SANDIA REPORT
SAND2007-7019
Unlimited Release
November 2007

Control Systems Security Standards

Accomplishments & Impacts

Ronald Halbgewachs

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-7019
Unlimited Release
November 2007

Control Systems Security Standards

Accomplishments & Impacts

Ronald Halbgewachs
Effects-Based Studies Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1235

Abstract

The National SCADA Test Bed (NSTB) Control Systems Security Standards Team (CS^3T) has been actively participating in select Control System security-related standards groups with an emphasis on the acceleration of field-proven best practices and baseline standards for control systems. This project has utilized the expertise and capabilities of the United States Department of Energy (DOE) National Laboratories, through the support of the NSTB, to provide consistent guidance and assistance to security-related standards groups in the development of new and improved standards specifically focused on the cyber-security of energy sector control systems. The CS^3T defined three goals for the team that would lead to the needed improvements.

This report describes the accomplishments and impacts of the standards team towards achieving these three goals and describes the follow-on efforts that need to be made toward meeting the priority strategies defined in the DOE/DHS *Roadmap to Secure Control Systems in the Energy Sector*.

Acknowledgements

The author would like to acknowledge that the work that produced the results presented in this paper was funded by the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program. This report represents work accomplished by a team of personnel from four DOE National Laboratories: Sandia National Laboratories (SNL), Argonne National Laboratory (ANL), Idaho National Laboratory (INL), and Pacific Northwest National Laboratory (PNNL).

Executive Summary

The Control Systems Security Standards Team (CS^3T) has been actively participating in select Control System (CS) security-related standards groups with an emphasis on the acceleration of field-proven best practices and baseline standards for control systems. This project has utilized the expertise and capabilities of the United States Department of Energy (DOE) National Laboratories through the support of the National SCADA Test Bed (NSTB), to provide consistent guidance and assistance to security related standards groups in the development of new and improved standards specifically focused on the cyber-security of energy sector control systems.

The improvement and implementation of standards addresses three of the priority strategies described in The *Roadmap to Secure Control Systems in the Energy Sector*[1]: (1) Measure and Assess Security Posture, (2) Develop and Integrate Protective Measures, and (3) Sustain Security Improvements.

In response to the strategies under the *Roadmap*, the first goal of the CS Security Standards project has focused on the National Laboratories' participation in Control System related standards development activities and organizations that have the potential of impacting the security posture of energy infrastructure systems. The second goal has been to continue DOE and National Laboratory efforts to understand the CS security standards-related needs of the energy sector industry. The third goal has been to incorporate lessons learned from NSTB assessments and analyses, combined with best practices and expertise, in recommendations to the appropriate standards groups. Such efforts assist in providing a common cyber-security architectural foundation for the assurance of safeguarding energy systems and the survivability of the U.S. critical infrastructures.

The efforts of the CS^3T have fostered an increased awareness and understanding of the significance of increased security for control systems. These efforts have also moved the energy sector partners closer to meeting the goals and milestones defined in the strategies of the *Roadmap*. The industrial partners have, for the most part, shown a positive approach to a working relationship with the CS^3T. Future efforts should focus on the need for continuing to involve the energy sector stakeholders in developing and implementing cyber security standards in design and operation of control systems. If standards are to be accepted and implemented by operators, they must be practical, straightforward, and applicable to specific industry sector CS and SCADA operations.

This report describes (1) the accomplishments and impacts the standards team has had to date toward achieving these three goals and (2) what follow-on efforts need to be made toward meeting the goals defined in the *Roadmap*. Additional work remains in achieving the goals outlined and gaining a better understanding of the barriers, gaps, and weaknesses that exist in the implementation of CS security standards by the standards groups and industry asset owners. Once these shortfalls are determined, the NSTB CS^3T can agree on how best to assist these groups in overcoming existing problems in meeting the strategies of the *Roadmap*

[1] *Roadmap to Secure Control Systems in the Energy Sector*, DOE and DHS, January 2006.

Table of Contents

Table of Tables

1 Introduction

This section provides a brief background description of the need for the United States Department of Energy (DOE) National SCADA Test Bed (NSTB) to provide assistance to energy sector industry standards groups and asset owners in the definition and development of control system cyber-security standards specifically addressing the needs of those groups to meet the strategies and milestones defined in the *Roadmap to Secure Control Systems in the Energy Sector* [1]. Included in this section is a description of the purpose and goals of the Control Systems (CS) Security Standards Task and the benefits to be realized through these efforts.

1.1 Background

1.1.1 Description

This project has utilized the expertise and capabilities of the United States Department of Energy (DOE) National Laboratories (SNL, ANL, INL, & PNNL), through the support of the National SCADA Test Bed (NSTB), to provide consistent guidance and assistance to security-related standards groups in the development of new and improved standards specifically focused on the cyber-security of energy sector control systems.

1.1.2 Historical Information

The National Labs have been providing a unique role as an independent body to identify inconsistencies and common areas of coverage in current and emerging cyber-security standards for control systems.

