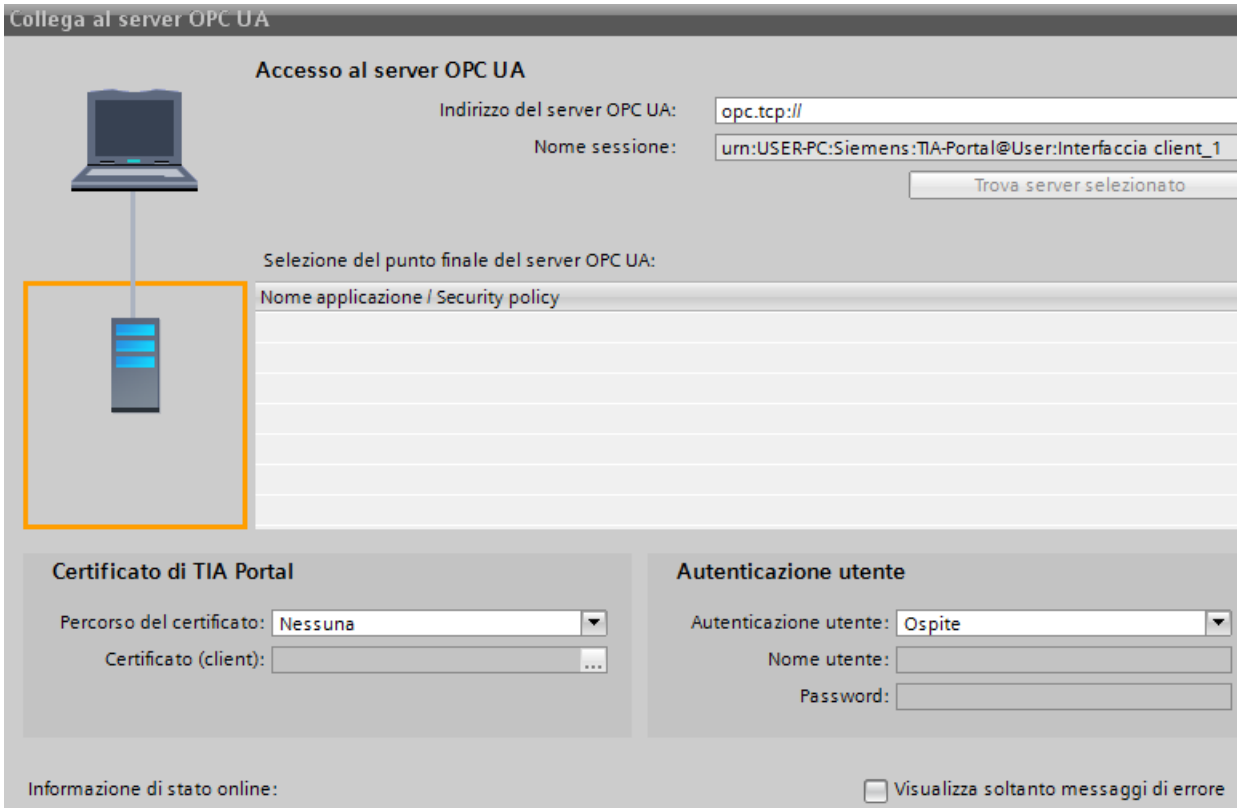


Figura 11-76 Finestra di dialogo "Collega al server OPC UA"

Suggerimento: Se si stabilisce per la prima volta un collegamento online al server OPC UA, usare il pulsante "Accessi online". Per ricollegarsi dopo un'interruzione del collegamento si deve invece selezionare "Collega al server online" a fianco del campo di selezione "Online".

Immettere in alto a destra l'indirizzo IP del server OPC UA di cui si vuole rilevare online l'interfaccia server.

7. Fare clic sul pulsante "Trova il server selezionato".

   STEP 7 crea un collegamento con il server OPC UA e rileva tutte le impostazioni di sicurezza (server endpoint) messe a disposizione dal server.

   STEP 7 visualizza i punti finali in un elenco:

Figura 11-77 Serve OPC UA trovati con i relativi punti finali

8. Fare clic sul punto finale che si vuole utilizzare per il collegamento di STEP 7 con il server OPC UA.
9. Si vuole utilizzare un collegamento protetto?
   – Se è stato selezionato un punto finale sicuro, selezionare la voce "TIA Portal" in "Archivio certificati".

     In "Certificato (client)" selezionare un certificato client per il PC sul quale viene eseguito STEP 7 (TIA Portal).

     Se non esiste ancora nessun certificato client per il PC, è possibile generare un certificato client nel TIA Portal.

     Per creare un nuovo certificato per il PC procedere nel seguente modo:

     - Fare clic sul pulsante nel campo di immissione "Certificato (client)".

     - Fare clic sul pulsante "Aggiungi".

     - In "Titolare certificato" immettere "STEP 7 (TIA Portal)".

     - Selezionare in "Destinazione d'uso" la voce "Client OPC UA".

     - In "Titolare alternativo del certificato (SAN)" immettere alla voce "Valore" l'indirizzo IP del PC in cui viene eseguito STEP 7 (TIA Portal). Sovrascrivere l'indirizzo IP già inserito.

     - Se il PC utilizza un secondo indirizzo IP immettere anche questo indirizzo. Se il PC non utilizza un secondo indirizzo IP eliminare il secondo indirizzo IP presente.

     - Fare clic sul pulsante "OK".

   – Se non è stato selezionato nessun punto terminale sicuro, mantenere la preimpostazione ("Nessuno").
10. Come ci si vuole connettere?
   – Se ci si vuole connettere al server OPC UA come ospite confermare l'impostazione di default di "Autenticazione utente".
   – Per connettersi con il nome utente e la password selezionare "Nome utente e password".

     Utilizzare il nome utente e la password impostate durante la configurazione del server OPC UA, alla voce "Generale > OPC UA > Server > Security > Autenticazione utente > Gestione utenti" nelle proprietà della CPU.
11. Fare clic sul pulsante "Collega".

    Con un collegamento protetto appare anche un messaggio, che indica la necessità di accettare il certificato server per poter creare il collegamento sicuro. Nella schermata messaggi è possibile visualizzare tramite un link ulteriori dettagli sul certificato server.

    Questa schermata standard di Windows fornisce solo informazioni sul certificato server. Se si fa clic sul pulsante per installare il certificato server, il certificato non viene inserito nella memoria certificati del TIA Portal e quindi al prossimo tentativo di collegamento sarà nuovamente richiesto di accettare il certificato server.

    STEP 7 crea quindi un collegamento con il server OPC UA e visualizza nuovamente l'editor per le interfacce client.

    Nell'area destra dell'editor STEP 7 visualizza il livello superiore dell'area degli indirizzi del server OPC UA:

12. Fare clic sul triangolino nero vicino a "Objects".
    STEP 7 visualizza anche il livello sotto Objects.
13. Fare clic sul triangolino nero vicino a "Productionline".
    STEP 7 visualizza anche il livello sotto Productionline.
14. Aprire altre cartelle subordinate:

OPC UA server interface

Name of the node	Node type	Access level
Server	Object	
DeviceSet	Object	
Productionline	Object	
Counters	Object	
DataBlocksGlobal	Object	
Icon	ImagePNG	RD
Data_from_OPC_UA_Clients	Object	
ProductionEnabled	Boolean	RD/WR
Data_for_OPC_UA_Clients	Object	
ProductNumber	Int16	RD
Temperature	Array of Float	RD
NewProduct	Boolean	RD
DataBlocksInstance	Object	
Icon	ImagePNG	RD
OpenDoor_DB	Object	
DeviceManual	String	RD

Figura 11-78 Vista online dell'interfaccia del server OPC UA

Ulteriori informazioni

Per informazioni sulle mappe dei tipi di dati consultare il capitolo Mappatura dei tipi di dati (Pagina 236).

Per informazioni sulla creazione di un'interfaccia client consultare il capitolo Creazione delle interfacce client (Pagina 371).

11.4.7 Utilizzo di testi multilingue

Nell'editor per le interfacce clienti, con i file XML OPC UA (modelli di informazione) si importano anche i testi che possono essere visualizzati in diverse lingue. Il supporto multilingue è opzionale, ciascun nodo (Node) può essere definito in modo diverso a seconda delle lingue proposte.

Nel file XML sono i seguenti campi che possono essere predisposti per diverse lingue:

- DisplayName
- Description

Esempio di testi multilingue definiti in un file XML OPC UA

Nel file XML rappresentato il nome del display e la descrizione sono inseriti ad es. sia con un testo "default" sia con più testi localizzati.

- Il testo di default è rispettivamente il primo inserimento senza informazione di localizzazione
- Il testo localizzato è rispettivamente il testo dopo "Locale=" seguito da una sigla della lingua, ad es. "it-IT" per italiano

```
<UAVariable NodeId="ns=3;i=6070" BrowseName="3:EngineeringRevision" ParentNodeId="ns=3;i=1002"
DataType="String">
    <DisplayName>EngineeringRevision</DisplayName>
    <DisplayName Locale="en-US">EngineeringRevision</DisplayName>
    <DisplayName Locale="de-DE">Revisionsstand</DisplayName>
    <Description>Revision Level of the engineering environment.</Description>
    <Description Locale="en-US">Revision Level of the engineering environment.</Description>
    <Description Locale="de-DE">Revisionsstand der Engineeringumgebung.</Description>
    <Description Locale="fr-FR">Niveau de révision de l'environnement d'ingénierie.</Description>
    <Description Locale="it-IT">Livello di revisione dell'ambiente di ingegneria.</Description>
<References>
    <Reference ReferenceType="HasTypeDefinition">i=68</Reference>
    <Reference ReferenceType="HasModellingRule">i=78</Reference>
</References>
</UAVariable>
```

Figura 11-79 Esempio di un testo multilingue definito in un file XML OPC UA

Visualizzazione di testi multilingue

Durante l'importazione di un'interfaccia server i testi multilingue disponibili vengono salvati internamente e caricati in una CPU anche con il progetto.

L'editor client indica il testo del file XML OPC UA nelle colonne "Nome del nodo" (corrisponde a "DisplayName") e "Descrizione" (corrisponde a "Description").

La lingua che viene visualizzata per un nodo dipende dalle seguenti regole in cascata:

- Se il nodo contiene il testo nella lingua di editazione attualmente utilizzata, il testo viene visualizzato anche nella lingua di editazione.

  (Impostazione lingua di editazione: Nella navigazione del progetto selezionare il campo "Lingue & risorse > Lingue del progetto".
- Se il nodo non contiene testo nella lingua di editazione, ma se è definito un testo di default (senza sigla della lingua), viene visualizzato il testo di default.

- Colonna “Nome del nodo”: Se non è definito nemmeno un testo di default, ma un testo in una qualsiasi altra lingua, il testo DisplayName viene visualizzato nella prima lingua disponibile. Per i testi di descrizione questa regola non è valida.
- Se non è soddisfatta nessuna delle condizioni indicate sopra, non viene visualizzato nessun testo.

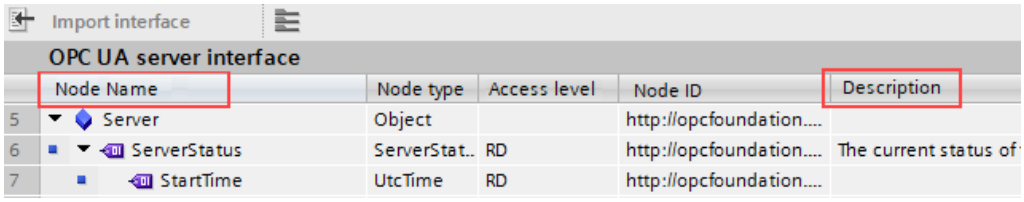


Figura 11-80 Visualizzazione di testi multilingue

Se si cambia la lingua di editazione, cambia anche il testo multilingue nell’interfaccia importata secondo le regole descritte sopra.

Successivamente i nodi possono essere acquisiti negli elenchi corrispondenti (elenco di lettura, elenco di scrittura, elenco di metodi) tramite Drag&Drop.

Negli elenchi (elenco di lettura, elenco di scrittura, elenco di metodi) non è possibile un cambio di lingua.

Acquisizione dei testi di descrizione visualizzati come commento nel tipi di dati PLC

Quando si compila il programma, STEP 7 genera automaticamente tipi di dati PLC (UDT) per ciascun elenco di lettura, elenco di scrittura e per gli ingressi o uscite di ciascun metodo. Questi UDT dispongono rispettivamente di un elemento per ciascun nodo.

Gli UDT acquisiscono il testo di descrizione come commento secondo le regole descritte sopra. STEP 7 genera il commento solo in una lingua; anche i testi nell’interfaccia server OPC UA possono essere visualizzati solo in una lingua.

11.4.8 Regole per l'accesso alle strutture

Di seguito sono spiegate le regole per l'accesso alle strutture, che vanno seguite quando si leggono e si scrivono valori di strutture complete messe a disposizione da un server OPC UA.

Modalità di accesso dei client delle CPU S7-1500 alle strutture

Per accedere in modo efficiente alle strutture durante il runtime il client OPC UA della CPU S7-1500 non si serve né dei TypeDictionaries, né degli attributi DataTypeDefinition forniti dai server per la risoluzione delle strutture.

Di conseguenza i client OPC UA hanno possibilità limitate di controllare gli elementi delle strutture mentre il programma utente è in esecuzione nel client.

Regole per l'accesso alle strutture

Se si progettano gli elenchi di lettura e di scrittura mediante le interfacce client (parametrizzazione del collegamento) e si assegnano i tipi di dati PLC in base al modello indirizzi del server importato o rilevato online, gli accessi in lettura e in scrittura alle strutture durante il runtime funzionano correttamente.

Questo perché la progettazione mediante l'interfaccia client garantisce automaticamente che l'ordine e i tipi di dati degli elementi delle strutture sul lato client e server corrispondano.

Suggerimento: Aggiornare una CPU S7-1500 CPU (come server) alla versione firmware attuale (ad es. V2.0 > V2.5.2 o superiore).

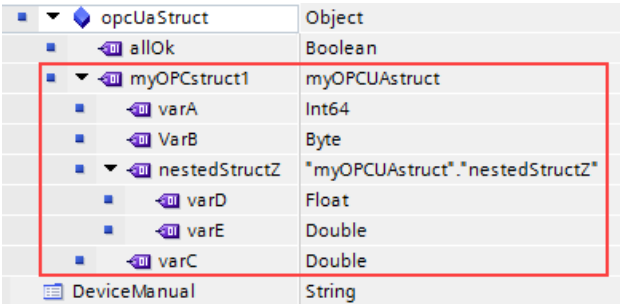
Durante il runtime il client OPC UA verifica solamente la lunghezza complessiva del valore trasmesso, non si possono invece eseguire verifiche più dettagliate.

Nelle strutture sono consentite anche le stringhe (WSTRING, STRING e OPC UA ByteString). Le stringhe hanno una lunghezza variabile, ma OPC UA supporta questa variabilità: Durante il trasferimento, infatti, a ogni stringa viene anteposto un campo di lunghezza nel quale è codificata la lunghezza della stringa. Una CPU S7-1500 come client OPC UA, pertanto, può verificare la lunghezza di una stringa e determinare se "si inserisca" nella variabile CPU assegnata. In questo modo la CPU può verificare anche la lunghezza totale della struttura.

Quando si assegnano strutture OPC UA a variabili PLC o DB, si devono seguire le regole previste per il mapping (vedere Mappatura dei tipi di dati (Pagina 236)).

Esempio di assegnazione corretta di elementi di strutture

Nel file Nodeset importato (file di esportazione XML) la struttura è definita nel seguente modo:



opcUaStruct	Object
allOk	Boolean
myOPCstruct1	myOPCUAstruct
varA	Int64
VarB	Byte
nestedStructZ	"myOPCUAstruct"."nestedStructZ"
varD	Float
varE	Double
varC	Double
DeviceManual	String

La struttura rappresentata nell'elenco di lettura corrisponde, rispetto sia all'ordine che ai tipi di dati assegnati, al nodo corrispondente del file Nodeset.

myOPCstruct1	myOPCUAstruct
varA	LINT
VarB	USINT
nestedStructZ	"myOPCUAstruct"."nestedStructZ"
varD	REAL
varE	LREAL
varC	LREAL

Se la struttura nel server cambia, ad es. perché si scambiano tra loro varA e varB, ma l'elenco di lettura del client resta invariato, l'assegnazione non corrisponde più:

- la lunghezza complessiva dei dati resta uguale (è cambiato solo l'ordine),
- la struttura nel client e nel server è diversa.

⚠ AVVERTENZA

Le differenze fra la struttura nel client e quella nel server non vengono segnalate con un errore

Se le strutture del client e del server non corrispondono, durante la compilazione e il runtime non viene segnalato un errore nonostante non siano state rispettate le regole.

Verificare che le assegnazioni progettate per le strutture non cambino in runtime. Se necessario riprogettarle negli elenchi di lettura e di scrittura.

11.4.9 Utilizzo della parametrizzazione del collegamento

11.4.9.1 Creazione e parametrizzazione dei collegamenti

Le istruzioni per i client OPC UA consentono di creare un programma utente che scambia dati con un server OPC UA. Per questo è necessaria una serie di tipi di dati di sistema.

Per semplificare le operazioni con questi tipi di dati di sistema, STEP 7 (TIA Portal) dalla versione 15.1 dispone di una parametrizzazione del collegamento per i client OPC UA.

La parametrizzazione del collegamento è un'opzione facoltativa e non obbligatoria. I tipi di dati di sistema possono anche essere creati manualmente.

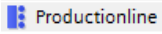
Affinché la descrizione sia comprensibile viene utilizzato un esempio, vedere la descrizione dell'esempio (Pagina 369).

Apertura della parametrizzazione del collegamento

Per parametrizzare il collegamento a un server OPC UA, procedere nel modo seguente:

1. Fare due volte clic nell'area "Comunicazione OPC UA" nella navigazione del progetto sull'interfaccia client da parametrizzare.

   Per la configurazione di esempio: Fare due volte clic sull'interfaccia client "Productionline":

   Per informazioni su come creare un'interfaccia client consultare il capitolo "Creazione di interfacce client (Pagina 371)".
2. Fare clic sulla scheda "Proprietà" (finestra di ispezione), se non è già visualizzata.

   STEP 7 visualizza quindi la parametrizzazione del collegamento per le istruzioni del client OPC UA.

   La scheda "Generale" è aperta.
3. Fare clic sulla scheda "Configurazione" e impostare il collegamento con il server OPC UA.

Impostazione dei parametri di collegamento

1. Scegliere un nome significativo per la sessione. Per l'esempio selezionare il nome "OPC UA Connection to Productionline".
2. Nel campo "Indirizzo" inserire l'indirizzo IP del server OPC UA con il quale il programma utente che funziona come client OPC UA deve creare un collegamento. Nella configurazione dell'esempio la CPU che controlla la linea di produzione ha l'indirizzo IP "192.168.1.1". Per creare il collegamento al server OPC UA di questa CPU inserire questo indirizzo IP nel campo "Indirizzo". In questo caso il server OPC UA utilizza la porta standard 4840.
   In alternativa è possibile inserire nel campo "Indirizzo" un nome DNS valido. La lunghezza del nome DNS è limitata a 242 caratteri.
   Se l'indirizzo non è valido, viene visualizzato il seguente messaggio di errore: "Inserire un indirizzo valido".
   Se la sequenza di caratteri dei campi "Indirizzo", "Porta" e "Percorso" contiene più di 254 caratteri, viene visualizzato un messaggio di errore.

3. Specificare un percorso all'interno del server OPC UA in modo da limitare l'accesso solo a quel percorso specifico. Questa indicazione è opzionale Anche se alcuni server si collegano solo se è stato indicato il percorso.

   Il percorso indicato viene inserito automaticamente nella voce "ServerEndpointUrl" del DB di configurazione per l'interfaccia client. La voce è costituita dai componenti "Prefisso dello schema OPC", "Indirizzo IP", "Numero di porta" e "Percorso del server", ad es.: "opc.tcp://192.168.0.10:4840/Esempio/Percorso".

   La seguente figura illustra l'immissione dell'indirizzo IP del server OPC UA:

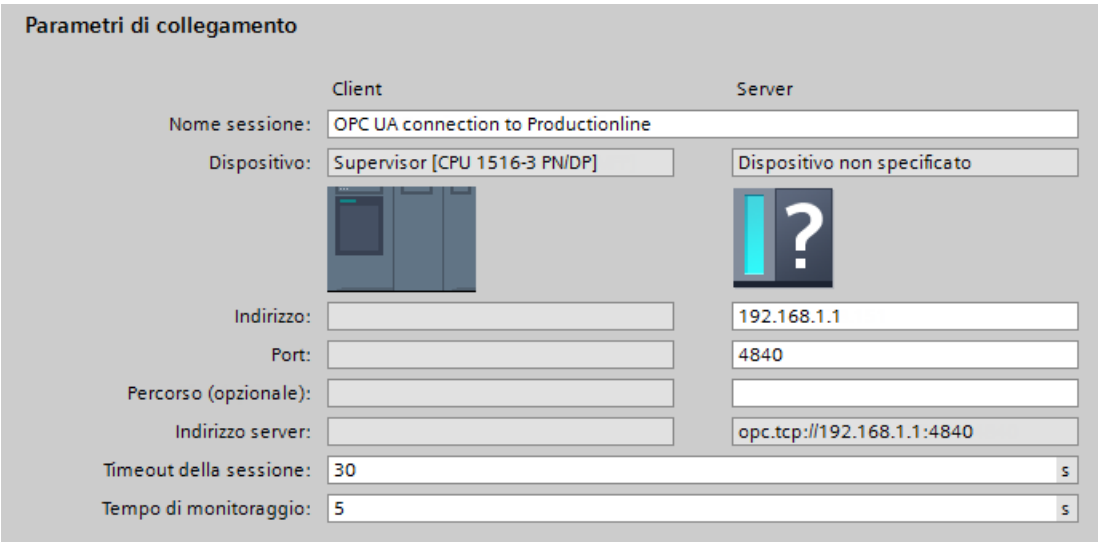


Figura 11-81 Parametri di collegamento

4. Se il server OPC UA non utilizza la porta standard 4840, è necessario inserire qui il numero di porta.

   Ad esempio inserire nel campo il numero 65535 se il server OPC UA da collegare utilizza questo numero di porta.

5. Inoltre vengono applicati i valori preimpostati per il "Timeout della sessione" (30 secondi) e il "Tempo di controllo" (5 secondi).

Impostazione dei parametri Security

1. Fare clic sull'area "Security" nella scheda "Configurazione".

   In questa area si trovano tutte le impostazioni di sicurezza per il collegamento al server OPC UA.

Sono possibili ad es. le seguenti impostazioni:

Area "Generale"

Modalità di sicurezza:

Selezionare nella casella di riepilogo la modalità di sicurezza che il collegamento al server OPC UA deve avere.

Se il server non è conforme alla modalità selezionata non viene creata nessuna sessione.

È possibile scegliere tra le seguenti impostazioni:

- None: Nessun collegamento protetto!
- Firma: Il server e il client OPC UA firmano il trasferimento dei dati (tutti i messaggi): È così possibile riconoscere eventuali manipolazioni.
- Firma e crittografia: Il server e il client OPC UA firmano e crittografano il trasferimento dei dati (tutti i messaggi):

Security Policy:

Impostare le tecniche di crittografia per la firma e la crittografia dei messaggi.

Sono possibili le seguenti impostazioni:

- None
- Basic128Rsa15
- Basic256
- Basic256Sha256

Per configurare un collegamento protetto è necessario osservare i seguenti punti:

- Per un collegamento protetto è necessario un certificato per il client.
- È quindi necessario comunicare al server questo certificato del client.

Il procedimento è descritto al capitolo "Handling dei certificati dei client e dei server (Pagina 267)" in "Certificato del client OPC UA".

Area “Certificati"

Certificato client:

Il certificato conferma l’autenticità del client OPC UA.

Per selezionare un certificato fare clic sull’icona seguente:

STEP 7 visualizza un elenco di certificati.

Selezionare il certificato comunicato al server.

Fare clic sull’icona con il segno di spunta verde:

Oppure creare un nuovo certificato. Per eseguire questa operazione, fare clic sull’icona “Aggiungi”.

Se si genera un nuovo certificato è necessario comunicarlo al server.

Area "Autenticazione utente"

Per l’autenticazione utente sono possibili le seguenti impostazioni:

- Ospite
- Nome utente e password
- Utente (TIA Portal - Impostazioni di sicurezza)

Per maggiori informazioni consultare Gestione utenti e ruoli con diritti di accesso alle funzioni OPC UA (Pagina 278).

Impostazione delle lingue

Le variabili UA del tipo String possono essere localizzate in OPC UA, ovvero i testi (valori per la variabile UA) possono essere disponibili nel server in diverse lingue nazionali. Ad es. per DisplayName (nome del nodo) e Description (descrizione) possono essere disponibili testi localizzati.

Nell'area "Lingue" della scheda "Configurazione" esiste la possibilità di influire sulla lingua dei testi forniti dal server nel modo seguente:

Inserire nell'area "Lingue" una sequenza di lingue che il server trasmette al client durante la creazione del collegamento.

La lingua o l'ID locale combinato alla lingua ("sigla della lingua") che si inserisce nella prima riga è la lingua preferenziale del client.

- Se il server può fornire la variabile UA nella lingua desiderata, la lingua viene trasmessa al client.
- Se il server non può fornire la variabile UA nella lingua desiderata, controlla se può fornire la variabile UA nella lingua indicata nella seconda riga (prima lingua sostitutiva).
- Il server conclude l'elaborazione dell'elenco e se non può fornire né la lingua desiderata né una lingua sostitutiva, visualizza la lingua di default.

Ulteriori informazioni

Quali cause esistono se il collegamento ad un server OPC UA non riesce? FAQ. (https://support.industry.siemens.com/cs/ww/it/view/109766709)

11.4.9.2 Handling dei certificati client della CPU S7-1500

Da dove proviene il certificato del client?

Se si utilizza il client OPC UA di una CPU S7-1500 (client OPC UA attivato), da STEP 7 V15.1 è possibile creare certificati per i client come indicato nei paragrafi che seguono.

Se si utilizzano client UA di altri produttori o della OPC Foundation, al momento dell'installazione o del primo richiamo del programma viene generato automaticamente un certificato client. I certificati devono essere importati in STEP 7 da Gestione certificato e utilizzati per la CPU corrispondente.

Se si programma autonomamente un client OPC UA, è possibile creare i certificati nel programma. In alternativa è possibile creare i certificati con altri tool come OpenSSL o con il generatore di certificati OPC Foundation:

- Il procedimento da adottare in OpenSSL è descritto in: "Creazione autonoma di coppie di chiavi PKI e di certificati (Pagina 204)".
- Il procedimento nel caso del generatore di certificati OPC Foundation è descritto in: "Creazione dei certificati autofirmati (Pagina 203)".

Certificato del client OPC UA della CPU S7-1500

Il collegamento tra il server OPC UA e il client OPC UA è sicuro solo se il server classifica il certificato del client come attendibile.

È quindi necessario comunicare al server il certificato del client.

I paragrafi che seguono spiegano come creare il certificato per il client OPC UA della CPU S7-1500 e come metterlo a disposizione del server.

1. Creazione ed esportazione del certificato per il client

Per poter stabilire un collegamento sicuro è necessario creare un certificato client ed esportarlo - se server e client si trovano in progetti diversi.

Se client e server si trovano nello stesso progetto non è necessario esportare e successivamente importare il certificato client.

Presupposti

L'interfaccia della CPU è configurata e è presente un indirizzo IP.

Tenere presente che In "Titolare alternativo del certificato (SAN)" viene indicato l'indirizzo IP della CPU nell'impianto.

Creazione di un certificato client OPC UA

La soluzione più semplice per creare un certificato client per una CPU S7-1500 è usare la progettazione di un’interfaccia client.

La progettazione dell’interfaccia client prevede la selezione o la creazione di un certificato client, vedere Creazione e parametrizzazione dei collegamenti (Pagina 387).

In alternativa è anche possibile creare il certificato client come segue:

1. Nell’area "Navigazione del progetto" selezionare la CPU che funge da client.
2. Fare doppio clic su "Configurazione del dispositivo".
3. Fare clic su "Protezione & Security > Gestione certificato" nelle proprietà della CPU.
4. Fare doppio clic su "<Aggiungi nuovo>" nella tabella "Certificati dei dispositivi".

   STEP 7 apre una finestra di dialogo.
5. Fare clic sul pulsante "Aggiungi".
6. Selezionare dall'elenco "Destinazione d’uso" la voce "Client OPC UA".
7. Fare clic su "OK".

   STEP 7 visualizza il certificato client nella tabella "Certificati dei dispositivi".
8. Se il server si trova in un altro progetto: Fare clic con il tasto destro del mouse sulla riga corrispondente e selezionare il menu di scelta rapida "Esporta certificato".
9. Selezionare la directory di destinazione in cui salvare il certificato client.

2. Comunicazione del certificato client al server

Per poter stabilire un collegamento sicuro è necessario fornire al server il certificato del client.

Per eseguire questa operazione procedere nel seguente modo:

1. Se il client è stato configurato in un altro progetto e si è creato ed esportato il certificato client in tale progetto:
   - Attivare l'opzione "Utilizza impostazioni di security globali per la Gestione certificato" nella Gestione certificato locale del server. In questo modo diventa disponibile la Gestione certificato globale.

     Questa opzione si trova in “Protezione & Security > Gestione certificato", nelle proprietà della CPU utilizzata come server.
   - Se il progetto non è ancora protetto selezionare la voce "Impostazioni Security > Impostazioni" nella navigazione nel progetto di STEP 7, fare clic sul pulsante "Proteggi questo progetto" ed effettuare il login.

     In "Impostazioni Security" di "Navigazione del progetto" di STEP 7 ora compare la voce "Impostazioni Security globali".
   - Fare doppio clic su "Impostazioni Security globali".
   - Fare doppio clic su "Gestione certificato".

     STEP 7 apre la Gestione certificato globale.
   - Fare clic sulla scheda "Certificati dei dispositivi".
   - Fare clic con il tasto destro del mouse su una superficie libera nella scheda (non su un certificato).
   - Selezionare il menu di scelta rapida "Importazione".

     Si apre la finestra di dialogo per l'importazione dei certificati.
   - Selezionare il certificato client attendibile per il server.
   - Fare clic sul pulsante "Apri" per importare il certificato.

     Il certificato del client è ora contenuto nella gestione certificato globale. Prendere nota dell'ID del certificato client appena importato.
2. Fare clic sulla scheda "Generale" nelle proprietà della CPU utilizzata come server.
3. Fare clic sull’area "OPC UA > Server > Security > Secure Channel".
4. Far scorrere verso il basso la finestra di dialogo "Secure Channel" fino alla sezione "Client affidabili".
5. Fare doppio clic sulla riga vuota della tabella con "<Aggiungi nuovo>". Nella riga viene visualizzato un pulsante con tre puntini.
6. Fare clic su questo pulsante.
7. Selezionare il certificato client preparato.
8. Selezionare il pulsante con il segno di spunta verde.
9. Compilare il progetto.
10. Caricare la configurazione nella CPU S7-1500 (server).

Risultato

Il server ora considera il client attendibile. Inoltre, se il certificato server è considerato attendibile, il server e il client possono stabilire un collegamento sicuro.

11.4.9.3 Autenticazione dell'utente

Nell'interfaccia client OPC UA dell'S7-1500 è possibile impostare come si deve autenticare un utente del client OPC UA se vuole accedere al server. Per questa funzione è necessario selezionare l'interfaccia client corrispondente nella navigazione del progetto della CPU S7-1500 desiderata in "Comunicazione OPC UA > Interfacce client" e il tipo di autenticazione utente nella finestra di ispezione in "Proprietà > Configurazione > Security".

Tipi di autenticazione utente

Per l'autenticazione utente sono disponibili le seguenti possibilità:

- **Ospite**

  L'utente non deve dimostrare di essere autorizzato (accesso anonimo). A tale scopo la CPU genera per l'utente una sessione anonima e il server OPC UA non verifica l'autorizzazione dell'utente client.

- **Nome utente e password**

  L'utente deve dimostrare di essere autorizzato (nessun accesso anonimo). Il server OPC UA verifica se l'utente client è autorizzato ad accedere al server. Come prova vale il nome utente con la password corretta. Questi inserimenti non possono essere verificati dall'interfaccia client, di conseguenza vengono accettati come validi tutti i valori.

  NOTA

  STEP 7 memorizza nome utente e password senza crittografarli nel blocco dati/blocco dati di istanza. Suggerimento: Usare l'autenticazione utente per il progetto TIA "Utente (TIA Portal - Impostazioni Security)".

- **Utente (TIA Portal - Impostazioni di sicurezza)**

  Per l'autenticazione è possibile inserire un nome utente dall'elenco degli utenti inseriti nel progetto. Il nome degli utenti inseriti del progetto attuale è riportato nella gestione utenti, navigazione del progetto in "Impostazioni Security > Utenti e ruoli". Qui inoltre è possibile inserire altri utenti.

  È possibile inserire anche un nome che non si trova nella gestione utenti del progetto oppure lasciare vuoto il campo. Questo è necessario se il nome utente corrispondente proviene da un'altra sorgente durante il runtime, ad esempio tramite HMI o da un altro client OPC UA.

Security Policy “None” e autenticazione tramite nome utente e password

Si possono impostare le seguenti combinazioni:

Security Policy = “None” e autenticazione tramite il nome utente e la password.

- Il server OPC UA delle CPU S7-1500 supporta questa combinazione. I client OPC UA possono collegarsi e codificare o meno i dati di autenticazione.
- Anche il client OPC UA della CPU S7-1500 supporta questa combinazione: durante il runtime si collega tuttavia solo se può trasmettere i dati di autenticazione codificati.

Conseguenza: con la seguente configurazione non è possibile stabilire il collegamento con il controllore in runtime:

- S7-1500 come client OPC UA,
- server OPC UA che, se è impostata la Security Policy "None", non supporta il criptaggio dei dati di autenticazione.

Ulteriori informazioni

Per informazioni su utenti e ruoli con diritti di accesso OPC UA consultare il capitolo Gestione utenti e ruoli con diritti di accesso alle funzioni OPC UA (Pagina 278).

11.4.9.4 Utilizzo di un collegamento parametrizzato

Introduzione

Questo capitolo illustra l’utilizzo di un collegamento parametrizzato con le istruzioni OPC UA (Passo terzo).

Presupposti

- È stata creata un’interfaccia client e le sono stati aggiunti variabili e metodi PLC, vedere (“Primo passo (Pagina 371)”).
- È stato parametrizzato un collegamento a un server OPC UA (Secondo passo (Pagina 387)).

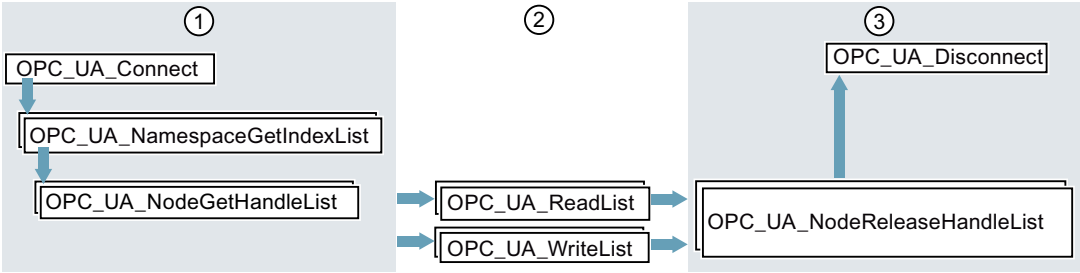
Panoramica

Per leggere i dati da un server OPC UA o scrivere i dati in un server OPC UA, utilizzare le seguenti istruzioni:

- OPC_UA_Connect
- OPC_UA_NamespaceGetIndexList
- OPC_UA_NodeGetHandleList
- OPC_UA_ReadList o OPC_UA_WriteList
- OPC_UA_NodeReleaseHandleList
- OPC_UA_Disconnect

Sequenza delle istruzioni OPC UA

La figura seguente illustra la sequenza in cui vengono richiamate le istruzioni OPC UA in un programma utente per leggere o scrivere variabili PLC:



① Istruzioni per le operazioni preliminari di scrittura e lettura

② Istruzioni di lettura e scrittura

③ Istruzioni per il “clean up” al termine delle operazioni di lettura o scrittura
L’istruzione “OPC_UA_NodeReleaseHandleList” può essere tralasciata se viene richiamata subito l’istruzione “OPC_UA_Disconnect”.

Figura 11-82 Sequenza di richiamo dei processi di scrittura e lettura.

STEP 7 (TIA Portal) assegna automaticamente i parametri a questa istruzione se si utilizza un’interfaccia client e un collegamento parametrizzato a un server OPC UA.

Il procedimento è descritto nel capitolo seguente.

Utilizzo di interfaccia client e collegamento parametrizzato

Per utilizzare un collegamento OPC UA parametrizzato, procedere nel modo seguente:

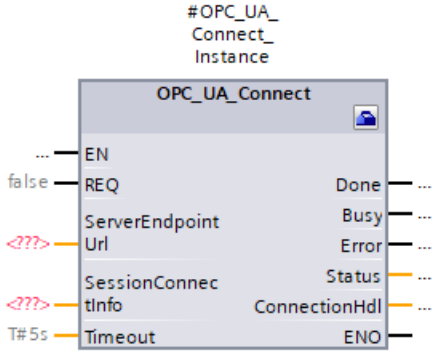
1. Aprire il programma utente nel TIA Portal.
2. Trascinare l'istruzione "**OPC_UA_Connect**" nell'editor di programma utilizzando il mouse.

   L'istruzione si trova in "Istruzioni > Comunicazione > OPC UA" nel TIA Portal.
3. Selezionare un'opzione di richiamo per l'istruzione.

   Nell'esempio viene utilizzata una multiistanza.

   STEP 7 rappresenta l'istruzione nell'editor di programma.

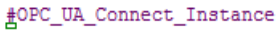
   L'editor per il linguaggio di programmazione schema logico (FUP) utilizza la seguente rappresentazione:



   L'editor per il linguaggio di programmazione schema a contatti (KOP) visualizza l'istruzione in modo analogo.
4. Fare clic nell'editor per FUP o KOP sull'icona rappresentante una cassetta per attrezzi.

   L'icona si trova nell'intestazione dell'istruzione:

   Se si utilizza l'editor per AWL o SCL: Fare clic sul piccolo rettangolo verde al di sotto del primo carattere del nome dell'istanza:

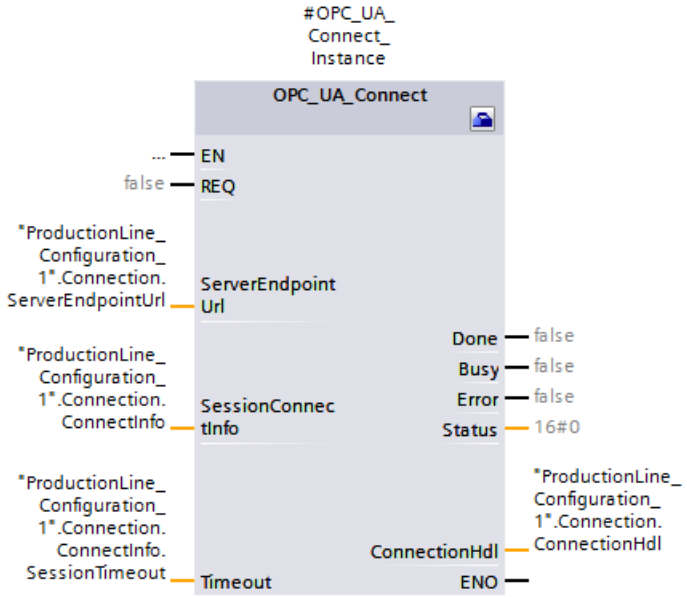
   Nell'esempio (Pagina 369) viene utilizzato "#OPC_UA_Connect_Instance" come nome dell'istanza.

   STEP 7 rappresenta le proprietà dell'istruzione in una finestra di dialogo separata.

