TeSys Active

TeSys Tera Motor Management System

Guide de cybersécurité

TeSys propose des solutions innovantes et connectées pour les démarreurs de moteur

DOCA0260FR-00
11/2025

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Table des matières

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.

La présence de ce symbole sur une étiquette “Danger” ou “Avertissement” signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.

Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

⚠ DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

⚠ AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

⚠ ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

Remarque Importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

À propos du document

Objectif du document

Ce guide fournit des informations sur les aspects liés à la cybersécurité du système TeSys™ Tera afin d'aider les concepteurs et les opérateurs du système à promouvoir un environnement d'exploitation sécurisé pour le produit.

Ce guide explique comment sécuriser votre réseau de technologie opérationnel ou le réseau de votre entreprise Ethernet réseau.

NOTE: Dans ce guide, le terme **sécurité** fait référence à la cybersécurité.

Champ d'application

Ce document s'applique aux composants certifiés suivants du TeSys Tera system :

- LTMTEFM : LTMT main unit avec EtherNet/IP ou Modbus TCP/IP protocole, 100–240 Vac/Vdc
- LTMTEBD : LTMT main unit avec EtherNet/IP ou Modbus TCP/IP protocole, 24 Vdc
- LTMTMFM : LTMT main unit avec Modbus RTU le protocole, 100–240 Vac/Vdc
- LTMTMBD : LTMT main unit avec Modbus RTU le protocole, 24 Vdc
- LTMTPFM : LTMT main unit avec PROFIBUS DP le protocole, 100–240 Vac/Vdc
- LTMTPBD : LTMT main unit avec PROFIBUS DP le protocole, 24 Vdc

Informations relatives à la cybersécurité générale

Ces dernières années, le nombre croissant de machines en réseau et d'usines de production a entraîné une augmentation correspondante du potentiel de cybermenaces, telles que les accès non autorisés, les violations de données et les perturbations opérationnelles. Vous devez donc envisager toutes les mesures de cybersécurité possibles pour protéger les ressources et les systèmes contre de telles menaces.

Pour garantir la sécurité et la protection de vos produits Schneider Electric, il est dans votre intérêt d'appliquer les meilleures relatives à la cybersécurité telles que décrites dans le document Cybersecurity Best Practices.

Schneider Electric fournit des informations supplémentaires et une assistance :

- Abonnez-vous à la newsletter sur la sécurité de Schneider Electric.
- Consultez la page Web Cybersecurity Support Portal pour :
  - obtenir des notifications de sécurité.
  - signaler les vulnérabilités et incidents.
- Consultez la page Web Schneider Electric Cybersecurity and Data Protection Posture pour :
  - accéder à la position sur la cybersécurité.
  - en savoir plus sur la cybersécurité dans l'académie de cybersécurité.
  - découvrir les services de cybersécurité de Schneider Electric.

Données environnementales

Pour plus d'informations sur la conformité des produits avec les normes environnementales, reportez-vous à la documentation Schneider Electric Environmental Data Program.

Langues disponibles du document

Ce document est disponible dans les langues suivantes :

- Anglais
- Chinois
- Français
- Allemand
- Italien
- Coréen
- Espagnol

Document(s) à consulter

Titre du document	Description	Numéro de référence
TeSys Tera Motor Management System Catalogue	Le catalogue : • Décrit le TeSys Tera system • Contient les caractéristiques techniques de TeSys Tera	LVCATENTER
TeSys Tera Motor Management System Guide Utilisateur	Il s'agit du principal guide utilisateur qui présente l'ensemble de TeSys Tera system. Il décrit les fonctions essentielles des LTMT main units, LTMTCT/LTMTCTV Sensor Module, LTMT expansion modules et LTMTCUF control operator unit.	DOCA0257EN
TeSys Tera Motor Management System Guide D'installation	Ce guide décrit l'installation, la mise en service et l'entretien des produits LTMT main unit, LTMTCT/ LTMTCTV Sensor Module, LTMT expansion modules et LTMTCUF control operator unit.	DOCA0356EN
TeSys Tera Motor Management System DTM library Guide d'aide en ligne	Ce guide décrit la bibliothèque TeSys Tera DTM qui permet de personnaliser les fonctions de contrôle de TeSys Tera Motor Management System.	DOCA0275EN
TeSys Tera Motor Management System Modbus RTU Guide de Communication	Ce guide décrit la communication du protocole réseau Modbus de LTMT main unit.	DOCA0355EN
TeSys Tera Motor Management System PROFIBUS DP Guide de Communication	Ce guide décrit la communication du protocole de réseau PROFIBUS DP de LTMT main unit.	DOCA0256EN
TeSys Tera Motor Management System EtherNet/IP Guide de Communication	Ce guide décrit la EtherNet/IPcommunication du protocole réseau de LTMT main unit.	DOCA0258EN
TeSys Tera Motor Management System LTMTCUF control operator unit Guide Utilisateur	Ce guide décrit comment installer, configurer et utiliser LTMTCUF control operator unit.	DOCA0233EN
TeSys Tera Motor Management System DTM library Note de mise à jour logicielle	Ce document fournit des informations importantes sur TeSys Tera DTM Library et fournit un résumé des nouvelles fonctionnalités et améliorations.	DOCA0279EN
TeSys Tera Motor Management System Note de Publication du Micrologiciel	Ce document fournit des informations sur les versions des packages de micrologiciel du TeSys Tera system et récapitule les nouvelles fonctionnalités et les améliorations.	DOCA0276EN
Comment réduire la vulnérabilité aux cyberattaques ?	Ce guide décrit les risques liés à la cybersécurité et les stratégies de réduction dans les systèmes de contrôle et d'automatisation.	Comment réduire la vulnérabilité aux cyberattaques ?