1.1.3 Significance

Various programs and initiatives involving the National Laboratories within both the Department of Energy (DOE) and the Department of Homeland Security (DHS) are focusing on improving industry-wide control system cyber-security through involvement in industry-driven standards organizations. There are other related government supported efforts such as with the National Institute of Standards & Technology (NIST), Process Control Systems Forum (PCSF), and the Institute for Information Infrastructure Protection (I3P). Coordination between DOE and DHS is needed to ensure standards efforts are not being duplicated and to facilitate the sharing of products, contacts, and knowledge between the teams supporting these efforts.

1.1.4 Literature review

See Appendix E, “Cyber and Control System Security Standards”, in this document for a description of the standards considered during the work described herein.

1.2 Purpose

The purpose of this task has been to utilize the expertise and capabilities of the DOE National Laboratories (SNL, PNNL, ANL, and INL), through the support of the NSTB, to provide consistent guidance and assistance to security related standards groups in the development of new and improved standards specifically focused on the cyber-security of energy sector control systems.

1.2.1 Reasons for Investigation

With many national and international groups/organizations working on control systems security standards, coordination of these efforts is both essential and at the same time difficult. Inconsistencies in standards generated from these various groups often confuse industry and asset owners.

1.2.2 Roadmap challenges

The *Roadmap to Secure Control Systems in the Energy Sector* [1] identifies specific strategies, goals, challenges, and priorities with defined milestones for achieving secure CS for critical applications. Among them is the specific mandate that "mandatory security standards and interoperability protocols must be established and implemented to guide continuous development of … control system technology and software … Standards should be defined across the full life cycle of the control system to facilitate technology transition."

This Standards Task seeks to support the recommendations of the *Roadmap* for clearly defined cyber security standards by working with industry and stakeholders to develop consistent and effective standards.

1.2.3 Audience

The audience for this work is made up of the bodies that formulate these standards and the asset owners, industry bodies, and energy sector stakeholders to whom the standards are relevant.

1.2.4 Desired Response

New and emerging standards will produce benefits to asset owners, industry, and stakeholders within the energy sector (1) through the establishment and development of best practices in cyber security toward the protection of control systems from cyber-related events and (2) by providing a common cyber-security architectural foundation for the assurance of safeguarding energy systems and the survivability of the U.S. critical infrastructures.

Encompassed within the purpose described in Section 1.2, specific benefits realized through the implementation of this task are: (1) increased standardization of control system cyber security requirements for energy sector industries, (2) more consistent recommendations to energy sector standards organizations regarding secured practices, and (3) assistance with the implementation of these emerging standards.

1.3 Scope

1.3.1 Extent and limits of investigation

Each Laboratory participating on this task has identified standard organizations and/or vendor user/groups (see Section 3.1, Control system security standards industry partners) to develop a strategic working relationship. The team has provided standards recommendations and encouraged consistent application of cyber security standards. Specific accomplishments and impacts of the CS^{3}T are detailed later in this report (Sections 3.2 and 3.3).

This task involves an on-going effort to ensure that the DOE and DHS standards-specific programs remain integrated and leverage any work, products, contacts, and knowledge gained in the DOE/NSTB and the DHS/CSS Programs. Weekly teleconference meeting of all CS^{3}T members have assured the coordination necessary for this effort. Face-to-face team meetings were planned to coincide with occurrences of those standards group meetings that would normally be attended by members in support of such groups. Participation in these standards activities has provided visibility for the support of the DOE NSTB program and national laboratory standards efforts. Whenever possible, interactions with other government supported security standards efforts such as NIST and PCSF has been attained.

1.3.2 Goals

The NSTB Control Systems Security Standards Team (CS^{3}T) has been working to assist asset owners in maneuvering through existing cyber security standards and encouraging the development of consistent control systems cyber security standards across all critical infrastructure sectors, including the energy sector.

1.3.3 Objectives

The primary objectives of this effort have been to (1) identify ways the National Laboratories (SNL, INL, PNNL, ANL) will support standards development activities, (2) provide appropriate assistance to standards development efforts, (3) inform the standards bodies of efforts of the NSTB standards team, and (4) assist standards groups and industry to overcome barriers, gaps, and weaknesses in the implementation of CS security standards.

The first goal of the CS Security Standards task has focused on the National Laboratories' participation in Control System related standards development activities and organizations that have the potential of impacting the security posture of energy infrastructure systems.

The second goal has been to continue DOE and National Laboratory efforts to understand the CS security standards-related needs of the energy sector industry.

The third goal has been to incorporate lessons learned from NSTB assessments and analysis, combined with best practices and expertise, in recommendations to the appropriate standards groups.

— This page intentionally left blank —

2 Approach

2.1 Methods

The CS^{3}T is composed of staff members from the DOE National Laboratories: Sandia National Laboratories (SNL), Idaho National Laboratory (INL), Pacific Northwest National Laboratory (PNNL), and Argonne National Laboratory (ANL). Using their expertise and experience in process control systems within the energy sector and cyber-security requirements necessary for the protection of these industrial assets, this team works to partner with security related standards and key industry groups of the energy sector.

The technical approach taken by this team has been to actively participate in select CS security related standards groups. A list of the meetings attended by the CS^{3}T to accomplish this is provided in Appendix A. The primary objectives of this effort have been to (1) identify ways the National Laboratories (SNL, INL, PNNL, ANL) will support standards development activities, (2) provide appropriate assistance to standards development efforts, (3) inform the standards bodies of efforts of the NSTB standards team, and (4) assist standards groups and industry to overcome barriers, gaps, and weaknesses in the implementation of CS security standards.

