TeSys Active

TeSys Tera Motor Management System

Cybersecurity Guide

TeSys offers innovative and connected solutions for motor starters

DOCA0260EN-00
11/2025

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information.....5
About the Document.....6
Precautions.....9
Cybersecurity Safety Notice.....11
Introduction to Cybersecurity.....12
Introduction.....13
Schneider Electric Guidelines.....14
Schneider Electric's Approach on Cybersecurity.....15
Security Threats.....16
Policies and Rules.....17
Security Hardening Guidelines.....18
TeSys Tera System Information.....20
Overview.....21
Communication Interfaces.....22
Supported Protocols.....24
Security Features.....25
TeSys Tera System Features.....26
Firmware Update.....27
Date and Time.....28
Disable Unused Ports/Interface.....29
Ports.....30
Syslog.....31
Decommissioning.....32
Network Security.....33
Introduction.....34
Network Segmentation.....35
Product Web Server Certificate.....36
Safety Information on Connected Devices.....37
Physical Security.....38
Security Recommendations During Maintenance.....39
Maintenance Operations.....40
Verification of Security Functionality.....41
Web Authentication.....42
Web Authorization.....42
Syslog.....42
Firmware Update.....42
Disabling Services.....43
Schneider Electric Cybersecurity Support Portal.....44
Overview.....45
Cybersecurity Support Portal.....46
Vulnerability Reporting and Management.....47

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

⚡ The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Document

Document Scope

This guide provides information on cybersecurity aspects for the TeSys™ Tera System to help system designers and operators promote a secure operating environment for the product.

This guide addresses on how to secure your operational technology network, or your company Ethernet network.

NOTE: In this guide, the term **security** is used to refer to cybersecurity.

Validity Note

This document is valid for the following certified components of the TeSys Tera system:

- LTMTEFM: LTMT main unit with EtherNet/IP or Modbus TCP/IP protocol, 100–240 Vac/Vdc
- LTMTEBD: LTMT main unit with EtherNet/IP or Modbus TCP/IP protocol, 24 Vdc
- LTMTMFM: LTMT main unit with Modbus RTU protocol, 100–240 Vac/Vdc
- LTMTMBD: LTMT main unit with Modbus RTU protocol, 24 Vdc
- LTMTPFM: LTMT main unit with PROFIBUS DP protocol, 100–240 Vac/Vdc
- LTMTPBD: LTMT main unit with PROFIBUS DP protocol, 24 Vdc

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Available Languages of the Document

The document is available in these languages:

- English
- Chinese
- French
- German
- Italian
- Korean
- Spanish

Related Documents

Title of documentation	Description	Reference number
TeSys Tera Motor Management System Catalog	The catalog: • Describes the TeSys Tera system • Contains the TeSys Tera technical characteristics	LVCATENTER
TeSys Tera Motor Management System User Guide	This is the main user guide that introduces the complete TeSys Tera system. It describes the main functions of the LTMT main units, LTMTCT/LTMTCTV sensor modules, LTMT expansion modules, and LTMTCUF control operator unit.	DOCA0257EN
TeSys Tera Motor Management System Installation Guide	This guide describes the installation, commissioning, and maintenance of the LTMT main units, LTMTCT/LTMTCTV sensor modules, LTMT expansion modules, and LTMTCUF control operator unit.	DOCA0356EN
TeSys Tera Motor Management System DTM library Online Help Guide	This guide describes the TeSys Tera DTM library which allows the customization of the control functions of the TeSys Tera Motor Management System.	DOCA0275EN
TeSys Tera Motor Management System Modbus RTU Communication Guide	This guide describes the Modbus network protocol communication of the LTMT main unit.	DOCA0355EN
TeSys Tera Motor Management System PROFIBUS DP Communication Guide	This guide describes the PROFIBUS DP network protocol communication of the LTMT main unit.	DOCA0256EN
TeSys Tera Motor Management System EtherNet/IP Communication Guide	This guide describes the EtherNet/IP network protocol communication of the LTMT main unit.	DOCA0258EN
TeSys Tera Motor Management System LTMTCUF control operator unit User Guide	This guide describes how to install, configure, and use the LTMTCUF control operator unit.	DOCA0233EN
TeSys Tera Motor Management System DTM library Software Release Note	This document provides important information about the TeSys Tera DTM Library software and provides summary of new features and enhancement.	DOCA0279EN
TeSys Tera Motor Management System Firmware Release Note	This document provides information about firmware package versions of the TeSys Tera system and provides summary of new features and enhancement.	DOCA0276EN
How Can I Reduce Vulnerability to Cyber Attacks?	This guide describes the cybersecurity risks and abatement strategies in control system and automation	How Can I Reduce Vulnerability to Cyber Attacks?

