MasterPact MTZ

Guía de ciberseguridad

12/2019

DOCA0122ES-02

www.schneider-electric.com

La información que se ofrece en esta documentación contiene descripciones de carácter general y/o características técnicas sobre el rendimiento de los productos incluidos en ella. La presente documentación no tiene como objeto sustituir dichos productos para aplicaciones de usuario específicas, ni debe emplearse para determinar su idoneidad o fiabilidad. Los usuarios o integradores tienen la responsabilidad de llevar a cabo un análisis de riesgos adecuado y completo, así como la evaluación y las pruebas de los productos en relación con la aplicación o el uso de dichos productos en cuestión. Ni Schneider Electric ni ninguna de sus filiales o asociados asumirán responsabilidad alguna por el uso inapropiado de la información contenida en este documento. Si tiene sugerencias de mejoras o modificaciones o ha hallado errores en esta publicación, le rogamos que nos lo notifique.

Usted se compromete a no reproducir, salvo para su propio uso personal, no comercial, la totalidad o parte de este documento en ningún soporte sin el permiso de Schneider Electric, por escrito. También se compromete a no establecer ningún vínculo de hipertexto a este documento o su contenido. Schneider Electric no otorga ningún derecho o licencia para el uso personal y no comercial del documento o de su contenido, salvo para una licencia no exclusiva para consultarla "tal cual", bajo su propia responsabilidad. Todos los demás derechos están reservados.

Al instalar y utilizar este producto es necesario tener en cuenta todas las regulaciones sobre seguridad correspondientes, ya sean regionales, locales o estatales. Por razones de seguridad y para garantizar que se siguen los consejos de la documentación del sistema, las reparaciones solo podrá realizarlas el fabricante.

Cuando se utilicen dispositivos para aplicaciones con requisitos técnicos de seguridad, siga las instrucciones pertinentes.

Si con nuestros productos de hardware no se utiliza el software de Schneider Electric u otro software aprobado, pueden producirse lesiones, daños o un funcionamiento incorrecto del equipo.

Si no se tiene en cuenta esta información, se pueden causar daños personales o en el equipo.

© 2019 Schneider Electric. Reservados todos los derechos.

Tabla de materias

Información 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.

⚠ 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 LO SIGUIENTE:

La instalación, el manejo, las revisiones y el 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.

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 los accesos no autorizados 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.
- Ponga los dispositivos en red tras varias capas de ciberdefensas (como firewall, 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.

El incumplimiento de estas instrucciones puede causar la muerte, lesiones serias o daño al equipo.

Acerca de este libro

Presentación

Objeto

Esta guía proporciona información sobre aspectos de ciberseguridad para interruptores automáticos MasterPact™ MTZ con unidades de control MicroLogic™ X para ayudar a los diseñadores y operadores de sistemas a promover un entorno de funcionamiento 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 incluida en esta guía corresponde a los interruptores automáticos MasterPact MTZ con unidades de control MicroLogic X.

La información incluida en este documento está sujeta a actualizaciones en cualquier momento. Schneider Electric recomienda encarecidamente tener la versión más reciente y actualizada que está disponible en *www.schneider-electric.com/docs*.

Documentos relacionados

Título de la documentación	Número de referencia
MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario	*DOCA0102ES*
How Can I Reduce Vulnerability to Cyber Attacks?	*Cybersecurity System Technical Note*
MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note	*DOCA0144EN*
Enerlin'X IFM - Modbus-SL Interface for One Circuit Breaker - Release Note	*DOCA0146EN*
Enerlin'X IFE Switchboard Server IFE/EIFE Ethernet Interface - Release Note	*DOCA0147EN*
Enerlin'X IO Input/Output Application Module for One Circuit Breaker - Release Note	*DOCA0149EN*
Enerlin'X FDM128 - Ethernet Display for Eight Devices - Release Note	*DOCA0151EN*

Puede descargar estas publicaciones técnicas y otra información técnica de nuestro sitio web https://www.se.com/ww/en/download/ .

Aviso de marca comercial

Todas las marcas comerciales son propiedad de Schneider Electric Industries SAS o sus filiales.

Capítulo 1
Introducción a la ciberseguridad

Descripción general

En este capítulo se ofrece información general sobre la política de ciberseguridad de Schneider Electric y se explica por qué la ciberseguridad es importante para los interruptores automáticos MasterPact MTZ con unidades de control MicroLogic X.

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Introducción a la ciberseguridad

Introducción

La ciberseguridad tiene como objetivo proteger su red de comunicaciones y todos los equipos conectados a ella frente a ataques que puedan interrumpir las operaciones (disponibilidad), modificar la información (integridad) o revelar información confidencial (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. Hay muchos aspectos que tener en cuenta por lo que respecta a la ciberseguridad, incluido el diseño de sistemas seguros, la restricción del acceso utilizando métodos físicos y digitales, la identificación de los usuarios y la implementación de procedimientos de seguridad y políticas de mejores prácticas.

Directrices de Schneider Electric

Además de las recomendaciones que se ofrecen en esta guía, que son específicas de los interruptores automáticos MasterPact MTZ, debe seguir el método de defensa exhaustivo de Schneider Electric para la ciberseguridad.

Este método 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 *(véase página 37)*.

Por qué es importante la ciberseguridad para los interruptores automáticos MasterPact MTZ

