Consideraciones sobre tecnología de redes para la creación de fábricas conectadas y seguras

08 November 2023

La interconectividad es imprescindible para hacer realidad las aplicaciones orientadas al futuro del Internet Industrial de las Cosas (IIoT), que pueden aprovechar la información procesable de diferentes partes de una empresa para respaldar las operaciones inteligentes y automatizadas de una fábrica. Sin embargo, aunque la conectividad abre la puerta a nuevas oportunidades, también puede exponer las redes de automatización industrial a ciberataques si los sistemas no se configuran de forma correcta. Por eso, es más importante que nunca seguir unas estrictas directrices de seguridad a la hora de implantar y utilizar dispositivos de red.

Mariana Alvarado, Especialista en Marketing de CC-Link Partner Association (CLPA-México), analiza cómo los integradores de sistemas de automatización y los usuarios finales pueden configurar redes IIoT orientadas al futuro al tiempo que minimizan el riesgo de ciberamenazas.

No cabe duda de que las fábricas y empresas altamente interconectadas, en las que se fusionan los dominios de la tecnología de la información (TI) y la tecnología operativa (TO), pueden brindar una serie de ventajas competitivas a las empresas que las crean. Por ejemplo, permite a las empresas compartir información y conocimientos clave para respaldar una toma de decisiones altamente eficaz y basada en hechos, así como identificar y resolver anomalías, ineficiencias o cuellos de botella para mejorar la productividad. Además, la inclusión de dispositivos IP en

las redes TO puede añadir funcionalidades y capacidades adicionales. Por ejemplo, es posible compartir datos de alta resolución procedentes de cámaras y otros sistemas de visión a fin de supervisar y analizar los productos en tiempo real.

Además de desempeñar un papel protagonista en la transformación digital de las empresas, la interconectividad también puede simplificar las arquitecturas de red y su configuración. En consecuencia, es posible reducir el tiempo y el coste asociados a las operaciones de cableado, al tiempo que se crea una infraestructura más flexible y escalable que mejora el coste total de propiedad de la red.

Con el fin de satisfacer la creciente demanda de comunicaciones en toda la empresa, se están creando tecnologías innovadoras para dar respuesta a estas necesidades. Por ejemplo, el Ethernet industrial abierto CC-Link IE TSN, que combina el ancho de banda de un gigabit y la conexión en red sensible al tiempo (TSN). Estas características permiten a los usuarios integrar eficazmente en la misma red tanto el tráfico de control de tiempo crítico procedente del taller como los mensajes menos transitorios procedentes del nivel informático. Al dar más importancia a esta tecnología, TSN es ampliamente reconocida por los líderes del sector, como Mitsubishi Electric, como un elemento imprescindible para aplicaciones IIoT altamente eficaces.

Especificar los componentes adecuados

Junto con las muchas ventajas que aporta la convergencia de los ámbitos de TI y TO, la mejora de la disponibilidad y accesibilidad de las redes puede exponer potencialmente las comunicaciones de la planta de producción a fallas en la ciberseguridad y a sus consecuencias si no se aplica correctamente. Por ejemplo, el acceso no autorizado a datos, aplicaciones, líneas, máquinas, dispositivos y

redes de la fábrica podría comprometer el tiempo de actividad, la productividad y la calidad del producto.

Dado que las estrategias de ciberseguridad convencionales para las plantas de las fábricas no pueden adaptarse con éxito a las necesidades de confiabilidad de las aplicaciones IIoT, es importante adoptar medidas más eficaces. Si bien los enfoques de seguridad TO actuales pueden no ser suficientes debido a los diferentes requisitos operativos y la necesidad limitada de comunicaciones de alta velocidad, ya están disponibles soluciones adecuadas que pueden cumplir con los estrictos requisitos de latencia y fiabilidad. En efecto, muchos de los mecanismos de seguridad de última generación actuales pueden garantizar el funcionamiento seguro de los marcos IIoT basados en TSN.

En la práctica, un buen punto de partida para los fabricantes de maquinaria, los integradores de sistemas de automatización y los usuarios finales es adoptar dispositivos que sigan las directrices de seguridad líderes del sector centradas en la confidencialidad, la integridad y la disponibilidad.

