INL/EXT-09-15244

Control Systems Cyber Security Standards Support Activities

Robert P. Evans

January 2009

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-09-15244

Control Systems Cyber Security Standards Support Activities

Robert P. Evans

January 2009

DHS National Cyber Security Division
Control Systems Security Program
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Control Systems Cyber Security Standards Support Activities

January 2009

Homeland Security

Control Systems Security Program

National Cyber Security Division

EXECUTIVE SUMMARY

The Department of Homeland Security's Control Systems Security Program (CSSP) is working with industry to secure critical infrastructure sectors from cyber intrusions that could compromise control systems. This document describes CSSP's current activities with industry organizations in developing cyber security standards for control systems. In addition, it summarizes the standards work being conducted by organizations within the sector and provides a brief listing of sector meetings and conferences that might be of interest for each sector.

Control systems cyber security standards are part of a rapidly changing environment. The participation of CSSP in the development effort for these standards has provided consistency in the technical content of the standards while ensuring that information developed by CSSP is included.

CONTENTS

Abbreviations and Acronyms

ACC	American Chemistry Council
AGA	American Gas Association
ANL	Argonne National Laboratory
API	American Petroleum Institute
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
AWWA	American Water Works Association
CFATS	Chemical Security Anti-Terrorism Standards
CIKR	critical infrastructure and key resources
CSSP	Control Systems Security Program
DHS	Department of Homeland Security's
DoD	Department of Defense
HSPD-7	Homeland Security Presidential Directive 7
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronic Engineers
INGAA	Interstate Natural Gas Association of America
INL	Idaho National Laboratory
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
NCSD	National Cyber Security Division
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Council
NFPA	National Fire Prevention Association
NIST	National Institute of Standards and Technology
ORNL	Oak Ridge National Laboratory
PNNL	Pacific Northwest National Laboratory
PSTN	Public Switched Telecommunications Network
TC	Technical Committee
TIA	Telecommunication Industry Association
USPS	U.S. Postal Service

Control Systems Cyber Security Standards Support Activities

1. INTRODUCTION

This document summarizes the efforts being made by the Department of Homeland Security's (DHS) Control Systems Security Program (CSSP) to interface with industry on standards associated with control system security, especially in the area of cyber security. This document identifies work being done by both industry and CSSP in relation to cyber security standards for the 18 critical infrastructure and key resource (CIKR) sectors. Standards work is addressed individually for each sector as well as for cross-sector (i.e., standards work that relates to multiple sectors). CSSP is working to reduce cyber risk to critical infrastructure control systems by providing guidance and building partnerships.

1.1 Background

Homeland Security Presidential Directive 7 (HSPD-7) identifies 17 sectors of critical infrastructure and key resources vital to the United States. This was updated to 18 sectors in March 2008 with the addition of the Critical Manufacturing sector. The President designated these sectors as critical infrastructure and key resources based on the potential national impact of a terrorist attack on infrastructure functions, resources, and systems within these sectors. HSPD-7 identifies characteristics of critical infrastructures and key resources and establishes the policy to identify and protect them against terrorist acts

The DHS National Cyber Security Division (NCSD) is charged with working collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. One of NCSD's focus areas is to work with the various organizations that develop standards for the CIKR sectors. To facilitate this process, the CSSP organized the Standards Awareness Team (SAT) to work with the various standards organizations. The SAT is comprised of members from four of the Department of Energy National Laboratories (Argonne National Laboratory, Idaho National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories) and the National Institute of Standards and Technology (NIST). Members of the team have various areas of expertise, in addition to a background in standards, allowing them to interface on a technical level.

It is recognized that each of the sectors listed have numerous standards activities for various aspects of the sector operation. Only those that can be related to cyber security are addressed in this document.

1.2 Document Layout

This document provides a summary of cyber security standards activities relating to the 18 CIKR sectors. Section 2 gives an outline of CSSP activities in support of industry control system cyber security standards; Section 3 lists the 18 CIKR sectors and known cyber security standards efforts within those sectors along with an abbreviated listing of planned sector meetings of interest.

Appendix A lists industry standards that relate to cyber security.

2. CSSP CONTRIBUTIONS TO SECTOR STANDARDS ACTIVITIES

The DHS CSSP has supported several standards organizations through members of the SAT in the development of standards for industries in the 18 CIKR sectors. This work has been in five major areas: (1) cross-sector standards including government standards, (2) energy sector standards, (3) nuclear standards, (4) telecommunications standards, and (5) transportation sector standards. It should be realized that all of the CIKR sectors are interrelated and hence, many of the standards bodies, though prepared by a specific standards organization, may also apply to organizations in other sectors.