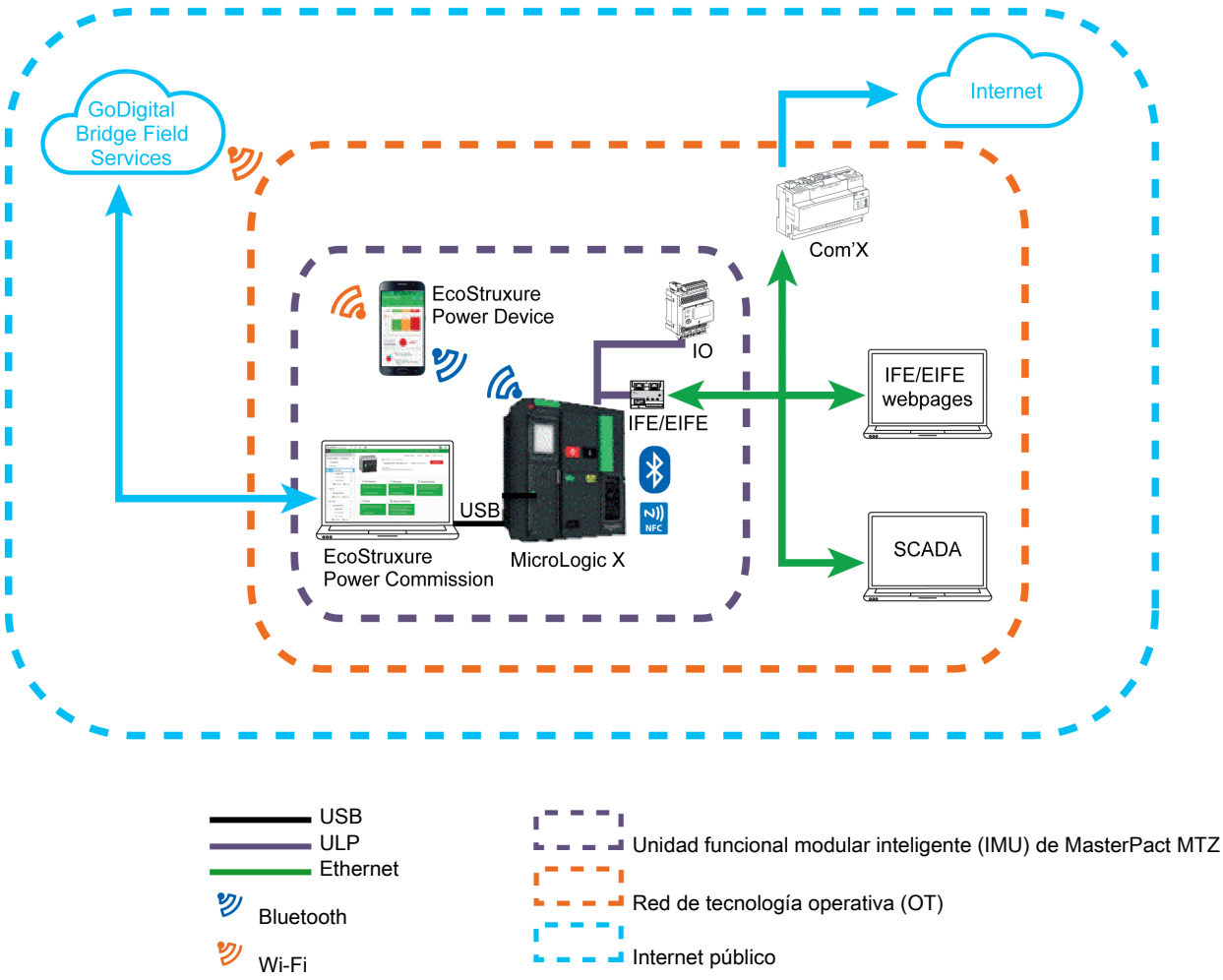
Descripción general

El interruptor automático MasterPact MTZ es un componente clave de cualquier planta o equipo porque controla la alimentación eléctrica del sistema, proporciona protección eléctrica y ofrece información confidencial.

Los interruptores automáticos MasterPact MTZ con funciones de comunicación también proporcionan acceso 24 horas al día y 7 días a la semana a funciones de control en tiempo real y a datos de supervisión. Estas funciones aumentan la eficiencia y la flexibilidad de gestión del sistema. No obstante, también hacen que resulte potencialmente vulnerable a los ciberataques.

Interruptor automático MasterPact MTZ y entorno operativo

En la imagen siguiente se muestran las distintas maneras de comunicarse con la unidad de control MicroLogic X que se interconecta con el interruptor automático MasterPact MTZ.



La unidad funcional modular inteligente (IMU) de MasterPact MTZ representa el interruptor automático, la unidad de control MicroLogic X y los módulos ULP asociados, la interfaz de comunicación y el módulo IO.

Para comunicarse con el interruptor automático MasterPact MTZ por medio de su unidad de control MicroLogic X, se encuentran disponibles las siguientes rutas de comunicación:

- Interfaz hombre-máquina (HMI) de MicroLogic X
- Conexión inalámbrica NFC desde un smartphone
- Conexión inalámbrica Bluetooth Low Energy (BLE) desde un smartphone
- Conexión al puerto mini tipo B USB de la unidad de control MicroLogic X desde:
  - Un PC que ejecute el software EcoStruxure™ Power Commission. EcoStruxure™ Power Commission es el nuevo nombre del software Ecoreach.
  - Un smartphone que tenga instalada la aplicación Aplicación EcoStruxure Power Device
- Conexión Ethernet a través de la red de tecnología operativa (OT) cuando la interfaz de comunicación está presente
- Conexión Modbus-SL a través de la red de tecnología operativa (OT) cuando la interfaz de IFM está presente

Vulnerabilidad del sistema frente a ciberataques

Cada una de las rutas de comunicación enumeradas anteriormente representa un punto vulnerable de su sistema si no se toman medidas de seguridad. Esta guía ofrece directrices para ayudar a proteger estas rutas de comunicación frente a ataques intencionados o mal uso accidental.

Capítulo 2
Recomendaciones de ciberseguridad para el diseño, la planificación y la instalación del sistema

Descripción general del capítulo

Este capítulo proporciona información importante a tener en cuenta durante las fases de diseño, planificación e instalación de una red de tecnología operativa (OT) que incluya la unidad funcional modular inteligente (IMU) de MasterPact MTZ. Las recomendaciones y directrices incluidas en este capítulo ayudan a crear un entorno de funcionamiento seguro.

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Identificación y protección de información y operaciones confidenciales y críticas

Descripción general

Al planificar y diseñar una red de tecnología operativa, es importante identificar la información crítica para sus operaciones. Una vez identificada, esta información confidencial se debe proteger.

Como principio general, la información confidencial incluye:

- Cualquier información que se pueda utilizar para acceder a su instalación y a su red de tecnología operativa
- Información sobre las operaciones accesibles a través de la IMU de MasterPact MTZ

Es responsabilidad suya determinar cómo se puede analizar y utilizar esta información en contra de la empresa.

Información sobre la red de comunicación empresarial

Entre la información confidencial que se puede utilizar para acceder a su instalación y a su red de control se encuentra la siguiente:

- La arquitectura del sistema
- Las direcciones IP o MAC de los dispositivos que se comunican a través de la red
- Los números de puerto utilizados para la comunicación Ethernet
- ID y contraseñas de usuario

Esta lista no es exhaustiva, y es importante tener en cuenta toda la información específica de su organización que pueda facilitar el acceso a sistemas críticos.

Control de accesos

Una parte importante de la ciberseguridad consiste en diseñar una política de control de accesos eficaz. El control de accesos consiste en identificar grupos de usuarios o empleados individuales de su organización y determinar el tipo de acceso que necesitan para desempeñar sus trabajos eficazmente.

Resumen de información y operaciones accesibles a través de cada ruta de acceso

Según la interfaz de comunicación o la ruta de comunicación utilizadas para acceder a la unidad funcional modular inteligente (IMU) de MasterPact MTZ, la información y las operaciones de control disponibles son diferentes. La siguiente tabla resume el acceso a la información y las operaciones de control:

Información y operaciones de control	Acceso local				Acceso remoto
	HMI de MicroLogic X	NFC	Bluetooth low energy	USB	Ethernet / Modbus-SL
Supervisión de datos	Lectura	Lectura	Lectura	Lectura	Lectura
Configuración de la protección	Lectura/Escritura	Lectura	Lectura/Escritura	Lectura/Escritura	Lectura/Escritura
Otros ajustes	Lectura/Escritura	Lectura	Lectura/Escritura	Lectura/Escritura	Lectura/Escritura
Abrir/Cerrar/Restablecer	No	No	Sí	Sí	Sí

Para obtener información sobre la protección de cada interfaz de comunicación y ruta de acceso, consulte las recomendaciones para el acceso local *(véase página 19)* o el acceso remoto *(véase página 27)*, según corresponda.

Diseño de una política de contraseñas

Descripción general

Una política de contraseñas minuciosamente diseñada es la primera línea de defensa frente a ciberataques.

