ANSI TECHNICAL REPORT PREPARED BY ISA

ANSI/ISA-TR99.00.01-2007

Security Technologies for Industrial Automation and Control Systems

Approved 29 October 2007

ANSI/ISA-TR99.00.01-2007
Security Technologies for Industrial Automation and Control Systems

ISBN: 978-1-934394-42-7

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ANSI/ISA-TR99.00.01-2007.

This document has been prepared as part of the service of ISA toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; Email: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA adheres to the policy of the American National Standards Institute with regard to patents. If ISA is informed of an existing patent that is required for use of the standard, it will require the owner of the patent to either grant a royalty-free license for use of the patent by users complying with the document or a license on reasonable terms and conditions that are free from unfair discrimination.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.

However, ISA asks that anyone reviewing this document who is aware of any patents that may impact implementation of the document notify the ISA Standards and Practices Department of the patent and its owner.

Additionally, the use of this document may involve hazardous materials, operations or equipment. The document cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions. The user of this document must exercise sound professional judgment concerning its use and applicability under the user's particular circumstances. The user must also consider the applicability of any governmental regulatory limitations and established safety and health practices before implementing this document.

The following served as voting members of ISA99:

NAME	COMPANY
B. Singer, Chair	FluidIQs
R. Webb, Managing Director	Consultant
E. Byres, Working Group 1 Leader	Byres Security, Inc.
R. Evans, Lead Editor	Idaho National Laboratory
R. Bhojani	Bayer Technology Services - Americas
M. Braendle	ABB
D. Brandl	BR&L Consulting, Inc.
R. Clark	Wonderware
A. Cobbett	BP Process Control Digital Protection
E. Cosman	The Dow Chemical Co.
J. Dalzon	ISA France
T. Davis	Citect
R. Derynck	Verano, Inc.
R. Forrest	The Ohio State University
J. Gilsinn	NIST
T. Glenn	Yokogawa
T. Good	DuPont Engineering
E. Hand	Sara Lee Food & Beverage
M. Heard	Eastman Chemical Co.
D. Holstein	OPUS Publishing
C. Hoover	Rockwell Automation
B. Huba	Emerson Processing Management
M. Lees	Schering-Plough Corp.
C. Mastromonico	Westinghouse Savannah River Co.
D. Mills	Procter & Gamble Co.
G. Morningstar	Cedar Rapids Water Dept.
A. Nangia	3M
J. Nye	ExxonMobil Research and Engineering
T. Phinney	Honeywell ACS Adv Tech Lab
E. Rakaczky	Invensys Process Systems
C. Sossman	Washington Safety Management Solutions LLC
L. Steinocher	Fluor Enterprises, Inc.
I. Susanto	Chevron Information Technology Co.
B. Taylor	The George Washington University
D. Teumim	Teumim Technical LLC
D. Tindill	Matrikon, Inc.
L. Uden	Lyondell Chemical Co.
J. Weiss	Applied Control Solutions, LLC
M. Widmeyer	Consultant
L. Winkel	Siemens SG

The ISA Standards and Practices Board approved the first edition of this technical report for publication on 27 August 2007.

NAME	COMPANY
T. McAvinew, Chair	Jacobs Engineering Group
M. Coppler	Ametek, Inc.
E. Cosman	The Dow Chemical Co.
B. Dumortier	Schneider Electric
D. Dunn	Aramco Services Co.

J. Gilsinn	NIST
W. Holland	Consultant
E. Icayan	ACES, Inc.
J. Jamison	Consultant
K. Lindner	Endress & Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
A. McCauley, Jr.	Chagrin Valley Controls, Inc.
G. McFarland	Emerson Process Management
R. Reimer	Rockwell Automation
N. Sands	E I du Pont
H. Sasajima	Yamatake Corp.
T. Schnaare	Rosemount, Inc.
J. Tatera	Consultant
I. Verhappen	MTL Instrument Group
R. Webb	Consultant
W. Weidman	Parsons Energy & Chemicals Group
J. Weiss	Applied Control Solutions LLC
M. Widmeyer	Consultant
M. Zielinski	Emerson Process Management

This page intentionally left blank.

Contents

Foreword

The need for protecting Industrial Automation and Control System (IACS) computer environments from malicious cyber intrusions has grown significantly over the last decade. The combination of the increased use of open systems, platforms, and protocols in the IACS environment, along with an increase in joint ventures, alliance partners and outsourcing, has lead to increased threats and a higher probability of cyber attacks. As these threats and vulnerabilities increase, the risk of a cyber attack on an industrial communication network correspondingly increases, as well as the need for protection of computer and networked-based Information Sharing and Analysis Centers. Additionally, the growth in intelligent equipment and embedded systems; increased connectivity to computer and networked equipment and software; and enhanced external connectivity coupled with rapidly increasing incidents of network intrusion, more intelligent hackers, and malicious yet easily accessible software, all add to the risk as well.

There are numerous electronic security technologies and cyber intrusion countermeasures potentially available to the IACS environment. This technical report addresses several categories of cyber security technologies and countermeasure techniques and discusses specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for their deployment, and their known strengths and weaknesses. Additionally, guidance is provided for using the various categories of security technologies and countermeasure techniques for mitigation of the above-mentioned increased risks.

This technical report does not make recommendations of one cyber security technology or mitigation method over others, but provides suggestions and guidance for using the technologies and methods, as well as information to consider when developing a site or corporate cyber security policy, program and procedures for the IACS environment.

The ISA99 standards development committee intends to update this technical report periodically to reflect new information, cyber security technologies, countermeasures, and cyber risk mitigation methods. The committee cautions the reader that following the recommended guidance in this report will not necessarily ensure that optimized cyber security is attained for the reader's industrial automation or control systems environment. It will, however, help to identify and address vulnerabilities, and to reduce the risk of undesired cyber intrusions that could compromise confidential information or, even worse, cause human and environmental harm, as well as disruption or failure of the industrial network or control systems and the industry and infrastructure critical assets they monitor and regulate.

Publication of this Registered Technical Report has been approved by the Accredited Standards Developer. This document is registered as a Technical Report series of publications according to the procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to the Accredited Standards Developer.

ActiveX®, Microsoft®, Win32®, Win32s®, and Windows® are registered trademarks of Microsoft Corporation.
ControlNet™ and EtherNet/IP™ are trademarks of ControlNet International, Inc.
CIP™ is a trademark of ODVA.
FOUNDATION Fieldbus® is a registered trademark of the Fieldbus Foundation.
Java® is a registered trademark of Sun Microsystems, Inc.
Linux® is a registered trademark of Linus Torvalds.
MODBUS® and MODBUS/TCP® are registered trademarks of Schneider Automation Inc.
OPC® is a registered trademark of OPC Foundation.
Pretty Good Privacy® and PGP® are registered trademarks of PGP Corporation.
PROFIBUS® and PROFInet® are registered trademarks of PROFIBUS User Organization.
RSA® is a registered trademark of RSA Security Inc.
UNIX® is a registered trademark of The Open Group.

This page intentionally left blank.

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.

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.

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