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Trademarks

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

Precautions

Read and understand the following precautions before performing any procedures in this guide.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- This equipment must only be installed and serviced by qualified electrical personnel.
- Turn off all power supplying this equipment before working on or inside this equipment.
- Use only the specified voltage when operating this equipment and any associated products.
- Always use a properly rated voltage sensing device to confirm power is off.
- Use appropriate interlocks where personnel and/or equipment hazards exist.
- Power line circuits must be wired and protected in compliance with local and national regulatory requirements.
- Apply appropriate personal protective equipment (PPE) and follow safe electrical work practices per NFPA 70E, NOM-029-STPS, or CSA Z462 or local equivalent.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Do not disassemble, repair, or modify this equipment. There are no user serviceable parts.
- Install and operate this equipment in an enclosure appropriately rated for its intended application environment.
- Each implementation of this equipment must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Qualified Personnel

Only appropriately trained person who is familiar with and understand the content of this guide and all other related product documentation are authorized to work on and with this product.

The qualified person must be able to detect possible hazards that may arise from modifying parameter values and generally from mechanical, electrical, or electronic equipment. The qualified person must be familiar with the standards, provisions, and regulations for the prevention of industrial accidents, which they must observe when designing and implementing the system.

The use and application of the information contained in this guide requires expertise in the design and programming of automated control systems. Only you, the user, panel builder, or integrator, can be aware of all the conditions and factors present during installation, setup, operation, and maintenance of a process plant or machine, and can therefore determine the automation and associated equipment and the related safeties and interlocks which can be effectively and properly used when selecting automation and control equipment, and any other related equipment or software, for a particular application. You must also consider applicable local, regional, or national standards and/or regulations.

Pay particular attention to conformance with any safety information, electrical requirements, and normative standards that apply to your process plant or machine in the use of this equipment.

Intended Use

The products described in this guide, together with software, accessories, and options, are a part of starters for low-voltage electrical loads, intended for industrial use according to the instructions, directions, examples, and safety information contained in the present document and other supporting documentation.

The product may only be used in compliance with all applicable safety regulations and directives, the specified requirements, and the technical data.

Before using the product, you must perform a risk assessment of the planned application. Based on the results, appropriate safety-related measures must be implemented.

Since the product is used as a component of a process plant or machine, you must ensure the safety of person by means of the overall system design.

Operate the product only with the specified cables and accessories. Use only genuine accessories and spare parts.

Any use other than the use explicitly permitted is prohibited and can result in unanticipated hazards.

Cybersecurity Safety Notice

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls, and information.
- Disable unused ports/services to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example, least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Introduction to Cybersecurity

What’s in This Part

Introduction..13
Schneider Electric Guidelines..14
Schneider Electric's Approach on Cybersecurity..15
Security Threats..16
Policies and Rules..17
Security Hardening Guidelines..18

Introduction

Cybersecurity as part of Process, Tools and Technology, Compliance, and Governance, aims at safeguarding your communication network and all connected devices from attacks that could disrupt operations (availability), alter information (integrity), or expose confidential data (confidentiality).

The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. There are many aspects to cybersecurity including designing secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security control/measurement procedures and best practice policies.

Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to TeSys Tera system, you should follow the Schneider Electric defense-in-depth approach to cybersecurity.

