Serie PacT

Transfer**PacT** Active Automatic (LCD)
Transfer**PacT** Automatic (rotativo)

Guía de ciberseguridad

Pact series ofrece interruptores e interruptores automáticos de primer nivel.

DOCA0215ES-01
06/2022

www.se.com

Información legal

La instalación, utilización, mantenimiento y reparación de los productos y equipos de Schneider Electric la debe realizar solo personal cualificado.

Debido a la evolución de las normativas, especificaciones y diseños con el tiempo, la información contenida en esta guía puede estar sujeta a cambios 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 material o por las consecuencias derivadas o resultantes del uso de la información contenida en el presente documento.

Como parte de un grupo de empresas responsables e inclusivas, estamos actualizando nuestras comunicaciones que contienen terminología no inclusiva. Sin embargo, hasta que completemos este proceso, es posible que nuestro contenido todavía contenga términos estandarizados del sector que pueden ser considerados inapropiados para nuestros clientes.

Tabla de contenido

Advertencias de seguridad

Información importante

AVISO

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.

⚠ ⚠ DANGER

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

⚠ 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 LO SIGUIENTE:

La instalación, el manejo, las revisiones y el mantenimiento de equipos eléctricos deben ser realizados únicamente por el 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 la capacidad y los 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.

AVISO DE SEGURIDAD SOBRE CIBERSEGURIDAD

⚠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 y las cuentas predeterminadas para ayudar a reducir al mínimo los caminos de entrada de posibles ataques.
- Coloque 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.

Acerca de este libro

Alcance del documento

En esta guía se proporciona información sobre los aspectos de ciberseguridad de los dispositivos para ayudar a los diseñadores y los operadores de sistemas a promover un entorno operativo seguro para el producto. En esta guía no se trata el tema más general de cómo proteger su red de tecnología operativa o su red Ethernet empresarial. Para ver una introducción general a las amenazas de ciberseguridad y cómo afrontarlas, consulte How Can I Reduce Vulnerability to Cyber Attacks.

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

Campo de aplicación

La información de esta guía es relevante para los dispositivos relacionados con los interruptores de transferencia Transfer**PacT** Automatic y Transfer**PacT** Active Automatic.

Información en línea

La información incluida en este documento está sujeta a actualizaciones en cualquier momento. Schneider Electric recomienda instalar la versión más reciente y actualizada disponible en www.se.com/ww/en/download.

Las características técnicas de los dispositivos que se describen en este documento también se encuentran en línea. Si desea consultar la información en línea, visite la página de inicio de Schneider Electric www.se.com.

Las características técnicas que se describen en esta guía deben ser las mismas que las que aparecen en línea. Si observa una diferencia entre la información de esta guía y la información en línea, tenga en cuenta esta última.

Para obtener información sobre la conformidad de los productos con las directivas medioambientales como RoHS, REACH, PEP y EOLI, visite *www.se.com/green-premium*.

Documentación relacionada

Título del documento	**Número del documento**
Guía del usuario del Equipo de conmutación de transferencia (ATSE) TransferPacT Active Automatic	DOCA0214ES–01
How Can I reduce Vulnerability to Cyber Attacks	How Can I Reduce Vulnerability to Cyber Attacks

Introducción a la ciberseguridad

Introducción

La ciberseguridad protege la red de comunicación y los dispositivos frente a interrupciones de las operaciones (disponibilidad), modificaciones de los ajustes (integridad) o revelación de información confidencial (confidencialidad).

El objetivo de la ciberseguridad es:

- Proporcionar mayores niveles de protección de la información y los activos físicos contra robo, corrupción, uso indebido o accidentes a la vez que se mantiene el acceso para los usuarios previstos.
- Diseñar sistemas seguros, restringiendo el acceso mediante métodos físicos y digitales, identificando a los usuarios e implementando procedimientos y buenas prácticas de seguridad.

Directrices de Schneider Electric

Además de las recomendaciones que se ofrecen en esta guía, que son específicas de los dispositivos, debe seguir el enfoque de defensa exhaustivo de Schneider Electric para la ciberseguridad.

