TeSys Active

TeSys Tera Motor Management System

网络安全指南

TeSys 为电机起动器提供了创新的互联解决方案。

DOCA0260ZH-00
11/2025

法律声明

本文档中提供的信息包含与产品/解决方案相关的一般说明、技术特性和/或建议。

本文档不应替代详细调研、或运营及场所特定的开发或平面示意图。它不用于判定产品/解决方案对于特定用户应用的适用性或可靠性。任何此类用户都有责任就相关特定应用场合或使用方面，对产品/解决方案执行或者由所选择的任何业内专家（集成师、规格指定者等）对产品/解决方案执行适当且全面的风险分析、评估和测试。

施耐德电气品牌以及本文档中涉及的施耐德电气及其附属公司的任何商标均是施耐德电气或其附属公司的财产。所有其他品牌均为其各自所有者的商标。

对于将本文档 或其内容用作商业用途的行为，施耐德电气未授予任何权利或许可，但以“原样”为基础进行咨询的非独占个人许可除外。

对于本文档或其内容或其格式，施耐德电气有权随时修改或更新，恕不另行通知。

在适用法律允许的范围内，对于本文档信息内容中的任何错误或遗漏，以及对本文档内容的任何非预期使用或误用，施耐德电气及其附属公司不会承担任何责任或义务。

目录

安全信息

重要信息

在试图安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。下述特定信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。

在“危险”或“警告”安全标签上添加此符号表示存在触电危险，
如果不遵守使用说明，会导致人身伤害。

这是提醒注意安全的符号。它用于提醒您注意潜在人身伤害风险。
遵守此符号后面的安全说明，以免发生伤害或死亡事故。

⚠ 危险

危险表示若不加以避免，将会导致严重人身伤害甚至死亡的危险情况。

⚠ 警告

警告表示若不加以避免，可能会导致严重人身伤害甚至死亡的危险情况。

⚠ 小心

小心表示若不加以避免，可能会导致轻微或中度人身伤害的危险情况。

注意

注意用于指示与人身伤害无关的危害。

请注意

电气设备的安装、操作、维修和维护工作仅限于有资质的人员执行。施耐德电气不承担由于使用本资料所引起的任何后果。

有资质的人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

关于本文档

文档范围

本指南提供了有关TeSys™ Tera系统网络安全方面的信息，旨在协助系统设计人员和操作人员为该产品营造安全的运行环境。

本指南阐述了如何保护您的运营技术(OT)网络或企业Ethernet网络。

注: 在本指南中，术语**安全**是指网络安全。

有效性说明

本文档适用于 TeSys Tera system 的以下认证组件：

- LTMTEFM: LTMT main unit 采用 EtherNet/IP 或 Modbus TCP/IP 协议，100–240 Vac/Vdc
- LTMTEBD: LTMT main unit 采用 EtherNet/IP 或 Modbus TCP/IP 协议，24 Vdc
- LTMTMFM：采用 Modbus RTU 协议的 LTMT main unit，100-240 Vac/Vdc
- LTMTMBD：采用 Modbus RTU 协议的 LTMT main unit，24 Vdc
- LTMTPFM：采用 PROFIBUS DP 协议的 LTMT main unit，100-240 Vac/Vdc
- LTMTPBD：采用 PROFIBUS DP 协议的 LTMT main unit，24 Vdc

一般网络安全说明

近年来，随着联网机器和生产设备的数量日益增多，发生非法访问、数据泄露和运营中断等网络威胁的几率也相应增加。因此，您必须考虑众多可能的网络安全措施，以帮助保护资产和系统免于此类威胁。

为了有助于保持和保护 Schneider Electric 产品的安全，强烈建议您采取 Cybersecurity Best Practices 文档中所述的网络安全最佳做法。

