CC-Link Partner Association (CLPA)

Vernon Hills, IL United States; May 31, 2017

Subject: Establishment of a CLPA Working Group on Industrial Ethernet Security

Issued on behalf of: CC-Link Partner Association (CLPA)

Keywords: CLPA, CC-Link Partner Association, CC-Link IE, Industrial Ethernet , CC-Link IE Field, CC-Link IE Basic, CC-Link IE Field Basic, Industry 4.0, IIoT, SLMP, seamless communication, Ethernet Security, Industrial Ethernet Security, Industrial Security, CLPA Working Group

Byline: Robert Miller, Director of the CLPA-Americas

Establishment of a CLPA Working Group on Industrial Ethernet Security

Recently, the IT and OT 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.

■ CC-Link IE Security Working Group (WG)

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 WG

The first step of the CLPA Security WG 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 Ethernet Security Working Group includes participation from Cisco Systems, Hilscher, Mitsubishi Electric, HMS, Belden-Hirschmann, MOXA, Panduit and MIND.

■ CC-Link Partner Association

The CC-Link Partner Association is an international open network organization founded in 2000 dedicated to the technical development and promotion of the CC-Link family of open automation networks. 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 Industry 4.0 applications due to its unmatched bandwidth. Its main activities include the development of CC-Link IE and CC-Link technical specifications, conducting of conformance tests, development support, and promotion of the CC-Link technologies. The CLPA, which began with 163 corporate members, has expanded yearly and, as of the end of 2016, boasts more than 2,800 members. 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-Americas
John Wozniak, P.E.
500 Corporate Woods Parkway
Vernon Hills, IL 60061

TEL: (847) 478-2647
E-Mail info@CCLinkAmerica.org
URL: http://am.cc-link.org/en/index.html