2.2 Assumptions

There were no overt assumptions made in carrying out the work described in this report.

2.3 Procedures

The CS^{3}T attended many invitation-only meetings of relevant standards working groups in order to become recognized as possessing relevant security expertise required to safeguard the nation's control systems and to achieve partner status. In coordination with standards groups, working sub-groups, and proposed working sub-groups, the CS^{3}T provided presentations on the goals and strategies of the *Roadmap* and on the various NSTB tasks that support the efforts of improved security for the energy sector. The team has also conducted training courses on self-assessments of current security posture and security awareness. These efforts have resulted in participation in several standards efforts, which the CS^{3}T has used to advance *Roadmap* goals in the area of control systems standards.

— This page intentionally left blank —

3 Results and discussion

3.1 Control system security standards industry partners

Table 1 defines the organizations partnered with the CS Security Standards Team during this past year. This table also summarizes the current role of the standards groups, working sub-groups, or proposed working sub-groups activities and responsibilities. In coordination with these groups, the CS^{3}T provided presentations on the goals and strategies of the *Roadmap* and on the various NSTB tasks that support the efforts of improved security for the energy sector. The team has also conducted training courses on self-assessments of current security posture and security awareness.

Through these presentations and discussions, the CS^{3}T has been able to also be in contact with industry asset owners and their current corporate efforts to establish cyber-security measures within their individual organizations.

Table 1. Control System Security Standards Industry Partners

Organization	Role
AGA – American Gas Association	CS security standards group; development of standards for the natural gas industry in cyber security, protocols, and encryption
API – American Petroleum Institute	CS security standards group; cybernetics committee evaluating security standards
GTI – Gas Technology Institute	CS standards group; research, development, & training for natural gas industry
IEC – International Electrotechnical Commission	CS security standards group; responsible for two of the primary protocols used in electric industry
IEEE – Institute of Electrical and Electronics Engineers	CS security standards group; preparation of standards for power substations intelligent electronic device cyber security
INGAA – Interstate Natural Gas Association of America	The North American association represents interstate and inter-provincial natural gas pipeline companies and speaks for the companies that own and operate those lines. The INGAA is forming a working group focused on CS security issues.
ISA – Instrumentation, Systems, & Automation Society	CS security standards group; preparing a multipart standard for CS cyber security and wireless systems for automation
NERC – North American Electric Reliability Council	CS security standards group; development of CIP standards
NIST – National Institute of Standards and Technology	CS security standards group; preparing or modifying several CS standards documents
PCSF – Process Control Systems Forum	CS security standards group; coordination of PCS security efforts and transition to industry

3.2 Results of contacts and meetings

The following sections describe the accomplishments of the CS^{3}T resulting from partnering and working with the energy sector standards and industry groups described in Table 1. These accomplishments are described in terms of contacts made with the energy sector industrial standards groups and specific industry asset owners. More importantly, these sections describe the results of the contacts and meetings that progress the efforts toward meeting the goals and strategies of the *Roadmap*.

3.2.1 Contact responsibilities with CS standards organizations

One of the first tasks of the team was to determine the contact responsibilities with the possible energy sector industrial standards organizations. This approach was taken to avoid overlap of efforts, to best utilize the strengths and expertise of the team members, and to assure that all of the organizations identified were contacted. Primary assignments indicate the primary responsibility for contact, while secondary assignments indicate both backup to the primary tasking and to assist in the contact and workload effort. In some instances, for particular meetings or discussions, other Lab members would be included.

Table 2. Contact Responsibilities with CS Standards Organizations

Organization	Responsible Lab	Secondary Responsibility
American Gas Association (AGA)	ANL	PNNL
American Petroleum Institute (API)	ANL	SNL
Gas Technology Institute (GTI)	ANL	SNL
International Electrotechnical Commission (IEC)	PNNL	SNL
Interstate Natural Gas Association of America (INGAA)	ANL	SNL
Instrumentation, Systems, & Automation Society (ISA)	INL	PNNL
Institute for Electrical and Electronics Engineers (IEEE)	PNNL	SNL
National Institute of Standards and Technology (NIST)	All Labs	All Labs
North American Electric Reliability Council (NERC)	PNNL	SNL
Process Control Systems Forum (PCSF)	SNL	All Labs

3.2.2 Results of meetings and contacts with industry partners

The CS^{3}T has had great success over the past year in meeting and working with the industry partners identified in Tables 1 and 2. In some instances, meetings of the different groups have occurred at or nearly the same time, and in other instances, meetings have occurred simultaneous with conferences hosted or sponsored by I3P, PCSF, ISA, ASME, SANS, and KEMA. Multiple contact responsibilities have allowed the team to participate and respond to the meetings of all these organizations in a timely manner. It is important to note that attendance at the meetings of these industry organizations is by invitation only, since the groups are specifically established to meet the needs of the industrial asset owners and stakeholders and are often closed to non-members. Often, attendance by team members will occur only during a part of the overall organization meeting.

Accomplishments by the CS^{3}T and the impacts made on the energy sector industrial standards groups and asset owners are detailed in Section 3.3. The CS^{3}T has achieved recognition by the security standards working groups and committees within these organizations and is viewed as a critical partner for the security expertise required to safeguard their systems.

