TeSys Active

TeSys Tera Motor Management System

Handbuch zur Cybersicherheit

TeSys bietet innovative und vernetzte Lösungen für Motorabgänge

DOCA0260DE-00
11/2025

Rechtliche Hinweise

Die in diesem Dokument enthaltenen Informationen umfassen allgemeine Beschreibungen, technische Merkmale und Kenndaten und/oder Empfehlungen in Bezug auf Produkte/Lösungen.

Dieses Dokument ersetzt keinesfalls eine detaillierte Analyse bzw. einen betriebs- und standortspezifischen Entwicklungs- oder Schemaplan. Es darf nicht zur Ermittlung der Eignung oder Zuverlässigkeit von Produkten/Lösungen für spezifische Benutzeranwendungen verwendet werden. Es liegt im Verantwortungsbereich eines jeden Benutzers, selbst eine angemessene und umfassende Risikoanalyse, Risikobewertung und Testreihe für die Produkte/Lösungen in Übereinstimmung mit der jeweils spezifischen Anwendung bzw. Nutzung durchzuführen bzw. von entsprechendem Fachpersonal (Integrator, Spezifikateur oder ähnliche Fachkraft) durchführen zu lassen.

Die Marke Schneider Electric sowie alle anderen in diesem Dokument enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Dokuments oder dessen Inhalts, mit Ausnahme einer nicht-exklusiven und persönlichen Lizenz, es „wie besehen“ zu konsultieren.

Schneider Electric behält sich das Recht vor, jederzeit ohne entsprechende schriftliche Vorankündigung Änderungen oder Aktualisierungen mit Bezug auf den Inhalt bzw. am Inhalt dieses Dokuments oder dessen Format vorzunehmen.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der sachgemäßen oder missbräuchlichen Verwendung der hierin enthaltenen Informationen entstehen.

Inhaltsverzeichnis

Sicherheitshinweise

Wichtige Informationen

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.

Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge hat.**

⚠ WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann.**

⚠ VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann.**

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

Bitte beachten

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Informationen zum Dokument

Ziel dieses Dokuments

Dieser Leitfaden bietet Informationen über Cybersicherheitsfragen des TeSys™ Tera Systems, damit Systemdesigner und Anwender eine sichere Nutzung des Produkts fördern können.

In diesem Leitfaden wird beschrieben, wie Sie die Sicherheit Ihres Operational-Technology-Netzwerks oder Ihres Firmennetzwerks gewährleistenEthernet Netzwerk.

HINWEIS: In diesem Handbuch bezieht sich der Begriff **Sicherheit** auf Cybersicherheit.

Gültigkeitsbereich

Dieses Dokument gilt für die folgenden zertifizierten Komponenten des TeSys Tera system:

- LTMTEFM: LTMT main unit mit EtherNet/IP oder Modbus TCP/IP Protokoll, 100–240 Vac/Vdc
- LTMTEBD: LTMT main unit mit EtherNet/IP oder Modbus TCP/IP Protokoll, 24 Vdc
- LTMTMFM: LTMT main unit mit dem Modbus RTU-Protokoll, 100–240 Vac/Vdc
- LTMTMBD: LTMT main unit mit dem Modbus RTU-Protokoll, 24 Vdc
- LTMTPFM: LTMT main unit mit dem PROFIBUS DP-Protokoll, 100–240 Vac/Vdc
- LTMTPBD: LTMT main unit mit PROFIBUS DP-Protokoll, 24 Vdc

Allgemeine Informationen zur Cybersicherheit

In den letzten Jahren hat sich durch die wachsende Anzahl an vernetzten Maschinen und Produktionsanlagen das Potenzial für Cyberbedrohungen wie unbefugter Zugriff, Datenverletzungen und Betriebsunterbrechungen entsprechend erhöht. Sie müssen daher alle möglichen Maßnahmen zur Cybersicherheit in Betracht ziehen, um Anlagen und Systeme vor solchen Bedrohungen zu schützen.

Um die Sicherheit und den Schutz Ihrer Schneider Electric-Produkte zu gewährleisten, ist es in Ihrem Interesse, die Best Practices für die Cybersicherheit umzusetzen, die im Dokument Cybersecurity Best Practices beschrieben sind.

Schneider Electric bietet zusätzliche Informationen und Unterstützung:

- Abonnieren Sie den Sicherheits-Newsletter von Schneider Electric.
- Besuchen Sie die Webseite Cybersecurity Support Portal, um:
  - Sicherheitshinweise zu suchen
  - Schwachstellen und Vorfälle zu melden
- Besuchen Sie die Webseite Schneider Electric Cybersecurity and Data Protection Posture, um:
  - auf den Cybersicherheitsstatus zuzugreifen
  - mehr über Cybersicherheit in der Cybersecurity Academy zu erfahren
  - die Cybersicherheits-Services von Schneider Electric zu entdecken

Umgebungsdaten

Informationen zu Produktkonformität und Umgebungsbedingungen finden Sie im Schneider Electric Environmental Data Program.