En el contexto de las instalaciones que incluyen el interruptor automático MasterPact MTZ con la unidad de control MicroLogic X, se requieren contraseñas para:

- Ejecutar comandos intrusivos en la unidad de control MicroLogic X, sea cual sea el modo de acceso (por medio de Ethernet/Modbus-SL, conexión USB o Bluetooth)
- Iniciar sesión en el PC en el que se ejecuta el software EcoStruxure Power Commission
- Iniciar sesión en las páginas web de las interfaces IFE y EIFE
- Iniciar sesión en las páginas web del servidor IFE

Recomendaciones de ciberseguridad referentes a la política de contraseñas

⚠ 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 los accesos no autorizados a la configuración, los controles y la información del dispositivo.

El incumplimiento de estas instrucciones puede causar la muerte, lesiones serias o daño al equipo.

La política de contraseñas es uno de los elementos principales de la política de ciberseguridad. Una buena política de contraseñas consiste en:

- Usar contraseñas seguras
- Cambiar periódicamente las contraseñas
- Usar un gestor de contraseñas para gestionar las contraseñas de acceso
- Prohibir la reutilización de contraseñas antiguas
- Recordar periódicamente a los usuarios las prácticas recomendadas sobre las contraseñas

Para contribuir a proteger su sistema, lo mínimo es:

- Aplicar el uso de contraseñas seguras
- Establecer la longitud mínima de las contraseñas en 10 caracteres
- Establecer el periodo de validez mínimo en tres días y el máximo en 90 días
- Conservar el historial de las ocho últimas contraseñas y prohibir que se vuelvan a utilizar

Todos los usuarios deben conocer las prácticas referentes a las contraseñas. Son las siguientes:

- No compartir contraseñas personales
- No mostrar las contraseñas al introducirlas
- No transmitir contraseñas por correo electrónico ni por ningún otro medio
- No guardar las contraseñas en los PC u otros dispositivos

Contraseña para ajustes y controles críticos de MicroLogic X

Al acceder a la unidad de control MicroLogic X mediante una interfaz de comunicación, cualquier comando intrusivo que modifique el comportamiento del interruptor automático MasterPact MTZ requiere una contraseña. Por ejemplo, para realizar cambios de los ajustes de protección o para utilizar el interruptor automático se necesita la contraseña de la unidad de control MicroLogic X.

Se definen cuatro contraseñas para una unidad e control MicroLogic X, una para cada uno de los siguientes cuatro perfiles de usuario:

- Administrador
- Servicios
- Ingeniero
- Operador

Si desea más información sobre perfiles de usuario, consulte *DOCA0102EN MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario*.

Cuando se realiza la conexión por medio de Aplicación EcoStruxure Power Device o el software EcoStruxure Power Commission, se solicita al usuario que proporcione una de estas contraseñas.

Cuando se realiza la conexión desde una interfaz de supervisión y control remota, la contraseña debe formar parte de la solicitud de comunicación.

La contraseña consta de cuatro caracteres ASCII. La contraseña distingue mayúsculas y minúsculas y los caracteres permitidos son:

- Dígitos del 0 al 9
- Letras minúsculas de la "a" a la "z"
- Letras mayúsculas de la "A" a la "Z"

Las contraseñas predeterminadas deben cambiarse en la primera instalación del interruptor automático MasterPact MTZ y periódicamente tras la primera instalación, usando el software EcoStruxure Power Commission. Almacene las contraseñas usando un gestor de contraseñas. Comparta las contraseñas con un número limitado de usuarios de confianza. Siga las recomendaciones de la política de contraseñas cuando corresponda.

Contraseñas e ID de usuario para PC en red

Los PC en los que se ejecuta el software EcoStruxure Power Commission o que acceden a la unidad de control MicroLogic X utilizando cualquier otro medio (por ejemplo, páginas web de IFE o EIFE, o SCADA) deben solicitar a los usuarios un nombre de usuario y una contraseña. Debe asegurarse de que los usuarios definan contraseñas seguras y las cambien periódicamente. Además, debe ajustar un temporizador para bloquear la pantalla del PC automáticamente después de un periodo de tiempo de inactividad.

Una contraseña segura incluye letras mayúsculas y minúsculas, números y caracteres especiales, si es posible utilizarlos. Debe tener una longitud mínima de 10 caracteres.

Siga las recomendaciones de la política de contraseñas cuando corresponda.

Contraseñas para páginas web del servidor IFE, la interfaz de IFE y la interfaz de EIFE

Cada usuario de las páginas web del servidor IFE o las interfaces IFE o EIFE tiene un ID de usuario personal y una contraseña para iniciar sesión en las páginas web. Los usuarios deben cambiar la contraseña después de iniciar sesión en las páginas web por primera vez.

Debe definir qué usuarios de su organización deben iniciar sesión en las páginas web de IFE y EIFE y seguir las recomendaciones de la política de contraseñas cuando corresponda.

Formación

Descripción general

La concienciación y formación de los empleados es un fundamento sumamente importante de la estrategia de ciberseguridad. Debe asegurarse de que todos los usuarios a los que se otorga acceso a la red de control de su instalación conozcan la política de información de seguridad de la empresa. También debe asegurarse de que hayan recibido una formación adecuada para el desempeño de sus tareas de acuerdo con dicha política.

Concretamente, los usuarios deben conocer (y se les deben recordar periódicamente) las prácticas recomendadas referentes a lo siguiente:

- No compartir información confidencial como contraseñas o códigos de acceso de equipos o de salas cerradas
- Mantener los PC bloqueados mientras no se utilicen
- Asegurarse de llevar siempre encima los smartphones que puedan utilizarse para acceder al sistema y de que estos no se puedan piratear a través de Bluetooth o de Internet
- No contravenir ninguna política de seguridad por motivos de comodidad

Para obtener más información sobre cómo diseñar e implementar una buena política de formación, consulte *How Can I Reduce Vulnerability to Cyber Attacks?*.

Capítulo 3
Recomendaciones de ciberseguridad para el acceso local

Descripción general del capítulo

Este capítulo ofrece una lista de las rutas de acceso locales al interruptor automático MasterPact MTZ. También proporciona recomendaciones para proteger estas rutas de acceso. Son cuestiones importantes que tener en cuenta para el funcionamiento.

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Restricción del acceso local al interruptor automático MasterPact MTZ

Descripción general

La unidad funcional modular inteligente (IMU) de MasterPact MTZ ofrece posibilidades de acceso local y remoto. Debe asegurarse de que solo se otorgue acceso a usuarios autorizados.

Acceso local al interruptor automático MasterPact MTZ

El acceso local a la unidad funcional modular inteligente de MasterPact MTZ proporciona varias posibilidades para acceder a información sobre el sistema y controlarlo.