Pour rechercher des documents en ligne, visitez le centre de téléchargement Schneider Electric (www.se.com/ww/en/download/).

Informations concernant la terminologie inclusive/sensible

Schneider Electric s'efforce de mettre constamment à jour ses communications et ses produits pour respecter ses engagements en matière de terminologie inclusive/sensible. Il se peut malgré tout que nos contenus présentent encore des termes jugés inappropriés par certains clients.

Les marques

QR Code est une marque déposée de DENSO WAVE INCORPORATED au Japon et dans d'autres pays.

Précautions

Lisez attentivement les précautions suivantes avant d'effectuer les procédures décrites dans ce guide.

⚠⚠DANGER

RISQUE DE CHOC ÉLECTRIQUE, D'EXPLOSION OU D'ARC ÉLECTRIQUE

- L'installation et l'entretien de cet équipement doivent être effectués par du personnel qualifié.
- Coupez toutes les alimentations de cet équipement avant de travailler sur ou dans celui-ci.
- Utilisez uniquement la tension indiquée pour faire fonctionner cet équipement et les produits associés.
- Utilisez toujours un tensiomètre correctement réglé pour vous assurer que l'alimentation est coupée.
- Utilisez les verrouillages appropriés dès lors qu'il existe des risques pour le personnel et/ou pour l'équipement.
- Les circuits d'alimentation doivent être câblés et protégés conformément aux réglementations locales et nationales.
- Portez un équipement de protection individuelle (EPI) adapté et respectez les normes de sécurité en vigueur pour les travaux électriques (normes NFPA 70E, NOM-029-STPS ou CAN/CSA Z462 ou équivalentes).

Le non-respect de ces instructions provoquera la mort ou des blessures graves.

⚠AVERTISSEMENT

FONCTIONNEMENT INATTENDU DE L'ÉQUIPEMENT

- Vous ne devez en aucun cas démonter, réparer ni modifier cet équipement. Il ne comprend aucune pièce remplaçable par l'utilisateur.
- Installez et utilisez cet équipement dans une armoire adaptée à l'environnement prévu de l'application.
- Chaque mise en oeuvre de cet équipement doit être individuellement et rigoureusement testée quant à son bon fonctionnement avant toute mise en service.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Personnel qualifié

Seules les personnes dûment formées, familiarisées avec le contenu du présent guide et de toute autre documentation relative au produit, et en ayant compris le contenu, sont autorisées à travailler sur et avec ce produit.

La personne qualifiée doit être en mesure de détecter les dangers possibles afférents à la modification des valeurs de paramètres et, plus généralement, au fonctionnement des équipements mécaniques, électriques et électroniques. La personne qualifiée doit être familiarisée avec les normes, dispositions et règlements concernant la prévention des accidents industriels, et doit les observer lors de la conception et de la mise en oeuvre du système.

L'utilisation et l'application des informations contenues dans ce manuel exigent une connaissance experte de la conception et de la programmation des systèmes de contrôle automatisés. Seul vous - utilisateur, tableautier ou intégrateur - pouvez connaître toutes les conditions et tous les facteurs présents lors de l'installation, de la configuration, de l'exploitation et de l'entretien d'une usine ou d'une machine. Par conséquent, au moment de sélectionner l'équipement d'automatisme et de

contrôle et les équipements et logiciels connexes pour une application particulière, vous êtes la seule personne à pouvoir déterminer les équipements, les sécurités et les verrous qui peuvent être utilisés efficacement et sans danger. Vous devez également tenir compte des normes, lois et réglementations en vigueur au niveau local, régional et national.

Une attention particulière doit être apportée au respect des informations de sécurité, des exigences électriques et des normes qui s'appliquent à l'usine ou à la machine dans le cadre de l'utilisation de cet équipement.