This is particularly true of cross-sector standards. These standards are designed to be applicable to any organization that uses control systems. Although other sectors may be represented on cross-sector standards organizations, the following sectors are specifically identified in the membership of one of the cross-sector standards bodies:

- Agriculture and Food
- Drinking Water and Water Treatment Systems
- Banking and Finance
- Chemical
- Commercial Facilities
- Defense Industrial Base
- Transportation

The following is a summary of CSSP standards support activities:

2.1 Cross-Sector Standards

Three standards organizations have been identified as developing cross-sector control system cyber security standards: the International Society of Automation (ISA), the NIST, and the International Electrotechnical Commission (IEC). Each cross-sector standard, along with its current status and direction, are described below.

2.1.1 International Society of Automation

Within ISA, two committees are addressing cyber security: ISA-99 (previously ISA-SP99) is developing standards for Industrial Automation and Control Systems, and ISA-100 (previously ISA-SP100) is developing standards for wireless communication with a section dealing with wireless security. Each of these standards will be comprised of multiple parts, which will be released as they are finished and approved.

2.1.1.1 ISA-99—Security for Industrial Automation and Control Systems

ISA-99, "Security for Industrial Automation and Control Systems," is currently scheduled to consist of four parts. Because ISA-99 is now working with IEC, the numbering and layout of these parts may change to conform to the IEC standards. The current layout of the ISA-99 standard is listed in Table 1.

The ISA-99 standard is designed to be general in nature and can thus be applied to any of the critical infrastructure sectors. Although it may be necessary for an organization to add specific requirements to make the standard specific to their sector or organization, the requirements in the standard can provide increased security by themselves.

ISA-99 is currently working with the IEC to make these standards into IEC 62443. Each of the ISA-99 standards would then become International Standard IEC 62443.

Table 1. Current layout of ISA-99 standards.

Document Number	Title	Status	Notes
ISA-99.01.01	Terminology, Concepts, and Models	Released Oct 2007	
ISA-99.01.02	Master Glossary	Available to ISA-99 members	Technical Report
ISA-99.01.03	Foundational Requirements	Under development	Technical Report
ISA-99.02.01	Establishing an Industrial Automation and Control Systems Security Program	Approved	Scheduled for release in early 2009
ISA-99.02.02	Operating an Industrial Automation and Control Systems Security Program	Proposed but not started	Scheduled to start 2009
ISA-99.02.03	Patch Management in the Industrial Automation and Control Systems Environment	Under development	Technical Report
ISA-99.03.01	Security Technologies for Industrial Automation and Control Systems	Released in 2007	Technical Report released as ISA-TR99.00.01-2007
ISA-99.03.02	Technical Requirements: Target Security Levels	Under development	
ISA-99.03.03	Technical Requirements: System Security Compliance Metrics	Under development	
ISA-99.03.04	Technical Requirements: Protection of Data at Rest	Under development	

Members of the SAT, representing the CSSP, have participated in the ISA-99 standards process in the following roles:

- As members of various working groups, SAT members have participated in the review of the various ISA-99 standards. Every one of the ISA-99 standards has been reviewed by at least one member of the SAT.
- SAT members have participated in the preparation of the various ISA standards. This has included preparation of various sections of ISA-99.02.02 (Operating an Industrial Automation and Control Systems Security Program) and working as the technical editor for ISA-99.03.01 (Security Technologies for Industrial Automation and Control Systems). There are SAT members on each of the ISA-99 working groups. Telecons are held for these meetings as well as face-to-face meetings.
- A SAT member is on the leadership of ISA-99.
- SAT members have presented to ISA and other functions on cyber security standards topics and conferences. These included the 54th ISA IIS, 2008 ISA EXPO and the Process Control Systems Industry Conference.

2.1.1.2 ISA-100—Wireless Systems for Automation

The ISA-100 Wireless Systems for Industrial Automation is a global wireless family of standards being developed. These standards will define a complete architecture and be open standards that will foster new development. They will give other developing protocols a platform to access many applications and systems (e.g., WiHART, Zigbee, Foundation Fieldbus, Profibus).

Six standards are currently being developed within the ISA-100 family: ISA-100.11a, "Process Applications"; ISA-100.15, "Wireless Backhaul Backbone Network"; ISA-100.14, "Trustworthy Wireless"; ISA-100.21, "People and Asset Tracking and Identification"; ISA-100.12, "WirelessHART™"; and ISA-100.11a, "Converged Network Applications." Of these standards, ISA-100.14 is the only one that directly applies to control systems security.

