# TeSys Active

## TeSys Tera Motor Management System

## Guía de Ciberseguridad

**TeSys ofrece soluciones innovadoras y conectadas para arrancadores de motor**

**DOCA0260ES-00**
**11/2025**

# Información legal

La información proporcionada en este documento contiene descripciones generales, características técnicas o recomendaciones relacionadas con productos o soluciones.

Este documento no pretende sustituir a un estudio detallado o un plan de desarrollo o esquemático específico de operaciones o sitios. No debe usarse para determinar la adecuación o la fiabilidad de los productos o las soluciones para aplicaciones de usuario específicas. Es responsabilidad del usuario realizar o solicitar a un experto profesional (integrador, especificador, etc.) que realice análisis de riesgos, evaluación y pruebas adecuados y completos de los productos o las soluciones con respecto a la aplicación o el uso específicos de dichos productos o dichas soluciones.

La marca Schneider Electric y cualquier otra marca comercial de Schneider Electric SE y sus filiales mencionadas en este documento son propiedad de Schneider Electric SE o sus filiales. Todas las otras marcas pueden ser marcas comerciales de sus respectivos propietarios.



Schneider Electric se reserva el derecho de realizar cambios o actualizaciones con respecto a o en el contenido de este documento o con respecto a o en el formato de dicho documento en cualquier momento sin previo aviso.

**En la medida permitida por la ley aplicable, Schneider Electric y sus filiales no asumen ninguna responsabilidad u obligación por cualquier error u omisión en el contenido informativo de este documento o por el uso no previsto o el mal uso del contenido de dicho documento.**

# Tabla de contenido

# Información de seguridad

## Información importante

Lea atentamente estas instrucciones y observe el equipo para familiarizarse con el dispositivo antes de instalarlo, utilizarlo, revisarlo o realizar su mantenimiento. Los mensajes especiales que se ofrecen a continuación pueden aparecer a lo largo de la documentación o en el equipo para advertir de peligros potenciales, o para ofrecer información que aclara o simplifica los distintos procedimientos.

La inclusión de este icono en una etiqueta “Peligro” o “Advertencia” indica que existe un riesgo de descarga eléctrica, que puede provocar lesiones si no se siguen las instrucciones.

Éste es el icono de alerta de seguridad. Se utiliza para advertir de posibles riesgos de lesiones. Observe todos los mensajes que siguen a este icono para evitar posibles lesiones o incluso la muerte.

**⚠ PELIGRO**

**PELIGRO** indica una situación de peligro que, si no se evita, **provocará** lesiones graves o incluso la muerte.

**⚠ ADVERTENCIA**

**ADVERTENCIA** indica una situación de peligro que, si no se evita, **podría provocar** lesiones graves o incluso la muerte.

**⚠ ATENCIÓN**

**ATENCIÓN** indica una situación peligrosa que, si no se evita, **podría provocar** lesiones leves o moderadas.

***AVISO***

***AVISO*** indica una situación potencialmente peligrosa que, si no se evita, **puede provocar** daños en el equipo.

## Tenga en cuenta

La instalación, manejo, puesta en servicio y mantenimiento de equipos eléctricos deberán ser realizados sólo por personal cualificado. Schneider Electric no se hace responsable de ninguna de las consecuencias del uso de este material.

Una persona cualificada es aquella que cuenta con capacidad y conocimientos relativos a la construcción, el funcionamiento y la instalación de equipos eléctricos, y que ha sido formada en materia de seguridad para reconocer y evitar los riesgos que conllevan tales equipos.

# Acerca del Documento

## Objeto

Esta guía proporciona información sobre aspectos de ciberseguridad para el sistema TeSys™ Tera con el fin de ayudar a los diseñadores y operadores del sistema a promover un entorno operativo seguro para el producto.

Esta guía aborda cómo proteger la red de tecnología operativa o la red de su empresa Ethernet.

**NOTA:** En esta guía, el término **security** se utiliza para hacer referencia a la ciberseguridad.

## Campo de aplicación

Este documento es válido para los siguientes componentes certificados del TeSys Tera system:

- LTMTEFM: LTMT main unit con protocolo EtherNet/IP o Modbus TCP/IP, 100-240 Vac/Vdc
- LTMTEBD: LTMT main unit con protocoloEtherNet/IP o Modbus TCP/IP, 24 Vcc
- LTMTMFM: LTMT main unit con protocolo Modbus RTU, 100-240 Vac/Vdc
- LTMTMBD: LTMT main unit con protocolo Modbus RTU, 24 Vdc
- LTMTPFM: LTMT main unit con protocolo PROFIBUS DP, 100-240 Vac/Vdc
- LTMTPBD: LTMT main unit con protocolo PROFIBUS DP, 24 Vdc

## Información general sobre ciberseguridad

En los últimos años, el creciente número de equipos y plantas de producción conectados a la red ha aumentado de la mano del potencial de las amenazas cibernéticas, como el acceso no autorizado, violaciones de datos e interrupciones operativas. Por lo tanto, es recomendable considerar todas las medidas de ciberseguridad posibles con el fin de ayudar a proteger los activos y los sistemas de dichas amenazas.

