Rockwell Automation

Proteger la cuarta revolución industrial

El enfoque de confianza cero para una transformación digital en OT segura

Introducción

La transformación digital es tanto un excelente motor de progreso y eficiencia como una interrupción económica que puede afectar en gran medida a el ritmo de innovación y desarrollo de las organizaciones.

La adopción de la tecnología digital para transformar productos, servicios y empresas involucra obtener una mayor perspectivas y control a fin de mejorar la eficiencia, aprovechando normalmente nuevos flujos de datos. Estos esfuerzos a menudo redefinen experiencias, como la experiencia del cliente, y pueden incluir cambios de los modelos de operación que influyen en la seguridad de activos digitales.

En la tecnología de operaciones (OT), la transformación digital está impulsando dos cambios importantes:

- Los sistemas de OT se conectan hoy a redes a las cuales no estaban conectadas previamente a fin de extraer nuevos datos sobre las operaciones. Por definición, estos sistemas residen en la periferia de la infraestructura y, por tanto, se deben implementar, proteger y gestionar como puntos finales.
- Las aplicaciones de software ricas en datos se despliegan en los entornos de producción de OT en que estos nuevos datos se utilizan de la mejor manera. Las restricciones de latencia respecto al procesamiento de datos pueden ser el resultado por su alto volumen y ancho de banda. Par resolver este problema, se implementan, protegen y gestionan aplicaciones en el punto final.

Además, las organizaciones de OT encaran otros retos comunes que afectan a la seguridad y deben abordarse durante el viaje hacia la modernización.

1. Los sensores de procesos, aún los modelos más recientes, no tienen incorporadas seguridad y contraseñas. En un ejemplo reciente, un proveeder líder acaba de enviar 3000 nuevos sensores al EAU sin contraseñas.
2. Los proveedores de seguridad de red de IT normalmente abordan la seguridad a los niveles 2-7. Esta es una buena solución para la mayor parte de las redes de IT. Pero las amenazas de OT a menudo entran por la ruta de nivel 0-1 en que no se monitorea la telemetría y, por consiguiente, las amenazas no se detectan.
3. Sigue sin estar claro quién tiene la responsabilidad definitiva de la seguridad de OT. En teoría, los CISO podrían ser responsables y muchas organizaciones industriales toman medidas para asignar esta responsabilidad a los CISO. No obstante, los líderes de planta son propietarios del espacio y normalmente son reacios a dejarle el control a los CISO ya que estos frecuentemente no están suficientemente familiarizados con las operaciones de planta.
4. Las pautas de ciberseguridad de ductos de la Administración de Seguridad de Transporte (TSA) no abordan los sistemas de control, lo que incluye los sensores. Pero según la Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE. UU. (CISA), la TSA es propietaria de toda la red eléctrica.

5. La norma 1164 del Instituto de Petróleo de EE. UU., Ciberseguridad de Sistemas de Control para Transporte por Tubería (agosto de 2021), excluyó en la práctica los sensores de procesos (cláusula 6.6.5.4 (b)): "El inventario no debe incluir instrumentos individuales no conectados en red".

Pese al valor de herramientas como, por ejemplo, la herramienta MITRE ATT&CK y la metodología CVE, se necesita trabajar más en esta área. Por ejemplo, la herramienta MITRE ATT&CK no aborda el tema de los sensores de procesos y otros dispositivos de campo del sistema de control, y la metodología CVE para vulnerabilidades de software no tiene equivalente en materia de hardware del sistema de control.

Entender las normas actuales, y abordar brechas en normas que evolucionan menos rápido que las amenazas de OT, no es nada fácil.

Además, para garantizar el logro de la transformación digital segura, los grupos de IT y OT deben comprometerse a colaborar en torno a la implementación, seguridad y gestión de cambios de procesos. Esto asegura que se realicen las mejoras de productividad deseadas y que sean seguras y confiables, y que cumplan con la normativa.

Obstáculos comunes para la transformación digital

Hay razones comunes que impiden que las empresas logren sus metas de transformación digital. Estos problemas pueden agravarse durante la transformación de OT.

Hay que trasladar los sistemas de OT anticuados de las islas al continente.