This approach is described in the *Recommended Cybersecurity Best Practices*.

In addition, you will find many useful resources and up-to-date information on the Schneider Electric Cybersecurity Support Portal, page 44.

Schneider Electric's Approach on Cybersecurity

Schneider Electric adheres to industries best practice in the development and implementation of control systems. This includes a defense-in-depth approach to secure an industrial control system. This approach places the controllers behind one or more firewalls to restrict access to authorized personnel and protocols only.

⚠WARNING

UNAUTHENTICATED ACCESS AND SUBSEQUENT UNAUTHORIZED OPERATION

- Evaluate whether your equipment or complete environment are connected to your critical infrastructure. If so, take appropriate steps in terms of prevention, based on defense-in-depth, before connecting the automation system to any network.
- Limit the number of devices connected to a network inside your company.
- Isolate your industrial network from other networks inside your company.
- Protect any network against unintended access by using firewalls, VPN, or other, proven security measures.
- Monitor activities within your systems.
- Prevent subject devices from direct access or direct link by unauthorized parties or unauthenticated actions.
- Prepare a recovery plan including backup of your system and process information.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Security Threats

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of PCs and PC networks. These actions can be initiated from within the physical facility or from an external location. Security challenges for the control environment include:

- Diverse physical and logical boundaries
- Multiple sites and large geographic spans
- Adverse effects of security implementation on process availability
- Increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open
- Increased exposure to malicious software from USB devices, vendor and service technician laptops, and the enterprise network
- Direct impact of control systems on physical and mechanical systems

Policies and Rules

Schneider Electric has a Secure Development Lifecycle (SDL) process, a key product development-based framework that helps ensure products follow secure design processes across all lifecycle stages. The Schneider Electric SDL process complies with IEC 62443-4.1 standards.

The SDL process includes:

- SDL practices applied to internal development actions throughout the supply chain.
- Final security review required for project release.
- Security training for personnel involved in the product development.

Security Hardening Guidelines

Introduction

Your PC can run a variety of applications to enhance security in your control environment. The system has factory default settings that require reconfiguration to align with Schneider Electric's device hardening recommendations of the defense-in-depth approach.

The following guidelines describe procedures in a Windows operating system. They are provided as examples only. Your operating system and application may have different requirements or procedures.

Disabling the Remote Desktop Protocol

Schneider Electric’s defense-in-depth approach recommendations include disabling remote desktop protocol (RDP) unless your application requires the RDP.

In Windows 11, remote desktop protocol (RDP) is disabled using **Settings > System > Remote Desktop > Enable Remote Desktop** (toggle to **Off**).

Updating Security Policies

Update the security policies on the PCs in your system by `gpupdate` in a command window. For more information, refer to the Microsoft documentation on `gpupdate`.

Managing Updates

Before deployment, update all PC operating systems using the utilities on Microsoft’s **Windows Update** Web page. To access this tool in Windows, select **Start > All Programs > Windows Update**.

Workstation Protection

To reduce the security risks associated with the engineering workstation, enable the memory exploit settings such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). These security settings can be enabled by using the system exploit protection settings in Windows 11 operating system. For more information, refer to the Microsoft security features web page.

Enforce Secure Passwords

Use strong passwords meeting the required elements such as uppercase letters, lowercase letters, numbers, and special characters. Enabling this feature helps prevent unauthorized access by reducing the risk of weak passwords.

Use of Non-Default Ports

Changing the default communication ports for protocols such as HTTPS, DWPS, and Modbus TCP adds an additional layer of security.

IP Allow List

The IP allow list feature restricts access to the system by permitting only specified IP addresses. This helps prevent unauthorized devices from connecting to the system and ensures that only trusted sources can communicate with the TeSys Tera system. To access the IP allow list feature, navigate to **Security > IP Allow List > IP Allow List** in the Standard Web Server.