Para mantener sus productos de Schneider Electric seguros y protegidos, es conveniente que implemente las prácticas recomendadas de ciberseguridad que se indican en el documento Cybersecurity Best Practices.

Schneider Electric proporciona información y asistencia adicionales:

- Suscríbase al boletín de seguridad de Schneider Electric .
- Consulta la página web de Cybersecurity Support Portal para:
  - Buscar notificaciones de seguridad.
  - Notificar vulnerabilidades e incidentes.
- Consulta la página web de Schneider Electric Cybersecurity and Data Protection Posture para:
  - Acceder a la perspectiva de ciberseguridad.
  - Obtener más información sobre la ciberseguridad en la academia de ciberseguridad.
  - Explorar los servicios de ciberseguridad de Schneider Electric.

# Datos ambientales

Para obtener más información sobre el cumplimiento de los productos y el ambiente, consulte el Environmental Data Program de Schneider Electric.

# Idiomas disponibles del documento

Este documento está disponible en los siguientes idiomas:

- Inglés
- Chino
- Francés
- Alemán
- Italiano
- Coreano
- Español

# Documentos relacionados

| Título de la documentación | Descripción | Número de referencia |
|---|---|---|
| TeSys Tera Motor Management System Catálogo | El catálogo:<br>• Describe el TeSys Tera system.<br>• Incluye las características técnicas del TeSys Tera. | LVCATENTER |
| TeSys Tera Motor Management System Manual de Usuario | Se trata de la guía de usuario principal que presenta el TeSys Tera system completo. En ella se describen las funciones principales de LTMT main units, LTMTCT/ LTMTCTV sensor modules, LTMT expansion modules y LTMTCUF control operator unit. | DOCA0257ES |
| TeSys Tera Motor Management System Guía de Instalación | En esta guía se describen los procedimientos de instalación, puesta en marcha y mantenimiento de los LTMT main units, LTMTCT/LTMTCTV sensor modules, LTMT expansion modules y LTMTCUF control operator unit. | DOCA0356ES |
| Guía de Ayuda en Línea de TeSys Tera Motor Management System DTM library | En esta guía se describe la biblioteca TeSys Tera DTM que permite personalizar las funciones de control del TeSys Tera Motor Management System. | DOCA0275ES |
| Guía de Comunicación Modbus RTU del TeSys Tera Motor Management System | En esta guía se describe la comunicación del protocolo de red Modbus del LTMT main unit. | DOCA0355ES |
| Guía de comunicación PROFIBUS DP del TeSys Tera Motor Management System | En esta guía se describe la comunicación del protocolo de red PROFIBUS DP de la LTMT main unit. | DOCA0256ES |
| Guía de Comunicación EtherNet/IP del TeSys Tera Motor Management System | En esta guía se describe la comunicación del protocolo de red EtherNet/IP de la LTMT main unit. | DOCA0258ES |
| Guía del Usuario de la LTMTCUF control operator unit del TeSys Tera Motor Management System | En esta guía se describe cómo instalar, configurar y utilizar LTMTCUF control operator unit. | DOCA0233ES |
| TeSys Tera Motor Management System DTM library Nota sobre el lanzamiento del Software | Este documento proporciona información importante acerca de TeSys Tera DTM Library, así como un resumen de las nuevas características y mejoras. | DOCA0279EN |
| TeSys Tera Motor Management System Nota de la Versión del Firmware | En este documento se proporciona información acerca de las versiones del paquete de firmware del TeSys Tera system y se incluye un resumen de las nuevas características y mejoras. | DOCA0276EN |
| ¿Cómo puedo reducir la vulnerabilidad a los ciberataques? | Esta guía describe los riesgos de ciberseguridad y las estrategias de mitigación en los sistemas de control y automatización. | ¿Cómo puedo reducir la vulnerabilidad a los ciberataques? |

Para consultar documentos en línea, visite el centro de descargas de Schneider Electric (www.se.com/ww/en/download/).

# Información sobre terminología no inclusiva o insensible

Como empresa responsable e inclusiva, Schneider Electric actualiza constantemente sus comunicaciones y productos que contienen terminología no inclusiva o insensible. Sin embargo, a pesar de estos esfuerzos, nuestro contenido aún puede contener términos que algunos clientes consideren inapropiados.

# Marcas comerciales

*QR Code* es una marca comercial registrada de DENSO WAVE INCORPORATED en Japón y otros países.

# Precauciones

Lea y comprenda las precauciones siguientes antes de realizar los procedimientos de esta guía.

**⚠⚠PELIGRO**

**PELIGRO DE DESCARGA ELÉCTRICA, EXPLOSIÓN O ARCO ELÉCTRICO**

- La instalación y el mantenimiento de este equipo solo deberá realizarlos personal eléctrico cualificado.
- Desconecte toda la alimentación suministrada a este equipo antes de trabajar en él.
- Utilice solo la tensión especificada al utilizar este equipo y cualquier producto asociado.
- Utilice siempre un dispositivo detector de tensión con la capacidad correcta para confirmar que el equipo está apagado.
- Utilice enclavamientos adecuados cuando existan peligros para el personal y/o los equipos.
- Los circuitos de la línea de suministro deben estar cableados y protegidos conforme a las normativas locales y nacionales.
- Utilice equipos de protección individual (PPE) adecuados y siga las prácticas seguras para trabajos eléctricos contempladas en las normas NFPA 70E, NOM-029-STPS o CSA Z462 o sus equivalentes en la normativa local.