Por lo tanto, es importante restringir el acceso local al interruptor automático MasterPact MTZ instalándolo en un área cerrada para evitar:

- El acceso no autorizado a la HMI de MicroLogic X, que supone el riesgo de que se realicen cambios en los ajustes desde la HMI
- El acceso no autorizado a la comunicación inalámbrica Bluetooth, que supone el riesgo de que se realicen cambios en los ajustes desde Aplicación EcoStruxure Power Device
- El acceso no autorizado a la comunicación inalámbrica NFC, que supone el riesgo de revelación de datos
- La conexión no autorizada a través del puerto mini USB de la unidad de control MicroLogic X, que supone el riesgo de que se realicen cambios en los ajustes desde el software EcoStruxure Power Commission o un smartphone con Aplicación EcoStruxure Power Device
- El acceso no autorizado al módulo IO, que supone el riesgo de que se realicen cambios en el ajuste del conmutador para la aplicación predefinida que se está utilizando

También es importante implementar reglas para gestionar el acceso al área cerrada. Concretamente, se debe asegurar de que:

- El área se mantenga cerrada en todo momento.
- El área disponga de un sistema de autenticación y autorización.
- Solo el personal autorizado disponga de una llave o un código de acceso.
- Los cables de la red de comunicación que entren en la sala y los puertos de conexión de los dispositivos de comunicación de fuera de la sala estén protegidos.
- Todos los dispositivos, como PC, smartphones y tabletas, que accedan a la unidad de control MicroLogic X estén protegidos de acuerdo con las directrices más recientes del proveedor.

Cuando el interruptor automático MasterPact MTZ esté instalado en un área cerrada, se debe implementar un proceso de apertura de emergencia. Por ejemplo:

- Debe disponer en el área como mínimo de un botón de parada de emergencia que resulte accesible desde el exterior.
- El interruptor automático debe disponer de una bobina de disparo por falta de tensión MN (sistema de modo seguro).

Recomendaciones para proteger el acceso local a la HMI de MicroLogic X

Funciones accesibles desde la HMI

Cualquier persona que tenga acceso a la carcasa en la que se encuentra el interruptor automático MasterPact MTZ tendrá acceso a la HMI de la unidad de control MicroLogic X.

Algunas funciones críticas, como los ajustes de protección para el equipo, se pueden configurar desde la HMI de MicroLogic X.

Recomendaciones para proteger el acceso a través de la HMI de MicroLogic X

La HMI de MicroLogic X no está protegida por contraseña ni se puede bloquear físicamente para impedir el acceso a la pantalla. Por lo tanto, para proteger el acceso a la HMI, se debe:

- Instalar el interruptor automático MasterPact MTZ en un área cerrada.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener información adicional sobre cómo proteger el acceso al interruptor automático MasterPact MTZ, consulte Implementación de una política de acceso restringido *(véase página 20)*.

Bloqueo de los ajustes de protección

Puede bloquear los ajustes de protección del interruptor automático MasterPact MTZ para evitar que se cambien localmente en la HMI. De forma predeterminada, se permite cambiar los ajustes de protección en la HMI.

Se recomienda desactivar la modificación local de los ajustes de protección en la HMI si no se utiliza esta función. Si desea más información, consulte *DOCA0102EN MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario*.

Recomendaciones para proteger el acceso a través de NFC

Funciones accesibles a través de NFC

Por medio de la comunicación de campo cercano inalámbrica (NFC), se pueden descargar datos de la unidad de control MicroLogic X a un smartphone, aunque la unidad de control no esté encendida. No es posible cambiar ningún ajuste en la unidad de control, ni abrir, cerrar o reiniciar el interruptor automático MasterPact MTZ.

Requisitos previos para establecer una conexión NFC

Para establecer una conexión inalámbrica NFC con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- Debe tener acceso físico a la sala en la que está el interruptor automático MasterPact MTZ y a la carcasa del equipo.
- Aplicación EcoStruxure Power Device debe estar instalada en el smartphone.
- El smartphone debe admitir NFC.

Cualquier persona que cumpla estas condiciones puede descargar datos que pueden ser confidenciales para las operaciones. En la unidad de control MicroLogic X, no se registran las conexiones establecidas a través de NFC.

Si desea conocer los procedimientos detallados de establecimiento de una conexión NFC, consulte *DOCA0102EN MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario*.

Recomendaciones generales para proteger el acceso a través de NFC

Para proteger el acceso a los datos a través de una conexión inalámbrica NFC, se recomienda:

- Instalar el interruptor automático MasterPact MTZ en un área cerrada para que ninguna persona sin autorización pueda acceder a la unidad de control MicroLogic X.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener más información, consulte las recomendaciones para restringir el acceso local al interruptor automático MasterPact MTZ *(véase página 20)*.

Recomendaciones para la comunicación NFC

Para proteger el acceso a las funciones a las que se puede acceder a través de una conexión inalámbrica NFC, se recomienda:

- Desconectar el smartphone de Internet (por ejemplo, colocarlo en modo avión) durante una conexión NFC con la unidad de control MicroLogic X.
- Desactivar la comunicación Bluetooth en el smartphone.
- No introducir un código de emparejamiento si se le solicita, porque no es necesario para una conexión NFC.

Recomendaciones para el uso de Aplicación EcoStruxure Power Device

Para restringir el acceso a la unidad de control MicroLogic X desde un smartphone en el que se ejecute Aplicación EcoStruxure Power Device, se recomienda utilizar únicamente la Aplicación EcoStruxure Power Device oficial de Schneider Electric para conectarse al interruptor automático MasterPact MTZ.

Recomendaciones para el uso de smartphones

Para restringir el acceso a la unidad de control MicroLogic X desde un smartphone, se recomienda:

- Asegurarse de que los smartphones que dispongan de Aplicación EcoStruxure Power Device estén protegidos con contraseña y se utilicen solo para el trabajo.
- Proteger los smartphones en los que se haya instalado Aplicación EcoStruxure Power Device implementando todas las funciones de seguridad recomendadas por el proveedor o el fabricante del smartphone.
- Mantener actualizadas las aplicaciones antivirus para smartphones.
- No facilitar información acerca del smartphone (número de teléfono, dirección MAC) a menos que sea estrictamente necesario.
- Desconectar el smartphone de Internet (por ejemplo, colocarlo en modo avión) durante una conexión NFC con la unidad de control MicroLogic X.
- No almacenar información confidencial en un smartphone.

Recomendaciones para proteger el acceso a través de Bluetooth

Funciones accesibles a través de Bluetooth

AVISO

RIESGO DE FUNCIONAMIENTO IMPREVISTO

- Solo personal cualificado debe ser el encargado de configurar y preparar el aparato, usando los resultados del estudio del sistema de protección de la instalación.
- Durante la puesta en marcha de la instalación y después de cualquier modificación, compruebe que la configuración de MicroLogic X y los ajustes de las funciones de protección sean acordes con los resultados de este estudio.
- Las funciones de protección de MicroLogic X están establecidas de manera predeterminada en su valor mínimo, a excepción de la función de protección de largo retardo, que se establece de manera predeterminada en su valor máximo.

El incumplimiento de estas instrucciones puede causar daño al equipo.

Al usar las comunicaciones inalámbricas de Bluetooth low energy (BLE), puede acceder a la unidad de control MicroLogic X desde un smartphone que esté ejecutando Aplicación EcoStruxure Power Device. Esta aplicación ofrece una interfaz orientada a tareas con la unidad de control. Los datos transferidos a través de Bluetooth se cifran utilizando el cifrado AES de 128 bits.

Requisitos previos para establecer una conexión Bluetooth

Para establecer una conexión inalámbrica Bluetooth con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- La unidad de control MicroLogic X debe estar encendida.
- La función Bluetooth de la unidad de control MicroLogic X debe estar activada.
- Solo se puede conectar un smartphone a una unidad de control a la vez.
- Debe tener un smartphone con Aplicación EcoStruxure Power Device instalada.
- El smartphone debe admitir Bluetooth low energy (4.0 o superior).
- Debe tener acceso a la unidad de control MicroLogic X para activar el pulsador Bluetooth y encontrarse físicamente en la zona de cobertura durante la conexión (normalmente, de 20 a 30 metros o yardas).

Cualquier persona que cumpla estas condiciones y establezca una conexión tendrá acceso a funciones que pueden afectar a la instalación.

Si desea conocer los procedimientos detallados de establecimiento de una conexión Bluetooth, consulte *DOCA0102EN MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario*.

Recomendaciones generales para proteger el acceso a través de Bluetooth

Para proteger el acceso a las funciones a las que se puede acceder a través de una conexión inalámbrica Bluetooth, se recomienda:

- Instalar el interruptor automático MasterPact MTZ en un área cerrada para que ninguna persona sin autorización pueda acceder a la unidad de control MicroLogic X.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener información adicional sobre cómo proteger el acceso al interruptor automático MasterPact MTZ, consulte Implementación de una política de acceso restringido *(véase página 20)*.

Recomendaciones para el uso de Bluetooth

Para proteger el acceso a las funciones a las que se puede acceder a través de una conexión inalámbrica Bluetooth, se recomienda:

- Desactivar la función Bluetooth en la unidad de control MicroLogic X, tal como se explica en *MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario*, y activarla solo cuando esté listo para establecer una conexión.
- Ajustar el temporizador de desconexión de Bluetooth en 5 minutos.
- Excepto cuando inicie una conexión Bluetooth, Bluetooth no debe activarse por medio del pulsador de activación de la parte frontal de la unidad de control MicroLogic X. La conexión Bluetooth debe permanecer apagada cuando no se utilice.
- Pulse el pulsador Bluetooth para finalizar la comunicación cuando haya terminado.
- El emparejamiento se debe realizar con la menor frecuencia posible y en un área segura, para que no haya intrusos que puedan ver el código de emparejamiento al introducirlo.
- No introduzca ningún código de emparejamiento si se le solicita de forma imprevista.
- Durante el emparejamiento de Bluetooth, mantenga el smartphone lo más cerca posible de la unidad de control MicroLogic X.

Recomendaciones para el uso de Aplicación EcoStruxure Power Device

Para restringir el acceso a la unidad de control MicroLogic X desde un smartphone en el que se ejecute Aplicación EcoStruxure Power Device, se recomienda utilizar únicamente la Aplicación EcoStruxure Power Device oficial de Schneider Electric para conectarse al interruptor automático MasterPact MTZ.

Recomendaciones para el uso de smartphones

Para restringir el acceso a la unidad de control MicroLogic X desde un smartphone, se recomienda:

- Asegurarse de que los smartphones que dispongan de Aplicación EcoStruxure Power Device estén protegidos con contraseña y se utilicen solo para el trabajo.
- Proteger los smartphones en los que se haya instalado Aplicación EcoStruxure Power Device implementando todas las funciones de seguridad recomendadas por el proveedor o el fabricante del smartphone.
- Mantener actualizadas las aplicaciones antivirus para smartphones.
- No facilitar información acerca del smartphone (número de teléfono, dirección MAC) a menos que sea estrictamente necesario.
- Desconectar el smartphone de Internet durante la conexión Bluetooth con la unidad de control MicroLogic X.
- No almacenar información confidencial en un smartphone.

Recomendaciones para proteger el acceso a la unidad de control MicroLogic X a través del puerto mini USB

Funciones accesibles a través del puerto mini USB

Es posible acceder a todas las funciones de la unidad de control MicroLogic X al:

- Conectar un PC en el que se ejecute el software EcoStruxure Power Commission al puerto mini USB de la unidad de control.
- Conectar un smartphone en el que se ejecute Aplicación EcoStruxure Power Device al puerto mini USB de la unidad de control a través de un adaptador USB OTG.

Tenga en cuenta que la función de almacenamiento masivo no se implementa en la unidad de control. Por lo tanto, no es posible atacar el sistema descargando malware desde una memoria USB u otro dispositivo de almacenamiento masivo.

Requisitos previos para establecer una conexión USB o USB OTG

Para establecer una conexión USB con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- Debe disponer de acceso físico a la sala en la que se encuentra el interruptor automático MasterPact MTZ.
- Para una conexión desde un PC:
  - Debe disponer de un cable USB con un conector mini USB para conectar su PC al puerto mini USB de la unidad de control MicroLogic X.
  - Debe disponer de un PC en el que se ejecute el software EcoStruxure Power Commission.
- Para una conexión desde un smartphone:
  - Debe contar con un adaptador OTG y un cable USB con un conector mini USB para conectar el smartphone al puerto mini USB de la unidad de control MicroLogic X.
  - Debe disponer de un smartphone en el que se ejecute Aplicación EcoStruxure Power Device.

Recomendaciones generales para proteger el acceso a través del puerto mini USB

Para proteger el acceso a las funciones a las que se puede acceder a través del puerto mini USB de la unidad de control MicroLogic X, se recomienda:

- Instalar el interruptor automático MasterPact MTZ en un área cerrada para que ninguna persona sin autorización pueda acceder a la unidad de control MicroLogic X.
- Mantener el área cerrada en todo momento.
- Facilitar la llave o el código de acceso únicamente a personal autorizado.

Para obtener más información, consulte las recomendaciones para restringir el acceso local al interruptor automático MasterPact MTZ *(véase página 20)*.

Recomendaciones para PC que en los que se ejecuta el software EcoStruxure Power Commission

Para proteger el acceso a la unidad de control MicroLogic X desde un PC conectado localmente al puerto mini USB de la parte frontal de la unidad de control, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que los PC en los que se ejecute el software EcoStruxure Power Commission requieran un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras *(véase página 15)*.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger los PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite utilizar el software EcoStruxure Power Commission.
- Mantener actualizadas las aplicaciones antivirus para PC.

Recomendaciones para smartphones en los que se ejecute Aplicación EcoStruxure Power Device

Para proteger el acceso a la unidad de control MicroLogic X desde un smartphone conectado localmente al puerto mini USB de la parte frontal de la unidad de control, se recomienda:

- Asegurarse de que los smartphones en los que se ejecuta Aplicación EcoStruxure Power Device estén protegidos con contraseña y se utilicen solo para el trabajo.
- Proteger los smartphones en los que se haya instalado Aplicación EcoStruxure Power Device implementando todas las funciones de seguridad recomendadas por el proveedor o el fabricante del smartphone.
- Mantener actualizadas las aplicaciones antivirus para smartphones.
- No facilitar información sobre el smartphone (número de teléfono, dirección MAC) a menos que sea estrictamente necesario.
- Desconectar el smartphone de Internet durante la conexión USB OTG con la unidad de control MicroLogic X.
- No almacenar información confidencial en un smartphone.

Capítulo 4
Recomendaciones de ciberseguridad para el acceso remoto

Descripción general del capítulo

Este capítulo ofrece una lista de las rutas de acceso remotas al interruptor automático MasterPact MTZ. También proporciona recomendaciones para proteger estas rutas de acceso. Son cuestiones importantes que tener en cuenta para el funcionamiento.

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Restricción del acceso remoto al interruptor automático MasterPact MTZ

Descripción general

La unidad funcional modular inteligente (IMU) de MasterPact MTZ ofrece posibilidades de acceso local y remoto. Debe asegurarse de que solo se otorgue acceso a usuarios autorizados.

Acceso remoto al interruptor automático MasterPact MTZ

Según la arquitectura de su sistema, probablemente haya varios modos de obtener acceso remoto al interruptor automático MasterPact MTZ.

Es sumamente importante controlar el acceso remoto a su sistema, pues el acceso remoto a través de las siguientes rutas de comunicación puede otorgar control total sobre su instalación:

- Software EcoStruxure Power Commission mediante una conexión Ethernet con una interfaz de IFE, EIFE o IFM
- Software EcoStruxure Power Commission mediante Modbus-SL con una interfaz de IFM
- Páginas web de IFE o EIFE mediante una conexión Ethernet con una interfaz IFE o EIFE

Concretamente, debe tener en cuenta lo siguiente:

- Cómo se puede acceder al sistema utilizando las distintas rutas de comunicación disponibles *(véase página 12)*
- La información y los controles disponibles a través de cada ruta de acceso *(véase página 14)*

Activación y desactivación del control remoto del interruptor automático MasterPact MTZ

El control remoto del interruptor automático MasterPact MTZ hace referencia a las operaciones siguientes:

- Apertura, cierre y restablecimiento del interruptor automático
- Modificación de los ajustes del interruptor automático

Si el control remoto del interruptor automático MasterPact MTZ no es un requisito, es muy recomendable desactivar el control remoto utilizando las interfaces de IFE o EIFE, el servidor IFE o la interfaz de IFM. El control remoto está activado de forma predeterminada.

En la interfaz de IFE o el servidor IFE, utilice el conmutador de bloqueo del panel frontal para activar o desactivar los comandos de control remoto enviados mediante la red Ethernet.

En la interfaz de EIFE, conecte un PC en el que se ejecute el software EcoStruxure Power Commission al puerto mini USB de la parte frontal de la unidad de control MicroLogic X para activar o desactivar el control remoto del interruptor automático MasterPact MTZ a través de la red Ethernet.

En la interfaz de IFM, utilice el conmutador de bloqueo del panel frontal para activar o desactivar los controles remotos enviados mediante la red Modbus-SL.

Bloqueo de los ajustes de protección

Puede bloquear los ajustes de protección del interruptor automático MasterPact MTZ para evitar que se cambien remotamente. De forma predeterminada, se permite el cambio remoto de los ajustes de protección.

Se recomienda desactivar la modificación remota de los ajustes de protección si no utiliza esta función. Si desea más información, consulte *DOCA0102EN MasterPact MTZ - MicroLogic X - Unidad de control - Guía del usuario*.

Separación de la red OT y la red corporativa

Descripción general

En el diseño y la implementación de su red de tecnología operativa, debe utilizar mecanismos de segregación para mantenerla separada de su red corporativa. Esto le ayudará a restringir el acceso a la unidad funcional modular inteligente de MasterPact MTZ.

Concretamente, debe tener en cuenta lo siguiente:

- Uso de cortafuegos
- Creación de zonas desmilitarizadas
- Uso de dispositivos de sistema de detección de intrusiones (IDS) o sistema de prevención de intrusiones (IPS)
- Implementación de políticas de seguridad y programas de formación
- Definición de mecanismos de respuesta frente a incidentes

Diversas organizaciones especializadas (por ejemplo, NIST) y organismos de normalización (por ejemplo, ISO, IEC/IEEE) publican y actualizan directrices para diseñar una red de tecnología operativa y mantenerla separada de la intranet corporativa. Consulte estas publicaciones para abordar los puntos indicados anteriormente.

Recomendaciones para proteger el acceso a la unidad de control MicroLogic X a través de Ethernet

Funciones accesibles a través de Ethernet

Cuando un PC en el que se ejecuta el software de supervisión y control (software SCADA, EcoStruxure Power Commission) está conectado a la red Ethernet, se puede acceder a todas las funciones de la unidad de control MicroLogic X en las siguientes situaciones:

- El interruptor automático MasterPact MTZ está conectado a una interfaz de IFE o un servidor IFE.
- El interruptor automático MasterPact MTZ incluye la interfaz de EIFE.
- El interruptor automático MasterPact MTZ está conectado a una interfaz de IFM apilada en un servidor IFE.

Requisitos previos para establecer una conexión Ethernet

Para establecer una conexión Ethernet con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- La unidad de control MicroLogic X debe estar encendida
- La unidad de control MicroLogic X se debe conectar a una red Ethernet a través de una de las interfaces siguientes:
  - Una interfaz de IFE o EIFE
  - Un servidor IFE
  - Una interfaz de IFM apilada en un servidor IFE
- Debe disponer de un PC u otro dispositivo (por ejemplo, pantalla FDM128 o PLC) en el que se ejecute el software de control y supervisión (SCADA, EcoStruxure Power Commission) conectado a la red Ethernet, que ofrezca acceso remoto
- Debe tener un PC con un navegador conectado a la red Ethernet, que ofrezca acceso a las páginas web de IFE o EIFE
- Debe disponer de un ID de usuario y una contraseña con los permisos de acceso adecuados para iniciar sesión en:
  - Páginas web de las interfaces de IFE y EIFE
  - Páginas web del servidor IFE
- Debe disponer de un ID de usuario y una contraseña con los permisos de acceso adecuados para iniciar sesión en el software EcoStruxure Power Commission

Recomendaciones para PC conectados a Ethernet

Para proteger el acceso a la unidad de control MicroLogic X desde un PC conectado en red, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que el PC que ofrece acceso a la unidad de control MicroLogic X usando Ethernet (por ejemplo, a través de las páginas web de las interfaces de IFE o EIFE, las páginas web del servidor IFE o SCADA) requiera un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras *(véase página 16)*.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger el PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite acceder a la unidad de control MicroLogic X desde un PC en red.
- Mantener actualizadas las aplicaciones antivirus para PC.

Además de las precauciones anteriores, también debe seguir las directrices y recomendaciones generales para proteger su instalación que se proporcionan en *How Can I Reduce Vulnerability to Cyber Attacks?*.

Recomendaciones para proteger el acceso remoto a la unidad de control MicroLogic X a través de Modbus-SL

Funciones accesibles a través de Modbus-SL

Cuando un PC en el que se ejecuta el software de supervisión y control (SCADA) se conecta a la red Modbus-SL, se puede acceder a todas las funciones de la unidad de control MicroLogic X cuando el interruptor automático MasterPact MTZ está conectado a una interfaz de IFM.