Utilisation prévue

Les produits décrits dans ce guide, ainsi que les logiciels, accessoires et options, font partie des démarreurs pour charges électriques basse tension qui sont destinés à une utilisation industrielle conformément aux instructions, consignes, exemples et informations de sécurité contenus dans le présent document ou d'autres documentations connexes.

Le produit doit être utilisé dans le respect de toutes les directives et réglementations de sécurité applicables, des exigences spécifiées et des données techniques fournies.

Avant d'utiliser le produit, vous devez effectuer une évaluation des risques pour l'application envisagée. En fonction des résultats obtenus, les mesures de sécurité appropriées devront être mises en oeuvre.

Étant donné que le produit est utilisé comme composant d'une installation ou d'une machine de traitement, vous devez garantir la sécurité des personnes grâce à la conception globale du système.

N'utilisez le produit qu'avec les câbles et accessoires spécifiés. N'employez que des accessoires et des pièces de rechange authentiques.

Toute utilisation autre que celle explicitement autorisée est interdite et peut entraîner des risques imprévus.

Avis sur la Cybersécurité

⚠AVERTISSEMENT

RISQUES POUVANT ALTÉRER LA DISPONIBILITÉ, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DU SYSTÈME

- Modifiez les mots de passe par défaut à la première utilisation afin d'empêcher tout accès non autorisé aux paramètres, contrôles et informations de l'équipement.
- Désactivez les ports/services inutilisés pour réduire le risque d'attaques malveillantes.
- Protégez les périphériques en réseau par plusieurs niveaux de cyberdéfense (pare-feux, segmentation du réseau, détection des intrusions et protection du réseau).
- Respectez les bonnes pratiques de cybersécurité (par exemple : moindre privilège, séparation des tâches) afin de réduire les risques d'intrusion, la perte ou l'altération des données et journaux, ou l'interruption des services.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Initiation à la Cybersécurité

Contenu de cette partie

Introduction

La cybersécurité, qui fait partie intégrante des processus, des outils et des technologies, de la conformité et de la gouvernance, vise à protéger votre réseau de communication et tous les périphériques connectés contre les attaques susceptibles de perturber les opérations (disponibilité), d’altérer les informations (intégrité) ou d’exposer des données confidentielles (confidentialité).

Son objectif consiste à augmenter les niveaux de protection des informations et des actifs physiques contre le vol, la corruption, l'utilisation abusive ou les accidents, tout en maintenant l'accès pour les utilisateurs cibles. La cybersécurité comporte de nombreux aspects, notamment la conception de systèmes sécurisés, la restriction de l’accès à l’aide de méthodes physiques et numériques, l’identification des utilisateurs, ainsi que la mise en œuvre de procédures de contrôle/mesure de la sécurité et de politiques de bonnes pratiques.

Consignes Schneider Electric

En plus des recommandations fournies dans ce guide spécifiques à TeSys Tera system, vous devez suivre l'Schneider Electric approche de la cybersécurité basée sur la défense en profondeur.

Cette approche est décrite dans les *Recommandations sur les meilleures pratiques en matière de cybersécurité*.

De plus, vous trouverez de nombreuses ressources utiles et des informations mises à jour sur le Portail d’assistance à la cybersécurité de Schneider Electric, page 44.

Approche de Schneider Electric en matière de cybersécurité

Schneider Electric adhère aux bonnes pratiques du secteur en matière de développement et de mise en œuvre des systèmes de contrôle. Cela inclut une approche de défense en profondeur pour sécuriser un système de commande industriel. Cette approche consiste à placer les contrôleurs derrière un ou plusieurs pare-feux de façon à limiter l'accès au personnel et aux protocoles autorisés uniquement.

⚠ AVERTISSEMENT

ACCÈS NON AUTHENTIFIÉ ET FONCTIONNEMENT NON AUTORISÉ EN DÉCOULANT

- Évaluez si votre équipement ou l'intégralité de votre environnement sont connectés à votre infrastructure critique. Si tel est le cas, prenez les mesures de prévention appropriées, fondées sur une défense en profondeur, avant de connecter le système d'automatisation à un réseau.
- Limitez le nombre de périphériques connectés à un réseau au sein de votre entreprise.
- Isolez votre réseau industriel des autres réseaux dans votre entreprise.
- Protégez tout réseau contre les accès non autorisés, en utilisant des pare-feux, des VPN ou autres mesures de sécurité éprouvées.
- Surveillez les activités dans vos systèmes.
- Veillez à empêcher tout accès ou lien direct aux périphériques en question de la part de parties non autorisées, ainsi que toute action non authentifiée.
- Préparez un plan de reprise incluant la sauvegarde de votre système et les informations des processus.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Menaces de sécurité

