TeSys Active

TeSys Tera Motor Management System

Guida alla sicurezza informatica

Tesys offre soluzioni innovative e connesse per gli avviatori per motori

DOCA0260IT-00
11/2025

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.

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

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'incolumità 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'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 sul Documento

Scopo del documento

Questa guida fornisce informazioni sugli aspetti relativi alla Sicurezza Informatica del sistema TeSys™ Tera per aiutare i progettisti e gli operatori del sistema a promuovere un ambiente operativo sicuro per il prodotto.

Questa guida spiega come proteggere la rete tecnologica operativa o la rete aziendale Ethernet.

NOTA: In questa guida, il termine **security** è utilizzato per indicare la sicurezza informatica.

Nota di validità

Il presente documento è valido per i seguenti componenti certificati di TeSys Tera system:

- LTMTEFM: LTMT main unit con protocollo EtherNet/IP o Modbus TCP/IP, 100–240 Vca/Vdc
- LTMTEBD: LTMT main unit con protocollo EtherNet/IP o Modbus TCP/IP, 24 Vdc
- LTMTMFM: LTMT main unit con protocollo Modbus RTU, 100-240 Vca/Vdc
- LTMTMBD: LTMT main unit con protocollo Modbus RTU, 24 Vdc
- LTMTPFM: LTMT main unit con protocollo PROFIBUS DP, 100-240 Vca/Vdc
- LTMTPBD: LTMT main unit con protocollo PROFIBUS DP, 24 Vdc

Informazioni generali sulla sicurezza informatica

Negli ultimi anni, il numero crescente di macchine e impianti di produzione collegati in rete ha visto un corrispondente aumento del potenziale di minacce informatiche, come accessi non autorizzati, violazioni dei dati e interruzioni operative. È pertanto necessario prendere in considerazione tutte le possibili misure di sicurezza informatica per proteggere risorse e sistemi da tali minacce.

Per consentire di mantenere i prodotti Schneider Electric sicuri e protetti, è nell'interesse dell'utente implementare le pratiche migliori di sicurezza informatica come indicato nel documento Cybersecurity Best Practices:

Schneider Electric fornisce ulteriori informazioni e assistenza:

- Iscriversi alla newsletter sulla sicurezza Schneider Electric.
- Visitare la pagina Web Cybersecurity Support Portal per:
  - Trovare notifiche di sicurezza.
  - Segnalare vulnerabilità e incidenti.
- Visitare la pagina Web Schneider Electric Cybersecurity and Data Protection Posture per:
  - Accedere alla postura di sicurezza informatica.
  - Ulteriori informazioni sulla sicurezza informatica nell'accademia di sicurezza informatica.
  - Esplorare i servizi di sicurezza informatica di Schneider Electric.

Dati ambientali

Per informazioni sulla compatibilità ambientale dei prodotti, consultare l' Environmental Data Program di Schneider Electric.

Lingue disponibili per il documento

Il documento è disponibile nelle seguenti lingue:

- Inglese
- Cinese
- Francese
- German
- Italiano
- Korean
- Spagnolo

Documenti correlati

Titolo della documentazione	Descrizione	Codice di riferimento
Catalogo TeSys Tera Motor Management System	Il catalogo: • Descrive TeSys Tera system • Contiene le caratteristiche tecniche di TeSys Tera	LVCATENTER
Guida Utente TeSys Tera Motor Management System	Questa è la guida principale per l'utente che introduce l'intero TeSys Tera system. Descrive le funzioni principali di LTMT main units, LTMTCT/LTMTCTV Sensor Module, LTMT expansion modulese LTMTCUF control operator unit.	DOCA0257IT
TeSys Tera Motor Management System Guida all'installazione	Questa guida descrive l'installazione, la messa in servizio e la manutenzione di LTMT main unit LTMTCT/ LTMTCTV Sensor Module, LTMT expansion modulese LTMTCUF control operator unit.	DOCA0356IT
Guida in linea TeSys Tera Motor Management System DTM library	Questa guida descrive TeSys Tera DTM, che consente la personalizzazione delle funzioni di controllo di TeSys Tera Motor Management System.	DOCA0275IT
Guida di Comunicazione TeSys Tera Motor Management System Modbus RTU	Questa guida descrive la comunicazione del protocollo di rete Modbus della LTMT main unit.	DOCA0355IT
Guida di comunicazione TeSys Tera Motor Management System PROFIBUS DP	Questa guida descrive la comunicazione del protocollo di rete PROFIBUS DP della LTMT main unit.	DOCA0256IT
Guida di comunicazione TeSys Tera Motor Management System EtherNet/IP	Questa guida descrive la comunicazione del protocollo di rete EtherNet/IP della LTMT main unit.	DOCA0258IT
Guida utente TeSys Tera Motor Management System LTMTCUF control operator unit	Questa guida descrive come installare, configurare e utilizzare la LTMTCUF control operator unit.	DOCA0233IT
Note di rilascio del software TeSys Tera Motor Management System DTM library	Questo documento fornisce importanti informazioni su TeSys Tera DTM Library e fornisce un riepilogo delle nuove funzioni e dei miglioramenti apportati.	DOCA0279IT
TeSys Tera Motor Management System Nota di Rilascio del Firmware	Questo documento fornisce informazioni sulle versioni dei pacchetti firmware di TeSys Tera system e fornisce un riepilogo delle nuove funzioni e dei miglioramenti apportati.	DOCA0276IT
Come posso ridurre la vulnerabilità agli attacchi informatici?	Questa guida descrive i rischi legati alla Sicurezza informatica e le strategie di mitigazione nei sistemi di controllo e automazione.	Come posso ridurre la vulnerabilità agli attacchi informatici?