5. In "Interfaccia client" selezionare l'interfaccia client da utilizzare per l'istruzione.

   Nell'esempio viene utilizzata l'interfaccia client "ProductionLine".

   STEP 7 interconnette quindi l'interfaccia client "ProductionLine" con i parametri dell'istruzione OPC_UA_Connect:



   "ProductionLine" è l'interfaccia che il client OPC UA dell'esempio (Pagina 369) utilizza per lo scambio dati con il server OPC UA "ProductionLine".

6. Trascinare l'istruzione "**OPC_UA_NamespaceGetIndexList**" nell'editor di programma utilizzando il mouse.

   L'istruzione si trova in "Istruzioni > Comunicazione > OPC UA" nel TIA Portal.

   Selezionare l'opzione di richiamo "Multiistanza".

   Se l'editor non è già aperto, fare clic sull'icona rappresentante una cassetta per gli attrezzi (KOP e FUP) oppure sulla casella verde sotto al nome dell'istanza (AWL e SCL).

   Selezionare l'interfaccia client da utilizzare (nell'esempio "ProductionLine").

   STEP 7 interconnette quindi automaticamente tutti i parametri dell'istruzione "OPC_UA_NamespaceGetIndexList":

7. Trascinare l'istruzione "**OPC_UA_NodeGetHandleList**" nell'editor di programma utilizzando il mouse.

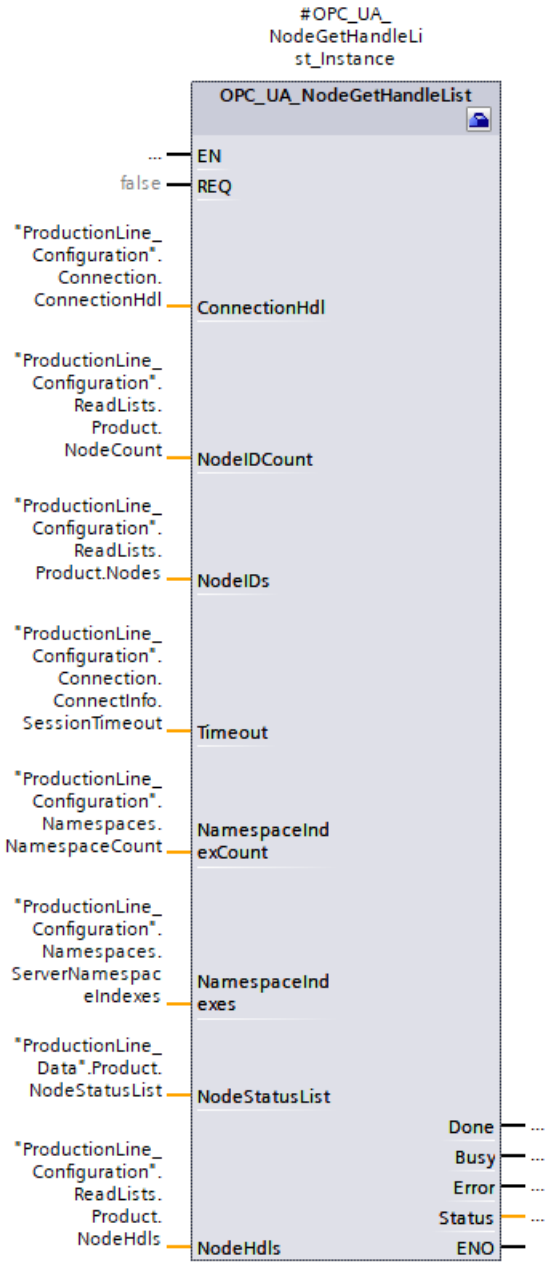
   Selezionare l'opzione di richiamo "Multiistanza".

   Se l'editor non è già aperto, fare clic sull'icona rappresentante una cassetta per gli attrezzi (KOP e FUP) oppure sulla casella verde sotto al nome dell'istanza (AWL e SCL).

   Selezionare l'interfaccia client da utilizzare. Nell'esempio viene utilizzata l'interfaccia client "ProductionLine".

   Selezionare in "Accesso ai dati > Elenco di lettura/scrittura" l'elenco di lettura da utilizzare (nell'esempio l'elenco di lettura "Product").

STEP 7 interconnette quindi automaticamente tutti i parametri dell'istruzione "OPC_UA_NodeGetHandleList":



Se si intendono scrivere dati in un server OPC UA, selezionare in "Accesso ai dati > Elenco di lettura/scrittura" l'elenco di scrittura da utilizzare (nell'esempio sarebbe l'elenco di scrittura "ProductionStatus").

8. Trascinare l'istruzione "**OPC_UA_ReadList**" nell'editor di programma utilizzando il mouse.

   Selezionare l'opzione di richiamo "Multiistanza".

   Se l'editor non è già aperto, fare clic sull'icona rappresentante una cassetta per gli attrezzi (KOP e FUP) oppure sulla casella verde sotto al nome dell'istanza (AWL e SCL).

Selezionare l'interfaccia client da utilizzare. Nell'esempio viene utilizzata l'interfaccia client "ProductionLine".

Selezionare in "Accesso ai dati > Elenco di lettura" l'elenco di lettura da utilizzare (nell'esempio l'elenco di lettura "Product").

STEP 7 interconnette quindi automaticamente tutti i parametri dell'istruzione "OPC_UA_ReadList".

Se si intendono scrivere dati in un server OPC UA, utilizzare l'istruzione "**OPC_UA_WriteList**" e selezionare in "Accesso ai dati > Elenco di scrittura" l'elenco delle variabili da inviare al server (nell'esempio l'elenco di scrittura "ProductionStatus").

9. Se si dovessero utilizzare nel programma utente diversi elenchi di lettura o di scrittura comandati dal programma, trascinare l'istruzione "**OPC_UA_NodeReleaseHandleList**" nell'editor di programma utilizzando il mouse.

   Selezionare l'interfaccia client da utilizzare.

   Selezionare quindi un elenco di lettura o di scrittura da abilitare: Abilitare elenchi di lettura / o scrittura usati raramente, in quanto la ripetizione della registrazione fa perdere molto tempo.

   Ripetere i passi dal passo 7 con l'istruzione "OPC_UA_NodeGetHandleList".

10. Trascinare l'istruzione "**OPC_UA_Disconnect**" nell'editor di programma utilizzando il mouse.

    Selezionare l'opzione di richiamo "Multiistanza".

    Se l'editor non è già aperto, fare clic sull'icona rappresentante una cassetta per gli attrezzi (KOP e FUP) oppure sulla casella verde sotto al nome dell'istanza (AWL e SCL).

    Selezionare l'interfaccia client da utilizzare. Nell'esempio viene utilizzata l'interfaccia client "ProductionLine".

    STEP 7 interconnette quindi automaticamente tutti i parametri dell'istruzione OPC_UA_Disconnect.

Istruzioni supportate

Nelle seguenti istruzioni STEP 7 assegna automaticamente i parametri se si utilizza un'interfaccia client e un collegamento parametrizzato al server OPC UA:

- OPC_UA_Connect
- OPC_UA_NamespaceGetIndexList
- OPC_UA_NodeGetHandleList
- OPC_UA_MethodGetHandleList
- OPC_UA_MethodReleaseHandleList
- OPC_UA_ReadList
- OPC_UA_WriteList
- OPC_UA_MethodCall
- OPC_UA_NodeReleaseHandleList
- OPC_UA_Disconnect

Istruzioni compatte

A partire da TIA Portal V17 sono disponibili istruzioni compatte per OPC UA, che riassumono la creazione del collegamento e il job di scrittura//job di lettura/richiamo del metodo.

- OPC_UA_ReadList_C per la creazione di un collegamento e la lettura di variabili
- OPC_UA_WriteList_C per la creazione di un collegamento e la scrittura di variabili
- OPC_UA_MethodCall_C per la creazione di un collegamento e il richiamo dei metodi

Informazioni sulle istruzioni compatte sono disponibili nella Guida a TIA Portal.

11.5 Suggerimenti e raccomandazioni

11.5.1 Regole per Subscription

Le seguenti regole valgono per Subscription:

- Raggruppare le Subscription nel client in base a diversi intervalli di campionamento e di trasmissione e ripartire gli elementi controllati (variabili) su questi gruppi.

  Esempio: Formare una Subscription per gli intervalli di trasmissione estesi (ad es. 5 secondi) e una Subscription per gli intervalli di trasmissione più brevi (ad es. 0,1 secondi).
- Disattivare le Subscription non necessarie.

  Motivo: La modalità Subscription “Disattivata" riduce l’utilizzo di risorse.
- Per ottimizzare ulteriormente l'utilizzo delle risorse ridurre il subscription timeout nel client. Il subscription timeout non può essere specificato direttamente; questo tempo è determinato dalle impostazioni Subscription "PublishingInterval" e "LifetimeCount" confermate dal server.
  Spiegazione: Se un client ha creato delle subscription e si chiude la sessione, queste rimangono inizialmente nel server e occupano risorse di memoria. Il server OPC UA libera nuovamente le risorse necessarie solo dopo che il subscription timeout ha determinato la conclusione delle subscripton.
- Rispettare il numero massimo di elementi controllati (Monitored Items) di Subscription per la CPU S7-1500 corrispondente.

  Le indicazioni si trovano nei dati tecnici della rispettiva CPU e si riferiscono all’intervallo di campionamento/di trasmissione di 1 secondo.

  Ulteriore informazioni sono riportante nel FAQ 109755846 (https://support.industry.siemens.com/cs/it/it/view/109755846).
- Selezionare per il client OPC UA e per il server OPC UA gli stessi intervalli di campionamento e di trasmissione.
- Evitare array e strutture come elementi di Subscription – se il processo è ammesso.

  Motivo: Se si modifica solo anche un valore di un array / una struttura, viene trasmessa l’intera struttura generando un carico inutile della comunicazione.
- Il server OPC UA della CPU S7-1500 conferma un’occasionale non osservanza della velocità di campionamento con un codice di errore "GoodOverload" in base alla specifica OPC UA, vedere anche la guida a TIA Portal. Client OPC UA diversi reagiscono in modo diverso a codici di errore "Good” diversi da "0". Osservare questo comportamento e ridurre, se possibile, il carico di comunicazione in base alle misure indicate sopra.

Ulteriori informazioni

Per informazioni sull'impostazione delle subscription per il server consultare il capitolo Impostazioni del server per le sottoscrizioni (Pagina 263).

11.5.2 Regole per il programma utente

Programmi utente per OPC UA

Le seguenti regole valgono per i programmi utente:

- Se l'applicazione lo consente e il carico di comunicazione è elevato, è preferibile impostare un tempo minimo per gli OB di ciclo.

  Vantaggi:

  – Il tempo di ciclo resta costante
  – Alla CPU resta più tempo per i compiti di comunicazione

  Suggerimento: Per l'analisi del carico della CPU (ad es. comunicazione) utilizzare l'istruzione "Runtime_Info"; modalità 21 o modalità 25 (vedere la guida a TIA Portal).
- Ridurre il numero di variabili e di blocchi dati accessibili da OPC UA/HMI. Come standard, durante la creazione di variabili/DB/IDB tutte le variabili sono accessibili da OPC UA/HMI. Questa misura comporta una migliore performance durante il caricamento in RUN.

  Suggerimento: Grazie alla visualizzazione dettagliata dell'oggetto in TIA Portal è possibile contrassegnare in modo semplice i blocchi dati non rilevanti per OPC UA come "non accessibili da OPC UA".
- Una trasmissione coerente di dati oltre i limiti di tipi di dati semplici è possibile solo con metodi OPC UA. Se si utilizzano altre funzioni OPC UA (subscription, Read/Write), è necessario garantire la coerenza dei dati.
- Per accessi in lettura o scrittura ricorrenti alle stesse variabili, OPC UA offre il servizio "RegisterNodes". Questo servizio consente ai server di preparare l'accesso ottimizzato alle variabili. L'istruzione "OPC_UA_NodeGetHandleList" della CPU S7-1500 come client OPC UA richiama in modo implicito questo servizio per preparare il server ad accessi ottimizzati (nel linguaggio dell'OPC UA "Registered Read/Write").

Richiamo della visualizzazione dettagliata degli oggetti in TIA Portal

Per richiamare la visualizzazione dettagliata degli oggetti procedere nel modo seguente:

1. Passare alla vista del Portal “Programmazione PLC".
2. Selezionare “Visualizza tutti gli oggetti".
3. Passare alla scheda “Dettagli” nella finestra di selezione.
4. Disattivare nella colonna "DB accessibile da OPC UA" l’accessibilità da OPC UA per i singoli oggetti.

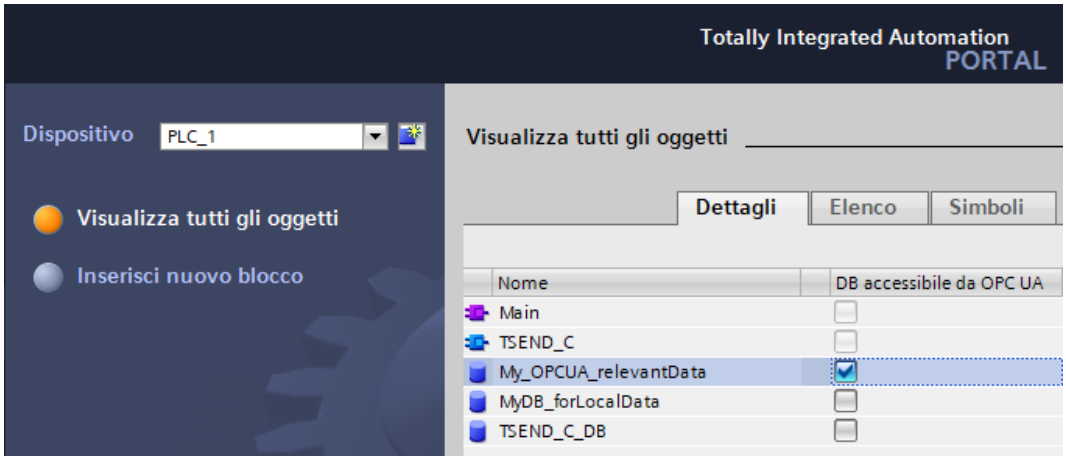


Figura 11-83 Richiamo della visualizzazione dettagliata degli oggetti in TIA Portal

11.5.3 Copie master per la comunicazione OPC UA

Copie master per le interfacce OPC UA

Le interfacce dei server OPC UA e dei client OPC UA che si vogliono utilizzare più volte possono essere salvate nella biblioteca del progetto o in una biblioteca globale. Le copie master nella biblioteca del progetto possono essere utilizzate soltanto all'interno di quest'ultimo. Se creata in una biblioteca globale, la copia master può essere utilizzata in diversi progetti.

Le CPU con funzione OPC UA distinguono 3 diversi tipi di interfacce del server OPC UA:

- Interfaccia server usuale
- Specifica Companion interfaccia
- Riferimento namespace

Quando si aggiunge l’interfaccia OPC-UA nella navigazione del progetto in “Comunicazione OPC UA" ciascun tipo di interfaccia ottiene un’icona propria. Lo stesso simbolo acquisisce anche la copia master.

Creare singole copie master o una copia master con diverse interfacce.

Creazione di diverse copie master dalla selezione

Selezionare uno o più elementi in base ai quali creare copie master.

1. Aprire la biblioteca nella task card "Biblioteche"
2. Selezionare gli elementi desiderati
3. Tramite drag&drop trascinare gli elementi nella cartella "Copie master" o in una qualsiasi sottocartella di "Copie master".

Creazione di una copia master dalla selezione

selezionare più elementi in base ai quali creare una singola copia master che li contiene tutti.

1. Copiare negli appunti gli elementi di cui creare una copia master
2. Con il tasto destro del mouse fare clic sulla cartella "Copie master" o su una qualsiasi sottocartella nella biblioteca
3. Selezionare il comando "Inserisci come copie master singole" dal menu di scelta rapida

Se il server OPC UA o il client OPC UA aggiunge più interfacce ad una copia master, vengono modificate di conseguenza l'intestazione e l'icona nella biblioteca.

Al posto dell'icona semplice viene visualizzata un'icona con "+".

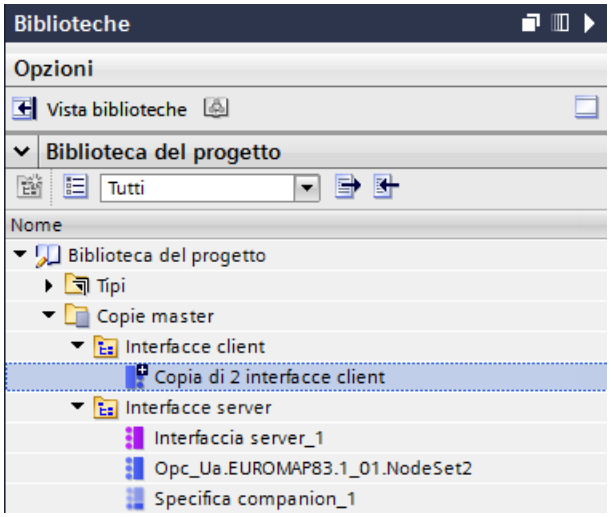


Figura 11-84 Creazione copia master in STEP 7.

Ulteriori informazioni

Per informazioni su come creare un'interfaccia server definita dall'utente consultare il capitolo Creazione dell'interfaccia server personalizzata (Pagina 296).

Assegnazione di indirizzi tramite DHCP

12

Per assicurare un'automazione moderna, potente e flessibile, sempre più componenti supportano gli standard IT del settore di produzione. Gli standard Ethernet utilizzati in tutto il mondo, la comunicazione omogenea e la grande versatilità fanno dell'automatizzazione su base informatica una soluzione conveniente che soddisfa ogni esigenza. L'estensione funzionale delle modalità di comunicazione delle CPU S7-1500 va in questa direzione, ampliando le possibilità di impiego dell'impianto o della macchina. Le CPU si avvalgono della tecnologia IT per garantire un'automazione efficiente. Con l'introduzione di DHCP e l'estensione di DNS per la CPU S7-1500 dalla versione firmware V2.9, la flessibilità di configurazione delle soluzioni di automazione viene incrementata.

Per le interfacce di una CPU S7-1500, è possibile predisporre che i parametri di indirizzo, ad es. l'indirizzo IP con maschera di sottorete, vengano richiesti da un server DHCPv4 (di seguito server DHCP).

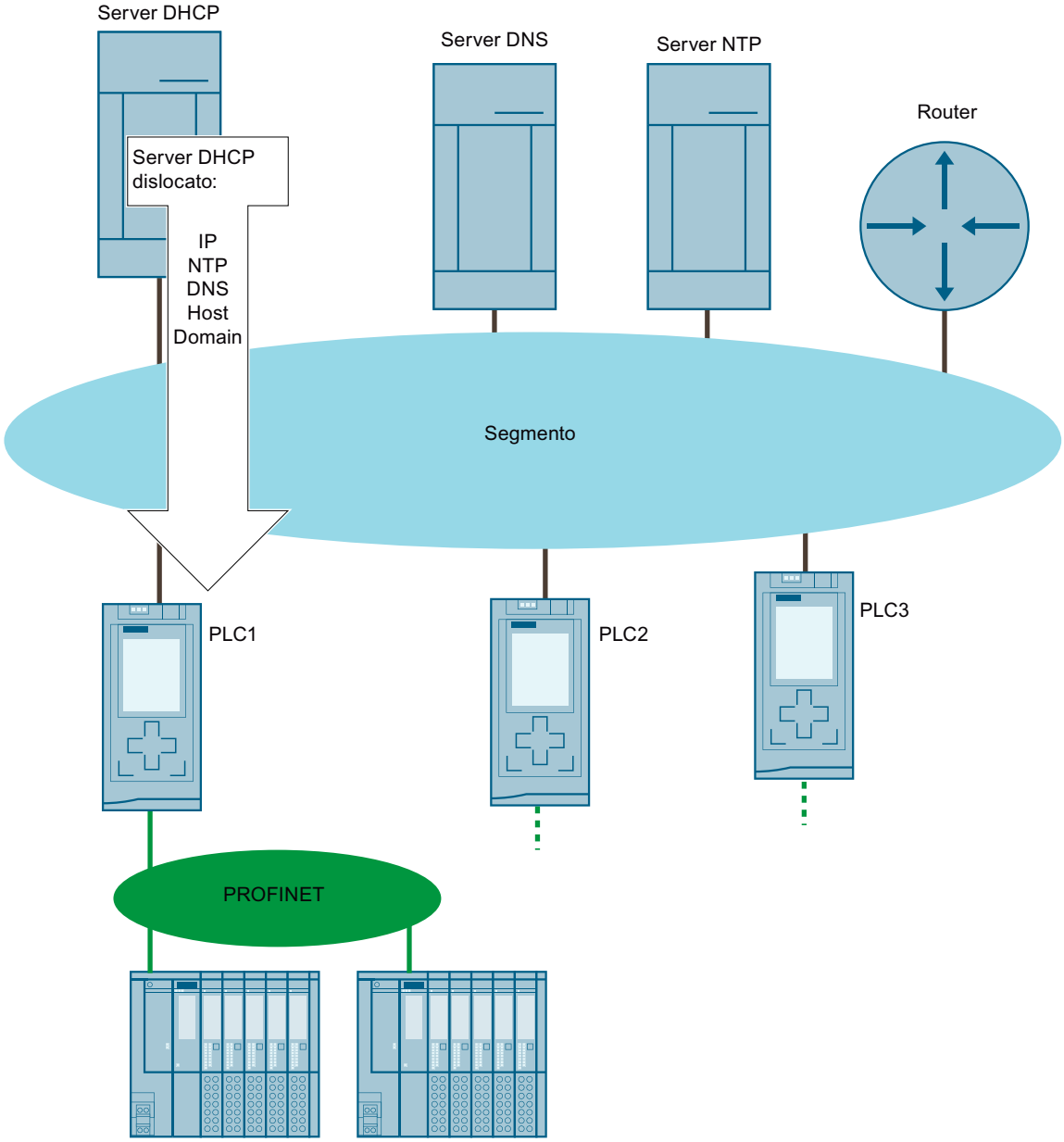


Figura 12-1 Panoramica DHCP

Campi d'impiego

- Impiego della CPU S7-1500 in un ambiente IT controllato
- Integrazione di nuovi dispositivi in una struttura di produzione modulare

12.1 Principio di assegnazione degli indirizzi con DHCP

Presupposti per la progettazione

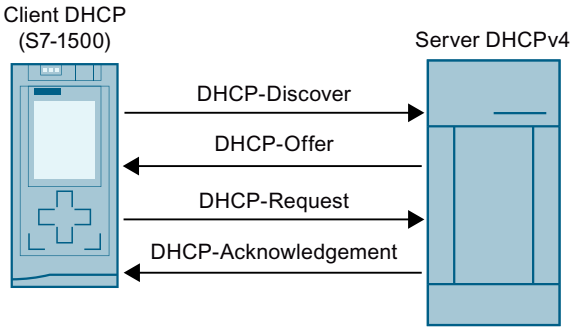
Affinché un'interfaccia PROFINET della CPU S7-1500 possa acquisire i parametri dell'indirizzo IP da un server DHCP, devono essere soddisfatti i seguenti presupposti:

- L'assegnazione dell'indirizzo deve essere configurata tramite un server DHCP.

  Disattivazione di DHCP (Pagina 413)
- Per l'interfaccia non deve essere progettata nessuna comunicazione PROFINET IO.

Principio di assegnazione dell'indirizzo DHCP

Il processo di assegnazione dell'indirizzo DHCP ha inizio non appena il progetto viene caricato nella CPU o quando la CPU in cui è progettata l'assegnazione di quest'indirizzo viene accesa e avviata:



DHCP Discover	Il client DHCP cerca un server DHCP idoneo tramite broadcast. Il client DHCP si identifica presso il server DHCP con l'ID client configurato o con l'indirizzo MAC.
DHCP Offer	Il server DHCP fornisce al client DHCP, i parametri dell'indirizzo IP (indirizzo IPv4, maschera di sottorete, router di default opzionale) ed eventualmente altri dati (opzioni).
DHCP Request	Il client DHCP richiede i parametri dell'indirizzo IP e le opzioni proposte nell'offerta DHCP. Il client DHCP della CPU S7-1500 accetta sempre la prima offerta DHCP di un server DHCP che soddisfa i requisiti (indirizzo IP con maschera di sottorete).
DHCP Acknowledgement	Il server DHCP conferma e trasmette i parametri dell'indirizzo IP e le opzioni proposte nell'offerta DHCP. Il server DHCP comunica inoltre al client DHCP per quanto tempo potrà utilizzare i parametri di indirizzo (Lease-Time).

Figura 12-2 Principio di assegnazione degli indirizzi con DHCP

I parametri degli indirizzi IP e le opzioni vengono salvati nella memoria di caricamento della CPU. Dopo una cancellazione totale o un riavvio della CPU i parametri degli indirizzi IP e le opzioni vengono nuovamente acquisiti tramite DHCP.

Opzioni di assegnazione dell'indirizzo DHCP

Per la CPU S7-1500 è possibile configurare l'acquisizione delle seguenti opzioni tramite un server DHCP:

- Indirizzi con max. quattro server DNS

  Acquisizione degli indirizzi del server DNS tramite DHCP (Pagina 416)
- Indirizzo con max. 4 server NTP

  Acquisizione degli indirizzi del server NTP tramite DHCP (Pagina 416)
- Nome dell’host e del dominio

  Acquisizione del nome dell'host e del dominio tramite DHCP (Pagina 417)

Se necessario, il server DHCP fornisce, come opzione, anche l'indirizzo di un router (gateway predefinito).

Per quanto tempo la CPU S7-1500 può utilizzare i parametri di indirizzo DHCP?

Oltre ai parametri di indirizzo, il server DHCP comunica alla CPU S7-1500 (client DHCP) anche il Lease-Time. Il Lease-Time determina per quanto tempo la CPU può utilizzare i parametri di indirizzo.

Trascorso il Lease-Time, la CPU restituisce i parametri di indirizzo. La CPU dispone di un controllo del tempo interno per il Lease-Time.

Durante il Lease-Time, in alcuni momenti la CPU ha la possibilità di prolungarne la durata:

- Renewal: È trascorsa la metà del Lease-Time: La CPU contatta il server DHCP originario per chiedere un prolungamento del Lease-Time. Il server DHCP originario può confermare il Lease-Time preesistente o assegnarne uno nuovo. In caso di assegnazione di un nuovo Lease-Time, il controllo del tempo della CPU viene resettato.
- Rebinding: Sono trascorsi 7/8 del Lease-Time: La CPU contatta tutti i server DHCP disponibili tramite broadcast per chiedere un prolungamento del Lease-Time. Il server DHCP può confermare il Lease-Time preesistente o assegnarne uno nuovo. In caso di assegnazione di un nuovo Lease-Time, il controllo del tempo della CPU viene resettato.

  In caso di risposta negativa o di nessuna risposta da parte del server DHCP durante il rebinding, dopo 8/8 del Lease-Time, la CPU restituisce i parametri di indirizzo.

Se dopo la scadenza del Lease-Time la CPU ha restituito i parametri di indirizzo, la CPU con il nuovo DHCP-Discover inizia un nuovo ciclo di assegnazione dell'indirizzo DHCP.

Ulteriori informazioni

Per informazioni sulla configurazione dell'ID del client consultare il capitolo Configurazione dell'ID del client (Pagina 414).

12.2 DHCP con DNS

A partire da STEP 7 V17, la CPU S7-1500 supporta i parametri di indirizzo, il nome dell'host e del dominio, utilizzati nella comunicazione (DNS) basata sul nome.

Per determinati servizi di comunicazione, l'indirizzamento basato sul nome, tramite nome completo costituito da nome host e dominio, può rivelarsi utile:

- La CPU è indirizzabile con il nome completo, ad es. Open User Communication nel caso di OPC UA. In caso di assegnazione dinamica dell'indirizzo IP da parte del server DHCP, è sempre possibile un indirizzamento univoco tramite il nome DNS.
- I certificati della CPU S7-1500 possono contenere il nome completo, ad es. per la comunicazione OPC UA, il Web server, la comunicazione sicura.
  - Soltanto se il nome host e il dominio della CPU S7-1500 vengono configurati in STEP 7, il nome completo viene inserito nei certificati del dispositivo nel progetto come Subject Name alternativo (SAN).
  - Se il nome host o il dominio sono stati forniti da DHCP o assegnati nel programma utente, il nome completo non viene salvato nei certificati dei dispositivi nel progetto.

L'impostazione della configurazione DNS nella CPU dipende dalla modalità di assegnazione di nome host e dominio nella rete.

- Assegnazione centrale del nome host e del dominio

  L'assegnazione del nome host e del dominio avviene al livello centrale nella rete, ad es. tramite un server DNS configurato. In STEP 7 configurare la CPU in modo da acquisire tramite DHCP il nome dell'host e del dominio.

  Nella configurazione seguente, nella CPU S7-1500 è configurato solo l'ID del client. Durante l'assegnazione dell'indirizzo DHCP, il server DHCP fornisce alla CPU le opzioni nome host e dominio.

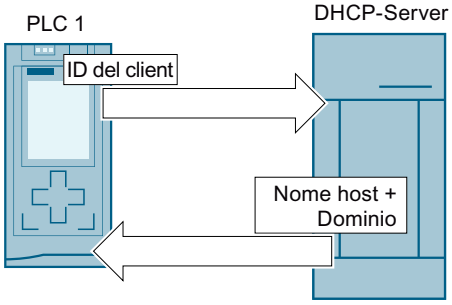


Figura 12-3 Acquisizione del nome dell'host e del dominio tramite DHCP

Per questa configurazione occorre innanzitutto attivare la configurazione del nome host e del dominio in STEP 7. Successivamente configurare l'acquisizione del nome host e del dominio tramite DHCP.

Acquisizione del nome dell'host e del dominio tramite DHCP (Pagina 417)

- Assegnazione locale del nome dell'host e del dominio

  Il nome host e il dominio possono essere progettati in STEP 7 oppure assegnati nel programma utente.

NOTA

Validità dei dati ottenuti tramite DHCP

In caso di modifica del nome host o del dominio nel programma utente, tutti i dati ottenuti tramite DHCP (IP Suite, nome host, dominio, server NTP, server DNS), perdono validità e devono essere nuovamente richiesti al server DHCP. Si raccomanda quindi di non apportare modifiche al nome host o al dominio se non in casi urgenti e, in quest'eventualità, non durante il funzionamento.

Se l'indirizzo IP dell'interfaccia subisce variazioni, tutti i collegamenti possono essere respinti.

Nella configurazione seguente, nella CPU S7-1500 oltre all'ID del client, sono configurati anche il nome host e il dominio. Durante l'assegnazione dell'indirizzo DHCP, la CPU fornisce al server DHCP anche il nome host e il dominio insieme all'ID del client. Il server DHCP contiene le informazioni per l'aggiornamento di un server DNS con i dati dell'indirizzo della CPU.

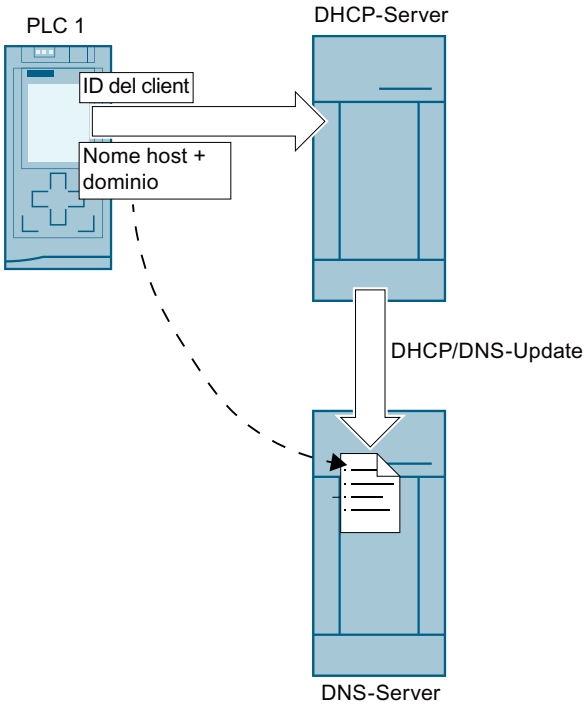


Figura 12-4 Configurare il nome dell'host e del dominio

Per questa configurazione occorre innanzitutto attivare la configurazione del nome host e del dominio in STEP 7. Configurare infine il nome dell'host e del dominio in STEP 7.

- Assegnazione centrale del dominio e assegnazione locale del nome host.
  - In STEP 7 configurare la CPU in modo da acquisire il dominio tramite DHCP.
  - Il nome host può essere progettato in STEP 7 oppure assegnato nel programma utente.

  Nella configurazione seguente, nella CPU S7-1500 è configurato, oltre all'ID del client, anche il nome dell'host. Durante l'assegnazione dell'indirizzo DHCP, la CPU fornisce al server DHCPv4 anche il nome host e l'ID del client. Il server DHCP fornisce alla CPU l'opzione dominio.

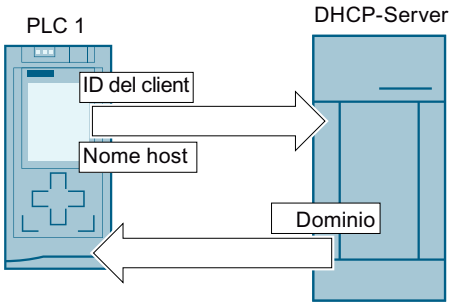


Figura 12-5 Configurazione del nome host, acquisizione del dominio tramite DHCP

Per questa configurazione occorre innanzitutto attivare la configurazione del nome host e del dominio in STEP 7. Configurare infine il nome dell'host in STEP 7 e predisporre che il dominio venga fornito tramite DHCP.

Presupposti

- L'assegnazione degli indirizzi tramite DHCP è stata attivata almeno per un'interfaccia della CPU S7-1500.

Attivazione della configurazione del nome host e del dominio

Per attivare la configurazione del nome host e del dominio in STEP 7, procedere nel modo seguente:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host".
3. Attivare la casella di opzione "Attiva nome host e dominio".

Configurazione del nome dell'host in STEP 7

Per configurare il nome dell'host in STEP 7 procedere nel seguente modo:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host" > "Nome host".
3. Alla voce "Configurazione del nome host:" della casella di riepilogo selezionare "Impostazione del nome host nel progetto".
4. Inserire il nome dell'host sotto "Nome host:".
   - Inserire il nome host desiderato.
   - Se si attiva la casella di opzione "Nome host identico al nome del dispositivo", STEP 7 assegna automaticamente il nome del dispositivo come nome dell'host.

Soltanto se il nome dell'host e il dominio sono stati configurati in STEP 7, alla voce "Nome completo:" viene visualizzato il nome per esteso.

Assegnazione del nome host nel programma utente

Per l'assegnazione del nome host nel programma utente procedere nel modo seguente:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host" > "Nome host".
3. Alla voce "Configurazione del nome host:" della casella di riepilogo selezionare "Imposta nome host direttamente nel dispositivo (ad es. programma PLC, display)".
4. Richiamare l'istruzione "CommConfig" nel programma utente. Il parametro DATA deve indicare un UDT "Conf_Hostname" nel quale è stato definito il nome host.

Ulteriori informazioni sull'istruzione "CommConfig" e sull'UDT "Conf-Hostname" sono disponibili nella Guida in linea a STEP 7.

Configurazione del dominio in STEP 7

Per configurare il dominio in STEP 7 procedere nel seguente modo:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host" > "Dominio".
3. Alla voce "Configurazione del dominio:" della casella di riepilogo selezionare "Impostazione del dominio nel progetto".
4. Sotto "Dominio:" inserire il dominio desiderato.

Soltanto se il nome dell'host e il dominio sono stati configurati in STEP 7, alla voce "Nome completo:" viene visualizzato il nome completo.

Assegnazione del dominio nel programma utente

Per l'assegnazione del dominio nel programma utente procedere nel modo seguente:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host" > "Dominio".
3. Alla voce "Configurazione del nome host:" della casella di riepilogo selezionare "Imposta dominio direttamente nel dispositivo (ad es. programma PLC, display)".
4. Richiamare l'istruzione "CommConfig" nel programma utente. Il parametro DATA deve indicare un UDT "Conf_Domainname" nel quale è stato definito il nome del dominio.

Ulteriori informazioni sull'istruzione "CommConfig" e sull'UDT "Conf-Domainname" sono disponibili nella Guida in linea a STEP 7.

Regole sulla lunghezza massima del nome host, del dominio e dell'ID del client

Osservare le seguenti lunghezze massime in byte: Un byte corrisponde ad un carattere:

- Nome host: max. 63 byte
- Dominio: max. 252 byte
- ID del client: max. 254 byte
- Nome host + dominio: max. 254 byte
- Nome host + dominio + ID del client: max. 260 byte

  Vale soltanto quando il nome host e il dominio devono essere trasmessi al server DHCP.

12.3 Disattivazione di DHCP

Presupposti

- CPU S7-1500 a partire dalla versione firmware V2.9

Procedura

Per attivare DHCP per l'interfaccia PROFINET di una CPU S7-1500, procedere nel seguente modo:

1. Selezionare in STEP7 l'interfaccia PROFINET della CPU S7-1500.
2. Nelle proprietà dell'interfaccia aprire il menu "Indirizzi Ethernet" > "Internet Protocol Version 4 (IPv4)".
3. Selezionare l'opzione "Indirizzo IP dal server DHCP".

Risultato

È impostata l'acquisizione da parte dell'interfaccia dell'indirizzo IP tramite un server DHCP.

Come modo di funzionamento per DHCP, nella CPU S7-1500 è impostato "Utilizza indirizzo MAC come ID del client". Come modificare l'ID del client è descritto in Configurazione dell'ID del client (Pagina 414).

12.4 Configurazione dell'ID del client

ID del client

In un server DHCP la CPU S7-1500 si identifica sempre con l'ID client (opzione DHCP 61). L'ID del client è specifico per l'interfaccia.

Per l'ID del client, la CPU S7-1500 supporta i due modi di funzionamento seguenti:

- Utilizzo dell'indirizzo MAC come ID del client: L'indirizzo MAC della CPU viene utilizzato come ID del client DHCP. Tenere presente che in caso di sostituzione della CPU in questo modo di funzionamento, l'indirizzo MAC e quindi anche l'ID del client subiscono modifiche.
- ID del client definito dall'utente: Con questa opzione, l'ID del client viene definito nella progettazione di STEP7. L'utente può inoltre adattare l'ID del client al runtime, ad es. nel programma utente con l'istruzione "CommConfig".
  Se in questo modo di funzionamento, ha luogo una sostituzione della CPU, alla nuova CPU viene assegnato l'ID client progettato.

Presupposti

- L'assegnazione degli indirizzi tramite DHCP è attivata per l'interfaccia.

Configurazione dell'ID del client

Per configurare l'ID del client in STEP 7 procedere nel seguente modo:

1. Selezionare in STEP7 l'interfaccia PROFINET della CPU S7-1500.
2. Nelle proprietà dell'interfaccia aprire il menu "Indirizzi Ethernet" > "Internet Protocol Version 4 (IPv4)" > "Indirizzo IP dal server DHCP".
3. Selezionare il modo di funzionamento desiderato nella casella di riepilogo "Modo di funzionamento:".
   - Utilizza indirizzo MAC come ID del client (predefinito)
   - ID del client definito dall'utente

   Se si seleziona l'opzione "Utilizza indirizzo MAC come ID del client", la procedura è conclusa. Se si seleziona "ID del client definito dall'utente" proseguire con il punto 4.

4. Alla voce "ID del client" inserire un ID del client valido.
   - Una sequenza di caratteri ASCII a 7 bit nel campo da 0x21 a 0x7e è consentita.
   - Alcuni server DHCP (ad es. alcuni dispositivi SCALANCE) richiedono che sia preceduto da uno "0". In questo caso digitare "\0" prima dell'ID del client.
   - Il campo può anche essere lasciato vuoto. In questo caso occorre attivare la casella di scelta "L'ID del client può essere modificato durante il runtime".
5. Per rendere possibile l'adattamento dell'ID del client durante il runtime, attivare la casella di scelta "L'ID del client può essere modificato durante il runtime".