Requisitos previos para establecer una conexión Modbus-SL

Para establecer una conexión Modbus-SL con la unidad de control MicroLogic X, los requisitos previos son los siguientes:

- La unidad de control MicroLogic X debe estar encendida.
- La unidad de control MicroLogic X se debe conectar a una interfaz de IFM.
- Debe disponer de un PC u otro dispositivo (por ejemplo, PLC) en el que se ejecute el software de control y supervisión (SCADA) conectado a la red Modbus-SL que brinda acceso remoto.
- Debe disponer de un ID de usuario y una contraseña con los permisos de acceso adecuados para iniciar sesión en el software EcoStruxure Power Commission.

Recomendaciones para PC conectados a Modbus-SL

Para proteger el acceso a la unidad de control MicroLogic X desde un PC conectado en red, se recomienda:

- Mantener los PC bloqueados mientras no se utilicen.
- Asegurarse de que el PC que ofrece acceso a la unidad de control MicroLogic X usando Modbus-SL (por medio de SCADA, por ejemplo) requiera un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras *(véase página 16)*.
- Asegurarse de que las contraseñas de usuario se cambien periódicamente.
- Prohibir la reutilización de contraseñas antiguas.
- Ajustar un temporizador para bloquear la pantalla del PC tras un periodo de inactividad.
- Proteger el PC siguiendo las directrices más recientes del proveedor para el sistema operativo que se ejecute en el PC.
- Limitar el número de usuarios a los que se permite acceder a la unidad de control MicroLogic X desde un PC en red.
- Mantener actualizadas las aplicaciones antivirus para PC.

Además de las precauciones anteriores, también debe seguir las directrices y recomendaciones generales para proteger su instalación que se proporcionan en *How Can I Reduce Vulnerability to Cyber Attacks?*.

Capítulo 5
Recomendaciones de ciberseguridad para actualizaciones de firmware y Digital Module

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Instalación de actualizaciones de firmware

Descripción general

Un ciberataque cada vez más común consiste en la distribución de paquetes de software manipulados o ilegítimos que pueden contener aplicaciones modificadas o adicionales. Estas aplicaciones pueden poner en peligro la integridad del software original y su uso previsto.

Para contribuir a garantizar la integridad y la autenticidad de todos los componentes de la IMU de MasterPact MTZ, es decir, la unidad de control MicroLogic X, el servidor IFE, las interfaces de IFE o EIFE, la interfaz de IFM y el módulo IO, todo el firmware original de Schneider Electric está firmado digitalmente.

Actualice todo el firmware usando el software EcoStruxure Power Commission. Debe tener la última versión del software EcoStruxure Power Commission. Utilice el software EcoStruxure Power Commission para actualizar todo el firmware a través del menú del firmware.

Recomendaciones de ciberseguridad referentes a actualizaciones de firmware

⚠ ADVERTENCIA

RIESGO DE FUNCIONAMIENTO IMPREVISTO

- Actualice la versión del software EcoStruxure Power Commission en cuanto reciba una notificación que le indique que hay una actualización disponible.
- Utilice esta última versión del software EcoStruxure Power Commission para actualizar el firmware de todos sus productos.
- Consulte de forma periódica la lista de revocación de certificados que se publica en el sitio web oficial de Schneider Electric. Si hay un certificado revocado para uno de sus productos, no instale firmware de una fecha anterior a la de la revocación.

El incumplimiento de estas instrucciones puede causar la muerte, lesiones serias o daño al equipo.

Al instalar actualizaciones de firmware para componentes de la IMU de MasterPact MTZ, se recomienda:

- Solo use la última versión del software EcoStruxure Power Commission para descargar e instalar las actualizaciones del firmware.
- Proteja el PC en el que se ejecuta el software EcoStruxure Power Commission siguiendo las directrices más recientes del proveedor para el sistema operativo.
- Instale actualizaciones siguiendo las prácticas de tecnología operativa (OT) aceptadas, como la prueba en un sistema que no sea de producción (si es posible) para la validación antes de instalarlas e implementarlas en el entorno de producción.

Consulte la nota de la versión *(véase página 7)* correspondiente para comprobar si la actualización más reciente ofrece mejoras de ciberseguridad. Si es así, le recomendamos que se actualice a esta versión.

Firmware firmado

Todo el firmware diseñado para la IMU de MasterPact MTZ se firma con la infraestructura de claves públicas (PKI) de Schneider Electric. Las firmas digitales se autentican utilizando el certificado público que hay en el software EcoStruxure Power Commission.

Cuando se carga el firmware en la IMU de MasterPact MTZ a través del software EcoStruxure Power Commission, la unidad de control MicroLogic X también verifica automáticamente la firma digital del paquete de actualización. Esta verificación se lleva a cabo a través del certificado público presente en la unidad de control.

Por motivos de seguridad, los certificados públicos están sujetos a cambios. Por lo tanto, es un requisito de seguridad de primer orden (y es su responsabilidad) comprobar que la versión del software EcoStruxure Power Commission utilizada para descargar e instalar actualizaciones de firmware sea la última versión. Si cuenta con la última versión del software EcoStruxure Power Commission, los certificados públicos utilizados para firmar el firmware están actualizados.

Los certificados que ya no son válidos se publican en la lista de revocación de certificados (CRL) disponible en el sitio web oficial de *Schneider Electric*.

Ventajas del uso del software EcoStruxure Power Commission para las actualizaciones de firmware

El software EcoStruxure Power Commission desempeña una función importante para ayudar a garantizar la integridad de su red de tecnología operativa durante las actualizaciones de firmware. Utilice solo la última versión del software EcoStruxure Power Commission para descargar e instalar el firmware, ya que es el único software que puede ofrecer las siguientes ventajas:

- Al descargar los paquetes de firmware del centro de descargas oficial de Schneider Electric utilizando el software EcoStruxure Power Commission, la firma digital de los paquetes se verifica automáticamente.
- Al cargar firmware en la unidad de control MicroLogic X (utilizando el software EcoStruxure Power Commission con una conexión USB o Ethernet), la firma digital del paquete de actualización se verifica automáticamente.

Las verificaciones automáticas realizadas por el software EcoStruxure Power Commission dependen completamente de la validez del certificado público que utiliza.

Consulte *DOCA0144EN MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note* para conocer los procedimientos detallados en los que se explica cómo actualizar el firmware MicroLogic X.

Compra e instalación de Digital Modules

Descripción general

Digital Modules son módulos opcionales que amplían las funciones disponibles a través de la gama de unidades de control MicroLogic X. Se pueden comprar junto con el interruptor automático MasterPact MTZ en el pedido inicial o en una fecha posterior en el mercado GoDigital online de Schneider Electric.

Todos los Digital Modules diseñados para la unidad de control MicroLogic X están firmados digitalmente para aumentar la seguridad utilizando la infraestructura de clave pública (PKI) de Schneider Electric. La PKI ayuda a garantizar la autenticidad y la integridad de estas descargas. Los Digital Modules se deben instalar utilizando el software EcoStruxure Power Commission.

Recomendaciones de ciberseguridad para la compra de Digital Modules

Para comprar Digital Modules para la unidad de control MicroLogic X, utilice únicamente el mercado GoDigital del centro de descargas oficial de Schneider Electric.

