Masterpact MTZ

Guía de ciberseguridad

06/2017

DOCA0122ES-01

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.

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.

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

- Cambie las contraseñas predeterminadas para evitar accesos no autorizados a la configuración 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 cortafuegos, segmentación de red y protección y detección de intrusiones en la red).
- Siga las prácticas recomendadas de ciberseguridad (por ejemplo, privilegio mínimo, separación de tareas) para evitar exposición no autorizada, pérdida, modificación de datos y registros, o interrupción 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 control industrial 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.

Documentos relacionados

Título de la documentación	Número de referencia
Micrologic X - Unidad de control - Guía del usuario	DOCA0102EN DOCA0102ES DOCA0102FR DOCA0102ZH
How Can I Reduce Vulnerability to Cyber Attacks?	Cybersecurity System Technical Note

Puede descargar estas publicaciones técnicas e información técnica adicional de nuestro sitio web *http://www.schneider-electric.com/en/download*.

Aviso de marca registrada

Todas las marcas registradas 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 siguiente nota técnica del sistema:

- *How Can I Reduce Vulnerability to Cyber Attacks?*

Además, encontrará muchos recursos útiles e información actualizada sobre la seguridad en una página específica del sitio web global de *Schneider Electric*.

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

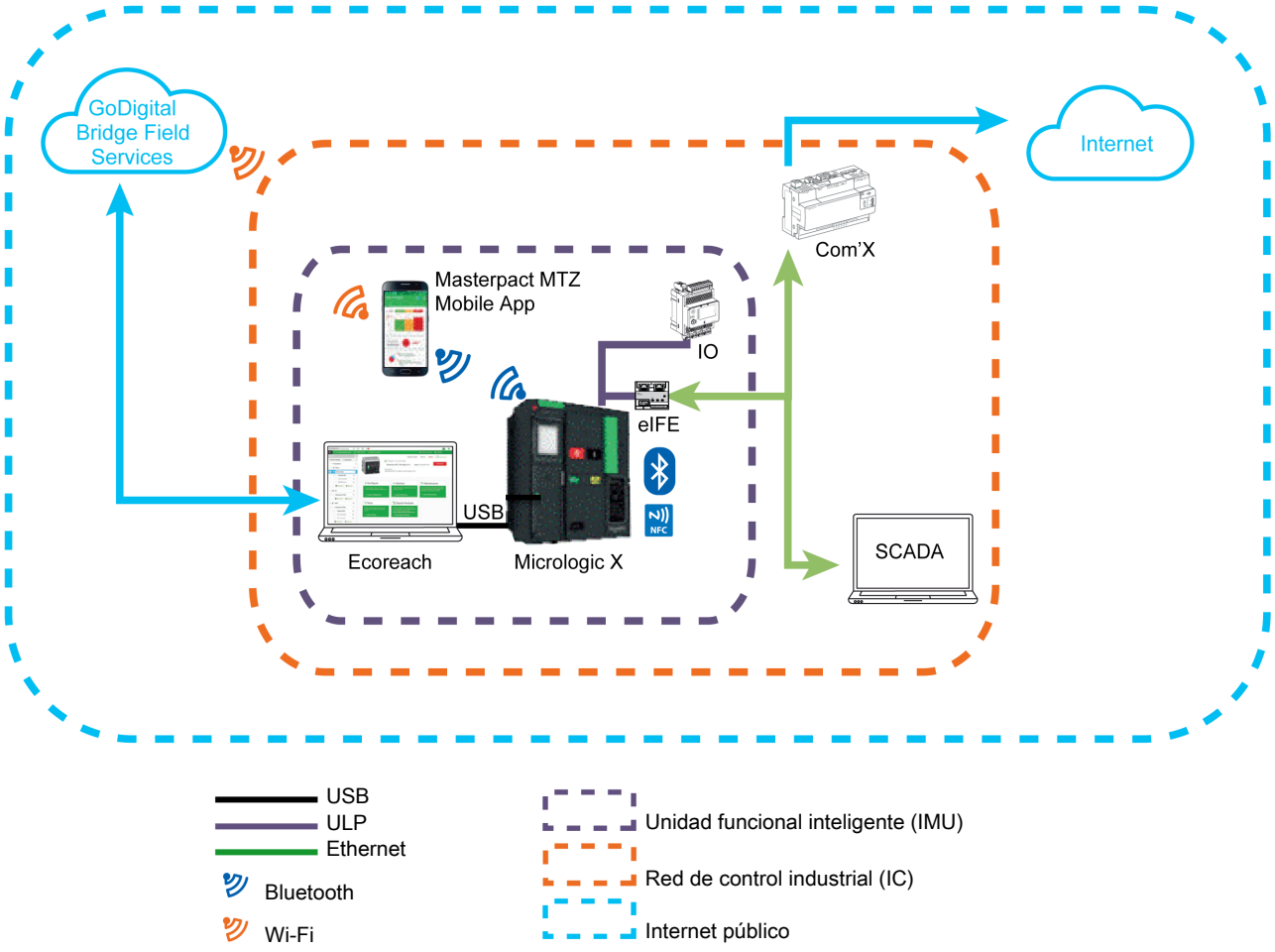
Descripción general

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 seguridad 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 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 de USB de la unidad de control Micrologic X desde:
  - Un PC que ejecute el software Ecoreach
  - Un smartphone que ejecute la aplicación móvil de Masterpact MTZ
- Conexión de Ethernet a través de la red de control industrial (IC) cuando la interfaz de comunicación está presente
- Conexión de Modbus-SL a través de la red de control industrial (IC) cuando la interfaz IFM está presente.

Vulnerabilidad del sistema frente a ciberataques

Cada una de las rutas de comunicación indicadas anteriormente representa un punto potencialmente vulnerable del sistema. 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 control industrial (IC) que incluya la unidad funcional inteligente (IMU) de Masterpact MTZ. Las recomendaciones y directrices incluidas en este capítulo ayudan a promover un entorno de funcionamiento seguro.

