SYNOPSIS

DOC. ETD 18 (14668)
IS/IEC 62443-2-1: 2010

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY PART 2-1: ESTABLISHING AN INDUSTRIAL AUTOMATION AND CONTROL SYSTEM SECURITY PROGRAM

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. Cyber security 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 IS/IEC 62443 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IS/IEC 62443-1-1.
The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.