Network technology considerations for the creation of secure, connected factories

08 November 2023

Interconnectivity is a must to realize future-oriented Industrial Internet of Things (IIoT) applications that can leverage actionable insights from different part of an enterprise to support smart, automated factory operations. However, as connectivity opens the door to new opportunities, it can also expose industrial automation networks to cyberattacks if systems are not set up correctly. Following strict security guidelines when implementing and using network devices is therefore more important than ever.

Tom Burke, Global Strategic Advisor at the CC-Link Partner Association (CLPA) Americas, looks at how automation system integrators and end users can set up future-oriented IIoT networks while minimizing the risk of cyber threats.

There is no doubt that highly interconnected factories and enterprises, where information technology (IT) and operational technology (OT) domains merge, can offer a number of competitive advantages to the companies that create them. For example, it enables firms to share key information and knowledge to support highly effective, fact-based decision making as well as identify and resolve anomalies, inefficiencies or bottlenecks to improve productivity. Furthermore, the inclusion of IP devices within OT networks can deliver additional functionalities and capabilities. For example, it is possible to share high-resolution data from cameras and other vision systems for real-time monitoring and analysis of products.

In addition to playing a leading role in the digital transformation of business, interconnectivity can also simplify network architectures and their configuration. As a result, it is possible to reduce the time and cost associated with wiring operations

while creating a more flexible and scalable infrastructure that improves the network's total cost of ownership.

In order to support the growing demand for enterprise-wide communications, innovative technologies are being developed to address these needs. For example, CC-Link IE TSN open industrial Ethernet, which combines gigabit bandwidth and Time-Sensitive Networking (TSN). These features enable users to effectively accommodate both time-critical control traffic from the shop floor and less transient messages from the IT level on the same network. Giving more importance to this technology, TSN is widely acknowledged by industry leaders, such as Mitsubishi Electric, as a must for highly effective IIoT applications.

Specifying the right components

Along with the many benefits that the convergence of IT and OT domains brings, enhancing the availability and accessibility of networks can potentially expose shop floor communications to cybersecurity breaches and the consequences thereof if not correctly implemented. For example, unauthorized access to factory data, applications, lines, machines, devices and networks could compromise uptime, productivity as well as product quality.

As conventional cybersecurity strategies for factory floors cannot successfully accommodate the reliability needs of IIoT applications, it is important to set up more effective measures. While current OT security approaches may not be sufficient due to the different operational requirements and limited need for high-speed communications, suitable solutions that can meet strict latency and reliability requirements are already available. In effect, many of today's state-of-the-art security mechanisms can ensure the secure operation of IIoT frameworks based on TSN.

In practice, a good starting point for machine builders, automation system integrators and end users is to adopt devices that follow industry-leading security guidelines focusing on confidentiality, integrity and availability.

The CLPA recommends the incorporation of a number of cyber defense mechanisms to developers and vendors interested in offering CC-Link IE TSN compatible industrial automation devices that can support secure IIoT systems. Key capabilities include authentication and network filtering to limit access to key resources as well as log and management functions to record security incidents. Similarly, anti-malware capabilities, such as intrusion detection and prevention systems, can block unauthorized software from being installed or running.

In addition, band limitation, network filtering and protection against denial of service (DoS) attacks are advised. These predefine acceptable capacity to ensure the availability of all connected elements, preventing network congestion and flooding by limiting atypically large volumes of traffic that exceed the available bandwidth.
Besides adopting industrial automation products that can drive interconnectivity while featuring key security tools, the CLPA recommends its system integration members to implement zoning when configuring machines and network infrastructures. This virtual segmentation of the network can help establish suitable, individual measures to effectively protect each zone based on its specific security level. For example, machine builders and end users may decide to set up network, end point and/or data defense solutions.

Conclusions

There is no doubt that convergent network architectures based on TSN represent the future of industrial communications, offering a multitude of competitive advantages. Such a game-changing reshape of the way data are transferred across the shop floor and the entire enterprise requires the adoption of a new mindset when it comes to preventing cyber threats.

By using CC-Link IE TSN compatible automation devices, machine builders and end users can benefit from state-of-the-art components that have been developed in accordance with the CLPA’s security guidelines. As a result, they support the creation of robust, future oriented IIoT applications.

Image captions:

Image 1: Automation system integrators and end users can set up future-oriented IIoT networks while minimizing the risk of cyber threats.

About The CC-Link Partner Association (CLPA)

The CLPA is an international organization founded in 2000, now celebrating its 20th Anniversary. Over the last 20 years, the CLPA has been dedicated to the technical development and promotion of the CC-Link open industrial network family. The CLPA's key technology is CC-Link IE TSN, the world's first open industrial Ethernet to combine gigabit bandwidth with Time-Sensitive Networking (TSN), making it the leading solution for Industry 4.0 applications. Currently the CLPA has over 4,100 corporate members worldwide, and more than 2,000 compatible products available from over 370 manufacturers. Around 38 million devices using CLPA technology are in use worldwide.

Anyone interested in joining the organization can apply here: https://www.cc-link.org/en/clpa/members/index.html

Press contact:
CC-Link Partner Association Americas
Thomas Burke
Global Strategic Advisor
Tel.: (847) 478-2100
tom.burke@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