The ISA-100.14 working group is working, in conjunction with ISA-99, on a document describing trustworthiness in industrial wireless automation.

Members of the SAT, representing CSSP, have participated in the ISA-100 standards process in following roles:

- A member of the SAT is a co-chair of the ISA-100 Committee.
- Members of the SAT are involved with the various SP100 working groups and participate in face-to-face meetings and telecons on a regular basis.
- A member of the SAT has presented on wireless security at technical conferences around the world including: Chongqing, China; Nice, France; Ottawa, Canada; Cleveland, OH; and San Diego, CA.
- Members of the SAT are represented on the following subcommittees: ISA-100.11a, "Interoperability, Factory Automation, and Backhaul."
- A member of the SAT has worked with ISA to develop training for wireless.

2.1.1.3 Trustworthy Wireless Working Group

Trustworthy Wireless Working Group (TWWG) is a working group devoted to ensuring cyber security in wireless systems. It was originally designated as an interest group to interface between ISA-99 and ISA-100 committees. It was later elevated to a joint working group supporting the two committees.

Members of the SAT, who represent CSSP, have participated in the TWWG process in the following roles:

- A SAT member serves as the co-chair of the ISA TWWG which supports both ISA-99 and ISA-100.
- Members of the SAT have attended TWWG face-to-face meetings and are involved in the working group.

2.1.2 National Institute of Standards and Technology

NIST has developed two documents that relate to control system cyber security. While NIST standards are only binding on federal government organizations, the information contained in these documents is of great value for any organization desiring to secure their control systems from cyber intrusion.

NIST SP800-53, "Recommended Security Controls for Federal Information Systems," was developed primarily for Information Technology systems, but has been updated to address industrial control systems as well. It contains information for securing electronic systems from cyber intrusion. The standard is organized in sections or families of security categories.

NIST SP800-82, "Guide to Industrial Control Systems (ICS) Security," is a guideline for securing industrial control systems. It is organized much the same as NIST SP800-53, but focuses on industrial control systems. Release of this document is expected in early 2009.

Members of the SAT representing CSSP have participated in the NIST standards process in following roles:

- A member of the SAT is one of the leads in both the NIST SP800-53 and NIST SP800-82 efforts

- Members of the SAT provided several technical reviews of the two NIST standards.
- Members of the SAT provided technical input into the two NIST standards.

2.1.3 International Electrotechnical Commission

IEC Technical Committee 65 Working Group 10 has been tasked with the development of standard IEC 62443, “Industrial Process Measurement and Control.” IEC has essentially stopped work on this standard and has put its full effort behind the ISA-99 effort rather than developing a separate standard. The ISA-99 standard will then, after acceptance by IEC, become the IEC 62443 standard.

2.2 Power Systems Standards

Two standards organizations have been identified as developing control system cyber security standards for power systems: the IEC and the Institute of Electrical and Electronic Engineers (IEEE). These standards, along with current status and direction, are described in more detail below.

2.2.1 International Electrotechnical Commission

The IEC focuses on the electric power systems and has developed, or is in the process of developing three documents relating to the cyber security of control systems. Although the SAT has not had any direct involvement with this organization the team is trying to work with them in a review role. The IEC is considered extremely important in the international standards community and hence the SAT is making an effort to become involved.

IEC Working Group (WG) 15 of Technical Committee (TC) 57 has developed a standard, IEC 62351, “Data and Communication Security,” focusing on power system control, data communications, and security. Although this standard, which consists of seven parts, addresses information security for control of power systems.

In addition, TC 57 WG 15 has produced a technical report, IEC TR 62210, “Power system control and associated communications—Data and communication security,” which provides a method for presenting security in power system control.

IEC TC 65 WG 10 has been tasked with the development of standard IEC 62443, “Industrial Process Measurement and Control.” IEC has essentially stopped work on this standard and has put full effort behind the ISA-99 effort rather than develop a separate standard. The ISA-99 standard will then, after acceptance by IEC, become the IEC 62443 standard.