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

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.

Marchi

QR Code è un marchio registrato di DENSO WAVE INCORPORATED in Giappone e in altri paesi.

Precauzioni

Prima di eseguire qualsiasi procedura descritta in questa guida, leggere con attenzione le seguenti precauzioni.

⚠⚠PERICOLO

RISCHIO DI FOLGORAZIONE, ESPLOSIONE O ARCHI ELETTRICI

- Questa apparecchiatura deve essere installata e sottoposta a manutenzione solo da elettricisti qualificati.
- Prima di lavorare sull'apparecchiatura o al suo interno, disattivare completamente l'alimentazione elettrica.
- Utilizzare l'apparecchiatura e tutti i prodotti associati solo alla tensione specificata.
- Utilizzare sempre un dispositivo di rilevamento di tensione di capacità adeguata per confermare l'assenza di alimentazione.
- Utilizzare interblocchi adeguati qualora siano presenti pericoli per il personale e/o l'apparecchiatura.
- I circuiti della linea di alimentazione devono essere cablati e protetti in conformità alle normative locali e nazionali.
- Utilizzare dispositivi di protezione individuale (PPE) adeguati e conformarsi alle norme relative agli obblighi di sicurezza elettrica sui luoghi di lavoro ai sensi delle norme NFPA 70E, NOM-029-STPS o CSA Z462 o equivalenti locali.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Non smontare, riparare o modificare questa apparecchiatura. Non sono presenti parti riparabili direttamente dall'utente.
- Installare e utilizzare questa apparecchiatura in un alloggiamento opportunamente tarato per l'ambiente applicativo previsto.
- Ciascuna implementazione di questa apparecchiatura deve essere testata singolarmente e accuratamente per valutarne il funzionamento corretto prima della messa in servizio.

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

Personale Qualificato

Solo personale adeguatamente formato, che conosca e comprenda il contenuto della presente guida e di tutta la documentazione relativa al prodotto, è autorizzato a lavorare su e con questo prodotto.

Il personale qualificato deve essere in grado di rilevare possibili pericoli che potrebbero derivare dalla modifica dei valori parametro e in genere dall'apparecchiatura meccanica, elettrica o elettronica. Il personale qualificato deve conoscere perfettamente le norme, le disposizioni e le normative per la prevenzione di incidenti industriali e deve attenersi ad esse in fase di progettazione e implementazione del sistema.

L'uso e l'applicazione delle informazioni contenute nella presente guida richiedono esperienza nella progettazione e programmazione di sistemi di controllo automatizzati. Solo l'utente, il costruttore di quadri elettrici o l'integratore sono a conoscenza delle condizioni e dei fattori che entrano in gioco durante l'installazione, la configurazione, il funzionamento e la manutenzione di un impianto o di una macchina di processo e possono pertanto determinare l'automazione e le apparecchiature associate e i dispositivi di sicurezza e

interblocchi correlati che è possibile utilizzare in modo efficace e corretto durante la scelta delle apparecchiature di automazione e controllo e di qualsiasi altra apparecchiatura o software correlato per una particolare applicazione. È inoltre necessario tenere in considerazione le norme e/o disposizioni locali, regionali o nazionali applicabili.

È particolarmente importante attenersi a qualsiasi informazione di sicurezza, requisito elettrico e standard normativo applicabile all'impianto o alla macchina di processo durante l'utilizzo di questa apparecchiatura.