Verfügbare Sprachen des Dokuments

Dieses Dokument ist in folgenden Sprachen verfügbar:

- English
- Chinesisch
- Französisch
- Deutsch
- Italienisch
- Koreanisch
- Spanisch

Weiterführende Dokumentation

Titel der Dokumentation	Beschreibung	Referenznummer
TeSys Tera Motor Management System - Katalog	Der Katalog: • Beschreibt das TeSys Tera system. • Enthält die technischen Kenndaten für das TeSys Tera.	LVCATENTER
TeSys Tera Motor Management System - Benutzerhandbuch	Das Hauptbenutzerhandbuch, in dem das vollständige TeSys Tera systemvorgestellt wird. Es beschreibt die Hauptfunktionen der LTMT main units, LTMTCT/ LTMTCTV Sensor Modules, LTMT expansion modulesund LTMTCUF control operator unit.	DOCA0257DE
TeSys Tera Motor Management System - Installationshandbuch	In diesem Handbuch werden die Installation, Inbetriebnahme und Wartung der LTMT main unit, LTMTCT/LTMTCTV Sensor Modules, LTMT expansion modulesund LTMTCUF control operator unitbeschrieben.	DOCA0356DE
TeSys Tera Motor Management System DTM library - Online-Hilfe	Dieses Handbuch beschreibt die TeSys Tera DTM-Bibliothek, die eine Anpassung der Steuerungsfunktionen des TeSys Tera Motor Management System-Systems ermöglicht.	DOCA0275DE
TeSys Tera Motor Management System Modbus RTU - Kommunikationshandbuch	Dieses Handbuch beschreibt das Modbus-Netzwerkprotokoll für die LTMT main unit-Einheit.	DOCA0355DE
TeSys Tera Motor Management System PROFIBUS DP - Kommunikationshandbuch	Dieses Handbuch beschreibt das PROFIBUS DP-Netzwerkprotokoll für die LTMT main unit.	DOCA0256DE
TeSys Tera Motor Management System EtherNet/IP - Kommunikationshandbuch	Dieses Handbuch beschreibt das EtherNet/IP-Netzwerkprotokoll für die LTMT main unit.	DOCA0258DE
TeSys Tera Motor Management System LTMTCUF control operator unit - Benutzerhandbuch	In diesem Handbuch werden die Installation, Konfiguration und Verwendung der LTMTCUF control operator unitbeschrieben.	DOCA0233DE
TeSys Tera Motor Management System DTM library Software-Versionshinweis	Dieses Dokument enthält wichtige Informationen zur Software der TeSys Tera DTM Library und bietet einen Überblick über neue Funktionen und Verbesserungen.	DOCA0279DE
TeSys Tera Motor Management System - Versionshinweise zur Firmware	Dieses Dokument enthält Informationen zu Firmwarepaketversionen des TeSys Tera systems und bietet einen Überblick über neue Funktionen und Verbesserungen.	DOCA0276DE
Wie kann ich Cyberangriffen vorbeugen?	Dieser Leitfaden beschreibt die Cybersicherheitsrisiken und Minderungsstrategien in Steuerungs- und Automatisierungssystemen	Wie kann ich Cyberangriffen vorbeugen?

Um Dokumente online zu finden, besuchen Sie das Schneider Electric Download-Center (www.se.com/ww/en/download/).

Informationen zu nicht-inklusiver oder unsensibler Terminologie

Als verantwortungsbewusstes, integratives Unternehmen aktualisiert Schneider Electric kontinuierlich seine Kommunikationen und Produkte, die nicht-integrative oder unsensible Terminologie enthalten. Trotz dieser Bemühungen können unsere Inhalte jedoch nach wie vor Begriffe enthalten, die von einigen Kunden als unangemessen betrachtet werden.

Marken

QR Code ist eine eingetragene Marke von DENSO WAVE INCORPORATED in Japan und anderen Ländern.

Sicherheitsvorkehrungen

Machen Sie sich mit den folgenden Vorsichtsmaßnahmen vertraut, bevor Sie in diesem Handbuch beschriebene Arbeiten durchführen.

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS, EINER EXPLOSION ODER EINES LICHTBOGENÜBERSCHLAGS

- Dieses Gerät darf ausschließlich von qualifizierten Elektrofachkräften installiert und gewartet werden.
- Schalten Sie vor Arbeiten am bzw. im Gerät die gesamte Spannungsversorgung ab.
- Verwenden Sie für den Betrieb dieses Geräts und jeglicher verbundener Produkte ausschließlich die vorgeschriebenen Spannungswerte.
- Verwenden Sie stets ein genormtes Spannungsprüfgerät, um festzustellen, ob die Spannungsversorgung wirklich abgeschaltet ist.
- Verwenden Sie angemessene Verriegelungen, wenn Personen- bzw. Gerätegefahren vorhanden sind.
- Netzstromkreise müssen gemäß den lokalen und nationalen Vorschriften verdrahtet und geschützt werden.
- Tragen Sie eine geeignete persönliche Schutzausrüstung (PPE) und befolgen Sie sichere Arbeitsweisen für die Ausführung von Elektroarbeiten gemäß NFPA 70E, NOM-029-STPS oder CSA Z462 bzw. gemäß den entsprechenden lokalen Bestimmungen.

Die Nichtbeachtung dieser Anweisungen hat Tod oder schwere Verletzungen zur Folge.

⚠ WARNUNG

NICHT VORGESEHENER GERÄTEBETRIEB

- Sie dürfen dieses Gerät nicht auseinanderbauen, reparieren oder verändern. Es gibt keine vom Benutzer zu wartenden Teile.
- Installieren und betreiben Sie dieses Gerät in einem Gehäuse, das eine angemessene Schutzklasse für die vorgesehene Anwendungsumgebung hat.
- Jede Implementierung dieses Geräts muss vor seiner Inbetriebnahme separat und gründlich auf ordnungsgemäßen Betrieb getestet werden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Qualifiziertes Personal

Über eine Schnittstelle, mit der Sie Cybersicherheitsvorfälle oder Schwachstellen melden können. Nur entsprechend geschulte Personen, die mit dem Inhalt dieses Handbuchs sowie allen zugehörigen Produktdokumentationen vertraut sind und diese verstehen, sind berechtigt, mit diesem Produkt zu arbeiten.