Schneider Electric 还提供其他信息和帮助：

- 订阅 Schneider Electric 安全资讯。
- 访问 Cybersecurity Support Portal 网页，以：
  - 查看安全通知。
  - 报告漏洞和事件。
- 访问 Schneider Electric Cybersecurity and Data Protection Posture 网页，以：
  - 了解网络安全态势。
  - 在网络安全学院中了更详细地了解网络安全。
  - 深入了解 Schneider Electric 的网络安全服务。

环境数据

有关产品合规性和环境信息，请参阅 Schneider Electric Environmental Data Program。

文档的可用语言

文档提供以下语言版本:

- 英语
- 中文
- 法语
- 德语
- 意大利语
- 韩语
- 西班牙语

相关的文件

文档名称	描述	参考编号
TeSys Tera Motor Management System 目录	目录： • 介绍了 TeSys Tera system • 包含 TeSys Tera 技术特性	LVCATENTER
TeSys Tera Motor Management System 用户指南	它是主要用户指南，其中介绍了完整的 TeSys Tera system。其中还介绍了 LTMT main units、LTMTCT/LTMTCTV Sensor Module、LTMT expansion modules 和 LTMTCUF control operator unit 的主要功能。	DOCA0257ZH-CN-00
TeSys Tera Motor Management System 安装指南	该指南介绍了 LTMT main unit、LTMTCT/LTMTCTV Sensor Module、LTMT expansion modules 和 LTMTCUF control operator unit 的安装、调试和维护。	DOCA0356ZH
TeSys Tera Motor Management System DTM library 在线帮助指南	该指南介绍了 TeSys Tera DTM 库，此库允许自定义 TeSys Tera Motor Management System 的控制功能。	DOCA0275ZH
TeSys Tera Motor Management System Modbus RTU 通讯指南	该指南介绍了 LTMT main unit 的 Modbus 网络协议通讯。	DOCA0355ZH
TeSys Tera Motor Management System PROFIBUS DP 通讯指南	该指南介绍了 LTMT main unit 的 PROFIBUS DP 网络协议通讯。	DOCA0256ZH
TeSys Tera Motor Management System EtherNet/IP 通讯指南	该指南介绍了 LTMT main unit 的 EtherNet/IP 网络协议通讯。	DOCA0258ZH
TeSys Tera Motor Management System LTMTCUF control operator unit 用户指南	该指南介绍了如何安装、配置和使用 LTMTCUF control operator unit。	DOCA0233ZH
TeSys Tera Motor Management System DTM library 软件发布说明	该文档提供了有关 TeSys Tera DTM Library 软件的重要信息，并概述了新功能和增强功能。	DOCA0279ZH
TeSys Tera Motor Management System 固件发行说明	该文档提供了有关 TeSys Tera system 固件包版本的重要信息，并概述了新功能和增强功能。	DOCA0276ZH
我如何减少网络攻击漏洞？	本指南阐述了控制系统与自动化系统中的网络安全风险及缓解策略。	我如何减少网络攻击漏洞？

要在线查找文档，请访问 Schneider Electric 下载中心 (www.se.com/ww/en/download/)。

有关非包容性或非敏感术语的信息

作为一家负责任、具有包容性的公司，Schneider Electric 不断更新其包含非包容性或非敏感术语的沟通方式和产品。但是，尽管我们做了这些努力，我们的内容仍可能包含某些客户认为不合适的条款。

商标

QR Code 是 DENSO WAVE INCORPORATED 在日本和其他国家或地区的注册商标。

注意事项

在执行本指南中的任何步骤之前，请阅读并理解以下注意事项。

⚠⚠危险

电击、爆炸或电弧闪光危险

- 只有具备相应资质的电气人员才能安装和维修该设备。
- 在设备上或其内部作业之前，请先关闭该设备的所有电源。
- 操作此设备和任何关联产品时，只能使用指定电压。
- 确保使用合适的额定电压传感器确认电源已关闭。
- 在人员和/或设备面临危险的环境中，请使用适合的联锁装置。
- 电源线路必须按照当地和国家法规要求进行接线和保护。
- 佩戴适当的个人防护设备 (PPE) 并遵循 NFPA 70E、NOM-029-STPS 或 CSA Z462 或当地同等标准的安全电气工作实践。

