

ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems

Abstract:

The need for protecting Manufacturing and Control Systems computer environments has grown significantly over the last few years. The combination of open systems; an increase in joint ventures; alliance partners and outsourced services; growth in intelligent manufacturing equipment; increased connectivity to other equipment/software; enhanced external connectivity; along with rapidly increasing incidents of network intrusion, more intelligent hackers, and malicious software, all lead to increased threats and probability of attack. As these threats and vulnerabilities increase, so does the need for protection of Manufacturing and Control Systems.

There are numerous electronic security technologies potentially available to the Manufacturing and Control Systems environment. This document introduces several categories of electronic security technologies and discusses specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for deployment, and known strengths and weaknesses, as well as some forms of mitigation for the mentioned risks.

Introduction:

This ISA technical report provides an evaluation and assessment of many current types of electronic security technologies and tools that apply to the Manufacturing and Control Systems environment, including development, implementation, operations, maintenance, engineering and other user services. It provides guidance to manufacturers, vendors, and security practitioners at end-user companies on the technological options for securing these systems against electronic (cyber) attack. It is the first ISA technical report in a series, and deals with analyzing technologies and determining applicability to securing the Manufacturing and Control Systems environment.

This second technical report in the series will be:

- **ISA-TR99.00.02, Integrating Security into the Manufacturing and Control Systems Environment**— Includes guidance on broad policy goals and objectives, and more detailed and specific criteria, standards, and requirements to help ensure that the goals and objectives are achieved. It also provides guidance for auditing a system against the defined electronic security policy to determine security breaches or vulnerabilities, and assists in verifying compliance with security policies and procedures. It includes guidance on using metrics to measure progress, identify potential pitfalls, and potentially modify the audit procedure. ISA-TR99.00.02 calls for extensive testing and audits throughout the recommended policies and procedures and includes guidance on appropriate approaches, methodology, and metrics for these tests and audits.

Please refer to ISA-TR99.00.02 for a more comprehensive discussion of the technologies, programs, and audits and testing necessary to provide electronic security to the Manufacturing and Control Systems environment.

Following the recommended guidance in this report will not necessarily ensure that adequate electronic security is attained. It will, however, help to identify and address vulnerabilities, and to reduce the risk of undesired intrusions that could compromise confidential information or cause disruption or failure of manufacturing or control systems.

The guidance as presented in this document is general in nature, and should be applied to each system or network as appropriate by personnel knowledgeable in the manufacturing or control systems to which it is being applied. The guidance identifies those activities and actions that are typically important to provide electronically secure control systems, but whose application is not always compatible with maintenance of a system's functions. The guidance includes suggestions on appropriate application to specific control systems; however, selection of activities and practices for a given system is the responsibility of the system's owner.

It is intended that this guidance will mature and be updated over time, as experience is gained with systems vulnerability, security implementations mature, and new technologies become available. As such, while the general format of this guidance is expected to remain relatively stable, the specifics of its application and specific solutions are expected to evolve.

Scope:

This ISA technical report provides a current assessment of security tools and technologies that apply to the Manufacturing and Control Systems environment. It describes several categories of security technologies; the types of products available in those categories; the pros and cons of using those products in the Manufacturing and Control Systems environment; relative to expected threats and known vulnerabilities; along with preliminary recommendations and guidance for using those security technologies.

The concept of Manufacturing and Control Systems electronic security is applied in this ISA technical report in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and Control Systems include, but are not limited to:

- Hardware and software systems such as Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, networked electronic sensing systems, and monitoring, diagnostic, and assessment systems;
- Associated internal, human, network, or machine interfaces used to provide control, safety, maintenance, quality assurance, and other manufacturing operations functionality to continuous, batch, discrete, and combined processes.

Similarly, the concept of cyber security technologies is also broadly applied in this ISA technical report and includes, but is not limited to, the following technologies:

- Authentication and Authorization
- Filtering/Blocking/Access Control
- Encryption
- Data Validation
- Audit
- Measurement
- Monitoring and Detection Tools
- Operating Systems

In addition, a non-cyber technology—physical security control—is an essential requirement for some aspects of cyber security and is discussed in this report.

Purpose:

The purpose of this ISA technical report is to categorize and define electronic security technologies and tools currently available in order to provide a common technology basis for later technical reports and standards to be produced by the ISA-SP99 committee. Each technology in this technical report is discussed in terms of:

- Security vulnerabilities addressed by the technology
- Typical deployment
- Known issues and weaknesses
- Assessment of use in the Manufacturing and Control Systems environment
- Future directions
- Recommendations and guidance
- Information sources and reference material

The intention is to document the known state of the art of cyber security technologies applicable to the Manufacturing and Control Systems environment, clearly define which technologies can reasonably be deployed today, and define areas where more research is needed.