Modbus TCP Communication Device Type Manager

Manuale dell'utente

02/2019

EIO0000000368.06

www.schneider-electric.com

Questa documentazione contiene la descrizione generale e/o le caratteristiche tecniche dei prodotti qui contenuti. Questa documentazione non è destinata e non deve essere utilizzata per determinare l'adeguatezza o l'affidabilità di questi prodotti relativamente alle specifiche applicazioni dell'utente. Ogni utente o specialista di integrazione deve condurre le proprie analisi complete e appropriate del rischio, effettuare la valutazione e il test dei prodotti in relazione all'uso o all'applicazione specifica. Né Schneider Electric né qualunque associata o filiale deve essere tenuta responsabile o perseguibile per il cattivo uso delle informazioni ivi contenute. Gli utenti possono inviarci commenti e suggerimenti per migliorare o correggere questa pubblicazione.

Si accetta di non riprodurre, se non per uso personale e non commerciale, tutto o parte del presente documento su qualsivoglia supporto senza l'autorizzazione scritta di Schneider Electric. Si accetta inoltre di non creare collegamenti ipertestuali al presente documento o al relativo contenuto. Schneider Electric non concede alcun diritto o licenza per uso personale e non commerciale del documento o del relativo contenuto, ad eccezione di una licenza non esclusiva di consultazione del materiale "così come è", a proprio rischio. Tutti gli altri diritti sono riservati.

Durante l'installazione e l'uso di questo prodotto è necessario rispettare tutte le normative locali, nazionali o internazionali in materia di sicurezza. Per motivi di sicurezza e per assicurare la conformità ai dati di sistema documentati, la riparazione dei componenti deve essere effettuata solo dal costruttore.

Quando i dispositivi sono utilizzati per applicazioni con requisiti tecnici di sicurezza, occorre seguire le istruzioni più rilevanti.

Un utilizzo non corretto del software Schneider Electric (o di altro software approvato) con prodotti hardware Schneider Electric può costituire un rischio per l'incolumità del personale o provocare danni alle apparecchiature.

La mancata osservanza di queste indicazioni può costituire un rischio per l'incolumità del personale o provocare danni alle apparecchiature.

© 2019 Schneider Electric. Tutti i diritti riservati.

Indice

	Informazioni di sicurezza	5
	Informazioni su...	7
Capitolo 1	**Requisiti hardware e software**	9
	Requisiti di sistema	10
	Compatibilità	11
	Installazione e rimozione	12
Capitolo 2	**Tipi di collegamento e modelli di comunicazione**	13
	Tipo di connessione	14
	Modello di comunicazione	15
Capitolo 3	**Interfaccia grafica utente**	17
	Interfaccia grafica utente	17
Capitolo 4	**Configurazione**	21
	Scheda Configurazione	22
	Scheda Runtime	24
	Tabella degli indirizzi	28
	Configurazione dell'analisi	30
Capitolo 5	**Cybersicurezza**	33
	Che cos'è la cybersicurezza?	34
	Linee guida Schneider Electric	36
Glossario		39
Indice analitico		43

Informazioni di sicurezza

Informazioni importanti

AVVISO

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'incolumità personale.

⚠ PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **provoca** la 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'incolumità 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 su...

In breve

Scopo del documento

Il presente Manuale dell'utente descrive l'uso del Communication Device Type Manager (Comm DTM) per Modbus.

Nota di validità

Questo documento è stato aggiornato con la release di Modbus Communication Library V2.6.9.

Informazioni relative al prodotto

⚠ AVVERTIMENTO

PERDITA DI CONTROLLO

- Il progettista di qualsiasi schema di controllo deve prendere in considerazione le modalità di errore potenziali dei vari percorsi di controllo e, per alcune funzioni di controllo particolarmente critiche, deve fornire i mezzi per raggiungere uno stato di sicurezza durante e dopo un errore di percorso. Esempi di funzioni di controllo critiche sono ad esempio l'arresto di emergenza e gli stop di fine corsa, l'interruzione dell'alimentazione e il riavvio.
- Per le funzioni di controllo critiche occorre prevedere sequenze di controllo separate o ridondanti.
- Le sequenze di controllo del sistema possono includere link di comunicazione. È necessario tenere presente le possibili implicazioni di ritardi di trasmissione imprevisti o di errori del collegamento.
- Osservare tutte le norme per la prevenzione degli incidenti e le normative di sicurezza locali.[1]
- Prima della messa in servizio dell'apparecchiatura, controllare singolarmente e integralmente il funzionamento di ciascun controller.

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

[1] 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.

Capitolo 1
Requisiti hardware e software

Contenuto di questo capitolo

Questo capitolo contiene le seguenti sottosezioni:

Argomento	Pagina
Requisiti di sistema	10
Compatibilità	11
Installazione e rimozione	12

Requisiti di sistema

Requisiti hardware

Requisito	Minimo	Consigliato
Computer	Pentium 4 o equivalente	
RAM	1 GB	2 GB
Spazio libero sul disco rigido dell'unità di sistema	100 MB	
Spazio libero sul disco rigido dell'unità di installazione	100 MB	
File swap	1024 MB	2048 MB
Monitor	Risoluzione SVGA 800 x 600 a 256 colori	Risoluzione True Color XGA 1024 x 768

Requisiti software

Sistemi operativi software

Sistema operativo	Edizione/Service Pack	Considerazioni particolari
Windows 7 a 32 bit	SP1	Per installare il sono necessari i diritti di accesso come amministratore.Modbus TCP Comm DTM
Windows 7 a 64 bit	SP1	
Windows 8.1, 10 Professional	–	

Software installato sul PC

Software	Edizione	Considerazioni particolari
Microsoft .NET Framework	V2.0 SP2	–
Applicazione FDT Frame	FDT 1.2 o FDT 1.2.1	Il Comm DTM di Modbus TCP richiede un'applicazione FDT Frame conforme allo standard FDT. L'applicazione FDT Frame deve supportare Microsoft.NET Framework 2.0.

