Introduction

This ISA technical report provides an evaluation and assessment of many current types of electronic-based cyber security technologies, mitigation methods, and tools that may apply to protecting the IACS environment from detrimental cyber intrusions and attacks. For the various technologies, methods and tools introduced in this report, a discussion of their development, implementation, operations, maintenance, engineering and other user services is provided. The report also provides guidance to manufacturers, vendors, and security practitioners at end-user companies, facilities, and industries on the technological options and countermeasures for securing automated IACSs (and their associated industrial networks) against electronic (cyber) attack.

Following the recommended guidance in this technical report will not necessarily ensure that optimized cyber security is attained for IACSs. 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 control systems and the critical infrastructure assets they automate and control. Of more concern, use of the recommendations may aid in reducing the risk of any human or environmental harm that may result after the cyber compromise of an automated control system, or its associated industrial network.

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

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

The ISA99 Series of Standards

In addition to this technical report, the ISA99 committee is developing a series of standards on cyber security for the industrial automation and control systems environment. The series includes:

1. **ANSI/ISA99.00.01-2007 – Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts and Models**

   Published in November 2007, this Part 1 standard establishes the context for all of the remaining standards in the series by defining a common set of terminology, concepts and models for electronic security in the industrial automation and control systems environment.

2. **ISA99.00.02 – Part 2: Establishing an Industrial Automation and Control System Security Program**

   Part 2, expected to be published in mid-late 2008, describes the elements of a cyber security management system and provide guidance for their application to industrial automation and control systems.

Copyright 2007 ISA. All rights reserved.

3. ISA99.00.03 – Part 3: Operating an Industrial Automation and Control System Security Program

Part 3 will address how to operate a security program after it is designed and implemented. This includes definition and application of metrics to measure program effectiveness. Work on Part 3 will begin following completion of Part 2.

4. ISA99.00.04 – Part 4: Technical Security Requirements for Industrial Automation and Control Systems

Work began in mid-2007 on the Part 4 standard, which will define the characteristics of industrial automation and control systems that differentiate them from other information technology systems from a security point of view. Based on these characteristics, the standard will establish the security requirements that are unique to this class of systems.

For information on the ISA99 series of standards, please visit www.isa.org/standards.

Copyright 2007 ISA. All rights reserved.

1 Scope

This ISA technical report provides a current assessment of various cyber security tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cyber security technologies; the types of products available in those categories; the pros and cons of using those products in the automated IACS environments relative to the expected threats and known cyber vulnerabilities; and, most important, the preliminary recommendations and guidance for using these cyber security technology products and/or countermeasures.

The concept of IACS cyber security as applied in this ISA technical report is in the broadest possible sense, encompassing all types of components, plants, facilities, and systems in all industries and critical infrastructures. IACSs include, but are not limited to:

- Hardware (e.g., data historian servers) and software systems (e.g., operating platforms, configurations, applications) 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. Inclusive in this hardware and software domain is the essential industrial network and any connected or related information technology (IT) devices and links critical to the successful operation to the control system at large. As such, this domain also includes, but is not limited to: firewalls, servers, routers, switches, gateways, fieldbus systems, intrusion detection systems, intelligent electronic/end devices, remote terminal units (RTUs), and both wired and wireless remote modems.

- Associated internal, human, network, or machine interfaces used to provide control, data logging, diagnostics, safety, monitoring, maintenance, quality assurance, regulatory compliance, auditing and other types of operational functionality for either continuous, batch, discrete, and combined processes.

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

- Authentication and Authorization
- Filtering, Blocking, and Access Control
- Encryption
- Data Validation
- Auditing
- 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.

2 Purpose

The purpose of this ISA technical report is to categorize and define cyber security technologies, countermeasures, and tools currently available to provide a common basis for later technical reports and

Copyright 2007 ISA. All rights reserved.