未按说明操作将导致人身伤亡等严重后果。

⚠警告

意外的设备操作

- 请勿拆卸、修理或修改此设备。没有用户可维修的部件。
- 在适合其预期应用环境的外壳中安装和操作此设备。
- 为了保证正确运行，在投入使用前，必须对此设备的每次执行情况单独进行全面测试。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

具有相应资质的人员

只有经过适当培训且熟悉并理解本指南内容和所有其他相关产品文档的人员才有权使用本产品。

合格人员必须能够检测可能由于修改参数值而产生的危险，这通常来自机械、电气或电子设备。合格人员必须熟悉工业事故预防的标准、预防措施和规定，在设计和实施系统时必须遵守这些标准、预防措施和规定。

使用和应用本指南中包含的信息时需要掌握自动化控制系统的设计和编程方面的专业知识。只有您（用户、面板制造商或集成商）才能够了解在过程设备或机器的安装、设置、运行和维护期间出现的各条件和因素，因此能够确定相应的自动化及相关设备和相关安全装置和联锁装置，以便在为特定应用选择自动化和控制设备以及任何其他相关设备或软件时，能够有效、正确地使用这些设备和装置。此外，您必须考虑适用的当地、地区或国家标准和/或法规。

在使用本设备时，请特别注意遵守适用于您过程设备或机器的任何安全说明、电气要求和规范标准。

预期用途

本文档所述的产品，连同其软件、附件和选配件，是低压电气负载的启动器的一部分，设计用于工业用途，使用时应遵循本文档及其他辅助文档中的相关说明、指导、示例和安全说明。

本产品的使用必须符合一切适用的安全法律法规、指定的要求和技术参数。

在使用本产品之前，您必须对计划的应用进行风险评估。根据结果，必须采取适当的安全相关措施。

由于本产品应作为过程设备或机器的组成部分来使用，因此必须通过对整个系统的设计来确保人员安全。

本产品必须与规定的电缆和附件一同使用。务必使用原装附件和备件。

禁止用于除明确允许的用途之外的任何其他用途，否则可能导致意料之外的危害。

网络安全注意事项

⚠警告

系统可用性、完整性和保密性面临的潜在威胁

- 首次使用时，更改默认密码，以有助于防止擅自访问设备设置、控件和信息。
- 禁用未使用的端口/服务将有助于尽量减少恶意攻击的途径。
- 将联网设备布置在多层网络防御（例如防火墙、网络分段、网络入侵检测和保护）之后。
- 采用网络安全最佳实践（例如，最低权限、责任分离）来帮助阻止非法曝露、丢失、数据和日志修改、或服务中断。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

网络安全简介

此部分内容

介绍

网络安全作为流程、工具与技术、合规及治理体系的重要组成部分，旨在保护您的通信网络及所有联网设备免受攻击，此类攻击可能导致：运行中断（破坏可用性）、信息篡改（破坏完整性）或机密数据泄露（破坏机密性）。

网络安全的目的在于，提升信息和物理资产的保护级别，以免遭受盗窃、破坏、滥用或发生事故，同时保证其预期用户的访问和使用。网络安全涉及诸多方面，包括：设计安全系统、采用物理及数字手段限制访问、识别用户身份，以及实施安全控制/防护规程与最佳实践策略。

Schneider Electric 指南

除了本指南中针对 TeSys Tera system所给的具体建议之外，您还应遵循网络安全的 Schneider Electric 深度防御方法。

该方法在 推荐网络安全最佳实践进行了描述。

此外，Schneider Electric 网络安全支持门户, 44 页 中也提供了许多有用的资源和最新信息。

Schneider Electric 的网络安全策略

Schneider Electric 在控制系统的开发与实施中遵循行业最佳实践。这包括采用深度防御策略来保护工业控制系统。该策略将控制器置于一个或多个防火墙之后，以仅限制授权人员及协议的访问。