Uso Previsto

I prodotti descritti in questa guida, insieme a software, accessori e opzioni, fanno parte degli starter per carichi elettrici a bassa tensione, previsti per uso industriale secondo le istruzioni, indicazioni, esempi e informazioni di sicurezza contenuti nel presente documento e altra documentazione di supporto.

Il prodotto può essere utilizzato solo in conformità a tutte le normative e direttive di sicurezza applicabili, i requisiti specificati e i dati tecnici.

Prima di utilizzare il prodotto, eseguire una valutazione dei rischi dell'applicazione pianificata. In base ai risultati, adottare adeguate misure collegate alla sicurezza.

Poiché il prodotto è utilizzato come componente di un impianto di processo o di una macchina, è necessario garantire la sicurezza delle persone attraverso la progettazione complessiva del sistema.

Utilizzare il prodotto esclusivamente con i cavi e gli accessori indicati. Utilizzare solo accessori e ricambi originali.

Impieghi diversi da quelli esplicitamente consentiti sono vietati e possono provocare pericoli imprevisti.

Avviso per la sicurezza informatica

⚠AVVERTIMENTO

POSSIBILITÀ DI COMPROMETTERE LA DISPONIBILITÀ, L'INTEGRITÀ E LA CONFIDENZIALITÀ DEL SISTEMA

- Modificare le password predefinite al primo utilizzo per contrastare l'accesso non autorizzato alle regolazioni, ai comandi e ai dati del dispositivo.
- Disattivare le porte/i servizi non utilizzati per ridurre al minimo i percorsi degli attacchi dannosi.
- Inserire i dispositivi di rete all'interno di numerosi livelli di difesa (come firewall, segmentazione della rete e rilevamento e protezione dalle intrusioni nella rete).
- Seguire le procedure consigliate per la sicurezza informatica (ad esempio, minimo privilegio, separazione dei doveri) per evitare l'esposizione non autorizzata, perdita o malfunzionamento di dati e registri o interruzione dei servizi.

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

Introduzione alla Sicurezza Informatica

Contenuto della sezione

Introduzione

La Cybersecurity (sicurezza informatica) che fa parte dei processi, degli strumenti e delle tecnologie, della conformità e della governance, mira a proteggere la rete di comunicazione e tutti i dispositivi collegati da attacchi che potrebbero interrompere le operazioni (disponibilità), alterare le informazioni (integrità) o esporre dati riservati (riservatezza).

L'obiettivo della sicurezza informatica è quello di garantire un livello più elevato di protezione dei dati e delle risorse fisiche da furti, danneggiamento, abusi o incidenti, pur mantenendo l'accesso per gli utenti a cui sono destinate. La Sicurezza informatica comprende molti aspetti, tra cui la progettazione di sistemi sicuri, la limitazione dell'accesso tramite metodi fisici e digitali, l'identificazione degli utenti e l'implementazione di procedure di controllo/misurazione della sicurezza e politiche basate sulle migliori pratiche.

Linee guida Schneider Electric

Oltre alle raccomandazioni fornite in questa guida che sono specifiche per TeSys Tera system, è necessario seguire l'approccio di difesa approfondita Schneider Electric alla Sicurezza informatica.

Questo approccio è descritto nelle *Migliori pratiche raccomandate per la Sicurezza informatica*.

Inoltre, sono disponibili molte risorse utili e informazioni aggiornate sul portale di supporto alla Sicurezza informatica di Schneider Electric., pagina 44.

Approccio di Schneider Electric alla sicurezza informatica

Per lo sviluppo e l'implementazione dei sistemi di controllo, Schneider Electric si attiene alle migliori pratiche del settore, le quali includono un approccio Defense-in-Depth per la protezione di un sistema di controllo industriale. In base a questa filosofia, i controller si trovano dietro uno o più firewall, allo scopo di limitare l'accesso esclusivamente al personale e ai protocolli autorizzati.

⚠ AVVERTIMENTO

ACCESSO NON AUTENTICATO E CONSEGUENTE FUNZIONAMENTO NON AUTORIZZATO

- Valutare se le apparecchiature o l'ambiente completo sono collegati all'infrastruttura critica. In tal caso, 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 a una rete all'interno dell'azienda.
- Isolare la rete industriale da altre reti all'interno dell'azienda.
- Proteggere le reti dall'accesso accidentale mediante firewall, VPN o altra misura di sicurezza comprovata.
- Monitorare le attività nei sistemi.
- Evitare che terzi non autorizzati o azioni non autenticate accedano o si colleghino direttamente ai dispositivi soggetti agli attacchi.
- Preparare un piano di ripristino, che includa il backup del sistema le delle informazioni del processo.