Les cybermenaces désignent des actions volontaires ou non, susceptibles de perturber le fonctionnement normal des PC et des réseaux de PC. Ces actions peuvent être déclenchées dans les locaux ou à l'extérieur du site. Les défis de l'environnement de contrôle en matière de sécurité sont les suivants :

- Diversité des limites physiques et logiques
- Multiplicité des sites et ampleur des zones géographiques
- Effets négatifs de la sécurité sur la disponibilité des processus
- Vulnérabilité accrue aux vers et virus qui contaminent les systèmes de contrôle à partir des systèmes commerciaux, à mesure que les communications entre ces systèmes s'ouvrent
- Vulnérabilité accrue aux logiciels malveillants provenant de périphériques USB, des ordinateurs portables de fournisseurs et de techniciens d'entretien, et du réseau de l'entreprise
- Impact direct des systèmes de contrôle sur les systèmes physiques et mécaniques

Politiques et Règles

Schneider Electric dispose d'un processus de cycle de vie de développement sécurisé (SDL), un cadre clé basé sur le développement de produits qui permet de garantir que les produits suivent des processus de conception sécurisés à toutes les étapes de leur cycle de vie. Le processus SDL de Schneider Electric est conforme aux IEC 62443-4.1 normes.

Le processus SDL comprend :

- Les pratiques SDL sont appliquées aux actions de développement interne tout au long de la chaîne d'approvisionnement.
- Examen de sécurité final obligatoire avant le lancement des produits.
- Formation en sécurité du personnel participant au développement des produits.

Informations relatives au renforcement de la sécurité

Introduction

Votre PC peut exécuter de nombreuses applications pour améliorer la sécurité dans votre environnement de contrôle. Les paramètres par défaut du système doivent être reconfigurés en fonction des recommandations de Schneider Electric concernant le renforcement de la protection des équipements.

Les instructions suivantes décrivent les procédures relatives à Windows. Elles sont fournies à titre d'exemple. Les exigences ou procédures de votre système d'exploitation et de votre application peuvent être différentes.

Désactivation du protocole de bureau à distance

Les recommandations de Schneider Electric en matière de défense en profondeur incluent la désactivation du protocole Bureau à distance (RDP - Remote Desktop Protocol), sauf si votre application nécessite RDP.

Sous Windows 11, le protocole RDP peut être désactivé via **Paramètres > Système > Bureau à distance > Activer le bureau à distance** (sélectionnez **Désactiver**).

Mise à jour des stratégies de sécurité

Mettez à jour les stratégies de sécurité sur les PC de votre système en exécutant `gpupdate` dans une fenêtre de commandes. Pour plus d'informations, consultez la documentation Microsoft sur `gpupdate`.

Gestion des mises à jour

Avant le déploiement, mettez à jour tous les systèmes d'exploitation des PC à l'aide des utilitaires disponibles sur le site Web **Windows Update** de Microsoft. Pour accéder à cet outil dans Windows, sélectionnez **Start > All Programs > Windows Update**.

Protection de la station de travail

Pour réduire les risques de sécurité associés à la station de travail d'ingénierie, activez les paramètres mémoire tels que Data Execution Prevention (DEP) et Address Space Layout Randomization (ASLR). Ces paramètres de sécurité peuvent être activés à l'aide des paramètres de protection contre les exploits du système dans le système d'exploitation Windows 11. Pour plus d'informations, consultez la page Web sur Microsoft security features.

Appliquer des mots de passe sécurisés

Utilisez des mots de passe forts qui répondent aux critères requis, tels que des lettres majuscules, des lettres minuscules, des chiffres et des caractères

spéciaux. L'activation de cette fonctionnalité permet d'empêcher tout accès non autorisé en réduisant le risque lié aux mots de passe faibles.

Utilisation de ports non par défaut

La modification des ports de communication par défaut pour les protocoles tels que HTTPS, DWPS et Modbus TCP ajoute un niveau de sécurité supplémentaire.

Liste blanche d'adresses IP

La fonctionnalité de liste blanche d'adresses IP restreint l'accès au système en n'autorisant que les adresses IP spécifiées. Cela permet d'empêcher les appareils non autorisés de se connecter au système et garantit que seules les sources fiables peuvent communiquer avec le TeSys Tera system. Pour accéder à la fonctionnalité de liste blanche d'adresses IP, allez sur **Security > IP Allow List > IP Allow List** dans le serveur Web standard.