Este enfoque se describe en la nota técnica del sistema How Can I Reduce Vulnerability to Cyber Attacks.

Además, encontrará numerosos recursos útiles e información actualizada en el Cybersecurity Support Portal del sitio web global de Schneider Electric.

Funciones del dispositivo

Descripción general

El Equipo de conmutación de transferencia (ATSE) Transfer**PacT** Automatic se ha diseñado con funciones de seguridad, y estas funciones se encuentran en un estado preestablecido y pueden modificarse para satisfacer las necesidades de su instalación. Solo personal cualificado debe instalar y configurar el dispositivo, ya que desactivar o modificar los ajustes afectará a la solidez general de la seguridad del dispositivo y de la red de comunicación.

Utilice esta guía junto con la guía del usuario DOCA0214ES-01 para obtener información detallada sobre la configuración de las funciones y los ajustes del dispositivo.

Características de la comunicación

La comunicación con el ATSE TransferPacT se realiza mediante los siguientes tipos de interfaz:

- Comunicación cableada mediante:
  - Modbus-RTU
  - CANopen
- Interacción hombre-máquina (HMI) mediante:
  - Pantalla LCD con botones de visualización y funcionamiento.
  - Interruptores rotativos y DIP con LED para el funcionamiento.

Protocolos compatibles

- Modbus-RTU para la comunicación con los dispositivos o los sistemas de tecnología operativa (OT).
- CANopen para la comunicación interna entre el controlador principal y los accesorios (por ejemplo, módulo DI/DO o módulo de comunicación Modbus).

  NOTA: Modbus-RTU y CANopen son protocolos heredados, que tienen deficiencias inherentes de seguridad y deben compensarse con seguridad física adicional en su aplicación.

Funciones de seguridad

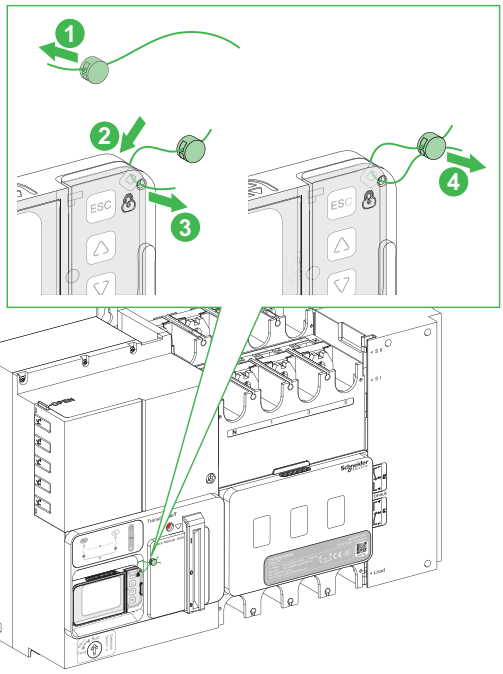
Se admiten las siguientes funciones de seguridad:

- El firmware se puede actualizar de forma segura mediante el firmware firmado digitalmente por la infraestructura de clave pública (PKI) de Schneider.
- Comprueba la integridad de los datos almacenados en el dispositivo para evitar que se manipulen las configuraciones, los datos empresariales y otros datos.
- Validación de entrada robusta para evitar ataques remotos desde Modbus-RTU o CANopen.
- Cualquier modificación de la configuración está protegida con contraseña.
- La contraseña se almacena como hash con sal y se puede restablecer. Para el restablecimiento de la contraseña, consulte la guía del usuario DOCA0214ES-01.
- La función de control de la comunicación está deshabilitada de forma predeterminada y solo se puede utilizar después de haberla habilitado localmente. Desactívela a tiempo cuando no sea necesaria.