**Si no se siguen estas instrucciones, se producirán lesiones graves o la muerte.**

**⚠ADVERTENCIA**

**FUNCIONAMIENTO IMPREVISTO DEL EQUIPO**

- No desmonte, repare ni modifique el equipo. El equipo no contiene piezas que el usuario pueda reparar.
- Instale y utilice este equipo dentro de un alojamiento adecuado cuyas características nominales se ajusten a las del entorno de aplicación previsto.
- Cada instalación del equipo deberá someterse a pruebas exhaustivas para garantizar su correcto funcionamiento antes de ponerse en marcha.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

# Personal cualificado

Solo las personas debidamente formadas que estén familiarizadas con el contenido de esta guía y toda la documentación relacionada con el producto y lo comprendan están autorizadas a trabajar con este producto.

La persona cualificada deberá ser capaz de detectar posibles peligros que puedan presentarse como consecuencia de la modificación de los valores de los parámetros y, en general, del trabajo en equipos mecánicos, eléctricos o electrónicos. La persona cualificada deberá conocer las normas, las disposiciones y los reglamentos relativos a la prevención de accidentes industriales, los cuales deberá observar a la hora de diseñar e implantar el sistema.

El uso y la aplicación de la información contenida en esta guía requiere de conocimientos especializados en el diseño y la programación de sistemas de control automatizados. Solo el usuario, el constructor del panel o el integrador puede estar al corriente de todas las condiciones y factores presentes durante la instalación, la configuración, el funcionamiento y el mantenimiento de la máquina o planta de procesos y, por tanto, determinar qué sistemas de automatización y equipos asociados y qué medidas de seguridad y enclavamientos relacionados podrían resultar eficaces y adecuados a la hora de seleccionar los equipos de

automatización y control, y cualquier otro equipo o software relacionado para una aplicación en concreto. Deben considerarse también las normas y reglamentos locales, regionales y nacionales aplicables.

Asegúrese de cumplir con todas las disposiciones de seguridad, requisitos eléctricos y normativas aplicables a su máquina o planta de procesos al utilizar este equipo.

# Uso previsto

Los productos descritos en esta guía, además del software, los accesorios y las opciones, son componentes de arrancadores de cargas eléctricas de baja tensión destinados a utilizarse en entornos industriales de acuerdo con las instrucciones, indicaciones, ejemplos y disposiciones de seguridad contenidos en el presente documento y otros documentos de apoyo.

El producto solo se puede utilizar si se cumplen todas las normativas y directivas de seguridad aplicables, los requisitos especificados y las disposiciones técnicas.

Antes de utilizar el producto, deberá llevar a cabo una evaluación de riesgos de la aplicación planificada. A partir de los resultados, deberán aplicarse medidas de seguridad adecuadas.

Dado que el producto se utiliza como componente de una planta de procesamiento o una máquina, debe garantizar la seguridad de las personas mediante el diseño general del sistema.

Solo debe utilizar el producto con los cables y accesorios especificados. Utilice únicamente accesorios y piezas de repuesto originales.

Cualquier uso distinto del permitido explícitamente está prohibido y puede ocasionar riesgos imprevistos.

# Aviso de Seguridad Informática

## ⚠ADVERTENCIA

**RIESGO POTENCIAL PARA LA DISPONIBILIDAD, LA INTEGRIDAD Y LA CONFIDENCIALIDAD DEL SISTEMA**

- La primera vez que utilice el sistema, cambie las contraseñas predeterminadas para evitar el acceso no autorizado a la configuración, los controles y la información del dispositivo.
- Desactive los puertos/servicios no utilizados para reducir al mínimo las vías de acceso de atacantes dañinos.
- Ponga los dispositivos en red tras varias capas de ciberdefensas (como cortafuegos, segmentación de red y protección y detección de intrusiones en red).
- Siga las prácticas recomendadas de ciberseguridad (por ejemplo, privilegio mínimo, separación de tareas) para evitar exposiciones no autorizadas, pérdidas, modificaciones de datos y registros, o interrupciones de los servicios.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

# Introducción a la Ciberseguridad

## Contenido de esta parte

# Introducción

La ciberseguridad, como parte de los procesos, herramientas y tecnología, el cumplimiento normativo y la gobernanza, tiene como objetivo proteger su red de comunicaciones y todos los dispositivos conectados frente a ataques que podrían interrumpir las operaciones (disponibilidad), alterar la información (integridad) o exponer datos confidenciales (confidencialidad).

El objetivo de la ciberseguridad es proporcionar mayores niveles de protección contra robo, corrupción, mal uso o accidentes de la información y los activos físicos y, a la vez, garantizar el acceso a los usuarios legítimos. La ciberseguridad abarca muchos aspectos, entre ellos el diseño de sistemas seguros, la restricción del acceso mediante métodos físicos y digitales, la identificación de los usuarios, así como la implementación de procedimientos de control y medición de la seguridad y políticas de buenas prácticas.