A template was created for the NSTB Standards Team members to report on any industry standards meetings attended (list of meetings attended are provided in Appendix B). The template described in Appendix C was used to collect the information and data pertinent to such meetings. Included in the information being collected are short-term and long-term needs of the standards groups and recommendations for the NSTB standards team based upon what is heard/discussed during those meetings. A Standards Meeting Report is created soon after a meeting has occurred so information is fresh and does not rely on memory months after the meeting occurred.

Presentations by team members on the role of the NSTB and CSSP programs and the key tenets, goals, and strategies of the Roadmap have been given during meetings with ISA, IEEE, NERC, IEC, AGA, API, INGAA, ASME, and PCSF. Specific contacts and discussions held during the past year with each of the industry organizations are shown in Table 3.

Table 3. Industry-specific Established Contacts

Organization	Established Contacts
AGA – American Gas Association	AGA 12: Kimberly Denbow and Dr. Bill Rush (formerly GTI)
API – American Petroleum Institute	Cybernetics Committee: Tom Frobase and Karen Simons
GTI – Gas Technology Institute	Dr. Bill Rush (formerly GTI)
IEC – International Electrotechnical Commission	TC 57 WG 15: Herb Falk, Grant Gilchrist, and Stan Klein TC 65 WG 10: Tom Phinney & Hans Daniel
IEEE – Institute of Electrical and Electronics Engineers	Samuel Sciacca
INGAA – Interstate Natural Gas Association of America	SCADA Committee: Terry Boss and Page Clark
ISA – Instrumentation, Systems, & Automation Society	SP 99 and SP100: Brian Singer, Richard Sanders, and Dan Sexton
NERC – North American Electric Reliability Council	Tom Flowers CSSWG: Marty Sidor and Linda Nappier
NIST – National Institute of Standards and Technology	Keith Stouffer and Dr. Joe Falco
PCSF - Process Control Systems Forum	David Norton and Dr. Bill Rush

Detailed interactions and accomplishments with each of these groups are summarized in the following paragraphs. In these paragraphs, only the identifiers of the standards are used; the full titles of all standards are provided in Appendix C.

AGA: Continued interaction to support the AGA 12 standards and the development of cryptographic devices with vendors. AGA (Kimberly Denbow) was provided a copy of *A Summary of Control System Security Standards Activities in the Energy Sector* [2]. Ms. Denbow has expressed an interest in seeking assistance from the CS^{3}T with the preparation of AGA Report No. 12, Part 3, "Cryptographic Protection of SCADA Communications: Protection of Network Systems", and AGA Report No. 12, Part 4, "Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components." However, this has not been a formal written request to date (see additional note in Section 3.2.3, *Future planning and contacts with industry partners*).

API: Active in communications with the API Cybernetics Committee. By attending the API Pipeline Conference and Cybernetics Symposium in April 2006, the CS^{3}T established future opportunities for CS^{3}T collaboration with API and build on their interest in the DOE NSTB programs and developments. Extending from these contacts, ANL hosted a meeting with the API Cybernetics Committee in September 2006 to elaborate on the efforts of the DOE NSTB and the work of the CS^{3}T. Finally, API provided reviewers for the DOE NSTB Peer Review program in October 2006. The CS^{3}T was requested to perform a comparison/mapping of ISA TR99-00-04 to the API 1164 requirements.

IEC: Ongoing support with Working Group (WG) 15 of the Technical Committee (TC) 57 for standards and document reviews and security training. Initialized support with TC 65 WG 10 on the development of a new standard 62443. Requests have been made by the IEC for assistance in using the NSTB test bed.

IEEE: Participated with the CI Application of Computer-Based Systems Working Group in the development of IEEE P1686.

INGAA: Long-term contacts and efforts for collaboration came to fruition in a meeting held jointly with members of the CS^{3}T in February 2007. Furthermore, tours of several asset-owner facilities (El Paso NG and Panhandle Energy NG) were arranged for the CS^{3}T. Between these two companies and their subsidiaries, nearly 74000 miles of NG pipelines, related compressor stations, interconnects, etc. are controlled. CS self-assessments and consistent methodology are the key issues with the INGAA members.

ISA: Constant contact with the SP 99 committee; working in partnership through Technical Report (TR) 99-1 and TR 99-2. Attended the ISA Expo 2006 Technical Conference in October 2006.

NERC: Continued contact with NERC for standards review and security training. The CS^{3}T provided NERC mitigation strategies to address new vulnerabilities identified by NERC members (see the NERC report *Top 10 Vulnerabilities of Control Systems and their Associated Mitigations* [4].)

NIST: The CS^{3}T (SAT) attended a NIST workshop in April 2006 to discuss NIST SP 800-53 and SP 800-82 standards documents and their applicability to control systems. From this workshop, an effort by the DHS CSSP developed a *Catalog of Control System Security Requirements* [3].

PCSF: The CS^{3}T attended the PCSF/PCSRF/I3P meetings in June 2006. A joint collaborative DHS CSSP and CS^{3}T meeting was held at the conclusion of these meetings.