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

Minacce alla sicurezza

Le minacce informatiche sono azioni deliberate o incidenti che possono interrompere il normale funzionamento di PC e reti di PC. 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

Politiche e Regole

Schneider Electric dispone di un processo Ciclo di vita di sviluppo sicuro (SDL), un framework chiave basato sullo sviluppo dei prodotti che contribuisce a garantire che i prodotti seguano processi di progettazione sicuri in tutte le fasi del ciclo di vita. Il processo SDL di Schneider Electric è conforme agli standard IEC 62443-4.1.

Il processo SDL comprende:

- pratiche SDL applicate alle azioni di sviluppo interno lungo tutta la catena di fornitura.
- Verifica della sicurezza finale necessaria per la versione del progetto.
- Formazione sulla sicurezza per il personale coinvolto nello sviluppo del prodotto.

Linee guida per il rafforzamento della sicurezza

Introduzione

PC può eseguire una serie di applicazioni per migliorare la sicurezza nell'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 .

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

Disablitazione di Remote Desktop Protocol

Nell'ambito dell'approccio di difesa in profondità di Schneider Electric, è consigliabile disattivare il protocollo desktop remoto (RDP) a meno che l'applicazione non richieda esplicitamente RDP.

In Windows 11, il protocollo desktop remoto (RDP) viene disattivato selezionando **Settings > System > Remote Desktop > Enable Remote Desktop** (commutare su **Disattivato**).

Aggiornamento dei criteri di sicurezza

Aggiornare i criteri di sicurezza sui PC del sistema tramite `gpupdate` in una finestra di comando. Per ulteriori informazioni, fare riferimento alla documentazione Microsoft su `gpupdate`.

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, selezionare **Start > All Programs > Windows Update**.

Protezione della workstation

Per ridurre i rischi della sicurezza associati alla workstation di engineering, abilitare le impostazioni di sfruttamento della memoria come Protezione esecuzione programmi (DEP) e Address Space Layout Randomization (ASLR). Queste impostazioni di sicurezza possono essere abilitate utilizzando le impostazioni di protezione dallo sfruttamento del sistema nel sistema operativo Windows 11. Per ulteriori informazioni, fare riferimento alla pagina Web Funzionalità di sicurezza Microsoft.

Applicare password sicure

Utilizzare password complesse che soddisfino i requisiti richiesti, come ad esempio lettere maiuscole, lettere minuscole, numeri e caratteri speciali.

Abilitando questa funzione è possibile impedire accessi non autorizzati riducendo il rischio di password deboli.

Utilizzo di porte non predefinite

La modifica delle porte di comunicazione predefinite per protocolli quali HTTPS, DWPS e Modbus TCP aggiunge un ulteriore livello di sicurezza.

Elenco degli indirizzi IP consentiti

La funzione di elenco degli indirizzi IP consentiti limita l'accesso al sistema consentendo solo indirizzi IP specifici. Questo consente di impedire che dispositivi non autorizzati si connettano al sistema e garantisce che solo fonti affidabili possano comunicare con TeSys Tera system. Per accedere alla funzione Elenco IP consentiti, passare a **Security > IP Allow List > IP Allow List** nel server Web standard.

Informazioni su TeSys Tera System

Contenuto della sezione

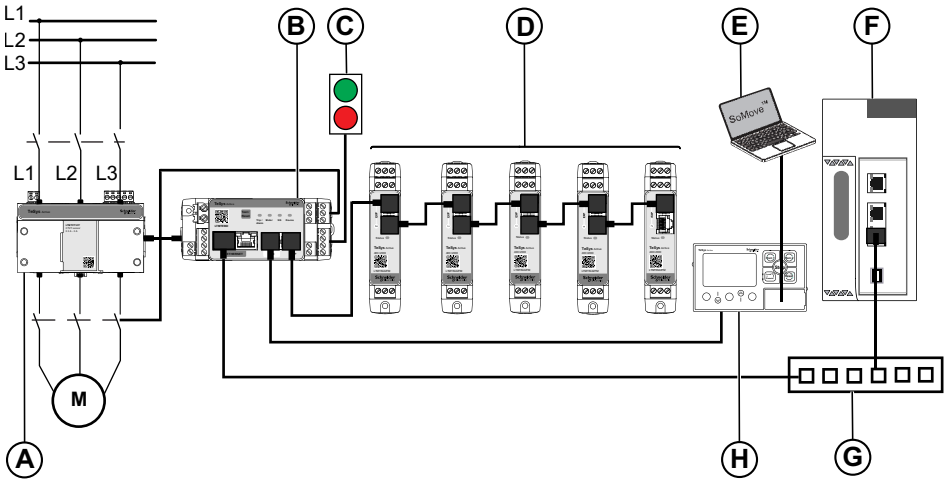
Panoramica

TeSys Tera Motor Management System (o TeSys Tera system) fa parte della TeSys gamma Active di relè intelligenti e avviatori motore. TeSys Tera system è progettato come un modulo affidabile per i centri di controllo motore intelligenti (iMCC) per fornire protezione completa, misurazione, controllo e monitoraggio per motori a induzione AC monofase o trifase.