# Directrices de Schneider Electric

Además de las recomendaciones proporcionadas en esta guía que son específicas para TeSys Tera system, debe seguir el enfoque de defensa en profundidad de la ciberseguridad Schneider Electric.

Este enfoque se describe en las *Mejores Prácticas Recomendadas de Ciberseguridad*.

Además, encontrará muchos recursos útiles e información actualizada en el Portal de Asistencia de Ciberseguridad de Schneider Electric., página 44.

# Enfoque de Schneider Electric en materia de ciberseguridad

Schneider Electric sigue las prácticas recomendadas del sector en el desarrollo e implementación de sistemas de control. Esto incluye un enfoque de defensa exhaustivo para proteger un sistema de control industrial. Este método sitúa los controladores detrás de uno o más firewalls para restringir el acceso únicamente al personal autorizado y a los protocolos.

## ⚠ADVERTENCIA

**ACCESO NO AUTENTICADO Y POSTERIOR USO NO AUTORIZADO DE LA MÁQUINA**

- Evalúe si el equipo o todo el entorno está conectado a la infraestructura crítica. De ser así, tome las medidas de prevención adecuadas conforme al método de defensa exhaustiva antes de conectar el sistema de automatización a cualquier red.
- Limite el número de dispositivos conectados a una red dentro de su empresa.
- Aísle su red industrial de otras redes dentro de su empresa.
- Proteja cualquier red contra el acceso imprevisto mediante firewalls, VPN u otras medidas de seguridad demostradas.
- Supervisa las actividades dentro de tus sistemas.
- Evite que los dispositivos en cuestión accedan directamente o se conecten directamente por parte de personas no autorizadas o acciones no autenticadas.
- Prepare un plan de recuperación que incluya una copia de seguridad del sistema y de la información de proceso.

**Si no se siguen estas instrucciones, pueden producirse lesiones graves, muerte o daños en el equipo.**

# Amenazas a la Seguridad

Las ciberamenazas son acciones deliberadas o accidentes que pueden interrumpir el funcionamiento normal de redes y sistemas informáticos. Estas acciones pueden iniciarse desde dentro del sitio físico o desde una localización externa. Los desafíos a la seguridad para el entorno de control incluyen:

- Diversos límites físicos y lógicos
- Múltiples sitios y grandes áreas geográficas
- Efectos adversos de la implementación de seguridad en la disponibilidad de procesos
- Mayor exposición a gusanos y virus al migrar de los sistemas empresariales a los sistemas de control a medida que las comunicaciones de control empresarial se vuelven más abiertas
- Mayor exposición a software malintencionado desde dispositivos USB, ordenadores portátiles de proveedores y servicio técnico, y red empresarial
- Impacto directo de los sistemas de control en sistemas mecánicos y físicos

# Políticas y Normas

Schneider Electric cuenta con un proceso de Ciclo de Vida de Desarrollo Seguro (SDL), un marco clave basado en el desarrollo de productos que ayuda a garantizar que los productos sigan procesos de diseño seguros en todas las etapas de su ciclo de vida. El proceso SDL de Schneider Electric cumple con IEC 62443-4.1 normas.

El proceso SDL incluye:

- Las prácticas de SDL se aplican a las acciones de desarrollo interno a lo largo de toda la cadena de suministro.
- Revisión de seguridad final requerida para publicar el proyecto.
- Formación en seguridad para el personal que participa en el desarrollo de productos.

# Directrices de mejora de la seguridad

## Introducción

Su PC puede ejecutar una serie de aplicaciones para mejorar la seguridad en su entorno de control. El sistema viene con una configuración predeterminada de fábrica que debe reconfigurarse para que coincida con la recomendación de Schneider Electric de emplear un método de defensa exhaustivo para el endurecimiento de los dispositivos.

En las siguientes directrices se describen procedimientos llevados a cabo en un sistema operativo Windows. Solamente se recogen a modo de ejemplo. Su sistema operativo y aplicación podrían necesitar procedimientos o requisitos diferentes.

## Deshabilitación del protocolo de escritorio remoto

El método de defensa exhaustivo de Schneider Electric recomienda deshabilitar el protocolo de escritorio remoto (RDP) a menos que la aplicación requiera el RDP.

Para deshabilitar el protocolo de escritorio remoto (RDP) en Windows 11, vaya a **Configuración > Sistema > Escritorio remoto > Habilitar escritorio remoto** (**Desactive** la opción).

## Actualización de las directivas de seguridad

Actualice las directivas de seguridad de los PC en su sistema escribiendo `gpupdate` en una ventana de comando. Para obtener más información, consulte la documentación de Microsoft en `gpupdate`.

## Gestión de actualizaciones

Antes de la implementación, actualice todos los sistemas operativos de PC mediante las utilidades de la página web de **Windows Update** de Microsoft. Para acceder a esta herramienta en Windows, seleccione **Inicio > Todos los programas > Windows Update**.

## Protección de la estación de trabajo

Para reducir los riesgos de seguridad asociados con la estación de trabajo de ingeniería, habilite la configuración de explotación de memoria, como Prevención de Ejecución de Datos (DEP) y Aleatorización del Diseño del espacio de Direcciones (ASLR). Estos ajustes de seguridad se pueden habilitar mediante la configuración de protección contra vulnerabilidades del sistema en el sistema operativo Windows 11. Para obtener más información, consulte la página web de características de seguridad de Microsoft.

