SYNOPSIS

DOC. ETD 18 (14664)
IS/IEC 62443-1-1: 2009

INDUSTRIAL COMMUNICATION NETWORKS – PART 1: NETWORK AND SYSTEM SECURITY – SEC 1: TERMINOLOGY, CONCEPTS AND MODELS

SCOPE:

The subject of this technical specification 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 "security" 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 IACS. Cybersecurity which is the particular focus of this technical specification, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

This part of the IS/IEC 62443 series is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.

To fully articulate the systems and components the IEC 62443 series address, the range of coverage may be defined and understood from several perspectives, including the following:
a) range of included functionality;
b) specific systems and interfaces;
c) criteria for selecting included activities;
d) criteria for selecting included assets