⚠警告

未认证访问及后续未授权操作

- 评估您的设备或整个环境是否连接到关键基础设施。如果是，在将自动化系统连接到任何网络之前，请根据深度防御采取适当的预防措施。
- 限制公司内部连接到网络的设备数量。
- 将您的工业网络与公司内部的其他网络隔离。
- 通过使用防火墙、VPN 或其他经过验证的安全措施，防止任何网络受到意外访问。
- 监视系统中的活动。
- 防止未经授权的人员或未经授权的行为直接访问或链接相关设备。
- 准备一个恢复计划，包括系统及过程信息的备份。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

安全威胁

网络威胁是指可破坏 PC 和 PC 网络正常操作的蓄意行为或意外行为。这些行为可在物理设施内或从外部位置发起。控制环境的安全挑战包括：

- 各种物理和逻辑界限
- 多个站点和较大的地理范围
- 对流程可用性安全实施的负面影响
- 随着业务控制的通讯越来越开放，从业务系统到控制系统的迁移越来越容易接触蠕虫和病毒
- 通过 USB 设备、供应商和服务专员的笔记本电脑以及企业网络越来越多地接触恶意软件
- 控制系统对物理和机械系统的直接影响

政策与规则

Schneider Electric 建立了 安全开发生命周期(SDL) 流程，这是一个基于产品开发的重要框架，有助于确保产品在寿命期的各个阶段中遵守安全设计流程。
Schneider Electric SDL流程符合 IEC 62443-4.1 标准。

SDL流程包括：

- 贯穿整个供应链且应用到内部开发操作中的 SDL 实践。
- 产品发行所需的最终安全审查。
- 产品开发相关人员的安全培训。

安全强化指南

简介

PC 可以运行各种应用程序，以增强控制环境中的安全。系统具有出厂默认设置，要求重新配置以与 Schneider Electric 的深度防御方法的设备加强建议保持一致。

下面的指南介绍了 Windows 操作系统中的流程。这些仅作为示例提供。您的操作系统和应用程序可能有不同的要求或操作流程。

禁用远程桌面协议

Schneider Electric 的深度防御方法建议包括禁用远程桌面协议 (RDP)，除非您的应用程序需要 RDP。

在 Windows 11 中，使用**设置 > 系统 > 远程桌面 > 禁用远程桌面**（切换到**关**），来禁用远程桌面协议 (RDP)。

更新安全策略

通过命令窗口中的 `gpupdate` 更新您系统中与 PC 相关的安全策略。有关详细信息，请参阅 `gpupdate` 上的 Microsoft 文档。

管理更新

部署前，使用 Microsoft **Windows 更新**网页上的实用程序，更新所有 PC 操作系统。要在 Windows 中访问此工具，请选择**开始 > 所有程序 > Windows 更新**。

工作站保护

为了降低与工程工作站相关的安全风险，请启用内存利用设置，比如数据执行预防（DEP）和地址空间布局随机化（ASLR）。这些安全设置可以通过使用 Windows 11 操作系统中的系统 Expoit Protection 设置来启用。有关详细信息，请参阅 Microsoft 安全功能网页。

强制使用安全密码

使用满足要求的强密码，包含大写字母、小写字母、数字和特殊字符。启用此功能可通过降低弱密码风险，有助于防止未经授权的访问。

使用非默认端口

更改协议（如 HTTPS、DWPS 和 Modbus TCP）的默认通信端口，可增加一层额外的安全性。

IP允许列表 (IP Allow List)

IP允许列表功能通过仅允许指定的IP地址，限制对系统的访问。这有助于防止未经授权的设备连接到系统，并确保只有受信任的来源能与系统通信。 TeSys Tera system. 要访问IP允许列表功能，请在标准Web服务器 (Standard Web Server)中导航至 **Security > IP Allow List > IP Allow List** 。