Al instalar Digital Modules para componentes de la IMU de MasterPact MTZ, se recomienda:

- Instalar Digital Modules siguiendo las prácticas de tecnología operativa (OT) aceptadas, como la prueba en un sistema que no sea de producción, para la validación antes de instalarlos e implementarlos en el entorno de producción.
- Usar solo la última versión del software EcoStruxure Power Commission para descargar e instalar Digital Modules.
- Proteger los PC utilizados para descargar e instalar Digital Modules siguiendo las directrices más recientes del proveedor para el sistema operativo.

Recomendaciones de ciberseguridad para la instalación de Digital Modules

⚠ ADVERTENCIA

RIESGO DE FUNCIONAMIENTO IMPREVISTO

- Actualice la versión del software EcoStruxure Power Commission en cuanto reciba una notificación que le indique que hay una actualización disponible.
- Utilice esta última versión del software EcoStruxure Power Commission para actualizar el firmware de todos sus productos.
- Consulte de forma periódica la lista de revocación de certificados que se publica en el sitio web oficial de Schneider Electric. Si hay un certificado revocado para uno de sus productos, no instale firmware de una fecha anterior a la de la revocación.

El incumplimiento de estas instrucciones puede causar la muerte, lesiones serias o daño al equipo.

Solo debe usar el software EcoStruxure Power Commission para instalar Digital Modules para la unidad de control MicroLogic X.

El software EcoStruxure Power Commission desempeña una función importante para ayudar a garantizar la integridad de la red de tecnología operativa. Utilice solo la última versión del software EcoStruxure Power Commission para instalar Digital Modules, ya que es el único software que puede ofrecer las siguientes ventajas:

- Cuando actualice el firmware de un dispositivo de IMU usando el software EcoStruxure Power Commission con una conexión USB o Ethernet, la firma digital de la actualización del firmware se verifica automáticamente.
- Al cargar un Digital Module en la unidad de control MicroLogic X utilizando software EcoStruxure Power Commission con una conexión USB, la firma digital de Digital Module se verifica automáticamente.

Las verificaciones automáticas realizadas por el software EcoStruxure Power Commission dependen completamente de la validez del certificado público utilizado.

Consulte *DOCA0144EN MasterPact MTZ MicroLogic X Control Unit - Firmware Release Note* para tener acceso a los procedimientos detallados que explican cómo descargar e instalar Digital Modules.

Cybersecurity Support Portal de Schneider Electric

Descripción general

El *cybersecurity support portal* de Schneider Electric describe la política de gestión de vulnerabilidad de Schneider Electric.

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

Schneider Electric trabaja junto a investigadores, equipos de CERT (del inglés Cyber Emergency Response Team, equipo de respuesta ante ciberemergencias) y propietarios de equipos para asegurar que se proporcione información precisa de manera oportuna para proteger correctamente las instalaciones.

El equipo CPCERT (del inglés Corporate Product Cyber Emergency Response Team, equipo de respuesta ante ciberemergencias para productos corporativos) de Schneider Electric es responsable de administrar y emitir alertas sobre vulnerabilidades y mitigaciones que afectan a productos y soluciones.

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

Información disponible en 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 informar sobre incidentes o vulnerabilidades de ciberseguridad.

Glosario

B

BLE - Bluetooth low energy

Una tecnología de red de área personal inalámbrica que reduce el consumo de energía.

C

Conectividad ULP

ULP es un enlace rápido de comunicación dedicado a la supervisión y el control de interruptores automáticos. Conecta el interruptor automático a una interfaz de Ethernet o a un módulo IO. ULP funciona a una velocidad de 1 Mb/s y es plug and play.

G

GoDigital

El mercado online de Schneider Electric para comprar Digital Modules diseñados para la unidad de control MicroLogic X.

H

HMI: interfaz hombre-máquina

Hace referencia a las pantallas de la parte frontal de un dispositivo que un operador puede utilizar para leer información o configurar el dispositivo.

I

IFM

La interfaz Modbus-SL de IFM permite que una IMU se conecte a una red Modbus de línea serie RS 485 de dos hilos. Cada IMU tiene su propia interfaz IFM y dirección Modbus correspondiente.

IMU: unidad funcional modular inteligente

En el caso del interruptor automático MasterPact MTZ, IMU hace referencia al propio interruptor automático, la unidad de control MicroLogic X y los módulos ULP asociados, las interfaces IFE, EIFE y IFM y el módulo IO.

Interfaz de EIFE

Interfaz de Ethernet integrada que es un módulo opcional del interruptor automático seccionable MasterPact MTZ. Con este módulo, se puede acceder al interruptor automático por medio de la intranet de la empresa.

Interfaz de IFE

Interfaz de IFE Ethernet para un interruptor automático que se puede conectar al interruptor automático MasterPact MTZ. Con este módulo, se puede acceder al interruptor automático por medio de páginas web.

IP : protocolo de Internet

Las direcciones IP se utilizan para identificar dispositivos conectados a la intranet de la empresa o a Internet.

L

LAN : red de área local

Hace referencia a la intranet o la red de TI de la empresa.

N

NFC - Near field communication

Hace referencia a un protocolo de comunicación inalámbrica.

O

OT: tecnología operativa

Hace referencia a los sistemas de hardware y software que la empresa utiliza para supervisar y controlar directamente los procesos y equipos de producción, lo que también se conoce como red de control industrial (IC). OT se suele utilizar para hacer referencia a la red operativa de la empresa, en contraposición a su red de TI.

P

PIN: número de identificación personal

Código formado por números o letras que se usa para verificar la identidad de la persona que accede a un sistema informático.

PKI: infraestructura de clave pública

Define un conjunto de servicios que se utilizan para generar y autenticar firmas digitales. Una infraestructura de clave pública está diseñada para garantizar la confidencialidad, la integridad y la autenticidad de la información.

Política de seguridad

La política de seguridad de un sistema es la configuración de seguridad aplicada en todo el sistema protegido. Las políticas de seguridad suelen hacer referencia al uso de normas. Se usan para definir la configuración de seguridad compartida por todos los dispositivos. Ejemplos de políticas de seguridad son el registro de eventos de seguridad según la norma BDEW y el uso de contraseñas NERC.

R

RBAC: control de acceso basado en funciones

Un método para restringir el acceso a los recursos a los usuarios autorizados. RBAC es una alternativa al control de acceso obligatorio (MAC) y al control de acceso discrecional (DAC) tradicionales.

S

SCADA - Supervisory control and data acquisition

Hace referencia a los sistemas diseñados para obtener datos en tiempo real sobre los procesos y equipos de producción para supervisarlos y controlarlos remotamente.

Servidor IFE

Servidor de panel IFE Ethernet que se puede conectar a más de un interruptor automático MasterPact MTZ. Con este módulo, se puede acceder a los interruptores automáticos por medio de páginas web.

Syslog

Protocolo que define el servicio de registros de eventos del sistema y cómo intercambiar estos registros.

T

TCP/IP - Transmission control protocol/Internet protocol

Hace referencia al conjunto de protocolos que se utilizan para las comunicaciones por Internet.

TI : tecnología de la información

Hace referencia a los sistemas de información y a la red de información de la empresa en contraposición a su red de OT (tecnología operativa).

V

VPN: red privada virtual

Las VPN se utilizan para establecer un "túnel" protegido o privado entre un punto de acceso externo autenticado y la red empresarial de confianza.