3.2.3 Future planning and contacts with industry partners

AGA: The CS^{3}T plans to attend the AGA Operations Conference & Biennial Exhibition Operating Section Spring Committee Meetings to be held on April 22-26, 2007 in Grapevine (Dallas) Texas. There is a possibility of an opportunity to present information on the DOE NSTB and DHS CSSP programs and industry/multiple-laboratory collaboration in these programs. As noted in Section 3.2.2, the AGA expressed an interest in CS^{3}T assistance with AGA Report No. 12, Parts 3 & 4. If formally requested, this effort will only proceed pursuant to the availability of funds and the approval of the DOE NSTB Program Manager.

API: Additional discussions and collaborations in support of API 1164 standard review are being considered. There is a possibility of applying the *Catalog* [3] to revisit the API 1164 SCADA Security Standards and any impact to the recent release of API 1165. API 1165 is a new standard that focuses on the design and implementation of displays used for the display, monitoring, and control of information on pipeline SCADA.

GTI: Efforts are underway to establish new contacts with GTI (due to the departure of Dr. William Rush from GTI) and direct dialogue with GTI and a possible meeting during the second quarter of 2007. The goal is to determine if GTI will continue to support the AGA standards efforts.

IEC: The CS^{3}T will continue support to TC57/WG15. Based upon experiences with the authenticator, PNNL will provide processor requirements for various key update algorithms for multiple computing platforms. The CS^{3}T will also provide support to the TC65/WG10 on IEC 62443.

IEEE: The CS^{3}T will provide continued support, interaction, and technical feedback with the C1 Application of Computer-Based Systems WG in the development of IEEE P1686.

INGAA: Long-term relationships and partnering with INGAA appear positive. Possible assistance with self-assessments and reviews of vendor systems/applications and information on the *Catalog* [3] in standards development applicable to the interstate natural gas transmission pipeline are possible tasks in 2007.

ISA: The CS^{3}T will provide continued support and interaction with the Standards and Practices group (SP 99). It is anticipated members from the CS^{3}T will attend the ISA Expo 2007 Technical Conference, October 23-24 2007 in Houston, Texas.

NERC: The CS3T will provide continued support and interaction with NERC as standards reviewers and annual updates to the Top 10 Vulnerabilities [4] by the Control System Security WG (CSSWG).

NIST: Continued cooperation and collaboration between NIST and the CS^{3}T is anticipated. Attendance is planned by the CS^{3}T members at a workshop to review the *Catalog* [3], SP800-53 Revision 1, and NERC CIP comparison with SP800-53 study by MITRE. This workshop will be held on March 27-28, 2007 at the NIST facility in Gaithersburg, Maryland.

PCSF: Attendance by the CS^{3}T at the PCSF 2007 Annual Meeting, March 2007 in Atlanta, Georgia.

3.3 Impacts on energy sector industrial standards groups & asset owners

As described in the preceding sections of this report, the CS^{3}T has been working closely with many of the energy sector industrial standards groups. Through these efforts there has been a natural relationship of cooperation developed with many asset owners and representatives from the industry companies. This section describes additional accomplishments not already described in earlier sections, but also the impacts that have been achieved toward the goals and milestones of the *Roadmap* [1].

3.3.1 Accomplishments and impact with CS industry partners

The CS^{3}T has been actively participating in meetings with the technical committees, working groups, special interest groups, and cyber-security groups of the organizations listed in Table 1. Through these efforts the NSTB Standards program has been proactive in providing information on the NSTB program, the *Roadmap* efforts, and assisting these groups to define and approve standards relevant to each of the particular areas of application.

One of the greatest impacts delivered to the energy sector organizations and asset owners belonging to these organizations has been to help these groups to understand the multi-laboratory efforts and role in the DOE NSTB program and project efforts to secure control systems in the energy sector. Furthermore, the NSTB Standards team has made a concerted effort to help these organizations understand the goals and strategies of the *Roadmap*.

Some noteworthy indicators of impact realized through these efforts are:

1. Assisted in the completion of ISA TR 99-1 Revision 1, ISA 99.00.01, and ISA 99.00.02 drafts through the process of reviews and comments on the revisions to these drafts,
2. Negotiated with API to provide support in reviewing and providing input to the amendments associated with API 1164 and API 1165 standards and to provide recommendations of how best to implement these standards,
3. Provided active participation and collaboration with INGAA as this group begins to make decisions about standards applicable to their particular part of the energy sector,
4. Provided active participation and collaboration with IEC TC65/WG10 as this group develops the international standard IEC 62443,
5. Participated in the development of IEEE P1686, and
6. Continued the process of developing new contacts within each of the sector organizations.

The security standards working groups and committees within the organizations identified in Table 1 have all indicated a desire to continue working with the NSTB standards team. These groups understand the critical nature of developing security standards that will be applicable to their control systems and make a definite difference in safeguarding their systems. The DOE NSTB Standards team is viewed as a critical partner for the security expertise required.

3.3.2 Status of Security Standards

The current cyber and control system security standards are listed in Appendix C. The *2005 Summary* [2] provided a status review of all the standards listed. Rather than repeat the information contained in that report, this report will concentrate on changes in those standards that have occurred since the release of the *2005 Summary*.

AGA Report No. 12, Part 1, was issued March 14, 2006.

