Industrial Control System (ICS)

THE REFERENCE MODEL OF IEC 62443-1

The term of reference model became popular in IT world since the introduction of Open Systems Interconnection (OSI) model. The OSI model split the layers of communication into 7 layers.

A couple of time after the introduction of OSI model, the Transport Control Protocol/Internet Protocol (TCP/IP) model also introduced to the public with the more simple layer segregation, it is only consist 4 layers.

Refer to U.S. NASA Office of Standards and Technology (NOST), the “reference model” is defined as: “A reference model is a framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist.”

From the Industrial Control System (ICS) point of view, a reference model describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels. IEC 62443 reference model adopting the segregation layers principle, with 5 layers in total that describe the fundamental categorization based on the functionality, interconnectivity, nature of operations and integrative approach. Following is the IEC 62443 reference model for the Industrial Control System environment including the interface with the enterprise network.

The proper layer segregation management as per shown in the previous diagram can help the organization to leverage their operations management performance and security assurance.

A similar reference model for SCADA specific system can also derived from the above diagram, following is the reference model,

THE LAYERS ENTITIES

Each layer in the reference model has specific system entities. Most of them will be integrated by networked environment but some of them may be still standalone.

For simplicity explanation of which system correlated to which layer, following is the example of the system entities for each layer,
INDUSTRIAL CONTROL SYSTEM DEFENSE-IN-DEPTH

The term defense-in-depth is explicitly depicted on the IEC 62443-1 reference model. Security management on each layer and the interconnected layers will contribute to the whole security posture of the system.

The L0 (process) is not considered as part of the ICS environment, due to the characteristic on this layer. The security management system for the ICS environment will take care L1, L2, L3 (including the interconnection between L3 & L4) and any external connection from/to third party. L4 usually is managed by business network organization, while for L0 it can be governed by the plant management procedure to ensure the security access and interface to these systems.

Based on the reference model, the security implementation of ICS environment can be implemented by using the zoning method framework. Each layer should have internal protection framework, and between layers interconnection should also have protection framework. Following is the diagram that shown the adoption of defense-in-depth framework in the ICS environment.

From the security perspective, the reference model of IEC 62443-1 has strong correlation in ensuring the security posture and protection framework. Each layer and cross layers protection management will drive the whole security posture on the ICS environment. Another emphasize is the interconnection between L3 and L4, which should be considered as the main external access gateway from the ICS environment.

Join us in “ICS Cyber Security Management System” training. Training schedule, detail syllabus and registration can be found at fedco.co.id/ics-security-training

Image source: ICS-CERT US Govt.