2.2.2 Institute of Electrical and Electronic Engineers

The IEEE Power Engineering Society has developed several standards that support cyber security in control systems: IEEE 1619 "Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices,” addresses data storage on disk drives; IEEE 1619.1 "Standard for Authenticated Encryption with Length Expansion for Storage Devices,” deals with data encryption on enterprise-class tape drives; IEEE Std 1686-2007, “IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities,” assists utilities in procuring IEDs that will not compromise their programs; IEEE Std 1402-2000, “IEEE Guide for Electric Power Substation Physical and Electronic Security,” provides guidelines for securing electric poser substations; and IEEE P1777 is a draft recommended practice for using wireless data communications in power systems operations.

Members of the SAT, representing the CSSP, have participated in the IEEE standards process in following roles:

- A member of the SAT is on the C2 Working Group of the IEEE Power and Energy Society’s Substations Committee for: IEEE Std 1686-2007, “IEEE Standard for Substation Intelligent

Electronic Devices (IEDs) Cyber Security Capabilities," and IEEE P1613-2003, "Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations."

- A member of the SAT has contributed to the following IEEE standards through review of the standards and discussion with standards leaders: IEEE 1451, a family of Smart Transducer Interface Standards; IEEE P1777™/D1, "Draft Recommended Practice for Using Wireless Data Communications in Power System Operations"; and "IEEE 1547, "Standard for Interconnecting Distributed Resources with Electric Power Systems."
- A member of the SAT made a presentation to the IEEE Power Engineering Society committee meetings on cyber security.

2.2.3 American Petroleum Institute

American Petroleum Institute (API) is a national trade association that represents America's oil and natural gas industry. The 400 corporate members represent all segments of the industry. Argonne National Laboratory (ANL) has taken the lead in interfacing with API through coordinating reviews of API Standard 1164, "Pipeline SCADA Security," providing technical input to the standard, and meeting with and presenting to association leaders. Members of the SAT have provided a technical review of the latest revision of the API 1164 standard.

Members of the SAT, representing CSSP, have participated in the API standards process as follows:

- Attended API Information Technology Security Forum committee meetings and presented information dealing with cyber security to committee members representing major petroleum companies.
- Attended the API Cybernetics Symposium and Committee meetings. Discussed the update of API 1164 and cyber security in the API standards. Invited to a private cybernetics committee session where SAT support was offered in the API 1164 process.
- Provided a review of API 1164. This review was acknowledged by API's Karen Simon and task lead Morgan Henrie.

2.2.4 Interstate Natural Gas Association of America

The Interstate Natural Gas Association of America (INGAA) is an association representing interstate and interprovincial natural gas pipeline companies. ANL has taken the lead in interfacing with INGAA through providing technical input to the organization, and meeting with and presenting to organization leaders.

Members of the SAT, representing CSSP, have participated in the API standards process in following roles:

- Attended an INGAA SCADA Workshop and participated in a presentation and panel discussion to assist in the standards development for cyber security.

2.3 Nuclear

The Nuclear Energy Institute (NEI) has developed NEI 04-04, Cyber Security Program for Power Reactors. There may be other standards activities, but the nuclear industry is fairly closed and information is difficult to obtain. The Nuclear Regulatory Commission (NRC) is in the process of developing a Nuclear Regulatory Guide (NUREG), which will address wireless issues.

Members of the SAT, representing CSSP, have participated in the nuclear-related standards process in following roles:

- Pacific Northwest National Laboratory (PNNL) is working with the nuclear industry in the area of standards. Oak Ridge National Laboratory (ORNL) has provided a review of the NUREG. Cross sector standards.

2.4 Telecommunications

The telecommunications industry is becoming highly dependent on wireless communications. There are several organizations such as IEEE, that are contributing to wireless communication standards. The ISA-100 (wireless) standards development effort is different in that it is also considering the security aspects of wireless communication, which fits well with the goals of the CSSP.

Members of the SAT, representing CSSP, have participated in the wireless standards process in following roles:

- A member of the SAT is a co-chair of the ISA-100 Committee.
- Members of the SAT are involved with the various ISA-100 working groups and participate in face-to-face meetings and telecons on a regular basis.
- A member of the SAT has presented on wireless security at technical conferences around the world including: Chongqing, China; Nice, France; Ottawa, Canada; Cleveland, OH; and San Diego, CA.
- Members of the SAT are represented on the following subcommittees: ISA-100.11a, "Interoperability, Factory Automation, and Backhaul."
- A member of the SAT has worked with ISA to develop training for wireless.
- A member of the SAT has supported the effort through leadership of the standard development and the IEEE wireless standards.

