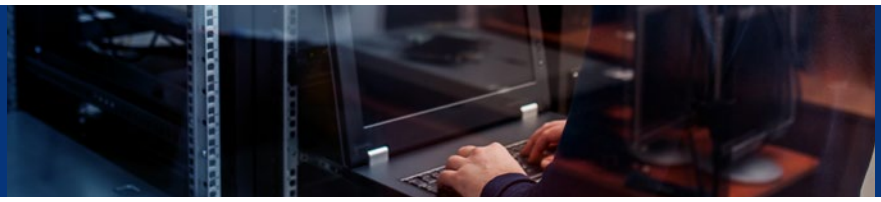

Sistema de monitoreo de condición inteligente Rexnord
Pautas de seguridad

Consideraciones de seguridad física

Gabinetes
El gabinete del dispositivo Rexnord Edge está diseñado para proteger el equipo de daños y accesos físicos no autorizados. No hay partes reparables por el usuario dentro del gabinete y debe permanecer sellado durante toda la vida útil del equipo.

Ubicaciones
El dispositivo Rexnord Edge debe ser tratado como otro equipo de red en lo referente al control de acceso físico. Se espera que solo personal autorizado tenga acceso físico al dispositivo Rexnord Edge.

Cableado
Los cables de red físicos utilizados para conectar el dispositivo Rexnord Edge a la red tecnológica operativa de su organización deben estar protegidos para evitar la intervención, daños deliberados y ataques y accidentes relacionados. Los métodos de protección incluyen conductos, pistas, ductos y similares.

Sistema operativo y aplicaciones del dispositivo Rexnord Edge

Sistema operativo y software Rexnord Edge
No intente acceder, modificar o manipular el sistema operativo del dispositivo Rexnord Edge o cualquier software que se ejecute en el mismo, fuera de la configuración de red del PLC como se especifica en esas instrucciones. Tales acciones pueden hacer que los dispositivos fallen o no funcionen correctamente.
Los intentos deliberados de modificar o manipular el dispositivo Rexnord Edge pueden anular los acuerdos de servicio entre su organización y Rexnord. No hay ninguna disposición para conectar un teclado o monitor directamente al dispositivo Rexnord Edge.

Interfaz del PLC
El dispositivo Rexnord Edge emitirá las lecturas actuales del sensor y cualquier advertencia a través de un paquete de datos accesible a través de Ethernet/IP, Modbus TCP o ProfiNet. Estos datos solo se proporcionan cuando los solicita el PLC.
Este puerto no permite el acceso a las aplicaciones del dispositivo Rexnord Edge o al sistema operativo y no enviará ningún dato al PLC a menos que se solicite. La arquitectura impide una ruta o capacidad para que la nube o Rexnord Edge ocasione disrupción o cambie el control del PLC.

Consideraciones de redes/nube

Acceso a la red en la nube
El portal web Rexnord Connect utiliza tecnologías OAuth de autorización y autenticación estándar de la industria. Los únicos datos almacenados en la nube son datos de sensores basados en el tiempo, alertas y advertencias. El centro de datos es compatible con SOC2 y certificado por FedRAMP.

Acceso al portal
Cualquier usuario nuevo que desee acceder al activo conectado se registrará en Rexnord.com, verificará su dirección de correo electrónico y será verificado por el administrador del sitio antes de permitirle el acceso a los datos de monitoreo de activos.

Tecnología operativa y redes de tecnología de la información
Su organización debe configurar sus enrutadores y cortafuegos para permitir que el tráfico del dispositivo Rexnord Edge se enrute a Internet para que pueda comunicarse con el servicio en la nube. No es necesario abrir puertos de entrada. El dispositivo Rexnord Edge utiliza el puerto 443 y los puertos MQTT estándar.
El dispositivo Rexnord Edge utiliza cifrado TLS basado en certificados x509v3 y autenticación asimétrica bidireccional.
Es una buena práctica aislar cualquier dispositivo de terceros de su red corporativa.

Se deben permitir los siguientes puertos, protocolos y URL de destino:

Puerto HTTPS 443:

h2s://nodev2.iotium.io
https://checkip.amazonaws.com
https://update.iotium.io
https://download.iotium.io
https://journal.iotium.io
https://upload.iotium.io
https://index.docker.io/v1/
https://rexnorddockerregistry.azuercr.io

MQTT sobre el puerto TLS 8883

ssl://*.messaging.internetofthings.ibmcloud.com

LTE o Ethernet

Rexnord Cloud y
Rexnord Connect Portal

Sus datos están protegidos en la nube

- Autenticación OAuth
- No se permite el acceso de terceros sin el permiso del usuario

Configuraciones de cortafuegos estándar

- No es necesario abrir puertos de entrada
- Solo puertos MQTT estándar de la industria abiertos

Comunicaciones cifradas

- Cifrado TLS
- Basado en certificados x509v3 con autenticación bidireccional

PLC	Redes de automatización
SIEMENS	EtherNet/IP
Allen-Bradley	PROFINET
Otro	MODBUS TCP

Conexión a PLC

Su red de operaciones está protegida

- Solo se publican datos cuando se solicitan
- El dispositivo Edge no realiza ningún control

Evaluación de riesgos

Rexnord sigue el estándar de la industria para el Método de Evaluación de Riesgos de Seguridad de Internet (CIS RAM) para evaluar los riesgos de seguridad cibernética en todos los componentes del ecosistema Rexnord IIoT. CIS RAM está alineado con ISO 27005 y NIST SP 800-30 para asegurar una implementación razonable y apropiada de los controles de seguridad para cumplir con un Análisis de Riesgo de Deber de Atención para el cumplimiento de la normativa (norma NIST 800-171 y el Marco de Seguridad Cibernética), así como requisitos legales. *El alcance incluye la plataforma del Sistema de Monitoreo de Condición Inteligente, sistemas en la nube, servidor de red, soporte a estaciones de trabajo/de escritorio y equipos de seguridad. Las evaluaciones de riesgo no se comparten externamente.*

Un tercero se utiliza para escanear los activos internos y las vulnerabilidades identificadas se revisan y corrigen en función de la prioridad. Se realizan pruebas de penetración externas al menos una vez al año y las vulnerabilidades identificadas se revisan y corrigen según la prioridad.

©2019 Rexnord