TeSys Tera系统信息

此部分内容

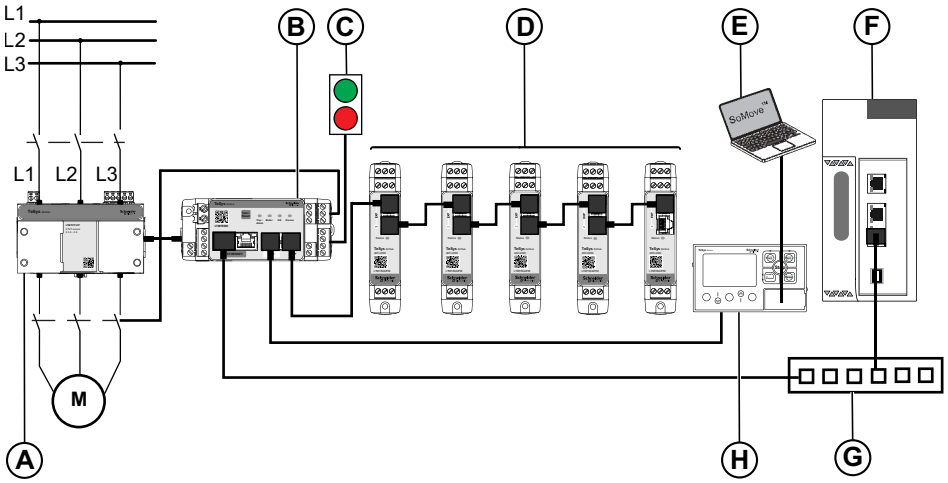
概述

TeSys Tera Motor Management System（或 TeSys Tera system)是 TeSys 智能继电器和电机启动器的Active系列产品的组成部分之一。TeSys Tera system 被设计作为智能电机控制中心 (iMCC) 的可靠基石，为单相或三相 AC 感应电机提供较完整的保护、测量、控制和监视功能。

TeSys Tera system 安装在低压开关设备系统中，通过现场总线网络和电机馈电器连接更高级别的自动化系统。

TeSys Tera system:

- 将iMCC 馈电器中的常规与高级电机保护、电量计量及监控功能，集成于单个易于配置的紧凑型通讯模块，并配备独立式人机界面HMI设备。
- 为低压接触器控制的电机启动器馈电器提供保护控制器。
- 为低压应用中的恒速电机提供灵活且模块化的电机管理系统。



A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C 启动/停止命令

D LTMT expansion modules

E 运行 SoMove FDT 容器软件且安装有 TeSys Tera DTM 的 PC

F 可编程逻辑控制器 (PLC) 或分布式控制系统 (DCS)

G Ethernet 交换机

H LTMTCUF control operator unit

通讯接口

TeSys Tera system通过以下类型的接口进行通讯：

LTMT main unit	型号	端口
Modbus RTU 	• LTMTMFM（100–240 Vac/ Vdc） • LTMTMBD（24 Vdc）	• Modbus RTU 带端子连接器的通讯端口 • 用于配置的Modbus RTU通讯 HMI 端口
PROFIBUS DP 	• LTMTPFM（100–240 Vac/ Vdc） • LTMTPBD（24 Vdc）	• PROFIBUS DP 带D9型连接器 • Profibus 带端子连接器端口 • Modbus RTU通讯HMI 端口

LTMT main unit	型号	端口
Modbus TCP/IP 	• LTMTEFM(100–240 Vac/Vdc) • LTMTEBD(24 Vdc)	• 两个 Ethernet 端口 Modbus TCP/IP • Modbus RTU带通讯HMI 端口
EtherNet/IP 	• LTMTEFM(100–240 Vac/Vdc) • LTMTEBD(24 Vdc)	• 两个 Ethernet 端口 EtherNet/IP • Modbus RTU带通讯HMI 端口