A las "islas de automatización" en la infraestructura de OT tradicional les faltan las bases necesarias para permitir acceso a los datos. Además, los entornos industriales están mal inventariados, lo cual resulta en una falta de consciencia en cuanto a lo que está conectado en el entorno.

Los sensores de procesos, que son tan comunes en las entradas a sistemas de control y de seguridad, y las decisiones de operador, no son intrínsecamente seguros. Pueden ocurrir fallos catastróficos. Esto frecuentemente significa que la atención a la seguridad, que es bien conocida por organizaciones de ingeniería, ha sustituido la atención a la protección, algo que las organizaciones de ingeniería han tendido a considerar como responsabilidad de la organización de IT.

A su vez, las organizaciones de IT han tenido la tendencia a pasar por alto la seguridad de los sensores puesto que la consideran como una responsabilidad de ingeniería y, por lo tanto, fuera de su ámbito.

Sin embargo, a nivel de los sensores de procesos, la seguridad y la protección son en realidad la misma cosa.

Estrategia desalineada o indefinida.

La estrategia de transformación digital debe incluir esfuerzos coordinados para establecer resultados definidos y medibles en materia de metas empresariales clave, a la vez que mantiene la seguridad de los activos digitales críticos y garantiza conformidad con las normas industriales.

La hoja de ruta no crea valor temprano.

El desarrollo de una hoja de ruta de corto y largo plazo para suministrar valor a partir de la transformación digital, orientado por resultados comerciales y no solo por tecnología, constituye una base esencial para un proyecto exitoso.

Partes interesadas clave que persiguen objetivos diferentes.

La transformación digital requiere un cambio en la cultura de la organización. Debe existir un alineamiento entre las mentalidades de los líderes de IT y OT para que los dos grupos de partes interesadas logren el alcance de los objetivos empresariales del proyecto

El primer paso consiste en identificar y priorizar lo que debe protegerse en la organización: datos, activos, aplicaciones y servicios (DAAS).

Una mirada más de cerca de los sensores de procesos

Los sistemas anticuados que han funcionado durante más de 20 años a menudo no están diseñados para funcionar en un entorno de IoT con miles de sensores de procesos, lo cual presenta vulnerabilidades de seguridad. Sin planificación y controles adecuados, los esfuerzos de modernización pueden multiplicar los riesgos de ciberseguridad.

¿Por qué es tan importante la protección de sensores de procesos?

Según un informe reciente: "Las amenazas de ciberseguridad están en aumento y, como consecuencia, el envío de datos de sensores podrían ser jaqueado. Hay que comprender cómo el jaqueo de los datos de sensores afectan el rendimiento de los controles. Una situación típica podría incluir datos de sensores modificados por jáquers y enviados a los bucles de control, lo cual resultaría en acciones de control extremas".

Algunos ciberincidentes con sensores de procesos han incluido:

- Mal funcionamiento de represas, colapso debido a bajas lecturas erróneas
- Un sensor que dio lugar a la evacuación de 10 millones de galones de aguas residuales sin tratar
- Una válvula de alivio de seguridad en una central nuclear no se levantó puesto que el sensor de presión nunca alcanzó su punto de ajuste
- Un fallo de sensor de voltaje en una planta de ciclo combinado en la Florida provocó una oscilación de la carga de 200 MW en la planta que, a su vez, ocasionó una oscilación de carga de 50 MW en Nueva Inglaterra.
- Explosiones en el patio de tanques por lecturas erróneas de los sensores de nivel
- Accidente aéreo por lecturas erróneas de sensores
- Explosión de una refinería por lecturas erróneas de sensores

Sensores de procesos sin ciberseguridad, autentificación o registro cibernético hacen imposible saber si incidentes como estos fueron actos malintencionados, creados para que parecieran accidentales.