TeSys Tera system è installato nel sistema di commutazione a bassa tensione e collega il sistema di automazione di livello superiore tramite la rete del bus di campo e l'alimentatore motore.

TeSys Tera system:

- Copre la protezione, la misurazione e il monitoraggio convenzionali e avanzati dei motori negli alimentatori iMCC in un unico modulo di comunicazione compatto e facile da configurare con un dispositivo HMI autonomo.
- Fornisce un controller di protezione per alimentatori di avviatori a bassa tensione controllati da contattori.
- Offre un sistema di gestione flessibile e modulare per motori a velocità costante in applicazioni a bassa tensione.



A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C Comandi di avvio/arresto

D LTMT expansion modules

E PC che esegue il software per container SoMove FDT con TeSys Tera DTM installato

F Controller logico programmabile (PLC) o sistema di controllo distribuito (DCS)

G interruttore Ethernet

H LTMTCUF control operator unit

Interfacce di comunicazione

TeSys Tera system comunica attraverso i seguenti tipi di interfaccia:

LTMT main unit	Reference	Porte
Modbus RTU 	• LTMTMFM (100–240 Vac/ Vdc) • LTMTMBD (24 Vdc)	• Porta di comunicazione Modbus RTU con connettore terminale • Porta HMI con comunicazione Modbus RTU per la configurazione
PROFIBUS DP 	• LTMTPFM (100–240 Vac/Vdc) • LTMTPBD (24 Vdc)	• PROFIBUS DP con connettore sub D9 • PortaProfibus con connettore terminale • Porta HMI con comunicazione Modbus RTU

LTMT main unit	Reference	Porte
Modbus TCP/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Due porte Ethernet con Modbus TCP/IP • Porta HMI con comunicazione Modbus RTU
EtherNet/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Due porte Ethernet con EtherNet/IP • Porta HMI con comunicazione Modbus RTU

Protocolli supportati

Dispositivi di comunicazione seriale

I moduli Modbus RTU e PROFIBUS DP di TeSys Tera system supportano Modbus RTU e PROFIBUS per la comunicazione con i dispositivi bus di campo.

Per i protocolli di comunicazione e i rispettivi riferimenti commerciali, consultare Interfacce di comunicazione, pagina 22.

Dispositivi di comunicazione Ethernet

I moduli Modbus TCP/IP e EtherNet/IP di TeSys Tera system supportano i seguenti protocolli:

- HTTPS tramite strumenti di configurazione e pagine web incorporate
- Modbus TCP/IP e EtherNet/IP per le comunicazioni con i dispositivi bus di campo
- DHCP per indirizzamento IP di rete
- DNS per risoluzione del nome di rete
- NTP per sincronizzazione dell'ora
- DPWS per il rilevamento dei dispositivi

Per i protocolli di comunicazione e i rispettivi riferimenti commerciali, consultare Interfacce di comunicazione, pagina 22.

Funzionalità di Sicurezza

TeSys Tera system supporta le seguenti funzionalità:

- Il firmware firmato digitalmente da Schneider Electric si può installare solo su TeSys Tera system.
- A ogni avvio, la firma digitale del firmware viene convalidata prima dell'esecuzione.
- Le password degli utenti sono archiviate in modo sicuro (applicabile ai moduli di interfaccia Ethernet).

  Per ulteriori informazioni sulla politica relativa alle password, consultare *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- È possibile eseguire il ripristino delle impostazioni di fabbrica di TeSys Tera system utilizzando l'impostazione **Factory Default** tramite il pulsante TeSys Tera DTM o **Test / Reset** su LTMT main unit.

  Per ulteriori informazioni sul pulsante **Test / Reset** , consultare *TeSys Tera Motor Management System User Guide – DOCA0257EN*.
- TeSys Tera system ha un orologio interno e ricorda la data e l'ora per 12 ore senza alimentazione (valido per Modbus RTU e PROFIBUS DP e non applicabile per il modulo Ethernet).
- Utilizzando TeSys Tera DTM, la funzionalità opzionale di gestione dei pin consente di abilitare o disabilitare la configurazione di TeSys Tera system. È inoltre possibile reimpostare il PIN per TeSys Tera DTM utilizzando la funzionalità di gestione del PIN.