Die qualifizierte Person muss in der Lage sein, mögliche Gefahren zu erkennen, die durch Änderungen von Parameterwerten entstehen sowie allgemein Gefahren, die von mechanischen, elektrischen oder elektronischen Geräten ausgehen können. Die qualifizierte Person muss mit den Normen, Vorschriften und Verordnungen zur Verhütung von Industrieunfällen vertraut sein und diese bei der Gestaltung und Implementierung des Systems einhalten.

Die Nutzung und Anwendung der in dieser Anleitung enthaltenen Informationen erfordert Fachkenntnisse in Bezug auf die Gestaltung und Programmierung von automatisierten Steuersystemen. Nur Sie – der Nutzer, der Bauer des

Schaltschranks oder der Systemintegrator – können alle Bedingungen und Faktoren kennen, die bei Installation, Einrichtung, Betrieb und Wartung einer Betriebsanlage oder Maschine zutreffen, und Sie sind deshalb in der Lage, bei der Auswahl von Automatisierungs- und Steuergeräten sowie von zugehörigen Geräten oder entsprechender Software für eine bestimmte Anwendung die Automatisierungs- und zugehörigen Geräte sowie die entsprechenden Sicherheitseinrichtungen und Verriegelungen zu bestimmen, die effizient und ordnungsgemäß verwendet werden können. Sie müssen außerdem alle anwendbaren lokalen, regionalen oder nationalen Normen bzw. Bestimmungen berücksichtigen.

Achten Sie besonders auf die Einhaltung der jeweiligen Sicherheitshinweise, elektrischen Anforderungen und normativen Vorgaben, die für die Verwendung Ihrer Betriebsanlage oder Maschine gelten, wenn Sie diese Ausrüstung verwenden.

Verwendungszweck

Die in dieser Anleitung beschriebenen Produkte, einschließlich Software, Zubehör und Optionen, sind ein Teil der Starter für Niederspannungslasten, die für industrielle Zwecke gemäß den Anweisungen, Aufforderungen, Beispielen und Sicherheitshinweisen in diesem Dokument und sonstigen Begleitunterlagen vorgesehen sind.

Das Produkt darf nur in Übereinstimmung mit sämtlichen geltenden Sicherheitsvorschriften und -regelungen, den genannten Anforderungen und den technischen Daten verwendet werden.

Vor der Verwendung des Produkts müssen Sie eine Risikobeurteilung der geplanten Anwendung durchführen. Entsprechend den Ergebnissen sind angemessene Sicherheitsmaßnahmen zu implementieren.

Da das Produkt als Bestandteil einer Prozessanlage oder Maschine verwendet wird, müssen Sie die Sicherheit von Personen durch das Gesamtsystemdesign sicherstellen.

Das Produkt darf nur mit den spezifizierten Kabeln und Zubehörteilen betrieben werden. Verwenden Sie ausschließlich Originalzubehör und -ersatzteile.

Jede Verwendung außer der ausdrücklich zugelassenen Verwendung ist untersagt und kann unvorhergesehene Gefahren und Risiken zur Folge haben.

Cybersicherheit - Sicherheitshinweise

⚠WARNUNG

MÖGLICHE BEEINTRÄCHTIGUNG DER VERFÜGBARKEIT, INTEGRITÄT UND VERTRAULICHKEIT DES SYSTEMS

- Ändern Sie das Standardpasswort bei der ersten Verwendung, um jeden unberechtigten Zugriff auf die Geräteeinstellungen, Steuerelemente und Informationen zu unterbinden.
- Deaktivieren Sie nicht verwendete Ports/Dienste, um potenzielle Zugänge für bösartige Angreifer zu blockieren.
- Richten Sie mehrere Cyber-Schutzschichten vor allen Netzwerkgeräten ein (z. B. Firewalls, Netzwerksegmentierung, Netzwerkangriffserkennung (Intrusion Detection) und -schutz).
- Wenden Sie die Best Practices zur Cybersicherheit an (z. B. Prinzip der geringsten Rechte, Funktionstrennung), um die unberechtigte Offenlegung von Daten, Datenverlust oder die Änderung von Daten und Protokollen bzw. die Unterbrechung der Dienstbereitstellung zu verhindern.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Einführung in die Cybersicherheit

Inhalt dieses Abschnitts

Einführung

Cybersicherheit als Bestandteil von Prozessen, Werkzeugen und Technologien, Compliance und Governance zielt darauf ab, Ihr Kommunikationsnetzwerk und alle angeschlossenen Geräte vor Angriffen zu schützen, die den Betrieb stören (Verfügbarkeit), Informationen verändern (Integrität) oder vertrauliche Daten offenlegen könnten (Vertraulichkeit).

Ziel der Cybersicherheit ist es, einen höheren Schutzgrad für Daten und physische Ressourcen bereitzustellen, um diese vor Diebstahl, Beschädigung, Missbrauch oder Unfällen zu schützen, und dabei gleichzeitig den Zugriff für die vorgesehenen Benutzer aufrechtzuerhalten. Cybersicherheit umfasst viele Aspekte, darunter das Entwerfen sicherer Systeme, die Beschränkung des Zugriffs durch physische und digitale Methoden, die Identifizierung von Benutzern sowie die Implementierung von Sicherheitskontrollen, Messverfahren und Best-Practice-Richtlinien.

Richtlinien von Schneider Electric

Zusätzlich zu den Empfehlungen in diesem Leitfaden, die speziell für TeSys Tera system, sollten Sie den Schneider Electric Ansatz der tief gestaffelten Verteidigung für Cybersicherheit befolgen.

Dieser Ansatz wird in den *Empfohlenen Best Practices für Cybersicherheit*.

Darüber hinaus finden Sie viele nützliche Ressourcen und aktuelle Informationen auf dem Cybersicherheit-Support-Portal von Schneider Electric, Seite 44.