Compatibilità

Compatibilità FDT

Il Modbus Comm DTM è conforme agli standard FDT FDT 1.2 e FDT 1.2.1. È basato su FDT Modbus Annex 1.0.

Compatibilità Modbus

Il Modbus Comm DTM supporta i servizi Modbus indicati nella specifica Modbus Application Protocol V1.1b

Installazione e rimozione

Installazione

Fare doppio clic sul file *setup.exe* e seguire le istruzioni della procedura di installazione guidata.

Rimozione

Per rimuovere il DTM dal computer, selezionare **Start** → **Impostazioni** → **Pannello di controllo** → **Installazione applicazioni**.

Capitolo 2
Tipi di collegamento e modelli di comunicazione

Introduzione

Questo capitolo fornisce una panoramica delle configurazioni che possono essere utilizzate per stabilire le comunicazioni Modbus.

Contenuto di questo capitolo

Questo capitolo contiene le seguenti sottosezioni:

Argomento	Pagina
Tipo di connessione	14
Modello di comunicazione	15

Tipo di connessione

Introduzione

Il Modbus TCP Comm DTM può essere utilizzato per stabilire una comunicazione Modbus e basata sul seguente tipo di connessione.

Connessione TCP

Il Modbus TCP Comm DTM permette di stabilire una comunicazione Modbus via TCP. La connessione verrà stabilita tramite la scheda di rete Ethernet del PC.

Modello di comunicazione

Introduzione

Questo capitolo descrive il modello di comunicazione supportato dal Modbus TCP Comm DTM.

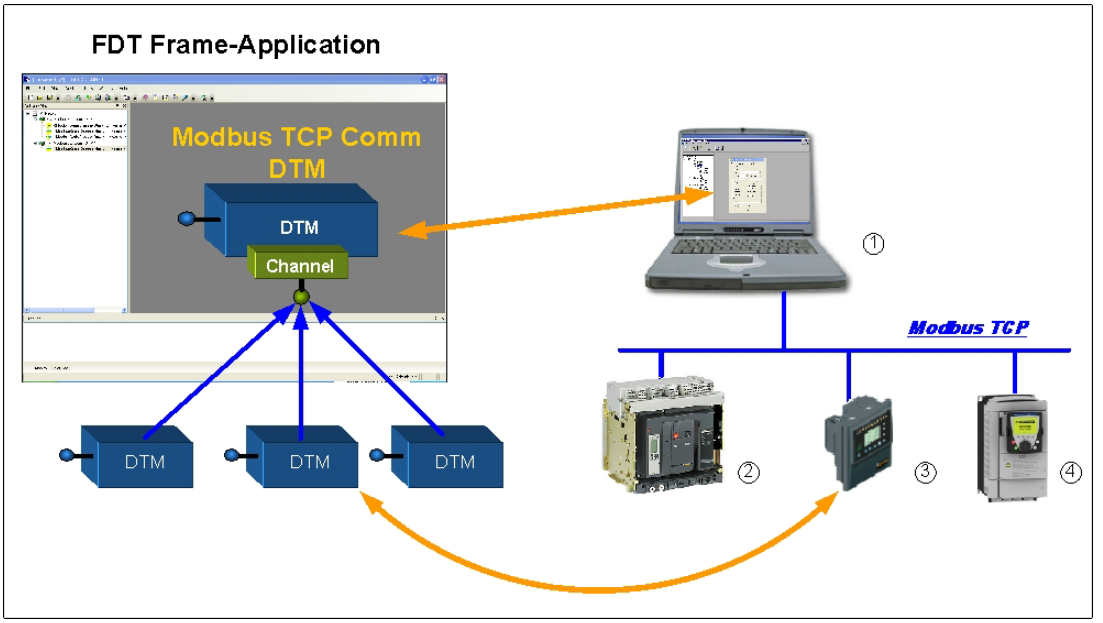
NOTA: La tecnologia FDT non è stata progettata per un trasferimento dati in tempo reale. In funzione del sistema e del modello di comunicazione impiegato, i dati potrebbero non riflettere lo stato effettivo del dispositivo in tempo reale.

⚠ AVVERTIMENTO
INFORMAZIONI SULLO STATO DEL DISPOSITIVO NON VALIDE Non utilizzare il Modbus Comm DTM per task di controllo o di monitoraggio con requisiti di tempo critici poiché i dati trasferiti potrebbero non riflettere lo stato effettivo del dispositivo. La tecnologia FDT non è destinata a questo scopo. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Connessione di rete

Il Modbus TCP Comm DTM può essere utilizzato per stabilire una comunicazione Modbus tra il PC e il dispositivo di destinazione tramite una rete Ethernet.

In questa configurazione il Modbus TCP Comm DTM funge da client Modbus.