Adattamento dell'ID del client durante il runtime

L'istruzione "CommConfig" consente di adattare l'ID del client nel programma utente. Richiamare quindi quest'istruzione. Il parametro DATA deve indicare un UDT "Conf_ClientId" o un UDT "Conf_ClientId_Opaque". Nell'UDT deve essere stato definito l'ID del client.

Se il campo dell'ID del client nella progettazione di STEP 7 è stato lasciato vuoto, la CPU utilizza l'indirizzo MAC come ID del client fino al primo adattamento dell'ID del client.

NOTA

Validità dei dati ottenuti tramite DHCP

In caso di modifica di ClientId tramite "CommConfig", tutti i dati ottenuti tramite DHCP perdono validità: IP Suite, nome del dominio, server NTP, server DNS. Si raccomanda quindi di non apportare modifiche ai ClientId se non in casi urgenti e, in quest'eventualità, non durante il funzionamento.

Ulteriori informazioni sull'istruzione "CommConfig" e sugli UDT "Conf_ClientId" e "Conf_ClientId_Opaque", sono reperibili nella Guida in linea a STEP 7.

12.5 Acquisizione degli indirizzi del server DNS tramite DHCP

Presupposti

- L'assegnazione degli indirizzi tramite DHCP è stata attivata almeno per un'interfaccia della CPU S7-1500.

Acquisizione degli indirizzi dei server DNS tramite DHCP

Per acquisire gli indirizzi di massimo 4 server DNS tramite DHCP procedere nel seguente modo:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Configurazione DNS" > "Elenco server".
3. Alla voce "Risoluzione del nome tramite DNS:" della casella di riepilogo selezionare "Impostare il server DNS remoto (ad es. DHCP)".

Risultato: Se il server DHCP fornisce, come opzione, gli indirizzi dei server DNS, la CPU utilizza fino a 4 indirizzi.

12.6 Acquisizione degli indirizzi del server NTP tramite DHCP

Presupposti

- L'assegnazione degli indirizzi tramite DHCP è stata attivata almeno per un'interfaccia della CPU S7-1500.

Acquisizione degli indirizzi dei server NTP tramite DHCP

Per acquisire gli indirizzi di massimo quattro server NTP tramite DHCP procedere nel seguente modo:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU passare a "Ora" > "Sincronizzazione dell'ora" > "Procedura NTP".
3. Alla voce "Sincronizzazione dell'ora:" della casella di riepilogo selezionare "Impostare il server NTP remoto (ad es. DHCP)".

Risultato: Se il server DHCP fornisce, come opzione, gli indirizzi dei server NTP, la CPU utilizza fino a 4 indirizzi.

12.7 Acquisizione del nome dell'host e del dominio tramite DHCP

Presupposti

- L'assegnazione degli indirizzi tramite DHCP è stata attivata almeno per un'interfaccia della CPU S7-1500.
- La configurazione del nome dell'host e del dominio è configurata in STEP 7.

Acquisizione del nome dell'host tramite DHCP

Per acquisire il nome dell'host tramite DHCP procedere nel seguente modo:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host" > "Nome host".
3. Alla voce "Configurazione del nome host:" della casella di riepilogo selezionare "Impostazione remota del nome host (ad es. DHCP)".

Risultato: Se il server DHCP fornisce come opzione un nome host, la CPU utilizza questo nome.

Acquisizione del dominio tramite DHCP

Per acquisire il dominio tramite DHCP procedere nel seguente modo:

1. Selezionare la CPU S7-1500 in STEP 7.
2. Nelle proprietà della CPU aprire "Configurazione ampliata" > "Nome dell'host e del dominio" > "Configurazione del dominio e del nome host" > "Dominio".
3. Alla voce "Configurazione del dominio:" della casella di riepilogo selezionare "Impostazione remota del nome del dominio (ad es. DHCP)".

Risultato: Se il server DHCP fornisce come opzione un dominio, la CPU utilizza questo dominio.

Routing

13

13.1 Panoramica dei meccanismi di routing delle CPU S7-1500

La seguente tabella fornisce una panoramica dei meccanismi di routing delle CPU S7-1500.

Meccanismo di routing	Descrizione	Applicazioni	Capitolo
Routing S7	Il routing S7 consiste nel trasferimento di dati oltre i limiti delle sottoreti S7. Questa tecnica consente l'invio di informazioni da un mittente a un ricevente attraverso diverse sottoreti S7.	Caricamento dei programmi utente Caricamento della configurazione hardware Esecuzione di funzioni di diagnostica e di test	Routing S7 (Pagina 419)
IP Forwarding	L'IP Forwarding è una funzione dei dispositivi che viene utilizzata per inoltrare i pacchetti IP tra 2 sottoreti IP connesse tra loro.	Semplice accesso da livello gestione a livello di campo per la configurazione e la parametrizzazione di device, ad es. tramite PDM o browser web. Semplice integrazione di device per accesso remoti, ad es. per diagnostica con manutenzione remota o aggiornamento firmware.	IP Forwarding (Pagina 423)
Routing di set di dati	I dati possono essere inviati alle apparecchiature da campo da una stazione di engineering da PROFINET attraverso diverse reti. Poiché la stazione di engineering accede alle apparecchiature da campo tramite set di dati normalizzati e il routing di questi ultimi avviene tramite dispositivi S7, per questo tipo di routing si è affermata la definizione "routing di set di dati".	Il routing di set di dati viene impiegato ad es. se si utilizzano apparecchiature da campo di diversi produttori. Le apparecchiature da campo vengono indirizzate tramite set di dati normalizzati (PROFINET) per la parametrizzazione e la diagnostica.	Routing dei set di dati (Pagina 430)

13.2 Routing S7

Definizione di routing S7

Il routing S7 consiste nel trasferimento di dati oltre i limiti delle sottoreti S7. Questa tecnica consente l'invio di informazioni da un mittente a un ricevente attraverso diverse sottoreti S7. Il passaggio da un sottorete S7 a una o più sottoreti diverse avviene nel router S7. Il router S7 è un dispositivo che accede alle sottoreti S7 interessate attraverso le interfacce. Il routing S7 è possibile attraverso diverse sottoreti S7 (PROFINET/Industrial Ethernet e/o PROFIBUS).

Presupposti per il routing S7

- Tutti i dispositivi accessibili in una rete sono stati configurati e caricati all'interno di un progetto in STEP 7.
- Tutti i dispositivi compresi nel routing S7 devono ricevere informazioni indicanti quali sottoreti S7 sono accessibili attraverso quali router S7 (= informazione di routing). I dispositivi ricevono quest'informazione di routing con il caricamento della configurazione hardware nelle CPU in quanto queste ultime svolgono il ruolo di router S7.

  In una topologia con più sottoreti S7 collocate una dietro l'altra occorre rispettare l'ordine seguente durante il caricamento: innanzitutto caricare la configurazione hardware nelle CPU che sono collegate direttamente alla stessa sottorete S7 del PG/PC, quindi caricare una dopo l'altra le CPU delle altre sottoreti S7 situate a valle, partendo dalla sottorete S7 più vicina fino alla sottorete S7 più remota.
- Il PG/PC con il quale si vuole creare un collegamento attraverso un router S7 deve essere assegnato alla sottorete S7 con la quale è anche effettivamente collegato fisicamente. Il PG/PC può essere assegnato a un altro PG/PC in STEP 7 selezionando Online & Diagnostica > Accessi online > Collegamento con interfaccia/sottorete.
- Per le sottoreti S7 di tipo PROFIBUS: la CPU deve essere configurata come master DP oppure se è configurata come slave DP, nelle proprietà dell'interfaccia DP dello slave DP deve essere attivata la casella di controllo "Test, messa in servizio e routing".
- Il routing S7 per i collegamenti HMI è possibile da STEP 7 V13 SP1 in poi.

NOTA

Firewall e routing S7

Nel routing S7 il firewall non riconosce l'indirizzo IP del mittente, se questo si trova all'esterno della sottorete S7 che confina con il firewall.

Una panoramica dei dispositivi che supportano la funzione "Routing S7" si trova in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/584459).

Routing S7 per i collegamenti online

Con il PG/PC è possibile accedere a dispositivi oltre i limiti delle sottoreti S7, ad esempio:

- Per caricare programmi utente
- Per caricare una configurazione hardware
- Per eseguire funzioni di test e di diagnostica

Nella figura seguente la CPU 1 è il router S7 tra la sottorete S7 1 e la sottorete S7 2.

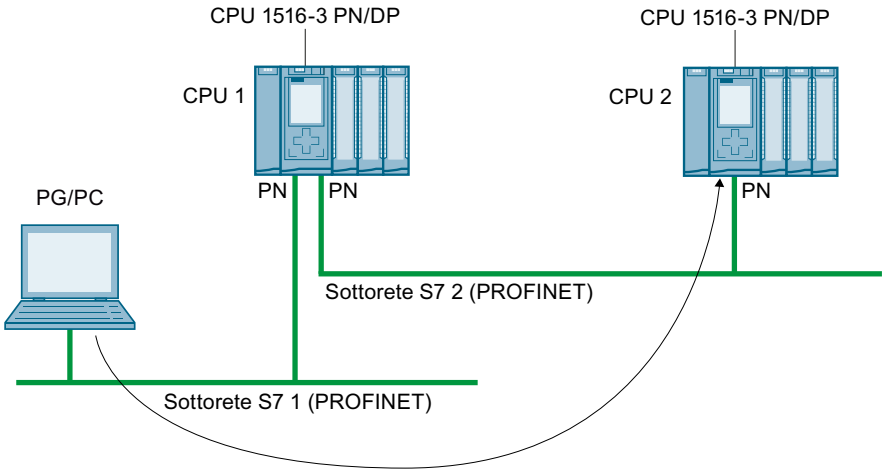


Figura 13-1 Routing S7: PROFINET - PROFINET

Nella figura seguente è rappresentato l'accesso da PROFINET a PROFIBUS da un PG. La CPU 1 funge da router S7 tra la sottorete S7 1 e la sottorete S7 2; la CPU 2 funge da router S7 tra la sottorete S7 2 e la sottorete S7 3.

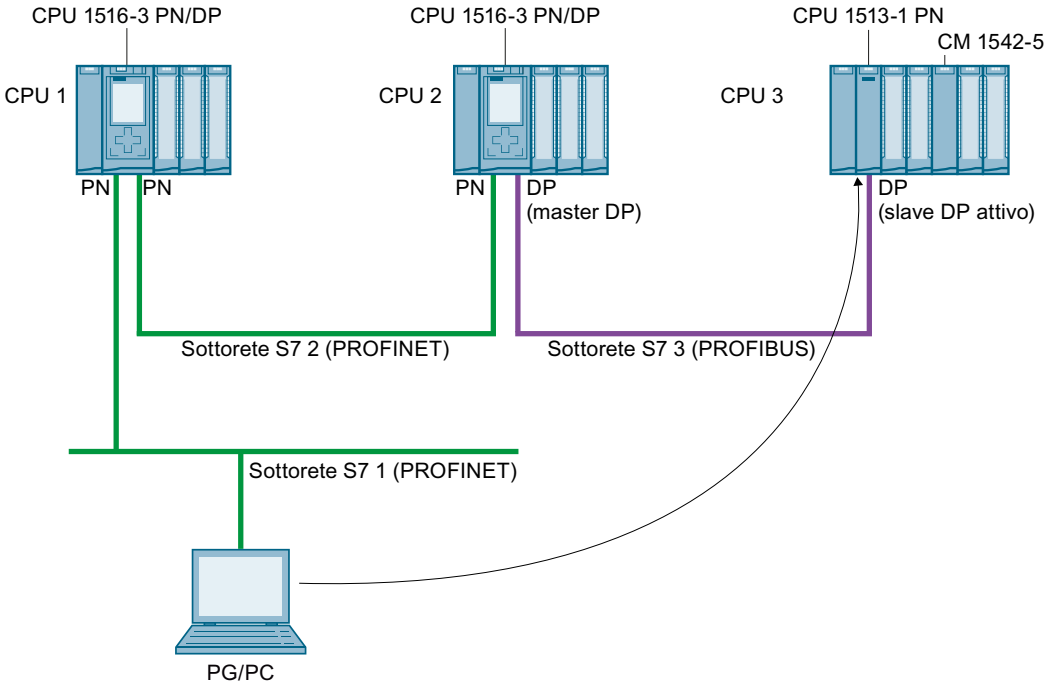


Figura 13-2 Routing S7: PROFINET - PROFIBUS

Routing S7 per i collegamenti HMI

È possibile configurare un collegamento S7 da un HMI a una CPU da diverse sottoreti (PROFIBUS e PROFINET o Industrial Ethernet). Nella figura seguente la CPU 1 è il router S7 tra la sottorete S7 1 e la sottorete S7 2.

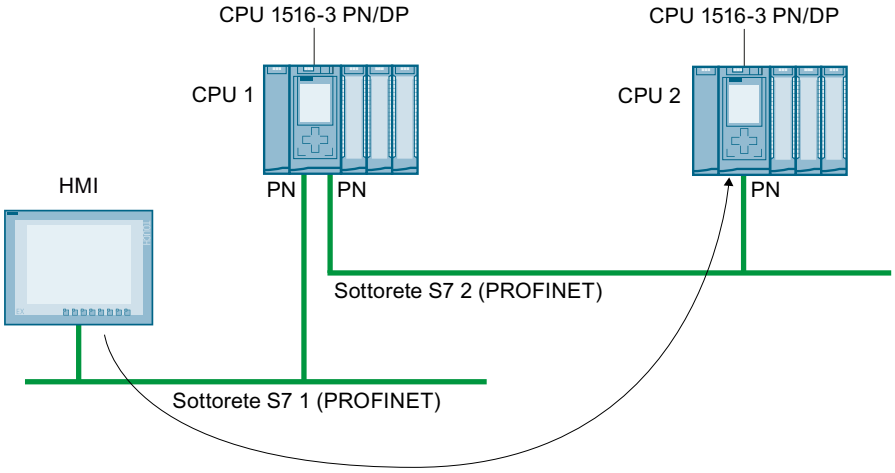


Figura 13-3 Routing S7 tramite collegamento HMI

Routing S7 per la comunicazione CPU-CPU

È possibile configurare un collegamento S7 da una CPU a un'altra tramite diverse sottoreti (PROFIBUS e PROFINET o Industrial Ethernet). Il procedimento è descritto con esempi nel capitolo Comunicazione S7 (Pagina 166).

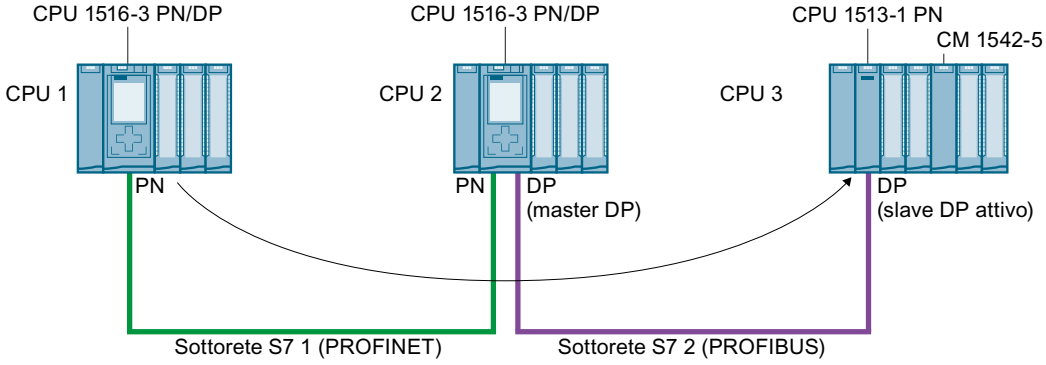


Figura 13-4 Routing S7 tramite comunicazione CPU-CPU

Utilizzo del routing S7

Per la CPU selezionare nella finestra di dialogo "Collega online" di STEP 7 l'interfaccia PG/PC e la sottorete S7. Il routing S7 viene eseguito automaticamente.

Numero di collegamenti per il routing S7

Il numero dei collegamenti disponibili per il routing S7 nei router S7 (CPU, CM o CP) è riportato nei dati tecnici nei rispettivi manuali del prodotto di CPU/CM/CP.

Routing S7: esempio applicativo

La figura seguente mostra come esempio applicativo la manutenzione remota di un impianto tramite un PG. Il collegamento si realizza in questo caso mediante un collegamento via modem oltre i limiti di due sottoreti S7.

Un collegamento remoto tramite TeleService si progetta in STEP 7 tramite "Accessi online" o "Collega online".

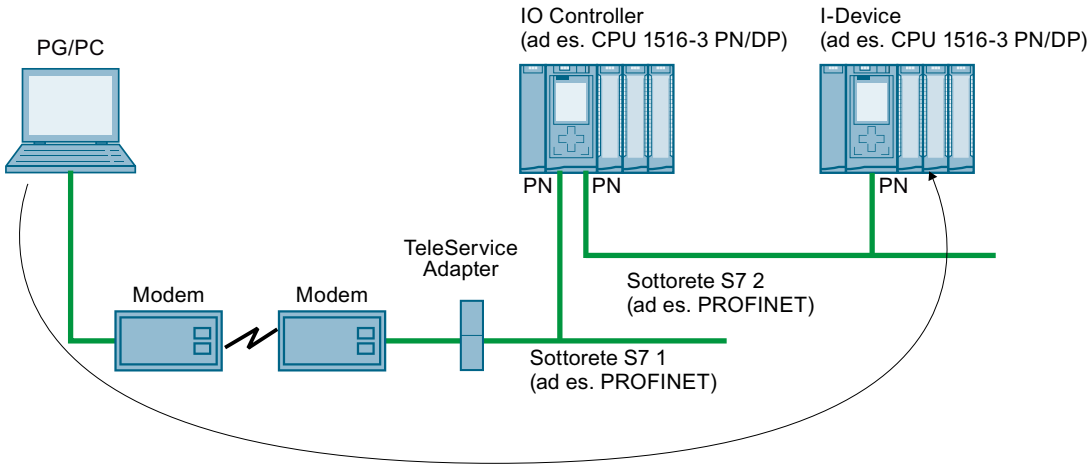


Figura 13-5 Manutenzione remota di un impianto tramite TeleService

Ulteriori informazioni

- L'occupazione delle risorse di collegamento per il routing S7 è descritta nel capitolo Occupazione delle risorse di collegamento (Pagina 440).
- Informazioni dettagliate sulla configurazione di TeleService sono disponibili nella Guida in linea a STEP 7.
- Per informazioni sulla comunicazione HMI consultare il capitolo Comunicazione HMI (Pagina 137).
- Per maggiori informazioni sul routing S7 e i TeleService Adapter utilizzare la ricerca in Internet nei seguenti link
  - Manuale del prodotto Industrie Software Engineering Tools TS Adapter IE Basic (https://support.industry.siemens.com/cs/it/it/view/51311100)
  - Download per TS Adapter (https://support.industry.siemens.com/cs/it/it/ps/16006/dl)

13.3 IP Forwarding

Inoltro di pacchetti IP con IP Forwarding

L'IP Forwarding è una funzione dei dispositivi che viene utilizzata per inoltrare i pacchetti IP tra 2 sottoreti IP connesse tra loro.

La funzione IP Forwarding può essere attivata e disattivata in STEP 7. Quando la funzione IP-Forwarding è attiva, la CPU S7-1500 inoltra i pacchetti IP ricevuti e non indirizzati a se stessa, alle sottoreti IP locali collegate oppure a un router configurato.

La seguente figura illustra in che modo un PG accede ai dati di un dispositivo HMI. Il PG e il dispositivo HMI si trovano in sottoreti IP diverse. Le sottoreti IP sono collegate a entrambe le interfacce X1 e X2 della CPU.

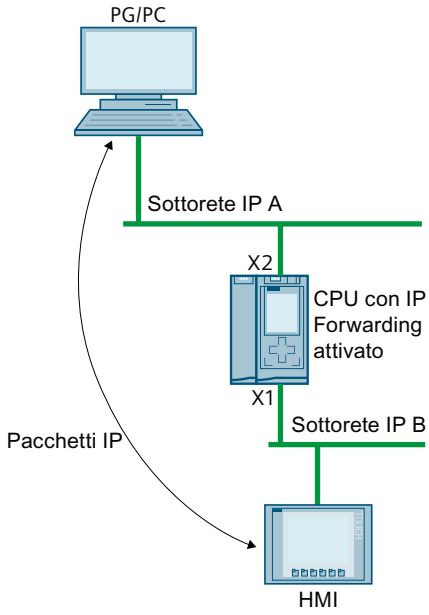


Figura 13-6 Accesso di un PG a un'HMI tramite IP Forwarding

Ambiti di impiego

- Semplice accesso da livello gestione a livello di campo per la configurazione e la parametrizzazione di apparecchiature da campo, ad es. tramite PDM o Webbrowser.
- Semplice integrazione di device per accesso remoti, ad es. per diagnostica con manutenzione remota o aggiornamento firmware.

Requisiti per l'utilizzo della funzione IP Forwarding

- CPU S7-1500 a partire dalla versione versione firmware V2.8
- Numero di interfacce Ethernet:
  - la CPU ha almeno 2 interfacce Ethernet,
  - oppure la CPU ha un'interfaccia Ethernet e un CP 1543-1 con versione firmware min. V2.2 mette a disposizione l'altra interfaccia Ethernet. In questo caso nella CPU deve essere attiva la funzione "Accesso al PLC tramite il modulo di comunicazione" per il CP.
- L'IP Forwarding è attivato.
- In tutti i dispositivi collocati lungo il percorso di andata e ritorno dei pacchetti IP sono parametrizzati gateway/rotta di default adatti.

Tabella di routing IP

Se la funzione IP Forwarding è attiva, la CPU inoltra i pacchetti IP ricevuti ma indirizzati ad un destinatario diverso. Il modo in cui la CPU inoltra i pacchetti IP è definito nella tabella di routing IP.

La CPU crea automaticamente la tabella di routing IP in base alle seguenti informazioni della configurazione hardware caricata:

- Configurazione IP delle interfacce Ethernet
- Router configurato

Esempio di configurazione con IP Forwarding

La seguente figura mostra un esempio di configurazione assieme alle necessarie impostazioni di indirizzo IP e router.

- Un PC che nella sottorete IP 192.168.4.0 comunica con un dispositivo HMI nella sottorete IP192.168.2.0.
- Nell'interfaccia Ethernet X3 della CPU è configurato l'indirizzo IP di un router ("standard gateway"); nella figura che segue questo dispositivo è definito "IP router".
  In STEP 7 il router può essere configurato in "Indirizzi Ethernet" > "Protocollo IP" nelle proprietà dell'interfaccia.

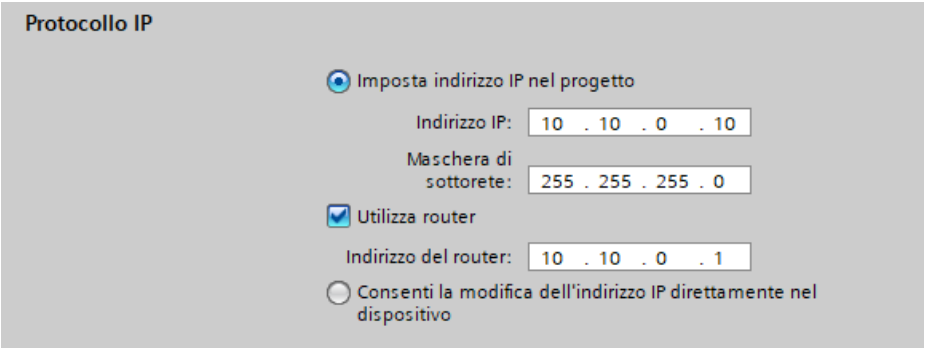


Figura 13-7 Configurazione del router

- Per il PC, il router IP, l'IO device e il dispositivo HMI sono indicati anche gli indirizzi IP del gateway standard e le corrispondenti rotte.

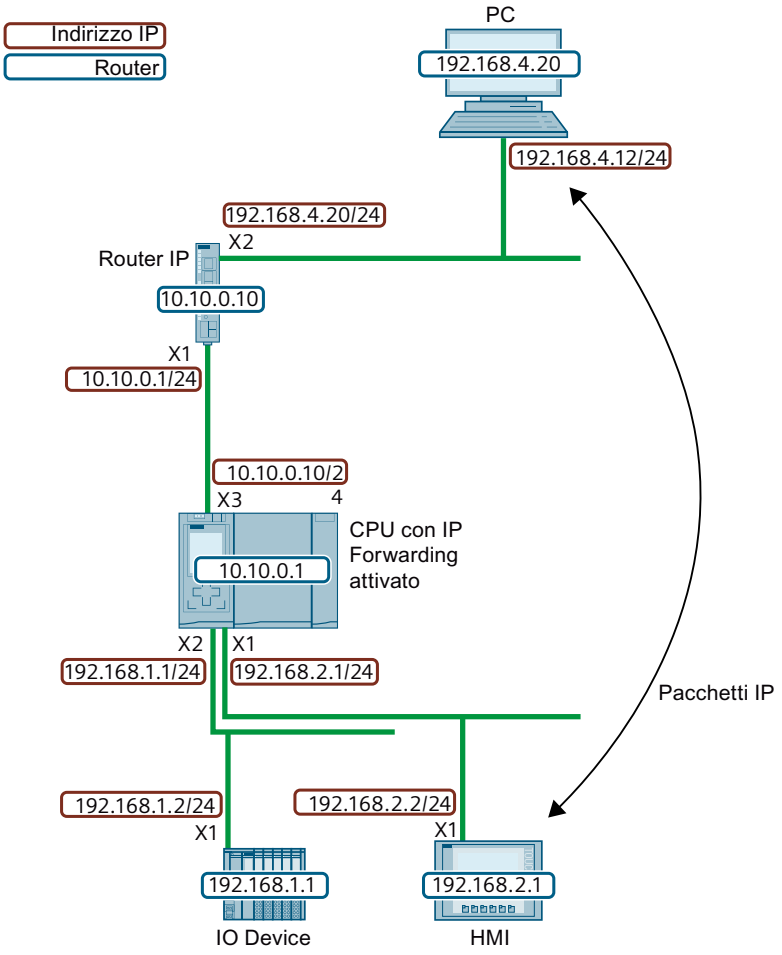


Figura 13-8 Configurazione di esempio

Dalla configurazione illustrata nell'esempio risulta la seguente tabella di routing IP per la CPU.

Tabella 13-1 Tabella di routing IP della CPU

Destinazione della rete	Interfaccia	Gateway
0.0.0.0/0	10.10.0.10	10.10.0.1
192.168.1.0/24	192.168.1.1	-
192.168.2.0/24	192.168.2.1	-
10.10.0.0/24	10.10.0.10	-

Per poter stabilire la comunicazione IP tra il PG/PC e il dispositivo HMI è necessario configurare, sia nel PC che nel router IP, ulteriori rotte IP per la sottorete IP del dispositivo HMI. Progettare nel dispositivo HMI viene progettato l'indirizzo IP dell'interfaccia X1 della CPU come gateway standard.

Nei computer Windows configurare ad es. un'ulteriore rotta IP nel prompt dei comandi utilizzando il comando "route add <sottorete IP di destinazione> mask <maschera di sottorete> <gateway>". Per poter procedere è tuttavia necessario disporre di diritti di accesso specifici. Per questo esempio immettere il seguente prompt:

- "route add 192.168.2.0 mask 255.255.255.0 192.168.4.20"

In un router IP configurare ulteriori route, ad es. mediante un'interfaccia web. Per questo esempio configurare la seguente route:

- Sottorete IP di destinazione 192.168.2.0
- Maschera di sottorete: 255.255.255.0
- Gateway: 10.10.0.10

Limitazioni

Per le CPU S7-1500 non è possibile configurare altri router IP oltre a quello definito ("standard gateway"). La destinazione della rete è una sottorete IP collegata oppure è accessibile attraverso uno specifico router configurabile. Poiché la CPU S7-1500 non supporta altri router IP, non è possibile configurare router IP in cascata bidirezionali.

Nella seguente configurazione si possono progettare nella CPU il "router 1" o "router 2". Nell'esempio è stato progettato il "router 1". In questo caso non è quindi possibile progettare il "router 2". Il PC e il dispositivo HMI non possono utilizzare la comunicazione IP perché la route non è percorribile in entrambe le direzioni.

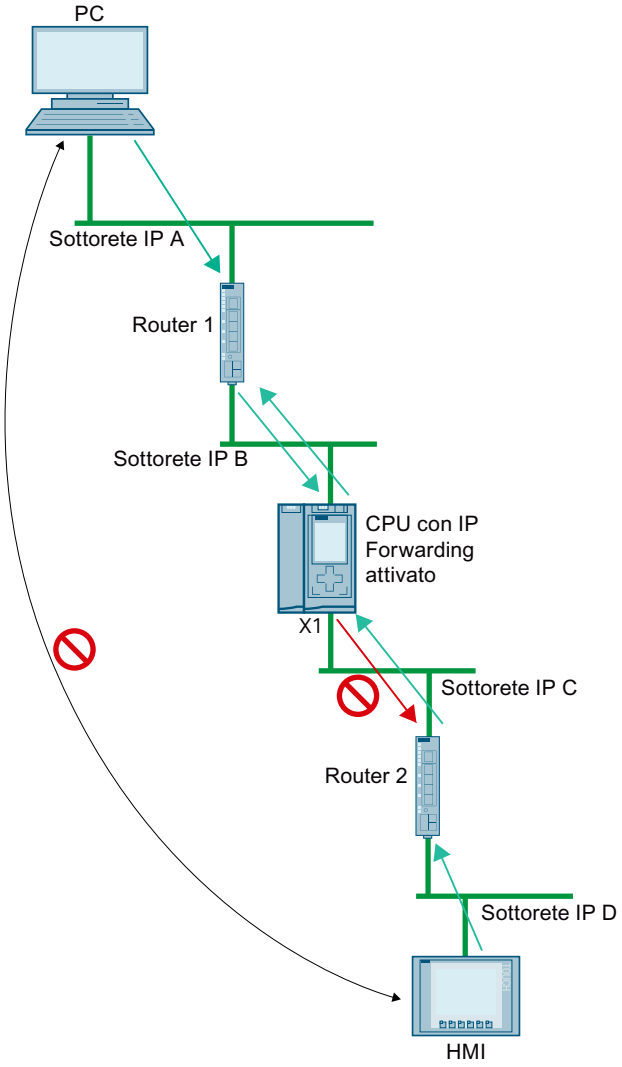


Figura 13-9 Collegamento in cascata dei router IP non supportato

IP Forwarding attraverso l'interfaccia di un CP

L'IP Forwarding funziona anche attraverso l'interfaccia di un CP. In questo caso si deve attivare nella CPU la funzione "Accesso al PLC tramite il modulo di comunicazione".

Maggiori informazioni sull'attivazione di questa funzione sono disponibili nella Guida in linea di STEP 7.

L'IP Forwarding tramite l'interfaccia di un CP **non** è supportato da CP (IE) per le CPU ET 200SP.

Accesso al runtime C/C++ della CPU-1518-4 PN/DP MFP attraverso le interfacce X1 o X2

Se si attiva IP Forwarding per la CPU 1518-4 PN/DP MFP, attraverso le interfacce X1 e X2 non si accede soltanto ai dispositivi nella sottorete IP dell'interfaccia X3 ma anche al runtime di C/C++. Dal sistema runtime C/C++ della CPU 1518-4 PN/DP MFP si accede a tutti i dispositivi nelle sottoreti IP delle interfacce X1, X2 e X3.

Condizioni generali:

- L'IP Forwarding è stato attivato per la CPU 1518-4 PN/DP MFP.
- L'indirizzo IP del runtime C/C++ e l'indirizzo IP dell'interfaccia X3 si trovano nella stessa sottorete IP.
- Nel runtime C/C++ sono stati inseriti i percorsi delle sottoreti IP su X1 e X2.
  Per inserire un percorso nel runtime C/C++ utilizzare il comando seguente: "Route add-net <sottorete IP di destinazione> mask <maschera di sottorete> gw <gateway>

La figura seguente illustra una configurazione, nella quale un PC accede al runtime C/C++ della CPU 1518-4 PN/DP MFP tramite l'interfaccia X2.

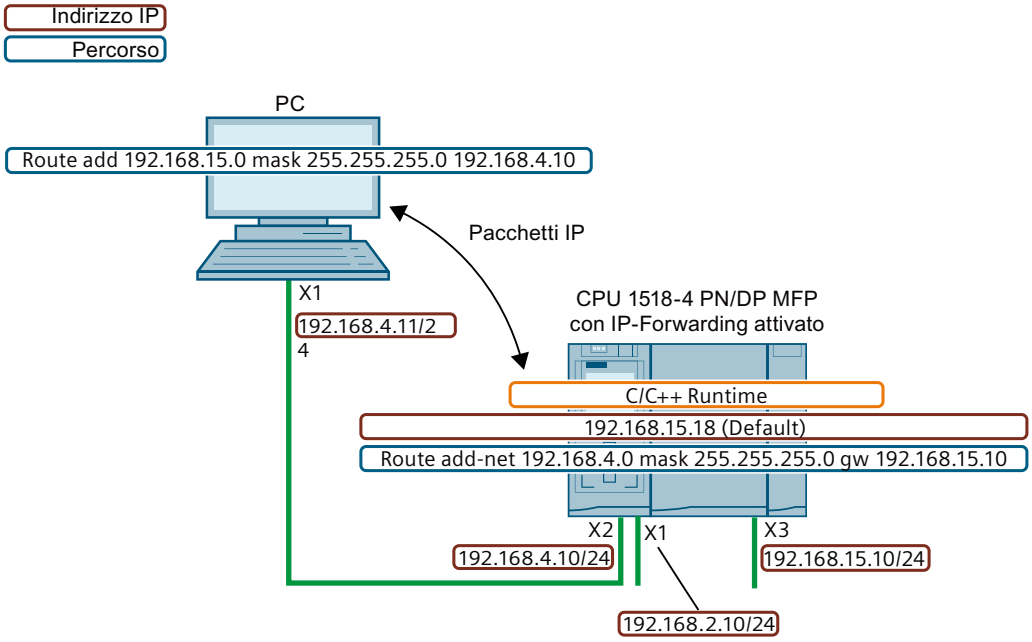


Figura 13-10 Accesso al runtime C/C+ tramite l'interfaccia X2

L'importanza della sicurezza di rete nell'IP Forwarding

Se si attiva l'IP Forwarding per una CPU, si consente l'accesso "dall'esterno" a dispositivi a cui in realtà accede solo la CPU e che solo lei controlla. Di conseguenza, generalmente questi dispositivi non sono protetti dagli attacchi informatici.

La seguente figura spiega come proteggere il sistema di automazione dagli accessi non autorizzati.

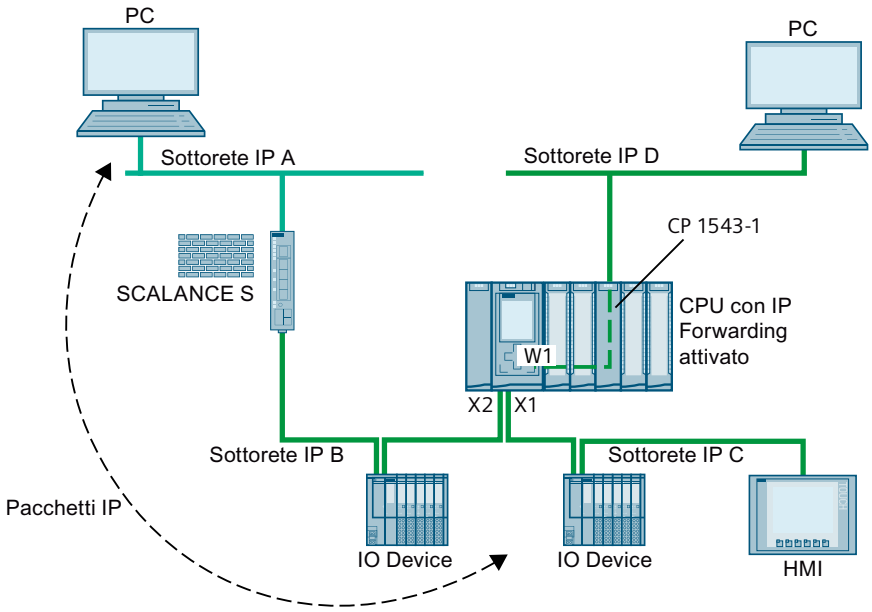


Figura 13-11 La sicurezza di rete nell'IP Forwarding

- La CPU accede attraverso le interfacce X1 e X2 a tutti i dispositivi delle sottoreti IP B e C vicine, di colore verde scuro.
- Nella CPU è integrato un router SCALANCE S. Tramite il router la CPU accede ai dispositivi della sottorete IP più lontana di colore verde chiaro.
- In questo caso nella CPU deve essere attiva, per il CP 1543, la funzione "Accesso al PLC tramite il modulo di comunicazione". Tramite l'interfaccia W1 la CPU accede a tutti i dispositivi della sottorete IP D.

Se nella CPU è attivata la funzione IP Forwarding, un dispositivo che si trovi nella sottorete IP A può accedere a qualsiasi dispositivo delle sottoreti IP B, C e D all'interno della CPU.

È fondamentale proteggere il sistema di automazione e i dispositivi ad esso collegati dall'accesso esterno di utenti non autorizzati.

Separare con un firewall le sottoreti IP vicine alla CPU da quelle più lontane, Per questo scopo utilizzare ad esempio i moduli Security SCALANCE S con firewall integrato.
Per maggiori informazioni su come proteggere una cella di automazione con il Security Module SCALANCE S602 V3 e SCALANCE S623 con firewall integrato consultare questo esempio applicativo (https://support.industry.siemens.com/cs/ww/it/view/22376747).

Attivazione/disattivazione dell'IP Forwarding

Per attivare l'IP Forwarding procedere nel seguente modo:

1. Selezionare la CPU nella vista di rete di STEP 7 (TIA Portal).
2. Nella finestra di ispezione selezionare "Generale" > "Configurazione ampliata" > "IP Forwarding" nelle proprietà della CPU.
3. Attivare la casella di opzione "Attiva IPv4 Forwarding per le interfacce di questi PLC" nell'area "Configurazione IPv4 Forwarding".

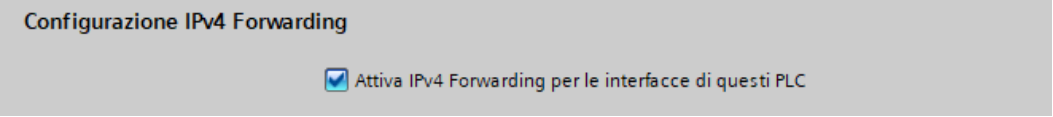


Figura 13-12 Attivazione dell'IP Forwarding

Risultato: l'IP Forwarding è attivo per tutte le interfacce della CPU S7-1500.

Per disattivare l'IP Forwarding fare nuovamente clic sulla casella di opzione "Attiva IPv4 Forwarding per le interfacce di questi PLC".

13.4 Routing dei set di dati

Definizione del routing di set di dati

I dati possono essere inviati alle apparecchiature da campo da una stazione di engineering da PROFINET attraverso diverse reti. Poiché la stazione di engineering accede alle apparecchiature da campo tramite set di dati normalizzati e il routing di questi ultimi avviene tramite dispositivi S7, per questo tipo di routing si è affermata la definizione "routing di set di dati".

I dati inviati tramite il routing dei set di dati contengono, oltre alla parametrizzazione delle apparecchiature da campo interessate (slave DP), anche informazioni specifiche sui dispositivi, p. es. setpoint, valori limite.

Il routing di set di dati viene impiegato ad es. se si utilizzano apparecchiature da campo di diversi produttori. Le apparecchiature da campo vengono indirizzate tramite set di dati normalizzati (PROFINET) per la parametrizzazione e la diagnostica.