Informations sur le système TeSys Tera

Contenu de cette partie

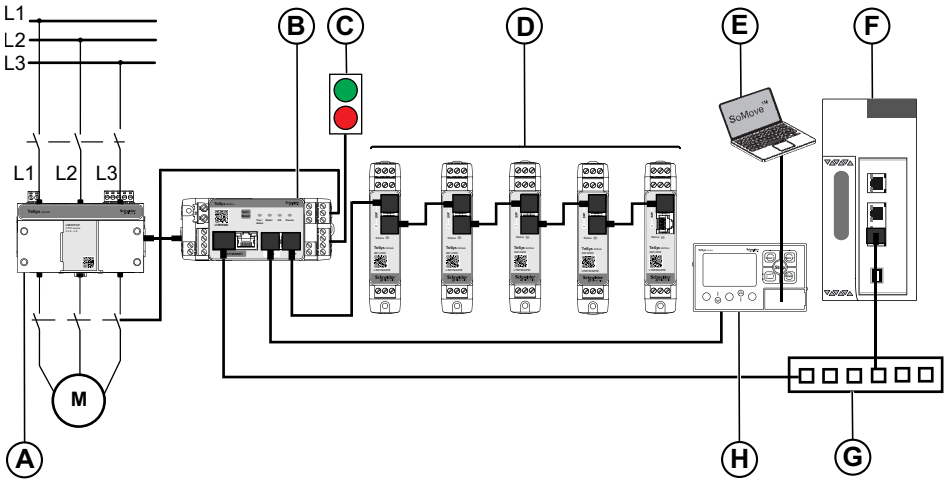
Présentation

Le TeSys Tera Motor Management System (ou TeSys Tera system) fait partie de la TeSys gamme active de relais intelligents et de démarreurs de moteur. Le TeSys Tera system est conçu comme un composant fiable pour les centres de contrôle moteur intelligents (iMCC) afin d'offrir des capacités complètes de protection, de mesure, de commande et de surveillance pour les moteurs à induction AC monophasés ou triphasés.

Le TeSys Tera system est installé dans l'appareillage basse tension et connecte le système d'automatisation de niveau supérieur via le réseau de bus de terrain et le départ moteur.

TeSys Tera system:

- Couvre la protection, le comptage et la surveillance conventionnels et avancés des moteurs dans les alimentations iMCC dans un module de communication compact, facile à configurer et autonome avec un dispositif HMI autonome.
- Fournit un contrôleur de protection pour les départs moteur commandés par contacteurs basse tension.
- Offre un système de gestion moteur flexible et modulaire pour les moteurs à vitesse constante dans les applications basse tension.



A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C Commandes de démarrage/arrêt

D LTMT expansion modules

E PC exécutant SoMove un conteneur FDT avec TeSys Tera DTM installé

F Automate programmable (PLC) ou système de contrôle distribué (DCS)

G Ethernet Commutateur

H LTMTCUF control operator unit

Interfaces de communication

TeSys Tera system communique via les types d'interface suivants :

LTMT main unit	Référence	Ports
Modbus RTU 	• LTMTMFM (100–240 Vac/ Vdc) • LTMTMBD (24 Vdc)	• Modbus RTU port de communication avec connecteur de borne • Port HMI avec Modbus RTU communication pour la configuration
PROFIBUS DP 	• LTMTPFM (100–240 Vac/Vdc) • LTMTPBD (24 Vdc)	• PROFIBUS DP avec connecteur sub D9 • Profibus port avec connecteur de borne • Port HMI avec Modbus RTU communication

LTMT main unit	Référence	Ports
Modbus TCP/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Deux Ethernet ports avec Modbus TCP/IP • Port HMI avec Modbus RTU communication
EtherNet/IP 	• LTMTEFM (100–240 Vac/Vdc) • LTMTEBD (24 Vdc)	• Deux Ethernet ports avec EtherNet/IP • Port HMI avec Modbus RTU communication

Protocoles pris en charge

Périphériques de communication série

Le Modbus RTU et PROFIBUS DP modules du TeSys Tera system support Modbus RTU et PROFIBUS protocole de communication avec les périphériques de bus de terrain.

Pour les protocoles de communication et les références commerciales correspondantes, consultez les Interfaces de communication, page 22.

Périphériques de Communication Ethernet

Le Modbus TCP/IP et EtherNet/IP modules du TeSys Tera system prennent en charge les protocoles suivants :

- HTTPS via des outils de configuration et des pages Web intégrées
- Modbus TCP/IP et EtherNet/IP pour les communications avec les périphériques de bus de terrain
- DHCP pour l'adressage IP du réseau
- DNS pour la résolution de nom réseau
- NTP pour la synchronisation horaire
- DPWS pour la découverte des périphériques

Pour les protocoles de communication et les références commerciales correspondantes, consultez les Interfaces de communication, page 22.

Fonctionnalités de Sécurité

Le TeSys Tera system prend en charge les fonctionnalités suivantes :

- Le micrologiciel signé numériquement par Schneider Electric ne peut être installé que sur TeSys Tera system.
- À chaque démarrage, la signature numérique du micrologiciel est validée avant l'exécution.
- Les mots de passe des utilisateurs sont stockés de manière sécurisée (applicable aux Ethernet modules d'interface).