支持的协议

串行通讯设备

TeSys Tera system的Modbus RTU和PROFIBUS DP模块支持 Modbus RTU 和 PROFIBUS 协议，用于与现场总线设备通讯。

有关通讯协议及其对应的商业代码，请参见 通讯接口, 22 页章节。

以太网通讯设备

TeSys Tera system的Modbus TCP/IP 和 EtherNet/IP 模块支持以下协议：

- 通过配置工具及嵌入式网页实现的 HTTPS 协议
- Modbus TCP/IP 以及 EtherNet/IP 用于与现场总线设备通讯。
- DHCP，用于网络 IP 寻址
- DNS，用于网络名称解析
- NTP，用于时间同步
- DPWS用于设备发现

有关通讯协议及其对应的商业代码，请参见 通讯接口, 22 页章节。

安全特性

TeSys Tera system支持以下功能：

- 只能在 Schneider Electric 上安装经 TeSys Tera system 数字签名的固件。
- 每次启动时，固件的数字签名都会在执行前完成验证。
- 用户密码以安全方式存储（适用于 Ethernet 接口模块）。

  有关密码策略的更多信息，请参见 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- 可TeSys Tera system通过**Factory Default**设置选项TeSys Tera DTM或上**Test / Reset**按钮执行恢复出厂设置 LTMT main unit。

  Test / Reset 按钮的操作说明，请参阅 *TeSys Tera Motor Management System User Guide – DOCA0257EN*。
- TeSys Tera system 内置时钟，断电后仍可记忆日期和时间达12小时（适用于 Modbus RTU 和 PROFIBUS DP 型号，不适用于 Ethernet 模块）。
- 使用 TeSys Tera DTM，可选的PIN码管理功能支持启用/禁用配置访问权限及重置PIN码 TeSys Tera system。您还可以重置用于 TeSys Tera DTM 通过PIN管理功能重置密码。

  有关PIN管理功能的更多信息，请参阅 *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- 为确保 TeSys Tera system， LTMTCUF control operator unit 配备了PIN码功能。需输入六位数字PIN码方可访问。 LTMTCUF control operator unit

  有关维护PIN码功能的更多信息，请参阅 *TeSys Tera Motor Management System User Guide – DOCA0257EN*。

有关通讯协议及相关商业代码，请参阅 通讯接口, 22 页。

TeSys Tera系统特性

此部分内容

固件更新

将 TeSys Tera system 更新至最新固件版本，以便获得最新特性和安全补丁更新。为 TeSys Tera system 设计的所有固件均使用Schneider Electric公钥基础设施 (PKI) 进行签名，旨在确保运行于该设备上的固件的完整性和真实性。TeSys Tera system

有关通过TeSys Tera DTM进行固件更新的更多信息，请参见 *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*。

有关通过标准 Web 服务器（适用于Ethernet 接口模块）进行固件更新的更多信息，请参见 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*。

要获取有关安全更新的更多信息，请注册加入*Security Notifications*Schneider Electric网络安全支持门户。

日期与时间

为了避免错误，必须保持日期和时间同步。

以下步骤说明如何使用标准网页服务器或 TeSys Tera DTM: 更新Ethernet接口模块的日期和时间设置。

1. 导航至 **Settings > General > Date & Time**。
2. 使用 **Date & Time Selection** 下拉列表，选择以下选项之一：
   - **手动**

     注:

     - 当手动设置日期和时间时， LTMT main unit 设备将在重启时恢复出厂设置。
     - 日期和时间设置可通过以下方式手动更新： TeSys Tera DTM 或 LTMTCUF control operator unit.
   - **NTP**