1 PC con Modbus TCP Comm DTM
2 - 4 dispositivi di destinazione

Capitolo 3
Interfaccia grafica utente

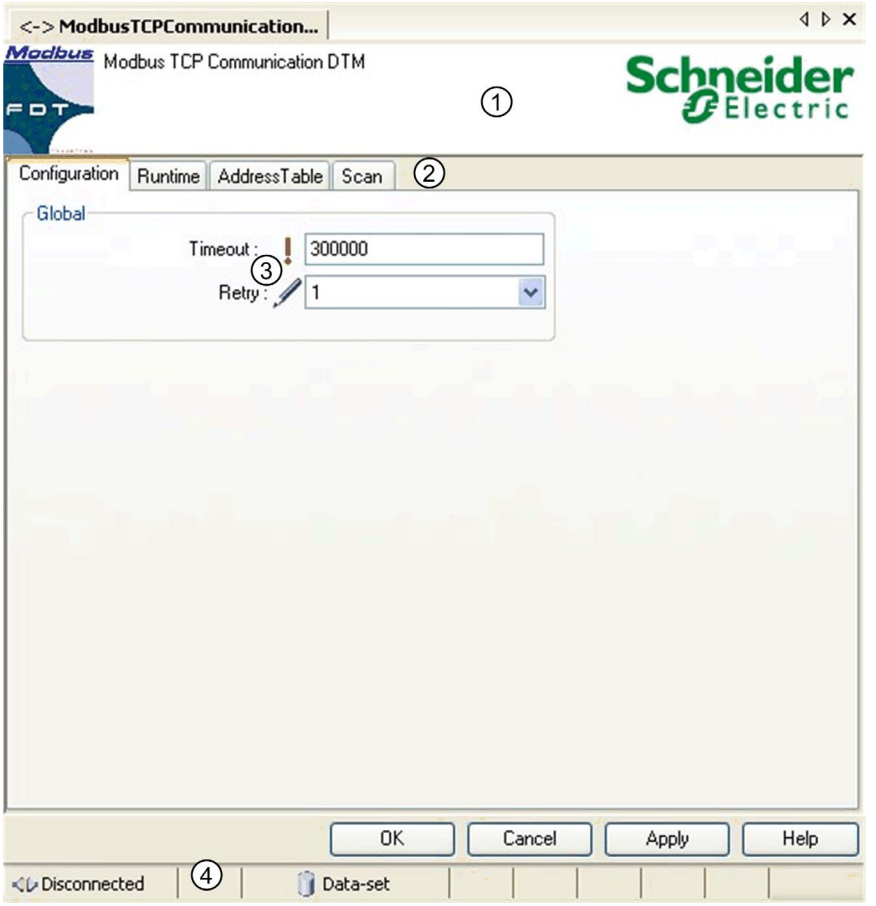
Interfaccia grafica utente

Panoramica

Questo capitolo descrive l'interfaccia grafica utente (GUI) del Modbus TCP Comm DTM.

Introduzione

La seguente figura mostra l'interfaccia grafica utente (GUI) del DTM.



1 Area di identificazione
2 Schede
3 Icone di stato dei parametri
4 Barra di stato

Area di identificazione

L'area di identificazione mostra il nome e la versione del DTM.

Schede

Le schede disponibili permettono di accedere alle varie funzioni del DTM.

Icone di stato dei parametri

Le icone di stato dei parametri forniscono informazioni sullo stato corrente dei parametri.

Stati dei parametri possibili

Icona	Significato
	Il parametro è stato modificato e ha un valore non valido.
	Il parametro è stato modificato e ha un valore valido.

Barra di stato

La barra di stato fornisce informazioni sullo stato corrente del DTM.

Stati di connessione possibili

Icona	Text	Significato	Stato DTM
	Collegamento	collegamento in corso	Passaggio in online
	Collegato	collegato	online
	Scollegato	scollegamento in corso	passaggio in offline
	interrotto	interrotto	rilevata interruzione della comunicazione
	Scollegato	scollegato	tutti gli altri stati

Stati origine dati possibili

Icona	Text	Comportamento
	Set di dati	I valori visualizzati vengono caricati dal set di dati dell'istanza. I valori modificati si riferiscono solo al set di dati dell'istanza.
	Set di dati bloccato	I valori visualizzati vengono caricati dal set di dati dell'istanza. Il set di dati è bloccato.

Capitolo 4
Configurazione

Contenuto di questo capitolo

Questo capitolo contiene le seguenti sottosezioni:

Argomento	Pagina
Scheda Configurazione	22
Scheda Runtime	24
Tabella degli indirizzi	28
Configurazione dell'analisi	30

Scheda Configurazione

Introduzione

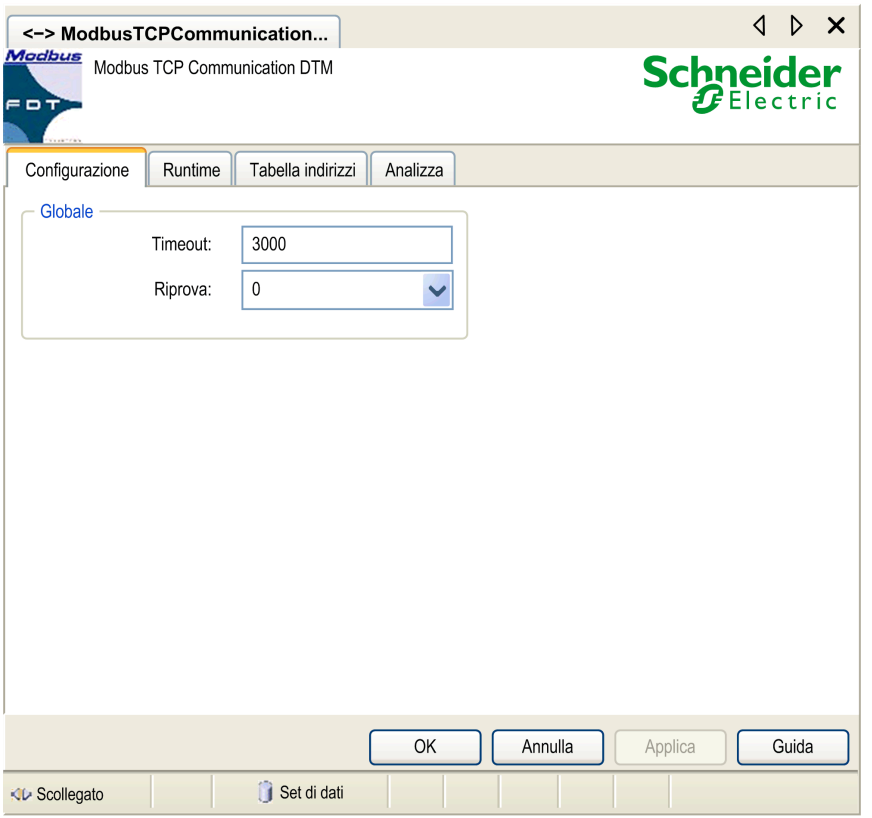
La scheda **Configurazione** del Modbus TCP Comm DTM contiene i parametri di comunicazione.

Scheda Configurazione

È possibile accedere alla scheda **Configurazione** del Modbus TCP Comm DTM in vari modi:

- Nella rappresentazione della rete dell'applicazione frame FDT, fare doppio clic sull'icona Modbus TCP Comm DTM.
- Nella rappresentazione della rete dell'applicazione frame FDT, fare clic con il pulsante destro sull'icona Modbus TCP Comm DTM, quindi fare clic su **Configurazione**.

La seguente figura mostra la scheda **Configurazione** della finestra di dialogo Modbus TCP Comm DTM:



Parametri di comunicazione

La seguente tabella contiene una descrizione dei parametri di comunicazione per la connessione Modbus TCP:

Parametro	Descrizione	Valore predefinito
Globale - Timeout	Timeout risposta del server Modbus.	3000 ms
Numero di tentativi	Numero di volte che il Modbus TCP Comm DTM rinvierà la richiesta Modbus sulla connessione TCP in caso di timeout di comunicazione.	0

Comandi di configurazione

Comandi di configurazione disponibili nella scheda **Configurazione**

Comando	Descrizione
OK	Tutti i parametri vengono salvati e la finestra del Modbus TCP Comm DTM viene chiusa. I nuovi valori dei parametri verranno applicati al collegamento successivo.
Annulla	Le modifiche dei parametri vengono salvate e la finestra Modbus TCP Comm DTM viene chiusa. I valori originali verranno applicati al collegamento successivo.
Applica	Salva i parametri ma la finestra Modbus TCP Comm DTM rimane aperta. I nuovi valori dei parametri verranno applicati al collegamento successivo.

Scheda Runtime

Introduzione

Il Modbus TCP DTM Comm offre vari tipi di informazioni di runtime. Questo capitolo descrive le informazioni fornite dal Modbus TCP DTM Comm e la configurazione della funzione di registro.

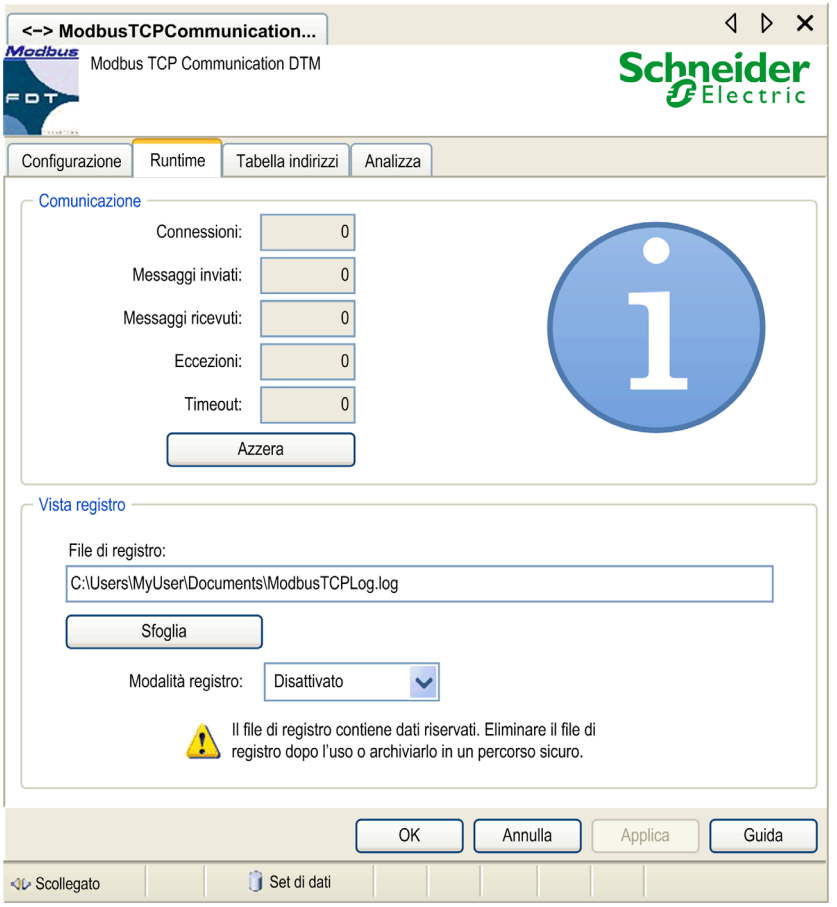
Scheda Runtime

Il Modbus TCP DTM Comm fornisce vari tipi di informazioni di runtime, che possono essere utilizzate per monitorare le comunicazioni stabilite.

Le informazioni di runtime sono disponibili nella scheda **Runtime** del Modbus TCP Comm DTM, alla quale si può accedere nel seguente modo:

- Nella rappresentazione della rete dell'applicazione frame FDT, fare doppio clic sull'icona Modbus TCP DTM Comm. Selezionare la scheda **Runtime**.
- Nella rappresentazione della rete dell'applicazione frame FDT, fare clic con il pulsante destro sull'icona Modbus TCP, quindi fare clic su **Configurazione**. Selezionare la scheda **Runtime**.

La seguente figura mostra la scheda **Runtime** della finestra di dialogo Modbus TCP Comm DTM:



Comandi di configurazione

La tabella contiene una descrizione dei comandi di configurazione disponibili nella scheda **Runtime**

Comando	Descrizione
OK	I parametri vengono salvati e la finestra Modbus TCP Comm DTM viene chiusa. I nuovi valori dei parametri verranno applicati al collegamento successivo.

Comando	Descrizione
Annulla	Le modifiche dei parametri vengono annullate e la finestra Modbus TCP Comm DTM viene chiusa. I valori originali verranno applicati al collegamento successivo.
Sfoglia	Apre il browser del file, dove l'utente può specificare il percorso del file di registro
Reimposta	Azzera tutti i parametri di runtime
Applica	Memorizza i parametri, ma la finestra Modbus TCP Comm DTM rimane aperta. I nuovi valori dei parametri verranno applicati al collegamento successivo.

Parametri di runtime

La tabella contiene una descrizione dei parametri di runtime disponibili nella scheda **Runtime** del Modbus TCP Comm DTM:

Comando	Descrizione
Connessioni	Numero di connessioni attive al Modbus TCP Comm DTM.
Messaggi inviati	Numero di messaggi inviati dal Modbus TCP Comm DTM.
Messaggi ricevuti	Numero di messaggi ricevuti dal Modbus TCP Comm DTM.
Eccezioni	Numero di messaggi di eccezione Modbus ricevuti dal Modbus TCP Comm DTM.
Timeout	Numero di errori di timeout rilevati alla ricezione.