  Pour plus d'informations sur la politique relative aux mots de passe, consultez *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- Vous pouvez réinitialiser les paramètres d'usine du TeSys Tera system en utilisant **Factory Default** à l'aide du TeSys Tera DTM ou le **bouton Test / Reset** sur LTMT main unit.

  Pour plus d'informations sur le **bouton Test / Reset** , consultez*TeSys Tera Motor Management System User Guide – DOCA0257EN*.
- L' TeSys Tera system dispose d'une horloge interne et mémorise la date et l'heure pendant 12 heures sans alimentation (valable pour Modbus RTU et PROFIBUS DP et non applicable pour le Ethernet module).
- En utilisant TeSys Tera DTM, la fonctionnalité optionnelle de gestion des broches vous permet d'activer ou de désactiver la configuration du TeSys Tera system. Vous pouvez également réinitialiser le code pin pour TeSys Tera DTM en utilisant la fonctionnalité de gestion du code pin.

  Pour plus d'informations sur la fonctionnalité de gestion des broches, consultez*TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- Pour garantir la TeSys Tera system, le LTMTCUF control operator unit est équipé d'une fonctionnalité de verrouillage. Vous devez disposer d'un code pin à six chiffres pour accéder au LTMTCUF control operator unit.

  Pour plus d'informations sur la fonctionnalité des broches, consultez*TeSys Tera Motor Management System User Guide – DOCA0257EN*.

Pour les protocoles de communication et les références commerciales correspondantes, consultez les Interfaces de communication, page 22.

Caractéristiques du système TeSys Tera

Contenu de cette partie

Mise à jour du micrologiciel

Mettez à jour l'TeSys Tera system vers la dernière version du micrologiciel pour bénéficier des fonctions et correctifs de sécurité les plus récents. Tous les micrologiciels conçus pour le TeSys Tera system est signé à l'aide de l'infrastructure à clé publique (PKI) de Schneider Electric afin de garantir l'intégrité et l'authenticité du micrologiciel exécuté sur le TeSys Tera system.

Pour plus d'informations sur la mise à jour du micrologiciel via TeSys Tera DTM, consultez *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.

Pour plus d'informations sur la mise à jour du micrologiciel via le serveur Web standard (applicable aux Ethernet modules d'interface), consultez la section *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Pour en savoir plus sur les mises à jour de sécurité, inscrivez-vous sur le *Security Notifications* sur le portail d'assistance cybersécurité de Schneider Electric.

Date et heure

Il est important de synchroniser la date et l'heure pour éviter les erreurs.

La procédure suivante explique comment mettre à jour les paramètres de date et de l'heure pour les Ethernet modules d'interface à l'aide d'un serveur Web standard ou TeSys Tera DTM :

1. Accédez à **Settings > General > Date & Time**.
2. Utilisation de la **Date & Time Selection**, sélectionnez l'une des options suivantes :
   - **Manuel**

     NOTE:

     - Lorsque la date et l'heure sont réglées manuellement, le LTMT main unit réinitialise les paramètres d'usine au redémarrage.
     - Les paramètres de date et d'heure peuvent être mis à jour manuellement à l'aide du TeSys Tera DTM ou le LTMTCUF control operator unit.
   - **NTP**

     NOTE: Le protocole NTP n'est disponible que pour les Ethernet versions du LTMT main unit.

Désactiver les ports/interfaces inutilisés

La désactivation des ports/interfaces inutilisés permet de réduire la surface d'attaque du système en désactivant les ports de communication et les interfaces qui ne sont pas activement utilisés.

Les paramètres suivants du TeSys Tera system peuvent être désactivés à l'aide du serveur Web standard :

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

NOTE: Pour plus d'informations, consultez la section *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*

Ports

Le Modbus TCP/IP et EtherNet/IP modules du TeSys Tera system utilisent par défaut les ports suivants pour la communication :

Type de 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

Le TeSys Tera system génère des journaux système pour enregistrer des événements tels que les tentatives de connexion non valides et les mises à jour du micrologiciel. Les journaux ne contiennent aucune information personnelle.

Il est recommandé de surveiller régulièrement les journaux pour détecter les comportements inattendus (par exemple, redémarrages fréquents, mise à jour incorrecte du micrologiciel ou tentatives de connexion non valides).

Pour plus d'informations sur les journaux, consultez *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* et *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Mise hors service

Le TeSys Tera system contient des informations confidentielles configurées lors de la mise en service, les valeurs récentes des données et les journaux.

Par exemple, ces informations peuvent inclure Modbus LTMT main unit ou les consommations électriques mesurées.