  Per ulteriori informazioni sulla funzionalità di gestione dei pin, consultare *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- Per garantire TeSys Tera system, LTMTCUF control operator unit è dotato di funzionalità pin. È necessario disporre di un codice PIN a sei cifre per accedere a LTMTCUF control operator unit.

  Per ulteriori informazioni sulla funzionalità dei pin, consultare *TeSys Tera Motor Management System User Guide – DOCA0257EN*.

Per i protocolli di comunicazione e i rispettivi riferimenti commerciali, consultare Interfacce di comunicazione, pagina 22.

Funzionalità di TeSys Tera System

Contenuto della sezione

Aggiornamento del firmware

Aggiornare TeSys Tera system alla versione più recente del firmware per ottenere le funzionalità più recenti e mantenerlo aggiornato con le patch di sicurezza. Tutto il firmware progettato per TeSys Tera system è firmato utilizzando l'infrastruttura a chiave pubblica (PKI) di Schneider Electric per garantire l'integrità e l'autenticità del firmware in esecuzione su TeSys Tera system.

Per ulteriori informazioni sull'aggiornamento del firmware tramite TeSys Tera DTM, consultare *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.

Per ulteriori informazioni sull'aggiornamento del firmware tramite il server web standard (applicabile ai moduli di interfaccia Ethernet), fare riferimento a *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Per ulteriori informazioni sugli aggiornamenti di sicurezza, registrati sul portale di supporto alla sicurezza informatica di Schneider Electric *Security Notifications*.

Data e ora

Per evitare errori, è importante mantenere data e ora sincronizzate.

La procedura seguente mostra come aggiornare le impostazioni di data e ora per i moduli di interfaccia Ethernet utilizzando un server web standard o TeSys Tera DTM:

1. Passare a **Settings > General > Date & Time**.
2. Utilizzando dell'elenco a discesa **Date & Time Selection**, selezionare una delle opzioni seguenti:
   - **Manual**

     NOTA:

     - Quando la data e ora vengono impostate manualmente, LTMT main unit viene ripristinato alle impostazioni di fabbrica al riavvio.
     - Le impostazioni di data e ora si possono aggiornare manualmente utilizzando TeSys Tera DTM o LTMTCUF control operator unit.
   - **NTP**

     NOTA: Il protocollo**NTP** è disponibile solo per le versioni Ethernet di LTMT main unit.

Disattiva porte/interfacce inutilizzate

La disattivazione delle porte/interfacce inutilizzate contribuisce a ridurre la superficie di attacco del sistema, disattivando le porte di comunicazione e le interfacce che non vengono utilizzate attivamente.

Le seguenti impostazioni di TeSys Tera system si possono disabilitare utilizzando il server web standard:

- **Modbus TCP**
- **Device Dicovery**
- **Modbus RTU**

NOTA: Per ulteriori informazioni, consultare *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*

Porte

I moduli Modbus TCP/IP e EtherNet/IP di TeSys Tera system utilizzano le seguenti porte per la comunicazione predefinita:

Tipo di porte	EtherNet/IP	Modbus TCP/IP
TCP Port 443 (HTTPS)	✓	✓
TCP Port 502 (Modbus TCP/IP)	✓	✓
TCP Port 5357 (DPWS)	✓	✓
TCP Port 44814 (EtherNet/IP)	✓	X
UDP Port 2222 (EtherNet/IP)	✓	X
SNTP UDP Port 123 (EtherNet/IP)	✓	✓
DNS Port 53 (EtherNet/IP)	✓	✓
DHCP Port 68 (EtherNet/IP)	✓	✓

Syslog

TeSys Tera system genera registri di sistema per registrare eventi come ad esempio tentativi di accesso non validi e aggiornamenti del firmware. I registri non contengono informazioni personali.

Per rilevare comportamenti imprevisti (ad esempio, riavvii frequenti, aggiornamenti firmware errati o tentativi di accesso non validi), si consiglia di monitorare regolarmente i registri.

Per ulteriori informazioni sui registri, consultare *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* e *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Annullamento messa in servizio

TeSys Tera system contiene informazioni riservate configurate durante la messa in servizio, valori dei dati recenti e registri.

Ad esempio, queste informazioni possono includere la topologia Modbus LTMT main unit o i consumi energetici misurati.

È necessario eseguire un reset di fabbrica prima di smaltire TeSys Tera system.