2.5 Transportation

Transportation industries are becoming more dependent on control systems for operation. These range from the control of passenger transportation systems to inventory tracking, to vehicle tracking to pipelines. Many of these areas, though using control systems, are not yet addressing security in their control systems. Two areas which are now considering security are passenger transportation and pipelines. Four organizations have been identified as developing standards relating to cyber security in the transportation sector; three relate to the pipeline subsector (API, AGA, and INGAA) and the other to public transportation (APTA). The American Public Transportation Association is currently developing a Recommended Practice for control system security in the public transportation subsector.

Members of the SAT, representing CSSP, are supporting transportation standards process in following roles:

- A member of the SAT has supported the standards efforts of public transportation through working group membership, standards review, and information input.
- Members of the SAT are supporting standards efforts for the petroleum and natural gas part of the pipeline subsector through standards reviews and information input to the standards.

3. INDUSTRY SUPPORT OF CYBER SECURITY STANDARDS

The United States Department of Homeland Security has designated 18 CIKR sectors, as listed in HSPD-7, modified to include the Critical Manufacturing sector. The organizations in each of these sectors have varying degrees of dependence on control systems for their operation and hence differing levels of concern with cyber intrusions into those control systems. This section considers what industry organizations are doing in each of the 18 CIKR sectors in relation to cyber security for control systems. It is realized that this may not be complete and that there are other standards activities relating to organizations within the sector, but this document only considers those standards that relate to cyber security. In addition, upcoming meetings and conferences, that relate to the each sector, which might be of interest to those involved with control systems for the sector, are included.

3.1 Food and Agriculture

No Agriculture and Food sector-specific cyber security standard activity has been identified.

The following meetings and conferences, relating to this sector have been identified:

- American Society of Agronomy and Crop Science Society of America—International Annual Meetings, November 1–5, 2009, Pittsburg, Pennsylvania

3.2 Drinking Water and Water Treatment Systems

One sector-specific security effort identified for the Drinking Water and Water Treatment Systems sector is a document addressing physical security guidelines, which is only marginally related to cyber security. This document consists of a set of voluntary guidelines, jointly developed by the American Society of Civil Engineers (ASCE) and the AWWA with technical input from the Water Environment Federation. These guidelines were created under ASCE's American National Standards Institute accredited standards development program. Titled "Guidelines for the Physical Security of Water Utilities" and "Guidelines for the Physical Security of Wastewater/Stormwater Utilities," the draft guidelines were open for public comment and trial use until June 30, 2007.

Another document is the "Roadmap to Secure Control Systems in the Water Sector." Although not a standard, the Roadmap provides a framework to address the needs for mitigating cyber security risks to industrial control systems across the water sector. This Roadmap was released in March 2008.

The following meetings and conferences, relating to this sector have been identified:

- American Water Works Association (AWWA) Water Security Congress, April 8–10, 2009, Washington, D.C.
- AWWA Annual Conference and Exposition, June 14–18, 2009, San Diego, CA
- The National Association of Clean Water Agencies, February 3–6, 2009, Atlanta, GA
- The National Association of Regulatory Utility Commissioners (NARUC), February 15–18, 2009, February 14–17, 2010, February 13–17, 2011, and February 5–8, 2012, Washington, D.C.
- WQA Aquatech USA, March 17–21, 2009, Chicago, IL

3.3 Banking and Finance

No specific cyber security standard activity has been identified for the Banking and Finance sector.

The following meetings and conferences, relating to this sector have been identified:

- National Conference for Community Bankers, February 15–18, Phoenix, AZ

- ABA Operational Risk Management Forum, April 22–24, 2009, Savannah, GA

3.4 Chemical

Soon after the terrorist attacks of September 11, 2001, ACC's member companies took the lead in securing their facilities. Members adopted the Responsible Care Security Code to enhance the security of their facilities, communities, and products. The Security Code addresses facility, cyber, and transportation security and requires companies to conduct comprehensive security vulnerability assessments of their facilities, implement security enhancements, and obtain independent verification that those enhancements have been made. The Security Code also requires companies to create security management systems, which are documented to provide quality control and assurances.

Version 3.0 of "Guidance for Addressing Cyber Security in the Chemical Industry" was released in May 2006 by the ACC's ChemITC Chemical Sector Cyber Security Program. A companion guide was released in March 2008, "Implementing a Cyber Security Management System."

A "Roadmap to Secure Control Systems in the Chemical Sector," is in the preparation process. Although it is not a standard, the Roadmap provides a framework to address the needs for mitigating cyber security risks to industrial control systems across the chemical sector. Release of the Roadmap is anticipated in 2009.