Hay que plantear tres preguntas de seguridad importantes para comprender las vulnerabilidades intrínsecas de los sensores de procesos:

1. ¿Se necesita una presencia física para comprometer el sensor?
   No. Se puede lograr de forma remota.
2. ¿Cuánto daño pueden causar los impactos de un sensor afectado por un delito cibernético?
   El calibrador de campo calibra los sensores uno por uno, pero tiene una conexión no segura a la Internet. Los sistemas de gestión de activos (AMS) tienen acceso a miles de sensores. Por otra parte, los AMS pueden tener conexiones no seguras a la Internet y se conectan a menudo a los sistemas de planificación de recursos empresariales (ERP).
   Un ejemplo real de un fallo catastrófico por problemas con sensores: Colonial Pipeline.
3. ¿Que pasa cuando se envían datos de sensores comprometidos a la nube para aplicaciones de analítica de macrodatos, IoT o Industria 4.0?
   Se supone que los datos de sensores no estén comprometidos.

Las organizaciones de OT deben abordar las deficiencias de los sensores de procesos a medida que emprenden programas de transformación digital seguros y comprenden cómo los actores de amenazas pueden interrumpir, degradar, o posiblemente perjudicar y destruir la infraestructura. Cuáles son los riesgos y costos, y qué medidas pueden tomarse para eliminar las vulnerabilidades.

La confianza cero es una estrategia disponible para eliminar el exceso de confianza y los riesgos en torno a los sensores de procesos. La confianza cero ofrece total visibilidad y validación continua de la confiabilidad de cada "entidad" en una empresa, ya sea que se trate de datos, aplicaciones, servicios o dispositivos, entre ellos sensores de procesos, a partir de la suposición de un nivel de confianza cero.

Planificación de una transformación digital segura

En vista de todos los retos relativos a la transformación digital segura agravados en los entornos de OT, no sorprende que las organizaciones industriales se queden rezagadas con respecto a las industrias más centradas en IT en lo que respecta a modernización.

La buena noticia es que existen rutas probadas hacia el éxito.

El logro de una transformación digital segura en la OT involucra algunas estrategias clave:

- Un enfoque de confianza cero
- Las soluciones digitales modernas adecuadas
- Cambios de responsabilidad de los encargados de entidades dentro de las organizaciones
- La mejora del cumplimiento normativo en torno a activos tan comunes y vulnerables como son los sensores de procesos. En vez de estas mejoras, el abordaje directo de las brechas

Si bien cada uno de estos puntos es importante, el enfoque de confianza cero ahora es el foco de esta conversación.

El enfoque de confianza cero

La confianza cero representa una excelente estrategia para desplegar tecnologías de transformación digital seguras en entornos industriales. Esta admite nuevos grupos de usuarios, modelos de participación de clientes, rápidas adopciones y nuevos dispositivos y sensores de IoT y OT a medida que madura la transformación, todo con protección de ciberseguridad.

La confianza cero se basa en cinco principios de diseño que pueden integrarse con los siguientes cinco pasos esenciales necesarios para impulsar la transformación digital segura en toda la empresa.

1. Definir activos y proteger superficies
2. Asignar flujos de transacciones
3. Diseñar la arquitectura
4. Aplicar políticas
5. Realizar el monitoreo y mantenimiento continuos

Definir activos y proteger superficies. Como afirma John Kindervag, originador de la confianza cero: "La confianza cero es una estrategia para alinear la estrategia empresarial con las prácticas de ciberseguridad". Al enfocarse en los resultados empresariales, la seguridad puede considerarse habilitadora en vez de inhibidora.

El primer paso consiste en identificar y priorizar lo que debe protegerse en la organización: elementos de datos, activos, aplicaciones y servicios (DAAS). Los elementos DAAS son muy críticos para la empresa y cada uno de ellos se prioriza. Estos se consideran superficies de protección, por ej., controles de ICS, redes de IT, bases de datos de información sobre clientes, datos de propiedad intelectual (IP), etc.