Der Cybersicherheits-Ansatz von Schneider Electric

Schneider Electric befolgt bei der Entwicklung und Implementierung von Steuerungssystemen bewährte Branchenverfahren. Dazu zählt auch ein Defense-in-Depth-Ansatz zur Sicherung industrieller Steuerungssysteme. Bei diesem Ansatz befinden sich die Steuerungen hinter mindestens einer Firewall, um den Zugriff ausschließlich auf befugte Personen und Protokolle zu beschränken.

⚠WARNUNG

NICHT AUTHENTIFIZIERTER ZUGRIFF UND ANSCHLIESSENDER UNBEFUGTER BETRIEB

- Prüfen Sie, ob Ihre Anlage oder die gesamte Umgebung mit Ihrer kritischen Infrastruktur verbunden ist. In diesem Fall müssen Sie angemessene Präventionsmaßnahmen ergreifen, die auf einer Defense-in-Depth-Strategie basieren, bevor Sie das Automatisierungssystem mit einem Netzwerk verbinden.
- Begrenzen Sie die Anzahl der Geräte, die an einem Netzwerk innerhalb Ihres Unternehmens angeschlossen sind.
- Isolieren Sie Ihr Industrienetzwerk von anderen Netzwerken außerhalb Ihres Unternehmens.
- Schützen Sie jedes Netzwerk vor unbeabsichtigtem Zugriff, indem Sie Firewalls, VPN oder andere bewährte Sicherheitsmaßnahmen implementieren.
- Überwachen Sie die Aktivität in Ihren Systemen.
- Verhindern Sie jeden direkten Zugriff bzw. jede direkte Verbindung mit den betroffenen Geräten durch Unbefugte oder über nicht authentifizierte Aktionen.
- Erarbeiten Sie einen Wiederherstellungsplan, einschließlich des Backups Ihrer System- und Prozessdaten.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Sicherheitsbedrohungen

Cyberbedrohungen sind vorsätzliche Handlungen oder Unfälle, die den normalen Betrieb von PCs und PC-Netzwerken stören können. Diese Handlungen können von der Einrichtung selbst oder von einem externen Standort ausgehen. In Steuerungsumgebungen bestehen u. a. folgende Herausforderungen im Hinblick auf die Sicherheit:

- Diverse physische und logische Grenzen
- Mehrere Standorte und große geografische Entfernungen
- Negative Auswirkungen der Sicherheitsimplementierung auf die Prozessverfügbarkeit
- Erhöhtes Risiko, dass Würmer und Viren von Geschäftssystemen auf Steuerungssysteme übertragen werden, da die Kommunikation zwischen diesen Systemen offener geworden ist
- Erhöhtes Risiko einer Übertragung von Malware über USB-Geräte, Laptops von Anbietern und Wartungstechnikern und das Unternehmensnetzwerk
- Direkte Auswirkungen der Steuerungssysteme auf physische und mechanische Systeme

Richtlinien und Regeln

Schneider Electric nutzt den Sicherer Entwicklungslebenszyklus (SDL), ein wichtiges Rahmenwerk für die Produktentwicklung, das gewährleistet, dass Produkte in allen Phasen ihres Lebenszyklus nach sicheren Designprinzipien entwickelt werden. Der SDL-Prozess von Schneider Electric entspricht den IEC 62443-4.1 Normen.

Der SDL-Prozess umfasst:

- SDL-Praktiken werden auf interne Entwicklungsmaßnahmen entlang der gesamten Lieferkette angewendet.
- Abschließende Sicherheitsüberprüfung für die Freigabe erforderlich.
- Sicherheitsschulung für Personal, das in der Produktentwicklung tätig ist.

Richtlinien zur Sicherheitsverstärkung

Einführung

Auf Ihrem PC können verschiedene Anwendungen ausgeführt werden, um die Sicherheit in Ihrer Steuerungsumgebung zu erhöhen. Das System verfügt über werkseitige Standardeinstellungen, die umkonfiguriert werden müssen, um den Empfehlungen von Schneider Electric für die Verstärkung der Sicherheit des Geräts im Rahmen eines Defense-in-Depth-Ansatzes zu entsprechen.

Die folgenden Richtlinien beschreiben die Vorgehensweisen für ein Windows - Betriebssystem. Sie dienen lediglich als Beispiele. Für Ihr Betriebssystem und Ihre Anwendungen können unterschiedliche Voraussetzungen oder Verfahren gelten.

Remote Desktop-Protokoll deaktivieren

Zu den Empfehlungen von Schneider Electric Defense-in-Depth gehört die Deaktivierung des Remote Desktop Protocol (RDP), es sei denn, Ihre Anwendung benötigt das RDP.

Unter Windows 11 wird das Remote Desktop Protocol (RDP) über **Settings > System > Remote Desktop > Remote Desktop aktivieren** (Umschalten auf **Aus**) deaktiviert.

Aktualisieren der Sicherheitsrichtlinien

Aktualisieren Sie die Sicherheitsrichtlinien auf dem PC, indem Sie `gpupdate` in einem Befehlsfenster ausführen. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu `gpupdate`.

Verwalten von Updates

Aktualisieren Sie vor der Bereitstellung alle PC-Betriebssysteme mithilfe der Dienstprogramme auf der **Windows Update**-Webseite von Microsoft. Für den Zugriff auf dieses Tool in Windows wählen Sie **Start > All Programs > Windows Update** aus.

