Roles and Responsibilities in the Security Lifecycle

Industrial Automation and Control System: Principal Roles and Responsibilities

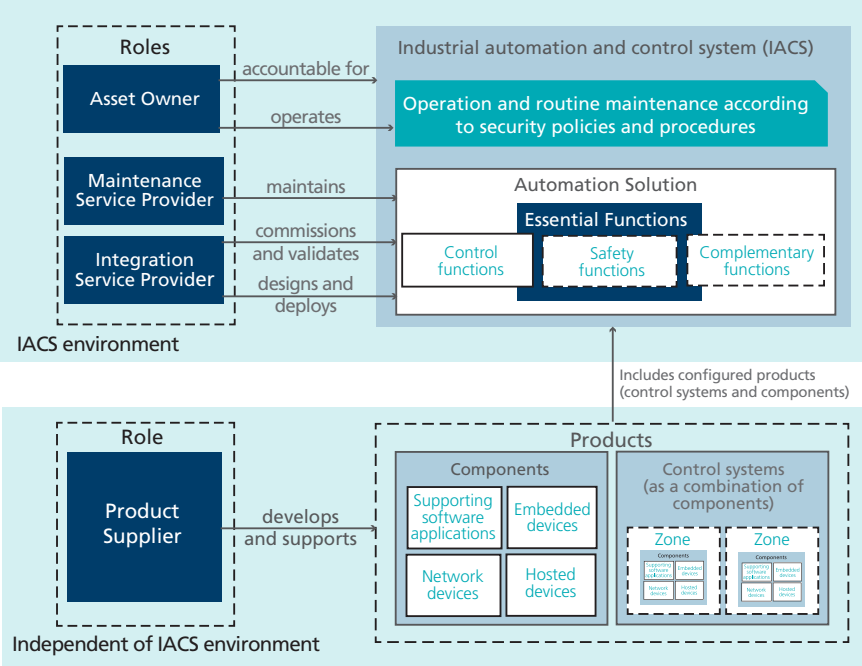

Figure 1

Principal Roles

To understand how to use the ISA/IEC 62443 Series, it is first necessary to understand the relationship between Roles, Control System, Automation Solution, and IACS. Figure 1 visualizes this relationship. The left-hand side of Figure 1 shows the roles that are identified in the ISA/IEC 62443 Series:

- **Asset Owner** is accountable and responsible for the IACS. The Asset Owner is also the operator of the IACS and the Equipment Under Control.
- **Maintenance Service Provider** provides support activities for an Automation Solution.
- **Integration Service Provider** provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover to the Asset Owner. The Integration Service Provider may also facilitate and assist in the activity to partition the System Under Consideration into Zones and Conduits and perform the Risk Assessment.
- **Product Supplier** manufactures and supports a hardware and/or software product. Products may include Control Systems, Embedded Devices, Host Devices, Network Devices, and/or Software Applications.

It is important to understand that a role is not necessarily an organization. An organization can have multiple roles, and the responsibilities for a particular role can be split among multiple organizations.

More

Security Program Throughout the Automation Solution Lifecycle

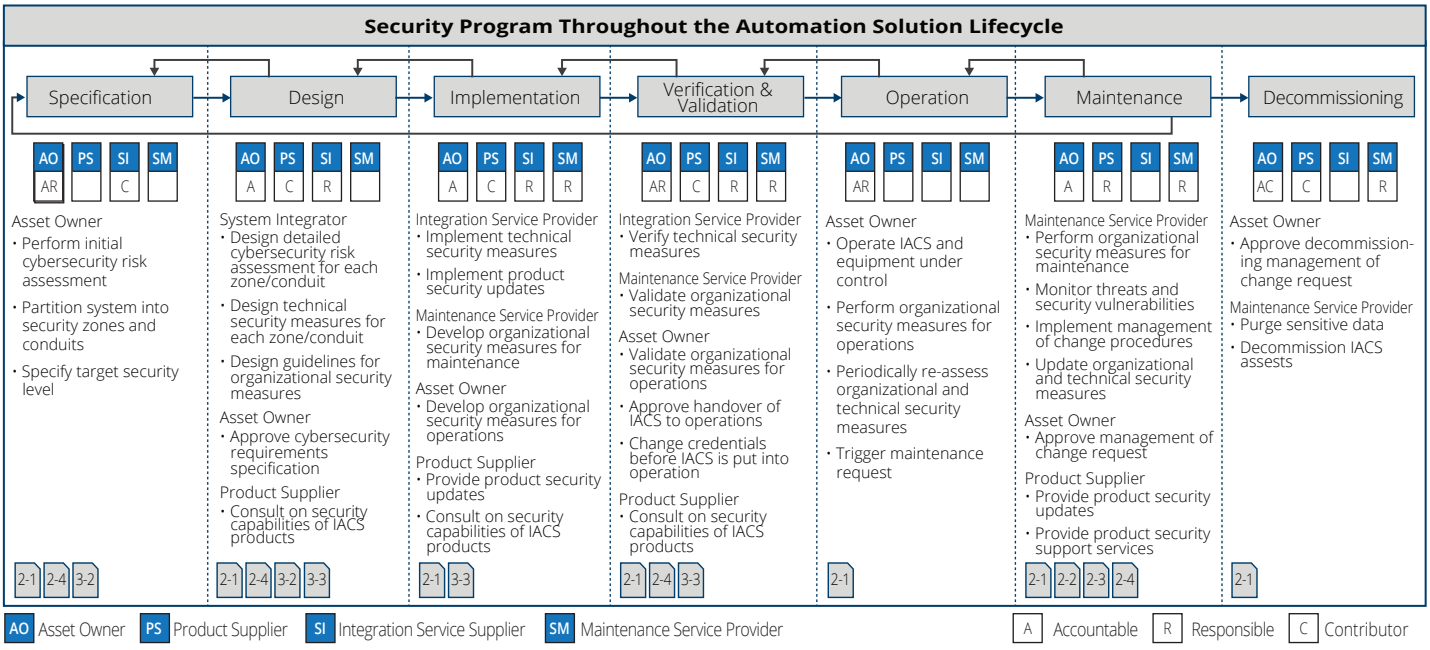

Figure 2

The Automation Solution Security Lifecycle is shown in Figure 2 and is currently documented in ISA/IEC-62443-2-2 Annex A (draft). It is based on the system lifecycle from ISO/IEC/IEEE 24748-1 – Systems and software engineering – Lifecycle management Part 1: Guidelines for lifecycle management.

Security Program

Before the Automation Solution Security Lifecycle begins, the Asset Owner must first establish the IACS Security Program for the organization. The security requirements for an Asset Owner Security Program is specified in Part 2-1 and is based on the overall security policies of the organization with consideration for the security requirements of IACS. IACS-specific security policies for the organization include, but are not limited to:

- Establishing the roles and responsibilities for Product Suppliers and Service Providers
- A risk assessment methodology that is based on the organization's risk assessment methodology and includes the consequences for an IACS failure or compromise
- The minimum set of technical and organizational security measures for IACS across the organization
- The use of IACS-specific standards and practices such as ISA/IEC 62443
- The use of IACS-specific certifications such as ISASecure®