Introduction

The subject of this standard is *security for industrial automation and control systems*. In order to address a range of applications (i.e., industry types), each of the terms in this description have been interpreted very broadly.

The term *industrial automation and control systems (IACS)* includes control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.

The term s*ecurity* is considered here to mean the prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in industrial automation and control systems. *Electronic security,* the particular focus of this standard, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

The audience for this standard includes all users of industrial automation and control systems (including facility operations, maintenance, engineering, and corporate components of user organizations), manufacturers, suppliers, government organizations involved with, or affected by, control system cyber security, control system practitioners, and security practitioners. Because mutual understanding and cooperation between information technology (IT) and operations, engineering, and manufacturing organizations is important for the overall success of any security initiative, this standard is also a reference for those responsible for the integration of industrial automation and control systems and enterprise networks.

Typical questions addressed by this Part 1 standard include:

a) What is the general scope of application for “industrial automation and control systems security”?

b) How can the needs and requirements of a security system be defined using consistent terminology?

c) What are the basic concepts that form the foundation for further analysis of the activities, system attributes, and actions that are important to provide electronically secure control systems?

d) How can the components of an industrial automation and control system be grouped or classified for the purpose of defining and managing security?

e) What are the different electronic security objectives for control system applications?

f) How can these objectives be established and codified?

Each of these questions is addressed in detail in subsequent clauses of this standard.

1 Scope

This standard defines the terminology, concepts and models for industrial automation and control systems (IACS) security. It establishes the basis for the remaining standards in the ISA99 series.

To fully articulate the systems and components the ISA99 standards address, the range of coverage may be defined and understood from several perspectives, including:

a) range of functionality included

b) specific systems and interfaces

c) criteria for selecting included activities

d) criteria for selecting included assets

Each of these is described in the following paragraphs.

Functionality Included

The scope of this standard can be described in terms of the range of functionality within an organization's information and automation systems. This functionality is typically described in terms of one or more models.

This standard is focused primarily on industrial automation and control, as described in a reference model (see clause 6). Business planning and logistics systems are not explicitly addressed within the scope of this standard, although the integrity of data exchanged between business and industrial systems is considered.

Industrial automation and control includes the supervisory control components typically found in process industries. It also includes SCADA (supervisory control and data acquisition) systems that are commonly used by organizations that operate in critical infrastructure industries. These include:

a) electricity transmission and distribution

b) gas and water distribution networks

c) oil and gas production operations

d) gas and liquid transmission pipelines

This is not an exclusive list. SCADA systems may also be found in other critical and non-critical infrastructure industries.

Systems and interfaces

In encompassing all industrial automation and control systems, this standard covers systems that can affect or influence the safe, secure, and reliable operation of industrial processes. They include, but are not limited to:

a) Industrial control systems and their associated communications networks[1], including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems, networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. (In this context, industrial control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.)

b) Associated systems at level 3 or below of the reference model described in clause 6. Examples include advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, pipeline leak detection systems, work management, outage management, and electricity energy management systems.

c) Associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

Activity-based criteria

ANSI/ISA-95.00.03 [5, Annex A] defines a set of criteria for defining activities associated with manufacturing operations. A similar list has been developed for determining the scope of this standard. A system should be considered to be within the range of coverage of these standards if the activity it performs is necessary for any of the following:

a) predictable operation of the process

b) process or personnel safety

c) process reliability or availability

d) process efficiency

e) process operability

f) product quality

g) environmental protection

h) regulatory compliance

i) product sales or custody transfer.

[1] The term “communications networks” includes all types of communications media, including various types of wireless communications. A detailed description of the use of wireless communications in industrial automation systems is beyond the scope of this standard. Wireless communication techniques are specifically mentioned only in situations where their use or application may change the nature of the security applied or required.

Asset-based criteria

The coverage of this standard includes those systems in assets that meet any of the following criteria, or whose security is essential to the protection of other assets that meet these criteria:

a) The asset has economic value to a manufacturing or operating process.

b) The asset performs a function necessary to operation of a manufacturing or operating process.

c) The asset represents intellectual property of a manufacturing or operating process.

d) The asset is necessary to operate and maintain security for a manufacturing or operating process.

e) The asset is necessary to protect personnel, contractors, and visitors involved in a manufacturing or operating process.

f) The asset is necessary to protect the environment.

g) The asset is necessary to protect the public from events caused by a manufacturing or operating process.

h) The asset is a legal requirement, especially for security purposes of a manufacturing or operating process.

i) The asset is needed for disaster recovery.

j) The asset is needed for logging security events.

This range of coverage includes systems whose compromise could result in the endangerment of public or employee health or safety, loss of public confidence, violation of regulatory requirements, loss or invalidation of proprietary or confidential information, environmental contamination, and/or economic loss or impact on an entity or on local or national security.