# Aplicación de contraseñas seguras

Utilice contraseñas seguras que cumplan con los requisitos necesarios, como letras mayúsculas, minúsculas, números y caracteres especiales. Habilitar esta función ayuda a prevenir el acceso no autorizado al reducir el riesgo de utilizar contraseñas débiles.

# Uso de puertos no predeterminados

Cambiar los puertos de comunicación predeterminados para protocolos como HTTPS, DWPS y Modbus TCP añade una capa adicional de seguridad.

# Lista de direcciones IP permitidas

La función de lista de direcciones IP permitidas limita el acceso al sistema permitiendo únicamente direcciones IP específicas. Esto ayuda a evitar que dispositivos no autorizados se conecten al sistema y garantiza que solo fuentes fiables puedan comunicarse con el TeSys Tera system. Para acceder a la función de lista de direcciones IP permitidas, vaya a **Security > IP Allow List > IP Allow List** en el servidor web estándar.

# Información del sistema TeSys Tera

## Contenido de esta parte

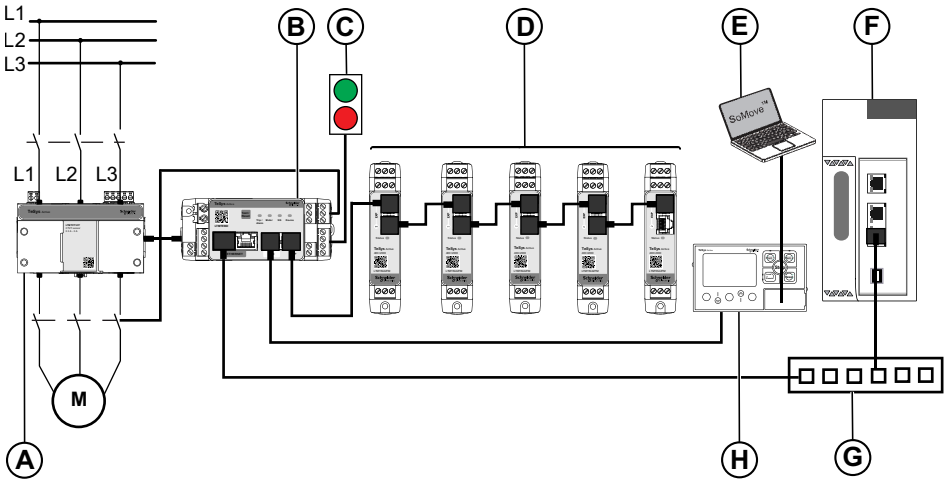
# Resumen

El TeSys Tera Motor Management System (o TeSys Tera system) forma parte de la TeSys gama Active de relés inteligentes y arrancadores de motor. El TeSys Tera system está diseñado como un componente básico fiable para Centros de Control de Motor Inteligente (iMCC) con el fin de proporcionar capacidades completas de protección, medición, control y supervisión para motores de inducción de AC monofásicos o trifásicos.

El TeSys Tera system se instala en el sistema de aparamenta eléctrica de baja tensión y se conecta al sistema de automatización de nivel superior a través de una red de bus de campo y el alimentador del motor.

TeSys Tera system:

- Cubre la protección, medición y supervisión convencionales y avanzadas de motores en alimentadores iMCC en un módulo de comunicación compacto, fácil de configurar y con un dispositivo HMI independiente.
- Proporciona un controlador de protección para alimentadores de arrancador de motor controlados por contactor de baja tensión.
- Proporciona un sistema de administración de motores flexible y modular para motores con velocidades constantes en aplicaciones de baja tensión.




A LTMTCT/LTMTCTV sensor module

B LTMT main unit

C Comandos de arranque/parada

D LTMT expansion modules

E PC que ejecuta el software de contenedores FDT SoMove con TeSys Tera DTM instalado

F Controlador Lógico Programable (PLC) o Sistema de Control Distribuido (DCS)

G Conmutador Ethernet

H LTMTCUF control operator unit

# Interfaces de comunicación

TeSys Tera system se comunica a través de los siguientes tipos de interfaz:

| LTMT main unit | Referencia | Puertos |
|---|---|---|
| Modbus RTU<br>  | • LTMTMFM (100-240 Vac/Vdc)<br>• LTMTMBD (24 Vdc) | • Puerto de comunicación Modbus RTU con conector terminal<br>• Puerto HMI con Modbus RTU comunicación para configuración |
| PROFIBUS DP<br>  | • LTMTPFM (100-240 Vac/Vdc)<br>• LTMTPBD (24 Vdc) | • PROFIBUS DP con conector sub D9<br>• Puerto Profibus con conector terminal<br>• Puerto HMI con Modbus RTU comunicación |

| LTMT main unit | Referencia | Puertos |
|---|---|---|
| Modbus TCP/IP<br>  | • LTMTEFM (100-240 Vac/Vdc)<br>• LTMTEBD (24 Vdc) | • Dos puertos Ethernet con Modbus TCP/IP<br>• Puerto HMI con Modbus RTU comunicación |
| EtherNet/IP<br>  | • LTMTEFM (100-240 Vac/Vdc)<br>• LTMTEBD (24 Vdc) | • Dos puertos Ethernet con EtherNet/IP<br>• Puerto HMI con Modbus RTU comunicación |

# Protocolos Compatibles

## Dispositivos de Comunicación en Serie

Los módulos Modbus RTU y PROFIBUS DP del TeSys Tera system protocolo Modbus RTU y PROFIBUS protocolo de soporte para comunicaciones con dispositivos de bus de campo.