Routing di set di dati con STEP 7

STEP 7 consente di eseguire il routing di set di dati richiamando un tool dei dispositivi (ad es. PCT) attraverso l'interfaccia TCI (Tool Calling Interface) e inoltrando i parametri di richiamo. Per la comunicazione con l'apparecchiatura da campo il tool dei dispositivi utilizza gli stessi percorsi di comunicazione impiegati anche da STEP 7.

Questo tipo di routing non richiede alcuna progettazione ma soltanto l'installazione del tool TCI sul computer di STEP 7.

Esempio: Routing di set di dati con Port Configuration Tool (PCT)

Il Port Configuration Tool (PCT) consente la configurazione dei master IO-Link dell'ET200 e la parametrizzazione dei dispositivi IO-Link ad essi collegati. Le sottoreti sono collegate tra loro attraverso router di set di dati. Alcuni router di set di dati sono, ad esempio, CPU, CP, IM e master IO-Link.

Le combinazioni di router di set di dati supportate dal PCT sono indicate in questa FAQ (https://support.industry.siemens.com/cs/it/it/view/87611392).

La figura seguente mostra un esempio di configurazione per il routing di set di dati con PCT.

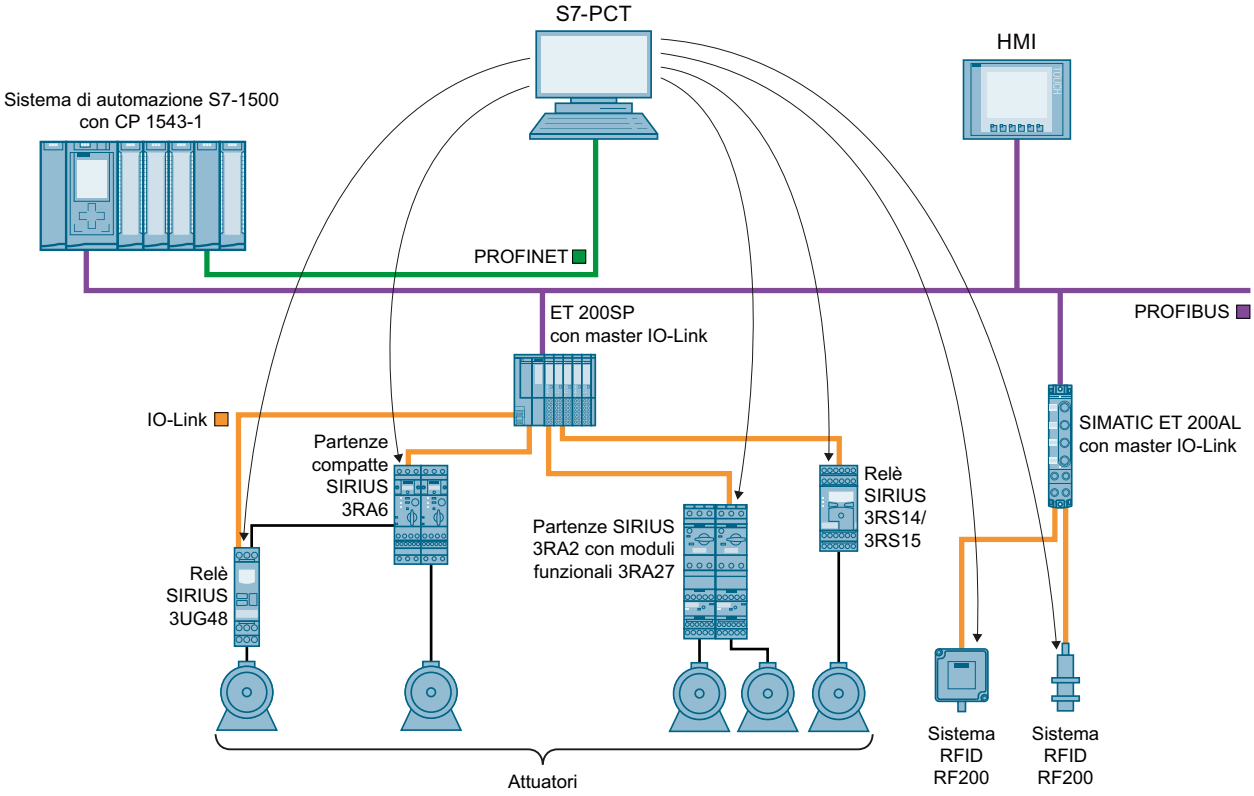


Figura 13-13 Esempio di configurazione per routing di set di dati con PCT

Maggiori informazioni

- La differenza tra routing "normale" e routing "dei set di dati" è descritta nella seguente FAQ (https://support.industry.siemens.com/cs/ww/it/view/7000978).
- Se la CPU utilizzata, il CP o il CM supporta il routing di set di dati, è descritto nei rispettivi manuali del prodotto.
- L'occupazione delle risorse di collegamento per il routing di set di dati è descritta al capitolo Occupazione delle risorse di collegamento (Pagina 440).
- Maggiori informazioni sulla configurazione con STEP 7 sono disponibili nella Guida in linea a STEP 7.

13.5 Interfaccia virtuale per applicazioni basate su IP

Dalla versione firmware 2.8 in poi, la CPU S7-1500 offre la possibilità di accedere all'applicazione basata su IP, come ad es. OPC UA, non solo tramite le interfacce (PN) locali, ma anche tramite le interfacce dei processori di comunicazione nella stessa stazione. I processori di comunicazione supportati sono indicati nell'elenco dei requisiti. Un partner di comunicazione accede a queste applicazioni basate su IP attraverso un'interfaccia virtuale configurabile in TIA Portal a partire dalla versione V16. L'interfaccia virtuale viene denominata W1 (secondo IEC 81346-2).

Caratteristica dell'interfaccia virtuale

L'interfaccia virtuale non è un'interfaccia con capacità diagnostica completa e non presenta le proprietà delle normali interfacce. Nelle viste grafiche l'interfaccia virtuale non viene visualizzata in quanto il collegamento interno tramite il bus backplane non costituisce una sottorete S7 e non dispone di porte. Il collegamento fisico tramite un cavo di rete non è quindi possibile.

L'indirizzo IP dell'interfaccia virtuale viene visualizzato (in TIA Portal, sul display della CPU) e può essere configurato.

L'interfaccia virtuale W1 consente di utilizzare le seguenti opzioni di comunicazione

- OPC UA (client e server)
- Collegamenti OUC programmati
- Comunicazione PG/HMI
- Accessi partner delle CPU S7 tramite istruzioni PUT/GET

L'interfaccia attivata può essere utilizzata nelle finestre di dialogo in cui vengono configurati i collegamenti basati su IP.

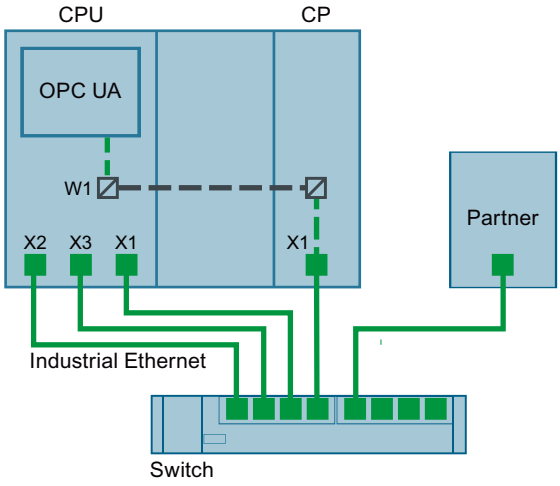


Figura 13-14 Principio dell'interfaccia virtuale

Rispetto alle interfacce convenzionali, l'interfaccia virtuale presenta le seguenti limitazioni:

- Dall'interfaccia virtuale non è possibile accedere al Web server.
- Non è possibile eseguire un backup online attraverso un dispositivo di programmazione collegato con TIA Portal.
- Se la CPU e il partner di comunicazione sono collegati tra loro attraverso l'interfaccia virtuale, non possono scambiarsi dati tramite LLDP (Link Layer Discovery Protocol).
- Il servizio di routing S7 non utilizza l'interfaccia W1.

Presupposti

Per garantire l'accessibilità di un servizio della CPU attraverso l'interfaccia Ethernet di un CP sono necessari i presupposti seguenti:

- CPU S7-1500 dalla versione firmware V2.8
- CP 1543-1 dalla versione firmware V2.2

Suggerimento: Utilizzare un CP 1543-1 dalla versione firmware V3.0. A partire da questa versione, le funzioni Security (firewall) sono disponibili anche per l'interfaccia virtuale rendendo superflua l'installazione di un firewall supplementare tra la stazione e la rete non sicura.

Configurazione dell'interfaccia W1 virtuale

Nelle proprietà di una CPU S7-1500 con firmware V2.8 o superiore è possibile selezionare l'opzione "Configurazione avanzata > Accesso al PLC tramite il modulo di comunicazione" e assegnare all'interfaccia virtuale W1 un modulo di comunicazione innestato. Da quest'ultimo sarà poi possibile accedere alla CPU dall'esterno. Se non sono stati inseriti CP, o se i CP inseriti non supportano l'accesso alla CPU, questa casella di scelta è vuota.

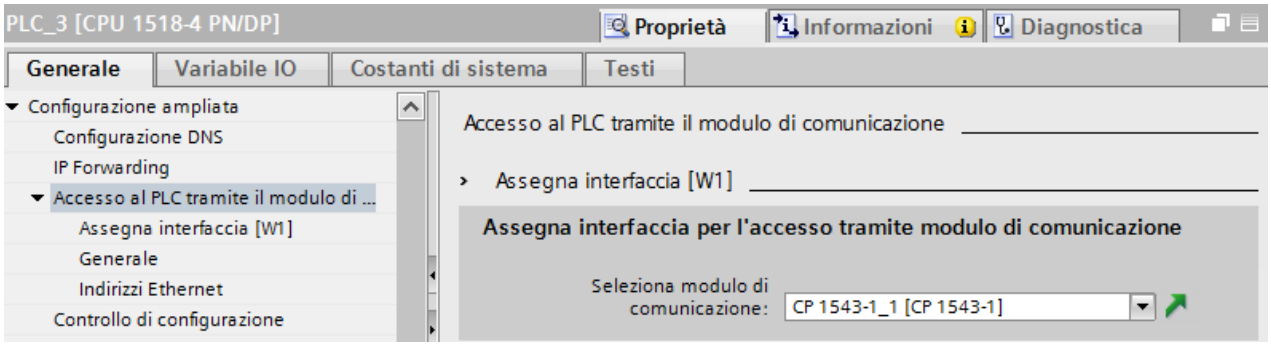


Figura 13-15 Selezione della CPU nelle proprietà della stessa

Dopo la selezione del CP vengono visualizzati i dati e i parametri dell'interfaccia virtuale. Qui si possono modificare le impostazioni per il protocollo IP e i parametri PROFINET:

- La sottorete IP può essere scelta liberamente come per il CP. Per inserire la sottorete IP si utilizzano la maschera di sottorete e l'indirizzo IP dell'interfaccia virtuale.
- Nell'inserire la sottorete IP per l'interfaccia virtuale fare attenzione a non utilizzare la stessa sottorete IP delle interfacce locali della CPU.

Dopo essere stato inserito, l'indirizzo IP è visibile nella finestra di dialogo delle proprietà del server OPC UA, nell'elenco degli indirizzi del server. Con queste impostazioni si definisce la nuova interfaccia virtuale W1 per la CPU attraverso la quale è possibile accedere ai servizi della CPU sopra descritti, quali il server OPC UA, mediante un modulo di comunicazione. I collegamenti creati e la comunicazione S7 (ad es. HMI e BSEND, BRCV) passano da quest'interfaccia. Il server OPC UA non consente di selezionare un'interfaccia specifica (selezione dell'indirizzo IP), si possono selezionare tutte le interfacce o nessuna.

NOTA

L'indirizzo IP dell'interfaccia virtuale non è elencato come W1 nel display del dispositivo sotto le interfacce (Xn) locali attualmente visualizzate, bensì alla voce "Indirizzi" nella sezione "Impostazioni": L'interfaccia virtuale è visibile anche quando non è attivata o non è inserito alcun CP. In assenza di una IP Suite, gli indirizzi IP e la maschera di sottorete hanno il valore 0.0.0.0.

Se si modificano i parametri dell'indirizzo IP dell'interfaccia virtuale già configurati e caricati tramite display, l'istruzione T_CONFIG oppure online, la configurazione caricata sarà nuovamente attiva dopo il riavvio della CPU.

Modifiche della configurazione nel CP

La modifica del modulo di comunicazione assegnato può influire sulla configurazione dell'interfaccia virtuale:

- Nelle proprietà del CPU:
  - Assegnazione di un altro CP: la configurazione viene acquisita per il nuovo CP.
  - Deselezione del CP assegnato: l'interfaccia virtuale W1 viene disattivata e la configurazione viene eliminata.
    Se il CP viene nuovamente assegnato la configurazione deve essere reimpostata.
- Sul dispositivo:
  - Spostamento del CP: se il CP viene soltanto spostato in un altro posto connettore del dispositivo, la configurazione rimane valida.
  - Rimozione del CP: se il CP viene cancellato o spostato in un altro dispositivo, la configurazione viene mantenuta. Nella casella di riepilogo della CPU il CP viene visualizzato come mancante e la compilazione della configurazione segnala un errore. Per eliminare l'errore si può deselezionare il CP o assegnare un altro CP.

Visualizzazione della diagnostica e delle costanti di sistema

L'interfaccia W1 virtuale viene visualizzata nella vista di diagnostica alla voce "Online & diagnostica". Nelle proprietà della CPU, l'identificazione hardware dell'interfaccia virtuale viene visualizzata nelle costanti di sistema.

Impostazioni nel modulo di comunicazione (CP 1543-1 dalla versione FW V3.0)

Dalla versione firmware V3.0, per garantire la sicurezza del traffico dati tramite l'interfaccia virtuale è possibile utilizzare il firewall interno del CP. Per attivare il firewall nel modulo di comunicazione, nel progetto protetto procedere come indicato nel seguito:

1. Nell'area di lavoro di STEP 7 selezionare il modulo di comunicazione.
2. Nella finestra di ispezione selezionare "Proprietà > Security".
3. Attivare l'opzione "Attiva funzioni Security".
   Le funzioni Security configurabili vengono ora visualizzate nella finestra di ispezione.
4. Attivare l'opzione "Attiva firewall".
   Nella finestra di ispezione ora è possibile consentire l'uso dell'interfaccia virtuale W1.

La sicurezza del traffico dati tramite l'interfaccia virtuale W1 della CPU può essere garantita soltanto per il servizio OPC UA.

NOTA

Verifica della configurazione manuale

Se il firewall è attivo, è necessario verificare manualmente se i servizi richiesti vengono ammessi dal firewall. Per i filtri IP e MAC attivare soltanto i servizi ai quali si intende accedere anche dall'interfaccia CP. Osservare le avvertenze relative alle impostazioni di sicurezza e alle regole del firewall dei CP S7-1500 riportate nel sistema di informazione di TIA Portal.

Impostazioni nel modulo di comunicazione (CP 1543-1, versione FW V2.2, < V3.0)

Le funzioni Security del CP 1543-1 con versione firmware inferiore alla V3.0 non sono in grado di garantire la sicurezza del traffico dati tramite l'interfaccia virtuale. In TIA Portal l'attivazione delle funzioni Security è possibile, ma questa configurazione non può essere compilata.

ATTENZIONE

Collegamento con reti non sicure

Se si collega il CP con una rete che non è sicura, è necessario inserire un ulteriore firewall tra il CP e tale rete. Utilizzare ad esempio i Security Module SCALANCE S602 V3 e SCALANCE S623 con firewall integrato.

Risorse di collegamento 14

14.1 Risorse di collegamento di una stazione

Introduzione

Alcuni servizi di comunicazione necessitano di collegamenti. I collegamenti occupano risorse nel sistema di automazione (stazione). Le risorse di collegamento vengono messe a disposizione della stazione dalle CPU, dai processori di comunicazione (CP) e dai moduli di comunicazione (CM).

Risorse di collegamento di una stazione

Le risorse di collegamento disponibili dipendono dalle CPU, dai CP e dai CM utilizzati e non devono superare un numero max. per stazione.

Il numero max. di risorse di una stazione è determinato dalla CPU.

Risorse di collegamento riservate

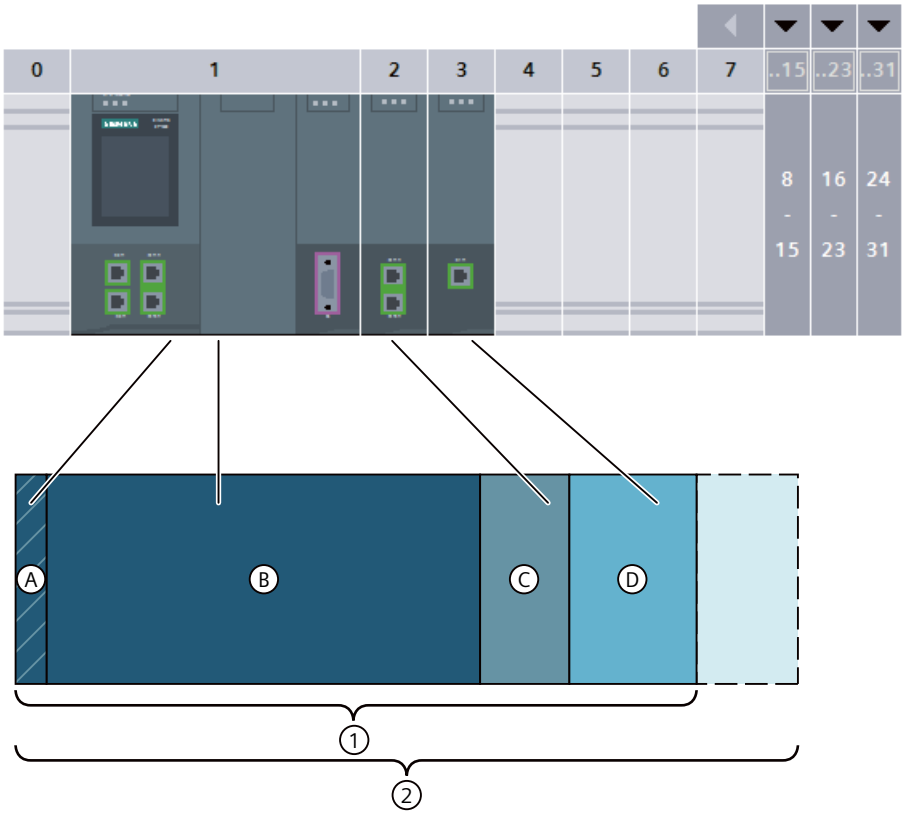
Ogni CPU è dotata di risorse di collegamento riservate per la comunicazione PG, HMI e Web server. Ciò garantisce ad es. che un PG può sempre creare almeno un collegamento online con la CPU, indipendentemente da quanti servizi di comunicazione occupano già le risorse di collegamento.

Risorse di collegamento dinamiche

Inoltre sono disponibili risorse dinamiche. La differenza tra il numero max. di risorse di collegamento e il numero di risorse di collegamento riservate è il numero max. di risorse di collegamento dinamiche.

Il pool delle risorse di collegamento dinamiche serve per i servizi di comunicazione PG, comunicazione HMI, comunicazione S7, Open User Communication, comunicazione web, comunicazione client/server OPC UA e altri.

La figura seguente mostra ad es. come i singoli componenti mettono le risorse di collegamento a disposizione di una stazione S7-1500.



① Risorse di collegamento disponibili della stazione, di cui

- A Risorse di collegamento riservate della stazione
- A + B Risorse di collegamento della CPU 1518
- C Risorse di collegamento del modulo di comunicazione CM 1542-1
- D Risorse di collegamento del processore di comunicazione CP 1543-1

② Risorse di collegamento max. della stazione ad es. in una configurazione con CPU 1518, CM 1542-1 e CP 1543-1

Figura 14-1 Risorse di collegamento di una stazione

Numero delle risorse di collegamento di una stazione

Tabella 14-1 N° max. di risorse di collegamento supportate per alcuni tipi di CPU

Risorse di collegamento di una stazione		**1511C**	**1511 1512C 1513**	**1515 1516**	**1517**	**1518**
Risorse di collegamento max. della stazione		96	128	256	320	384
	di cui riservate	10				
	di cui dinamiche	86	118	246	310	374

Risorse di collegamento di una stazione	1511C	1511 1512C 1513	1515 1516	1517	1518
Risorse di collegamento della CPU	64	88	128	288	320
Risorse di collegamento max. utilizzabili ulteriormente con l'inserimento di CM/CP	32	40	128	32	64
Risorse di collegamento supplementari CM 1542-1	64				
Risorse di collegamento supplementari CP 1543-1	118				
Risorse di collegamento supplementari CM 1542-5	48				
Risorse di collegamento supplementari CP 1542-5	16				

Il numero delle risorse di collegamento supportate da una CPU o da un modulo di comunicazione è riportato nei dati tecnici del manuale del prodotto.

Esempio

È stata configurata una CPU 1516-3 PN/DP con un modulo di comunicazione CM 1542-1 e un processore di comunicazione CP 1542-5.

- Risorse di collegamento max. della stazione: **256**
- Risorse di collegamento disponibili:
  - CPU 1516-3 PN/DP: 128
  - CM 1542-1: 64
  - CP 1542-5: 16
  - Totale: **208**

La struttura mette a disposizione 208 risorse di collegamento. Se si inseriscono ulteriori moduli di comunicazione la stazione può supportare max. 48 ulteriori risorse di collegamento.

Risorse di collegamento riservate

Per le stazioni con CPU S7-1500, ET 200SP ed ET 200pro basate su S7-1500 sono riservare 10 risorse di collegamento:

- 4 per la comunicazione PG, che STEP 7 impiega ad es. per funzioni di test e di diagnostica o per il caricamento nella CPU
- 4 per la comunicazione HMI, che vengono occupate dai primi collegamenti HMI progettati in STEP 7
- 2 per la comunicazione con il Web server

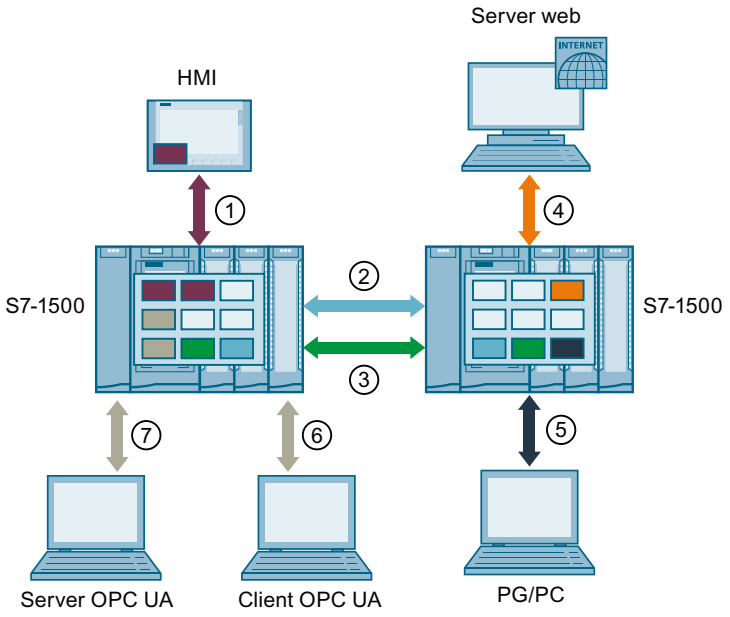
Ulteriori informazioni

Per informazioni sulle risorse di collegamento dei sistemi ridondanti S7-1500R/H consultare il capitolo Risorse di collegamento del sistema ridondante S7-1500R/H (Pagina 467).

14.2 Occupazione delle risorse di collegamento

Panoramica dell'assegnazione delle risorse di collegamento

La figura seguente mostra come diversi collegamenti occupino le risorse dell'S7-1500.



① Comunicazione HMI: vedere oltre

② Open User Communication: i collegamenti della Open User Communication occupano una risorsa di collegamento in ogni punto finale.

③ Comunicazione S7: i collegamenti della comunicazione S7 occupano una risorsa di collegamento in ogni punto finale.

④ Comunicazione Web: il collegamento del Web server occupa almeno una risorsa di collegamento nella stazione. Il numero dei collegamenti utilizzati dipende dal browser.

⑤ Comunicazione PG: Il collegamento PG occupa una risorsa di collegamento nella stazione.

⑥ Comunicazione server/client OPC UA: Per l'assegnazione delle risorse di collegamento nel server vedere più sotto

⑦ Comunicazione server/client OPC UA: Per l'assegnazione delle risorse di collegamento nel Client vedere più sotto

Risorsa di collegamento per la comunicazione HMI

Risorsa di collegamento per la comunicazione OpenUser

Risorsa di collegamento per la comunicazione S7

Risorsa di collegamento per la comunicazione web

Risorsa di collegamento per la comunicazione PG

Risorsa di collegamento per la comunicazione client/server OPC UA

Figura 14-2 Occupazione delle risorse di collegamento

Risorse di collegamento per la comunicazione HMI

Nella comunicazione HMI, l'occupazione delle risorse di collegamento nella stazione dipende dal dispositivo HMI in uso.

Tabella 14-2 N° max. di risorse di collegamento occupate per diversi dispositivi HMI

Dispositivo HMI	N° max. di risorse di collegamento della stazione occupate per ogni collegamento HMI
Basic Panel	1
Unified Basic Panel	3
Comfort Panel	2[1]
Unified Comfort Panel	3
Mobile Panel	2[1]
RT Advanced	2[1]
RT Professional	3
Unified PC	3

[1] Se non si utilizza la diagnostica di sistema né la progettazione di messaggi, la stazione occupa una sola risorsa per collegamento HMI.

Esempio: per una CPU 1516-3 PN/DP sono stati configurati i seguenti collegamenti HMI:

- Due collegamenti HMI a un HMI TP700 Comfort (2 risorse di collegamento ciascuno)
- Un collegamento HMI a un HMI KTP1000 Basic (1 risorsa di collegamento)

Nella CPU vengono occupate complessivamente 5 risorse di collegamento per la comunicazione HMI.

Risorsa di collegamento per la comunicazione client OPC UA

Ogni collegamento stabilito dal client OPC UA della CPU con un server OPC UA occupa una risorsa di collegamento nella stazione.

Durante la creazione e l'interruzione di un collegamento OPC UA, il client OPC UA occupa temporaneamente un'ulteriore risorsa di collegamento. Secondo RFC 793, questa risorsa di collegamento viene nuovamente resa disponibile dopo un intervallo di attesa di circa 60 secondi.

NOTA

Carenza di risorse a causa delle risorse di collegamento temporanee

Una carenza di risorse di collegamento può verificarsi nel caso seguente:

- Il client OPC UA stabilisce o interrompe più collegamenti contemporaneamente.
- Il numero delle risorse di collegamento disponibili della stazione non è sufficiente per le risorse di collegamento permanenti e temporanee della comunicazione client OPC UA.

Assicurarsi che nella stazione sia sempre disponibile un numero sufficiente di risorse di collegamento per stabilire e interrompere i collegamenti OPC UA.

Provvedimenti:

- Progettare un numero sufficiente di risorse per i collegamenti client OPC UA.
- Eventualmente stabilire o interrompere i collegamenti OPC UA in successione.

Risorse di collegamento per il routing

Per la trasmissione dei dati oltre le sottoreti S7 ("Routing S7") viene creato un collegamento S7 tra due CPU. Le sottoreti S7 sono collegate tra loro tramite accoppiamenti ad altra rete, i cosiddetti router S7. CPU, CM e CP nell'S7-1500 sono router S7.

Per un collegamento S7 con routing vale quanto segue:

- Un collegamento con routing occupa una risorsa in ciascuno dei punti finali; in STEP 7 queste risorse di collegamento sono visualizzate nella tabella "Risorse di collegamento".
- Nel router S7 vengono occupate due risorse di collegamento speciali per il routing S7. In STEP 7 le risorse di collegamento speciali per il routing S7 non sono visualizzate nella tabella "Risorse di collegamento". Il numero di risorse per il routing S7 dipende dalla CPU. Le risorse per il routing S7 si trovano nei dati tecnici della CPU nella sezione "Numero di collegamenti S7-Routing".

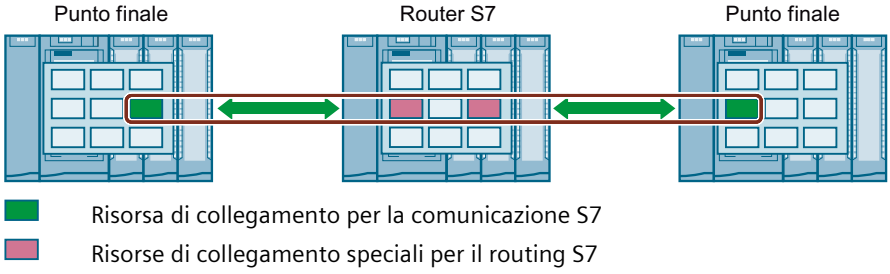


Figura 14-3 Risorse di collegamento per routing S7

Anche il routing di set di dati consente di trasferire dati oltre le sottoreti S7, da una stazione di engineering collegata a PROFINET a diverse apparecchiature da campo attraverso PROFIBUS.

Come per il routing S7, anche per il routing dei set di dati vengono occupate in ogni router dei set di dati due delle risorse di collegamento speciali per il routing S7.

NOTA

Risorse di collegamento nel routing di set di dati

Per il routing dei set di dati, nel router del set di dati vengono occupate due risorse di collegamento speciali per il routing S7. Nella tabella delle risorse di collegamento non figurano né il collegamento al set di dati né le risorse di collegamento occupate.

Quando vengono occupate le risorse di collegamento?

Il momento in cui vengono occupate le risorse di collegamento dipende da come è configurato il collegamento. (Vedere il capitolo Configurazione di un collegamento (Pagina 49)).

- **Configurazione programmata di un collegamento**:
  viene occupata una risorsa di collegamento non appena nel programma utente della CPU si richiama un'istruzione per creare un collegamento (TSEND_C/TRCV_C o TCON).

  Parametrizzando opportunamente il parametro CONT delle istruzioni TSEND_C/TRCV_C o richiamando l'istruzione TDISCON è possibile interrompere il collegamento dopo la trasmissione dei dati e abilitare la risorsa di collegamento. Un volta interrotto il collegamento, le relative risorse sono di nuovo disponibili nella CPU/nel CP/CM.
- **Collegamenti configurati** (ad es. collegamento a S7):
  se si configura un collegamento in STEP 7 la risorsa viene occupata non appena si carica la configurazione hardware nella CPU.

  I collegamenti progettati non vengono interrotti dopo che sono stati utilizzati per il trasferimento dei dati. La risorsa di collegamento rimane occupata in modo permanente. Per riabilitarla è necessario cancellare il collegamento progettato in STEP 7 e caricare la progettazione modificata nella CPU.
- **Collegamento PG**:
  le risorse di collegamento vengono occupate non appena si collega il PG a una CPU online in STEP 7.
- **Server Web**:
  finché il Web server di una CPU è aperto in un browser, nella CPU vengono occupate delle risorse di collegamento.
- **Server OPC UA**

  Ogni collegamento al server OPC UA della CPU occupa una risorsa di collegamento nella stazione. Questa risorsa di collegamento è di nuovo libera non appena il collegamento viene disattivato.

- **Client OPC UA**

  Ogni collegamento creato dal client OPC UA della CPU con un server OPC UA occupa una risorsa di collegamento nella stazione. Durante la creazione di un collegamento OPC UA, il client OPC UA occupa temporaneamente un'ulteriore risorsa di collegamento. Durante la disattivazione di un collegamento OPC UA questa risorsa di collegamento viene resa nuovamente libera, secondo RFC 793, dopo un tempo di attesa di ca. 60 s.

Controllo del numero massimo possibile di risorse di collegamento

Offline

STEP 7 controlla l'occupazione delle risorse di collegamento durante la configurazione dei collegamenti. STEP 7 segnala con un opportuno avviso il superamento del numero max. possibile di risorse di collegamento.

Online

La CPU controlla il consumo delle risorse di collegamento nel sistema di automazione. Se si creano più collegamenti nel programma utente di quante siano le risorse messe a disposizione dal sistema di automazione, la CPU conferma con un errore l'istruzione per la creazione del collegamento.

Confronto tra S7-1500 e S7-300

Un confronto sulla gestione delle risorse di comunicazione dell'S7-1500 e dell'S7-300 si trova in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/109747092).

14.3 Visualizzazione delle risorse di collegamento

Visualizzazione delle risorse di collegamento in STEP 7 (vista offline)

Le risorse di collegamento di un sistema di automazione possono essere visualizzate nella configurazione hardware. Queste risorse si trovano nella finestra di ispezione, nelle proprietà della CPU.

Risorse di collegamento

	① Risorse della stazione			② Risorse del mo...	Risorse del mo...	Risorse del mo...
	Riservate		Dinamiche	PLC_1 [CPU 15...	CM 1542-1_1 [..	CP 1543-1_1 [...
Numero max. di risorse:		10	246	128	64	118
	Max.	Configurate	Configurate	Configurate	Configurate	Configurate
Comunicazione PG:	4	-	-	-	-	-
Comunicazione HMI:	4	4	6	6	0	4
Comunicazione S7:	0	-	7	4	3	0
Open User Communication:	0	-	13	8	5	0
Comunicazione Web:	2	-	-	-	-	-
Comunicazione Client/Server OPC UA:	0	-	-	-	-	-
Altri tipi di comunicazione:	-	-	0	0	0	0
Risorse totali utilizzate:		4	26	18	8	4
Risorse disponibili:		6	220	110	56	114

Figura 14-4 Esempio: Risorse di collegamento riservate e disponibili (vista offline)

① Risorse di collegamento specifiche della stazione

Le colonne delle risorse di collegamento specifiche della stazione forniscono informazioni sulle risorse di collegamento in uso e quelle disponibili della stazione.

Nell'esempio sono disponibili per il sistema di automazione max. 256 risorse di collegamento specifiche della stazione.

- 10 risorse di collegamento riservate, di cui 4 sono già in uso e 6 ancora disponibili.
  Le risorse impiegate si suddividono come segue:
  - 4 risorse per la comunicazione HMI
- 246 risorse di collegamento dinamiche, di cui 26 sono già in uso e 220 ancora disponibili.
  Le risorse impiegate si suddividono come segue:
  - 6 risorse per la comunicazione HMI
  - 7 risorse per la comunicazione S7
  - 13 risorse per la Open User Communication

Poiché la somma delle risorse massime di collegamento disponibili di CPU, CP e CM (= 310 risorse di collegamento) supera il limite della stazione di 256, nella colonna delle risorse dinamiche della stazione è visualizzato un triangolo di segnalazione.

NOTA

Superamento delle risorse di collegamento disponibili

Il superamento delle risorse di collegamento specifiche della stazione viene segnalato da STEP 7 con un avviso. Per poter utilizzare tutte le risorse di collegamento disponibili di CPU, CP e CM è necessario utilizzare una CPU con un numero massimo di risorse di collegamento disponibili specifiche della stazione maggiore oppure ridurre il numero dei collegamenti di comunicazione.

---

① Risorse di collegamento specifiche del modulo

Le colonne delle risorse di collegamento specifiche del modulo forniscono informazioni sull'utilizzo delle risorse nelle CPU, nei CP e nei CM di un sistema di automazione.

La visualizzazione è granulare per modulo e non per interfaccia.

Nell’esempio la CPU mette a disposizione al massimo 128 risorse di collegamento dinamiche, di cui 18 già in uso e 110 ancora disponibili.
Le risorse impiegate si suddividono come segue:

- 6 risorse per la comunicazione HMI
- 4 risorse per la comunicazione S7
- 8 risorse per la Open User Communication

Visualizzazione delle risorse di collegamento in STEP 7 (vista online)

Se si è collegati online con la CPU, è possibile visualizzare in "Informazione sul collegamento" anche il numero delle risorse in uso al momento.

Proprietà | Informazioni | Diagnostica

Informazione sui dispositivi | Informazione sul collegamento | Vista di messaggi

Risorse di collegamento

	Risorse della stazione					Risorse del modulo	
		Riservate		Dinamiche		CPU 1516-3 PN/DP (R0/S1)	
Numero max. di risorse:		10	10	194	194	86	86
	Max.	Configurate	Utilizzate	Configurate	Utilizzate	Configurate	Utilizzate
Comunicazione PG:	4	-	4	-	0	-	0
Comunicazione HMI:	4	4	4	4	4	8	8
Comunicazione S7:	0	-	0	72	68	34	34
Open User Communication:	0	-	0	118	118	45	45
Comunicazione Web:	2	-	0	-	0	-	0
Comunicazione Client/Server OPC ...	0	-	0	-	0	-	0
Altri tipi di comunicazione:	-	-	0	0	0	0	0
Risorse totali utilizzate:		4	8	194	190	82	82
Risorse disponibili:		6	0	0	4	4	4

Figura 14-5 Risorse di collegamento - online

La vista online della tabella "Risorse di collegamento" contiene, oltre alla vista offline, delle colonne con le risorse di collegamento attualmente in uso. Nella vista online vengono visualizzate **tutte** le risorse di collegamento utilizzate nel sistema di automazione, indipendentemente da come è stato configurato il collegamento.

Nella riga "Altri tipi di comunicazione" vengono visualizzate le risorse di collegamento occupate per la comunicazione con dispositivi di terze parti. La tabella viene aggiornata automaticamente.

NOTA

Se un collegamento S7 con routing passa attraverso una CPU, le risorse di collegamento necessarie della CPU non vengono indicate nella tabella delle risorse!

Visualizzazione delle risorse di collegamento per HMI

Le informazioni sulla disponibilità e l'assegnazione delle risorse per i collegamenti HMI sono riportate nella vista offline nel contesto del dispositivo HMI (nella finestra di ispezione, nelle proprietà nel campo “Risorse di collegamento”).

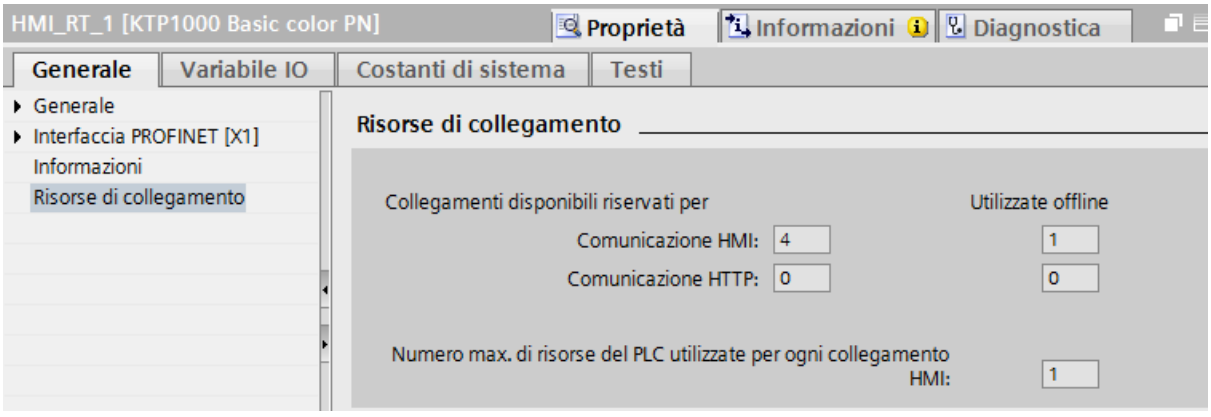


Figura 14-6 Risorse di collegamento - comunicazione HMI

Nell'area delle risorse di collegamento vengono visualizzati:

- Numero di collegamenti in HMI riservati per la comunicazione HMI e HTTP
- Numero delle risorse di collegamento offline utilizzate in HMI per la comunicazione HMI e HTTP

  Se si supera il numero massimo di risorse di collegamento disponibili per un dispositivo HMI, STEP 7 emette una segnalazione.
- “Numero max. di risorse del PLC utilizzate per ogni collegamento HMI” Questo parametro è un fattore che deve essere moltiplicato per il numero dei collegamenti HMI utilizzati offline. Il prodotto fornisce il numero delle risorse HMI occupate nella CPU.

Visualizzazione delle risorse di collegamento nel server Web

È possibile visualizzare le risorse di collegamento in STEP 7 ma anche con un browser che mostra la pagina corrispondente del server Web.

Per informazioni sulla visualizzazione delle risorse di collegamento sul server web consultare il manuale di guida alle funzioni Server web (https://support.industry.siemens.com/cs/it/it/view/59193560).

Diagnostica ed eliminazione di guasti 15

15.1 Diagnostica dei collegamenti

Tabella dei collegamenti nella vista online

Per una CPU selezionata nell'editor hardware e di rete di STEP 7 viene visualizzato, nella vista online, lo stato dei collegamenti.

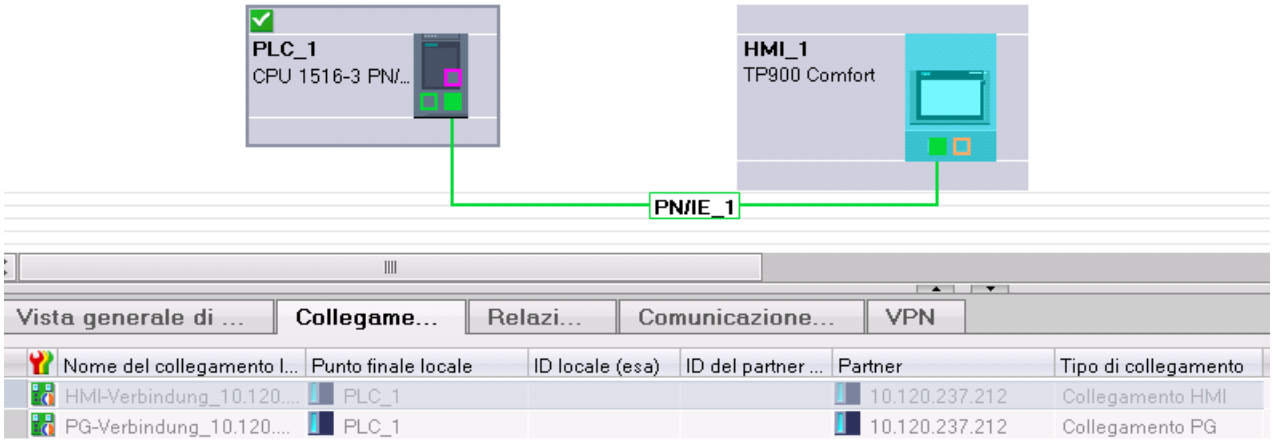


Figura 15-1 Vista online della tabella dei collegamenti

Nella scheda "Informazione sul collegamento" sono disponibili informazioni di diagnostica dettagliate per il collegamento selezionato nella tabella dei collegamenti.

Scheda "Informazione sul collegamento": Dettagli del collegamento

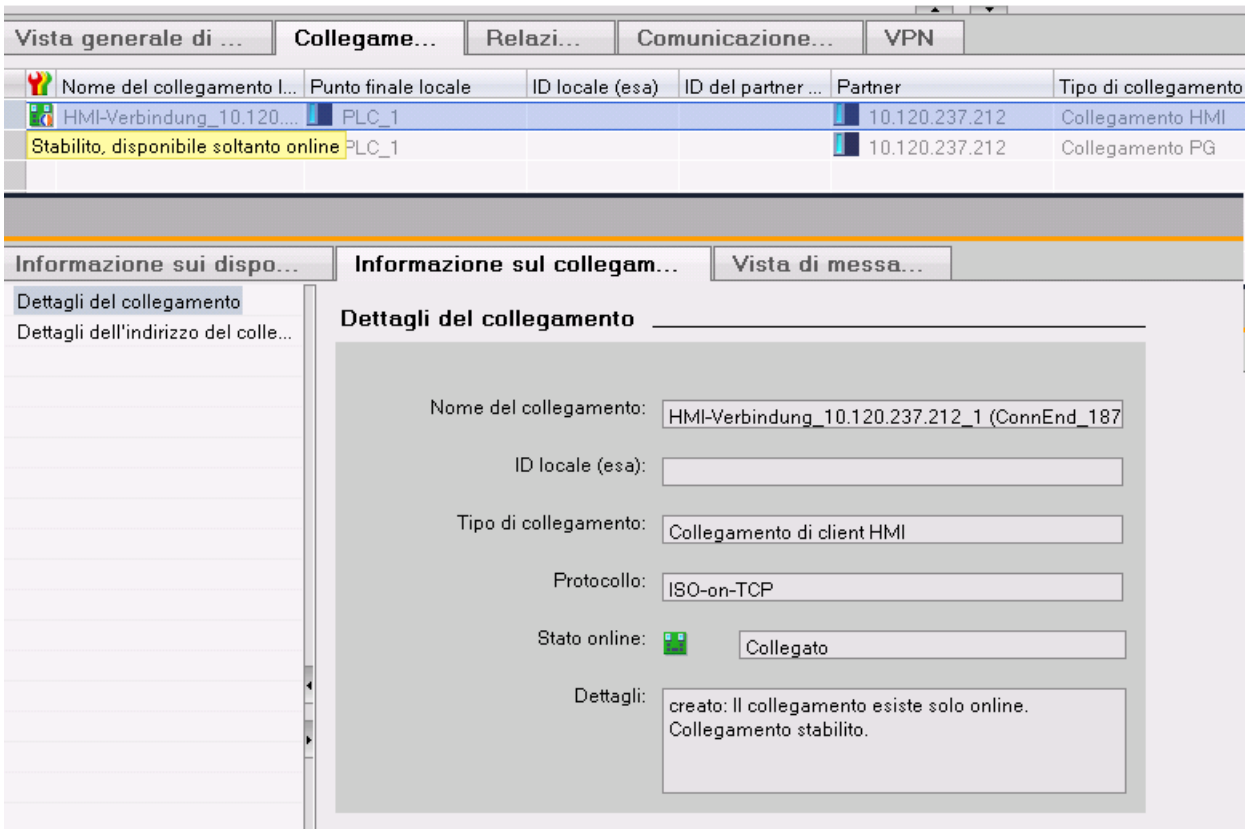


Figura 15-2 Diagnostica dei collegamenti - Dettagli del collegamento

Scheda "Informazione sul collegamento": Dettagli dell'indirizzo

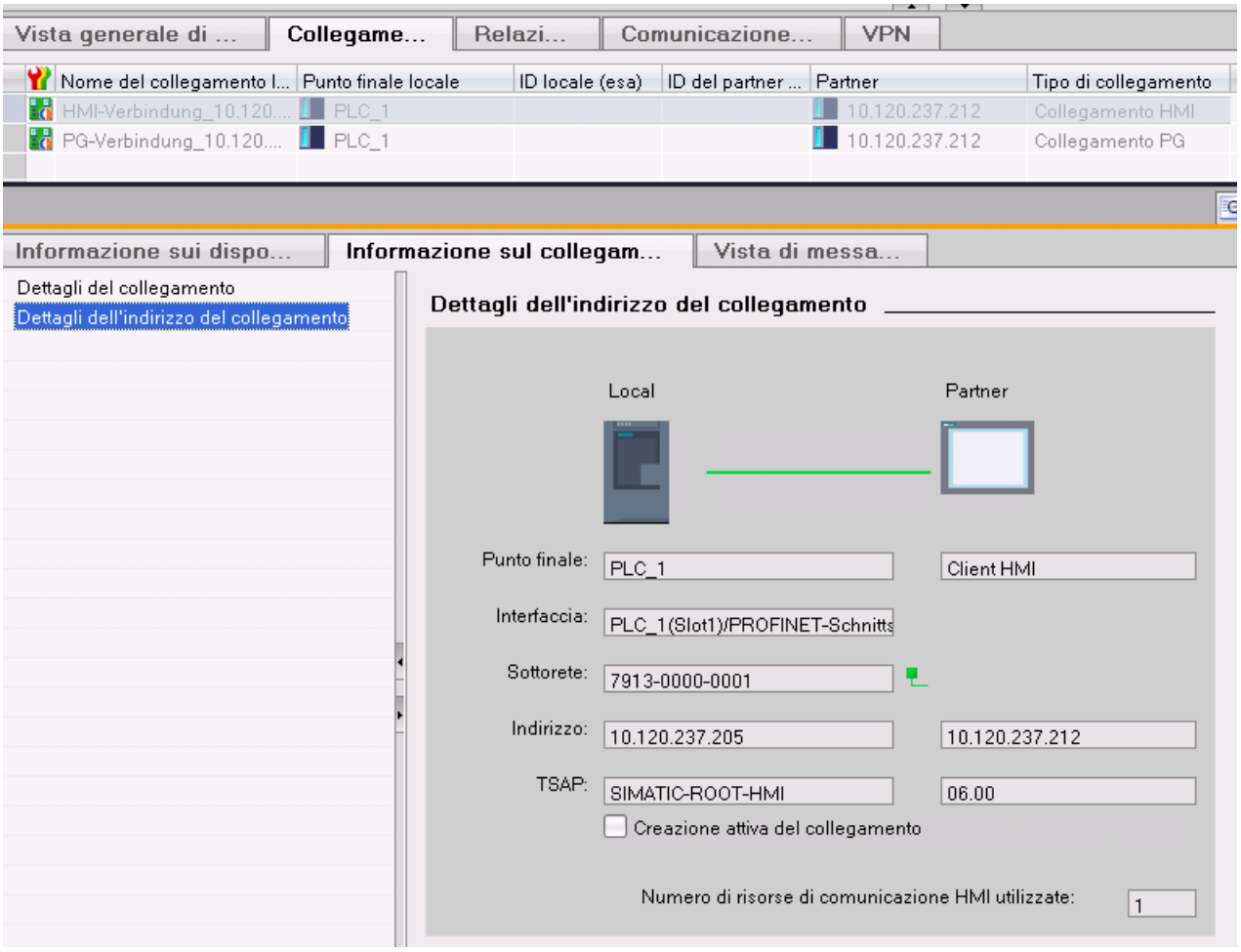


Figura 15-3 Diagnostica dei collegamenti - Dettagli dell'indirizzo

Diagnostica tramite Web server

Con il Web server integrato di una CPU è possibile analizzare le informazioni di diagnostica della CPU mediante un browser Web.

La pagina Web "Comunicazione" contiene varie schede con informazioni dettagliate sulla comunicazione tramite PROFINET:

- Informazioni sulle interfacce PROFINET della CPU (ad es. indirizzi, sottoreti, proprietà fisiche)
- Informazioni sulla qualità della trasmissione dati (ad es. num di pacchetti di dati inviati/ricevuti correttamente)
- Informazioni sull'occupazione/disponibilità delle risorse di collegamento
- La pagina "Stato del collegamento" è simile alla vista online di STEP 7 e fa un riepilogo dei collegamenti e dei relativi dettagli

Diagnostica tramite il programma utente

Se si programma l'istruzione T_DIAG, è possibile analizzare le informazioni di diagnostica relative ai collegamenti progettati e programmati dalla CPU mediante il programma utente.

Ulteriori informazioni

La descrizione delle funzionalità del Web server è disponibile nel manuale di guida alle funzioni Server web (https://support.industry.siemens.com/cs/it/it/view/59193560).

15.2 Indirizzo d'emergenza

Se la CPU non è accessibile dall'indirizzo IP, è possibile impostare, per questa CPU, un indirizzo di emergenza temporaneo (Emergency IP). Dall'indirizzo di emergenza è possibile ripristinare il collegamento con la CPU per il caricamento della configurazione del dispositivo con un indirizzo IP valido.

L'indirizzo di emergenza può essere impostato a prescindere dal livello di protezione della CPU

Quando si necessita di un indirizzo di emergenza?

La CPU non è accessibile nei seguenti casi:

- Indirizzo IP dell'interfaccia PROFINET è stato assegnato due volte.
- L’impostazione della maschera di sottorete è errata.

Presupposti

- Per il protocollo IP, nella configurazione dispositivi in STEP 7 deve essere stata selezionata l'opzione "Imposta indirizzo IP nel progetto".
- Non è stata caricata nessuna progettazione con protezione in scrittura DCP attivata.
- La CPU deve trovarsi nello stato di funzionamento STOP.

Ripristino della configurazione valida con un indirizzo di emergenza

1. Con un tool DCP impostare l'indirizzo di emergenza per l'interfaccia della CPU. SIMATIC Automation Tool dispone ad esempio del comando DCP "Definisci indirizzo IP".
   Il LED di manutenzione della CPU è acceso. Anche il buffer di diagnostica indica l'attivazione di un indirizzo di emergenza per l'interfaccia Ethernet.
2. Caricare nella CPU un progetto STEP 7 con un indirizzo IP valido.
3. Disinserire e reinserire la CPU.
   L'indirizzo di emergenza è stato resettato.

Risultato

La CPU opera con l'indirizzo IP valido.

Comunicazione con il sistema ridondante S7-1500R/H

16

Introduzione

La comunicazione con il sistema ridondante S7-1500R/H funziona fondamentalmente come nei sistema standard S7-1500.

Questo capitolo descrive le particolarità e le limitazioni per la comunicazione con il sistema ridondante S7-1500R/H.

Possibilità di comunicazione per il sistema ridondante S7-1500R/H

- Open User Communication tramite TCP/IP, UDP, ISO-on-TCP e Modbus/TCP
- Secure Open User Communication ad eccezione della funzione "Secure OUC tramite e-mail" (vedere anche Secure Open User Communication (Pagina 94))
- Comunicazione S7 come server
- Comunicazione HMI, comunicazione PG
- Scambio dati tramite OPC UA come server
- Comunicazione Secure PG/HMI (vedere anche Comunicazione PG/HMI sicura (Pagina 112))
- SNMP
- Sincronizzazione dell'ora tramite NTP
- Web server (solo tramite API web)
- Supporto del processore di comunicazione CP 1543-1 come modulo centrale fisso (vedere anche il manuale di sistema S7-1500R/H (https://support.industry.siemens.com/cs/it/it/view/109754833))

Limitazioni per la comunicazione con il sistema ridondante S7-1500R/H

- Open User Communication:
  - Nessun collegamento progettato
  - E-mail: Le CPU S7-1500R/H supportano solo le versioni < V5.0 dell'istruzione "TMAIL_C". Le versioni a partire dalla V5.0 non sono supportate.
  - Le descrizioni dei collegamenti secondo "TCON_Param" non vengono supportate
- Nessuna comunicazione S7 come client
- Comunicazione PG: non è possibile accedere simultaneamente ad entrambe le CPU. è possibile accedere alla CPU principale o alla CPU di backup.

16.1 Indirizzi IP di sistema nelle R/H-CPU

Introduzione

Oltre agli indirizzi IP dei dispositivi delle CPU il sistema ridondante S7-1500R/H supporta gli indirizzi IP:

- Indirizzo IP di sistema per le interfacce PROFINET X1 di entrambe le CPU (indirizzo IP di sistema X1)
- Indirizzo IP di sistema per le interfacce PROFINET X2 di entrambe le CPU (indirizzo IP di sistema X2)
- Indirizzo IP di sistema per le interfacce PROFINET X3 di entrambe le CPU (indirizzo IP di sistema X3)

Gli indirizzi IP di sistema si utilizzano per la comunicazione con altri dispositivi (ad es. dispositivi HMI, CPU, PC). Tramite l'indirizzo IP di sistema i dispositivi comunicano sempre con la CPU principale del sistema ridondante. Questo garantisce ad es. che, dopo un guasto della CPU principale, il partner della comunicazione in funzionamento ridondante possa comunicare con la nuova CPU principale (prima CPU di backup) nello stato di sistema RUN-Solo.

Un indirizzo MAC virtuale fa parte di ogni indirizzo IP di sistema.

Gli indirizzi IP di sistema vengono attivati in STEP 7.

Vantaggi degli indirizzi IP di sistema rispetto agli indirizzi IP dei dispositivi

- Il partner di comunicazione comunica miratamente con la CPU principale.
- La comunicazione del sistema ridondante S7-1500R/H attraverso un indirizzo IP di sistema continua a funzionare anche in caso di guasto della CPU principale.

Casi applicativi

Gli indirizzi IP di sistema vengono utilizzati per le seguenti applicazioni:

- Comunicazione HMI con il sistema ridondante S7-1500R/H: HMI consente di comandare o di controllare il processo del sistema ridondante S7-1500R/H.
- Open User Communication con il sistema ridondante S7-1500R/H:
  - Un'altra CPU o applicazione su un PC accede ai dati del sistema ridondante S7-1500R/H.
  - Il sistema ridonante S7-1500R/H accede ad un altro dispositivo.

  Sono possibili collegamenti TCP, UDP e ISO-on-TCP.
- IP Forwarding: Se per le route IP tramite il sistema ridondante S7-1500R/H vengono utilizzati come gateway/route standard gli indirizzi IP di sistema, i pacchetti IP vengono inviati anche in caso di avaria di una CPU.

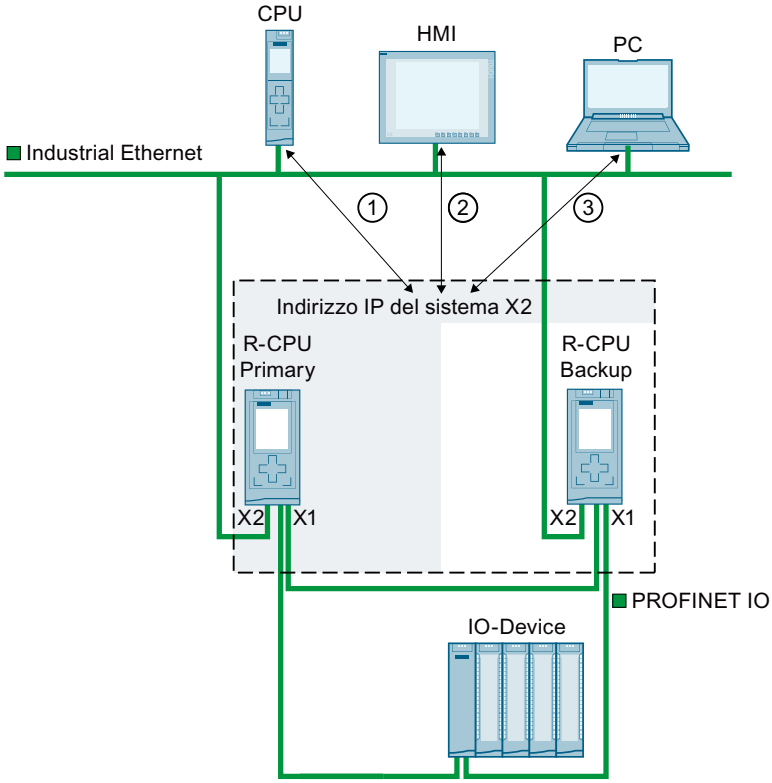
Presupposti

- L'interfaccia del partner di comunicazione è collegato con entrambe le CPU tramite la stessa interfaccia (ad es. X2).
- L'indirizzo IP di sistema per le interfacce del sistema S7-1500R/H è attivato.

Comunicazione tramite gli indirizzi IP di sistema X2 e X3

Se le CPU del sistema ridondante S7-1500R/H dispongono di due o tre interfacce PROFINET, utilizzare l'interfaccia PROFINET X2 o X3 per la comunicazione con altri dispositivi.

La figura seguente mostra una configurazione nella quale i partner di comunicazione sono collegati con le CPU del sistema ridondante S7-1500R/H tramite le rispettive interfacce PROFINET X2.



① Open User Communication tra un'altra CPU e il sistema ridondante S7-1500R.

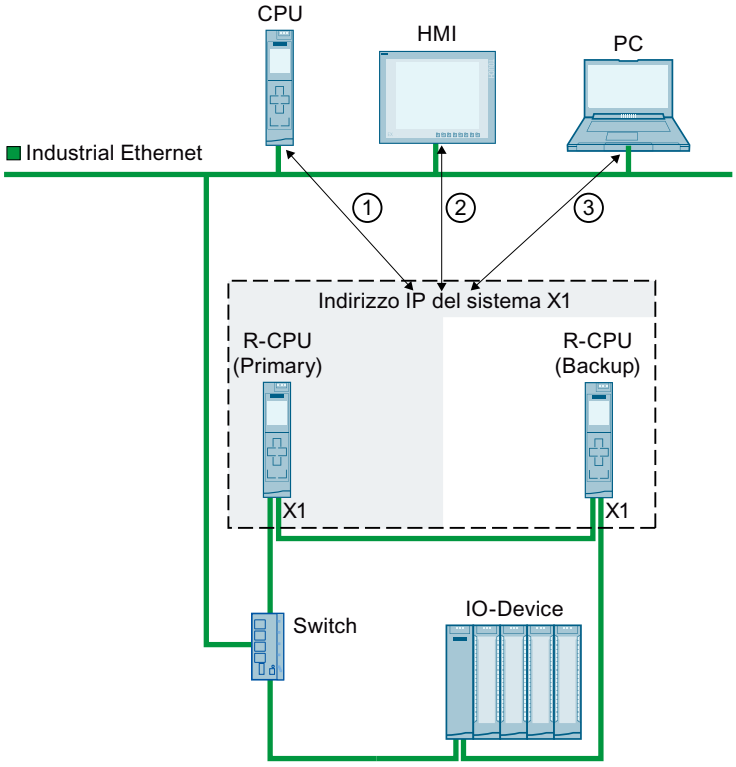
② Comunicazione HMI con il sistema ridondante S7-1500R

③ Open User Communication tra il sistema ridondante S7-1500R e un PC

Figura 16-1 Esempio: Comunicazione del sistema ridondante S7-1515R tramite l'indirizzo IP di sistema X2

Comunicazione tramite l'indirizzo IP di sistema X1

La seguente figura illustra una configurazione nella quale i partner di comunicazione sono collegati ad uno switch nell'anello PROFINET del sistema ridondante S7-1500R/H. L'anello PROFINET collega i partner di comunicazione con le rispettive interfacce PROFINET X1 delle due CPU.
Poiché la CPU 1513R-1 PN dispone di una sola interfaccia PROFINET, il collegamento tramite l'anello PROFINET è l'unica possibilità per comunicare utilizzando l'indirizzo IP di sistema X1.



① Open User Communication tra il sistema ridondante S7-1500R e un'altra CPU

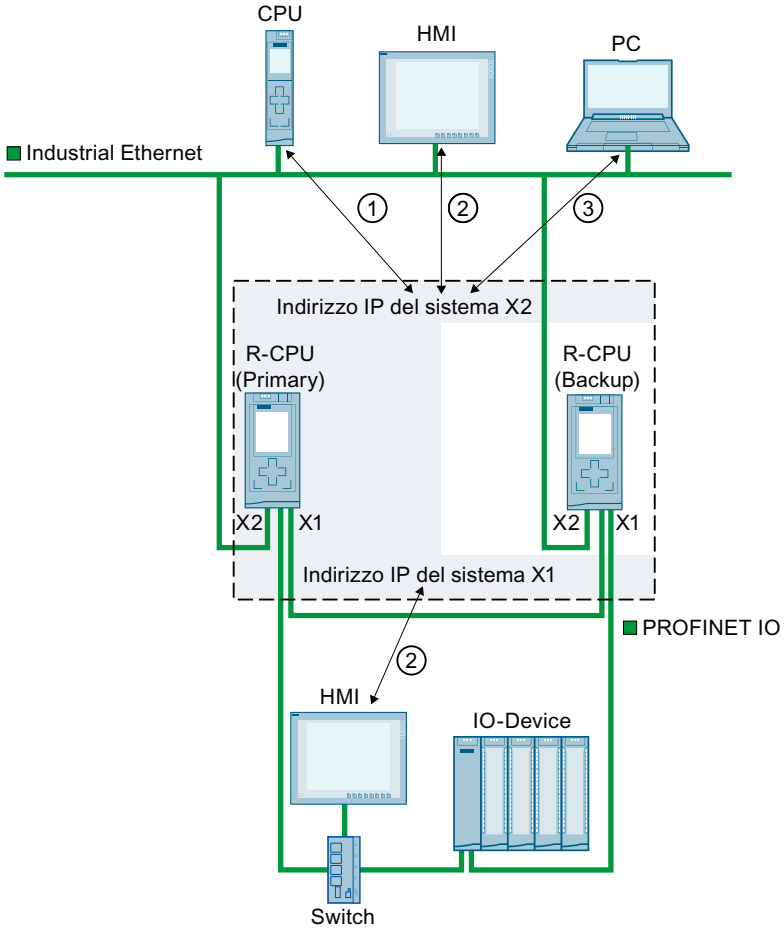
② Comunicazione HMI con il sistema ridondante S7-1500R

③ Open User Communication tra il sistema ridondante S7-1500R e un PC

Figura 16-2 Esempio: Comunicazione del sistema ridondante S7-1513R tramite l'indirizzo IP di sistema X1

Comunicazione tramite gli indirizzi IP di sistema X1, X2 e X3

Per ogni singola interfaccia PROFINET del sistema ridondante S7-1500R/H, è possibile utilizzare un indirizzo IP di sistema. I dispositivi PROFINET collegati alle interfacce X1 delle CPU comunicano tramite l'indirizzo IP di sistema X1. I dispositivi PROFINET collegati alle interfacce X2 delle CPU comunicano tramite l'indirizzo IP di sistema X2. I dispositivi PROFINET collegati alle interfacce X3 delle CPU comunicano tramite l'indirizzo IP di sistema X3.



① Open User Communication tra il sistema ridondante S7-1500R e un'altra CPU.

② Comunicazione HMI con il sistema ridondante S7-1500R

③ Open User Communication tra il sistema ridondante S7-1500R e un PC

Figura 16-3 Esempio: Comunicazione del sistema ridondante S7-1515R tramite gli indirizzi IP di sistema X1 e X2

Un sistema S7-1500H(F) offre inoltre la possibilità di suddividere il proprio impianto in diversi anelli PROFINET.

Se è richiesto l'impiego di dispositivi S1/S2, il collegamento deve avvenire in un anello PROFINET dedicato a valle di uno switch Y.

Suggerimento: Per una maggiore disponibilità degli S1/S2 Device sono necessari 2 switch Y con ridondanza DNA (SCALANCE XF204-2BA DNA). Uno switch Y assume i ruoli di manager MRP e manager DNA. E un secondo switch Y i ruoli di client MRP e client DNA. La ridondanza DNA è possibile solo con un anello PROFINET collegato.

Per ulteriori informazioni sulle varie opzioni di configurazione con switch Y, consultare il manuale di sistema Sistema ridondante S7-1500R/H (https://support.industry.siemens.com/cs/ww/it/view/109754833).

IP Forwarding con gli indirizzi IP di sistema

Se per le rotte IP tramite il sistema ridondante S7-1500R/H vengono utilizzati come gateway/route standard gli indirizzi IP di sistema, i pacchetti IP vengono inviati anche in caso di avaria di una CPU.

Nella figura seguente il PC è collegato con entrambe le interfacce X2 delle CPU S7-1500R. Per il percorso verso il dispositivo HMI nel PC è impostato come gateway l'indirizzo IP di sistema X2. Il dispositivo HMI e collegato all'anello PROFINET del sistema ridondante S7-1500 tramite uno switch. Nel dispositivo HMI è progettato come router l'indirizzo IP di sistema X1.

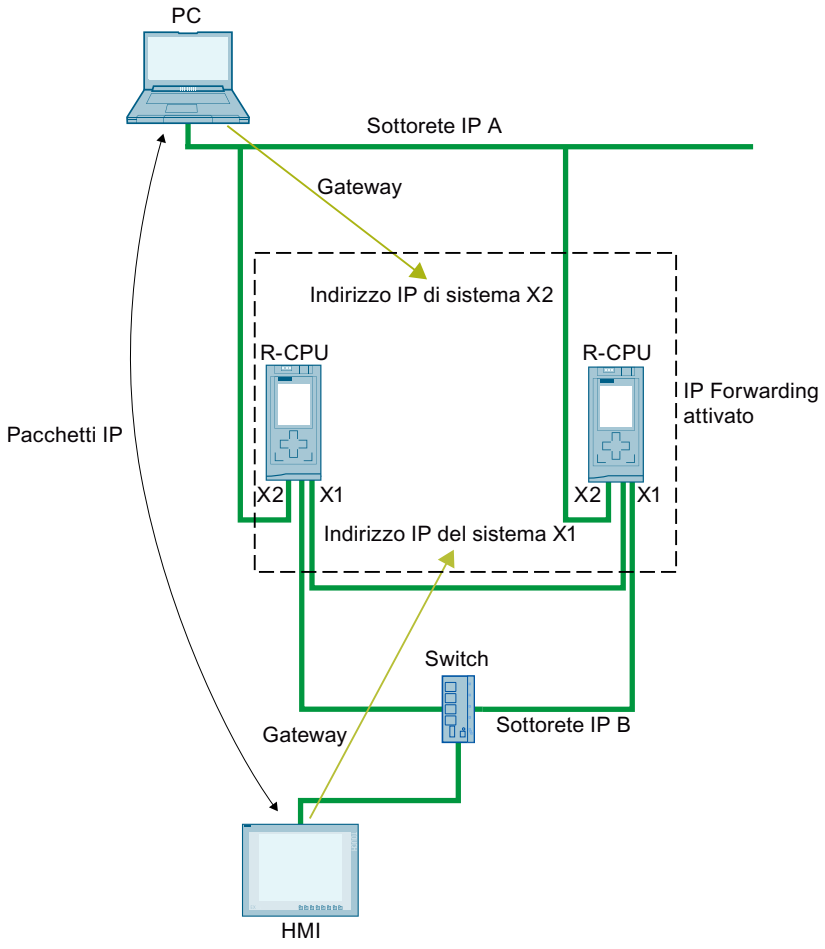


Figura 16-4 Esempio: IP Forwarding con gli indirizzi IP di sistema

Attivazione degli indirizzi IP di sistema

Presupposti:

- STEP 7 V15.1 o superiore
- sistema ridondante S7-1500R/H con due CPU, ad es. due CPU 1513R-1 PN

Se le CPU del sistema ridondante S7-1500R/H dispongono di due interfacce PROFINET (X1 e X2), è possibile attivare un indirizzo IP di sistema per entrambe le interfacce PROFINET. Di seguito vengono descritte le modalità di attivazione dell'indirizzo IP di sistema per l'interfaccia X1.

Per attivare l'indirizzo IP di sistema per il sistema ridondante S7-1500R/H, procedere nel modo seguente:

1. Nella vista di rete di STEP 7, selezionare l'interfaccia X1 di una delle due CPU.
2. Nella finestra di ispezione aprire la voce "Proprietà > Generale > Indirizzi Ethernet" nell'area "Indirizzo IP di sistema per la comunicazione commutata".
3. Attivare la casella di scelta "Attiva l'indirizzo IP di sistema per la comunicazione commutata".

   STEP 7 crea automaticamente un indirizzo IP di sistema.

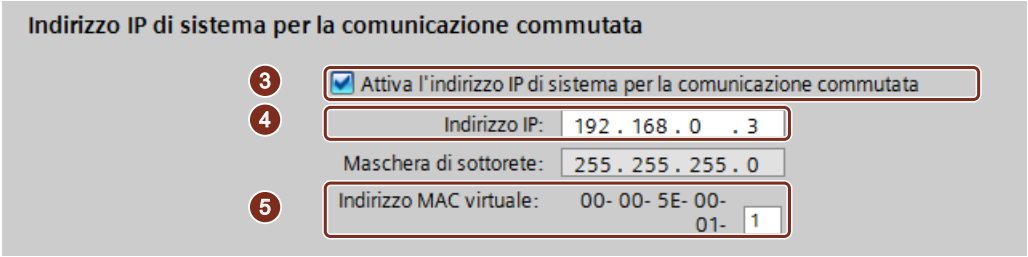


Figura 16-5 Progettazione dell'indirizzo IP di sistema

4. Se necessario è possibile modificare l'indirizzo IP di sistema.
5. Se necessario modificare l'indirizzo MAC virtuale. Assegnare quindi nell'"Indirizzo MAC virtuale" per l'ultimo byte un valore univoco per tutto il progetto (campo dei valori 01_H ... FF_H).

NOTA

Univocità dell'indirizzo MAC virtuale

Il sistema ridondante S7-1500R/H utilizza, per ogni indirizzo IP del sistema, un indirizzo MAC dall'area di indirizzi compresa tra 00-00-5E-00-01-00 e 00-00-5E-00-01-00. Questa area di indirizzi viene utilizzata anche per il VRRP (Virtual Ridondante ProTool).

Se si impiegano dispositivi con VRRP, ad es. switch, prestare attenzione all'univocità degli indirizzi MAC all'interno di un Ethernet-Broadcast-Domain.

Risultato: È attivato l'indirizzo IP di sistema X1 per le interfacce PROFINET X1 di entrambe le CPU.

16.2 Indirizzi IP di sistema nei processori di comunicazione

Introduzione

A partire da STEP 7 V19 esiste la possibilità di ampliare un sistema ridondante S7-1500R/H dalla versione FW V3.1 con i processori di comunicazione CP 1543-1 dalla versione FW V3.0. Le R/H-CPU, grazie all'ampliamento con i processori di comunicazione CP 1543-1, supportano la progettazione di un'interfaccia virtuale W1 con indirizzo IP del dispositivo e del sistema. I partner di comunicazione collegati ai CP comunicano con le R/H-CPU tramite questi indirizzi IP.

L'indirizzo IP di sistema di W1 deve essere attivato in STEP 7.

Un indirizzo MAC virtuale fa parte di ogni indirizzo IP di sistema.

Guasto di un processore di comunicazione

In caso di guasto di un processore di comunicazione CP 1543-1, il sistema ridondante S7-1500R/H si comporta come segue:

- S7-1500R:
  In caso di guasto di un CP, la CPU corrispondente commuta nello stato di funzionamento STOP. Il sistema S7-1500R passa allo stato di sistema RUN-Solo.
  In caso di guasto del CP nella CPU principale, il sistema ridondante S7-1500R commuta dalla CPU principale-alla CPU di backup. L'indirizzo IP di sistema assegnato passa alla nuova CPU principale. La configurazione di un nuovo collegamento di comunicazione avviene tramite il CP ridondante.
  In caso di guasto del CP nella CPU di backup, il guasto non si ripercuote sulla comunicazione esistente tramite l'indirizzo IP di sistema.
- S7-1500H con bus backplane attivo:
  In caso di guasto di un CP il sistema S7-1500H rimane nello stato di sistema RUN-Redundant.
  In caso di guasto del CP nella CPU principale, il sistema ridondante S7-1500H non esegue alcuna commutazione tra la CPU principale-e la CPU di backup. L'indirizzo IP di sistema W1 è stato assegnato al CP guasto tramite la CPU principale. Per commutare l'indirizzo IP di sistema W1 sulla CPU di backup si deve richiamare l'istruzione "RH_CTRL" con Mode=15 nel programma utente. L'indirizzo IP di sistema W1 verrà assegnato alla CPU di backup. La configurazione di un nuovo collegamento di comunicazione avviene tramite il CP ridondante della CPU di backup.

  Se un altro CP collegato alla CPU principale subisce un guasto, per stabilire un nuovo collegamento di comunicazione con il CP ridondante si dovrà utilizzare l'indirizzo IP che è stato assegnato al dispositivo.

NOTA

Se si comunica con il sistema ridondante tramite gli indirizzi IP del dispositivo, è preferibile utilizzare l'indirizzo IP del dispositivo della CPU principale. La velocità di trasmissione è migliore e il carico di comunicazione è inferiore tramite l'indirizzo IP della CPU principale.

Per ulteriori informazioni sull'istruzione "RH_CTRL" consultare la Guida in linea a STEP 7.

Informazioni sulla progettazione dell'indirizzo IP del sistema per l'interfaccia virtuale W1 e l'indirizzo MAC virtuale sono contenute nel manuale di sistema del sistema ridondante S7-1500R/H (https://support.industry.siemens.com/cs/it/it/view/109754833).

Vantaggi dell'ampliamento con i processori di comunicazione CP 1543-1

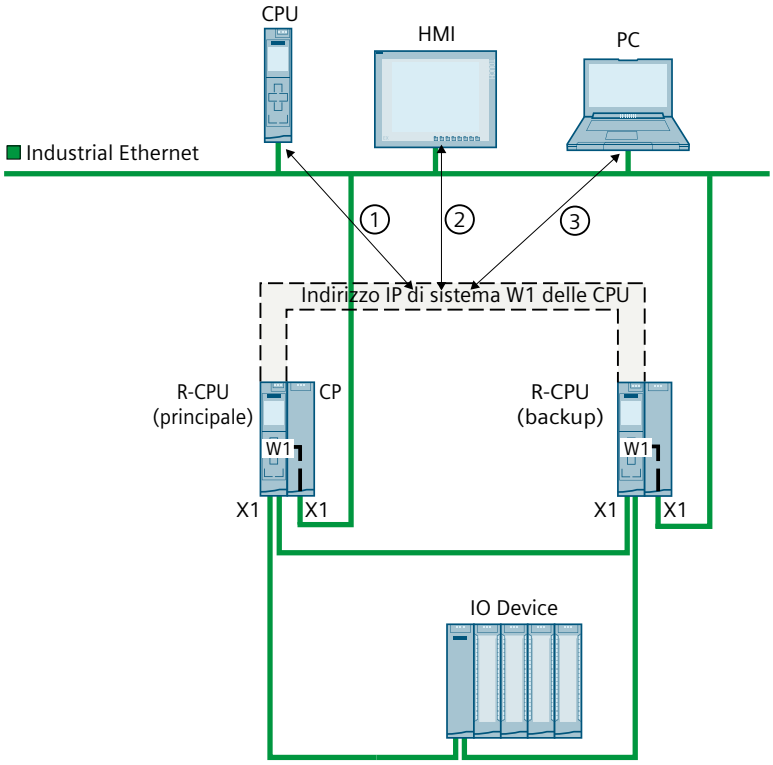
Se si amplia il sistema ridondante con i processori di comunicazione CP 1543-1 sono disponibili delle interfacce di comunicazione aggiuntive. Questo vantaggio può essere utilizzato per la CPU 1513R-1 PN con una sola interfaccia PROFINET ad es. per la separazione della rete.

Presupposti per l'utilizzo dell'indirizzo IP di sistema di W1

- L'interfaccia virtuale W1 è assegnata a un CP 1543-1.
- L'indirizzo IP di sistema dell'interfaccia virtuale W1 è attivato.
- All'interfaccia virtuale W1 è assegnato un indirizzo IP di sistema.
- Un partner di comunicazione può raggiungere entrambi i CP utilizzando l'indirizzo IP di sistema assegnato.

Comunicazione tramite l'indirizzo IP di sistema di W1

La figura seguente mostra la configurazione di un sistema ridondante S7-1513R ampliato con i CP. I partner di comunicazione comunicano con il sistema ridondante tramite l'indirizzo IP di sistema assegnato di W1.



① Comunicazione tra il sistema ridondante S7-1500R e un'altra CPU

② Comunicazione HMI con il sistema ridondante S7-1500R

③ Comunicazione tra il sistema ridondante S7-1500R e un PC

Figura 16-6 Esempio: Comunicazione del sistema ridondante S7-1513R tramite l'indirizzo IP di sistema assegnato di W1

IP Forwarding con gli indirizzi IP di sistema

Se per le rotte IP tramite il sistema ridondante S7-1500R vengono utilizzati come gateway/route standard gli indirizzi IP di sistema, i pacchetti IP vengono inviati anche in caso di avaria di una CPU.

NOTA

Commutazione tra CPU principale e CPU di backup nei sistemi S7-1500H con bus backplane attivo

In caso di guasto di un CP del sistema S7-1500H con bus backplane attivo non ha luogo alcuna commutazione tra CPU principale e CPU di backup. Se necessario configurare la commutazione tra CPU principale e CPU di backup nel programma utente.

Nella figura seguente il PC è collegato con entrambe le interfacce X1 dei CP 1543-1. Per il percorso verso il dispositivo HMI nel PC è impostato come router l'indirizzo IP di

sistema assegnato di W1. Il dispositivo HMI e collegato all'anello PROFINET del sistema ridondante S7-1500R tramite uno switch. Nel dispositivo HMI è configurato come router l'indirizzo IP di sistema X1 della CPU.

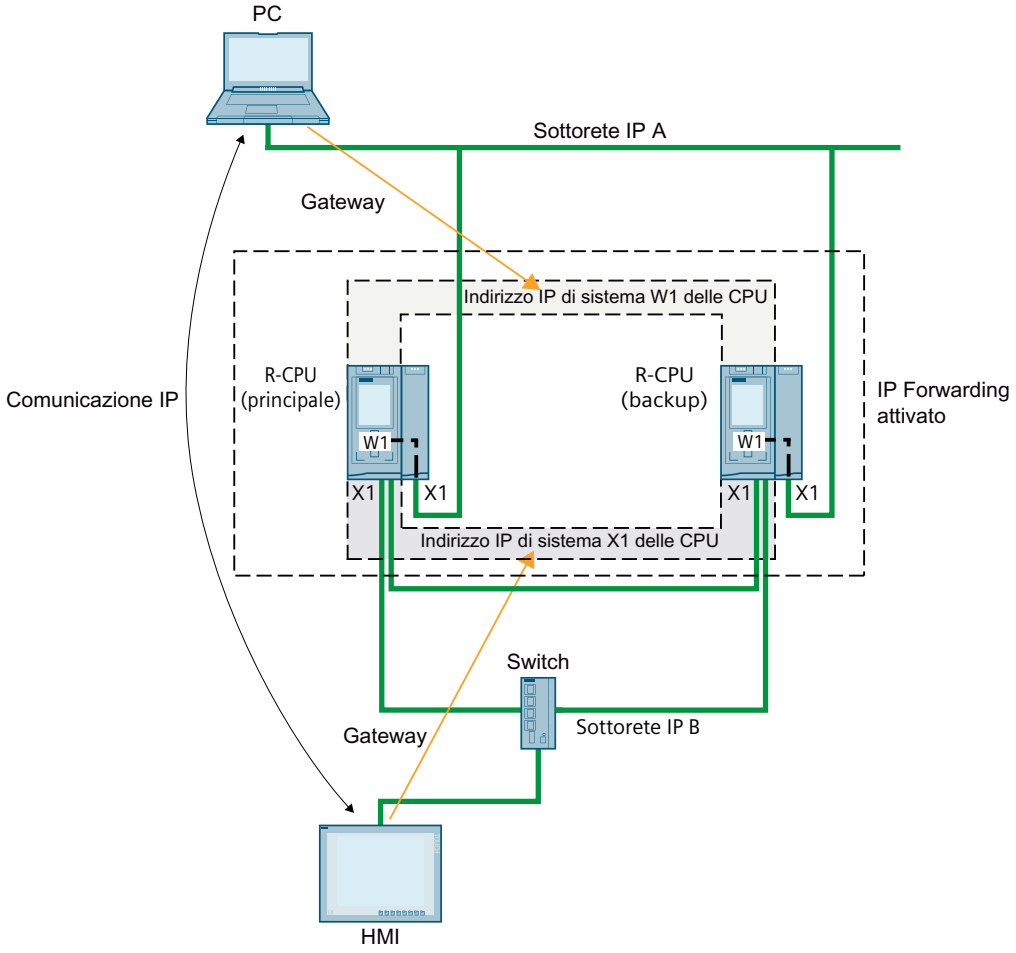


Figura 16-7 Esempio: IP Forwarding con gli indirizzi IP di sistema delle CPU e dei CP

Assegnazione dell'indirizzo IP di sistema dell'interfaccia virtuale W1 delle R/H-CPU

A partire da STEP 7 V19 è possibile assegnare un indirizzo IP di sistema all'interfaccia virtuale W1 delle R/H-CPU. I partner di comunicazione collegati ai CP comunicano con il sistema R/H tramite l'indirizzo IP di sistema assegnato.

Per modificare l'indirizzo IP di sistema dell'interfaccia virtuale W1 delle R/H-CPU, procedere come indicato di seguito:

1. Nella vista dispositivi selezionare la R/H-CPU sulla guida profilata_0.
2. Nella finestra di ispezione spostarsi fino a "Configurazione ampliata > Accesso al PLC tramite il modulo di comunicazione".

3. Nella sezione "Assegnazione dell'interfaccia [W1]" nella casella di riepilogo "Selezione del modulo di comunicazione", selezionare il CP richiesto.
   Dopo la selezione, viene visualizzata una segnalazione di avviso indicante i possibili rischi di questa impostazione. Alla conferma della segnalazione di avviso vengono visualizzate le opzioni di configurazione per l'interfaccia virtuale W1.
4. Accedere all'area "Internet Protocol Version 4 (IPv4)".
5. Confermare l'impostazione suggerita o assegnare un nuovo indirizzo IP.
6. Navigare fino all'area "Indirizzo IP di sistema per la comunicazione commutata".
7. Attivare l'opzione "Attiva l'indirizzo IP di sistema per la comunicazione commutata".
8. Confermare l'impostazione suggerita o assegnare un nuovo indirizzo IP di sistema (e l'indirizzo MAC virtuale).
9. La R/H-CPU sulla guida profilata_1 acquisisce automaticamente le impostazioni.

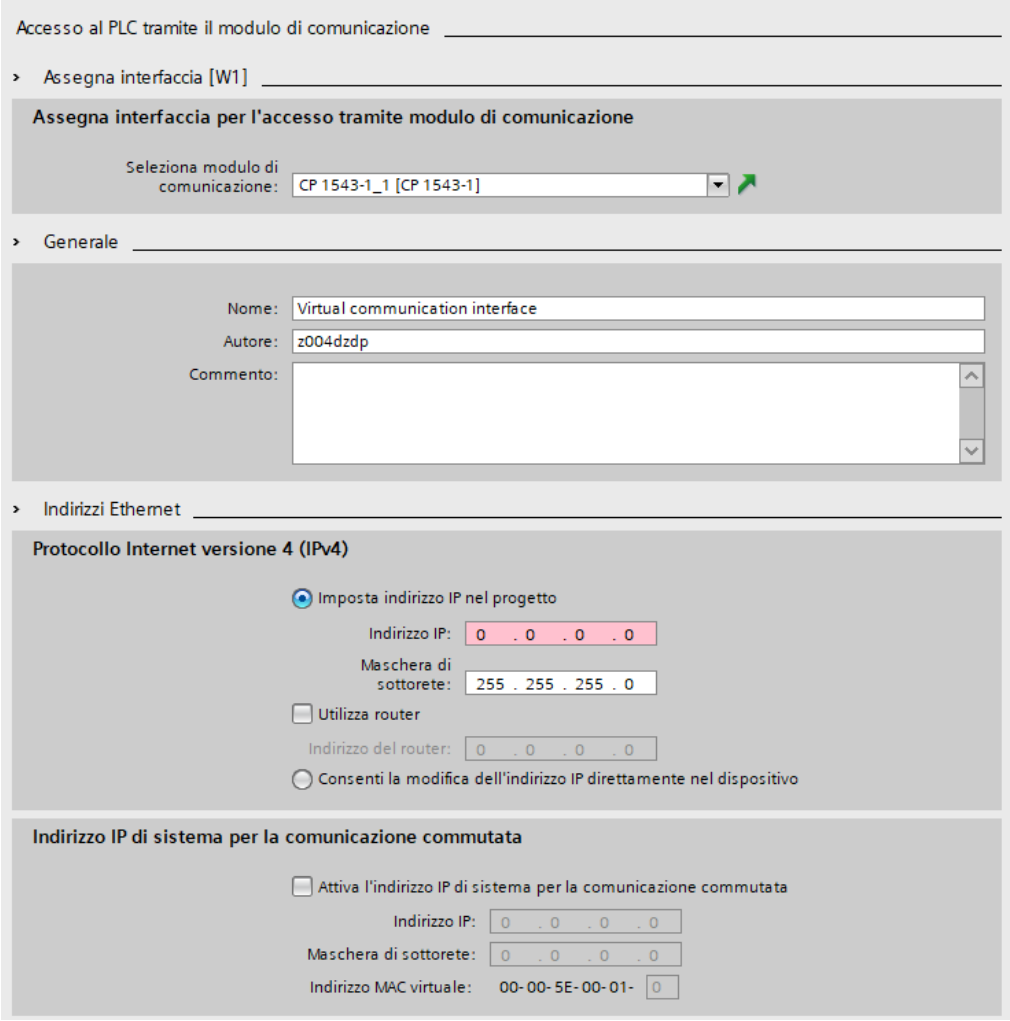


Figura 16-8 Configurazione dell'indirizzo IP di sistema di W1

Risultato: L'interfaccia virtuale W1 è assegnata a un CP 1543-1 e l'indirizzo IP del dispositivo/sistema è configurato.

16.3 Raggiungibilità ottimizzata tramite commutazione dell'indirizzo IP di sistema

Commutazione dell'indirizzo IP di sistema in caso di mancata raggiungibilità della CPU

Come standard, l'indirizzo IP di sistema è assegnato alla CPU principale.

A partire da TIA Portal V20 (versione firmware della CPU V4.0 o successiva), è possibile utilizzare modalità aggiuntive per assegnare l'indirizzo IP di sistema della CPU di backup all'istruzione "RH_CTRL", in modo da mantenere la comunicazione, ad es., se la CPU principale non è disponibile.

Ulteriori informazioni

Una descrizione della commutazione controllata da programma dell'indirizzo IP di sistema si trova nelle istruzioni speciali per i sistemi ridondanti S7-1500R/H nel Manuale di sistema S7-1500R/H (https://support.industry.siemens.com/cs/it/it/view/109754833).

16.4 Comportamento con Syncup

Comportamenti dei collegamenti di comunicazione tramite l'indirizzo IP di sistema nello stato di sistema SYNCUP

- I collegamenti HMI, PG, e S7 vengono temporaneamente chiusi. Per una breve durata durante il SYNCUP non è possibile realizzare collegamenti al sistema ridondante S7-1500R/H.
- Vengono interrotti tutti i collegamenti esistenti dell'Open User Communication:
  - I collegamenti configurati dalle CPU del sistema ridondante come partner attivi del collegamento vengono riconfigurati dopo il SYNCUP.
  - Dopo SYNCUP il sistema ridondante S7-1500R/H riconfigura i punti terminali del collegamento per la realizzazione passiva del collegamento.
- La modifica delle istanze in esecuzione delle applicazioni TSEND e TRCV viene arrestata. Il parametro del blocco STATUS fornisce $80C4_H$ (errore di comunicazione temporaneo).

16.5 Comportamento in caso di commutazione principale/di backup

Comportamenti dei collegamenti di comunicazione tramite l'indirizzo IP di sistema durante una commutazione principale/di backup

- Le istanze in esecuzione delle istruzioni TSEND e TRCV vengono arrestate e forniscono lo stato $80C4_H$ (errore di comunicazione temporaneo).
- I collegamenti attivi riusciti, realizzati dal sistema ridondante S7-1500R/H vengono nuovamente realizzati dalla nuova CPU principale.
- La CPU principale riconfigura i punti terminali del collegamento per la realizzazione passiva del collegamento.

NOTA

Maggiore durata dell'interruzione del collegamento

Se il sistema remoto dopo la commutazione del backup primario non effettua invii in modo attivo, può essere necessario che il monitoraggio del collegamento (es. TCP-Keep-Alive oppure l'applicazione) sia eseguito dal sistema remoto, fino a quando non viene ristabilito il collegamento.

16.6 Risorse di collegamento del sistema ridondante S7-1500R/H

Numero massime di risorse di collegamento del sistema ridondante S7-1500R/H

Il sistema ridondante S7-1500R/H supporta un numero massimo di risorse di collegamento.

La CPU impiegata determina il numero massimo di risorse per il sistema ridondante:

- CPU 1513R: max. 88 risorse di collegamento
- CPU 1515R: max. 128 risorse di collegamento (dalla versione V3.0), max. 108 risorse di collegamento (fino alla versione V2.9.x)
- CPU 1517H: max. 288 risorse di collegamento
- CPU 1518HF: max. 320 risorse di collegamento

Occupazione delle risorse di collegamento

I collegamenti di comunicazione occupano risorse di collegamento nel sistema ridondante S7-1500R/H.

Tutti i collegamenti di comunicazione del sistema ridondante S7-1500R/H occupano risorse di collegamento nella stazione S7-1500R/H. La stazione S7-1500R/H comprende l'installazione hardware di entrambe le CPU del sistema ridondante S7-1500R/H.

In funzione dell'indirizzo IP utilizzato, il collegamento di comunicazione occupa risorse anche in una o in entrambe le CPU del sistema ridondante S7-1500R/H.

La seguente tabella indica la CPU nella quale un collegamento di comunicazione occupa risorse di collegamento in funzione dell'indirizzo IP utilizzato.

Collegamento tramite...	risorse di collegamento della stazione	risorse di collegamento CPU con l'ID di ridondanza 1	risorse di collegamento CPU con l'ID di ridondanza 2
un indirizzo IP di sistema	X	X	X
un indirizzo IP di dispositivo della CPU con l'ID di ridondanza 1	X	X	-
un indirizzo IP di dispositivo della CPU con l'ID di ridondanza 2	X	-	X

Visualizzazione delle risorse di collegamento occupate in STEP 7

Presupposti: collegamento online con il sistema ridondante S7-1500R/H

La vista online delle risorse di collegamento si trova nella finestra di ispezione "Diagnostica > Informazioni sul collegamento". STEP 7 visualizza sempre le risorse di collegamento della CPU selezionata e della stazione S7-1500R/H.

Risorse di collegamento

	Risorse della stazione					Risorse del modulo	
		Riservate		Dinamiche		CPU 1517H-3 PN (R0/S1)	
Numero max. di risorse:		10	10	150	150	160	160
	Max.	Configurate	Utilizzate	Configurate	Utilizzate	Configurate	Utilizzate
Comunicazione PG:	4	-	2	-	0	-	2
Comunicazione HMI:	4	0	0	0	0	0	0
Comunicazione S7:	0	-	0	0	0	0	0
Open User Communication:	0	-	0	0	0	0	0
Comunicazione Web:	2	-	0	-	0	-	0
Altri tipi di comunicazione:	-	-	0	0	0	0	0
Risorse totali utilizzate:		0	2	0	0	0	2
Risorse disponibili:		10	8	150	150	160	158

Figura 16-9 Visualizzazione delle risorse di collegamento del sistema ridondante S7-1500R/H in STEP 7

16.7 Comunicazione HMI con il sistema ridondante S7-1500R/H

16.7.1 Configurazione del collegamento HMI tramite l'indirizzo IP di sistema

Presupposti

- Sistema ridondante S7-1500R/H, ad es. la CPU 1513R-1PN
- L'indirizzo IP di sistema è attivato
- Dispositivo HMI con interfaccia PROFINET

Procedimento

Per configurare un collegamento HMI con un sistema ridondante S7-1500R/H procedere nel modo seguente:

1. Selezionare l'interfaccia PROFINET del dispositivo HMI nella vista di rete di STEP 7.
2. Tramite Drag&Drop tracciare una linea tra l'interfaccia PROFINET del dispositivo HMI e un'interfaccia PROFINET del sistema ridondante S7-1500R/H.
   Il dispositivo HMI e il sistema ridondante S7-1500R/H sono collegati in rete tra loro.

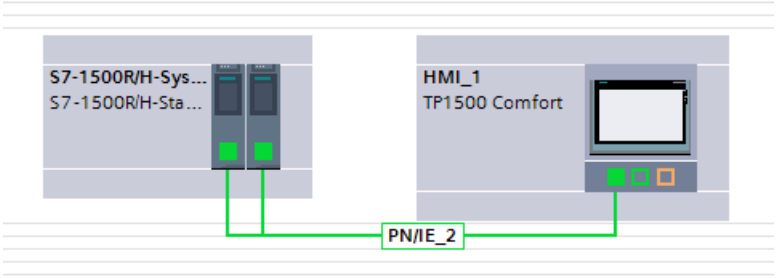


Figura 16-10 Dispositivo HMI collegato in rete con il sistema ridondante S7-1500R/H

3. Fare clic sul simbolo "Collegamenti" della barra degli strumenti. In questo modo viene attivata la modalità di collegamento.
4. Tramite Drag&Drop tracciare una linea tra il dispositivo HMI e una CPU del sistema ridondante S7-1500R/H.
   Si apre l'elenco "Partner del collegamento" .

Figura 16-11 Configurazione del collegamento HMI con il sistema ridondante S7-1500R/H

5. Selezionare nell'elenco "Partner del collegamento" il sistema ridondante S7-1500R/H.

Risultato: È stato configurato un collegamento HMI tra il dispositivo HMI e il sistema ridondante S7-1500R/H. Il collegamento HMI utilizza l'indirizzo IP di sistema. Il dispositivo HMI si collega sempre con la CPU principale.

Commutare il collegamento HMI sull'indirizzo IP di dispositivo

Per convertire il collegamento HMI in modo fisso su una CPU selezionata, disattivare la casella di controllo "Utilizza l'indirizzo IP di sistema per la comunicazione collegata" nelle proprietà del collegamento HMI. Il collegamento HMI utilizza l'indirizzo IP di dispositivo dell'interfaccia PROFINET. Se questa CPU si guasta, il collegamento HMI con questa CPU si guasta in modo permanente.

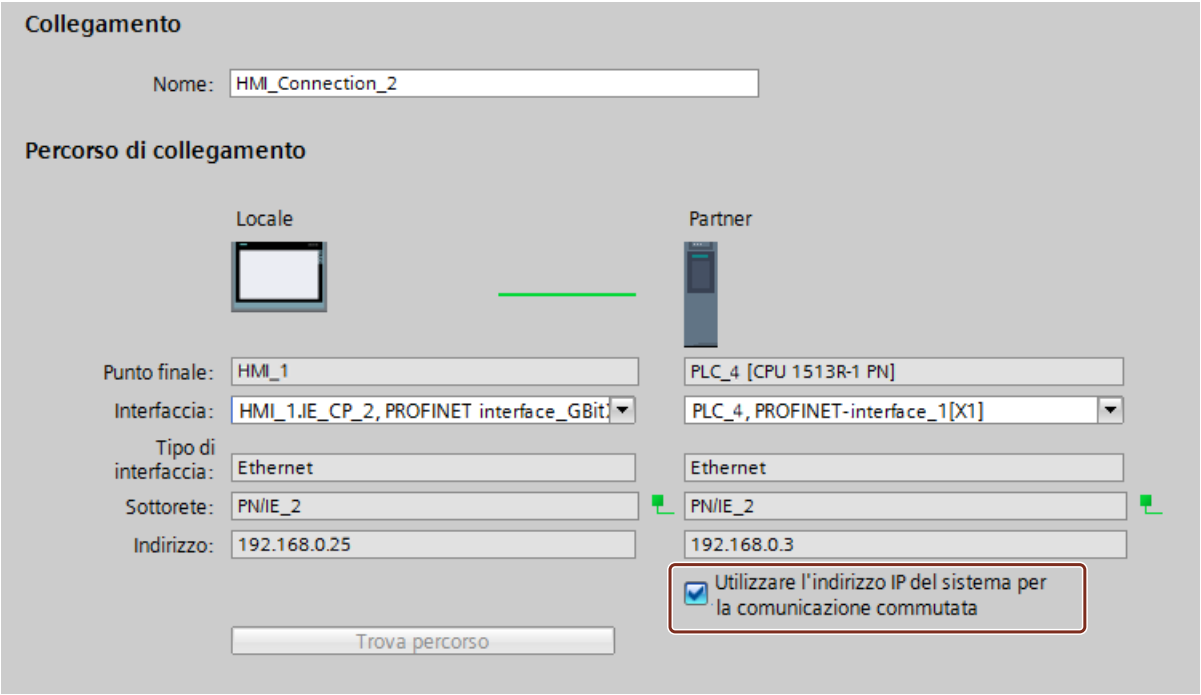


Figura 16-12 Proprietà del collegamento HMI

NOTA

Configurazione automatica del collegamento HMI

Con il trascinamento di una variabile da un sistema S7-1500R/H ridondante ad una pagina HMI oppure nella tabella delle variabili HMI, STEP 7 configura automaticamente un collegamento HMI. Come standard questo collegamento HMI è realizzato tra l'interfaccia PROFINET del dispositivo HMI e l'interfaccia PROFINET X1 della CPU con l'ID di ridondante 1. Il collegamento utilizza l'indirizzo IP di dispositivo dell'interfaccia PROFINET X1.

Nelle proprietà del collegamento HMI è possibile convertire il collegamento HMI su un indirizzo IP di sistema.

Ulteriori informazioni

È possibile creare un collegamento HMI al sistema ridondante S7-1500R/H anche tramite l'indirizzo IP del dispositivo. Con l'ausilio di script nella progettazione HMI, il collegamento viene commutato automaticamente dalla CPU guasta alla CPU ancora in funzione. La descrizione di questo procedimento si trova nella seguente FAQ (https://support.industry.siemens.com/cs/it/it/view/109781687).

16.8 Open User Communication con il sistema ridondante S7-1500R/H

Introduzione

I sistemi S7-1500R/H a partire dalla versione FW V3.1 supportano anche Secure Open User Communication (Secure OUC).

In caso di ampliamento di un sistema S7-1500R/H dalla versione FW V3.1 con i processori di comunicazione CP 1543-1, è possibile utilizzare Secure OUC anche tramite i CP collegati.

Presupposti:

- STEP 7 V19 o superiore
- CP 1543-1 dalla versione firmware V3.0

Protocolli della Secure Open User Communication per il sistema ridondante S7-1500R/H

La seguente tabella elenca i protocolli della Open User Communication che possono essere utilizzati per il sistema S7-1500R/H e i relativi tipi di sistemi di dati e le istruzioni.

Tabella 16-1 Protocolli, tipi di dati di sistema e istruzioni utilizzabili per Open User Communication con il sistema ridondante S7-1500R/H

Protocollo	Tipo di dati di sistema	Istruzioni
TCP	• TCON_QDN • TCON_QDN_SEC • TCON_IP_v4 • TCON_IP_V4_SEC	Creazione del collegamento e invio/ricezione dei dati tramite: • TSEND_C/TRCV_C oppure • TCON, TSEND/TRCV oppure • TCON, TUSEND/TURCV (interruzione del collegamento possibile con TDISCON)
TLS over TCP		
ISO-on-TCP	• TCON_IP_RFC	
UDP	• TCON_IP_v4 • TADDR_Param • TADDR_SEND_QDN • TADDR_RCV_IP	Creazione del collegamento e invio/ricezione dei dati tramite: • TSEND_C/TRCV_C • TUSEND/TURCV/TRCV (interruzione del collegamento possibile con TDISCON)
Modbus TCP	• TCON_IP_v4 • TCON_IP_V4_SEC • TCON_QDN • TCON_QDN_SEC	• MB_CLIENT • MB_RED_CLIENT • MB_SERVER • MB_RED_SERVER

16.8.1 Configurazione del collegamento tra Open User Communication e il sistema ridondante S7-1500R/H

Open User Communication tramite le interfacce PROFINET integrate della CPU

Il sistema ridondante S7-1500R/H può comunicare con altri dispositivi tramite Open User Communication.

I collegamenti vengono configurati nel programma utente, ad es. tramite l'istruzione "TSEND_C". I collegamenti progettati non supportano il sistema ridondante S7-1500R/H.

I collegamenti possono essere configurati tramite i seguenti indirizzi IP delle interfacce PROFINET integrate:

- Indirizzi IP dei dispositivi:
  Nel funzionamento ridondante, il sistema può creare e disattivare collegamenti nonché ricevere e inviare dati da tutti gli indirizzi IP dei dispositivi del sistema ridondante.
  Se il collegamento viene configurato con un indirizzo IP del dispositivo, la comunicazione si svolge tramite la CPU corrispondente. Se la CPU si guasta, si interrompe l'intera comunicazione tramite gli indirizzi IP di dispositivo di questa CPU.
- Indirizzi IP di sistema:
  Se si configura il collegamento tramite un indirizzo IP di sistema, la comunicazione funziona sempre tramite la CPU principale.

Valutare il caso applicativo specifico per decidere quali collegamenti configurare.

Open User Communication tramite i processori di comunicazione CP 1543-1

Ampliando un sistema ridondante S7-1500R/H con i processori di comunicazione CP 1543-1 è possibile utilizzare le opzioni di comunicazione seguenti:

- Interfaccia locale X1 del CP 1543-1
- Indirizzo IP specifico del dispositivo per l'interfaccia virtuale W1 di ciascuna R/H-CPU
- Indirizzo IP comune del sistema per l'interfaccia virtuale W1 del sistema R/H

Per informazioni sull'utilizzo di un CP 1543-1 in un sistema S7-1500R/H, vedere il capitolo Indirizzi IP di sistema nei processori di comunicazione (Pagina 461).

Configurazione del collegamento tramite un indirizzo IP di sistema

Di seguito è descritta la configurazione di un collegamento ad una CPU partner tramite l'indirizzo IP di sistema di un'interfaccia PROFINET integrata nel sistema ridondante S7-1500R/H.

Il collegamento viene configurato nel programma utente del sistema ridondante S7-1500R/H ad es. con un'istruzione TSEND_C. Nel programma utente della CPU partner creare un'istruzione TRCV_C corrispondente.

Il procedimento è descritto con l'esempio di un collegamento TCP tra il sistema ridondante S7-1500R/H e una CPU 1516-3PN/DP.

Presupposti

- Un sistema ridondante S7-1500R/H come client TCP, ad es. 2 CPU 1513-1PN
- L'indirizzo IP di sistema dell'interfaccia PROFINET X1 è attivato.
- Partner di collegamento come server TCP, ad es. CPU 1516-3 PN/DP
- Le interfacce PROFINET X1 delle CPU ridondanti 1513R e l'interfaccia PROFINET X2 della CPU 1516-3PN/DP si trovano nella stessa sottorete.

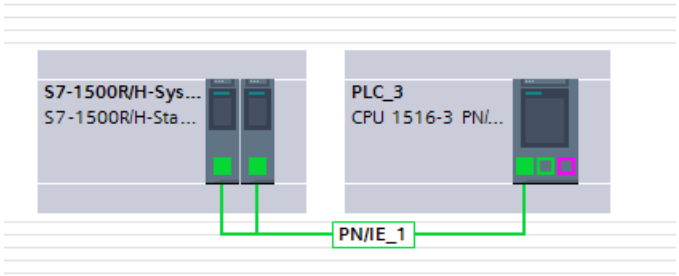


Figura 16-13 Esempio di configurazione per il collegamento TCP

Istruzione TSEND_C nel programma utente del sistema ridondante S7-1500R/H

Per configurare un collegamento TCP con un'altra CPU procedere nel modo seguente:

1. Creare un'istruzione "TSEND_C" nel programma utente.

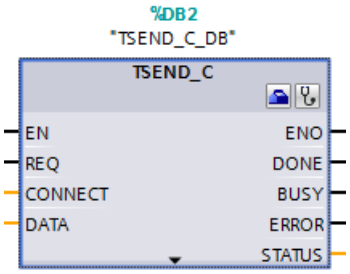


Figura 16-14 S7-1500R/H: Istruzione "TSEND_C"

2. Selezionare l'istruzione "TSEND_C".
3. Nelle finestra di ispezione navigare alla voce "Proprietà > Configurazione > Parametri di collegamento".
   Sul lato sinistro è visibile il sistema ridondante S7-1500R/H come punto finale locale del collegamento:
   - "Interfaccia:": È preimpostata l'interfaccia X1.
   - "Sottorete:": Se l'interfaccia X1 è assegnata ad una sottorete S7, STEP 7 visualizza il nome della sottorete S7.
   - La casella di scelta "Utilizza indirizzo IP di sistema" è attivata. In "Indirizzo:" si trova l'indirizzo IP del sistema ridondante S7-1500R/H.

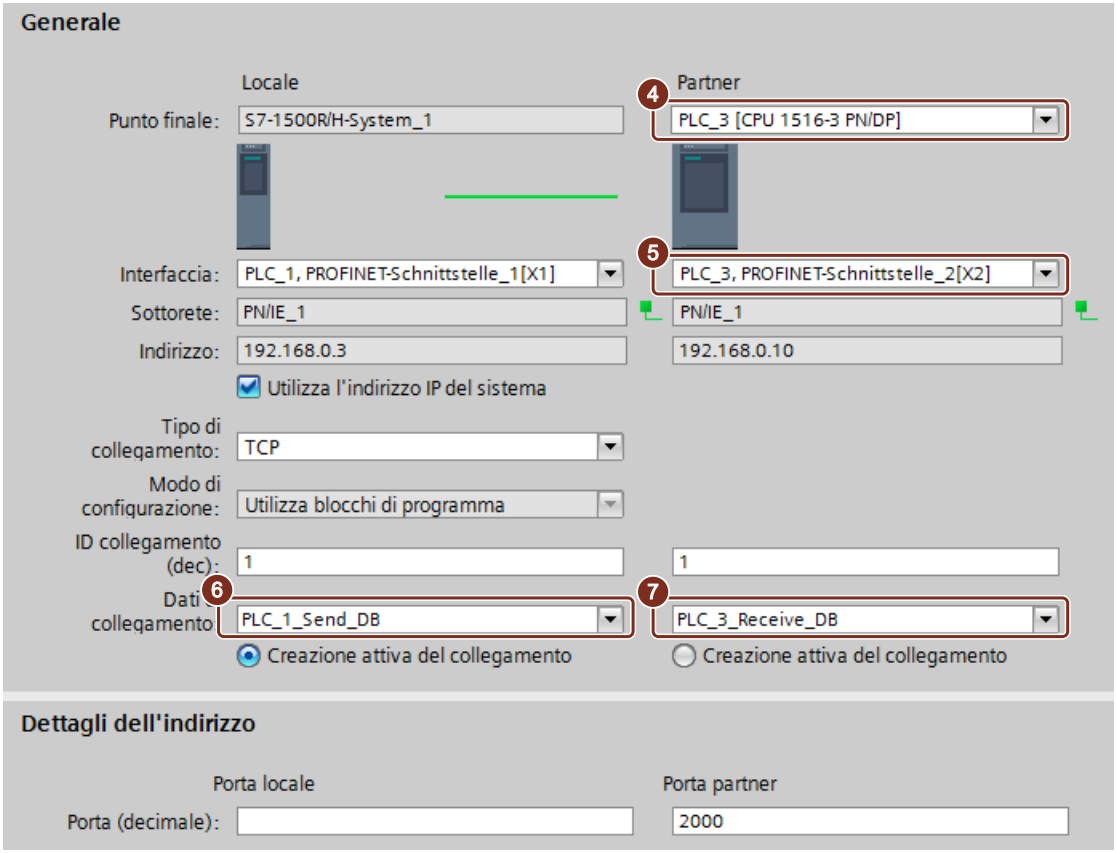


Figura 16-15 S7-1500R/H: Parametrizzazione dell'istruzione TSEND_C in STEP 7

4. Come partner di collegamento selezionare in "Partner" alla voce "Punto finale:" la CPU 1516-3PN/DP.
5. Selezionare in "Partner" alla voce "Interfaccia:" l'interfaccia PROFINET X2 della CPU 1516-3PN/DP.
6. Selezionare in "Locale" alla voce "Dati del collegamento" l'impostazione "<nuovo>".
   STEP 7 crea un blocco dati per i dati del collegamento nel programma utente del sistema ridondante S7-1500R/H, ad es."PLC_1_Send_DB".
   Come "Tipo di collegamento" è preimpostato "TCP".
7. Selezionare in "Partner" alla voce "Tipo di collegamento" l'impostazione "nuovo".
   STEP 7 crea un blocco dati per i dati del collegamento nel programma utente dell'altra CPU, ad es. "PLC_3_Receive_DB".

Istruzione TRCV_C nel programma utente della CPU 1516-3PN/DP

Creare nel programma utente della CPU 1516-3PN/DP un'istruzione TRCV_C e parametrizzarla nel modo seguente:

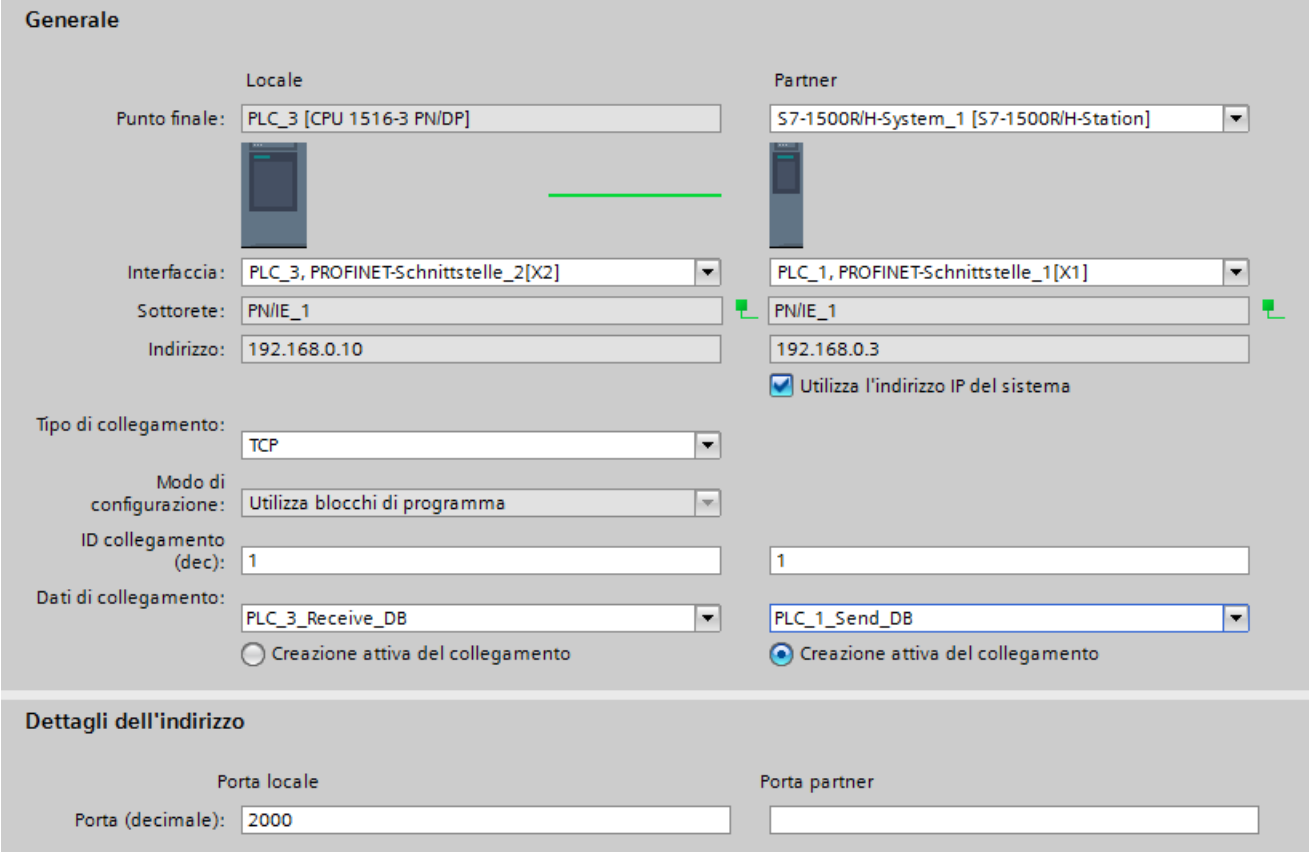


Figura 16-16 S7-1500-3PN/DP: Parametrizzazione dell'istruzione TRCV_C in STEP 7

Configurazione del collegamento tramite l'indirizzo IP di dispositivo

Per configurare un collegamento OUC tramite un indirizzo IP di dispositivo di una delle due CPU:

- Selezionare un'interfaccia PROFINET adatta del sistema ridondante S7-1500R/H.
- Attivare la casella di scelta "Utilizza indirizzo IP di sistema".

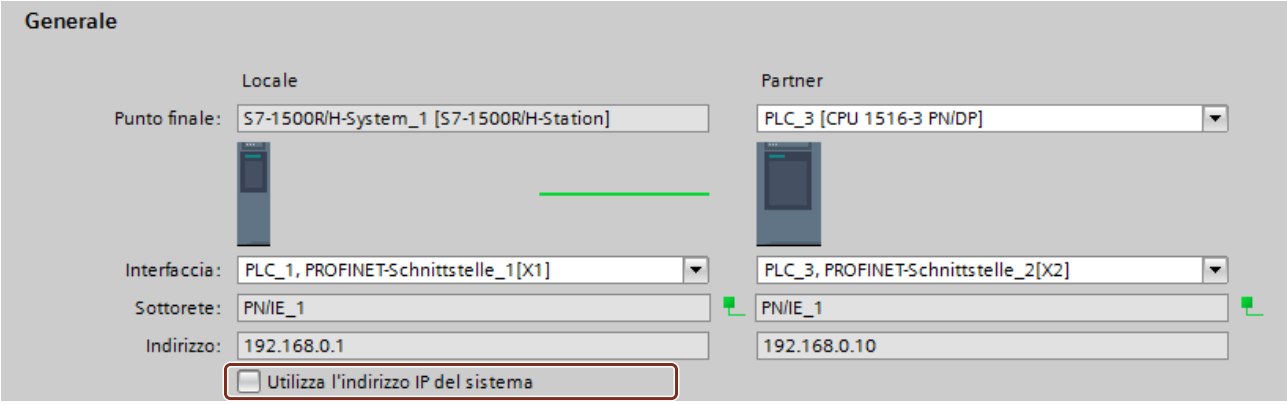


Figura 16-17 Collegamento OUC tramite un indirizzo IP di dispositivo

Ulteriori informazioni

Per ulteriori informazioni sugli stati di sistema, consultare il manuale di sistema S7-1500R/H (https://support.industry.siemens.com/cs/ww/it/view/109754833).

Ulteriori informazioni sulla configurazione e parametrizzazione del sistema PROFINET IO sono disponibili nel Manuale di guida alle funzioni PROFINET (https://support.industry.siemens.com/cs/ww/it/view/49948856).

16.8.2 Open User Communication con i processori di comunicazione CP 1543-1

Introduzione

Con i processori di comunicazione CP 1543-1 è possibile utilizzare sia Open User Communication (OUC) sia Secure OUC.

Per poter utilizzare Secure OUC devono essere soddisfatti anche i presupposti seguenti in modo che sia possibile gestire i certificati dei dispositivi e i certificati CA:

- La protezione del progetto è attivata
- Le funzioni Security sono attivate in ciascun CP 1543-1 utilizzato per Secure OUC
- Stesse impostazioni Security in ciascun CP della CPU principale e di backup nello stesso posto connettore
- Per i due CP sono configurati gli stessi certificati CA
- I certificati dei dispositivi dei CP si riferiscono sempre a entrambi i CP, ad es. la configurazione di un nome alternativo per il proprietario del certificato (SAN) ha effetto su entrambi i certificati

---

NOTA

Nessuna sincronizzazione automatica delle impostazioni di sicurezza

In STEP 7 le impostazioni di sicurezza non vengono sincronizzate automaticamente nei CP. Pertanto i CP della CPU principale e della CPU di backup che si trovano nello stesso posto connettore devono essere configurati in modo identico.

Possibilità di collegamento per Open User Communication tramite CP

Nelle configurazioni seguenti, il collegamento OUC con un partner passa sempre attraverso l'interfaccia CP locale, indipendentemente dal fatto che venga utilizzato OUC o Secure OUC. A seconda della configurazione utilizzata, è necessario modificare i parametri di collegamento durante la configurazione del collegamento di comunicazione. Selezionare l'ID HW dell'interfaccia nei parametri di collegamento scegliendo una delle opzioni seguenti:

- Utilizzo dell'interfaccia CP con indirizzo IP locale:
  Indicare nel parametro di collegamento "InterfaceId" l'ID HW dell'interfaccia Ethernet locale di un CP, ad es. "Local1~CP_1543-1_1~Ethernet_interface_1". Nello stato del sistema RUN-Redundant vengono utilizzate sia le interfacce CP della CPU principale sia quelle della CPU di backup.
- Utilizzo dell'interfaccia virtuale W1 della CPU con indirizzo IP del dispositivo configurato:
  Indicare nel parametro di collegamento "InterfaceId" l'ID HW dell'interfaccia virtuale di una CPU, ad es. "Local1~Virtual_communication_interface". Nello stato del sistema RUN-Redundant vengono utilizzate sia le interfacce virtuali W1 della CPU principale sia quelle della CPU di backup.
- Utilizzo dell'interfaccia virtuale W1 della CPU con indirizzo IP di sistema configurato:
  Indicare nel parametro di collegamento "InterfaceId" l'ID HW dell'oggetto con la sequenza di caratteri "...HSystemIPRef..." e l'identificazione "Virtual" nel nome predefinito, ad es. "Local1~Virtual_communication_interface~HsystemIPRef_1". Questo oggetto referenzia l'indirizzo IP di sistema dell'interfaccia virtuale W1 della CPU.

Realizzazione del collegamento tramite CP

Il collegamento viene realizzato come nell'interfaccia PROFINET integrata del sistema ridondante S7-1500R/H. Tuttavia è necessario modificare i parametri di collegamento. Selezionare il processore di comunicazione CP 1543-1 da utilizzare nell'elenco a discesa "Interfaccia".

Se si desidera utilizzare l'opzione "Utilizza indirizzo IP di sistema", per l'interfaccia virtuale W1 deve essere configurato un indirizzo IP di sistema.

Selezione dei certificati per Secure Open User Communication tramite CP

A seconda della configurazione della stazione S7-1500R/H con un CP 1543-1 si applicano le seguenti regole dei certificati per la comunicazione con i partner di collegamento:

- Comunicazione tramite interfaccia CP con indirizzo IP locale:
  Utilizzare il certificato del dispositivo del CP per l'autenticazione. Affinché il partner del collegamento possa convalidare il certificato del dispositivo, il certificato CA del CP deve essere presente nell'elenco "Certificati dei dispositivi partner" del partner del collegamento.
- Comunicazione tramite le interfacce virtuali W1 delle CPU con indirizzo IP di sistema configurato:
  Utilizzare un certificato del dispositivo della CPU per l'autenticazione. Affinché il partner del collegamento possa convalidare il certificato del dispositivo, l'autorità di certificazione della CPU deve essere presente nell'elenco "Certificati dei dispositivi partner" del partner del collegamento.

Ulteriori informazioni

Per informazioni sulla creazione e l'assegnazione dei certificati consultare il capitolo Gestione dei certificati (Pagina 68).

Per informazioni sulla Secure Open User Communication tramite l'interfaccia di un CP vedere il capitolo Secure OUC tramite interfaccia CP (Pagina 102).

16.9 Utilizzo di server OPC UA in un sistema S7-1500R/H

16.9.1 Informazioni importanti sul server OPC UA nel sistema S7-1500R/H

Dalla versione firmware V3.1 le CPU S7-1500R/H supportano le funzioni del server OPC UA. Il client OPC UA non è supportato.

Gli ampliamenti per il server OPC UA dei sistemi S7-1500R/H corrispondono alla specifica OPC 10000-4: Services (Rel. 1.04), tenendo conto delle restrizioni descritte di seguito.

Il server OPC UA è accessibile da tutte le interfacce integrate delle CPU e da un CP 1543-1. Allo scopo, il CP deve essere collegato attraverso l'interfaccia W1 virtuale della CPU (area "Accesso al PLC tramite modulo di comunicazione" nelle proprietà della CPU).

Un server OPC UA consente un accesso aperto e standardizzato alla CPU. Nel sistema R/H su ciascuna delle due CPU opera un server OPC UA. I server OPC UA della CPU principale e di quella di backup si sincronizzano tramite meccanismi di ridondanza. Nel funzionamento ridondante, dal punti vista di un client OPC UA si tratta di **un'**applicazione server.

Rispetto alle CPU standard, le CPU S7-1500R/H offrono un modello di informazione ampliato. Con questo modello informativo esteso, è possibile per i client tenere conto delle specifiche del sistema ridondante.

Dal punto di vista di un client OPC UA, per l'accesso al sistema S7-1500R/H vengono utilizzati gli stessi meccanismi (ad es., il Discovery Service) utilizzati per l'accesso alle CPU S7-1500 standard.

Limitazioni per il server OPC UA

Con l'utilizzo del server OPC UA nel sistema S7-1500R/H, sussistono limitazioni sotto il profilo delle prestazioni delle CPU S7-1500 standard:

- Accesso ai dati solo tramite interfacce server. L'interfaccia server SIMATIC standard non è supportata. Pertanto, nessuna esportazione di nodeset (file XML OPC UA dell'interfaccia standard del server SIMATIC).
- L'impiego del GDS non viene supportato (Gestione certificati in runtime)
- Alarms & Conditions non viene supportato
- Nessun accesso all'area di indirizzi del proprio server OPC UA tramite le istruzioni OPC_UA_ReadList e OPC_UA_WriteList.

  In altri termini, le funzioni descritte nelle sezioni seguenti del sistema di informazione TIA Portal non sono possibili:

  – Diagnostica del server OPC UA con OPC_UA_ReadList
  – Impostazione di OPC UA-DataValue con OPC_UA_WriteList
- La risoluzione di data e ora fornita dal server è di 1 ms (CPU standard 1 ns).

Una panoramica delle limitazioni generali del sistema ridondante S7-1500R/H rispetto al sistema di automazione S7-1500 è disponibile nel capitolo "Operazioni preliminari > Limitazioni" nel Manuale di sistema del sistema ridondante S7-1500R/H (https://support.industry.siemens.com/cs/ww/it/view/109754833).

Una descrizione per la progettazione di un server OPC UA (ad es. creazione di interfacce server) si trova nel capitolo Comunicazione OPC UA (Pagina 179) o nel sistema di informazione di TIA Portal.

Influenza sui tempi di ciclo e di reazione

Se si attiva il server OPC UA di un sistema S7-1500R/H, si ha un'influenza sui tempi di ciclo e di reazione.

È necessario considerare i seguenti effetti:

- Il tempo di ciclo per un sistema S7-1500R/H nello stato di sistema ridondante RUN si prolunga attivando il server OPC UA.
- La precisione con cui gli allarmi a priorità più elevata interrompono un ciclo OB, ad es., diminuisce. Esempio: Il "Jitter" per un allarme di schedulazione orologio aumenta.
- Negli altri casi valgono le regole di base indicate nel seguente documento: Manuale di guida alle funzioni "Tempi di ciclo e di reazione" (https://support.industry.siemens.com/cs/it/it/view/59193558).

> ⚠ **CAUTELA**
>
> **Test accurato del tempo di ciclo massimo nella fase di messa in servizio**
>
> Nella fase di messa in servizio controllare se il sistema S7-1500R/H funziona in modo affidabile con il tempo di ciclo massimo impostato, anche in presenza di condizioni Worst-Case (allarmi, carico di comunicazione con il max. numero di Client nonché creazione e interruzione del collegamento).

Presupposti

- TIA Portal V19 con Hardware Support Package (HSP) installato "HSP_V19_0445_001_S71500_RH_3.1".

  Con questo HSP vengono installate le CPU S7-1500R/H.

Ridondanza con OPC UA

Il sistema ridondante composto da 2 o più server è chiamato "Set di server ridondanti" in OPC UA. La ridondanza del server in base alla specifica OPC UA supporta i seguenti modi di funzionamento (Modes of Redundancy):

- Transparent Mode (transparent Redundancy)

  Con il modo di funzionamento trasparente, solo il server è responsabile della commutazione in caso di guasto (Failover). Il client OPC UA non necessita di nozioni di ridondanza per eseguire lo scambio di dati. Per utilizzare il Transparent Mode, il client deve collegarsi con l'indirizzo IP di sistema dell'interfaccia CPU. Se si utilizza un CP 1543-1, impiegare l'interfaccia virtuale W1 della CPU con l'indirizzo IP di sistema configurato.
- Non-transparent Mode (non-transparent Redundancy)

  Nel modo di funzionamento non trasparente, il client è responsabile del passaggio da un server all'altro in caso di guasto (Failover). Il client deve inizializzare le azioni necessarie per beneficiare del sistema ridondante. Per utilizzare il non-transparent Mode, il client deve collegarsi con gli indirizzi IP dei dispositivi delle CPU R/H. Se si utilizza un CP 1543-1, impiegare l'interfaccia virtuale W1 delle CPU con indirizzi IP dispositivi configurati.

Un sistema S7-1500R/H supporta in ugual misura entrambi i modi di funzionamento.

Il Redundant Server Set consente l'accesso alle informazioni per la disponibilità sulla variabile "ServiceLevel"; un byte che riflette numericamente lo "stato di salute" di un server.

Il ServiceLevel consente di trarre conclusioni sullo stato di ridondanza, ad es. se la CPU è principale o di backup o se il sistema si trova nello stato di sistema ridondante RUN. Per le informazioni sul ServiceLevel consultare il capitolo relativo alla modalità non trasparente (Pagina 483).

Ulteriori informazioni

Ulteriori informazioni aggiornate sull'utilizzo del server OPC UA con i sistemi S7-1500R/H sono disponibili nel seguente articolo: FAQ Come si utilizza il server OPC UA in un sistema S7-1500 R/H? (https://support.industry.siemens.com/cs/ww/it/view/109822965)

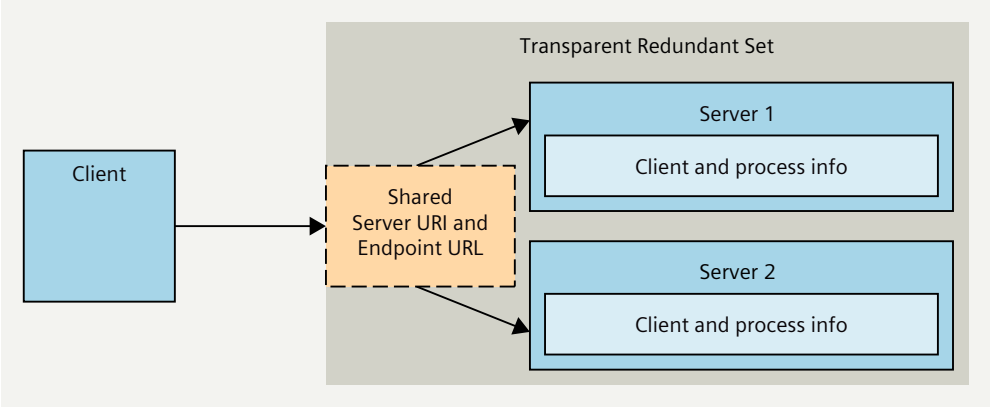
16.9.2 Transparent Mode (transparent Redundancy)

Di seguito vengono illustrati i dettagli della ridondanza trasparente, un modo di funzionamento che consente a un client di gestire il sistema ridondante come se fosse un sistema singolo o un server OPC UA di una CPU standard.

CPU principale sempre raggiungibile tramite l'indirizzo IP del sistema

Per una stazione S7-1500R/H utilizzare l'indirizzo IP di sistema per la ridondanza trasparente. Un client utilizza l'indirizzo IP di sistema per raggiungere la CPU principale, ovvero la CPU che ospita attualmente questo indirizzo IP.

La figura seguente mostra un esempio per l'utilizzo della ridondanza trasparente secondo OPC UA 10000-4.



Comportamento in caso di guasto della CPU principale (RUN-Redundant > RUN-Solo)

In caso di errore (Failover) la comunicazione tra client e server è interrotta per breve tempo. Tutte le sessioni e le sottoscrizioni create vengono mantenute e possono essere riprese - con la nuova CPU principale. Il comportamento dal punto di vista del client corrisponde in questo caso al comportamento in caso di errori temporanei della comunicazione, nei quali la sessione viene ripresa.

Non appena la nuova CPU principale torna ad essere accessibile con l'indirizzo IP di sistema dopo il failover, il client può riprendere la comunicazione (riattivare la sessione).

Comportamento in caso di ripristino della ridondanza (SYNCUP > RUN-Redundant)

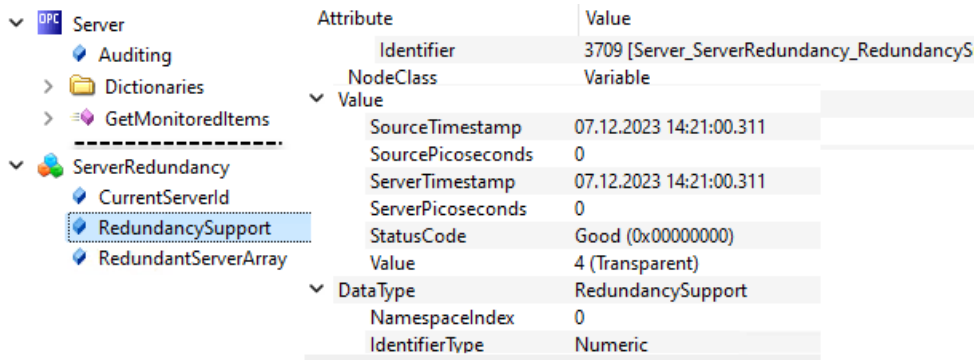
Se lo stato iniziale del sistema ridondante viene ripristinato dopo un failover, ad es. dopo la sostituzione della CPU guasta, il sistema esegue un SYNCUP.

Durante il SYNCUP, in entrambe le CPU vengono riavviati rispettivamente i server OPC UA. Tutte le sessioni e le sottoscrizioni esistenti vengono cancellate.

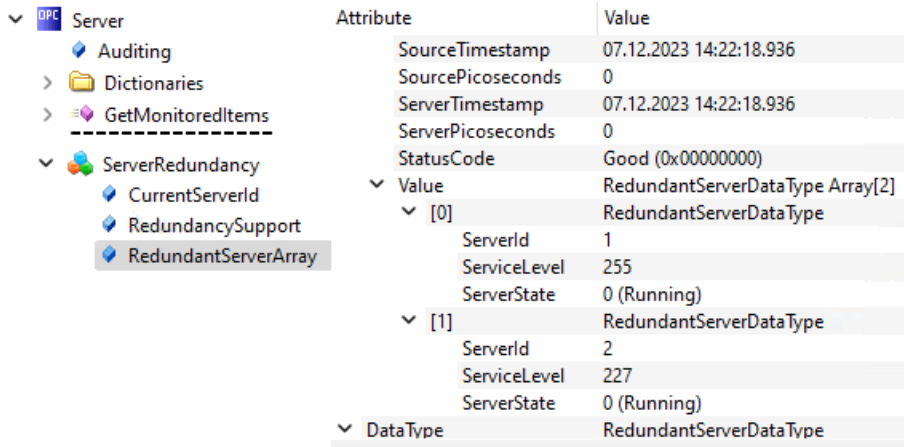
Non appena il server della CPU principale è nuovamente accessibile, il client deve ricreare le sessioni e le sottoscrizioni.

Nodi rilevanti nel modello di informazione per la ridondanza trasparente

Informazioni nel modello informativo relative alla modalità trasparente della stazione R/H si trovano nell'oggetto "ServerRedundancy" (indice dello spazio dei nomi "0" o spazio dei nomi "http://opcfoundation.org/UA/").



I ServerState e ServiceLevel dei server ridondanti possono essere rilevati tramite RedundantServerArray:



Maggiori informazioni sul ServiceLevel sono riportate nella sezione seguente.

16.9.3 Non-transparent Mode (non-transparent Redundancy)

Di seguito sono illustrati i dettagli sulla ridondanza non trasparente. In questo modo di funzionamento, OPC UA mette a disposizione le seguenti informazioni per un client:

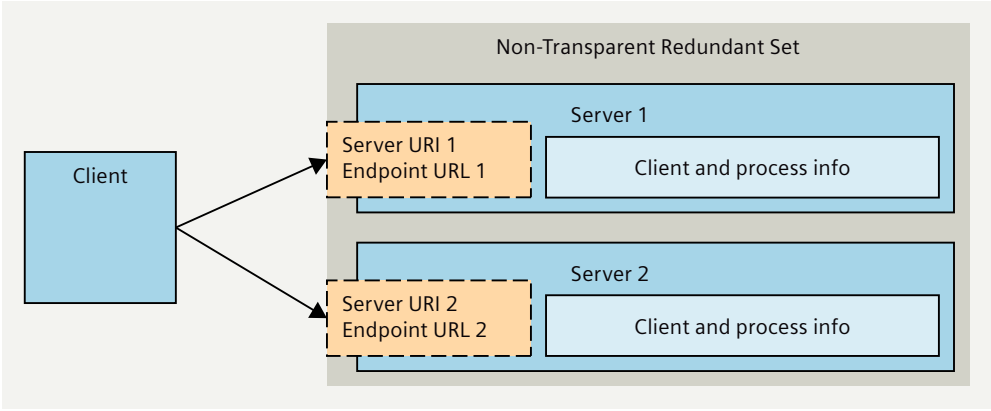
- Quali server sono disponibili nel set di server ridondanti
- Quali tipi di commutazione (Failover) sono supportati tra i server disponibili

Queste informazioni consentono al client di determinare le operazioni da eseguire per ottenere una commutazione. Il client non deve solo poter interpretare l'attributo ServerRedundancy, ma anche conoscere il modello di informazione esteso del server ridondante.

Parametri di indirizzamento del server OPC UA ridondante in un sistema R/H

A differenza della ridondanza trasparente, i server del sistema R/H sono indirizzati tramite il loro indirizzo IP univoco (indirizzo IP del dispositivo o indirizzo IP virtuale nel caso di un CP 1543-1 progettato).

La figura seguente mostra un esempio per l'utilizzo della ridondanza non trasparente secondo OPC UA 10000-4.



Comportamento in caso di guasto della CPU principale: Modalità di commutazione (Failover modes)

Secondo OPC 1000-4: Services, i server possono supportare diverse modalità di commutazione: Cold, Warm, Hot e HotAndMirrored.

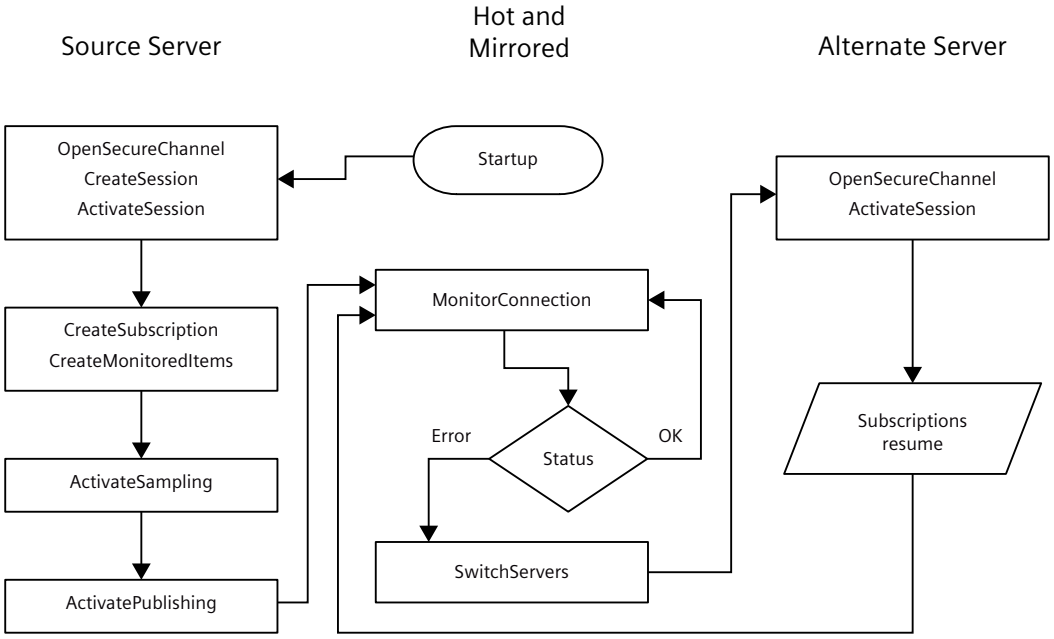
Il server OPC UA di una CPU S7-1500R/H supporta la modalità di commutazione "HotAndMirrored".

Il client deve sapere che il server OPC UA è un server ridondante e deve eseguire il processo di commutazione in un certo modo grazie alle modalità di commutazione supportate (Failover modes).

Il modo in cui deve avvenire il processo di commutazione è descritto nella specifica OPC 10000-4: Services al cap. "Client Failover behaviour - HotAndMirrored". Il client è responsabile del monitoraggio dello stato del server, ossia dell'interrogazione periodica del ServiceLevel e della commutazione al server alternativo (nel caso di un sistema S7-1500R/H, si tratta della CPU di backup) in caso di guasto. Questo tipo di controllo della ridondanza offre i vantaggi seguenti:

- Il client ha il pieno controllo sulla selezione del server alternativo.
- Il client può accedere al server OPC UA attraverso reti separate.

La seguente figura della specifica OPC 10000-4: Services mostra i passi che il client esegue quando riceve il segnale di commutare al "Server alternativo" a causa di un basso valore del livello di servizio del "Server sorgente".



ServiceLevel

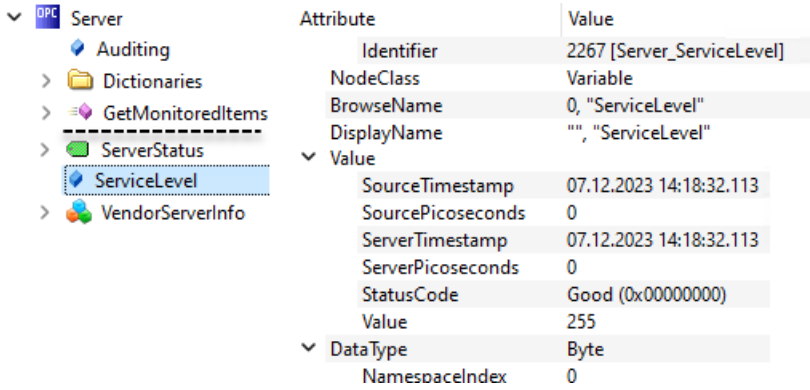
Il ServiceLevel è una variabile modellata come proprietà dell'oggetto ServerType nell'area indirizzi del server. È possibile utilizzare il ServiceLevel per sapere, ad es. se il server indirizzato sta ancora fornendo dati. Il ServiceLevel è un valore numerico per lo "Stato di salute" del server e fornisce quindi al client un trigger per la commutazione del server.

La struttura dell'oggetto ServerType è descritta nella specifica OPC 10000-5: Information Model al cap. "ServerType".

In S7-1500R/H per i relativi server OPC UA valgono i seguenti valori ServiceLevel:

- RUN-Redundant ServiceLevel CPU principale = 255 (CPU in RUN), ServiceLevel CPU di backup = 227 (CPU in RUN).
- **CPU in STOP**: ServiceLevel della CPU guasta (passaggio RUN-STOP) = 1 (NoData). È il trigger per il client per la commutazione (Failover).

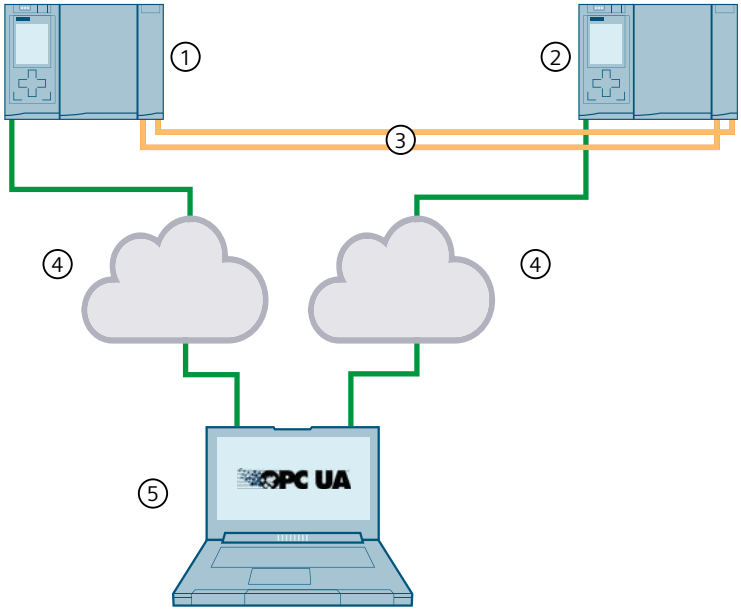
Esempio di una CPU principale in RUN:



Applicazione della ridondanza non trasparente

Se un client accede al server OPC UA attraverso sottoreti diverse, cioè indipendenti, non è possibile una ridondanza trasparente utilizzando l'indirizzo IP di sistema.

La seguente figura mostra una configurazione con un sistema H, collegati tramite due sottoreti con un client.

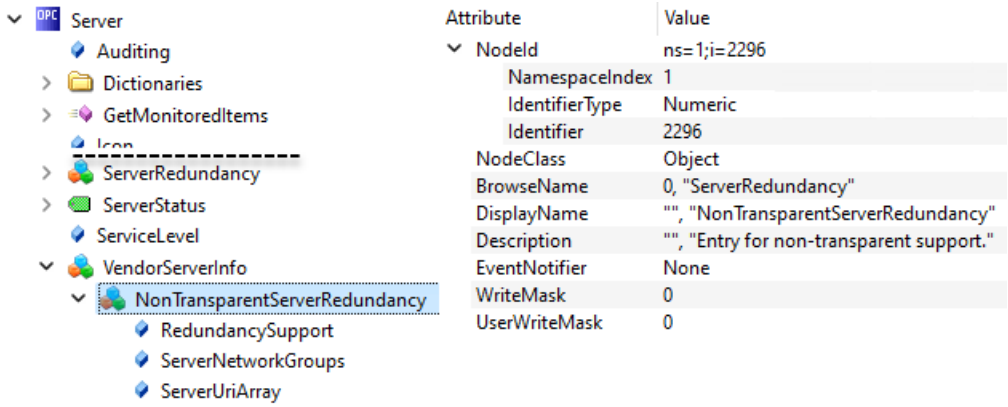


Il client può collegarsi al sistema H tramite le due reti indipendenti. Entrambe le H-CPU non sono collegate tramite una delle reti. In questo modo è possibile tolleranze il guasto di una rete.

Per la modalità non trasparente non sono richieste sottoreti indipendenti. È possibile utilizzare la modalità non trasparente anche per le configurazioni con una sottorete.

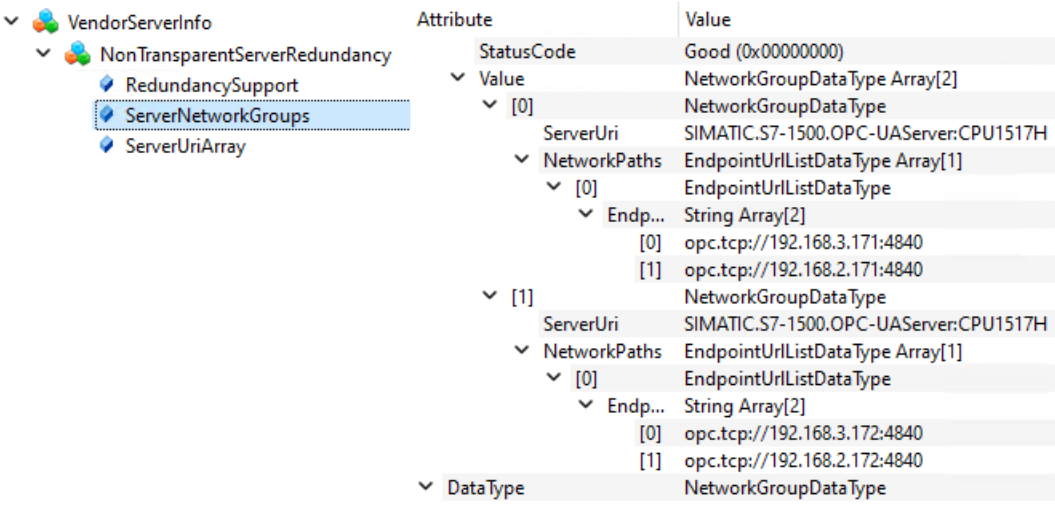
Nodi rilevanti nel modello di informazione per la ridondanza non trasparente

Le informazioni rilevanti per la modalità non trasparente nel modello di informazione della stazione R/H si trovano nell'oggetto "VendorServerInfo", un oggetto segnaposto per le informazioni specifiche del produttore sul server OPC UA. Questo nodo specifico del vendor e i nodi sottostanti si trovano nello spazio dei nomi definiti per il server locale, ad es. urn: SIMATIC.S7-1500.OPC-UA.Application:PLC_1 con l'indice dello spazio dei nomi 1.



Nell'oggetto ServerRedundancy riportato di seguito, un client può trovare tutte le informazioni necessarie per collegarsi al sistema R/H.

L'attributo ServerUriArray-Property consente al client di selezionare un server adatto. Le informazioni sui percorsi di rete da utilizzare per raggiungere i server sono reperibili tramite il tipo di oggetto NonTranparentNetworkRedundancyType - un sottotipo di NonTransparentRedundancyType. Il tipo di oggetto NonTranparentNetworkRedundancyType fa riferimento alla variabile ServerNetworkGroups che contiene un array di server (EndpointUrlList) e informazioni sui percorsi di rete ridondanti per ciascun server (NetworkPaths).



La descrizione dettagliata dei nodi rilevanti con i relativi riferimenti sotto il nodo VendorServerInfo si trova nella specifica OPC UA (OPC 10000-5: Information Model).

Per un sistema S7-1500R/H, il sito EndpointUrlList contiene una voce per ogni indirizzo IP di dispositivo o indirizzo IP di dispositivo virtuale (se configurato insieme a un CP 1543-1) tramite il quale è possibile raggiungere i server del sistema S7-1500R/H. In caso di guasto, il

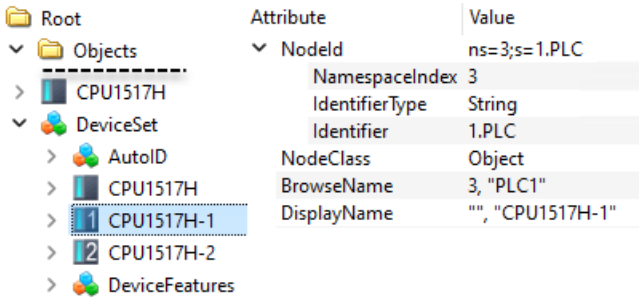
client può decidere se connettersi allo stesso server attraverso un percorso diverso o se selezionare il server ridondante.

16.9.4 Modello di informazione in dettaglio

Le sezioni seguenti illustrano la struttura del modello di informazione di un sistema S7-500R/H in dettaglio. Il modello di informazione è adatto sia ai client che accedono al sistema R/H come una CPU standard, sia ai client che desiderano il pieno controllo sul sistema R/H.

Modello di informazione esteso per sistemi ridondanti

La figura seguente mostra, a titolo di esempio, come il sistema R/H sia modellato nel nodo DeviceSet come un oggetto separato insieme alle singole CPU R/H.



Sistema R/H come nodo separato nel modello di informazione

Sotto il nodo DeviceSet, oltre ai nodi per ciascuna CPU R/H, è presente anche un nodo come rappresentante del sistema R/H.

Il server OPC UA è momentaneamente non disponibile nello stato di sistema SYNCUP (stato operativo RUN-Syncup per la CPU principale). In questo stato il server si riavvia.

I nodi rappresentano le seguenti informazioni:

Nodi <Nome parametrizzato>	Contenuto	Dati raggiungibili nello stato di sistema RUN-Redundant	Dati raggiungibili nello stato di sistema RUN-Solo
<Sistema R/H>	Informazioni sul sistema R/H	Dati dell'interfaccia server (identici per entrambe le CPU) Informazioni specifiche per la CPU della CPU principale	Il client è collegato con: • CPU principale: Dati dell'interfaccia server della CPU principale. • CPU di backup: i dati dell'interfaccia server (se ServiceLevel = NoData: i dati dell'interfaccia server non sono validi o non sono disponibili).
<PLC 1>	Informazioni su R/H-CPU con ID ridondanza 1	Dati dell'interfaccia server (identici per entrambe le CPU) Informazioni specifiche della CPU con ID ridondanza 1	Il client è collegato con:

Nodi <Nome parametrizzato>	Contenuto	Dati raggiungibili nello stato di sistema RUN-Redundant	Dati raggiungibili nello stato di sistema RUN-Solo
			• PLC 1 (= CPU principale): Dati dell'interfaccia server della CPU principale. • PLC 1 (= CPU di backup): dati dell'interfaccia server (contrassegnati tramite ServiceLevel = NoData come non validi o non disponibili). • PLC 2 (= CPU di backup): Nessun dato (errore di accesso BadInvalidState / (BadResourceUnavailable))
<PLC 2>	Informazioni su R/H-CPU con ID ridondanza 2	Dati dell'interfaccia server (identici per entrambe le CPU) Informazioni specifiche della CPU con ID ridondanza 2	Il client è collegato con: • PLC 2 (= CPU principale): Dati dell'interfaccia server della CPU principale. • PLC 2 (= CPU di backup): dati dell'interfaccia server (contrassegnati tramite ServiceLevel = NoData come non validi o non disponibili). • PLC 1 (= CPU di backup): Nessun dato (errore di accesso BadInvalidState / (BadResourceUnavailable))

Nodi sotto i nodi del dispositivo

Per nodi dei dispositivi si intendono i nodi sotto il nodo DeviceSet (sistema R/H, PLC 1, PLC 2).

Gli attributi "OperatingMode" e "RedundancyMode" sono di particolare interesse.

OperatingMode

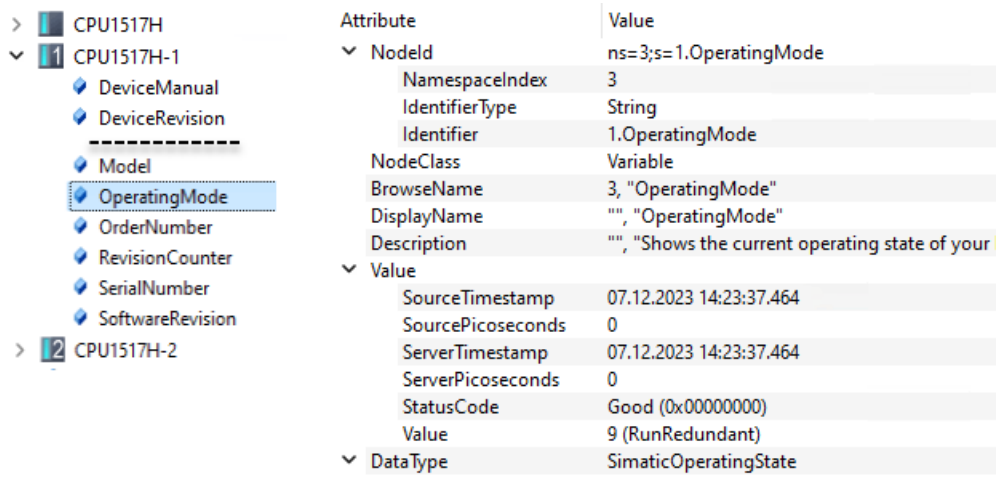
OperatingMode-Property sotto il nodo di sistema R/H mostra lo stato di funzionamento della CPU principale per il nodo di sistema R/H.

Per le singole CPU del sistema R/H e per il sistema R/H sono stati definiti i seguenti valori:

OperatingMode	Sistema R/H	R/H-CPU
1 (STOP - aggiornamento FW)	x	x
3 (STOP - inizializzazione)	x	x
4 (STOP)	x	x
6 (avviamento)	x	x
8 (RUN)	x	x
9 (run ridondante)	x	x
10 (HALT)	x	x
13 (guasto)	x	x
14 (Ricerca degli errori)	x	x
15 (No Power)	x	x

OperatingMode	Sistema R/H	R/H-CPU
17 (STOP - senza attivazione senza corrente/del valore sostitutivo per le uscite)	x	x
18 (RUN - con attivazione senza corrente/del valore sostitutivo per le uscite)	x	x
19 (test del programma)	x	x
20 (Run Program Test)	8 (RUN)	x (principale; backup in Test Mode)
21 (RUN Syncup)	8 (RUN)	x
22 (Syncup)	8 (RUN)	x
31 (Remote Unknown)	x	-

Esempio con attributi dei nodi per OperatingMode:

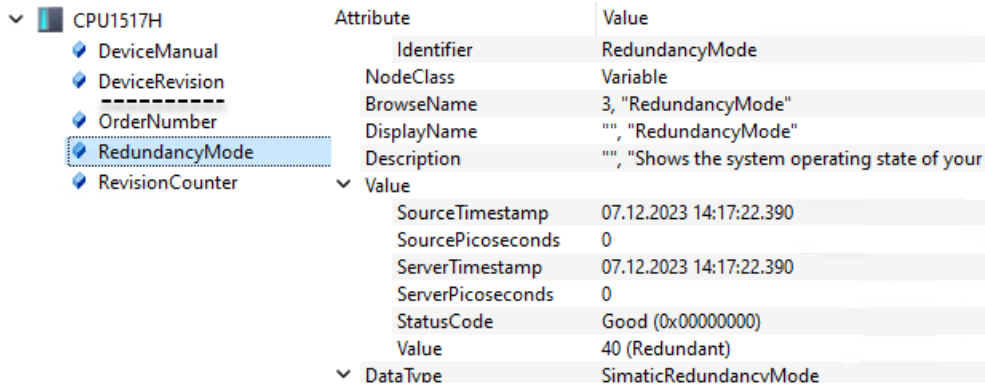


RedundancyMode

RedundancyMode-Property mostra lo stato del sistema R/H ed è disponibile solo nel nodo di sistema R/H.

RedundancyMode	Sistema R/H	R/H-CPU
32 (No Power)	x	-
33 (STOP)	x	-
34 (HALT)	x	-
35 (avviamento)	x	-
37 (Run Solo)	x	-
38 (Syncup)	x	-
39 (test del programma)	x	-
40 (ridondante)	x	-

Esempio con attributi dei nodi per RedundancyMode:



16.9.5 Istruzioni aggiornate per metodi Server

Per implementare i metodi server in una CPU S7-1500 utilizzare le istruzioni "OPC_UA_ServerMethodPre" e "OPC_UA_ServerMethodPost". Di seguito sono illustrati i dettagli della nuova versione V1.1 di queste due istruzioni.

- Per le CPU S7-1500R/H a partire dalla versione FW V3.1 la versione V1.1 delle istruzioni server è obbligatoria - l'utilizzo della versione V1.0 non è ammessa.
- Per le CPU standard S7-1500 vale la raccomandazione: Per i nuovi progetto da TIA Portal V19 e dalla versione firmware CPU V3.1, utilizzare sempre la nuova versione di istruzioni server V1.1 o superiore.
- All'interno di un progetto è possibile utilizzare sia le istruzioni della versione V1.0, sia le istruzioni della versione V1.1. All'interno di un programma utente CPU è possibile utilizzare solo una versione.

Per implementare i metodi del server nel programma utente, utilizzare l'esempio di programma qui pubblicato e non quello della guida di TIA Portal.

Implementazione dei metodi del server nel programma utente

In primo luogo, ecco una breve sintesi della procedura per fornire un metodo OPC UA al server OPC UA di una CPU S7-1500 tramite il programma utente. Questo metodo può essere richiamato da ogni client OPC UA.

- Un blocco funzionale (FB) rappresenta il metodo server nel programma utente.
- Questo FB deve essere richiamato ciclicamente (ad es. con l'OB 1).
- Nel blocco funzionale deve essere prima richiamata l'istruzione "OPC_UA_ServerMethodPre" per mappare i parametri di ingresso del metodo che il client ha fornito al richiamo nelle corrispondenti variabili della CPU (trasferimento dei dati di ingresso).
- Dopo aver richiamato l'istruzione "OPC_UA_ServerMethodPre", viene elaborato l'algoritmo programmato (il metodo stesso con l'elaborazione dei parametri di ingresso e la preparazione dei parametri di uscita).

- Una volta eseguito l'algoritmo programmato e calcolati i parametri di uscita, è necessario richiamare l'istruzione "OPC_UA_ServerMethodPost". L'istruzione "OPC_UA_ServerMethodPost" assicura che i dati di uscita validi del metodo messi a disposizione del client.
- Durante la creazione dei metodi OPC UA osservare le convenzioni dei nomi:
  - Quando si richiamano i metodi server, la funzione deve essere creata come multistanza; il nome della multistanza deve essere "OPC_UA_ServerMethodPre_Instance"/"OPC_UA_ServerMethodPost_Instance" in modo che il metodo venga creato nello spazio degli indirizzi.
  - Quando si definiscono i parametri di ingresso per il metodo OPC UA nell'area statica del blocco, il nome della variabile deve essere "UAMethod_InParameters", in modo da visualizzare i parametri di ingresso del metodo.
  - Quando si definiscono i parametri di uscita del metodo OPC UA nell'area statica del blocco, il nome della variabile deve essere "UAMethod_OutParameters", in modo da visualizzare i parametri di uscita del metodo.

Sequenza del programma utente

Le due istruzioni "OPC_UA_ServerMethodPre" e "OPC_UA_ServerMethodPost" sono istruzioni asincrone che non hanno un "ingresso REQ" che attiva l'avvio della rispettiva istruzione.

L'istruzione "OPC_UA_ServerMethodPre" viene attivata implicitamente dal client OPC UA che richiama il metodo OPC UA (trigger del fronte). Ciò significa che ogni volta che il metodo non è stato richiamato dal client in un ciclo e viene richiamato nel ciclo successivo, si verifica quanto segue:

- Lo stato STATUS passa da 0x7000 (nessun richiamo) a 0x7001 (primo richiamo). Il parametro di uscita BUSY viene impostato su "1".
- Se il trasferimento dei dati dura più di un ciclo, dopo il primo ciclo lo stato passa a 0x7002 (richiamo intermedio).
- Se il trasferimento dei dati di ingresso è concluso:
  - DONE passa a "1".
  - UAMethodCalled passa a "1".
  - BUSY viene resettato su "0".
- "OPC_UA_ServerMethodPre" e "OPC_UA_ServerMethodPost":
  - Quando il trasferimento dei dati di uscita per l'istruzione OPC_UA_ServerMethodPost è concluso, DONE passa a "1".
    Questa è la condizione per resettare i parametri di ingresso "UAMethod_Finished" e "UMethod_Result" (vedere il programma di esempio).
  - Dopo un ulteriore ciclo, tutti i parametri di uscita vengono resettati (corrisponde a un fronte di discesa per le istruzioni attivate da REQ).
  - Le rispettive istanze delle istruzioni vengono quindi abilitate di nuovo (possono essere attive al massimo 20 istanze simultaneamente).

Compatibilità tra la versione V1.0 e V1.1 delle istruzioni

Tra la versione V1.0 e la V1.1 esistono le seguenti differenze per quanto riguarda le istruzioni del server:

- Reset dei parametri di uscita "UAMethod_Called" dell'istruzione server "OPC_UA_ServerMethodPre":
  - V1.0: "UAMethod_Called" viene resettato automaticamente se sia "DONE" dell'istruzione "OPC_UA_ServerMethodPre" sia "DONE" dell'istruzione "OPC_UA_ServerMethodPost" sono resettati. "UAMethod_Called" viene quindi resettato solo quando anche "OPC_UA_ServerMethodPost" è stato terminato.
  - V1.1: "UAMethod_Called" viene resettato automaticamente se il parametro di uscita "DONE" dell'istruzione "OPC_UA_ServerMethodPre" viene resettato.
- Abilitazione delle istanze di "OPC_UA_ServerMethodPre" e "OPC_UA_ServerMethodPost":
  - V1.0: Nessun richiamo ciclico delle istruzioni server.
  - V1.1: È necessario richiamare ciclicamente le istruzioni del server.

NOTA

Quando si passa ai metodi del server OPC UA dalla versione V1.0 alla versione V1.1, verificare se il programma utente tiene conto delle regole descritte e della modalità di funzionamento adattata. Adattare eventualmente il programma.

Programma di esempio

```
FUNCTION_BLOCK "mySERVER_METHOD"
{ S7_Optimized_Access := 'TRUE' }
VERSION : 0.1
 VAR DB_SPECIFIC
 UAMethod_InParameters : Struct
 IN_BOOL : Bool;
 IN_INT : Int;
 END_STRUCT;
 UAMethod_OutParameters : Struct
 OUT_BOOL : Bool;
 OUT_INT : Int;
 END_STRUCT;
 END_VAR
 VAR
OPC_UA_ServerMethodPre_Instance {InstructionName :=
'OPC_UA_ServerMethodPre'; LibVersion := '1.1'} :
OPC_UA_ServerMethodPre;
 DONE_PRE { S7_SetPoint := 'True'} : Bool;
 BUSY_PRE : Bool;
 ERROR_PRE : Bool;
 STATUS_PRE : DWord;
 UAMethod_Called : Bool;
 OPC_UA_ServerMethodPost_Instance {InstructionName :=
'OPC_UA_ServerMethodPost'; LibVersion := '1.1'} :
OPC_UA_ServerMethodPost;
 UAMethod_Result { S7_SetPoint := 'True'} : DWord;
 UAMethod_Finished : Bool;
 DONE_POST { S7_SetPoint := 'True'} : Bool;
 BUSY_POST : Bool;
 ERROR_POST : Bool;
```

```
 STATUS_POST : DWord;
 END_VAR
BEGIN
 #OPC_UA_ServerMethodPre_Instance(Done => #DONE_PRE,
 Busy => #BUSY_PRE,
 Error => #ERROR_PRE,
 Status => #STATUS_PRE,
 UAMethod_Called => #UAMethod_Called,
 UAMethod_InParameters := #UAMethod_InParameters);

//Method is called
IF #UAMethod_Called AND NOT #ERROR_PRE THEN

(* Functionality:
InParameters are valid
and copied to OutParameters *)

#UAMethod_OutParameters.OUT_BOOL:= #UAMethod_InParameters.IN_BOOL;

#UAMethod_OutParameters.OUT_INT := #UAMethod_InParameters.IN_INT;


(* If Method is finished without errors
prepare output parameters of OPC_UA_ServerMethodPost accordingly *)

#UAMethod_Result := 0;
 #UAMethod_Finished := TRUE;
 END_IF;



#OPC_UA_ServerMethodPost_Instance(UAMethod_Result :=
#UAMethod_Result,
 UAMethod_Finished := #UAMethod_Finished,
 Done => #DONE_POST,
 Busy => #BUSY_POST,
 Error => #ERROR_POST,
 Status => #STATUS_POST,
 UAMethod_OutParameters := #UAMethod_OutParameters);

//Reset Input Parameters after OPC_UA_ServerMethodPost is done
IF #DONE_POST OR #ERROR_POST THEN

#UAMethod_Finished := FALSE;
 #UAMethod_Result := 0;

END_IF;



END_FUNCTION_BLOCK
```

Industrial Ethernet Security con CP 1543-1 17

Protezione completa - Compito di Industrial Ethernet Security

Industrial Ethernet Security consente di proteggere singoli dispositivi, celle di automazione o segmenti di una rete Ethernet. La trasmissione dei dati può essere inoltre protetta attraverso la combinazione di diverse misure di sicurezza:

- Spionaggio di dati
- Manipolazione dei dati
- Accessi non autorizzati

Misure di sicurezza

- Firewall
  - IP Firewall con Stateful Packet Inspection (layer 3 e 4)
  - Firewall anche per telegrammi Ethernet "non IP" secondo IEEE 802.3 (layer2)
  - Limitazione della larghezza di banda
  - Regole firewall globali

  Tutti i nodi che si trovano in un segmento di rete interno di un CP 1543-1 sono protetti da questo firewall. Eccezione: Quando si accede alla CPU tramite l'interfaccia del CP con la funzione "Accesso al PLC tramite il modulo di comunicazione", il collegamento non è protetto da firewall.
- Logging

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

  Per la trasmissione di pagine Web crittografate, ad es. per il controllo del processo.
- FTPS (modalità esplicita)

  Per la trasmissione codificata di file.
- NTP protettto

  Per la sincronizzazione e la trasmissione sicura dell'ora.
- SNMPv3

  Per la trasmissione continua sicura delle informazioni di analisi della rete.

- Gruppi VPN
  Con la progettazione è possibile unire il CP 1543-1 ad altre unità Security per formare dei gruppi VPN . Tra tutte le unità Security di un gruppo VPN vengono creati dei tunnel IPsec (VPN). Tutti i nodi interni di queste unità Security possono comunicare tra loro in modo sicuro attraverso questo tunnel.
- Protezione per dispositivi e segmenti di rete

  Le funzioni di protezione Firewall e gruppi VPN possono estendersi dal funzionamento di singoli dispositivi, a più dispositivi, fino a interi segmenti di rete.

Ulteriori informazioni

Una panoramica dei link agli articoli principali sulla Industrial Security si trova in questa FAQ (https://support.industry.siemens.com/cs/ww/it/view/92651441).

17.1 Firewall

Compiti di Firewall

La funzionalità Firewall ha il compito di proteggere reti e stazioni da influenze esterne e disturbi. Ciò significa che sono consentite solo determinate relazioni di comunicazione definite precedentemente.

Per filtrare il traffico di dati si possono utilizzare tra l'altro indirizzi IPv4, sottoreti IPv4, numeri di porta o indirizzi MAC.

La funzionalità Firewall può essere configurata per i seguenti livelli di protocollo:

- IP Firewall con Stateful Packet Inspection (layer 3 e 4)
- Firewall anche per telegrammi Ethernet "non IP" secondo IEEE 802.3 (layer 2)

Regole firewall

Le regole del firewall descrivono quali pacchetti sono consentiti o vietati in una determinata direzione.

17.2 Logging

Funzionalità

Ai fini del test e del controllo il modulo Security dispone delle funzioni di diagnostica e di logging.

- Funzioni di diagnostica

  Comprendono diverse funzioni di sistema e di stato che possono essere utilizzate in modalità online.

- Funzioni di logging

  Si tratta della registrazione degli eventi di sistema e di sicurezza. A seconda del tipo di evento la registrazione avviene in un area di buffer locale temporanea o permanente del CP 1543-1. In alternativa è anche possibile eseguire la registrazione in un server di rete.

  La parametrizzazione e valutazione di queste funzioni presuppone un collegamento alla rete.

Registrazione di eventi con funzioni di logging

Gli eventi da registrare vengono definiti con le impostazioni di Log. Per la registrazione si possono configurare le seguenti varianti:

- Logging locale

  In questa variante si registrano gli eventi nei buffer locali del CP 1543-1. Nella finestra di dialogo Online del Security Configuration Tool si può quindi accedere a queste registrazioni, visualizzarle e archiviarle nella service station.

- Rete Syslog

  Nella rete Syslog si utilizza un server Syslog presente nella rete. Questo server registra gli eventi in funzione della configurazione nelle impostazioni di Log.

17.3 Client NTP

Funzionalità

Per verificare la validità temporale di un certificato e per registrare la data e l'ora delle registrazioni Log, nel CP 1543-1, proprio come nella CPU, vengono indicate la data e l'ora. L'ora è sincronizzabile tramite NTP. Il CP 1543-1 inoltra alla CPU l'ora sincronizzata attraverso il bus backplane del sistema di automazione. In questo modo anche la CPU dispone di un'ora sincronizzata per elaborare gli eventi temporizzati nel programma utente.

L'impostazione automatica e la sincronizzazione periodica dell'ora viene effettuata tramite un server NTP con o senza protezione. Al CP 1543-1 possono essere assegnati max. 4 server NTP. Non è possibile eseguire una configurazione mista di server NTP senza protezione e server NTP con protezione.

17.4 SNMP

Funzionalità

Il CP 1543-1 supporta, proprio come la CPU, la trasmissione di informazioni di Management tramite il Simple Network Management Protocol (SNMP). A tale scopo, sul CP/sulla CPU è installato un "agente SNMP" che riceve e risponde alle richieste del SNMP. Le informazioni sulle proprietà dei dispositivi che supportano SNMP sono contenute nei cosiddetti file MIP (Management Information Base) per accedere ai quali l'utente deve disporre dei diritti necessari.

Con il SNMPv1 viene inviato anche la "Community String". La "Community String" è come una password che viene inviata insieme alla richiesta del SNMP. Se la Community String è corretto le informazioni richieste vengono inviate. Se la stringa è errata la richiesta viene ignorata.

Nel SNMPv3 i dati possono essere trasferiti codificati. Per questo, selezionare una procedura di autenticazione (ad es. SHA) oppure una procedura di autenticazione e di codifica (ad es. AES).

L'utilizzo di SNMP per il CP/la CPU può essere attivato e disattivato. Disattivare SNMP se le direttive di sicurezza nella rete non ammettono SNMP o se si utilizza una propria soluzione SNMP.

L'attivazione e la disattivazione di SNMP per la CPU è descritta al capitolo SNMP (Pagina 125).

17.5 VPN

Funzionalità

Per le unità Security che proteggono la rete interna, i tunnel VPN (Virtual Private Network) mettono a disposizione un collegamento dati sicuro attraverso la rete esterna non sicura.

Per il tunneling, l'unità utilizza il protocollo IPsec (modo di tunneling di IPsec).

In STEP 7 è possibile assegnare le unità Security a dei gruppi VPN. Tra tutte le unità di un gruppo VPN vengono creati automaticamente dei tunnel VPN. Un'unità in un progetto può appartenere contemporaneamente a più gruppi VPN diversi.

Glossario

Accoppiamento punto a punto

Scambio di dati bidirezionale mediante moduli di comunicazione con interfaccia seriale tra due partner di comunicazione.

Apparecchiatura da campo

→ Dispositivo

Bus

Supporto di trasmissione che collega tra di loro più nodi. La trasmissione dati, affidata a cavi elettrici o in fibra ottica, può essere sia seriale che parallela.

Certificati autofirmati

Sono certificati firmati con la propria chiave privata e utilizzati come certificati di entità finale.

La firma di questi certificati viene verificata con la chiave pubblica di chi li ha emessi.

Gli attributi "Richiedente" ed "Emittente" dei certificati autofirmati devono essere identici: infatti sono stati firmati dalla stessa persona.

Il campo "CA" deve essere "False".

I certificati autofirmati si possono utilizzare ad es. come certificato dell'applicazione per un client OPC UA.

Il procedimento per creare un certificato autofirmato con il generatore di certificati OPC Foundation è descritto qui (Pagina %getreference).

Certificati CA root

→ *Vedere anche Certificato radice*

Certificati dei dispositivi

Questi certificati sono firmati da un'autorità di certificazione (CA).

La firma di un certificato di entità finale viene verificata con la chiave pubblica del certificato dell'autorità di certificazione.

Gli attributi "Richiedente" ed "Emittente" non devono essere identici.

Nel "Richiedente" è indicato ad es. il nome di un programma come nel certificato dell'applicazione OPC UA.

L'"Emittente" deve contenere l'autorità di certificazione che ha firmato questo certificato.

Il campo "CA" deve essere "False".

Certificato CA intermedio

Questo è il certificato di un'autorità di certificazione firmato con la chiave privata di un'autorità di certificazione root.

Questa autorità intermedia firma con la propria chiave privata i certificati di entità finale.

La firma di questi certificati di entità finale viene verificata con la chiave pubblica dell'autorità di certificazione intermedia.

Gli attributi "Richiedente" ed "Emittente" del certificato CA intermedio non devono essere identici: infatti questa autorità di certificazione non ha firmato il certificato personalmente.

Il campo "CA" deve essere "True".

Certificato di entità finale

→ *Vedere anche Certificato del dispositivo*

Certificazione radice

Questo è il certificato di un'autorità di certificazione. Questa autorità firma con la propria chiave privata i certificati di entità finale e i certificati CA intermedi.

Gli attributi "Richiedente" ed "Emittente" di questo certificato devono essere identici: questa autorità di certificazione ha firmato il certificato personalmente.

Il campo "CA" deve essere "True".

TIA Portal V14 possiede un certificato CA root di questo tipo:

Se si configura in TIA Portal il server OPC UA di un S7-1500, TIA Portal genera per il server OPC UA un certificato di entità finale e lo firma con la propria chiave privata.

La firma di questo certificato di entità finale è verificabile con la chiave pubblica di TIA Portal. Questa chiave è contenuta nel certificato CA root di TIA Portal.

Client

Nodo in una rete che richiede un servizio da un altro nodo nella rete (server).

CM

→ Modulo di comunicazione

Comunicazione commutata

Oltre agli indirizzi IP dei dispositivi delle CPU il sistema ridondante S7-1500R/H supporta gli indirizzi IP:

- Indirizzo IP di sistema per le interfacce PROFINET X1 di entrambe le CPU (indirizzo IP di sistema X1)
- Indirizzo IP di sistema per le interfacce PROFINET X2 di entrambe le CPU (indirizzo IP di sistema X2)

Gli indirizzi IP di sistema si utilizzano per la comunicazione con altri dispositivi (ad es. dispositivi HMI, CPU, PG/PC). Attraverso l'indirizzo IP di sistema i dispositivi comunicano sempre con la CPU principale del sistema ridondante. Questo garantisce che, dopo un guasto della CPU principale, il partner della comunicazione in funzionamento ridondante possa

comunicare con la nuova CPU principale (prima CPU di backup) nello stato di sistema RUN singolo.

CP

→ Processore di comunicazione

CPU

Central **P**rocessing **U**nit = unità centrale del sistema di automazione S7 con unità di controllo, di calcolo, memoria, sistema operativo e interfaccia per il dispositivo di programmazione.

CPU di backup

Se il sistema R/H si trova nello stato di sistema RUN-Redundant, la CPU principale esegue il processo. La CPU di backup elabora il programma utente in modo sincrono e può assumere il controllo del processo in caso di guasto della CPU principale.

CPU principale

Se il sistema R/H si trova nello stato di sistema RUN-Redundant, la CPU principale esegue il processo. La CPU di backup elabora il programma utente in modo sincrono e può assumere il controllo del processo in caso di guasto della CPU principale.

Dati coerenti

Dati dai contenuti correlati che non possono essere separati duranti la trasmissione.

Dispositivo

Termine generico per:

- Sistemi di automazione (ad es. PLC, PC)
- Sistemi di periferia decentrata
- Apparecchiature da campo (p. es. PLC, PC, dispositivi idraulici, pneumatici, ecc.) e
- Componenti di rete attivi (ad es. switch, router)
- Accoppiamenti di rete con PROFIBUS, AS-Interface o altri sistemi di bus di campo

Dispositivo di programmazione

I dispositivi di programmazione sono fondamentalmente personal computer portatili, compatti e adatti all'impiego industriale. Essi si distinguono per una speciale dotazione hardware e software per PLC.

Dispositivo PROFIBUS

Dispositivo con almeno un'interfaccia PROFIBUS, elettrica (ad es. RS485) o ottica (ad es. Polymer Optical Fiber).

Dispositivo PROFINET

Dispositivo che dispone sempre di un'interfaccia PROFINET (elettrica, ottica, wireless).

Duplex

Procedimento di trasmissione dati; si distingue tra procedimento full e half duplex.

Half duplex: è disponibile un canale per lo scambio alternato di dati (invio e ricezione alternati rispettivamente in una direzione).

Full duplex: sono disponibili due canali per lo scambio simultaneo di dati in entrambe le direzioni (invio e ricezione simultanei in entrambe le direzioni).

Ethernet

Tecnologia standard internazionale per reti locali (LAN) basata su frame. Essa definisce i tipi di cavi, la segnalazione per il livello fisico, i formati dei pacchetti e i protocolli per il controllo dell'accesso ai supporti dati.

FETCH/WRITE

Servizi server tramite TCP/IP, ISO on TCP e ISO per l'accesso alle aree della memoria di sistema delle CPU S7. L'accesso (funzione client) è possibile da un SIMATIC S5 o da un dispositivo di terzi/PC. FETCH: lettura diretta dei dati; WRITE: scrittura diretta dei dati.

Freeport

Protocollo ASCII liberamente programmabile; qui per la trasmissione dei dati tramite accoppiamento punto a punto.

FTP

File **T**ransfer **P**rotocol; un protocollo di rete per la trasmissione di file tramite reti IP. FTP viene utilizzato per scaricare file dal server al client o per caricare file dal client al server. Inoltre tramite FTP si possono creare e leggere directory, nonché rinominare o cancellare sia le directory che i file.

HMI

Human **M**aschine **I**nterface, dispositivo per la visualizzazione e il comando dei processi di automazione.

IE

→ Industrial Ethernet

IM

→ Modulo d'interfaccia

Immagine di processo (I/O)

In quest'area di memoria la CPU trasmette i valori delle unità di ingressi e uscite. All'inizio del programma ciclico la CPU trasferisce l'immagine di processo delle uscite come stato di segnale ai moduli di uscita. Successivamente la CPU legge gli stati di segnale dei moduli di ingresso nell'immagine di processo degli ingressi. Infine la CPU elabora il programma utente.

Indirizzo IP

Numero binario utilizzato in combinazione con un protocollo Internet (IP) come indirizzo univoco in una rete di computer. Questi dispositivi sono così indirizzabili in modo univoco e accessibili singolarmente. Con l'ausilio di una maschera di sottorete binaria, un indirizzo IPv4 può essere impostato in modo che la parte di rete o la parte di host formi una struttura. La rappresentazione testuale di un indirizzo Ipv4 è costituita ad es. da 4 decimali con un campo di valori da 0 a 255. I decimali sono separati da un punto.

Indirizzo MAC

ID del dispositivo univoco a livello mondiale per tutti i dispositivi Ethernet. L'indirizzo MAC viene già assegnato dal produttore e si compone di 3 byte per l'ID del produttore e 3 byte per l'ID del dispositivo come numero progressivo.

Indirizzo PROFIBUS

Identificativo univoco di un nodo collegato al PROFIBUS. Per l'indirizzamento di un nodo viene trasmesso l'indirizzo PROFIBUS nel telegramma.

Industrial Ethernet

Direttiva per la configurazione di un Ethernet in ambito industriale. La differenza fondamentale rispetto alla tecnologia Ethernet standard è costituita dalla resistenza meccanica e dall'insensibilità ai disturbi dei singoli componenti.

Interfaccia PROFINET

Interfaccia di un modulo che supporta funzioni di comunicazione (ad es. CPU, CP), con una o più porte. All'interfaccia è assegnato un indirizzo MAC già dalla fabbrica. Insieme all'indirizzo IP e al nome del dispositivo (dalla configurazione individuale) questo indirizzo dell'interfaccia garantisce l'identificazione univoca del dispositivo PROFINET nella rete. L'interfaccia può essere elettrica, ottica o wireless.

IO Controller, PROFINET IO Controller

Dispositivo centrale in un sistema PROFINET, per lo più un tradizionale controllore a memoria programmabile o un PC. L'IO Controller configura i collegamenti e gestisce lo scambio di dati con gli IO Device, quindi comanda e controlla il sistema.

IO Device, PROFINET IO Device

Dispositivo della periferia decentrata di un sistema PROFINET che viene controllato e comandato da un IO Controller (ad es. ingressi/uscite decentrati, gruppi di valvole, convertitori di frequenza, switch).

Istruzione

La più piccola unità indipendente di un programma utente, caratterizzata per struttura, funzione o scopo come parte delimitata del programma utente. L'istruzione rappresenta una procedura del processore.

Maschera di sottorete IPv4

Maschera binaria con la quale un indirizzo IPv4 (come numero binario) viene suddiviso in una "parte di rete" e una "parte host".

Master

Nodo attivo di livello superiore nella comunicazione/sottorete PROFIBUS. Se in possesso di diritti di accesso al bus (token), il master può richiedere e trasmettere dati.

→ *Vedere anche Master DP*

Master DP

All'interno del PROFIBUS DP, un master nella periferia decentrata che si comporta secondo la norma EN 50170, parte 3.

→ *Vedere anche Slave DP*

Modbus RTU

Remote **T**erminal **U**nit; protocollo di comunicazione aperto per interfacce seriali basato su un'architettura master/slave.

Modbus TCP

Transmission **C**ontrol **P**rotocol; protocollo di comunicazione aperto per Ethernet basato su un'architettura master/slave. I dati vengono trasmessi come pacchetti TCP/IP.

Modulo di comunicazione

Unità per compiti di comunicazione che viene utilizzata in un sistema di automazione come ampliamento dell'interfaccia della CPU (ad es. PROFIBUS) e che offre possibilità di comunicazione supplementari (PtP).

Modulo d'interfaccia

Modulo nel sistema di periferia decentrata. Il modulo di interfaccia collega il sistema di periferia decentrata con la CPU (IO Controller/master DP) attraverso un bus di campo e appronta i dati per i moduli di periferia.

NTP

Il **N**etwork **T**ime **P**rotocol (NTP) è uno standard per la sincronizzazione degli orologi nei sistemi di automazione tramite Industrial Ethernet. Per Internet, NTP impiega il protocollo di trasporto UDP non orientato alla connessione.

OPC UA

OPC Unified **A**utomation è un protocollo per la comunicazione tra macchine sviluppato dalla OPC Foundation

PG

→ Dispositivo di programmazione

PNO

→ PROFIBUS Nutzerorganisation (organizzazione degli utenti di PROFIBUS)

Porta

Possibilità di collegamento fisico per i dispositivi che sono nodi PROFINET. Le interfacce PROFINET dispongono di una o più porte.

Processore di comunicazione

Unità per compiti di comunicazione ampliati che esegue speciali casi applicativi, ad es. nell'ambito Security.

PROFIBUS

Process **Fi**eld **Bus**: norma europea sui bus di campo.

PROFIBUS DP

Un PROFIBUS con protocollo DP che si comporta conformemente alla norma EN 50170. DP è l'abbreviazione di "periferia decentrata" (scambio di dati ciclico rapido in tempo reale). Dal punto di vista del programma utente la periferia decentrata viene indirizzata esattamente come la periferia centrale.

PROFIBUS Nutzerorganisation (organizzazione degli utenti di PROFIBUS)

Comitato tecnico incaricato della definizione e del continuo sviluppo degli standard PROFIBUS e PROFINET.

PROFINET

Sistema di comunicazione industriale aperto component based per sistemi di automazione distribuiti basato su Ethernet. Tecnologia di comunicazione promossa dall'Organizzazione degli utenti di PROFIBUS.

PROFINET IO

IO è l'abbreviazione di Input/Output, indica la "periferia decentrata" (scambio di dati ciclico, rapido, in tempo reale). Dal punto di vista del programma utente la periferia decentrata viene indirizzata esattamente come la periferia centrale.

In quanto standard di automazione dell'organizzazione PROFIBUS & PROFINET International basato su Ethernet, PROFINET IO definisce un modello di comunicazione, automazione e engineering esteso a tutti i produttori.

PROFINET IO si avvale di una tecnologia switching che consente a ogni nodo di accedere alla rete in qualsiasi momento. La trasmissione simultanea dei dati di più nodi permette così uno sfruttamento della rete molto più efficace. L'invio e la ricezione simultanei sono resi possibili dal funzionamento full duplex di switched Ethernet.

PROFINET IO si basa su switched Ethernet con funzionamento full duplex e una larghezza di banda di 100 Mbit/s.

Programma utente

In SIMATIC si opera una distinzione tra sistema operativo della CPU e programmi utente. Il programma utente contiene tutte le istruzioni, le dichiarazioni e i dati che consentono di controllare un impianto o un processo. Il programma utente è assegnato a un modulo programmabile (ad es. CPU, FM) e può essere strutturato in unità più piccole.

Protocollo

Accordo sulle regole che disciplinano lo svolgimento della comunicazione tra due o più partner di comunicazione.

Protocollo ISO

Protocollo di comunicazione per la trasmissione di dati in Ethernet orientata ai messaggi o ai pacchetti. Questo protocollo è legato all'hardware, molto veloce e consente lunghezze di dati dinamiche. Il protocollo ISO è ideale per quantità di dati medie e grandi.

Protocollo ISO-on-TCP

Protocollo di comunicazione che supporta il routing S7 per la trasmissione di dati in Ethernet orientata ai pacchetti; offre un indirizzamento di rete. Il protocollo ISO-on-TCP è ideale per quantità di dati medie e grandi e consente lunghezze di dati dinamiche.

PtP

Point-**t**o-**P**oint, interfaccia e/o protocollo di trasmissione per lo scambio di dati bidirezionale tra due partner di comunicazione.

Rete

Una rete è costituita da una o più sottoreti interconnesse con un numero qualunque di nodi. Sono ammesse diverse reti contemporaneamente.

Router

Nodo di rete con identificazione univoca (nome e indirizzo) che collega tra loro le sottoreti e realizza il trasporto dei dati ai nodi di comunicazione caratterizzati in modo univoco nella rete.

Routing S7

Comunicazione tra sistemi di automazione S7, applicazioni S7 o stazioni PC in diverse sottoreti S7 tramite uno o più nodi di rete che fungono da router S7.

RS232, RS422 e RS485

Standard per interfacce seriali.

RTU

Modbus RTU (RTU: **R**emote **T**erminal **U**nit, unità terminale remota) trasmette i dati in forma binaria; consente un buon flusso di dati. I dati devono essere convertiti in un formato leggibile prima di poter essere valutati.

Scheda di rete Ethernet

Circuito elettronico per il collegamento di un computer con una rete Ethernet. Consente lo scambio di dati / la comunicazione all'interno della rete.

Security

Termine che riassume le misure per la protezione da quanto segue:

- Perdita dell'affidabilità in seguito all'accesso non autorizzato ai dati
- Perdita dell'integrità in seguito alla manipolazione dei dati
- Perdita della disponibilità in seguito alla distruzione dei dati

Server

Un dispositivo o in generale un oggetto che può fornire determinati servizi; il servizio viene fornito in base alla richiesta del client.

Servizio SDA

Send Data with Acknowledge. SDA è un servizio elementare con il quale un iniziatore (ad es. il master DP) può inviare un messaggio ad un altro nodo e ricevere immediatamente la conferma di avvenuta ricezione.

Servizio SDN

Send Data with No Acknowledge. Questo servizio viene utilizzato principalmente per inviare dati a più stazioni e non viene pertanto confermato. È ideale per compiti di sincronizzazione e segnalazioni di stato.

Sincronizzazione dell'ora

Funzione di trasmissione di un'ora di sistema standard da una singola fonte a tutti i dispositivi nel sistema che consente di impostarne gli orologi in base a questa ora standard.

Sistema di automazione

Controllore a memoria programmabile per la regolazione e il controllo di catene di processo nell'industria di processo e nella tecnica di produzione. A seconda del compito da svolgere il sistema di automazione è costituito da diversi componenti e funzioni di sistema integrate.

Sistema operativo

Software che consente l'utilizzo e il funzionamento di un computer. Il sistema operativo gestisce i supporti operativi come memoria, dispositivi di ingresso e uscita e comanda l'esecuzione dei programmi.

Sistemi ridondanti

I sistemi ridondanti sono caratterizzati dal fatto che importanti componenti di automazione sono presenti più volte (sono ridondanti). In caso di guasto di uno dei componenti ridondanti il controllo del processo viene mantenuto attivo.

Slave

Dispositivo decentrato in un sistema di bus di campo può scambiare dati con un master solo su richiesta di quest'ultimo.

→ *Vedere anche Slave DP*

Slave DP

Slave nella periferia decentrata che viene impiegato in PROFIBUS con il protocollo PROFIBUS DP e che si comporta secondo la norma EN 50170, parte 3.

→ *Vedere anche Master DP*

SNMP

Simple **N**etwork **M**anagement **P**rotocol utilizza il protocollo di trasmissione UDP senza connessione. SNMP funziona in modo analogo al modello client/server. Il manager SNMP controlla i nodi della rete. Gli agenti SNMP raccolgono nei singoli nodi diverse informazioni specifiche della rete, rendendole richiamabili e comandabili in forma strutturata nel MIB (**M**anagement **I**nformation **B**ase). Grazie a queste informazioni un sistema di gestione della rete può eseguire una diagnostica di rete completa.

Sottorete

Parte di una rete i cui parametri devono essere sincronizzati nei nodi (ad es. in PROFINET). Una sottorete comprende i componenti del bus e tutte le stazioni collegate. Le sottoreti possono essere accoppiate ad una rete ad es. tramite gateway o router.

Stati di funzionamento

Gli stati di funzionamento descrivono il comportamento di una singola CPU in un qualsiasi momento.

Le CPU dei sistemi SIMATIC standard dispongono degli stati di funzionamento STOP, AVVIAMENTO e RUN.

La CPU principale del sistema ridondante S7-1500R/H dispone degli stati di funzionamento STOP, AVVIAMENTO, RUN, RUN-Syncup e RUN ridondante. La CPU di backup ha gli stati di funzionamento STOP, SYNCUP e RUN ridondante.

Stati di sistema

Gli stati di sistema del sistema ridondante S7-1500R/H risultano dagli stati di funzionamento della CPU principale e di quella di backup. Il termine stato di sistema viene utilizzato per semplificare un'espressione che indica gli stati di funzionamento di entrambe le CPU che si verificano contemporaneamente. Gli stati di sistema dell'S7-1500R/H sono STOP, AVVIAMENTO, RUN singolo, SYNCUP e RUN ridondante.

Switch

Componenti di rete per il collegamento di più apparecchiature terminali o segmenti di rete in una rete locale (LAN).

TCP/IP

Transmission **C**ontrol **P**rotocol /**I**nternet **P**rotocol; protocollo di rete orientato alla connessione, standard generalmente riconosciuto per lo scambio di dati in reti eterogenee.

Topologia ad albero

Topologia di rete caratterizzata da una struttura ramificata: ad ogni nodo di bus vengono collegati due o più nodi di bus.

Topologia ad anello

Tutti i nodi di una rete sono riuniti in un anello.

Topologia lineare

Topologia di rete caratterizzata dalla disposizione dei nodi di bus in una riga.

Twisted Pair

Fast Ethernet con cavi Twisted Pair basato sullo standard IEEE 802.3u (100 Base-TX). Il supporto di trasmissione è un cavo a 2×2 conduttori, schermato e intrecciato, con un'impedenza caratteristica di 100 Ohm (AWG 22). Le proprietà di trasmissione di questo cavo devono essere conformi alla categoria 5.

La lunghezza max. del collegamento tra terminale e componente di rete non deve essere superiore a 100 m. Le connessioni si basano sullo standard 100 Base-TX con il sistema di connettori RJ45.

UDP

User **D**atagram **P**rotocol; protocollo di comunicazione per una trasmissione dei dati facile e veloce senza conferma. Non dispone dei meccanismi di sicurezza che invece sono presenti in TCP/IP.

USS

Universelles **s**erielles **S**chnittstellen-Protokoll: (protocollo di interfaccia seriale universale); definisce un metodo di accesso secondo il principio masterslave per la comunicazione mediante un bus seriale.

Web server

Software / Servizio di comunicazione per lo scambio di dati via Internet. Il Web server trasmette i documenti a un browser Web tramite protocolli di trasmissione standardizzati (HTTP, HTTPS). I documenti possono essere statici oppure, su richiesta del browser Web, possono essere composti in modo dinamico da fonti diverse attraverso il Web server.

Indice analitico

A

Accoppiamento punto a punto, 35, 174

Advanced Encryption Algorithm, 61

AES, 61

Attacco Man-in-the-Middle, 64

Autorità di certificazione, 64

B

BRCV, 167

BSEND, 167

C

Certificati autofirmati, 65

Certificati digitali, 64

Certificato di entità finale, 67

Certificato server, 273

Certificazione radice, 67

Client OPC UA
- Nozioni di base, 194
- Certificato, 391
- Autenticazione, 393

CM, 29

Coerenza dei dati, 53, 53

Collegamento
- Istruzioni per Open User Communication, 143
- Diagnostica, 449

Comunicazione
- Comunicazione PG, 134
- Comunicazione HMI, 137
- Open User Communication, 140
- Comunicazione aperta, 140
- Protocolli di comunicazione, 141
- Creazione e interruzione, 165
- Comunicazione S7, 166
- Accoppiamento punto a punto, 174
- Routing S7, 419
- Routing di set di dati, 430

Comunicazione aperta
- Parametrizzazione del collegamento, 149
- TCP, ISO on TCP, UDP, configurazione , 149
- Configurazione dell'e-mail, 161
- Configurazione dell'FTP, 162

Comunicazione HMI, 35, 137

Comunicazione PG, 35, 134

Comunicazione S7, 35, 166, 442

Comunicazione sicura, 57

Comunicazione tramite istruzione PUT/GET
- Creazione e parametrizzazione del collegamento, 168

Configurazione del collegamento, 49
- tramite progettazione, 153
- Collegamento ISO con CP 1543-1, 154

CP, 29

Creazione e interruzione di una comunicazione, 165

Crittografia a chiave asimmetrica, 62

Crittografia a chiave simmetrica, 61

D

Diagnostica del collegamento, 449

E

E-mail, 35, 142, 161

F

FDL, 142

Fetch, 35

File di esportazione per OPC UA, 255

Firewall, 496

Firma, 66

FTP, 35, 142, 161, 162

G

GDS, 210, 215
GET, 167
Global Discovery Server (GDS), 210, 215

H

Handshake Protocol, 63

I

IM, 33
Indirizzo IP, indirizzo di emergenza (temporaneo), 452
Industrial Ethernet Security, 495
Interfacce dei moduli di comunicazione
  Accoppiamento punto a punto, 32
Interfacce dei processori di comunicazione, 31
Interfacce di comunicazione, 30
IP Forwarding, 423
ISO, 35, 141
ISO-on-TCP, 141, 149

L

Logging, 497

M

Misure di sicurezza, 495
  Firewall, 496
  Logging, 497
  NTP, 497
  SNMP, 498
Modbus TCP, 142
Modulo d'interfaccia, 33
Modulo di comunicazione, 29

N

NTP, 35, 497

O

Occupazione delle risorse di collegamento, 443
OPC UA
  Introduzione, 184
  NodeId, 189
  Namespace, 189
  Identifier, 190
  Meccanismi di sicurezza, 197
  Firma e crittografia, 200
  Certificati X.509, 202
  Generatore di certificati, 203
  OpenSSL, 204
  Secure Channel, 207
  Collegamento sicuro, 207
  Modello di livello, 208
  GDS, 210
  GDS, 215
  Impostazioni di sicurezza, 234
  Punti finali, 234
  Variabili PLC, 246
  Variabili DB, 246
OpenSSL, 204
Open User Communication
  Caratteristiche, 140
  Protocolli, 141
  Istruzioni, 143
Opzioni di comunicazione
  Panoramica, 35

P

PCT, 431
Private Key, 57
Procedura 3964 (R), 174
Processore di comunicazione, 29
Protocolli per Open User Communication, 141
Protocollo Freeport, 174
Protocollo Modbus (RTU), 174
Protocollo USS, 174
Public Key, 57
PUT, 167

R

Record Protocol, 63

RFC 5280, 57
Richiedente, 64
Risorse di collegamento
  Panoramica, 47
  Panoramica, 436
  Comunicazione HMI, 441
  Routing S7, 442
  Routing di set di dati, 442
  Occupazione, 443
  specifiche della stazione, 445
  specifiche del modulo, 446
Routing di set di dati, 430
Routing S7, 419
  Risorse di collegamento, 442

S

Secure Socket Layer, 63
Security, 495
Server OPC UA
  Area degli indirizzi, 191
  Nozioni di base, 232
  Diritti di scrittura e lettura, 246
  Performance, 254
  Incremento della potenza, 254
  File di esportazione XML, 255
  Messa in servizio, 257
  Nome dell'applicazione, 258
  Indirizzamento, 259
  Porta TCP, 261
  Subscription, 261
  Porta TCP, 263
  Intervallo di trasmissione, 264
  Intervallo di campionamento, 264
  Creazione del certificato server, 267
  Impostazioni di sicurezza, 271
  Adattamento del certificato server, 273
  Autenticazione, 276
  Licenze di runtime, 280
  Licenze di runtime, 281
Servizi di comunicazione
  Risorse di collegamento, 47
Sincronizzazione dell'ora, 35
SNMP, 35, 498
SSL, 63
Syslog, 497

T

TCON, 143
TCP, 35, 141, 149
TDISCON, 143
Tipo di dati di sistema, 144
Titolare del certificato, 64
TLS, 63
Transport Layer Security, 63
TRCV, 143
TRCV_C, 143
TSEND, 143
TSEND_C, 143

U

UDP, 35, 141, 149
URCV, 167
USEND, 167

W

Web server, 35
Write, 35

X

X.509, 57