AGA Report No. 12, Part 2, is near completed and is pending decision from the new development SCADA Task Group for final proceedings.

IEC 62443 is a three-part international development with two standards sections and a third section to be used as a set of recommended guidelines.

ISA 99.00.01 anticipated for approval and release as a standard in 2nd quarter of 2007.

ISA 99.00.02 anticipated balloting by membership also in 2nd quarter of 2007.

NERC 1200 was put into place as an "urgent action" standard intended strictly as a temporary standard to be replaced by a permanent standard. This was not a mandatory standard but strictly voluntary.

NERC 1300 was intended to be the permanent replacement standard for NERC 1300, but as work began it was determined that a more comprehensive set of standards to be developed as a series of standards was needed, known collectively as the Critical Infrastructure Protection (CIP) standards.

NERC CIP became the official series of standards for the NERC; there are a total of nine standards currently underway CIP-001 through CIP-009. In 2006, NERC was approved as the Electric Reliability Organization (ERO).

— This page intentionally left blank —

4 Conclusions

There have been very positive changes in the development of cyber-security standards specifically focused on the control systems within the energy industrial sector. Over the past year, asset owners and the industry standards groups have come to understand the differences of reliability and safety standards for their control systems and the need for additional security incorporated into the computers, networks, controllers, and communications elements that make up the front design of these systems.

As described in the preceding sections of this report, the NSTB CS^{3}T efforts have moved the energy sector partners closer to meeting the goals and milestones defined in the strategies of the *Roadmap* [1]. For the most part, industrial standards groups and asset owners have been open to the development of partnerships and working with the DOE NSTB Program. However, such partnerships and cooperative teaming take time to build the trust necessary for these partnerships to work well.

Additional work remains in gaining a better understanding of the barriers, gaps, and weaknesses that exist in the implementation of CS security standards by the standards groups and industry asset owners. Once these shortfalls are determined, the NSTB CS^{3}T can agree on how best to assist these groups in overcoming existing problems in meeting the strategies of the *Roadmap*.

— This page intentionally left blank —

5 Recommendations

The CS^{3}T recommends that the following tasks be funded in FY07:

1. Better understanding is needed of the barriers, gaps, and weaknesses that exist in the implementation of CS security standards by the standards groups and industry asset owners. Once determined, the DOE NSTB CS Security Standards team can then determine how best to assist these groups to overcome these existing problems in meeting goals and milestones of the *Roadmap* [1]. Such efforts will assist in providing a common cyber-security architectural foundation for the assurance of safeguarding energy systems and the survivability of the U.S. critical infrastructures.

2. Continued support of the CS^{3}T for active participation in select Control System (CS) security-related standards groups with an emphasis on the acceleration of field-proven best practices and baseline standards for control systems. Focus the CS^{3}T efforts in Control System related standards development activities and organizations that have the potential of impacting the security posture of energy infrastructure systems.

3. Using the NSTB Metrics Taxonomy developed in FY06, perform a cross-walk of one selected industry control system standard to identify what metrics might be applied to each defined standard that would provide traceability from the standards definition to the implementation of elements expected to deliver protection and security. This effort would demonstrate to asset owners a means of quantifying the success of meeting security and operational goals as defined in the *Roadmap*.

— This page intentionally left blank —

Appendix A: References

[1] *Roadmap to Secure Control Systems in the Energy Sector*, Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, prepared by Energetics Incorporated, January 2006.

[2] *A Summary of Control System Security Standards Activities in the Energy Sector*, DOE Office of Electricity Delivery and Energy Reliability, October 2005.

[3] *Catalog of Control Systems Security: Recommendations for Standards Developers*, Department of Homeland Security, release date yet to be determined.

[4] *Top 10 Vulnerabilities of Control Systems and their Associated Mitigations – 2007*, NERC, February 2007.

— This page intentionally left blank —

Appendix B: Acronyms

AGA	American Gas Association
AHWG06	Ad hoc working group 06
ANL	Argonne National Laboratory
ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
CIGRE	International Council on Large Energy Systems
CIP	Critical Infrastructure Protection
CISSWG	Critical Infrastructure Security Standards Working Group
CS	Control System
CSSP	Control System Security Program
CS^3T	Control Systems Security Standards Team for the DOE NSTB
DCS	Distributed Control Systems
DHS	United States Department of Homeland Security
DOE	United States Department of Energy
ERO	Electric Reliability Organization
FERC	Federal Energy Regulatory Commission
GRI	Gas Research Institute
GTI	Gas Technology Institute
HV	High Voltage
I3P	Institute for Information Infrastructure Protection
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGT	Institute of Gas Technology
INEEL	Idaho National Engineering and Environmental Laboratory
INGAA	Interstate Natural Gas Association of America
INL	Idaho National Laboratory
ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
IT	Information Technology
MMS	ISO/IEC 9506 - Manufacturing Message Specification
NERC	North American Electric Reliability Council
NG	Natural Gas
NIST	National Institute of Standards and Technology
NSTB	National SCADA Test Bed
OE	Office of Electricity Delivery and Energy Reliability (within DOE)