Para los protocolos de comunicación y las referencias comerciales correspondientes, consulte Interfaces de comunicación, página 22.

## Dispositivos de comunicación Ethernet

Los módulos Modbus TCP/IP y EtherNet/IP módulos del soporte TeSys Tera system admiten los siguientes protocolos:

- HTTPS a través de herramientas de configuración y páginas web integradas
- Modbus TCP/IP y EtherNet/IP para comunicaciones con dispositivos de bus de campo
- DHCP para el direccionamiento IP en la red
- DNS para la resolución de nombres de red
- NTP para la sincronización horaria
- DPWS para la detección de dispositivos

Para los protocolos de comunicación y las referencias comerciales correspondientes, consulte Interfaces de comunicación, página 22.

# Funciones de seguridad

El TeSys Tera system admite las siguientes funciones:

- Firmware firmado digitalmente por Schneider Electric solo se puede instalar en TeSys Tera system.
- En cada arranque, se valida la firma digital del firmware antes de su ejecución.
- Las contraseñas de los usuarios se almacenan de forma segura (aplicable a Ethernet los módulos de interfaz).

  Para obtener más información sobre la política de contraseñas, consulte *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*
- Puede restablecer los ajustes de fábrica del TeSys Tera system utilizando la configuración **Factory Default** utilizando el TeSys Tera DTM o el botón **Test / Reset** en LTMT main unit.

  Para obtener más información sobre el botón **Test / Reset** , consulte *TeSys Tera Motor Management System User Guide – DOCA0257EN*.
- El TeSys Tera system tiene un reloj interno y recuerda la fecha y la hora durante 12 horas sin alimentación (válido para las variantes Modbus RTU y PROFIBUS DP y no aplicable para el Ethernet módulo).
- Mediante TeSys Tera DTM, la funcionalidad opcional de gestión de pines le permite habilitar o deshabilitar la configuración del TeSys Tera system. También puede restablecer el pin para TeSys Tera DTM utilizando la función de gestión del pines.

  Para obtener más información sobre la funcionalidad de gestión de pines, consulte *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.
- Para asegurar el TeSys Tera system, el LTMTCUF control operator unit viene con funcionalidad de pin. Debe tener un pin de seis dígitos para acceder al LTMTCUF control operator unit.

  Para obtener más información sobre la funcionalidad del pin, consulte *TeSys Tera Motor Management System User Guide – DOCA0257EN*.

Para los protocolos de comunicación y las referencias comerciales correspondientes, consulte Interfaces de comunicación, página 22.

# Características del sistema TeSys Tera

## Contenido de esta parte

# Firmware Update

Actualice el TeSys Tera system a la versión de firmware más reciente para obtener las funciones más recientes y tener actualizados los parches de seguridad. Todo el firmware diseñado para el TeSys Tera system se firma utilizando la Infraestructura de Clave Pública (PKI) de Schneider Electric para ayudar a garantizar la integridad y autenticidad del firmware que se ejecuta en el TeSys Tera system.

Para obtener más información sobre la actualización del firmware a través de TeSys Tera DTM, consulte *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*.

Para obtener más información sobre la actualización del firmware a través del servidor web estándar (aplicable a los módulos de interfaz Ethernet), consulte *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

Para obtener más información sobre las actualizaciones de seguridad, regístrese con el *Security Notifications* en el portal de asistencia de ciberseguridad de Schneider Electric.

# Date and Time

Para evitar errores, es importante mantener la fecha y la hora sincronizadas.

El siguiente procedimiento muestra cómo actualizar la configuración de fecha y hora de los módulos de interfaz de Ethernet utilizando un servidor web estándar o TeSys Tera DTM:

1. Navegue a **Settings > General > Date & Time**.
2. Utilizando la lista desplegable de **Date & Time Selection**, seleccione una de las siguientes opciones:
   - **Manual**

     **NOTA:**

     - Cuando la fecha y la hora se configuran manualmente, el LTMT main unit se restablece a la configuración de fábrica al reiniciarse.
     - La configuración de fecha y hora se puede actualizar manualmente utilizando el TeSys Tera DTM o el LTMTCUF control operator unit.
   - **NTP**

     **NOTA:** El protocolo **NTP** solo está disponible para las versiones Ethernet del LTMT main unit.

# Desactivar puertos/interfaces que no se utilicen

Desactivar los puertos/interfaces que no se utilizan ayuda a reducir la superficie de ataque del sistema, ya que se desactivan los puertos de comunicación y las interfaces que no se utilizan activamente.