On March 6th, 2008 the House Committee on Homeland Security approved the "Chemical Anti-Terrorism Act of 2008." The ACC supports chemical security federal regulations and its member companies are working closely with the DHS to implement the Chemical Security Anti-Terrorism Standards (CFATS).

The following meetings and conferences, relating to this sector have been identified:

- ChemSecure: American Chemistry Council's (ACC) Security Conference and Exposition, April 6–8, 2009, Baltimore, MD

3.5 Commercial Facilities

No specific cyber security standard activity has been identified for the Commercial Facilities sector.

No meetings or conferences relating to control systems in this sector have been identified.

3.6 Dams, Locks, and Levees

NIST standards apply to dams, locks, and levees under Federal government control. Several NIST standards, including SP800-53, are specific to cyber security. Members of the sector, including Tennessee Valley Authority, have participated in the development and review of these standards.

The following meetings and conferences, relating to this sector have been identified:

- 2009 Northwest Hydroelectric Association (NWHA) Conference, March 17–19, 2009, Portland, OR
- United States Society on Dams, April 20–24, 2009, Nashville, TN, 2010 Conference, Sacramento, CA, and 2011 Conference, San Diego, CA
- Waterpower, July 27–30, 2009, Spokane, WA
- HydroVision, July 25–31, 2009, Spokane, WA and July 23–31, 2010, Charlotte, NC

3.7 Defense Industrial Base

No specific cyber security standard activity has been identified for the Defense Industrial Base sector.

No meetings or conferences relating to control systems in this sector have been identified.

3.8 Emergency Services

The Emergency Services sector relies highly on communication. The Telecommunications Industry Association (TIA) is developing standards dealing with communications, including between the field and control systems. These standards address control systems, wireless communication, encryption, etc.

Although the United States' National Fire Protection Association 1600, “Disaster/Emergency Management and Business Continuity Programs,” does not focus on cyber security, it does address the topic stating that it needs to be considered in disaster planning.

The following meetings and conferences, relating to this sector have been identified:

- National Fire Prevention (NFPA) World Safety Conference and Exposition®, June 8–11, 2009, Chicago, IL
- Americas’ Fire and Security Expo, July 28–30, 2009, Miami Beach, FL
- APCO International's 73rd Annual Conference and Exposition, August 16–20, 2009, Las Vegas, NV

3.9 Energy

Six industry organizations have been identified as developing cyber security standards for the Energy sector: North American Electric Reliability Corporation (NERC), IEC, IEEE, API, American Gas Association (AGA), and INGAA.

The “Roadmap to Secure Control Systems in the Energy Sector,” outlines a plan for improving cyber security in the energy sector. Although not a standard, the Roadmap provides a framework to address the needs for mitigating cyber security risks to industrial control systems across the energy sector. This Roadmap was released in January 2006.

The following meetings and conferences, relating to this sector have been identified:

- 30th Annual Energy Generation Conference, January 27, 2009, Bismarck, ND
- 2009 TechAdvantage Conference and Expo, February 1–16, 2009, New Orleans, LA
- DistribuTECH, February 3–5, 2009, San Diego, CA
- 2009 NPRA Security Conference, March 10–11, 2009, Woodlands, TX
- 2009 Power Systems Conference and Exposition, March 15–18, 2009, Seattle, WA
- Edison Electric Institute (EEI) Spring Transmission, Distribution and Metering Conference April 5–8, 2009, New Orleans, LA
- ISA POWID/EPRI Controls & Instrumentation Conference, May 12–14, 2009, Chicago, IL
- Institute of Electrical and Electronic Engineers (IEEE) Power Engineering Society (PES) General Meeting, July 26–30, 2009, Calgary, Alberta, Canada

3.10 Government Facilities

No specific cyber security standard activity has been identified for the Government Facilities sector.

No meetings or conferences relating to control systems in this sector have been identified.

3.11 Information Technology

Two standards related to the Information Technology sector have been identified: international standards developed by International Organization for Standardization (ISO), and IEC. ISO/IEC 27001, "Information Technology—Security Techniques—Information Security Management Systems—Requirements," was released October 2005. ISO/IEC 27002, "Information Technology—Code of Practice for Information Security Management," was released in June 2005 and is an update of ISO/IEC 17799. These are premier standards in the IT sector and have been used as the basis for industrial automation and control system cyber security standards.