- **Datos**: Clasifique los datos en función de la importancia que tienen para su organización, su valor potencial para los jáquers y si están sujetos a los reglamentos. Documentar un plan en torno a la gobernabilidad de datos –globalmente y en especial dentro de una superficie de protección– permite que la organización pueda identificar, clasificar, transmitir, retener y eliminar datos con la implementación de controles de seguridad eficaces.
- **Aplicaciones**: Comprenda qué aplicaciones usan datos sensibles o código de propiedad exclusiva que podrían ser útiles para un actor de amenazas. El diseño debe realizarse de dentro hacia fuera. Describa cómo los sistemas deben funcionar y cómo los varios componentes del elemento DAAS interactúan con otros recursos en la red. Comprender cómo el tráfico se desplaza en la red, específicamente respecto a los datos en la superficie de protección, ayudará con el desarrollo de políticas para proteger los datos dentro de las aplicaciones y y entre ellas.
- **Activos**: Elabore un inventario detallado de todos sus dispositivos (computadoras portátiles, teléfonos celulares, equipo de fabricación, PLC, dispositivos de IoT como sensores de procesos, y otros activos conectados en red) para saber lo que debe incluirse en su superficie de protección.
- **Servicios**: Identifique todos los servicios de red fundamentales para la empresa que se necesiten proteger como Active Directory, DHCP y correo electrónico. Por lo general, las cuentas de servicio deben mostrar comportamientos conocidos y disponer de privilegios de conexión limitados. Nunca deben intentar acceder directamente a un controlador de dominio o un sistema de autentificación, y todas las anomalías en lo que respecta a comportamiento deben identificarse rápidamente y remitirse a instancias superiores cuando aparezcan.

Debido al enfoque de las defensas de ciberseguridad en torno a cada superficie de protección priorizada según su importancia para la organización, es posible crear perímetros defendibles mucho más pequeños y más gestionables que la superficie de ataque de empresa tradicional que se podría considerar como la totalidad de la Internet.

Cada organización encontrará múltiples proyectos de transformación digital y sus correspondientes superficies de protección. Empezar con una iniciativa de transformación estratégica, impactante y medible, inicialmente más pequeña, puede brindarle a la organización experiencia con la implementación de ciberseguridad de confianza cero y un marco para asegurar el éxito de proyectos futuros.

Asignar flujos de transacciones. Los entornos individuales normalmente están mal inventariados en lo que concierne a los activos, lo cual ocasiona vulnerabilidades respecto a qué debe estar conectado en el entorno en vez de qué está conectado en realidad. Estos sistemas a menudo han crecido orgánicamente provocando frecuentes brechas de conocimientos de diseño; o dispositivos que se suponen ser seguros pueden proporcionar puntos de entrada de Internet no protegidos a las redes.

Para diseñar correctamente una red, usted debe diseñarla de dentro hacia fuera. Es esencial comprender cómo deben funcionar los sistemas y cómo varios componentes DAAS interactúan con otros recursos en la red. Con la asignación de flujos de tráfico e interdependencias, la documentación de cómo los recursos específicos interactúan entre sí y la incorporación de estas interdependencias en políticas y controles de seguridad, es posible determinar los tipos y niveles de protección necesarios.

La asignación de flujos de transacciones e interdependencias DAAS, específicamente respeto a cualquier cosa que se cruza con sus superficies de protección, permite mejores protecciones sin romper accidentalmente aplicaciones, servicios o flujos de trabajo relacionados. También permite una mejor comprensión e información necesaria para tomar decisiones más informadas en el siguiente paso.

Diseñar la arquitectura. Tras la definición de la superficie de protección y la asignación de flujos, normalmente se presentará la arquitectura de confianza cero.

Las mejores prácticas de confianza cero exigen que los controles de seguridad se sitúen lo más cerca posible de los elementos que se protegen. Salvo por eso, la arquitectura de confianza cero no se basa en una plantilla universal. En cambio, aprovecha varios tipos de herramientas y políticas de ciberseguridad específicas de cada superficie de protección a fin de lograr las metas. Las organizaciones deben desplegar e integrar una combinación de capacidades que mejoren las identidades y la gestión de acceso, controles de acceso, segmentación de redes, microperímetros y más según los requisitos del elemento DAAS en cada superficie de protección.

Por tanto, el diseño de la red de confianza cero debe basarse en cómo fluyen las transacciones en una red hacia y desde los elementos DAAS de la superficie de protección, y debe tomar en consideración cómo los usuarios y aplicaciones obtienen datos de la superficie de protección. Con un flujo optimizado en mente, es posible tomar decisiones relativas a la colocación de la segmentación y microperímetros usando dispositivos físicos y/o virtuales.