     注: NTP 协议仅适用于 Ethernet 版本 LTMT main unit。

禁用未使用的端口/接口

通过关闭未主动使用的通信端口和接口，禁用未使用的端口/接口有助于减少系统的攻击面。

以下设置可TeSys Tera system 通过标准 Web 服务器禁用：

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

注: 有关更多信息，请参阅 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*。

端口

TeSys Tera system的Modbus TCP/IP和EtherNet/IP 模块 默认使用以下端口进行通信：

端口类型	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

该系统 TeSys Tera system 生成系统日志以记录诸如无效登录、固件更新等事件。日志中不包含任何个人信息。

为检测非预期行为（比如，频繁重启、不正确的固件更新、或无效登录），建议定期监控日志。

有关 *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* 日志的更多信息，请参阅 和 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*。

停用

TeSys Tera system 包含调试期间配置的敏感信息、实时运行数据及事件日志。

例如，此类信息可能涉及Modbus LTMT main unit 通信端口配置、功耗测量值等参数。

在废弃 TeSys Tera system 之前，必须执行出厂复位。

您可以通过以下方式重置TeSys Tera system:

- LTMT main unit上的**Test / Reset** 按钮：按住 **Test / Reset** 按钮 LTMT main unit 10秒钟。
- TeSys Tera DTM Library:有关详细信息，请参考 出厂重置 章节 *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unit:有关详细信息，请参考 命令菜单*TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*章节：

网络安全

此部分内容

注: 此部分仅适用于TeSys Tera system模块的Modbus TCP/IP 和 EtherNet/IP 。

介绍

TeSys Tera system系统非设计用于直接暴露于公共互联网环境。它必须至少安装在网络地址转换 (NAT) 防火墙之后，最好是在多重防火墙之后。如需了解更多信息，请参阅以下网页：

- *Schneider Electric* 网络安全咨询服务
- 美国国家标准与技术研究院 *(NIST)*
- 欧盟网络与信息安全局 *(ENISA)*

网络分段

TeSys Tera system 是一种在不同网络间建立桥接的网关设备。网络分段有助于确保网络防御。为增强网络分段能力，TeSys Tera system EtherNet/IP 版本LTMT main unit 配备了两个Ethernet以太网端口。可用Ethernet以太网端口可分别用于信息技术(IT)和运营技术(OT)。

HHTTPS 及 Modbus在所有TeSys Tera system Ethernet 接口(ETH1, ETH2)上均可用。

建议在未使用 Modbus TCP/IP 服务的网络上禁用 SNMP 服务。

产品 Web 服务器证书

为了支持 HTTPS安全通讯，TeSys Tera system 默认配备 X.509v3 证书。此证书有助于确保 HTTPS 通讯的完整性和保密性。

网络浏览器仅识别由第三方证书颁发机构（CA）签发的证书。该自签名证书是不安全的。建议将第三方CA签发的证书导入接口模块，TeSys Tera system同时应保持日期和时间同步。

该接口模块支持以下TeSys Tera system证书格式：

格式	页眉/页脚	密钥类型
PKCS#1	–––––RSA私钥开始–––––	仅限RSA
PKCS#8	–––––RSA私钥开始–––––	RSA、EC、DSA等
加密PKCS#8	–––––开始加密私钥–––––	任意

注: 修改过的测试证书是不可接受的。

有关第三方证书的更多详情，请参阅 *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*。

联网设备安全信息

建议定期检查与Ethernet的TeSys Tera system网络连接的一系列设备。如果发现连接了未知的设备，请将其找出并移除。您也可以重新构建网络，然后仅重新连接已识别的设备。

物理安防

安装

为了保护系统物理安全，建议采用以下安装方式：

- 将设备安装TeSys Tera system在防护外壳中，外壳的防护等级应与其安装现场的风险等级相适应（例如，配备挂锁或钥匙锁具的外壳）。
- 如果 TeSys Tera system 安装在配电盘上，那么请将配电盘安装在受保护的房间（例如，配有可锁上的门或摄像头）中。

维护期间的安全建议

此部分内容

维护操作

在 TeSys Tera system 的寿命期内，建议定期执行以下操作：

- 请确保设备运行的是最新版本固件。
- 请确认所有网络和安全补丁均已更新至最新版本。
- 遵循推荐的网络安全最佳实践。
- 对于异常行为，例如无效的登录尝试或频繁重启，请检查 Syslog, 31 页。
- 检查 日期与时间, 28 页，以免与当前日期存在偏差。
- 请遵循Schneider Electric为本设备制定的安全标准。