Rétablissez les paramètres d'usine avant de mettre au rebut l'TeSys Tera system

Vous pouvez utiliser les méthodes suivantes pour réinitialiser le TeSys Tera system:

- Bouton **Test / Reset** sur le LTMT main unit: Appuyez et maintenez enfoncé le bouton **Test / Reset** sur le LTMT main unit pendant 10 secondes.
- TeSys Tera DTM Library: Pour plus d'informations, consultez la section *Réinitialisation d'usine* dans le *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unitPour plus d'informations, consultez la section *Menu de commande* dans le *TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*

Sécurité du réseau

Contenu de cette partie

NOTE: Cette partie n’est valable que pour Modbus TCP/IP et EtherNet/IP modules du TeSys Tera system.

Introduction

Le TeSys Tera system n’est pas conçu pour résister à une exposition directe à l’Internet public. Il doit être installé au moins derrière un système de traduction d’adresses réseau (NAT) ou, de préférence, derrière plusieurs pare-feux. Pour plus d’informations, consultez les pages Web suivantes :

- *Services de conseil en cybersécurité Schneider Electric*
- *National Institute of Standards and Technology (NIST)*
- *European Union Agency for Cybersecurity (ENISA)*

Segmentation réseau

Le TeSys Tera system est une porte qui crée un pont entre différents réseaux. La segmentation du réseau garantit la cyberdéfense. Pour améliorer la segmentation du réseau, la TeSys Tera system EtherNet/IP version LTMT main unit dispose de deux Ethernet ports. Les Ethernet ports disponibles peuvent être utilisés pour les technologies de l'information (IT) et les technologies opérationnelles (OT).

HTTPS et Modbus sont disponibles sur TeSys Tera system Ethernet interfaces (ETH1, ETH2).

Il est recommandé de désactiver le Modbus TCP/IP service sur les réseaux où il n'est pas utilisé.

Certificat de serveur Web du produit

Pour prendre en charge les communications HTTPS sécurisées, le TeSys Tera system est équipé d'un X.509v3 certificat par défaut. Ce certificat assure l'intégrité et la confidentialité des communications HTTPS.

Les navigateurs Web ne reconnaissent que les certificats signés par une autorité de certification (CA) tierce. Le certificat auto-signé n'est pas sécurisé. Il est recommandé d'importer un certificat signé par une CA tierce dans le TeSys Tera system et de synchroniser la date et l'heure.

Les formats de certificats suivants sont pris en charge par le TeSys Tera system:

Format	En-tête/Pied de page	Type de clé
PKCS#1	– – – – –DÉMARRAGE DE LA CLÉ PRIVÉE RSA– – – – –	RSA uniquement
PKCS#8	– – – – – DÉMARRAGE DE LA CLÉ PRIVÉE – – – – –	RSA, EC, DSA, etc.
PKCS#8 chiffré	– – – – – DÉMARRAGE DE LA CLÉ PRIVÉE CHIFFREÉE – – – – –	N'importe laquelle

NOTE: Les certificats de test modifiés ne sont pas acceptables.

Pour plus d'informations sur le certificat tiers, consultez *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Informations de sécurité sur les périphériques connectés

Il est recommandé de vérifier régulièrement la liste des périphériques connectés au Ethernet réseau de la TeSys Tera system. En cas de périphérique connecté inconnu, localisez-le et supprimez-le. Vous pouvez également reconstruire le réseau et reconnecter uniquement les périphériques identifiés.

Sécurité physique

Installation

Il est recommandé de procéder à l'installation suivante pour de protéger la sécurité physique des systèmes :

- Installez le TeSys Tera system dans un boîtier sécurisé de manière appropriée au niveau de risque de votre installation (par exemple, un boîtier avec un cadenas ou une clé).
- Si le TeSys Tera system est monté sur un tableau électrique, installez ce dernier dans un local sécurisé (par exemple, avec une porte verrouillée ou une caméra).

Recommandations de sécurité pendant l’entretien

Contenu de cette partie

Opérations d’entretien

Il est recommandé de réaliser régulièrement les opérations suivantes pendant toute la durée de vie de l'TeSys Tera system :

- Assurez-vous que le périphérique utilise la dernière version du micrologiciel.
- Vérifiez que tous les correctifs réseau et de sécurité sont à jour.
- Suivez les meilleures pratiques recommandées en matière de cybersécurité.
- Pour les comportements inattendus tels que les tentatives de connexion invalides ou les redémarrages fréquents, vérifiez le Syslog, page 31.
- Pour éviter de vous éloigner de la date courante, vérifiez le Date et heure, page 28.
- Respectez les normes de sécurité recommandées par Schneider Electric pour le périphérique.

Vérification de la fonctionnalité de sécurité

Contenu de ce chapitre

Authentification Web

NOTE: Ce sujet n'est valable que pour Modbus TCP/IP et EtherNet/IP modules du TeSys Tera system.