Los siguientes ajustes del TeSys Tera system se pueden desactivar utilizando el servidor web estándar:

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

**NOTA:** Para obtener más información, consulte *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*

# Puertos

Los módulos Modbus TCP/IP y EtherNet/IP del TeSys Tera system utilizan los siguientes puertos para la comunicación de forma predeterminada:

| Tipo de Puertos | 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

El TeSys Tera system genera registros del sistema para registrar eventos tales como intentos de inicio de sesión no válidos y actualizaciones de firmware. Los registros no contienen información personal.

Para detectar comportamientos inesperados (por ejemplo, reinicios frecuentes, actualizaciones incorrectas del firmware o intentos de inicio de sesión no válidos), se recomienda supervisar los registros con regularidad.

Para obtener más información sobre los registros, consulte *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN* y *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

# Retirada de servicio

El TeSys Tera system contiene información confidencial configurada durante la puesta en servicio, valores de datos recientes y registros.

Por ejemplo, esta información puede incluir topología de Modbus LTMT main unit o consumos de energía medidos.

Es necesario realizar un restablecimiento de fábrica antes de eliminar TeSys Tera system.

Puede utilizar las siguientes formas para restablecer el TeSys Tera system:

- Botón **Test / Reset** en el LTMT main unit: Mantenga pulsado el botón **Test / Reset** del LTMT main unit durante 10 segundos.
- TeSys Tera DTM Library: Para obtener más información, consulte la sección *Restablecimiento de fábrica* en el *TeSys Tera Motor Management System DTM Library Online Help Guide – DOCA0275EN*
- LTMTCUF control operator unit: Para obtener más información, consulte la sección *Menú de comandos* en el *TeSys Tera Motor Management System LTMTCUF Control Operator Unit User Guide – DOCA0233EN*

# Seguridad de la Red

## Contenido de esta parte



**NOTA:** Esta parte solo es válida para los módulos Modbus TCP/IP y EtherNet/IP del TeSys Tera system.

# Introducción

El TeSys Tera system no está diseñado para soportar la exposición directa a la red pública de Internet. Debe instalarse al menos detrás de la Traducción de Direcciones de Red (NAT) o, preferiblemente, detrás de varios cortafuegos. Para obtener más información, consulte las siguientes páginas web:

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

# Segmentación de la Red

El TeSys Tera system es una pasarela que crea un puente entre diferentes redes. La segmentación de la red ayuda a garantizar la ciberdefensa. Para mejorar la segmentación de la red, la versión TeSys Tera system EtherNet/IP LTMT main unit cuenta con dos puertos Ethernet. Los puertos Ethernet disponibles se pueden utilizar para Tecnología de la Información (IT) y Tecnología Operativa (OT).

HTTPS y Modbus están disponibles en las interfaces TeSys Tera system Ethernet (ETH1, ETH2).

Se recomienda desactivar el servicio Modbus TCP/IP en las redes en las que no se utiliza.

# Certificado de Servidor web del Producto

Para admitir comunicaciones HTTPS seguras, el TeSys Tera system está equipado con un certificado X.509v3 por defecto. Este certificado contribuye a garantizar la integridad y la confidencialidad a la hora de configurar la comunicación HTTPS.

Los navegadores web solo reconocen certificados firmados por Autoridades de Certificación (CA) de terceros. El certificado autofirmado no es seguro. Se recomienda que importe un certificado firmado por una CA externa al TeSys Tera system y también debe mantener la fecha y la hora sincronizadas.

Los siguientes formatos de certificado son compatibles con el TeSys Tera system:

| Formato | Encabezado/Pie de página | Tipo de Clave |
|---|---|---|
| PKCS#1 | – – – – –COMIENZO DE LA CLAVE PRIVADA RSA– – – – – | Solo RSA |
| PKCS#8 | – – – – –COMIENZO DE LA CLAVE PRIVADA– – – – – | RSA, EC, DSA, etc. |
| Encriptado PKCS#8 | – – – – –COMIENZO DE LA CLAVE PRIVADA ENCRIPTADA– – – – – | Cualquiera |

**NOTA:** No se aceptarán certificados de pruebas modificados.

Para obtener más información sobre el certificado de terceros, consulte *TeSys Tera Motor Management System EtherNet/IP Communication Guide - DOCA0258EN*.

# Información de seguridad sobre dispositivos conectados

Se recomienda comprobar periódicamente la lista de dispositivos conectados a la red Ethernet del TeSys Tera system. En caso de que haya un dispositivo conectado desconocido, localícelo y elimínelo. También puede reconstruir la red y volver a conectar solo los dispositivos identificados.

# Seguridad física

## Instalación

Para ayudar a proteger la seguridad física de los sistemas, se recomienda la siguiente instalación:

- Instale el TeSys Tera system en un montaje en pared asegurado de manera adecuada al nivel de riesgo de su instalación (por ejemplo, un montaje en pared con candado o llave).
- Si el TeSys Tera system se monta en un cuadro eléctrico, instale el cuadro en una sala segura (por ejemplo, con una puerta cerrada con llave o una cámara).

