June 5, 2017
CC-Link Partner Association (CLPA)

Establishment of a CLPA Working Group on Industrial Ethernet Security

Recently, the IT (Information Technology) and OT (Operational Technology) worlds have started to overlap. While this has brought many benefits to manufacturing, it also means that plant staff now also needs to consider IT security threats to their operations. Actual measures for reducing those risks need to be considered and implemented. From the factory system point of view, it is said that the priority of protection requirements is availability, integrity, and confidentiality. Another difference from IT systems is “the human factor”. Personnel are in a plant floor to manufacture, maintain, or manage the plant. The role and the authorization assigned to personnel related to a target plant system should also be considered.

■ CLPA Security Working Group

Both physical and cyber security measures have to be considered for plant security. In general, one measure is insufficient and the “defense in depth” concept, combining multiple measures, needs to be contemplated.

System security architecture
Physical access control
Industrial network security access control, integrity, and confidentiality
Security monitoring

■ Scope of the CLPA Security Working Group

CC-Link IE Field Basic　　SLMP Seamless Message Protocol

The first step of the CLPA Security Working Group focuses on network security, especially when the user adopts the Seamless Message Protocol (SLMP) and CC-Link IE Field Basic where general IP communication is used for both cyclic and transient communications. A guideline document for secure network design will be created. The guideline document will be based on IEC62443 including the defense in depth security approach. Router/switch configuration examples for secure SLMP and CC-Link IE Field Basic are also described.

Overview of Industrial network security
Security concerns viewpoint for industrial networks
Defense-in-depth security approach
Use-case examples

■ Participating Companies

The CC-Link Partner Association Security Working Group includes participation from Belden-Hirschmann, Cisco Systems, Hilscher, HMS, MIND, Mitsubishi Electric, MOXA and Panduit.

■ CC-Link Partner Association

The CC-Link Partner Association is an open network promotion organization established in 2000 for the promotion of the widespread usage of CC-Link. The CLPA's key technology is CC-Link IE, the world's first and only open gigabit Ethernet for automation and an ideal solution for Industry4.0 applications due to its unmatched bandwidth. Its main activities include the formulation of CC-Link IE and CC-Link technical specifications and the conduction of conformance tests, development support for devices and equipment using CC-Link, user support for device selection, and public relations for the wider acceptance of CC-Link. The CLPA, which began with 163 corporate members, has expanded yearly and, as of the end of April 2017, boasts 2,982 members, of whom 2,248 are overseas corporations. CC-Link is the leading open industrial automation network technology in Asia and is becoming increasingly popular in Europe and the Americas.

Contact for inquiries

CC-Link Partner Association
6F Ozone-front Building, 3-15-58, Ozone, Kita-ku,
Nagoya 462-0825, Japan
Tel.: 81-52-919-1588 / Fax: 81-52-916-8655 / E-mail: info@cc-link.org
Web: https://www.cc-link.org