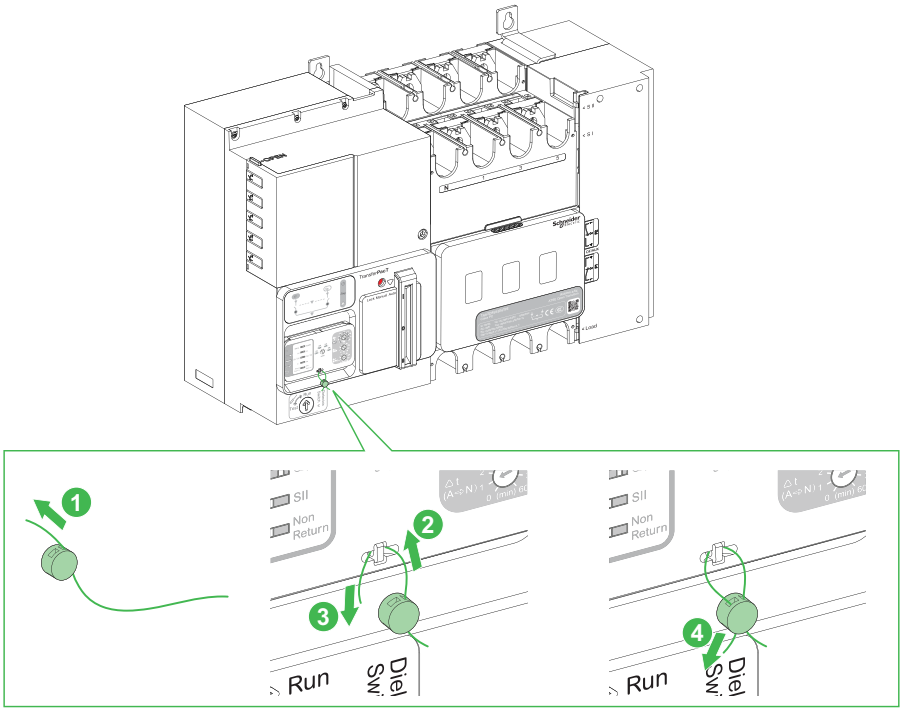
  NOTA: La función de control de comunicación solo se admite en TransferPact Active Automatic. Para obtener más información, consulte la guía del usuario DOCA0214ES-01 .
- El dispositivo se bloqueará durante 10 min después de 3 intentos fallidos de introducir la contraseña, lo que se utiliza para evitar ataques de fuerza bruta.
- Genera registros de auditoría para registrar operaciones importantes y lógicas de negocio para el análisis y la previsión, el seguimiento posterior al evento, la investigación y la recopilación de pruebas.

- Cubierta de plástico con orificio para ayudar a los usuarios a colocar precintos de plomo para evitar el acceso físico no autorizado a los botones (para TransferPact Active Automatic) o conmutadores rotativos (para TransferPact Automatic).

TransferPacT Active Automatic



TransferPacT Automatic



Seguridad del dispositivo

Actualización de firmware

El firmware diseñado para el dispositivo está firmado por la infraestructura de clave pública (PKI) de Schneider Electric para garantizar la integridad y la autenticidad del firmware que se ejecuta en el dispositivo.

- Regístrese en el Cybersecurity Support Portal de Schneider Electric.
- Póngase en contacto con el soporte técnico o una gente local de Schneider Electric si necesita ayuda para actualizar el firmware del dispositivo.

Contraseña

La contraseña predeterminada es **0000**; debe modificarse cuando se utiliza por primera vez.

NOTA: Evite utilizar contraseñas antiguas. Si olvida la contraseña o desea cambiarla, póngase en contacto con el servicio local o consulte la guía del usuario DOCA0214ES-01.

Fecha y hora

Hay certificados y firmas digitales en el dispositivo, así como registros de auditoría. Para evitar errores, es importante mantener la fecha y la hora sincronizadas. Para obtener más información sobre la fecha y la hora, consulte la guía del usuario DOCA0214ES-01.

Registros de auditoría

Genere los registros de auditoría que registran los eventos, como los intentos de inicio de sesión no válidos y la actualización del firmware.

Los registros de auditoría no contienen información personal ni confidencial.