# Recomendaciones de seguridad durante el mantenimiento

## Contenido de esta parte

# Operaciones de Mantenimiento

Durante la vida útil del TeSys Tera system, se recomienda realizar las siguientes operaciones con regularidad:

- Asegúrese de que el dispositivo esté ejecutando la última versión del firmware.
- Verifique que todos los parches de red y seguridad estén actualizados.
- Siga las mejores prácticas recomendadas en materia de ciberseguridad.
- Para comportamientos inesperados, como intentos de inicio de sesión no válidos o reinicios frecuentes, compruebe el Syslog, página 31.
- Para evitar desviarse de la fecha actual, compruebe el Date and Time, página 28.
- Cumpla con las normas de seguridad recomendadas por Schneider Electric para el dispositivo.

# Verificación de las Funciones de Seguridad

## Contenido de este capítulo

# Autenticación Web

**NOTA:** Este tema solo es válido para los módulos Modbus TCP/IP y EtherNet/IP del TeSys Tera system.

Para verificar la funcionalidad de autenticación web, proceda de la siguiente manera:

1. Intente iniciar sesión en el servidor web estándar del TeSys Tera system sin contraseña o introduciendo una contraseña incorrecta.

   **Resultado:** El TeSys Tera system no le da acceso al servidor web estándar.

2. Introduzca las credenciales incorrectas para tres instancias.

   **Resultado:** El TeSys Tera system se bloquea durante 15 minutos antes de permitirle intentarlo por cuarta vez.

# Autorización Web

**NOTA:** Este tema solo es válido para los módulos Modbus TCP/IP y EtherNet/IP del TeSys Tera system.

Para verificar la funcionalidad de autorización web, proceda de la siguiente manera:

1. Inicie sesión en el Servidor Web Estándar TeSys Tera system.

   **Resultado:** Después de iniciar sesión, tendrá acceso completo a los datos y funciones.

2. Marcar una página web (por ejemplo, **Settings**).
3. Abra una ventana de navegación privada en su navegador y abra la página web marcada como favorita.

   **Resultado:** No puede acceder a la página web, sin embargo, se le redirige a la página de inicio de sesión.

# Syslog

Para verificar la funcionalidad de Syslog, proceda de la siguiente manera:

1. Después de algunas o todas las pruebas anteriores, utilizando el TeSys Tera DTM o el servidor web estándar, acceda a los **Logs**.
2. Descargue los archivos de registro.
3. Verifique que la prueba realizada o los intentos fallidos estén presentes en los registros.

# Firmware Update

Para verificar la funcionalidad de actualización del firmware, proceda de la siguiente manera:

1. Navegue hasta la función de **Firmware Update** en el TeSys Tera DTM o el servidor web estándar.
2. Cargue un archivo de actualización de firmware autenticado.
3. Espere a que se valide el firmware.

   **Resultado:** El reinicio del sistema solo se produce cuando se actualiza el firmware del LTMT main unit se actualiza y los detalles del nuevo firmware se actualizan en el TeSys Tera DTM.

# Desactivación de servicios

**NOTA:** Este tema solo es válido para los módulos Modbus TCP/IP y EtherNet/IP del TeSys Tera system.

Para verificar la funcionalidad de los servicios de desactivación, proceda de la siguiente manera:

1. Navegando a **IP Network List > Security > Device Discovery** utilizando el servidor web estándar.
2. Desactive la detección de dispositivos.
3. Conecte un PC con Windows sistema operativo a la misma red.
4. Haga clic en **Network** en el **Explorador de archivos**.

   **Resultado:** El TeSys Tera system no se detecta, por lo que no aparece en la lista de dispositivos de la red.

Navegue a **IP Network List > Security** y siga el procedimiento anterior para verificar los siguientes métodos de desactivación:

- Modbus TCP
- Modbus RTU

# Portal de Soporte de Ciberseguridad de Schneider Electric

## Contenido de esta parte

# Resumen

El Schneider Electric *Cybersecurity support portal* describe la política de gestión de vulnerabilidades de Schneider Electric.

El objetivo de la política de gestión de vulnerabilidad de Schneider Electric es abordar las vulnerabilidades en la ciberseguridad que afectan productos y sistemas de Schneider Electric para proteger las soluciones instaladas, los clientes y el entorno.

Schneider Electric trabaja junto a investigadores, Equipos de Respuesta ante Emergencias Cibernéticas (CERT) y propietarios de equipos para asegurar que se proporcione información precisa de manera oportuna para proteger correctamente las instalaciones.

El CERT de Producto Corporativo (CPCERT) de Schneider Electric es responsable de administrar y emitir alertas sobre vulnerabilidades y mitigaciones que afectan a productos y soluciones.

El CPCERT coordina las comunicaciones entre los CERT pertinentes, los investigadores independientes, los gerentes de productos y todos los clientes afectados.

# Portal de Soporte de Ciberseguridad

El Schneider Electric Cybersecurity support portal proporciona la siguiente información:

- Acerca de las vulnerabilidades de ciberseguridad de los productos
- Acerca de los incidentes de ciberseguridad
- Acerca de una interfaz que permite declarar incidentes o vulnerabilidades de ciberseguridad.

# Informes y Gestión de Vulnerabilidades

Los incidentes y las potenciales vulnerabilidades de ciberseguridad pueden notificarse mediante el sitio web de Schneider Electric Report a Vulnerability.

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

www.se.com

Debido a que las normas, especificaciones y diseños cambian periódicamente, solicite la confirmación de la información dada en esta publicación.



DOCA0260ES-00