Arbeitsplatz-Absicherung

Um die mit dem Engineering-Arbeitsplatz verbundenen Sicherheitsrisiken zu verringern, aktivieren Sie die Speicher-Exploit-Einstellungen, wie z. B. die Datenausführungsverhinderung (DEP) und die Speicherverwürfelung (ASLR). Diese Sicherheitseinstellungen können mithilfe der Exploit-Schutzeinstellungen des Systems unter Windows 11 aktiviert werden. Weitere Informationen hierzu finden Sie auf der Webseite Microsoft-Sicherheitsfunktionen.

Sichere Passwörter durchsetzen

Verwenden Sie sichere Passwörter, die die erforderlichen Elemente wie Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Durch

Aktivieren dieser Funktion wird unbefugter Zugriff verhindert, indem das Risiko schwacher Passwörter verringert wird.

Verwendung von nicht standardmäßigen Ports

Das Ändern der Standardkommunikationsports für Protokolle wie HTTPS, DWPS und Modbus TCP fügt eine zusätzliche Sicherheitsebene hinzu.

IP-Zulassungsliste

Die IP-Zulassungsliste beschränkt den Zugriff auf das System, indem nur bestimmte IP-Adressen zugelassen werden. Dies verhindert, dass unbefugte Geräte eine Verbindung zum System herstellen, und stellt sicher, dass nur vertrauenswürdige Quellen mit dem System kommunizieren können TeSys Tera system. Um auf die Funktion IP-Zulassungsliste zuzugreifen, navigieren Sie zu **Security > IP Allow List > IP Allow List** im Standard-Webserver.

TeSys Tera Systeminformationen

Inhalt dieses Abschnitts

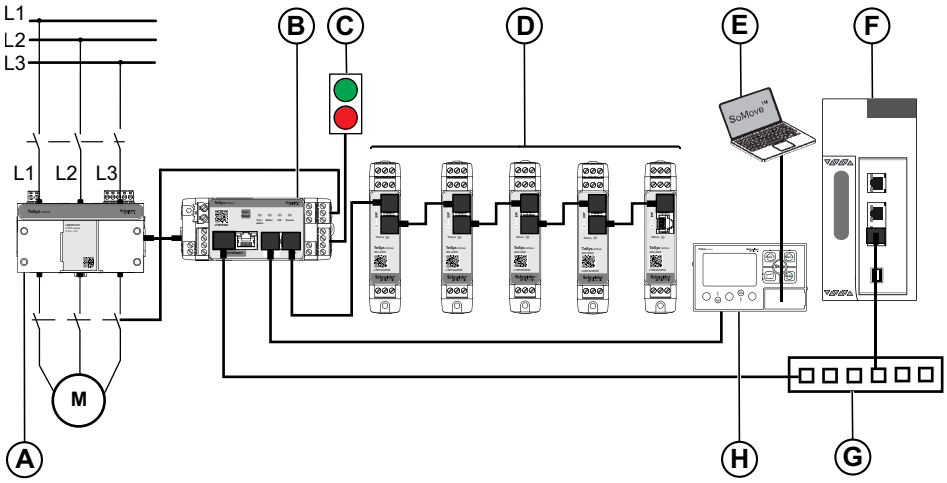
Überblick

Die TeSys Tera Motor Management System (oder TeSys Tera system) ist Teil der TeSys Aktiven Reihe intelligenter Relais und Motorstarter. Das TeSys Tera system Ist als zuverlässiger Bestandteil von Intelligent Motor Control Centres (iMCCs) konzipiert und bietet vollständigen Schutz, Messung, Steuerung und Überwachung für einphasige oder dreiphasige AC-Asynchronmotoren.

Das TeSys Tera system wird in der Niederspannungsschaltanlage installiert und verbindet das übergeordnete Automatisierungssystem über das Feldbus-Netzwerk und den Motorabgang.

TeSys Tera system:

- Deckt herkömmlichen und erweiterten Motorschutz, Messung und Überwachung in iMCC-Einspeisungen in einem einzigen, einfach zu konfigurierenden, kompakten Kommunikationsmodul mit eigenständigem HMI-Gerät ab.
- Bietet Schutz-Steuerung für Niederspannungs-Motorabgänge mit Schützsteuerung.
- Stellt ein flexibles und modulares Motormanagementsystem für Motoren mit konstanten Drehzahlen in Niederspannungsanwendungen bereit.



A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C Start-/Stopp-Befehle

D LTMT expansion modules

E PC mit SoMove FDT-Container-Software und installiertem TeSys Tera DTM

F Programmierbare Logiksteuerung (SPS) oder verteiltes Steuerungssystem (DCS)

G Ethernet-Switch

H LTMTCUF control operator unit

Kommunikations-Schnittstellen

TeSys Tera system kommuniziert über die folgenden Schnittstellentypen:

LTMT main unit	Referenz	Ports
Modbus RTU 	• LTMTMFM (100–240 Vac/ Vdc) • LTMTMBD (24 Vdc)	• Modbus RTU Kommunikationsanschluss mit Klemme • HMI-Port mit Modbus RTU Kommunikation für die Konfiguration
PROFIBUS DP 	• LTMTPFM (100–240 Vac/Vdc) • LTMTPBD (24 Vdc)	• PROFIBUS DP mit Sub-D9-Stecker • Profibus Anschluss mit Klemme • HMI-Anschluss mit Modbus RTU Kommunikation

LTMT main unit	Referenz	Ports
Modbus TCP/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Zwei Ethernet Anschlüsse mit Modbus TCP/IP • HMI-Anschluss mit Modbus RTU Kommunikation
EtherNet/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Zwei Ethernet Anschlüsse mit EtherNet/IP • HMI-Anschluss mit Modbus RTU Kommunikation

Unterstützte Protokolle

Serielle Kommunikationsgeräte

Die Modbus RTU und PROFIBUS DP Module des TeSys Tera system Unterstützung Modbus RTU und PROFIBUS Protokoll für die Kommunikation mit Feldbusgeräten.