File di registro

Il Modbus TCP Comm DTM offre la possibilità di creare un file di registro. Nella casella **File di registro** specificare il percorso nel quale archiviare il file di registro.

La tabella descrive le informazioni che verranno scritte nel file di registro a seconda della **Modalità di registro** selezionata:

Modalità di registro	Descrizione
Disattivato	Disattiva la funzione del file di registro.
Registrazione errori	Nel file di registro vengono scritte solo le informazioni relative agli errori di timeout rilevati e alle eccezioni Modbus ricevute.
Tutto registrato	Oltre alle informazioni sugli errori di timeout e alle eccezioni Modbus ricevute, nel file di registro vengono scritte anche le informazioni relative alle richieste Modbus inviate e alle risposte Modbus ricevute dal DTM del dispositivo.

Raccomandazione per l'ottimizzazione della sicurezza informatica

Il file di registro in genere contiene dati riservati, quali:
- indirizzi dispositivo
- nomi dispositivo
- dettagli della topologia di rete
- dettagli della configurazione di rete

Questo file è memorizzato sul disco rigido del PC. Eliminare il file di registro se non è più necessario o salvarlo in un percorso sicuro, in modo che sia accessibile senza autorizzazione.

Tabella degli indirizzi

Introduzione

Il Modbus Comm DTM fornisce una tabella degli indirizzi nella quale sono elencati tutti i DTM del dispositivo e i relativi indirizzi di destinazione. Questo capitolo descrive le informazioni riportate nella tabella degli indirizzi e la configurazione degli indirizzi di destinazione dei dispositivi.

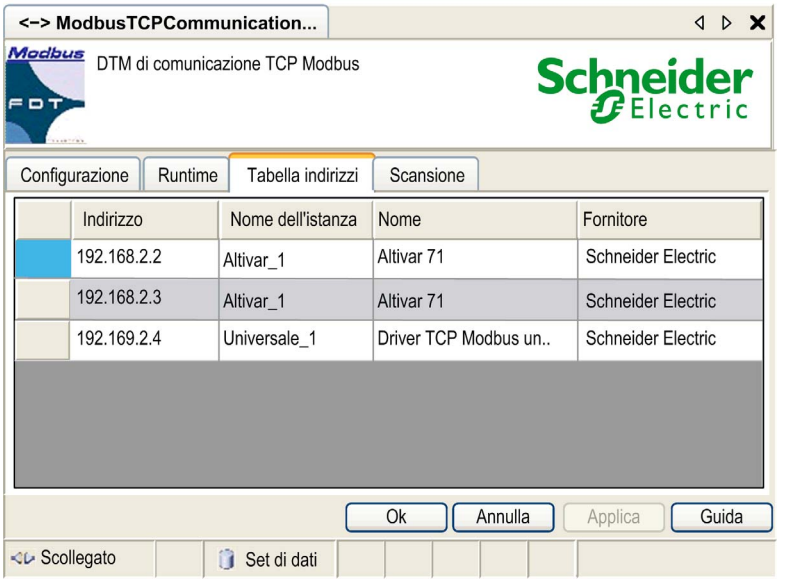
Tabella degli indirizzi

Il DTM di comunicazione del Modbus TCP fornisce una tabella degli indirizzi nella quale sono elencati tutti i DTM del dispositivo e i relativi indirizzi di destinazione. In questa tabella di indirizzi è possibile specificare gli indirizzi di destinazione dei DTM dispositivo collegati.

Per accedere alla scheda **Tabella degli indirizzi** procedere nel seguente modo:

- Nella rappresentazione della rete dell'applicazione frame FDT, fare doppio clic sull'icona Modbus TCP Comm DTM. Selezionare la scheda **Tabella degli indirizzi**.
- Nella **Rappresentazione rete** dell'applicazione frame FDT, fare clic con il pulsante destro sull'icona Modbus TCP Comm DTM, quindi fare clic su **Configurazione**. Selezionare la scheda **Tabella degli indirizzi**.

La seguente figura mostra la scheda **Tabella degli indirizzi** della finestra di dialogo Modbus TCP Comm DTM:



Comandi di configurazione

La seguente tabella contiene una descrizione dei comandi di configurazione disponibili nella scheda **Tabella degli indirizzi**

Comando	Descrizione
OK	Le modifiche vengono salvate e la finestra Modbus TCP Comm DTM viene chiusa. I nuovi valori verranno applicati al collegamento successivo.
Annulla	Le modifiche vengono annullate e la finestra Modbus TCP Comm DTM viene chiusa. I valori originali verranno applicati al collegamento successivo.
Applica	Salva le modifiche ma la finestra Modbus TCP Comm DTM rimane aperta. I nuovi valori verranno applicati al collegamento successivo.

Informazioni sull'indirizzo

La tabella contiene una descrizione delle informazioni relative all'indirizzo disponibili nella scheda **Tabella degli indirizzi** del Modbus TCP Comm DTM:

Parametro	Descrizione
Indirizzo	Indirizzo di destinazione del dispositivo hardware da configurare con il DTM collegato
Nome dell'istanza	Nome dell'istanza del DTM
Nome	Nome specifico del DTM
Produttore	Nome del produttore del DTM

Assegnazione degli indirizzi

La tabella degli indirizzi del Modbus TCP Comm DTM può essere utilizzato per specificare l'indirizzo di destinazione del dispositivo hardware da configurare con un DTM specifico. Per specificare l'indirizzo di destinazione, immettere il nuovo indirizzo nel corrispondente campo **Indirizzo** di questo DTM e confermare questa modifica facendo clic sul pulsante **Applica** o facendo clic sul pulsante **Ok**.

Configurazione dell'analisi

Introduzione

Il Modbus Comm DTM offre la possibilità di specificare l'intervallo degli indirizzi analizzati per l'analisi FDT. Questo capitolo descrive la configurazione dei parametri di analisi per l'analisi FDT.