PCS	Process Control System
PCSF	Process Control Security Forum
PCSRF	Process Control Security Requirements Forum
PNNL	Pacific Northwest National Laboratory
PSRC	Power Systems Relay Committee
SAT	Standards Awareness Team
SCADA	Supervisory Control and Data Acquisition
SNL	Sandia National Laboratories
SSEMP	Security Standards for Electric Market Participants
SP	Special Product
TASE.2	Telecontrol Application Service Element Two
TC	Technical Committee
TC 57	Technical Committee 57 on Power System Control and Associated Communications
TCP/IP	Transmission Control Protocol/Internet Protocol
TR	Technical Report
WAN	Wide Area Network
WG	Working Group
WG 15	Working Group 15 on Data and Communications Security

Appendix C: Meetings Attended by CS^{3}T
Funded fully or in part by NSTB
March 1, 2006 – March 28, 2007

Meeting Name	Date of Meeting	Meeting Location	Team Members
Standards Awareness Team & CISSWG Planning Meeting	February 27-28, March 1, 2006	Albuquerque, NM	Baca, Dagle, Hadley, Hammond, Robbins, Shamsuddin, Young,
NIST First FISMA CS Workshop	April 18-20, 2006	Gaithersburg, MD	Evans, Young
Instrumentation, Systems, & Automation Society (ISA) Meeting	May 7-11, 2006	Cleveland, OH	Evans
Gas Institute of Technology (GTI) Meeting	May 16, 2006	Chicago, IL	Hadley
North American Electric Reliability Council (NERC) Cyber Security Standards Education Team Meeting	May 18-19, 2006	Las Vegas, NV	Hadley
Platts 4th Annual Cyber Security Conference	May 22-24, 2006	Houston, TX	Shamsuddin
Process Controls Systems Forum (PCSF) and I3P Meeting	June 5-10, 2006	La Jolla, CA	Evans, Dagle, Hadley, Hammond, Young, Shamsuddin,
KEMA Cyber Security – Control Systems Conference	August 7-9, 2006	Portland, OR	Dagle, Hadley, McBride
Standards Awareness Team Meeting	August 9, 2006	Portland, OR	Evans, Dagle, Hadley, Halbgewachs, Hill, Hammond, Shamsuddin
International Control Systems Security & Standards Coordination Workshop	August 10-11, 2006	Portland, OR	Evans, Dagle, Hadley, Halbgewachs
American Petroleum Institute (API) Cybernetics Meeting	September 13, 2006	Argonne, IL	Hadley, Halbgewachs, Hammond
Standards Awareness Team Meeting	September 14, 2006	Argonne, IL	Hadley, Halbgewachs, Hammond
SANS Cyber Security Meeting	September 27, 2006	Las Vegas, NV	Halbgewachs, McBride
International Electrotechnical Commission (IEC) Technical Committee Working Group 57	October 10, 2006	Silver Spring, MD	McBride
NERC Control System Security WG (CSSWG)	October 12, 2006	St. Louis, MO	Dagle, Hadley
ISA SP 99 Meeting	October 15-19, 2006	Houston, TX	Evans
NSTB Peer Review Meeting	October 17-19, 2006	Arlington, VA	Hammond, Halbgewachs

North American Electric Reliability Council (NERC) Control System Security WG (CSSWG)	October 10, 2006	St. Louis, MO	Dagle, Hadley
Network Information Technology R&D – Beyond SCADA	November 8-9, 2006	Pittsburgh, PA	Shaw
American Society of Mechanical Engineers (ASME)	November 10, 2006	Chicago, IL	Shamsuddin
ISA SP 100 Workshop Meeting	February 12-15, 2007	Phoenix, AZ	Hammond
Interstate Natural Gas Association of American (INGAA) Security Meeting	February 13, 2007	Houston, TX	Halbgewachs, Hill, Shamsuddin
Institute for Information Infrastructure Protection (I3P) Meeting	February 14-15, 2007	Houston, TX	Hill, Shamsuddin
PCSF 2007 Annual Meeting	March 6-8, 2007	Atlanta, GA	Halbgewachs
IEC TC 65/WG 10 – Standard 62443	March 5 & 8-9, 2007	Atlanta, GA	Halbgewachs
NIST Second FISMA CS Workshop	March 27-28, 2007	Gaithersburg, MD	Hadley, Halbgewachs, Shamsuddin

Note: Others from the CS^{3}T may have also attended some of these meetings, but utilized funding sources other than NSTB.

NSTB CS^{3}T Members:

Ronald Halbgewachs – SNL – Team Lead

Michael Baca – SNL

Kevin Robbins – SNL

Mary Young – SNL

Jeffery Dagle – PNNL

Mark Hadley – PNNL

Justin McBride – PNNL

James Shaw – PNNL

Virgil Hammond – ANL

Shabbir Shamsuddin – ANL

Robert Evans – INL

Robert Hill – INL

Appendix D:
NSTB Standards Meeting Report Template

This template is used by the NSTB Standards Team members to report on any industry standards group meetings attended. The intent of this form is to collect the information and data pertinent to that meeting. Included in the information being collected are short-term and long-term needs of the standards groups and recommendations for the standards team based upon what is heard/discussed during those meetings. The Standards Meeting Report is to be created soon after the meeting occurred so information is fresh and does not rely on memory months after the meeting occurred.