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Identificación y protección de información confidencial y operaciones

Descripción general

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

Como principio general, la información confidencial incluye:

- Cualquier información que se pueda utilizar para acceder a su instalación y a su red de control industrial
- 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 beneficio 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 industrial se encuentra la siguiente:

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

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 accesible a través de cada ruta de acceso

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

Operaciones de información y 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:

- Realizar ciertas tareas 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 Ecoreach
- Acceder a las páginas web IFE y EIFE

Contraseña para ajustes y controles críticos de Micrologic X

Al acceder a la unidad de control Micrologic X, cualquier comando 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, cada una de las cuales corresponde a un nivel.

Se asigna un nivel a una función:

- Los niveles 1, 2 y 3 se utilizan para funciones generales, como una función de operador.
- El nivel 4 es el del administrador. El nivel de administrador es obligatorio para escribir los ajustes en las unidades de control Micrologic X utilizando el software Ecoreach.

Cuando se realiza la conexión por medio de Masterpact MTZ Mobile App o el software Ecoreach, 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"

Estas contraseñas se deben cambiar periódicamente después de la primera instalación del interruptor automático Masterpact MTZ, utilizando el software Ecoreach. Sólo se deben compartir con un número limitado de usuarios de confianza. Siga las recomendaciones de la política de contraseñas que se indican a continuación cuando corresponda.

Contraseñas e ID de usuario para PC en red

Los PC en los que se ejecuta el software Ecoreach o que acceden a la unidad de control Micrologic X utilizando cualquier otro medio (por ejemplo, páginas web 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.

Vea las recomendaciones referentes a la política de contraseñas a continuación.

Contraseñas para páginas web IFE y EIFE

Los usuarios de las páginas web IFE y EIFE tienen un ID de usuario personal y una contraseña para iniciar sesión en estas páginas web. Deben cambiar la contraseña después de iniciar sesión por primera vez en las páginas web IFE y EIFE.

Debe definir qué usuarios de su organización requieren un nombre de usuario para iniciar sesión en las páginas web IFE y EIFE y seguir estas recomendaciones de la política de contraseñas.

Recomendaciones de ciberseguridad referentes a la política de contraseñas

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
- Prohibir la reutilización de contraseñas antiguas
- Recordar periódicamente a los usuarios las prácticas recomendadas sobre las contraseñas

Para proteger su PC y todo el software que se ejecuta en él, como mínimo debe:

- 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 180 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

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 o sensible 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 conveniencia

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 inteligente (IMU) de Masterpact MTZ ofrece posibilidades de acceso local y remoto. Debe asegurarse de que sólo se otorgue acceso a usuarios autorizados.

Acceso local al interruptor automático Masterpact MTZ

El acceso local a la unidad funcional 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 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 la Masterpact MTZ Mobile App
- 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 en la unidad de control Micrologic X, que supone el riesgo de que se realicen cambios en los ajustes desde el software Ecoreach o un smartphone con Masterpact MTZ Mobile App
- 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.
- Sólo 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 en 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 de la HMI.

Se recomienda desactivar la modificación local de los ajustes de protección de la HMI si no se utiliza esta función. Consulte la publicación *Micrologic X - Unidad de control - Guía del usuario* para obtener instrucciones.

Recomendaciones para proteger el acceso a través de NFC

Funciones accesibles a través de NFC

Por medio de la comunicación de campo cercano (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 disponer de acceso físico a la sala en la que se encuentra el interruptor automático Masterpact MTZ.
- La Masterpact MTZ Mobile App 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.

Para conocer el procedimiento detallado para establecer una conexión NFC consulte la publicación *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 introduzca un código de emparejamiento si se le solicita, porque no es necesario para una conexión NFC.

Recomendaciones para el uso de Masterpact MTZ Mobile App

Para restringir el acceso a la unidad de control Micrologic X desde un smartphone en el que se ejecute Masterpact MTZ Mobile App, se recomienda utilizar únicamente la Masterpact MTZ Mobile App 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:

- Asegúrese de que los smartphones que dispongan de Masterpact MTZ Mobile App estén protegidos con contraseña y se utilicen sólo para el trabajo.
- Proteger los smartphones en los que se haya instalado la Masterpact MTZ Mobile App 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

- Sólo 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 a 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 Bluetooth low energy (BLE), puede acceder a la unidad de control Micrologic X desde un smartphone que esté ejecutando la Masterpact MTZ Mobile App. Esta aplicación ofrece una interfaz orientada a tareas de 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 en la unidad de control Micrologic X debe estar activada.
- Sólo se puede conectar un smartphone a una unidad de control a la vez.
- Debe tener un smartphone con la Masterpact MTZ Mobile App 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 dentro del alcance 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 la instalación.

Para conocer los procedimientos detallados para establecer una conexión Bluetooth consulte la publicación *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 *Micrologic X - Unidad de control - Guía del usuario*, y activarla sólo 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 hacerlo de forma imprevista.
- Durante el emparejamiento de Bluetooth, mantenga el smartphone lo más cercano posible a la unidad de control Micrologic X.

Recomendaciones para el uso de Masterpact MTZ Mobile App

Para restringir el acceso a la unidad de control Micrologic X desde un smartphone en el que se ejecute Masterpact MTZ Mobile App, se recomienda utilizar únicamente la Masterpact MTZ Mobile App 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:

- Asegúrese de que los smartphones que dispongan de Masterpact MTZ Mobile App estén protegidos con contraseña y se utilicen sólo para el trabajo.
- Proteger los smartphones en los que se haya instalado la Masterpact MTZ Mobile App 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.
- Desconecte el smartphone de Internet durante la conexión Bluetooth con la unidad de control Micrologic X.
- No almacene 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 Ecoreach al puerto mini USB de la unidad de control.
- Conectar un smartphone en el que se ejecute Masterpact MTZ Mobile App en el 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 Ecoreach.
- 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 en la unidad de control Micrologic X.
  - Debe disponer de un smartphone en el que se ejecute Masterpact MTZ Mobile App.

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 USB en 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 Ecoreach

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 Ecoreach requieran un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras *(véase página 16)*.
- Asegurarse de que las contraseñas 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 Ecoreach.
- Mantener actualizadas las aplicaciones antivirus para PC.

Recomendaciones para smartphones en los que se ejecute Masterpact MTZ Mobile App

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

- Asegurarse de que los smartphones en los que se ejecuta Masterpact MTZ Mobile App estén protegidos con contraseña y se utilicen sólo para el trabajo.
- Proteger los smartphones en los que se haya instalado Masterpact MTZ Mobile App 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 inteligente (IMU) de Masterpact MTZ ofrece posibilidades de acceso local y remoto. Debe asegurarse de que sólo 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. Concretamente, el acceso remoto por medio de Ethernet o Modbus-SL puede ofrecerle control total de su instalación. Por lo tanto, es sumamente importante controlar el acceso remoto al sistema.

Concretamente, debe tener en cuenta lo siguiente:

- Cómo se puede acceder al sistema utilizando las distintas rutas de comunicación disponibles *(véase página 11)*
- 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 rearme 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 la interfaz IFE, EIFE o IFM. El control remoto está activado de forma predeterminada.

En la interfaz IFE, utilice el conmutador de bloqueo del panel frontal para activar o desactivar los controles remotos enviados por la red Ethernet.

En la interfaz EIFE, conecte un PC en el que se ejecute el software Ecoreach 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 IFM , utilice el conmutador de bloqueo del panel frontal para activar o desactivar los controles remotos enviados por 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. Consulte la publicación *Micrologic X - Unidad de control - Guía del usuario* para obtener instrucciones.

Separación de la red IC y la red corporativa

Descripción general

En el diseño y la implementación de su red de control industrial, debe utilizar mecanismos de segregación para mantenerla separada de su red corporativa. Esto le ayudará a restringir el acceso a la unidad funcional 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 control industrial 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 Ecoreach 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 IFE.
- El interruptor automático Masterpact MTZ incluye la interfaz EIFE.
- El interruptor automático Masterpact MTZ está conectado a una interfaz 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 IFE
  - Una interfaz EIFE
  - Una interfaz IFM apilada en un servidor IFE
- Debe disponer de un PC u otro dispositivo (por ejemplo, FDM128 o PLC) en el que se ejecute un software de control y supervisión (SCADA, Ecoreach) conectado a la red Ethernet que ofrezca acceso remoto.
- Debe disponer de un ID y una contraseña con los permisos de acceso adecuados para iniciar sección en el software Ecoreach.

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 IFE o EIFE, o SCADA) requiera un nombre de usuario y una contraseña.
- Aplicar el uso de contraseñas seguras *(véase página 15)*.
- Asegurarse de que las contraseñas 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 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 Ecoreach 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 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 IFM.
- Debe disponer de un PC u otro dispositivo (por ejemplo, PLC) en el que se ejecute el software de control y supervisión (SCADA, Ecoreach) conectado a la red Modbus-SL que brinda acceso remoto.
- Debe disponer de un ID y una contraseña con los permisos de acceso adecuados para iniciar sección en el software Ecoreach.

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 15)*.
- Asegurarse de que las contraseñas 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 módulos digitales

Contenido de este capítulo

Este capítulo contiene los siguientes apartados:

Instalar las 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 de todos los componentes de la IMU de Masterpact MTZ, es decir, la unidad de control Micrologic X, la interfaz IFE, EIFE o IFM , y el módulo IO, todas las actualizaciones del firmware original de Schneider Electric están firmadas digitalmente.

Actualice todos los firmware usando el software Ecoreach. Debe tener la última versión del software Ecoreach. Utilice el software Ecoreach para actualizar todos los firmware a través del menú del firmware. Los documentos de Ecoreach se pueden descargar del sitio de descarga de Schneider Electric (*https://www.schneider-electric.com/en/download/*).

Recomendaciones de ciberseguridad referentes a actualizaciones de firmware

Es fundamental instalar la última versión de firmware.

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

- Instalar actualizaciones que se ciñan a las prácticas de tecnología operativa (TO), como la prueba en un sistema que no sea de producción para la validación antes de instalarlas y desplegarlas en el entorno de producción.
- Sólo use la última versión del software Ecoreach para descargar e instalar las actualizaciones del firmware.
- Proteja el PC en el que se ejecuta el software Ecoreach siguiendo las directrices más recientes del proveedor para el sistema operativo.

Firmware firmado

Todo el firmware diseñado para la IMU de Masterpact MTZ está firmado con la infraestructura de clave pública de Schneider Electric. Las firmas digitales se autentican utilizando el certificado público que hay en el software Ecoreach.

Cuando se carga el firmware en la IMU de Masterpact MTZ a través del software Ecoreach, 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 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 Ecoreach utilizada para descargar e instalar actualizaciones de firmware sea la última versión. Si cuenta con la última versión del software Ecoreach, los certificados públicos utilizados para firmar el firmware están actualizados.

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

Ventajas del uso del software Ecoreach para las actualizaciones de firmware

El software Ecoreach desempeña una función importante para ayudar a garantizar la integridad de su red de control industrial durante las actualizaciones de firmware. Utilice sólo la última versión del software Ecoreach 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 Ecoreach, la firma digital de los paquetes se verifica automáticamente.
- Al cargar actualizaciones de firmware en la unidad de control Micrologic X (utilizando el software Ecoreach con una conexión USB), la firma digital del paquete de actualización se verifica automáticamente.

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

Consulte la ayuda en línea de Ecoreach para tener acceso a los procedimientos detallados que explican cómo descargar e instalar las actualizaciones de firmware.

⚠ ADVERTENCIA

RIESGO DE FUNCIONAMIENTO IMPREVISTO

- Actualice la versión del software Ecoreach en cuanto reciba una notificación que le indique que hay una actualización disponible.
- Utilice esta última versión del software Ecoreach 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.

Comprobación de la lista de revocación de certificados

A intervalos regulares, y como mínimo cada tres meses, debe examinar la lista de revocación de certificados (CRL) publicada por Schneider Electric para asegurarse de que no incluya ningún certificado utilizado por sus equipos.

Para comprobar la CRL, haga lo siguiente:

Paso	Acción
1	Visualice la CRL publicada en el sitio web de Schneider Electric *(véase página 38)*.
2	Si la lista está vacía, significa que sus certificados actuales son válidos; no se requiere ninguna acción adicional. Si la lista no está vacía, siga con el Paso 3.
3	Verifique que está utilizando la última versión del software Ecoreach. Si no es el caso, actualice el software Ecoreach.
4	Actualice el firmware.

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 la plaza de 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 Ecoreach.

Recomendaciones de ciberseguridad para la compra de Digital Modules

Para comprar Digital Modules para la unidad de control Micrologic X utilice únicamente la plaza de 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 que se ciñan a las prácticas de tecnología operativa (TO), como la prueba en un sistema que no sea de producción, para la validación antes de instalarlos y desplegarlos en el entorno de producción.
- Sólo use la última versión del software Ecoreach para descargar e instalar Digital Modules.
- Proteja los PC utilizados para descargar Digital Modules e instálelos siguiendo las directrices más recientes del proveedor para el sistema operativo.

Recomendaciones de ciberseguridad para la instalación de Digital Modules

Sólo debe usar el software Ecoreach para instalar Digital Modules para la unidad de control Micrologic X.

El software Ecoreach desempeña una función importante para ayudar a garantizar la integridad de la red de control industrial. Utilice sólo la última versión del software Ecoreach 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 Ecoreach con una conexión USB, 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 Ecoreach con una conexión USB, la firma digital del Digital Module se verifica automáticamente.

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

Consulte la ayuda en línea de Ecoreach para tener acceso a los procedimientos detallados que explican cómo descargar e instalar Digital Modules.

⚠ ADVERTENCIA

RIESGO DE FUNCIONAMIENTO IMPREVISTO

- Actualice la versión del software Ecoreach en cuanto reciba una notificación que le indique que hay una actualización disponible.
- Utilice esta última versión del software Ecoreach 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.

Comprobación de la lista de revocación de certificados

A intervalos regulares, y como mínimo cada tres meses, debe examinar la lista de revocación de certificados (CRL) publicada por Schneider Electric para asegurarse de que no incluya ningún certificado utilizado por sus equipos.

Para comprobar la CRL, haga lo siguiente:

Paso	Acción
1	Visualice la CRL publicada en el sitio web de Schneider Electric *(véase página 38)*.
2	Si la lista está vacía, significa que sus certificados actuales son válidos; no se requiere ninguna acción adicional. Si la lista no está vacía, siga con el Paso 3.
3	Verifique que está utilizando la última versión del software Ecoreach. Si no es el caso, actualice el software Ecoreach.
4	Actualice el módulo digital.

Portal de ciberseguridad de Schneider Electric

Descripción general

El portal de ciberseguridad 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 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 Team, equipo de emergencia de ciberseguridad para productos corporativos) de Schneider Electric es responsable de administrar y emitir alertas sobre vulnerabilidades y mitigaciones que afectan productos y soluciones.

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

Se puede acceder al portal de ciberseguridad de Schneider Electric en *http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp*.

Información disponible sobre el portal de ciberseguridad de Schneider Electric

El 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.
- Acceso a recursos que ofrecen información sobre seguridad del entorno del sistema.
  Estos entornos incluyen lo siguiente:
  - Procesos industriales.
  - Sistemas de control de acceso y administración del edificio.
  - Centros de datos.
  - Sistemas de control de infraestructura eléctrica.
- Certificados y listas de revocación de certificados a través de la pestaña **Firmware PKI**.

Listas de revocación de certificados (CRL) disponibles en el portal de ciberseguridad Schneider Electric.

La siguiente tabla incluye la lista de CRL:

Producto	CRL
Unidad de control MTZ	Maestro Micrologic del interruptor LV
Módulo IO	Maestro Micrologic del interruptor LV
IFE	Maestro de comunicación avanzada
EIFE	Maestro de comunicación avanzada
IFM	Maestro Micrologic del interruptor LV

Glosario

B

BLE

Bluetooth low energy.

E

EIFE

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

G

GoDigital

La plaza de mercado en línea 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

IC

Control industrial. Hace referencia a los sistemas de hardware y software utilizados para supervisar y controlar los procesos y equipos de producción de una empresa.

IFE

Interfaz Ethernet que se puede conectar al interruptor automático Masterpact MTZ. Con este módulo, se puede acceder al interruptor automático por medio de la intranet de la empresa.

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 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, IFE, EIFE, la interfaz IFM y el módulo IO.

IP

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

IT

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 control industrial (IC) o red de tecnología operativa (OT).

L

LAN

Red de área local Hace referencia a la intranet o la red de TI de la empresa.

N

NFC

Comunicación de campo cercano. 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 con su red de TI.

P

PIN

Número de identificación personal.

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.

R

RAS

Servidor de acceso remoto.

S

SCADA

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

T

TCP/IP

Protocolo de control de transmisión/protocolo de Internet. Hace referencia al conjunto de protocolos que se utilizan para las comunicaciones por Internet.

V

VPN

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

DOCA0122ES-01

Schneider Electric Industries SAS
35, rue Joseph Monier
CS30323
F - 92506 Rueil Malmaison Cedex

http://www.schneider-electric.com

06/2017