Bezüglich der Kommunikationsprotokolle und der entsprechenden Handelsreferenzen siehe Kommunikationsschnittstellen, Seite 22.

Ethernet-Kommunikationsgeräte

Die Modbus TCP/IP und EtherNet/IP Module des TeSys Tera system unterstützen die folgenden Protokolle:

- HTTPS über Konfigurationstools und eingebettete Webseiten
- Modbus TCP/IP und EtherNet/IP für die Kommunikation mit Feldbusgeräten
- DHCP für die netzwerkbasierte IP-Adressierung
- DNS für die Netzwerknamensauflösung
- NTP für die Zeitsynchronisierung
- DPWS für die Geräteerkennung

Bezüglich der Kommunikationsprotokolle und der jeweiligen Handelsreferenzen siehe Kommunikationsschnittstellen, Seite 22.

Sicherheitsfunktionen

Das TeSys Tera system unterstützt die folgenden Funktionen:

- Firmware, die digital signiert ist von Schneider Electric kann nur auf TeSys Tera system.
- Bei jedem Start wird die digitale Signatur der Firmware vor der Ausführung überprüft.
- Benutzerkennwörter werden sicher gespeichert (gilt für Ethernet Schnittstellenmodule).

  Weitere Informationen zur Passwortrichtlinie finden Sie unter *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- Sie können das Gerät auf die Werkseinstellungen zurücksetzen, indem Sie TeSys Tera system über **Factory Default** über die TeSys Tera DTM oder die **Test-/Reset** Taste auf LTMT main unit.

  Weitere Informationen zum **Test-/Reset-Taste** finden Sie unter *TeSys Tera Motor Management System User Guide – DOCA0257EN*.
- Das TeSys Tera system verfügt über eine interne Uhr und speichert Datum und Uhrzeit für 12 Stunden ohne Stromversorgung (gültig für Modbus RTU und PROFIBUS DP Varianten und gilt nicht für das Ethernet Modul).
- Mit TeSys Tera DTMkönnen Sie mit der optionalen Pin-Management-Funktion die Konfiguration des TeSys Tera system. Sie können die PIN auch zurücksetzen, indem Sie TeSys Tera DTM über die PIN-Verwaltungsfunktion zurücksetzen.

  Weitere Informationen zur Pin-Verwaltungsfunktion finden Sie unter *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- Um die TeSys Tera system, verfügt das LTMTCUF control operator unit mit einer Stiftfunktion ausgestattet. Sie benötigen eine sechsstellige PIN, um auf das LTMTCUF control operator unit.

  Weitere Informationen zur Pin-Funktionalität finden Sie unter *TeSys Tera Motor Management System User Guide – DOCA0257EN*.

Die Kommunikationsprotokolle und die entsprechenden kommerziellen Referenzen finden Sie unter Kommunikationsschnittstellen, Seite 22.

TeSys Tera Systemfunktionen

Inhalt dieses Abschnitts

Firmware Update

Aktualisieren Sie den TeSys Tera system auf die neueste Firmwareversion, um die neuesten Funktionen und die aktuellen Sicherheitspatches zu erhalten. Die gesamte für das TeSys Tera system wird mit der Public Key Infrastructure (PKI) von Schneider Electric signiert, um die Integrität und Authentizität der auf dem TeSys Tera system.

Weitere Informationen zum Firmware-Update über TeSys Tera DTMfinden Sie unter *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.

Weitere Informationen zum Firmware-Update über den Standard-Webserver (gilt für Ethernet Schnittstellenmodule) finden Sie unter *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Um mehr über die Sicherheitsupdates zu erfahren, registrieren Sie sich beim *Security Notifications* auf dem Portal für Cybersicherheit von Schneider Electric.

Date and Time

Um Fehler zu vermeiden, müssen das Datum und die Uhrzeit synchronisiert bleiben.

Das folgende Verfahren zeigt, wie die Datums- und Uhrzeiteinstellungen fürEthernet Schnittstellenmodule über den Standard-Webserver oder TeSys Tera DTM:

1. Navigieren Sie zu **Settings > Allgemein > Date & Time**.
2. Mit der **Dropdown-Liste Date & Time Selection** eine der folgenden Optionen aus:
   - **Manuell**

     HINWEIS:

     - Wenn Datum und Uhrzeit manuell eingestellt werden, LTMT main unit wird beim Neustart auf die Werkseinstellungen zurückgesetzt.
     - Die Datums- und Zeiteinstellungen können manuell über die TeSys Tera DTM oder LTMTCUF control operator unit.
   - **NTP**

     HINWEIS: Das NTP Protokoll ist nur für die Ethernet Versionen des LTMT main unit.

Nicht verwendete Ports/Schnittstellen deaktivieren

Das Deaktivieren nicht verwendeter Ports und Schnittstellen hilft dabei, die Angriffsfläche des Systems zu reduzieren, indem Kommunikationsports und -schnittstellen, die nicht aktiv genutzt werden, abgeschaltet werden.

Die folgenden Einstellungen des TeSys Tera system können über den Standard-Webserver deaktiviert werden:

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

HINWEIS: Weitere Informationen finden Sie unter *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*

Ports

Die Modbus TCP/IP und EtherNet/IP Module des TeSys Tera system verwenden standardmäßig die folgenden Ports für die Kommunikation:

Art der Anschlüsse	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

Das TeSys Tera system erstellt Systemprotokolle, um Ereignisse wie ungültige Anmeldeversuche und Firmware-Updates aufzuzeichnen. Die Protokolle enthalten keine personenbezogenen Informationen.