TeSys Tera System Information

What's in This Part

Overview 21
Communication Interfaces 22
Supported Protocols 24
Security Features 25

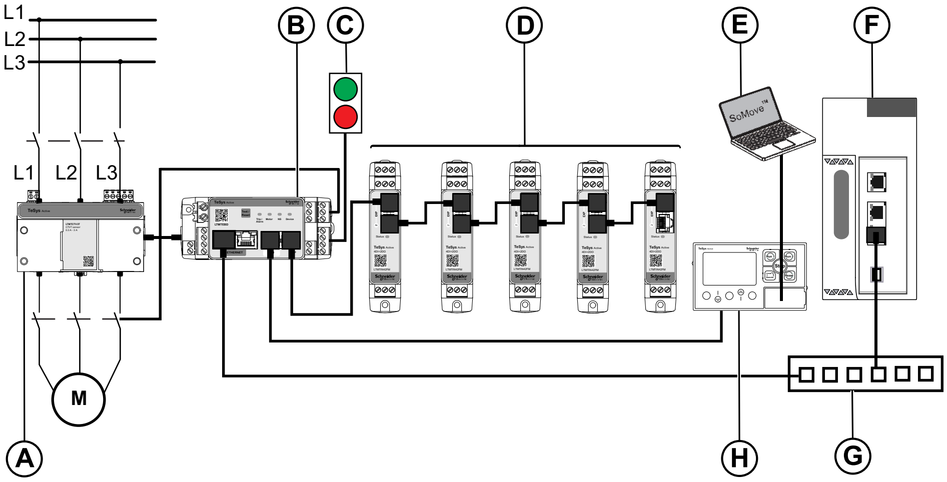
Overview

The TeSys Tera Motor Management System (or TeSys Tera system) is part of the TeSys Active range of intelligent relays and motor starters. The TeSys Tera system is designed as a reliable building block for Intelligent Motor Control Centres (iMCCs) to provide complete protection, metering, control, and monitoring capabilities for single-phase or three-phase AC induction motors.

The TeSys Tera system is installed in the low voltage switchgear system and connects the higher level automation system through fieldbus network and the motor feeder.

TeSys Tera system:

- Covers conventional and advanced motor protection, metering, and monitoring in iMCC feeders into single, easy to configure, compact communicating module with a standalone HMI device..
- Provides protection controller for low voltage contactor-controlled motor starter feeders.
- Provides flexible and modular motor management system for motors with constant speeds in low voltage applications.



A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C Start/Stop commands

D LTMT expansion modules

E PC running SoMove FDT container software with TeSys Tera DTM installed

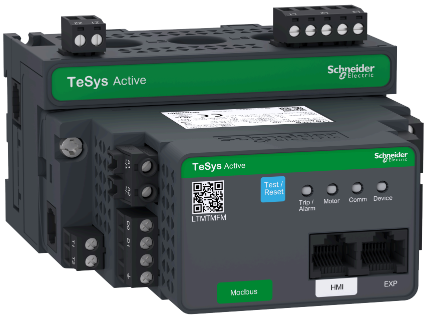
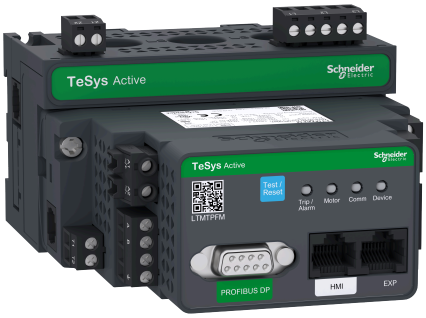
F Programmable Logic Controller (PLC) or Distributed Control System (DCS)

G Ethernet switch

H LTMTCUF control operator unit

Communication Interfaces

TeSys Tera system communicates through the following interface types:

LTMT main unit	Reference	Ports
Modbus RTU  TeSys Active Schneider Electric Test / Reset Trip / Alarm Motor Comm Device LTMTMFM Modbus HMI EXP	• LTMTMFM (100–240 Vac/ Vdc) • LTMTMBD (24 Vdc)	• Modbus RTU communication port with terminal connector • HMI port with Modbus RTU communication for configuration
PROFIBUS DP  TeSys Active Schneider Electric Test / Reset Trip / Alarm Motor Comm Device LTMTPFM PROFIBUS DP HMI EXP	• LTMTPFM (100–240 Vac/Vdc) • LTMTPBD (24 Vdc)	• PROFIBUS DP with sub D9 connector • Profibus port with terminal connector • HMI port with Modbus RTU communication

LTMT main unit	Reference	Ports
Modbus TCP/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Two Ethernet ports with Modbus TCP/IP • HMI port with Modbus RTU communication
EtherNet/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Two Ethernet ports with EtherNet/IP • HMI port with Modbus RTU communication

Supported Protocols

Serial Communication Devices

The Modbus RTU and PROFIBUS DP modules of the TeSys Tera system support Modbus RTU and PROFIBUS protocol for communications with fieldbus devices.

For the communication protocols and the respective commercial references, refer to Communication Interfaces, page 22.

Ethernet Communication Devices

The Modbus TCP/IP and EtherNet/IP modules of the TeSys Tera system support the following protocols:

- HTTPS through configuration tools and embedded webpages
- Modbus TCP/IP and EtherNet/IP for communications with fieldbus devices
- DHCP for network IP addressing
- DNS for network name resolution
- NTP for time synchronization
- DPWS for device discovery

For the communication protocols and the respective commercial references, refer to Communication Interfaces, page 22.

Security Features

The TeSys Tera system supports the following features:

- Firmware digitally signed by Schneider Electric can only be installed on TeSys Tera system.
- At each boot, the digital signature of the firmware is validated before execution.
- User passwords are securely stored (applicable for Ethernet interface modules).

  For more information about the password policy, refer to *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- You can perform factory reset of the TeSys Tera system by using **Factory Default** setting using the TeSys Tera DTM or the **Test / Reset** button on LTMT main unit.

  For more information about the **Test / Reset** button, refer to *TeSys Tera Motor Management System User Guide – DOCA0257EN*.
- The TeSys Tera system has an internal clock and remembers the date and time for 12 hours without power (valid for Modbus RTU and PROFIBUS DP variants and not applicable for the Ethernet module).
- Using TeSys Tera DTM, the optional pin management functionality allows you to enable or disable the configuration of the TeSys Tera system. You can also reset the pin for TeSys Tera DTM using the pin management functionality.

  For more information about the pin management functionality, refer to *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- To secure the TeSys Tera system, the LTMTCUF control operator unit comes with pin functionality. You must have a six-digit pin to access the LTMTCUF control operator unit.

  For more information about the pin functionality, refer to *TeSys Tera Motor Management System User Guide – DOCA0257EN*.

For the communication protocols and the respective commercial references, refer to Communication Interfaces, page 22.

TeSys Tera System Features

What's in This Part

Firmware Update 27
Date and Time 28
Disable Unused Ports/Interface 29
Ports 30
Syslog 31
Decommissioning 32

Firmware Update

Update the TeSys Tera system to the latest firmware version to obtain the latest features and keep up-to-date with security patches. All firmware designed for the TeSys Tera system is signed using the Schneider Electric Public Key Infrastructure (PKI) to help provide integrity and authenticity of the firmware running on the TeSys Tera system.

For more information about the firmware update through TeSys Tera DTM, refer to *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.

For more information about the firmware update through the standard web server (applicable for Ethernet interface modules), refer to *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

To know more on the security updates, register with the *Security Notifications* on Schneider Electric Cybersecurity Support Portal.

Date and Time

To avoid errors, it is important to keep the date and time synchronized.

The following procedure shows how to update the date and time settings for Ethernet interface modules using standard web server or TeSys Tera DTM:

1. Navigate to **Settings > General > Date & Time**.
2. Using the **Date & Time Selection** drop-down list, select one of the following options:
   - **Manual**

     NOTE:

     - When the date and time are set manually, the LTMT main unit resets to factory settings upon reboot.
     - The date and time settings can be update manually using the TeSys Tera DTM or the LTMTCUF control operator unit.
   - **NTP**

     NOTE: NTP protocol is available only for the Ethernet versions of the LTMT main unit.