È possibile utilizzare i seguenti metodi per reimpostare TeSys Tera system:

- Pulsante**Test / Reset** su LTMT main unit: Tenere premuto il pulsante **Test / Reset** su LTMT main unit per 10 secondi.
- TeSys Tera DTM Libraryper ulteriori informazioni, consultare la sezione *Ripristino impostazioni di fabbrica* nel *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unitPer ulteriori informazioni, consultare la sezione *Menu Comandi* nel *TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*

Sicurezza di Rete

Contenuto della sezione

NOTA: Questa parte è valida solo per i moduli Modbus TCP/IP e EtherNet/IP di TeSys Tera system.

Introduzione

TeSys Tera system non è progettato per resistere all'esposizione diretta alla rete Internet pubblica. Dovrebbe essere installato almeno dietro un Traduzione degli indirizzi di rete (NAT) o, preferibilmente, dietro più firewall. Per ulteriori informazioni, consultare le seguenti pagine web:

- *Schneider Electric cybersecurity consulting services*
- *National Institute of Standards and Technology (NIST)*
- *European Union Agency for Cybersecurity (ENISA)*

Segmentazione della rete

TeSys Tera system è un gateway che crea un ponte tra reti diverse. La segmentazione della rete contribuisce ad assicurare la difesa dagli attacchi informatici. Per migliorare la segmentazione della rete, TeSys Tera system EtherNet/IP versione LTMT main unit presenta due porte Ethernet. Le porte Ethernet disponibili si possono utilizzare per la tecnologia dell'informazione (IT) e la tecnologia operativa (OT).

HTTPS e Modbus sono disponibili su interfacce TeSys Tera system Ethernet (ETH1, ETH2).

Si consiglia di disabilitare il servizio Modbus TCP/IP sulle reti in cui non viene utilizzato.

Certificato server Web del prodotto

Per supportare comunicazioni HTTPS sicure, TeSys Tera system è dotato di un certificato X.509v3 predefinito. Questo certificato garantisce l'integrità e la riservatezza per impostare la comunicazione HTTPS.

I browser Web riconoscono solo i certificati firmati da autorità di certificazione (CA) di terze parti. Il certificato autofirmato non è protetto. Si consiglia di importare un certificato firmato da una CA di terze parti in TeSys Tera system e di mantenere sincronizzati data e ora.

I seguenti formati di certificato sono supportati da TeSys Tera system:

Formato	Intestazione/Piè di pagina	Tipo di chiave
PKCS#1	– – – – –INIZIO CHIAVE PRIVATA RSA– – – – –	Solo RSA
PKCS#8	– – – – –INIZIO CHIAVE PRIVATA– – – – –	RSA, EC, DSA e così via
PKCS#8 crittografato	– – – – –INIZIO CHIAVE PRIVATA CRITTOGRAFATA– – – – –	Qualsiasi

NOTA: I certificati di prova modificati non sono accettabili.

Per ulteriori dettagli sul certificato di terze parti, consultare *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Informazioni sulla sicurezza dei dispositivi connessi

Si consiglia di controllare regolarmente l'elenco dei dispositivi collegati alla rete Ethernet di TeSys Tera system. In caso di dispositivo collegato sconosciuto, individuarlo e rimuoverlo. È anche possibile ricostruire la rete e ricollegare solo i dispositivi identificati.

Sicurezza Fisica

Installazione

Per proteggere la sicurezza fisica dei sistemi, si consiglia la seguente installazione:

- Installare TeSys Tera system in un involucro fissato in modo adeguato al livello di rischio dell'installazione (ad esempio, un involucro con lucchetto o chiave).
- Se TeSys Tera system è montato su un quadro elettrico, installare il quadro elettrico in una stanza sicura (ad esempio, con una porta chiusa a chiave o una telecamera).

Raccomandazioni di sicurezza durante la manutenzione

Contenuto della sezione

Operazioni di manutenzione

Durante il ciclo di vita di TeSys Tera system, si raccomanda di eseguire regolarmente le operazioni seguenti:

- Assicurarsi che il dispositivo utilizzi l'ultima versione del firmware.
- Verificare che tutte le patch di rete e di sicurezza siano aggiornate.
- Seguire le migliori pratiche di Sicurezza informatica come raccomandato.
- Per comportamenti imprevisti quali tentativi di accesso non validi o riavvii frequenti, fare riferimento a Syslog, pagina 31.
- Per evitare di allontanarsi dalla data corrente, fare riferimento a Data e ora, pagina 28.
- Attenersi agli standard di sicurezza raccomandati da Schneider Electric per il dispositivo.

Verifica della funzionalità di sicurezza

Contenuto del capitolo

Autenticazione Web

NOTA: Questo argomento è valido solo per i moduli Modbus TCP/IP e EtherNet/IP di TeSys Tera system.