Aplicar políticas. En este cuarto paso, se escriben las reglas de las políticas para el gateway de segmentación con base base en el comportamiento esperado de los datos y la interacción del usuario o las aplicaciones con dichos datos.

Una vez que el equipo de diseño ha determinado el flujo del tráfico óptimo, el paso siguiente es determinar cómo aplicar el control de acceso y las políticas de inspección en el gateway de segmentación. La política debe empezar con un enfoque general y hacerse más granular a medida que emergen una mayor comprensión de las

necesidades del usuario y los requisitos empresariales, madura la transformación digital y se desarrolla la perspectiva empresarial.

Un principio clave de la confianza cero es restringir el acceso a información y permitirlo solo si es necesario (el principio de privilegio mínimo) y aplicar estrictamente este control de acceso. Para definir estas reglas, el equipo de diseño debe contar con una comprensión detallada de cuáles usuarios tienen acceso a cuáles datos, además de información contextualizada.

Ya no basta con saber la dirección de origen, la dirección de destino, el puerto y el protocolo. Los equipos de seguridad necesitan comprender la identidad de usuario impuesta, así como la aplicación, que servirá a menudo como proxy del tipo de datos en el gateway de segmentación moderno.

Una regla específica debe permitir el tráfico para que un recurso se comunique con el otro. Hay que contestar las preguntas siguientes para desarrollar dicha regla:

- ¿Quién debe tener acceso? Esto define la "identidad impuesta".
- ¿Cuál aplicación a cuál recurso? ¿Cuál aplicación es usada por la identidad impuesta para obtener acceso a un recurso en la superficie de protección?
- ¿Cuándo el usuario debe tener acceso? ¿Cuándo se intenta obtener acceso al recurso?
- ¿Desde dónde se debe obtener acceso? ¿Dónde está el destino del paquete de datos?
- ¿Por qué estamos haciendo esto? ¿Por qué este paquete intenta obtener acceso a este recurso en la superficie de protección? Esto se refiere a la clasificación de datos en que los metadatos ingeridos automáticamente de las herramientas de clasificación de datos contribuyen a hacer que su política sea más granular.
- ¿Cómo debemos protegerlo? Para protegerlo, usted debe comprender cómo la identidad impuesta de un paquete obtiene acceso a la superficie de protección mediante una aplicación específica.

Monitoreo y mantenimiento continuos. Este es el quinto paso de la implementación del enfoque de confianza cero.

Este proceso iterativo implica la observación continua de todos los registros internos y externos hasta la capa 7 con foco en los aspectos operativos de la confianza cero. Al enviar tanta telemetría como sea posible sobre el entorno se obtendrán nuevas perspectivas relativas a cómo mejorar la seguridad y eficiencia con el paso del tiempo, así como desarrollar información útil para transformar nuevas áreas.

Los entornos de tecnología están sujetos a un sinnúmero de amenazas. Las empresas deben mantener una capacidad de monitoreo continuo para asegurarse de estar al corriente de lo que sucede en sus entornos. Cuanto más se ataca una red, más fuerte se hace debido al refuerzo de la seguridad de las políticas y la modificación de diseños iterativos con ajustes arquitectónicos que mejoran aún más la seguridad.

Normas de seguridad industrial

Hay cuatro normas de seguridad principales que rigen las industrias de OT.

- IEC 62.443 Industrial Automation and Control Systems (IAC) Security
- Department of Homeland Security/The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- NIST 800-82 Industrial – National Institute of Standards and Technology
- Department of Homeland Security/Idaho National Lab

Cada una tiene como base una arquitectura de seguridad de defensa en profundidad que tiene a su vez vulnerabilidades. Además, estas normas no representan una estrategia en sí, sino una implementación de tácticas para abordar vulnerabilidades puntuales específicas mediante el uso de una solución de control o producto con base en el concepto de zona desmilitarizada industrial (IDMZ) que es una frontera, búfer o separación en la instalación de fabricación o procesos entre los sistemas empresariales y los sistemas de control industrial de la organización con requisitos de seguridad diferentes y sin confianza inherente entre ellos.

La transformación digital modifica el factor de confianza de ambos sistemas. Hoy la confianza debe ser observadora, contextual y adaptiva si se desea que la interacción de los nuevos modelos empresariales desarrollados con la transformación digital logren éxito y suministren los resultados positivos esperados.