CLPA recomienda la incorporación de una serie de mecanismos de ciberdefensa a los desarrolladores y proveedores interesados en ofrecer dispositivos de automatización industrial compatibles con CC-Link IE TSN que puedan admitir sistemas IIoT seguros. Las capacidades clave incluyen autenticación y filtrado de red para limitar el acceso a recursos clave, así como funciones de registro y gestión para registrar incidentes de seguridad. Del mismo modo, las capacidades antimalware, como los sistemas de detección y prevención de intrusiones, pueden bloquear la instalación o ejecución de software no autorizado.

Además, se aconseja la limitación de banda, el filtrado de red y la protección contra ataques de denegación de servicio (DoS). Éstos predefinen la capacidad aceptable

para garantizar la disponibilidad de todos los elementos conectados, lo que evita la congestión y las inundaciones de la red al limitar volúmenes de tráfico atípicamente grandes que superan el ancho de banda disponible.

Además de adoptar productos de automatización industrial que puedan impulsar la interconectividad a la vez que incorporan herramientas de seguridad clave, CLPA recomienda a sus miembros de integración de sistemas que apliquen la zonificación a la hora de configurar máquinas e infraestructuras de red. Esta segmentación virtual de la red puede ayudar a establecer medidas adecuadas e individuales a fin de proteger de manera eficaz cada zona en función de su nivel de seguridad específico. Por ejemplo, los fabricantes de máquinas y los usuarios finales pueden decidir establecer soluciones de defensa de red, punto final o datos.

Conclusiones

No cabe duda de que las arquitecturas de redes convergentes basadas en TSN representan el futuro de las comunicaciones industriales y tienen gran cantidad de ventajas competitivas. Una remodelación tan revolucionaria de la forma en que se transfieren los datos en el taller y en toda la empresa requiere la adopción de una nueva mentalidad en materia de prevención de ciberamenazas.

Al utilizar dispositivos de automatización compatibles con CC-Link IE TSN, los fabricantes de maquinarias y los usuarios finales pueden beneficiarse de componentes de última generación que se han creado de acuerdo con las directrices de seguridad de CLPA. De este modo, contribuyen a la creación de aplicaciones IIoT sólidas y orientadas al futuro.

Pies de foto:

Imagen 1: Los integradores de sistemas de automatización y los usuarios finales pueden configurar redes IIoT orientadas al futuro al tiempo que minimizan el riesgo de ciberamenazas.

Las imágenes distribuidas con este comunicado de prensa sólo pueden utilizarse para acompañar esta copia y están sujetas a derechos de autor. Póngase en contacto con DMA Europa si desea obtener una licencia para un uso posterior de la imagen.

Acerca de CC-Link Partner Association (CLPA)

CLPA es una organización internacional fundada en 2000, que ahora celebra su vigésimo aniversario. Durante los últimos 20 años, CLPA se ha dedicado desarrollo técnico y a la promoción de la familia de redes de automatización abiertas CC-Link. La tecnología clave de CLPA es CC-Link IE TSN, la primera Ethernet industrial abierta del mundo que combina un ancho de banda gigabit con una red de trabajo en tiempo real (TSN), lo que la convierte en la solución líder para aplicaciones de la Industria 4.0. Actualmente, la CLPA tiene más de 4.100 miembros corporativos en todo el mundo y más de 2.600 productos compatibles disponibles de más de 370 fabricantes. Alrededor de 38 millones de dispositivos utilizan tecnología CLPA en todo el mundo.

Press contact:
CC-Link Partner Association Americas
Mariana Alvarado
Marketing Specialist
Tel.: +52 (55) 3067-7500 / ext. 5417
mariana.alvarado@cclinkamerica.org

PR agency:
DMA Europa
Chiara Civardi
Progress House, Great Western Avenue, Worcester,
WR5 1AQ, UK
Tel.: +44 (0) 1905 917477
chiara.civardi@dmaeuropa.com
news.dmaeuropa.com