Disable Unused Ports/Interface

Disabling unused ports/interface helps reduce the system’s attack surface by turning off communication ports and interfaces that are not actively used.

The following settings of the TeSys Tera system can be disabled using the standard web server:

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

NOTE: For more information, refer to *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*

Ports

The Modbus TCP/IP and EtherNet/IP modules of the TeSys Tera system use the following ports for communication by default:

Type of Ports	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

The TeSys Tera system generates system logs to record events such as invalid login attempts and firmware updates. The logs do not contain any personal information.

To detect unexpected behaviors (for example, frequent rebooting, incorrect firmware update, or invalid login attempts), it is recommended to monitor logs regularly.

For more information about the logs, refer to *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* and *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Decommissioning

The TeSys Tera system contains confidential information configured during commissioning, recent data values, and logs.

For example, this information can include Modbus LTMT main unit topology, or measured power consumptions.

It is required to perform a factory reset before disposing of the TeSys Tera system.

You can use the following ways to reset the TeSys Tera system:

- **Test / Reset** button on the LTMT main unit: Press and hold the **Test / Reset** button on the LTMT main unit for 10 seconds.
- TeSys Tera DTM Library: For more information, refer to section *Factory Reset* in the *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unit: For more information, refer to section *Command Menu* in the *TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*

Network Security

What's in This Part

Introduction......34
Network Segmentation......35
Product Web Server Certificate......36
Safety Information on Connected Devices......37

NOTE: This part is valid only for Modbus TCP/IP and EtherNet/IP modules of the TeSys Tera system.

Introduction

The TeSys Tera system is not designed to withstand direct exposure to the public internet. It should be installed at least behind Network Address Translation (NAT) or preferably behind multiple firewalls. For more information, refer to the following webpages:

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

Network Segmentation

The TeSys Tera system is a gateway that creates a bridge between different networks. Network segmentation helps ensure cyber defense. To enhance network segmentation, the TeSys Tera system EtherNet/IP version LTMT main unit features two Ethernet ports. The Ethernet ports available can be used for Information Technology (IT) and Operational Technology (OT).

HTTPS and Modbus are available on TeSys Tera system Ethernet interfaces (ETH1, ETH2).

It is recommended to disable the Modbus TCP/IP service on networks where it is not used.

Product Web Server Certificate

To support secure HTTPS communications, the TeSys Tera system is equipped with an X.509v3 certificate by default. This certificate helps ensure the integrity and confidentiality to set up HTTPS communication.

Web browsers only recognize third-party Certificate Authority (CA) signed certificates. The self-signed certificate is not secured. It is recommended to import a third-party CA signed certificate to the TeSys Tera system and also you should keep the date and time synchronized.

The following certificate formats are supported by the TeSys Tera system:

Format	Header/Footer	Key Type
PKCS#1	–––––BEGIN RSA PRIVATE KEY–––––	RSA only
PKCS#8	–––––BEGIN PRIVATE KEY–––––	RSA, EC, DSA and so on
Encrypted PKCS#8	–––––BEGIN ENCRYPTED PRIVATE KEY–––––	Any

NOTE: Modified test certificates are not acceptable.

For more details on the third-party certificate, refer to *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Safety Information on Connected Devices

It is recommended to regularly check the list of devices connected to the Ethernet network of the TeSys Tera system. In case of an unknown connected device, locate it and remove it. You can also rebuild the network and reconnect only the identified devices.

Physical Security

Installation

To help protect the systems physical security, the following installation is advised:

- Install the TeSys Tera system in an enclosure that is secured in a manner appropriate to the risk level of your installation (for example, an enclosure with a padlock or a key).
- If the TeSys Tera system is mounted on a switchboard, install the switchboard in a secured room (for example, with a locked door or camera).