Rockwell Automation se alinea con la norma de seguridad IEC 62443 de sistemas de control y automatización industrial y con el enfoque de confianza cero. Los principios de diseño de confianza cero se ajustan bien a los requisitos de la norma IEC 62443 simplificando la conformidad y fortaleciendo las defensas frente a un entorno de amenazas en evolución constante.

Resumen

La transformación digital segura en la OT puede aprovechar la confianza cero como un marco clave para garantizar que los proyectos de transformación se lancen con la protección de ciberseguridad apropiada ya incorporada.

Tanto la confianza cero como la transformación digital segura constituyen viajes que se deben implementar de forma incremental. Puesto que la transformación digital modifica el factor de confianza entre los sistemas de control industrial y sistemas empresariales, un plan para lograr una transformación digital segura debe ejecutarse usando estrategias complementarias para facilitar eficiencia mejorada y productividad aumentada con total visibilidad y aplicación de la ciberseguridad que cubran cada punto de conexión en la red.

La planificación de un proyecto inicial de transformación digital segura, así como la identificación, priorización y protección de los elementos DAAS en cada superficie de protección, ayudará a la organización a conseguir valor temprano por sus esfuerzos, y a establece un patrón de protecciones de ciberseguridad para proteger la organización durante la transformación.

Combinando todos los criterios

Rockwell Automation cuenta con conocimientos profundos de la transformación digital segura en entornos de OT complejos. Aproveche nuestros conocimientos profundos para ayudarlo a diseñar, implementar y monitorear los proyectos de su organización a fion de conseguir mayores ganancias operacionales, lo cual garantiza la implementación de las protecciones de ciberseguridad adecuadas desde la planificación hasta la producción.

Tome acción

Obtenga más información sobre la transformación digital segura

Obtenga más información sobre la confianza cero en la ciberseguridad de OT.

Hable con un experto sobre cómo empezar.

Conéctese con nosotros.

rockwellautomation.com — expanding **human possibility**®

AMÉRICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel.: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPA/MEDIO ORIENTE/ÁFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel.: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA-PACÍFICO: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel.: (852) 2887 4788, Fax: (852) 2508 1846
ARGENTINA: Rockwell Automation S.A., Av. Leandro N. Alem 1050, Piso 5, Ciudad Autónoma de Buenos Aires, Tel.: (54) 11.5554.4040, www.rockwellautomation.com.ar
CHILE: Rockwell Automation Chile S.A., Av. Presidente Riesco 5435, Piso 15, Las Condes, Santiago, Tel.: (56) 2.290.0700, www.rockwellautomation.com.cl
COLOMBIA: Rockwell Automation S.A., Edf. North Point, Carrera 7 N 156-78 Piso 19, PBX: (57) 1.649.9600, www.rockwellautomation.com.co
ESPAÑA: Rockwell Automation S.A., C/ Josep Plà, 101-105, Barcelona, España 08019, Tel.: 34 902 309 330, www.rockwellautomation.es
MÉXICO: Rockwell Automation de S.A. de C.V., Av. Santa Fe 481, Piso 3 Col. Cruz Manca, Deleg, Cuajimalpa, Ciudad de México C.P. 05349, Tel.: 52 (55) 5246-2000, www.rockwellautomation.com.mx
PERÚ: Rockwell Automation S.A., Av. Victor Andrés Belaunde N 147, Torre 12, Of.102, San Isidro Lima, Perú, Tel.: (511) 211-4900, www.rockwellautomation.com.pe
PUERTO RICO: Rockwell Automation, Inc., Calle 1, Metro Office #6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, www.rockwellautomation.com.pr
VENEZUELA: Rockwell Automation S.A., Edf. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, www.rockwellautomation.com.ve

Allen-Bradley y expanding human possibility son marcas comerciales de Rockwell Automation, Inc.
Las marcas comerciales que no pertenecen a Rockwell Automation son propiedad de sus respectivas empresas.

Publicación GMSN-WP003A-ES-P – Mayo de 2022

Copyright © 2022 Rockwell Automation, Inc. Todos los derechos reservados. Impreso en EE. UU.