Um unerwartete Verhaltensweisen (z. B. häufige Neustarts, fehlerhafte Firmware-Updates oder ungültige Anmeldeversuche) zu erkennen, wird empfohlen, die Protokolle regelmäßig zu überwachen.

Weitere Informationen zu den Protokollen finden Sie unter *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* und *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Außerbetriebnahme

Die TeSys Tera system beinhaltet vertrauliche Daten, die bei der Inbetriebnahme eingerichtet wurden, sowie aktuelle Werte und Logeinträge.

Diese Informationen können beispielsweise Folgendes umfassen Modbus LTMT main unit oder gemessene Leistungsaufnahmen.

Vor der Entsorgung des TeSys Tera systemist eine Rücksetzung auf die Werkseinstellungen erforderlich.

Sie können die folgenden Methoden verwenden, um das TeSys Tera system:

- **Test / Reset** Taste auf dem LTMT main unit: Drücken und halten Sie die **Test-/Reset-Taste** Taste auf dem LTMT main unit 10 Sekunden lang gedrückt.
- TeSys Tera DTM LibraryWeitere Informationen finden Sie im Abschnitt *Werkseinstellungen zurücksetzen* im *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unitWeitere Informationen finden Sie im Abschnitt *Befehlsmenü* im *TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*

Netzwerksicherheit

Inhalt dieses Abschnitts

HINWEIS: Dieser Teil gilt nur für Modbus TCP/IP und EtherNet/IP Module der TeSys Tera system.

Einführung

Das TeSys Tera system ist nicht dafür ausgelegt, einer direkten Exposition gegenüber dem öffentlichen Internet standzuhalten. Es sollte mindestens hinter einer Network Address Translation (NAT) installiert werden, vorzugsweise jedoch hinter mehreren Firewalls. Weitere Informationen finden Sie auf den folgenden Webseiten:

- *Schneider Electric cybersecurity consulting services*
- *National Institute of Standards and Technology (NIST)*
- *Agentur der Europäischen Union für Cybersicherheit (ENISA)*

Netzwerksegmentierung

Das TeSys Tera system Gerät ist ein Gateway, das eine Brücke zwischen verschiedenen Netzwerken herstellt. Die Netzwerksegmentierung trägt zur Gewährleistung der Cybersicherheit bei. Zur Verbesserung der Netzwerksegmentierung wurde die TeSys Tera systemEtherNet/IP Version LTMT main unit über zwei Ethernet Ports. Die Ethernet verfügbaren Ports können für Informationstechnologie (IT) und Betriebstechnologie (OT) verwendet werden.

HTTPS und Modbus sind verfügbar auf TeSys Tera system Ethernet Schnittstellen (ETH1, ETH2).

Es wird empfohlen, den Dienst Modbus TCP/IP Dienst in Netzwerken zu deaktivieren, in denen er nicht verwendet wird.

Webserver-Zertifikat des Produkts

Zur Unterstützung sicherer HTTPS-Kommunikation ist das TeSys Tera system standardmäßig mit einem X.509v3 Zertifikat ausgestattet. Mit diesem Zertifikat wird die Integrität und Vertraulichkeit beim Einrichten der HTTPS-Kommunikation sichergestellt.

Webbrowser akzeptieren ausschließlich Zertifikate, die von externen Zertifizierungsstellen (CA) ausgestellt und signiert wurden. Das selbstsignierte Zertifikat ist nicht sicher. Es wird empfohlen, ein von einer Drittanbieter-CA signiertes Zertifikat in das TeSys Tera system und außerdem sollten Sie Datum und Uhrzeit synchronisieren.

Die folgenden Zertifikatsformate werden von der TeSys Tera system:

Format	Kopfzeile/Fußzeile	Art des Schlüssels
PKCS#1	– – – – –BEGIN RSA PRIVATE KEY– – – – –	Nur RSA
PKCS#8	– – – – –BEGIN PRIVATE KEY– – – – –	RSA, EC, DSA usw.
Verschlüsseltes PKCS#8	– – – – –BEGIN ENCRYPTED PRIVATE KEY– – – – –	Beliebig

HINWEIS: Geänderte Prüfzertifikate sind nicht zulässig.

Weitere Informationen zum Zertifikat eines Drittanbieters finden Sie unter *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Sicherheitshinweise zu verbundenen Geräten

Es empfiehlt sich, die Aufstellung der verbundenen Geräte regelmäßig zu kontrollieren. Ethernet Netzwerk des TeSys Tera system. Wenn ein unbekanntes Gerät verbunden ist, suchen Sie es und entfernen Sie es. Sie können auch das Netzwerk neu aufbauen und nur die identifizierten Geräte wieder verbinden.

Physische Sicherheit

Montage

Um die physische Sicherheit der Systeme zu gewährleisten, wird folgende Installation empfohlen:

- Installieren Sie das TeSys Tera system in einem Gehäuse, das entsprechend dem Risikograd Ihrer Installation gesichert ist (z. B. ein Gehäuse mit Vorhängeschloss oder Schlüssel).
- Wenn das TeSys Tera system auf einer Schalttafel montiert ist, installieren Sie die Schalttafel in einem gesicherten Raum (z. B. mit einer verschlossenen Tür oder einer Kamera).

Sicherheitsempfehlungen während der Wartung

Inhalt dieses Abschnitts

Wartungsvorgänge

Während der Lebensdauer des TeSys Tera systemwird empfohlen, regelmäßig folgende Vorgänge durchzuführen:

- Stellen Sie sicher, dass auf dem Gerät die neueste Firmware-Version installiert ist.
- Stellen Sie sicher, dass sämtliche Netzwerk- und Sicherheitsupdates aktuell installiert sind.
- Befolgen Sie die empfohlenen Best Practices für Cybersicherheit.
- Bei unerwarteten Verhaltensweisen wie ungültigen Anmeldeversuchen oder häufigen Neustarts überprüfen Sie die Syslog, Seite 31.
- Um eine Abweichung vom aktuellen Datum zu vermeiden, überprüfen Sie die Date and Time, Seite 28.
- Halten Sie sich an die von Schneider Electric für das Gerät empfohlenen Sicherheitsstandards.