Per verificare la funzionalità di autenticazione web, procedere come segue:

1. provare ad accedere al server web standard di TeSys Tera system senza password o inserire una password errata.

   Risultato: TeSys Tera system non consente l'accesso al server web standard.

2. Inserire credenziali errate per tre istanze.

   Risultato: TeSys Tera system si blocca per 15 minuti prima di consentire di provare per la quarta volta.

Autorizzazione Web

NOTA: Questo argomento è valido solo per i moduli Modbus TCP/IP e EtherNet/IP di TeSys Tera system.

Per verificare la funzionalità di autorizzazione web, procedere come segue:

1. Accedere al server Web standard TeSys Tera system.

   Risultato: dopo aver eseguito l'accesso, si dispone del pieno accesso ai dati e alle funzionalità.

2. Aggiungere una pagina web ai preferiti (ad esempio, **Settings**).
3. Aprire una finestra di navigazione privata nel browser e aprire la pagina web aggiunta ai segnalibri.

   Risultato: non è possibile accedere alla pagina web, ma si viene reindirizzati alla pagina di accesso.

Syslog

Per verificare la funzionalità Syslog, procedere come segue:

1. Dopo alcuni o tutti i test precedenti, utilizzando TeSys Tera DTM o il server web standard, accedere ai **Logs**.
2. Scaricare i file di registro.
3. Verificare che il test eseguito o i tentativi non riusciti siano presenti nei registri.

Aggiornamento del firmware

Per verificare la funzionalità dell'aggiornamento del firmware, procedere come segue:

1. Passare alla funzionalità **Firmware Update** su TeSys Tera DTM o sul server web standard.
2. Caricare un file di aggiornamento firmware autenticato.
3. Attendere la convalida del firmware.

   Risultato: il riavvio del sistema avviene solo quando il firmware di LTMT main unit viene aggiornato e i dettagli del nuovo firmware vengono aggiornati in TeSys Tera DTM.

Disabilitazione dei servizi

NOTA: Questo argomento è valido solo per i moduli Modbus TCP/IP e EtherNet/IP di TeSys Tera system.

Per verificare la funzionalità dei servizi di disabilitazione, procedere come segue:

1. passare a **Security > IP Network List > Device Discovery** utilizzando il server web standard.
2. Disattivare il rilevamento dei dispositivi.
3. Collegare un PC con il sistema operativo Windows alla stessa rete.
4. Fare clic su **Network** da **File Explorer**.

   Risultato: TeSys Tera system non viene rilevato, pertanto non compare nell'elenco dei dispositivi presenti nella rete.

Passare a **Security > IP Network List** e seguire la procedura sopra indicata per verificare i seguenti metodi di disabilitazione:

- Modbus TCP
- Modbus RTU

Portale per il supporto alla sicurezza informatica Schneider Electric

Contenuto della sezione

Panoramica

Schneider Electric *Cybersecurity support portal* delinea la politica di gestione delle vulnerabilità Schneider Electric.

L'obiettivo della politica di gestione delle vulnerabilità Schneider Electric è quello di affrontare le vulnerabilità nella Sicurezza informatica che influiscono sui prodotti e sistemi Schneider Electric per proteggere le soluzioni installate, i clienti e l'ambiente.

Schneider Electric collabora con ricercatori, Squadre di risposta alle emergenze informatiche(CERT) e proprietari di risorse per garantire che vengano fornite informazioni precise in modo tempestivo per proteggere adeguatamente le loro installazioni.

Il Corporate Product CERT (CPCERT) diSchneider Electricè responsabile della gestione e dell'emissione di avvisi relativi a vulnerabilità e misure di mitigazione che interessano prodotti e soluzioni.

Il CPCERT coordina le comunicazioni tra i CERT pertinenti, i ricercatori indipendenti, i product manager e tutti i clienti interessati.

Portale di supporto alla Sicurezza informatica

Schneider Electric Cybersecurity support portal fornisce le seguenti informazioni:

- Informazioni sulle vulnerabilità dei prodotti in materia di Sicurezza informatica
- Informazioni sugli incidenti di Sicurezza informatica
- Informazioni su un'interfaccia che consente di segnalare incidenti o vulnerabilità relativi alla Sicurezza informatica

Gestione e segnalazione delle vulnerabilità

Gli incidenti di sicurezza informatica e le potenziali vulnerabilità possono essere segnalati tramite il sito Web di Schneider Electric: Segnala una vulnerabilità.

Schneider Electric Industries SAS
35 rue Joseph Monier
92500 Rueil Malmaison
France

www.se.com

DOCA0260IT-00