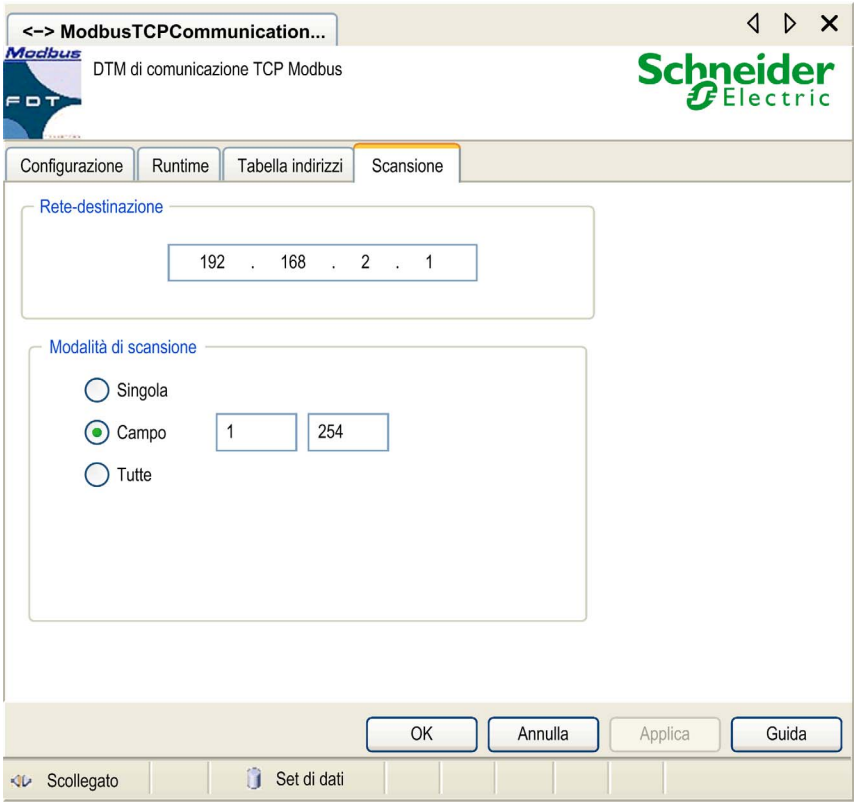
Scheda Analizza

Il Modbus TCP Comm DTM supporta la funzione di analisi come definito nella specifica FDT V1.2.1. L'analisi può essere utilizzata per creare automaticamente la topologia della rete di comunicazione indicata. Il Modbus TCP Comm DTM offre la possibilità di specificare l'intervallo di indirizzi analizzati.

I parametri di analisi sono disponibili nella scheda **Analizza** del Modbus TCP Comm DTM, al quale si può accedere nel seguente modo:

- Nella **Rappresentazione rete** dell'applicazione frame FDT, fare doppio clic sull'icona Modbus TCP Comm DTM. Selezionare la scheda **Analizza**.
- Nella **Rappresentazione rete** dell'applicazione frame FDT, fare clic con il pulsante destro sull'icona Modbus TCP Comm DTM, quindi fare clic su **Configurazione**. Selezionare la scheda **Analizza**.

La figura mostra la scheda **Analizza** della finestra di dialogo Modbus TCP Comm DTM:



Comandi di configurazione

La tabella contiene una descrizione dei comandi di configurazione disponibili nella scheda **Analizza**:

Comando	Descrizione
OK	Le modifiche vengono salvate e la finestra del Modbus Comm DTM viene chiusa. I nuovi valori verranno applicati all'analisi successiva.
Annulla	Le modifiche vengono annullate e la finestra Modbus Comm DTM viene chiusa. I valori originali verranno applicati all'analisi successiva.
Applica	Salva le modifiche ma la finestra Modbus Comm DTM rimane aperta. I nuovi valori verranno applicati all'analisi successiva.

Parametri di analisi per Modbus TCP

La tabella contiene una descrizione dei parametri di scansione disponibili nella scheda **Analizza** del Modbus TCP Comm DTM:

Comando	Descrizione	
Rete-destinazione	Specifica l'intervallo di rete da analizzare.	
Modalità di analisi	**Singolo**	Analizza un solo indirizzo di un dispositivo di destinazione compreso nell'intervallo da 0 a 255 della rete specificata.
	Intervallo	Analizza un intervallo di indirizzi specificato tra 0 e 255 nell'intervallo di rete definito.
	Tutto	Analizza l'intervallo di indirizzi completo dell'intervallo di rete (ossia tutti gli indirizzi compresi tra 0 e 255).

Capitolo 5
Cybersicurezza

Introduzione

La cybersicurezza è un ramo dell'amministrazione di rete che si occupa degli attacchi indirizzati a o provenienti da computer e presenti sulle reti informatiche dai quali possono derivare interruzioni accidentali o intenzionali. L'obiettivo della cybersicurezza è contribuire ad aumentare i livelli di protezione delle informazioni e delle risorse fisiche da furti, danneggiamento, uso improprio o altro problema, mantenendole al contempo accessibili agli utenti che le devono utilizzare.

Non esiste un approccio alla cybersicurezza a se stante adeguato. Schneider Electric raccomanda l'adozione di un approccio di difesa in profondità ("Defense-in-Depth", DiD). Tale approccio, concepito dalla National Security Agency (NSA), suddivide la rete in più livelli distinti per funzioni di sicurezza, apparecchiature e processi. I componenti di base di questo approccio sono:

- valutazione dei rischi
- un piano di sicurezza elaborato sulla base dei risultati della valutazione dei rischi
- una campagna di formazione multifase
- separazione fisica delle reti industriali dalle reti aziendali, con la creazione di una zona demilitarizzata (DMZ) e con l'uso di firewall e instradamento per delimitare altre zone di sicurezza
- controllo degli accessi al sistema
- riduzione delle vulnerabilità dei dispositivi ("hardening")
- monitoraggio e manutenzione delle reti

Questo capitolo definisce gli elementi che consentono di configurare un sistema meno sensibile agli attacchi informatici. Per informazioni dettagliate sull'approccio di difesa in profondità, fare riferimento a *TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room*, sul sito *Schneider Electric website*.