安全功能验证

此章节内容

Web 身份验证

注: 本主题仅适用于TeSys Tera system模块的Modbus TCP/IP 和 EtherNet/IP 。

要验证网页授权功能，请按以下步骤操作：

1. 尝试在不使用密码或者输入错误的密码的情况下登录到TeSys Tera system 标准网页。

   结果：TeSys Tera system 不授予您对标准网页服务器的访问权限。

2. 连续三次输入错误凭证后。

   结果：TeSys Tera system系统将锁定15分钟，之后才允许进行第四次尝试。

Web 授权

注: 本主题仅适用于 TeSys Tera system模块的Modbus TCP/IP 和 EtherNet/IP .

要验证网页授权功能，请按以下步骤操作：

1. 登录TeSys Tera system标准 Web服务器

   结果：登录后，您将获得数据和功能的完整访问权限。

2. 标记网页（例如，**Settings**）。
3. 在浏览器中打开私有导航窗口，然后打开标记的网页。

   结果：您无法访问该网页，但会被重定向至登录页面。

Syslog

要验证Syslog功能，请按以下步骤操作：

1. 在上述测试已部分或全部完成后，通过TeSys Tera DTM或网页服务器访问**Logs**网页。
2. 下载日志文件。
3. 确认日志中已记录已执行的测试或失败操作。

固件更新

要验证固件更新功能，请按以下步骤操作：

1. 导航至 **Firmware Update** 功能，该功能位于 TeSys Tera DTM 或标准网页服务器上。
2. 上传经过认证的固件更新文件。
3. 请等待固件验证完成。

   结果：LTMT main unit固件完成更新后，且新版固件详情已在TeSys Tera DTM更新后，才会触发系统重启。

禁用服务

注: 本主题仅适用于TeSys Tera system模块的 Modbus TCP/IP 和 EtherNet/IP 。

要验证禁用服务功能是否生效，请按以下步骤操作：

1. 使用标准 Web 服务器，导航至 **Security > IP Network List > Device Discover** 。
2. 禁用设备发现功能。
3. 将一台运行 Windows 操作系统 的 PC 连接到同一网络。
4. 在**Network**中，单击**File Explorer**。

   结果：TeSys Tera system 未被发现，因此，不会显示在网络中的设备列表中。

导航至 **Security > IP Network List** ，并遵循上述步骤验证以下禁用方法：

- Modbus TCP
- Modbus RTU

Schneider Electric Cybersecurity Support Portal

此部分内容

概述

Schneider Electric *Cybersecurity support portal* 系统阐述了Schneider Electric 其漏洞管理策略。

Schneider Electric 隐患管理策略旨在处理影响 Schneider Electric 产品和系统的网络安全隐患，从而为现有的解决方案、客户和环境提供有效保护。

Schneider Electric 与研发人员、网络应急响应小组 (CERT) 和资产所有人密切合作，确保及时提供准确信息，适时保护系统安全。

Schneider Electric 的企业产品 CERT (CPCERT) 负责管理并发出与影响产品和解决方案的隐患和漏洞有关的警示。

CPCERT 协调相关 CERT、独立研发人员、产品经理和所有受影响客户之间的沟通。

公共网络安全支持门户

Schneider Electric Cybersecurity support portal 提供以下信息：

- 涉及产品网络安全漏洞的信息
- 涉及网络安全事件的信息
- 关于一个可申报网络安全事件或漏洞的接口的信息

漏洞报告与管理

可以通过 Schneider Electric 网站来报告网络安全事件和潜在漏洞：报告漏洞。

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

www.se.com

由于各种标准、规范和设计不时变更，请索取对本出版物中给出的信息的确认。

DOCA0260ZH-00