Security Recommendations During Maintenance

What’s in This Part

Maintenance Operations....................40
Verification of Security Functionality....................41

Maintenance Operations

Over the lifetime of the TeSys Tera system, it is recommended to regularly do the following operations:

- Ensure that the device is running the latest firmware version.
- Verify that all network and security patches are up to date.
- Follow cybersecurity best practices as recommended.
- For unexpected behaviors such as invalid login attempts or frequent rebooting, check the Syslog, page 31.
- To avoid drifting away from the current date, check the Date and Time, page 28.
- Adhere to the security standards recommended by Schneider Electric for the device.

Verification of Security Functionality

What’s in This Chapter

Web Authentication 42
Web Authorization 42
Syslog 42
Firmware Update 42
Disabling Services 43

Web Authentication

NOTE: This topic is valid only for Modbus TCP/IP and EtherNet/IP modules of the TeSys Tera system.

To verify the web authentication functionality, proceed as follows:

1. Try to log in to the standard web server of the TeSys Tera system with no password or enter a wrong password.

   Result: The TeSys Tera system does not give you access to the standard web server.

2. Enter the wrong credentials for three instances.

   Result: The TeSys Tera system locks for 15 minutes before allowing you to try for the fourth instance.

Web Authorization

NOTE: This topic is valid only for Modbus TCP/IP and EtherNet/IP modules of the TeSys Tera system.

To verify the web authorization functionality, proceed as follows:

1. Log in to the TeSys Tera system Standard Web Server.

   Result: After logging in, you have full access to the data and features.

2. Bookmark a webpage (for example, **Settings**).
3. Open a private navigation window in your browser and open the bookmarked webpage.

   Result: You cannot access the webpage, however you are redirected to the login page.

Syslog

To verify the Syslog functionality, proceed as follows:

1. After some or all the preceding tests, using the TeSys Tera DTM or standard web server, access the **Logs**.
2. Download the log files.
3. Verify that the performed test or failing attempts are present in the logs.

Firmware Update

To verify the firmware update functionality, proceed as follows:

1. Navigate to the **Firmware Update** functionality on the TeSys Tera DTM or the standard web server.
2. Upload an authenticated firmware update file.
3. Wait for the firmware to be validated.

   Result: A system reboot occurs only when the firmware of the LTMT main unit is updated and the new firmware details updated in the TeSys Tera DTM.

Disabling Services

NOTE: This topic is valid only for Modbus TCP/IP and EtherNet/IP modules of the TeSys Tera system.

To verify the disabling services functionality, proceed as follows:

1. Navigating to **Security > IP Network List > Device Discovery** using the Standard Web Server.
2. Disable the device discovery.
3. Connect a PC with Windows operating system to the same network.
4. Click **Network** from the **File Explorer**.

   Result: The TeSys Tera system is not discovered, therefore it does not appear in the list of devices in the network.

Navigate to **Security > IP Network List** and follow the above procedure to verify the following disabling methods:

- Modbus TCP
- Modbus RTU

Schneider Electric Cybersecurity Support Portal

What’s in This Part

Overview 45
Cybersecurity Support Portal...46
Vulnerability Reporting and Management 47

Overview

The Schneider Electric *Cybersecurity support portal* outlines the Schneider Electric vulnerability management policy.

The aim of the Schneider Electric vulnerability management policy is to address vulnerabilities in cybersecurity affecting Schneider Electric products and systems, in order to protect installed solutions, customers, and the environment.

Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to adequately protect their installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and issuing alerts on vulnerabilities and mitigations affecting products and solutions.

The CPCERT coordinates communications between relevant CERTs, independent researchers, product managers, and all affected customers.

Cybersecurity Support Portal

The Schneider Electric Cybersecurity support portal provides the following information:

- About cybersecurity vulnerabilities of products
- About cybersecurity incidents
- About an interface that enables you to declare cybersecurity incidents or vulnerabilities

Vulnerability Reporting and Management

Cybersecurity incidents and potential vulnerabilities can be reported via the Schneider Electric website: Report a Vulnerability.

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

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

© 2025 Schneider Electric. All rights reserved.