The following meetings and conferences, relating to this sector have been identified:

- Network and Distribution System Security (NDSS) Symposium 2009, February 8–11, 2009 San Diego, CA
- RSA Conference 2009, April 20–24, 2009 San Francisco, CA
- Association of Information Technology Professionals (AITP) National Collegiate Conference, April 2–4, 2009, Oklahoma City, OK
- International Conference on Information Technology : New Generations (ITNG), April 27–29, 2009, Las Vegas, NV

3.12 Critical Manufacturing

No specific industry-related cyber security standards have been identified for the Critical Manufacturing sector.

The following meetings and conferences, relating to this sector have been identified:

- Association for Iron and Steel Technology Conference, May 4–7, 2009, St. Louis, MO, May 3–6, 2010, Pittsburg, PA, and May 2–5, 2011, Indianapolis, IN
- Society of Manufacturing Engineers (SME), February 24–26, 2009, Houston, TX

3.13 National Monuments and Icons

No specific cyber security standard activity has been identified for the National Monuments and Icons sector.

No meetings or conferences relating to control systems in this sector have been identified.

3.14 Commercial Nuclear Reactors, Materials, and Waste

The Nuclear Energy Institute (NEI) has developed NEI 04-04, Cyber Security Program for Power Reactors. There may be other standards activities, but the nuclear industry is fairly closed and information is difficult to obtain.

The Nuclear Regulatory Commission is in the process of developing a Nuclear Regulatory Guide, which will address wireless issues.

The following meetings and conferences, relating to this sector have been identified:

- American Nuclear Society (ANS) Annual Meeting, June 14–18, 2009, Atlanta, GA
- ANS Winter Meeting, November 15–19, 2009, Washington, D.C.
- Nuclear Information and Records Management (NIRMA) Conference, August 9–12, 2009, Las Vegas, NV

3.15 Postal and Shipping

No specific cyber security standard activity has been identified for the Postal and Shipping sector.

No meetings or conferences relating to control systems in this sector have been identified.

3.16 Public Health and Healthcare

No specific cyber security standard activity has been identified for the Public Health and Healthcare sector.

The following meetings and conferences, relating to this sector have been identified:

- American Public Health Association, November 7–11, 2009, Philadelphia, PA
- Public Health Preparedness Summit, February 18–20, 2009, San Diego, CA
- Federation of American Hospitals Public Policy Conference and Business Exposition, March 1–4, 2009, Washington, D.C.
- AHCA/NCAL's Quality Care Plus Annual Convention and Expo, October 4–7, 2009 Chicago, IL
- International Association for Food Protection, July 12–15, 2009, Grapevine, TX

3.17 Telecommunications

No specific cyber security standard activity has been identified for the Telecommunications sector.

The following meetings and conferences, relating to this sector have been identified:

- Utility Telecom Forum, February 9–11, 2009, Reno, NV
- Utility Telecom Council (UTC), June 1–4, 2009, Las Vegas, NV

3.18 Transportation Systems

Four organizations have been identified as developing standards relating to cyber security in the transportation sector; three relate to the pipeline subsector and the other to public transportation. The pipeline subsector organizations are API, AGA, and INGAA.

The APTA is currently developing a Recommended Practice for control system security in the public transportation subsector.

The following meetings and conferences, relating to this sector have been identified:

- FY09 FAA IT/ISS Conference, March 23, 2009 Dallas, TX
- American Petroleum Institute (API) 2009 Pipeline Conference, April 21–22, 2009, Fort Worth, TX
- Railway Age/Parsons Transportation Group 7th International Conference on Communications-Based Train Control, May 4–5, 2009, Washington, D.C.
- Railway Security Forum & Expo, January 27–28, 2009, Arlington, VA
- American Public Transportation Association (APTA) Rail Conference, June 14–18, 2009, Chicago, IL; June 6–9, 2010, Vancouver, B.C., June 12–15, 2011, Boston, MA; June 2–7, 2012, Dallas, TX; June 9–12, 2013, Philadelphia, PA
- APTA Annual Meeting, October 4–7, 2009, Orlando, FL
- Transportation Research Board Annual Meeting, January 11–15, 2009 Washington, D.C.