The Standards Meeting Report is also a means of identifying issues, problems, and barriers to implementation of standards that will affect an accelerated development and implementation of consistent standards to better secure control systems in the energy sector.

Completing the template is relatively straightforward as information is transferred from notes that one would normally take at these meetings. The formatted template is simply a means of standardizing the information reported. Guidance to the Standards Team is to also include any notes to be added that do not seem to fit into any of the template categories of information.

— This page intentionally left blank —

NSTB Standards Meeting Report **< Date >**

Meeting Report
Title of Meeting

Author(s)
Name of Laboratory
Dates of Meeting
Locations of Meetings

Outline of the Report:

NSTB Standards Meeting Report **< Date >**

TITLE OF THIS MEETING

Date of meeting

Location of the meeting

The Near Term:

5.1.1 What was the purpose or goal attending this meeting?

-

5.1.2 Who was in attendance?

-

5.1.3 What are the key outcomes?

-

5.1.4 What key issues did this uncover?

-

5.1.5 What action items resulted from the meeting?

ACTION	OWNER	DUE DATE

5.1.6 What suggestions do you have for follow-up?

-

(repeat this page as necessary for multiple meetings on same trip)

THE LONGER TERM:

Any new insights into standards group/stakeholder needs?

-

Any new insights about technology trends or applications?

-

Any new insights about standards efforts?

-

Any new ideas for future standards or task development?

-

Appendix E:
Cyber and Control System Security Standards

The following standards and guidelines deal with cyber or control system security. In many cases, guidelines published by an organization are considered comparable in significance to published standards and so those guidelines are also included in this list. There are recognized differences in standards aimed at the manufacturing section, as opposed to those for energy distribution. There are also differences between technical and operating standards, and most of the cyber security standards fall into the operating standards category. Most good standards are based on best practices developed by asset owners/operators. This is not an exhaustive list of the standards, but it is believed to include those that are most relevant to energy sector control system security. These standards are listed by sector.

Electric Power

IEEE 1402-2000	*IEEE Guide for Electric Power Substation Physical and Electronic Security*, January 2000.
IEEE P1686	*Substation Intelligent Electronic Device Cyber Security Standards* (draft proposed).
IEC 60870-6	*Telecontrol Equipment and systems Part 6*. Telecontrol protocols compatible with ISO standards and ITU-T recommendations.
IEC 61850-SER	*Communication Networks and Systems in Substations*.
IEC TR62210	*Power System Control and Associated Communications – Data and Communications Security*, Report from IEC TC 57 ad-hoc WG06, May 2003.
IEC 62351-1	*Data and Communication Security, Introduction* (draft).
IEC 62443	*Security for Industrial Process Measurement and Control* (in development).
NERC CIP	*Cyber Security*, also known as CIP-001-1 through CIP-009-1, June 2006.
NERC Security Guidelines	*Security Guidelines for the Electricity Sector: Control System – Business Network Electronic Connectivity*, May 2005.
NERC Security Guidelines	*Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 2002.
FERC SSEMP	*Security Standards for Electric Market Participants (SSEMP)*.

Oil and Gas

API 1164	*Pipeline SCADA Security*, September 2004.
API 1165	*Recommended Practice for Pipeline SCADA Displays*, 1st Ed., January 2007.

API Guideline	*Security Guidelines for the Petroleum Industry, 3rd Ed.*, April 2005.
API SVA	*Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, 2nd Ed,*. October 2004.
AGA Report No. 12 Part 1	*Cryptographic Protection of SCADA Communications Background, Policies & Test Plan*
AGA Report No. 12 Part 2	*Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications*
AGA Report No. 12 Part 3	*Cryptographic Protection of SCADA Communications: Protection of Networked Systems*
AGA Report No. 12 Part 4	*Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components.*

Cross-Cut Organizations

ISA SP99.00.01	*Security for Industrial Automation and Control Systems, Part 1: Concepts, Terminology and Models,* (draft).
ISA SP99.00.02	*Security for Industrial Automation and Control Systems, Part 2: Establishing an Industrial Automation and Control System Security Program*, (draft).
ISA TR99.00.01-2004	*Technical Report: Security Technologies for Manufacturing and Control Systems*, March 2004.
ISA TR99.00.01 Rev.1	*Revision of TR99.00.01-2004*, September 2006.
ISA TR99.00.02-2004	*Technical Report: Integrating Electronic Security into Manufacturing and Control Systems Environment*, April 2004.
ISO 15408	*Common Criteria for Information Technology Security Evaluation*.
ISO 17799	*Information Technology – Code of practice for information security management*, June 2005.
ISO 27001	*Information Technology – Security Techniques – Information Security Management Systems – Requirements*, October 2005.
NIST PCSRF	*Security Capabilities Profile for Industrial Control Systems*.
NIST SPP	*System Protection Profile: Industrial Control Systems*, April 2004.
NIST SP 800-53, Rev.1	*Recommended Security Controls for Federal Information Systems*, (Rev.1 specific to Control Systems), December 2006.
NIST SP 800-82	*Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security* (draft).

Distribution:

1 MS 1368 Jennifer Depoy, 5628

1 MS 0671 Robert Pollock, 5633

1 MS 1235 Ronald Halbgewachs, 5633

1 MS 0899 Technical Library, 9536 (electronic copy)