Überprüfung der Sicherheitsfunktionalität

Inhalt dieses Kapitels

Webauthentifizierung

HINWEIS: Dieses Thema gilt nur für Modbus TCP/IP und EtherNet/IP Module der TeSys Tera system.

Um die Web-Authentifizierungsfunktion zu überprüfen, gehen Sie wie folgt vor:

1. Versuchen Sie, sich ohne Passwort beim Standard-Webserver des TeSys Tera system ohne Passwort oder geben Sie ein falsches Passwort ein.

   Ergebnis: Der TeSys Tera system Sie haben keinen Zugriff auf den Standard-Webserver.

2. Geben Sie für drei Instanzen die falschen Anmeldedaten ein.

   Ergebnis: Die TeSys Tera system blockiert für 15 Minuten, bevor Sie den vierten Versuch starten können.

Webautorisierung

HINWEIS: Dieses Thema gilt nur für Modbus TCP/IP und EtherNet/IP Module der TeSys Tera system.

Um die Webautorisierungsfunktion zu überprüfen, gehen Sie wie folgt vor:

1. Melden Sie sich beim TeSys Tera system Standard-Webserver an.

   Ergebnis: Nach der Anmeldung haben Sie vollen Zugriff auf die Daten und Funktionen.

2. Eine Webseite mit einem Lesezeichen versehen (zum Beispiel **Settings**).
3. Öffnen Sie ein privates Navigationsfenster in Ihrem Browser und öffnen Sie die mit einem Lesezeichen versehene Webseite.

   Ergebnis: Sie können nicht auf die Webseite zugreifen, werden jedoch zur Anmeldeseite weitergeleitet.

Syslog

Um die Syslog-Funktionalität zu überprüfen, gehen Sie wie folgt vor:

1. Nach einigen oder allen vorangegangenen Tests können Sie über den TeSys Tera DTM oder Standard-Webserver auf die **Logs**.
2. Laden Sie die Protokolldateien herunter.
3. Überprüfen Sie, ob die durchgeführten Tests oder fehlgeschlagenen Versuche in den Protokollen vorhanden sind.

Firmware Update

Um die Firmware-Update-Funktionalität zu überprüfen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Firmware-Update** auf dem TeSys Tera DTM oder dem Standard-Webserver.
2. Laden Sie eine authentifizierte Firmware-Update-Datei hoch.
3. Warten Sie, bis die Firmware validiert ist.

   Ergebnis: Ein Systemneustart erfolgt nur, wenn die Firmware des LTMT main unit aktualisiert wird und die neuen Firmware-Details in der TeSys Tera DTM.

Deaktivieren der Dienste

HINWEIS: Dieses Thema gilt nur für Modbus TCP/IP und EtherNet/IP Module der TeSys Tera system.

Um die Funktionalität der Deaktivierungsdienste zu überprüfen, gehen Sie wie folgt vor:

1. Navigieren zu **Security > IP Network List > Device Discovery** über den Standard-Webserver.
2. Deaktivieren Sie die Geräteerkennung.
3. Verbinden Sie einen PC mit Windows Betriebssystem mit demselben Netzwerk.
4. Klicken Sie auf **Network** im **File Explorer**.

   Ergebnis: Das TeSys Tera system Ist nicht auffindbar und taucht deshalb nicht in der Gerätesliste des Netzwerks auf.

Navigieren Sie zu **Sicherheit > IP-Netzwerkliste** und befolgen Sie die oben beschriebenen Schritte, um die folgenden Deaktivierungsmethoden zu überprüfen:

- Modbus TCP
- Modbus RTU

Schneider Electric Support-Portal für Cybersicherheit

Inhalt dieses Abschnitts

Überblick

Die Schneider Electric *Cybersecurity support portal* beschreibt die Schneider Electric Richtlinie zum Schwachstellenmanagement.

Das Ziel der Schneider Electric Richtlinie zum Schwachstellenmanagement besteht darin, Schwachstellen in der Cybersicherheit zu beheben, die sich auf Schneider Electric Produkten und Systemen zu beheben, um installierte Lösungen, Kunden und die Umgebung zu schützen.

Schneider Electric arbeitet eng mit Forschern, Cyber-Notfallteams (CERTs) und Anlagenbetreibern zusammen, um sicherzustellen, dass genaue Informationen rechtzeitig bereitgestellt werden, damit ihre Anlagen angemessen geschützt werden können.

Schneider ElectricDas Corporate Product CERT (CPCERT) ist für die Verwaltung und Herausgabe von Warnmeldungen zu Schwachstellen und Abhilfemaßnahmen verantwortlich, die Produkte und Lösungen betreffen.

Das CPCERT koordiniert die Kommunikation zwischen relevanten CERTs, unabhängigen Forschern, Produktmanagern und allen betroffenen Kunden.

Support-Portal Cybersicherheit

Die Schneider Electric Cybersecurity support portal enthält folgende Informationen:

- Über Cybersicherheitslücken von Produkten
- Über Vorfälle der Cybersicherheit
- Über eine Schnittstelle, mit der Sie Cybersicherheitsvorfälle oder Schwachstellen melden können

Meldung und Management von Schwachstellen

Cybersicherheitsvorfälle und potenzielle Schwachstellen können über die Website von Schneider Electric gemeldet werden: Eine Schwachstelle melden.

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

www.se.com

DOCA0260DE-00