- 2007 ASME/IEEE Joint Rail Conference, March 3–5, 2009, Pueblo, CO
- Maritime and Port Security Conference and Expo, January 27–28, 2009, Arlington, VA
- American Road and Transportation Builders Association National Convention, October 6–9, 2009, Charleston, SC

Appendix A

Cyber Security Related Industry Standards

Appendix A—Cyber Security Related Industry Standards

The following standards (documents) are applicable to Control System cyber security:

- AGA Report No. 12, "Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan," American Gas Association, March 2006
- AGA Report No. 12, Part 2
- API Standard 1164, "Pipeline SCADA Security," September 2004
- API Security Guidelines for the Petroleum Industry, April 2005 [http://new.api.org/policy/otherissues/upload/Security.pdf]
- "Guidance for Addressing Cybersecurity in the Chemical Industry," Version 3.0, May 2006 (The Chemical Industry Data Exchange Cyber Security Initiative was consolidated into the Chemical Sector Cyber Security Program under the Chemical Information Technology Council in 2006.) [http://www.americanchemistry.com/s_rctoolkit/sec.asp?CID=1803&DID=6763]
- Chemical Facility Anti Terrorism Standard (CFATS) 6 CFR Part 27, Department of Homeland Security, April 2007 [http://edocket.access.gpo.gov/2007/E7-6363.htm]
- CIGRE B5.22, Wi-Fi Protected Access for Protection and Automation, International Council on Large Electric Systems, 2007 [http://www.cigre.org/userfiles/Publications/CATALOGUE%20of%20PUBLICATIONS%2014%20October%2008.pdf]
- FIPS PUB 140-2, Security Requirements for Cryptographic Modules, NIST, December 2002, [http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf]
- FIPS PUB 140-3 (DRAFT), Security Requirements for Cryptographic Modules, NIST, 2007 [http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf]
- IEC 61850-SER, "Communication Networks and Systems in Substations"
- IEC 60870-6, "Telecontrol Equipment and Systems Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations," (Also referred to as IEC standard TASE.2)
- IEC 62351-1, Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues, "Data and Communications Security, Introduction," May 2007
- IEC/PAS 62443-3, "Security for Industrial Process Measurement and Control," 2008
- IEC TR 62210, "Power system control and associated communications - Data and communication security," May 2003
- IEEE Std 1402-2000, "IEEE Guide for Electric Power Substation Physical and Electronic Security," January 2000
- IEEE Std 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, February 2008, [http://standards.ieee.org/standardswire/archives/sw_apr08_email.html]
- IEEE P1613-2003, Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations, 2003, [http://standards.ieee.org/reading/ieee/std_public/description/subst/1613-2003_desc.html]

- IEEE P1777/D1, Draft Recommended Practice for Using Wireless Data Communications in Power System Operations, Draft D1, February 2007, [http://www.ewh.ieee.org/soc/pes/pscc/Wireless_WG_P1777/P1777%20Recommended%20Practices-v2.pdf]
- ANSI/ISA-99.00.01-2007, "Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models," October 2007 [http://www.isa.org/Template.cfm?Section=Standards8&template=/Ecommerce/ProductDisplay.cfm&ProductID=9657]
- ISA-99.00.02-2008, "Security for Industrial Automation and Control Systems, Part 2: Establishing an Industrial Automation and Control System Security Program," December 2008
- ISA-TR99.00.01-2007, "Security Technologies for Manufacturing and Control Systems," January 2007 [http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9665]
- ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment," April 2004
- ISO/IEC 17799, "Information technology - Code of practice for information security management," June 2005
- ISO/IEC 27001, "Information technology - Security techniques - Information security management systems - Requirements," October 2005
- ISO/IEC 27002:2005, "Information technology - Code of practice for information security management," June 2005 (Redesignation of ISO/IEC 17799:2005)
- NEI 04-04 Rev 1, Review of Nuclear Energy Institute (NEI) Cyber Security Program for Nuclear Reactors, November 2005, [http://www.riskwatch.com/NEI0404ComplianceProduct.html]
- NERC Standard CIP-002 through -009, "Cyber Security," June 2006 [http://www.nerc.com/files/Reliability_Standards_Complete_Set_21Jul08.pdf]
- NERC, "Security Guidelines for the Electricity Sector: Control System - Business Network Electronic Connectivity," May 2005
- NERC, "Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment," June 2002
- NIST, "System Protection Profile – Industrial Control Systems," April 2004
- NIST, "Field Device Protection Profile for SCADA Systems in Medium Robustness Environments," Ver. 0.71, May 2006, [http://www.isd.mel.nist.gov/projects/processcontrol/FieldDevicePP/Field_Device_PP_0_71.pdf]
- NIST Special Publication 800-53 Revision 1, "Recommended Security Controls for Federal Information Systems," December 2006, Appendix F, Augmented for ICS, June 2007
- NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," FINAL PUBLIC DRAFT [http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf]