

# Modicon TMS

## Moduli di espansione

### Guida alla programmazione

Traduzione delle istruzioni originali

EIO0000003695.05

12/2024



# Informazioni di carattere legale

Le informazioni contenute nel presente documento contengono descrizioni generali, caratteristiche tecniche e/o raccomandazioni relative ai prodotti/soluzioni.

Il presente documento non è inteso come sostituto di uno studio dettagliato o piano schematico o sviluppo specifico del sito e operativo. Non deve essere utilizzato per determinare idoneità o affidabilità dei prodotti/soluzioni per applicazioni specifiche dell'utente. Spetta a ciascun utente eseguire o nominare un esperto professionista di sua scelta (integratore, specialista o simile) per eseguire un'analisi del rischio completa e appropriata, valutazione e test dei prodotti/soluzioni in relazione all'uso o all'applicazione specifica.

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nel presente documento sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari.

Il presente documento e il relativo contenuto sono protetti dalle leggi vigenti sul copyright e vengono forniti esclusivamente a titolo informativo. Si fa divieto di riprodurre o trasmettere il presente documento o parte di esso, in qualsiasi formato e con qualsiasi metodo (elettronico, meccanico, fotocopia, registrazione o altro modo), per qualsiasi scopo, senza previa autorizzazione scritta di Schneider Electric.

Schneider Electric non concede alcun diritto o licenza per uso commerciale del documento e del relativo contenuto, a eccezione di una licenza personale e non esclusiva per consultarli "così come sono".

Schneider Electric si riserva il diritto di apportare modifiche o aggiornamenti relativi al presente documento o ai suoi contenuti o al formato in qualsiasi momento senza preavviso.

**Nella misura in cui sia consentito dalla legge vigente, Schneider Electric e le sue consociate non si assumono alcuna responsabilità od obbligo per eventuali errori od omissioni nel contenuto informativo del presente materiale, o per qualsiasi utilizzo non previsto o improprio delle informazioni ivi contenute.**

# Sommario

Informazioni di sicurezza .....	5
Informazioni sul manuale.....	6
Descrizione del TMS .....	10
TMS - Descrizione generale .....	10
Configurazione del bus di comunicazione (COM_Bus) .....	10
Aggiunta di un modulo di espansione TMS .....	12
Modulo Ethernet TMSES4.....	14
Servizi Ethernet.....	14
Presentazione .....	14
Configurazione dell'indirizzo IP .....	16
Modicon M262 Logic/Motion Controller come un dispositivo di destinazione su EtherNet/IP .....	20
Modicon M262 Logic/Motion Controller come dispositivo slave su TCP Modbus .....	21
Configurazione del firewall .....	25
Introduzione .....	25
Procedura per le modifiche dinamiche .....	27
Comportamento del firewall .....	28
Comandi di script del firewall.....	30
Porte utilizzate .....	33
Modulo di comunicazione CANopen TMSCO1 .....	34
Configurazione dell'interfaccia CANopen.....	34
Glossario .....	37
Indice .....	40



# Informazioni di sicurezza

## Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.



L'aggiunta di questo simbolo a un'etichetta di "Pericolo" o "Avvertimento" indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.



Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolinità personale.

### ⚠ PERICOLO

**PERICOLO** indica una situazione di potenziale rischio che, se non evitata, **può provocare morte o gravi infortuni**.

### ⚠ AVVERTIMENTO

**AVVERTIMENTO** indica una situazione di potenziale rischio che, se non evitata, **può provocare morte o gravi infortuni**.

### ⚠ ATTENZIONE

**ATTENZIONE** indica una situazione di potenziale rischio che, se non evitata, **può provocare ferite minori o leggere**.

### AVVISO

Un **AVVISO** è utilizzato per affrontare delle prassi non connesse all'incolinità personale.

## Nota

Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

# Informazioni sul manuale

## Ambito del documento

Questo documento descrive la configurazione dei moduli di espansione TMS per EcoStruxure Automation Expert - Motion e EcoStruxure Machine Expert. Per ulteriori informazioni, consultare i documenti separati forniti nella Guida in linea.

## Nota sulla validità

Per maggiori informazioni sulla validità del presente documento, consulta la guida online del prodotto.

## Lingue disponibili del presente documento

Il presente documento è disponibile nelle seguenti lingue:

- Inglese (EIO0000003691)
- Francese (EIO0000003692)
- Tedesco (EIO0000003693)
- Spagnolo (EIO0000003694)
- Italiano (EIO0000003695)
- Cinese (EIO0000003696)

## Documenti correlati

Titolo della documentazione	Codice prodotto
EcoStruxure Automation Expert - Motion, EcoStruxure Machine Expert, Guida alla programmazione	EIO0000002854 (ENG) EIO0000002855 (FRE) EIO0000002856 (GER) EIO0000002858 (SPA) EIO0000002857 (ITA) EIO0000002859 (CHS)
Modicon M262 Logic/Motion Controller - Guida alla programmazione	EIO0000003651 (ENG) EIO0000003652 (FRA) EIO0000003653 (GER) EIO0000003654 (SPA) EIO0000003655 (ITA) EIO0000003656 (CHS)
TMS Moduli di espansione - Guida hardware	EIO0000003699 (ENG) EIO0000003700 (FRA) EIO0000003701 (GER) EIO0000003702 (SPA) EIO0000003703 (ITA) EIO0000003704 (CHS)

Titolo della documentazione	Codice prodotto
TMSES4 Moduli di espansione - Scheda di istruzioni	PHA44907
TMSCO1 Moduli di espansione - Scheda di istruzioni	PHA44909

Per trovare i documenti online, visitare il centro download Schneider Electric ([www.se.com/ww/en/download/](http://www.se.com/ww/en/download/)).

## Informazioni sul prodotto

### AVVERTIMENTO

#### PERDITA DI CONTROLLO

- Eseguire un'analisi FMEA (Failure Mode and Effects Analysis) o un'analisi dei rischi equivalente dell'applicazione e applicare i controlli di prevenzione e rilevazione prima dell'implementazione.
- Fornire uno stato di posizionamento di sicurezza per sequenze o eventi di controllo indesiderati.
- Fornire percorsi di controllo separati o ridondanti qualora richiesto.
- fornire i parametri appropriati, in particolare per i limiti.
- Esaminare le implicazioni dei ritardi di trasmissione e stabilire azioni di mitigazione.
- Esaminare le implicazioni delle interruzioni del collegamento di comunicazione e stabilire azioni di mitigazione.
- Fornire percorsi indipendenti per le funzioni di controllo (ad esempio, arresto di emergenza, condizioni di superamento limiti e condizioni di guasto) in base alla valutazione dei rischi effettuata e alle normative e regolamentazioni applicabili.
- Applicare le direttive locali per la prevenzione degli infortuni e le linee guida e regolamentazioni sulla sicurezza.<sup>1</sup>
- Testare ogni implementazione di un sistema per il funzionamento adeguato prima di metterlo in servizio.

**Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

<sup>1</sup> Per ulteriori informazioni, fare riferimento a NEMA ICS 1.1 (ultima edizione), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* e a NEMA ICS 7.1 (ultima edizione), *Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems* o alla pubblicazione equivalente valida nel proprio paese.

### AVVERTIMENTO

#### FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Con questa apparecchiatura utilizzare esclusivamente il software approvato da Schneider Electric.
- Aggiornare il programma applicativo ogni volta che si cambia la configurazione dell'hardware fisico.

**Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

# Informazioni sulla terminologia non inclusiva o non sensibile

In qualità di azienda responsabile e inclusiva, Schneider Electric aggiorna costantemente le sue comunicazioni e i suoi prodotti che contengono una terminologia non inclusiva o indelicata. Tuttavia, nonostante questi sforzi, i nostri contenuti possono ancora contenere termini ritenuti inappropriati da alcuni clienti.

## Terminologia derivata dagli standard

I termini tecnici, la terminologia, i simboli e le descrizioni corrispondenti nelle informazioni contenute nel presente documento, o che compaiono nei o sui prodotti stessi, derivano generalmente dai termini o dalle definizioni delle norme internazionali.

Nell'ambito dei sistemi di sicurezza funzionale, degli azionamenti e dell'automazione generale, tali espressioni possono includere, tra l'altro, termini quali *sicurezza*, *funzione di sicurezza*, *stato sicuro*, *guasto*, *reset guasto*, *malfunzionamento*, *errore*, *reset errore*, *messaggio di errore*, *pericoloso* e così via.

Queste norme comprendono, tra le altre:

Norma	Descrizione
IEC 61131-2:2007	Controller programmabili, parte 2: Requisiti per apparecchiature e test.
ISO 13849-1:2023	Sicurezza dei macchinari: Parti di sicurezza dei sistemi di controllo. Principi generali per la progettazione.
EN 61496-1:2020	Sicurezza dei macchinari: Electro-Sensitive Protective Equipment, dispositivo eletrosensibile di protezione. Parte 1: Requisiti generali e test
ISO 12100:2010	Sicurezza dei macchinari - Principi generali di progettazione - Valutazione e riduzione dei rischi
EN 60204-1:2006	Sicurezza dei macchinari - Equipaggiamento elettrico delle macchine - Parte 1: Requisiti generali
ISO 14119:2013	Sicurezza dei macchinari - Dispositivi di interblocco associati alle protezioni - Principi di progettazione e selezione
ISO 13850:2015	Sicurezza dei macchinari - Arresto di emergenza - Principi di progettazione
IEC 62061:2021	Sicurezza dei macchinari - Sicurezza funzionale dei sistemi di controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza
IEC 61508-1:2010	Sicurezza funzionale di sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti generali.
IEC 61508-2:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili.
IEC 61508-3:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti software.
IEC 61784-3:2021	Reti di comunicazione industriale - Profili - Parte 3: Bus di campo di sicurezza funzionale - Regole generali e definizioni dei profili.
2006/42/EC	Direttiva macchine
2014/30/EU	Direttiva compatibilità elettromagnetica
2014/35/EU	Direttiva bassa tensione

I termini utilizzati nel presente documento possono inoltre essere utilizzati indirettamente, in quanto provenienti da altri standard, quali:

Standard	Descrizione
Serie IEC 60034	Macchine elettriche rotative
Serie IEC 61800	Variatori di velocità elettrici regolabili
Serie IEC 61158	Comunicazioni dati digitali per misurazioni e controlli – Bus di campo per l'uso con i sistemi di controllo industriali

Infine, l'espressione *area di funzionamento* può essere utilizzata nel contesto di specifiche condizioni di pericolo e in questo caso ha lo stesso significato dei termini *area pericolosa* o *zona di pericolo* espressi nella *Direttiva macchine (2006/42/EC)* e *ISO 12100:2010*.

**NOTA:** Gli standard indicati in precedenza possono applicarsi o meno ai prodotti specifici citati nella presente documentazione. Per ulteriori informazioni relative ai singoli standard applicabili ai prodotti qui descritti, vedere le tabelle delle caratteristiche per tali codici di prodotti.

# Descrizione del TMS

## TMS - Descrizione generale

### Introduzione

I moduli di espansione TMS si montano sul lato sinistro del controller e sono dedicati a Ethernet e CANopen. È possibile configurare i moduli di espansione TMS nella **struttura Dispositivi** del software.

### Caratteristiche dei moduli di espansione TMS

Nella seguente tabella vengono illustrate le funzionalità dei moduli di espansione TMS:

Codice prodotto del modulo	Tipo	Tipo di morsettiera	Compatibilità
TMSES4	Comunicazioni Ethernet	RJ45	TM262L10MESE8T TM262L20MESE8T TM262M15MESS8T TM262M25MESS8T TM262M35MESS8T
TMSCO1	Modulo master CANopen	Sub-D 9-pin, maschio	TM262L• TM262M•

**NOTA:** Il modulo di espansione TMSES4 non è uno switch Ethernet.

## Configurazione del bus di comunicazione (COM\_Bus)

### Configurazione del bus di comunicazione

Per configurare il bus di comunicazione, procedere come segue:

Passo	Azione
1	Nella Struttura dispositivi, fare doppio clic su <b>COM_Bus</b> . <b>Risultato:</b> viene visualizzata la finestra di configurazione <b>COM_Bus</b> .
2	Fare clic su una delle schede: <ul style="list-style-type: none"><li>• <b>Bus TMS</b></li><li>• <b>Mapping I/O</b></li><li>• <b>Tabella di diagnostica</b></li></ul>

### Scheda Bus TMS

Il bus di comunicazione TMS è dotato di un'architettura di rete IP interna. L'indirizzo di rete viene stabilito per le configurazioni generali, tuttavia, l'indirizzo di rete deve essere immesso manualmente per le configurazioni complesse che necessitano di reti multiple e controller M262 interconnessi.

Per configurare l'indirizzo di rete, procedere come segue:

Passo	Azione
1	Fare clic su <b>Indirizzi di rete</b> .
2	Immettere il nuovo indirizzo di rete. <b>Risultato:</b> i campi <b>Maschera di sottorete</b> , <b>Host min</b> e <b>Host max</b> vengono aggiornati automaticamente.

## Scheda Mapping I/O

La scheda **Mapping I/O** è fissa e non può essere modificata.

## Scheda Tabella diagnostica

La scheda **Tabella di diagnostica** fornisce uno stato di diagnostica di ciascuno dei moduli collegati.

**NOTA:** Questa tabella è solo per i moduli TMSES4.

Parametro	Tipo di dati	Valore predefinito	Valore	Descrizione
<i>ConfState</i>	UNIT	0	0: Nessuna configurazione 1: Configurazione non valida 2: Riservato 3: Configurazione valida e applicata	Stato globale del bus
<i>NbModules</i>	UNIT	0	0...3	Numero di moduli TMS rilevati
<i>Name</i>	STRING(15)	–	–	Nome modulo TMS
<i>MajorType</i>	WORD	0	–	Codice tipo del modulo TMS
<i>SubType</i>	WORD	0	–	Codice sottotipo del modulo TMS
<i>Version</i>	STRING(15)	–	–	Versione firmware del modulo TMS <sup>(1)</sup>
<i>ModuleState</i>	DWORD	TMS_MODULE_POWERED	0	Individuazione del modulo TMS dal controller
		TMS_MODULE_INITIALIZED	1	
		TMS_MODULE_CONFIGURED	2	
		TMS_MODULE_EXCHANGE_FAULT	3	
		MODULE_ERROR	4	
		TMS_MODULE_HEALTH_SEND_FAULT	5	
		TMS_MODULE_HEALTH_RCV_TIMEOUT	6	
		TMS_MODULE_HEALTH_RCV_MISC	7	
		TMS_MODULE_HEALTH_RESP_ERR	8	
		TMS_MODULE_DISCOVERY	9	

Parametro	Tipo di dati	Valore predefinito	Valore	Descrizione
<i>IpState</i>	DWORD	TMS_IP_PING_SUCCESS	0	Comunicazione IP tra M262 e modulo TMS
		TMS_IP_CONFIG_CMD_ERROR	1	
		TMS_IP_CONFIG_RESP_WAIT	2	
		TMS_IP_CONFIG_RESP_ERROR	3	
		TMS_IP_CONFIG_RESP_NONE	4	
		TMS_IP_CONFIG_SUCCESS	5	
		TMS_IP_PING_CMD_ERROR	6	
		TMS_IP_PING_RESP_WAIT	7	
		TMS_IP_PING_RESP_ERROR	8	
		TMS_IP_PING_RESP_NONE	9	
<i>PixCmdState</i>	Enumeration of DWORD	TMS_PIXCMD_EXCHING	0	Il modulo TMS gestisce un'immagine processo
		TMS_PIXCMD_CONFIG_NONE	1	
		TMS_PIXCMD_CONFIG_CMD_ERROR	2	
		TMS_PIXCMD_CONFIG_RESP_WAIT	3	
		TMS_PIXCMD_CONFIG_RESP_ERROR	4	
		TMS_PIXCMD_CONFIG_ONLY	5	
		TMS_PIXCMD_CONFIG_SUCCESS	6	
		TMS_PIXCMD_ENABLE_CMD_ERROR	7	
		TMS_PIXCMD_ENABLE_RESP_WAIT	8	
		TMS_PIXCMD_ENABLE_RESP_ERROR	9	
		TMS_PIXCMD_EXCH_ERROR	10	
		TMS_PIXCMD_DISABLING	11	
		TMS_PIXCMD_DISABLED	12	
(1) Vedere Aggiornamento del firmware del modulo di espansione TMSES4 (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione) per informazioni su come aggiornare il firmware del modulo di espansione TMSES4.				

## Aggiunta di un modulo di espansione TMS

### Aggiunta di un modulo di espansione TMS

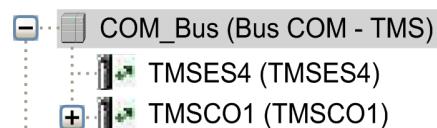
Per aggiungere un modulo di espansione TMS al controller, selezionare il modulo di espansione nel **Catalogo hardware**, trascinarlo nella **Struttura dispositivi** e rilasciarlo nel nodo**COM\_Bus**.

Per maggiori informazioni sull'aggiunta di un dispositivo nel progetto, vedere:

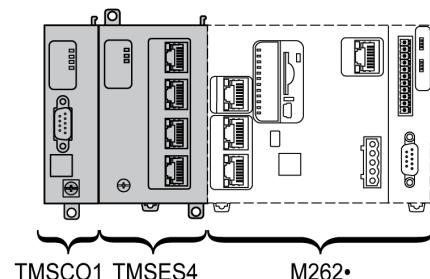
- Utilizzo del Metodo di trascinamento della selezione nella EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione
- Utilizzo del Il menu contestuale o il pulsante Più si trovano nel menu EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione

## Layout modulo di espansione

Nel software, il layout del modulo viene visualizzato dall'alto verso il basso:



Fisicamente, i moduli di espansione sono collegati da destra a sinistra:



Per ulteriori informazioni sulla compatibilità con il M262 Logic/Motion Controller, vedere [Caratteristiche dei moduli di espansione TMS](#), pagina 10.

## Configurazione di un modulo di espansione

Per configurare il modulo di espansione TMS, fare doppio clic sul nodo del modulo di espansione nella **Struttura dispositivi**.

# Modulo Ethernet TMSES4

## Introduzione

In questo capitolo è descritta la configurazione del modulo di espansione Ethernet TMSES4.

## Servizi Ethernet

### Introduzione

Questa sezione descrive come configurare i servizi Ethernet forniti dal modulo di espansione TMSES4.

## Presentazione

### Servizi Ethernet

Il modulo di espansione TMSES4 fornisce un'interfaccia Ethernet per estendere il numero di porte Ethernet di un controller.

Il modulo supporta i seguenti servizi del controller:

- Server Modbus TCP, pagina 15
- Web Server (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione)
- Server FTP (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione)
- SNMP (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione)
- M262 Logic/Motion Controller come dispositivo di destinazione su EtherNet/IP, pagina 20
- M262 Logic/Motion Controller come dispositivo slave su Modbus TCP, pagina 21
- Accesso IEC VAR, pagina 15

**NOTA:** La comunicazione NVL (Network Variable List) richiede che la porta Ethernet abbia un indirizzo IP valido e che il dispositivo sia collegato.

## Protocollo Ethernet

Il modulo Ethernet supporta i seguenti protocolli:

- IP (Internet Protocol)
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- ARP (Address Resolution Protocol)
- ICMP (Internet Control Messaging Protocol)
- IGMP (Internet Group Management Protocol)

## Connessioni server TCP

Questa tabella mostra il totale delle connessioni del server TCP per il controller e i moduli TMSES4:

Tipo connessione	Numero massimo di connessioni server simultanee
Server Modbus	8 connessioni server TCP simultanee al massimo per TMSES4 e il controller o per il solo controller.
Dispositivo EtherNet/IP	16
Server FTP	4
Server Web	10

Ogni server basato su TCP gestisce il proprio set di connessioni.

Quando un client cerca di aprire una connessione con il server Modbus che supera il numero massimo di connessioni, il controller chiude la connessione meno recente. In altri casi, il tentativo di apertura di una connessione viene negato.

Se tutte le connessioni sono occupate (scambio in corso), quando un client cerca di aprire una nuova connessione, questa viene rifiutata.

Le connessioni al server restano aperte finché il controller si trova negli stati operativi (*RUN*, *STOP*, *HALT*).

Le connessioni al server vengono chiuse quando si esce o si entra negli stati operativi (*RUN*, *STOP*, *HALT*), tranne in caso di interruzione dell'alimentazione (perché il controller non ha il tempo di chiudere le connessioni).

Per maggiori informazioni sugli stati operativi, vedere il diagramma di stato del controller (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione).

## Server Modbus TCP

Il server Modbus supporta le seguenti richieste Modbus:

Codice funzione Dec (Hex)	Sottofunzione Dec (Hex)	Funzione
1 (1h)	–	Lettura uscite digitali (%Q)
2 (2h)	–	Lettura ingressi digitali (%I)
3 (3h)	–	Lettura registro di mantenimento (%MW)
6 (6h)	–	Scrittura registro singolo (%MW)
8 (8h)	–	Diagnostica
15 (Fh)	–	Scrittura su più uscite digitali (%Q)
16 (10h)	–	Scrittura su più registri (%MW)
23 (17h)	–	Lettura/scrittura di più registri (%MW)
43 (2Bh)	14 (Eh)	Lettura identificazione dispositivo

## Servizi disponibili

In una comunicazione Ethernet, il controller supporta il servizio **IEC VAR ACCESS**. Il servizio **IEC VAR ACCESS** permette lo scambio di variabili tra il controller e un HMI.

Inoltre, il servizio **Variabili di rete** è supportato dal controller. Il servizio **Variabili di rete** consente uno scambio di dati fra i controller.

**NOTA:** Per ulteriori informazioni, vedere EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione.

## Configurazione dell'indirizzo IP

### Introduzione

TMSES4, quando non è configurato, si attiva e ottiene automaticamente il proprio indirizzo IP predefinito:

- 10.12.x.z per il primo modulo
- 10.13.x.z per il secondo modulo
- 10.14.x.z per il terzo modulo

x e z rappresentano il 5° e il 6° byte dell'indirizzo MAC dell'interfaccia. Ad esempio, con un indirizzo MAC di 00:80:F4:50:02:5D, l'indirizzo IP sarà 10.12.2.93.

Vedere Configurazione Ethernet, pagina 18 per ulteriori informazioni sulla posizione dell'indirizzo MAC.

La subnet mask predefinita è 255.255.0.0.

Esistono diversi modi per assegnare l'indirizzo IP all'interfaccia Ethernet aggiuntiva del controller:

- Assegnazione dell'indirizzo da parte del server DHCP
- Assegnazione dell'indirizzo da parte del server BOOTP
- Indirizzo IP fisso
- File di post-configurazione (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione). Se esiste un file di post-configurazione, questo metodo di assegnazione ha la priorità sugli altri.

L'indirizzo IP può anche essere modificato dinamicamente tramite:

- Scheda **Impostazioni di comunicazione** (vedi Guida alla programmazione del Modicon M262 Logic/Motion Controller)
- **changeIPAddress** blocco funzione (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione)

**NOTA:** Se il metodo di indirizzamento utilizzato non funziona, il collegamento utilizza un indirizzo IP predefinito ricavato dall'indirizzo MAC.

Gestire attentamente gli indirizzi IP tenendo presente che ogni dispositivo della rete richiede un indirizzo univoco. La presenza di più dispositivi con lo stesso indirizzo IP può causare il funzionamento imprevisto della rete e dell'apparecchiatura collegata.

### AVVERTIMENTO

#### FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Verificare che vi sia solo un controller master configurato sulla rete o sul collegamento remoto.
- Verificare che tutti i dispositivi abbiano un indirizzo univoco.
- Contattare l'amministratore di sistema per richiedere l'indirizzo IP da utilizzare.
- Prima della messa in servizio del sistema verificare che l'indirizzo IP del dispositivo sia univoco.
- Non assegnare lo stesso indirizzo IP ad altre apparecchiature di rete.
- Aggiornare l'indirizzo IP dopo aver clonato un'applicazione che include comunicazioni Ethernet a un indirizzo univoco.

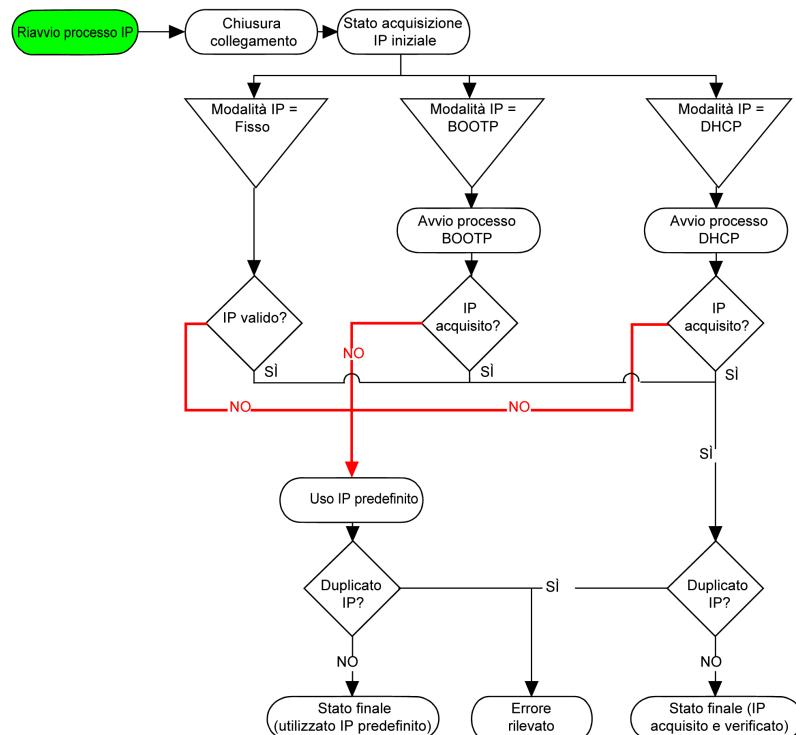
**Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

**NOTA:** Verificare che l'amministratore del sistema registri tutti gli indirizzi IP assegnati nella rete e nella sottorete; segnalare all'amministratore eventuali modifiche eseguite nella configurazione.

**NOTA:** Il modulo TMSES4 deve trovarsi in una sottorete differente da quella utilizzata dalle porte del controller Ethernet.

## Gestione degli indirizzi

La figura mostra i diversi tipi di sistemi di indirizzamento per il controller:



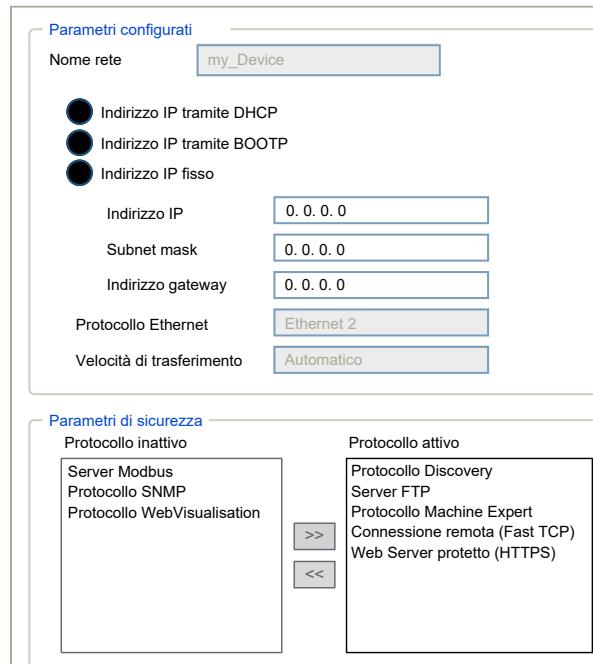
**NOTA:** Se un dispositivo programmato per utilizzare i metodi di indirizzamento DHCP o BOOTP non riesce a contattare il rispettivo server, il controller utilizza l'indirizzo IP predefinito. Tuttavia, il processo viene ripetuto fino a quando si raggiunge il rispettivo server e si acquisisce un indirizzo IP.

Il processo IP si riavvia nei seguenti casi:

- Riavvio del controller
- Riconnessione del cavo Ethernet
- Download dell'applicazione (se vi è una modifica dei parametri IP)
- Server DHCP o BOOTP rilevato dopo un tentativo di indirizzamento precedente non riuscito.

## Configurazione Ethernet

Nella **Struttura dispositivi**, fare doppio clic su **TMSES4**:



### NOTA:

- Se ci si trova in modalità offline, viene visualizzata la finestra **Parametri configurati** (visualizzata sopra). È possibile modificare i parametri.
- Se ci si trova in modalità online, è possibile vedere la finestra **Parametri configurati** e **Impostazioni correnti**. Non è possibile modificare i parametri.

Questa tabella descrive i parametri configurati:

Parametri configurati	Descrizione
<b>Nome di rete</b>	Usato come nome dispositivo per recuperare l'indirizzo IP tramite DHCP, massimo 15 caratteri.
<b>Indirizzo IP tramite DHCP</b>	L'indirizzo IP viene ottenuto tramite il server DHCP.
<b>Indirizzo IP tramite BOOTP</b>	L'indirizzo IP viene ottenuto tramite il server BOOTP. L'indirizzo MAC è situato sulla parte sinistra del controller.
<b>Indirizzo IP fisso</b>	Indirizzo IP, maschera di sottorete e indirizzo gateway vengono definiti dall'utente.
<b>Protocollo Ethernet</b>	Tipo di protocollo utilizzato: Ethernet 2
<b>Velocità di trasferimento</b>	Speed e Duplex sono in modalità autonegoziazione.

### Indirizzo IP predefinito

L'indirizzo MAC della porta Ethernet può essere recuperato sull'etichetta apposta sul lato anteriore del controller M262. L'indirizzo MAC della porta TMSES4 può essere recuperato sull'etichetta applicata sul lato sinistro del controller M262.

**NOTA:** un indirizzo MAC è scritto in formato esadecimale e un indirizzo IP in formato decimale. Convertire l'indirizzo MAC in formato decimale.

Esempio di conversione:

Porta	Indirizzo MAC	Indirizzo IP
TMS_1	00.80.F4.50.03.31	10.12.3.49
TMS_2	00.80.F4.50.03.32	10.13.3.50
TMS_3	00.80.F4.50.03.33	10.14.3.51

### Maschera di sottorete

La subnet mask o maschera di sottorete consente di indirizzare più reti fisiche con un unico indirizzo. La maschera serve a separare l'indirizzo di sottorete e del dispositivo nell'ID host.

L'indirizzo di sottorete si ottiene mantenendo i bit dell'indirizzo IP che corrispondono alle posizioni della maschera contenenti 1 e sostituendo gli altri con 0.

L'indirizzo di sottorete del dispositivo host, invece, si ottiene mantenendo i bit dell'indirizzo IP corrispondente alle posizioni della maschera contenente 0 e sostituendo gli altri con 1.

Esempio di indirizzo di sottorete:

Indirizzo IP	192 (11000000)	1 (00000001)	17 (00010001)	11 (00001011)
Subnet mask	255 (11111111)	255 (11111111)	240 (11110000)	0 (00000000)
Indirizzo di sottorete	192 (11000000)	1 (00000001)	16 (00010000)	0 (00000000)

**NOTA:** il dispositivo non comunica sulla propria sottorete in assenza di gateway.

### Indirizzo gateway

Il gateway permette a un messaggio di essere instradato a un dispositivo che non è la rete corrente.

In assenza di gateway, l'indirizzo del gateway è 0.0.0.0.

L'indirizzo del gateway deve essere definito sull'interfaccia Ethernet\_1. Il traffico verso reti esterne deve essere inviato tramite questa interfaccia.

### Parametri di sicurezza

Questa tabella descrive i vari parametri di sicurezza:

Parametri di sicurezza	Descrizione	Impostazioni predefinite
<b>Protocollo Discovery</b>	Questo parametro attiva/disattiva il <b>protocollo discovery</b> . Quando è disattivato, le richieste Discovery vengono ignorate.	Attivo
<b>Server FTP</b>	Questo parametro attiva/disattiva il serverFTP del controller. Quando è disattivato, le richieste FTP vengono ignorate.	Attivo
<b>Protocollo Machine Expert</b>	Questo parametro attiva/disattiva il protocollo Machine Expert sulle interfacce Ethernet. Quando è disattivato, qualsiasi richiesta Machine Expert proveniente da un dispositivo viene rifiutata. Pertanto, non è possibile una connessione su Ethernet da un PC di programmazione, da un target HMI che intende scambiare variabili con questo controller, da un server OPC o da Controller Assistant.	Attivo
<b>Server Modbus</b>	Questo parametro attiva/disattiva il serverModbus del controller. Quando è disattivato, le richieste Modbus al controller vengono ignorate.	Inattivo
<b>Connessione remota</b>	Questo parametro attiva/disattiva la connessione remota. Quando è disattivato, le richieste Fast TCP vengono ignorate.	Attivo
<b>Web Server protetto</b>	Questo parametro attiva/disattiva il Server Web protetto del controller. Quando è disattivato, le richieste HTTPS al Server Web protetto del controller vengono ignorate.	Attivo
<b>Protocollo SNMP</b>	Questo parametro attiva/disattiva il serverSNMP del controller. Quando è disattivato, le richieste SNMP vengono ignorate.	Inattivo
<b>Protocollo WebVisualisation</b>	Questo parametro attiva/disattiva la funzione WebVisualisation pagine del controller. Quando è disattivato, le richieste HTTP al protocollo WebVisualisation del logic controller vengono ignorate.	Inattivo

# Modicon M262 Logic/Motion Controller come un dispositivo di destinazione su EtherNet/IP

## Introduzione

Questa sezione descrive la configurazione del M262 Logic/Motion Controller come dispositivo di destinazione EtherNet/IP.

Per ulteriori informazioni su EtherNet/IP, vedere il sito Web [www.odva.org](http://www.odva.org).

## Configurazione di destinazione EtherNet/IP

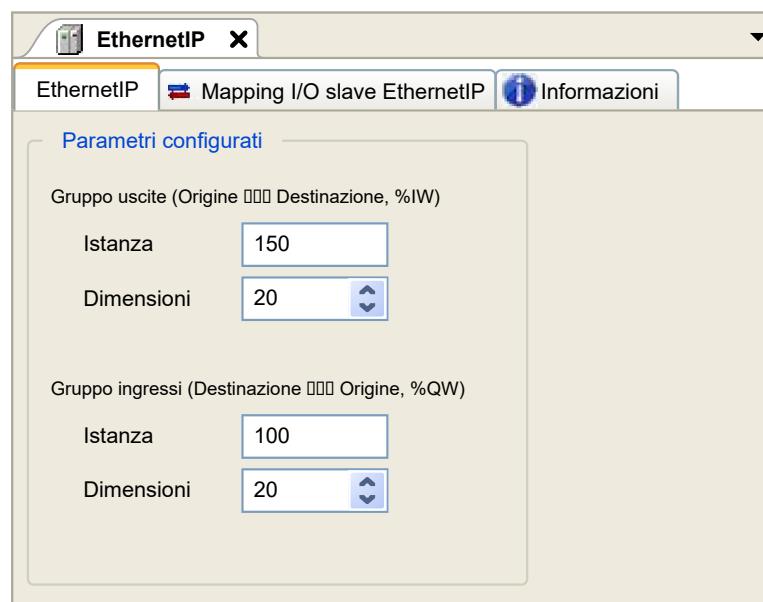
Per configurare il M262 Logic/Motion Controller come dispositivo di destinazione su Ethernet/IP, attenersi ai seguenti passi:

Passo	Azione
1	Selezionare <b>EthernetIP</b> nel menu <b>Catalogo hardware</b> .
2	<p>Selezionarlo e trascinarlo nella <b>Struttura dispositivi</b> su uno dei nodi evidenziati.</p> <p><b>NOTA:</b> Se il nodo scelto è <b>COM_Bus</b>, un modulo di espansione TMSES4 viene aggiunto automaticamente alla configurazione.</p> <p>Per maggiori informazioni sull'aggiunta di un dispositivo nel progetto, vedere:</p> <ul style="list-style-type: none"> <li>Utilizzo del Metodo di trascinamento della selezione nella EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione</li> <li>Utilizzo del II menu contestuale o il pulsante Più si trovano nel menu EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione</li> </ul>

## Configurazione dei parametri EtherNet/IP

Per configurare i parametri EtherNet/IP, fare doppio clic su **EthernetIP** nella **Struttura dispositivi**.

Viene visualizzata questa finestra di dialogo:



I parametri di configurazione I/O EtherNet/IP sono definiti come:

- **Istanza:**

Numero che si riferisce all'Assembly di ingresso o uscita.

- **Dimensione:**

Numero di canali di un Assembly di ingresso o uscita.

Ciascun canale dispone di una memoria di 2 byte che memorizza il valore di un oggetto  $\%IWx$  o  $\%QWx$ , dove  $x$  è il numero del canale.

Ad esempio, se la **Capacità dell'Assembly di uscita** è 20, significa che vi sono 20 canali di ingresso (IW0 - IW19) che indirizzano  $\%IWy...%IW(y+20-1)$ , dove  $y$  è il primo canale disponibile per l'Assembly.

Elemento		Gamma controller ammissibile	Valore predefinito
Assembly di uscita	Istanza	150...189	150
	Capacità	2...250	20
Assembly di ingresso	Istanza	100...149	100
	Capacità	2...250	20

Consultare la M262 Logic/Motion Controller Guida alla programmazione per ulteriori informazioni sui seguenti argomenti:

- Creazione di un file EDS
- Configurazione degli I/O
- Oggetti supportati dal controller

## Modicon M262 Logic/Motion Controller come dispositivo slave su TCP Modbus

### Panoramica

Questa sezione descrive la configurazione del M262 Logic/Motion Controller come un **Dispositivo slave Modbus TCP**.

Per configurare il M262 Logic/Motion Controller come **Dispositivo slave Modbus TCP**, occorre aggiungere la funzionalità **Dispositivo slave Modbus TCP** al controller (vedere Aggiunta di un dispositivo slave Modbus TCP).

Questa funzionalità crea una specifica area di I/O nel controller accessibile con il protocollo Modbus TCP. Tale area di I/O viene usata qualora un master esterno richieda di accedere agli oggetti  $\%IW$  e  $\%QW$  del controller. Questa funzionalità **Dispositivo slave Modbus TCP** consente di fornire a questa area il controller degli oggetti di I/O a cui è poi possibile accedere con una singola richiesta dei registri di lettura/scrittura Modbus.

Il **Dispositivo slave Modbus TCP** aggiunge un'altra funzione del server Modbus al controller. Questo server viene indirizzato dall'applicazione client Modbus specificando un ID unità configurato (indirizzo Modbus) nell'intervallo 1...247. Il server Modbus integrato del controller slave non richiede configurazione e viene indirizzato specificando un ID unità uguale a 255. Vedere Configurazione Modbus TCP, pagina 22.

Gli ingressi/uscite vengono visti dal controller slave: gli ingressi sono scritti tramite il master e le uscite sono lette dal master.

Il **Dispositivo slave Modbus TCP** può anche definire un'applicazione client Modbus privilegiata, la cui connessione non viene chiusa forzatamente (le connessioni Modbus integrate possono essere chiuse quando sono necessarie più di connessioni).

La durata del timeout associata alla connessione privilegiata permette di verificare se il controller è interrogato dal master privilegiato. Se non vi sono richieste

Modbus entro la durata del timeout, il dato di diagnostica *i\_byMasterIpLost* è impostato a 1 (TRUE). Per ulteriori informazioni, vedere Porta Ethernet, Variabili di sistema di sola lettura (vedere Modicon M262 Logic/Motion Controller, Funzioni e variabili di sistema, Guida della libreria di sistema).

Per ulteriori informazioni su TCP Modbus, consultare il sito Web [www.modbus.org](http://www.modbus.org).

## Aggiunta di un dispositivo slave Modbus TCP

Per aggiungere la funzionalità Dispositivo slave Modbus TCP al M262 Logic/Motion Controller, attenersi ai seguenti passi:

Passo	Azione
1	Selezionare <b>Dispositivo slave Modbus TCP</b> nel <b>Catalogo hardware</b> .
2	Selezionarlo e trascinarlo nella <b>Struttura dispositivi</b> su uno dei nodi evidenziati. <b>NOTA:</b> Se il nodo scelto è <b>COM_Bus</b> , un modulo di espansione TMSES4 viene aggiunto automaticamente alla configurazione. Per maggiori informazioni sull'aggiunta di un dispositivo nel progetto, vedere: <ul style="list-style-type: none"><li>• Utilizzo del Metodo di trascinamento della selezione nella EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione</li><li>• Utilizzo del Il menu contestuale o il pulsante Più si trovano nel menu EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione</li></ul>

## Configurazione di un dispositivo slave TCP Modbus

Per configurare il Dispositivo slave Modbus TCP, fare doppio clic su **ModbusTCP\_Slave\_Device** nella **Struttura dispositivi**.

Viene visualizzata questa finestra di dialogo:

### Parametri configurati

Indirizzo master IP	0 . 0 . 0 . 0
<input checked="" type="checkbox"/> Watchdog	2000 <input type="button" value="▲"/> <input type="button" value="▼"/> (ms) <input type="checkbox"/> Chiudere il socket TCP
Porta slave	502 <input type="button" value="▲"/> <input type="button" value="▼"/> <input type="checkbox"/> Collega all'adattatore
ID unità	247
Registri di holding	10 <input type="button" value="▲"/> <input type="button" value="▼"/> (%IW) <input type="checkbox"/> Scrivibile
Registri di ingresso	10 <input type="button" value="▲"/> <input type="button" value="▼"/> (%QW)
<input type="checkbox"/> Aree bit discreti	
Bobine	0 <input type="button" value="▲"/> <input type="button" value="▼"/> (%IX)
Ingressi discreti	0 <input type="button" value="▲"/> <input type="button" value="▼"/> (%QX)

### Data Model

Indirizzi di avvio	
Bobine	0 <input type="button" value="▲"/> <input type="button" value="▼"/>
Ingressi discreti	0 <input type="button" value="▲"/> <input type="button" value="▼"/>
Registro di holding	0 <input type="button" value="▲"/> <input type="button" value="▼"/>
Registro di ingresso	0 <input type="button" value="▲"/> <input type="button" value="▼"/>
<input type="checkbox"/> Sovrapposizione delle aree di dati registro di holding e di ingresso	

Elemento	Descrizione
<b>Indirizzo IP Master</b>	Indirizzo IP del master Modbus Le connessioni non sono chiuse su questo indirizzo.
<b>Watchdog</b>	Watchdog in incrementi di 500 ms <b>NOTA:</b> Il watchdog si applica all' <b>indirizzo IP Master</b> a meno che l'indirizzo sia 0.0.0.0.
<b>Chiudere il socket TCP</b>	Quando viene selezionato <b>Chiudere il socket TCP</b> , il socket TCP viene chiuso se il <b>watchdog</b> è attivato e viene superato il tempo impostato.
<b>Porta slave</b>	Porta di comunicazione Modbus (502)
<b>ID unità</b>	Inviare le richieste a Dispositivo slave Modbus TCP (1...247), anziché al server Modbus integrato (255).
<b>Registri di mantenimento (%IW)</b>	Numero dei registri %IW da utilizzare nello scambio (2...120) (ciascun registro è 2 byte)
<b>Registri di ingresso (%QW)</b>	Numero dei registri %QW da utilizzare nello scambio (2...120) (ciascun registro è 2 byte)

## Scheda Mapping I/O dispositivo slave Modbus TCP

Gli I/O sono assegnati ai registri Modbus dal punto di vista del Master nel modo seguente:

- Le %IW vengono mappate dal registro 0 a n-1 e sono R/W (n = quantità del registro di mantenimento, ciascun registro %IW è di 2 byte).
- Le %QW vengono mappate dal registro n a n+m-1 e sono di sola lettura (m = quantità di registri di ingresso, ciascun registro %QW è di 2 byte).

Dopo aver configurato il **Dispositivo slave Modbus TCP**, i comandi Modbus inviati al relativo ID Unità (indirizzo Modbus) sono gestiti in modo diverso se lo stesso comando fosse stato indirizzato a ogni altro dispositivo Modbus sulla rete. Ad esempio, il comando Modbus 3 (3 hex), quando viene inviato a un dispositivo Modbus, legge e restituisce il valore di uno o più registri. Quando questo medesimo comando viene inviato al Modbus TCP Slave (vedi M262 Logic/Motion Controller, Guida alla programmazione) è possibile facilitare l'operazione di lettura da parte dello scanner I/O esterno.

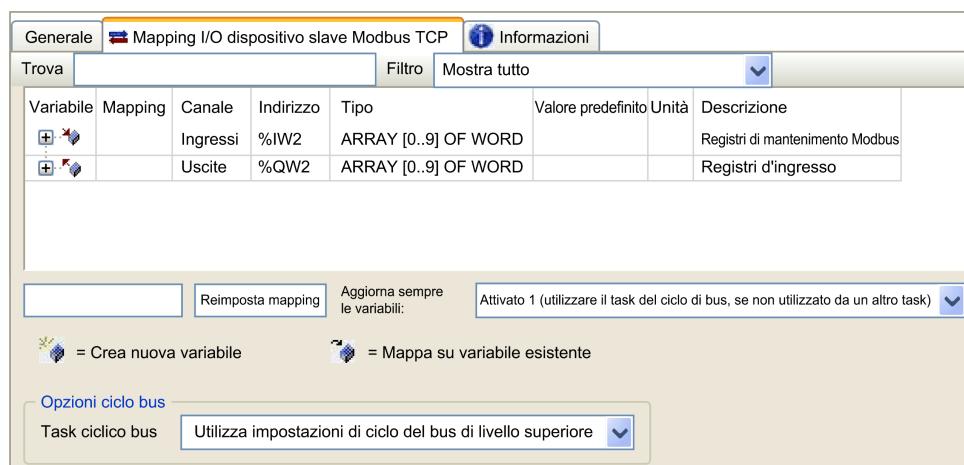
Dopo aver configurato il **dispositivo slave Modbus TCP**, i comandi Modbus vengono inviati al relativo ID unità (indirizzo Modbus) accedono agli oggetti di %IW e %QW del controller, collegati al dispositivo Modbus TCP, anziché alle parole standard Modbus (a cui si accede quando l'ID unità è 255). Questo semplifica le operazioni di lettura/scrittura da parte di un'applicazione scanner degli I/O Modbus TCP.

Il **Modbus TCP Slave** risponde a un sottoinsieme di comandi Modbus per scambiare dati con lo scanner degli I/O esterno. I seguenti comandi Modbus sono supportati dal **Dispositivo slave Modbus TCP**:

Codice funzione dec (hex)	Funzione	Commento
3 (3)	Lettura registro di mantenimento	Consente al master di leggere gli oggetti %IW e %QW del dispositivo
6 (6)	Scrittura singolo registro	Consente al master di leggere gli oggetti %IW del dispositivo
16 (10)	Scrittura registri multipli	Consente al master di scrivere l'oggetto %IW del dispositivo
23 (17)	Lettura/scrittura registri multipli	Consente al master di leggere gli oggetti %IW e %QW del dispositivo e di scrivere gli oggetti %IW del dispositivo
Altro	Non supportato	-

**NOTA:** le richieste Modbus che provano ad accedere ai registri sopra n+m-1 ricevono come risposta il codice di eccezione 02 - ILLEGAL DATA ADDRESS.

Per collegare gli oggetti I/O alle variabili, selezionare la scheda **Mapping I/O del dispositivo slave Modbus TCP**:



Canale		Tipo	Descrizione
<b>Ingres-so</b>	IW0	WORD	Registro di mantenimento 0
	...	...	...
	IWx	WORD	Registro di mantenimento x
<b>Uscita</b>	QW0	WORD	Registro di ingresso 0
	...	...	...
	QWy	WORD	Registro di ingresso y

Il numero di parole dipende dai parametri **Registri di mantenimento (%IW)** e **Registri di ingresso (%QW)** della scheda **Modbus TCP**.

**NOTA:** uscita significa USCITA dal controller client/master (%IW per il controller server/slave). Ingresso significa INGRESSO dal controller client/master (%QW per il controller server/slave).

Per il parametro **Aggiorna variabili sempre** scegliere una delle seguenti opzioni:

- **Utilizza le impostazioni del dispositivo di livello superiore**
- **Attivati 1 (utilizzare il task del ciclo di bus, se non utilizzato da un altro task)** (impostazione predefinita)
- **Attivato 2 (sempre nel task del ciclo di bus)**

## Opzioni del ciclo di bus

Nella scheda **Mapping I/O dispositivo Modbus TCP Slave** selezionare il **task del ciclo di bus** da utilizzare:

- **Utilizza impostazioni di ciclo del bus di livello superiore** (impostazione predefinita)
- **MAST**
- **Un task esistente del progetto:** è possibile selezionare un task esistente e associarlo allo scanner. Per ulteriori informazioni sui task dell'applicazione, consultare la EcoStruxure Automation Expert - Motion / EcoStruxure Machine Expert Guida alla programmazione.

**NOTA:** È presente un parametro **Task ciclo bus** corrispondente nell'editor mapping degli I/O del dispositivo che contiene il **Dispositivo slave Modbus TCP**. Questo parametro definisce il task responsabile dell'aggiornamento dei registri %IW e %QW.

## Configurazione del firewall

### Introduzione

Questa sezione descrive come configurare il firewall del Modicon M262 Logic/Motion Controller.

### Introduzione

### Presentazione del firewall

In linea di principio, i firewall permettono di proteggere il perimetro della zona di sicurezza bloccando l'accesso non autorizzato e consentendo l'accesso autorizzato. Un firewall è un dispositivo o un insieme di dispositivi configurati per permettere, rifiutare, codificare, decodificare o gestire il traffico tra le diverse zone di sicurezza in base a una serie di regole e altri criteri.

I dispositivi di controllo del processo e le macchine di produzione ad alta velocità richiedono la trasmissione di dati veloce e spesso non sono in grado di tollerare la latenza introdotta da una strategia aggressiva nella rete di controllo. I firewall, quindi, svolgono un ruolo fondamentale nell'ambito della strategia di sicurezza, fornendo livelli di protezione su tutto il perimetro della rete. I firewall sono componenti importanti di una strategia globale, a livello del sistema.

**NOTA:** Schneider Electric aderisce alle migliori pratiche del settore nello sviluppo e nell'implementazione dei sistemi di controllo. Ciò include un approccio "Defense-in-Depth" per la protezione di un sistema di controllo industriale. Secondo questo tipo di approccio, i controller sono protetti da uno o più firewall per limitare l'accesso al personale e ai protocolli autorizzati.

## **AVVERTIMENTO**

### **ACCESO NON AUTENTICATO E CONSEGUENTE FUNZIONAMENTO NON AUTORIZZATO DELLA MACCHINA**

- Valutare se gli ambienti applicativi sono connessi all'infrastruttura critica e, in caso positivo, adottare le misure appropriate in termini di prevenzione, secondo l'approccio "Defense-in-Depth", prima di collegare il sistema di automazione a una rete.
- Limitare il numero di dispositivi collegati alla rete al minimo necessario.
- Isolare la rete industriale da altre reti interne all'azienda.
- Proteggere le reti dall'accesso involontario utilizzando firewall, VPN o altre misure di sicurezza comprovate, come ad esempio un sistema di prevenzione delle intrusioni o un sistema di rilevamento delle intrusioni.
- Monitorare le attività interne dei propri sistemi.
- Impedire a questi dispositivi l'accesso diretto o il collegamento diretto da parte di terzi non autorizzati o azioni non autenticate.
- Installare i certificati rilasciati dalle autorità di certificazione attendibili note a livello pubblico.
- Mantenere i sistemi aggiornati e affidarli solo a fonti legittime.
- Preparare un piano di ripristino che includa il backup del sistema e delle informazioni di processo.

**Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Per ulteriori informazioni sulle misure organizzative e le regole relative all'accesso alle infrastrutture, consultare ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security e inoltre Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment.

## **Configurazione del firewall**

Vi sono tre modi per gestire la configurazione del firewall del controller:

- configurazione statica
- modifiche dinamiche
- impostazioni dell'applicazione

I file di script vengono utilizzati nella configurazione statica e per le modifiche dinamiche.

## **Configurazione statica**

La configurazione statica viene caricata all'avvio del controller.

Il firewall del controller può essere configurato in modo statico gestendo un file di script predefinito posizionato nel controller. Il percorso di questo file è */usr/Cfg/FirewallDefault.cmd*.

**NOTA:** il nome di file distingue fra maiuscole/minuscole.

## Modifiche dinamiche

Dopo l'avvio del controller, la configurazione del firewall del controller può essere modificata utilizzando i file di script.

Esistono due metodi per caricare queste modifiche dinamiche utilizzando:

- Una scheda SD, pagina 27 fisica.
- Un blocco funzione, pagina 28 nell'applicazione.

## Impostazioni dell'applicazione

Consultare Configurazione Ethernet, pagina 18.

## Procedura per le modifiche dinamiche

### Uso di una scheda SD

Questa tabella descrive la procedura per eseguire un file di script da una scheda SD:

Passo	Azione
1	Creare un file di script, pagina 30 valido. Ad esempio, assegnare un nome al file di script <i>FirewallMaintenance.cmd</i> .
2	Caricare il file di script sulla scheda SD. Ad esempio, caricare il file di script nella cartella <i>usr/Cfg</i> .
3	Nel file <i>Sys/Cmd/Script.cmd</i> , aggiungere una riga di codice con il comando <i>Firewall_install "/pathname/FileName"</i> Ad esempio, la riga di codice è <i>Firewall_install "/sd0/usr/Cfg/FirewallMaintenance.cmd"</i> <b>NOTA:</b> il nome di file distingue fra maiuscole/minuscole.
4	Inserire la scheda SD sul controller.

## Utilizzando un blocco funzione nell'applicazione

Questa tabella descrive la procedura per eseguire un file di script da un'applicazione:

Passo	Azione
1	Creare un file di script, pagina 30 valido. Ad esempio, assegnare un nome al file di script <i>FirewallMaintenance.cmd</i> .
2	Caricare il file di script nella memoria del controller. Ad esempio, caricare il file di script nella cartella <i>usr/Syslog</i> con FTP.
3	Utilizzare un blocco funzione <code>ExecuteScript</code> . Per ulteriori informazioni, vedere M262 System, Guida della libreria (vedere Modicon M262 Logic/Motion Controller, Funzioni e variabili di sistema, Guida della libreria di sistema). Ad esempio, l'ingresso <b>[SCmd]</b> è 'Firewall_install "/usr/Syslog/FirewallMaintenance.cmd"' <b>NOTA:</b> il nome di file distingue fra maiuscole/minuscole.

## Comportamento del firewall

### Introduzione

La configurazione del firewall dipende dall'azione eseguita sul controller e dallo stato di configurazione iniziale. Esistono cinque stati iniziali possibili:

- Nel controller non vi è alcun file di script predefinito.
- È presente un file di script corretto.
- È presente un file di script non corretto.
- Non vi è alcun file di script predefinito e l'applicazione ha configurato il firewall.
- È già stata eseguita una configurazione del file di script dinamico.

**NOTA:** Per determinare se il firewall sia configurato e abilitato, consultare il logger messaggi.

### Nessun file di script predefinito

Condizione	Conseguenza
Avvio del controller	Il firewall non è configurato. Nessuna protezione è attivata.
Esecuzione del file di script dinamico	Il firewall è configurato in base al file di script dinamico.
Esecuzione del file di script dinamico non corretta	Il firewall non è configurato. Nessuna protezione è attivata.
Download dell'applicazione	Il firewall è configurato in base alle impostazioni dell'applicazione.

## Presente file di script predefinito

Condizione	Conseguenza
Avvio del controller	Il firewall è configurato in base al file di script predefinito.
Esecuzione del file di script dinamico	L'intera configurazione del file di script predefinito viene eliminata. Il firewall è configurato in base al file di script dinamico.
Esecuzione del file di script dinamico non corretta	Il firewall è configurato in base al file di script predefinito. Il file di script dinamico non viene preso in considerazione.
Download dell'applicazione	L'intera configurazione dell'applicazione viene ignorata. Il firewall è configurato in base al file di script predefinito.

## Presente file di script predefinito non corretto

Condizione	Conseguenza
Avvio del controller	Il firewall non è configurato. Nessuna protezione è attivata
Esecuzione del file di script dinamico	Il firewall è configurato in base al file di script dinamico.
Download dell'applicazione	Il firewall è configurato in base alle impostazioni dell'applicazione.

## Impostazioni dell'applicazione con nessun file di script predefinito

Condizione	Conseguenza
Avvio del controller	Il firewall è configurato in base alle impostazioni dell'applicazione.
Esecuzione del file di script dinamico	L'intera configurazione delle impostazioni dell'applicazione viene ignorata. Il firewall è configurato in base al file di script dinamico.
Esecuzione del file di script dinamico non corretta	Il firewall è configurato in base alle impostazioni dell'applicazione. Il file di script dinamico non viene preso in considerazione.
Download dell'applicazione	L'intera configurazione dell'applicazione precedente viene eliminata. Il firewall è configurato in base alle nuove impostazioni dell'applicazione.

## Esecuzione file di script dinamico già effettuata

Condizione	In questo caso...
Avvio del controller	Il firewall è configurato in base alla configurazione del file di script dinamico (vedere nota).
Esecuzione del file di script dinamico	L'intera configurazione del file di script dinamico precedente viene eliminata. Il firewall è configurato in base al nuovo file di script dinamico.
Esecuzione del file di script dinamico non corretta	Il firewall è configurato in base alla configurazione del file di script dinamico precedente. Il file di script dinamico non corretto non viene preso in considerazione.
Download dell'applicazione	L'intera configurazione dell'applicazione viene ignorata Il firewall è configurato in base al file di script dinamico.

## Comandi di script del firewall

### Panoramica

In questa sezione viene descritto come vengono scritti i file di script (file di script predefiniti o file di script dinamici) in modo che possano essere eseguiti durante l'avvio del controller o durante l'attivazione di un comando specifico.

**NOTA:** Le regole di stratificazione MAC vengono gestite separatamente e hanno una priorità maggiore rispetto alle altre regole di filtro pacchetto.

### Sintassi del file di script

La sintassi dei file di script è descritta in Creazione di uno script (vedere Modicon M262 Logic/Motion Controller, Guida alla programmazione).

### Comandi generici del firewall

I comandi seguenti sono disponibili per la gestione del firewall Ethernet del M262 Logic/Motion Controller:

Comando	Descrizione
Firewall Enable	Blocca i frame dalle interfacce Ethernet. Se non è autorizzato alcun indirizzo IP specifico, non è possibile comunicare sulle interfacce Ethernet.  <b>NOTA:</b> Per impostazione predefinita, quando il firewall è attivato, vengono rifiutati i frame.
Firewall Disable	Le regole del firewall non sono applicate. I frame non sono bloccati.
Firewall Ethx Default Allow <sup>(1)</sup>	I frame vengono accettati dal controller.
Firewall Ethx Default Reject <sup>(1)</sup>	I frame vengono rifiutati dal controller.  <b>NOTA:</b> Per impostazione predefinita, questa riga, se non è presente, corrisponde al comando Firewall Eth1 Default Reject.

**(1)** Dove Ethx =

- Eth1: Ethernet\_1
- Eth2: Ethernet\_2
- Eth3: TMSES4 (primo modulo Ethernet da sinistra)
- Eth4: TMSES4 (secondo modulo Ethernet da sinistra)
- Eth5: TMSES4 (terzo modulo Ethernet da sinistra)

### Comandi specifici del firewall

I comandi seguenti sono disponibili per configurare le regole del firewall per indirizzi e porte specifiche:

Comando	Intervallo	Descrizione
Firewall Eth1 Allow IP .. . . . .	• = 0 - 255	I frame provenienti dall'indirizzo IP specificato sono consentiti su tutti i numeri di porta e i tipi di porta.
Firewall Eth1 Reject IP .. . . . .	• = 0 - 255	I frame provenienti dall'indirizzo IP specificato sono rifiutati su tutti i numeri di porta e i tipi di porta.
Firewall Eth1 Allow IPs .. . . . . to .. . . . .	• = 0 - 255	I frame provenienti dagli indirizzi IP nell'intervallo specificato sono consentiti per tutti i numeri di porta e i tipi di porta.
Firewall Eth1 Reject IPs .. . . . . to .. . . . .	• = 0 - 255	I frame provenienti dagli indirizzi IP nell'intervallo specificato sono rifiutati per tutti i numeri di porta e i tipi di porta.
Firewall Eth1 Allow port_type port Y	Y = (numeri della porta di destinazione)	I frame con il numero della porta di destinazione specificato sono consentiti.
Firewall Eth1 Reject port_type port Y	Y = (numeri della porta di destinazione)	I frame con il numero della porta di destinazione specificato sono rifiutati.

Comando	Intervallo	Descrizione
Firewall Eth1 Allow port_type ports Y1 to Y2	Y = (numeri della porta di destinazione)	I frame con un numero della porta di destinazione nell'intervallo specificato sono consentiti.
Firewall Eth1 Reject port_type ports Y1 to Y2	Y = (numeri della porta di destinazione)	I frame con un numero della porta di destinazione nell'intervallo specificato sono rifiutati.
Firewall Eth1 Allow IP .. . . . . on port_type port Y	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti dall'indirizzo IP specificato e con il numero della porta di destinazione specificato sono consentiti.
Firewall Eth1 Reject IP .. . . . . on port_type port Y	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti dall'indirizzo IP specificato e con il numero della porta di destinazione specificato sono rifiutati.
Firewall Eth1 Allow IP .. . . . . on port_type ports Y1 to Y2	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti dall'indirizzo IP specificato e con un numero della porta di destinazione nell'intervallo specificato sono consentiti.
Firewall Eth1 Reject IP .. . . . . on port_type ports Y1 to Y2	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti dall'indirizzo IP specificato e con un numero della porta di destinazione nell'intervallo specificato sono rifiutati.
Firewall Eth1 Allow IPs .. 1..1..1..1 to .. 2..2..2..2 on port_type port Y	• = 0 .. 255 Y = (numeri della porta di destinazione)	I frame provenienti da un indirizzo IP nell'intervallo specificato e con il numero di porta di destinazione specificato sono consentiti.
Firewall Eth1 Reject IPs .. 1..1..1..1 to .. 2..2..2..2..2 on port_type port Y	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti da un indirizzo IP nell'intervallo specificato e con il numero di porta di destinazione specificato sono rifiutati.
Firewall Eth1 Allow IPs .. 1..1..1..1 to .. 2..2..2..2..2 on port_type ports Y1 to Y2	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti da un indirizzo IP nell'intervallo specificato e con il numero di porta di destinazione nell'intervallo specificato sono consentiti.
Firewall Eth1 Reject IPs .. 1..1..1..1 to .. 2..2..2..2..2 on port_type ports Y1 to Y2	• = 0 - 255 Y = (numeri della porta di destinazione)	I frame provenienti da un indirizzo IP nell'intervallo specificato e con il numero di porta di destinazione nell'intervallo specificato sono rifiutati.
Firewall Eth1 Allow MAC .. : .. : .. : .. : ..	• = 0 - F	I frame provenienti dall'indirizzo MAC .. : .. : .. : .. : .. specificato sono consentiti. <b>NOTA:</b> Quando vengono applicate le regole che consentono l'indirizzo MAC, solo gli indirizzi MAC elencati possono comunicare con il controller, anche se altre regole lo consentono.
Firewall Eth1 Reject MAC .. : .. : .. : .. : ..	• = 0 - F	I frame provenienti dall'indirizzo MAC .. : .. : .. : .. : .. specificato sono rifiutati.
Firewall Ethx <sup>(1)</sup> Established to port_type port Y	Y = 0..65535	I frame stabiliti dal controller con i protocolli TCP/UDP per il numero di porta di destinazione specificato sono consentiti.

## Esempio di script

Di seguito viene riportato un esempio di Firewall in modalità white list. Nell'esempio, tutte le comunicazioni sono bloccate per impostazione predefinita e vengono consentiti solo i servizi necessari.

**NOTA:** Questo esempio è progettato per mostrare la maggior parte dei comandi disponibili con il firewall. Deve essere adattato alla configurazione e testato prima dell'implementazione.

Comandi	Commenti
Firewall Enable	Abilita il firewall.
<b>Configurazione Eth1</b>	
Firewall Eth1 Default Reject	Rifiuta tutti i frame sull'interfaccia ETH1.  In questo esempio, ETH1 è collegato alla rete di dispositivi Industrial Ethernet, quindi è possibile considerarlo affidabile.
Firewall Eth1 Allow TCP port 502	Consente il server Modbus TCP sull'interfaccia ETH1.  Non è presente alcuna autenticazione sul Modbus, quindi deve essere consentito solo su reti affidabili.
Firewall Eth1 Established to TCP port 502	Consente risposte a comunicazioni stabilite dal controller alla porta TCP 502.  Ciò è necessario quando viene utilizzata la libreria PlcCommunication per comunicare utilizzando il protocollo Modbus TCP.
Firewall Eth1 Allow UDP port 2222	Consente allo scanner ETHIP scambi impliciti di risposte alla porta UDP 2222 (ETHIP) sull'interfaccia ETH1.
Firewall Eth1 Established to TCP port 44818	Consente risposte a comunicazioni stabilite dal controller alla porta TCP 44818 (ETHIP) sull'interfaccia ETH1.  Gli ultimi 2 comandi consentono allo scanner EtherNetIP di comunicare con i dispositivi Ethernet industriali.
<b>Configurazione Eth2</b>	
Firewall Eth2 Default Reject	Rifiuta tutti i frame sull'interfaccia ETH2. Questa interfaccia è collegata alla rete utilizzata principalmente per la messa in servizio..
Firewall Eth2 Allow TCP port 4840	Consente il server OPC-UA sull'interfaccia ETH2.
Firewall Eth2 Allow TCP port 443	Consente il server Web (https) sull'interfaccia ETH2.
Firewall Eth2 Allow TCP port 8089	Consente il Web visu (https) sull'interfaccia ETH2.
Firewall Eth2 Allow TCP ports 20 to 21	Consente ftp in modalità attiva sull'interfaccia ETH2.
Firewall Eth2 Allow IP 192.168.1.1 on UDP ports 27126 to 27127	Consente l'IP per il PC di messa in servizio per individuare e configurare l'indirizzo IP del controller.  Ciò dovrebbe essere consentito solo su una rete affidabile perché l'IP può essere modificato anche quando i Diritti utente sono configurati.
Firewall Eth2 Allow IPs 192.168.1.1 to 192.168.1.2 on UDP port 1740	Consente l'IP del PC di messa in servizio e un HMI per comunicare con il controller utilizzando il protocollo Machine Expert.
Firewall Eth2 Allow TCP port 11740	Consente Fast TCP sull'interfaccia ETH2. Consente di collegare il controller utilizzando TCP.
Firewall Eth2 Allow TCP port 2222	Consente la comunicazione implicita con la porta UDP 2222 (ETHIP) sull'interfaccia ETH2.
Firewall Eth2 Allow TCP port 44818	Consente la comunicazione esplicita con la porta TCP 44818 (ETHIP) sull'interfaccia ETH2. Gli ultimi 2 comandi consentono di utilizzare il controller come adattatore EtherNetIP.
Firewall Eth2 Allow MAC 4C:CC:6A:A1:09:C8	Consente l'indirizzo MAC dell'HMI.
Firewall Eth2 Allow MAC 00:0C:29:92:43:A8	Consente l'indirizzo MAC del PC di messa in servizio. Solo gli indirizzi MAC consentiti possono comunicare con il controller.
<b>Configurazione Eth3 TMSES4</b>	
Firewall Eth3 Default Reject	Rifiuta i frame su TMSES4. Questa interfaccia è collegata alla rete dell'impianto e può accedere al Web. Dovrebbe essere considerato come non affidabile.
Firewall Eth3 Established to TCP port 443	Consente il client https (ad esempio per collegarsi a Machine Advisor) sull'interfaccia TMSES4.
Firewall Eth3 Allow TCP port 11740	Consente Fast TCP sull'interfaccia TMSES4. Ciò consente il collegamento da remoto al controller. Non dovrebbe essere consentito a meno che i Diritti utente siano attivati sul controller.

**NOTA:** I caratteri sono limitati a 200 per riga, compresi i commenti.

## Porte utilizzate

Questa tabella elenca i numeri di porta utilizzati dai servizi M262 Logic/Motion Controller:

Servizio	Numeri di porta	Configurazione predefinita/predefinita <sup>(1)</sup>
Software di programmazione	TCP 11740 UDP 1740	Sì
FTP su TLS	TCP 20, 21	Sì
HTTP <sup>(2)</sup>	TCP 80	Sì
HTTPS	TCP 443	Sì
ModbusTCP	TCP 502	No
OPC UA	TCP 4840	No
Discovery	UDP 27126, 27127	Sì
Bonjour Discovery Protocol	UDP 5353	Sì
Web Services Dynamical Discovery	TCP 5357 UDP 3702	Sì
SNMP	UDP 161	No
NVL	Valore predefinito UDP: 1202 (porta di destinazione)  (La porta di origine viene assegnata dinamicamente).	No
EtherNet/IP	TCP 44818 UDP 2222, 44818	No
WebVisualisation	TCP 8080 (HTTP), 8089 (HTTPS)	No
DHCP/BOOTP	UDP 68	Sì
TFTP	UDP 69	No
NTP	UDP 123	No
<b>Safe Logger</b> <sup>(3)</sup>	UDP 35021, 45000	Sì
<b>Machine Assistant</b>	UDP 45001, 45003, 45004	Sì
<p><b>(1)</b> La configurazione predefinita viene utilizzata quando nel controller viene caricato un progetto predefinito. Lo stato della porta è esattamente uguale a quello delle impostazioni di fabbrica.</p> <p><b>(2)</b> L'HTTP viene reindirizzato automaticamente all'HTTPS.</p> <p><b>(3)</b> Le porte<b>Safe Logger</b> sono applicabili solo ai riferimenti di TM262M•.</p>		

# Modulo di comunicazione CANopen TMSCO1

## Introduzione

Questo capitolo descrive la configurazione del modulo di comunicazione CANopen TMSCO1.

## Configurazione dell'interfaccia CANopen

### Introduzione

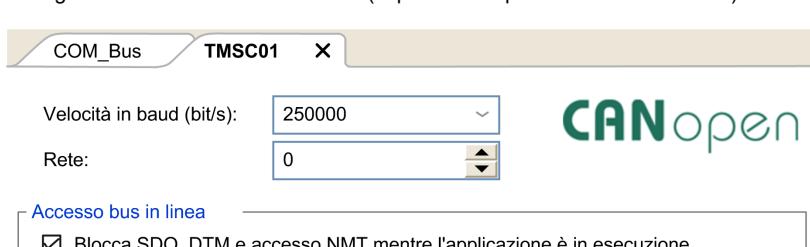
CANopen è un protocollo di comunicazione aperto standard nel settore e di specifica del profilo dispositivo (EN 50325-4) basato sul protocollo Controller Area Network (CAN). Il protocollo CAN "Layer 7" è stato sviluppato per le applicazioni di rete integrate e definisce le comunicazioni e le funzioni di dispositivo per sistemi CAN.

CANopen supporta sia le comunicazioni cicliche che dettate da eventi, consentendo di ridurre al minimo il carico del bus e di mantenere tempi di reazione brevi.

È possibile impostare le comunicazioni CANopen utilizzando un modulo TMSCO1. Questo modulo si collega al bus di comunicazione (**COM\_Bus**) sul lato sinistro del controller, utilizzando l'interfaccia del connettore sinistro del bus. È possibile collegare un modulo TMSCO1. Deve essere l'ultimo modulo sul lato sinistro del controller.

## Configurazione del bus CAN

Per configurare il bus **CAN** del controller, procedere nel modo seguente:

Passo	Azione
1	Aggiungere un modulo <b>TMSCO1</b> .
2	Nella <b>Struttura dispositivi</b> , fare doppio clic su <b>TMSCO1</b> .
3	Configurare la velocità di trasmissione (impostazione predefinita: 250000 bit/s):  <b>NOTA:</b> L'opzione <b>Accesso bus online</b> consente di bloccare l'invio di SDO, DTM e NMT dalla schermata di stato.

Quando si collega un DTM a un dispositivo utilizzando la rete, il DTM comunica in parallelo con l'applicazione in esecuzione. Questo influenza le prestazioni globali del sistema e può causare un sovraccarico della rete, con possibili ripercussioni sulla coerenza dei dati nei dispositivi controllati.



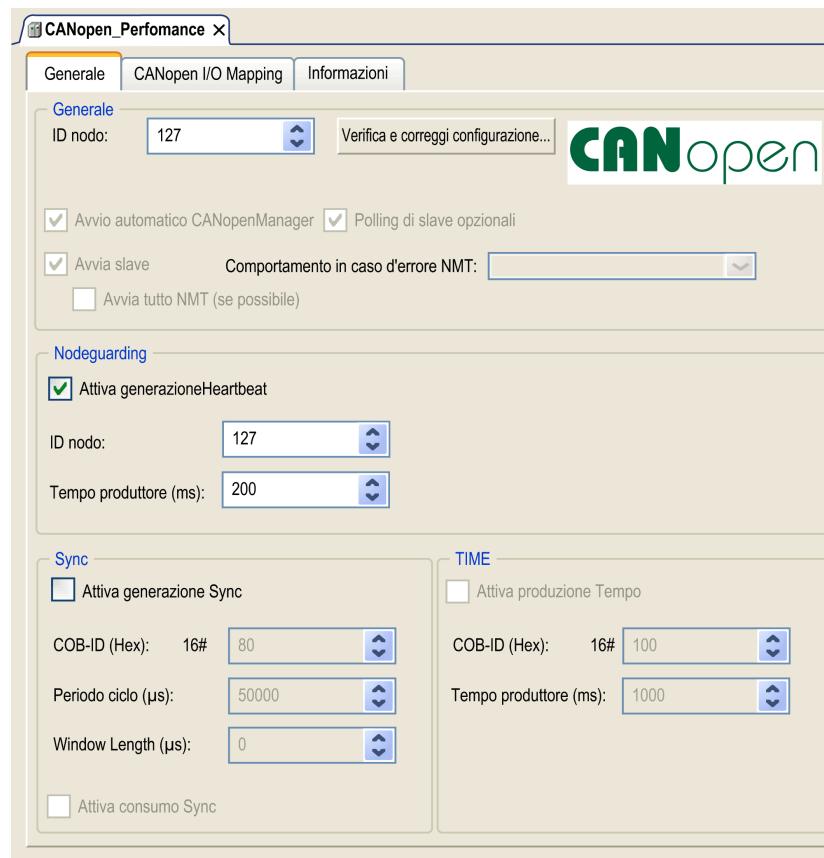
## Aggiunta di un Gestore di prestazioni CANopen

L'aggiunta di un modulo **TMSCO1** aggiunge automaticamente la funzionalità **Gestore di prestazioni CANopen** al controller in uso.

## Configurazione di un Gestore di prestazioni CANopen

Per configurare **CANopen Performance**, fare doppio clic su **COM\_Bus > TMSCO1 > CANopen Performance** nella **Struttura dispositivi**.

Viene visualizzata questa finestra di dialogo:



La scheda **Generale** della finestra di dialogo di configurazione **CANopen\_Performance** è suddivisa in quattro aree:

- **Generale**: informazioni generali contenenti ID del nodo e opzioni di configurazione abilitate.
- **Guarding**: se viene selezionato **Attiva generazione heartbeat**, Guarding viene abilitato e il master NMT può verificare lo stato attuale dei singoli nodi. Il meccanismo heartbeat consente al master di rete di individuare una perdita di comunicazione dagli slave di rete e a questi ultimi di reagire a una perdita di comunicazione con il master. L'impostazione predefinita è heartbeat che genera a 200 ms.
- **Sync**: se si seleziona **Attiva produzione Sync**, viene aggiunto un oggetto specifico per l'evento. Il task **TMSC01\_Sync** viene aggiunto al nodo **Applicazione > Configurazione task** nella **Struttura applicazioni**.  
Se si deseleziona l'opzione **Attiva produzione Sync** in questa finestra di dialogo, il task **TMSC01\_Sync** viene eliminato automaticamente dalla **Struttura applicazioni** nel programma.  
**NOTA:** non eliminare o modificare gli attributi **Tipo** o **Evento esterno** dei task **TMSC01\_Sync**. Se si esegue questa operazione, il software rileverà un errore al momento di compilare l'applicazione e non sarà possibile scaricarla nel controller.
- **TIME**: Non modificabile.

## Limiti operativi CANopen

Il master CANopen ha i seguenti limiti operativi:

- Numero massimo di dispositivi slave: 63
- Numero massimo di PDO di ricezione (RPDO): 252
- Numero massimo di PDO di trasmissione (TPDO): 252

### AVVERTIMENTO

#### FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Non collegare più di 63 dispositivi slave CANopen al controller
- Programmare l'applicazione in modo da utilizzare al massimo 252 PDO di trasmissione (TPDO).
- Programmare l'applicazione in modo da utilizzare al massimo 252 PDO di ricezione (RPDO).

**Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

## Formato bus CAN

Il formato del bus CAN è CAN2.0A per CANopen.

# Glossario

## A

**ARP:**

(*Address Resolution Protocol*) Un protocollo del livello di rete IP per Ethernet che associa un indirizzo IP a un indirizzo MAC (hardware)

## B

**BOOTP:**

(*bootstrap protocol*) Un protocollo di rete UDP che può essere utilizzato come client di rete per ottenere automaticamente un indirizzo IP (ed eventualmente altri dati) da un server. Il client si identifica per il server con l'indirizzo MAC del client. Il server, che conserva una tabella preconfigurata degli indirizzi MAC del dispositivo client e gli indirizzi IP associati, invia al client l'indirizzo IP preconfigurato. Originariamente, BOOTP era utilizzato come metodo per consentire l'avvio remoto di host senza disco tramite rete. Il processo BOOTP assegna gli indirizzi IP per un periodo di tempo indefinito. Il servizio BOOTP utilizza le porte 67 e 68 UDP.

## C

**CANopen:**

Un protocollo di comunicazione standard industriale aperto e una specifica del profilo dispositivo (EN 50325-4).

## D

**DHCP:**

(*Dynamic Host Configuration Protocol*) Un'estensione avanzata di BOOTP. DHCP è più avanzato, ma sia DHCP che BOOTP sono comuni. (DHCP può gestire le richieste client BOOTP).

**DNS:**

(*Domain Name System*) Il sistema di assegnazione dei nomi per computer e dispositivi collegati a una LAN o a Internet.

**DTM:**

(*device type manager*) Classificato in 2 categorie:

- I DTM dispositivo si collegano ai componenti della configurazione dei dispositivi di campo.
- CommDTMs si collegano ai componenti della comunicazione software.

Il DTM fornisce una struttura unificata per l'accesso ai parametri del dispositivo e la configurazione, il funzionamento e la diagnostica dei dispositivi. I DTM possono essere una semplice interfaccia utente grafica per l'impostazione dei parametri dei dispositivi su un'applicazione altamente sofisticata che supporta l'esecuzione di calcoli complessi in tempo reale a scopo di diagnostica e manutenzione.

## E

**EDS:**

(*Electronic Data Sheet*) Un file per la descrizione del dispositivo del bus di campo che contiene, ad esempio, le proprietà di un dispositivo come i parametri e le impostazioni.

**EtherNet/IP:**

(*Protocollo industriale Ethernet*) Un protocollo di comunicazione aperto per la produzione di soluzioni di automazione nei sistemi industriali. EtherNet/IP fa parte di una famiglia di reti che implementa il protocollo CIP ai livelli superiori. L'organizzazione di supporto (ODVA) specifica EtherNet/IP per il raggiungimento dell'adattabilità globale e l'indipendenza del supporto.

**Ethernet:**

Una tecnologia di livello fisico e di collegamento dati per LANs, noto anche come IEEE 802.3.

**I****ICMP:**

(*Internet Control Message Protocol*) Riporta gli errori e fornisce informazioni relative all'elaborazione dei datagrammi.

**IGMP:**

(*Internet group management protocol*) Un protocollo di comunicazione utilizzato dagli host e dai router adiacenti sulle reti IPv4 per stabilire associazioni tra gruppi multicast.

**IP:**

(*Internet Protocol*) Parte della famiglia di protocolli TCP/IP che individua gli indirizzi Internet dei dispositivi, instrada i messaggi in uscita e riconosce i messaggi in ingresso.

**M****MAC indirizzo:**

(*Media Access Control*) Un numero univoco a 48 bit associato a un componente hardware specifico. L'indirizzo MAC viene programmato in ogni scheda di rete o dispositivo alla produzione.

**MSB:**

(*Bit/byte più significativo*) La parte di un numero, un indirizzo o un campo scritto nella posizione più a sinistra in notazione esadecimale o binaria convenzionale.

**N****NMT:**

(*network management*). I protocolli di gestione CANopen che forniscono servizi per l'inizializzazione della rete, il controllo degli errori e il controllo dello stato dei dispositivi.

**P****PDO:**

(*Process Data Object, Oggetto dati di processo*) Un messaggio di trasmissione non confermato o inviato da un dispositivo generatore a un dispositivo utilizzatore in una rete basata su CAN. Il PDO trasmesso dal dispositivo generatore possiede un identificativo specifico che corrisponde al PDO ricevuto dai dispositivi utilizzatori.

**protocollo:**

Una convenzione o una definizione degli standard che controlla o attiva il collegamento, la comunicazione e il trasferimento di dati tra 2 sistemi e dispositivi informatici.

**R****rete di controllo:**

Una rete contenente logic controller, sistemi SCADA, PC, HMI, switch, ...

Sono supportati due tipi di topologie:

- piana: tutti i moduli e i dispositivi di questa rete appartengono alla stessa subnet.
- su due livelli: la rete è suddivisa in una rete operativa e una rete inter-controller.

Queste due reti possono essere fisicamente indipendenti, ma sono generalmente collegati da un dispositivo di instradamento.

**RPI:**

*(requested packet interval)* Il periodo di tempo che intercorre tra le trasmissioni di dati cicliche richieste dallo scanner. I dispositivi EtherNet/IP pubblicano i dati alla velocità specificata dal RPI a loro assegnato dallo scanner e ricevono richieste di messaggio dallo scanner con un periodo uguale a RPI.

**RSTP:**

*(Rapid Spanning Tree Protocol)* Un protocollo di rete ad alta velocità che crea una topologia logica senza anelli per le reti Ethernet.

**S****SDO:**

*(Service Data Object, Oggetto dati del servizio)* Un messaggio utilizzato dal master del bus di campo per accedere (in lettura/scrittura) alle directory oggetto dei nodi di rete nelle reti basate su CAN. I tipi SDO includono i servizi SDOs (SSDOs) e client SDOs (CSDOs).

**T****TCP:**

*(Transmission Control Protocol)* Protocollo di livello di trasporto basato su connessione che fornisce una trasmissione dei dati bidirezionale simultanea. TCP è parte di una suite di protocollo TCP/IP.

**TPDO:**

*(Transmit Process Data Object, Oggetto dati di processo di trasmissione)* Un messaggio di trasmissione non confermato o inviato da un dispositivo generatore a un dispositivo utilizzatore in una rete basata su CAN. Il PDO trasmesso dal dispositivo generatore possiede un identificativo specifico che corrisponde al PDO ricevuto dai dispositivi utilizzatori.

**U****UDP:**

*(User Datagram Protocol)* Un protocollo in modalità senza connessione (definito da IETF RFC 768) nel quale i messaggi sono trasmessi in un datagramma (telegramma dati) a un computer di destinazione su una rete IP. Il protocollo UDP è tipicamente raggruppato con il protocollo Internet. I messaggi UDP/IP non attendono una risposta e sono perciò ideali per le applicazioni in cui i pacchetti scartati non richiedono una ritrasmissione (come nel caso di streaming video e delle reti che richiedono esecuzioni in tempo reale).

# Indice

## E

espansione, moduli	
Configurazione .....	13
Ethernet	
Dispositivo slave Modbus TCP .....	21
EtherNet/IP, dispositivo.....	20
servizi .....	14

## F

firewall	
comandi script .....	30
configurazione .....	28
file di script predefinito.....	28

## M

moduli di espansione	
aggiunta .....	12

## P

protocolli.....	14
Protocolli	
IP.....	16

## S

script, comandi	
firewall .....	30



**Schneider Electric**  
35 rue Joseph Monier  
92500 Rueil Malmaison  
France

+ 33 (0) 1 41 29 70 00

[www.se.com](http://www.se.com)

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.