Pour vérifier le fonctionnement de l'authentification Web, procédez comme suit :

1. Essayez de vous connecter au serveur web standard du TeSys Tera system sans mot de passe ou entrez un mot de passe incorrect.

   Résultat : Le TeSys Tera system ne vous donne pas accès au serveur web standard.

2. Entrez les informations d'identification incorrectes à trois reprises.

   Résultat : Le TeSys Tera system verrouille pendant 15 minutes avant de vous permettre d'essayer pour la quatrième fois.

Autorisation Web

NOTE: Ce sujet n'est valable que pour Modbus TCP/IP et EtherNet/IP modules du TeSys Tera system.

Pour vérifier le fonctionnement de l'autorisation Web, procédez comme suit :

1. Connectez-vous au TeSys Tera system serveur Web standard.

   Résultat : Une fois connecté, vous avez un accès complet aux données et aux fonctionnalités.

2. Ajoutez une page Web aux favoris (par exemple, **Settings**).
3. Ouvrez une fenêtre de navigation privée dans votre navigateur et ouvrez la page Web enregistrée dans vos favoris.

   Résultat : Vous ne pouvez pas accéder à la page Web, mais vous êtes redirigé vers la page de connexion.

Syslog

Pour vérifier le fonctionnement de Syslog, procédez comme suit :

1. Après avoir effectué une partie ou tous les tests précédents, à l'aide du TeSys Tera DTM ou du serveur web standard, accédez aux **Logs**.
2. Téléchargez les fichiers journaux.
3. Vérifiez que le test effectué ou les tentatives infructueuses sont consignés dans les journaux.

Mise à jour du micrologiciel

Pour vérifier le bon fonctionnement de la mise à jour du micrologiciel, procédez comme suit :

1. Accédez à la section **Firmware Update** sur le TeSys Tera DTM ou le serveur Web standard.
2. Téléchargez un fichier de mise à jour du micrologiciel authentifié.
3. Attendez que le micrologiciel soit validé.

   Résultat : Le redémarrage du système n'a lieu que lorsque le micrologiciel du LTMT main unit est mis à jour et que les détails du nouveau micrologiciel sont mis à jour dans le TeSys Tera DTM.

Désactivation des services

NOTE: Ce sujet n'est valable que pour Modbus TCP/IP et EtherNet/IP modules du TeSys Tera system.

Pour vérifier la fonctionnalité de désactivation des services, procédez comme suit :

1. Entrez dans **Security > IP Network List > Device Discovery** à l'aide du serveur Web standard.
2. Désactivez la détection des périphériques.
3. Connectez un PC équipé d'un Windows système d'exploitation au même réseau.
4. Cliquez **Network** dans l' **File Explorer**.

   Résultat : Le TeSys Tera system n'est pas détecté, il n'apparaît donc pas dans la liste des périphériques du réseau.

Accédez à **Security > IP Network List** et suivez la procédure ci-dessus pour vérifier les méthodes de désactivation suivantes :

- Modbus TCP
- Modbus RTU

Portail d’assistance à la cybersécurité de Schneider Electric

Contenu de cette partie

Présentation

Le Schneider Electric *Cybersecurity support portal* décrit la Schneider Electric politique de gestion des vulnérabilités.

L'objectif de la politique de gestion des vulnérabilités de Schneider Electric est de gérer les vulnérabilités qui ont un impact sur les produits et systèmes Schneider Electric, afin de protéger les solutions installées, les clients et l'environnement.

Schneider Electric travaille en collaboration avec des chercheurs, des équipes d'intervention en cas d'urgence cybernétique (CERT) et des propriétaires d'actifs afin de garantir que des informations précises soient fournies en temps opportun pour protéger adéquatement leurs installations.

Schneider ElectricLe CERT (CPCERT) de l'entreprise est chargé de gérer et d'émettre des alertes sur les vulnérabilités et les mesures d'atténuation affectant les produits et les solutions.

Le CPCERT coordonne la communication avec les équipes CERT compétentes, les chercheurs indépendants, les chefs de produit et tous les clients concernés.

Portail d’assistance en Matière de Cybersécurité

Le Schneider Electric Cybersecurity support portal fournit les informations suivantes :

- À propos des vulnérabilités des produits en matière de cybersécurité
- À propos des incidents liés à la cybersécurité
- À propos d’une interface qui vous permet de signaler des incidents ou des vulnérabilités liés à la cybersécurité

Signalement et gestion des vulnérabilités

Les incidents liés à la cybersécurité et les vulnérabilités potentielles peuvent être signalés via le site Web de Schneider Electric : Report a Vulnerability.

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

www.se.com

DOCA0260FR-00