Contenuto di questo capitolo

Questo capitolo contiene le seguenti sottosezioni:

Argomento	Pagina
Che cos'è la cybersicurezza?	34
Linee guida Schneider Electric	36

Che cos'è la cybersicurezza?

Introduzione

Le cyberminacce, o minacce cibernetiche, sono azioni deliberate o eventi avversi che possono interrompere il normale funzionamento di computer e reti informatiche. Tali azioni possono essere avviate all'interno di una struttura fisica o provenire da una posizione esterna. Le esigenze di sicurezza per l'ambiente di controllo includono:

- limiti fisici e logici separati
- più siti e ampie distanze geografiche
- conseguenze negative dell'implementazione della sicurezza sulla disponibilità dei processi
- maggiore esposizione a worm e virus che migrano dai sistemi aziendali ai sistemi di controllo quando le comunicazioni di controllo aziendale diventano più aperte
- maggiore esposizione a software dannoso proveniente da dispositivi USB, laptop di fornitori e tecnici dell'assistenza e rete aziendale
- impatto diretto dei sistemi di controllo su apparecchiature fisiche e meccaniche

Origine dei cyberattacchi

Implementare un piano di cybersicurezza che tenga conto delle diverse origini da cui possono provenire i cyberattacchi e gli eventi avversi, inclusi:

Origine	Descrizione
interna	• comportamento inappropriato di dipendenti o fornitori • dipendente o fornitore scontento
esterno opportunistico (indiretto)	• script kiddie* • hacker "ricreativi" • scrittori di virus
esterno deliberato (diretto)	• gruppi criminali • attivisti • terroristi • agenzie di stati esteri
accidentale	
* termine dello slang usato per descrivere gli hacker che utilizzano script dannosi scritti da altri senza comprendere esattamente il funzionamento dello script o il suo potenziale impatto su un sistema	

Un cyberattacco deliberatamente lanciato su un sistema di controllo può essere motivato dall'intento di causare una serie di conseguenze dannose, inclusi:

- interruzione del processo di produzione con il blocco o il ritardo del flusso di informazioni
- danno, disattivazione o spegnimento di apparecchiature per influire negativamente sulla produzione o sull'ambiente
- modifica o disattivazione di sistemi di sicurezza per causare intenzionalmente un danno

Metodi di accesso degli autori degli attacchi

L'autore di un attacco cibernetico aggira le difese adottate per ottenere accesso alla rete del sistema di controllo. I punti di accesso comuni includono:

- accesso remoto ai dispositivi di un'unità terminale remota (RTU)
- punti di accesso del fornitore (come i punti di accesso dell'assistenza tecnica)
- prodotti di rete con controllo IT
- rete privata virtuale aziendale (VPN)
- collegamenti a database
- firewall configurati in modo non corretto
- utility "peer"

Certificazioni di cybersicurezza

Schneider Electric ha sviluppato linee guida per la cybersicurezza sulla base delle seguenti raccomandazioni:

- Achilles
- ISA Secure

Domande?

Per inviare una domanda relative alla cybersicurezza e a problemi di sicurezza dei report, oppure per informarsi sulle ultime novità di Schneider Electric, visitare il *website*.

Linee guida Schneider Electric

Introduzione

Il sistema del PC può eseguire una serie di applicazioni per aumentare la sicurezza dell'ambiente di controllo. Il sistema è dotato di impostazioni predefinite che richiedono la riconfigurazione per l'allineamento alle raccomandazioni sull'hardening dei dispositivi Schneider Electric dell'approccio di difesa in profondità (Defense-in-Depth, DiD).

Le seguenti linee guida descrivono le procedure in un sistema operativo Windows 7. Sono fornite solo a titolo esemplificativo. Ogni sistema operativo e applicazione può avere requisiti o procedure diverse.

Disabilitazione delle schede di interfaccia di rete inutilizzate

Verificare che le schede dell'interfaccia di rete non richieste dall'applicazione siano disattivate. Ad esempio, se il sistema è dotato di 2 schede e l'applicazione ne utilizza solo una, verificare che l'altra scheda di rete (connessione alla rete locale, LAN 2) sia disattivata.

Per disattivare una scheda di rete in Windows 7:

Passo	Azione
1	Selezionare **Pannello di controllo → Rete e Internet → Centro connessioni di rete e condivisione → Modifica impostazioni scheda**.
2	Fare clic con il pulsante destro del mouse sulla connessione non utilizzata. Selezionare **Disabilita**.

Configurazione della connessione all'area locale

Diverse impostazioni di rete Windows forniscono un miglioramento della sicurezza in linea con l'approccio di difesa in profondità (DiD) raccomandato da Schneider Electric.

Nei sistemi Windows 7, accedere a queste impostazioni selezionando **Pannello di controllo → Rete e Internet → Centro connessioni di rete e condivisione → Modifica impostazioni scheda → Connessione alla rete locale (x)**.

Questo elenco è un esempio delle modifiche alla configurazione che possono essere apportate nel sistema dalla schermata **Proprietà connessione alla rete locale (LAN):**:

- Disattivare tutti gli stack IPv6 sulle rispettive schede di rete (questo esempio di sistema non richiede l'intervallo di indirizzi IPv6 e la disattivazione degli stack IPv6 limita la vulnerabilità a potenziali rischi di sicurezza IPv6).
- Disabilitare **Condivisione di file e stampanti per rete Microsoft**.

Le raccomandazioni di Schneider Electric per una difesa in profondità includono anche quanto segue:

- Definire solo indirizzi IPv4, maschere di sottorete e gateway statici.
- Non utilizzare DHCP o DNS nella sala di controllo.

Gestione dei firewall Windows

Le raccomandazioni di Schneider Electric sull'approccio di difesa in profondità (DiD) includono l'attivazione del firewall dell'host Windows su tutti i PC. Attivare i firewall per tutti i profili pubblici o privati elencati.

È consigliabile che gli utenti definiscano le regole dei firewall che rifiutano le connessioni dirette o provenienti da qualunque host esterno sconosciuto/non affidabile.

Disabilitazione del protocollo RDP

Nell'ambito del proprio approccio alla difesa in profondità (Defense-in-Depth, DiD), Schneider Electric consiglia di disabilitare il protocollo RDP a meno che l'applicazione non richieda esplicitamente RDP. La procedura seguente descrive come disattivare il protocollo:

Passo	Azione
1	In Windows 2008R2 o Windows 7, disabilitare RDP selezionando **Computer → Proprietà del sistema → Impostazioni di sistema avanzate**.
2	Nella scheda **Connessione remota**, deselezionare la casella di controllo **Consenti connessioni di Assistenza remota al computer**.
3	Selezionare la casella di controllo **Non consentire la connessione al computer**.

Aggiornamento dei criteri di sicurezza

Aggiornare i criteri di sicurezza sui PC del sistema da `gpupdate` in una finestra di comando. Per maggiori informazioni, vedere la documentazione di Microsoft su `gpupdate`.

Disabilitazione di LANMAN e NTLM

Il protocollo Microsoft LAN Manager (LANMAN o LM) e il suo successore NT LAN Manager (NTLM) presentano delle vulnerabilità che ne sconsiglino l'utilizzo nelle applicazioni di controllo.

La procedura seguente illustra come disabilitare LM e NTLM in un sistema Windows 7 o Windows 2008R2:

Passo	Azione
1	In una finestra di comando, eseguire `secpol.msc` per aprire la finestra **Criteri di sicurezza locali**.
2	Aprire **Impostazioni di protezione → Criteri locali → Opzioni di sicurezza**.
3	Selezionare **Invia solo risposta NTLMv2. Rifiutare LM & NTLM** nel campo **Sicurezza di rete: livello di autenticazione LAN Manager**.
4	Selezionare la casella di controllo **Sicurezza di rete: non memorizzare il valore hash di LAN Manager al prossimo cambio di password**.
5	In una finestra di comando, immettere `gpupdate` per confermare il criterio di sicurezza modificato.

Gestione degli aggiornamenti

Prima della distribuzione, aggiornare tutti i sistemi operativi del PC utilizzando le utility nella pagina Web **Windows Update** di Microsoft. Per accedere a questo strumento in Windows 2008R2, Windows 7 o Windows XP, selezionare **Start → Tutti i programmi → Windows Update**.

Glossario

C

Codice funzione

Un codice funzione è un set di istruzioni che ordina a uno o più dispositivi slave a un indirizzo specificato di eseguire un determinato tipo di azione, ad esempio leggere un insieme di registri dati e rispondere con il contenuto.

Configurazione

La disposizione e interconnessione di componenti hardware all'interno di un sistema e le selezioni hardware e software che determinano le caratteristiche operative del sistema.

CRC

Cyclic Redundancy Check (controllo di ridondanza ciclico)

I messaggi che implementano questo meccanismo di verifica degli errori hanno un campo CRC calcolato dal trasmettitore in base al contenuto del messaggio. I nodi riceventi ricalcolano il campo. Una discordanza tra i due codici indica che vi è una differenza tra il messaggio trasmesso e quello ricevuto.

D

DTM

Un DTM (Device Type Manager) è un tipo di driver del dispositivo fornito dal produttore del dispositivo di campo. Un DTM contiene le informazioni specifiche del dispositivo e fornisce un'interfaccia grafica utente. Un DTM può essere utilizzato per eseguire task di monitoraggio e di configurazione sul dispositivo specifico. Un DTM non è un'applicazione standalone. Per poter essere eseguito richiede una FDT Frame Application.

E

Ethernet

Cablaggio di rete locale (LAN) e specifica di segnalazione utilizzata per connettere apparecchiature nell'ambito di un'area definita, ad es. un edificio. Ethernet utilizza un bus o una topologia a stella per connettere diversi nodi in un rete.

F

FDT

La tecnologia FDT (Field Device Tool) standardizza l'interfaccia di comunicazione tra i dispositivi e i sistemi di campo (*www.fdtgroup.org*).

G

Gateway

Programma o hardware che esegue lo scambio di dati tra reti diverse.

I

Interfaccia

L'interfaccia rappresenta la connessione fisica con la rete, ad esempio una scheda di rete o un convertitore USB-RS 232.

IP

Internet Protocol (Protocollo Internet).

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

L

LAN

Local Area Network.

Rete per la comunicazione di dati a breve distanza.

M

Master/slave, modello

La direzione di controllo in una rete che implementa il modello master/slave è dal master verso i dispositivi slave.

MB

Abbreviazione di Modbus

Modbus

Modbus è un protocollo di messaggistica di livello applicazione. Modbus offre molti servizi, specificati da codici di funzione.

S

SL

Abbreviazione di Serial Line

T

TCP

Transmission Control Protocol.

Un protocollo del livello di trasporto orientato alle connessioni che fornisce una trasmissione dati full-duplex affidabile. TCP fa parte della serie di protocolli TCP/IP.

Telegramma

Pacchetto dati utilizzato nelle comunicazioni seriali.

Indice analitico

C

compatibilità, *11*
Configurazione dell'analisi, *30*
Connessione
    rete, *15*
    TCP, *14*
    tipo, *14*
Cybersicurezza, *33*
    certificazioni, *34*
    introduzione, *34*

I

installazione, *12*
Interfaccia grafica utente, *17*
Interfaccia utente, *17*

M

Modalità di analisi, *30*
Modello di comunicazione, *15*

N

numero di tentativi, *23*

R

Requisiti
    hardware, *10*
    software, *10*
Runtime, scheda, *24*

S

Scheda Configurazione, *22*
sicurezza informatica
    connessione all'area locale, *36*
    desktop remoto, *37*
    firewall, *37*
    LANMAN/NTLM, *37*
    linee guida, *36*
    schede di interfaccia di rete, *36*

T

Tabella degli indirizzi, *28*