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

Eliminación del dispositivo

El dispositivo contiene información confidencial configurada durante la puesta en servicio, valores de datos recientes y registros. Por ejemplo, esta información puede incluir contraseñas, topología de dispositivos Modbus y consumos de energía medidos.

Es necesario restablecer la configuración y restaurar la contraseña predeterminada antes de eliminar el dispositivo. Debe tener acceso físico al dispositivo mientras esté encendido. Para obtener información detallada sobre cómo restablecer la configuración predeterminada, consulte la guía del usuario DOCA0214ES-01.

NOTA: Es fundamental planificar la retirada del servicio durante el funcionamiento y antes de la eliminación del dispositivo.

NOTA: Asegúrese de que se exportan los últimos registros de eventos antes de retirar el dispositivo del servicio.

Seguridad física del dispositivo

A continuación se indican los puntos de seguridad física importantes que se deben tener en cuenta para instalar el dispositivo:

- Se recomienda instalar y utilizar el equipo de conmutación de acuerdo con un método de defensa exhaustivo recomendado por Schneider Electronic para reducir el riesgo de ataques al equipo de conmutación.
- Instale el ATSE en un armario protegido de manera adecuada, por ejemplo con un candado o una llave, para evitar riesgos durante la instalación o el riesgo de acceso físico no autorizado.
- Los accesorios de E/S (si los hay) se instalarán de forma segura para evitar el acceso no autorizado y mitigar el riesgo de cambio de la configuración del conmutador para la aplicación predefinida que se esté utilizando.
- Para los accesorios Modbus-RTU (si los hay) que se reconocen como un riesgo de seguridad en el sector, se recomiendan medidas de seguridad física (como tuberías dedicadas) para proteger los cables de comunicación del acceso no autorizado, las caídas de comunicación, la filtración y manipulación de datos, etc.
- En el caso de la HMI (si la hay), se utilizará un precinto de plomo para evitar el acceso no autorizado a los botones o conmutadores rotativos.
- Para la HMI independiente (si la hay), se recomienda encarecidamente implementarla con el ATSE en el mismo armario para garantizar la seguridad de las comunicaciones CANopen, o proteger los cables de comunicación con medidas de seguridad física (como tuberías dedicadas).

Operaciones de mantenimiento recomendadas

Debe realizarse periódicamente el mantenimiento recomendado a lo largo de la vida útil del dispositivo:

- Asegúrese de actualizar el firmware.
- Compruebe los registros de auditoría en busca de comportamientos inesperados, como intentos de inicio de sesión no válidos o reinicios frecuentes.
- Cambie periódicamente la contraseña de administrador.
- Compruebe periódicamente los cables de E/S para asegurarse de que están conectados correctamente y de que no hay accesos no autorizados.
- Compruebe periódicamente los cables de comunicación Modbus-RTU y CANopen para asegurarse de que no haya accesos no autorizados.
- Deshabilite la función de control de comunicación a tiempo cuando no sea necesario. Para obtener más información, consulte la guía del usuario DOCA0214ES-01 .

Cybersecurity Support Portal de Schneider Electric

Descripción general

El Cybersecurity Support Portal de Schneider Electric describe la política de gestión de vulnerabilidades de Schneider Electric.

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

Schneider Electric trabaja con un enfoque colaborativo con investigadores, equipos de respuesta a ciberemergencias (CERT) y propietarios de activos para garantizar que se proporcione información exacta en el momento oportuno para proteger adecuadamente sus instalaciones.

El CERT de producto corporativo (CPCERT) de Schneider Electric es responsable de gestionar 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.

Información disponible en el Cybersecurity Support Portal de Schneider Electric

Cybersecurity Support Portal brinda lo siguiente:

- Información sobre vulnerabilidades de ciberseguridad de los productos.
- Información sobre incidentes de ciberseguridad.
- Una interfaz que permite a los usuarios 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 Informar de una vulnerabilidad.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

+ 33 (0) 1 41 29 70 00

www.se.com

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

DOCA0215ES-01